APRILE 2020

Autore: MULTIBUSINESS SRL – *"GarantePrivacyItalia"*

Categoria: Economia, lavoro e Pubblica Amministrazione

Sotto-Categoria: Tutela e Protezione Dati Personali - "Privacy"

Norme e prassi: *Regolamento UE 679/2016 – D.Lgs. 196/2003 e ss.mm.ii (D.Lgs. 101/2018)*

Notizia del giorno:

RISCHIA IL PENALE CHI FOTOGRAFA CHI VIOLA I DIVIETI IMPOSTI DAL DPCM E POSTA LE IMMAGINI SUI SOCIAL

Segnalare chi esce di casa sui social network, violando le misure restrittive imposte dal Governo, potrebbe rivelarsi pericoloso. Oltre ad un eventuale risarcimento in sede civile, si rischia di dover rispondere del **reato di diffamazione aggravata** se la "fotografia" è accompagnata da post che etichettano gli interessati come trasgressori che hanno violato le disposizioni anti contagio.

Indice Rassegna:

IL COMUNE DI GRAGNANO METTE ALLA "GOGNA" ON LINE I CITTADINI INDIGENTI

Tra le misure approvate nel periodo dell'emergenza COVID-19, sono stati previsti anche degli aiuti per le famiglie che si trovano in difficoltà economiche.

Il Comune di Gragnano volendo gestire i fondi in maniera **fin troppo trasparente**, il

Sindaco ha disposto la pubblicazione degli elenchi completi di tutti i cittadini che hanno fatto richiesta dei contributi (buoni spesa e generi alimentari/di prima necessità), con tanto di nominativi, specificando altresì la loro data di nascita, includendo inoltre nelle liste non solo i richiedenti ammessi all'agevolazione, ma anche gli altri cittadini non beneficiari dei contributi, **dando così adito all'opinione pubblica**, subito coinvolta attraverso i vari social network.

> *Quanto accaduto dimostra la carente sensibilità per la dignità dei cittadini, nonchè la quasi assente "preparazione" degli Enti locali sulle tematiche del GDPR.*

Infatti, cercando sul sito dell'Ente i riferimenti del Responsabile della Protezione dei Dati/DPO (ricordando che tale figura ha il compito, tra gli altri, di essere punto di contatto per gli interessati che vogliono esercitare i diritti riconosciuti dalla normativa "privacy", nonché adempimento obbligatorio), si riscontra la mancata pubblicazione dei dati di contatto del DPO, a cui i cittadini, come premesso, dovrebbero potersi liberamente rivolgere per esercitare i loro diritti, come appunto il diritto di opporsi alla illegittima pubblicazione delle loro generalità sul sito del Comune e chiedere l'immediata cancellazione.

Ovviamente sarà onere del Garante per la Privacy di verificare l'accaduto e valutare i conseguenti provvedimenti da adottare, ma a prescindere dalle decisioni che assumerà, sta di fatto che quanto accaduto è l'ennesimo caso di P.A. che dimostrano poca attenzione per la normativa relativa ai dati personali, e come in questo periodo di emergenza, gli individui più deboli potrebbero subire conseguenze significative.

UN RANSOMWARE COLPISCE IL COMUNE DI MARENTINO CANCELLANDO I BACKUP DI TUTTI I DATI

Con un comunicato sul proprio sito istituzionale, il Comune di Marentino ha informato tutti gli interessati di aver subito un attacco informatico, di tipo "Ransomware", che, sfruttando il periodo emergenziale causato dall'emergenza sanitaria dovuta al diffondersi del COVID-19, ha violato i dati personali presenti sul server centrale. L'Ente si è prontamente attivato, **procedendo a notificare la violazione subita** (c.d. "Data Breach", adempimento obbligatorio previsto agli artt. 33 e 34 del GDPR) all'Autorità Garante (in Italia il Garante per la protezione dei dati personali)

I dipendenti dell'Ente, una volta collegati all'account istituzionale per svolgere l'attività lavorativa in modalità "Smart Working", si sono accordi di quanto accaduto.

Tecnicamente, gli "Hacker" hanno introdotto un "CryptoLocker" (ovvero un Trojan che infetta i sistemi operativi criptandoli, cioè rendendo i dati incomprensibili se non si possiede la "chiave" per decodificarli), che ha messo fuori uso il sistema per poi cancellare anche il backup dei file, chiedendo un riscatto (prassi ormai "consolidata") in **Bitcoin** (c.d. "criptovaluta", ossia una moneta virtuale) per sbloccare i dati, addirittura prevedendo anche un pagamento "in misura ridotta", dell'ammontare di 50 mila euro, se il pagamento fosse avvenuto entro due giorni, cifra raddoppiata a 100mila euro dopo la scadenza del termine.

APPROPRIAZIONE INDEBITA PER IL DIPENDENTE CHE SI IMPOSSESSA DEI FILE CON I DATI DELL'AZIENDA

Accusato di appropriazione indebita il dipendente che sottrae dal PC aziendale i "files" contenenti dati informatici, provvedendo poi alla cancellazione e restituzione del PC formattato (ossia "svuotato" dei dati).

LA VICENDA

La Corte di cassazione, con la sentenza n. 11959, **respinge il ricorso contro la condanna** per il reato di appropriazione indebita, previsto dall'articolo 646 del Codice penale, a carico dell'imputato.

Il ricorrente, dipendente di una società, aveva dato le sue dimissioni ed era stato assunto da una compagnia costituita di recente, che operava nello stesso settore della precedente.

Prima delle dimissioni l'imputato aveva restituito il notebook aziendale, affidatogli precedentemente nel corso del rapporto di lavoro, con **l'hard disk formattato**, senza traccia dei dati che erano presenti in origine, poi ritrovati su PC da lui utilizzati.

LA NORMATIVA

La difesa (ovvero il dipendente imputato) contestava il verdetto poichè la Corte d'Appello aveva considerato i dati informatici suscettibili di appropriazione indebita, mentre questi non potevano essere qualificati come "cose mobili".

La Cassazione, pur consapevole di orientamenti differenti, **non è d'accordo** con la lettura della difesa. La Suprema corte valorizza la capacità dei file di essere trasferiti da un supporto informatico ad un altro, mantenendo le proprie caratteristiche strutturali, così come la possibilità che lo stesso dato viaggi attraverso internet per essere inviato da un dispositivo ad un altro, anche a distanze rilevanti.

In più il file può essere custodito in ambienti virtuali (c.d. "Cloud"), corrispondenti ai

luoghi fisici in cui gli elaboratori conservano i dati informatici. Caratteristiche che confermano il presupposto della possibilità di sottrarre o appropriarsi dei dati.

Per questo, anche in assenza della apprensione materialmente percepibile del file in sè, questo va considerato una "cosa mobile".