European Journal of Privacy Law & Technologies



2018/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2018/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published online by G. Giappichelli in October 2019
www.ejplt.tatodpr.eu

DATI SENSIBILI "INDIRETTI" IN CHIARO E RESPONSABILITÀ DEGLI ISTITUTI DI CREDITO. BREVI NOTE A CASS. 19 MAGGIO 2014 N. 19047

Ilaria Amelia Caggiano

Sommario: 1. Il fatto e la soluzione dei giudici. – 2. Inquadramento della decisione in commento e rilievi critici. – 3. La nozione di dato sensibile "indiretto" e l'adozione di misure idonee da parte dell'istituto di credito nel trattamento di un dato "indiretto". – 3. Le questioni sotto scrutinio nella prospettiva del Regolamento (UE) 2016/679.

1. – I fatti portati all'attenzione del Supremo Collegio nel provvedimento in commento riguardano il trattamento di un dato sensibile (o, in ogni caso, ritenuto tale) "indiretto", cioè un'informazione idonea a rivelare, indirettamente, un dato personale sensibile, che, nella fattispecie sotto scrutinio, è lo stato di salute di una persona, identificata o identificabile (art. 4 lett. *b)* e *d)* d. lgs. 193/2003, d'ora in poi c.d. cod. priv.) [1].

Il caso di specie riguardava una richiesta risarcitoria conseguente all'indicazione della l. 210/1992 (che riconosce il diritto a un indennizzo a chi abbia riportato menomazioni, a causa di vaccinazioni obbligatorie, ovvero risulti contagiato da HIV per la somministrazione di sangue o derivati ovvero agli operatori sanitari che durante il servizio abbiano riportato i medesimi danni) nella causale di alcuni ordini di pagamento eseguiti dalla Regione Campania, al beneficiario dell'indennizzo, e pertanto, oggetto di conoscenza da parte di altro ente (privato), l'istituto di credito. Il medesimo dato era stato ulteriormente fatto circolare, per essere riportato negli estratti conto indirizzati al destinatario del pagamento.

La Suprema Corte, nel cassare la pronuncia di primo grado (Trib. Napoli, 07 aprile 2011), accoglie il ricorso dell'interessato, statuendo il principio della responsabilità dei due enti coinvolti nel trattamento (*recte* nei trattamenti) del dato,

[1] Cass.,19 maggio 2014 n. 19047 in *Banca dati Foro it.*

principio che il medesimo tribunale partenopeo è chiamato ad applicare nel rinvio.

Secondo la Corte, sia la Regione sia la banca avrebbero violato l'art. 22 cod. priv. per non aver criptato il riferimento alla l. 210/1992, attraverso cifrature, numeri di codice non identificabili, altre soluzioni idonee a rendere temporaneamente inintellegibili i dati sensibili anche agli incaricati o altri soggetti autorizzati. La sussistenza di tale obbligo non può ritenersi superata o esclusa né dal fatto che la Regione Campania si fosse limitata a comunicare (e non diffondere) il dato a un solo soggetto determinato, né dal concorrente obbligo (contrattuale) in capo all'Istituto di credito, di indicare nell'estratto conto la causale del bonifico disposto dalla Regione. È facile desumere, da tale argomento, che anche alla semplice comunicazione, costituendo essa trattamento, si applica l'obbligo di cui all'art. 22 e, nel secondo caso, quest'ultimo è idoneo a integrare (conformandolo) il contenuto dell'obbligazione contrattuale.

La cifratura, nelle comunicazioni e notificazioni, ritenuta misura minima, ove omessa, integra pertanto la condotta *colposa* di cui all'art. 2050 c.c., come richiamato dall'art. 15 cod. priv.

2. – La sentenza di legittimità non chiarisce, con riguardo alla fattispecie concreta, quale sia l'evento dannoso verificatosi in capo all'interessato (il beneficiario dell'indennizzo oggetto di bonifico) per effetto della trasmissione in chiaro del dato sensibile "indiretto" da parte dell'ente pubblico e del soggetto privato. Quale esso sia, può inferirsi, dal tenore del provvedimento, l'esistenza di una lesione della riservatezza (o di altro diritto fondamentale) dimostrato in sede probatoria, e conseguente alla diffusione o svelamento della comunicazione (contenuta negli estratti conto) a terzi [2].

La questione relativa alla difficoltà di attualizzazione (o prova) dell'illecito da violazione della normativa c.d. *privacy* in ambito civile, che si riscontra nell'attuale esiguità della giurisprudenza relativa all'art. 15, non può essere oggetto della presente trattazione. Tuttavia, essa costituisce oggetto di sicuro interesse, e, probabilmente, riflessione circa la configurazione sotto il profilo delle tutele civili, del diritto alla protezione dei dati personali [3].

Quanto, invece, agli aspetti oggetto di espressa valutazione, il provvedimen-

[2] Sulla non ristorabilità del danno *in re ipsa*, per effetto della violazione delle norme sulla protezione dei dati personali, Cass. civ., sez. III, 05.03.2016, n. 4443, in *DeJure*. Sulla necessità di verifica, anche per il danno non patrimoniale, ristorabile ai sensi dell'art. 15 del codice della *privacy*, della gravità della lesione e della serietà del danno, in considerazione della c.d. soglia di risarcibilità, Cass., sez. III, 15 luglio 2014, 16133, ancora di *DeJure*.

[3] Sul punto CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale*, in corso di pubblicazione.

to in esame può iscriversi nell'attuale orientamento giurisprudenziale che, facendo uso della esegesi letterale e sistematica della normativa vigente in materia di protezione dei dati personali [4], tende ad applicare rigorosamente gli obblighi a tutela della protezione dei dati, per finalità di massima preservazione degli stessi, in ossequio al riconoscimento della protezione dei dati quale libertà fondamentale (sebbene non prerogativa assoluta!) della persona [5].

Ci sia consentito rilevare come tale scelta costituisce non sempre l'unica opzione possibile non solo se si guarda a sistemi giuridici che hanno concettualizzato una diversa nozione di *privacy*, ma talora con riguardo allo stesso ordinamento italiano, in una visione che pur non *negligendo* i principi e valori dell'ordinamento, tenga in debito conto i meccanismi di funzionamento della realtà tecnologica.

Un esempio di tale scenario d'interpretazione (e soluzione) alternativa può ravvisarsi nel caso di specie, ove i giudici, non solo operano – plausibilmente *ex post* – una valutazione sul carattere personale (e sensibile) del dato, ma individuano il titolo della responsabilità anche in capo all'istituto bancario direttamente nella violazione delle norme prescritte a carico dei soggetti pubblici (ai sensi dell'art. 22).

3. – Se, per un verso, la questione circa la diretta applicabilità degli obblighi di cui all'art. 22 all'ente pubblico che, per primo, ha trattato il dato appare non facilmente dubitabile, può essere meglio articolata, a nostro modo di vedere, quella relativa all'inquadramento della responsabilità dell'istituto bancario.

Ciò che appare maggiormente evidente è il passaggio ricostruttivo relativo a:

a) l'idoneità dell'informazione (non cifrata) a rivelare lo stato di salute di un soggetto identificabile (al minimo), ovvero i margini della qualificazione di

---

[4] Espressamente nel senso della interpretazione letterale è Cass., sez. II, 21 aprile 2016, n. 8105, in banca dati *Foro it.*, in relazione all'applicabilità dell'obbligo di notificazione *ex* art. 37 cod. priv. e all'interpretazione dell'espressione "a fini di … rilevazione di malattie etc." di cui all'art. 37, lett. *b*), cod. priv., intendendo tale espressione come comprendente anche le rilevazioni occasionate da trattamenti non finalizzati *ab initio* all'individuazione delle patologie elencate dalla norma. Appare ermeneuticamente pacifica anche Cass., 13 maggio 2015, n. 9785, in banca dati *Foro it.*, che, con riguardo alla divulgazione da parte dell'ufficio elettorale di un Comune ad altro Comune di tutto il fascicolo personale del soggetto danneggiato contenente i dati anagrafici e la annotazione della sentenza di rettificazione di attribuzione di sesso, ha ritenuto sussistente la responsabilità di entrambi i Comuni per omissione nella cifratura dei dati, non essendosi interrotto il nesso di causalità. Così anche, Cassazione Civile, sez. I, sentenza 12013 n° 21014, ove è stato ritenuto illegittimo il trattamento dei dati genetici ottenuto senza il consenso dell'interessato, anche per l'utilizzo finalizzato a far valere un diritto in sede giudiziaria, nella specie l'azione per il disconoscimento di paternità.

[5] Appare superfluo citare in proposito l'art. 8 della Carta di Nizza, e il considerando 4 Reg. (UE) 2016/679.

quello che abbiamo identificato come dato "indiretto" (cioè informazione che, sebbene per via indiretta, è idonea a rivelare una persona identificata o identificabile);

b) l'idoneità dell'istituto di credito a rilevare la caratteristica del dato comunicato da terzi come sensibile e quindi l'imputabilità della responsabilità.

Il caso di specie riguarda, infatti, un'informazione (gli estremi della legge che riconosce un'indennità per essere portatori di patologie – HIV – o menomazioni fisiche) contenuta in un ordine di bonifico a favore di un determinato soggetto, informazione poi trattata dalla banca.

Sulla nozione di dato personale (e quindi, per derivazione, anche sensibile), la lettera della legge è chiara nel considerare elemento qualificante dell'informazione il fatto che essa sia riferibile a un soggetto determinato o determinabile (individuato o individuabile), cioè tale che l'identità della persona cui si riferisce il dato possa risultare non solo dall'informazione da sola, ma dalla combinazione con altre informazioni, in possesso del *data user*[6]. I limiti al procedimento di associazione di informazioni, al fine di identificare il soggetto cui si riferisce quella iniziale, tendono ad essere interpretati come molto esigui, assecondando il tenore letterale della disposizione, relativamente ai termini dell'associazione (il riferimento è a "qualunque informazione" e "qualsiasi altra informazione" *ex* art. 4, lett. *b*), cod. priv.), e concentrando il discrimine sul procedimento di collegamento ispirato ad un criterio di proporzionalità ed economicità[7], al fine di evitare una eccessiva espansione della nozione di dato personale.

Già sulla base di queste considerazioni, si può aprire una più ampia riflessione in ordine alla natura di dato sensibile "indiretto". In una prospettiva generale e secondo una valutazione *ex ante*, gli estremi della l. 210/1992, associati (inclusi) all'ordine di giro, non necessariamente costituiscono un dato "potenzialmente" sensibile. Si pensi, banalmente, all'ipotesi in cui l'indennizzo, per le più svariate ragioni e comunque per indicazione del beneficiario, venga accreditato sul conto di un terzo. La mera indicazione della legge all'interno del mandato di pagamento (e non ad esempio nelle liste dei beneficiari dell'indennizzo) potrebbe non essere dato idoneo a rivelare lo stato di salute della persona (art. 22 co.

[6] La qualificazione che ci appare adeguata è in P.M. VECCHI, sub *art. 4, comma 1, lett.* b*)* in AA.VV., *La protezione dei dati personali. Commentario* a cura di C. M. Bianca e F. D. Busnelli, I, Padova, 2007, p. 51 e ivi nt. 8.

[7] Sul punto, P.M. VECCHI, sub *art. 4, comma 1, lett.* b*)*, cit., p. 54, ove, a nostro modo di vedere correttamente, si ritiene che l'identificazione debba ritenersi possibile se il dato può essere ricondotto ad un determinato soggetto soltanto attraverso operazioni che non comportano un elevato dispendio di spese ed energie, sproporzionate rispetto al risultato conseguito. In tal senso, espressamente, come si vedrà è anche il nuovo Regolamento sulla protezione dei dati personali 2016/679.

7). Questa possibile lettura non è stata presa in considerazione dai giudici, probabilmente in un'ottica *ex post*, funzionale alla garanzia di massima protezione della persona, ove il caso concreto abbia rivelato sicura funzione di dato sensibile, conformemente all'idea secondo cui «se un'informazione è stata comunque ricondotta ad un soggetto determinato, essa, indipendentemente dai costi delle ricerche svolte, non potrà che essere considerata alla stregua di un dato personale, già per il fatto che essa riguarda non più un soggetto identificabile, ma uno ormai identificato» [8]. Tuttavia, le valutazioni finora condotte ci appaiono utili per un ragionamento sui confini dei dati personali "indiretti", al fine della valutazione in termini di responsabilità.

La qualificazione degli estremi della legge, come probabile dato sensibile, a parere del collegio, avrebbe dovuto in ogni caso far scattare gli obblighi previsti a carico degli enti pubblici.

Sicuramente più problematica appare l'ascrizione della responsabilità in capo all'istituto bancario.

Come anticipato, la responsabilità della banca non può discendere dalla diretta applicazione dell'art. 22 cod. priv., relativo ai soli soggetti pubblici, e quindi dalla mancata adozione di tecniche di cifratura, quale misura minima idonea ad evitare il danno (art. 2050).

Con riguardo alla banca, le regole del trattamento dei dati sensibili, e quindi il nocciolo delle misure idonee a evitare il danno, in aggiunta alle regole generali, sono stabilite dal capo III del titolo III del d.lgs. n. 196/2003, ove non vi è quantomeno in termini espliciti un obbligo di criptazione, bensì obblighi specifici formali di autorizzazione e consenso scritto.

In presenza di entrambi i requisiti [9], che sottraggono il trattamento di un dato sensibile da parte della banca alla sfera della illiceità, quanto meno in prima

---

[8] VECCHI, *op. ult. cit.*, p. 55. Ipoteticamente, un caso di sicura (ovvero più che probabile corrispondenza tra dato e soggetto) potrebbe ipotizzarsi nell'ipotesi in cui il beneficiario del pagamento (e presumibilmente dell'indennizzo) svolga la professione infermieristica.

[9] È ben nota in proposito l'Autorizzazione generale 5/2014 per il trattamento da parte di diverse categorie di titolari che autorizza anche gli istituti di credito al trattamento dei dati sensibili (disponibile sul sito www.garanteprivacy.it). Non trattano dei dati sensibili le Linee guida per trattamenti relativi al rapporto banca-clientela del 25 ottobre 2007 (disponibili sempre sul sito www.garanteprivacy.it). Di particolare interesse, è l'analisi della modulistica bancaria in proposito di consenso al trattamento dei dati sensibili, che può ritenersi nella maggioranza dei casi adempiuto con la clausola generale del tipo "*dà il consenso al trattamento di tali dati sensibili, da parte della banca − ivi compresa la comunicazione ai soggetti appartenenti alle categorie sopra indicate, per i correlati trattamenti − esclusivamente per l'esecuzione di specifiche operazioni o per l'erogazione e la gestione di specifici prodotti/servizi richiesti dal/dalla sottoscritto/a, consapevole che, in mancanza di tale consenso, la banca non potrà eseguire quelle operazioni che richiedono tali trattamenti o comunicazioni"* (es. informativa e consenso UBI Banca disponibile sul sito www.ubibanca.it).

istanza, si può passare a verificare se, in virtù delle regole generali, il trattamento da parte dell'istituto, possa qualificarsi come fonte di responsabilità *ex* artt. 15 cod. priv. e 2050 c.c.

Ci si può domandare allora se sia stato illecito il trattamento del dato, una volta ottenuto, da parte della Banca.

In verità, riteniamo possa sostenersi che in radice difettino requisiti di colpevolezza in capo a quest'ultima, poiché la stessa, nell'automaticamente, e meccanicamente per via informatica, riportare gli estremi della causale nell'estratto conto, non avrebbe avuto ragionevolmente modo di verificare la portata e il contenuto della legge richiamata, in modo da inferirne la potenziale "pericolosità". Una contraria interpretazione della diligenza dell'istituto comporterebbe un onere in capo a questi di verificare volta per volta i contenuti delle leggi richiamate nelle causali di pagamento ovvero di controllare tutti i contenuti delle causali, al fine di evitare potenziali danni, onere che ci appare plausibilmente sovrabbondante rispetto ai mezzi richiedibili all'impresa bancaria.

Anche non volendo aderire a una più restrittiva nozione di dato sensibile "indiretto", appare sostenibile che la condotta della banca non sia configurabile in termini di illecito.

Questa ricostruzione dell'operato della banca, in sostanza quale mero *nuncius*, ci sembra rispondente a quel richiamo alle «profonde trasformazioni operate dalla società industriale e post-industriale» […] al «più ampio dinamismo e circolazione dei soggetti» i quali non solo richiedono «l'individuazione di più efficaci ed adeguate difese» [10] ma anche una realistica considerazione delle sfere di possibile intervento all'interno di una realtà informatizzata e automatizzata.

4. – Un ultimo e finale accenno ci sembra debba esser fatto alle nozioni appena richiamate nel prisma nella disciplina portata dal nuovo regolamento (UE) 2016/679, che segnerà quanto meno per il prossimo ventennio, le coordinate di riferimento del trattamento dei dati personali per i cittadini europei.

Alcune delle considerazioni già fatte possono essere mantenute con riguardo al GDPR, relativamente a:

– distinzione tra dati personali e dati sensibili (*recte,* nel nostro caso, dati relativi alla salute) (art. 4, n. 15);

– limiti al collegamento nel caso di dati personali indirettamente qualificabili come tali. In proposito il considerando (26) fa espresso riferimento al criterio economico e probabilistico sopra accennato [11];

[10] Si tratta di affermazioni contenute nel provvedimento commentato e che sono ripetute, a mo' di mantra, nei più recenti provvedimenti del Supremo Collegio.

[11] "… È opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamen-

– esclusione del trattamento degli istituti di credito dalla disciplina sul trattamento per motivi di interesse pubblico (cons. 54 [12]);

– la distinzione, rimessa alla discrezionalità degli Stati membri, nel definire la base giuridica per la legittimità del trattamento, di dati personali e dati relativi alla salute (art. 9, para. 4) [13].

Sotto questi profili, potrebbe dirsi che il Regolamento poco modifichi rispetto al precedente assetto normativo.

In verità, la rinnovata visione propria del Regolamento che ben ha riguardo all'esponenziale velocità dello sviluppo tecnologico, anche sotto i profili dei requisiti del consenso o della profilazione, è indice di un diverso approccio, ispirato a criteri di maggiore efficacia ed efficienza.

Su di esso, ci sembra possa avanzarsi la considerazione che il baluardo della protezione della *privacy* individuale, a fronte della gestione sempre più capillare e diffusa dei dati personali, sia destinato, quanto meno nei fatti ad arretrare, in una visione realistica delle dinamiche economico – sociali e dell'adeguatezza dei mezzi di tutela, ad oggi.

---

te o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici».

[12] «Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato. Tale trattamento dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche … Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito»

[13] Nel definire, oltre al consenso e ad altri casi specifici, le cause di esclusione dell'antigiuridicità del trattamento di categorie particolari di dati personali (tra cui quelli relativi alla salute), il regolamento prevede che «Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute". Questa previsione apre alla possibilità che il trattamento dei dati sensibili in Italia continui ad essere basato sul modello consenso + autorizzazione del Garante.