HOT TOPIC (/HOT-TOPIC)

29 Gennaio 2021

Spam e phishing: facciamo il punto della situazione

GIOVANNA BOSCHETTI (/giovanna-boschetti)

Abstract

Spam e phishing sono fenomeni legati all'**invio di comunicazioni commerciali non richieste** che devono essere attentamente valutati alla luce della vigente **normativa in ambito privacy e data protection**, presentando (fatta eccezione per il c.d. "soft spam") fattispecie di illecito trattamento di dati personali con rilevanza civile e penale. Tali fenomeni, in costante aumento in quanto legati allo sviluppo tecnologico, hanno visto un sensibile incremento a seguito dell'**emergenza sanitaria da Covid-19**.

* * *

Spam

Nel linguaggio di internet, per "**spam**" si intende l'**invio di comunicazioni commerciali non richieste**: tale definizione, inizialmente applicata con riferimento alle comunicazioni on line con precipue finalità commerciali (di tipo promozionale o pubblicitario) come definite nel D.Lgs. 70/2003, si è successivamente ampliata sino a ricomprendere ulteriori fattispecie di comunicazioni atte a veicolare la **diffusione di software malevoli e nocivi per computer** tramite la presenza di **link dannosi** o di sistemi di "**furto di credenziali**", assumendo in tal caso la specifica definizione di **phishing**.

Nel vigente sistema di **privacy** e **data protection**, alla luce delle previsioni normative, l'**invio di comunicazioni di carattere commerciale e promozional**e a mezzo posta elettronica è consentito in presenza di un **comprovato consenso, libero e specifico**, che costituisce la base giuridica del trattamento

di dati personali; l'invio di comunicazioni commerciali non richieste a mezzo posta elettronica, difettando dell'elemento del consenso, presenta in sé e per sé i caratteri dell'illiceità ai sensi dell´art. 130, commi 1 e 2, del Codice Privacy (D.Lgs. 196/03, come da ultimo modificato dal D.Lgs. 101/18, di seguito, il "Codice Privacy") e della non conformità al principio di correttezza di cui all´art. 11, comma 1, lett. a), del Codice Privacy con rilevanza civile e penale.

Di fronte alla pratica dello **spam**, nel nostro ordinamento, plurimi sono stati i provvedimenti del Garante della Privacy e numerose le sanzioni amministrative e pecuniarie nei confronti degli operatori che l'hanno posto in essere.

Sul fronte del contenzioso, è peraltro riconosciuto al **destinatario di spam** il **diritto di richiedere anche il risarcimento del danno** derivante da spam, **fornendo prova del danno e della serietà e gravità del pregiudizio subito** (Cassazione civile sez. I, 31/12/2020, n.29982): il pregiudizio, secondo la giurisprudenza di legittimità, non può limitarsi ad un mero "fastidio" nel dover di volta in volta cancellare le e-mail indesiderate, ma deve tradursi in un **pregiudizio concreto**, anche non patrimoniale, ma pur sempre **suscettibile di essere giuridicamente apprezzato** consistente in un pregiudizio effettivo, che si rilevi proporzionato rispetto all'invasività del comportamento di chi invia i contenuti sgraditi, restando magari indifferente ad eventuali richieste di porre termine alla spedizione di una determinata tipologia di messaggi (Cassazione penale sez. III, 20/06/2019, n.41604).

Di fronte allo spam, è necessario effettuare una fondamentale distinzione vigente nel nostro ordinamento tra l'attività di mero spam e quella c.d. di **soft spam**.

Infatti, mentre la pratica dello spam, generalmente intesa, configura una pratica di legittimo trattamento di dati personali, è pienamente lecito il c.d. soft spam previsto all'art. 130 comma 4 del Codice Privacy, che costituisce anzi un'importante risorsa per gli operatori commerciali on line.

L'attività di c.d. soft spam, infatti, secondo il dettato dell'**art. 130 del Codice Privacy** e nei limiti ivi indicati consente l'invio, da parte degli operatori di e-commerce, di comunicazioni promozionali ai propri clienti al fine di pubblicizzare prodotti e/o servizi analoghi a quelli già in precedenza acquistati on line dal cliente anche in assenza di un espresso consenso a tal fine.

Nell'ambito del **soft spam**, pertanto, l'invio di messaggi promozionali può avvenire in **assenza di espresso consenso** del cliente destinatario, fermo restando l'esercizio del diritto di opporsi in ogni momento a tale trattamento che deve essere sempre garantito al destinatario dei messaggi promozionali (sia esso persona fisica o giuridica, in qualità di "contrente" del servizio) mediante la messa a disposizione di strumenti effettivi di tutela.

Phishing

Per "*phishing*" si intende l'attività di invio di email in cui apparentemente un sito web o un istituto finanziario – in generale dotati di un sistema di registrazione per gli utenti mediante l'inserimento di credenziali – invitano l'utente a **fornire i propri dati di accesso**, segnalando problemi principalmente legati al sistema di autenticazione.

Il phishing integra, oltre che una fattispecie di illecito trattamento di dati, la più frequente ipotesi di **truffa realizzata mediante l'uso di Internet** con lo scopo di ingannare gli utenti, richiedendo al destinatario di

inserire i propri dati all'interno di un link che appare collegato ad un sito web affidabile (spesso, ma non esclusivamente, di natura finanziaria) e realizza invece il **reindirizzamento ad un link atto a catturare dati e credenziali informatiche** del destinatario al fine di trarne profitto mediante azioni dirette o richieste di riscatto.

Il *phishing* si configura come anche illecito penale ai sensi degli **articoli 167 e 167 *ter* del Codice Privacy**, i quali rispettivamente puniscono il trattamento illecito dei dati e l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala. Il *phishing* non è tipizzato all'interno del codice penale in una fattispecie, rientrando in più di una fattispecie di reati già previsti: **truffa** (art. 640 c.p.), **frode informatica** (640 *ter* c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615 c.p.), e anche danneggiamento di informazioni e sistemi informatici o telematici (art. 635 *bis, ter, quater e quinquies* c.p.), falsa dichiarazione o attestazione sull'identità o su qualità personali proprie o di altri (art. 495 *bis* c.p.) e persino il cosiddetto "***identity theft***" di cui all'art. 494 c.p.

Sul fronte del contenzioso civile, **le vittime di *phising* hanno diritto ad un risarcimento del danno a titolo extracontrattuale**; la giurisprudenza ha ritenuto di escludere la responsabilità di quelle società o enti che vedono i propri segni distintivi artatamente riprodotti dal *phisher* per trarre in inganno la vittima, qualora tali soggetti possano dimostrare di adottato tutte le idonee misure di sicurezza volte ad evitare l'esposizione dei destinatari a tali truffe.

Il fenomeno, strettamente collegato allo sviluppo tecnologico è, purtroppo, fortemente aggravato dall'emergenza sanitaria da **COVID-19**; nel Report l'ENISA (*European Union Agency for Cybersecurity)* sulle minacce del 2020 dedicato al *phishing* (disponibile all'indirizzo **www.enisa.europa.eu/publications/phishing (https://www.enisa.europa.eu/publications/phishing)**), è evidenziato che gli **attacchi di *phishing* collegati al COVID-19**, rilevati inizialmente alla fine del 2019, **sono aumentati del 667% nel periodo di un mese** (tra la fine di febbraio 2020 e la fine di marzo 2020).

In caso di phishing è sempre consigliata la **denuncia del tentato o avvenuto attacco alle Forze dell'Ordine** (la Polizia Postale ha specifica competenza in merito); nei casi in cui le controversie vedano il coinvolgimento di istituti di credito nei rapporti con i clienti è possibile ricorrere allo strumento di risoluzione delle controversie dell'Arbitro Bancario Finanziario.

Il presente articolo è stato redatto con la collaborazione della Dott.ssa Anna Iorio, Trainee presso CBA Studio Legale e Tributario

Autore dell'articolo:
GIOVANNA BOSCHETTI (/giovanna-boschetti) | Associate senior di CBA Studio Legale e