10638/16

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

LA CORTE SUPREMA DI CASSAZIONE

PRIMA SEZIONE CIVILE

Oggetto

Trattamento dati personali; abusive operazioni di prelevamento on line; risarcimento dei danni.

Composta dagli Ill.mi Sigg.ri Magistrati:

Dott. FABRIZIO FORTE - Presidente -

Dott. RENATO BERNABAI - Consigliere -

Dott. MARIA CRISTINA GIANCOLA - Consigliere -

Dott. MARIA ACIERNO - Consigliere -

Dott. FRANCESCO TERRUSI - Rel. Consigliere -

R.G.N. 20042/2013

Cron. 10638

Rep. C.I.

Ud. 13/04/2016

PU

ha pronunciato la seguente

SENTENZA

sul ricorso 20042-2013 proposto da:

[redacted] (c.f. [redacted], elettivamente domiciliata in ROMA, VIA ARNO 96, presso l'avvocato DAVIDE CICCARONE, rappresentata e difesa dall'avvocato MASSIMO DI MARCO, giusta procura in calce al ricorso;

- *ricorrente* -

2016

794

contro

[redacted], in persona del legale rappresentante pro tempore, elettivamente domiciliata in ROMA, VIALE EUROPA 175, presso l'AREA

[redacted] rappresentata e difesa dagli avvocati GAETANO POLLIO, SIMONETTA GUADAGNI, giusta procura a margine del controricorso;

- controricorrente -

contro

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI;

- intimato -

avverso la sentenza n. 869/2013 del TRIBUNALE di MILANO, depositata il 23/01/2013;

udita la relazione della causa svolta nella pubblica udienza del 13/04/2016 dal Consigliere Dott. FRANCESCO TERRUSI;

udito, per la ricorrente, l'Avvocato CONTUCCI LORENZO, con delega avv. DI MARCO, che si riporta;

udito, per la controricorrente, l'Avvocato FABBRI PAOLA, con delega avv. POLLIO, che ha chiesto il rigetto del ricorso;

udito il P.M., in persona del Sostituto Procuratore Generale Dott. FRANCESCA CERONI che ha concluso per l'inammissibilità, in subordine il rigetto del ricorso.

20042-13

Svolgimento del processo

[redacted] conveniva in giudizio, con rito ordinario poi mutato ai sensi dell'art. 152 del d.lgs. n. 196 del 1993 (cd. codice della privacy), le [redacted] e ne chiedeva la condanna al risarcimento dei danni conseguenti a un illecito trattamento dei propri dati personali.

L'attrice lamentava che era stato consentito il 29-1-2010 un bonifico online dal proprio conto, non da essa disposto.

Nel contraddittorio con [redacted] contumace il Garante per la protezione dei dati personali, il tribunale di Milano respingeva la domanda ritenendo non adeguatamente provati i fatti costitutivi.

Ad avviso del tribunale, la c.t.u. aveva consentito di appurare che il sistema implementato da [redacted] non consentiva in sé, ai terzi, di venire a conoscenza dei dati necessari per compiere operazioni all'insaputa del destinatario, donde non era possibile che l'operazione *de qua* fosse avvenuta senza che la correntista avesse comunicato i propri codici identificativi. Nulla dunque autorizzava a ritenere che terzi estranei fossero venuti a conoscenza dei dati necessari all'esecuzione dell'operazione di "postagiro" sul conto in questione (nome utente, password e codice

identificativo), e il fenomeno di phishing, richiamato dalle difese e anche nella relazione del c.t.u., dovevasi considerare ininfluente, non essendo stato provato che l'attrice avesse subito attraverso la rete internet il furto dei dati personali.

In questo senso, l'attrice non aveva adempiuto all'onere di provare il nesso di causalità tra il danno subito e l'attività, pur considerata pericolosa ai sensi dell'art. 2050 cod. civ., relativa al trattamento dei dati personali.

Il tribunale aggiungeva che la società [redacted] si era avveduta dell'anomalia dell'operazione in ragione dell'entità della somma (euro 5.734,99) e della provenienza dell'ordine da un computer diverso da quello comunemente usato dalla correntista, tanto da aver contattato telefonicamente l'attrice pochi minuti dopo, e bloccato, quindi, il conto. In simile situazione, tuttavia, poteva al più discorrersi di responsabilità di [redacted] per inesatto adempimento del contratto, e non di responsabilità per illecito trattamento dei dati personali, in quanto il sistema all'epoca adottato (vale a dire il codice identificativo segreto composto di dieci caratteri) non era sufficientemente efficace nella prevenzione di frodi informatiche, tanto da essere stato

sostituito un paio di mesi dopo il fatto. In ragione di ciò, il tribunale compensava le spese processuali.

Per la cassazione della sentenza, depositata il 28-2-2013, la [redacted] ha proposto ricorso per cassazione affidato a due motivi.

[redacted] ha replicato con controricorso.

Il Garante non ha svolto difese.

Le parti costituite hanno depositato una memoria.

Motivi della decisione

I. - Col primo motivo, deducendo omessa, insufficiente e contraddittoria motivazione, la ricorrente censura la sentenza per aver affermato l'ininfluenza del fenomeno del phishing senza tener conto degli elementi probatori acquisiti, e in particolare senza tener conto della c.t.u., che aveva esplicitamente riferito la fattispecie a tale fenomeno. Censura inoltre la sentenza nella parte in cui ha ritenuto che, anche a voler considerare la responsabilità di [redacted] nell'alveo dell'art. 2050 cod. civ., sarebbe stato disatteso l'onere probatorio. Era stato difatti prodotto in giudizio l'atto di querela e la conseguente diffida, e l'art. 2050 cod. civ. stabilisce una presunzione di responsabilità per il titolare del trattamento, che può esser vinta solo dalla prova liberatoria a suo carico circa l'adozione delle misure necessarie a evitare il danno.

II. - Col secondo motivo la ricorrente denunzia la violazione ed errata applicazione di norme di diritto ai fini della determinazione della responsabilità della convenuta, avendo il tribunale omesso di considerare il disposto ex art. 31 del codice della privacy a misura della accertata inefficacia del sistema di sicurezza utilizzato all'epoca dei fatti. Ed erronea in tal senso era da considerare anche l'applicazione dell'art. 2050 cod. civ. in punto di onere della prova.

III. - Giova premettere che non possiede fondamento l'eccezione con la quale, rispetto ai citati due motivi, la società controricorrente ha sollecitato la declaratoria di inammissibilità del ricorso per carenza dei requisiti di cui all'art. 366, 1° comma, n. 3, cod. proc. civ.

Il ricorso invero contiene l'esposizione dei fatti essenziali in rapporto alle censure prospettate, e non occorre, per rispettare l'art. 366 cod. proc. civ., che l'esposizione sia pure analitica e particolareggiata.

Quel che interessa è che i fatti di causa siano esposti in modo da far risultare chiaramente quale fossero le reciproche pretese delle parti con i presupposti di fatto e le ragioni di diritto poste a loro sostegno, oltre che lo svolgersi della vicenda processuale nei profili essenziali per la valutazione che si richiede alla corte.

IV. - Devesi considerare fondato, nei termini che seguono, il secondo motivo di ricorso, il cui esame si rivela assorbente.

La sentenza del tribunale riferisce che l'attrice, intestataria di un conto corrente postale, aveva chiamato [redacted] a rispondere dei danni risentiti a causa di un'operazione di bonifico online transitata sul proprio conto e disconosciuta.

Invero l'attrice aveva chiesto il ristoro del danno patrimoniale e di quello non patrimoniale invocando una responsabilità della convenuta in base al codice della privacy, per illecito trattamento dei dati personali afferenti al conto.

In simile condizione, il tribunale ha riferito la fattispecie all'art. 15 del codice della privacy e all'art. 2050 cod. civ.

V. - Ora, la sentenza ha rigettato la domanda sottolineando che dalla c.t.u. era emerso che "il sistema implementato da [redacted] non consentiva a terzi di venire a conoscenza dei dati necessari per compiere operazioni online all'insaputa del correntista".

Tuttavia la sentenza, nella parte finale, ha pure affermato che la c.t.u. aveva evidenziato essere "il sistema all'epoca adottato dalla società convenuta (codice dispositivo segreto composto di dieci caratteri)

non (..) sufficientemente efficace nella prevenzione delle frodi informatiche" e che appunto, subito dopo i fatti, quel sistema era stato sostituito con altro più sicuro.

Può d'altronde osservarsi che proprio su tale presupposto il tribunale ha compensato tra le parti le spese processuali.

La sentenza ha poi motivato dicendo che l'attrice non aveva provato che l'operazione era stata "eseguita da terzi contro la sua volontà", né di aver subito "attraverso la rete internet il furto dei suoi dati identificativi personali, che era tenuta a custodire gelosamente sapendo che essi avrebbero consentito anche a terzi di operare per via telematica sul suo conto corrente acceso presso [redacted]. Da questo punto di vista dovevasi considerare ininfluente il riferimento del c.t.u. al fenomeno noto come phishing.

VI. - Osserva la corte che la prima considerazione del tribunale è contraddetta dalla seconda; mentre la terza è nella sua assolutezza errata, dal momento che, ove si discuta di responsabilità per l'abusiva utilizzazione di credenziali informatiche del correntista nell'ambito di un servizio equiparabile a quello di home banking, non spetta al correntista provare di non aver autorizzato l'esecuzione dell'operazione (prova negativa

difficilmente ipotizzabile finanche in astratto) o, specificamente, di aver subito il furto dei dati identificativi personali.

La ripartizione dell'onere della prova, in casi simili, segue la disciplina dettata dalle norme sopra richiamate, le quali postulano l'adozione di un criterio di responsabilità efficacemente definito, in dottrina, come di tipo "semioggettivo", atteso il rinvio all'art. 2050 cod. civ. contenuto nell'art. 15 del codice della privacy, e atteso che il modello di responsabilità è coerente con quello delineato finanche a livello comunitario dall'art. 23 e dal considerando n. 55 della direttiva comunitaria n. 95/46-CE, relativamente alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.

In tal guisa l'attore è onerato soltanto della prova del danno siccome riferibile al trattamento del suo dato personale, mentre è il convenuto onerato della prova liberatoria consistente nell'aver adottato tutte le misure idonee a evitare il danno (cfr. Sez. 6^-3 n. 18812-14).

VII. - Tra codeste misure rilevano giustappunto quelle previste dal titolo V del codice della privacy (artt. 31-36), stante la regola generale secondo la quale, in sede di trattamento dei dati personali, è richiesto sempre il

rispetto di un onere di diligenza da valutare concretamente, sia "in relazione alle conoscenze acquisite in base al progresso tecnico", sia in relazione alla natura dei dati e alle specifiche caratteristiche del trattamento (v., quanto ai dati sensibili, Sez. 1^ n. 10947-14).

Tale onere si traduce nell'adozione di misure preventive di sicurezza volte a ridurre al minimo i rischi di eventi dannosi, ivi compresi quelli correlati all'accesso non autorizzato ai dati personali.

Consegue che, in base al rinvio all'art. 2050 cod. civ., operato dall'art. 15 del codice della privacy, l'istituto che svolga un'attività di tipo finanziario o in generale creditizio (nella specie [redacted] s.p.a. quanto alla gestione di conti correnti abilitati a operazioni online) risponde, quale titolare del trattamento di dati personali, dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico del cliente mediante la captazione dei suoi codici di accesso e le conseguenti illegittime disposizioni di bonifico, se non prova che l'evento dannoso non gli è imputabile perché discendente da trascuratezza, errore (o frode) dell'interessato o da forza maggiore.

VIII. - Una simile ricostruzione dei principi informatori della fattispecie è d'altronde coerente con quanto disposto pure del d.lgs. 27 gennaio 2010, n. 11, in ordine all'obbligo del prestatore del servizio di pagamento di assicurare che i dispostivi personalizzati forniti dai gestori non siano accessibili a soggetti diversi dal legittimo titolare.

Anche in tal caso, in punto di ripartizione delle responsabilità derivanti dall'utilizzazione del servizio, il citato d.lgs., artt. 10 e 11, prevede che, qualora l'utente neghi di aver autorizzato un'operazione di pagamento già effettuata, l'onere di provare la genuinità della transazione ricade essenzialmente sul prestatore del servizio. E nel contempo obbliga quest'ultimo a rifondere con sostanziale immediatezza il correntista in caso di operazione disconosciuta, tranne ove vi sia un motivato sospetto di frode, e salva naturalmente la possibilità per il prestatore di servizi di pagamento di dimostrare anche in un momento successivo che l'operazione di pagamento era stata autorizzata, con consequenziale diritto di chiedere e ottenere, in tal caso, dall'utilizzatore, la restituzione dell'importo rimborsato.

IX. - Tutto quanto esposto non appare esser stato considerato dall'impugnata sentenza, la quale, con

motivazione lacunosa e in parte contraddittoria, ha fatto malgoverno delle regole che presidiano il criterio di ripartizione dell'onere della prova *inter partes* laddove risulti negata dal correntista l'avvenuta disposizione sul conto.

Consegue che la sentenza va cassata con rinvio al medesimo tribunale di Milano, affinché, in diversa composizione, provveda a riesaminare il materiale istruttorio uniformandosi al sopra indicato principio di diritto.

Il tribunale provvederà anche sulle spese del giudizio svoltosi in questa sede di legittimità.

p.q.m.

la Corte accoglie il secondo motivo, assorbito il primo, cassa l'impugnata sentenza e rinvia, anche per le spese del giudizio di cassazione, al tribunale di Milano.

Deciso in Roma, nella camera di consiglio della prima sezione civile, addì 13 aprile 2016.

Il Consigliere estensore

Il Presidente

IL FUNZIONARIO GIUDIZIARIO
Franca Caldarola

Depositato in Cancelleria

il 23 MAG 2016

IL FUNZIONARIO GIUDIZIARIO
Franca Caldarola

Non vi sono dati personali da oscurare
18.6.2016