INVII DI E-MAIL PROMOZIONALI AI CLIENTI "NON PAGANTI": IL *SOFT SPAM* AL VAGLIO DELLA CORTE DI CASSAZIONE

Nota a Cass. 15 marzo 2023, n. 7555

Di Lavinia Vizzoni

SOMMARIO*: 1. Prova gratuita di un servizio online e ricezione di e-mail promozionali. - 2. La Cassazione sul soft spam. - 3. La disciplina delle comunicazioni indesiderate fra presente e futuro. - 4. Il soft spam fra consenso e contratto. - 5. Cassazione e spammming: uno sguardo al versante risarcitorio*

ABSTRACT. Il commento ha ad oggetto una recente pronuncia della Corte di Cassazione in materia di spamming. Che conferma la sanzione irrogata dal Garante per la protezione dei dati personali alla società ricorrente. Quest'ultima offriva un servizio online di comparazione di preventivi e inviava e-mail a contenuto promozionale a tutti gli utenti che si registravano sul proprio sito compilando il relativo form, inclusi coloro che si avvalevano della mera prova gratuita del servizio. La Corte di Cassazione, nelle proprie argomentazioni, pur manifestando una certa sovrapposizione fra il consenso e la distinta ipotesi di cui all'art. 130, c. 4 codice privacy, offre una disamina dei contenuti e dei limiti del c.d. soft spam. Il commento evidenzia luci ed ombre della pronuncia, e ipotizza qualche scenario futuro, prendendo infine in esame anche le ultime decisioni di legittimità in tema di risarcimento del danno da ricezione di comunicazioni indesiderate.

The paper deals with a recent decision by the Court of Cassation on spamming, which confirms the sanction imposed by the Data Protection Authority on the plaintiff company. The latter offered an online service of comparing quotes and sent e-mails with promotional content to all users who registered on its website by filling out a form, including those who benefitted of the mere free trial of the service. The Court of Cassation, in its arguments, while manifesting a certain overlap between consent and the distinct situation of Art. 130, c. 4, "Privacy Code", offers an examination of the contents and limits of the so-called soft spam. The paper investigates lights and shadows of the decision and imagines some future scenarios, finally also analyzing the latest decisions on damage compensation for spamming.

1. Prova gratuita di un servizio *online* e ricezione di e-mail promozionali

In un momento storico in cui l'avvento massiccio delle tecnologie digitali ha reso le comunicazioni indesiderate un fenomeno sempre più diffuso – con correlativa intrusione nelle vite personali degli interessati – la Cassazione ha pronunciato una sentenza in tema di *spamming*, la quale va ad unirsi al novero, per vero non particolarmente consistente, delle decisioni in materia[1]. Peraltro, la pronuncia in esame riveste un sicuro rilievo poiché si colloca tra quelle, ancora meno numerose, che si occupano non già del profilo risarcitorio, ma solo della configurazione della pratica illegittima dello *spam*[2], risultando la prima pronuncia – a quanto consta – emessa sul c.d. *soft spam*. Per di più, pur facendo applicazione, *ratione temporis*, della normativa precedente l'emanazione del Regolamento UE 679/2016, "GDPR", le affermazioni in essa contenute conservano piena attualità, avendo riguardato specificamente, come si dirà subito, una norma non modificata dal d.lg. 101/2018.

Nel caso di specie, una società, previa registrazione degli utenti sul relativo sito tramite compilazione di un apposito *form*, forniva un servizio *online* di comparazione di preventivi. La società risultava destinataria di un accertamento *ex* art. 157 del d.l.gs. 196/2003 (codice *privacy*, nel testo non ancora novellato), dal quale emergeva che la stessa aveva trattato, sul proprio sito internet, dati personali di utenti-clienti e non, senza acquisire il consenso degli interessati liberamente e specificamente previsto in relazione ad un trattamento chiaramente individuato, consistente, in questo caso, nella finalità di *marketing*. La società è stata dunque destinataria di un successivo provvedimento del Garante per la protezione dei dati personali del 2015, con il quale le è stata irrogata una sanzione pecuniaria, e contro il quale la stessa ha proposto opposizione innanzi all'autorità giudiziaria. Il Tribunale competente (di Trani) si è allineato alla ricostruzione del Garante, non ritenendo applicabile nel caso di specie l'art. 130, comma 4 del codice privacy, sul quale la società opponente aveva incentrato la propria linea difensiva, e ha rigettato l'opposizione.

La società in questione ha infine presentato ricorso per cassazione avverso la sentenza del giudice di prime cure, basando le sue doglianze sull'errata interpretazione proprio dell'art. 130, comma 4 del codice *privacy*. Secondo la ricorrente, tale previsione derogherebbe infatti al sistema del preventivo consenso dell'interessato (c.d. "*opt in*"), nell'ipotesi in cui sia "i clienti a pagamento" sia i "clienti non paganti" instaurino un rapporto con la società, richiedendo il suo servizio di comparazione di preventivi.

In particolare siffatta eccezione sarebbe applicabile, a parere della ricorrente, anche agli utenti che non avessero acquisito la qualifica di clienti in senso stretto, ossia a coloro che avessero effettuato solo la registrazione sul sito, compilando il relativo *form* per poter fruire del servizio, senza però concludere alcun contratto, o meglio inquadrandosi nell'ambito di quello che la società ricorrente qualifica come "contratto di prova del servizio": tali utenti venivano infatti poi raggiunti da comunicazioni promozionali inviate via e-mail.

L'ambito applicativo della deroga *ex* art. 130, c. 4 codice *privacy* si estenderebbe, quindi, secondo la prospettazione della ricorrente «a tutti i soggetti che, a titolo gratuito o oneroso, siano destinatari del servizio offerto», sempre che le e-mail inviate all'indirizzo fornito in sede di registrazione riguardassero prodotti analoghi a quelli già offerti ai clienti.

Inoltre, la società ha evidenziato come la stessa avesse fornito un'adeguata informativa in materia di trattamento dei dati personali sia nella comunicazione iniziale sia in quelle successive, anche al fine di rendere il destinatario edotto circa la possibilità di opporsi in ogni momento alla ricezione delle comunicazioni.

Sarebbe dunque da disattendere la soluzione adottata dal Tribunale del merito, il quale aveva ribadito la sussistenza di un obbligo di acquisizione del previo consenso al trattamento dei dati per finalità commerciali ogniqualvolta si utilizzi un sistema automatizzato per l'invio delle comunicazioni di *marketing*.

2. La Cassazione sul *soft spam*

La Corte di Cassazione ha rigettato il ricorso, confermando la decisione del Tribunale e così la correttezza del provvedimento del Garante.

[1] Il testo di Cass. 15 marzo 2023, n.7555 è pubblicato nella banca dati *dejure* e la decisione è massimata in *Giust. civ. Massimario*, 2023.

[2] Uno dei pochi precedenti in materia è piuttosto recente: si tratta di Cass. 26 aprile 2021, n. 11019, ord., in *Nuova giur. civ.*, 2021, 1064 ss., con nota di F. IRACI GAMBAZZA, F. LAVIOLA, *Finalità di marketing e consenso: profili in evoluzione*. Con tale pronuncia la Cassazione ha sancito che contattare telefonicamente chi ha precedentemente negato il consenso rappresenta una comunicazione commerciale. In sostanza, il trattamento dei dati dell'interessato per chiedere il consenso per fini di *marketing* deve considerarsi anch'esso un trattamento per finalità di *marketing*.

In primo luogo, come già osservato correttamente dal Tribunale, il giudice di legittimità rileva che il *form* di raccolta dati inserito dalla società ricorrente nel proprio sito Internet era privo del consenso necessario per il trattamento di *mailing marketing*, in contrasto con l'art. 23 codice *privacy*, che prevede l'obbligo di prestare il consenso per un trattamento di dati chiaramente individuato.

La decisione opera un'attenta disamina dei contenuti dell'art. 130, con particolare riferimento al comma 4, qui al centro del contrasto fra Garante e società sanzionata.

In primis, la Corte ricorda come l'art. 130 al comma 1 prevede che «l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso del contraente o utente», richiedendo quindi il rilascio del consenso per l'invio di qualunque comunicazione commerciale.

La disciplina nazionale – ricorda la Suprema Corte – costituisce attuazione della Direttiva *e-privacy* 2002/58/CE, la cui finalità è quella di «evitare l'utilizzo surrettizio di mezzi rivolti all'attività di marketing nonostante la mancanza di consensi esplicitamente, e anteriormente, non rilasciati dai soggetti interessati». Soprattutto, «I punti 40 e 41 del Considerando della Direttiva evidenziano la necessità di tutelare gli abbonati da interferenze nella loro vita privata mediante comunicazioni indesiderate a scopo di commercializzazione diretta (...)». E il comma 2 della disposizione estende l'ambito applicativo del consenso preventivo anche «alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo».

In particolare, la disciplina nazionale rappresenta una riproduzione fedele dell'art. 13 della Direttiva *e-privacy*, secondo la quale «l'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta elettronica a fini di commercializzazione diretta è consentito soltanto nei confronti degli abbonati che abbiano espresso preliminarmente il loro consenso».

Precisato ciò, la Cassazione ha rammentato come la sua stessa giurisprudenza abbia chiarito nei suoi precedenti arresti che ogni consenso all'invio di comunicazioni commerciali è valido solo a condizione che sia prestato liberamente e specificamente in relazione ad un trattamento precipuamente individuato[3].

La previsione della tecnica di *opt-in ex* art. 130, c. 1, è dunque una «regola di ordine generale, in ragione della quale il previo consenso del contraente o utente risulta indispensabile per l'invio da parte del titolare di materiale pubblicitario o di comunicazione commerciale mediante l'uso di sistemi automatizzati».

Il comma 4 introduce un'eccezione rispetto alla regola generale di cui al comma 1, relativa all'ipotesi in cui il titolare del trattamento abbia ottenuto gli indirizzi di posta elettronica degli interessati[4] nel contesto della vendita di un prodotto. In questo caso gli è consentito utilizzare tali indirizzi a scopi di commercializzazione diretta di propri analoghi prodotti o servizi, sempre che il cliente non abbia esercitato la c.d. facoltà di *opt-out* rifiutando inizialmente tale uso e che, al momento della raccolta degli indirizzi e-mail, agli interessati sia data adeguata possibilità di opporsi ad ulteriori rinvii.

La necessità di ottenere un consenso dell'interessato ai fini dell'invio di comunicazioni commerciali è esclusa – ribadisce la pronuncia – solo se le coordinate di posta elettronica sono state acquisite dal titolare del trattamento «nel contesto della vendita di un prodotto o di un servizio»: se ne ricava *in primis* l'estromissione, dall'ambito di applicazione dell'eccezione di cui al comma 4, di tutte le situazioni in cui tale acquisizione sia avvenuta in modo e per finalità diverse.

La decisione precisa che il termine "vendita" deve essere inteso in senso strettamente tecnico, tale

[3] Così Cass., 2 luglio 2018, n. 17278, in *Nuova giur. civ.*, 2018, 1775 ss., con nota di F. ZANOVELLO, *Consenso libero e specifico alle email promozionali*, e in *Giur. it.*, 2019, 530 ss., con nota di S. THOBANI, *Operazioni di tying e libertà del consenso* e Cass. 25 maggio 2021, n. 14381, in *Dir. inf. informatica*, 2021, 1005 ss., con nota di F. BRAVO, *Rating reputazionale e trasparenza dell'algoritmo. Il caso «Mevaluate»*.

[4] Si deve notare che la nozione di "interessato" del comma 4 esclude dal suo ambito di applicazione le persone giuridiche o altri enti non personificati, quando la nozione di "contraente o utente", impiegata nel comma 1 dell'art. 130, in forza dell'entrata in vigore del d.lg. n. 69/2012, a far data dal 1° giugno 2012, ha sostituito, nelle disposizioni del Codice, quello di "abbonato", utilizzato in precedenza, certamente applicabile tanto alle persone fisiche quanto a quelle giuridiche: in tal senso, cfr. il considerando 12 della menzionata direttiva 2002/58/CE, secondo il quale «gli abbonati ad un servizio di comunicazione elettronica accessibile al pubblico possono essere persone fisiche o persone giuridiche». In argomento cfr. il provvedimento del Garante per la protezione dei dati personali in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011 del 20 settembre 2012.

da richiedere l'instaurazione di un rapporto contrattuale a titolo oneroso tra titolare del trattamento e destinatario delle comunicazioni, nel corso del quale il secondo ha fornito il proprio indirizzo e-mail, e sempre che oggetto dell'invio pubblicitario siano servizi analoghi a quelli oggetto della vendita, ferma restando la possibilità, che deve essere garantita al destinatario, di opporsi a successivi invii.

Per concludere, a detta della Suprema Corte è da confermare la decisione del tribunale, che ha fatto corretta applicazione dell'art. 130 codice *privacy*, dal momento che, da una parte nel *form* di raccolta dati della società opponente mancava il consenso per il trattamento di *mailing marketing* e, dall'altra parte venivano illegittimamente utilizzate le coordinate di posta elettronica dei clienti che avevano effettuato la semplice prova del servizio, senza concludere alcun contratto con la società.

Il comma 4 dell'art. 130 del Codice Privacy può trovare applicazione, secondo la decisione, ai soli "clienti paganti", ossia ai clienti che abbiano concluso un contratto di vendita e, in tale occasione abbiano fornito le proprie coordinate di posta elettronica, e non anche ai "clienti non paganti", ovvero coloro che si siano solamente registrati o abbiano effettuato una prova del servizio. Non è pertanto sufficiente che l'utente del sito manifesti un interesse verso il servizio offerto dalla società opponente attraverso la registrazione per far scattare la deroga in questione.

3. La disciplina delle comunicazioni indesiderate fra presente e futuro

La questione affrontata dalla pronuncia in commento attiene alla legittimità e ai limiti del c.d. *soft spam*, ossia l'invio di comunicazioni commerciali nei confronti di clienti, dei cui indirizzi e-mail il titolare del trattamento sia già in possesso in virtù dell'instaurazione di un precedente rapporto contrattuale.

A monte, si osserva che di fronte all'invio di comunicazioni commerciali non richieste, il primo quesito che si pone riguarda proprio la tecnica da adottare in risposta a tale fenomeno[5]. L'alternativa di fondo risiede nella scelta fra *opt-in* e *opt-out*, fra necessità di consenso preventivo e possibilità di opporsi a posteriori all'invio non sollecitato.

L'art. 130 sembra optare per la prima delle due modalità: d'altronde la norma si apre proprio con la proclamazione della necessità del consenso del contraente o utente. Come evidenziato, non mancano però indici di una vera e propria ''erosione'' a cui la regola del consenso preventivo va incontro[6]. Fra questi, anche a tacere dell'art. 9 d.lg. 70/2003 - che in materia di commercio elettronico adotta una soluzione diametralmente opposta[7] - non possono non considerarsi i commi 3-*bis* (questo per vero non presente nella formulazione originaria dell'art. 130, ma inserito dal d. lgs. 135/1999, convertito dalla l. 166/2009) e 4 dello stesso art. 130, i quali prevedono essi stessi ipotesi di *opt-out*, seppur condizionate a precisi presupposti[8].

Nel primo caso, il trattamento dei dati personali per finalità commerciale effettuato esclusivamente mediante l'uso del telefono o della posta cartacea è consentito senza consenso nei confronti di chi non

[5] In materia di *spamming* v. F. Di Ciommo, *Commento all'art. 130*, in F. D. Busnelli, C. M. Bianca (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 «Codice della privacy»*, Padova, 2007, 1570 ss. e C. Rinaldo, *Le comunicazioni commerciali non sollecitate tra libertà di impresa e diritto alla tranquillità individuale*, in *Nuove leggi civ*, 2013, 653 ss. Sia inoltre consentito rinviare a L. Vizzoni, *Sub art. 130*, in R. Sciaudone, E. Caravà, (a cura di), *Il codice della privacy. Commento al D. Lgs. 30 giugno 2003, n. 196 e al D. Lgs. 10 agosto 2018 n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, 2019, 636 ss.
Più in generale, in tema di *marketing* e comunicazioni elettroniche cfr. M. Massimi, *Quali orizzonti per il marketing?* in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Ccommentario al regolamento UE n. 2016/679 e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Milano, 2019, 483 ss., G. Scorza, *Prospettive de iure condendo della protezione dei dati personali nel settore delle comunicazioni elettroniche, tra Regolamento generale 2016/679 e futuro Regolamento e-Privacy*, in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 741 ss., A. Mantovani, *Questioni relative al trattamento dei dati personali per finalità di marketing e profilazione*, in *MediaLaws*, 2019, 1 ss.

[6] Cfr. S. Fadda, *Commento all'art. 130*, in G. Cassano, S. Fadda (a cura di), *Codice in materia di protezione dei dati personali. Commento articolo per articolo al Testo Unico sulla Privacy*, Milano, 2004, 593 ss.

[7] Vi è tuttavia chi non ravvisa sostanziali contrasti fra art. 9 del dlg. 70/2003 e art. 130 codice *privacy*, ritenendoli entrambi espressione del principio dell'*opt-in*. Così F. Di Ciommo, *op. cit.*, 1577, anche n. 15. L'A. evidenzia come l'*opt-in* sia la soluzione da tempo prescelta dall'ordinamento italiano e ricorda che già in occasione dell'emanazione della direttiva 2000/31/CE, il Garante pose in luce, in un parere sullo schema di decreto attuativo richiesto dalla Presidenza del Consiglio dei Ministri, che l'Italia aveva già in precedenza aderito al principio del consenso preventivo. Cfr. *E-commerce: niente registri inutili*, newsletter 28 ottobre-3 novembre 2002, doc. web n. 41314. Sul parere negativo del Garante, si v. anche A. Stazi, *La disciplina delle comunicazioni elettroniche non richieste alla luce del D.lgs. n. 70/2003 sul commercio elettronico e del nuovo ''codice in materia di protezione dei dati personali''*, in *Dir. inf. informatica*, 2003, 1102.

[8] Con precipuo riguardo al *soft spam*, v. M. Massimi, *op. cit.*, 500 ss.

abbia manifestato il proprio dissenso attraverso l'iscrizione nel registro pubblico delle opposizioni; nel secondo caso – che viene in rilievo nella decisione in esame – si può prescindere dal consenso sempre che la modalità di trasmissione delle comunicazioni sia esclusivamente la posta elettronica, che le coordinate di posta elettronica siano quelle fornite nel contesto della vendita di un prodotto o di un servizio, che si tratti di messaggi inviati a fini di vendita diretta di prodotti e/o servizi forniti dal titolare del trattamento sempre che si tratti di servizi analoghi a quelli oggetto della vendita e che l'interessato, adeguatamente informato, non rifiuti tale uso inizialmente o in occasione di successive comunicazioni e possa «opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente».

In effetti, la stessa aggiunta del comma 3 *ter* all'art. 130, e a maggior ragione il recente rafforzamento del registro delle opposizioni[9], collide - almeno ad una prima analisi - con il meccanismo dell'*opt-in*, essendo invece strumento tipico di un sistema di *opt-out*.

D'altronde, il GDPR stesso sembra orientarsi verso una soluzione conforme all'*opt-out*: l'art. 21, comma 2[10] detta una disposizione analoga a quella che era contenuta nell'abrogato art. 7 del codice *privacy* (lettera b), con l'aggiunta del riferimento alla profilazione, e l'esemplificazione contenuta nel noto ultimo inciso del considerando 47 («[p]uò essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto») depone a favore di una (criticata) sostituzione del legittimo interesse al consenso quale base giuridica del trattamento effettuato per finalità di *marketing*.

La materia appare peraltro destinata a ulteriori sviluppi in vista della futura approvazione del Regolamento *e-privacy*, che sostituirà la Direttiva e-*privacy*, di cui, come ricordato dalla stessa sentenza in esame, l'art. 130 del codice *privacy* costituisce attuazione[11].

È pur vero che la situazione appare ormai stagnante da un po' di anni, e il futuro Regolamento sembra ancora lontano dal vedere la luce, ma la bozza di Regolamento *e-privacy* su cui è stato raggiunto l'accordo in seno al Consiglio dell'Unione Europea il 10 febbraio 2021 ha da un lato confermato alcuni principi già espressi dalla Direttiva *e-privacy* in tema di *direct marketing*, dall'altro lato ha introdotto alcune innovazioni[12].

Fermo restando l'obbligo del consenso preventivo (art. 16, comma 1, bozza di Regolamento), esso non rimane circoscritto al caso di utilizzo di sistemi automatizzati di chiamata e di comunicazione senza intervento di un operatore, del telefax o dell'e-mail, come nella Direttiva *e-privacy*, bensì si estende anche ad ulteriori ipotesi[13].

Viene inoltre fatta salva (art. 16, comma 4) la possibilità per gli Stati Membri di introdurre un regime di *opt-out* per le chiamate V2V, in base al

[9] Di recente, il percorso di costruzione del nuovo registro delle opposizioni si è completato con il D.P.R. del 27 gennaio 2022, n. 26, che ha infine reso operativo il registro pubblico delle opposizioni (RPO). Si è così concretizza la già ricordata possibilità di iscrivere al registro anche i numeri di telefono cellulare, con conseguente revoca dei consensi precedentemente rilasciati all'utilizzo dei dati personali da parte degli operatori di telemarketing, i quali dovranno dunque consultare il registro periodicamente, o comunque prima dell'avvio di iniziative pubblicitarie. La chiamata verso un numero iscritto nel registro è possibile solo a condizione che l'operatore abbia ottenuto uno specifico consenso al trattamento dei dati successivamente alla data di iscrizione, oppure nell'ambito di un rapporto contrattuale in essere o conclusosi da non più di trenta giorni. Restano in ogni caso valide tutte le iscrizioni inserite precedentemente all'operatività del nuovo RPO. In tal proposito, si veda il Regolamento recante disposizioni in materia di istituzione e funzionamento del registro pubblico dei contraenti che si oppongono all'utilizzo dei propri dati personali e del proprio numero telefonico per vendite o promozioni commerciali, ai sensi dell'articolo 1, comma 15, della legge 11 gennaio 2018, n. 5.

[10] Secondo tale previsione «Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto». L'opposizione è caratteristica dei sistemi di *opt-out*.

[11] Sulle novità della proposta di Regolamento e-privacy, cfr. E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice Privacy*, in E TOSI, (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, 41 ss., e L. BOLOGNINI, C. BISTOLFI, G. CREA, *Il Regolamento e-Privacy tra principi giuridici e impatti sull'economia digitale*, Istituto Italiano per la *privacy* e la valorizzazione dei dati, 2018. Sul Regolamento e-privacy, sia inoltre permesso rinviare a L. VIZZONI, *Domotica e diritto. La Smart Home tra regole e responsabilità*, Milano, 2021, 90 ss.

[12] Cfr. F. GIULIANI, M. LEFFI, G. VECCHI, *La disciplina prevista dall'ultima bozza di Regolamento ePrivacy e un confronto con la normativa vigente in materia di marketing*, in *www.agendadigitale.eu*, 9 giugno 2021.

[13] Tale obbligo si estende ai c.d. servizi di comunicazione interpersonale indipendenti dal numero, quali i servizi di messagistica Over-The-Top ("OTT"). Ciò, in ragione del richiamo, contenuto nella nella bozza di Regolamento, alla definizione che di tali servizi dà il Codice europeo delle Comunicazioni Elettroniche, Direttiva UE 2018/1972, e alle c.d. "voice-to-voice calls", ossia le chiamate "in diretta" con operatore e, quindi, senza utilizzo di dispositivi automatici di chiamata e comunicazione ("Chiamate V2V"). Sul punto v. F. Giuliani, M. Leffi, G. Vecchi, *op. cit*.
Si ricorda che il Codice europeo delle Comunicazioni Elettroniche ha trovato attuazione solo con il d.lg. 8 novembre 2021, n. 207, entrato in vigore il 24 dicembre 2021, oltre il termine ultimo del 21 dicembre 2020 stabilito dalla Direttiva 2018/1972: motivo per il quale l'Italia è stata oggetto di una procedura di infrazione (infrazione INFR (2021)0056) da parte della Commissione Europea.

quale le chiamate per finalità di *marketing* potranno essere effettuate solo nei confronti degli utenti che non si siano opposti al trattamento per tali finalità. In tale meccanismo ben si ascriverebbe il Registro delle opposizioni italiano.

L'obbligo del consenso preventivo non troverà invece applicazione in relazione alle forme di promozione commerciale in cui non vi sia un invio di una comunicazione ricevuta su un indirizzo, numero o altro dato di contatto dell'utente finale (ad esempio una pubblicità mostrata all'interno di una pagina *web*), in base a quanto previsto dal Considerando n. 32 della bozza di Regolamento.

Con precipuo riguardo al *soft spam* (art. 16, comma 2), si conferma non necessario il consenso preventivo dell'utente alle condizioni già previste, con l'ulteriore previsione per cui tale eccezione risulta applicabile – oltre che alle comunicazioni realizzate via e-mail, come previsto già dalla Direttiva *e-privacy* – anche a quelle effettuate mediante SMS, MMS e applicazioni e tecniche funzionalmente equivalenti. Viene al contempo significativamente concessa agli Stati Membri la facoltà di stabilire un limite temporale massimo, decorrente dalla vendita del prodotto, entro il quale è permesso l'invio di comunicazioni di *soft spam* senza il consenso dell'utente finale (art. 16, comma 3, bozza di Regolamento)[14].

Nel futuro assetto dunque, se la deroga del *soft spam* avrà un ambito applicativo più esteso – ampliandosi comprensibilmente fino a comprendere anche le varie forme di messaggistica – dall'altro lato potrà andare incontro a una limitazione temporale sancita a livello nazionale.

Peraltro, la possibilità di introdurre un siffatto limite temporale rappresenterebbe una concretizzazione dei principi di necessità e di finalità del trattamento, secondo i quali i dati raccolti non possono essere trattati per un tempo ulteriore rispetto a quello strettamente necessario allo scopo della raccolta. In tal senso, come noto, l'art. 5, c. 1, lett. e), GDPR prevede espressamente che i dati personali debbano essere «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati»[15]. La fissazione di un limite temporale massimo consentirebbe dunque l'individuazione di quell'«arco di tempo» a cui la norma fa espresso riferimento, con specifico riguardo all'invio di comunicazioni commerciali di *soft spam*. Diversamente, la conservazione dell'indirizzo di posta elettronica del cliente potrebbe sostanzialmente protrarsi per un periodo illimitato, dipendendo il suo utilizzo da periodiche, nuove offerte di beni o servizi analoghi.

In ogni caso, anche alla luce di quelle che saranno le future modifiche alla disciplina dello *spamming*, si può osservare che lo stesso dibattito di fondo, per l'una o l'altra soluzione (*opt-in*, *opt-out*, *soft-spam* o *soft opt-in*) perda sempre più di rilievo, laddove – all'interno di un sistema assai articolato e differenziato, in cui si intrecciano regole, ma anche eccezioni e possibilità di deroga lasciate agli Stati membri – si tratta piuttosto di individuare correttamente l'ambito applicativo di singole disposizioni, assai dettagliate, e diversificate anche in base al tipo di tecnologia utilizzata per operare la comunicazione.

4. Il *soft spam* fra consenso e contratto

Due sono i punti nodali affrontati dalla decisione in questione: la necessità/rilevanza del consenso[16] e la qualifica di contraente-cliente o meno del destinatario delle comunicazioni commerciali non richieste, con correlativa necessità di appurare che fra titolare del trattamento e interessato sia intercorso un vero e proprio rapporto contrattuale.

Per vero, nella decisione si evidenzia anche una certa sovrapposizione fra i due profili.

Nella parte finale, precedente all'enunciazione del principio di diritto, si legge infatti «la deroga prevista dall'art. 130 del D. Lgs 196/2003 non si estende alla mera registrazione sul sito, né ai contratti a titolo gratuito ma solamente nell'ipotesi in cui vi sia stato un rapporto contrattuale di vendita del bene o del servizio e, in tale occasione, sia stato espresso il consenso all'invio di mailing marketing (...). Ne consegue che, in assenza del consenso regolarmente acquisito, non rileva che le e-mail inviate contenessero l'informazione relativa alla possibilità di disattivazione del servizio».

[14] F. GIULIANI, M. LEFFI, G. VECCHI, *op. cit.*

[15] Cfr. F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (dir. da), *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2017, 103 ss.

[16] Sul consenso cfr. V. CUFFARO, *Il consenso dell'interessato*, in V. CUFFARO, V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, Torino, 1997, 221 ss., S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, 460 ss., e più di recente, S. THOBANI, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016, specie 13 ss., I. A. Caggiano, *Il consenso al trattamento dei dati personali tra nuovo Regolamento Europeo e analisi comportamentale*, in *Dir. merc. tecnol.*, 25 gennaio 2017, 7 ss., A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019, specie 57 ss.

Ora, è chiaro che se a monte vi fosse stato un regolare consenso dell'interessato all'invio del materiale promozionale, il relativo trattamento sarebbe avvenuto legittimamente sulla base del consenso *ex* art. 130, comma 1, e non vi sarebbe stato bisogno di applicare la deroga di cui al comma 4, con accertamento dei relativi presupposti, inclusa la qualifica di cliente dell'interessato stesso.

Nel *soft spam*, la base giuridica sulla quale si fonda il trattamento pare da individuarsi nel legittimo interesse del titolare, condizionato nel suo esercizio alla presenza dei requisiti previsti dalla norma: il consenso difetta, ma – nel caso di impiego delle coordinate di posta elettronica – tale mancanza è legittimata proprio dall'operatività del meccanismo di *opt-out* previsto nello stesso comma 4 dell'art. 130, sempre che sussistano i relativi presupposti[17]. Ne deriva una sorta di fattispecie tipizzata *ex lege* di legittimo interesse del titolare, nel quale il bilanciamento con "gli interessi o i diritti e le libertà fondamentali dell'interessato", come recita l'art. 6 comma 1, lettera f) GDPR, è affidato alle condizioni (e anche alle guarentigie) previste dal comma 4 dell'art. 130.

Nel caso di specie, viene censurato il fatto che il consenso all'invio di materiale promozionale non fosse inserito nel *form* di registrazione sul sito della società opponente. In verità, se tale consenso fosse stato validamente prestato da coloro che si registravano volontariamente sul sito compilando il *form* e spuntando la relativa casella, non vi sarebbe stato neppure bisogno di indagare sui margini di applicabilità del *soft spam*.

Il nodo della questione inerente alla possibile configurazione di una deroga *ex* art. 130, comma 4, è dunque da tenere ben distinto dal consenso, visto che il *soft spam* prescinde da esso.

Ci si domanda cioè se anche il cliente "non pagante" come viene definito nella pronuncia, cioè quello che si registra sul sito per provare gratuitamente il servizio, possa divenire legittimo destinatario di *soft spam*, al pari del soggetto con cui il titolare del trattamento abbia intrattenuto un rapporto contrattuale a tutti gli effetti. E, conseguentemente, ci si interroga sul rilievo rivestito dalla stessa registrazione sul sito operata dal cliente non pagante, che in tal modo manifesta interesse per il servizio offerto.

La risposta offerta dalla Cassazione è piuttosto rigorosa: il cliente "non pagante" non può essere considerato un contraente. Il solo soggetto al quale è applicabile l'eccezione di cui al comma 4 è il cliente pagante, e il termine "vendita" è, secondo la Corte, usato in senso tecnico, tale da richiedere che tra il titolare del trattamento ed il destinatario delle comunicazioni si sia stabilito un rapporto contrattuale a titolo oneroso. A nulla rilevano né l'interesse indirettamente espresso dal cliente non pagante né il rispetto delle altre condizioni che legittimano il *soft spam* (ossia l'offerta di prodotti o servizi analoghi e la possibilità di *opt-out*). Secondo la decisione, la situazione del cliente non pagante non integra propriamente una "vendita".

I giudici di legittimità adottano dunque un'interpretazione restrittiva della norma, sul presupposto che la stessa deroghi alla regola generale del consenso preventivo e che dunque, come aveva già sostenuto il Garante per la protezione dei dati personali in precedenti provvedimenti, che le condizioni della sua operatività non debbano essere intese in maniera elastica o estensiva[18].

Tuttavia, l'interpretazione del termine "vendita" *ex* art. 130, comma 4 potrebbe oggi trovare nuove declinazioni, tanto più all'interno di una realtà in cui il rilievo del profilo contrattuale nella circolazione dei dati personali è quanto mai enfatizzato. Nel contesto, caratteristico della contemporanea *data economy*, della "patrimonializzazione" dei dati personali[19], a cui in

[17] Per ulteriori considerazioni cfr. L. VIZZONI, *Sub art. 130*, cit., 642.
V. inoltre il provvedimento del 15 gennaio 2020 (noto per la sanzione di oltre 27 milioni di euro inflitta a TIM), con cui il Garante, con specifico riferimento alle attività di *marketing* effettuate tramite *call center*, ha sancito che il legittimo interesse di cui all'art. 6, par. 1, lett. f), del Regolamento - già previsto sia dall'abrogata direttiva 95/46/CE, nonché dal Codice previgente alle modifiche apportate dal d.lg. n. 101/2018 (d.lg. n. 196/2003, art. 24, comma 1, lett. g) e ammesso solo «a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali» - non può surrogare, in via generale, il consenso dell'interessato quale base giuridica del *marketing.* Peraltro, aggiunge il provvedimento, «qualora non ricorrano i sopra delineati presupposti per il legittimo interesse e ad eccezione delle ipotesi del c.d. "soft spam" (art. 130, comma 4, Codice), nonché del sistema di "opt-out" per i dati presenti negli elenchi pubblici – si deve ritenere che la regola generale da seguire per i trattamenti per finalità promozionali sia quella del previo consenso informato, libero, specifico e documentato degli interessati». Viene così significativamente confermato che la base giuridica del trattamento dei dati nel *soft spam* non è il consenso dell'interessato, bensì il legittimo interesse del titolare, che trova – nell'ipotesi di impiego degli indirizzi mail – i limiti ulteriori posti dall'art. 130 comma 4.

[18] Cfr. il provvedimento indicato nella nota precedente.

[19] Il tema della patrimonializzazione dei dati personali è stato indagato soprattutto da V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, 95 ss., ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 23 ss.,

questa sede si può soltanto accennare, non è in effetti escluso che si possa considerare "contratto" anche il rapporto che si instaura fra il fornitore di un servizio digitale e chi si registra sul relativo sito compilando un *form* e accettando le condizioni contrattuali, per ottenere in cambio il relativo servizio, senza dover versare un corrispettivo in termini monetari ma fornendo propri dati personali.

D'altronde, come noto, la Direttiva 770/2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, ha trovato attuazione nel diritto interno con il d.lg. 2021, n. 173, che ha inserito nel codice del consumo il nuovo Capo I-*bis*, in cui l'art. 135 *octies*, al comma 4, avalla definitivamente una struttura contrattuale così articolata, proprio nell'ambito della fornitura di un contenuto o di un servizio digitale[20]. In effetti, già nel testo della Direttiva, con particolare riguardo all'art. 3, seconda parte, molti studiosi leggevano un consolidamento del modello contrattuale come presupposto per la commercializzazione dei dati personali[21].

È pur vero che, anche aderendo alla ricostruzione in chiave contrattuale del fenomeno, non risulta chiaro a quale tipo sarebbe da ascrivere lo schema dati contro servizio/contenuto digitale. In tal senso, come osservato, sarebbe da rifiutare decisamente la ricostruzione secondo le maglie della compravendita, poiché importerebbe un trasferimento definitivo di diritti, non configurabile rispetto ai dati personali, che costituiscono attributi irrinunciabili della persona. Più in generale, sarebbe da respingere l'adozione di configurazioni di stampo dominicale o anche in termini di proprietà intellettuale. Esclusa pure la riconduzione della cessione dei dati a schemi propri dei contratti di godimento su beni altrui, se si eccettua forse la licenza d'uso, sembra che l'unica soluzione sia quella di rifugiarsi nelle braccia dell'atipicità contrattuale, con sottoposizione della pattuizione al relativo vaglio di meritevolezza degli interessi perseguiti. In ogni caso, nella prospettiva delineata, la disposizione dei propri dati da parte dell'interessato-contraente rappresenterebbe, secondo taluni, una vera e propria controprestazione, in cambio della quale la parte fruisce del servizio o contenuto digitale[22].

Nel caso di specie, trattandosi appunto di un servizio digitale, si sarebbe forse potuto prendere in considerazione la possibilità di optare per l'accoglimento di una nozione più ampia di cliente, comprensiva anche dei clienti che, prestando i propri dati personali, ottengano il servizio in questione, sebbene nella forma "di prova".

Si tratterebbe, in un certo senso, di clienti a loro volta paganti sebbene in ottica diversa, ossia clienti che pagano fornendo i propri dati personali, *in primis* l'indirizzo e-mail rilasciato con la compilazione del *form* sul sito, ottenendo in cambio una versione ridotta del servizio digitale, rimanendo la versione completa riservata a quei clienti "doppiamente paganti", che, oltre a prestare dati personali, versano un corrispettivo pecuniario.

Peraltro, il riferimento testuale dell'art. 130, comma 4, al «contesto della vendita di un prodotto

---

ID., *Il contratto e i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, 642 ss.

[20] Questo il testo dell'art. 135 *octies*, comma 4: «Le disposizioni del presente capo si applicano altresì nel caso in cui il professionista fornisce o si obbliga a fornire un contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si obbliga a fornire dati personali al professionista, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dal professionista ai fini della fornitura del contenuto digitale o del servizio digitale a norma del presente capo o per consentire l'assolvimento degli obblighi di legge cui è soggetto il professionista e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti».
Sul punto, v. le riflessioni critiche di S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135 octies – 135 vicies ter c.cons. La nuova disciplina dei contratti b-to-c per la fornitura di contenuti e servizi digitali*, in *Nuove leggi civ.*, 2022, 1499 ss. E cfr. anche A. MORACE PINELLI, *Introduzione*, in Id. (a cura di), *La circolazione dei dati personali. Persona, contratto e mercato*, Pisa, 2023, 24 ss.

[21] Cfr. A. DE FRANCESCHI, *La vendita di beni con elementi digitali*, Napoli, 2019, specie 15. Più in generale, sul riconoscimento di valore economico dei dati personali, cfr. A. DE FRANCESCHI, R. SCHULZE, *Introduction*, in A. DE FRANCESCHI, R. SCHULZE (a cura di), *Digital Revolution - New Challenges for Law*, München- Baden-Baden, 2019, 4, e S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws*, 2019, 131 e 137 ss. Sul valore della direttiva, nel contesto della patrimonializzazione dei dati personali, v. inoltre le riflessioni di R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2020, 760 ss.

[22] Sul modello "servizi contro dati", v. G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la direttiva (UE) 2019/770 e il regolamento (UE) 2016/679*, in A. D'ANGELO, V. ROPPO (a cura di), *Annuario del contratto 2018*, Torino, 2019, 128 ss.
Per riflessioni sul mercato digitale e la circolazione dei dati con il consenso dell'interessato v. inoltre G. ALPA, L*a "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., 18 ss.: C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, specie 90 ss., A. METZGER, *A Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (Eds.), *Data as Counter-Performance - Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V*, Oxford - Baden-Baden, 2020, 25 ss.
Per una ricostruzione esplicita del consenso al trattamento in chiave di corrispettivo per l'erogazione di beni o servizi digitali v. ora P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv dir. civ.*, 2022, 1054 ss., specie 1065, 1078.

o di un servizio» è piuttosto generico, se non addirittura impreciso laddove si riferisce alla vendita di un servizio: si tratterebbe di ulteriore appiglio per intravedere alternative ad una ricostruzione in termini esclusivamente tecnici del termine "vendita", che certamente rappresenta l'approdo meno problematico per i giudici di legittimità.

5. Cassazione e *spammming*: uno sguardo al versante risarcitorio

La pronuncia in esame, come accennato, non si occupa di risarcimento del danno conseguente: un aspetto che non era in discussione dal momento che la società resistente si opponeva alla sanzione irrogata dal Garante sostenendo che non fosse configurabile la pratica illecita, mentre non risulta che alcun destinatario delle comunicazioni indesiderate abbia agito sul versante rimediale. Al contrario, la quasi totalità delle pronunce di legittimità rese in materia si sono dovute misurare con la configurabilità e risarcibilità del relativo danno.

In linea generale, al destinatario di comunicazioni commerciali effettuate in violazione di quanto disposto dall'art. 130 del codice *privacy* spettano vari rimedi e tutele.

Al di là del primo rimedio, di carattere tecnico, previsto dallo stesso art. 130, comma 6, – consistente nella possibilità, per l'Autorità Garante, di prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono state inviate le comunicazioni[23] – e alle sanzioni, sul versante penale come amministrativo, il destinatario di *spamming* potrà chiedere il risarcimento del danno sofferto[24].

Come noto, l'art. 15 della Codice della *privacy* – che garantiva in favore del danneggiato dall'illecito trattamento di dati personali il risarcimento del relativo danno *ex* art. 2050 c.c., di natura sia patrimoniale sia non patrimoniale – è stato abrogato dal d.lg. 101/2018[25].

La norma di riferimento è oggi l'art. 82 del GDPR, che sancisce il diritto di chiunque subisca un danno materiale o immateriale causato da violazioni del Regolamento stesso, al risarcimento del relativo danno da parte del titolare o del responsabile del trattamento. Nonostante una certa similitudine testuale fra le due norme, la formulazione dell'art. 15 codice *privacy* risultava più ampia rispetto a quella di cui all'art. 82 del Regolamento, che limita il novero dei potenziali danneggianti esclusivamente al titolare e al responsabile del trattamento[26], ponendo il problema del coordinamento con le regole di diritto comune.

Gli ultimi approdi della giurisprudenza di legittimità in materia di illecito trattamento dei dati personali da ricezione illegittima di comunicazioni indesiderate, e più in generale da illecito trattamento dei dati personali, hanno adottato posizioni piuttosto restie a concedere siffatto risarcimento in favore del soggetto danneggiato dalla pratica di *spamming*, pure accertata come in essere. Basterebbe ricordare una nota decisione del 2017[27], la quale ha ritenuto

[23] Sul filtraggio cfr. A. ROSSI, *Spamming e intercettazioni: cases of law*, in A. PACE, R. ZACCARIA, G. DE MINICO, *Mezzi di comunicazione e riservatezza. Ordinamento comunitario e ordinamento interno*, Napoli, 2008, 273.

[24] In materia di risarcimento del danno da illecito trattamento dei dati personali v. E. PELLECCHIA, *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. prev.*, 2006, 232 ss., F. GRITTI, *La responsabilità civile nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice di trattamento dei dati personali*, Torino, 2007, 157 ss. Con specifico riguardo al danno da ricezione di comunicazioni elettroniche indesiderate, v. O POLICELLA, *Il danno da spamming*, in *Danno e resp.*, 2005, 659 ss.

[25] Sul regime previgente cfr. E. TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019, 31 ss. Sui rapporti tra art. 15 cod. *privacy* e art. 82 GDPR sia inoltre consentito rinviare a L. VIZZONI, *Domotica e diritto*, cit., 196 ss.

[26] Sull'art. 82 GDPR v. C. CAMARDI, *Note critiche in tema di danno da illecitotrattamento dei dati personali*, in *Jus civile*, 2020, 3, 769 ss., E. TOSI, *La responsabilità civile per trattamento illecito dei dati personali, in* E. TOSI (a cura di), *Privacy digitale*, cit., 619 ss., S. SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, in D. POLETTI, A. MANTELERO (a cura di), *Regolare la tecnologia. Il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, 161 ss. Cfr. inoltre M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 1017 ss. e R. CATERINA, S. THOBANI, *Il diritto al risarcimento dei danni*, in *Giur. it.*, 2019, 2805 ss.

[27] Cass. 8 febbraio 2017, n. 3311, in *Dir. giust.*, 2017, 9 febbraio, con nota di F. VALERIO, *Danno da spamming: nessun risarcimento per poche email indesiderate*. Il caso era il seguente: un avvocato lamentava di aver ricevuto, nell'arco di tre anni a mezzo, dieci e-mail indesiderate di contenuto pubblicitario, da parte di una società di formazione, senza aver prestato il proprio consenso alla ricezione di tali messaggi. La società convenuta si era difesa sostenendo che il ricorrente non aveva dimostrato il nesso causale tra lo *spam* ricevuto e l'asserito danno, e dunque l'inesistenza della prova di un pregiudizio effettivo come diretta conseguenza dell'invio dei messaggi in questione. Aderendo alle ricostruzioni della società convenuta, la corte di legittimità ha rigettato il ricorso in quanto manifestamente infondato.
Quella del 2017 non è comunque la prima decisione di siffatto tenore in materia di responsabilità da illecito trattamento dei dati personali. Per una rassegna, anche in chiave critica, delle principali pronunce di legittimità in materia v. F. BRAVO, *Il principio di solidarietà in materia di protezione dei dati*

che il danno non patrimoniale risarcibile di fronte all'invio di comunicazioni non sollecitate *ex* art. 15 codice *privacy*, «pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 della CEDU, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato)». In particolare, anche per tale diritto viene ritenuto operativo il bilanciamento con il principio di solidarietà *ex* art. 2 Cost., «di cui il principio di tolleranza della lesione minima è intrinseco precipitato, sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del medesimo codice ma solo quella che ne offenda in modo sensibile la sua portata effettiva»[28]. Ai fini della richiesta condanna al risarcimento viene ritenuta necessaria la prova della «serietà del danno», il quale deve cioè superare la soglia minima di tollerabilità.

Tale orientamento, seguito da decisioni successive in tema di illecito trattamento dei dati personali[29], è stato confermato anche dinanzi all'art. 82 GDPR, nel frattempo entrato in vigore: in questa occasione[30], la Cassazione ha precisato ulteriormente che il danno da illecito trattamento dei dati personali «non sussiste in "re ipsa", non identificandosi il danno risarcibile con la mera lesione dell'interesse tutelato dall'ordinamento, ma con le conseguenze di tale lesione, seppur può essere provato anche attraverso presunzioni»[31].

La Corte di legittimità, dunque, mantiene un orientamento compatto nel negare risarcimenti del danno per lesioni le quali, pur attenendo a diritti fondamentali, vengono ritenute futili o di entità tale da non meritare risarcimento; e ciò è avvenuto precipuamente qualora il danno derivi dalla ricezione di comunicazioni indesiderate, tanto che il fenomeno dello spamming appartiene, in buona sostanza, ad una delle aree di responsabilità senza danno.

Il rigore adottato dal giudice di legittimità in tema di liceità dello *spamming*, che giustifica l'applicazione delle sanzioni amministrative previste dalla normativa speciale, nel cui solco si inserisce la pronuncia in commento, si coniuga quindi con le pronunce dello stesso giudice di legittimità, altrettanto rigorose nell'escludere la sussistenza di un danno risarcibile.

Proprio di recente, la questione è giunta all'attenzione della Corte di Giustizia dell'Unione Europea, la quale, chiamata a pronunciarsi sull'interpretazione dell'art. 82 GDPR ha ritenuto che la mera violazione del Regolamento non attribuisca un diritto al risarcimento, ma al contempo che non sia corretto subordinare il risarcimento alla condizione che il danno subito dall'interessato abbia raggiunto un certo grado di gravità[32].

La decisione della Corte del Lussemburgo alimenterà sicuramente il dibattito in argomento, troppo complesso per essere affrontato in questa sede. Quel che è certo è proprio il tema del danno da illecito trattamento dei dati personali (e del danno da *spamming* in particolare) mette alla prova la tenuta dello statuto del risarcimento del danno non patrimoniale, tanto che non mancano voci

personali nelle decisioni del Garante e della corte di Cassazione, in *Contr. impr*., 2023, 413 ss.

[28] Addirittura, la Cassazione in questa occasione si è spinta sino a ritenere integrata la responsabilità aggravata *ex* art. 96, comma 3, c.p.c. in capo al ricorrente, poiché questi aveva percorso tutti i gradi di giudizio per un danno giudicato come «ipotetico e futile, consistente al più in un modesto disagio o fastidio, senz'altro tollerabile», e lo ha pertanto condannato al pagamento di 1.500 euro per lite temeraria.

[29] V. Cass. 4 giugno 2018, n. 14242 e Cass. 8 gennaio 2019, n. 207, ord., in *Corr. giur*., 2019, 625 ss., con nota di M. S. Esposito, *Il risarcimento del danno non patrimoniale da illecito trattamento dei dati personali*. Richiamando precedente dottrina, l'A. (*ivi*, 633) evidenzia come non sia ammissibile introdurre un giudizio sulla rilevanza ed entità degli interessi tutelati laddove il risarcimento sia collegato alla violazione di diritti inviolabili della persona. La c.d. soglia di risarcibilità può essere impiegata piuttosto quale parametro per la determinazione dell'entità del risarcimento spettante.

[30] Cass. 10 giugno 2021, n. 16402, ord, in *Dir. giust*., 2021, 11 giugno, e in *Foro it*. 2021, 11, I, 3589 ss. In questo caso il ricorrente aveva agito per far accertare l'illecito trattamento dei suoi dati personali e ottenere il relativo risarcimento del danno da parte di un Istituto di Investigazioni, che, con la cooperazione dell'INPS, aveva ottenuto la documentazione attestante una certa sua situazione retributiva al fine di acquisire elementi di prova da far valere nell'ambito di un procedimento penale in cui lo stesso ricorrente era coinvolto.

[31] Sui recenti orientamenti di legittimità in tema di danno in *re ipsa* v. esemplarmente G. Alpa, *Danno in re ipsa e tutela dei diritti fondamentali (diritti della personalità e diritto di proprietà)*, in *Resp. civ. prev*., 2023, 6 ss.

[32] CGUE, decisione 4 maggio 2023, n. 72, causa C-300/21, Österreichische Post, pubblicata in www.eur-lex.europa.eu. Il caso di specie è il seguente: a partire dal 2017, le Poste austriache avevano raccolto informazioni sulle affinità politiche della popolazione austriaca, categorizzandola in «indirizzi di gruppi destinatari» con l'ausilio di un algoritmo. I dati così raccolti e trattati avevano consentito alla Österreichische Post di ricondurre uno specifico cittadino alla preferenza in favore di un determinato partito politico. Il cittadino in questione, che non aveva acconsentito al trattamento dei suoi dati personali, chiedeva al giudice austriaco un importo di 1.000 euro a titolo di risarcimento del danno immateriale subito. La Corte suprema austriaca ha espresso dubbi in merito alla portata del diritto al risarcimento *ex* art. 82 GDPR, chiedendo alla CgUe se la mera violazione del Regolamento sia sufficiente per conferire tale diritto e se sia possibile concedere il risarcimento solo oltre un determinato grado di gravità del danno immateriale subito.

critiche riguardo al mancato riconoscimento del *quantum* del danno[33], ma soprattutto si rafforzano i dubbi circa l'efficacia degli strumenti privatistici di tutela[34], specie considerando che la somma dei disagi arrecati ai singoli destinatari determina evidenti arricchimenti in capo ai mittenti.

In questo quadro, sollecita ulteriormente l'attenzione degli interpreti una decisione tedesca di merito, resa dal Tribunale regionale di Heidelberg il 16 marzo 2022, caso 4S 1/21[35], che adotta un'impostazione diametralmente opposta a quella della Cassazione in tema di risarcimento del danno da *spamming*, con riguardo a una vicenda particolarmente rilevante perché del tutto analoga a quella che condusse alla decisione di legittimità italiana del 2017. L'interessato aveva infatti ricevuto una prima e-mail pubblicitaria relative ad un corso di formazione, senza aver mai richiesto l'invio di comunicazioni di questo tipo, né prestato consensi. Il destinatario aveva poi manifestato al mittente/titolare del trattamento la sua opposizione, e ciononostante aveva comunque ricevuto un'ulteriore mail dello stesso tipo. Da qui aveva avuto inizio la vicenda giudiziaria del ricorrente, che si era visto negare il risarcimento del danno dal giudice di prime cure, il quale aveva sì ordinato al titolare del trattamento la cessazione degli invii indesiderati, ma, ritenendo che l'interessato non avesse ricevuto nessun pregiudizio rilevante, aveva negato il risarcimento del danno. Al contrario, la sentenza del giudice di Heidelberg ha riconosciuto al ricorrente il diritto *ex* art. 82 GDPR, ad ottenere un risarcimento del danno di 25 euro, pari a 12,50 euro per ogni e-mail indesiderata ricevuta. L'importo è evidentemente irrisorio, ma è significativo che il danno in questione abbia superato la soglia della risarcibilità e la relativa lesione non sia stata reputata futile.

Forse del danno da *spamming* (e anche del danno da *soft spamming*) si tornerà presto a discutere.

[33] In proposito cfr. le recenti riflessioni di F. BRAVO, *op. ult. cit.*, 417 (e 426 ss.), il quale osserva proprio come la giurisprudenza della Cassazione faccia talvolta applicazione del principio di solidarietà anche «per negare rilevanza a richieste risarcitorie concernenti danni non patrimoniali che, pur derivanti da illeciti effettivamente accertati, siano di lieve entità o siano cagionati da condotte socialmente ritenute non gravi». Tale argomentazione, come rilevato criticamente dall'A. stesso, applicata non di rado in materia di illecito trattamento di dati personali, si traduce nell'aggiunta di requisiti ulteriori rispetto agli elementi essenziali della struttura dell'illecito, nel caso di richieste risarcitorie *ex* art. 2059 c.c., ossia la serietà del danno e la gravità della lesione.

[34] V. A. I. CAGGIANO, *op. cit*., 17-18.

[35] Sulla decisione v. un primo commento di A. LO GIUDICE, *Lo spam è un fastidio che va risarcito: la sentenza tedesca che contraddice la nostra Cassazione*, in *www.agendadigitale.eu*, 27 maggio 2022.