Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3 – Opinion & Guidelines W29 EDPB – provvedimenti, trattamenti particolari

M3.1 Marketing, attività di web Marketing, Web, Fidelity Card

I pericoli di internet

Dott. Raffaele Grieco

Privacy e sicurezza sono strettamente legati

non si può avere la prima se manca la seconda

Sicurezza informatica
∩
Sicurezza fisica

(protezione di: server, PdL, sistemi di comunicazione, accessi…)

La falsa sicurezza


HOUSE
LUPICINI
Ottica

Falsi attacchi

Email inviate a me da… me stesso

("aha! ho hackerato il tuo account! ... se non mi mandi il denaro a questo indirizzo rivelerò a tutti che cosa fai col computer ...")

sfrutta la mancanza di sicurezza del protocollo SMTP

"10 ANNI INDIETRO RISPETTO A RISCHI ATTUALI". TRE REPORT SULLA SICUREZZA A CONFRONTO

"10 ANNI INDIETRO RISPETTO A RISCHI ATTUALI". TRE REPORT SULLA SICUREZZA A CONFRONTO

*(In questo articolo uscito originariamente sul canale Cyber Security di Startupitalia!, Alessia Valentini mette a confronto gli ultimi report sulle minacce cyber, tra cui anche la **Cyber Risk Management 2018 Survey** di The Innovation Group che sarà presentata al prossimo Cybersecurity Summit 2018, il 31 maggio a Milano).*

Analizzando le evidenze di tre degli ultimi report di sicurezza del 2018, il Verizon DBIR (Data Breach Investigations Report 2018), il Security Report Check Point 2018 e il Cyber Risk Management 2018 Survey di TIG (The Innovation Group), emergono dati sconfortanti sul **gap da colmare da parte delle aziende per l'attuazione di modalità di difesa dalle minacce informatiche**.

Indietro di 10 anni rispetto alle minacce attuali

Infatti, il **panorama della minaccia è attualmente caratterizzato da attacchi su larga scala (Mega attacks), multivettore, tesi a colpire qualsiasi potenziale vittima** (azienda o privato) **sufficientemente vulnerabile**. Sono stati definiti attacchi di V generazione da Check Point, a

http://channels.theinnovationgroup.it/cybersecurity/10-anni-indietro-rispetto-rischi-attuali/

"Protezione"

protezione dalla **perdita** (cancellazione)

protezione dal **breach** (spionaggio)

protezione dalla **perdita** (cancellazione)

COPIE

protezione dal **breach** (spionaggio)

CIFRATURA

Problemi per la sicurezza

- hardware
- software
- umani

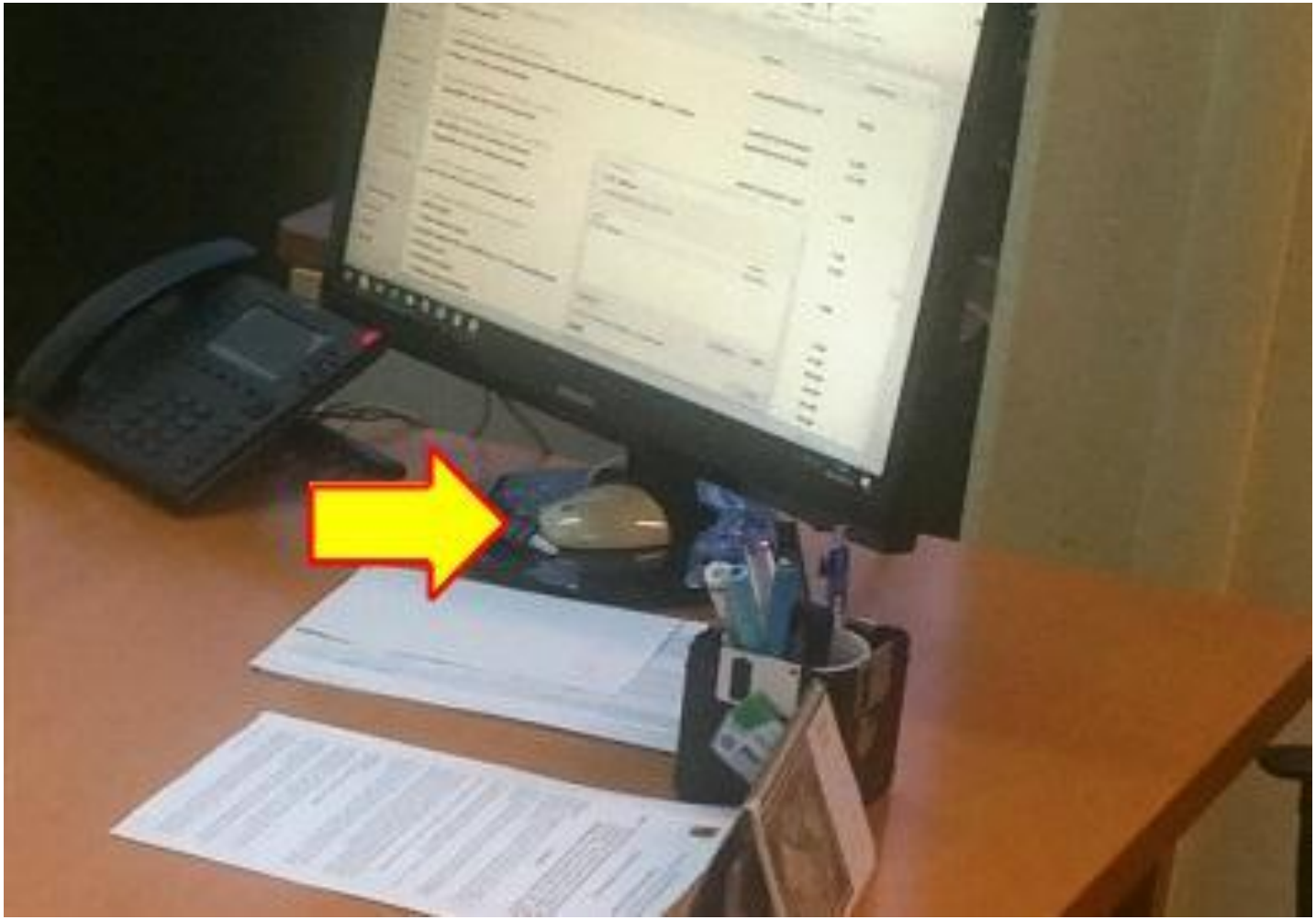
Il fattore umano è il vero problema della cybersecurity

Nuovi studi confermano che il crimine informatico non prende di mira infrastrutture critiche o vulnerabilità dei software informatici, ma le persone e le loro debolezze, per il furto di denaro e dati e per stabilire le basi per attacchi futuri.

il report completo :

www.key4biz.it/wp-content/uploads/2018/04/pfpt-us-wp-human-factor-report-2018-180425.pdf


caccia agli errori



www.punto-informatico.it/yoshitaka-sakurada-i-dont-know-what-im-doing/

Yoshitaka Sakurada, ministro incaricato per la sicurezza informatica del Giappone, dichiara di non aver mai utilizzato un computer in vita sua.

I pericoli del web

(i.e. di Internet)

anche un computer **isolato dalla rete** può essere attaccato in vari modi:

- Supporti esterni (penne USB, HD, CD, DVD…) [esempio: il virus **Stuxnet**]
- Intrusione nel sistema (cattura della password)
- attacchi hardware vari

Un attacco può portare a danneggiamenti del sistema o un **breach** (v.)

Provenienza delle minacce

- Siti web
- Email
- Social networks
- Altre fonti (peer-to-peer,…)

Tipi di minacce

- virus / malware / spyware
- script malevoli
- cookies / Flash cookies
- spam
- scam
- port scan
- intrusioni
- …

IL COMPUTER SICURO (?)

Il web (idealizzato)

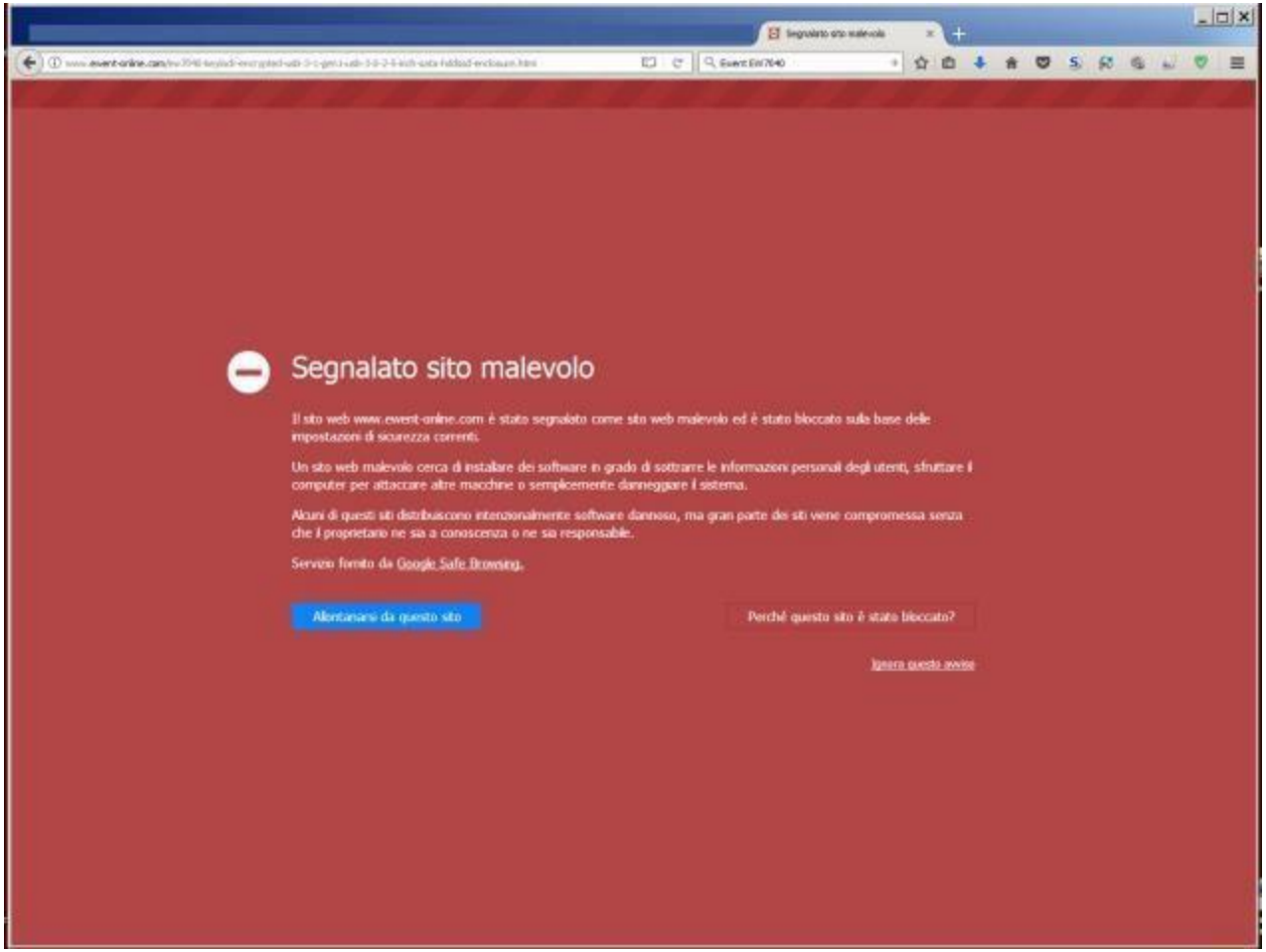
- Il **browser** manda la richiesta di una pagina a un sito
- Il **sito** risponde con il contenuto della pagina
- Inizialmente le pagine erano quasi tutte statiche; solo testo, immagini e Hyperlink…

…oggi la situazione si è complicata notevolmente;

dal sito possono arrivare contenuti non previsti e nella maggior parte dei casi non voluti.

Gli scopi sono molteplici:

- Il danno puro e semplice (virus)
- I tentativi di profilare l'utente
- Infiltrazione nel computer (p.e. per *mining*)
- Spionaggio
- ransom e truffe
- Attacchi DOS e DDOS
- …


Segnalato sito malevolo
Il sito web www.ewent-online.com è stato segnalato come sito web malevolo ed è stato bloccato sulla base delle impostazioni di sicurezza correnti.
Un sito web malevolo cerca di installare dei software in grado di sottrarre le informazioni personali degli utenti, sfruttare il computer per attaccare altre macchine o semplicemente danneggiare il sistema.
Alcuni di questi siti distribuiscono intenzionalmente software dannoso, ma gran parte dei siti viene compromessa senza che il proprietario ne sia a conoscenza o ne sia responsabile.
Servizio fornito da Google Safe Browsing.
Allontanarsi da questo sito
Perché questo sito è stato bloccato?
Ignora questo avviso

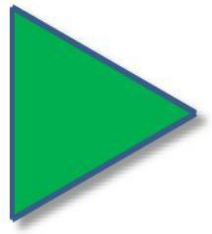

Segnalato sito malevolo
Il sito web www.ewent-online.com è stato segnalato come sito web malevolo ed è stato bloccato sulla base delle impostazioni di sicurezza correnti.
Un sito web malevolo cerca di installare dei software in grado di sottrarre le informazioni personali degli utenti, sfruttare il computer per attaccare altre macchine o semplicemente danneggiare il sistema.
Alcuni di questi siti distribuiscono intenzionalmente software dannoso, ma gran parte dei siti viene compromessa senza che il proprietario ne sia a conoscenza o ne sia responsabile.
Servizio fornito da Google Safe Browsing.
Allontanarsi da questo sito
Perché questo sito è stato bloccato?
Ignora questo avviso

globalità

Giù i servizi di Google: cosa è successo?

Alcuni servizi Google irraggiungibili per un paio d'ore, ma la causa del problema sembra essere da ricercare al di fuori del gruppo di Mountain View.

www.punto-informatico.it/giu-i-servizi-di-google-cosa-e-successo/

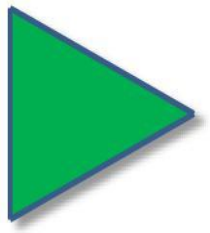


globalità

Giù i servizi di Google: cosa è successo?

Alcuni servizi Google irraggiungibili per un paio d'ore, ma la causa del problema sembra essere da ricercare al di fuori del gruppo di Mountain View.

www.punto-informatico.it/giu-i-servizi-di-google-cosa-e-successo/

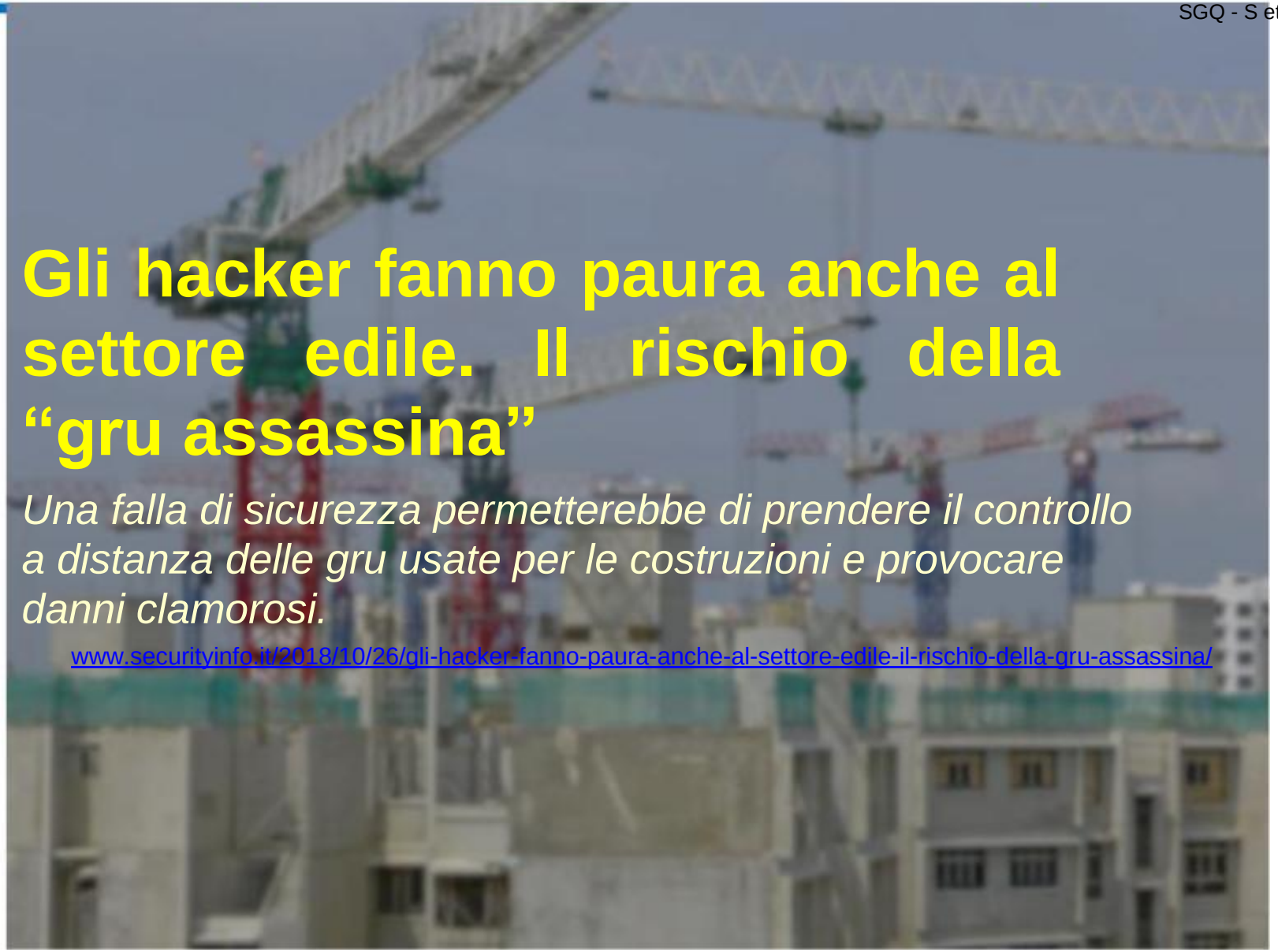


Blackout Google: colpa dell'ISP nigeriano MainOne

La posizione di MainOne

Un intoppo che ha provocato come conseguenza una reazione a catena, finendo per direzionare una parte considerevole del traffico destinato ai server di Google verso il gateway di China Telecom (partner di MainOne), transitando dall'ISP TransTelecom con base in Russia.

www.punto-informatico.it/blackout-google-responsabile-isp-nigeriano-mainone/



Gli hacker fanno paura anche al settore edile. Il rischio della "gru assassina"

Una falla di sicurezza permetterebbe di prendere il controllo a distanza delle gru usate per le costruzioni e provocare danni clamorosi.

www.securityinfo.it/2018/10/26/gli-hacker-fanno-paura-anche-al-settore-edile-il-rischio-della-gru-assassina/

Elezioni con voto elettronico, negli USA l'insicurezza del sistema è allarmante

Brian Verner, ricercatore in forza a Symantec che – incredibile ma vero – ha potuto ***comprare macchine per il voto elettronico su eBay****, come si acquista un qualsiasi smartphone. Dopo averle ricevute, le ha smontate e analizzate. "Ciò che ho trovato è allarmante"*

www.tomshw.it/altro/elezioni-con-voto-elettronico-negli-usa-linsicurezza-del-sistema-e-allarmante/

L'app di Eurosport attiva da sola servizi a pagamento. E svuota il credito a chi legge le news sull'iPhone

*Titolo forte, lo sappiamo, ma è quello che è successo in questi mesi a decine di utilizzatori dell'**applicazione** Eurosport su iPhone. Mentre utilizzavano l'**app** regolarmente scaricata dall'AppStore per leggere le notizie* ***molti utenti si sono visti consegnare un SMS di attivazione di servizi a pagamento con il classico costo di 5 euro a settimana****. Servizi inutili, soldi rubati ad utenti ignari.*

www.dday.it/redazione/28440/eurosport-app-servizi-pagamento

Nuovo attacco di phishing legato alle gift card

Con l'avvicinarsi delle feste, aumentano le truffe online che fanno riferimento ai buoni regalo.

...l'obiettivo è spingere la vittima a inviare buoni regalo al cybercriminale. Quest'ultimo sa bene che spesso le aziende chiedono ad assistenti, receptionist o agli office manager di acquistare buoni regalo per i dipendenti in vista delle feste.

www.zeusnews.it/n.php?c=26921

Visita 9.000 siti a luci rosse dall'ufficio e infetta l'intera rete aziendale

www.zeusnews.it/n.php?c=26806

California's new SB 327 law, which will take effect in January 2020, requires all **"connected devices"** to have a "reasonable security feature."
The good news is that the term "connected devices" is broadly defined to include just about everything connected to the Internet. The not-so-good news is that "reasonable security" remains defined such that companies trying to avoid compliance can argue that the law is unenforceable**.**

www.schneier.com/blog/archives/2018/11/new_iot_securit.html

Voragine di sicurezza in Kubernetes. A rischio i sistemi cloud

la vulnerabilità consente di accedere in remoto per rubare informazioni o sabotare le applicazioni. Aggiornamento disponibile, ma bisogna correre.

Una valutazione di 9.8 su 10 spiega meglio di qualsiasi altra cosa la gravità della falla di sicurezza individuata in Kubernetes, piattaforma open source che automatizza le operazioni dei container Linux.

www.securityinfo.it/2018/12/06/voragine-di-sicurezza-in-kubernetes-a-rischio-i-sistemi-cloud/

Attenzione a PHP: dal 2019 il 60% dei siti Web rischia grosso

Dal primo gennaio le versioni 5.x di PHP non otterranno più aggiornamenti per la sicurezza. Ma il numero di Web server che le usano è ancora altissimo.

www.securityinfo.it/2018/10/17/attenzione-a-php-dal-2019-il-60-dei-siti-web-rischia-grosso/

Browsing

non serve neanche cercare di connettersi solo a siti 'conosciuti'...

oltre a essere passibili di violazioni e breach,

esiste per esempio la possibilità di alterare i DNS per indirizzarci su un sito diverso da quello desiderato *(DNS spoofing)* esempio: MySpace

Attacco ai siti WordPress grazie a un bug in un plugin… per il GDPR

---

*Stiamo parlando di **WP GDPR Compliance**, un componente aggiuntivo che, almeno in teoria, dovrebbe aiutare gli amministratori di siti Internet a rispettare le regole del nuovo regolamento europeo sulla protezione dei dati.*

Il plugin, però, ha alcune falle di sicurezza che consentono di modificare le impostazioni del sito in remoto e, di conseguenza, prenderne il controllo.

www.securityinfo.it/2018/11/12/attacco-ai-siti-wordpress-grazie-a-un-bug-in-un-plugin-per-il-gdpr/

Attacco hacker a migliaia di smart TV. Sugli schermi i video di PewDiePie

TheHackerGiraffe colpisce ancora e prende di mira i dispositivi Chromecast per promuovere il canale YouTube del suo idolo.

www.securityinfo.it/2019/01/03/attacco-hacker-a-migliaia-di-smart-tv-sugli-schermi-i-video-di-pewdiepie/

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3 – Opinion & Guidelines W29 EDPB – provvedimenti, trattamenti particolari

M3.1 Marketing, attività di Web Marketing, Web, Fidelity Card

Unità didattica

M3.1.2 Motori di ricerca, Social Networks, sistemi operativi

Dott. Raffaele Grieco


Google
BIG BROTHER IS
WATCHING YOU

ovvietà

google dispone di fondi per realizzare progetti impegnativi come

- Google Maps
- Google Earth
- StreetView
- internet in Africa
- email gratis per tutti
- ...

ovvietà

1. La fonte di guadagno principale di Google (e altri…) è la vendita di **pubblicità**

2. La pubblicità *personalizzata* è molto più ricercata

3. Per personalizzare la pubblicità si viola la **privacy** e conseguentemente la **sicurezza**

Il giro d'affari della pubblicità al mondo è di

400G€

(5 volte il totale degli aiuti ai paesi poveri)

PROFILAZIONE

tentativo di raccogliere informazioni sugli utenti,
come abitudini, preferenze, scelte, storia informatica

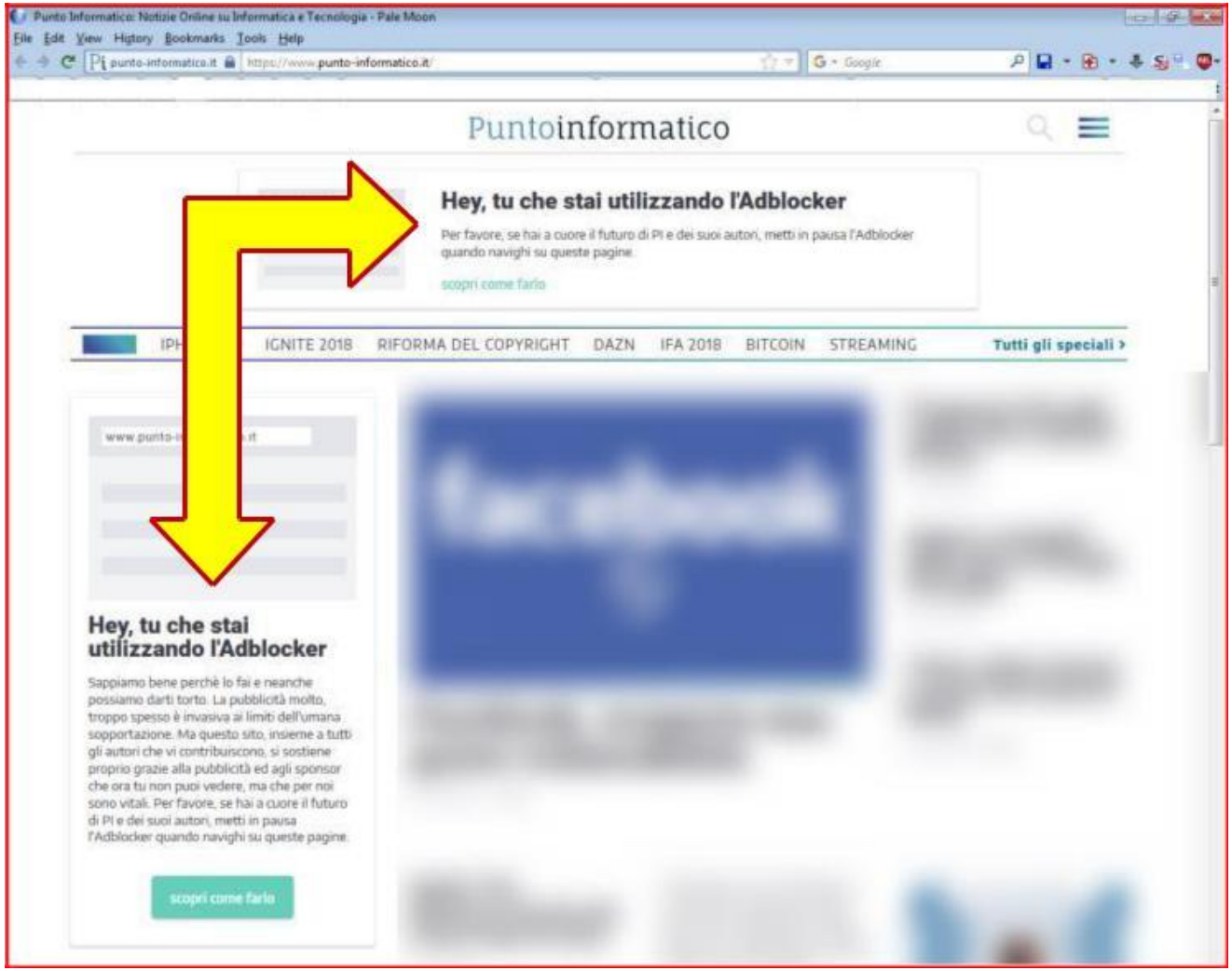
(cronologia, acquisti, "mi piace", geolocalizzazione, orari...)

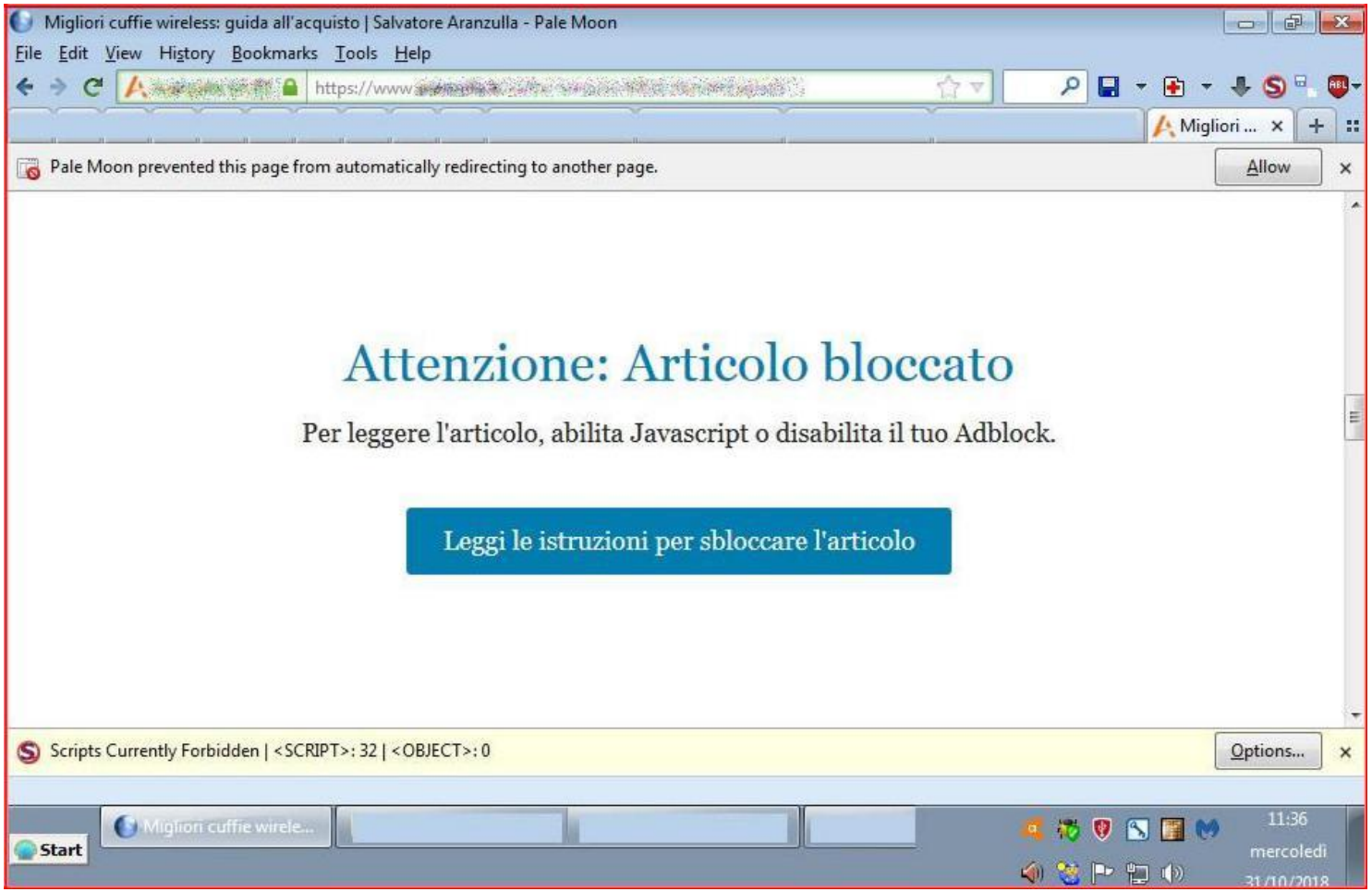
non avviene solo attraverso il PC o lo smartphone, ma anche (per esempio) attraverso le Smart TV e l'IoT

Garante Privacy:

Profilazione on line: regole chiare e più tutele per la privacy degli utenti

www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3921331

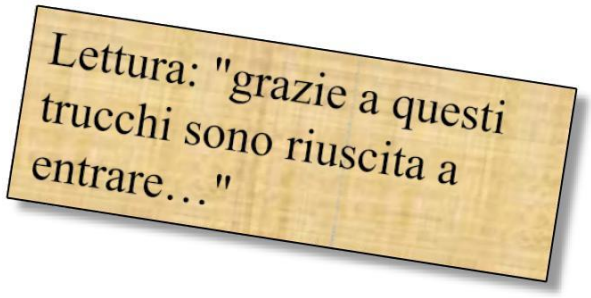

Punto Informatico: Notizie Online su Informatica e Tecnologia - Pale Moon
File Edit View History Bookmarks Tools Help
punto-informatico.it
https://www.punto-informatico.it/
Puntoinformatico
Hey, tu che stai utilizzando l'Adblocker
Per favore, se hai a cuore il futuro di PI e dei suoi autori, metti in pausa l'Adblocker quando navighi su queste pagine.
scopri come farlo
IGNITE 2018
RIFORMA DEL COPYRIGHT
DAZN
IFA 2018
BITCOIN
STREAMING
Tutti gli speciali ›
Hey, tu che stai utilizzando l'Adblocker
Sappiamo bene perchè lo fai e neanche possiamo darti torto. La pubblicità molto, troppo spesso è invasiva ai limiti dell'umana sopportazione. Ma questo sito, insieme a tutti gli autori che vi contribuiscono, si sostiene proprio grazie alla pubblicità ed agli sponsor che ora tu non puoi vedere, ma che per noi sono vitali. Per favore, se hai a cuore il futuro di PI e dei suoi autori, metti in pausa l'Adblocker quando navighi su queste pagine.
scopri come farlo


Migliori cuffie wireless: guida all'acquisto | Salvatore Aranzulla - Pale Moon
File Edit View History Bookmarks Tools Help
Migliori ...
Pale Moon prevented this page from automatically redirecting to another page.
Allow
Attenzione: Articolo bloccato
Per leggere l'articolo, abilita Javascript o disabilita il tuo Adblock.
Leggi le istruzioni per sbloccare l'articolo
Scripts Currently Forbidden | <SCRIPT>: 32 | <OBJECT>: 0
Options...
Start
11:36
mercoledì

Social networks

I social networks costituiscono:

- un doppio pericolo tecnico (locale e remoto)
- un pericolo umano locale
- un pericolo umano globale



"I social media danno diritto di parola a legioni di imbecilli che prima parlavano solo al bar dopo un bicchiere di vino, senza danneggiare la collettività. Venivano subito messi a tacere, mentre ora hanno lo stesso diritto di parola di un Premio Nobel.

È l'invasione degli imbecilli".

Umberto Eco durante una lectio magistralis a Torino

I social network ci rendono depressi?

Uno studio della University of Pennsylvania dimostra l'esistenza di un nesso tra l'utilizzo dei social e l'insorgere di stati d'animo depressivi.

www.punto-informatico.it/social-network-depressi/

Facebook, nuove accuse: spiati SMS e telefonate degli utenti

Ormai quasi non passa giorno senza che a Facebook venga attribuito qualche nuovo comportamento scorretto in materia di trattamento dei dati personali degli utenti.

Anche questa volta, la rivelazione avviene per tramite della pubblicazione dei documenti interni sequestrati dal Parlamento britannico, come nel caso di pochi giorni, quando apprendemmo che il social network a un certo punto della sua storia ha pensato di finanziarsi vendendo informazioni personali.

www.zeusnews.it/n.php?c=26893

Facebook, mail interne descrivono trucchi per raccogliere dati su SMS e chiamate di nascosto

una lettrice segnala che Facebook le aveva proposto, fra le persone che poteva conoscere, dei genitori di compagni di scuola di uno dei suoi figli, con i quali non aveva assolutamente scambiato coordinate personali.

(...) un utente aveva scaricato i propri dati da Facebook e aveva scoperto che contenevano la cronologia di tutte le sue telefonate.

www.zeusnews.it/n.php?c=26938

Facebook, accessibili le foto private di milioni di utenti

Ennesimo bug legato alla privacy nel social network.

16/12/2018

www.zeusnews.it/n.php?c=26933

15 ottobre 2018

Facebook, rubati per colpa del bug i dati personali di 15 milioni di utenti

Le conseguenze sono più gravi di quanto sembrasse inizialmente.

www.zeusnews.it//n.php?c=26767

La lista dei disastri di privacy di Facebook Questi sono solo quelli del 2018.

www.zeusnews.it/n.php?c=26978

Per Facebook non è stato un anno molto positivo, per dirla garbatamente. Stando alla compilation realizzata da Issie Lapowsky, il social network è stato al centro di almeno 21 scandali di primaria importanza nel corso del 2018.

Altroconsumo, avviata la class action contro Facebook

A sei mesi dallo scoppio dello scandalo dati Cambridge Analytica e con oltre 28mila aderenti, l'organizzazione contesta al social network la violazione della privacy e la mancata trasparenza delle informazioni al consumatore al momento della registrazione e chiede un risarcimento di oltre 285 euro per ciascun aderente, per ogni anno di registrazione Facebook.

(...) recentemente c'è stato un nuovo data breach che ha visto coinvolti almeno 50 milioni di utenti.

www.tomshw.it/altroconsumo-avviata-class-action-contro-facebook-98295

PRIVACY

Facebook ci risarcisca Al via la class action

Non bastano la scuse di Zuckerberg per l'uso improprio dei nostri dati

Zuckerberg si è scusato pubblicamente per quanto successo con Cambridge Analytica: «Le informazioni personali degli utenti sono state condivise in modo improprio». Ma le scuse non bastano. Facebook non ha fornito chiarimenti agli utenti registrati sull'uso che viene fatto dei loro dati, né dà la possibilità agli stessi utenti di scegliere consapevolmente in qualsiasi momento quali dati condividere. Una mancanza di trasparenza che fa si che molti iscritti, perlopiù in Italia, abbiano poca consapevolezza del valore, anche economico, dei propri dati personali. Più volte abbiamo chiesto a Facebook di rispondere alle nostre richieste, tra cui quella di risarcire gli utenti per queste condivisioni improprie dei loro dati. Senza ottenere risposta.

I nostri dati contano

Altroconsumo, premiato come paladino della privacy ai Big Brother Awards 2018, ha avviato una class action, insieme con le associazioni di consumatori di Belgio, Spagna e Portogallo. Chiediamo che ciascun iscritto a Facebook sia risarcito con almeno 200 euro, per l'uso improprio che il social network ha fatto dei dati in tutti questi anni.

- **Hai un account Facebook? Aderisci alla class action. Vai su** www.altroconsumo.it/azioni-collettive/facebook

AGCM: sanzione da 10M a Facebook per l'uso dei dati

L'Autorità Garante della Concorrenza e del Mercato ha sanzionato Facebook per 10 milioni di euro per l'uso dei dati degli utenti a fini commerciali.

www.punto-informatico.it/agcm-sanzione-10m-facebook-uso-dati/

7 maggio 2018

Twitter avvisa gli utenti: meglio cambiare password

Il social network dei cinguettii infatti ha comunicato ai propri utenti, circa 330 milioni, la necessità di impostare nuovamente la password, per motivi di sicurezza.

Sembrerebbe un bug o un errore interno ad aver reso le password visibili. Un dato allarmante per i responsabili sicurezza, anche se al momento non si registrano violazioni agli account.

www.domini.it/post/6381/cambiare-password-twitter/

Amnesty International affonda Twitter

Il difficile anno dei social media vede Twitter virare al ribasso a seguito delle accuse di Amnesty International sulla tossicità dei contenuti.

www.punto-informatico.it/amnesty-international-affonda-twitter

Falla in Google tenuta segreta per tre anni: segna la fine del social Google+

Il colosso di Mountain View ha sempre mantenuto il riserbo sulla vulnerabilità che metteva a rischio mezzo milione di utenti.

www.zeusnews.it/n.php?c=26753

Google+ chiude dopo aver messo a rischio i dati di 500 mila utenti

Google+ chiuderà per gli utenti privati: Google sapeva di una falla di sicurezza sul social da marzo, ma ha taciuto per non essere associata allo scandalo Cambridge Analytica che ha investito Facebook.

www.dday.it/redazione/28201/google-chiusura-dati-utenti

11-12-2018

Nuova falla in Google Plus, anticipata la data di morte

Il social network chiuderà i battenti prima del previsto.

www.zeusnews.it/n.php?c=26911

Giovanissimi in fuga da Facebook

Sempre più Instagram, Snapchat e YouTube.

www.zeusnews.it/n.php?c=26437

	2015	2018
facebook	71%	51%
instagram	50%	72%
snapchat	41%	69%

(giovani fra 13 e 17 anni)

L'app desktop di Signal lascia la chiave crittografica in chiaro

24/10/2018

Il bug consentirebbe a chiunque di decrittare con estrema facilità tutte le conversazioni attraverso il database memorizzato sul computer.

È diventata celebre quando si è scoperto che veniva usata nientemeno che da Edward Snowden,(...) che di privacy e sicurezza ha fatto un'ossessione.

la versione per PC e Mac ha infatti una "piccola" falla di sicurezza: **memorizza in chiaro** la chiave crittografica con cui vengono codificati i messaggi.

www.securityinfo.it/2018/10/24/lapp-desktop-di-signal-lascia-la-chiave-crittografica-in-chiaro

www.ilsoftware.it/articoli.asp?tag=L-app-Signal-Desktop-mostra-la-chiave-di-cifratura-in-chiaro-e-permette-di-accedere-al-database-dei-messaggi_18164

1

Android

Il sistema operativo creato da Google per gli smartphone

distribuito gratis *(Android Open Source Project)*

ma non è tutto oro eccetera

«... dispositivi cellulari più consapevoli della posizione e delle preferenze del proprietario». (Andy Rubin, cofondatore di Android inc., poi acquisita da Google)

- escono continuamente notizie su bug, vulnerabilità e altri malfunzionamenti di Android

- Google ha ammesso di usare Android per tracciare gli utenti:

www.ilcomizio.it/index.php/attualita/36-attualita/1357/si-the-big-g-ti-sta-seguendo-**google-**
ammette-di-tenere-traccia-degli-utenti-anche-quando-la-cronologia-delle-posizioni-e-disattivata

Google ammette: disattivare la cronologia delle posizioni non serve a niente

www.zeusnews.it/n.php?c=26619

Google ha ammesso di continuare a tracciare un utente tramite Google Maps nonostante il blocco imposto.

www.instanews.it/2018/08/17/google-maps-ci-spia/

Android, obbligatori due anni di patch di sicurezza. I produttori fanno comunque di testa loro

L'accordo tra Google e i produttori hardware prevede almeno quattro patch di sicurezza il primo anno; nessun obiettivo minimo per il secondo anno. Troppo poco per garantire un supporto efficiente, ma la colpa è soprattutto dei produttori.

www.dday.it/redazione/28436/android-aggiornamenti-patch-sicurezza-google

Avete un vecchio smartphone Android? Attenti al trojan AndroRAT!

www.securityinfo.it/2018/02/16/avete-un-vecchio-smartphone-android-attenti-al-trojan-androrat

sfrutta una vulnerabilità conosciuta di Android (CVE-2015-1805) individuata e corretta nel 2016.

Anche se si tratta di una vulnerabilità piuttosto “vintage”, molti dispositivi ancora in circolazione utilizzano versioni di Android per cui non è disponibile la patch.

Google ostenta ottimismo, ma i malware per Android crescono

Nel terzo trimestre 2018 sono comparse più di 3 milioni di applicazioni dannose per il sistema mobile di Google. Intanto l'azienda parla di "un sistema più sicuro".

www.securityinfo.it/2018/11/09/google-ostenta-ottimismo-ma-i-malware-per-android-crescono/

Google rimuove da Google Play 13 giochi infetti vittime del repackaging

(...) In pratica si tratta di predere un'applicazione innocua e "riconfezionarla", aggiungendovi un malware o comunque delle funzioni originariamente non previste, generalmente pensate per trarre vantaggio dagli utenti e dai loro dati.

www.zeusnews.it/n.php?c=26869

Trojan per Android ruba soldi da PayPal sotto il naso della vittima

Il malware aspetta che sia stata aperta l'app ufficiale, poi esegue il pagamento in meno di 5 secondi. Impossibile fermarlo.

www.securityinfo.it/2018/12/12/trojan-per-android-ruba-soldi-da-paypal-sotto-il-naso-della-vittima/

Violare il sistema di accesso di Android? Ci pensa Skype

Gen 08, 2019

Un bug nel software di messaggistica permette di accedere a un dispositivo con sistema Google aggirando l'inserimento del PIN.

www.securityinfo.it/2019/01/08/violare-il-sistema-di-accesso-di-android-ci-pensa-skype

Le versioni di Skype precedenti alla 8.36.0.52, rilasciata lo scorso 23 dicembre, contengono infatti un bug clamoroso, che permette di accedere a documenti, foto e applicazioni senza inserire il PIN o altri sistemi di autenticazione.

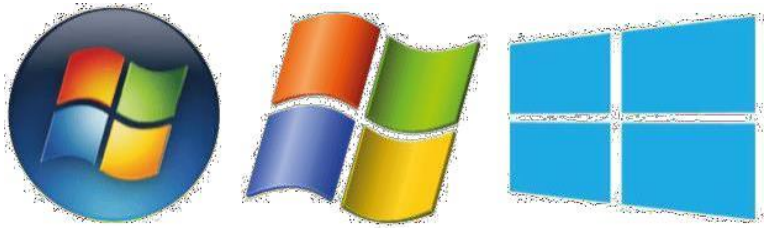
Tutto parte dal fatto che sia possibile rispondere a una chiamata Skype sul telefono anche se è in stato di blocco.

Clever Smartphone Malware Concealment Technique

www.schneier.com/blog/archives/2019/01/clever_smartpho.html

il malware si attiva solo dopo aver rilevato dati provenienti dai sensori di movimento (stabilendo così che non sta girando in un emulatore su PC)

windows



Oltre ai problemi tecnici, difetti, bug, vulnerabilità eccetera da sempre riscontrate,

- fin dalla presentazione windows 10 è stato accusato di essere uno 'spione‘
- con l’arrivo della versione 10 è stata fatta **eccezionale** pressione sugli utenti per indurli o costringerli a un upgrade

Windows 10 ci spia: come limitare il problema privacy

codexsprawl.wordpress.com/2015/08/17/windows-10-ci-spia-come-limitare-il-problema-privacy

...questo nuovo sistema operativo tra le righe della propria polizza (quellache firmiamo accettando di scaricare questa versione) dichiara:

(...)

*"**accederemo, sveleremo e conserveremo dati personali** (come i contenuti delle tue email, altre comunicazioni private o file salvati in cartelle private) quando crederemo in fede che questo sia necessario"*

Microsoft getta la spugna e ritira l'aggiornamento di ottobre per Windows 10

Troppi utenti si sono ritrovati con i file personali cancellati dopo l'update.

www.zeusnews.it/n.php?c=26749

1

Windows 10 condivide la Cronologia Attività con Microsoft. Anche senza permesso

Tutti gli utenti di Windows dovrebbero sapere che il sistema registra informazioni sul modo in cui il computer viene usato, e che queste informazioni - dietro esplicito permesso da parte dell'utente - vengono inviate a Microsoft, che le usa per «migliorare le nuove versioni di Windows».

Ciò che però fino a oggi non si sapeva è che quei dati vengono trasmessi anche quando il permesso non viene dato.

www.zeusnews.it/n.php?c=26913

Zero-Day per Windows permette di sovrascrivere qualsiasi file

Il bug è stato individuato e pubblicato da SandboxEscaper. La ricercatrice questa volta ha avvisato Microsoft con un'email.

www.securityinfo.it/2019/01/02/zero-day-per-windows-prmette-di-sovrascrivere-qualsiasi-file

La tecnica permetterebbe di mettere nel mirino qualsiasi file che normalmente non dovrebbe essere accessibile in scrittura. Un pirata informatico potrebbe sfruttarla per qualsiasi scopo, ad esempio per disabilitare il software antivirus.

BYOD

Bring Your Own Device

(*non* Bypass Your Own Defences)

Permesso di utilizzare il proprio apparecchio (smartphone, PC portatile, tablet...) per il lavoro, anche connettendolo alla rete aziendale

Banalmente potenziale vettore di enormi pericoli

Inizialmente le aziende bloccavano o proibivano l'uso del BYOD,

Arrivando anche all'estremo opposto (COPE, *corporate-owned, personally enabled*)

oggi le scelte sono più variate

adottato per esempio nella scuola italiana:

La scuola si apre al BYOD: tutti a scuola con smartphone e tablet

L'obiettivo è quello di "alleggerire" le classi da strumentazioni informatiche costose ed ingombranti

www.orizzontescuola.it/scuola-si-apre-al-byod-tutti-scuola-smartphone-e-tablet/

Come attuare il modello "Bring your own device" a scuola

www.forumpa.it/scuola-istruzione-e-ricerca/come-attuare-il-modello-bring-your-own-device-a-scuola

Sia il BYOD che il COPE hanno vantaggi e problemi

- Economia / rischi multipli
- Uniformità / aggiornamenti
- Semplificazione / complessità di gestione
- Produttività / mancanza di controllo

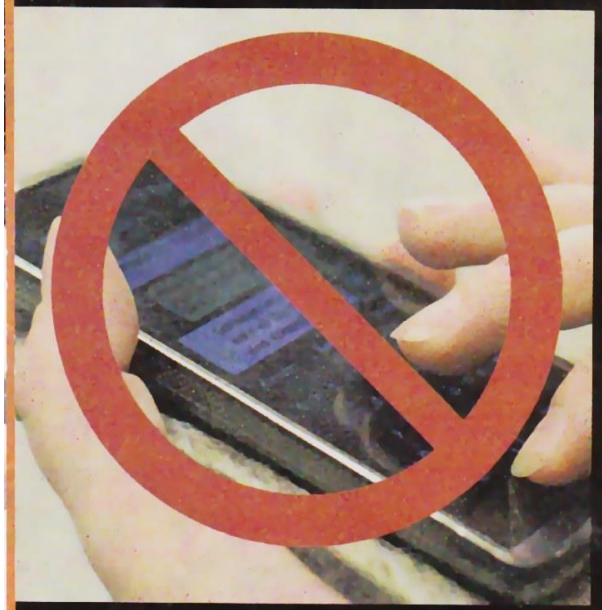
In entrambi i casi esistono strumenti e tecniche per **cercare** di limitare i pericoli

www.esecurityplanet.com/mobile-security/4-steps-to-securing-mobile-devices-and-apps-in-the-workplace-mdm-byod.html

www.lastampa.it/2013/10/17/tecnologia/dal-cloud-al-byod-ecco-le-frontiere-della-sicurezza-informatica-XkxTvlUqZxDFVQ6ySToeZN/pagina.html

www.manufacturing.net/article/2013/01/benefits-and-risks-byod

DATI SENSIBILI A RISCHIO: LE AZIENDE RIMUOVONO WHATSAPP E FACEBOOK DAGLI SMARTPHONE DEI DIPENDENTI



#HACKING **Sempre più aziende americane disinstallano le app social dagli smartphone usati dai propri dipendenti. Il rischio di fornire informazioni aziendali riservate attraverso le chat è infatti ritenuto molto alto**

Negli ultimi anni negli USA sempre più aziende forniscono in comodato d'uso lo smartphone aziendale al dipendente, chiedendo di usarlo anche come proprio dispositivo personale in modo da poter essere sempre reperibile. Da qualche tempo però i responsabili della sicurezza hanno preso di mira le app che utilizzano connessioni non protette e che sono quindi potenzialmente vittime di attacco o di un furto di dati. Tra le altre app di questo tipo ci sono le chat di Tinder, Whatsapp e Facebook, che sono state in molti casi rimosse. Peccato che i dipendenti più smanettoni un sistema per ripristinare le app riescano sempre a trovarlo, con conseguenze se possibile ancora peggiori per la security aziendale.

La Russia lavora sul suo OS mobile, per liberarsi di Android e iOS

www.mobileworld.it/2016/05/17/russia-sistema-operativo-sailfish-os-80228/

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3 – Opinion & Guidelines W29 EDPB – provvedimenti, trattamenti particolari

M3.2 Utilizzo di posta elettronica e web sul posto di lavoro

Unità didattica

M3.2.1 Le minacce

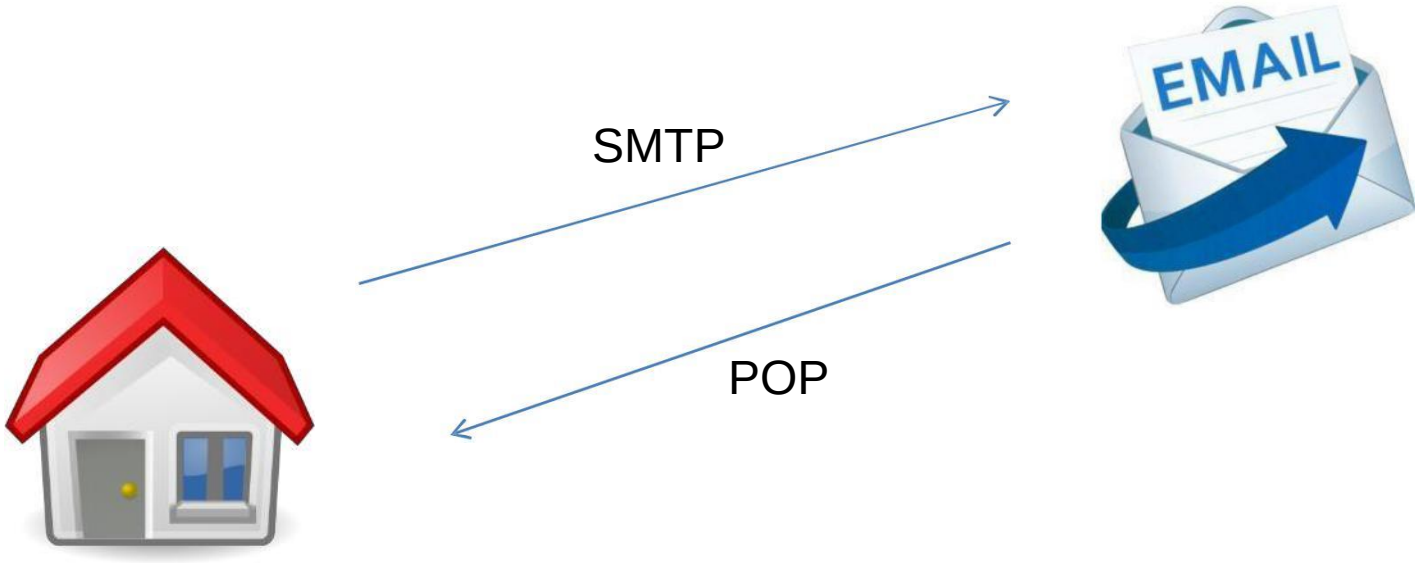
Dott. Raffaele Grieco

M3.2 – Utilizzo di posta elettronica e web sul posto di lavoro

Le minacce – I parte

EMAIL

- I protocolli di gestione della posta elettronica (POP e SMTP) non sono stati progettati per essere sicuri
- L'autenticazione è richiesta solo in ricezione (POP)
- Chiunque può farsi passare per chiunque



ATTACCHI VIA EMAIL

- 1. contenuto (phishing, ingegneria sociale)
- 2. allegati
- 3. link
- 4. contenuti aggiuntivi

«Un tipico esempio di Scam è la **truffa alla nigeriana**. Coloro che organizzano la truffa inviano un'email nella quale si parla di grosse somme di denaro che dovrebbero essere trasferite o recuperate da una banca estera che chiede garanzie: come la cittadinanza, un conto corrente, un deposito cauzionale…»

it.wikipedia.org/wiki/Scam

Il phishing del casellario giudiziale, una nuova truffa nel web e sui social

www.massimocappanera.it/truffa-del-casellario-giudiziale/

- L'analisi degli **header** del messaggio fornisce indicazioni per classificare un messaggio come spam / nocivo…

- …ma questo non è alla portata (o voglia) di tutti

From - Tue Feb 13 10:14:40 2018
X-Account-Key: account6
X-UIDL: UID5515-1430293419
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: <paparicio@presime.com.mx>
Delivered- To: <xxxxxxxxx@yyyyyyyyy>
Received: from mx1.pub.mailpod1-cph3.one.com ([10.27.24.11])
by mailstorage8.cst.mailpod1-cph3.one.com (Dovecot) with LMTP id QFUkJSq3gVo/AwAA7irNVg
for < xxxxxxxxx@yyyyyyyyy >; Mon, 12 Feb 2018 15:52:54 +0000
X-HalOne-ID: c7c645fb-100c-11e8-9dbd-405cfd1172c1
Received: from [181.67.211.152] (unknown [181.67.211.152])
by mx1.pub.mailpod1-cph3.one.com (Halon) with ESMTP
id c7c645fb-100c-11e8-9dbd-405cfd1172c1;
Mon, 12 Feb 2018 15:52:51 +0000 (UTC)
From: <paparicio@presime.com.mx>
To: <xxxxxxxxx@yyyyyyyyy>
Subject: Finora ti hanno MENTITO
Date: 12 Feb 2018 04:27:50 -0600
Message-ID: <002e01d3a3ef$04efaa62$76dc47b2$@presime.com.mx>
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_002B_01D3A3EF.04EAED7A"
X-Mailer: Microsoft Outlook 15.0
Thread-Index: Ac941s8shq38pkqd941s8shq38pkqd==
Content-Language: en-us

This is a multi-part message in MIME format.

SPAM

Shoulder of Pork And haM

Unsolicited bulk email / junk mail

email commerciale non richiesta

SPAM

- invio di messaggi non richiesti, fastidiosi o dannosi
- non sono caratteristici dell'email o di Internet (antica "catena di S. Antonio")
- stimato essere 80-90% di tutte le email mondiali

scopi dello spamming

- inviare pubblicità
- allegare virus e malware in genere
- carpire indirizzi email **validi** per:
    1. venderli
    2. usarli per DOS e DDOS
    3. altri scopi malevoli

frodi via email

- phishing
- la banca nigeriana
- schemi Ponzi
- multi-level marketing
- lotterie assortite

ESEMPI

personali

From: Polina52220@theark.ie

Subject: yo

Hi xxxxxxxxx, my name is Polina and i'm from Russia. Currently I live in US. Im so glad to see your profile on Facebook. You seem like my type and I would like us to know each other better. You are super cute and handsome. If you feel the same, email me lauragiselawb93@rambler.ru and I will send some of my photos. Hugs, Polina

From: Polina52220@theark.ie

Subject: yo

Hi xxxxxxxxx, my name is Polina and i'm from Russia. Currently I live in US. Im so glad to see your profile on Facebook. You seem like my type and I would like us to know each other better. You are super cute and handsome. If you feel the same, email me lauragiselawb93@rambler.ru and I will send some of my photos. Hugs, Polina

Hi xxxxxxx, my name is **Ksusha** and i'm from Russia. Currently I live in US. Im so glad to see your profile on Facebook. You seem like my type and I would like us to know each other better. You are super cute and handsome. If you feel the same, email me **monikadrv1ursula@rambler.ru** and I will send some of my photos. Hugs, Ksusha

Hi xxxxxxx, my name is **Svetlana** and i'm from Russia. Currently I live in US. Im so glad to see your profile on Facebook. You seem like my type and I would like us to know each other better. You are super cute and handsome. If you feel the same, email me **evaan3hd@rambler.ru** and I will send some of my photos. Hugs, Svetlana

Hi xxxxxxxx, My name is **Sofia** and i'm writing you to tell you that you are super cute from your photos on Facebook. I myself am from Russia, but now I live in the USA. I want to get to know you more! If you have the same, email me, this is my email **terezae5on@rambler.ru**. Lets know each other better. Cheers, Sofia

Saluto. Sono una signora spassosa, mi piace tutto cio che mi circonda e cerco di vivere con uno stato d'animo positivo. Amo i film, la musica e lo sport. Mi piace trascorrere del tempo con gli amici, cosi mi sento bene. Devo dire che ho tanti interessi nella mia vita. Vorrei trovare un maschio che possa essere l'uomo principale della mia vita. Credo che siamo in grado di raggiungere la completa felicita solo con qualcuno che ami. Mi piacerebbe avere un uomo dotato, affabile, beneducato e delicato. Sono molto serena e credo che con lo stesso maschio possa essere felice ogni giorno. Ho bisogno di un tipo affettuoso e attento nella mia vita. Voglio essere una vera donna nelle sue mani forti. Inoltre ho bisogno di un maschio che mi sostenga. Se avete bisogno di donne e volete svagarvi con calde emozioni e momenti di puro relax e divertimento vi aspetto numerosi! bacio. Resto in attesa della tua risposta al mio indirizzo e-mail romanticavalentyna@vividspices.eu Cordiali saluti. Valentyna.

Saluto Mi fa immensamente interessare incontrare meglio. Per me il connessione fra uomo e donna dev'essere quello di un completamento della coppia. Ci deve essere, una connessione fisica e spirituale. Se uomo ha un lavoro che pu? far fronte economicamente alla famiglia, la donna si pu? dedicarealla casa, renderla calda, accogliente, come il nido della famiglia e se anche la donna vuole lavorare, entrambi dovrebbero occuparsi della casa. Sia la donna sia uomo devono cercare di intendere l'un l'altro, cercare insieme la massima soddisfazione nello stare insieme, nel cibo, nel divertimento (viaggi, ballo, film, visite di mostre, musei, mare, montagna ...) nello sport, nel sesso, molto importante per l'unione della coppia, con gli amici ecc. ? molto importante fare in modo che gli interessi dell uomo coincidano anche con gli interessi della donna. Soprattutto, quando siamo insieme, dobbiamo dimenticarci degli eventuali problemi, essere felici per rendere felice anche l'altro. Quando uno di noi ha bisogno, qualunque sia il problema, l'altro deve sostenere, nella convinzione di superare insieme tutte le difficolt? della vita, per continuare ad essere felici. Ricordati che i primi costruttori della nostra felicit? siamo noi stessi!!! E non ? una frase stupida; te lo spiegher?, ricordamelo, quando saremo insieme. Ed io dico: "lasciamoci andare a questo destino"!!! Io ho fiducia in te, ma soprattutto un rapporto d'amore con un uomo, una famiglia da poter elargire tanto affetto, del quale credo tu ne abbia moltissimo. Ho veramente bisogno trova la mia altra meta
! Io tengo giornalmente pulita la casa, specialmente i letti, la cucina i bagni. A me piacciono molto i fiori, soprattutto le rose. se vuoi creare una relazione seria e forte. puoi scrivermi la mia e-mail valentynaamare@fittnowapp.com Valentyna.

From DHL EXPRESS <>
Subject **Your shipment has arrived!**
14/03/2018 08:09
To [redacted]

Reply | Forward | Delete | More

To protect your privacy, Thunderbird has blocked remote content in this message. Options

DHL_logo

DHL Capability Tool

Dear: [redacted],

Your shipment has arrived!

Arrival Information
Your package has been arrived to your local DHL office and it's ready for pick up.

ARRIVAL NOTICE

DATE & TIME : 2018-12-03 at 11:40
STATUS : Shipment arrived

****
Please print the receipt that is attached to this email and visit DHL location indicated in the receipt

DHL WorldWide Delivery

1 attachment: DHL AWB.doc 93,5 KB

Save

Come va oggi ? Scuse! Sono una donna militare, in cerca la tua gentile assistenza per spostare la somma di ($ 27 milioni di dollari) a te, per quanto riguarda come posso essere sicuro che il mio denaro sarà al sicuro nelle tue cure fino a quando Completo il mio servizio qui in Afghanistan e vieni dopo mese.

Questo è legittimo e non c'è pericolo. Se interessato, rispondere immediatamente per informazioni dettagliate.

Rispondi a questa email sgtbrittalopez212@outlook.com

Saluti ,

Sgt. Britta Lopez ---

From Amazon-Prime@sicurezza.it

Subject **Il tuo account è stato bloccato per motivi di sicurezza,**

08/08/2018 17:27

To [redacted]

To protect your privacy, Thunderbird has blocked remote content in this message.

BancoPosta online - Poste Italiane

Utente,[redacted]

Il 07 *augusto* **2018** è una data storica per la protezione dei dati personali: il Regolamento UE 2016/679, noto come GDPR (General Data Protection Regulation), entrerà in vigore in tutti gli Stati dell'eurozona.
Con il nuovo Regolamento molti aspetti di carattere normativo si semplificano e la gestione della Privacy assume caratteristiche più moderne.

Noi di Poste Italiane online, da sempre attenti alla tutela e ai diritti dei nostri utenti, abbiamo attuato quanto previsto e abbiamo adeguato i nostri servizi, il trattamento e la protezione dei tuoi dati al nuovo Regolamento.

Sul portale potrai trovare e leggere le nuove privacy policy e l'informativa completa: Non rinnovando il tuo Piano di Servizio, potresti non avere più accesso. Dopo aver cliccato sotto, se hai effettuato la registrazione e non visualizzi il pop up con i nostri aggiornamenti, puoi ritenere di aver già prestato il tuo consenso.

» Leggi e Acceta

Cordiali saluti,

BancoPosta online - Poste Italiane

From Amazon-Prime@sicurezza.it
Subject **Il tuo account è stato bloccato per mo zza,**
To [redacted]
08/08/2018 17:27

Reply

To protect your privacy, Thunderbird has blocked remote content in this message.

BancoPosta online - Poste Italiane

Utente,[redacted]

Il 07 *augusto* **2018** è una data storica per la protezione dei dati personali: il Regolamento UE 2016/679, noto come GDPR (General Data Protection Regulation), entrerà in vigore in tutti gli Stati dell'eurozona.
Con il nuovo Regolamento molti aspetti di carattere normativo si semplificano e la gestione della Privacy assume caratteristiche più moderne.

Noi di Poste Italiane online, da sempre attenti alla tutela e ai diritti dei nostri utenti, abbiamo attuato quanto previsto e abbiamo adeguato i nostri servizi, il trattamento e la protezione dei tuoi dati al nuovo Regolamento.

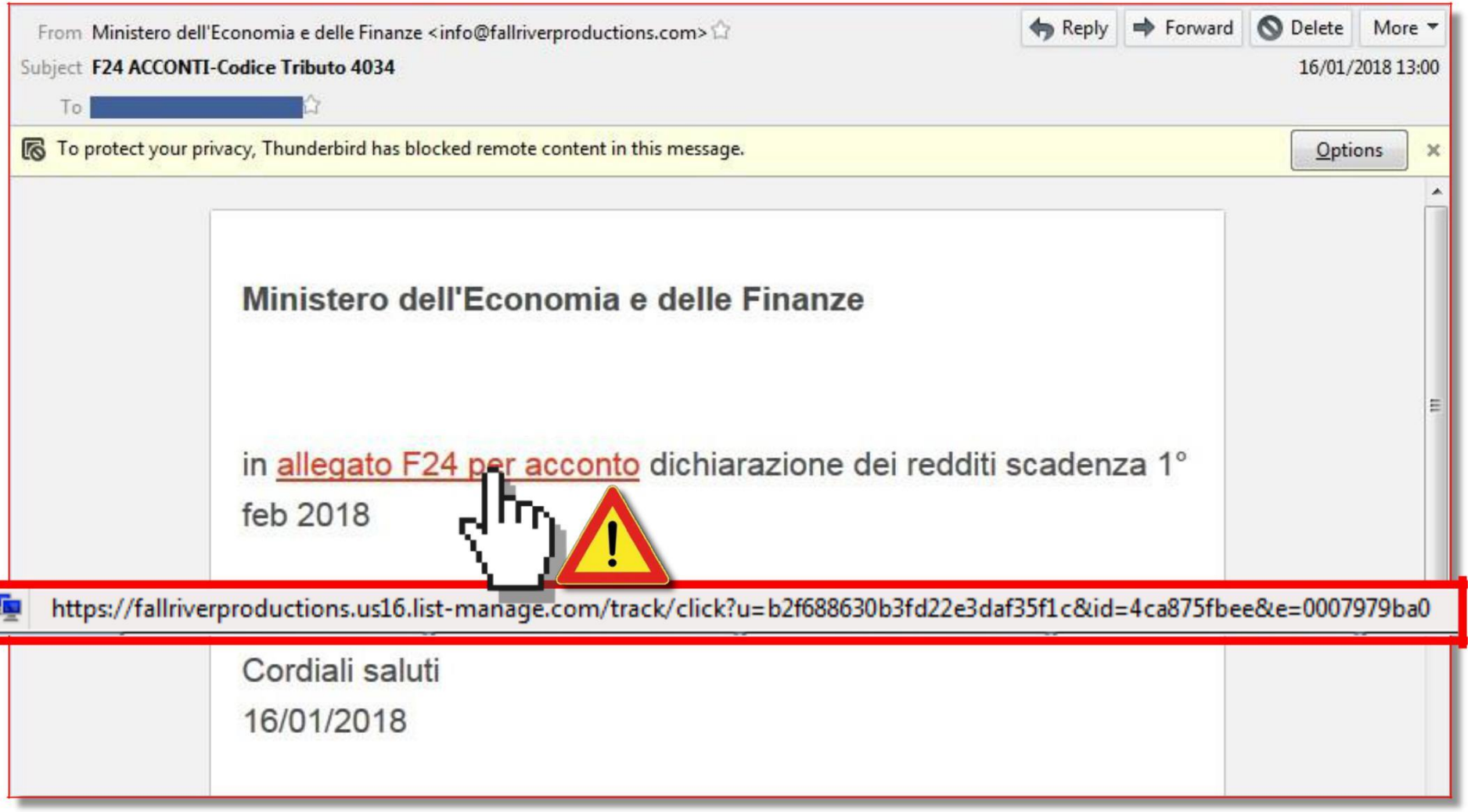
Sul portale potrai trovare e leggere le nuove privacy policy e l'informativa completa: Non rinnovando il tuo Piano di Servizio, potresti non avere più accesso. Dopo aver cliccato sotto, se hai effettuato la registrazione e non visualizzi il pop up con i nostri aggiornamenti, puoi ritenere di aver già prestato il tuo consenso.

» Leggi e Acceta

Cordiali saluti,

BancoPosta online - Poste Italiane


Reply
Forward
Delete
More
Subject F24 ACCONTI-Codice Tributo 4034
16/01/2018 13:00
To
To protect your privacy, Thunderbird has blocked remote content in this message.
Options
Ministero dell'Economia e delle Finanze
in allegato F24 per acconto dichiarazione dei redditi scadenza 1° feb 2018


From Ministero dell'Economia e delle Finanze <info@fallriverproductions.com>
Reply
Forward
Delete
More
Subject F24 ACCONTI-Codice Tributo 4034
16/01/2018 13:00
To
To protect your privacy, Thunderbird has blocked remote content in this message.
Options
Ministero dell'Economia e delle Finanze
in allegato F24 per acconto dichiarazione dei redditi scadenza 1° feb 2018
https://fallriverproductions.us16.list-manage.com/track/click?u=b2f688630b3fd22e3daf35f1c&id=4ca875fbee&e=0007979ba0
Cordiali saluti
16/01/2018


collegare
il cervello

Gentile cliente,

Il tuo ordine di acquisto stato comunicato all'esercente che provvedera ad evaderlo in base alle condizioni di vendita definite.

La conferma definitiva dell'acquisto la riceverai direttamente dall'esercente, che potra confermarla o annullarla.

Dati del negozio

Codice Esercente: WEB_00182389

Per scaricare i file da lei acquistati in formato digitale,

deve loggarsi a questo link: ordine.txt

Dati del pagamento

Data e ora: 8/16/2018 3:39:28 PM

Divisa: EUR

Importo: 3131,00

Codice XPay attribuito all'ordine di pagamento: PW92VVZF63368845

Codice autorizzativo assegnato dal circuito di pagamento: 3231858

Dati dell'acquirente

Circuito della carta: VISA

Indirizzo email dell'acquirente: xxxxxxx@xxxxx.it

Gentile cliente,

Il tuo ordine di acquisto stato comunicato all'esercente che provvedera ad evaderlo in base alle condizioni di vendita definite.

La conferma definitiva dell'acquisto la riceverai direttamente dall'esercente, che potra confermarla o annullarla.

Dati del negozio

Codice Esercente: WEB_00182389

Per scaricare i file da lei acquistati in formato digitale,

deve loggarsi a questo link: ordine.txt

Dati del pagamento

Data e ora: 8/16/2018 3:39:28 PM

Divisa: EUR

ftp://ftpuser:wrmTNlQImLx7OwL@ordine.lavanexpress.com/files/**ordine.exe**

Importo: 3131,00

Codice XPay attribuito all'ordine di pagamento: PW92VVZF63368845

Codice autorizzativo assegnato dal circuito di pagamento: 3231858

Dati dell'acquirente

Circuito della carta: VISA

Indirizzo email dell'acquirente: xxxxxxx@xxxxx.it

Bug nei chip Wi-Fi: miliardi di dispositivi a rischio attacco

Gen 21, 2019

Computer e smartphone, ma anche PS4, Xbox, router e dispositivi IoT. L'attacco funziona senza interazione dell'utente e non ci sono ancora patch.

www.securityinfo.it/2019/01/21/bug-nei-chip-wi-fi-miliardi-di-dispositivi-a-rischio-attacco

Router D-Link sotto attacco. Il nuovo worm si chiama Masuta

www.securityinfo.it/2018/01/25/router-d-link-attacco-worm-si-chiama-masuta

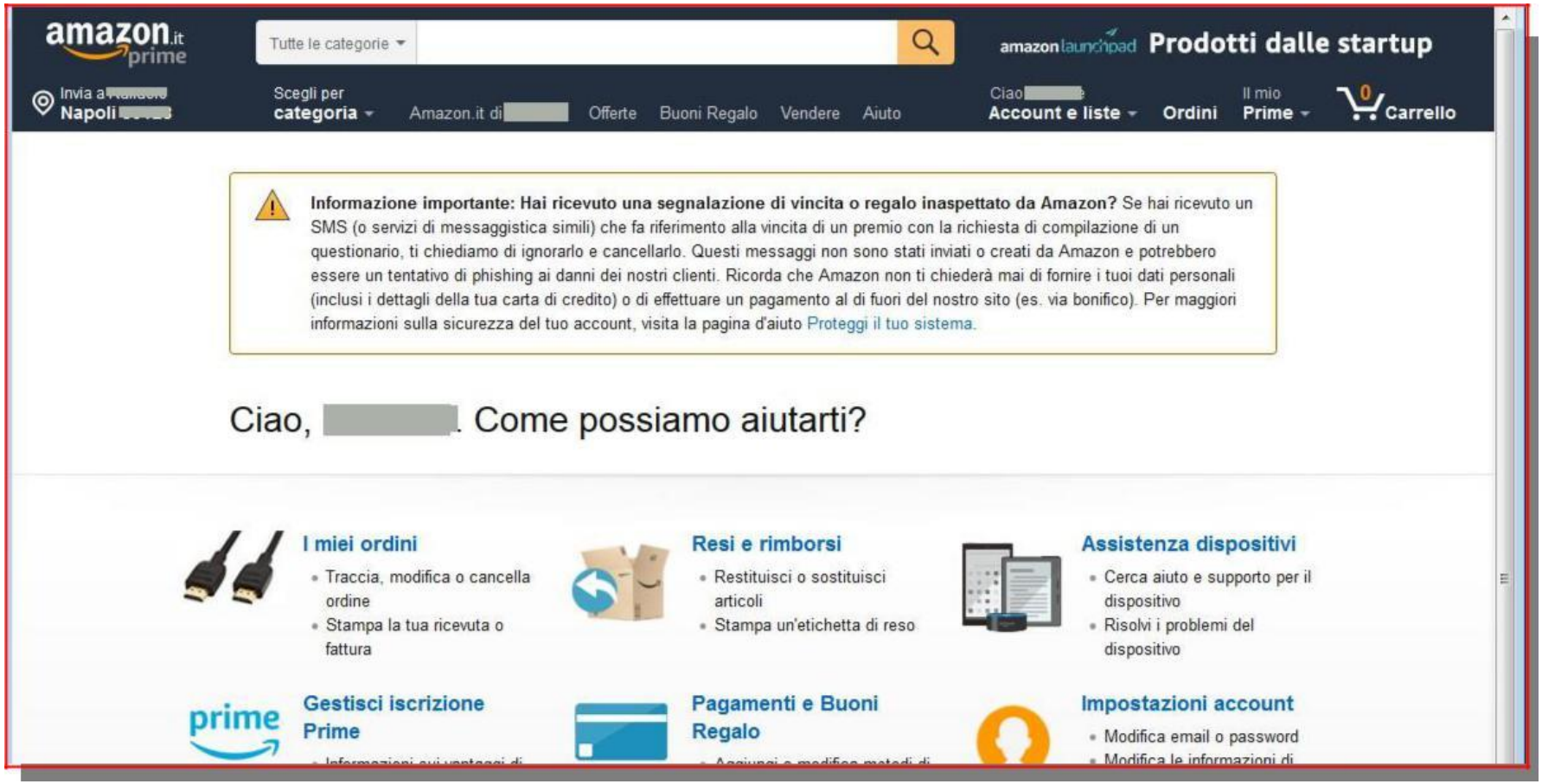
Il malware sfrutta un nuovo exploit per compromettere i dispositivi e arruolarli in una botnet che sta crescendo rapidamente.

Il malware ruba i dati dal tuo smartphone, ma ti fa risparmiare batteria

L'app per Android promette di monitorare i consumi della batteria. È vero, ma dentro c'è un trojan che fa tutt'altro.

Peccato che Advanced Battery Saver faccia anche altro. E per accorgersene *sarebbe sufficiente guardare con attenzione* ai permessi che richiede al momento dell'installazione, che comprendono l'accesso ai log di sistema, ai contatti e ai messaggi.

www.securityinfo.it/2018/06/26/il-malware-ruba-i-dati-dal-tuo-smartphone-ma-ti-fa-risparmiare-batteria


amazon.it prime
Tutte le categorie
amazon launchpad Prodotti dalle startup
Invia a Napoli
Scegli per categoria
Amazon.it di
Offerte
Buoni Regalo
Vendere
Aiuto
Ciao
Account e liste
Ordini
Il mio Prime
0 Carrello
Informazione importante: Hai ricevuto una segnalazione di vincita o regalo inaspettato da Amazon? Se hai ricevuto un SMS (o servizi di messaggistica simili) che fa riferimento alla vincita di un premio con la richiesta di compilazione di un questionario, ti chiediamo di ignorarlo e cancellarlo. Questi messaggi non sono stati inviati o creati da Amazon e potrebbero essere un tentativo di phishing ai danni dei nostri clienti. Ricorda che Amazon non ti chiederà mai di fornire i tuoi dati personali (inclusi i dettagli della tua carta di credito) o di effettuare un pagamento al di fuori del nostro sito (es. via bonifico). Per maggiori informazioni sulla sicurezza del tuo account, visita la pagina d'aiuto Proteggi il tuo sistema.
Ciao, . Come possiamo aiutarti?
I miei ordini
Traccia, modifica o cancella ordine
Stampa la tua ricevuta o fattura
Resi e rimborsi
Restituisci o sostituisci articoli
Stampa un'etichetta di reso
Assistenza dispositivi
Cerca aiuto e supporto per il dispositivo
Risolvi i problemi del dispositivo
prime
Gestisci iscrizione Prime
Pagamenti e Buoni Regalo
Impostazioni account
Modifica email o password

Dalla truffa a luci rosse alla minaccia dell'omicidio su commissione

Escalation clamorosa delle truffe via email. Si è passati dal ricatto alla minaccia di piazzare bombe, per arrivare ai sicari assoldati via Internet.

www.securityinfo.it/2018/12/21/dalla-truffa-a-luci-rosse-alla-minaccia-dellomicidio-su-commissione

Intorno al 10 dicembre ha fatto la sua comparsa la "truffa della bomba". I pirati, in sostanza, minacciavano di compiere degli attentati dinamitardi se i destinatari dei messaggi non avessero versato 20.000 dollari in Bitcoin sul loro conto.

A seguire, sono comparse altre (e sempre più odiose) varianti, che puntano a fare leva sulle paure delle potenziali vittime attraverso un mix di leggende metropolitane ed episodi di cronaca(...)

In quest'ultima versione, il ragionamento è il seguente: il mio cliente mi paga 4.000 dollari per farti uccidere da un sicario. Se me ne dai 1.600 non solo fermerò il killer, ma ti dirò anche chi è il mandante.

Che cosa vogliono gli spammer?

- I nostri $oldi
- I nostri dati
- Che clicchiamo sui link forniti (per mandarci virus, malware o per incrementare il loro conteggio)
- Che rispondiamo all'email
- …

In tutti i casi, ottengono comunque la conferma che l'indirizzo email è attivo («vivo») e possono inserirlo nella loro lista. Anche venderlo.

Come trovano il nostro indirizzo?

(e quindi a che cosa dobbiamo stare attenti?)

1. un **virus** può accedere alla rubrica del programma di posta e prendere gli indirizzi dei nostri corrispondenti...

magari anche accedendo ai messaggi e limitandosi per data in modo da scartare quelli non più in uso

(frequente)

...quindi se arriva una email da un indirizzo a noi **conosciuto**,

potrebbe essere spam che ha ricavato gli indirizzi dal nostro amico infetto

(frequente)

2. lo forniamo noi:

- Rispondendo a una email di spam
- Aprendo una email con contenuti estesi (v.)
- Compilando un form online
- …

(fin troppo frequente)

3. da **breach** su siti non adeguatamente protetti
   (casi di Yahoo, MySpace...)

preoccupante

Attacco a MySpace

www.wired.com/2006/12/myspace-passwords-arent-so-dumb-2

Una falsa pagina di login a MySpace ha permesso agli attaccanti di entrare in possesso di 34.000 coppie di credenziali (nome / password)

Su Internet compare un database con 1,1 miliardi di credenziali rubate

www.securityinfo.it/2019/01/18/su-internet-compare-un-database-con-11-miliardi-di-credenziali-rubate

...Nel dettaglio, il database contiene 1.160.253.228 combinazioni uniche di email e password, mentre le email uniche nel database sono 772.904.991.

Falle di sicurezza in tutti i maggiori servizi di Web Hosting

Lo studio è di Website Planet. I pirati informatici possono attaccare gli utenti per prendere il controllo di un sito Internet con un singolo clic.

www.securityinfo.it/2019/01/15/falle-di-sicurezza-in-tutti-i-maggiori-servizi-di-web-hosting

Casinò online si “dimenticano” online i dati di 100 milioni di utenti

Gen 22, 2019

Il database è stato lasciato senza alcuna protezione. Chiunque poteva accedere ai dati personali degli iscritti e alle informazioni sulle loro vincite.

...chiunque avrebbe potuto avere nome e cognome, numero di telefono, indirizzo email, residenza, indirizzo IP di tutti i frequentatori del sito. Non solo: tra i dati disponibili c’erano anche gli estratti dei conti sui siti e i dati delle carte di credito usate per il pagamento. Fortunatamente queste ultime erano (parzialmente) protette.

www.securityinfo.it/2019/01/22/casino-online-si-dimenticano-online-i-dati-di-100-milioni-di-utenti/

4. vengono generati automaticamente e poi messi alla prova inviando un messaggio e aspettando la risposta:

a@domain.com
aa@domain.com
ab@domain.com
...
pippo@domain.com
...

"Quanto sono vulnerabili ministeri, regioni e aziende alle mail infette in Italia"

Secondo uno studio, moltissimi uffici pubblici e privati non sono dotati delle difese minime per proteggersi da attacchi hacker via posta elettronica

Proofpoint ha effettuato un'analisi attenta sui domini dei ministeri e delle regioni italiane, scoprendo che **nessuno dei 13 ministeri né delle 20 regioni adotta il sistema Dmarc**.

www.wired.it/internet/web/2018/12/01/ministeri-regioni-aziende-cybersicurezza-email/

Italia: 72% di enti pubblici e aziende non protegge l'email

La ricerca di Proofpoint non lascia dubbi: nel nostro paese l'implementazione degli strumenti di sicurezza va decisamente a rilento

www.securityinfo.it/2018/12/11/italia-il-72-di-enti-pubblici-e-aziende-non-si-protegge-da-attacchi-via-email/

Attacco alla PEC

Un gestore di PEC italiano ha ricevuto un attacco informatico

Sono stati rubati i dati di circa 500mila caselle di posta elettronica certificata, causando gravi disservizi a migliaia di uffici pubblici e tribunali

www.ilpost.it/2018/11/20/pec-attacco-informatico

L'attacco informatico è iniziato il 12 novembre scorso e sembra sia provenuto dall'estero.

...

Repubblica spiega che il problema ha coinvolto almeno 98mila utenti "tra magistrati, militari e funzionari del Cisr, il Comitato Interministeriale per la sicurezza della Repubblica,...

Attacco hacker: violate 500 mila caselle postali, anche Pec di magistrati

www.corriere.it/cronache/18_novembre_20/attacco-hacker-pec-ora-vanno-cambiate-password-accesso-e83118e0-ec5c-11e8-8c58-7b683e5c5fc2.shtml

Colpiti nei giorni scorsi circa 3mila soggetti tra pubblico e privato, oltre 30mila domini e circa 500mila caselle postali (98mila delle quali di appartenenti alla Pubblica amministrazione).

quanto accaduto dimostra che «vanno prese al più presto misure adeguate per innalzare le difese cyber».

Lo Stato dopo l'attacco hacker ai tribunali: "Cambiate la password della vostra Pec"

Il numero 1 della sicurezza cibernetica italiano, Roberto Baldoni, invita tutti i possessori di un indirizzo di posta certificata a monitorare i propri account dopo l'attacco dei giorni scorsi.

www.repubblica.it/tecnologia/sicurezza/2018/11/19/news/dopo_l_attacco_hacker_ai_tribunali_cambiate_subito_la_password_della_vostra_pec_-212086305

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3 – Opinion & Guidelines W29 EDPB – provvedimenti, trattamenti particolari

M3.2 Utilizzo di posta elettronica e web sul posto di lavoro

Unità didattica

M3.2.2 Le difese

Dott. Raffaele Grieco

M3.2 – Utilizzo di posta elettronica e web sul posto di lavoro

Le difese – I parte

DIFESE

regole generali

- **mai** rispondere allo spam
- prestare attenzione a tutte le email
- usare sempre CCN: (BCC:)
- usare una molteplicità di account
- attivare il servizio anti-spam del provider ove possibile

regole per la lettura con client

- disattivare la conferma automatica
- giammai cliccare
- disabilitare l'autoload del contenuto aggiuntivo (immagini)
- non abituare male amici e conoscenti
- attivare la visualizzazione delle estensioni

regole per lettura via web

- disabilitare gli script (v.)
- cancellare frequentemente cookie e cronologia
- staccare la connessione appena non necessaria

A:, CC: e CCN: (to:, CC: e BCC:)

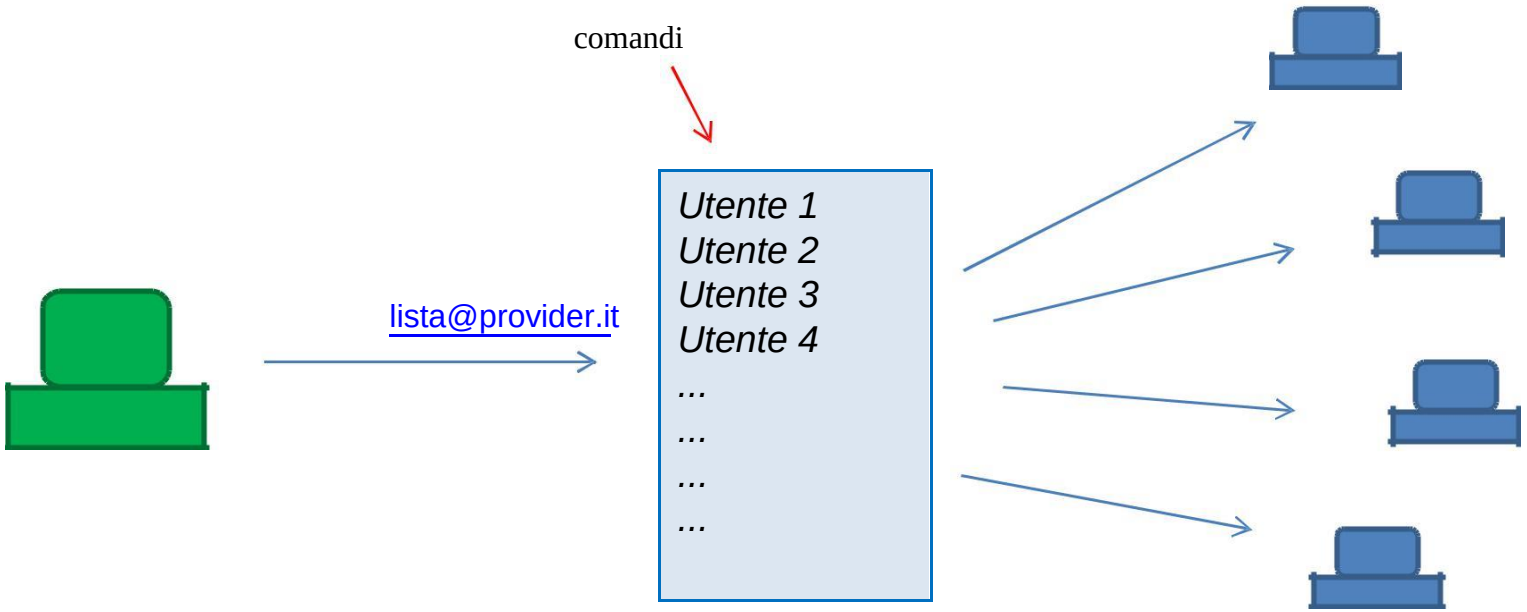
per colloquiare con più persone può venire la tentazione di usare il campo CC: per indirizzare i destinatari

questo semplifica le risposte ma espone a rischi

in alternativa si possono usare altri strumenti (Mailing list)

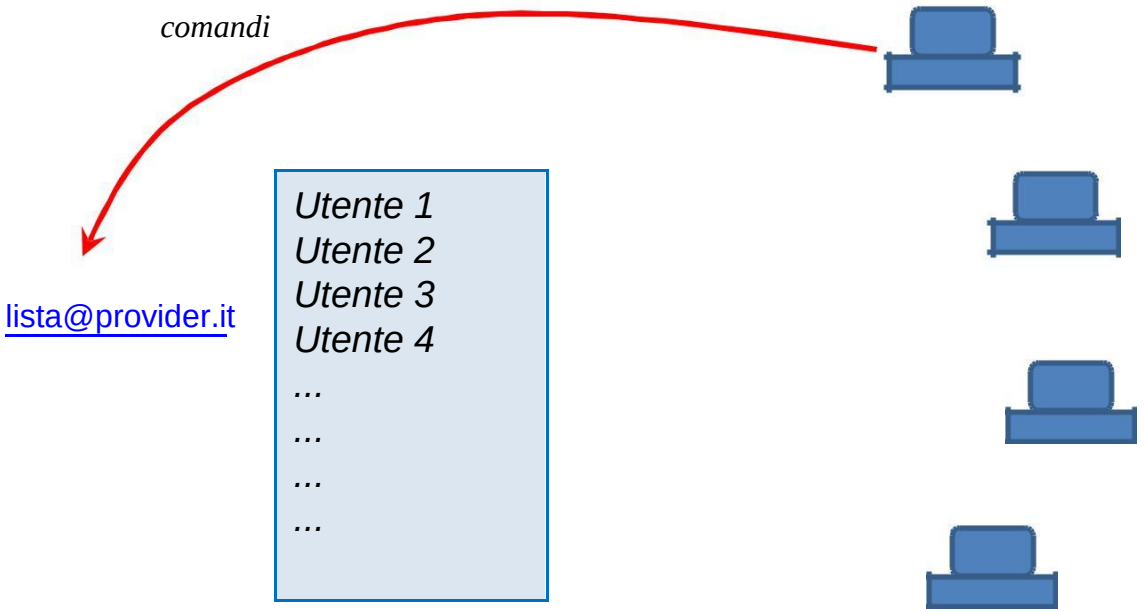
Mailing list

(lista di distribuzione, di diffusione, di discussione)



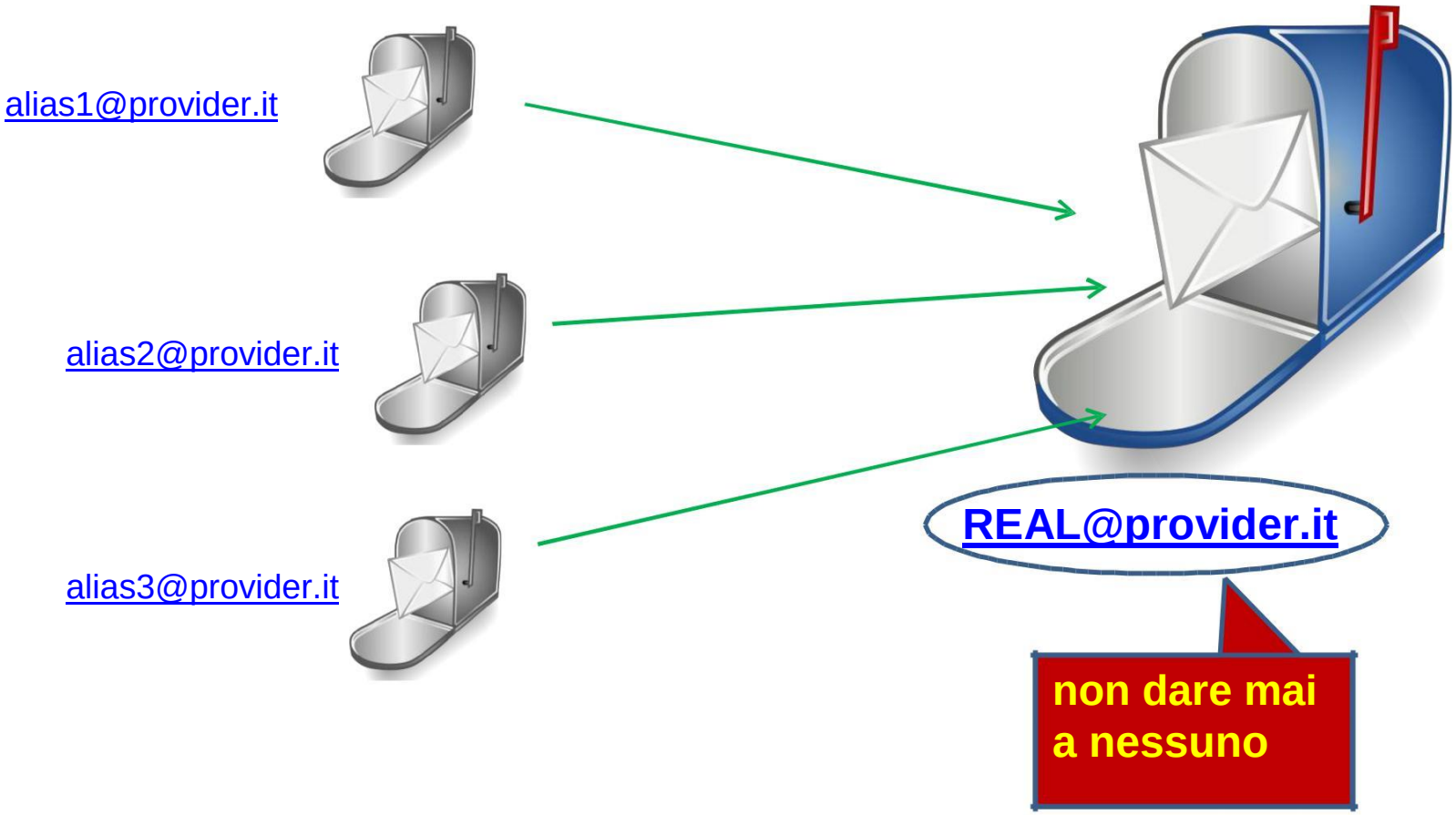
Mailing list

(lista di distribuzione, di diffusione, di discussione)

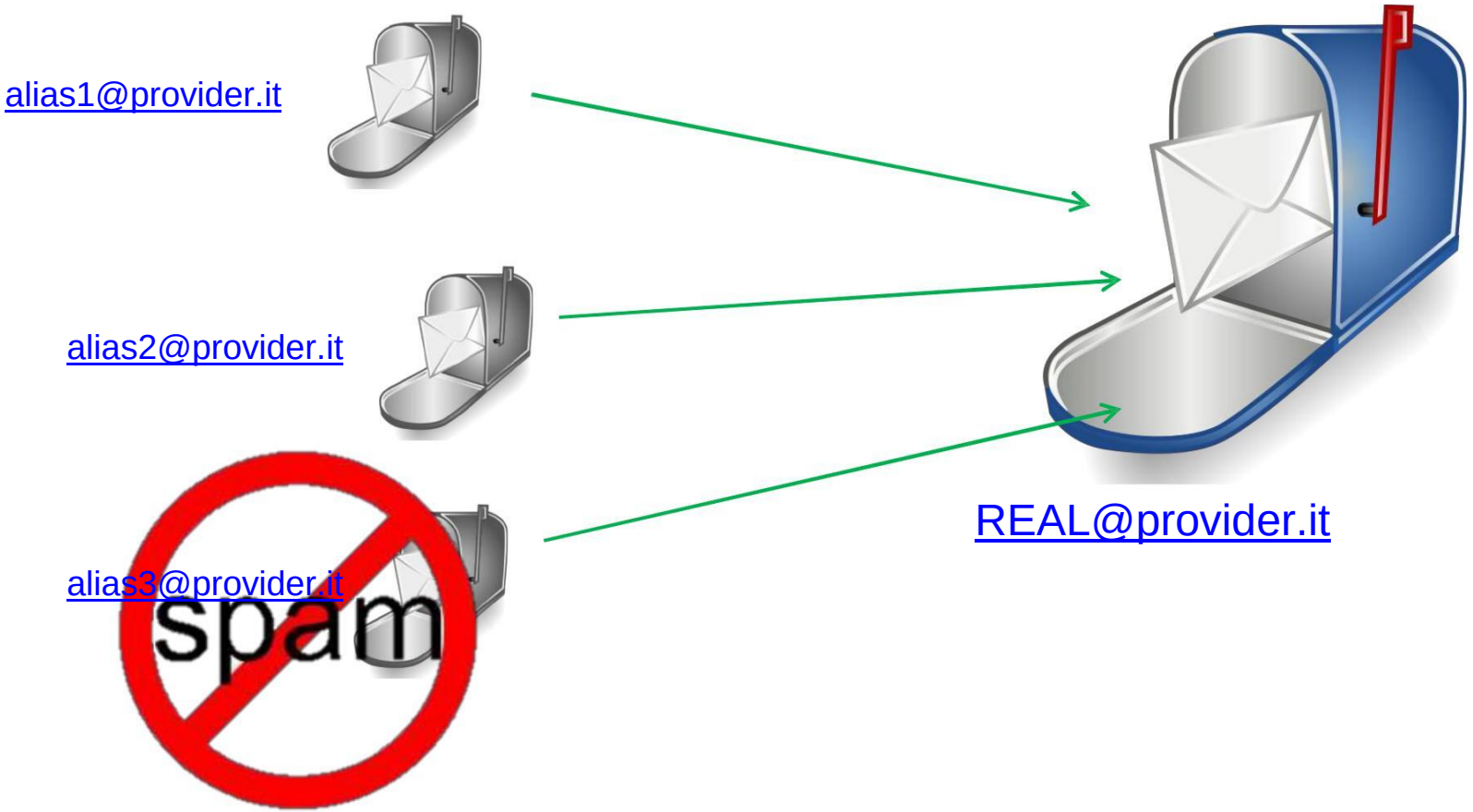


diretto / digest

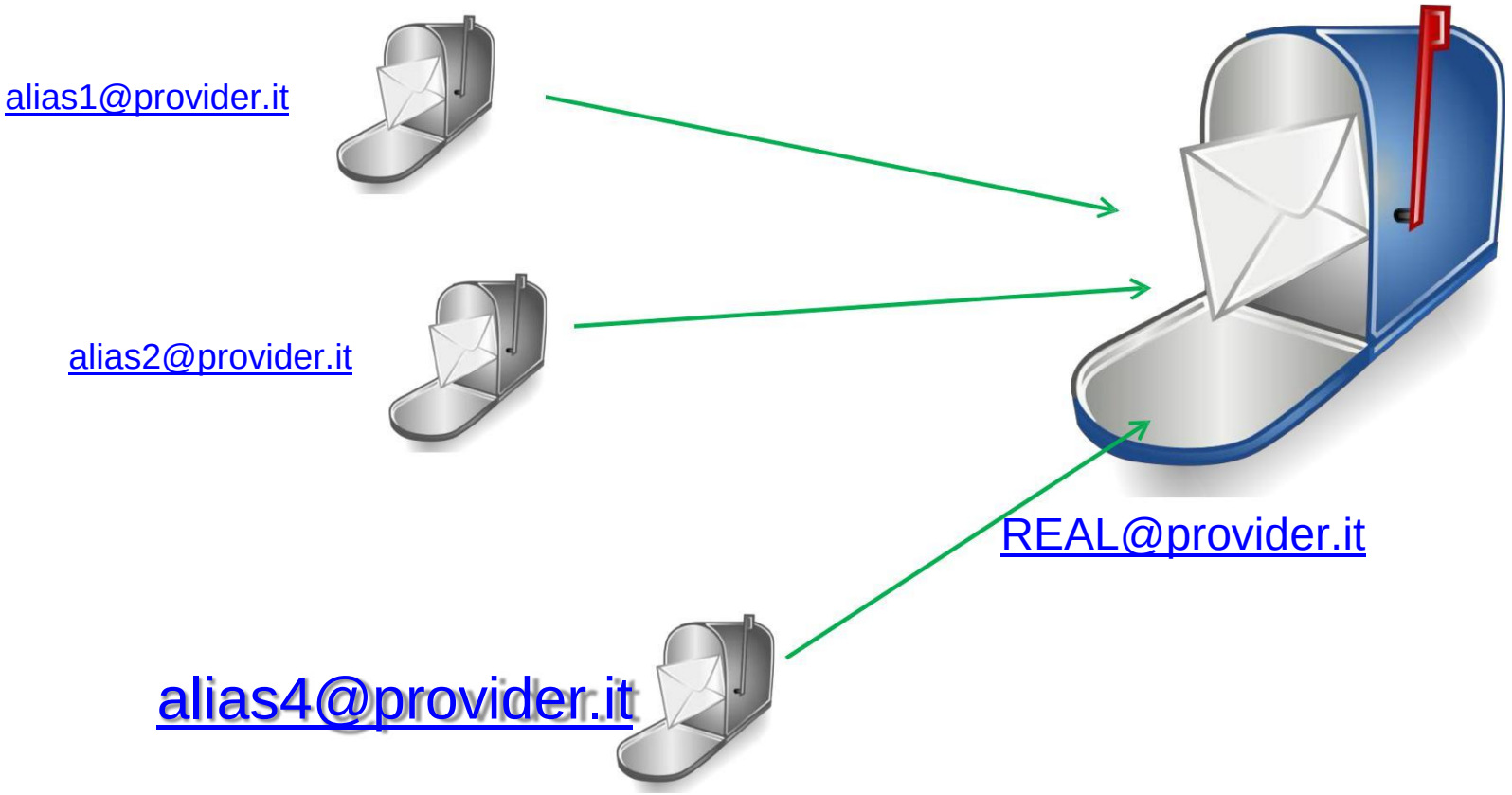
alias anti-spam (*indirizzi usa e getta)*



alias anti-spam (*indirizzi usa e getta)*



alias anti-spam (*indirizzi usa e getta)*

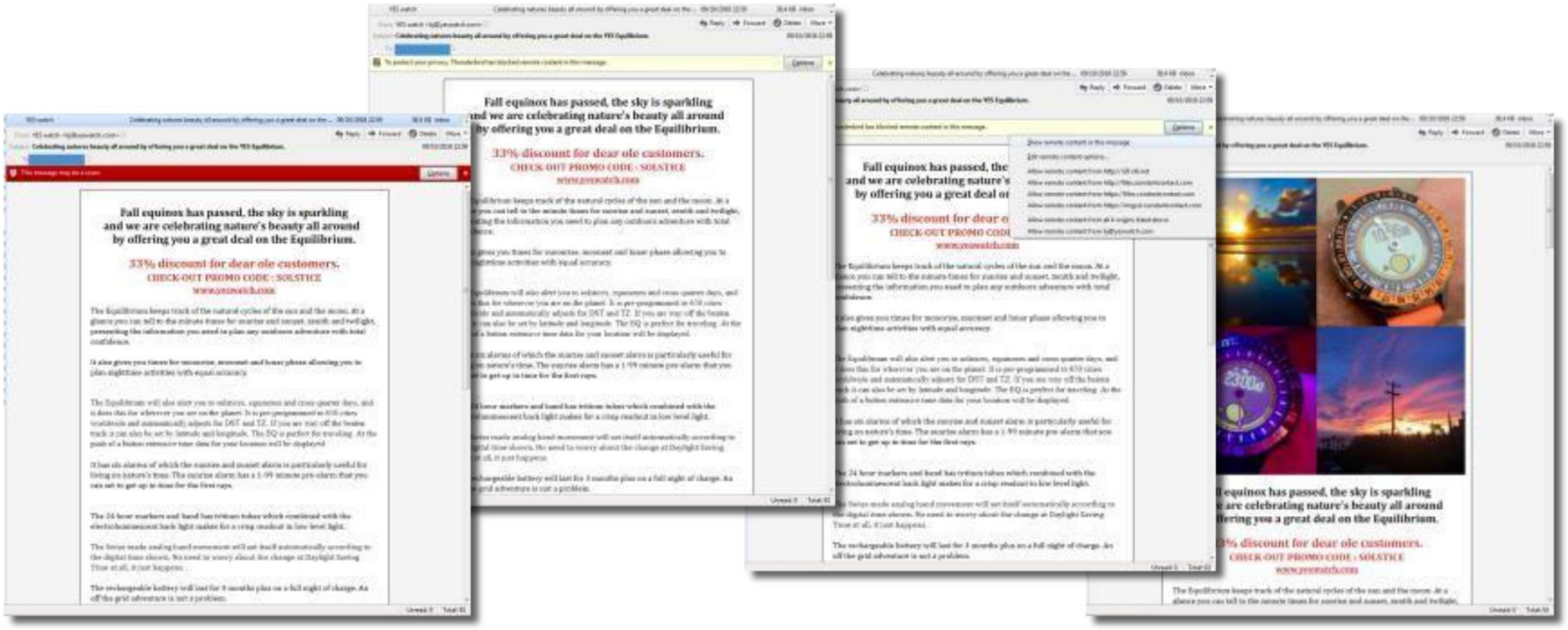


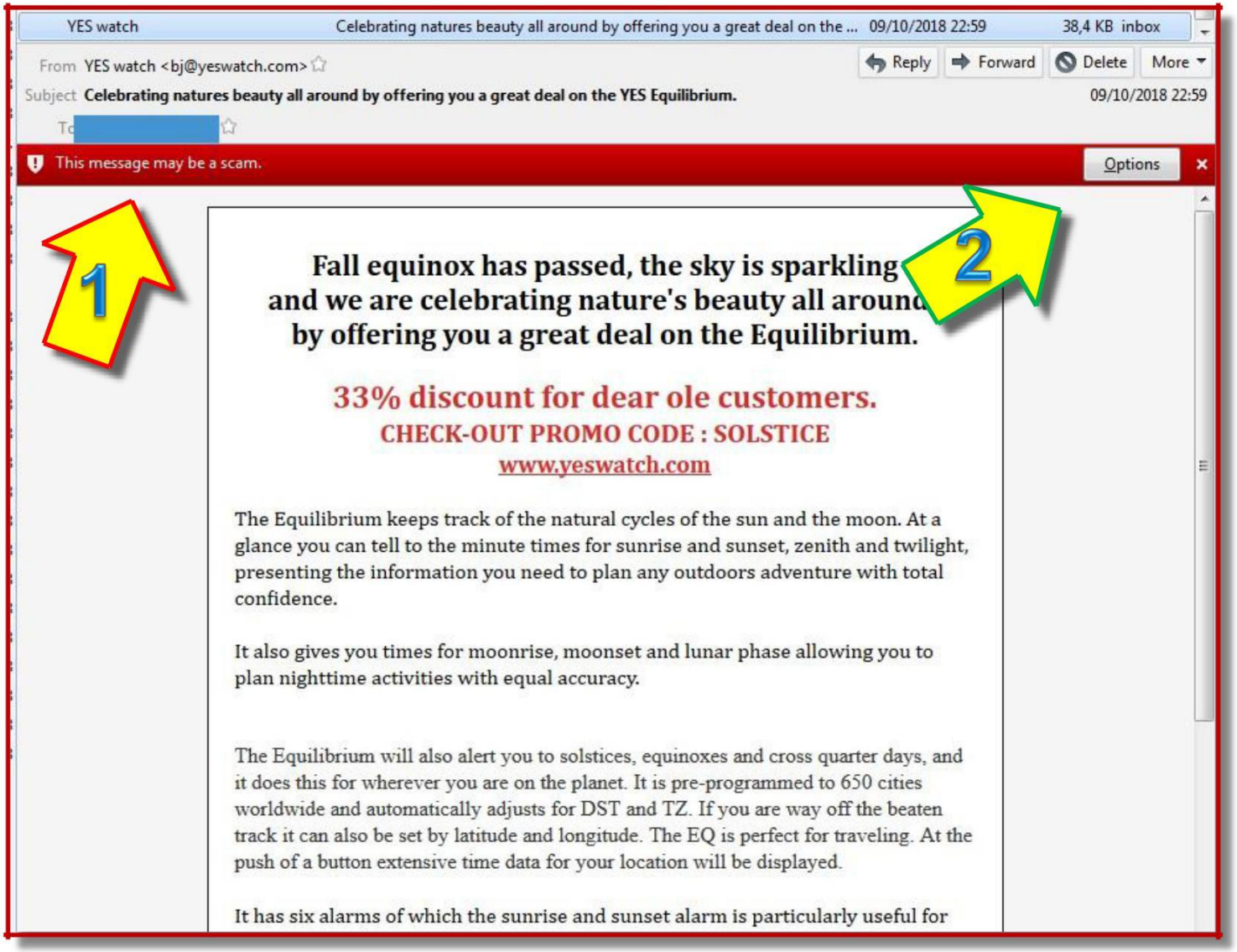
se a cadere in mano agli spammer è un account usato per cose serie (banca, e-commerce...),

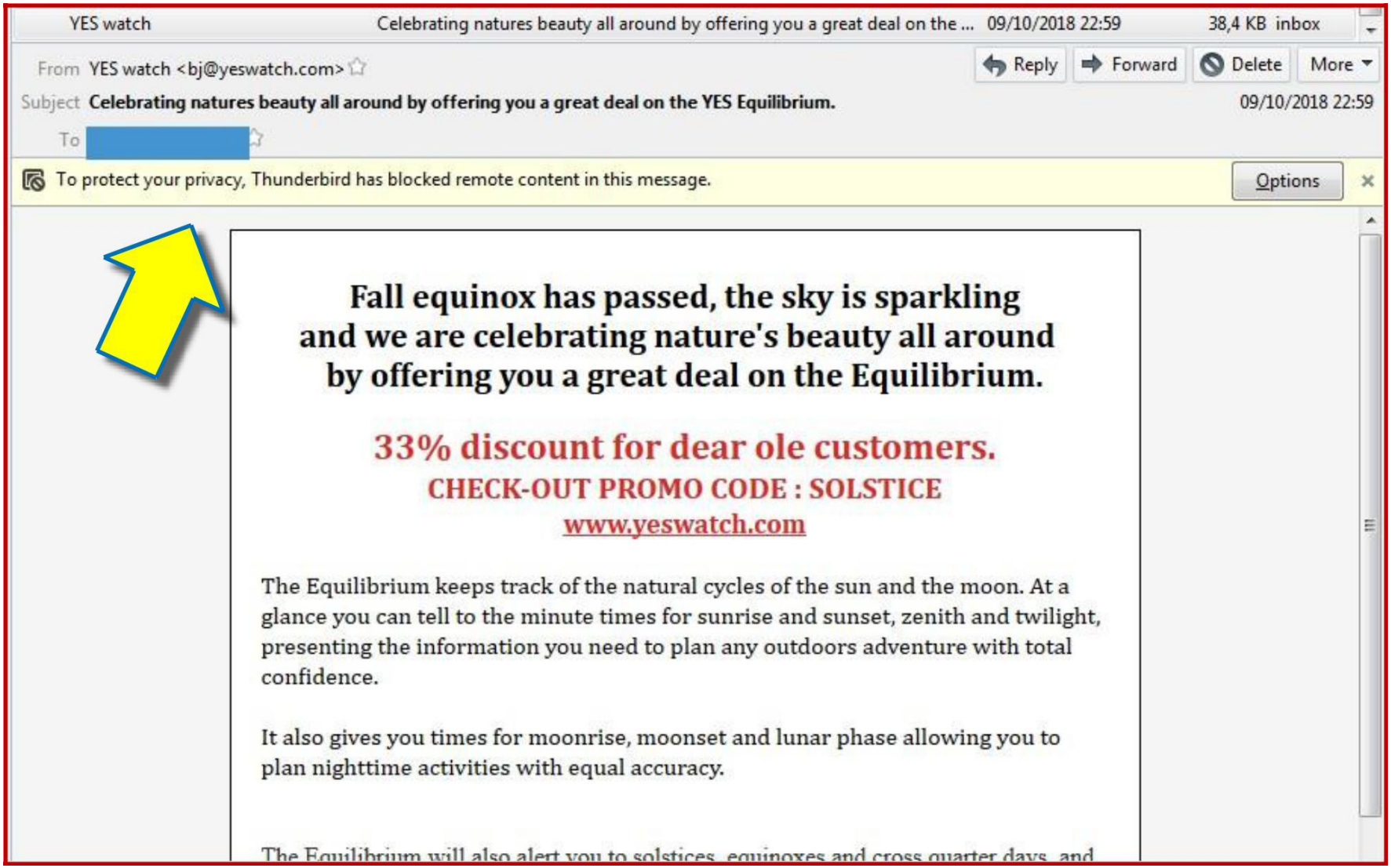
conviene non solo eliminarlo ma anche cambiare le credenziali di accesso al servizio e controllare

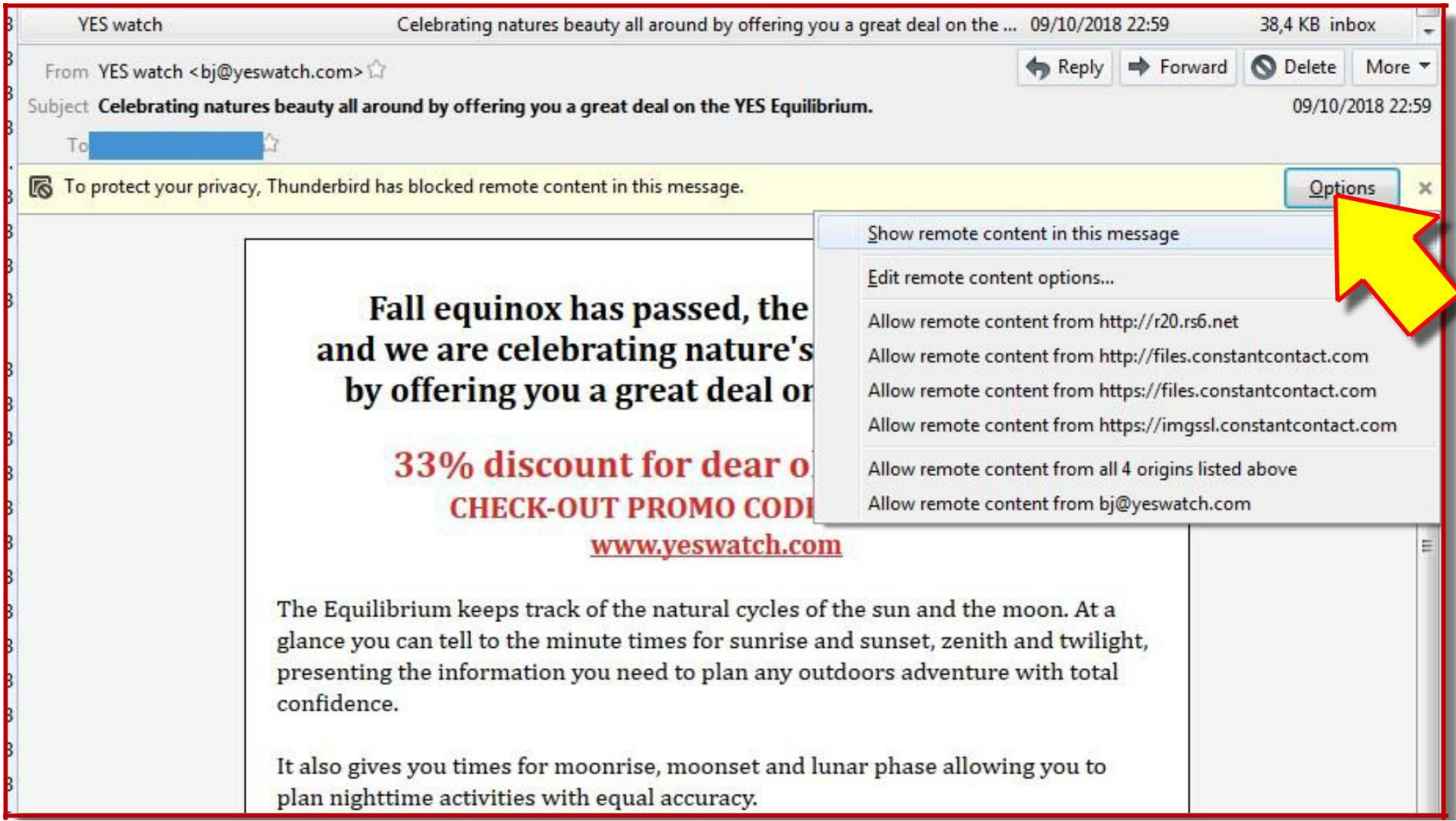
E comunque ricordarsi di cambiare periodicamente le password su tutti gli account online

ESEMPIO REALE




YES watch
Celebrating natures beauty all around by offering you a great deal on the ...
09/10/2018 22:59
38,4 KB inbox
From YES watch <bj@yeswatch.com>
Reply
Forward
Delete
More
Subject Celebrating natures beauty all around by offering you a great deal on the YES Equilibrium.
09/10/2018 22:59
This message may be a scam.
Options
1
2
Fall equinox has passed, the sky is sparkling
and we are celebrating nature's beauty all around
by offering you a great deal on the Equilibrium.
33% discount for dear ole customers.
CHECK-OUT PROMO CODE : SOLSTICE
www.yeswatch.com
The Equilibrium keeps track of the natural cycles of the sun and the moon. At a glance you can tell to the minute times for sunrise and sunset, zenith and twilight, presenting the information you need to plan any outdoors adventure with total confidence.
It also gives you times for moonrise, moonset and lunar phase allowing you to plan nighttime activities with equal accuracy.
The Equilibrium will also alert you to solstices, equinoxes and cross quarter days, and it does this for wherever you are on the planet. It is pre-programmed to 650 cities worldwide and automatically adjusts for DST and TZ. If you are way off the beaten track it can also be set by latitude and longitude. The EQ is perfect for traveling. At the push of a button extensive time data for your location will be displayed.
It has six alarms of which the sunrise and sunset alarm is particularly useful for


YES watch
Celebrating natures beauty all around by offering you a great deal on the ...
09/10/2018 22:59
38,4 KB inbox
From YES watch <bj@yeswatch.com>
Reply
Forward
Delete
More
Subject Celebrating natures beauty all around by offering you a great deal on the YES Equilibrium.
09/10/2018 22:59
To
To protect your privacy, Thunderbird has blocked remote content in this message.
Options
Fall equinox has passed, the sky is sparkling and we are celebrating nature's beauty all around by offering you a great deal on the Equilibrium.
33% discount for dear ole customers.
CHECK-OUT PROMO CODE : SOLSTICE
www.yeswatch.com
The Equilibrium keeps track of the natural cycles of the sun and the moon. At a glance you can tell to the minute times for sunrise and sunset, zenith and twilight, presenting the information you need to plan any outdoors adventure with total confidence.
It also gives you times for moonrise, moonset and lunar phase allowing you to plan nighttime activities with equal accuracy.
The Equilibrium will also alert you to solstices, equinoxes and cross quarter days, and


YES watch
Celebrating natures beauty all around by offering you a great deal on the ... 09/10/2018 22:59
38,4 KB inbox
From YES watch <bj@yeswatch.com>
Reply
Forward
Delete
More
Subject Celebrating natures beauty all around by offering you a great deal on the YES Equilibrium.
09/10/2018 22:59
To
To protect your privacy, Thunderbird has blocked remote content in this message.
Options
Show remote content in this message
Edit remote content options...
Allow remote content from http://r20.rs6.net
Allow remote content from http://files.constantcontact.com
Allow remote content from https://files.constantcontact.com
Allow remote content from https://imgssl.constantcontact.com
Allow remote content from all 4 origins listed above
Allow remote content from bj@yeswatch.com
Fall equinox has passed, the
and we are celebrating nature's
by offering you a great deal or
33% discount for dear o
CHECK-OUT PROMO CODE
www.yeswatch.com
The Equilibrium keeps track of the natural cycles of the sun and the moon. At a glance you can tell to the minute times for sunrise and sunset, zenith and twilight, presenting the information you need to plan any outdoors adventure with total confidence.
It also gives you times for moonrise, moonset and lunar phase allowing you to plan nighttime activities with equal accuracy.

YES watch Celebrating natures beauty all around by offering you a great deal on the ... 09/10/2018 22:59 38,4 KB inbox

Reply Forward Delete More

Celebrating natures beauty all around by offering you a great deal on the YES Equilibrium. 09/10/2018 22:59

To

The Equilibrium keeps track of the natural cycles of the sun and the moon. At a glance you can tell to the minute times for sunrise and sunset, zenith and twilight,

Unread: 0 Total: 92

regole generali

- mai rispondere allo spam
- disattivare la conferma automatica
- disattivare i contenuti remoti
- proteggere il browser (per accesso da web)
- attivare i filtri disponibili nel client (p.e. Thunderbird) e
- istruirli se adattativi

visualizzare le estensioni

in alcuni Sistemi Operativi ci portiamo dietro eredità di tempi più arretrati che per compatibilità non sono stati eliminati

esempio: il sistema di nomi di file MS-DOS secondo lo schema 8+3 (nome + estensione)

filename.txt

visualizzare le estensioni

oggi è possibile dare ai file nomi più lunghi e articolati:

abilitare le estensioni

PC 1

elenco.doc

in quale PC sono visualizzate le estensioni?

PC 2

elenco

abilitare le estensioni

PC 1

visualizzate)
(estensioni NON

elenco.doc

PC 2

(estensioni NON
visualizzate)

elenco

abilitare le estensioni

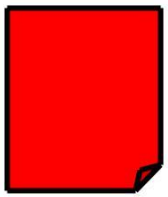
PC 1

elenco.doc

elenco.doc.exe

PC 2

elenco



elenco.doc

Anti-spam aziendale

al server di posta aziendale si affianca un server dedicato al servizio anti-spam

tramite un servizio on-line (a pagamento) si viene costantemente aggiornati sulle regole di filtraggio e sugli indirizzi degli spammer.

Denunciare gli spammer

in Italia lo spamming è vietato da varie leggi, a partire dalla *legge sulla privacy* 675/1996

diffondere virus è sanzionato dal Codice Penale (strumenti atti ad alterare il funzionamento di un sistema informatico)

per email italiane si può sporgere denuncia alla Naming e alla Registration Authority italiane (www.nic.it) e al Garante della Privacy

www.carabinieri.it/cittadino/consigli/tematici/giorno-per-giorno/questioni-di-privacy/spamming

purtroppo

- è tuttora diffusa la percezione che i reati informatici non sono considerati gravi (ossia non rilevanti penalmente)

- pochi presentano denuncia agli uffici di Polizia e all'Autorità Giudiziaria: spesso i titolari delle aziende reputano il danno d'immagine più grave di quello economico o pratico

- non è ancora diffusa una conoscenza corretta della sicurezza, per cui si va dal terrorismo psicologico all'indifferenza

- nemmeno vero è che solo i *big names* corrono rischi di attacco (MITM all'amministratore di condominio)

- ...oltretutto il livello di difesa ***potrebbe*** essere proporzionale alla grandezza dell'organizzazione

...se diventiamo noi spammer?

...se diventiamo noi spammer?

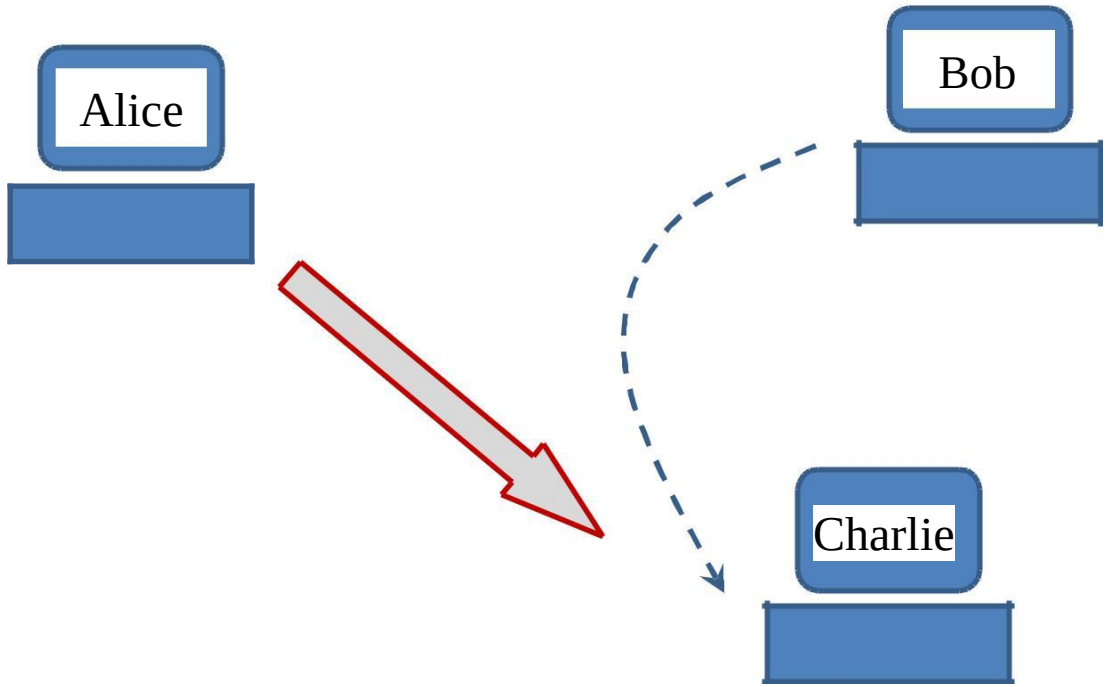
può accadere che -nonostante tutte le precauzioni- da un computer della nostra organizzazione escano messaggi o altri pacchetti che all'esterno risultano *indesiderati*

- come può accadere?

- virus
- vulnerabilità di sistema
- attacchi hacker
- software non aggiornato (CMS)
- effettivo spamming da un utente interno

Email spoofing

Bob
Charlie
Duncan
Hector
...
...



in questo caso il nostro indirizzo IP / dominio viene inserito in una **black list**

e

le email inviate da noi verranno rifiutate dai principali servizi di posta e dai servizi che hanno sistemi antispam correttamente configurati.

esistono numerosi siti dove verificare se il proprio IP / dominio è in blacklist

mxtoolbox.com/blacklists.aspx

www.spamcop.net/

http://barracudacentral.org/lookups

www.spamhaus.org/sbl/

...

la richiesta di essere cancellati dalla blacklist deve avvenire ovviamente solo DOPO aver eliminato tutti i problemi interni

esistono anche molti siti che si dedicano al *monitoraggio* delle blacklist; li usiamo anche per scegliere quali blacklist decidiamo di usare NOI per difenderci

(non dobbiamo affidare ciecamente ad altri la nostra protezione dell'email)

CONTROMISURE

SPF - Sender Policy Framework

sistema di validazione delle email progettato per individuare tentativi di *email spoofing.* Si crea una **lista** degli host autorizzati ad inviare email per un certo dominio *(mittente.com)*; questa lista viene inviata al DNS

il ricevente può confrontare il mittente del messaggio con la lista e se i conti non tornano può rifiutare l'email

CONTROMISURE

DKIM (DomainKeys Identified Mail)

metodo di autenticazione in cui *header* e *body* del messaggio sono protetti da crittografia. Il dominio *mittente.com* collega il proprio nome a ogni singola email allegando una firma digitale.

La chiave pubblica di mittente.com viene inserita nel DNS, e chi riceve un messaggio può quindi utilizzarla per verificarne l'autenticità.

CONTROMISURE

DMARC (*Domain-based Message Authentication, Reporting & Conformance)*

Sistema che usa i due precedenti per validare le email; attraverso il DKIM controlla che il messaggio arrivi dall'indirizzo dichiarato e non sia stato alterato; poi SPF verifica che l'host di partenza sia tra gli abilitati.

Se entrambi i test sono positivi il messaggio viene consegnato; altrimenti il mittente può aver stabilito che cosa farne (cancellazione, quarantena, segnato come spam...)

Inaugurato nel 2007 fra PayPal e Yahoo, e in seguito Gmail

https://dmarc.org/overview/

Government shutdown: TLS certificates not renewed, many websites are down

January 11, 2019

www.zdnet.com/article/government-shutdown-tls-certificates-not-renewed-many-websites-are-down

Over 80 government websites are down after TLS certificates expired and there's nobody on hand to renew them.

NASA, the US Department of Justice, and the Court of Appeals are just some of the US government agencies currently impacted.

- Websites with expired certificates where admins followed proper procedures and implemented correctly-functioning HSTS (HTTP Strict Transport Security) policies are down for good, and users can't access these portals, not even to browse for basic information.
- Government websites with expired TLS certificates but which didn't implement HSTS show an HTTPS errorin users' browsers, but this error can be bypassed to access the site via weakened HTTPS state.
- Nevertheless, visitors are warned not to log in or perform any sensitive operations on these sites, as traffic and authentication credentials aren't encrypted and could be intercepted by threat actors.

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3 – Opinion & Guidelines W29 EDPB – provvedimenti, trattamenti particolari

M3.3 Cookie policy (2002/58/EC - Directive on privacy and electronic communications)

Unità didattica

M3.3.1 Come proteggerci dai pericoli del web

Dott. Raffaele Grieco

Direttiva 2002/58/EC

Detta *Direttiva ePrivacy* (poi modificata dalla direttiva 2009/136/CE), tratta anche dei cookie (art.5), pur in modo generale senza fare riferimento a specifiche tecniche per memorizzare dati sul computer dell'utente.

cookies

piccoli file memorizzati sul nostro hard disk a cura del browser web, provenienti dai siti che visitiamo ma non solo

sono di 2 tipi: persistenti (scritti su disco) e temporanei (senza indicazione di scadenza, tenuti in RAM)

cookies

hanno 3 funzioni principali:

- gestione sessioni (il web è completamente *stateless*)
- personalizzazione (preferenze dell'utente, temi...)
- tracking (profilazione dell'utente)

sono specifici per browser (ottima ragione per separare i browser)

contenuto

- nome del cookie
- nome del sito che ha mandato il cookie
- scadenza del cookie (opzionale)
- codice univoco casuale che identifica il computer in quella particolare sessione
- informazioni tecniche (visibilità, cifratura)

e da terze parti:

- cookies per autenticare il profilo, per monitorare il traffico nel sito (*web analytics*), cookies relativi ai profili in *social networks*, cookies di network pubblicitari ma soprattutto **di tracciamento**

cookies

pericoli

nei cookie il sito può (contro tutte le raccomandazioni) memorizzare dati personali come username, password, numeri di carte di credito, conti bancari...

che un utente malevolo può trovare e prelevare

PROTEZIONE DEL BROWSER

Livelli di difesa

1. Bloccare gli script

2a. far cancellare cronologia e cookie a fine sessione
2b. abituarsi a pulizie in-session

4. isolare il browser

5a. installare un firewall sw
5b. usare un firewall hw

7. usare una Macchina Virtuale (VM)
8. separare il PC

1. BLOCCARE GLI SCRIPT

nei browser possono essere installate delle **estensioni** (‘componenti aggiuntivi’) che aggiungono funzionalità non previste dai progettisti.

Esempi:

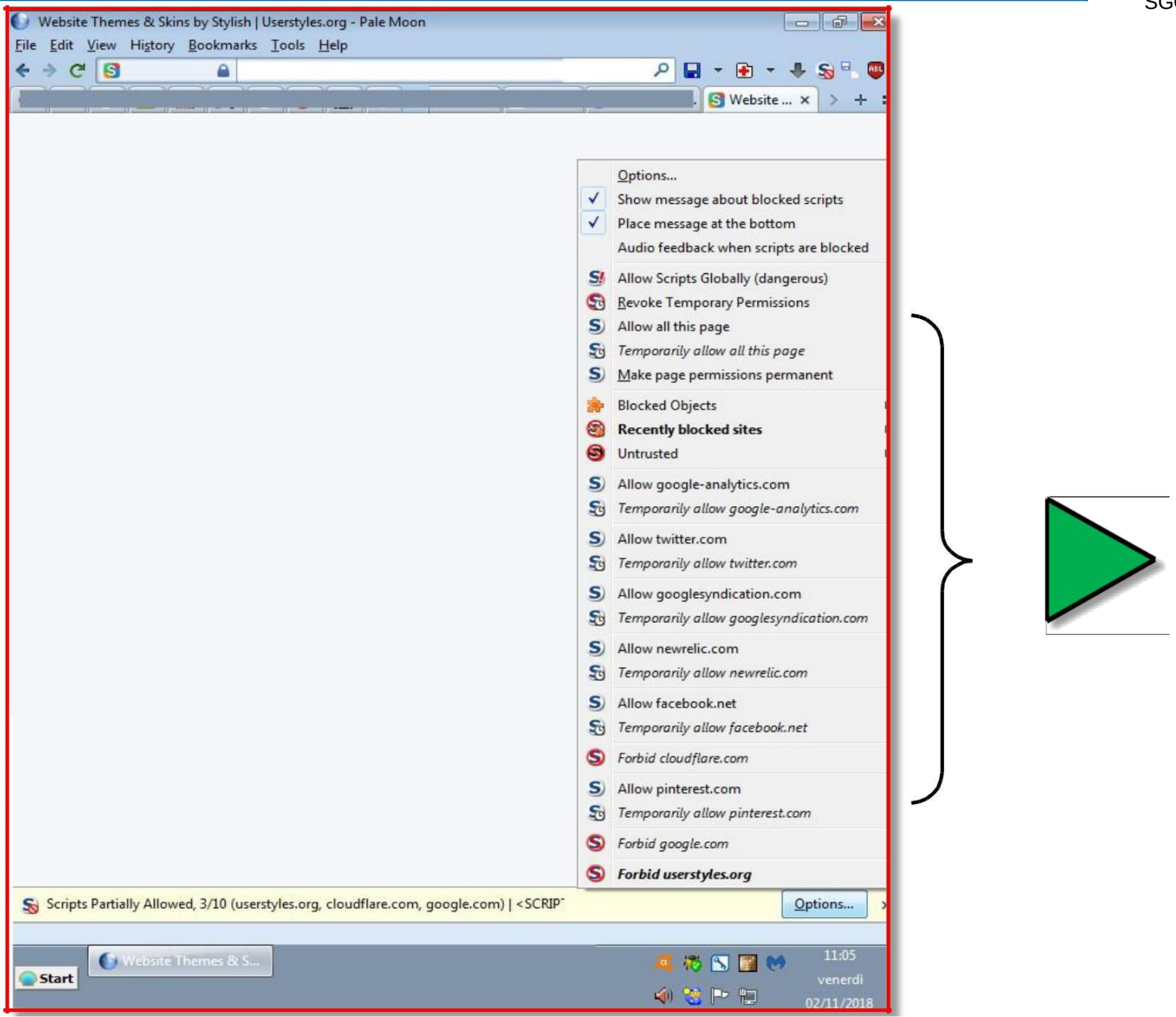
- Tool per scaricare video da YouTube e simili
- Gestori delle sessioni
- traduzioni automatiche
- ascoltare web radio
- cambiare aspetto del browser
- AD-blockers
- ...

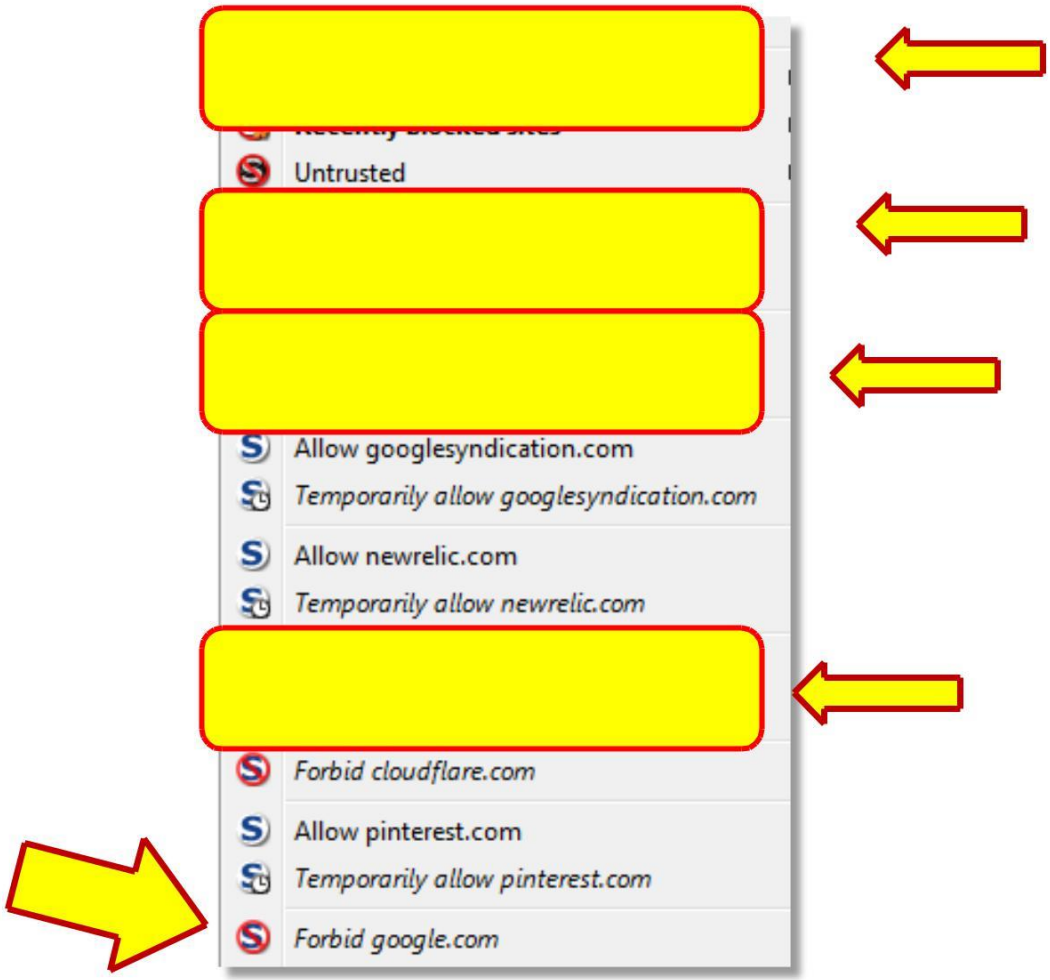
Esempio: *NoScript*

Estensione del browser Firefox e parenti

- Blocca l'esecuzione degli script
- Protegge da XSS e clickjacking
- Consente abilitazioni temporanee e definitive
- Consente blocchi definitivi

Raccomandata anche da Edward Snowden


Website Themes & Skins by Stylish | Userstyles.org - Pale Moon
File Edit View History Bookmarks Tools Help
Website ...
Options...
Show message about blocked scripts
Place message at the bottom
Audio feedback when scripts are blocked
Allow Scripts Globally (dangerous)
Revoke Temporary Permissions
Allow all this page
Temporarily allow all this page
Make page permissions permanent
Blocked Objects
Recently blocked sites
Untrusted
Allow google-analytics.com
Temporarily allow google-analytics.com
Allow twitter.com
Temporarily allow twitter.com
Allow googlesyndication.com
Temporarily allow googlesyndication.com
Allow newrelic.com
Temporarily allow newrelic.com
Allow facebook.net
Temporarily allow facebook.net
Forbid cloudflare.com
Allow pinterest.com
Temporarily allow pinterest.com
Forbid google.com
Forbid userstyles.org
Scripts Partially Allowed, 3/10 (userstyles.org, cloudflare.com, google.com) | <SCRIP
Options...
Start
Website Themes & S...
11:05
venerdì
02/11/2018


Untrusted
Allow googlesyndication.com
Temporarily allow googlesyndication.com
Allow newrelic.com
Temporarily allow newrelic.com
Forbid cloudflare.com
Allow pinterest.com
Temporarily allow pinterest.com
Forbid google.com

"Firefox bloccherà tutti gli script che tracciano gli utenti nel Web"

Mozilla li odia perché rallentano la navigazione.

www.zeusnews.it/n.php?c=26655

«*Il tracciamento rallenta il web*» afferma Mozilla.- *«Uno studio di Ghostery dimostra che il 55,4% del tempo necessario a caricare un normale sito web viene passato a caricare tracker di terze parti. Per gli utenti che si trovano a usare reti lente, l'effetto può essere anche peggiore»*.

A partire da Firefox 63, quindi, tutti gli script che richiederanno più di cinque secondi per il caricamento verranno bloccati.

2. PULIZIE

oltre ai cookie (visti prima), che possono inficiare la privacy,

La **cronologia** permette anche localmente di sapere quali siti abbiamo frequentato

Un rimedio ovvio è impostare i browser affinché:

- Cancellino la cronologia all'uscita
- Accettino solo cookies dai siti visitati
- Eliminino ogni altro tipo di traccia della *navigazione*

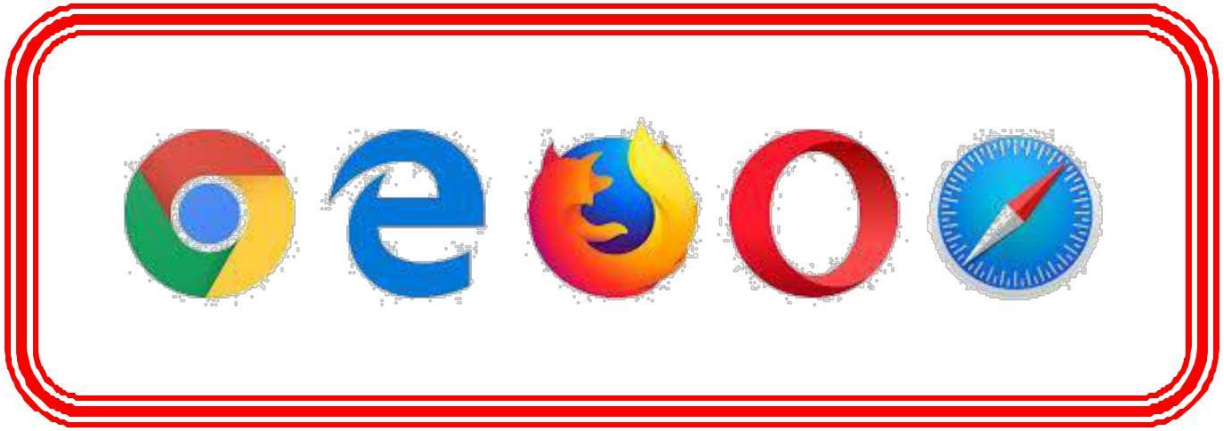
È anche bene che l'utente si abitui a non fare lunghe sessioni di accesso al web, o almeno 'spezzarle' chiudendo e riaprendo il browser a intervalli (se ha fatto quanto sopra)

- staccare la connessione quando non serve

Programmi di pulizia 'general purpose'; spesso hanno anche l'opzione per *ripulire* il browser

- Ccleaner (Crap Cleaner)
- Total PC Cleaner
- Glary Utilities
- Eusing registry cleaner
- Ashampoo WinOptimizer

3. ISOLARE IL BROWSER

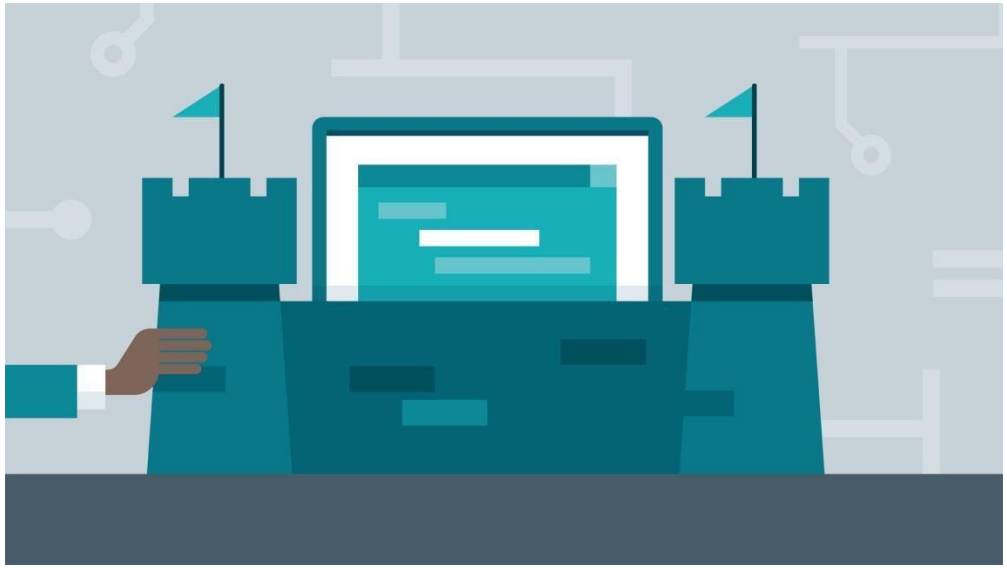


- Esistono programmi appositi che isolano il browser dal sistema operativo sottostante (o meglio il viceversa) facendolo eseguire in una **sandbox**.

- Eventuali danni saranno limitati alla sandbox, cioè al browser

- I problemi per la privacy sono trattati nel modulo apposito

4. IL FIREWALL



Funzione principale del **firewall** è limitare (al limite annullare) il traffico potenzialmente pericoloso, applicando:

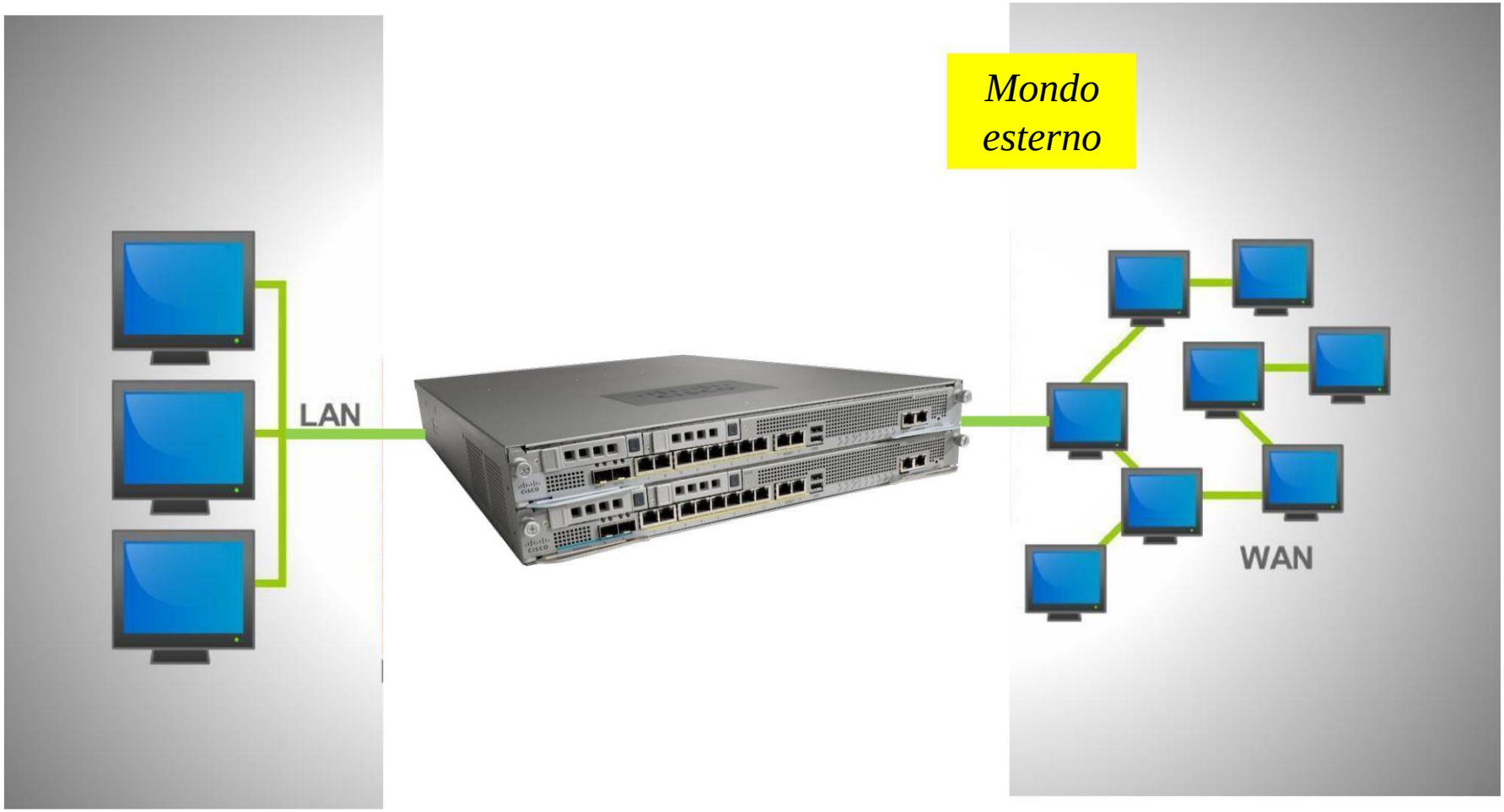
- Filtraggio degli indirizzi
- Suddivisione in sottoreti
- Blocco di tentativi di accesso dall'esterno
- ...

Per impedire ai dipendenti di accedere a siti non pertinenti col lavoro si usano altri sistemi *(net filtering)*

FIREWALL HARDWARE

Home

Enterprise

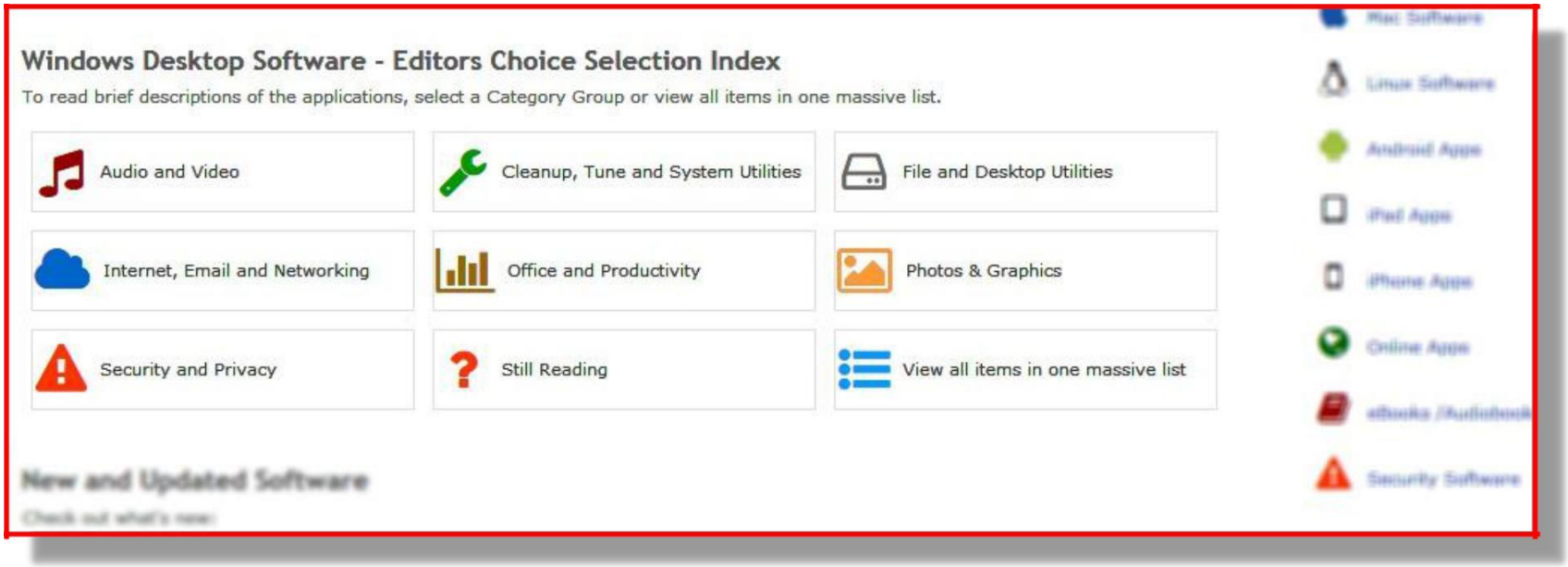

Mondo esterno
LAN
WAN

FIREWALL SOFTWARE

Ne esistono molti, per quelli free si può consultare il sito

www.techsupportalert.com

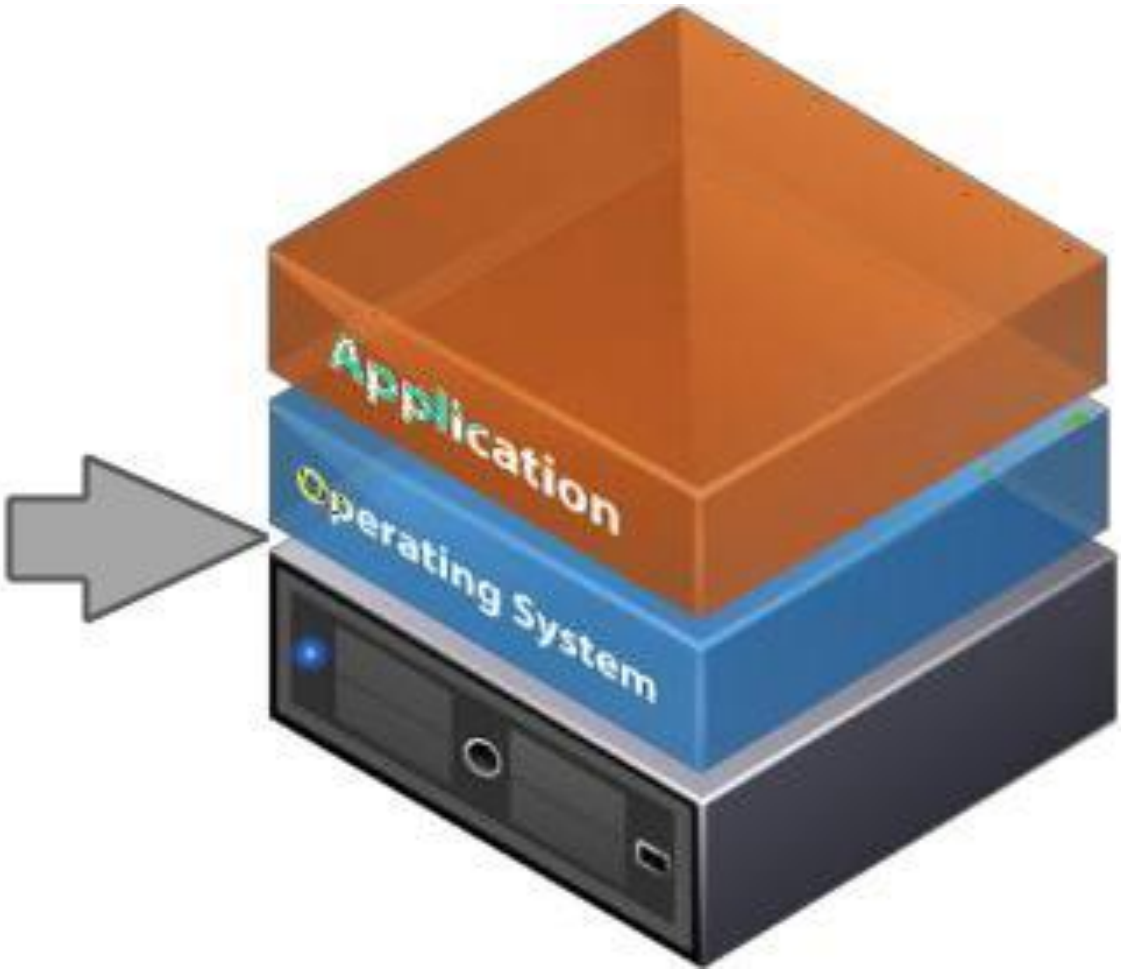
Per esempio nella sezione «best desktop applications for windows» si trova:

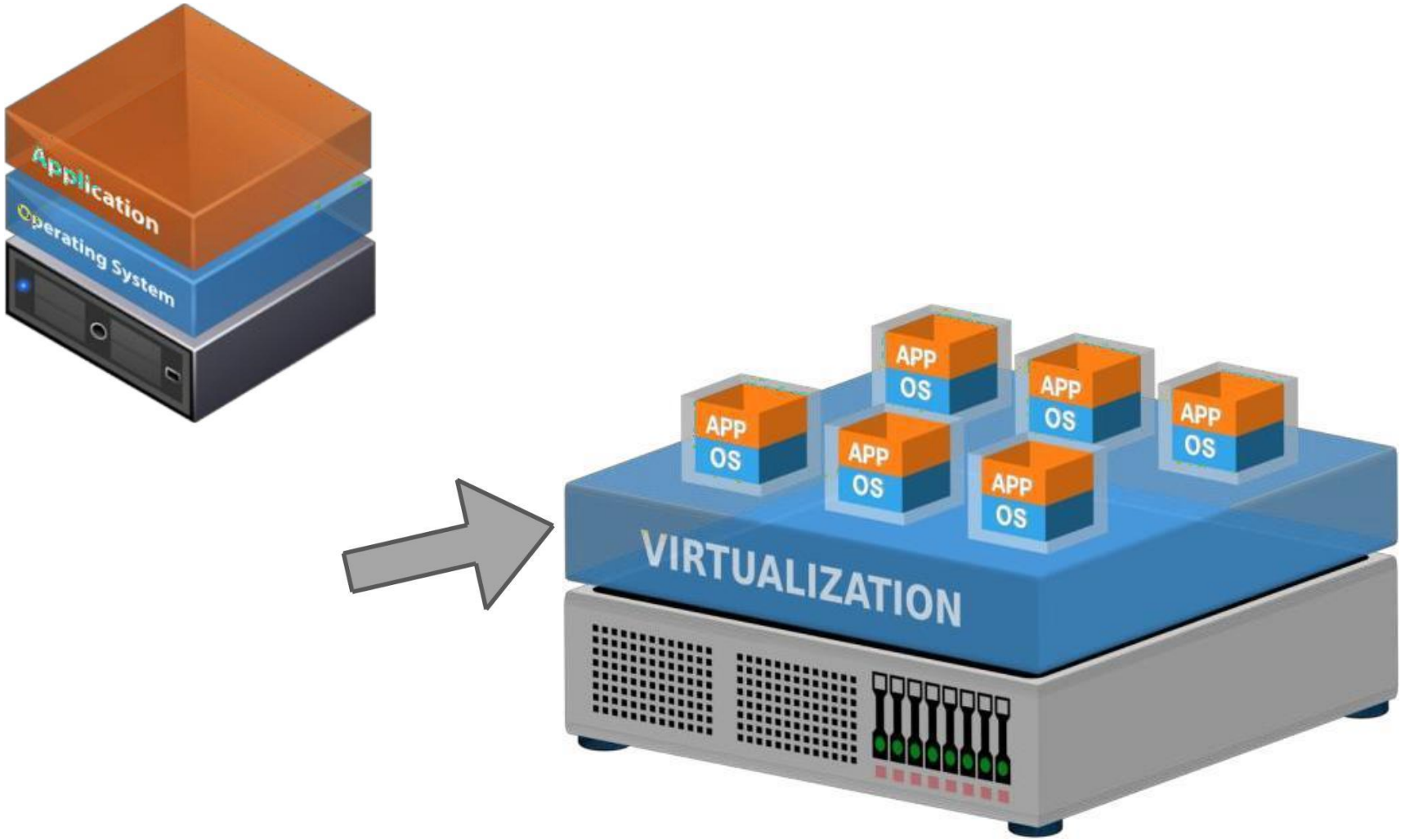


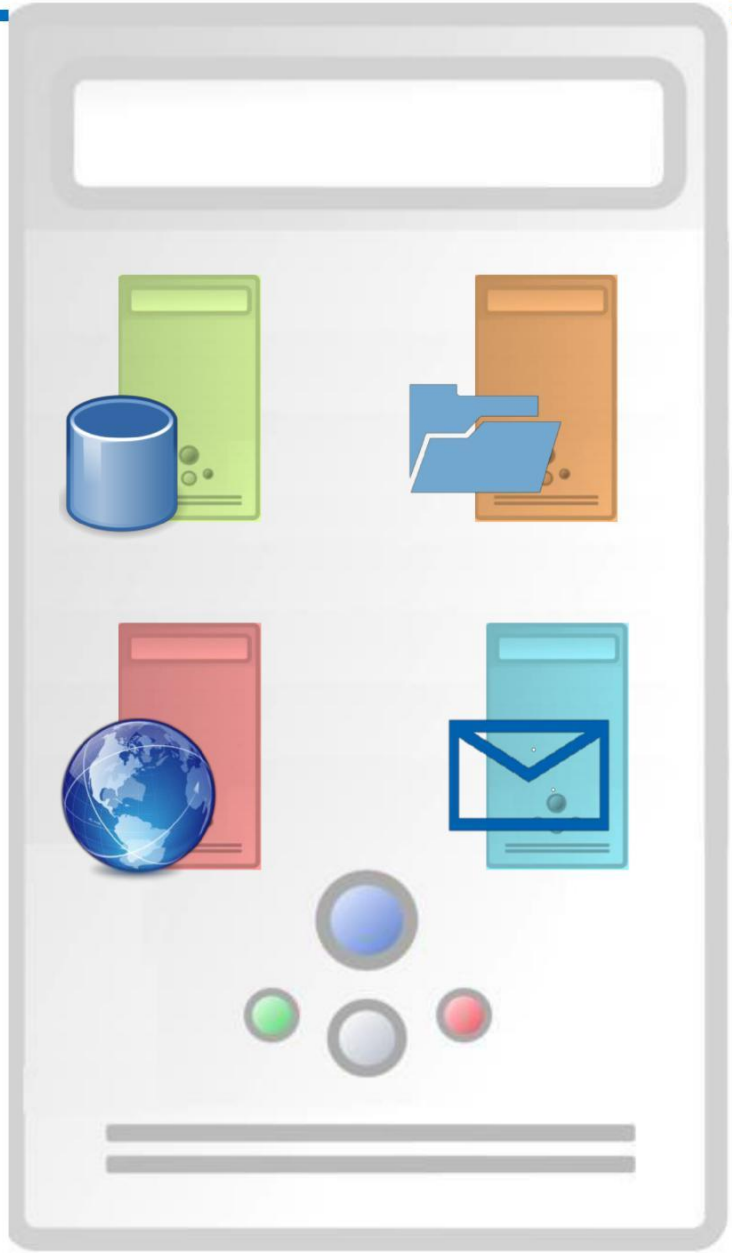
I firewall moderni possono avere numerose altre funzioni; alcune proteggono dalle minacce *interne*:

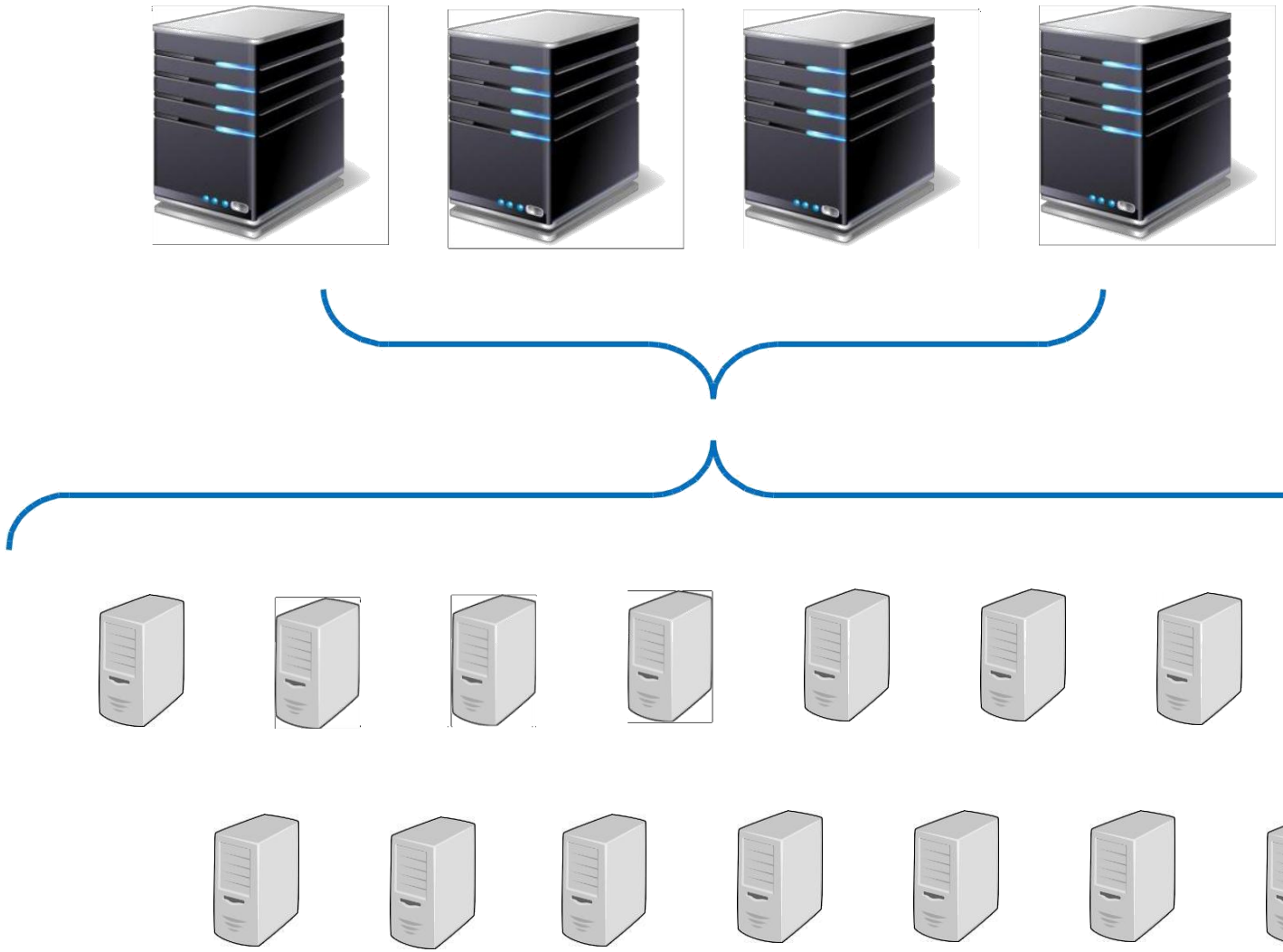
- Antivirus
- Packet sniffing
- VPN
- SSL inspection
- Data Leak prevention
- …

6. MACCHINE VIRTUALI


Application
Operating System


Application
Operating System
APP
OS
APP
OS
APP
OS
APP
OS
APP
OS
VIRTUALIZATION





con le VM si può

- usare tanti Sistemi Operativi diversi (cosa che non si potrebbe fare col semplice multitask)
- avere grande affidabilità
- ripartire la potenza dei server
- semplificare l'upgrade hardware
- semplificare la gestione dei server (aggiunte, modifiche, eliminazioni...)
- aumentare la sicurezza

gestori di VM

free

- Virtual Box
- Virtual PC
- VmWare player
- …

PRO

- Una VM isola il software dalla macchina hardware sottostante.
- Se la VM viene infettata, danneggiata o compromessa viene semplicemente eliminata e sostituita
- Si possono avere più VM ‘di scorta’ per affrontare particolari situazioni

CONTRO

- Occorrono server fisici (*host*) di caratteristiche adeguate (RAM, spazio disco, velocità, connessioni…)
- Si deve imparare a gestire un concetto nuovo

7. SEPARARE IL PC

ovvero

- usare un PC apposito per la navigazione e l'accesso alla rete
- essere pronti a sacrificarlo
- massima attenzione agli scambi di supporti

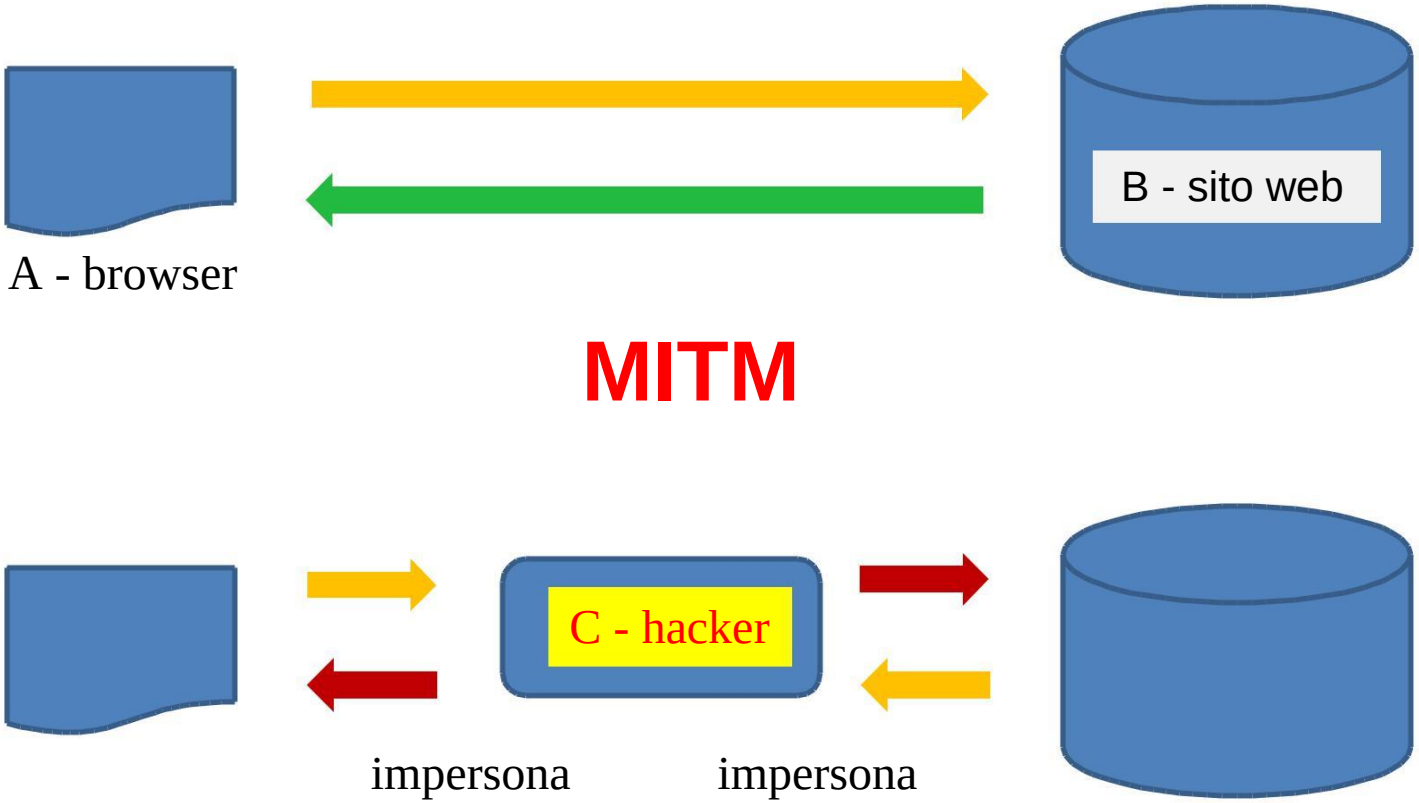
attacco Man-in-the-middle

(MITM)

attacco in cui il soggetto malevolo si intromette nelle comunicazioni tra 2 soggetti...

...senza che questi se ne accorgano

web browsing normale



canali di attacco

- falle nel browser (mancato aggiornamento?)
- bug negli apparati comunicazione (router)
- intrusione DHCP (DHCP spoofing)
- Falle nel DNS (DNS spoofing)
- simulazione di un hotspot WiFi pubblico (smartphone configurato per collegarsi automaticamente a un segnale forte)

esempi

- caso del router Belkin (2003)
- browser Nokia Xpress (2013)
- truffa della fattura con falso IBAN

DIFESE

- evitare le connessioni Wi-Fi gratuite (e non solo...)
- utilizzare plug-in per browser che forzino l'https, come HTTPS Everywhere o ForceTLS
- attivare la crittografia tra client e server (email)
- usare un secondo canale sicuro di verifica
- guardarsi dalla *evil maid*

DIFESE

- DNSSEC: estensioni DNS protette
- Infrastrutture a chiave pubblica (PKI)
- esame della latenza
- usare un *intrusion detection system* (IDS), anche se porta falsi positivi

USA, Russia e Cina fuori dalla "Convenzione di Ginevra" del cyber-spazio

Il **Paris Call for Trust and Security in Cyberspace**, nelle intenzioni, sarebbe dovuto essere un vero e proprio accordo globale per contrastare il dilagare del cyber-crimine. La "chiamata", però, non ha avuto un grande successo.

i governi maggiormente coinvolti non firmano il trattato di "non belligeranza" su Internet.

www.securityinfo.it/2018/11/13/usa-russia-e-cina-non-entrano-nella-convenzione-di-ginevra-del-cyber-spazio/

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3 – Opinion & Guidelines W29 EDPB – provvedimenti, trattamenti particolari

M3.4 E-Regulation: Nuove prospettive

Unità didattica

M3.4.1 Identificazione e autenticazione

Dott. Raffaele Grieco

definizione AGID

L'**identificazione** elettronica è un processo in cui si usano i dati di autenticazione personale in forma elettronica per identificare univocamente: una persona fisica e una persona giuridica.

L'**autenticazione** elettronica è il processo che permette di assicurare il riconoscimento dell'utente elettronico.

www.agid.gov.it/it/piattaforme/eidas/identificazione-autenticazione-elettroniche

L'**autenticazione** è diversa:

dall'**identificazione** (accertare che l'utente sia conosciuto dal sistema)

e dall'**autorizzazione** (dare a un utente il diritto ad usare specifiche risorse, sulla base della sua identità).

usi

- logon locale (a una PdL o un server)
- accesso a servizi online
- SPID - Sistema Pubblico di Identità Digitale

difesa dati personali

difesa dati sensibili > GDPR

difesa valori monetari (wallet)

Tentare di accertarsi dell'identità di qualcuno può basarsi su 3 principi:

- **conoscenza** (password, informazioni)
- **possesso** (token, tool di prossimità)
- **fisicità** (biometria)

variano per affidabilità, costi, velocità

ACCOUNT e PASSWORD

account locali

In un PC *(PdL)* gli account utente sono di 2 tipi di base:

- utente normale (per il lavoro quotidiano)
- amministratore (per la gestione del sistema)

La distinzione si fa per motivi di sicurezza e gestione

Nei **server** si può accedere con 2 tipi di account amministratore:

- locale ("di macchina")
- di dominio

pessima abitudine: condividere per semplicità e comodità l'account di amministratore locale tra più utenti

regole di base

- accedere col proprio account solo alla propria postazione (pericolo di keylogger, ...)
- Non dare MAI nessuna password a nessuno per nessun motivo
- Non scriverla mai
- cambiarla seguendo le indicazioni (frequenza, lunghezza, variazioni cicliche) date dall'amministratore e dal buon senso
- Non ri-utilizzarla per servizi online (sniffer)
- proteggere fisicamente la PdL o il server

GDPR

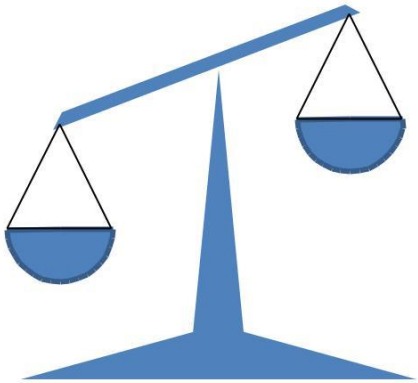
Per ottemperare al GDPR, occorre rispettare il principio di *accountability*: ognuno deve essere responsabile di tutte e sole le proprie azioni riguardo i dati.

- L'amministratore *di macchina* deve essere unico e la sua password depositata in maniera sicura in caso di necessità
- tutti gli account devono essere tracciati con i **log**
- i log devono essere protetti e conservati

PASSWORD

- Uso
- Errori
- Pericoli

Bilanciamento tra facilità di memorizzazione e sicurezza



Here's Why *[Insert Thing Here]* Is Not a Password Killer

Despite its many flaws, the one thing that the humble password has going for it over technically superior alternatives is that everyone understands how to use it. Everyone.

www.troyhunt.com/heres-why-insert-thing-here-is-not-a-password-killer/

regole elementari

- **MAI** scriverle(*)
- Cambiarle con frequenza *opportuna*
- Non riutilizzarle (localmente o per altri account)
- **Non** usare: nomi, targhe, sigle, parole da dizionario...
- *Depersonalizzarle*

regole elementari

MAI DARE

NESSUNA PASSWORD

a **NESSUNO**

per **NESSUN MOTIVO**

regole elementari

nessuno agg. e pron. indef. – **1.** Neanche uno; usato solamente al singolare, per escludere in maniera assoluta esistenza o presenza o altra qualità o condizione di persona, animale, o cosa.

regole elementari

*"**Fai sempre attenzione a chi chiede i tuoi dati.** Assicurati di non rispondere mai a richieste di informazioni **via email** sulla tua **carta di credito** (numero carta, data di scadenza o codice di sicurezza) e non digitare o inviare i tuoi codici di accesso al tuo conto o il tuo PIN dispositivo. ******** **non lo fara' mai**. Leggi i nostri consigli di sicurezza"*

(banca)

Errori comuni

- Cambiarla *troppo* spesso
- Similitudini fra successive
- Usare una regola troppo semplice per generarla
- Usare *argomenti* personali
- Inserirla dove non dovuto

- Cambiarla il venerdì

Password test

	memoria	sicurezza
1980-straker	☐	☐
SurAnoviremblAstirAn!	☐	☐
H2uYA%f$	☐	☐
nIITAKayAManABORa	☐	☐
NmDcDnVmRpUsOcLdVeS	☐	☐

(segue)

Requisiti di una password

La **lunghezza** è fondamentale per aumentare il numero di tentativi brute-force;

l'insieme dei simboli idem

Il numero di **combinazioni** (=tentativi) è dato dal numero degli oggetti (simboli) elevato al numero dei posti:

$$S_p$$

calcoli

Password di 4 caratteri con soli numeri:

10^4 = 10.000 (0000 – 9999)

Password di 4 caratteri con soli numeri:

10^4 = 10.000 (0000 – 9999)

4 caratteri: minuscole, maiuscole, numeri:

62^4 = 14.776.336

Password di 4 caratteri con soli numeri:

10^4 = 10.000 (0000 – 9999)

4 caratteri: minuscole, maiuscole, numeri:

62^4 = 14.776.336

10 caratteri, tutti i caratteri:

86^10 = 22130157888800000000 **($2{,}21 \times 10_{19}$)**

(2 seguito da 19 cifre)

non fare i furbi

www.schneier.com/blog/archives/2012/03/the_security_of_5.html

...if in the worst case users chose multi-word passphrases with a distribution identical to English speech, how secure would this be? Using the large Google n-gram corpus we can answer this question for phrases of up to 5 words. The results are discouraging: by our metrics, even 5-word phrases would be highly insecure against offline attacks

attacchi offline

Esporsi a un attacco a **dizionario** può indebolire la password di migliaia di volte,

ovvero la velocità di ricerca di un programma apposito aumenta di questo fattore

attacchi offline

PRTK

Password Recovery ToolKit

velocità di ricerca:

microsoft office	350.000	pwd/sec
WinZip 7.0	1.000.000	pwd/sec
WinZip 9.0	900	pwd/sec
PGP	900	pwd/sec

www.schneier.com/blog/archives/2007/01/choosing_secure.html

attacchi offline

Forensic Toolkit

fa una scansione dell'intero hard disk cercando tutte le stringhe stampabili: nei documenti, nelle e-mail, nel Registro di configurazione, nel file di swap, nei file cancellati.

Creato il dizionario, PRTK lo usa per cercare la password del file in esame.

La casa produttrice dichiara di trovare in questo modo oltre il 50% di password,

senza neanche iniziare la ricerca a forza bruta.

Password test

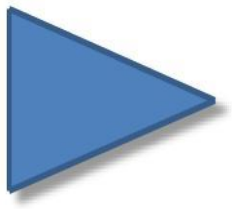
mem	sic
1980-straker	
SurAnoviremblAstirAn!	
H2uYA%f$	
nIITAKayAManABORa	
NmDcDnVmRpUsOcLdVeS	

Password test

	mem	sic
1980-straker	8	1
SurAnoviremblAstirAn!	7	2
H2uYA%f$	2	4
nIITAKayAManABORa	7	2
NmDcDnVmRpUsOcLdVeS	9	3

Check

Esistono numerosi siti dove verificare la *robustezza* di una password...



1. Non immettervi mai una password *reale*
2. spesso non considerano fattori come l'attacco a dizionario
3. possono dare un senso di falsa sicurezza

CATTIVI ESEMPI

Attacco a MySpace

www.wired.com/2006/12/myspace-passwords-arent-so-dumb-2

Una falsa pagina di login a MySpace ha permesso agli attaccanti di entrare in possesso di 34.000 coppie di credenziali (nome / password):

- Il 17% delle password era lungo 6 caratteri o meno
- Il 65% era lungo 8 caratteri o meno
- La lunghezza media era 8 caratteri

(segue)

CATTIVI ESEMPI

Breach di MySpace

Le 20 password più comuni:

password1	123abc	princess1
abc123	baseball1	jordan23
myspace1	football1	slipknot1
password	123456	superman1
blink182	soccer	iloveyou1
qwerty1	monkey1	monkey.
fuckyou	liverpool1	

(*blink182* e *slipknot* sono band musicali)

CATTIVI ESEMPI

Lettura:
unmasked_ an analysis of 10 million passwords

The 50 Most Used Passwords

1. 123456	11. 123123	21. mustang	31. 7777777	41. harley
2. password	12. baseball	22. 666666	32. f*cky*u	42. zxcvbnm
3. 12345678	13. abc123	23. qwertyuiop	33. qazwsx	43. asdfgh
4. qwerty	14. football	24. 123321	34. jordan	44. buster
5. 123456789	15. monkey	25. 1234...890	35. jennifer	45. andrew
6. 12345	16. letmein	26. p*s*y	36. 123qwe	46. batman
7. 1234	17. shadow	27. superman	37. 121212	47. soccer
8. 111111	18. master	28. 270	38. killer	48. tigger
9. 1234567	19. 696969	29. 654321	39. trustno1	49. charlie
10. dragon	20. michael	30. 1qaz2wsx	40. hunter	50. robert

As you can see, and probably already know, the most common passwords are all shining examples of things that straight away pop into someone's mind when a website prompts him or her to create a password. They are all extremely easy to remember and, by virtue of that fact, child's play to guess using a dictionary attack. When Mark Burnett analyzed 3.3 million passwords to determine the most common ones in 2014 (all of which are in his bigger list of 10 million), he found that 0.6 percent were *123456*. And using the top 10 passwords, a hacker could, on average, guess 16 out of 1,000 passwords.

MINACCE

ovvero come carpire una password

- keylogger
- termoscan
- ingegneria sociale
- (BAD USB)
- Brute-force
- ...

lettura:
come sono entrata...

keylogger hardware

"USBHarpoon: il cavo che ti spia, nella migliore delle ipotesi"

Torna l'attacco BadUSB, ma in una versione rivista che lo trasforma in USBHarpoon: un cavo USB apparentemente innocuo e pericolosissimo.

www.securityinfo.it/2018/08/21/usbharpoon-il-cavo-che-ti-spia-nella-migliore-delle-ipotesi/

contromisure

- anti-keylogger
- tastiera su schermo
- autenticazione a 2 fattori
- limitare i tentativi
- PIN parziale
- proteggere i file da copie abusive
- (USB keyboard guard)

tastiere virtuali

anti-keylogger

New "Injection Mode" allows for use with programs that don't allow drag-drop, so Neo's SafeKeys v3 works with KeePass, Roboform, Opera, WoW and others!

Mouse Entry modes only - 100% protection against key logging

Configurable keyboard layout - tailor the layout to suit your language and needs

Disables Print Screen button, is at least 1% transparent and has invisible protective shield - offering the best possible protection against screen logging

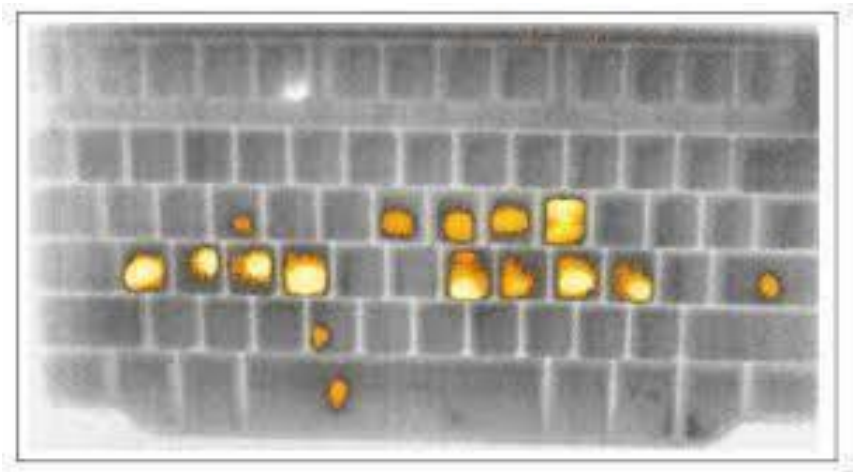
Clipboard is not used - 100% protection against clipboard logging

Password field is protected against field scraping

Transparency and automatic hiding makes dragging and dropping easier

...and your settings are remembered each time you run Neo's SafeKeys v3

thermal scan



limitare i tentativi

- esempio buono: PIN e PUK
- esempio cattivo: breach di iCloud del 2014 (ora max 10 ten

Autenticazione a 2 fattori

- Biometria (impronta digitale, scan retinico, voce…)
- SMS
- Token (chiavetta della banca, app…)

Autenticazione a 2 fattori

(2-factor authentication)

In alcuni casi conviene attivarla;

Anche se ci sono altre controindicazioni, protegge dall'immissione della password nel campo *'username'* davanti a terzi (fatto purtroppo frequente), da keylogger e altre minacce

lettura: 2-factor authentication

Facebook Is Using Your Two-Factor Authentication Phone Number to Target Advertising

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

google authentication token

Google dichiara guerra alle password

Per Google il sistema attuale è troppo insicuro: la soluzione è una chiavetta con tutti i dati per l'identificazione. E assolutamente da non perdere.

www.zeusnews.it/n.php?c=18795

L'anello digitale che sostituisce le password

L'anello smart Motiv Ring farà felice chiunque non sopporti di dover pescare il telefono dalla tasca per ricevere i codici di accesso ai propri siti preferiti

www.wired.it/gadget/accessori/2018/10/24/anello-password-autenticazione-due-fattori/

24/10/2018

PASSWORD

"People suck at passwords. (...) They suck at making genuinely strong ones, they suck at making *unique* ones and they suck at handling them in a secure fashion."

This leads to everything from simple account takeover (someone else now controls their eBay or their Spotify or whatever else), to financial damages (goods or services bought or sold under their identity) to full on data breaches (many of these occur due to admins reusing credentials). There is no escaping the fact that passwords remain high-risk security propositions for the vast majority of people.

www.troyhunt.com/heres-why-insert-thing-here-is-not-a-password-killer/

creare una password decente

Password hint

Livelli di password

Variare la complessità della P. in funzione della sicurezza richiesta:

1. protezione entry-level
2. protezione impegnativa
3. protezione massima

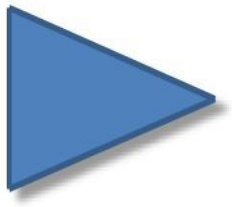
valutazione

- password del PC
- archivio criptato
- account di e-commerce (Amazon)
- account della banca

regola + dato base

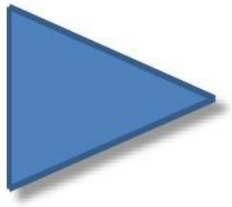
Si parte da un **dato base** (qualcosa semplice da tenere a mente o che si possa ricavare o ricostruire facilmente, ma da non rivelare mai)

e ci si applica una **regola**, che può essere anche scritta (!)



esempio

Tm8!Tr9"Te0£Te0$Cg1%Ty3&



regola + dato base

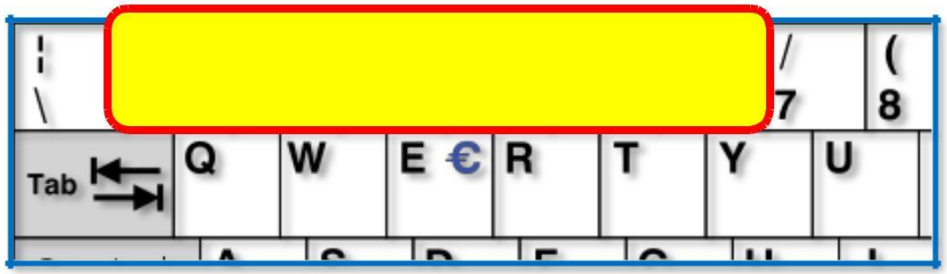
la *storia della seconda guerra mondiale*

di W. Churchill

- *The Gathering Storm* (1948)
- *Their Finest Hour* (1949)
- *The Grand Alliance* (1950)
- *The Hinge of Fate* (1950)
- *Closing the Ring* (1951)
- *Triumph and Tragedy* (1953)

Tm8!Tr9"Te0£Te0$Cg1%Ty3&

regola + dato base



- *The Gathering Storm* (1948)
- *Their Finest Hour* (1949)
- *The Grand Alliance* (1950)
- *The Hinge of Fate* (1950)
- *Closing the Ring* (1951)
- *Triumph and Tragedy* (1953)

Tm8! Tr9" Te0£ Te0$ Cg1% Ty3&

tgs8^HIO9?eal0=THF0)lhi1(ida3/

tecnica indicata per password
importantissime ma usate poco

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3 – Opinion & Guidelines W29 EDPB – provvedimenti, trattamenti particolari

Unità didattica

M3.5 Biometria e firma grafometrica

Dott. Raffaele Grieco

biometria

meccanismo di sicurezza usato per autenticare gli utenti e fornire accesso a un sistema (tip. informatico), basandosi sulle caratteristiche fisiche del singolo individuo.

Può essere fisiologica (volto, impronte digitali, impronta retinica) o comportamentale (firma, impronta vocale, movimenti...), meno stabile - risente dello stato psicologico

strumenti biometrici

- Lettore di impronta digitale
- Scanner di impronta retinica
- Lettore di impronta della mano
- Sistema di riconoscimento vocale

Rilevatori biometrici

Smartphone

- Lettori di impronta *(Toshiba G500 e G900, Motorola Atrix, Iphone 5S, Galaxy S5...)*
- Face ID (iPhone X)
- Iride (Galaxy S8)

www.news18.com/news/india/motorola-atrix-had-a-fingerprint-scanner-two-years-before-iphone-5s-638036.html

Il 2017 ha visto oltre mezzo miliardo di account rubati nel mondo e poco meno di 17.8 milioni di domini violati. Di fronte alle numerose violazioni dei dati personali sensibili, i consumatori riconoscono ormai ***l'inadeguatezza delle password tradizionali****, spesso vulnerabili*

iquii.com/2018/03/08/riconoscimento-biometrico/

La complessità e l'insicurezza dei sistemi per la sicurezza online attualmente in uso hanno spinto sempre più i consumatori a rinunciare nella finalizzazione di un acquisto.

Secondo uno studio di Mastercard e Oxford University, ***il 93% dei consumatori preferisce ricorrere alle tecnologie biometriche*** *piuttosto che all'uso di password per l'autenticazione dei pagamenti.*

newsroom.mastercard.com/eu/it/press-releases/mastercard-presenta-la-roadmap-per-garantire-pagamenti-piu-sicuri-e-innovativi-in-un-mondo-sempre-piu-digitale/

Firma grafometrica

Considerata una Firma Elettronica Avanzata

La Firma Grafometrica è un processo che prevede:

- legare univocamente il firmatario del documento alla firma
- il controllo esclusivo da parte del firmatario sul sistema di firma
- la possibilità di verificare che il documento sottoscritto non sia stato modificato dopo la firma

- Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche, su eur-lex.europa.eu.

- Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche, su camera.it.

- DLGS 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale, su parlamento.it.

- DLGS 30 dicembre 2010, n. 235 - Modifiche ed Integrazioni (PDF), su www1.interno.it.

www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4538440

Verifica preliminare relativa al trattamento di dati biometrici derivante dall'utilizzo, nell'ambito del contesto **notarile**, di un sistema di firma "grafometrica" - 25 novembre 2015 [4538440]

La firma grafometrica comprende molti parametri in più rispetto alla firma su carta (pressione, velocità, accelerazione, ritmo...)

E alcuni dispositivi rilevano persino quelli ‘aerei’ cioè quando lo strumento non è in contatto con la superficie sensibile ("invisibili")

Hardware

i dispositivi per la firma grafometrica non sono tutti uguali:

variano per sensibilità, risoluzione, campionamento, dati disponibili (ductus)

compatibilità

per far sì che la firma grafometrica possa essere compresa ("letta") da strumenti diversi nel 2014 è stato creato uno standard:

ISO/IEC 19794-7

che stabilisce come devono essere rappresentati i dati biometrici relativi

Rilevamento biometrico in ufficio?

I sindacati non sempre sono d'accordo...

Badge biometrico dipendenti, la Cassazione conferma sanzione da 66 mila euro ad un'azienda

www.privacy.it/2018/10/16/badge-biometrico-dipendenti-cassazione/

Cardarelli, sindacato in protesta: «No al marcatempo con impronte»

www.ilmattino.it/napoli/cronaca/chiudi_cardarelli_no_al_marcatempo_con_impronte-3326511.html

Dati biometrici. Ecco tutte le tutele previste dal Gdpr

www.privacyitalia.eu/dati-biometrici-ecco-le-tutele-previste-dal-gdpr/7393/

Controllo accessi (fisici) E il GDPR fa un passo avanti

www.secsolution.com/articolo.asp?id=613

Rilevazione presenze nella PA, usiamo la biometria? I problemi

www.agendadigitale.eu/sicurezza/rilevazione-presenze-nella-pa-con-la-biometria-usi-e-problemi/

I dati biometrici sono considerati informazioni "sensibili" che devono essere quindi gestite e protette seguendo le direttive e la legislazione in tema di protezione dei dati.

Inoltre i dati biometrici non possono essere revocati, come una password o una carta di credito

La conservazione di dati del genere a livello di rete aziendale crea la possibilità di un attacco al sistema di gestione dei dati biometrici

e può aprire le porte a un eventuale intruso, vanificando il ragionamento fatto in tema di necessità di accesso “fisico” ai terminali.

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3 – Opinion & Guidelines W29 EDPB – provvedimenti, trattamenti particolari

Unità didattica

M3.6 Amministratori di Sistema & Log

M3.6.1 Poteri e compiti di un amministratore di sistema

Dott. Raffaele Grieco

Distinzione fra

amministratore di un PC

e

amministratore di un Sistema Informatico complesso (insieme di server e altri dispositivi)

1 - Amministratore del PC

In un PC gli account utente sono di 2 tipi di base:

- utente normale (per il lavoro quotidiano)
- amministratore (per la gestione del sistema)

La distinzione si fa per motivi di sicurezza e gestione

è rischioso usare l'account amministratore per il lavoro quotidiano (perchè?)

l'utente normale può usare tutte le funzioni del PC che gli occorrono per il lavoro quotidiano, ma non quelle che:

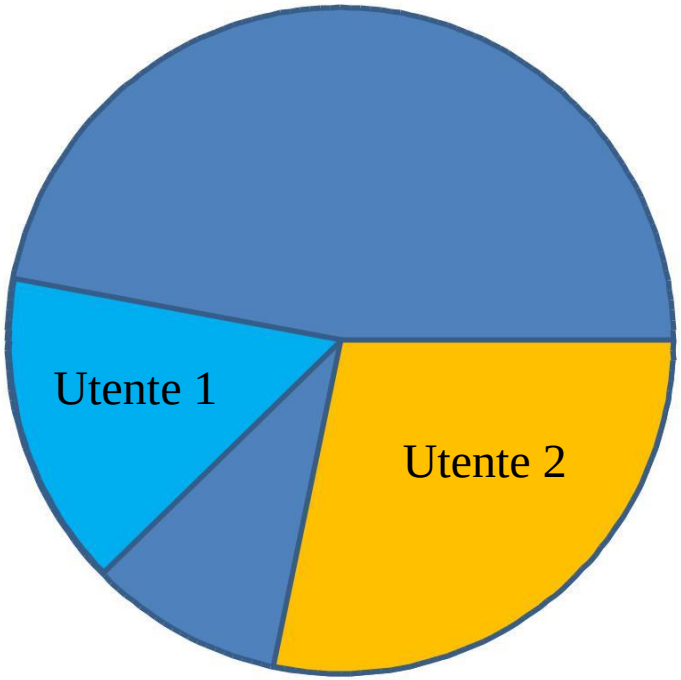
- gli permettano di intervenire su altri utenti
- comportano rischi
- richiedono scelte a livello superiore o
- implichino conoscenze tecniche specifiche

l'Amministratore del PC può:

- installare programmi
- modificare la configurazione
- alterare il funzionamento della macchina
- intervenire su funzioni tecniche

esempi: password, rete, dominio, quota disco, scelte prestazionali

Disk quota



- se l'utente avesse i permessi per svolgere le funzioni di Amministratore, potrebbe causare seri inconvenienti al proprio PC ma anche al resto del Sistema Informatico...

  ...magari non intenzionalmente

- esempio: se un virus entra in un PC in cui è attivo un utente di livello Administrator, avrà la possibilità di eseguire codice, accedere a zone di memoria protette e fare notevoli danni.
- se l'utente non è Administrator le possibilità di azione del virus sono molto limitate (bug di sistema permettendo).

2 – Amministratore di sistema

Nel GDPR uno dei principi di base è quello dell'***accountability***, ossia della individuazione del responsabile (prassi tipicamente occidentale)

questo si riflette immediatamente nella gestione degli account e della registrazione degli eventi (log)

Amministratore di sistema

Provvedimento del Garante del 27/11/2008:

"una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali"

(FAQ del provvedimento del 27.11.2008 del Garante per la protezione dei dati personali)

Che cosa deve intendersi per "amministratore di sistema"?

In assenza di definizioni normative e tecniche condivise, nell'ambito del provvedimento del Garante l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati (...)

Il Garante non ha inteso equiparare gli "operatori di sistema" di cui agli articoli del Codice penale relativi ai delitti informatici, con gli "amministratori di sistema": questi ultimi sono dei particolari operatori di sistema, dotati di specifici privilegi.

Amministratore di sistema

Nel nuovo Regolamento europeo sulla protezione dei dati personali (GDPR) non sembra ci sia un chiaro riferimento alla figura dell'amministratore di sistema nel processo di trattazione e custodia dei dati, pur trattandosi di una figura implicitamente richiamata, in alcune norme, per le sue specifiche competenze tecniche...

Amministratore di sistema

...ma

L'art. 32 del Regolamento descrive delle procedure altamente tecniche (cifratura dei dati personali, loro tempestivo ripristino in caso di incidenti, verifiche periodiche delle misure prese) che sicuramente lasciano intravedere una necessaria partecipazione di **personale specialistico esperto** nella gestione e nella trattazione informatica dei dati personali

Amministratore di sistema

Non può coincidere col DPO, che svolge autonome attività di audit nell'ambito della sicurezza informatica.

(ne parleremo nel modulo 5.2)

Tecnicamente, l'Amministratore di sistema si occupa di una molteplicità di funzioni che richiedono competenze variegate

In grandi organizzazioni non si tratta di una sola persona, ma talvolta addirittura di **squadre** che si occupano di vari aspetti (rete, server, applicazioni, database, sicurezza...)

Nella Pubblica Amministrazione: U.O.

esempi (U.O.)

1. gestione della rete (infrastruttura, accessi e autorizzazioni)
2. sicurezza fisica (firewall, filtraggio, backup)
3. gestione delle PdL
4. gestione dei Database
5. gestione del dominio (account, DC)

Assenze

(ferie, malattia, incarichi esterni...)

In un'organizzazione dove **non** sono presenti più persone che si occupano dello stesso compito (DB administrator, Network administrator, System manager...) si può far fronte ad eventuali situazioni di assenza del titolare conservando le necessarie password in buste sigillate affidate p.e. al dirigente

Usare il PC
come utente

L'utente 'normale' (non amministratore) ha delle limitazioni per le funzioni che può usare;

Tipicamente non può intervenire su tutto ciò che ha conseguenze sugli altri utenti, sulla sicurezza del sistema e sulla configurazione del PC

ESEMPI

L'utente normale può:

- Usare programmi applicativi
- Cambiare le impostazioni di personalizzazione (schermo, visualizzazione)
- Accedere alla rete e a Internet (nell'ambito dei limiti imposti p.e. dal web filtering)
- Creare file localmente

ESEMPI

L'utente normale NON può:

- Cambiare le impostazioni di rete (indirizzo, gateway, DNS, ...)
- Intervenire sulle impostazioni di sistema
- Installare programmi (rischio malware)
- ...

Le **autorizzazioni** dell'utente normale possono essere modificate dall'Amministratore, in caso di necessità;

È ovviamente opportuno, nel caso che esse siano ampliate, valutare a priori quali siano i rischi per la sicurezza delle operazioni e la privacy

Buona regola: **restringere** le autorizzazioni allo stretto indispensabile per svolgere i compiti assegnati (p.e. impedire di copiare file eseguibili da supporti esterni come CD o USB)

Nel caso (sconsigliato) che una postazione debba essere usata da più persone, occorre separare gli account e la visibilità dei dati di ogni account rispetto agli altri

Occorre anche educare gli utenti a rispettare delle regole di base per evitare problemi:

- bloccare il PC quando ci si assenta
- fare *log out* per pause più lunghe o al termine di una fase di lavoro
- gestire accortamente le password (v.)

Consigli per l'Amministratore

Impostare sempre una password per ogni account, anche quelli disabilitati

Dare regole sulle password per evitare che gli utenti ne scelgano di troppo semplici o cerchino di riutilizzarle

Trasformare gli account Microsoft in account locali

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3 – Opinion & Guidelines W29 EDPB – provvedimenti, trattamenti particolari

Unità didattica

M3.6 Amministratori di Sistema & Log

M3.6.3 I log di sistema e la loro conservazione

Dott. Raffaele Grieco

Con *log* si intende la raccolta di informazioni sul funzionamento dei sistemi informatici fatta **volontariamente** dall'utente proprietario del sistema (o suo delegato)

La raccolta fatta **da terzi** a insaputa dell'utente ricade nell'ambito di invasione della privacy o tentativo di hacking di un sistema

Finalità dei log

- sicurezza informatica
- supporto alle operazioni di sistema e di rete
- conformità con le normative specifiche
- Individuazione dei responsabili

I log sono lo strumento essenziale per risolvere un numero enorme di **problemi** che si possono avere in un sistema informatico

o

per migliorare le prestazioni e ottimizzare il rendimento del sistema...

...e purtroppo anche per compiere azioni illecite (furto di dati, sabotaggio, violazione della privacy...)

Il GDPR impone un limite di 72 ore per segnalare un *data breach*;

per accorgersi di un evento simile una delle armi principali è il monitoraggio dei log.

decreto del Garante per la Protezione dei Dati Personali

PROVVEDIMENTO del 27 novembre 2008

pubblicato sulla Gazzetta Ufficiale n.300 del 24.12.2008

...ogni azienda, dopo aver individuato i sistemi (dispositivi di rete, database, apparati di sicurezza...) che contengono i dati più critici deve prima di tutto nominarne gli **amministratori**, infine deve dotarsi di un sistema di **Log Management** che sia in grado di tracciare gli accessi degli operatori ai dispositivi ed alle applicazioni che gestiscono.

Il Garante ha introdotto l'obbligo per i titolari del trattamento dei dati di conservare gli "access log" degli amministratori di sistema, per almeno 6 mesi, in archivi immodificabili e inalterabili.

GDPR

L'analisi e la gestione dei log può essere compresa tra i criteri di valutazione dell’operato dei DPO

Tipi di log

- Log di riconoscimento e accesso
- Log di sistema
- Log di base dati
- Log di sicurezza
- Log di applicazione

Contenuti dei log

- Eventi attesi: quelli legati al normale funzionamento delle apparecchiature (orari di partenza e arresto di un processo, tempo di funzionamento, temperatura…)
- Eventi inattesi: accessi fuori orario, errori, parametri fuori scala, spazio esaurito…
- Eventi straordinari: guasti, intrusioni….

CASE STUDY

Esempio: sito web

il gestore può e deve usare i log per:

- adattare la configurazione al tipo di traffico
- migliorare le prestazioni del sistema dove richiesto
- profilare gli utenti (dove permesso)
- conservare traccia degli accessi per rintracciare autori di attacchi
- quantificare gli accessi al sito per motivi economici (CPM, campagne promozionali,...)

Tra i dati disponibili al gestore del sito ci sono:

- indirizzo IP e nome host
- data e ora dell'accesso
- browser e S.O. usato dal visitatore
- link di provenienza
- motore di ricerca utilizzato
- tempo di permanenza sul sito
- tempo di risposta del server
- numero delle pagine aperte
- file scaricati
- grandezza della pagina richiesta

Log di Apache

- %h Indirizzo IP del client
- %l Identità del client
- %u ID utente del client
- %t Marca temporale della data e ora di accesso.
- %r Informazioni sulle richieste HTTP (metodo, risorse richieste e versione di protocollo)
- %>s Codice di stato con il quale il server ha reagito alla richiesta
- %b Quantità di dati trasmessi in byte

- *Altre voci opzionali*

Log management

Conservazione

I log possono (e dovrebbero) essere conservati su una macchina differente da quella che li genera;

per esempio il protocollo **SysLog** è stato creato proprio per questa funzione

Molti fornitori di sistemi di log management salvano i dati sul proprio cloud

(quindi fisicamente inaccessibile ai dipendenti)

Provvedimento Garante Privacy del 27.11.2008
FAQ #12

12) Come va interpretata la caratteristica di inalterabilità dei *log*?Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di *log* sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito *software*. Il requisito può essere ragionevolmente soddisfatto con la strumentazione *software* in dotazione, nei casi più semplici, e con l'eventuale esportazione periodica dei dati di *log* su supporti di memorizzazione non riscrivibili. In casi più complessi i titolari potranno ritenere di adottare sistemi più sofisticati, quali i *log server* centralizzati e "certificati"

SIEM

security information and event management

SIM + SEM = **SIEM**

(non sono sinonimi)

SIM: *Security Information Management*

SEM: *Security Event Management*

SIM: *Security Information Management*

software utilizzato per automatizzare il processo di raccolta e gestione dei log non in tempo reale.

I dati raccolti vengono spediti ad un server centrale da agent installati sui vari dispositivi.

La conservazione di questi dati unita all'analisi degli stessi permette di generare report personalizzati

Più orientato a un punto di vista *storico*

SEM: *Security Event Management*

Più orientato a un punto di vista *real-time*

Fornisce monitor in tempo reale, raccolta e aggregazione di dati, una console per il controllo e la gestione degli eventi e sistemi di risposta automatica per problemi di sicurezza

Funzioni di un SIEM

- Raccolta dati (log)
- Normalizzazione dei dati
- Correlazione (con regole built-in o personalizzate)
- Report (per audit o analisi forense)
- Notifiche

un SIEM aiuta a individuare

- Accessi non autorizzati
- Violazioni delle policy di sicurezza
- Tentativi di attacco
- Intrusioni
- ...

esempi di allarme

virus - se un computer qualsiasi della rete individua un malware

attacco esterno - più di x *reject* o *deny* dallo stesso IP in un dato intervallo (p.e. 30 secondi)

intrusione - troppi tentativi di login errati su una postazione in 1 minuto

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3: Opinion & Guidelines W29 EDPB - provvedimenti, trattamenti particolari

Unità didattica

M3.7 WP 29 e linee guida sulle app

Avv. Ida Tascone

WP 29

- Era un organismo consultivo indipendente, composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione.
- Il gruppo di lavoro è stato costituito sulla base di quanto previsto dall'articolo 29 della direttiva europea 95/46/CE e aveva le seguenti finalità:
- Fornire un parere esperto agli Stati in merito alla protezione dei dati.
- Promuovere l'applicazione coerente della direttiva sulla protezione dei dati in tutti gli Stati membri dell'UE.

- Il WP29 è stato sostituito il 25 maggio 2018 dal Consiglio Europeo per la Protezione dei Dati (EDPB), ai sensi del Regolamento Europeo sulla Protezione dei Dati 2016/679 (GDPR).
- In questo primo incontro ci occuperemo di uno dei più importanti pareri espressi dal WP29 in tema di privacy connessa all'utilizzo dei dispositivi di ultima generazione: il Parere 02/2013 sulle applicazioni per dispositivi intelligenti (*Opinion 02/2013 on apps on smart devices o WP 202*), adottato il 27 febbraio 2013.
- Il testo completo può essere consultato in lingua inglese sul sito ufficiale del Garante della Privacy.

Linee guida app

- Il parere è, in buona sostanza, un compendio di linee-guida a cui gli sviluppatori di applicazioni per dispositivi intelligenti (principalmente smartphone e tablet, ma anche e-watch, televisori, automobili, allarmi, sistemi di domotica et al.) dovrebbero attenersi al fine di garantire il rispetto dei principi legati al trattamento dei dati personali:
- all'interno del documento viene chiarito il contesto giuridico applicabile al trattamento dei dati personali nelle varie fasi dello sviluppo, della distribuzione e dell'utilizzo delle applicazioni, con un focus particolare sui seguenti aspetti:
- Necessità di dotarsi delle informative adeguate al fine di fornire una informazione corretta agli utenti finali.
- Necessità di acquisire il consenso (ove applicabile).

Segue..

- Rispetto dei principi di limitazione della finalità e di minimizzazione dei dati.
- Necessità di adottare le adeguate misure di sicurezza volte a ridurre al minimo i rischi legati al *data breach*, agli accessi non autorizzati o ad altre violazioni.
- Rispetto dei diritti dell'interessato, con particolare riguardo alla possibilità di cancellazione della app e relativi dati.
- Definizione degli opportuni periodi di conservazione dei dati.
- Modalità di trattamento dei dati provenienti da minori ovvero ad essi relativi.

informativa

- Per quanto riguarda le informative, viene richiesta la presenza di una informativa sintetica che compaia immediatamente, ovvero al primo accesso, preferibilmente mediante un *pop-up o layer overlay*, ovvero una finestra che si sovrapponga all'interfaccia utente oscurando e disabilitando tutto il resto, contenente un link che rimandi alla Privacy Policy integrale.
- Questa raccomandazione, assieme al precedente Parere 04/2012 sulla *Cookie Consent Exemption (WP 194)* e al successivo *Working Document 02/2013 providing guidance on obtaining consent for cookies (WP 208)*, ha contribuito a porre le basi per il provvedimento dell'8 maggio 2014 del Garante della Privacy, volto a recepire in Italia quanto previsto dalla Direttiva Europea 2009/136/EC (*ePrivacy Directive*, impropriamente nota come *Cookie Law)* in materia di *Cookie*.

- E' importante notare come il parere attribuisca una serie di responsabilità specifiche agli *app store*, ovvero ai negozi virtuali che distribuiscono ovvero consentono l'installazione delle app (gratuite o a pagamento), sia in materia di sicurezza – come avremo modo di vedere in seguito – che in materia di presenza delle opportune informative privacy (sezione 3.7.2):

Le informazioni essenziali sul trattamento dei dati devono essere disponibili agli utenti prima dell'installazione dell'applicazione, tramite l'app store. In secondo luogo, le informazioni pertinenti sul trattamento dei dati devono essere accessibili anche dall'interno della app, dopo l'installazione. In qualità di responsabili congiunti del trattamento insieme agli sviluppatori per quanto concerne l'informazione, gli app store devono garantire che ogni applicazione fornisca le informazioni essenziali sul trattamento dei dati personali, verificando i link alle pagine con informazioni sulla privacy ed eliminando le applicazioni con collegamenti interrotti o comunque con informazioni non accessibili sul trattamento dei dati.

Consensi

- Per quanto concerne i consensi, il documento chiarisce la necessità di acquisire consensi diversi: quello relativo alla presenza dei *cookie tecnici*, ovvero che prevedono la "marcatura" del dispositivo utilizzato e che sono trattati all'interno della Direttiva Europea 2002/58/EC, e quello derivante dalla presenza dei *cookie di profilazione*, ovvero che prevedono la raccolta di dati relativi al comportamento dell'utente, per il quale vale quanto prescritto dalla Direttiva Europea 95/46/CE.
- Fatta salva questa importante considerazione, il parere chiarisce la possibilità di "fondere" questi due consensi in una singola *manifestazione di volontà libera, specifica e informata*, a patto di fornire una informativa adeguata.

..segue

- *È importante notare la distinzione tra il consenso richiesto per inserire o consultare informazioni nel dispositivo e il consenso necessario per legittimare il trattamento di diversi tipi di dati personali. Benché i due requisiti siano applicabili simultaneamente, ciascuno in virtù di una diversa base giuridica, sono entrambi soggetti alla condizione che si tratti di una "manifestazione di volontà libera, specifica e informata" (ai sensi della definizione all'articolo 2, lettera h), della direttiva sulla protezione dei dati). Di conseguenza, i due tipi di consenso si possono fondere nella pratica, durante l'installazione o prima che l'applicazione cominci a raccogliere dati personali dal dispositivo, purché l'utente sia reso consapevole in modo inequivocabile di quello a cui acconsente.*

Il parere chiarisce immediatamente cosa intende con il termine "libera", sottolineando la necessità di rispettare il diritto dell'utente di rifiutare il consenso ovvero di interrompere l'installazione:

- *Nel contesto dei dispositivi intelligenti, "libera" significa che l'utente deve poter scegliere se accettare o rifiutare il trattamento dei suoi dati personali. Quindi, se un'applicazione richiede il trattamento di dati personali, l'utente deve essere libero di accettare o rifiutare, senza trovarsi di fronte a uno schermo contenente un'unica opzione "Sì, accetto", per completare l'installazione; deve essere disponibile anche un'opzione "Cancella" o che comunque blocchi l'installazione*
- Risulta inoltre evidente come, in tutti i casi in cui il parere parla di necessità di acquisire il *consenso*, debba essere prevista anche la possibilità di revoca dello stesso, che deve avvenire in modo semplice ed efficace (cfr. sezione 3.8).

Per quanto riguarda i chiarimenti sul termine "specifica" il parere raccomanda l'adozione di un criterio di raccolta del consenso granulare in tutti i casi dove la app richiede il trattamento di tipologie diverse di dati:

"Specifica" significa che la manifestazione di volontà deve riferirsi al trattamento di un particolare dato o di una categoria limitata di dati. Per questo motivo, il semplice clic su un tasto "installa" non si può considerare un valido consenso per il trattamento di dati personali, in virtù del fatto che il consenso non può essere un'autorizzazione formulata genericamente. In alcuni casi, gli utenti sono in grado di fornire un consenso granulare, laddove il consenso è richiesto per ciascun tipo di dati ai quali l'applicazione intende accedere. Un simile approccio soddisfa due importanti requisiti giuridici: in primo luogo quello di informare adeguatamente l'utente in merito a elementi importanti del servizio e in secondo luogo quello di chiedere il consenso specifico per ognuno di essi. L'approccio alternativo per cui lo sviluppatore chiede ai propri utenti di accettare una lunga serie di termini e condizioni e/o politiche sulla privacy non costituisce un consenso specifico.

Una applicazione pratica di questa raccomandazione è evidente nel successivo *"esempio di consenso specifico"*, dove si evince come debba essere prevista la possibilità di esprimere un consenso separato per i servizi che prevedano la geolocalizzazione dell'interessato:

- *Un'applicazione fornisce informazioni sui ristoranti nelle vicinanze. Per l'installazione, lo sviluppatore deve ottenere il consenso. Per accedere ai dati di geolocalizzazione, lo sviluppatore deve chiede il consenso separatamente, ad esempio durante l'installazione o prima di accedere alla geolocalizzazione. Per consenso specifico s'intende il consenso limitato allo scopo specifico di informare l'utente in merito a ristoranti nelle vicinanze. Quindi è possibile accedere a dati di geolocalizzazione dal dispositivo solo quando l'utente utilizza l'applicazione a tale scopo. Il consenso dell'utente al trattamento di dati di geolocalizzazione non permette all'applicazione di raccogliere costantemente dati sull'ubicazione dal dispositivo. Questo ulteriore trattamento richiederebbe informazioni aggiuntive e un consenso separato.*

Limitazione e minimizzazione

- Per quanto riguarda i principi di *finalità* del trattamento e *minimizzazione* dei dati, il documento (sezione 3.5) chiarisce come le due cose procedano di pari passo: al fine di impedire trattamenti inutili e potenzialmente illeciti, gli sviluppatori di applicazioni devono valutare attentamente quali dati sono strettamente necessari per eseguire la funzionalità desiderata. A tale scopo, è bene che lo sviluppatore faccia attenzione a non introdurre improvvisi cambiamenti nelle condizioni fondamentali del trattamento.

esempio

Ad esempio, se una app originariamente aveva lo scopo di consentire agli utenti di scambiarsi e-mail, ma lo sviluppatore decide di modificare il modello di business e accorpa gli indirizzi e-mail degli utenti con i numeri telefonici di utenti di un'altra app. I rispettivi responsabili del trattamento dei dati a quel punto dovrebbero contattare singolarmente tutti gli utenti per richiedere il loro inequivocabile consenso preliminare per questa nuova finalità del trattamento dei loro dati personali.

sicurezza

- La sezione 3.6, dedicata alla sicurezza, è forse la meno incisiva, probabilmente per via del fatto che è molto difficile entrare nel merito delle *best-practices* in fatto di *software development* e/o *architecture design* in un documento di alto livello come questo.
- Al tempo stesso, vengono date alcune linee-guida degne di nota che è opportuno tenere presente fin dalla fase di progettazione dell'app o per meglio dire del servizio, nel pieno rispetto del concetto di *privacy by design*:

- Prima di progettare un'applicazione è importante decidere dove saranno archiviati i dati, con particolare riguardo alle implementazioni di servizi in modalità *client-server*, che prevedano cioè il trasferimento di dati presso un server remoto (ad es. in cloud).
- E' importante ridurre al minimo le linee e la complessità del codice e introdurre una serie dicontrolli volti a ridurre ovvero ad escludere il rischio di trasferimento o compromissione involontaria di dati.
- Tutti gli input dovrebbero essere convalidati per impedire casi di riempimento del buffer o episodi di attacchi di tipo *Brute-Force*, *DDoS* o *SQL Injection*.
- E' necessario implementare strategie adeguate per la gestione di patch di sicurezza e relative verifiche, periodiche e – se possibile – indipendenti.
- E' opportuno ricordare periodicamente agli utenti la necessità di effettuare gli aggiornamenti periodici della app alle ultime versioni disponibili, e ribadire alcune *best-practice* di portata generale come ad esempio l'importanza di evitare di utilizzare la stessa password per diversi servizi.
- Le applicazioni dovrebbero poter accedere esclusivamente ai dati di cui hanno veramente bisogno per rendere disponibile una funzionalità all'utente.

diritti

- Per quanto riguarda i diritti dell'interessato (sezione 3.8), il documento – oltre a riassumerli brevemente in termini di rettifica, cancellazione e opposizione al trattamento dei dati – sottolinea l'importanza di prevedere un sistema di disinstallazione della app che preveda anche la cancellazione di tutti i dati raccolti, sia localmente che sui server di produzione:
- *Deve essere possibile disinstallare le applicazioni eliminando nel contempo tutti i dati personali, anche dai server del responsabile del trattamento.*
- E' inoltre raccomandata la creazione, con puntuale pubblicazione nell'informativa, di un punto di contatto a cui l'utente possa rivolgersi al fine di poter far valere i propri diritti.

conservazione

- La sezione 3.9 è dedicata alla conservazione, i cui tempi specifici dovrebbero dipendere dallo scopo dell'applicazione e dalla rilevanza dei dati per l'utente finale. Inoltre, è previsto che gli sviluppatori prendano in considerazione le problematiche legate alla *retention* dei dati degli utenti che non usano l'applicazione da un lungo periodo di tempo: tale assenza può essere dovuta a una serie di situazioni potenzialmente pericolose, come lo smarrimento del dispositivo o la mancata disinstallazione della app (e relativi dati) a seguito di vendita, cessione o restituzione dello stesso all'azienda.
- Per tutti questi motivi, gli sviluppatori dovrebbero definire un periodo di tempo di inattività dopo il quale l'account dovrà essere considerato scaduto e garantire che l'utente ne sia informato. Alla scadenza di tale periodo di tempo, il responsabile del trattamento dovrebbe avvertire l'utente e dargli la possibilità di recuperare i dati personali: in caso di mancata risposta entro un periodo di tempo ragionevole, i suoi dati personali e relativi all'utilizzo dell'applicazione dovrebbero essere resi anonimi o cancellati in modo irreversibile.

Privacy by Design e Privacy by Default

Prima di concludere questa analisi è opportuno menzionare la preziosa definizione data (sezione 3.3.2) ai concetti di *Privacy by Design* e *Privacy by Default*, destinati a diventare punti chiave nel GDPR. Tale definizione è particolarmente rilevante in quanto altamente contestualizzata in relazione allo sviluppo di sistemi operativi, API e applicazioni:

Il concetto di "privacy by design", o privacy nella progettazione, è un principio importante a cui si fa riferimento indirettamente già nella direttiva sulla protezione dei dati e che, insieme alla "privacy by default", o privacy di default, emerge più chiaramente nella direttiva e-privacy e richiede ai produttori di un dispositivo o di un'applicazione di tenere conto della protezione dei dati fin dall'inizio della progettazione. La privacy by design è richiesta espressamente per la progettazione di apparecchiature di telecomunicazione, come previsto dalla direttiva riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione. Di conseguenza, i produttori di OS e dispositivi, insieme agli app store, svolgono un ruolo di notevole responsabilità nel fornire garanzie per la protezione dei dati personali e della vita privata degli utenti di applicazioni, anche assicurando la disponibilità di meccanismi adeguati per informare ed educare l'utente finale in merito a quello che le applicazioni possono fare e a quali dati sono in grado di accedere, nonché offrendo agli utenti le opportune impostazioni per modificare i parametri del trattamento.

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3: Opinion & Guidelines W29 EDPB - provvedimenti, trattamenti particolari

Unità didattica

M3.8 Trattamenti dati del personale di lavoratori

Avv. Ida Tascone

Privacy e lavoro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Cartellini identificativi

Nelle aziende private e pubbliche il lavoratore può essere dotato di un cartellino di riconoscimento.

Può essere eccessivo riportare per esteso tutti i dati anagrafici o le generalità complete del dipendente: a seconda dei casi può bastare un codice identificativo o il solo nome o solo il ruolo professionale

Comunicazioni

In ambito di lavoro privato per comunicare informazioni sul lavoratore ad associazioni di datori di lavoro, ex dipendenti o conoscenti, familiari, parenti occorre il consenso dell'interessato.

In ambito di lavoro pubblico è richiesta una norma di legge o di regolamento.

Bacheche aziendali

Nella bacheca aziendale possono essere affissi ordini di servizio, turni lavorativi o feriali.

Non si possono invece affiggere documenti contenenti gli emolumenti percepiti, le sanzioni disciplinari, le motivazioni delle assenze (malattie, permessi ecc.), l'eventuale adesione a sindacati o altre associazioni

3


Privacy
e lavoro
Le regole per il corretto trattamento dei dati personali
dei lavoratori da parte di soggetti pubblici e privati
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Privacy e lavoro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Principi generali

Il datore di lavoro può trattare informazioni personali solo se strettamente indispensabili all'esecuzione del rapporto di lavoro.

I dati possono essere trattati solo dal personale incaricato assicurando idonee misure di sicurezza per proteggerli da intrusioni o divulgazioni illecite.

Sul luogo di lavoro va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità delle persone garantendo la sfera della riservatezza nelle relazioni personali e professionali.

Le informazioni personali trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata dei lavoratori (ad esempio i dati sulla residenza e i recapiti telefonici) e dei terzi (ad esempio dati relativi al nucleo familiare per garantire determinate provvidenze).

I trattamenti di dati personali devono rispettare il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di informazioni personali e identificative.

Si deve inoltre rispettare il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori.

I trattamenti devono essere effettuati per finalità determinate, esplicite e legittime in base ai principi di pertinenza e non eccedenza.

Il trattamento di dati personali anche sensibili riferibili a singoli lavoratori è lecito, se finalizzato ad assolvere obblighi derivanti dalla legge, dal regolamento o dal contratto individuale (ad esempio, per verificare l'esatto adempimento della prestazione o commisurare l'importo della retribuzione).

2

Privacy e lavoro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Cartellini identificativi

Nelle aziende private e pubbliche il lavoratore può essere dotato di un cartellino di riconoscimento.

Può essere eccessivo riportare per esteso tutti i dati anagrafici o le generalità complete del dipendente: a seconda dei casi può bastare un codice identificativo o il solo nome o solo il ruolo professionale

Comunicazioni

In ambito di lavoro privato per comunicare informazioni sul lavoratore ad associazioni di datori di lavoro, ex dipendenti o conoscenti, familiari, parenti occorre il consenso dell'interessato.

In ambito di lavoro pubblico è richiesta una norma di legge o di regolamento.

Bacheche aziendali

Nella bacheca aziendale possono essere affissi ordini di servizio, turni lavorativi o feriali.

Non si possono invece affiggere documenti contenenti gli emolumenti percepiti, le sanzioni disciplinari, le motivazioni delle assenze (malattie, permessi ecc.), l'eventuale adesione a sindacati o altre associazioni

3

Privacy e lavoro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Pubblicazioni di dati del lavoratore sui siti web e sulle reti interne

In ambito di lavoro privato per pubblicare informazioni personali (foto, curricula) nella intranet aziendale e, a maggior ragione in internet, occorre il consenso dell'interessato.

In ambito di lavoro pubblico, le P.A., possono mettere a disposizione sui propri siti web istituzionali atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, solo se la **normativa di settore** preveda espressamente tale obbligo. In tal caso il datore di lavoro pubblico deve selezionare i dati personali da inserire in tali atti e documenti, evitando di divulgare dati eccedenti o non pertinenti, verificando, caso per caso, se ricorrono determinate informazioni che vanno **oscurate** dagli atti e documenti destinati alla pubblicazione.

I soggetti pubblici infatti sono tenuti a ridurre al minimo l'utilizzo di dati identificativi e di tutti gli altri dati personali e ad evitare il relativo trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante **dati anonimi** o altre modalità che permettano di identificare l'interessato solo in caso di necessità.

E' vietata la pubblicazione di qualsiasi informazione da cui si possa desumere lo stato di **malattia** o l'esistenza di **patologie** dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di **invalidità, disabilità** o handicap fisici e/o psichici.

In base alla normativa sulla **trasparenza** le P.A. devono pubblicare sui siti istituzionali **curricula, emolumenti** o **incarichi** di determinati soggetti (**dirigenti, consulenti, titolari di incarichi di indirizzo politico, ecc.**).

Su questa complessa materia il Garante è intervenuto di recente con Linee guida ampie e dettagliate.

4

Privacy e lavoro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Dati sanitari

I dati sanitari vanno conservati in fascicoli separati.

Il lavoratore assente per malattia è tenuto a consegnare al proprio ufficio un certificato senza diagnosi ma con la sola indicazione dell'inizio e della durata presunta dell'infermità.

Il datore di lavoro non può accedere alle cartelle sanitarie dei dipendenti sottoposti ad accertamenti dal medico del lavoro.

Nel caso di denuncia di infortuni o malattie professionali all'Inail, il datore di lavoro deve limitarsi a comunicare solo le informazioni connesse alla patologia denunciata.

E' del tutto vietata la diffusione di "dati idonei a rivelare lo stato di salute" del lavoratore.

5

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3: Opinion & Guidelines W29 EDPB - provvedimenti, trattamenti particolari

Unità didattica

M3.9 Controlli sul lavoro e Tecnologie | Riserva di legge

Avv. Ida Tascone

Controlli sul lavoro

E' vietato ai datori di lavoro privati e pubblici di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza dei lavoratori. Tale divieto vale anche per l'uso di strumenti di controllo quali la videosorveglianza e la geolocalizzazione

Videosorveglianza e geolocalizzazione

Non devono essere effettuati controlli a distanza al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge).

Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza o la geolocalizzazione sono rese necessarie da esigenze organizzative o produttive, o sono richieste per la sicurezza del lavoro

- E' vietato l'uso di strumenti atti ad effettuare un controllo a distanza. In tale ambito sono vietati la videosorveglianza e la geolocalizzazione al fine di "verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa".
- Questi strumenti possono essere previsti solamente per esigenze organizzative o produttive o per la sicurezza sul lavoro o per la sicurezza dei lavoratori.
- Per la installazione di apparecchiature che possono consentire di dare corso a questi controlli occorre il consenso dei soggetti sindacali e, ove non raggiunto, provvede la Direzione territoriale del lavoro.
- Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza o la geolocalizzazione sono rese necessarie da esigenze organizzative o produttive, o sono richieste per la sicurezza del lavoro.

- Nella gestione di internet e della posta elettronica il datore di lavoro deve adottare "misure di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati, anche per prevenire utilizzi indebiti" e deve informare i dipendenti delle modalità di utilizzo di utilizzo degli strumenti messi a disposizione ritenute corrette e dei controlli, anche in accordo con i soggetti sindacali. Ancora, i controlli devono essere motivati da ragioni organizzative o di sicurezza, si devono ispirare ai principii di pertinenza e sicurezza e si deve prevedere la cancellazione dei dati la cui conservazione non è necessaria. Inoltre deve essere chiaramente specificato se è consentita la navigazione per finalità non strettamente connesse ai doveri d'ufficio e devono essere indicate le conseguenze, anche disciplinari, in caso di uso indebito. Al riguardo si possono individuare i siti correlati alla prestazione lavorativa e prevedere filtri per impedire utilizzazioni diverse, Infine, la posta elettronica è tutelata in termini di segretezza della stessa, con possibilità di indirizzi comuni, di indirizzi individuali e di indirizzi ad uso privato. Può essere previsto l'invio di "coordinate" di altro dipendente. Il lavoratore può formalmente delegare un altro soggetto alla lettura della posta elettronica; il datore di lavoro può incaricare di ciò altro soggetto dandone informazione al dipendente ed ai destinatari.

....novità apportate dal D.lgs. 101/2018

- Il decreto legislativo 196/2003 «Codice privacy» non è stato abrogato ma è stato modificato e integrato con il nuovo

- D. Lgs. 10 agosto 2018 n. 101

che ne realizza l'adeguamento alle disposizioni del GDPR (General Data Protection Regulation)

Il decreto di adeguamento prevede l'inserimento nel Codice privacy novellato dell'art. 11 bis che stabilisce che le informazioni, di cui all'art. 13 del GDPR (informativa) in caso di candidature spontanee, vengono rese al primo contatto utile, successivo all'invio del curriculum.

Inoltre nei limiti, di cui all'art. 6 par.1 lett. b) (trattamento necessario per l'esecuzione di un contratto o di misure precontrattuali adottate su richiesta dell'interessato), il consenso al trattamento dei dati personali presenti nei curricula non è dovuto.

Il trattamento dei dati relativi a condanne penali o reati

Avv. Ida Tascone

L'articolo 2-*octies* del novellato Codice privacy prevede che il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento, che non avviene sotto il controllo dell'autorità pubblica, è consentito **solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento**, che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

Inoltre, il comma 3 del predetto articolo 2-*octies* stabilisce che il trattamento è consentito se autorizzato da una norma di legge **o, nei casi previsti dalla legge, di regolamento**, riguardanti, a puro titolo esemplificativo e non esaustivo, l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia, l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, l'adempimento degli obblighi previsti dalle normative vigenti in materia di contrasto al riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Le principali novità del d. lgs.101/2018

Sono innovativi anche i riferimenti al telelavoro, lavoro agile e domestico al controllo a distanza, in riferimento al quale è ribadito il divieto di controllo a distanza dei lavoratori previsto dall'art. 4 dello Statuto dei lavoratori.

telelavoro

- Il telelavoro è una forma di lavoro che è effettuata in un luogo distante dall'ufficio centrale o dal centro di produzione e che implica l'adozione di una nuova tecnologia che permette la separazione e facilita le comunicazioni.
- Lo statuto europeo del telelavoro (European Charter for telework, progetto Diplomat, del maggio 1997) definisce poi il telelavoro come "un modo di lavorare usando le tecnologie di informazione e comunicazione in cui il Lavoro è eseguito indipendentemente dall'ubicazione, in particolare da un posto diverso dal tradizionale posto di lavoro".
- Da queste definizioni emergono, pertanto, quelli che possono essere definiti i tre elementi essenziali del telelavoro:

- 1-l'utilizzo prevalente di strumenti informatici e telematici durante lo svolgimento dell'attività lavorativa;
- 2-la delocalizzazione dell'attività (domicilio, sede centrale, centri di telelavoro);
- 3-l'attività lavorativa contrattualmente definita

- E' evidente come il telelavoro consenta di sfruttare contemporaneamente tecnologie diverse come la televisione, il computer e il telefono dando vita ad una realtà multimediale ed interattiva. Siamo di fronte alla frontiera più avanzata delle tecnologie a cui si dà il nome di groupware (sistema costituito dall'hardware, il software e le reti, che dà vita ad una convergenza tra informatica, telecomunicazioni e multimedialità).
- Vi sono delle attività professionali, infatti, che essendo più flessibili possono essere svolte più facilmente rispetto ad altre con l'uso di queste tecnologie e sono, in particolare, le attività che utilizzano più frequentemente le banche dati e quelle che elaborano dei prodotti che possono essere trasmessi a distanza quali testi, programmi, tabelle dati
- In Italia, i principali progetti di telelavoro sono stati avviati mediante la stipula di accordi sindacali dal gruppo STET (Telecom, Sovitel, Italtel, Seat), dalla IBM, dalla Dun & Bredstreet e dalla Digital Equipment). Le iniziative italiane sono arrivate comunque con dieci anni di ritardo rispetto alle analoghe sperimentazioni francesi ed inglesi; e ciò è soprattutto dovuto ad un ritardo strutturale ed infrastrutturale oltre che culturale, che costituisce il primo ostacolo alla diffusione del telelavoro: quest'ultimo di certo rappresenta, ed ancor meglio rappresenterà nei prossimi decenni, "la cosiddetta società post-industriale, che si reggerà su valori differenti da quelli che hanno caratterizzato il mondo taylor-fordista".
- Per quanto concerne la realizzazione di forme di telelavoro, è possibile scegliere tra due percorsi:
- 1-il collegamento, ovvero un percorso "dalla periferia al centro" che consiste nel collegare posti di lavoro periferici con un centro aziendale o con altri posti di lavoro o con i clienti;
- 2-Il decentramento, ovvero un percorso "dal centro alla periferia", consistente nello spostare dall'azienda ad altri luoghi (domicilio o centri satellite) i posti di lavoro

- La materia della qualificazione del rapporto di telelavoro è governata da estrema instabilità. La dottrina e la giurisprudenza hanno infatti individuato cinque tipi diversi di telelavoro, ai quali corrispondono altrettanti tipi o sottotipi legali di contratto. Da ciò deriva la possibilità, una volta che sono stati individuati i tratti caratterizzanti della fattispecie, cioè la specifica modalità organizzativa del lavoro, di collegare la fattispecie alla propria tipologia contrattuale, e di applicare la corrispondente normativa ed il corrispondente sistema di tutela per il lavoratore.
- Il telelavoratore potrà pertanto essere classificato come:
- 1- imprenditore
- 2- lavoratore autonomo
- 3- lavoratore parasubordinato
- 4- lavoratore a domicilio
- 5- lavoratore subordinato

- Al telelavoratore imprenditore (art. 2082 c.c.) non si applica nessuna delle norme di tutela del diritto del lavoro, essendo la materia regolata dal diritto commerciale. Un esempio può essere quello dell'imprenditore individuale strettamente collegato al ciclo di produzione dell'impresa committente; ebbene, questa categoria rischia di essere sottotutelata e di non vedere applicate le garanzie normativa del caso.
- La seconda categoria è costituita dal lavoratore autonomo o dalla piccola impresa e si distingue dalla prima perché la prestazione è caratterizzata dalla personalità. Anche in questo caso non si applica la normativa di tutela del diritto del lavoro, ma avendo il contratto ad oggetto un'opera o un servizio ben individuati e delimitati, si configura come "contratto d'opera", disciplinato dagli artt. 2222-2237del Codice Civile.
- Nella categoria del telelavoratore lavoratore autonomo rientra il caso di un telelavoratore che si serve soltanto in via ausiliaria, e cioè in misura non prevalente rispetto al proprio lavoro, di manodopera ed attrezzatura esterna.

- Il telelavoro come lavoro subordinato "ingloba" quelle prestazioni di lavoro autonomo caratterizzate da continuità, coordinazione e prevalente personalità (art. 403 n.3 c.p.c.). A questa categoria si applica una parte della normativa di tutela del lavoro, anche se la quota di tutela rimane bassa.

- Al telelavoro a domicilio si applica la disciplina dettata dalla L.877/73 sul lavoro a domicilio. Sono casi di telelavoro di questo tipo "il telelavoro svolto con continuità, ma senza vincolo di coordinamento spazio-temporale (cioè con piena libertà di orario e di dislocazione geografica dal luogo di lavoro)". Anche in questo caso il diritto del lavoro si applica, ma non completamente. Il telelavoratore non può peraltro servirsi di manodopera esterna che non sia quella dei familiari, visto il carattere prettamente personale della sua prestazione che deve essere tuttavia soggetta alle direttive del committente.

- La quinta categoria è rappresentata dal telelavoratore lavoratore subordinato. La prestazione di tale tipo di telelavoratore è caratterizzata da un obbligo continuativo di obbedienza nei confronti del datore di lavoro. Questa categoria è poi caratterizzata dalla possibilità di un controllo diretto e dalla verificabilità di un orario di lavoro da parte del datore di lavoro. Al telelavoratore lavoratore subordinato si applica tutto l'apparato normativo del diritto del lavoro.

Rischi e benefici

- La diffusione del telelavoro ha apportato, come tutte le grandi innovazioni moderne, nella sua applicazione dei grandi vantaggi per il lavoratore, per le aziende e per la comunità in generale ma anche naturalmente degli svantaggi, che mettono in rilievo i limiti e i punti deboli di questa attività. Per capire in dettaglio quali siano i reali rischi e i benefici connessi alla diffusione del telelavoro può essere utile far riferimento ad un'indagine condotta dalla Siemens Mixdorf International di Stoccolma, azienda che, opera nel Settore dell'informatica e che produce essa stessa software ed hardware necessari per lo svolgimento del telelavoro. Il motto di questa azienda è significativo, cd è: "usa ciò che vendi". Dopo un anno dedicato all'attuazione del progetto di telelavoro, lavoratori, azienda e sindacati della Siemens hanno valutato i vantaggi e gli svantaggi dell'iniziativa, rispondendo ad un questionario anonimo, preparato dalle rappresentanze sindacali aziendali. I risultati dell'indagine sono poi stati suddivisi, per ragioni di chiarezza, in quattro gruppi:
- 1-vantaggi e svantaggi per i lavoratori
- 2-per l'azienda
- 3- per la città
- 4- per la nazione

Vantaggi e Svantaggi per i lavoratori:

- minor tempo speso per raggiungere il posto di lavoro, con conseguenze risparmio di denaro;-
- migliori condizioni di lavoro;
- possibilità di orari individuali di lavoro;
- possibilità di tempo libero;
- organizzazione del lavoro più efficiente;
- stipendio più alto;
- possibilità di lavorare per le persone disabili.

.....

- -non sono chiari i sistemi assicurativi nel caso di incidenti in ambito domestico;
- -non sono chiari i sistemi di assistenza sanitaria e di trattamento economico durante l'assenza;
- -il lavoro è troppo slegato dalla società;
- -non ci sono regole sull'orario di lavoro;
- -è difficile separare l'orario di lavoro dal tempo libero;
- -manca una legislazione chiara;
- -vi è una intromissione in casa;
- -ci sono pochi contatti sociali;
- -si deve lavorare anche quando si è malati;

- Vantaggi e svantaggi per l'azienda
- -scelta valida se la sede dell'azienda è collocata al centro della città;
- -costo inferiore nella gestione dell'auto aziendale;
- -costi generali più bassi per la diminuzione dello spazio occupato dagli uffici;
- -profili professionali più moderni;
- -maggiore possibilità di trattenere alle dipendenze dell'azienda lavoratori con alte professionalità;
- -minor perdita di tempo;
- -minori servizi interni.
- -i costi per le apparecchiature sono onerosi;
- -i costi operativi sono maggiori;
- -i costi assicurativi e di rischio sono maggiori;
- -è minore l'utilizzo dei servizi interni;
- -maggiore attività per l'amministrazione;
- -maggiori servizi esterni;
- -difficoltà nel controllo degli orari di lavoro e degli straordinari effettuati;
- -problemi di sicurezza;
- -sono più complicati i contatti con il sindacato aziendale e territoriale;
- -difficoltà a gestire troppi contratti di lavoro individuale.

Per quanto riguarda la disciplina del telelavoro in Italia, una primaria distinzione va effettuata tra settore privato e pubblico.

- Nel primo caso non abbiamo infatti una vera e propria disciplina, ma vi è un rimando all'accordo interconfederale del 9 giugno 2004, attuativo dell'accordo quadro europeo sul telelavoro datato 16 luglio 2002.

L'accordo, recepito da rappresentanti dei datori di lavoro e sindacati, ha l'obiettivo di fornire una disciplina generale, senza entrare nel dettaglio. Tale compito venne infatti lasciato ai contratti collettivi.

Brevemente, l'accordo quadro prevede che sia compito del datore di lavoro occuparsi di eventuali consumi, dei costi di fornitura, manutenzione, installazione e riparazione di attrezzature e di tutte le misure necessarie al fine di garantire che il lavoratore sia tutelato e non isolato.

Quest'ultimo, invece, da un lato, può gestire in maniera libera il proprio orario di lavoro, ma dall'altro lato i suoi carichi di lavoro non saranno differenti rispetto a quelli dei lavoratori presenti in azienda.

- Per quanto attiene al settore pubblico, invece, il telelavoro è disciplinato dalla legge n. 191/1998 (meglio nota come *Bassanini ter*) congiuntamente col d.p.r. 70/99 e con l'accordo quadro dell'8 giugno 2011.

Il trattamento retributivo e disciplinare dei dipendenti è rimesso, anche in questo caso, alla contrattazione collettiva e nazionale.

I diritti, ed i relativi doveri, dei telelavoratori sono uguali a quelli dei dipendenti che operano direttamente all'interno della struttura amministrativa.

Più recentemente è stato introdotto anche il "decreto Crescita 2.0", contenente l'obbligo, per le P.A., di stilare un piano per l'attività telelavorativa, specificando come essa si deve sviluppare ed in quali casi non si possa utilizzare.

Per quanto riguarda la tutela della RISERVATEZZA,

l'art.8 St. Lav. vieta l'effettuazione di indagini sulle opinioni politiche, religiose e sindacali del lavoratore, ovvero su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore. P

Può capitare che a forme di telelavoro on line si accompagni anche l'adozione di tecnologie particolari come la messa in opera di sofisticati sistemi di comunicazione telefonica interna, comportante , comunque, il divieto assoluto di intromissione da parte del datore di lavoro nelle conversazioni private del prestatore.

Sembra scontata l'applicabilità dell'art.8 St .Lav. anche al telelavoro nonché le norme sulla tutela della riservatezza.

Il controllo sul prestatore deve essere fatto anche per tutelare la riservatezza delle informazioni aziendali.

- Il rilievo più importante dal punto di vista penalistico, attinente i profili negativi del telelavoro, è costituito dal tema della tutela della privacy del telelavoratore. La disciplina della privacy assume, infatti, delle connotazioni particolari rapportata alle condizioni nelle quali si svolge questo tipo di attività lavorativa.

- Sono in effetti gli stessi strumenti usati dal telelavoratore (videoterminale, computer centrale, linee di telecomunicazione per il collegamento a distanza) che inevitabilmente comportano la registrazione dei dati personali relativi all'efficienza e all'assiduità del lavoro svolto; ciò comporta un controllo continuo e diretto del datore di lavoro sul telelavoratore che porta naturalmente alla violazione della sfera personale di quest'ultimo. A volte le ingerenze del datore di lavoro (specialmente nel caso di lavoro a domicilio) possono andare anche oltre l'attività lavorativa, invadendo la sfera privata. Per regolamentare tutto ciò, mancando una disciplina normativa ad hoc, che sarebbe tuttavia necessario predisporre al più presto attraverso un intervento legislativo specifico, ci si limita ad applicare l'art. 4 dello statuto dei lavoratori che "vieta l'uso di impianti audiovisivi e di altre apparecchiature, per finalità di controllo a distanza dell'attività dei lavoratori (comma I)", e subordina l'uso dei suddetti, qualora siano richiesti da "esigenze organizzative e produttive ovvero alla sicurezza del lavoro", al "previo accordo con le rappresentanze sindacali aziendali e, in mancanza, con la commissione interna (comma 2)"

- Quando non vi è "previo accordo", il datore di lavoro deve essere autorizzato dall'Ispettorato del lavoro all'installazione degli impianti, le cui modalità d'uso vengono definite dallo stesso Ispettorato.
- In tal modo, l'articolo 4 dello Statuto di fatto limita i poteri di controllo attribuiti all'azienda dagli articoli 2086 e 2104 del codice civile nel riguardi dei dipendenti.
- Il problema è dunque quello di cercare di scindere, il momento del controllo sulla riservatezza del lavoratore, che naturalmente è vietato, dal controllo tecnico sull'adempimento della prestazione, che è invece consentito.
- L'oggetto giuridico dell'art. 4 dello statuto dei lavoratori (L. 300/70) è la tutela delle libertà morali dei lavoratori, sotto l'aspetto dell'interesse a non essere sottoposti al controllo a distanza mediante impianti ed apparecchiature idonee a mettere in pericolo la libertà e le dignità, sottomettendole alla macchina.
- Al concetto di "controllo a distanza" dell'art. 4 statuto dei lavoratori si deve assegnare il significato sia di distanza fisica che temporale.
- In molti casi, per ovviare al problema della possibile violazione dell'art. 4 statuto dei lavoratori, si è stabilito, mediante accordo con le rappresentanze sindacali, di prevedere nel contratto di lavoro delle clausole con cui le parti convergono che i dati raccolti per la valutazione delle prestazioni del singolo lavoratore, anche a mezzo di sistemi informatici e/o telematici, non costituiscono violazione dell'art. 4 in quanto funzionali allo svolgimento del rapporto.
- Non sempre, però, avviene la stipulazione di questi accordi, data la difficoltà di conciliare interessi contrapposti: l'azienda, da una parte, cerca di tutelare le sue "banche dati" contro delle ingerenze esterne; i lavoratori, attraverso le rappresentanze sindacali, dall'altra, si preoccupano della propria privacy, non accettando il controllo del datore di lavoro sulle prestazioni individuali.

Caso giurisprudenziale

- Un caso giurisprudenziale, che pur non occupandosi specificatamente di telelavoro, comunque ne evidenze il problema fondamentale, costituito dal controllo a distanza dell'attività lavorativa svolta mediante elaboratori elettronici, è quello di una sentenza della Pretura di Milano datata 5 dicembre 1984.

In questo caso i denuncianti, dei lavoratori della IBM Italia Spa, affiancati dalle rappresentanze sindacali aziendali, chiamano in causa dei dirigenti della stessa società.

- L'accusa rivolta ai dirigenti, è quella di aver violato l'art. 4 comma 1 e 2 della L. 300 del 1970, in seguito all'installazione di un complesso sistema di hardware e software. I lavoratori della IBM e le rappresentanze sindacali, costituitesi parte civile, sostengono in particolare che "attraverso l'utilizzo di strumenti personalizzati di accesso al sistema, connessi all'esplicazione delle mansioni del lavoratore (codici individuali) è possibile per il datore di lavoro controllare in termini di quantità e qualità l'attività svolta dal lavoratore. In particolare, vi è la possibilità di registrare orari di inizio e fine della prestazione, eventuali pause e/o tempi morti, quantità di operazioni svolte e di dati trattati (quantificazione del lavoro svolto), eventuali errori e tempo impiegato per lo svolgimento delle singole operazioni".

- Vi è comunque, a parere del sindacato, un modo alternativo a quello dei codici individuali per tutelare le banche dati aziendali, in modo da preservare l'esigenza di riservatezza dell'azienda e quella dei lavoratori: è possibile, infatti, applicare un sistema di accesso agli elaboratori, costituito da un codice di gruppo, ma sul punto non si è riusciti a raggiungere un accordo con la dirigenza. Il principale oggetto della disputa è il sistema detto SLR (Service Level Reporter), un sistema di elaborazione che crea statistiche relative al livello del servizio, che ha per scopo la pianificazione del sistema e la ottimizzazione dello stesso. Questo programma produce dei "tabulati" (tabulati di controllo dell'efficienza) che pur registrando dei dati riferibili alle operazioni-macchina, a parere dell'accusa, costituiscono anche il mezzo di controllo a distanza dell'attività lavorativa, essendo aggregati sulla base di codici di riferimento individuali. E' quindi legittimo il dubbio che di fatto la "valutazione delle prestazioni" si risolva in una "valutazione delle risorse umane". La illiceità consiste, in effetti, non nel controllo sul prodotto, ma in quello esercitato sull'uomo. Il controllo non deve avvenire necessariamente in tempo reale, potendosi avere anche attraverso un controllo saltuario o posteriore all'esecuzione del lavoro.

- L' art. 4 comma 1 dello statuto dei lavoratori rappresenta una tipica contravvenzione a struttura dolosa.
- La nota a questa sentenza fatta da Padovani, spiega come il problema effettivo sia quello della "regolamentazione d'uso d'uno strumento di lavoro, affinché esso non si risolva in una forma di controllo sull'attività dei lavoratori chiamati ad avvalersene". Egli asserisce, inoltre, a proposito della sentenza della Pretura di Milano, che "in ben pochi lavoratori potrebbe ravvisarsi la coscienza dell'offesa relativa alle violazioni commesse a danno dei dipendenti". Padovani, pertanto, riconosce che, pur restando ferma la valutazione in termini di "non rimproverabilità dell'inosservanza, sia necessario spostare la rilevanza del concetto di coscienza dell'offesa del piano del dolo a quello della colpevolezza".
- E' evidente che l'impiego di elaboratori elettronici e di memorie artificiali, non costituisce di per se stesso un pericolo per la sfera personale altrui, anche se la potenzialità offensiva di tali strumenti è grandissima; la demonizzazione di questi strumenti è nociva e controproducente visto che rappresentano, e sempre più lo faranno negli anni futuri, degli indispensabili strumenti di lavoro. Tutto dipenderà da come verranno usati e soprattutto, sarà più che mai necessario approntare un sistema di tutela normativa del telelavoratore, un intervento legislativo che non potrà che nascere da un lavoro interdisciplinare di collaborazione tra informatici, esperti di diritto e psicologi in grado di allontanare i timori impliciti o espliciti legati al rischio di asservimento sempre maggiori dell'uomo alla tecnologia.

Statuto dei lavoratori

La riserva di legge

- Vi sono materie che i regolamenti non possono trattare perchè la Costituzione ha riservato la competenza esclusivamente al Parlamento attraverso le leggi.
- Si parla in questi casi di materie coperte da riserva di legge.
- Es. Art.13 co2; art.41 co3

....novità apportate dal D.lgs. 101/2018

- Art. 113 Raccolta di dati e pertinenza rinvia all'articolo 8 dello Statuto dei lavoratori ed all'articolo 10 del D.lgs. n. 276 del 2003.
- Artt. 114 rinvia all'articolo 4 dello Statuto dei Lavoratori
- Art. 115 riguarda il rapporto di lavoro domestico del telelavoro e del lavoro agile ed il rispetto della personalità e della libertà morale del lavoratore

Art. 4. Impianti audiovisivi.

- 1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.
- 2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.
- 3. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.
- 4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.

Art. 8. Divieto di indagini sulle opinioni.

- È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3: Opinion & Guidelines W29 EDPB - provvedimenti, trattamenti particolari

Unità didattica

M3.10 Il trattamento dei dati in ambito sanitario

Avv. Ida Tascone

Il trattamento dei dati sensibili da parte di soggetti pubblici

- I dati sensibili possono essere trattati solo se autorizzati da espressa disposizione di legge che specifichi:

- tipi di dati trattati;
- operazioni eseguibili;
- finalità di rilevante interesse pubblico perseguite.

- I dati idonei a rivelare lo stato di salute non possono essere diffusi.

I dati personali in ambito sanitario sono quelli idonei a rivelare lo **stato di salute** (oltre che la vita sessuale), vale a dire tutte le nozioni e le informazioni positive e negative sulle condizioni corporali e mentali di una persona.

Sono dati sanitari anche:
i dati genetici che riguardano i caratteri ereditari di un individuo;
le fotografie scattate a fini di interventi chirurgici.

A questi dati il Codice della Privacy dedica molta attenzione circondando il trattamento di particolari cautele e misure di sicurezza (quali ad esempio il divieto di diffusione), misure che variano a seconda del soggetto (pubblico o privato) che lo pone in essere ma, anche e soprattutto, a seconda della finalità del trattamento che cerca di mediare fra due interessi contrapposti:
quello dell'interessato a far si che l'informazione non sia trattata (se non per ragioni legate alla sua sfera personale) o comunicata o divulgata;
quello della collettività che, se esistente, è spesso contrapposto.

Generalmente, la disciplina connessa ai trattamenti in ambito sanitario è particolarmente favorevole alla tutela del singolo, ma viene ristretta quando vengono in rilievo esigenze di protezione o tutela (sanitaria) della collettività.

Dati personali in ambito sanitario

Articoli..

Art. 75 (Specifiche condizioni in ambito sanitario)

1. Il trattamento dei dati personali effettuato per finalita' di tutela della salute e incolumita' fisica dell'interessato o di terzi o della collettivita' deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell'articolo 2-septies del presente codice, nonche' nel rispetto delle specifiche disposizioni di settore.

Art. 77 (Modalita' particolari)

1. Le disposizioni del presente titolo individuano modalita' particolari utilizzabili dai soggetti di cui al comma 2:
2. a) per informare l'interessato ai sensi degli articoli 13 e 14 del Regolamento;
3. b) per il trattamento dei dati personali.
4. 2. Le modalita' di cui al comma 1 sono applicabili: a) dalle strutture pubbliche e private, che erogano prestazioni sanitarie e sociosanitarie e dagli esercenti le professioni sanitarie; b) dai soggetti pubblici indicati all'articolo 80.

Art. 78. Informazioni del medico di medicina generale o del pediatra

1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati negli articoli 13 e 14 del Regolamento.

2. Le informazioni possono essere fornite per il complessivo trattamento dei dati personali necessario per attività di diagnosi, assistenza e terapia sanitaria, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.

- 3. Le informazioni possono riguardare, altresì, dati personali eventualmente raccolti presso terzi e sono fornite preferibilmente per iscritto. 4. Le informazioni, se non è diversamente specificato dal medico o dal pediatra, riguardano anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che: a) sostituisce temporaneamente il medico o il pediatra; b) fornisce una prestazione specialistica su richiesta del medico e del pediatra; c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata; d) fornisce farmaci prescritti; e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile. 5. Le informazioni rese ai sensi del presente articolo evidenziano analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati: a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente; b) nell'ambito della teleassistenza o telemedicina; c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica; c-bis) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221; c-ter) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decretolegge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.

- Art. 79 (Informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie) 1. Le strutture pubbliche e private, che erogano prestazioni sanitarie e sociosanitarie possono avvalersi delle modalità particolari di cui all'articolo 78 in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate. 2. Nei casi di cui al comma 1 la struttura o le sue articolazioni annotano l'avvenuta informazione con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato. 3. Le modalità particolari di cui all'articolo 78, possono essere utilizzate in modo omogeneo e coordinato in riferimento all'insieme dei trattamenti di dati personali effettuati nel complesso delle strutture facenti capo alle aziende sanitarie. 4. Sulla base di adeguate misure organizzative in applicazione del comma 3, le modalità particolari possono essere utilizzate per più trattamenti di dati effettuati nei casi di cui al presente articolo e dai soggetti di cui all'articolo 80.

Art. 80 (Informazioni da parte di altri soggetti) 1. Nel fornire le informazioni di cui agli articoli 13 e 14 del Regolamento, oltre a quanto previsto dall'articolo 79, possono avvalersi della facolta' di fornire un'unica informativa per una pluralità di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, i competenti servizi o strutture di altri soggetti pubblici, diversi da quelli di cui al predetto articolo 79, operanti in ambito sanitario o della protezione e sicurezza sociale. 2. Le informazioni di cui al comma 1 sono integrate con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attivita' amministrative effettuate per motivi di interesse pubblico rilevante che non richiedono il consenso degli interessati.

- Art. 92 Cartelle cliniche 1. Nei casi in cui strutture, pubbliche e private, che erogano prestazioni sanitarie e sociosanitarie redigono e conservano una cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

- 2.Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità: a) di esercitare o difendere un diritto in sede giudiziaria ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale

dati relativi alla salute

sono quelli "*attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*" (art. 4 GDPR).

sono ricompresi nella più vasta categoria dei dati soggetti a trattamento speciale (art. 9 GDPR), in quanto in grado di rivelare dettagli molto intimi della persona, e per questo vi è una tutela rafforzata, di tali dati.

Base giuridica

Il regolamento europeo stabilisce che i dati relativi alla salute possono essere utilizzati solo per finalità connesse alla salute (finalità di cura), per la supervisione del Sistema Sanitario Nazionale (finalità di governo) e per la ricerca nel pubblico interesse. L'articolo 9, lett h), **non prevede la necessità del consenso** per il trattamento dei dati per "finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità". Una volta che il cittadino ha deciso di sottoporsi ad una cura non occorre il consenso al trattamento dei suoi dati a fini di cura e diagnosi.

- La norma, però, lascia agli Stati membri la possibilità di "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute" (comma 4).
- In tal senso il legislatore italiano ha previsto, col Codice Privacy novellato, misure di garanzia e regole deontologiche, fissate dall'autorità di controllo nazionale e riviste a cadenza biennale. Quindi, Il Garante nazionale dovrà adottare delle misure di garanzia, sentito il Consiglio superiore di sanità e tenendo conto delle linee guida, delle raccomandazioni e delle buone prassi del Garante europeo, in particolare con riferimento alle cautele relative alle "modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute. Inoltre l'autorità di controllo dovrà anche promuovere delle regole deontologiche per il trattamento dei dati relativi alla salute.

ENTE

Soggetti

- I soggetti che per legge possono trattare dati sanitari sono:
  - esercenti una professione sanitaria;
  - organismi sanitari pubblici.
- Gli esercenti una professione sanitaria, in base alle leggi vigenti (l. 24/2017), sono:
  - farmacista ex d.lgs. 258/1991;
  - medico chirurgo ex d.lgs. 368/1999;
  - odontoiatra ex l.409/1985;
  - veterinario ex l. 750/1984;
  - psicologo ex l. 56/1989;
  - infermiere ex l. 905/1980;
  - ostetrico ex l. 296/1985;
  - infermiere pediatrico ex d.l. 70/1997;
  - esercente professioni sanitarie riabilitative.

  Sono esclusi l'operatore di interesse sanitario (l. 403/1971 e l. 43/2006) e arti ausiliari delle professioni sanitarie (massaggiatore, ottico, odontotecnico, puericultrice); ciò in quanto si tratta di persone che svolgono un'attività che ha rilevanza sanitaria, oppure di affiancamento, ma non costituiscono esse stesse attività sanitarie.
- Altri soggetti, ovviamente, dovranno effettuare il trattamento quali autorizzati del titolare oppure su diversa base giuridica (consenso).

Soggetti

- I soggetti che per legge possono trattare dati sanitari sono:
  - esercenti una professione sanitaria;
  - organismi sanitari pubblici.
- Gli esercenti una professione sanitaria, in base alle leggi vigenti (l. 24/2017), sono:
  - farmacista ex d.lgs. 258/1991;
  - medico chirurgo ex d.lgs. 368/1999;
  - odontoiatra ex l.409/1985;
  - veterinario ex l. 750/1984;
  - psicologo ex l. 56/1989;
  - infermiere ex l. 905/1980;
  - ostetrico ex l. 296/1985;
  - infermiere pediatrico ex d.l. 70/1997;
  - esercente professioni sanitarie riabilitative.

  Sono esclusi l'operatore di interesse sanitario (l. 403/1971 e l. 43/2006) e arti ausiliari delle professioni sanitarie (massaggiatore, ottico, odontotecnico, puericultrice); ciò in quanto si tratta di persone che svolgono un'attività che ha rilevanza sanitaria, oppure di affiancamento, ma non costituiscono esse stesse attività sanitarie.
- Altri soggetti, ovviamente, dovranno effettuare il trattamento quali autorizzati del titolare oppure su diversa base giuridica (consenso).

Informativa

- L'informazione esclusiva del medico riguarda la prevenzione, il percorso diagnostico, la diagnosi e prognosi, la terapia e le eventuali alternative diagnostico-terapeutiche, i prevedibili rischi e complicanze, nonché i comportamenti che il paziente dovrà osservare nel processo di cura. Tale informazione deve essere integrata con quella proveniente dagli altri esercenti le professioni sanitarie, così realizzando un'informazione complessiva e completa. Da evitare sicuramente comportamenti tesi a supplire le carenze informative limitandosi a ottenere una firma del paziente a fronte di informazion incomplete.

- Prima di procedere alla raccolta dei dati occorre fornire l'informativa al paziente (eventualmente può essere fornita oralmente anche se è preferibile sia scritta). Il documento deve indicare:
  - chi è il soggetto che raccoglie i dati;
  - le finalità del trattamento;
  - le modalità del trattamento;
  - la natura obbligatoria o facoltativa del conferimento dei dati e conseguenze per un eventuale rifiuto;
  - i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati;
  - gli estremi identificativi del titolare;
  - le modalità per l'esercizio dei diritti a tutela dei propri dati.

L'**informativa in ambito sanitario** deve contenere:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato del responsabile.

- Possono essere previste, tramite provvedimento del Garante, modalità semplificate per l'informativa.

consenso

Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici trattano i **dati personali sanitari** con il consenso dell'interessato e senza autorizzazione del Garante se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato, oppure, senza il consenso dell'interessato, ma previa autorizzazione del Garante (che deve sentire il Consiglio Superiore di Sanità), se la finalità di tutela della salute riguarda un terzo o la collettività.

Il sistema del consenso è semplificato rispetto alla previsione generale che richiede che il consenso al trattamento dei dati sensibili avvenga espressamente e per iscritto.

Il **consenso al trattamento** di dati idonei a rivelare lo stato di salute non solo nel caso in cui esso riguardi informazioni utili a tutelare interessi della collettività, ma anche quando il trattamento attenga la salute o l'incolumità dell'interessato può essere espresso per iscritto o verbalmente.

In quest'ultimo caso si compie con registrazione dell'espressione da parte del professionista sanitario o dell'operatore per conto dell'azienda sanitaria.

- Può esprimere il consenso:
- l'interessato;
- il legale rappresentante o un prossimo congiunto o un familiare o un convivente o il responsabile della struttura presso cui dimora l'interessato, nel caso di impossibilità fisica o di incapacità di intendere e di volere dell'interessato (vedi la scheda sull'interdizione);

- Il consenso deve essere ottenuto prima del trattamento dei dati, ma vi sono casi in cui è possibile ottenerlo successivamente:
- se vi è impossibilità fisica, incapacità di agire o di intendere e volere dell'interessato e non vi sia una persona abilitata al consenso;
- se sussiste un grave rischio per la salute o l'incolumità dell'interessato;
- se vi sono esigenze di urgenza medica.

- La comunicazione dei dati deve avvenire in modo intellegibile anche attraverso una grafia comprensibile e, in caso di comunicazione di codici o sigle, devono essere forniti i parametri per la comprensione del significato.
  I dati che, anche a seguito di verifiche, risultino eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Modalità semplificate di consenso

- È previsto che l'informativa all'interessato ed il suo consenso al trattamento di dati personali possano essere forniti ed ottenuti in maniera semplificata in determinate condizioni da determinati soggetti:
- il **medico di medicina generale** ed il **pediatra** possono ricorrere ad un modello di informativa semplificato purché in forma chiara, fornita per iscritto, anche tramite modulistica e può riguardare anche il trattamento di dati compiuto dal sostituto del medico o dallo specialista la cui prestazione sia stata richiesta dal medico di base. Trattamenti potenzialmente a rischio devono essere evidenziati analiticamente dal medico;
- gli **organismi sanitari pubblici e privati**, anche in riferimento a pluralità di prestazioni erogate anche da distinti reparti, od unità o, ancora, strutture sanitarie e i competenti servizi o strutture di soggetti pubblici, che possono limitarsi ad un'unica informativa per una pluralità di trattamenti.
- Particolari disposizioni sono poi previste per il trattamento dei dati genetici, da chiunque effettuato, che è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante, con la quale vengono individuati gli ulteriori elementi da includere nell'informativa, con particolare riguardo alla specificazione delle finalità perseguite e dei risultati conseguibili.

reclamo

- Il Codice della Privacy riconosce il diritto all'interessato di **conoscere le finalità e le modalità del trattamento** dei dati personali che lo riguardano ottenendone l'**aggiornamento** ma, altresì, la **cancellazione**.
  I diritti di cui sopra possono essere esercitati e tutelati senza formalità, mediante richiesta rivolta al titolare o al responsabile (cd. interpello preventivo).
  In mancanza di riscontro o qualora il riscontro non sia soddisfacente, l'interessato può esperire un'azione giudiziaria oppure rivolgersi al Garante della privacy.

  Una volta che si è agito dinanzi al Garante, non è più possibile rivolgersi al Tribunale per la medesima questione.

I mezzi di tutela sono:

- il **reclamo**: è un atto tramite cui l'interessato denuncia al Garante una violazione della disciplina in materia di protezione dei dati personali.

Può essere proposto:

- - quando non si è ottenuta una tutela soddisfacente dei propri diritti;
  - quando si vuole promuovere una decisione del Garante su una questione di sua competenza.

Il **reclamo** non ha particolari formalità; ad esso seguono:

- - un'istruttoria preliminare;
  - un eventuale procedimento amministrativo nel quale possono essere adottati vari provvedimenti (ad esempio, prescrizione di: blocco del trattamento, adozione di misure opportune o necessarie per rendere il trattamento conforme alla normativa, ecc.).

- Il **reclamo** non è gratuito: occorre farsi carico dei diritti di segreteria che non vengono rimborsati;
- **la segnalazione**, finalizzata a sollecitare l'attività di controllo del Garante, non presenta particolare formalità e deve essere inviata al Garante.

Ad una o più **segnalazioni** possono seguire:

- - un'istruttoria preliminare;
  - un procedimento amministrativo;

Il ricorso

- il **ricorso** al Garante è un atto formale, che deve essere presentato rispettando particolari formalità nei seguenti casi:
- - tardiva o non soddisfacente risposta del titolare o del responsabile (se designato)
  - decorso dei termini relativi al riscontro dell'istanza.
- Il **ricorso** non è gratuito e, inoltre, su richiesta di una o entrambe le parti, il Garante può disporre la condanna alle spese nei confronti della parte soccombente o compensare le spese, anche parzialmente, se ricorrono giusti motivi.
  Il Garante, se ritiene fondato il **ricorso**, può ordinare la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione.
  Vige il principio del silenzio-diniego: la mancata pronuncia sul **ricorso**, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto.
  Contro il provvedimento (espresso o tacito) del Garante è possibile proporre **ricorso** dinanzi al tribunale del luogo ove risiede il titolare del trattamento.

conservazione

I documenti che contengono dati sanitari devono essere conservati in archivi ad accesso controllato (es. schedari con serratura), e comunque in modo che terzi non possano accedervi.

Diffusione dei dati

I dati sullo stato della salute possono essere forniti anche a terzi, come parenti, familiari, conviventi, conoscenti, personale volontario, purché ovviamente il paziente, se cosciente, sia stato informato e abbia consentito.

Occorre comunque rispettare l'eventuale richiesta della persona ricoverata a non rendere note neppure ai terzi legittimati la sua presenza nella struttura sanitaria o le informazioni sulle sue condizioni di salute.

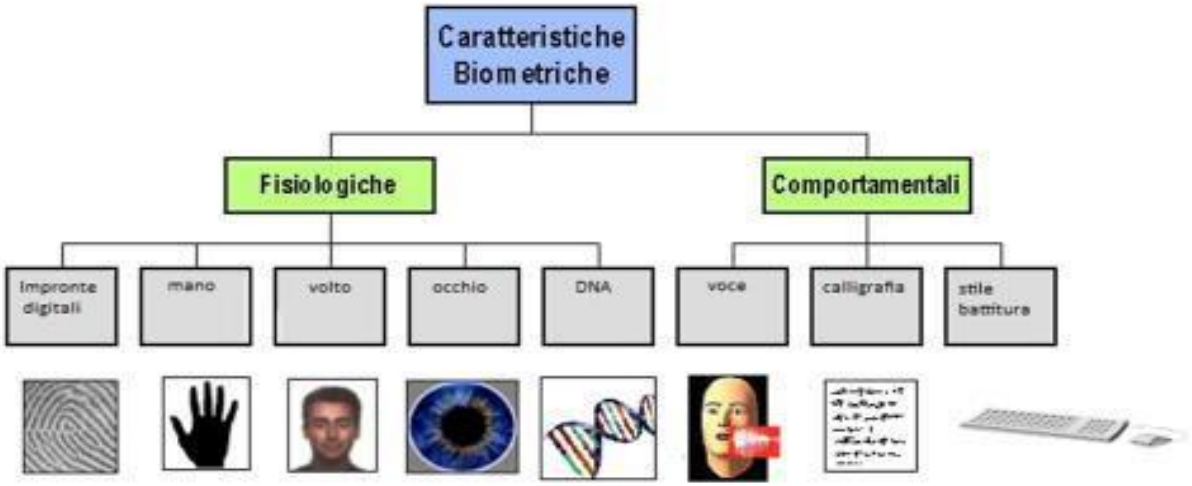
Fascicolo sanitario elettonico

- Il Fascicolo sanitario elettronico (FSE, previsto dall'art. 12 DL 179/2012) è uno strumento informatico che riunisce i dati e i documenti (digitali o digitalizzati) di tipo sanitario e sociosanitario, relativi all'assistito. La sua funzione è di condividere tali dati, e quindi la storia clinica del paziente, tra vari medici o organismi sanitari.
  Il fascicolo viene, quindi, aggiornato dalle strutture sanitarie e dai medici. Al FSE possono accedere, oltre al paziente (con modalità sicure, es. smart card), i medici e il personale sanitario autorizzato. Non possono accedere terzi, quali periti assicurativi o datori di lavoro.
- Non essendo stato abrogato l'articolo 12 del DL 179/2012, attualmente l'inserimento di dati all'interno dell'FSE dipende dal **consenso del paziente** (art. 3 bis). A tal proposito deve essere informato in merito a chi ha accesso ai suoi dati e come questi possono essere utilizzati. Il consenso alla formazione del FSE ovviamente è del tutto distinto dalle cure, nel senso che il mancato consenso alla costituzione del FSE, oppure semplicemente all'inserimento di alcuni dati nel fascicolo, non può precludere la possibilità di usufruire delle cure.
  Il consenso può essere sempre revocato, e il paziente ha il diritto di oscurare alcuni dati specifici dal FSE.

I dati sanitari

- I dati sanitari devono essere conservati in fascicoli separati.
- I certificati medici devono contenere solamente la indicazione dell'inizio e della data presunta della malattia. Il datore di lavoro non può accedere alle cartelle dei medici del lavoro.
- E' severamente "vietata la diffusione di dati idonei a rivelare lo stato di salute del lavoratore. I dati cd biometrici, impronte digitali, topografia della mano, non possono essere oggetto di "uso generalizzato ed incontrollato".

Misure biometriche



Misure biometriche

- Tecniche di tipo **fisico o fisiologico**:

  misurano le caratteristiche fisiologiche di una persona. Esse comprendono: la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, l'analisi della retina, il riconoscimento del volto, la geometria della mano, il riconoscimento della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi della struttura del DNA, l'analisi dei pori della pelle ecc..

Misure biometriche

- Di **tipo comportamentale**: misurano il comportamento di una persona. Esse comprendono la verifica della firma manoscritta, l'analisi della battitura su tastiera, l'analisi dell'andatura

decreto legislativo n. 101/2018

e delle cc.dd. «*misure di garanzia*» per il trattamento dei dati genetici, biometrici e relativi alla salute (Articolo 2-septies), nella consapevolezza che il dialogo con le parti, gli *stakeholders* e i settori direttamente interessati è essenziale al fine di elaborare regole condivisibili e stabilire modalità di attuazione che non risultino eccessivamente onerose ovvero

Art. 2-septies (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute).

1. In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, **i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento** in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed **in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.**

2. Il provvedimento che stabilisce le misure di garanzia, di cui al comma 1, **é adottato con cadenza almeno biennale** e tenendo conto:

a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;
b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;
c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

3. Lo schema di provvedimento è sottoposto a consultazione pubblica per

e delle cc.dd. «***misure di garanzia***» per il trattamento dei dati genetici, biometrici e relativi alla salute (Articolo 2-septies), nella consapevolezza che il dialogo con le parti, gli *stakeholders* e i settori direttamente interessati è essenziale al fine di elaborare regole condivisibili e stabilire modalità di attuazione che non risultino eccessivamente onerose ovvero inefficaci agli occhi degli operatori.

Art. 2-septies (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute).

4. Le misure di garanzia sono adottate nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, del Regolamento, e riguardano anche le cautele da adottare relativamente a: a) contrassegni sui veicoli e accessi a zone a traffico limitato;

b) profili organizzativi e gestionali in ambito sanitario;

c) modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute;

d) prescrizioni di medicinali.

5. Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalità del trattamento e possono individuare, in conformità a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati è consentito. In particolare, le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati.

e delle cc.dd. «*misure di garanzia*» per il trattamento dei dati genetici, biometrici e relativi alla salute (Articolo 2-septies), nella consapevolezza che il dialogo con le parti, gli *stakeholders* e i settori direttamente interessati è essenziale al fine di elaborare regole condivisibili e stabilire modalità di attuazione che non risultino eccessivamente onerose ovvero inefficaci agli occhi degli operatori.

Art. 2-septies (Misure di garanzia per il trattamento dei dati genet biometrici e relativi alla salute).

6. Le misure di garanzia che riguardano i dati genetici e il trattamento dati relativi alla salute per finalità di prevenzione, diagnosi e cura nonc quelle di cui al comma 4, lettere b), c) e d), sono adottate sentito il Minist della salute che, a tal fine, acquisisce il parere del Consiglio superiore sanità. Limitatamente ai dati genetici, le misure di garanzia posso individuare, in caso di particolare ed elevato livello di rischio, il conser come ulteriore misura di protezione dei diritti dell'interessato, a norr dell'articolo 9, paragrafo 4, del regolamento, o altre cautele specifiche.
7. Nel rispetto dei principi in materia di protezione dei dati personali, c riferimento agli obblighi di cui all'articolo 32 del Regolamento, è ammes l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisic logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure garanzia di cui al presente articolo. 8. I dati personali di cui al comma 1 n possono essere diffusi.

MISURE DI SICUREZZA.....

Pseudonimizzazione

Il termine **cyber security** è di uso piuttosto recente ed è stato diffuso principalmente dal NIST (National Institute for Standards and Technologies) degli Stati Uniti. La **cyber security** è focalizzata principalmente sulla **protezione dei sistemi informatici** (computer, reti di telecomunicazione, smartphone, ecc.) e dell'informazione in formato digitale da attacchi interni e, soprattutto, esterni. Altri termini utilizzati in alternativa e precedentemente sono **IT security, ICT security, sicurezza informatica e sicurezza delle informazioni.**

Quest'ultima comprende anche la protezione delle informazioni in formato non digitale, ad esempio cartaceo. Al netto dell'informazione in formato cartaceo, sono tutti termini abbastanza interscambiabili, a meno che non si stia discutendo in un contesto estremamente specialistico. Curiosamente, e ad aumentare la confusione, il NIST distingue anche fra "**cybersecurity**" e "**cyber security**" che ha come obiettivo "**la protezione del cyberspazio dai cyberattacchi**".

È invece molto più utile sottolineare che con il termine "**sicurezza**" si intendono alcuni concetti molto diversi, che in inglese hanno termini distinti: "**security**", che si occupa di protezione dagli attacchi, e "**safety**", che si occupa di protezione dagli accidenti e dai guasti. Ad esempio, le cinture di sicurezza (protezione dagli accidenti" si chiamano "**safety belts**", mentre una serratura di sicurezza (protezione dagli attacchi) si chiama "**security lock**".

La **cyber security** è una disciplina molto pratica. Si occupa di proteggere i sistemi informatici da minacce concrete che hanno una probabilità significativa di realizzarsi, fra le tante che sarebbero concepibili. In questo, la si può vedere come **uno strumento di gestione dei rischi.**

I rischi infatti non sono praticamente mai nulli: le misure di sicurezza sono utilizzate per ridurre i rischi, quasi mai per eliminarli. Per capire questo concetto, partiamo dalle password. Prendiamo come esempio un computer portatile che teniamo in casa. È possibile che non sia protetto da nessuna password (anche se non è una buona pratica).

È evidente che non tutti i dati personali debbano essere protetti allo stesso modo. Questa è la ragione per cui i responsabili delle organizzazioni devono introdurre dei livelli di sicurezza idonei e allineati con il livello di riservatezza che si vuole raggiungere.

Le misure di sicurezza che possono essere adottate sono numerose, come ad esempio:

- **la creazione di politiche e procedure**, che siano specialmente mirate a proteggere la riservatezza dei dati personali,
- **l'addestramento dei soggetti coinvolti**, che rappresenta una delle più efficienti ed efficaci misure di sicurezza, che oltretutto ha un costo relativamente contenuto. Nessun soggetto dovrebbe poter accedere ai dati, senza prima aver ricevuto uno specifico addestramento;
- **la anonimizzazione dei dati personali**, il che significa che deve essere possibile modificare i dati, seppure in modo reversibile, in maniera che anche l'accesso illegittimo al dato non potrebbe consentire ad un soggetto terzo di ricostruire il soggetto fisico, cui i dati si riferiscono. Questa tecnica è particolarmente efficace quando i dati vengono utilizzati per esami e correlazioni, e non devono essere individualmente analizzati;

- **l'utilizzo di politiche restrittive di accesso ai dati**, che oggi sono realizzabili con relativa facilità, grazie agli efficienti ed efficaci sistemi di controllo dell'accesso ai dati su supporto informatico;
- **l'attuazione di sistemi di controllo per gli apparati mobili**, laddove le organizzazioni possono impedire o limitare in modo incisivo all'accesso ai dati personali da parte di dispositivi mobili, che per solito presentano un rischio più elevato, rispetto ad apparati fissi o semi fissi, situati all'interno delle strutture fisiche dell'organizzazione;
- **l'adozione di protocolli sicuri di trasmissione**, laddove le organizzazioni devono essere in grado di garantire un adeguato livello di protezione delle informazioni, anche durante le fasi di trasmissione; uno degli strumenti più efficaci è evidentemente l'adozione di protocolli di criptografia, prima che il dato venga trasmesso;
- **l'effettuazione di audit periodici**, grazie ai quali si può tenere sotto controllo il livello di riservatezza dei dati e prendere tempestive misure correttive.

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3: Opinion & Guidelines W29 EDPB - provvedimenti, trattamenti particolari

Unità didattica

M3.11 Cenni sul diritto sindacale e accordi ai sensi della Legge 300/70 art.04 Jobs Act

Avv. Ida Tascone

Definizioni generali

Diritto sindacale

(Giugni, *Diritto sindacale* 2001)

Parte del diritto del lavoro concernente il sistema di norme strumentali poste dallo Stato, dalle organizzazioni lavoratori e degli imprenditori per disciplinare, in una economia di mercato, la dinamica dei conflitti di interessi derivante dall'ineguale distribuzione del potere nei processi produttivi

Segue: Definizioni generali

Relazioni industriali (sindacali)

(Giugni, *Diritto sindacale* 2001)

La disciplina delle relazioni industriali ha lo stesso oggetto del diritto sindacale, inquadrato sotto il profilo sociologico. E' un sottosistema del sistema sociale che rappresenta l'insieme delle interrelazioni fra tre soggetti (imprenditori, prestatori di lavoro organizzati ed organi pubblici) che agiscono in un sistema di variabili economiche, politiche, tecnologiche e normative dirette a regolare il sistema produttivo o a creare un sistema di controllo sullo stesso

Segue: Definizioni generali

Conflitto industriale

Conflitto tra capitale e lavoro, dapprima inquadrato nella lotta di classe tra chi ha la proprietà dei mezzi di produzione e chi, non avendola, cede la propria forza lavoro. In tempi recenti nel concetto sono ricomprese tutte le ipotesi di conflitto con l'autorità esercitata nell'organizzazione del lavoro, indipendentemente dalla proprietà pubblica o privata essendo l'organizzazione ispirata a modelli gerarchici. Il conflitto può avere dunque valenze politiche ed istituzionali diverse dalla lotta di classe

Segue: Definizioni generali

Relazioni industriali (sindacali)

La materia delle relazioni sindacali è il contesto normativo dei rapporti fra interessi organizzati nel loro aspetto strutturale non solo logico formale ma anche nei loro effetti sugli equilibri politici, economici e sociali. Nei conflitti sociali tuttavia, l'effettività delle norme valide può essere oggetto di mediazione politica che può indurre a non dare loro applicazione. Perciò il diritto sindacale poggia la sua effettività sulla costanza del consenso sociale e la mediazione politica contribuisce a dare al sistema stabilità e continuità. Come nel diritto internazionale la mediazione politica regola il conflitto tra Stati per cui si può anche rinunciare alla effettività di sanzioni

Segue: Definizioni generali

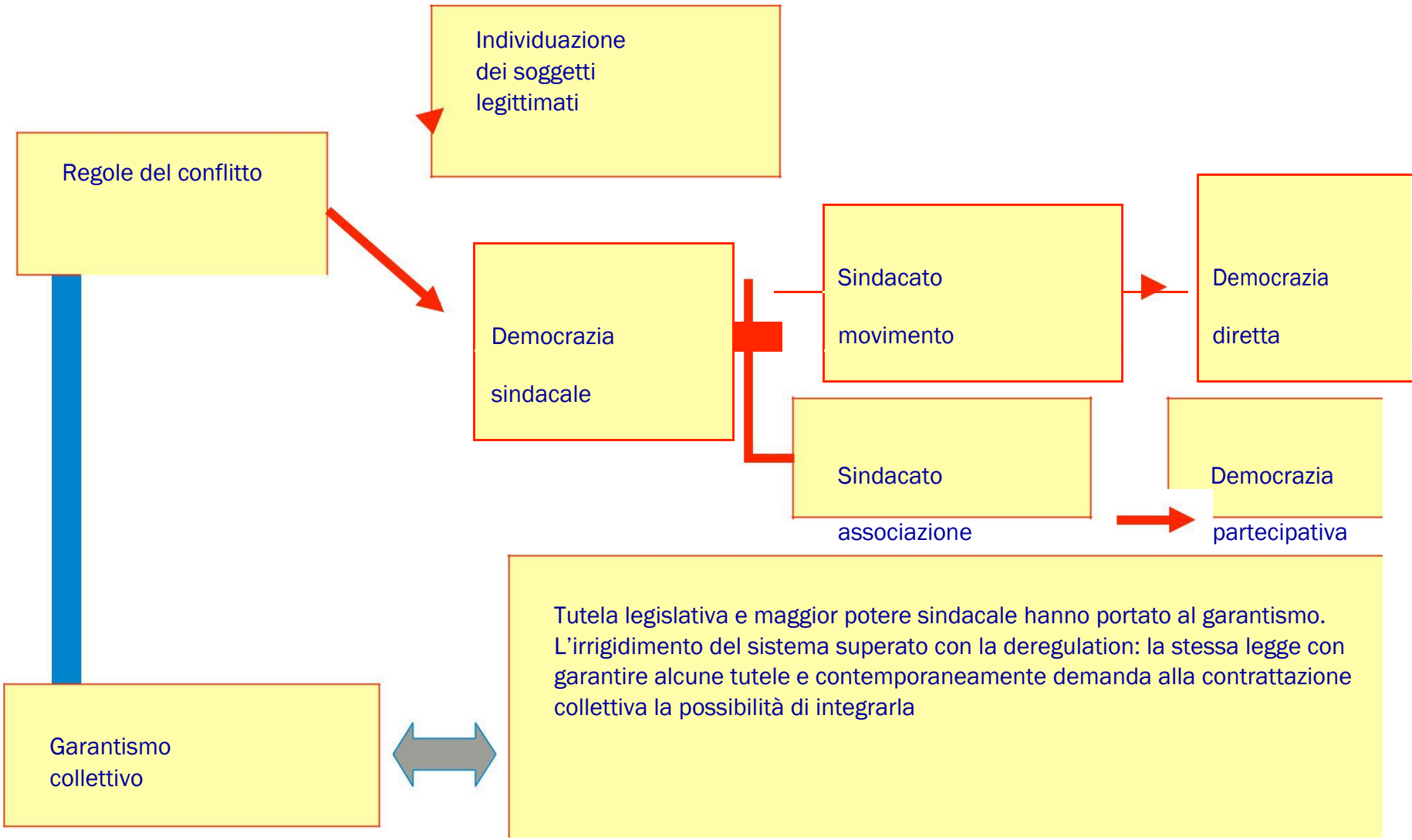
Regolazione del diritto sindacale nel sistema privato ⟺ Artt. 39 e 40 della Costituzione Legge 300/1970 Legge 146/1990 Legge 83/2000

Regolazione del diritto sindacale nel sistema pubblico ⟺ Artt. 39 e 40 della Costituzione Legge 300/1970 Legge 146/1990 Legge 83/2000 d.lgs. 165/2001

Importanza del ruolo della giurisprudenza nell'interpretazione dei principi costituzionali e delle leggi

Ordinamento intersindacale = insieme regole poste dai soggetti attori delle relazioni sindacali ed in alcuni casi anche dall'ordinamento statale

Segue: Definizioni generali n°327/01/05



Segue: Definizioni generali

Libertà sindacale

- Art. 18 Costituzione sulla libertà di associazione
- Art. 39 Costituzione sulla libertà di organizzazione per tutela propri interessi
  - Sotto profilo strumentale → Aggregazione soggetti in forma organizzata titolari libertà sindacale. Anche l'individuo per il proselitismo nella fase che precede l'organizzazione
  - Sotto il profilo teleologico → Atto diretto alla auto tutela di interessi giuridici connessi con l'attività di lavoro

I sindacati sono sottoposti a registrazione, il cui presupposto è la democraticità statuto. Acquistano così personalità giuridica e in proporzione ai loro iscritti stipulino i CCNL.
PARTE NON APPLICATA

Segue: Definizioni generali

Art. 39 della Costituzione sulla libertà di organizzazione sindacale prevede ai commi 2, 3 e 4 che:

I sindacati sono sottoposti a registrazione, il cui presupposto è la democraticità statuto. Acquistano così personalità giuridica e in proporzione ai loro iscritti possono stipulare i CCNL

Mancata realizzazione con legge ordinaria dei suddetti principi per motivi di politica sindacale (controlli, rappresentatività, etc.)

Ciò ha comportato che: CCNL non hanno efficacia erga omnes; normativa applicabile è quella civilistica anche se operano nella P.A.; le OO.SS. sono associazioni non riconosciute ma comunque soggetto giuridico, centro di imputazione giuridiche

Segue: Definizioni generali

Normativa comunitaria

- Carta dei diritti riconosce: libertà di associazione, livelli di negoziazione, diritto di sciopero
- Non vi è comunque una competenza comunitaria
- Gli stati membri regolano la materia dei diritti sindacali secondo la propria convenienza. La comunità interviene solo in caso di garanzie insufficienti

Segue: Definizioni generali


Livelli di contrattazione
Livello NAZIONALE
(o 1° livello)
Si svolge in ARAN. Dà luogo a
CCNQ
CCNL
Livello LOCALE
(o 2° livello)
Si svolge in ogni pubblica Amministrazione.Dà luogo a
C.I.
I livelli sono stabiliti dall'Accordo sulla politica dei redditi del 1993 e confermati dalla legge di riforma del pubblico impiego

Tipologie di contratti

CCNQ

- Accordo sulla definizione comparti e aree, propedeutico apertura negoziati
- Accordi su materie comuni a vari comparti o aree ovvero tra aree e comparti (es. diritti sindacali, telelavoro, lavoro interinale, conciliazione, arbitrato, etc.)

CCNL

- Riguarda ogni singolo comparto o area individuata e disciplina relativo rapporto di lavoro e relazioni sindacali

Contrattazione Integrativa

- Si svolge sulle materie, con i soggetti e nei limiti del CCNL nel rispetto dei vincoli di bilancio risultanti dagli strumenti di programmazione annuale o pluriennale

Differenze con il sistema privato

Soggetti per stipulazione CCNL

ARAN
(Rappresentanza Pubbliche Amministrazioni)

SINDACATI
rappresentativi

SINDACATI DI CATEGORIA
(che raggiungono il 5% al livello nazionale quale media tra il dato associativo ed elettorale)

CONFEDERAZIONI sindacali cui gli stessi aderiscono


REGOLE PER LA CONTRATTAZIONE
Le regole del CCNL sono le stesse per tutti i settori pubblici
Esse trattano:
La durata (validità) dei contratti
L'apertura procedure di negoziazione
I soggetti e le relazioni sindacali
Certificazione dei contratti

Contenuti del CCNL

- Disciplina del rapporto di lavoro
- Trattamento economico dei dipendenti e dirigenti pubblici
- Regole per la contrattazione integrativa che individuano:
  - Soggetti
  - Livelli relazioni sindacali (C.I., concertazione, consultazione, informazione)
  - Materie
  - Risorse
  - Procedure di raffreddamento dei conflitti


SEDI DEL II LIVELLO DI CONTRATTAZIONE
La contrattazione si svolge a livello di singola amministrazione nelle
La contrattazione di II livello è articolata sul territorio
La contrattazione di II livello è articolata con un sistema misto
Regioni Autonomie locali
Aziende sanitarie ed ospedaliere
Università
PCM
Accademie e conservatori
Ministeri
Scuola
Agenzie fiscali
Aziende autonome
Ricerca
EE.PP.
L'articolazione o meno sul territorio incide sulla composizione trattante di parte sindacale


CONTRATTAZIONE DECENTRATA INTEGRATIVA DI LIVELLO TERRITORIALE: ECCEZIONE PER ENTI MINORI ED IPAB PRIVE DI DIRIGENZA (Comparto Regioni-Autonomie locali)
Le eccezioni riguardano:
Livello (territoriale e non di ente)
La delegazione di parte pubblica
La delegazione sindacale
Procedure autorizzative
Le regole sono stabilite in un protocollo di intesa stipulato tra Anci, Uncem ed OO.SS. firmatarie del CCNL al quale possono aderire gli enti e le OO.SS interessate. Vengono derogate le norme sulla rappresentanza delle RSU non esistendo forme di coordinamento territoriale di queste. Gli atti di indirizzo sono formulati con apposita intesa. Il protocollo può riguardare anche la dirigenza. In tal caso partecipano anche l'UPI e l'Unioncamere

Concetto di rappresentatività a livello locale

Per le RSU deriva dal risultato elettorale

La rappresentatività dei componenti delle OO.SS. firmatarie dei CCNL è nazionale ed è misurata dall'ARAN. Le federazioni di più sindacati sono soggetto unitario

NON SONO AMMISSIBILI ALLA C.I.:

Sindacati non ammessi al CCNL anche se a livello locale hanno la media del 5% tra dato associativo ed elettorale

I sindacati ammessi alle trattative nazionali non firmatari del CCNL

Singoli componenti di federazioni sindacali


Soggetti sindacali del II livello
Sono dirigenti sindacali
Componenti delle RSU
Componenti delle OO.SS. firmatarie dei CCNL
Componenti dei terminali di tipo associativo (rimasti operativi o costituiti dopo le elezioni delle RSU), appartenenti alle OO.SS. rappresentative
Componenti organismi statutari non collocati in distacco o aspettativa e non coincidenti con gli altri soggetti

Contrattazione, concertazione, consultazione informazione

Contrattazione	=	Attività negoziale che può essere anche a termine CONTRATTARE È UN OBBLIGO; STIPULARE, SOLO SE CONVENIENTE
Concertazione	=	Attività non negoziale a termine. Si conclude con un verbale in cui si registrano posizioni parti
Consultazione	=	Attività informale prevista da leggi, CCNL e azienda
Informazione	=	Atti relativi al rapporto di lavoro individuati dall'azienda in C.I. Può essere preventiva o successiva

Le procedure di contrattazione e concertazione sono definite dal CCNL; quelle di consultazione ed informazione in azienda

Rappresentanza e rappresentatività
Riflessioni conclusive

- Nel pubblico impiego esiste un forte sistema di relazioni sindacali
- Trova la sua ragione nella partecipazione delle parti sociali al processo di riforma
- La fonte negoziale delle relazioni sindacali è regola di autodisciplina
- Rappresentanza e rappresentatività sono diverse ma interconnesse
- La rappresentatività deriva dal voto e dalle deleghe
- La rappresentatività permette la stabilità negoziale
- Le RSU vivono di vita propria (se nel triennio di vigenza decadono vanno rielette) ma non incidono sulla rappresentatività biennale
- RSU e Organizzazioni sindacali sono soggetti di pari dignità nel luogo di lavoro
- Il sistema deriva da un insieme di norme di legge e contrattuali consolidate dalla giurisprudenza
- Le materie relative ai diritti sindacali non sono disponibili se non nei limiti espressamente previsti dagli accordi quadro
- La normativa è collocabile sul piano delle fonti allo stesso livello dello Statuto dei diritti dei lavoratori (carattere di specialità del CCNQ sulle prerogative sindacali)

JOBS ACT

D.lgs. 151/2015

Come cambia l'articolo 4 della L. 300/1970 (Statuto dei Lavoratori) modificato dall'art. 23 del D.LGS. 15 settembre 2015 n. 151

1. ~~È vietato l'uso di~~ Gli **impianti audiovisivi e** ~~di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori~~.
~~Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma~~ gli altri strumenti **dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere** impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere **installati** ~~soltanto~~ **previo accordo** ~~con le~~ collettivo stipulato dalla rappresentanza sindacale unitaria o dalle **rappresentanze sindacali aziendali** ~~oppure~~. In alternativa, nel caso di imprese con unità produttive ubicate **in** ~~mancanza di queste, con la commissione interna. In difetto di~~ diverse province della stessa regione ovvero in più regioni, tale **accordo**, ~~su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.~~

Come cambia l'articolo 4 della L. 300/1970 (Statuto dei Lavoratori) modificato dall'art. 23 del D.LGS. 15 settembre 2015 n. 151

~~Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in~~ –può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In **mancanza di accordo** ~~con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato~~ gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero **del lavoro** ~~provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.~~

~~Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo~~ **e** ~~terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale~~ delle politiche sociali.

Come cambia l'articolo 4 della L. 300/1970 (Statuto dei Lavoratori) modificato dall'art. 23 del D.LGS. 15 settembre 2015 n. 151

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

Le novità dell'articolo 4 della L. 300/1970 (Statuto dei Lavoratori)

- **Impiego di impianti audiovisivi e strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori esclusivamente per:**
  - **esigenze organizzative e produttive;**
  - **la sicurezza del lavoro;**
  - **la tutela del patrimonio aziendale.**

- **Impianti e strumenti possono essere installati previo accordo collettivo con:**
  - **RSU o RSA;**
  - **Associazioni sindacali comparativamente più rappresentative sul piano nazionale;**
  - **DTL o Ministero Lavoro.**

Le novità dell'articolo 4 della L. 300/1970 (Statuto dei Lavoratori)

- **Non è richiesto alcun accordo e/o autorizzazione per gli *strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.***

- **Possibilità di utilizzare le informazioni raccolte *a tutti i fini connessi al rapporto di lavoro* (es. sanzioni disciplinari).**

- **Le informazioni raccolte possono essere utilizzate solo a condizione che sia data al lavoratore *adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196 (Codice della Privacy)*.**

Esigenze produttive e organizzative

In caso di esigenze organizzative di controllo sui lavoratori...

ai sensi dell'art. 4 della l. n. 300/1970

gli impianti e le apparecchiature, "dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto PREVIO ACCORDO con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna.

In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro [oggi DTL Direzioni territoriali del lavoro], dettando, ove occorra, le modalità per l'uso di tali impianti".

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3: Opinion & Guidelines W29 EDPB - provvedimenti, trattamenti particolari

Unità didattica

M3.12 Come predisporre un accordo sindacale | esercitazione

Avv. Ida Tascone

IL NUOVO ART. 4 DELLO STATUTO DEI LAVORATORI

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.
2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

COMMA 1

IMPIANTI AUDIOVISIVI

e gli altri strumenti dai quali derivi la possibilità di controllo a distanza dei lavoratori

POSSONO ESSERE IMPIEGATI

ESCLUSIVAMENTE

- Per esigenze organizzative e produttive
- Per la sicurezza sul lavoro
- Per la tutela del patrimonio aziendale

POSSONO ESSERE INSTALLATI

Unità produttive In una provincia	Unità produttive In più provincie
Accordo collettivo con RSU o RSA	Accordo collettivo con AA.SS. Comparativamente Più significative

IN MANCANZA DI ACCORDO

Autorizzazione DTL	Autorizzazione Ministero del Lavoro

COMMA 3

Sono utilizzabili a tutti i fini connessi al rapporto di lavoro

A Condizione

Che sia data al lavoratore adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli

E nel rispetto del Codice della Privacy

COMMA 2

STRUMENTI UTILIZZATI DAL LAVORATORE PER RENDERE LA PRESTAZIONE LAVORATIVA

E

STRUMENTI DI REGISTAZIONE DEGLI ACCESSI E DELLE PRESENZE

COMMA 3

Sono utilizzabili a tutti i fini connessi al rapporto di lavoro

A Condizione

Che sia data al lavoratore adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli

E nel rispetto del Codice della Privacy

IL NUOVO ART. 4 DELLO STATUTO DEI LAVORATORI: IL PRIMO COMMA

Una pronuncia della **Cassazione n. 22611/2012 ha ritenuto che il consenso scritto prestato da tutti i lavoratori all'installazione di un impianto di videosorveglianza potesse validamente sostituire quello richiesto dall'art. 4 Stat. Lav.**, che subordina l'installazione al previo accordo con le rappresentanze sindacali aziendali oppure, in mancanza di queste, con la commissione interna (ai sensi del «vecchio» art. 4).

L'UTILIZZABILITÀ DEGLI STRUMENTI IN USO AI LAVORATORI DAI QUALI DERIVI ANCHE LA POSSIBILITÀ DI CONTROLLO A DISTANZA

L'utilizzo di strumenti in uso ai lavoratori per rendere la prestazione lavorativa è possibile, senza accordo collettivo con RSU o RSA o senza autorizzazione della DTL o del ML, a tutti i fini connessi al rapporto di lavoro a condizione:

- Che **non siano costituiti da impianti audiovisivi**, che ricadono nel primo comma dell'art. 4 della L. 300/70
- Che siano utilizzati nel **rispetto del Codice della Privacy**, che richiede il rispetto dei principi:
  - **Di proporzionalità**: i dati trattati devono essere ridotti a quanto necessario per le finalità che giustificano i trattamenti
  - **Di liceità**: le finalità devono essere lecite e precisamente individuate
  - **Del bilanciamento degli interessi**: in tutti i casi in cui (come nei casi in esame) è impossibile o sproporzionato raccogliere il consenso degli interessati deve esistere equilibrio tra gli interessi di chi vuole utilizzare i dati e quelli del soggetto a cui i dati si riferiscono

Sono quindi **illeciti** controlli di tipo **preventivo, generalizzato e costante** delle

L'UTILIZZABILITÀ DEGLI STRUMENTI IN USO AI LAVORATORI DAI QUALI DERIVI ANCHE LA POSSIBILITÀ DI CONTROLLO A DISTANZA

Il terzo comma dell'art.4 stabilisce inoltre che **sia data al lavoratore adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli.**

I possibili controlli (con i limiti sopra ricordati) sono leciti nella misura in cui vi è **totale trasparenza** nei confronti del lavoratore, che deve essere compiutamente, completamente e chiaramente informato sulla possibile effettuazione dei controlli.

E' pertanto opportuno fornire l'informazione prevista non solo per i controlli che l'azienda intende eventualmente svolgere nelle situazioni contingenti del momento in cui fornisce l'informativa, ma di tutti quelli che, potenzialmente e lecitamente, potrebbe svolgere in base alle funzionalità esistenti negli strumenti in uso ai lavoratori.

I PIÙ FREQUENTI CONTROLLI PERMESSI DAI SISTEMI INFORMATICI AZIENDALI

Va altresì ricordato è preferibile che tutte le attività tecniche vengano svolte in presenza dell'utente ove non sussistano motivazioni tecniche od organizzative che le rendano urgentemente necessarie anche in sua assenza.

Inoltre la parte prescrittiva delle **Linee Guida del Garante su posta elettronica ed internet** del 1° marzo 2007 **vieta esplicitamente** ai datori di lavoro pubblici e privati:

a) **la lettura e la registrazione sistematica dei messaggi di posta elettronica** ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
b) **la riproduzione e l'eventuale memorizzazione sistematica delle pagine web** visualizzate dal lavoratore;
c) **la lettura e la registrazione dei caratteri inseriti tramite la tastiera** o analogo dispositivo;
d) **l'analisi occulta di computer portatili** affidati in uso.

I controlli resi possibili dai sistemi di registrazione degli accessi e delle presenze

Gli strumenti di **controllo accessi** e di **registrazione delle presenze** rientrano nel campo di applicazione del **comma 2 dell'art.4**, e quindi **non richiedono l'accordo sindacale** (o l'autorizzazione della DTL o del ML).

Tra questi:

- **Registrazione** (manuale o informatica) dei **visitatori** da parte della portineria
- **Rilevazione presenze** con cartellino o con badge

La loro utilizzabilità è quindi condizionata solamente alla fornitura di una corretta informativa ai lavoratori.

I controlli resi possibili dai sistemi di registrazione degli accessi e delle presenze

E' possibile l'incrocio tra le informazioni raccolte tra il sistema di rilevazione presenze ed i controlli derivanti dal sistema informatico?

La risposta è **affermativa se:**

- Viene data ai lavoratori corretta informazione della possibilità di controllo
- I dati vengono conservati per un ragionevole periodo di tempo, ma il loro utilizzo a fini di controllo è limitato ai casi di effettiva e motivata necessità (divieto di controlli generalizzati)

Si ricorda che l'utilizzo di **sistemi di rilevazione biometrica** per il controllo accessi è lecito solo in condizioni di **particolare rischiosità** o necessità di **protezione del patrimonio aziendale**

Gli adempimenti privacy per i sistemi di videosorveglianza

Necessità di interpello (ex art. 17 del Codice) in caso di funzionalità avanzate:

- Riconoscimento biometrico
- «Sistemi intelligenti»

Controllo del periodo di conservazione delle immagini

- Standard 1 giorno
- Valutabile fino a 7 giorni (in condizioni di particolare rischiosità)
- Richiesta art. 17 Oltre a 7 giorni
- Con cancellazione automatica delle immagini mediante sovra registrazione

Istruzioni agli incaricati

- Con selettività dei diritti d'accesso (immagini in diretta e/o registrate, zoom, brandeggio, estrazione spezzoni)

Autenticazione e profilazione nel sistema (digitale) di gestione delle immagini

Gli adempimenti privacy per i sistemi di videosorveglianza

Controllo dei manutentori esterni

- L'attività di manutenzione deve essere svolta in presenza di incaricati

Nomina dei centri di controllo esterni a responsabile del trattamento

- Il centro di controllo deve essere in possesso dell'autorizzazione Prefettizia

Presenza di informative

- **Cartelli di segnalazione** (informativa sintetica) in tutti i luoghi in cui si accede a una zona sottoposta a controllo
- Informativa completa per visitatori e dipendenti

Crittografia delle immagini

- Trasmissione in internet
- Trasmissione su reti WiFi od analoghe

IL PROVVEDIMENTO GENERALE SULLA GEOLOCALIZZAZIONE DEI VEICOLI
(alcuni sintetici richiami ai punti principali)
(applicabile «estensivamente» ad altre forme di geolocalizzazione – telefono, tablet, ecc.)

FINALITÀ AMMESSE E PRINCIPIO DEL BILANCIAMENTO DI INTERESSI

- Impiego dei sistemi in esame per soddisfare esigenze logistiche (consentendo di impartire tempestive istruzioni al conducente del veicolo oggetto di localizzazione)
- Elaborare rapporti di guida allo scopo di commisurare il tempo di lavoro del conducente
- Commisurare i costi da imputare alla clientela
- Assicurare una più efficiente gestione e manutenzione del parco veicoli, con effetti vantaggiosi anche sulla sicurezza sul lavoro e per la sicurezza della collettività

PRINCIPI DI PERTINENZA E NON ECCEDENZA (=esclusione obbligo raccolta consenso)

Per il conseguimento di ciascuna delle finalità legittimamente perseguite dal datore di lavoro titolare del trattamento **possono formare oggetto di trattamento**, mediante sistemi opportunamente configurati (art. 3 del Codice), solo i dati pertinenti e non eccedenti: tali possono essere, oltre **all'ubicazione del veicolo**, la **distanza percorsa**, i **tempi di percorrenza**, il **carburante consumato**, nonché la **velocità media del veicolo** (restando riservata alle competenti autorità la contestazione di eventuali violazioni dei limiti di velocità fissati dal codice della strada).

Nel rispetto del principio di necessità (artt. 3 e 11, comma 1, lett. d), del Codice), **la posizione del veicolo di regola non dovrebbe essere monitorata continuativamente** dal titolare del trattamento, ma solo quando ciò si renda necessario per il conseguimento delle finalità legittimamente perseguite.

Anche in base al principio di pertinenza e non eccedenza (art. 11, comma 1. lett. e), del Codice) i **tempi di conservazione** delle diverse tipologie di dati personali eventualmente trattati devono **essere commisurati** tenendo conto di ciascuna delle **finalità** in concreto perseguite.

IL PROVVEDIMENTO GENERALE SULLA GEOLOCALIZZAZIONE DEI VEICOLI

(alcuni sintetici richiami ai punti principali)

(applicabile «estensivamente» ad altre forme di geolocalizzazione – telefono, tablet, ecc.)

INFORMATIVA

- **Sintetica** (vetrofania sul veicolo)
- **COMPLETA** (necessaria ex comma 3 art. 4)

OBBLIGO DI NOTIFICA AI SENSI DELL'ART. 37 DEL CODICE DELLA PRIVACY

ISTRUZIONI AGLI INCARICATI e NOMINE DEI RESPONSABILI (obbligatorie in caso di esternalizzazione)

LA GEOLOCALIZZAZIONE E GLI ADEMPIMENTI DELL'ART.4 DELLA L.300/70

I sistemi di geolocalizzazione ricadono nel comma 1 o nel comma 2 dell'art.4?

Non è possibile dare una risposta di tipo generale, in quanto il regime applicativo dipende dalla **mansione lavorativa** e dalle **motivazioni** del sistema di geolocalizzazione.

Se ad esempio l'automezzo localizzato ed ha uso di un **tecnico** che svolge **servizi di assistenza in condizioni di urgenza** il sistema di geolocalizzazione può essere considerato un componente indispensabile di uno «strumento utilizzato dal lavoratore per svolgere la prestazione lavorativa» e quindi ricade **nell'ambito di applicabilità del 3° comma dell'art. 4**.

Se non esistono tali condizioni (se ad esempio il sistema ha il solo scopo della protezione patrimoniale del veicolo, si applica il 2° comma, e quindi **è necessario l'accordo sindacale o l'autorizzazione della DTL**.

LA GEOLOCALIZZAZIONE - PRECISAZIONI

Se il sistema di geolocalizzazione è **presente solo sul veicolo** e **l'azienda non ha accesso alle relative informazioni** (i normali navigatori installati sugli automezzi) non è possibile alcuna forma di controllo e quindi **non vi è applicabilità né dell'art. 4 né della normativa privacy**.
Può essere opportuno disattivare la registrazione dei percorsi o la non attivazione di tale funzionalità.

Se il sistema è **gestito da terzi** (società assicurative, fornitori di servizi di connettività per i tablet ed i portatili) e **l'azienda non accede se non eccezionalmente e non direttamente** (ad es. in caso di furto o di segnalazione di incidente) alle informazioni di geolocalizzazione **non vi è applicabilità né dell'art. 4 né della normativa privacy**.

Ulteriori funzionalità (ad es. cancellazione dei dati, installazione di applicazioni da remoto su tablet e cellulari aziendali), nella misura in cui **non richiedono e non permettono di detenere informazioni di geolocalizzazione, non hanno rilevanza.**

documenti di riferimento

- Linee guida per il trattamento di dati dei dipendenti privati – 23 novembre 2006 doc. web n. 1364099
- Linee guida per il trattamento di dati dei dipendenti pubblici – 14 giugno 2007 doc. web n. 1417809
- Linee guida del Garante per posta elettronica e internet – 10 marzo 2007 doc. web n. 1387522
- Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati – 12 giugno 2014 doc. web n. 3134436
- Provvedimento generale prescrittivo in tema di biometria – 12 novembre 2014 doc. web n. 3556992 All. A al Provvedimento 513 del 12 novembre 2014 - Linee-guida biometria doc. web n. 3563006
- Provvedimento in materia di videosorveglianza – 8 aprile 2010 doc. web n. 1712680
- Provvedimento Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro – 4 ottobre 2011 doc. web n. 1850581
- Provvedimento Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Wind Telecomunicazioni s.p.a. - 9 ottobre 2014 doc. web n. 3505371
- Provvedimento Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a. - 11 settembre 2014 doc. web n. 3474069

vademecum

- Prima di installare un impianto di videosorveglianza occorre valutare se la sua utilizzazione sia realmente proporzionata agli scopi perseguiti o se non sia invece superflua. Gli impianti devono cioè essere attivati solo quando altre misure (sistemi d'allarme, altri controlli fisici o logistici, misure di protezione agli ingressi ecc.) siano realmente insufficienti o inattuabili.]
- Per non incorrere in accuse o sanzioni, il titolare di un'azienda può installare un sistema di videosorveglianza nel totale rispetto della privacy dei propri lavoratori seguendo una procedura semplice.
- Nella domanda di autorizzazione, dovranno:
- essere evidenziate le circostanze e le motivazioni che rendono necessaria l'installazione di telecamere per motivi di sicurezza, oltre ad una opportuna e specifica informativa circa la videosorveglianza dei dipendenti. In questo caso, le telecamere dovranno avere spie luminose, per essere identificabili, ed essere installate solo in angoli dell'azienda (potenzialmente a rischio rapina o di attività criminali), sempre tenendo conto della privacy delle persone. Pertanto, la ripresa dell'attività lavorativa a distanza dei lavoratori deve essere occasionale ed esclusivamente finalizzata alla sicurezza aziendale e dello stesso dipendente;
- si devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni;
- prima di mettere in funzione l'impianto, il datore deve avvisare i lavoratori interessati fornendo un'informativa privacy;
- nominare un responsabile alla gestione dei dati registrati;
- posizionare le telecamere nella zona a rischio evitando di riprendere in maniera unidirezionale i lavoratori;

- è opportuno che venga predisposto un regolamento aziendale relativo ai sistemi di videosorveglianza e registrazioni di immagini in uso presso l'azienda. Il regolamento, oltre a riportare il censimento aggiornato dei sistemi e dei relativi trattamenti nell'ambito in oggetto, dovrebbe contenere le istruzioni operative suddivise per funzioni aziendali nonché le misure di sicurezza adottate. Nelle aziende più piccole il regolamento può essere sostituito da istruzioni scritte per gli incaricati;
- affiggere cartelli visibili che informino i dipendenti (ed eventuali clienti, ospiti o visitatori) della presenza dell'impianto di videosorveglianza;
- conservare le immagini per un tempo massimo di 24/48 ore;
- formare il personale addetto alla videosorveglianza;
- predisporre misure minime di sicurezza e misure atte a garantire l'accesso alle immagini solo al personale autorizzato;
- nel caso in cui le videocamere riprendano uno o più dipendenti mentre lavorano si deve procedere ad un accordo con le RSU (rappresentanze sindacali unitarie o aziendali). Qualora l'accordo non venga raggiunto, la legge prevede che la DPL (Direzione Provinciale del Lavoro) possa intervenire rilasciando l'autorizzazione all'installazione dei dispositivi elettronici di controllo a distanza. La Corte di Cassazione, infatti, ha ribadito che l'installazione di una telecamera sul posto di lavoro diretta verso il luogo in cui i propri dipendenti svolgono le proprie mansioni o su spazi dove essi hanno l'accesso anche sporadicamente, deve essere autorizzata preventivamente dall'Ispettorato del Lavoro o comunque da un particolare accordo con i sindacati

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3: Opinion & Guidelines W29 EDPB - provvedimenti, trattamenti particolari

Unità didattica

M3.13 Guidelines WP 29 su applicazione GDPR

Avv. Ida Tascone

Regolamento Europeo in materia di protezione dei dati personali

Efficacia diretta all'interno dei Paesi EU

Sostituisce e abroga la Direttiva 95/46/UE

Importanti innovazioni nel sistema *data protection* attuale

La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali.

Regolamento Europeo in materia di protezione dei dati personali: obiettivi

- Armonizzazione (non solo il testo ma anche l'interpretazione e l'applicazione, tramite l'one stop shop e i meccanismi di coerenza);
- Aggiornamento ed ampliamento del catalogo dei diritti (incluso anche il data breach)
- Accountability / nuovo focus sulla valutazione del rischio

"La Commissione sarà vigile nell'evitare re-nazionalizzazioni della privacy. Anche la mera riproduzione nelle leggi nazionali dello stesso testo di una direttiva comunitaria regolamentare è illegittima, in quanto crea incertezze e confusione" (Gencarelli, convegno Torino 6.11.17)

Regolamento Europeo in materia di protezione dei dati personali

Il Regolamento introduce nuovi adempimenti in capo ai titolari e responsabili del trattamento di dati personali (e.g. informativa, registro trattamenti, diritti dell'interessato, etc.)

Il Regolamento impone anche un'attività di adeguamento legislativo a livello nazionale

In determinati settori, il Regolamento prevede anche un margine di manovra degli Stati Membri per precisarne le norme, mediante apposite deleghe

Le Deleghe

- Riciclaggio o attività di medicina legale
- Base giuridica del trattamento
- Categorie particolari di dati personali
- Diritti degli interessati, incluse le decisioni basate sulla profilazione e data breaches
- Compiti dell'autorità pubblica o dell'organismo pubblico e lo specifico trattamento
- Autorità di controllo
- Trattamento dei dati personali dei dipendenti nell'ambito del rapporto di lavoro
- Sanzioni penali
- Codici di condotta
- Meccanismi di certificazione della protezione dei dati
- Rappresentanza degli interessati
- Trattamento e libertà di espressione e di informazioni

L'implementazione: il Governo

La Legge Comunitaria 2017, adottata il 18.10.17, delega il Governo ad adottare entro sei mesi, uno o più decreti legislativi per adeguare il quadro normativo al Regolamento nel rispetto dei seguenti principi e criteri:

1. abrogare espressamente le disposizioni del Codice Privacy incompatibili col Regolamento
2. modificare il Codice Privacy e successive modificazioni, limitatamente a quanto necessario per dare attuazione al Regolamento
3. coordinare le disposizioni vigenti con le disposizioni del Regolamento
4. prevedere il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante nell'ambito e per le finalità previste dal Regolamento
5. adeguare, nell'ambito delle modifiche al Codice Privacy, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del Regolamento con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione

L'implementazione: il Garante

Il 28 aprile 2017 il Garante per la protezione dei dati personali ha emanato una prima Guida all'applicazione del Regolamento, che definisce un quadro generale delle principali innovazioni introdotte dalla normativa e fornisce indicazioni sulle prassi da seguire e gli adempimenti da attuare

Il Garante ha fornito anche indicazioni preliminari su specifici aspetti :

- la certificazione in materia di dati personali (18 luglio 2017)
- come scegliere il Responsabile della protezione dei dati - RPD o Data Protection Officer - DPO (15 settembre 2017)

Il Garante ha anche avviato una serie di consultazioni con le imprese (e.g. nell'ambito delle istituzioni bancarie) per vagliare i Provvedimenti che rimarranno in vigore e quelli che dovranno essere abrogati o integrati conformemente al Regolamento

L'implementazione: il WP29

Il WP29 ha approvato numerose Linee Guida che riguardano:

- il **Responsabile per la protezione dei dati (Data Protection Officer - DPO)**, del 5 aprile 2017;
- Il **diritto alla portabilità dei dati,** del 13 dicembre 2016;
- L'**Autorità Capofila**, adottate il 13 dicembre 2016;
- La **valutazione d'impatto sulla protezione dei dati (DPIA)** del 4 aprile 2017;
- Il trattamento di dati personali nel **contesto lavorativo**, dell'8 giugno 2017;
- L'**applicazione delle sanzioni amministrative** (3 ottobre 2017);
- I **data breaches** (3 ottobre 2017);
- La **profilazione** (3 ottobre 2017).

Regolamento Europeo in materia di protezione dei dati personali: le novità

Applicazione territoriale

Il Regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, anche se effettuato da un titolare o responsabile del trattamento che non è stabilito nell'Unione quando il trattamento riguarda:

(a) l'offerta di beni e servizi, indipendentemente dall'obbligatorietà di un pagamento (e quindi anche la messa a disposizione di sevizi gratuiti);

(b) Il monitoraggio del comportamento, nella misura in cui tale comportamento ha luogo nell'interno dell'Unione

nomina per iscritto di un Rappresentante stabilito nell'Unione

ONE STOP SHOP

analisi preventiva e semplificazione

Il GDPR segna soprattutto una inversione di rotta. Infatti il titolare ed il responsabile sono tenuti a:

(a) adottare comportamenti e misure in grado di dimostrare la concreta adozione di misure atte ad assicurare l'applicazione del RGPD

(b) valutare preventivamente e autonomamente se il trattamento, con le relative modalità, finalità e limiti, può essere effettuato nei termini decisi in proprio (ad esempio, utilizzando il legittimo interesse come base giuridica del trattamento)

(c) tenere in preliminare considerazione il rischio inerente il trattamento, vale a dire il rischio di impatti negativi sulle libertà e sui diritti dell'interessato

(d) valutare preventivamente e autonomamente (es. con DPIA) se il trattamento non presenta rischi, e se può essere effettuato nei termini decisi in proprio, o se consultare l'autorità

(e) mettere in atto misure tecniche e organizzative adeguate per garantire il livello di sicurezza idoneo a minimizzare il rischio individuato

Registro dei trattamenti

Il Regolamento prevede per il titolare ed il responsabile l'obbligo di tenuta in forma scritta (anche elettronica) di un Registro dei trattamenti svolti sotto la propria responsabilità che indichi:

(a) Il titolare, il contitolare, ove applicabile, il rappresentante del trattamento e il DPO;
(b) Le finalità del trattamento;
(c) La descrizione delle categorie di interessati e di dati personali;
(d) Le categorie di destinatari;
(e) I trasferimenti di dati verso un paese terzo (compresa l'identificazione del paese e le garanzie del trasferimento)
(f) I termini per la cancellazione delle diverse categorie di dati;
(g) Una descrizione delle misure di sicurezza (tecniche ed organizzative)

NO OBBLIGO per imprese con meno di 250 dipendenti salvo che il trattamento (i) non presenti rischi per i diritti dell'interessato; (ii) il trattamento sia non occasionale; (iii) il trattamento non includa categorie particolari di dati

Data Protection Officer: *nomina*

Il Regolamento introduce un preciso modello organizzativo privacy prevedendo una nuova figura all'interno dell'organigramma aziendale.

Il **DPO è obbligatorio**:

(a) Se il trattamento è svolto da una autorità pubblica o da un organismo pubblico;

(b) Se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio sistematico e regolare degli interessati su larga scale;

(c) Se le attività del titolare o del responsabile consistono in trattamenti su larga scala di categorie particolari di dati o di dati idonee a rivelare condanne penali e reati

Negli altri casi la nomina del DPO può risultare utile in termine di *compliance* per la protezione dei dati (WP29)

Data Protection Officer: *compiti*

Il DPO deve svolgere i seguenti compiti:

(a) Informare e fornire consulenza in merito agli obblighi del Regolamento e di altre disposizioni in materia di trattamento dei dati;

(b) Sorvegliare l'attuazione del Regolamento, di altre disposizioni legislative sulla protezione dei dati e le politiche privacy compresi l'attribuzione delle responsabilità, la formazione del personale, e gli audit connessi;

(c) Fornire parere sulla valutazione d'Impatto e sorvegliarne lo svolgimento;

(d) Cooperare con l'autorità di controllo;

(e) Fungere da punto di contatto con l'autorità di controllo.

Data Protection Officer: *posizione*

Il Regolamento precisa **la posizione del DPO nell'ambito della compagine societaria:**

(a) Il DPO deve essere tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati;
(b) Il Titolare o il responsabile devono fornirgli tutte le risorse necessarie per assolvere ai compiti e accedere ai dati personali e mantenere la propria conoscenza specialistica;
(c) Il Titolare o il responsabile devono assicurargli l'autonomia ed indipendenza, senza dare istruzioni circa l'esercizio dei compiti
(d) Il DPO riferisce direttamente al vertice gerarchico
(e) Il DPO non è rimosso o penalizzato
(f) Il DPO può svolgere altri compiti e funzioni, ma il titolare o il responsabile si assicurano che non diano adito a conflitti.

Privacy By Design e By default

In base al Regolamento il titolare deve **sin dalla fase di progettazione** del trattamento individuare e mettere in atto misure tecniche ed organizzative adeguate per:

(a) Attuare in modo efficace i principi di protezione dei dati (es. Minimizzazione);
(b) Integrare nel trattamento le garanzie necessarie per soddisfare i requisiti del trattamento
(c) Tutelare i diritti degli interessati

Il titolare inoltre deve mettere in atto adeguate misure tecniche ed organizzative per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento. Questo obbligo vale per: quantità di dati raccolti; il periodo di conservazione, accessibilità.

Privacy By Design e By default

La PbD comprende 7 principi :

- Approccio proattivo non reattivo – prevenire non correggere
- Privacy come impostazione di default
- Privacy incorporata nella progettazione
- Massima funzionalità − Valore positivo, non valore zero
- Sicurezza fino alla fine − Piena protezione del ciclo vitale
- Visibilità e trasparenza − Mantenere la trasparenza
- Rispetto per la privacy dell'utente − Centralità dell'utente

Valutazione di Impatto (DPIA)

Il titolare è tenuto a realizzare, prima di procedere al trattamento, una DPIA quando:

(a) Il trattamento su larga scala di categorie particolari di dati e dati giudiziari
(b) Sorveglianza sistematica su larga scala di una zona accessibile al pubblico
(c) Valutazione sistematica e globale di aspetti relativi a persone fisiche basate su un trattamento automatizzato (es. Profilazione)

La PIA può riguardare plurime operazioni di trattamento se presentano caratteristiche simili, quanto a qualità e quantità dei rischi

Se la DPIA indica che i trattamenti presentano un rischio elevato che non può essere attenuato mediante misure opportune, prima del trattamento si dovrebbe consultare l'autorità di controllo

L'autorità di controllo redigerà un elenco di trattamenti da sottoporre o da sottrarre a PIA da sottoporre al Comitato Europeo

Valutazione di Impatto (DPIA): le linee guida del WP29

Le Linee Guida indicano 10 categorie di rischio elevato (fra cui profilazione e predizione, decisioni automatizzate, con ricadute legali; monitoraggio sistematico, trattamenti di dati sensibili o su larga scala, raffronto di dati, trattamento di dati di appartenenti a fasce deboli, innovazioni tecnologiche - come Internet of Things, trasferimenti di dati extra-UE, trattamento di dati che incidono sull'accesso a servizi o contratti (e.g. consultazioni dati di merito creditizio per concedere un mutuo).

Qualora un trattamento comprenda almeno due dei dieci criteri di rischio elevato, di regola la PIA è necessaria

La PIA non è richiesta (i) se non c'è rischio elevato; (ii) quando si può utilizzare una PIA per un altro trattamento simile; (iii) quando una base legale disciplina la gestione del rischio e sostanzialmente assorbe questo adempimento; (iv) quando il trattamento è compreso nella lista degli esoneri stilata dall'Autorità di controllo

Valutazione di Impatto (DPIA): le linee guida del WP29

Le Linee Guida indicano 10 categorie di rischio elevato (fra cui profilazione e predizione, decisioni automatizzate, con ricadute legali; monitoraggio sistematico, trattamenti di dati sensibili o su larga scala, raffronto di dati, trattamento di dati di appartenenti a fasce deboli, innovazioni tecnologiche - come Internet of Things, trasferimenti di dati extra-UE, trattamento di dati che incidono sull'accesso a servizi o contratti (e.g. consultazioni dati di merito creditizio per concedere un mutuo).

Qualora un trattamento comprenda almeno due dei dieci criteri di rischio elevato, di regola la PIA è necessaria

La PIA non è richiesta (i) se non c'è rischio elevato; (ii) quando si può utilizzare una PIA per un altro trattamento simile; (iii) quando una base legale disciplina la gestione del rischio e sostanzialmente assorbe questo adempimento; (iv) quando il trattamento è compreso nella lista degli esoneri stilata dall'Autorità di controllo

Valutazione di Impatto (DPIA): *contenuto*

La DPIA contiene almeno:

(a) Descrizione sistematica dei trattamenti, delle finalità e l'interesse legittimo del titolare;

(b) Valutazione della necessità e proporzionalità dei trattamenti rispetto alle finalità;

(c) Valutazione dei rischi

(d) Le misure per affrontare i rischi, includendo le garanzie e le misure di sicurezza e i meccanismi per garantire la protezione dei dati

Il titolare dovrà tener conto dei codici di condotta, eventualmente delle opinioni di interessati, rappresentanti (es. Associazioni di categoria) fatta salva la tutela degli interessi commerciali

Informativa: *contenuto*

Il Regolamento individua nuovi requisiti per il **CONTENUTO** dell'informativa che, che deve specificare:

(a) I dati di contatto del DPO, se nominato
(b) La base giuridica del trattamento;
(c) L'eventuale interesse legittimo, se costituisce la base giuridica del trattamento
(d) Se viene effettuato un trasferimento dei dati personali in paesi terzi e gli strumenti di detto trasferimento (es. consenso, BCR, clausole contrattuali etc.)
(e) Il periodo di conservazione dei dati o i criteri per stabilire il periodo
(f) Il diritto di presentare un reclamo all'Autorità di controllo
(g) Se il trattamento comporta processi automatizzati (es. profilazione)

Informativa: *tempi e modalità*

Se i dati personali non sono raccolti presso l'interessato l'informativa deve essere fornita **entro un termine ragionevole** (non più di 1 mese) o al momento della comunicazione dei dati a terzi o all'interessato

L'informativa deve essere **concisa, trasparente, intellegibile per l'interessato e facilmente accessibile.** L'informativa è data, generalmente, **per iscritto e preferibilmente in formato elettronico**

È ammesso l'uso di **icone** (informativa sintetica) ma solo in combinazione con l'informativa estesa. Le icone dovranno essere identiche in tutta al UE e quindi verranno definite prossimamente dalla Commissione

Spetta al Titolare valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato che esonera dall'informativa

Consenso

Il Regolamento individua nuovi requisiti per il consenso:

(a) per i dati sensibili e per i trattamenti automatizzati deve essere esplicito;

(b) NON deve essere necessariamente «documentato per iscritto» NON è richiesta la forma scritta ma deve essere inequivoco

(c) Il titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso

(d) Il consenso dei minori è valido a partire dai 16 anni, prima di tale età occorre il consenso dei genitori o di chi ne fa le veci

Esclusa ogni forma di consenso tacito oppure ottenuto proponendo ad un interessato opzioni già preselezionate.
I consensi ottenuti nel rispetto dei requisiti di cui al Regolamento restano legittimi, con il dubbio dell'informativa

L'opposizione al trattamento

Il Regolamento individua i tre casi in cui l'interessato può opporsi al trattamento dei dati personali che lo riguardano

1. Opposizione ai trattamenti per scopi di pubblico interesse o legittimo interesse (opposizione per motivi legittimi)
2. Opposizione al trattamento di marketing diretto, inclusa la relativa profilazione
3. Opposizione ai trattamenti per finalità scientifiche, storiche o statistiche

Sono esclusi dal diritto di opposizione tutti gli altri trattamenti

I nuovi diritti: diritto all'oblio e diritto alla limitazione del trattamento

Il Regolamento riconosce all'interessato due nuovi specifici diritti:

(a) Diritto all'oblio, cioè alla cancellazione in forma rafforzata (es. dei dati pubblicati su siti web), che include il dovere per i titolari di informare della richiesta di cancellazione altri titolari che trattano i dati cancellati (es. compresi i link);

(b) Diritto alla limitazione del trattamento, si applica non solo in alternativa alla cancellazione, ma anche se è richiesta la rettifica dei dati o l'opposizione al trattamento, nell'attesa che il titolare provveda alla rettifica o valuti l'opposizione)

Il diritto alla limitazione prevede che il dato sia «contrassegnato» in attesa di determinazioni ulteriori: necessaria integrazione dei sistemi informativi del titolare

I nuovi diritti: portabilità dei dati

Il Regolamento riconosce all'interessato il nuovo diritto della c.d. *data portability*, che prevede la possibilità che l'interessato richieda "la portabilità" dei propri dati ad un altro soggetto, a condizione che:

(a) il trattamento sia effettuato in maniera automatizzata (quindi non trova applicazione per gli archivi o registri cartacei);

(b) sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato

(c) il diritto è esercitabile solo se i dati sono stati forniti dall'interessato.

Al riguardo le Linee Guida del Gruppo dei 29 (c.d. Working Party) sulla portabilità dei dati illustrano requisiti e caratteristiche dell'esercizio di tale diritto.

Riscontro agli interessati

Il RGPD attribuisce al titolare un termine maggiore di quello attuale (15 giorni) per il riscontro all'interessato, vale a dire un mese, estensibile fino a tre mesi in casi di particolare complessità. A tal fine il titolare dovrà:

(a) Fornire un riscontro in forma scritta, salvo che non sia l'interessato a richiedere un riscontro orale
(b) Adottare misure tecniche ed organizzative per agevolare l'esercizio dei diritti da parte dell'interessato, anche tenendo in considerazione le indicazioni fornite in precedenza dal Garante
(c) Valutare in proprio la complessità del riscontro ed eventualmente stabilire l'ammontare del contributo da chiedere all'interessato (es. richieste manifestamente infondate, eccessive, ripetitive o se sono richieste più copie dei dati personali), mentre in generale il riscontro è gratuito

Data breach notification

In base al Regolamento il titolare notificare alle autorità di controllo le violazioni di dati personali di cui vengono a conoscenza, :

(a) entro 72 ore o, comunque, senza ritardo

(b) se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà dell'interessato;

(c) provvedendo a notificare i c.d. *data breach* senza ritardo anche agli interessati coinvolti qualora - all'esito della valutazione del rischio compiuta dal titolare - la probabilità di rischio sia elevata.

Le violazioni devono essere tutte documentate a prescindere se siano o meno notificate all'autorità. Ne consegue che i titolari dovranno predisporre le misure necessarie a documentare dette violazioni

Trasferimenti extra UE

Il titolare che intenda effettuare trasferimenti di dati personali in Paesi fuori dall'Unione Europea dovrà:

(a) trasferire i dati in Paesi terzi che presentano standard di adeguatezza riconosciuti dalla Commissione Europea (le decisioni di adeguatezza adottate dalla Commissione Europea prima dell'entrata in vigore del RGPD, es. Privacy Shield, restano valide);

(b) trasferire i dati sulla base delle c.d. clausole contrattuali tipo approvate dalla Commissione, o tramite norme vincolanti di impresa ("BCR"), **o ancora tramite l'adesione ai codici di condotta espressamente previsti nel Regolamento, ovvero all'esito di certificazione.**

Il RGPD prevede il divieto di trasferimento di dati personali basato su decisioni giudiziarie o ordinanze amministrative emesse da autorità di Paesi terzi, a meno dell'esistenza di appositi accordi internazionali fra gli Stati coinvolti.

Principio di accountability

Il RGPD prevede il nuovo obbligo di c.d. responsabilizzazione, per cui il titolare e il responsabile saranno tenuti a:

(a) mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di **dimostrare**, che il trattamento è effettuato conformemente al RGPD;

(b) redigere e conservare documentazione idonea ad attestare detta *compliance* (es. Registro dei trattamenti, portabilità)

(c) riesaminare e se necessario aggiornare tale documentazione.

L'adesione ai codici di condotta a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi di *accountability* del titolare del trattamento.

Codici di condotta e certificazioni

(a) Il Regolamento incoraggia l'elaborazione di **codici di condotta** da parte delle associazioni di categoria per precisare l'applicazione dei nuovi obblighi (es. legittimo interesse, pseudonimizzazione, notifica delle violazioni, diritti degli interessati, etc.)

(b) Il Regolamento promuove altresì l'istituzione a livello Europeo di meccanismi di **certificazione della protezione dei dati** nonché di sigilli e marchi allo scopo di dimostrare la conformità alla nuova normativa dei trattamenti effettuati dai titolari e responsabili del trattamento e dai responsabili del trattamento, anche tenendo in conto le esigenze specifiche delle micro, piccole e medie imprese

La profilazione

Per **profilazione** si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica (cfr. Art. 4)

La profilazione

La profilazione non è ammessa, salvo che sia necessaria per legge, che avvenga con il consenso dell'interessato, o sia necessaria per la conclusione o l'esecuzione di un contratto

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla persona (e.g. rifiuto automatico di una domanda di credito online, pratiche di assunzione elettronica senza interventi umani)

Richiede in ogni caso la PIA

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 3: Opinion & Guidelines W29 EDPB - provvedimenti, trattamenti particolari

Unità didattica

M.3.14 Case History: DPO - La nuova norma nazionale sulla privacy

Avv. Ida Tascone

Come scegliere il Data Protection Officer ?

Newsletter N. 432 del 15 settembre 2017

Le prime indicazioni del GARANTE

- Approfondita conoscenza della normativa e delle prassi in materia di privacy;

- Approfondita conoscenza delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

Il Data Protection Officer

- Responsabile della Protezione dei Dati -

Il **Data Protection Officer** (*Responsabile della Protezione dei Dati*) è una figura prevista dal Regolamento UE 679/2016 del 27aprile 2016, relativo alla *protezione delle persone fisiche con riguardo al trattamento dei dati personali .*

Art. 37 Regolamento UE 679/2016

Il titolare del trattamento e il responsabile del trattamento **designano sistematicamente un responsabile della protezione dei dati ogni qualvolta:**

a) il trattamento è effettuato da **un'autorità pubblica o da un organismo Pubblico**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali *(le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento**)* del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, **richiedono** il **monitoraggio regolare e sistematico degli interessati su «larga scala»: ****

- *numero di soggetti interessati dal trattamento, in termini assoluti* ovvero espressi in percentuale della popolazione di riferimento;
- *volume dei dati e/o le diverse tipologie di dati* oggetto di trattamento;
- *durata, ovvero la persistenza, dell'attività di trattamento*;
- *portata geografica* dell'attività di trattamento.

da Linee guida DPO – WP 243 -13/12/2016

Alcuni esempi di trattamento su larga scala **:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

NON rientra nel concetto di «*larga scala*»il trattamento dei dati di pazienti da parte di un singolo medico o quello relativo a condanne penali e reati da parte di un singolo avvocato

(** da «**Linee guida DPO –WP 243- 13/12/2016**»)

Il Responsabile della protezione dei dati è designato dal **Titolare** e dal **Responsabile** del trattamento. *Nel caso di designazione da parte di un Responsabile del trattamento, si tratterà di un Responsabile esterno oppure di un Responsabile interno delegato appositamente dal Titolare.*

Il responsabile della protezione dei dati è designato per iscritto con **analitica elencazione dei compiti e responsabilità**, cioè:

1. tutti quelli previsti dalla legge;
2. più eventualmente quelli oggetto di specifica delega di funzioni (proprie) da parte del Titolare (o del Responsabile)

Il **Responsabile della protezione dei dati** è designato in funzione:

- ✓ delle qualità professionali, in particolare della *conoscenza specialistica della normativa* e delle *prassi in materia di protezione dei dati;*
- ✓ e della capacità di assolvere i compiti (previsti dall'articolo 39).

Il responsabile della protezione dei dati può essere:

1.un dipendente del titolare del trattamento o del responsabile del trattamento;

*(Se **dipendente**: Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi)*

Il responsabile della protezione dei dati può:

2. assolvere i suoi compiti in base a un **contratto di servizi per la durata di 2 anni**.

«In base all'art. 37, paragrafo 6, il **DPO può "*assolvere i suoi compiti in base a un contratto di servizi*"**. In quest'ultimo caso il DPO sarà **esterno** e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.

Se il DPO è esterno, si applicano tutti i requisiti fissati negli articoli da 37 a 39. Come indicato nelle linee-guida, se la funzione di DPO è svolta da un fornitore esterno di servizi, i compiti stabiliti per il DPO potranno essere assolti efficacemente da un *team* operante sotto **l'autorità di un contatto principale** designato e "responsabile" per il singolo cliente".

In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale DPO soddisfi tutti i requisiti applicabili come fissati nel RGPD.

Per favorire efficienza e correttezza, le linee-guida raccomandano di procedere a una chiara ripartizione dei compiti nel *team* del DPO esterno, attraverso il contratto di servizi, e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente».

(** da «**Linee guida DPO –WP 243- 13/12/2016**»)

Il responsabile della protezione dei dati può:

2. assolvere i suoi compiti in base a un contratto di servizi.

.....

Se consulente/fornitore esterno di servizi:

In **possesso di adeguate professionalità e capacità**, quelle previste dalla legge, **formalizzate nel contratto di servizi**. Nel contratto di appalto di servizi o di consulenza occorre **inserire clausole** che prevedano espressamente responsabilità, oltre che di legge, contrattuali del DPO esterno, sia per l'effettuazione delle attività previste dalla legge e dalla nomina, sia per il mantenimento dei requisiti professionali richiesti.

Il responsabile della protezione dei dati può:

2. assolvere i suoi compiti in base a un contratto di servizi.

.....

Se consulente/fornitore esterno di servizi:

In **possesso di adeguate professionalità e capacità**, quelle previste dalla legge, **formalizzate nel contratto di servizi**. Nel contratto di appalto di servizi o di consulenza occorre **inserire clausole** che prevedano espressamente responsabilità, oltre che di legge, contrattuali del DPO esterno, sia per l'effettuazione delle attività previste dalla legge e dalla nomina, sia per il mantenimento dei requisiti professionali richiesti.


ovrà:
possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;
operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio.
titolare o il responsabile del trattamento dovranno ettere a disposizione del Responsabile della protezione ei dati le risorse umane e finanziarie necessarie l'adempimento dei suoi compiti.
N QUALI CASI E' PREVISTO?
ovranno designare obbligatoriamente un Responsabile della rotezione dei dati:
amministrazioni ed enti pubblici, fatta eccezione per le utorità giudiziarie;
tutti i soggetti la cui attività principale consiste in trattamenti ıe, per la loro natura, il loro oggetto o le loro finalità, richiedono il ontrollo regolare e sistematico degli interessati;
tutti i soggetti la cui attività principale consiste nel attamento, su larga scala, di dati sensibili, relativi alla salute o la vita sessuale, genetici, giudiziari e biometrici.
Un titolare del trattamento o un responsabile del trattamento possono comunque designare un Responsabile della protezione dei dati anche in casi diversi da quelli sopra indicati.
Un gruppo di imprese o soggetti pubblici possono nominare un unico Responsabile della protezione dei dati.
QUALI SONO I COMPITI?
Il Responsabile della protezione dei dati dovrà:
a) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;
d) fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;
e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

Competenze DPO

Qualità professionali:

1. Conoscenza della normativa in materia di protezione dei dati personali (*Regolamento, linee guida e autorizzazioni Autorità Garante*);
2. Conoscenza della normativa specifica del settore di appartenenza dell'impresa (*per obbligatorietà trattamen data retention etcc.*)
3. Conoscenza prassi (*provvedimenti e pareri Autori Garante*);
4. Conoscenza aspetti della sicurezza informatica (*per verifica misure sicurezza adeguate*)

Se procedo a nominare un DPO senza averne l'obbligo sono tenuto a rispettare i requisiti normativi come nel caso di una nomina obbligatoria?

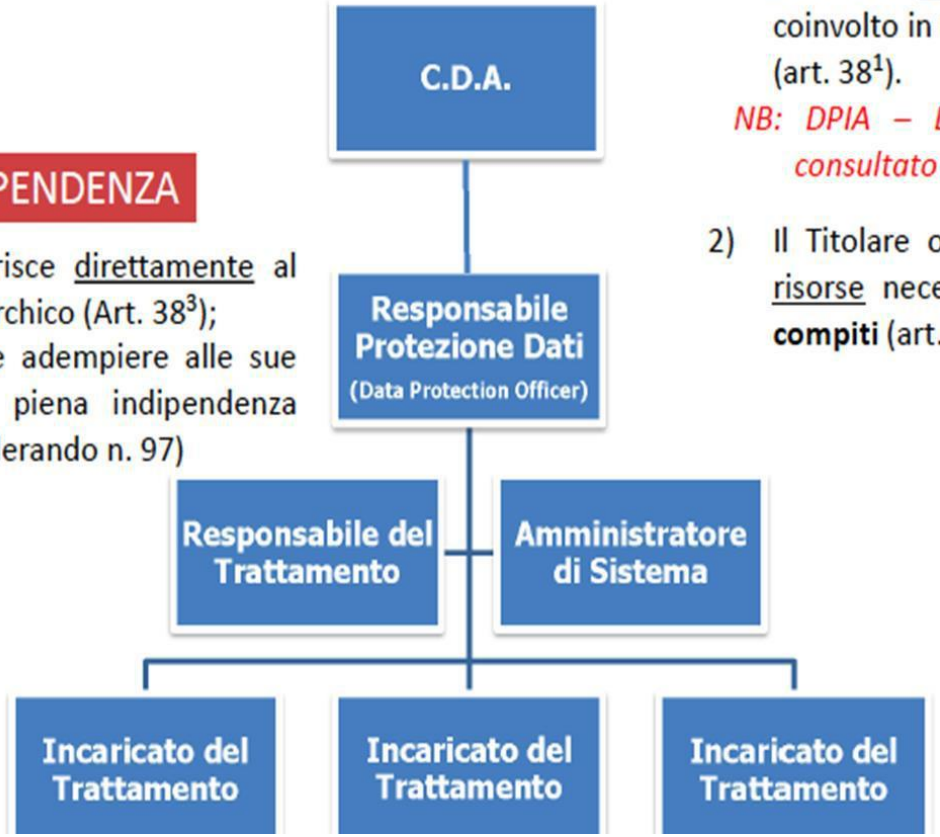
Se si procede alla nomina di un RPD su base volontaria, troveranno **applicazione tutti** i **requisiti** di cui agli artt. 37- 39 per quanto concerne la nomina stessa, lo status e i compiti del RPD esattamente come nel caso di una nomina obbligatoria.

When an organisation designates a DPO on a voluntary basis, the same requirements under Articles 37 to 39 will apply to his or her designation, position and tasks as if the designation had been mandatory. (WP 243, pag. 5).

POSIZIONE DEL DATA PROTECTION OFFICER Art. 38

INDIPENDENZA

Il DPO riferisce direttamente al vertice gerarchico (Art. 38[3]);
Il DPO deve adempiere alle sue funzioni in piena indipendenza (Vedi Considerando n. 97)



1) Il Titolare o Responsabile si assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni ad impatto privacy (art. 38[1]).

NB: DPIA – L'art. 35 prevede che il DPO sia consultato nella Valutazioni di impatto privacy.

2) Il Titolare o il Responsabile devono fornire le risorse necessarie al DPO per svolgere i Suoi **compiti** (art. 38[2])

Capacità di assolvere i compiti previsti dall'art. 39:

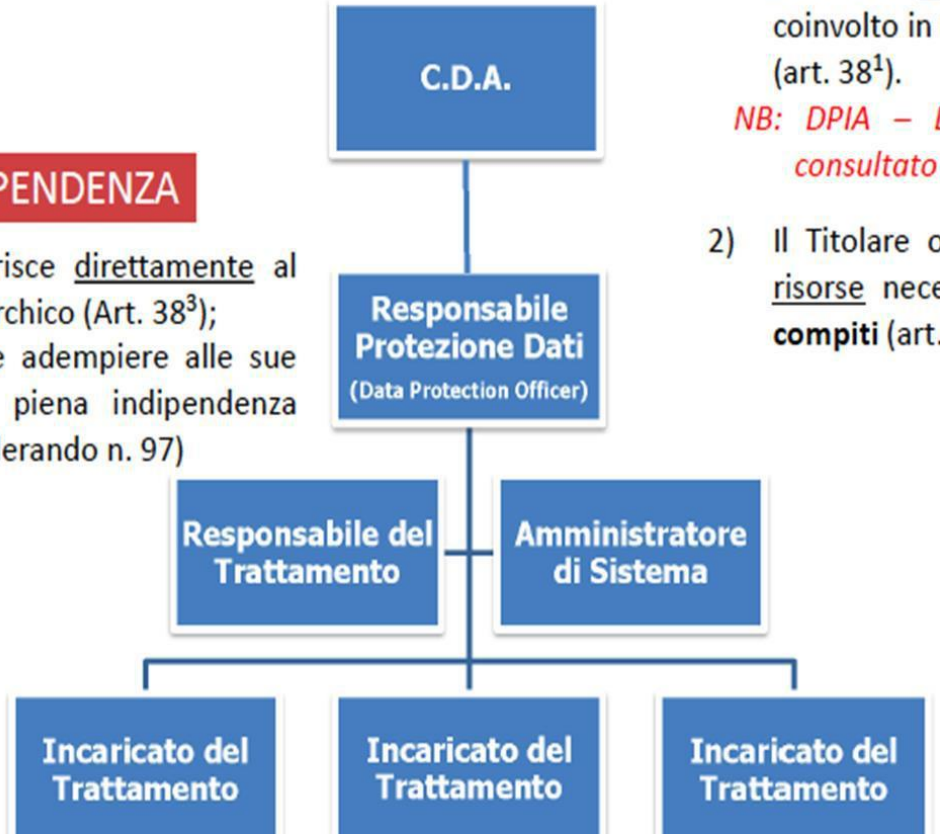
Conoscenza della realtà aziendale, dei processi interni e delle policies dell'azienda, delle politiche e delle prassi di trattamento dei dati personali degli *stakeholders* dell'impresa (*dipendenti, clienti, fornitori, consumatori, operatori sanitari, pazienti, media* etcc.) e delle relative modalità (es. *CRM, profilazione, marketing, biometria, geolocalizzazione, videosorveglianza etcc*)

Capacita relazionali, di management, di leadership, di teamwork……

POSIZIONE DEL DATA PROTECTION OFFICER Art. 38

INDIPENDENZA

Il DPO riferisce direttamente al vertice gerarchico (Art. 38[3]);
Il DPO deve adempiere alle sue funzioni in piena indipendenza (Vedi Considerando n. 97)



1) Il Titolare o Responsabile si assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni ad impatto privacy (art. 38[1]).

NB: DPIA – L'art. 35 prevede che il DPO sia consultato nella Valutazioni di impatto privacy.

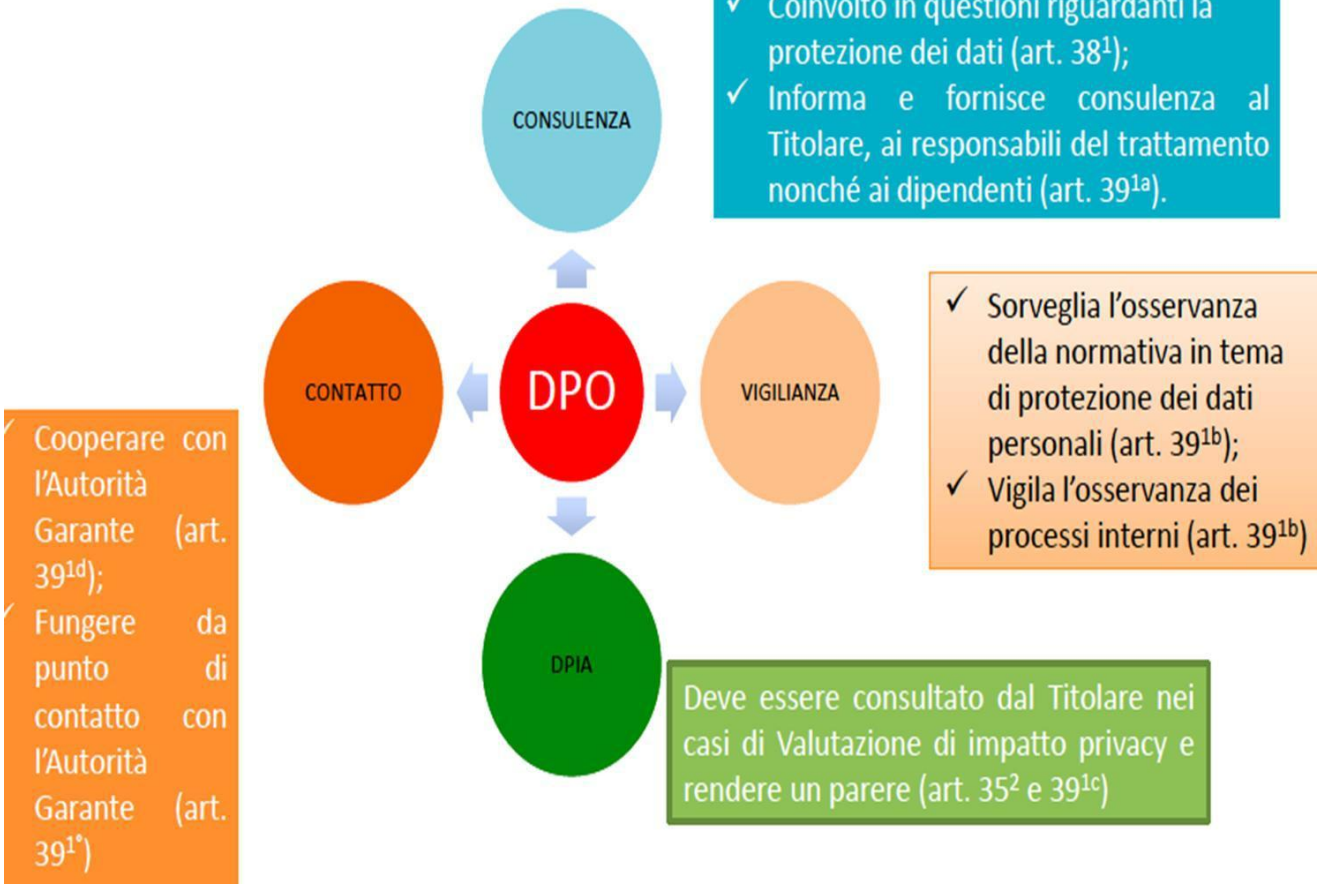
2) Il Titolare o il Responsabile devono fornire le risorse necessarie al DPO per svolgere i Suoi **compiti** (art. 38[2])

Capacità di assolvere i compiti previsti dall'art. 39:

Conoscenza della realtà aziendale, dei processi interni e delle policies dell'azienda, delle politiche e delle prassi di trattamento dei dati personali degli *stakeholders* dell'impresa (*dipendenti, clienti, fornitori, consumatori, operatori sanitari, pazienti, media* etcc.) e delle relative modalità (es. *CRM, profilazione, marketing, biometria, geolocalizzazione, videosorveglianza etcc*)

Capacita relazionali, di management, di leadership, di teamwork……

COMPITI - Art. 39



Il DPO ha le seguenti funzioni:

a) **informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) **sorvegliare l'osservanza del presente Regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle **politiche del titolare** del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la **sensibilizzazione e la formazione** del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un **parere in merito alla Valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) **cooperare con l'Autorità di controllo (ndr: il Garante Privacy)**;

e) **fungere da punto di contatto per l'Autorità di controllo** per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

- Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza
- E' responsabile per l'espletamento dei propri compiti nei confronti del Titolare o del Responsabile del trattamento che lo hanno designato
- E' responsabile verso l'Autorità di Controllo ai fini della cooperazione con la stessa

- ✓ il DPO non è responsabile personalmente in caso di inosservanza del regolamento.
- ✓ Il RGPD chiarisce che spetta al titolare o al responsabile del trattamento "*garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento*" (art. 24, paragrafo 1).
- ✓ La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare / sul responsabile del trattamento

(da «**Linee guida DPO –WP 243- 13/12/2016**»)

Coinvolgimento del DPO

Il titolare del trattamento e il responsabile del trattamento si assicurano che il Responsabile della Protezione dei dati sia adeguatamente e tempestivamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali

RESPONSABILITA'

Il Titolare o il responsabile mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza [Vedi articolo 5, comma 2 sul principio dell'accountability].

Se il Titolare o il responsabile assumono decisioni incompatibili con il RGPD e le indicazioni fornite dal RPD (DPO), quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso ai decisori.

- Quello del Data Protection Officer, **non è una figura professionale**, **bensì un ruolo** previsto dal Regolamento UE 2016/679, e definito in modo esaustivo dallo stesso testo normativo, dalla scheda informativa del Garante, dalla Linee Guida WP243, e dalle relative FAQ
- Il ruolo deve essere svolto da un soggetto che in primo luogo deve possedere un'**adeguata conoscenza della normativa** e delle prassi di gestione dei dati personali nazionali ed europee
- Non esiste al momento una qualche sorta di **"abilitazione"** che può sancire l'idoneità allo svolgimento del ruolo di DPO, anche perché le competenze richieste possono variare in base alla realtà in cui opera
- Le competenze devono essere quindi comprovate dal **curriculum**, di cui titolo di studio, corsi di formazione, esperienza maturata, ed eventuali certificazioni professionali, sono tutti tasselli che compongo le credenziali del candidato.

D.P.O.

INTERNET – LOCALIZZAZIONE SATELLITARE - BIOMETRIA

SYSTEM ADMINISTRATOR -CYBERCRIME

VIDEOSORVEGLIANZA – SOCIAL NETWORK

CLOUD COMPUTING – RFID – GPS – BYOD – BIG DATA