Ciclo di webinar in diretta

Sicurezza informatica & Protezione dei dati negli enti locali

Tecniche e Strumenti di prevenzione al cybercrime negli enti locali 12-12-2024

Relatore: Dottor Antonio Guzzo Funzionario Informatico Agenzia delle Entrate

Cyber security expert

DPO CERTIFIED ISO IEC 17024 e UNI 11697:2017

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54 (int.3)
Web: www.dpoinrete.it, www.asmel.eu

ASMEL

Indice

- Normativa europea ed italiana cybersecurity
- Strumenti di prevenzione per la sicurezza informatica nella pa e tecniche di prevenzione al cybercrime negli enti locali
- Linee guida nella navigazione web sicura ed in compliance per il dipendente pubblico schema di atto da approvare
- Tecniche di pseudonomizzazione ed anonimizzazione di data set pubblici
- Linee guida per l'espletamento della modalità lavorativa in smart-working secondo quanto previsto dal CSIRT Italiano della Presidenza del Consiglio dei Ministri nel mese di agosto 2020 nell'utilizzo dei device utilizzati in modalità safe (sicura) schema di atto da approvare
- Lo sviluppo software sicuro secondo quanto previsto da AGID
- Gli obblighi di cybersecurity ed il referente cyber
- Casi Pratici nella Pa

Normativa

- Decreto legislativo 18 maggio 2018, n. 65, *"Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione";*
- Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, *"relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»);*
- Decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre n. 133, recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*";

Normativa

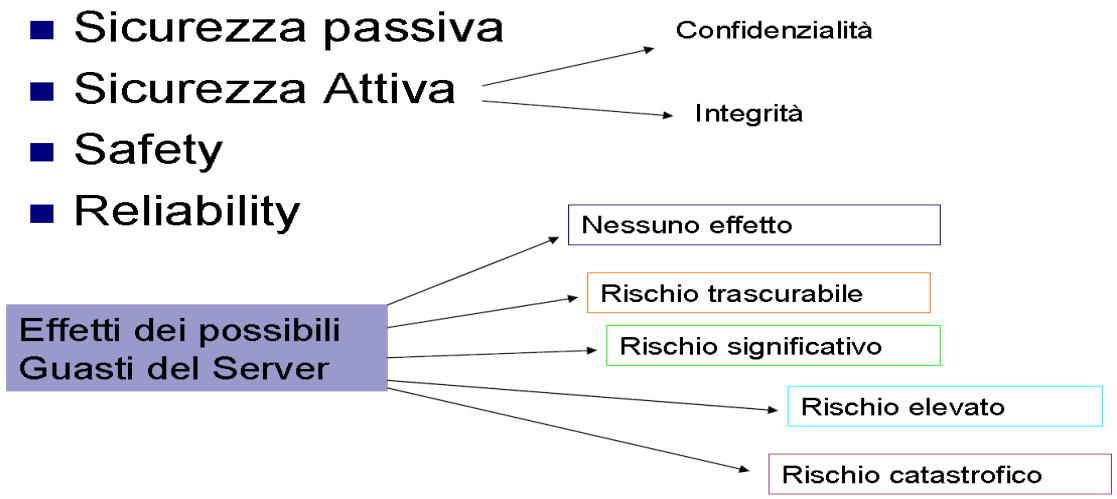
- Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, recante "Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133";
- Decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale";*
- Decreto-legge 9 giugno 2021, n. 80, convertito, con modificazioni, dalla legge 6 agosto 2021, n. 113, recante "*Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia",* che definisce percorsi veloci, trasparenti e rigorosi per il reclutamento di profili tecnici e gestionali necessari alle finalità del PNRR, tra cui la cybersicurezza;

Normativa

- Decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, recante *"Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale*";
- Decreto del Presidente del Consiglio dei ministri 15 giugno 2021, recante *"Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133";*
- Strategia Nazionale di Cybersicurezza 2022-2026 e il relativo Piano di Implementazione (di seguito anche "Piano") che definiscono come pianificare, coordinare e attuare misure tese al potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione, assicurando una trasformazione digitale sicura e resiliente;
- Legge 90/2024 del 28-06-2024 – Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici

Tecniche di prevenzione

- Al fine di prevenire un attacco informatico è necessario utilizzare un modello di sicurezza informatica cosi strutturato



Altri strumenti di prevenzione

- SVILUPPO E MANUTENZIONE DI SISTEMI (System Development and Maintenance)
- **Accertare** che la sicurezza sia stata costruita all'interno delle operazioni di sistema;
- **Impedire** la perdita, la modifica o il cattivo utilizzo dei dati dell'utente all'interno dei sistemi di applicazione;
- **Proteggere** la riservatezza l'autenticità e l'integrità delle in formazioni;
- **Accertarsi** che le attività di progetto e supporto alle attività siano condotte in modo sicuro e per mantenere la sicurezza del software e dei dati del sistema

Altri strumenti di prevenzione

- Al fine di prevenire i rischi di una **data exfiltration** è possibile utilizzare le seguenti contromisure
- Trasformare l'utente da anello debole a prima linea di difesa
- Applicare il principio del minimo privilegio per quanto riguarda l'accesso ai dati
- Adottare puntuali politiche di patching dei sistemi
- Crittografare i dati sensibili
- Utilizzare l'autenticazione a tre fattori (oggi si parla di 4 fattori)
- Rivolgere grande attenzione anche alla sicurezza fisica

Contromisure

- La miglior difesa dagli attacchi informatici è la prevenzione:
- Conoscenza dei possibili attacchi:
  - Aggiornamento continuo;
  - Valutazione impatto rispetto al proprio sistema.
- Gestione dei rischi:
  - Utilizzo di soluzioni tecnologiche;
  - Definizione di regole di utilizzo delle risorse.
- Diffusione della conoscenza:
  - Formazione e sensibilizzazione del personale interno;
  - Comunicazione ai soggetti con cui interagisce il sistema.

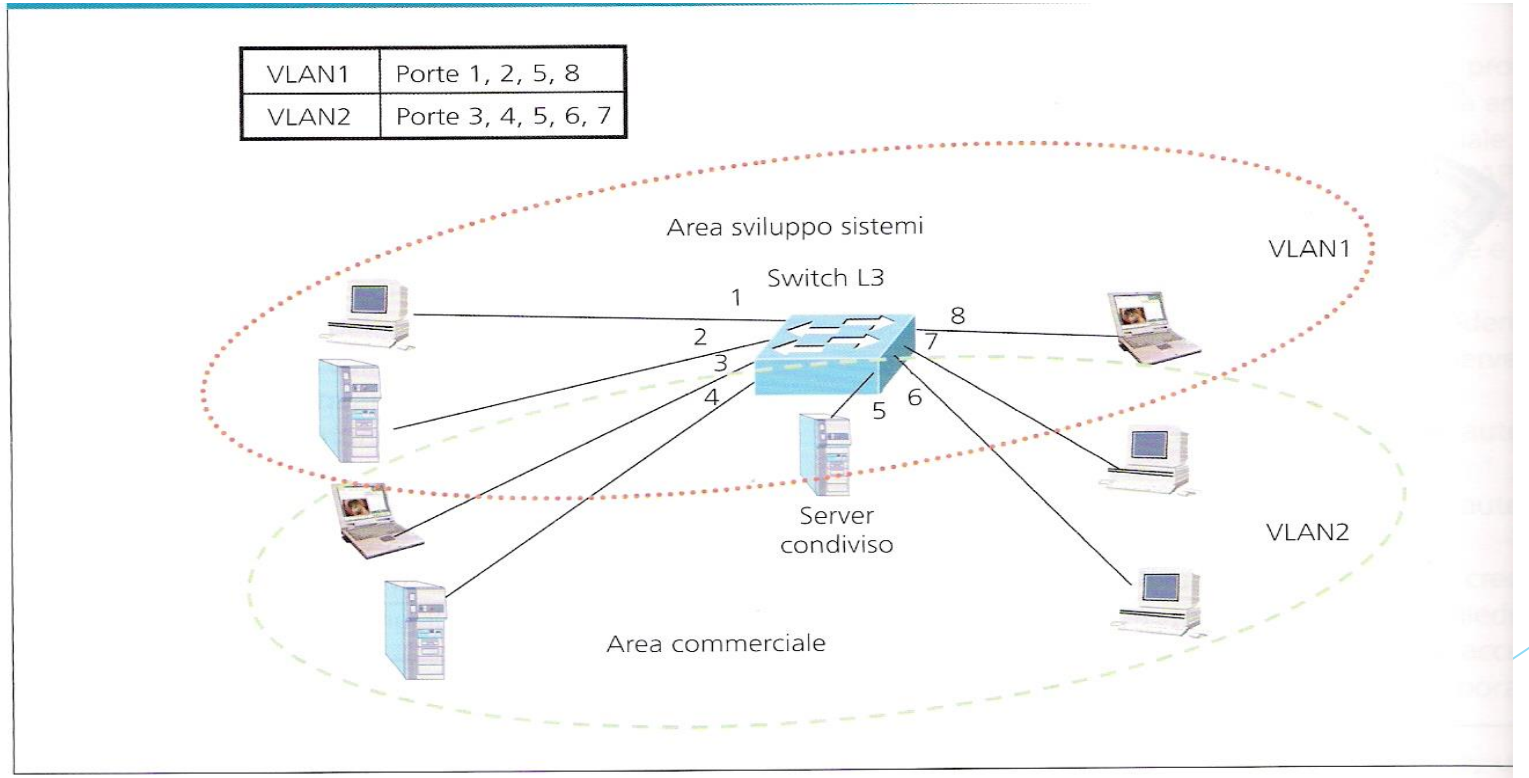
Contromisure

- ***Tutelare il bene più prezioso che circola in rete: i nostri dati personali*** (numeri di carte di credito, indirizzi, conti bancari);
- **La migliore contromisura per rispondere alle varianti del malware (malicious software) è quello di utilizzare un approccio integrato che comprenda barriere hardware e software ma anche corrette abitudini e regole ferree;**
- La somma delle contromisure è in gergo definita data loss prevention (perdita di informazioni);
- Introduzione della figura del security manager che ha il compito di interagire, conciliandolo sia a livello informatico che organizzativo;
- Strumenti software di duplice protezione del software di base che hanno il compito di recuperare tutte le diverse tipologie di informazioni utili per organizzare la sicurezza e dei dati che vengono elaborati e analizzati, tramite un processo di intelligence, in modo da essere strutturati secondo valori tematici;
- Definizione dei fattori di rischio e delle componenti da monitorare a livello di sicurezza, agendo nel tempo con dei piani di correzione.

Contromisure

- L’utilizzo di architetture di rete virtuali (vlan) che consentono di disaccoppiare le informazioni dai programmi e soprattutto dall’hardware utilizzato per trattarli, minimizzando i rischi di intrusione, sottrazione e danneggiamento;

Tecnicamente la virtualizzazione (ad es. con Symantec) viene fatta su 3 piani parallelli e cioè quello dello storage, quello dei server e quello degli endpoint (cioè i client);



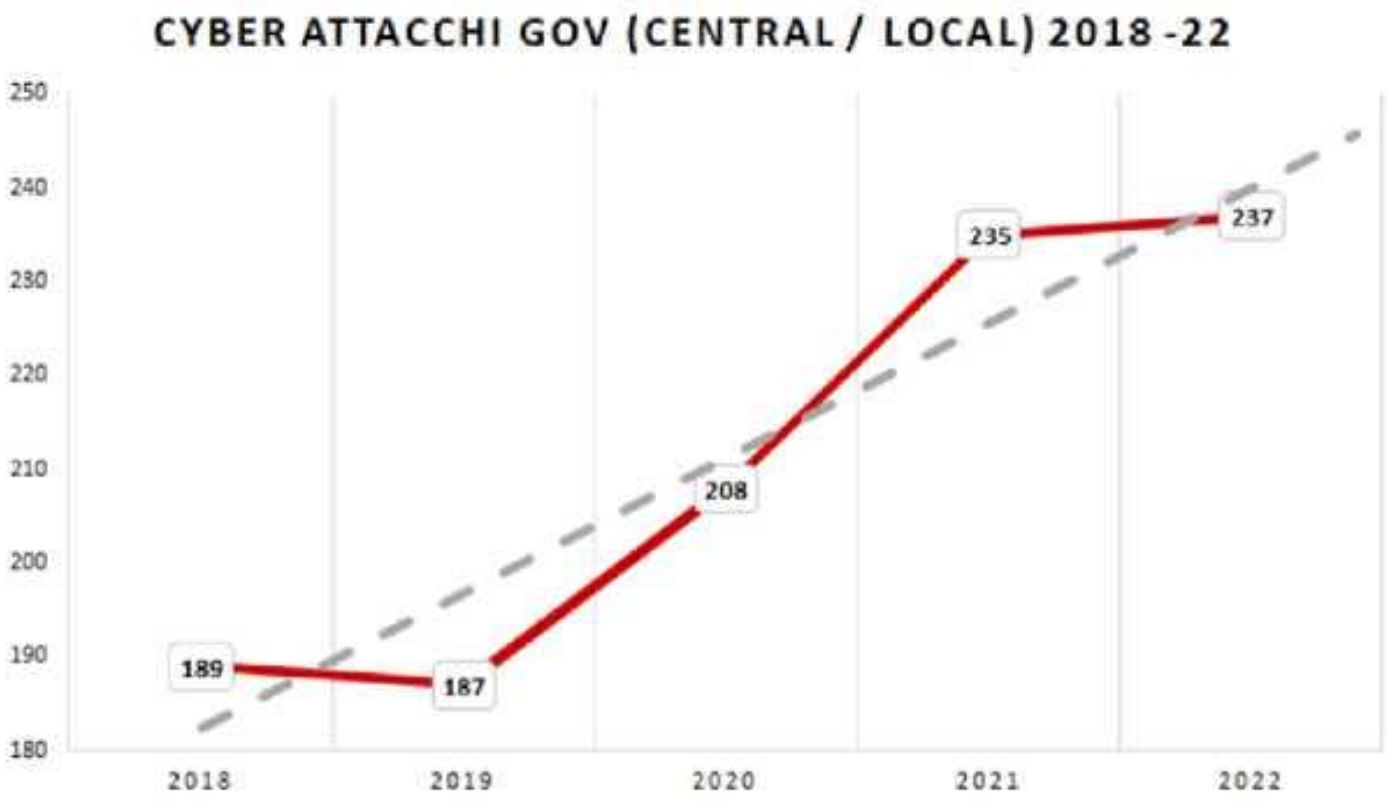
Cyber Data Incident Response Pack

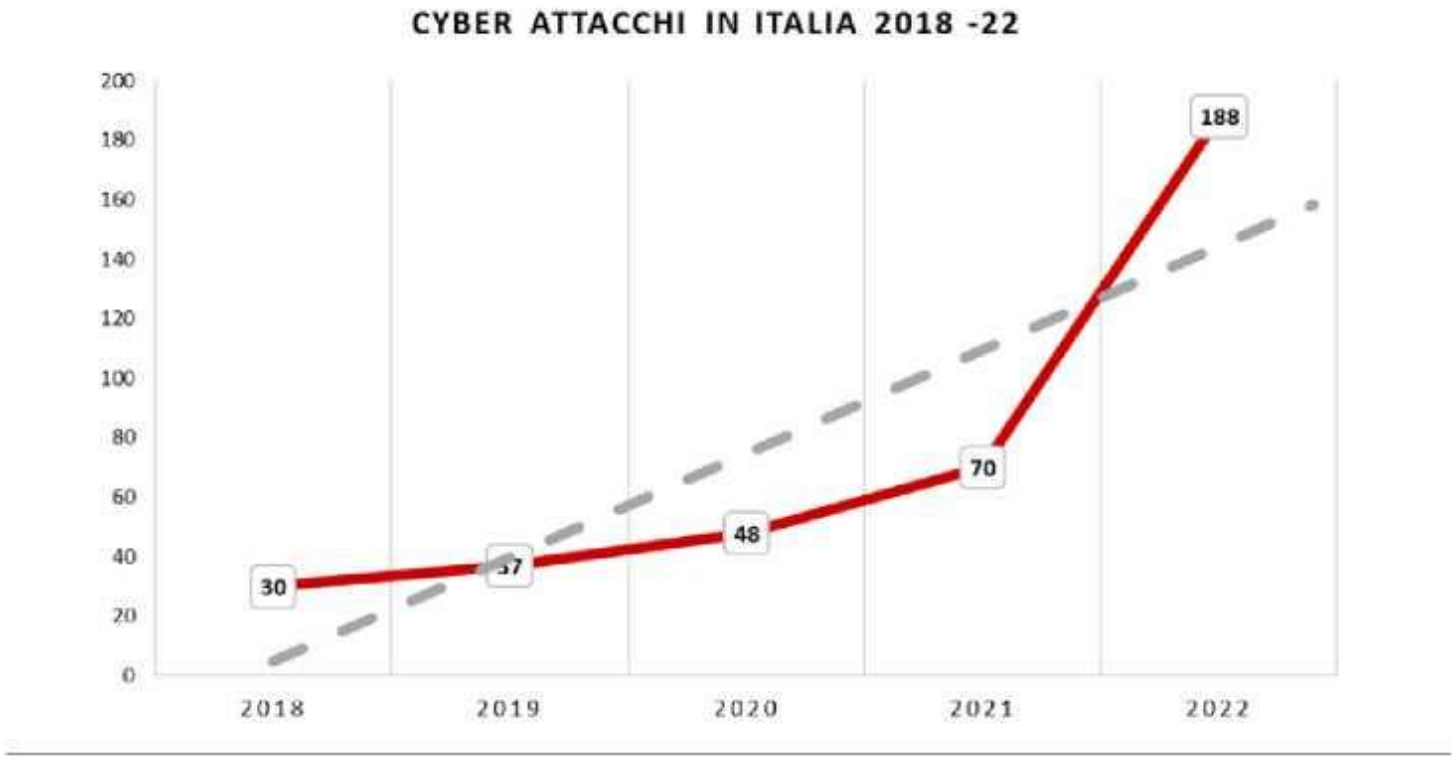
- A tale proposito è necessario approntare un **Cyber Data Incident Response Pack**, in grado di:
- - Gestire l'incident e supportare l'ente nelle attività;
- - Analizzare la natura della violazione;
- - Identificare le evidenze, prove e informazioni tecniche;
- - Determinare la tipologia dei dati compromessi;
- - Stabilire quali dati sono stati compromessi:
- - Formalizzare lo stato delle misure di sicurezza in essere;
- - Predisporre un piano di Remediation.

Cyber Data Incident Response Pack

- Nello specifico il servizio di **Cyber Data Breach Incident Response** permette di essere compliance alla normativa vigente di Data Protection normata nel GDPR. Ma oltre ad avere sempre un piano di "pronta risposta" bisogna anche intervenire giocando sul piano della Cyber Security preventiva, come con attività costanti di vulnerability assessment, penetration testing e Cyber Threat Intelligence per identificare le vulnerabilità e porvi rimedio; formazione e sensibilizzazione dei dipendenti; e sviluppo di policy e procedure in grado di assicurare la massima Cyber Resillience.

Cyber Attacchi Gov 2018-2022





Come è possibile vedere nel grafico , in cui il dato del 2022 supera la linea di tendenza degli ultimi anni, lo scorso anno il numero di incidenti rilevati è cresciuto significativamente, con **un aumento del 527% .**

Media Mensile Gov 2018-2023 primo semestre

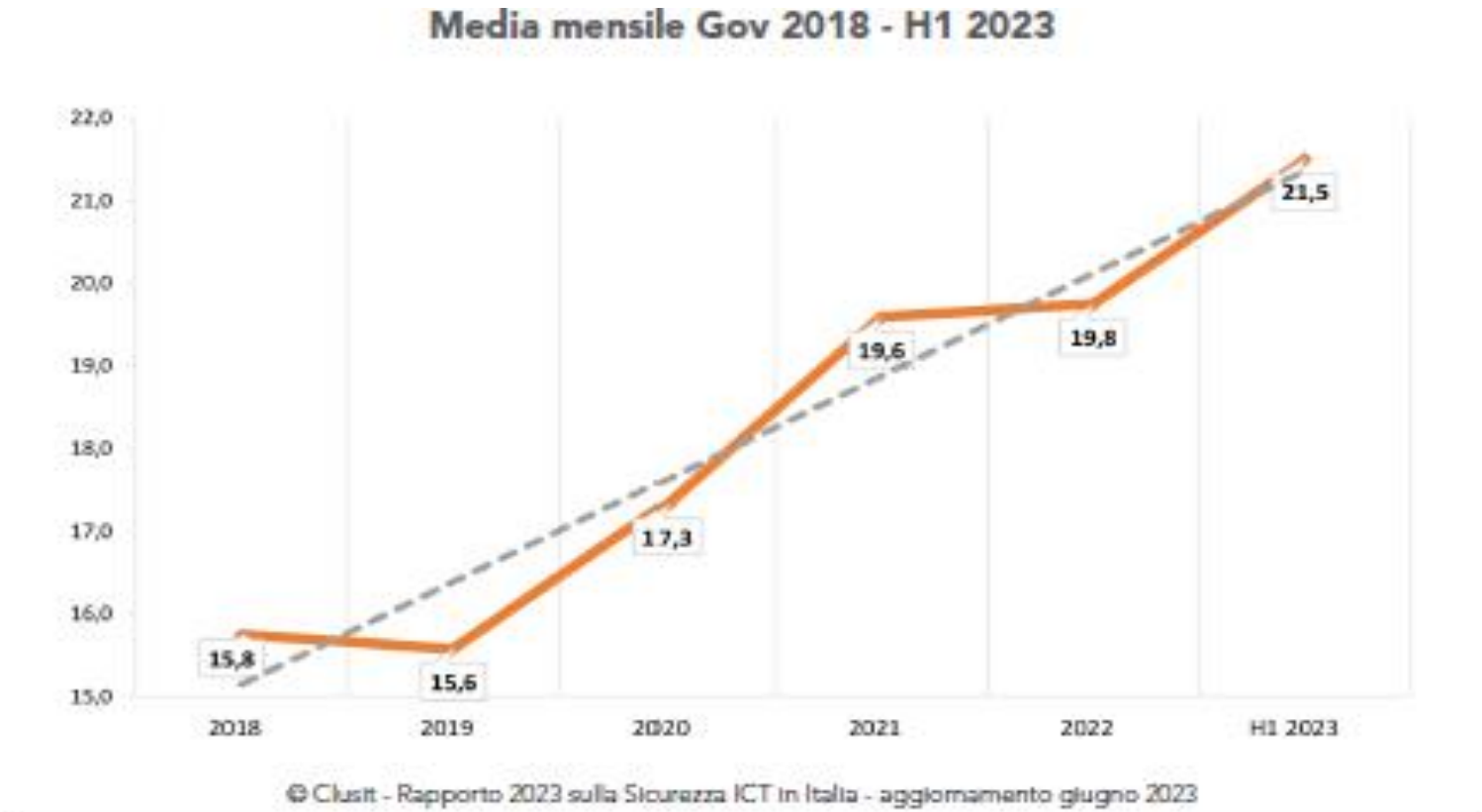


Fig. 32: *Media mensile degli attacchi al settore GOV (CENTRAL/LOCAL) nel periodo 2018- H12023*

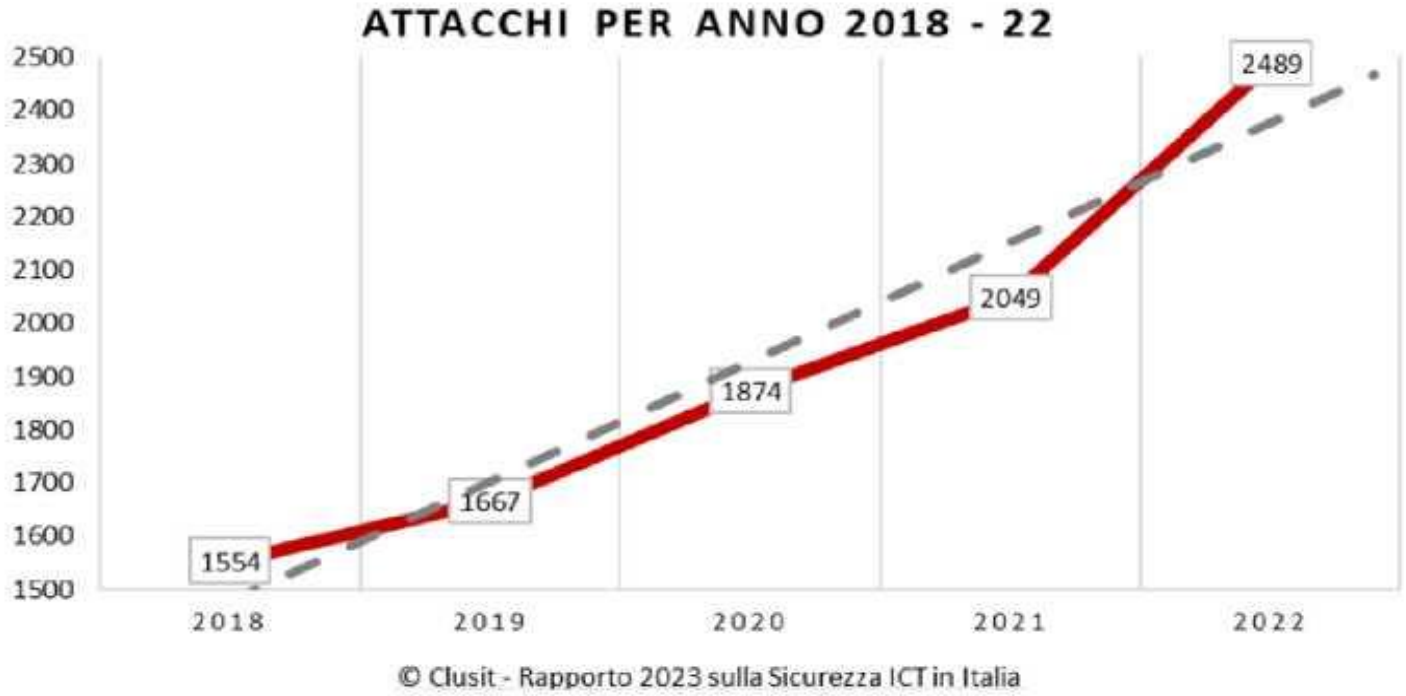
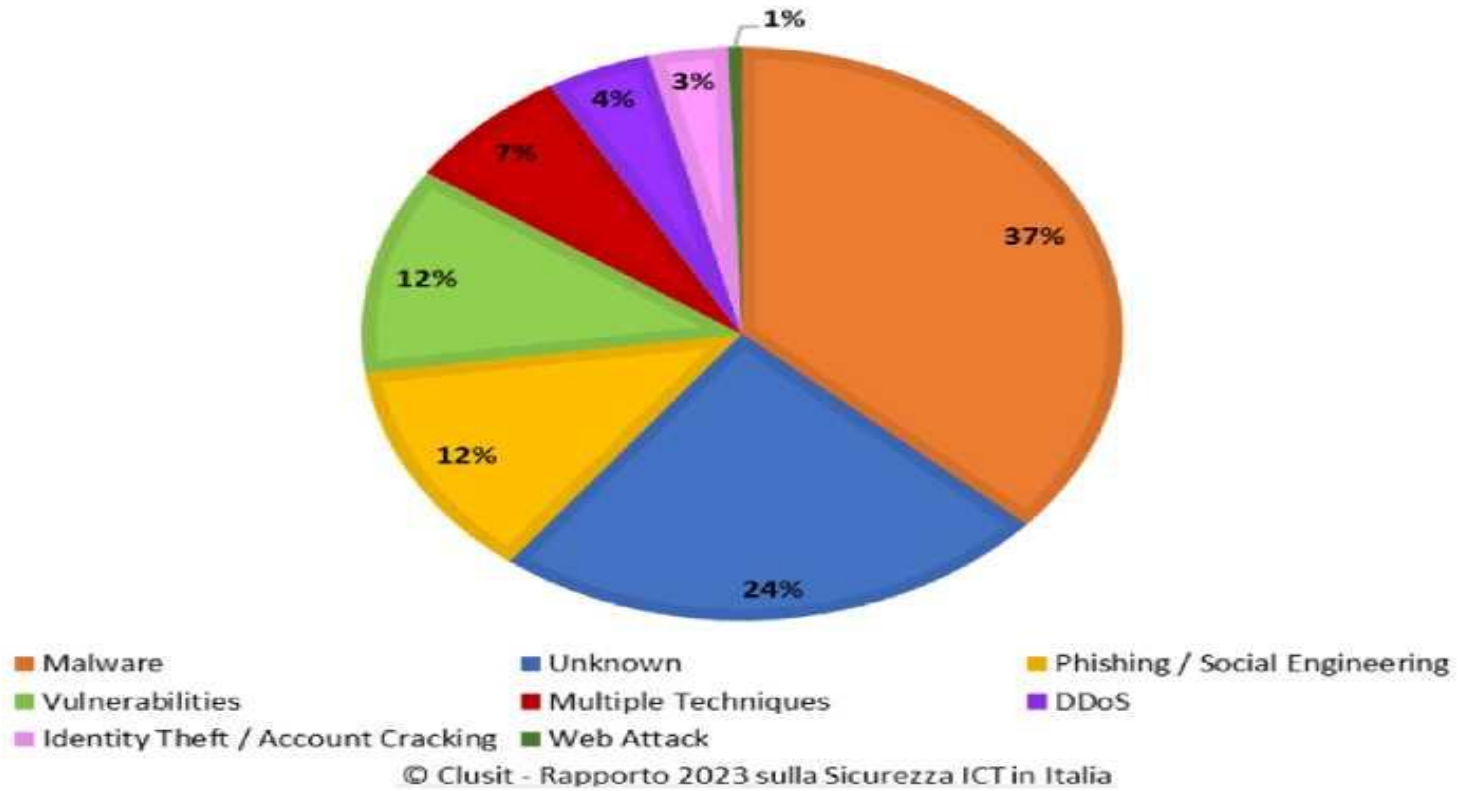


Fig. 1: *Andamento dei cyber attacchi nel periodo 2018 - 22*

DISTRIBUZIONE DELLE TECNICHE 2022



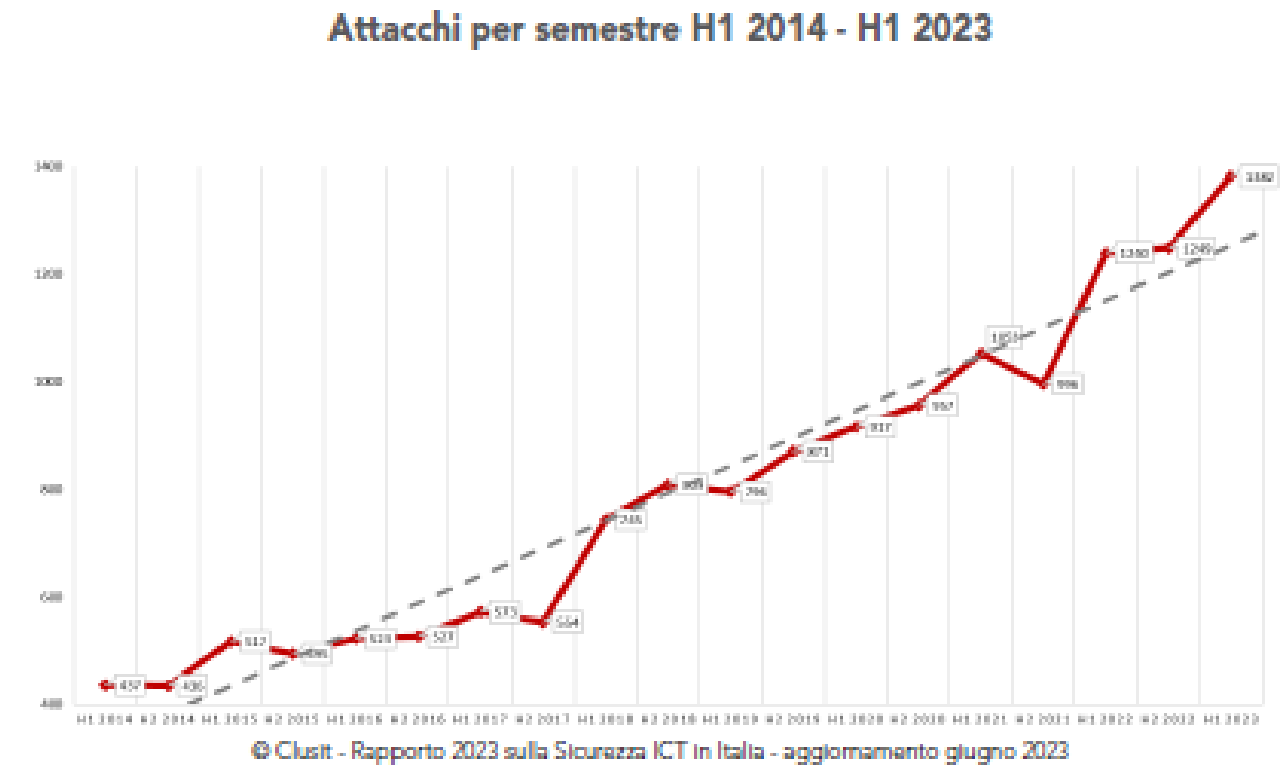


Fig. 1: *Andamento dei cyber attacchi per semestre da H1 2014 a H1 2023*

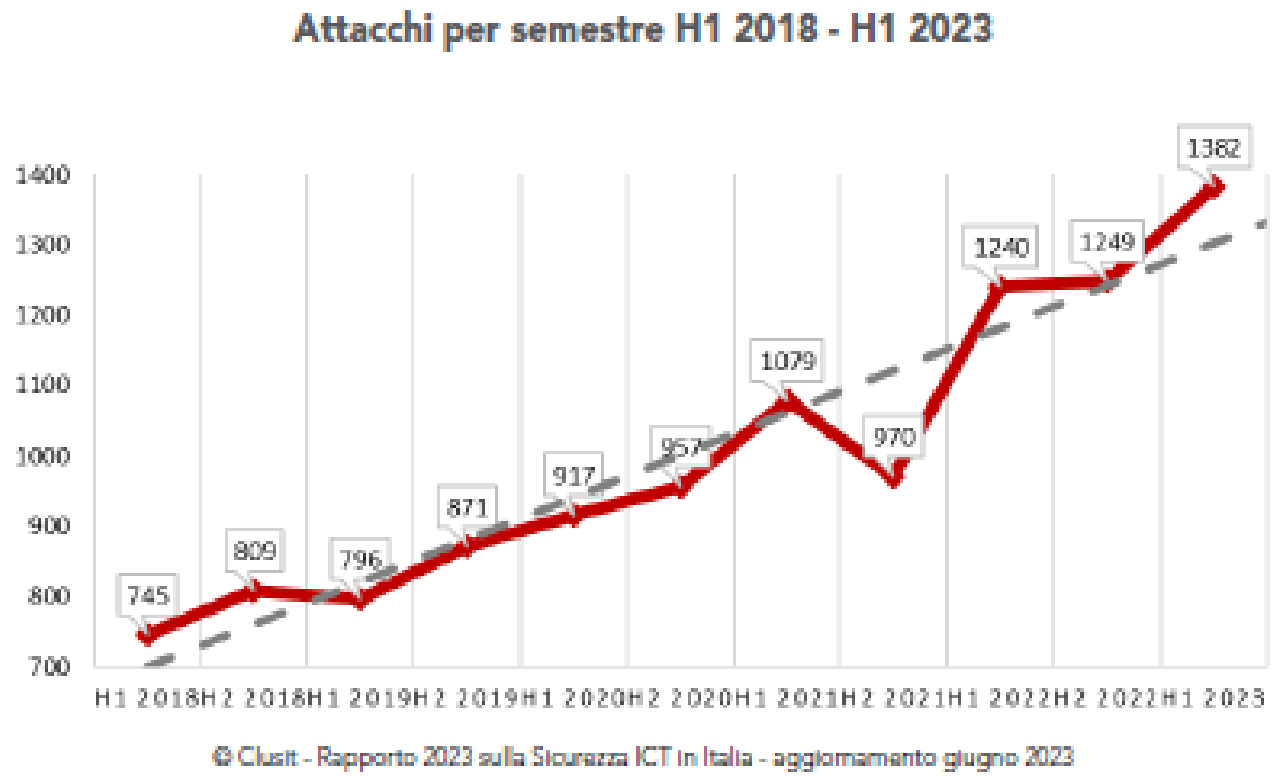


Fig. 2: *Andamento dei cyber attacchi nel periodo 2018 – H1 2023*

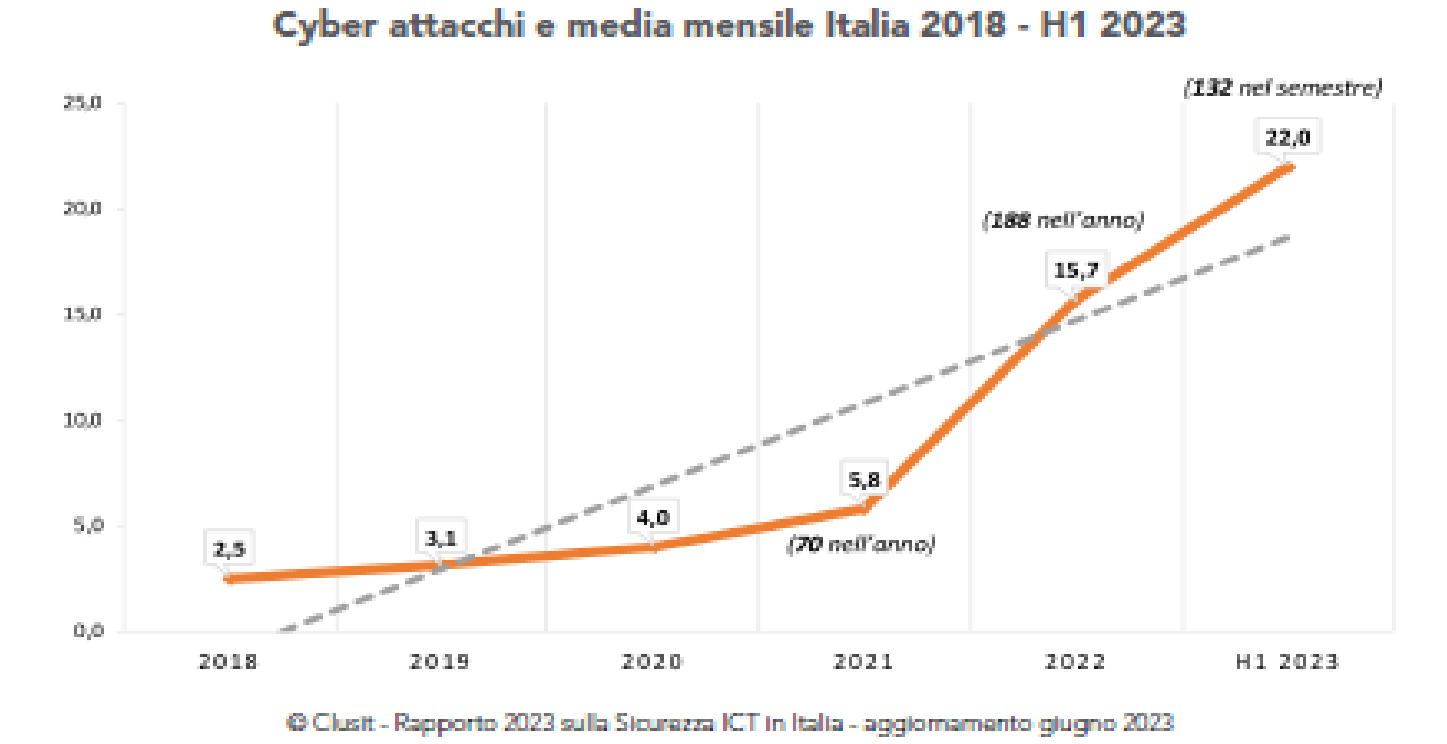


Fig. 21: *Distribuzione dei cyber attacchi e media mensile in Italia nel periodo 2018-H1 2023*

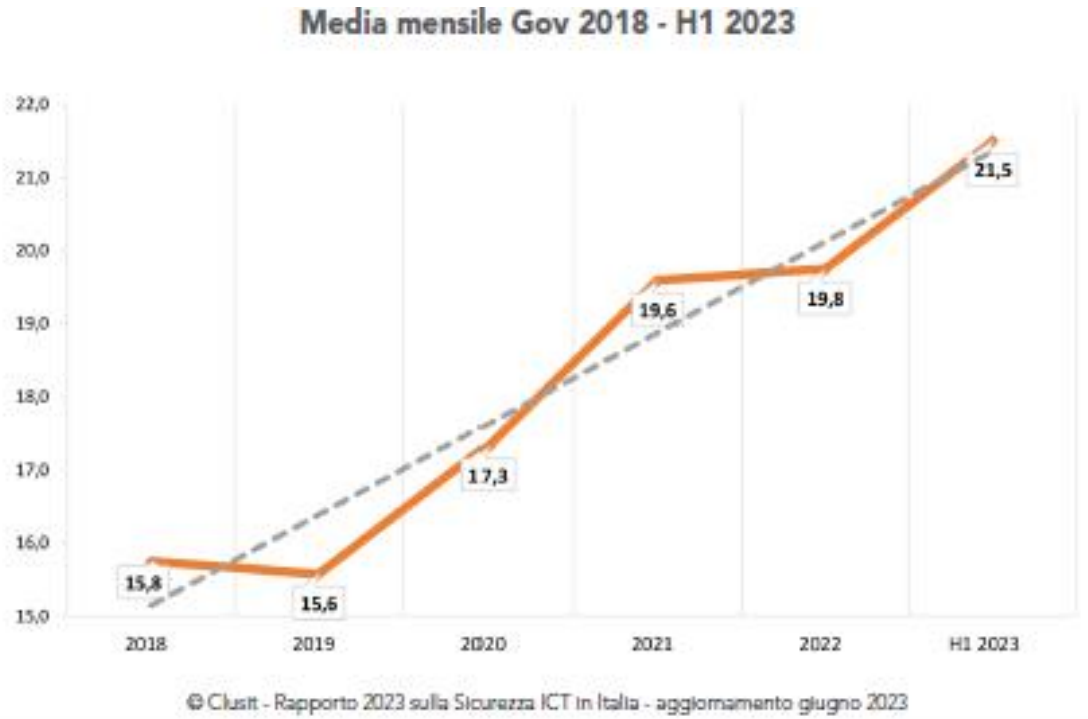
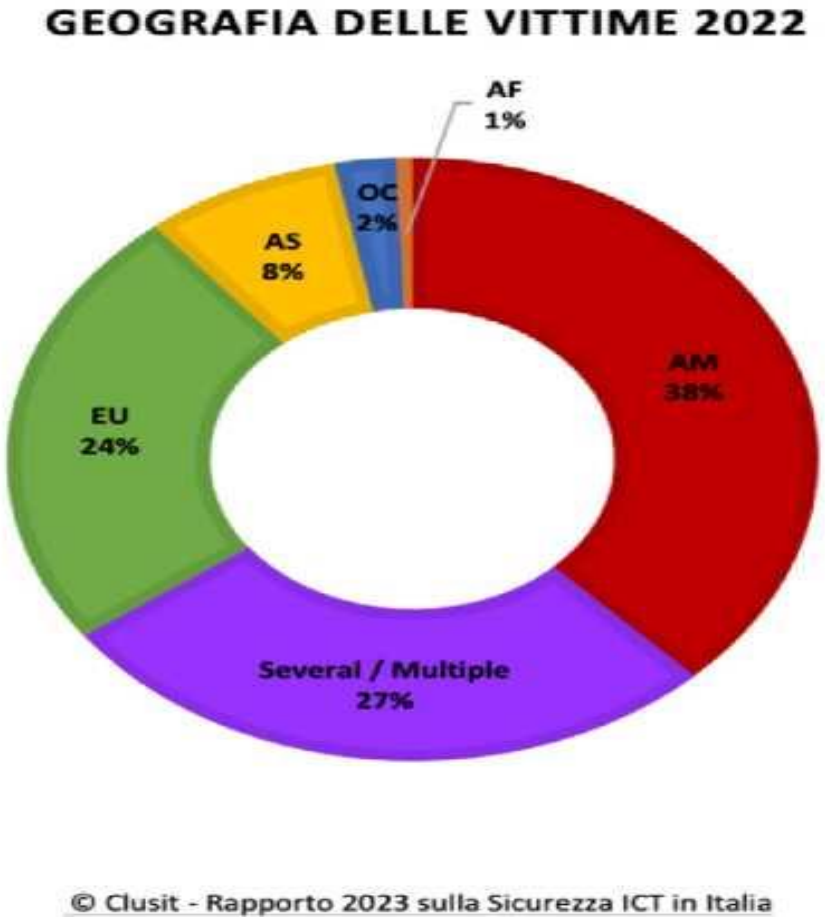
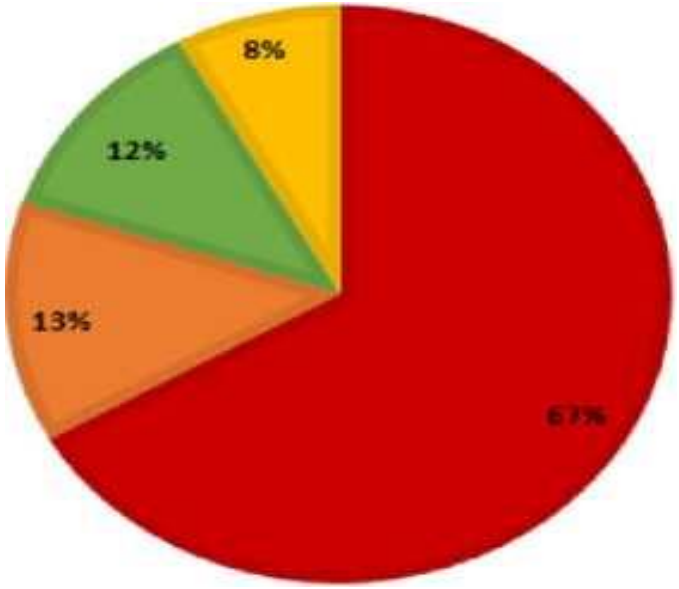


Fig. 32: *Media mensile degli attacchi al settore GOV (CENTRAL/LOCAL) nel periodo 2018- H12023*



Il 64% degli incidenti hanno come causa azioni “maldestre”, degli utenti o del personale ICT



La stragrande maggioranza degli attacchi condotti verso il settore pubblico, ben due terzi, è relativa alla categoria “**Cybercrime**”, con il 67% degli attacchi; seguono, molto distaccati ma quasi a pari merito “**Espionage/Sabotage**” e “**Hacktivism**”, rispettivamente al 13% e 12%, e infine “**Information Warfare**” al 8% ***ANNO 2022 FONTE CLUSIT***

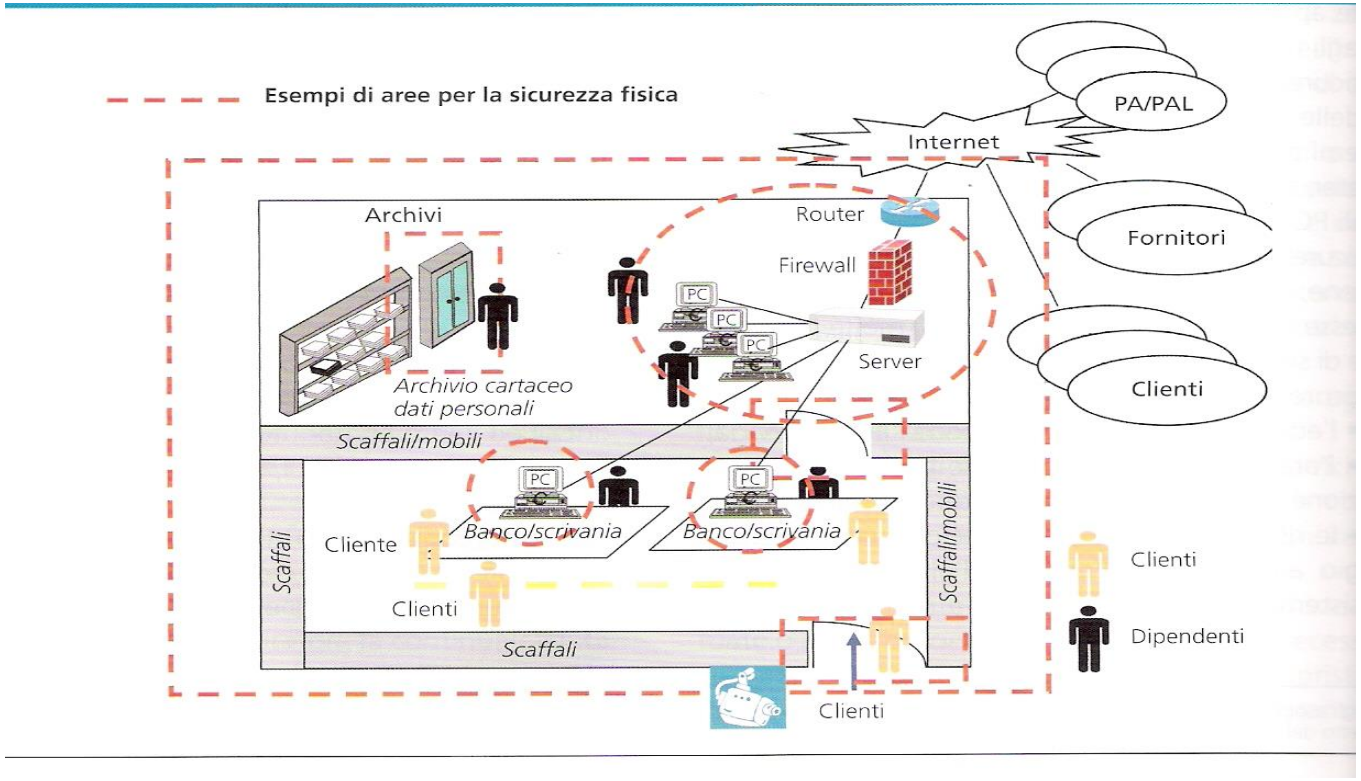
ALCUNI ACCORGIMENTI

- Al fine di prevenire i rischi di un “data breach” è possibile utilizzare le seguenti contromisure
- Trasformare l’utente da anello debole a prima linea di difesa
- Applicare il principio del minimo privilegio per quanto riguarda l’accesso ai dati
- Adottare puntuali politiche di patching dei sistemi
- Crittografare i dati sensibili
- Utilizzare l’autenticazione a due fattori
- Rivolgere grande attenzione anche alla sicurezza fisica

contromisure: sicurezza fisica

- La sicurezza fisica ha il compito di proteggere le aree nelle quali si trovano i dispositivi informatici e di telecomunicazione, e le relative strutture ed impianti (**tale aspetto è definito sicurezza perimetrale**), i componenti hardware all'interno delle aree di cui sopra, le persone che operano nei siti ove si trovano le apparecchiature informatiche, dagli operatori agli utenti finali.

Un esempio


Esempi di aree per la sicurezza fisica
PA/PAL
Internet
Fornitori
Clienti
Archivi
Router
Firewall
PC
PC
PC
Server
Archivio cartaceo
dati personali
Scaffali/mobili
PC
PC
Scaffali
Cliente
Banco/scrivania
Banco/scrivania
Scaffali/mobili
Clienti
Scaffali
Clienti
Clienti
Dipendenti

le misure di sicurezza fisica

- Il controllo perimetrale dell'edificio e di particolari zone all'interno o all'esterno dello stesso (parcheggi, cortili, ecc,);
- Controllo degli accessi fisici delle persone all'interno dell'edificio o di determinati locali da proteggere quali il ced;
- Il controllo e la prevenzione di mancanza di energia elettrica;
- Il controllo e la prevenzione di emissioni elettromagnetiche;
- Il controllo e la prevenzione antincendio, antifumo ed antigas;

sicurezza perimetrale

- La sicurezza perimetrale ha come misure di prevenzione i sistemi di sicurezza passiva quali sistemi di recinzione antiscavalcamento, ed attiva, quali sistemi di allarme perimetrali a micro-onde, monitoraggio TV a circuito chiuso o con altre tecnologie.

sicurezza logica

- La sicurezza logica prevede le seguenti contromisure: identificazione dell'interlocutore, autenticazione dell'interlocutore, autorizzazione ad accedere ed operare sulla risorsa richiesta in funzione dei diritti (**in inglese chiamati access rights**) che sono stai rilasciati al richiedente e preventivamente inseriti nei sistemi da un gestore delle risorse e/o della sicurezza.

modalità di accesso alle banche dati anagrafiche: l'identificazione

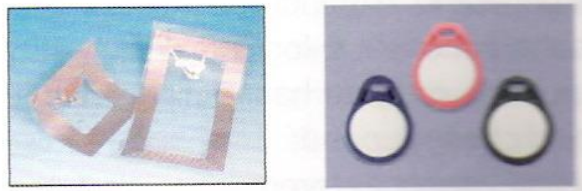
- L'identificazione di un interlocutore:
- La forma più comune per identificarsi è l'inserimento di credenziali di autenticazione. Tale meccanismo di identificazione (user e pwd) è debole e dipende dalla frequenza di cambio della pwd, dalla sua casualità e dalla sua lunghezza;
- Altre forme di prevenzione sono la cd, pwd monouso (one-time pwd) che sono create ed usate per ogni singola interazione tra la persona e l'applicazione, e non possono più essere utilizzate altre volte;
- Altra forma è il **token** che si basa sull'identificazione a due o più fattori: tipicamente l'utente deve possedere un oggetto chiamato token, riconoscibile dal pc oltre al proprio user-id e pwd;
- Es. di **token** (**carta con banda magnetica, smart card con processore con relativo lettore, chiavetta usb contenente i certificati digitali, generatore di pwd monouso, Tag RFID .**

Esempi di token

Smart card

Chiavetta USB

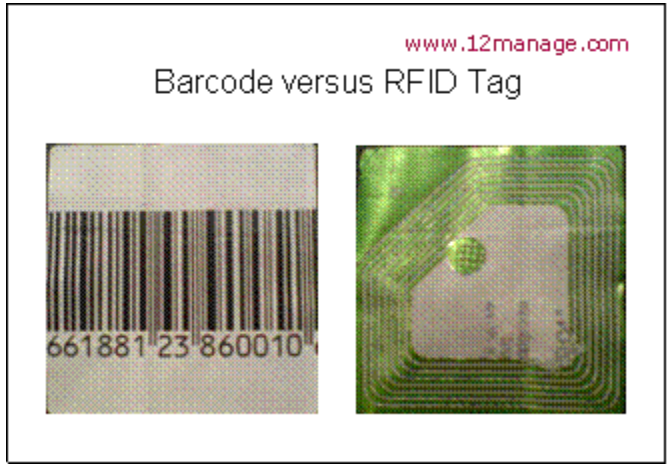
Generatore di codici casuali



Esempi di tag passivi RFID

RFID (Radio Frequency Identification)

- RFID (**Radio Frequency IDentification** o **Identificazione a radio frequenza**) è una tecnologia per la identificazione automatica di oggetti, animali o persone (AIDC Automatic Identifing and Data Capture) basata sulla capacità di memorizzare e accedere a distanza a tali dati usando dispositivi elettronici (chiamati TAG o transponder) che sono in grado di rispondere comunicando le informazioni in essi contenute quando "interrogati".
- **Tale tecnologia si basa su un transponder, chiamato anche tag, un ricetrasmettitore che invia un segnale radio in risposta ad un comando ricevuto da una stazione remota**)



autenticazione

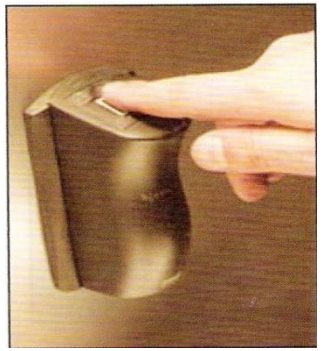
- I moderni sistemi tendono ad utilizzare logiche di autenticazione a due o più fattori richiedono cioè di presentare due (oggi sono 4) o più forme di identificazione per ottenere l'accesso, **tipicamente user-id e pwd associate ad un token**.

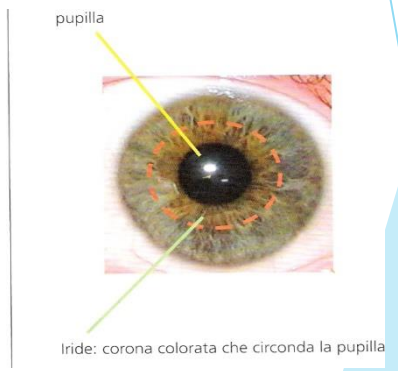
la biometria

- Per biometria, dal greco bios (vita) e metros (misura), si intende l'identificazione automatica o la verifica dell'identità di un soggetto sulla base di caratteristiche fisiche e/o comportamentali. Quando parliamo di chiavi biometriche ci riferiamo all'uso delle impronte digitali, l'impronta dell'iride, l'impronta del dna, l'impronta della pelle etc. **Da un lato si ha la necessità che mi devo identificare dall'altro che mi devo autenticare.**
- **Ad esempio l'utilizzo delle impronte digitali per entrare nell'area sicura di un qualunque CED ministeriale, in questo caso viene confrontata l'impronta con un set di impronte precedentemente dichiarate. Quindi in sostanza si passa ad effettuare un'associazione di un'identità a dei dati ed a verificare un'identità precedentemente dichiarata.**
- Un altro tema è quello dell'uso delle firme scritte come strumento di autenticazione.

tecniche biometriche

l'identificazione biometrica

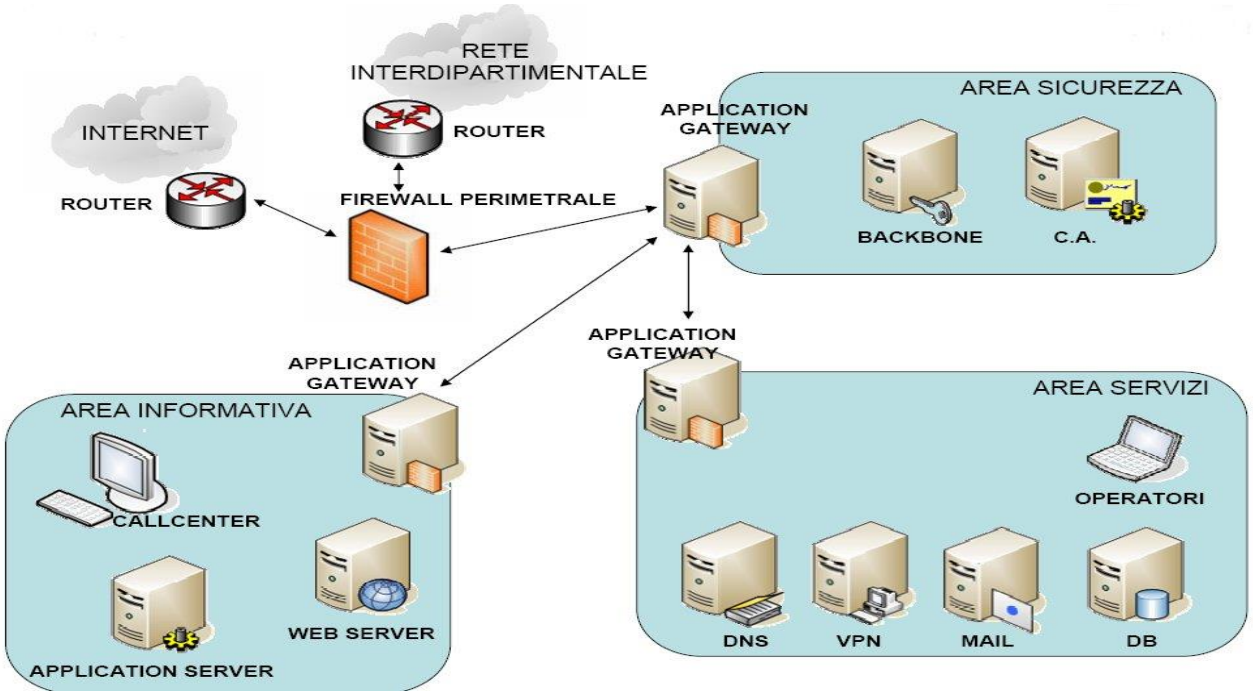




modalità di accesso

- Accesso profilato mediante credenziali di autenticazione (username e password);
- Si può anche utilizzare la procedura di login disponibile sul sistema operativo della postazione di lavoro connessa in rete;
- Disattivazione dell'account in caso di prolungata assenza o fuoriuscita dall'organizzazione;
- Utilizzo di modalità sostitutive in caso di assenza del dipendente (ad es. invio automatico di messaggi di posta elettronica ad un altro recapito.

un esempio concreto



Linee guida nella navigazione web sicura ed in compliance per il dipendente pubblico

E’ opportuno che l’ente locale al fine di evitare potenziali attacchi ai server del proprio portale istituzionale e/o alle proprie banche dati di approvare con apposito atto deliberativo uno schema di linee guida da adottare da parte del dipendente pubblico nella navigazione web sicura ed in compliance. Nello specifico si dovranno adottare le seguenti azioni precauzioni:

- - **non scaricare programmi sconosciuti** - Non scaricare mai programmi sconosciuti da internet prima di averne accertato la provenienza
- **aggiornamento del software dai siti dei produttori** - Scaricare gli aggiornamenti di software e driver esclusivamente dalla pagina web dei relativi produttori. È sempre buona norma anche verificarli successivamente con un programma antivirus aggiornato

Linee guida nella navigazione web sicura ed in compliance per il dipendente pubblico

- **prudenza nella trasmissione di informazioni** - Non comunicare mai a nessuno le proprie credenziali di accesso (nome di Nessun fornitore di servizi serio chiederà la vostra password (nemmeno telefonicamente). Questo vale anche quando la richiesta appare credibile. Tale garanzia è riconoscibile da un lucchetto dorato che appare all'interno del browser oppure dal protocollo utilizzato (tipicamente "https" invece di "http")
- **chiudere le applicazioni** - Utilizzare sempre l'apposita notifica di chiusura ("logout") quando si esce da un'applicazione web che abbia richiesto l'introduzione delle proprie credenziali di accesso
- **riservatezza nella divulgazione delle informazioni personali** - Evitate di rivelare dati personali durante la compilazione di moduli Web o la fornitura di contributi a newsgroup, forum o registri di visitatori

Linee guida nella navigazione web sicura ed in compliance per il dipendente pubblico

- **attenzione alla configurazione del browser** Molte delle minacce che si incontrano durante la navigazione in internet sono legate all'utilizzo dei componenti "dinamici" delle pagine web tipicamente realizzati tramite controlli ActiveX o funzioni JavaScript

Sensibilizzare il personale dell'ente sui rischi che la navigazione in Internet via Browser comporta

- Di seguito le principali norme comportamentali da seguire:
- Non fare clic su collegamenti senza considerare i rischi che ne potrebbero derivare (evitare di cliccare su link sospetti presenti nelle pagine).
- Prestare attenzione al fatto che gli indirizzi di pagine Web potrebbero essere mascherati e portare in un sito imprevisto.
- Considerare che ogni volta che un sito web richiede che vengano abilitate determinate funzionalità o installati software e aggiornamenti, si mette a rischio il computer. Ad es. non aggiornare mail il Flash Player su richiesta di una pagina web ma solo da pannello di controllo.

Linee guida nella navigazione web sicura ed in compliance per il dipendente pubblico

- **Non riutilizzare la stessa password per siti diversi**.
- **Non fornire mai online informazioni personali** a meno di non essere certi che il sito sia valido e le transazioni sicure: prima di inserire qualsiasi informazione personale, controllare la barra degli URL del browser al fine di accertarsi che il sito sia quello atteso e che sia presente la dicitura "https:" e un'icona a forma di lucchetto ad indicare che la connessione al sito è protetta e che il certificato server è valido.
- **Evitare Wi-Fi pubblici o gratuiti**: l'attaccante spesso utilizza sniffers wireless per rubare le informazioni degli utenti quando vengono inviate su reti non protette. Il modo migliore per proteggersi da questo attacco è evitare di utilizzare queste reti, oppure utilizzarle solo con una VPN che incapsuli tutto il traffico in un tunnel cifrato.
- In caso di individuazione di una “falsa” pagina di autenticazione segnalarla tempestivamente all’Assistenza Tecnica dell’Ente in sinergia con l’Ufficio CED Sistemi Informativi dell’ente locale per procedere all'oscuramento della medesima e possibilmente all'individuazione dei responsabili.

Tecniche di pseudonomizzazione ed anonimizzazione di data set pubblici

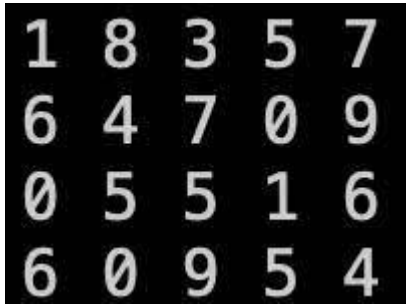
- L'ente locale al fine di garantire su tutte le tipologie di dati trattati i principi di accountability, compliance, privacy by default e privacy by design previsti dal vigente Regolamento UE 679/2016 (GDPR)deve utilizzare delle tecniche di pseudonomizzazione nei dataset dell'ente locale cosi dettagliate:
  - **TERZE PARTI COME ENTITÀ DI PSEUDONIMIZZAZIONE** - In questo scenario, la pseudonimizzazione viene eseguita da una terza parte (non dal responsabile del trattamento), che va poi a inoltrare i dati al titolare del trattamento

Tecniche di pseudonomizzazione ed anonimizzazione di data set pubblici

- **TECNICHE DI PSEUDONIMIZZAZIONE** ad oggi più comuni.
- **A) PSEUDONIMIZZAZIONE DI UN SINGOLO IDENTIFICATORE** - Partendo dalla pseudonimizzazione di un singolo identificativo, vengono di seguito elencati alcuni possibili approcci, con relativi vantaggi e limiti. Il **contatore** è la più semplice forma di pseudonimizzazione. Gli identificativi sono sostituiti da un numero scelto da un contatore monotono. I vantaggi del contatore derivano dalla sua semplicità, che lo rende un buon candidato per set di dati non complessi e di piccole dimensioni**. In termini di protezione dei dati, il contatore fornisce pseudonimi che non sono associabili agli identificativi iniziali (sebbene il carattere sequenziale del contatore possa comunque fornire informazioni sull'ordine dei dati all'interno di un set).**

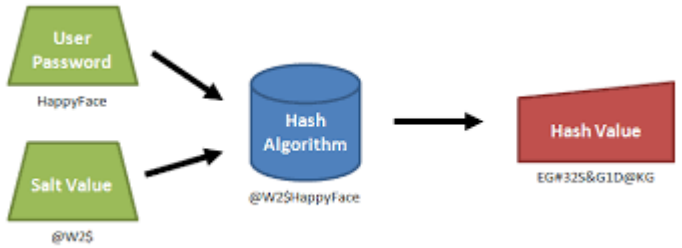
Tecniche di pseudonomizzazione ed anonimizzazione di data set pubblici

- **TECNICHE DI PSEUDONIMIZZAZIONE** ad oggi più comuni.
- **B) Generatore di numeri casuali** Il generatore di numeri casuali è un meccanismo che produce, all'interno di un set, valori che presentano tutti la stessa probabilità di essere selezionati, risultando pertanto imprevedibili **Il generatore di numeri casuali fornisce una solida protezione dei dati (poiché, a differenza del contatore, per creare ogni pseudonimo si va a utilizzare un numero casuale, rendendo difficile l'estrazione di informazioni riguardanti l'identificativo iniziale, a meno che la tabella di mappatura non sia stata compromessa).**



Tecniche di pseudonomizzazione ed anonimizzazione di data set pubblici

- **TECNICHE DI PSEUDONIMIZZAZIONE** ad oggi più comuni.
- **C) Funzione crittografica di hash-** Una funzione crittografica di hash prende stringhe di input di lunghezza arbitraria e le associa ad output di lunghezza fissa . Essa presenta le proprietà riportate di seguito:
  - 1) **Unidirezionale**: è computazionalmente impraticabile trovare input che si associno a output specificati in precedenza.
  - 2) **Senza collisioni**: è computazionalmente impraticabile trovare due input distinti che si associno al medesimo output. Si applica una funzione crittografica di hash direttamente all'identificativo, così da ottenere lo pseudonimo corrispondente.



Tecniche di pseudonomizzazione ed anonimizzazione di data set pubblici

- **TECNICHE DI PSEUDONIMIZZAZIONE** ad oggi più comuni.
- **D) Codice di autenticazione del messaggio -** Questa primitiva può essere considerata come una funzione di hash con chiave. Se non si è a conoscenza di tale chiave, non è possibile associare gli identificativi agli pseudonimi. HMAC è di gran lunga la più diffusa modalità di codice di autenticazione del messaggio impiegata nei protocolli Internet. **Il Codice di autenticazione del messaggio è generalmente considerato una tecnica di pseudonimizzazione solida dal punto di vista della protezione dei dati poiché, a meno che la chiave non sia stata compromessa, è impossibile decodificare lo pseudonimo**.
- **E) Crittografia-** la crittografia simmetrica (deterministica) e, in particolare, le cifrature a blocchi come l'AES, insieme alle loro modalità operative. Si utilizza una cifratura a blocchi per crittografare un identificativo servendosi di una chiave segreta, che è sia chiave di pseudonimizzazione sia la chiave da impiegare per il recupero. L'uso di cifrature a blocchi ai fini della pseudonimizzazione deve misurarsi con la dimensione del blocco. Gli identificativi possono avere dimensioni minori o maggiori rispetto alla dimensione del blocco di input della cifratura a blocchi.

Tecniche di pseudonomizzazione ed anonimizzazione di data set pubblici

- **E' necessario stabilire delle strategie di pseudonomizzazione che possono essere: a) pseudonimizzazione deterministica, b) randomizzata al documento e c) completamente randomizzata**.
- **Pseudonimizzazione deterministica**. In tutti i database e ogniqualvolta appare, ID viene sempre sostituito con lo stesso pseudonimo. Esso è uniforme all'interno di un database e tra database differenti. Per implementare tale modalità, occorre anzitutto estrarre l'elenco degli identificativi univoci contenuti nel database. In secondo luogo, l'elenco viene associato agli pseudonimi e gli identificativi sono infine sostituiti agli pseudonimi nel database.
- **Pseudonimizzazione randomizzata al documento**. Ogniqualvolta ID appare in un database, viene sostituito con un differente pseudonimo e così via).
- **Pseudonimizzazione completamente randomizzata**. Infine, per ogni occorrenza di ID all'interno di un database A o B, ID viene sostituito con uno pseudonimo differente.

Linee guida per l'utilizzo dello smart working in modalità sicura

- Tutto ciò ora risulta essere disciplinato alla luce delle nuove disposizioni normative introdotte dalla Legge 11 settembre 2020 n° 120 che ha modificato l'articolo 12 del CAD sullo smart working che cosi prevede:
- Art. 12. Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa
- …..3-bis. I soggetti di cui all'articolo 2, comma 2, favoriscono l'uso da parte dei lavoratori di dispositivi elettronici personali o, se di proprietà dei predetti soggetti, personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo. In caso di uso di dispositivi elettronici personali, i soggetti di cui all'articolo 2, comma 2, nel rispetto della disciplina in materia di trattamento dei dati personali, adottano ogni misura atta a garantire la sicurezza e la protezione delle informazioni e dei dati, tenendo conto delle migliori pratiche e degli standard nazionali, europei e internazionali per la protezione delle proprie reti, nonché ((a condizione che sia data al lavoratore adeguata informazione)) sull'uso sicuro dei dispositivi, **anche attraverso la diffusione di apposite linee guida**, e disciplinando, tra l'altro l'uso di webcam e microfoni((previa informazione alle organizzazioni sindacali.))

Linee guida per l’utilizzo dello smart working in modalità sicura

- 3-ter. Al fine di agevolare la diffusione del lavoro agile quale modalità di esecuzione del rapporto di lavoro subordinato, i soggetti di cui all'articolo 2, comma 2, lettera a), acquistano beni e progettano e sviluppano i sistemi informativi e i servizi informatici con modalità idonee a consentire ai lavoratori di accedere da remoto ad applicativi, dati e informazioni necessari allo svolgimento della prestazione lavorativa, nel rispetto della legge 20 maggio 1970, n. 300, del decreto legislativo 9 aprile 2008, n. 81 e della legge 22 maggio 2017, n. 81, assicurando un adeguato livello di sicurezza informatica, in linea con le migliori pratiche e gli standard nazionali ed internazionali per la protezione delle proprie reti, nonché' ((a condizione che sia data al lavoratore adeguata informazione)) sull'uso sicuro degli strumenti impiegati, con particolare riguardo a quelli erogati tramite fornitori di servizi in cloud, anche attraverso la diffusione di apposite linee guida, e disciplinando anche la tipologia di attività che possono essere svolte((previa informazione alle organizzazioni sindacali.))

Linee guida per l'utilizzo dello smart working in modalità sicura

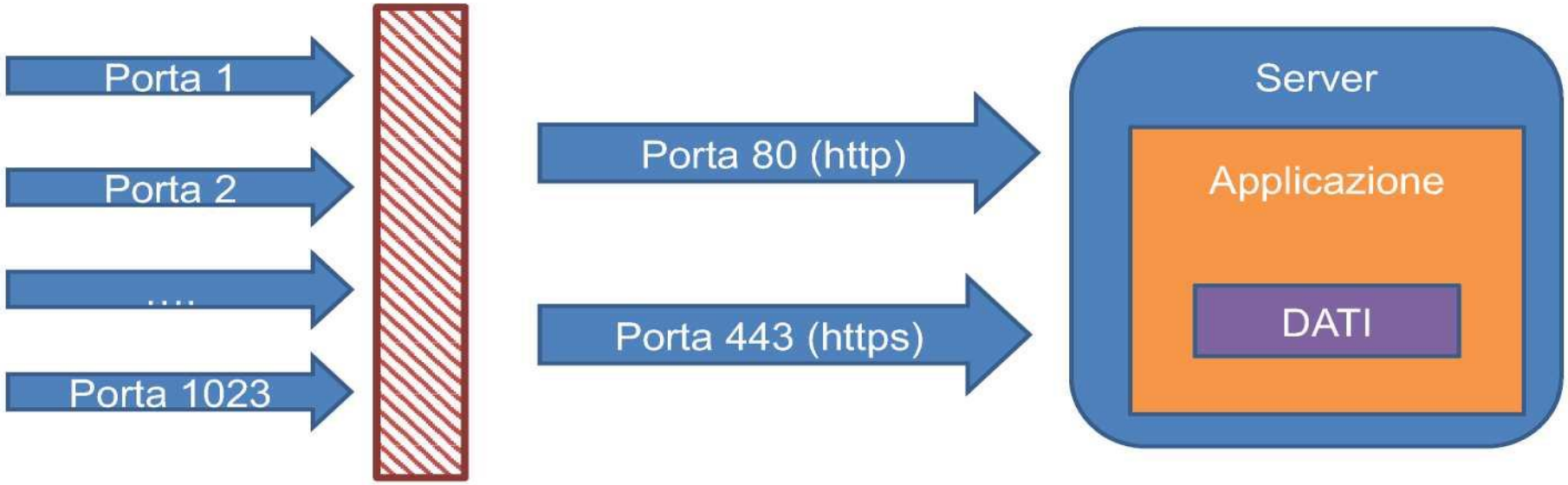
- **LE RACCOMANDAZIONI PER IL LAVORO DA REMOTO**
- Uso consapevole e sicuro dei dispositivi e degli strumenti da parte dei dipendenti
- Accesso sicuro alla rete dell'organizzazione
- Adeguata sicurezza dei dispositivi
- Adeguata sicurezza della rete
- Adeguata sicurezza del Cloud
- Navigazione web in modalità sicura
- Continuità operativa e risposta agli incidenti

Lo sviluppo software sicuro secondo quanto previsto da AGID

Le linee guida per lo sviluppo del software sicuro nella pubblica amministrazione si inseriscono nel contesto delle linee guida per la sicurezza ICT delle Pubbliche amministrazioni, aventi lo scopo di fornire indicazioni sulle misure da adottare in ciascuna componente della Mappa del Modello strategico del Piano Triennale AGID

- L'obiettivo è quello di pervenire a un'architettura della sicurezza per servizi sia critici che non critici, che definisca i principi e le linee guida del modello architetturale di gestione dei servizi e contestualizzazione rispetto al cluster dei dati gestiti. La sicurezza informatica ha un'importanza fondamentale in quanto oltre ad essere fondamentale per garantire disponibilità, integrità e riservatezza delle informazioni proprie del Sistema informativo della Pubblica amministrazione, è direttamente collegata ai principi di privacy previsti dall'ordinamento giuridico

Lo sviluppo software sicuro secondo quanto previsto da AGID



Lo sviluppo software sicuro secondo quanto previsto da AGID

Secure Software Development Life Cycle (SSDLC)

L’adozione di un Secure Software Development Life Cycle (SSDLC) atto a considerare ed implementare opportune attività di sicurezza nel corso di tutte le sue fasi del ciclo di vita del SW, dalla analisi alla progettazione, sviluppo, test fino alla manutenzione è una necessità inderogabile per rispondere alla domanda di sicurezza e per ridurre i costi che comporta trascurarla.

Lo sviluppo software sicuro secondo quanto previsto da AGID

Secure by Design

Definisce un software progettato per essere sicuro e capace di garantire riservatezza, integrità e disponibilità.

- Alcuni principi del Secure by Design:
- Ridurre al minimo la superficie d'attacco
- Stabilire valori prede finiti sicuri
- Non affidarsi ai servizi di terze parti
- Separare i ruoli
- Segmentare l’infrastruttura di rete
- Ridurre i single point of failure

Il referente per la cybersicurezza

Quali sono i compiti del referente?
La struttura e il referente devono provvedere allo sviluppo delle politiche di sicurezza informatica; alla produzione e all' aggiornamento di sistemi di analisi preventiva e di un piano per la gestione del rischio; alla produzione e all' aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture; alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici; all' attuazione delle misure previste dalle linee guida ACN.

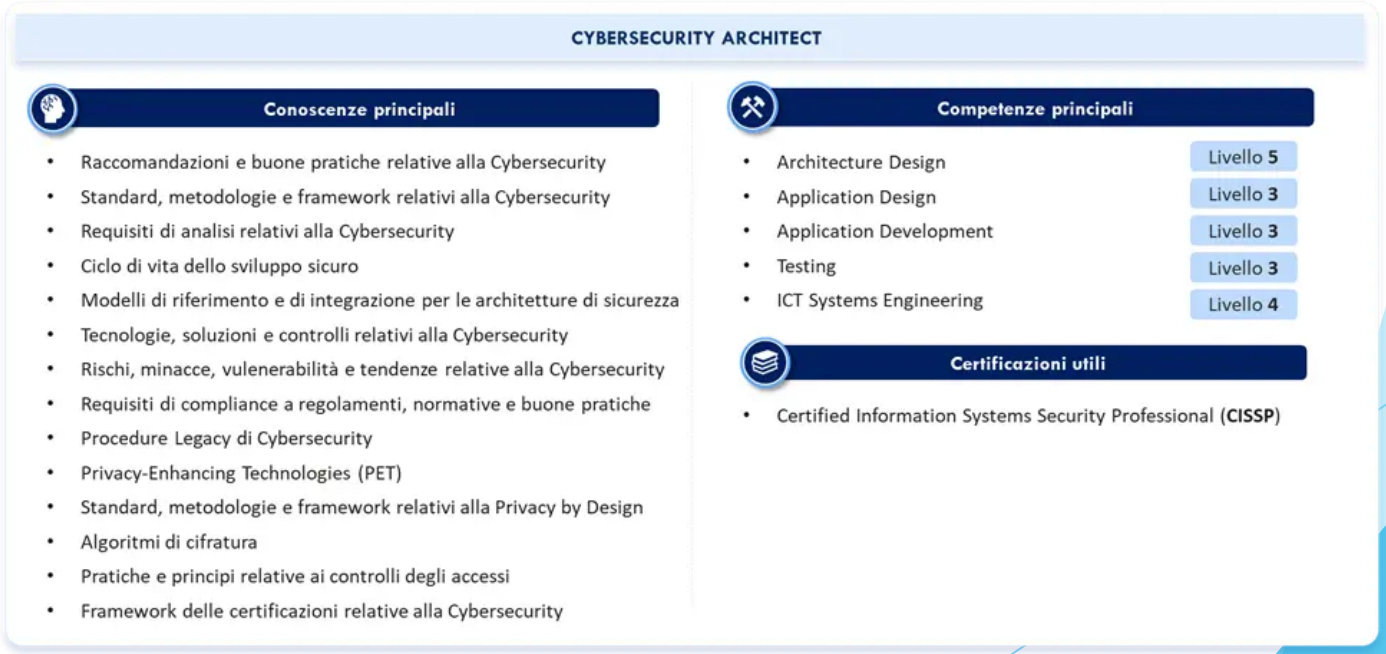
I criteri di cybersecurity

Art. 14. Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e disposizioni di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133

Comma 1…. sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, **gli elementi essenziali di cybersicurezza** che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici nonché i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi individuati con il decreto di cui al presente comma tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione. **Ai fini del presente articolo, si intende per «elementi essenziali di cybersicurezza» l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo**.

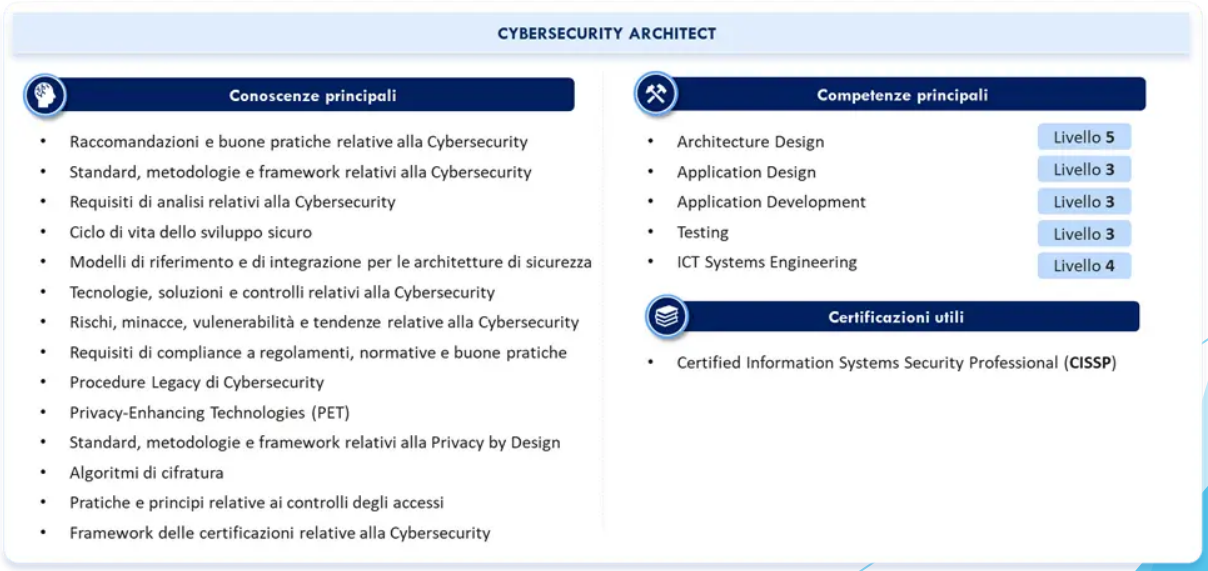
I criteri di cybersecurity

La Legge sulla Cybersicurezza inoltre introduce nella disciplina dei **contratti pubblici di beni e servizi informatici** alcuni **criteri di cybersecurity**, definiti dal legislatore come l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela degli interessi nazionali strategici. Tali **elementi essenziali di cybersicurezza** saranno individuati da uno specifico Decreto del Presidente del Consiglio dei Ministri da **emanarsi entro 120 giorni** dall'entrata in vigore della Legge sulla Cybersicurezza. Tale Decreto del Presidente del Consiglio dei Ministri, peraltro, provvederà anche a dettagliare i casi in cui, per la tutela della sicurezza nazionale, debbano essere previsti **criteri di premialità per le proposte o le offerte che contemplino l'uso di tecnologie di cybersicurezzaitaliane** o di Paesi appartenenti all'**Unione europea** o di Paesi aderenti all'Alleanza atlantica (**NATO**) o di **Paesi terzi** –individuati nel medesimo decreto – tra quelli che hanno **accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.**



I criteri di cybersecurity

2. Nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza:
a) possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1;
b) tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione;
c) nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del codice di cui al decreto legislativo n. 36 del 2023, inseriscono gli elementi di cybersicurezza di cui al comma 1 del presente articolo tra i requisiti minimi dell'offerta;
d) nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'articolo 108, comma 4, del codice di cui al decreto legislativo n. 36 del 2023, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento;

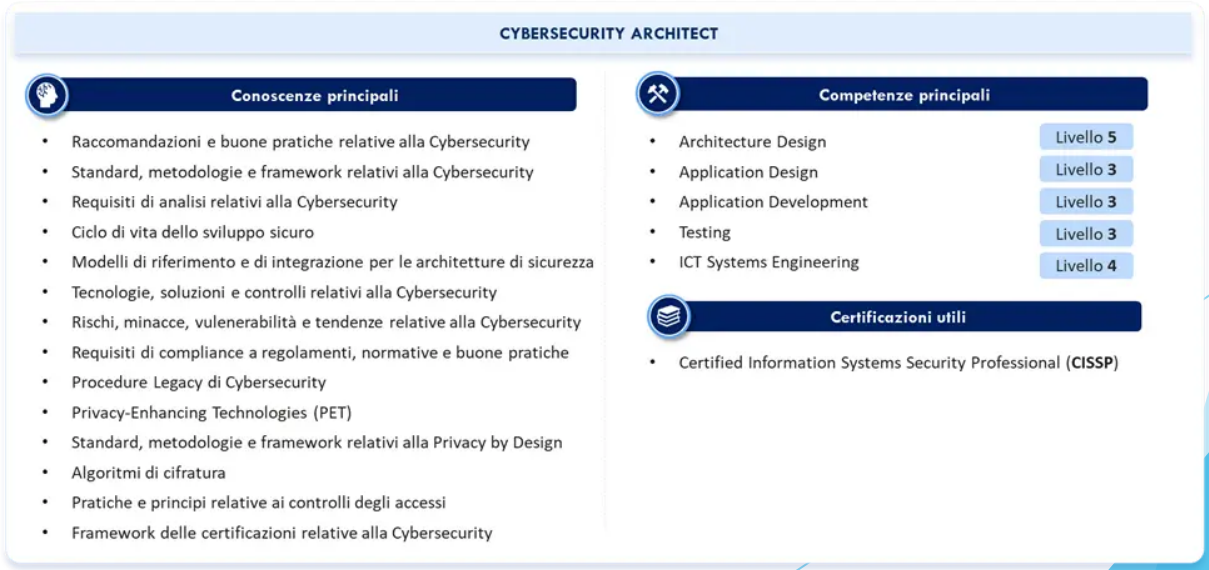


I criteri di cybersecurity: la premialità

e) **prevedono criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO** o di Paesi terzi individuati con il decreto di cui al comma 1 tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza.

3. Le disposizioni di cui al comma 1 si applicano anche ai soggetti privati non compresi tra quelli di cui all'articolo 2, comma 2, del codice di cui al decreto legislativo 7 marzo 2005, n. 82, e inseriti nell'elencazione di cui all'articolo 1, comma 2 -bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

4. Resta fermo quanto stabilito dall'articolo 1 del citato decreto-legge n. 105 del 2019 per i casi ivi previsti di approvvigionamento di beni, sistemi e servizi di information and communication technology destinati ad essere impiegati nelle reti e nei sistemi informativi nonché per l'espletamento dei servizi informatici di cui alla lettera b) del comma 2 del medesimo articolo 1.



CYBERSECURITY AWARENESS E DATA BREACH

- Per capire come le minacce interne generate dal fattore umano possano scatenare dei veri e propri data breach è sufficiente analizzare alcuni casi verificatisi nel 2020 e nel 2021 che hanno colpito alcune pubbliche amministrazioni sia in Italia che in Europa
- **Anonymous attacca i siti della Regione Basilicata e dei comuni della Val D'Agri**
- Denunciare lo sfruttamento petrolifero del territorio lucano e l'inquinamento. È questa la matrice dell'attacco informatico ai siti della Regione Basilicata e dell'Università lucana, perpetrato il 15-02-2020 dagli hacker di Anonymous.

CYBERSECURITY AWARENESS E DATA BREACH

- L’attacco informatico era stato preannunciato sul blog del gruppo il 14 febbraio, aveva stati colpito i portali web istituzionali di Giunta Regione, Consiglio Regionale, Apt, il vecchio sito dell’Unibasilicata e quelli dei Comuni della Val D’Agri, con obiettivo di divulgare nomi, cognomi, username, password ed email degli amministratori, oltre che le credenziali di 198 aziende lucane, con tanto di nome, email, telefono, siti web, partita Iva e codice fiscale, e una lista di una trentina di uffici per le relazioni col pubblico, l’elenco del personale amministrativo ed altro. L’attacco si è reso necessario per denunciare "le persone che hanno avuto e che hanno tuttora un ruolo nella situazione di sfruttamento petrolifero del territorio lucano e i relativi danni ambientali.

CYBERSECURITY AWARENESS E DATA BREACH

- L’attacco si è reso necessario per denunciare "le persone che hanno avuto e che hanno tuttora un ruolo nella situazione di sfruttamento petrolifero del territorio lucano e i relativi danni ambientali. L’attacco informatico di Anonymous si è concretizzato in un accesso non autorizzato su applicazioni in parte già dismesse e in parte in corso di dismissione e sostituzione, nell’ambito di un piano di verifica dell’integrità e sicurezza delle applicazioni che la Regione stessa stava portando avanti. Gli utenti e gli amministratori dei vari sistemi oggetto degli attacchi sono stati contattatati al fine di adottare le relative azioni di sicurezza. Come da prassi la Regione ha provveduto alla notifica e **segnalazione di Data Breach** all’Autorità Garante sulla Privacy ai sensi del Regolamento generale sulla protezione dei dati (GDPR).

CYBERSECURITY AWARENESS E DATA BREACH

- **Danimarca, sanzionati due comuni che avevano notificato Data Breach per furto di computer**

- L'autorità di controllo per la protezione dei dati danese il 13 marzo 2020 ha rilevato che due comuni, quello di ladsaxe e quello di Hørsholm non garantiscono un livello adeguato di sicurezza dei dati come richiesto dal Gdpr. Per i comuni di Gladsaxe e Hørsholm sono state quindi proposte multe rispettivamente di 100.000 e 50.000 corone danesi, ovvero circa 13mila euro nel primo caso e 6mila euro nel secondo. Il garante danese era venuto a conoscenza di entrambi i casi a seguito della notifica di Data Breach riguardanti violazioni relative al furto di computer contenenti dati personali, che gli stessi comuni avevano inviato all'autorità per ottemperare a quanto previsto dall'art.33 del Gdpr.

CYBERSECURITY AWARENESS E DATA BREACH

- Nessuno dei due computer era protetto dalla crittografia e la perdita di dati personali da parte dei comuni rappresentava pertanto un rischio indebito per i cittadini. In uno dei casi, l'inadeguato livello di sicurezza ha comportato una grave violazione dei dati personali, in quanto uno dei computer rubati al municipio di Gladsaxe conteneva dati personali di 20.620 cittadini, conteneva anche informazioni di natura sensibile. Un'altra violazione della sicurezza è avvenuta quando il computer di un dipendente del comune di Hørsholm è stato rubato dalla sua automobile. Sul computer c'erano informazioni riguardanti circa 1.600 dipendenti dello stesso comune, comprese informazioni di natura sensibile, rientranti nelle "categorie particolari di dati personali" ai sensi dell'art.9 del Regolamento UE 2016/679. Secondo **quanto rilevato dall'autorità danese**, tali violazioni manifestavano alcune delle possibili conseguenze dell'insufficiente livello di sicurezza che comporta un rischio elevato per tutti i cittadini di cui il comune tratta i dati personali, e perciò ha proposto le due sanzioni.

CYBERSECURITY AWARENESS E DATA BREACH

- **Ransomware colpisce il Comune di Marentino**
- Con un **comunicato sul proprio sito istituzionale**, il Comune di Marentino il 13-4-2020 aveva informato tutti gli interessati, residenti e non, di aver recentemente subito un attacco informatico di tipo **ransomware** che, sfruttando il periodo emergenziale causato dall'epidemia, ha violato i dati personali presenti sul server centrale. L'Ente aveva affermato di essersi prontamente attivato, procedendo anche a notificare il Data Breach al Garante per la protezione dei dati personali come previsto dal Gdpr. Ad accorgersi dell'accaduto sono stati i dipendenti comunali, quando da casa si sono collegati all'account dell'ente per lavorare in smartworking, come sono costretti a fare in questo periodo per disposizioni governative relative all'emergenza Covid-19.

CYBERSECURITY AWARENESS E DATA BREACH

- I criminali informatici hanno inoculato un cryptoLocker che ha messo fuori uso il sistema per poi cancellare anche il backup dei file, chiedendo un riscatto in bitcoin per sbloccare i dati, "in misura ridotta" di 50mila euro se il pagamento fosse avvenuto entro due giorni, cifra che è però raddoppiata a 100mila euro dopo la scadenza del termine. Preso atto della violazione, il piccolo comune piemontese aveva iniziato un processo di adeguamento per adottare tutte le misure più idonee a porre rimedio alla situazione di rischio, attenuando i possibili effetti negativi e tutelare i diritti e le libertà delle persone fisiche purtroppo coinvolte nella violazione. Nel frattempo, l'attacco era stato denunciato ai carabinieri di Sciolze ed è stata informata anche la polizia postale.

CYBERSECURITY AWARENESS E DATA BREACH 2020

GIUGNO

Pubblica amministrazione

Mail malevola avverte la vittima di un fantomatico "Contenzioso Civile"

Il CERT-AgID: Il cybercrime ha lanciato una massiccia campagna malspam per diffondere FTCODE via PEC in Italia. I bersagli sono le strutture della Pubblica Amministrazione e i privati. Il malware sfrutta un presunto contenzioso civile al Tribunale di Napoli

Fonte: https://www.difesaesicurezza.com/

2020

MARZO

Settore della Sanità

Il data breach al San Raffaele ha esposto i dati di ben 2400 dipendenti e 600 pazienti.

San Raffaele: data breach di gravità "media", ospedale obbligato a notificare gli utenti

Fonte: https://www.agendadigitale.eu/

SETTEMBRE

Settore finanziario

E-mail di spear-phishing che utilizzano come esca le normative KYC (Know Your Customer regulations).

Remote Access Trojan, arriva PyVil: cosa lo rende così temibile, come difendersi

Fonte: https://www.cybersecurity360.it/

CYBERSECURITY AWARENESS E DATA BREACH 2021

- **Sistema informativo del Comune di Brescia paralizzato da ransomware. Attacco hacker al Comune di Brescia, chiesto un riscatto da 1,3 milioni**

- Sempre nel mese di aprile 2021 è stato attaccato il sistema di posta elettronica e l'intera operatività dei server del Comune di Brescia. Come si legge nella nota pubblicata nello stesso sito istituzionale della pubblica amministrazione lombarda, la causa della paralisi è stata un attacco ransomware avvenuto il 30 marzo, e la richiesta di riscatto per fornire la chiave di sblocco avanzata dai criminali informatici per restituire la disponibilità dei dati è di 26 Bitcoin, l'equivalente al cambio odierno di 1,3 milioni di euro. Secondo quanto riferito dai media locali, il ransomware che ha colpito il Comune di Brescia è DoppelPaymer, per la verità non nuovo alle amministrazioni pubbliche italiane, il quale è capace di entrare silenziosamente nei server e bloccarne l'accesso crittografandone i file contenuti (il riscatto, appunto, servirebbe a ottenere la chiave per decriptarli).

CYBERSECURITY AWARENESS E DATA BREACH 2021

- Mentre gli uffici dell'amministrazione lombarda sono al lavoro per tentare di far ripartire la macchina digitale del comune che conta circa 200mila abitanti, resta ora da capire quanto ci metteranno i tecnici a ripristinare la normalità, perché ad essere bloccato, non è solo il sito web, ma anche il sistema che gestisce le gare e gli appalti, l'Archiweb per le pratiche edilizie, tutto il sistema scolastico e quello cimiteriale, le postazioni di lavoro della Ragioneria, della Loggia, dell'Anagrafe e della Polizia Locale. La riattivazione di alcuni servizi essenziali, incluso un sito web "muletto" per garantire le comunicazioni con i cittadini, dovrebbe avvenire nel giro di alcuni giorni, anche se fonti interne smorzano facili ottimismi: senza pagamento del riscatto, occorreranno mesi, addirittura anni per recuperare i dati criptati dal malware. L'unica alternativa, per ora, sarà quella di contare sui back up, sperando siano abbastanza aggiornati.

CYBERSECURITY AWARENESS E DATA BREACH 2021

- **Attacco informatico ai server dell'Agenzia Territoriale per la Casa di Torino, oltre mezzo milione di euro il riscatto chiesto dagli hacker**

- Un attacco informatico verificatosi nel week end e scoperto dai tecnici al rientro è avvenuto lunedì mattina 11 aprile 2021 che ha mandato in tilt i server dell'ATC Torino (Agenzia Territoriale per la Casa), l'azienda pubblica che gestisce 30mila appartamenti di edilizia popolare. Gli hacker hanno chiesto all'ente un riscatto di 700mila dollari per restituire i dati rubati e criptati. L'attacco riguarda circa 43 terabyte di dati gestiti. L'attacco si è svolto mediante la ricezione di una mail da parte del personale con la richiesta di un cospicuo riscatto dell'importo corrispondente al cambio attuale a 584mila euro, messaggio che si sarebbe subito autodistrutto dopo la lettura senza lasciare tracce, motivo per cui pare che dietro l'attacco di tipo ransomware vi siano professionisti di alto profilo.

CASI PRATICI PA

SOCIAL PRIVACY

ALCUNI CASI PRATICI

- ***L'UTILIZZO DEI SOCIAL FOTO CON IL CONSENSO – NOVEMBRE 2019***

- ***Ordinanza del Tribunale di Bari del 7-11-2019 – Causa 6359/2017***
- ***Con questa sentenza viene negata la diffusione sui social network di foto di persone senza il loro espresso consenso. E' l'assenso alla pubblicazione può essere revocato in qualsiasi momento. Il caso riguardava la pubblicazione su facebook di un migliaio di fotografie di una papà e dei suoi figli. Si verifica sia la violazione dell'articolo 10 del codice civile (abuso di immagine altrui) e sia la violazione dell'articolo 6 del GDPR 679/2016 (protezione dei dati- obbligo di consenso) e del considerando n° 18 del GDPR 679/2016 (che considera come esclusivamente personale l'uso di un social network)***

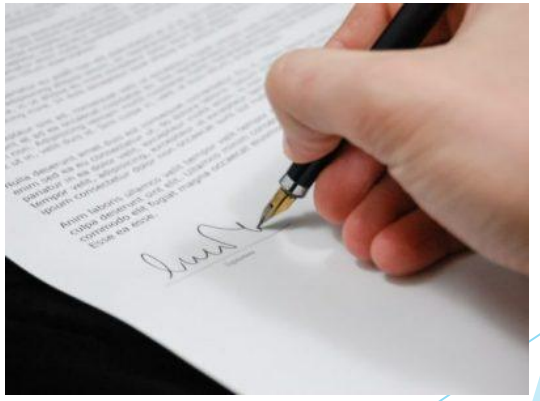
ALCUNI CASI PRATICI

- ***L'UTILIZZO DEI SOCIAL NEGLI ENTI LOCALI – FEBBRAIO 2019***

- ***ROMA CAPITALE il 13 febbraio 2019 ha approvato un regolamento per l'accesso a internet dove la navigazione web è consentita solo per fini istituzionali e di servizio fatte salve situazioni personali di tipo emergenziale. L'accesso alla rete internet non è consentito per scopi di profitto, per visione di siti non pertinenti con contenuti illeciti o porno, per downolad di software inclusi quelli gratuiti, senza la preventiva autorizzazione scritta del Dipartimento IT di Roma Capitale. Le navigazioni e le comunicazioni sono tracciate e conservate per il monitoraggio a tutela dell'ente e per eventuale richiesta dell'Autorità Giudiziaria.***

USO DI MAIL E SOCIAL NELLA PA

- ***Il datore di lavoro (sentenza Corte di Cassazione 32760 del 9-11-2021- uso di device digitali) deve comunicare ai dipendenti delle linee guida da utilizzare***
- ***In tale sentenza gli elementi raccolti sui device pubblici possono essere utilizzati anche per verificare la diligenza del dipendente nello svolgimento dell'attività lavorativa- obbligo di informativa da parte del datore di lavoro della pa (Sentenza Tribunale di Cosenza n° 4096 pubblicata il 23-02-2022)***
- ***- Sono legittimi tutti i controlli massivi attivati in assenza di un motivo specifico o di un pericolo attuale. Costituisce valido per attivare i controlli un fondato sospetto nei confronti del dipendente infedele***



USO DI MAIL E SOCIAL NELLA PA

- ***Anche i social possono entrare nelle policy privacy della pa. Post, video, commenti e like possono infatti costituire una violazione del generico obbligo di fedeltà dettato dall'articolo 2105 del codice civile che impone al dipendente di tenere un comportamento leale verso il datore di lavoro e di tutelarne in ogni modo gli interessi.***

WHATSAPP

- ***Gli screenshot dei messaggi whatsapp o i messaggi contenuti nella memoria di un telefono possono essere acquisiti nel processo penale e vengono valutati dl giudice in relazione all'attendibilità dei soggetti interessati al pari di altri documenti, senza la necessità di estrarre la cosiddetta copia forense, ossia la copia integrale del suo contenuto, che rappresenta la modalità tipica per la valutazione e l'eventuale acquisizione di dati informatici nell'ambito di un procedimento giudiziario (sentenza Corte di cassazione II Penale n. 39529 del 19-10-2022)***

WHATSAPP

- ***Secondo l'orientamento richiamato dalla Suprema Corte, quindi i messaggi scambiati tramite applicazione whatsapp devono essere considerati alla stregua di vere e proprie « prove documentali» , motivo per cui , ai fini della loro acquisizione quali elemnti di prova, trova applicazione la disciplina prevista dall'art. 234 c.p.p. («Prova documentale»), ai sensi del quale «è consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo (sentenza Corte di cassazione II Penale n. 39529 del 19-10-2022)***

WHATSAPP- IL PRINCIPIO

- ***Corte di cassazione II Penale n. 39529 del 19-10-2022***

- ***In temi di mezzi di prova, i messaggi WhatsApp e gli sms conservati nella memoria di un telefono cellulare hanno natura di documenti (art. 234 c.p.p.)***
- ***Legittima la loro acquisizione nel processo penale mediante mera riproduzione fotografica***
- ***Non è necessaria la c.d. copia forense dell'apparecchio cellulare***
- ***In questi casi non trova applicazione la disciplina delle intercettazioni telefoniche, né quella relativa al sequestro di corrispondenza (art. 254 c.p.p.)***
- ***I messaggi WhatsApp e gli sms vengono valutati dal Giudice in relazione all'attendibilità dei soggetti interessati (ad es. della persona offesa)***

WHATSAPP- NIENTE RECESSO PER INSULTI DIFFUSI SU UNA CHAT PRIVATA

- ***Tribunale di Firenze Sezione Lavoro sentenza del 16-10-2019***
- ***L'utilizzo di una chat su WhatsApp tra colleghi di lavoro per veicolare messaggi vocali di contenuto offensivo, minatorio e razzista nei confronti di un superiore gerarchico o di altri dipendenti, non ha contenuto diffamatorio, non costituisce violazione dell'obbligo di fedeltà e non ha, in definitiva, portata rilevante sul piano disciplinare.***
- ***Il Giudice di Firenze, in sintesi, conclude che quanto avvenuto equivale allo scambio di corrispondenza privata tra colleghi di lavoro, con conseguente insussistenza del fatto nella sua componente materiale. Pertanto né è derivato l'ordine al datore di lavoro di reintegrare il dipendente e di versargli le retribuzioni maturate nel frattempo.***

WHATSAPP- DIFFAMARE PUO' COSTARE IL POSTO DI LAVORO

- *TAR Sardegna Prima Sezione sentenza n. 174/22*
- ***Scatta la sanzione disciplinare per il dipendente pubblico che nel whatsapp al collega parla male dei capi: a inguaiarlo è proprio l'interlocutore che fa la spia ai superiori, perché una volta che l'amministrazione apprende il contenuto della conversazione non può non valutarlo sul piano disciplinare. A maggiore ragione quando l'incolpato è un militare: l'ordinamento del corpo lascia ampia discrezionalità nel valutare la rilevanza dei fatti.***
- ***Confermato il rimprovero inflitto all'ufficiale che nei messaggi rivolti all'(ex) amica si lamenta dei superiori: una serie di commenti e valutazioni che lede il prestigio dei vertici del corpo e lascia intendere che il servizio si svolga in condizioni di inaffidabilità***

WHATSAPP- DIFFAMARE PUO' COSTARE IL POSTO DI LAVORO

- ***Nel caso di specie, è una dei due partecipanti alla conversazione a far conoscere i messaggi al comando, mentre la giurisprudenza di legittimità, ad esempio non prende in considerazione la natura riservata delle mail denigratorie quando si pronuncia sul licenziamento: valuta la portata diffamatoria del messaggio o l'eventuale esercizio di critica. Senza dimenticare che la diffamazione semplice non richiede la divulgazione nell'ambiente sociale, ma si configura con la mera comunicazione che può essere privata e pure riservata. Il datore di lavoro, poi non viola libertà e segretezza della conversazione quando a rivelarne il contenuto è uno dei partecipanti. Infatti nella specie non conta che il messaggio sia one to one e non in un gruppo perché la contestazione disciplinare non richiama in alcun modo la configurabilità di una diffamazione rilevante sul piano penale.***

WHATSAPP- ALCUNI SUGGERIMENTI

- ***Evitare di creare gruppi whatsapp o quanto meno non essere l'amministratore del gruppo, infatti l'amministratore del gruppo è anche titolare del trattamento dati, con ogni conseguenza in relazione al GDPR (ad es, informativa, consenso, etc)***
- ***Se si ricevono continui messaggi l'amministratore è nel pieno diritto di revocare il consenso del trattamento del proprio numero di telefono dalla chat***
- ***Se si usa whatsapp come strumento di lavoro verso i fornitori ad es, questo va inserito nell'informativa che si mette a disposizione dei dipendenti e vanno organizzate per scritto delle procedure in relazione alla conservazione e cancellazione di dette informazioni***

INSULTI SUL WEB – BASTANO GLI INDIZI

- ***Il Reato commesso sui social network può essere accertato dal giudice penale anche su base indiziaria. Non occorrono, cioè specifiche tecniche, per esempio sul cosiddetto indirizzo IP per ricondurre l'eventuale post diffamatorio all'imputato, essendo sufficiente che emergano, nel corso del giudizio, indizi gravi, precisi e concordanti a carico dello stesso. Lo ha stabilito la Corte di Cassazione – quinta sezione penale con la sentenza n° 24212/2021 del 21-6-2021***

INSULTI SUL WEB – BASTANO GLI INDIZI

- ***Corte di Cassazione – quinta sezione penale con la sentenza n° 24212/2021 del 21-6-2021***
- ***QUADRO INDIZIARIO PER RESPONSABILITA' PENALE***
- ***Movente***
- ***Argomento del Forum sui cui è stato pubblicato il post offensivo***
- ***Rapporto parte offesa/imputato (ad esempio, quando circostanze specifiche possono essere conosciute solo dall'imputato)***
- ***Provenienza post diffamatorio dalla bacheca dell'imputato (per esempio profilo facebook)***
- ***Assenza di Denuncia, da parte dell'imputato, di furto di identità (cassazione Penale n. 45339/2018)***

MINISTERO DELLA GIUSTIZIA- GIORNALISTI

- ***I magistrati possono riferire notizie ai giornalisti secondo la sentenza della Corte di Giustizia UE del 24 marzo 2022, resa nella causa C-245/20. Il fatto che un organo giurisdizionale metta temporaneamente a disposizione dei giornalisti documenti di un procedimento giurisdizionale, contenenti dati personali, al fine di consentire loro di riferire in modo più completo sullo svolgimento di tale procedimento rientra nell'esercizio , da parte di tale organo giurisdizionale, delle sue «funzioni giurisdizionali», ai sensi dell'articolo 55, paragrafo 3, GDPR.***
- ***Infatti per la Corte UE, fornire informazioni che arrivano da un fascicolo giudiziario e che possono essere divulgate a un giornalista per garantire alla stampa la possibilità di fornire informazioni sui procedimenti giurisdizionali in corso è un'attività strettamente legata alle «funzioni giurisdizionali» esercitate dai giudici e, di conseguenza quest'attività non può essere sottoposta al controllo di un'autorità esterna.***

MINISTERO DELLA GIUSTIZIA- DATI GENETICI E BIOMETRICI

- ***Sul trattamento dei dati biometrici e genetici per finalità di giustizia, è intervenuta la sentenza della Corte di Giustizie UE del 26 gennaio 2023, resa nella causa C-205/21, con alcune affermazioni di principio . Il primo profilo riguarda il trattamento dei dati biometrici e genetici da parte delle autorità di polizia per le loro attività di ricerca, a fini di lotta contro la criminalità e di tutela dell'ordine pubblico. Secondo la sentenza questo trattamento deve essere autorizzato dal diritto interno dello Stato membro della UE.***
- ***Peraltro la normativa nazionale può prevedere che, in caso di rifiuto della persona formalmente accusata di un reato doloso perseguibile d'ufficio di cooperare spontaneamente alla raccolta dei dati biometrici e genetici che la riguardano, ai fini della loro registrazione, il giudice penale competente***

MINISTERO DELLA GIUSTIZIA- DATI GENETICI E BIOMETRICI

- ***sia tenuto ad autorizzare una misura di esecuzione coercitiva di tale raccolta, senza avere il potere di valutare se sussistano fondati motivi per ritenere che l'interessato abbia commesso il reato di cui formalmente è accusato.***
- ***La corte di Giustizia UE ha, infine, aggiunto che la normativa nazionale non può prevedere la raccolta sistematica di dati biometrici e genetici di qualsiasi persona formalmente accusata di un reato doloso perseguibile d'ufficio, ai fini della loro registrazione, senza prevedere l'obbligo, per l'autorità competente e di verificare e di dimostrare, da un lato, che tale raccolta sia strettamente necessaria per il raggiungimento dei concreti obiettivi perseguiti e, dall'altro, che tali obiettivi non possano essere raggiunti mediante misure che costituiscono un'ingerenza meno grave nei diritti e nelle libertà della persona interessata.***

MINISTERO DELLA GIUSTIZIA- PROVE

- ***Sul rapporto tra privacy e processo giurisdizionale è intervenuta la sentenza della Corte di Giustizia UE del 2 marzo 2023, resa nella causa C-268/21, con due affermazioni di principio.***
- ***- La prima affermazione della Corte sottolinea che il GDPR si applica nell'ambito di un procedimento giurisdizionale civile, alla produzione come elemento di prova di un registro del personale contenente dati personali di terzi raccolti principalmente ai fini dei controlli fiscali. Tale affermazione si riferisce all'articolo 6, paragrafi 3 e 4, del GDPR e cioè, oltre al resto, alla necessità che siano garantite garanzie adeguate a tutela della persona.***
- ***Le finalità di giustizia non devono, pertanto, essere il pretesto per calpestare la privacy altrui ed il regime speciale della privacy nelle aule dei tribunali è giustificato dal fatto che i protagonisti del processo agiscono mantenendosi nei limiti delle previsioni dei cosiddetti codici di rito.***

MINISTERO DELLA GIUSTIZIA- PROVE

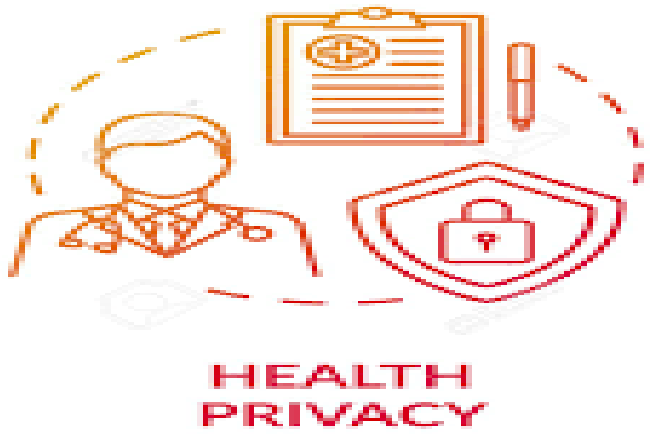
- ***La seconda affermazione si basa sull'assunto <u>che la Corte di Giustizia UE, nel valutare se debba essere disposta la produzione di un documento contenente dati personali, il giudice nazionale è tenuto a prendere in considerazione gli interessi delle persone di cui trattasi e a ponderarli in funzione delle circostanze di ciascun caso di specie del tipo di procedimento di cui trattasi e tenendo debitamente conto delle esigenze derivanti dal principio di proporzionalità e, in particolare, di quelle derivanti dal principio di minimizzazione dei dati</u> (articolo 5, paragrafo 1, lettera c) del GDPR. Infatti i principi formulati trovano corrispondenza nell'articolo 160-bi del D.lgs 196/2003 e s.m.i. (testo unico sulla privacy), ai sensi del quale la validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali***

MINISTERO DELLA GIUSTIZIA- PROVE

- ***IL SIGNIFICATO CONCRETO DELLE AFFERMAZIONI DELLA CORTE DI GIUSTIZIA EUROPEA E DELLE NORME DEL CODICE DELLA PRIVACY E' CHE LE DISPOSIZIONI A TUTELA DELLA RISERVATEZZA DELLE PERSONE FANNO UN PASSO INDIETRO RISPETTO ALLE REGOLE PROCESSUALI.***

MINISTERO DELLA GIUSTIZIA- PROVE

- ***SONO PER ALTRO, GLI STESSI CODICI DI PROCEDURA A SEGNARE I LIMITI DI AMMISSIONE DELLE PROVE ED IL LORO REGIME MANTIENE LA SUA SPECIALITA', ANCHE DI FRONTE ALL'ORDINAMENTO DELLA PROTEZIONE DEI DATI.***


HEALTH
PRIVACY

ALCUNI CASI PRATICI

- **CARTELLE SANITARIE E DI RISCHIO DEI LAVORATORI – GIUGNO 2019**

- ***Commissione per gli interpelli sulla sicurezza interpello 4/2019 (FNOMCEO- Federazione Nazionale degli Ordini dei medici chirurghi e degli odontoiatri)***

- ***Le cartelle sanitarie e di rischio dei lavoratori possono essere inserite in un db dell'ente a patto che nel rispetto del segreto professionale e della tutela della privacy, venga garantita l'accessibilità al solo medico competente***

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Dati sanitari

ALCUNI CASI PRATICI

- ***La Commissione afferma che è consentito l'impiego di sistemi di elaborazione automatica per memorizzare le cartelle sanitarie e di rischio anche su data base dell'ente.***
- ***Quanto alla custodia, però ritiene necessarie soluzioni concordate tra datore di lavoro e medico competente, che nel rispetto del segreto professionale e della privacy, garantiscano l'accessibilità ai dati solo al medico e non al datore di lavoro né all'amministratore di sistema***

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Dati sanitari

ALCUNI CASI PRATICI

- ***ACCESSI LIMITATI AL PROTOCOLLO INFORMATICO – FEBBRAIO 2021***
  - ***Sentenza Cassazione n° 3819/2021***

- ***Con questa sentenza la Suprema Corte ha sancito che un numero rilevante di accessi, da parte di un dipendente comunale, al protocollo informatico dell'ente, per conoscere atti che non rientravano in quelli di competenza del settore di assegnazione, possono giustificare il licenziamento con preavviso.***

ALCUNI CASI PRATICI

- **Sentenza Cassazione n° 3819/2021 – IL CASO**

- ***Una dipendente comunale è stata oggetto di un procedimento disciplinare espulsivo, a causa di un numero elevato di accessi al sistema informatico dell'ente (circa 2.138 accessi in un periodo di circa 5 mesi) per ragioni non attinenti al proprio ufficio.***
- ***Nel caso di specie, i giudici di appello, hanno indicato le ragioni per le quali la condotta della lavoratrice, tenuta in violazione dei doveri propri del dipendente pubblico, fosse da ritenere di gravità tale da giustificare il recesso con preavviso. Per tali motivazioni il ricorso della dipendente è stato considerato inammissibile in quanto volta al riesame delle motivazioni correttamente spiegati dai giudici di appello.***


Diritto all'oblio
Privacy
Privacy
GDPR
Privacy
Privacy
Diritto all'oblio
Privacy
Privacy
Privacy
GDPR
GDPR
Diritto di cronaca
GDPR
GDPR
Diritto di cronaca
GDPR
Diritto all'oblio
Diffamazione
Diritto di cronaca

ALCUNI CASI PRATICI

- **DIRITTO ALL'OBLIO(art. 17 GDPR) – IL CASO- LA DEINDICIZZAZIONE DEI MOTORI DI RICERCA**

- ***Con sentenza n° 3578 del 28/03/2018 il Tribunale di Milano ha sancito la disponibilità dei dati via web limitata ad un periodo di 4 anni al fine di porre un rimedio temporale alla permanente ed indistinta disponibilità di dati al pubblico degli internauti.***
- ***Con sentenza del Tribunale di Roma n° 12048 del 12-07-2018 viene dato il via libera alle indagini e chi svolge attività di consulenza in favore di aziende, di enti, di organizzazioni pubbliche e private esercita un «ruolo pubblico» proprio per effetto della professione svolta. I relativi dati personali risultano quindi trattati nel pieno rispetto dell'essenzialità dell'informazione finchè l'indagine giudiziaria non è conclusa.***

ALCUNI CASI PRATICI

- ***DIRITTO ALL'OBLIO - LA DEINDICIZZAZIONE DEI MOTORI DI RICERCA***

- ***La deindicizzazione a Google con sentenza n° 419 del 08/01/2018 il Tribunale di Milano ha comunicato a Google che la richiesta di deindicizzazione al motore di ricerca deve essere precisa e indicare tutti i link di cui si chiede la rimozione. La domanda non va formulata nei confronti di Google Italy srl, poiché il motore di ricerca è gestito da Google. Inc., società con sede negli Stati Uniti, alla quale occorre rivolgersi in via esclusiva.. La Società italiana Google Italy srl non ha, quindi, alcun ruolo sul funzionamento del servizio web Search.***

ALCUNI CASI PRATICI

- ***DIRITTO ALL'OBLIO – IL DIRITTO ALL'IDENTITA' PERSONALE***

- ***Le attività svolte dal motore di ricerca incidono sensibilmente sulle informazioni pubblicate sul web. L'utente deve veder tutelato il proprio diritto specifico all'identità personale, segnatamente il diritto alla dissociazione del proprio nome da un dato risultato di ricerca. Il cd ridimensionamento della propria visibilità telematica, difatti, rappresenta un aspetto «funzionale» del diritto all'identità personale, diverso dal diritto ad essere dimenticato. Questo è il principio sancito dalla sentenza n° 7846 del 05/09/2018 del Tribunale di Milano***

ALCUNI CASI PRATICI

- **DIRITTO ALL'OBLIO – PARERE DELLA CASSAZIONE**

- ***La Corte di Cassazione con ordinanza n° 28084 del 5-11-2018 ha rimesso gli atti al presidente per l'eventuale assegnazione alle sezioni unite. Il caso prende le mosse dalla richieste di un utente che dopo 12 anni di carcere ed un faticoso reinserimento sociale si era trovato nuovamente al centro dell'attenzione a causa di un articolo su un giornale locale che aveva ripreso la sua storia per una rubrica dedicata agli omicidi del passato. L'indicizzazione della notizia online aveva di fatto vanificato il suo percorso di recupero tanto da portare a chiedere giustizia fino all'ultimo grado di giudizio.***

ALCUNI CASI PRATICI

- **DIRITTO ALL'OBLIO**

- ***In sintesi il primo passo per ottenere il diritto all'oblio è inviare una richiesta scritta all'editore, al titolare del sito, al social network e/o motore di ricerca. Se i responsabili dei nostri dati personali non rispondono o danno esito negativo è possibile, inoltrare gratuitamente, un reclamo a mezzo pec (protocollo@pec.gdp.it) o raccomandata AR al Garante. Il reclamo può essere firmato direttamente dall'interessato o da un avvocato. Va indicato un proprio recapito, i link di cui si chiede la cancellazione o la deindicizzazione, e se conosciuti- gli estremi del responsabile del trattamento dei nostri dati. Il Garante decide in genere sul reclamo entro nove mesi dalla data di presentazione e, in ogni caso, entro tre mesi dalla predetta data informa l'interessato sullo stato del procedimento***

ALCUNI CASI PRATICI

- **DIRITTO ALL'OBLIO E LIMITAZIONE**

- ***Il GDPR (articoli da 12 a 23) prevede il catalogo dei diritti a favore degli interessati dell'interessato. Tra questi diritti troviamo il diritto alla cancellazione (meglio noto come diritto all'oblio – articolo 17) ed il diritto alla limitazione (blocco) del trattamento (articolo 18 GDPR). Sull'interpretazione degli articoli 17 e 18 è intervenuta la Corte di Giustizia UE con la sentenza del 4 maggio 2023, resa nella causa C-60/22.***

Diritto all'oblio

Corte di Giustizia UE con la sentenza del 4 maggio 2023

- **DIRITTO ALL'OBLIO E LIMITAZIONE**

- ***La pronuncia contiene due massime, la prima delle quali recita « la violazione da parte del titolare del trattamento, degli obblighi previsti agli articoli 26 e 30 del regolamento UE 679/2016, relativi rispettivamente, alla conclusione di un accordo che determina la contitolarità del trattamento e alla tenuta di un registro delle attività di trattamento, non costituisce un trattamento illecito che conferisce all'interessato il diritto alla cancellazione o alla limitazione del trattamento, poiché una siffatta violazione da parte del titolare del trattamento del principio di «responsabilizzazione» quale sancito dall'articolo 5, paragrafo 2 detto regolamento, il combinato disposto con l'articolo 5, paragrafo 1 lettera a), e con l'articolo 6, paragrafo 1, primo comma dello stesso».***

Diritto all'oblio

Corte di Giustizia UE sentenza del 4 maggio 2023

- **DIRITTO ALL'OBLIO E LIMITAZIONE**

- ***PER EFFETTO DEL PRINCIPIO ENUNCIATO SI FRENA L'ABUSO DEI DIRITTI DI OBLIO E DI LIMITAZIONE DEL TRATTAMENTO***

Diritto all'oblio

Corte di Giustizia UE sentenza del 4 maggio 2023

- **DIRITTO ALL'OBLIO E LIMITAZIONE**

- ***Con la seconda massima la CGUE afferma che «il diritto dell'Unione deve essere interpretato nel senso che, qualora il titolare del trattamento abbia violato gli obblighi che gli derivano dagli articoli 26 o 30 del regolamento UE 679/2016, la liceità della presa in considerazione di siffatti dati da parte di un giudice nazionale non è subordinata al consenso dell'interessato».***
- ***<u>Pertanto il giudice può prendere in considerazione fatti e dati a prescindere dalla violazione della privacy. L'acquisizione delle prove del giudizio è disciplinata dai codici di procedura e non dal GDPR</u>.***

Diritto all'oblio

Corte di Giustizia UE sentenza del 8 dicembre 2022

- **DIRITTO ALL'OBLIO SENZA SENTENZA**

- ***Sul diritto di cancellazione, noto come diritto di oblio (articolo 17 GDPR), è intervenuta la sentenza della Corte di giustizia dell'Unione Europea del 8 dicembre 2022, resa nella causa C-460/20, formulando i seguenti principi.***
- ***Innanzitutto, per ottenere la deindicizzazione di un risultato di una ricerca impostata su un motore di ricerca generale sul web l'interessato non deve avere una sentenza che, riconoscendo che il risultato è errato, lo autorizzi a chiedere tale rimozione. Pertanto con tale sentenza l'articolo 17 GDPR deve essere interpretato nel senso che, ai fini dell'esame di una richiesta di deindicizzazione rivolta al gestore di un motore di ricerca e diretta ad ottenere l'eliminazione, dall'elenco dei risultati di una ricerca, del link verso un contenuto che include affermazioni che la persona che ha presentato dette richiesta ritiene inesatte,***

Corte di Giustizia UE con la sentenza del 8 dicembre 2022

- **DIRITTO ALL'OBLIO SENZA SENTENZA**

- ***Tale deindicizzazione non è subordinata alla condizione che la questione dell'esattezza del contenuto indicizzato sia stata risolta, almeno provvisoriamente nel quadro di un'azione legale intentata da detta persona contro il fornitore di tale contenuto.***

ALCUNI CASI PRATICI

PRIVACY NEL RAPPORTO DI LAVORO

- ***Il Garante Privacy con provvedimento pubblicato su G.U. n° 176 del 29-7-2019 ha reso noto un provvedimento che raccoglie e aggiorna prescrizioni sul trattamento di particolari categorie di dati redatto ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101***
- ***Prescrizioni relative al trattamento di categorie particolari nei rapporti di lavoro. Se si è in presenza di un dato personale (capace di identificare una persona fisica) e di un rapporto di lavoro (subordinato, autonomo, libero-professionale di amministrazione o collaborazione comunque declinata) allora trovano applicazione le prescrizioni del provvedimento***

ALCUNI CASI PRATICI

- **FINALITA' DEL TRATTAMENTO DEI DATI**

- ***Vengono indicate tali finalità con particolare riferimento all'instaurazione, gestione ed estinzione del rapporto di lavoro (quindi a ogni vicenda connessa ai rapporti stessi) e alla difesa di un diritto in sede giudiziaria nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione (quindi per la gestione delle controversie tra datore di lavoro e lavoratore, o terze parti.***

- ***Sono due le categorie più importanti: il colloquio pre-assuntivo e la definizione della possibile causa relativa alla cessazione (anzi estinzione, un concetto ancora più ampio) del rapporto di lavoro***

ALCUNI CASI PRATICI

- ***La fase pre-assuntiva (sia gestita da agenzie di selezione, sia direttamente dal potenziale datore di lavoro) deve comportare trattamento di dati «strettamente pertinenti» con la ricerca del candidato. Tale principio viene applicato alle mansioni ed ai profili professionali per i quali la ricerca è effettuata. Dati esuberanti tale ambito non potranno essere oggetto di valutazione al fine dell'idoneità del candidato, con espressa esclusione dei dati genetici, il cui trattamento è definito illegittimo ai fini di valutare l'idoneità professionale, anche ove il candidato abbia prestato il suo consenso.***

ALCUNI CASI PRATICI

- ***Una volta assunto o comunque selezionato, il lavoratore fornisce al datore i dati necessari all'esecuzione del rapporto. Tali dati, specifica il Garante, non comprendono quelli relativi alle convinzioni religiose, alle idee politiche o all'esercizio di funzioni pubbliche e sindacali. Questi ultimi sono lecitamente trattati solo per le finalità specifiche e previste dall'ordinamento (ad es. permessi, trattenute o festività) e non per valutare il dipendente.***

ALCUNI CASI PRATICI

- ***PRIMA DELL'ASSUNZIONE-***

- ***Agenzie per il lavoro e società di intermediazione***

- ***Possono trattare dati idonei a rivelare, salute, origine etnica e razziale solo se è necessario per instaurare il rapporto di lavoro e/o per scopi determinati (ad es l'assunzione di persone disabili, ai fini della copertura della legge 68/1999)***

- ***Il Trattamento per l'instaurazione del rapporto di lavoro***

- ***Deve riguardare le informazioni pertinenti e limitate alla finalità di assunzione, anche in base alle mansioni e al profilo professionale richiesto. Se nei curricula sono presenti dati non pertinenti (situazione di salute o origine razziale o etnica) rispetto al ruolo ricercato, il datore deve astenersi dall'usare quelle informazioni cancellandole***

ALCUNI CASI PRATICI

- ***DURANTE IL RAPPORTO DI LAVORO-***

- ***Dati che rivelano la religione del lavoratore***

- ***Possono essere trattati per la concessione di permessi o per l'erogazione del servizio mensa***

- ***Dati che rivelino l'opinione politica o sindacale***

- ***Possono essere trattati per concedere permessi o aspettativa o per esercitare diritti sindacali – In caso di lavoratori rappresentanti di lista il datore non può trattare dati idonei a rivelare opinioni politiche (è sufficiente il certificato rilasciato dal presidente di seggio)***

ALCUNI CASI PRATICI

- ***PRESCRIZIONI SPECIFICHE SUL TRATTAMENTO-***

- ***La raccolta***

- ***I dati particolari devono essere raccolti di regola presso l'interessato, ossia la persona alla quale si riferiscono***

- ***Le comunicazioni***

- ***Le comunicazioni che contengono dati sensibili devono essere individualizzate. Possono essere effettuate a un delegato, anche tramite personale autorizzato (meglio se per iscritto). Le comunicazioni di dati sensibili possono avvenire in modalità elettronica (ad es. tramite e-mail), o in forma cartacea (in busta chiusa, salva la necessità di acquisire la firma per ricevuta).***

ALCUNI CASI PRATICI

- ***PRESCRIZIONI SPECIFICHE SUL TRATTAMENTO-***

- ***Le modalità di trasmissione***

- ***I documenti che contengono dati sensibili, ove debbano essere trasmessi ad altri uffici (anche interni), devono contenere solo le informazioni utili a svolgere la funzione***

- ***I dati sulle presenze***

- ***Se i dati delle assenze, per ragioni di servizio o di organizzazione (ad esempio turni di lavoro), devono essere messi a disposizione di più colleghi, il dato deve riportare solo l'assenza o non la ragione (malattia, infortunio, aspettativa, permesso sindacale e cosi via)***

ALCUNI CASI PRATICI

- ***PRESCRIZIONI SPECIFICHE SUL TRATTAMENTO-***
- ***CARTELLE SANITARIE***
- ***- Le cartelle sanitarie e di rischio dei lavoratori possono essere inserite anche in un database dell'ente a patto che, nel rispetto del segreto professionale, venga garantita l'accessibilità solamente al medico competente (si veda interpello n° 4/2019 della commissione per gli interpelli sulla sicurezza)***

ALCUNI CASI PRATICI

- ***IN PILLOLE***

- Il trattamento dei dati particolari (Articolo 9 GDPR 679/2016), può avvenire per soddisfare le seguenti finalità:

- ***Adempiere a obblighi specifici per l'erogazione di contributi o per l'applicazione della normativa sulla sicurezza del lavoro;***
- ***Per tenuta di contabilità o pagamento di stipendi;***
- ***Per tutelare l'incolumità o la salute dei lavoratori***
- ***Per far valere o difendere un diritto in sede giudiziaria, arbitrale o di conciliazione***
- ***Per adempiere a contratti di assicurazione (es stipule di polizze professionali per dolo o colpa grave dei dipendenti pubblici)***
- ***Per dare opportunità di lavoro***
- ***Per gli scopi delle associazioni datoriali o sindacali***


AREA
VIDEOSORVEGLIATA

ALCUNI CASI PRATICI

- **IMPIANTI DI VIDEOSORVEGLIANZA- Sentenza Cassazione 50919 del 17-12-2019**

- ***Il consenso espresso dai lavoratori non elimina la liceità del comportamento datoriale che ha installato un impianto di videosorveglianza senza il prescritto accordo sindacale o, in alternativa, senza l'autorizzazione dell'ITL (Ispettorato Territoriale del Lavoro). Secondo la suprema Corte che ritengono infondato il ricorso del datore di lavoro, non ha alcun rilievo la circostanza dedotta dal ricorrente, secondo la quale l'impianto di registrazione visiva era stato installato onde garantire la sicurezza degli stessi dipendenti, posto che la finalità di garantire la sicurezza sul lavoro è uno dei fattori che in linea astratta, rendono possibile l'attivazione di tale tipo di impianti.***

Informativa base

Informativa per collegamenti con le forze di polizia

ALCUNI CASI PRATICI

- **IMPIANTI DI VIDEOSORVEGLIANZA- Sentenza Cassazione 50919 del 17-12-2019**

- ***E' irrilevante, ai fini della possibile integrazione della contravvenzione contestata, la circostanza che il datore di lavoro non abbia avuto personalmente accesso al contenuto delle videoriprese essendo l'impianto attraverso il quale esse vengono effettuate, gestito da un soggetto terzo rispetto al datore di lavoro-***
- ***- Pertanto il consenso non è sufficiente a sanare l'illecito, anche in considerazione del ruolo di «parte debole» che connota il lavoratore rispetto alla parte datoriale.***

Informativa base

Informativa per collegamenti con le forze di polizia

ALCUNI CASI PRATICI

- **IMPIANTI DI VIDEOSORVEGLIANZA- Ordinanza di ingiunzione garante sulla privacy n° 20 del 27-01-2022**

- ***Il circolo che posiziona alcune telecamere sulla strada rivolte verso il pubblico passaggio riprendendo anche la vicina caserma dei carabinieri è sanzionabile, in quanto le riprese sulle pubbliche vie le possono effettuare solo i comuni e le forze di polizia locale. E' quanto successo a Firenze dove la polizia locale ha effettuato un sopralluogo in un circolo privato verificando l'attivazione di un sistema di videosorveglianza con telecamere sia interne che esterne e senza aver affisso alcun cartello informativo***

Informativa base

Informativa per collegamenti con le forze di polizia

ALCUNI CASI PRATICI

- **IMPIANTI DI VIDEOSORVEGLIANZA FACE-ID – Parere n° 54 Garante sulla privacy del 26-02-2020**

- ***Secondo questo parere la raccolta e la conservazione dei dati biometrici ed in particolare il riconoscimento facciale restano negati salvo che l'ente locale ottenga un parere favorevole dall'autorità garante. Infatti l'articolo 9, commi 9,10,11 e 12 del decreto legge 139/2021 convertito in legge 205/2021 stabilisce che dal 8-12-2021 e fino al 31-12-2023 è vietata in Italia l'installazione e l'utilizzazione dei sistemi di riconoscimento facciale.***

informativa base

informativa per collegamenti con le forze di polizia

ALCUNI CASI PRATICI

- **IMPIANTI DI VIDEOSORVEGLIANZA FACE-ID – Parere n° 54 Garante sulla privacy del 26-02-2020**

- ***Ma questo divieto ai sensi del comma 12 del medesimo articolo non si applica ai trattamenti effettuati dalle autorità competenti ai fini di prevenzione espressione dei reati ai sensi del Dlgs 51/2018 (reati perseguiti dall'ente locale relativamente alle attribuzioni di polizia giudiziaria della polizia locale o comunque a esigenze di tutela della sicurezza urbana) , previo parere positivo del Garante alla necessaria valutazione obbligatoria di impatto (DPIA).***

Informativa base

Informativa per collegamenti con le forze di polizia

ALCUNI CASI PRATICI- POLIZIA LOCALE

- **IL PRIVATO NON PUO' SCOPRIRE CHI LO DENUNCIA ALLA POLIZIA LOCALE- Sentenza TAR Emilia Romagna 136/2022 Sezione II**

- ***Bocciato il ricorso dell'artista di strada che si proclamava vittima di incessanti controlli della polizia locale durante la sue performance artistiche. Questo è accaduto a Bologna dove il difensore civico presso la Regione Emilia Romagna ha effettuato reclamo dopo il diniego della Polizia Locale. L'ostensione del nome va negata perché bisogna distinguere l'accesso agli atti amministrativi rispetto ai dati personali contenuti nella segnalazione, ciò perché il nominativo del segnalante è oggetto di una tutela costituzionale e pertanto deve trovare applicazione la disciplina del Regolamento UE 679/2016 – GDPR (articolo 4 comma lettera 1).***

ALCUNI CASI PRATICI- POLIZIA LOCALE

- **MULTE, DEI BUCHI PRIVACY RISPONDE IL FORNITORE Ordinanza Garante Privacy n° 9767635 del 24-03-2022**

- ***Se il sistema informativo della polizia locale viene violato il primo responsabile va ricercato nel fornitore esterno del servizio. Un utente è riuscito ad entrare abusivamente nel gestionale delle multe del Comune di Genova e per questo motivo il Garante ha aperto un'istruttoria che si è conclusa con l'applicazione di una sanzione amministrativa a carico unicamente del fornitore privato della piattaforma informatica.***

- ***Il comune infatti, in tale caso ha operato correttamente, in quanto ai sensi dell'articolo 32 del GDPR pone in capo sia al titolare che al responsabile esterno la responsabilità per l'adozione delle necessarie misure tecniche ed organizzative.***

ALCUNI CASI PRATICI- POLIZIA LOCALE

- **MULTE, DEI BUCHI PRIVACY RISPONDE IL FORNITORE Ordinanza Garante Privacy n° 9767635 del 24-03-2022**

- **Infatti, il fornitore della piattaforma non ha messo a disposizione un software perfettamente concepito *privacy by design , ovvero in grado ad esempio di obbligare l'utente a modificare la password al primo accesso al sistema.***

- ***Il Comune di Genova, però aveva ben formalizzato, ai sensi dell'articolo 28 del GDPR, i rapporti contrattuali con il privato, prevedendo, esplicitamente, tra l'altro, «l'obbligo per la società in ragione della sua esperienza tecnica nel settore, di mettere in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio inclusa una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure.***


Pa, smart working almeno al
50% per tutela salute e servizi

ALCUNI CASI PRATICI- SITO WEB ISTITUZIONALE

- **IL COMUNE NON PUO' VIOLARE LA PRIVACY Provvedimento Garante Privacy n° 198 del 26-05-2022**

- **Il Comune risponde delle violazioni privacy commesse dal gestore del suo sito istituzionale. *L'ente locale subisce sanzioni pecuniarie ed amministrative se non controlla l'operato del fornitore esterno*. Con questo provvedimento il Garante ha comminato una sanzione di € 10.000,00 per aver conservato sul sito istituzionale- sezione amministrazione trasparente, il curriculum di un ex dirigente senza aver schermato indirizzi fisici ed e-mail e numero di cellulare, e per un periodo superiore a quello previsto dalla legge (tre anni dopo la cessazione dal servizio). Sono due gli elementi importanti risultanti dalle motivazioni dell'ingiunzione.**

ALCUNI CASI PRATICI- SITO WEB ISTITUZIONALE

- **IL COMUNE NON PUO' VIOLARE LA PRIVACY Provvedimento Garante Privacy n° 198 del 26-05-2022**

1. **Il primo riguarda il fatto che affidare all'esterno un servizio non significa affatto trasferire la responsabilità amministrativa.**
2. **Il secondo profilo mette in evidenza che è compito dell'ente locale oscurare i dati eccedenti, anche quando il curriculum viene consegnato spontaneamente dall'interessato con troppe informazioni: la condotta o addirittura il consenso dell'interessato non esimono l'ente, che di sua iniziativa deve cancellare quello che non deve essere diffuso**

ALCUNI CASI PRATICI- SITO WEB ISTITUZIONALE

- **Provvedimento Garante Privacy n° 198 del 26-05-2022**
- **Pertanto il cv on line non deve contenere dati ulteriori rispetto a quelli necessari a raggiungere lo scopo della trasparenza amministrativa. Sono ad es. pertinenti le informazioni sui titoli di studio e professionali, le esperienze lavorative (ad es. gli incarichi ricoperti), ulteriori informazioni di carattere professionale (conoscenze linguistiche, competenze nell'uso delle tecnologie, partecipazioni a convegni e seminari oppure pubblicazioni). Secondo il Garante sono eccedenti l'indirizzo di residenza, il numero di cellulare, gli indirizzi di posta elettronica privati, il codice fiscale. Nella prassi è stata anche rilevata l'eccedenza della riproduzione della firma autografa. Queste limitazioni il Garante le ha giustificate con la necessità di ridurre il rischio di furti di identità (Linee Guida Garante n° 243 del 15-05-2014.**

ALCUNI CASI PRATICI- DELIBERE E DETERMINE

- **PRIVACY DI RIGORE PER DELIBERE E DETERMINE Ordinanza Garante Privacy n° 45 del 10-02-2022**
- **Nel caso di specie un cittadino ha proposto reclamo al Garante dopo aver appreso che sull'albo pretorio di un comune erano stati diffusi tutti i dettagli delle sue denunce e querele per giustificare la revoca dell'assunzione in servizio di un altro soggetto. Il comune è stato sanzionato con un multa per aver violato e non applicato il principio di minimizzazione previsto dal GDPR , pubblicando all'albo pretorio tutti gli atti amministrativi in spregio al diritto all'oblio ed alla tutela della riservatezza.**

ALCUNI CASI PRATICI- SCILA E CILA

- **SCILA E CILA Provvedimento Garante Privacy n° 1 del 03-01-2019- I DATI DEVONO ESSERE «COPERTI»**
- **Nel caso di specie un comune aveva rilasciato copia delle pratiche edilizie, solo in sintesi con dati aggregati, depurati di quelli personali. In materia, il Garante ha rilevato che la completa conoscenza delle informazioni riportate nella SCIA, può comportare un'invasione alla vita privata, poichè si rivelerebbero data e luogo di nascita, codici fiscali, residenza, e-mail, pec, numero di telefono fisso e mobile, documentazione tecnica sugli interventi. Il Garante ha concluso, ricordando che il no all'accesso civico generalizzato non impedisce di accedere ai documenti amministrativi con altri atti (es. legge 241/1990 e s.m.i.), sussistendone i presupposti**

ALCUNI CASI PRATICI

- **IBAN Corte di Cassazione ordinanza 4475/2021- Comunicare l'iban può costituire una violazione della privacy**

- ***La Suprema Corte, con ordinanza n. 4475/2021, dava ragione ai ricorrenti sulla base di un lineare (e logico) elemento fattuale: dare prova di aver risarcito il danno, siccome richiesto dall'assicurato, "non può in alcun modo ricomprendere anche la diffusione delle coordinate bancarie delle persone risarcite", non essendo tale trattamento del dato né funzionale alla finalità per cui esso era stato raccolto né necessario per adempiere alla richiesta recepita. Nella vicenda in argomento, il dato personale illecitamente comunicato è costituito dalle coordinate bancarie di un danneggiato.***

ALCUNI CASI PRATICI

- ***Per gli operatori ed i cultori del settore è ormai noto che le coordinate bancarie costituiscano un dato personale (sul punto, tra i tanti provvedimenti, cfr. Autorità Garante, provvedimento 21 aprile 2018, n. 231 ovvero Tribunale Ragusa, Sent., 31-01-2019). La Suprema Corte torna a ribadire che dare la prova di aver adempiuto un obbligo contrattuale non può costituire un pregiudizio alla riservatezza e alla tutela dei soggetti terzi nel rispetto dei cd. principi di proporzionalità, pertinenza e non eccedenza.***

ALCUNI CASI PRATICI

- ***La sentenza specifica che "il contratto di assicurazione del cui adempimento si tratta non aveva come suoi contraenti gli odierni ricorrenti", essendo al più applicabile al proprio assicurato. Il danneggiato era soggetto terzo rispetto al contratto assicurativo. Per questo, la Corte dapprima si rifà al principio di correttezza quale generale principio di solidarietà sociale, in base al quale, anche nell'ambito della responsabilità extracontrattuale, si è tenuti a mantenere un comportamento leale che, evidentemente, nel caso di specie è venuto a mancare.***

ALCUNI CASI PRATICI

- ***Più puntualmente, raccolti i dati dall'interessato (in questo caso le coordinate bancarie del danneggiato), comunicarli al proprio cliente per dimostrare di aver risarcito il danno viola i principi di correttezza e minimizzazione, specificamente pertinenza e limitazione del trattamento alle finalità della raccolta di tali dati. Al contrario, "sarebbe stato sufficiente inviare al D.B. una comunicazione in cui si dava atto dell'intervenuto ristoro dei danni, come solitamente d'uso nelle compagnie, e/o, al più, consegnargli la quietanza dopo averne debitamente oscurato le informazioni sui dati personali non divulgabili ai sensi della normativa sulla privacy"***

ALCUNI CASI PRATICI- SISTEMA SCOLASTICO

- **11 febbraio 2021 Privacy, graduatorie prof. On line- no a dati personali- Liceo Scientifico Pepe Calamo di Ostuni**
- Con provvedimento 51/2021 il Garante sulla privacy ha stabilito che viola la privacy dei docenti la scuola che diffonde sul web il file originale con le graduatorie provvisorie di istituto del personale docente di III fascia contenente informazioni personali quali mail, numeri di cellulari e sigle di preferenze per invalidità. (pubblicazione sul sito web istituzionale del Liceo Scientifico Pepe Calamo di Ostuni di graduatorie relative a personale docente di III fascia).
- Sanzione comminata di euro 5.000,00 (cinquemila

ALCUNI CASI PRATICI

- **Ordinanza di ingiunzione nei confronti di Ministero dello Sviluppo Economico - 11 febbraio 2021 Provvedimento n° 54 del 11-02-2021 Garante Privacy**
- ***Il Garante per la privacy ha ordinato al Mise il pagamento di una sanzione di 75mila euro per non avere nominato il Responsabile della protezione dati (Rpd) entro il 28 maggio 2018, data di piena applicazione del Gdpr, e avere diffuso sul sito web istituzionale informazioni personali di oltre 5mila manager.***

ALCUNI CASI PRATICI

- ***Per la prima volta l'Autorità ha sanzionato una Pa per non avere designato il Rdp entro il termine stabilito ed avere provveduto alla nomina e alla comunicazione al Garante dei dati di contatto con notevole ritardo. La mancata nomina, è emersa nel corso di una istruttoria, aperta dall'Ufficio anche a seguito di alcune segnalazioni, con la quale è stata accertata la presenza sul sito del Ministero di una pagina web con un elenco di manager nella quale erano visibili e liberamente scaricabili i dati personali di più di cinquemila professionisti: nominativo, codice fiscale, e-mail, curriculum vitae integrale con telefono cellulare e, in alcuni casi copia del documento di riconoscimento e della tessera sanitaria.***

ALCUNI CASI PRATICI

- ***Dal sito era inoltre possibile scaricare anche il decreto direttoriale con il quale l'elenco era stato approvato, contenente dati e informazioni di tutti i manager. Nel rilevare l'illiceità del trattamento, il Garante ha ritenuto che il decreto direttoriale richiamato dal Mise, contrariamente a quanto da esso sostenuto, non costituisce una adeguata base normativa per la diffusione dei dati online. L'Autorità ha ritenuto che la pubblicazione integrale dei curricula, senza alcun filtro, rappresenta un trattamento di dati sproporzionato, non in linea con i principi del Gdpr.***

ALCUNI CASI PRATICI

- ***Per consentire l'incontro tra la domanda delle società e l'offerta di consulenza da parte dei manager sarebbe stato sufficiente utilizzare strumenti meno invasivi rispetto alla pubblicazione sul web dei dati e delle informazioni di tutti i manager, evitando così il rischio di esporli ad utilizzi non legittimi da parte di terzi (es.: furti d'identità, profilazione illecita, phishing, ecc.). Si sarebbero potute prevedere, ad esempio, forme di accesso selettivo ad aree riservate del sito istituzionale mediante l'attribuzione di credenziali di autenticazione (es. username o password), oppure ancora tramite gli strumenti previsti dal CAD, che permettessero la consultazione solo alle Pmi interessate.***

ALCUNI CASI PRATICI

- **Ordinanza ingiunzione nei confronti di Regione Lazio - 14 gennaio 2021 Provvedimento n° 9 del 14-01-2021 Garante Privacy**

- ***Il Garante per la protezione dei dati personali ha sanzionato la Regione Lazio per 75.000 euro per non aver nominato responsabile del trattamento dati la Società Cooperativa Capodarco, a cui l'Ente aveva affidato la gestione delle prenotazioni delle prestazioni sanitarie, attraverso il call center regionale (ReCUP).***

ALCUNI CASI PRATICI

- ***La società ha dunque trattato i dati dei pazienti in modo illecito per un decennio, dal 1999 al 7 gennaio 2019, data in cui la Regione Lazio, in qualità di titolare, ha designato formalmente la Cooperativa responsabile del trattamento, ben oltre l'inizio di piena applicazione del Regolamento europeo in materia di protezione dei dati personali. Con il provvedimento il Garante ha ribadito che le società che prestano servizi per conto del titolare e che di conseguenza trattano i dati personali degli utenti, devono essere designate responsabili del trattamento.***

ALCUNI CASI PRATICI

- ***Il rapporto tra titolare e responsabile deve essere regolato da un contratto o da altro atto giuridico, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, prevede nel dettaglio le regole e i limiti con cui devono essere trattati i dati personali. Il responsabile è, pertanto, legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare".***

ALCUNI CASI PRATICI

- ***Inoltre il Comitato che riunisce le Autorità di protezione dati dell'Ue, l'assenza di una chiara definizione del rapporto tra titolare e responsabile può sollevare il problema della mancanza di base giuridica su cui ogni trattamento deve fondarsi: ad esempio, per quanto riguarda la comunicazione dei dati tra titolare e responsabile. Rilevato l'illecito, l'Autorità ha multato la Regione per 75.000 euro ed ha applicato la sanzione accessoria della pubblicazione del provvedimento sul sito dell'Autorità.***

ALCUNI CASI PRATICI

- ***Il Garante ha ritenuto invece sufficiente ammonire il titolare della Cooperativa perché la Società Capodarco aveva più volte rappresentato alla Regione la necessità di essere nominata responsabile del trattamento e messo in atto misure conformi alla disciplina privacy, istituendo, ad esempio, il registro dei trattamenti.***

ALCUNI CASI PRATICI

- **Ruoli privacy negli appalti pubblici: alcune soluzioni per i raggruppamenti temporanei di imprese**
- ***Le PA impongono gli obblighi relativi al trattamento dei dati personali in capo alle imprese appaltatrici, soprattutto sulla distribuzione dei ruoli e delle relative responsabilità nell'ambito della privacy che i committenti, stazioni appaltanti, propongono agli esecutori del lavoro o del servizio quando questi ultimi hanno costituito un raggruppamento temporaneo di imprese o associazione temporanea d'impresa (di seguito RTI), in quanto l'assegnazione di tali ruoli e responsabilità è proposta dopo attente analisi fattuali sul servizio erogato o sul lavoro effettuato e dallo schema definito nell'accordo (RTI verticale, orizzontale e misto).***

ALCUNI CASI PRATICI

- ***Lo strumento giuridico utilizzato dalle imprese che formano un RTI è quello del mandato con rappresentanza collettivo conferito dalle imprese mandanti all'impresa mandataria che agisce da capogruppo e che rappresenta tutta l'aggregazione nei rapporti con il committente (art. 48, co. 8, 12 e 15 Codice dei contratti pubblici).***
- ***Pertanto, nel RTI ciascun partecipante conserva la propria autonomia, non determinando tale struttura la costituzione di un'organizzazione stabile, rimanendo, tuttavia, solidalmente responsabile con gli altri nei confronti della stazione appaltante (art. 48, co. 4 e 16 Codice dei contratti pubblici).***

ALCUNI CASI PRATICI

- ***Distribuzione dei ruoli e delle responsabilità nell'ambito della privacy nei RTI***

- ***L'esecuzione dell'incarico oggetto del contratto pubblico può comportare il trattamento da parte del RTI dei dati personali di cui è titolare la stazione appaltante. Tale attività è soprattutto frequente nell'ambito degli appalti di servizi. Ebbene, il RTI, ai sensi dell'art. 28 del GDPR, agisce quale responsabile del trattamento. La distribuzione dei ruoli nell'ambito della privacy generalmente dipende dall'oggetto del contratto pubblico, dal tipo di RTI (verticale, orizzontale o misto), nonché dalle categorie dei dati personali trattati e dalle modalità di tale trattamento***

ALCUNI CASI PRATICI

- ***a) Designazione dell'impresa mandataria quale responsabile del trattamento dei dati - Il committente nomina quale responsabile del trattamento dei dati personali, ai sensi dell'art. 28 del Regolamento UE 2016/679, la società mandataria del raggruppamento temporaneo di imprese, rilasciandole un'autorizzazione specifica, che fa sì che sia quest'ultima a gestire le relazioni con la mandante e le eventuali ulteriori esecutrici.***

ALCUNI CASI PRATICI

- ***a) In questo caso, solitamente l'impresa mandataria ricorre a nomine di secondo livello volte a riflettere gli adempimenti contrattuali ai quali risponde il responsabile di primo livello, ovvero la mandataria, in modo tale che anche le altre società coinvolte nella commessa, quindi mandanti ed esecutrici dell'appalto, possano essere nominate sub responsabili (ovvero responsabili di secondo livello). In tale ipotesi, le società mandanti non hanno rapporti diretti con il committente e rispondono dei propri obblighi in materia di privacy esclusivamente nei confronti della società mandataria. Quest'ultima, a sua volta, risponde nei confronti della stazione appaltante dell'agire proprio e di quello delle mandanti.***

ALCUNI CASI PRATICI

- ***a) Tale approccio parrebbe in linea non soltanto con le disposizioni dell'art. 28, par. 4, del Regolamento UE 2016/679, ma anche con le previsioni del Codice dei contratti pubblici il quale, all'art. 48, co. 8, specifica che è il mandatario che stipula il contratto di appalto in nome e per conto proprio e dei mandanti.***

ALCUNI CASI PRATICI

- ***b) Designazione di tutte le imprese coinvolte nel RTI (mandataria, mandante ed esecutrici) quali responsabili del trattamento dei dati - In altre occasioni l'atto di nomina a responsabile del trattamento dati personali viene proposto a tutte le società esecutrici dell'appalto: la mandataria, le mandanti ed ogni esecutrice dell'appalto.***
- ***Tale fattispecie porta alla gestione da parte del committente di diverse nomine e di relazioni dirette con tutti i soggetti coinvolti nella commessa, dove i singoli attori risultano responsabili del trattamento di primo livello e sottoscrivono singoli accordi contrattuali.***

ALCUNI CASI PRATICI

- ***b) In tale ipotesi, infatti, non sono designati sub-responsabili: tutte le imprese facenti parte del RTI e tutte le esecutrici coinvolte nell'appalto agiscono sullo stesso piano e rispondono del proprio agire in materia privacy direttamente nei confronti del committente.***
- ***Pertanto, l'esecuzione dell'appalto pubblico avviene sul doppio binario: mentre nell'ambito del lavoro o del servizio oggetto del contratto la mandataria ha la rappresentanza esclusiva dei mandanti nei confronti della stazione appaltante, in ambito privacy tutte le imprese agiscono sullo stesso piano nei confronti del committente.***

ALCUNI CASI PRATICI

- ***c) Designazione della mandataria e della mandante quali responsabili del trattamento dei dati - È possibile individuare una soluzione intermedia alle due precedentemente esposte, ossia lo scenario in cui il Titolare del trattamento, committente del servizio, designa quali Responsabili del Trattamento i soggetti componenti/costituenti il RTI, mandataria e mandante, lasciando la possibilità che questi ultimi assegnino il ruolo di Sub Responsabile alle società esecutrici affidatarie del servizio. Secondo questo schema ciascun componente del RTI assume responsabilità dirette nei confronti della stazione appaltante e risponde dell'operato delle proprie società esecutrici.***

ALCUNI CASI PRATICI

- ***c) Tale soluzione potrebbe essere calzante nel caso in cui si presentasse un RTI verticale dove il flusso dei dati personali possa risultare distinto per servizio o lavoro svolto dalla mandataria e dalla mandante.***

ALCUNI CASI PRATICI

- ***d) Designazione dell'impresa mandataria quale responsabile del trattamento dei dati con effetti diretti sulle imprese mandanti***
- ***- Infine un'ultima soluzione, ma non per questo meno frequente, è quella in cui il committente chiede esplicitamente nell'atto di nomina a responsabile del trattamento dei dati personali che sia firmato dalla sola società mandataria ma abbia effetti diretti anche sulla mandante che viene citata nell'unico atto di designazione a responsabile proposto dal committente. In questo caso si è in presenza di due o più responsabili di primo livello che accettano le condizioni contrattuali privacy solo per mezzo della sottoscrizione dell'atto di nomina da parte della mandataria, che se ne fa portavoce.***

ALCUNI CASI PRATICI

- ***È opportuno in questi casi predisporre un patto parasociale (in caso di RTI composto da soci, come ad esempio, nelle realtà consortili) o un regolamento/accordo interno tra la mandataria e le altre società mandanti richiamate nell'atto di nomina proposto dal committente, al fine di poter adeguatamente imporre i medesimi adempimenti contrattuali alle altre società del RTI.***

ALCUNI CASI PRATICI

- ***Tale ipotesi appare un tentativo di conciliare la normativa privacy con quella sugli appalti pubblici: da un lato, il committente chiede un rapporto diretto in materia del trattamento dei dati personali su tutte le imprese del RTI, dall'altro lato, propone la sottoscrizione dell'atto di designazione a responsabile del trattamento soltanto alla mandataria in quanto la stessa rappresenta le società mandanti in virtù del mandato collettivo ex art. 48, co. 8, del Codice dei contratti pubblici.***

ALCUNI CASI PRATICI- SISTEMA SCOLASTICO

- **28-04-2022 - Le scuole non possono basare il trattamento dei dati personali sul consenso degli interessati**
- Le scuole non possono usare il consenso degli interessati per trattare i dati. La normativa sulla privacy impone alle pubbliche amministrazioni di agire con presupposti diversi dal consenso (osservanza dell'interesse pubblico). È quanto precisato dal Garante della privacy nella motivazione dell'Ingiunzione n. 148 del 28 aprile 2022.

ALCUNI CASI PRATICI- SISTEMA SCOLASTICO

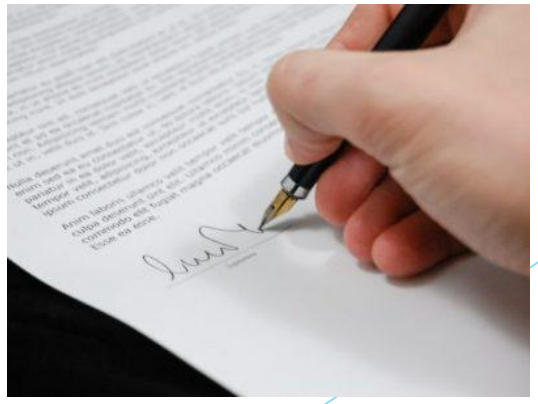
- **28-04-2022 - Ordinanza ingiunzione nei confronti di Liceo Statale "Isabella Gonzaga" - 28 aprile 2022- Fruizione benefici legge 104/92**

- Con reclamo del XX, è stato lamentata la pubblicazione in apposita sezione dedicata ai docenti ("bacheca contenente gli avvisi ai docenti"), del registro elettronico impiegato dal Liceo Statale "Isabella Gonzaga" di Chieti (di seguito "Istituto"), di un documento "relativo all'orario definitivo Anno Scolastico 2020-2021" recante, in corrispondenza del nominativo della reclamante, il riferimento alla fruizione dei benefici derivanti dalla legge 5 febbraio 1992, n. 104 e, in particolare, l'indicazione "legge 104 non grave".

ALCUNI CASI PRATICI- SISTEMA SCOLASTICO

- **28-04-2022 - Ordinanza ingiunzione nei confronti di Liceo Statale "Isabella Gonzaga" - 28 aprile 2022- Fruizione benefici legge 104/92 Il trattamento di dati personali effettuato dall'Istituto.**

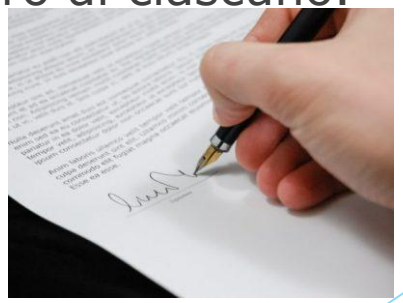
- Come risulta dagli atti e dalle dichiarazioni rese dall'istituto scolastico, **l'Istituto ha reso disponibile nella sezione del registro elettronico riservata ai soli insegnanti, un documento recante l'orario definitivo del personale docente contenente il riferimento alla fruizione dei benefici derivanti dalla legge 5 febbraio 1992, n. 104** da parte della reclamante e di altri docenti, nonché altre informazioni di dettaglio relative a vicende personali e familiari o legate allo specifico rapporto di lavoro di ciascuno (ed es. trasferimento, part-time, interdizione maternità, legge 104 non grav. Si veda anche il provv. 28 maggio 2020, n. 92, doc. web n. 9434609).
- Tale principio, già contenuto nelle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" (Provv. n. 23 del 14 giugno 2007, doc web n. 1417809, è stato ribadito nel tempo dal Garante nell'ambito di decisioni su singoli casi.



ALCUNI CASI PRATICI- SISTEMA SCOLASTICO

- **28-04-2022 - Ordinanza ingiunzione nei confronti di Liceo Statale "Isabella Gonzaga" - 28 aprile 2022- Fruizione benefici legge 104/92**
- Sebbene, quindi, per errore la messa a disposizione del documento in questione, nella propria versione integrale e contenente dati personali anche dati relativi alla salute degli interessati, sia avvenuta in un'area ad accesso riservato del registro elettronico dell'Istituto - non accessibile a chiunque e tale da determinare una diffusione di dati personali - **la conoscibilità dei dati ivi contenuti è avvenuta comunque in favore di un novero, determinato o determinabile, assai ampio di soggetti, ossia tutti i colleghi della reclamante appartenenti al personale docente e non, invece, esclusivamente a vantaggio del solo personale di segreteria autorizzato al trattamento di tali informazioni**.

- ha di fatto reso conoscibili a tutto il personale docente dell'Istituto informazioni, anche relative alla salute, della reclamante e di altri interessati e ha reso, inoltre, gli stessi docenti vicendevolmente edotti in merito a situazioni personali, familiari o comunque attinenti allo specifico rapporto di lavoro di ciascuno.



ALCUNI CASI PRATICI- SISTEMA SCOLASTICO

- **28-04-2022 - Ordinanza ingiunzione nei confronti di Liceo Statale "Isabella Gonzaga" - 28 aprile 2022- Fruizione benefici legge 104/92**

- Per tali ragioni l'Istituto, ancorché a seguito di un mero errore, ha posto in essere un trattamento di dati personali, in violazione degli artt. 5, 6, 9 del Regolamento e 2-ter e 2 sexies del Codice nel testo anteriore alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla l. 3 dicembre 2021, n. 205).
- Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della stessa sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento nella misura di euro 2.500,00 (duemilacinquecento).

PRIVACY IN PILLOLE IL VADEMECUM DEL GARANTE SETTEMBRE 2022

- **6 settembre 2022 - Privacy & Scuola: Il vademecum del Garante**
- **TELECAMERE**
- Si possono installare telecamere all'interno degli istituti scolastici, ma l'eventuale installazione di sistemi di videosorveglianza deve garantire il diritto allo studente alla riservatezza. Può risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio e i beni scolastici da atti vandalici, circoscrivendo e riprese alle sole aree interessate. E' inoltre necessario segnalare la presenza degli impianti con cartelli. Le telecamere che inquadrano all'interno degli istituti possono essere attivate solo negli orari di chiusura quindi non in coincidenza con lo svolgimento di attività scolastiche ed extrascolastiche. Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere devono essere opportunamente delimitate.

Misure di sicurezza

QUESITI