Privacy

Social marketing e social spam fra diritto alla protezione dei dati personali e casistica concreta

di **Luca Christian Natali**

1. *Il fenomeno del social marketing e del social spam*

Al fine di svolgere un discorso consapevole e corretto, tanto sul piano teorico quanto sul piano concreto, occorre anzitutto definire il concetto di "*social marketing*".

A parte le particolari possibili sfumature semantiche, in sostanza, per "*social marketing*" potremmo convenzionalmente intendere l'attività promozionale veicolata tramite i *social network* cioè l'invio di comunicazioni promozionali effettuato nel contesto del social (per esempio, inviando messaggi promozionali in bacheca o nella chat degli utenti social, oppure (o anche in aggiunta) l'invio di siffatte comunicazioni a dati di contatto (indirizzi e-mail; numeri di telefono) reperiti sui social.

Tale attività di per sé può considerarsi un'attività economica lecita, persino meritevole in ottica di utilità sociale, e comunque, potremmo dire, fisiologica nell'ambito dell'economia di mercato, e tanto più nell'ambito dell'economia digitale, considerate l'economicità e la diffusione del mezzo social. La medesima contribuisce all'attuazione della libertà di circolazione dei dati, che è anch'esso obiettivo fondamentale dell'UE proprio perché rilevante presupposto per lo sviluppo economico.

Tuttavia, il social marketing può trasformarsi in attività "patologica "sotto il profilo privacy, qualora fuoriesca dai binari della normativa in materia di protezione dei dati. Ed è allora, solo allora, che va qualificata come "social spam".

Ferma restando la mancanza di una specifica disciplina dedicata, a tale tipologia di trattamento non può essere applicato troppo rigidamente il Codice privacy (d.lgs. n.196/2003), soprattutto tenendo conto della peculiare funzione dei social network, che sono sinonimo di condivisione **volontaria** e circolazione di idee, conoscenze, foto, contatti, gusti, hobbies, e quindi di numerosi tipi di dati personali.

Con questa espressa consapevolezza, l'Autorità ha provato a dare definizione e disciplina al social marketing, con le ***Linee guida in materia di attività promozionale e contrasto allo spam*, 4 luglio 2013** [doc. web 2542348].

Ebbene, come osserva il Garante, il c.d. "social spam" consiste in un insieme di attività

mediante le quali lo spammer veicola messaggi e link attraverso le reti sociali online.

Un primo grave problema è che spesso tale attività viene svolta al di fuori, e quindi in violazione, dei fondamentali principi di informativa e consenso degli interessati.

Un secondo grave problema è che tali comunicazioni spesso, a dispetto dei contenuti apparentemente commerciali, possono nascondere intenti fraudolenti e truffaldini (v. fenomeni del *phishing*, ossia ..., o dello *smishing,* che è fenomeno analogo al phishing, ma svolto tramite sms), o anche veri e propri tentativi di hackeraggio, mediante *virus i*nformatici e *trojan horses,* destinati a distruggere i sistemi operativi dei destinatari.

Va considerato poi anche un terzo problema: l'indiscriminato e spesso inconsapevole impiego dei propri dati personali da parte degli utenti nell'ambito dei social network, tanto più, come si è già evidenziato, rispetto a profili di tipo "aperto".

Questo impiego si presta alla commercializzazione o ad altri trattamenti dei dati personali a fini di profilazione e marketing da parte di società terze che siano partner commerciali delle società che gestiscono tali siti oppure che “approfittino” della disponibilità di fatto di tali dati in Internet. Inoltre, essendo i social network reti sociali tra persone reali, lo spam in questo caso può mirare a catturare l'elenco dei contatti dell'utente interessato mirato per aumentare la portata virale del messaggio.

Al riguardo, l'Autorità anzitutto ricorda che l'agevole rintracciabilità di dati personali in Internet (quali numeri di telefono o indirizzi di posta elettronica) non autorizza a poter utilizzare tali dati per inviare comunicazioni promozionali automatizzate senza il consenso dei destinatari.

Riguardo a tale tipo di spam, si fa presente che i messaggi promozionali inviati agli utenti dei social network (come Facebook), in privato come pubblicamente sulla loro bacheca virtuale, sono sottoposti alla disciplina del Codice, e, in particolare, agli artt. 3, 11, 13, 23 e 130.

La medesima disciplina – stabilisce il Garante nelle citate Linee Guida - è applicabile ai messaggi promozionali inviati utilizzando strumenti o servizi sempre più diffusi tipo Skype, WhatsApp, Viber, Messanger, etc... Per questi, si ricorda il rischio di proliferazione dello spam dato che, come peraltro indicato nelle relative condizioni di servizio, tali strumenti talora comportano la condivisione indifferenziata di tutti i dati personali presenti negli *smart-phone* e nei *tablet* (quali rubrica, contatti, sms, dati della navigazione internet) o comunque la possibilità di accesso della società che li fornisce alla lista dei contatti e-mail o alla rubrica presente sul telefono mobile dell'utente per reperire e/o conservare tali dati personali.

Per gli utenti il rischio di ricevere spam, e in particolare il c.d. "spam mirato", basato sulla profilazione dei dati disponibili *on line*, è senz'altro aggravato dalla diffusione di piattaforme tecnologiche che prevedono l'integrazione dei diversi servizi resi (nonché dei relativi profili) consentendo ai loro gestori di pervenire ad una conoscenza sempre più approfondita ed

analitica degli utenti, a cui indirizzare messaggi diversificati sulla base dei gusti rilevabili su molteplici applicazioni.

Se da una parte questa nuova pratica può agevolare il rapporto commerciale tra produttore e consumatore, riducendo per il primo i costi di marketing e per il secondo i costi di ricerca del prodotto, tuttavia può causare all'interessato che viene profilato a dispetto della sua volontà, o perlomeno senza adeguata consapevolezza, oltre alla ricezione dello spam, anche la compressione della sua libertà di fruizione dei servizi della società dell'informazione.

Ciò premesso, ferma restando la liceità dei messaggi a scopo meramente personale, si possono individuare – secondo l'Autorità Garante - **alcune ipotesi** paradigmatiche.

Una **prima ipotesi** è quella in cui l'utente riceva, in privato, in bacheca o nel suo indirizzo di posta e-mail collegato al suo profilo social, un determinato messaggio promozionale relativo a uno specifico prodotto o servizio da un'impresa che abbia tratto i dati personali del destinatario dal profilo del social network al quale egli è iscritto.

Una **seconda ipotesi**, individuata nelle menzionate Linee Guida, è quella in cui l'utente sia diventato "fan" della pagina di una determinata impresa o società oppure si sia iscritto a un "gruppo" di follower di un determinato marchio, personaggio, prodotto o servizio (decidendo così di "seguirne" le relative vicende, novità o commenti) e successivamente riceva messaggi pubblicitari concernenti i suddetti elementi.

Orbene vediamo ora la disciplina applicabile il Garante.

Nel primo caso – osserva l'Autorità - il trattamento sarà da considerarsi illecito, a meno che il mittente non dimostri di aver acquisito dall'interessato un suo consenso preventivo, specifico, libero e documentato ai sensi dell'art. 130, commi 1 e 2, del Codice.

Nel secondo caso, l'invio di una comunicazione promozionale riguardante un determinato marchio, prodotto o servizio, effettuato dall'impresa a cui fa riferimento la relativa pagina, può considerarsi lecita se dal contesto o dalle modalità di funzionamento del *social network*, anche sulla base delle informazioni fornite, può evincersi **in modo inequivocabile** che l'interessato abbia in tal modo voluto manifestare anche la volontà di fornire il proprio consenso alla ricezione di messaggi promozionali da parte di quella determinata impresa.

Occorre fin d'ora osservare come tale disciplina individuata dal Garante risulti compatibile, anzi in armonia, con il dettato del Regolamento generale europeo di cui si dirà di seguito (v. para. 3), che evidenzia, per poter configurare il valido consenso degli interessati, la necessità di una inequivocabile manifestazione di volontà.

Riprendendo il citato caso (secondo), tuttavia, se invece l'interessato si cancella dal gruppo, oppure smette di "seguire" quel marchio o quel personaggio, o comunque si oppone ad eventuali ulteriori comunicazioni promozionali, il successivo invio di messaggi promozionali

sarà illecito, con le relative conseguenze sanzionatorie. Come ricorda il Garante, comunque resta salva la possibilità, talora fornita dai *social network* ai loro utenti, di bloccare l'invio di messaggi da parte di un determinato "contatto" o di segnalare quest'ultimo come *spammer*.

In base a quanto ricordato dal Garante, nell'ipotesi dei "contatti" (i c.d. "amici") dell'utente, dei quali spesso nei social network o nelle comunità degli iscritti ai servizi di cui sopra, sono visualizzabili numeri di telefono o indirizzi di posta elettronica, l'impresa o società che intenda inviare legittimamente messaggi promozionali dovrà aver previamente acquisito, per ciascun "contatto" o "amico", un consenso specifico per l'attività promozionale.

2. *Caso pratico di social marketing: provvedimento del 21 settembre 2017.*

In tema di social marketing, emerge lo specifico **provvedimento adottato il 21 settembre 2017** nei confronti di una società operante nell'ambito dei servizi *on line* [doc. web n. 7221917], con il quale il Garante ha affrontato una delle prime istruttorie riguardanti anzitutto il fenomeno del social marketing. Nell'occasione, l'Autorità ha evidenziato che, se un indirizzo e-mail è presente su un social network, ciò non significa che possa essere utilizzato liberamente per qualsiasi scopo, poiché, per inviare proposte commerciali, è sempre necessario il consenso dei destinatari.

L'intervento del Garante ha preso spunto da un'articolata segnalazione di una società di consulenza finanziaria, lamentante l'invio di numerose e-mail promozionali indirizzate alle caselle di posta elettronica di alcuni suoi promotori senza che questi avessero dato alcun consenso al trattamento dei loro dati.

Dagli accertamenti, svolti presso la società dall'Autorità in collaborazione con il Nucleo Speciale Privacy della GdF, è emerso che la raccolta degli indirizzi di posta elettronica per l'invio delle proprie comunicazioni promozionali avveniva anche attraverso i social, quali in particolare Linkedin, ove la società sanzionata è risultata avere fra i propri contatti alcuni intermediari finanziari della società segnalante.

Il Garante, anche sulla base delle Linee guida del 4 luglio 2013 che hanno disciplinato in via generale, fra i vari aspetti di protezione dei dati, anche il fenomeno del "social spam", ha quindi ritenuto illecito il trattamento degli indirizzi di posta elettronica. Infatti, come statuito nel provvedimento in questione, i dati reperiti sui *social network* e, più in generale, presenti *on line*, non possono essere utilizzati liberamente, a pena di violazione, anzitutto, dei principi di finalità e liceità del trattamento (potremmo aggiungere).

Non è stata ritenuta la tesi sostenuta dalla società secondo la quale l'iscrizione a un *social network* implica un consenso all'utilizzo dei dati personali per l'attività di marketing. Tale finalità non è stata ritenuta compatibile con le funzioni, potremmo dire naturali e tipiche dei social network che sono preordinate alla condivisione di informazioni e allo sviluppo di contatti professionali, e non alla commercializzazione di prodotti e servizi. Tesi peraltro affermata anche dal Gruppo ex art. 29, secondo il quale l'iscrizione a un servizio presente sul

web non comporta la legittimità del trattamento dei dati personali da parte di altri partecipanti alla medesima piattaforma ai fini dell'invio di informazioni commerciali.

Oltre alla contestazione amministrativa già effettuata dal Nucleo Speciale per il trattamento senza il necessario consenso, l'Autorità si è riservata di contestare, alla società autrice delle comunicazioni promozionali indesiderate, anche la violazione dell´obbligo di rilascio dell´informativa. Alla medesima società è stato anche prescritto di modificare il modello di richiesta di consenso presente sul sito, in modo che risulti chiaro lo svolgimento di finalità promozionali.

3. *La necessaria valorizzazione dei nuovi principi del regolamento UE anche nel settore e-privacy*

Con riferimento alle comunicazioni elettroniche, e in particolare a trattamenti potenzialmente notevolmente invasivi, come quelli svolti mediante i *social network*, è senz'altro auspicabile l'espressa valorizzazione - anche nel regolamento *e-privacy* in corso di definizione al quale è demandato il compito di ridisciplinare il settore in questione - di alcuni principi individuati già dal nuovo Regolamento UE, come peraltro quest'ultimo auspica espressamente[1].

Non va trascurato che, a nuova concezione di privacy, sempre più ricca di diritti e facoltà di vario contenuto a favore del lavoratore interessato (si pensi ai nuovi diritti all'*oblio* e alla *portabilità* dei dati), dovrebbe (*rectius:* deve) corrispondere, simmetricamente, una diversa posizione giuridica in capo ai *data controller*, che si deve necessariamente arricchire e rafforzare di nuovi obblighi e responsabilità.

In questo senso, dovrebbero stabilirsi espressamente anche con riferimento alle comunicazioni elettroniche i nuovi principi, quali quello di *accountability*, ossia il principio di "autoresponsabilità" dei *data controller*, che, come è stato definito da autorevole dottrina (Modugno), è la "capacità di render conto" degli adempimenti e dei controlli in materia, anche tramite la relativa necessaria documentazione, prima ancora e a prescindere da un'eventuale (successiva) attività di controllo da parte del Garante;

Inoltre, proprio in base all'applicazione di tali principi, a partire da quello di *accountability*, e per espressa previsione del regolamento generale europeo con riguardo alla generalità dei titolari del trattamento, non sarà più possibile limitarsi ad adottare misure minime di sicurezza, prestabilite dal legislatore nazionale in un apposito testo tecnico (qual è famigerato allegato B al Codice anche in base all'art. 33 del medesimo), ma occorrerà, indefettibilmente, **adottare tutte le misure idonee da individuarsi in base alla previa valutazione da effettuarsi, caso per caso, in rapporto ai rischi specificamente individuati**[2], con la possibilità, tuttavia, di ricorrere all'adesione a specifici codici di condotta oppure a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate[3].

Tuttavia, occorre, al contempo, ricordare quale sia l'ambito oggettivo del GDPR, dal quale risulta escluso il settore delle comunicazioni elettroniche in vista dell'approvazione di una

specifica disciplina di settore, la futura "*direttiva e-privacy*", per i citati trattamenti di dati personali nell'ambito dei *social network).* Nelle more, per tale trattamento di dati, la normativa europea di riferimento rimane la direttiva 2002/58/UE, con le sue successive modifiche. Conseguentemente, parte del Codice (titolo X " comunicazioni elettroniche": art. 121 ss.) e del *corpus* provvedimentale del Garante - incluse, solo ad esempio, le Linee Guida per posta elettronica e internet del 10 marzo 2007 [doc. web n. 1387522] e le menzionate Linee Guida in materia di spam - attenendo al settore della comunicazioni elettroniche e non risultando incompatibile con la disciplina eurounitaria, parrebbe ancora vitale, anche a seguito (dal 25 maggio scorso) della piena operatività della disciplina eurounitaria.

Al contempo, tuttavia, si può ritenere necessario implementare, sulla base di tale generale modello europeo, alcuni fondamentali adempimenti, quali quelli dell'informativa e del consenso. Sicché l'informativa resa agli utenti dei SSN dovrà contenere, tassativamente, tutti gli elementi dell'art. 13 GDPR (compresi i riferimenti al diritto alla portabilità; al diritto di reclamo presso il Garante e all'Autorità giudiziaria; ai tempi di conservazione dei dati raccolti). Inoltre, il consenso al trattamento dovrà essere acquisito con formulazione "inequivocabile", vale a dire con una manifestazione di volontà chiara, certo ed oggettivo, e dovrà essere documentato (o documentabile), in armonia con il menzionato fondamentale obbligo di *accountability*.

[1]Cfr. considerando 173.

[2]come previsto dall'art. 32 GDPR.

[3] Tuttavia, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.