GARANTEPRIVACYITALIA.it

Circolare del 15 Maggio 2020

INDICE

VIETATO REGISTRARE LA TEMPERATURA DEI "CLIENTI"

A seguito dall'emergenza sanitaria legata al Covid-19, sono stati tantissimi gli interventi del legislatore, e molti di questi hanno riguardato il diritto alla riservatezza dei cittadini. Proprio per tale motivazione diventano di centrale rilevanza documenti "linee guida" tipici oramai delle amministrazioni, e proprio in questo quadro si inseriscono le FAQ in tema di "COVID e Privacy" pubblicate dall'Autorità Garante per la protezione dei dati personali sul proprio sito web istituzionale.

In primo luogo si pone al centro la questione sulla **misurazione della temperatura** all'ingresso della sede aziendale: il Garante conferma che tale misura è ormai certamente **applicabile a chiunque**, che sia dipendente, fornitore o visitatore occasionale, e ribadisce l'importante distinguo tra la semplice rilevazione della temperatura (sempre possibile) e la registrazione della stessa.

Quest'ultima operazione è ammessa **solo laddove il valore superi il massimo consentito (37,5 gradi),** al fine di documentare le ragioni che hanno impedito l'accesso al luogo di lavoro. Di conseguenza, specifica sempre il Garante, la registrazione non è necessaria quando si tratti di visitatori occasionali o clienti.

Altro tema è **l'autocertificazione** relativa a contatti avvenuti con "soggetti contagiati" e la provenienza da zone c.d. a rischio (secondo la classificazione dell'OMS).

Anche in questo caso si ribadisce che la misura **può essere adottata** nei confronti di qualunque soggetto debba entrare in azienda, ferma restando la necessità di **limitare la raccolta ai dati necessari** per evitare la diffusione del "Coronavirus", evitando domande che "intacchino" la sfera privata dell'interessato e/o le località visitate.

Il Garante elenca i trattamenti che sul luogo di lavoro devono coinvolgere il Medico Competente, la cui centralità in questo periodo è stata fortemente ribadita. In tale contesto, non muta però il principio fondamentale per il quale […] anche laddove il Medico Competente dovesse segnalare al datore di lavoro situazioni di particolare fragilità dei dipendenti, **non deve rivelare le specifiche patologie** occorse agli stessi.

Il Garante ribadisce inoltre che i nominativi dei lavoratori affetti da Covid-19 **non possono essere comunicati** né agli altri dipendenti né al rappresentante dei lavoratori per la sicurezza (RLS). Si tratta di dati che, infatti, possono essere comunicati soltanto alle Autorità Sanitarie Competenti.

LE INSIDIE DEL "WEB" AI TEMPI DEL COVID

L'emergenza sanitaria, porta inevitabilmente molte più persone e per molto più tempo ad essere connesse online e utilizzare dispositivi digitali, esponendo di conseguenza sempre di più gli utenti alle continue insidie della rete. Solitamente quando si parla di attacchi del Web ci si riferisce ai classici virus, ma non sono gli unici pericoli e non sono tutti uguali.

Un virus, in linea di massima, tende ad eseguire poche operazioni ed impiega il minor numero di risorse, in modo da rendersi il più possibile invisibile. I virus informatici più semplici sono composti da due parti essenziali:

1) ricercare i file adatti ad essere infettati;
2) copiare il "codice virale" all'interno di ogni file selezionato perché venga eseguito ogni volta che il file infetto viene aperto, in maniera trasparente rispetto all'utente.

L'ultima frontiera sono i "Ransomware", ovvero programmi maligni che rendono inutilizzabili documenti, archivi, immagini e qualunque altro file. L'operazione è la premessa di una **manovra estorsiva** che si realizza con il rilascio di una "parola chiave" a fronte del pagamento di una determinata somma.

Per difendersi è necessario attenersi scrupolosamente ad alcune precauzioni:

A. Prestare la **massima attenzione** ai contenuti dei messaggi di posta elettronica.

B. Abilitare la visualizzazione delle estensioni in Windows.

C. Limitare l'accesso alle risorse di rete.

D. Fare **copie di backup periodiche** dei dati personali su dispositivi fissi o mobili.

E. Utilizzare un buon sistema antivirus eseguendo **regolari e giornalieri aggiornamenti**.

F. Mantenere aggiornato tutto il software.

G. Se possibile, utilizzare un personal firewall.

> Negli ultimi tempi molte "campagne di *Phishing*" stanno sfruttando l'attenzione rivolta al COVID per diffondere *Malware*, rubare credenziali e truffare gli utenti sottraendo.

Il Centro Nazionale Protezione Infrastrutture Critiche (CNAIPIC) della Polizia Postale e delle Comunicazioni, ha avvisato di recente circa una nuova campagna di *Phishing* e *Malware,* legata all'epidemia. In particolare tramite un **continuo e massivo invio di messaggi Email** e non solo.

Nella circostanza i criminali spacciano la minaccia informatica per **un'applicazione che mostra la mappa della diffusione del virus** nel mondo: la GUI (Graphical User Interface) che risulta particolarmente verosimile a quella "reale".

Il virus, oltre a scaricare ulteriori minacce nei Client colpiti, è in grado di raccogliere informazioni come nome, ID/password, numero della carta di pagamento, cryptovalute e altri "*dati sensibili*" presenti nei Browser (in alcuni casi consentono anche connessioni da Remoto).

Si sottolinea che il *Phishing* rientra nell'ambito della frode informatica, disciplinata dall'art. 640-ter del codice penale (può prevedere fino alla pena della reclusione **da due a sei anni** e della multa **da euro 600 a euro 3.000**), e dall'art. 615-quater sempre del cpdoce penale "detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici", quali password, PIN, Smart card.

Per evitare di rimanere vittime di queste truffe informatiche è necessario innanzitutto sapere che gli Istituti di Credito o le Società che emettono Carte di Credito **non chiedono mai la conferma di dati personali tramite Email**, ma contattano i propri clienti direttamente per tutte le operazioni riservate.

L'esempio classico di *Phishing* è quando un malintenzionato invia milioni di false Email, che SEMBRANO provenire da siti Web noti o fidati (come il sito della propria banca o della società di emissione della carta di credito), ma che invece sono creati "ad hoc" per "prelevare" fraudolentemente le credenziali di accesso delle vittime.

L'APP 'IMMUNI' ALLA PROVA DELLE LINEE GUIDA 4-2020 DELL'EUROPEAN DATA PROTECTION BOARD

Una tabella comparativa per mettere a confronto le cautele/caratteristiche definite per la "APP Immuni", dall'art. 6 ("sistema di allerta Covid-19") del Decreto Legge n. 28 del 30 aprile 2020 con i principali requisiti definiti dall'European Data Protection Board (Comitato europeo per la protezione dei dati) nelle recenti Linee Guida n. 4/2020 sull'uso dei **dati di localizzazione** e degli strumenti per il **tracciamento** dei contatti nel contesto dell'emergenza legata al COVID-19.

Un *'Work in Progress'*, aperto a contributi, al fine di comprendere quali siano o possano essere i punti critici di "Immuni". La pandemia può essere considerata come un involontario, gigantesco "*Test*" per il Governo e per le istituzioni pubbliche interessate, in grado di rivelare al cittadino quanta e quale riserva di cultura garantista.

"Immuni" dovrà convincere, secondo vari e concordi pareri, almeno il 60/70% della popolazione, e per farlo dovrà offrire certezze, garanzie, poiché, come scrive proprio il Comitato Europeo: […] "a nessuno dovrebbe essere chiesto di scegliere tra una risposta efficace all'attuale crisi e la tutela dei diritti fondamentali".

La tabella è composta da n. 2 colonne:

- in quella sinistra sono articolati, in successione, i punti delle Linee Guida (ritenuti) rilevanti per il caso specifico;
- nella colonna destra sono riportati i periodi o commi dell'art. 6 del D.L. 28/2020 e/o considerazioni/appunti circa il suo contenuto, in quanto correlati/correlabili ai contenuti delle Linee Guida a fianco.

Per chi volesse ricevere la suddetta Tabella, al fine di trarre le prime conclusioni, basta inviare una mail/risposta avente ad oggetti:

"IMMUNI" ALLA PROVA DELLE LINEE GUIDA EDPB 4-2020"