1. [Sistema biometrico di rilevazione delle presenze dei dipendenti in una scuola]

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clerici, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito "Codice");

VISTE le segnalazioni pervenute in data 20 luglio, 14 agosto e 12 dicembre 2012;

ESAMINATE le risultanze istruttorie degli accertamenti effettuati in data 28 e 29 novembre 2012 presso la sede del Liceo Scientifico Statale "Giuseppe Battaglini" di Taranto;

ESAMINATA la documentazione acquisita agli atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Antonello Soro;

PREMESSO

1.1. Il Garante, ricevute alcune segnalazioni (in data, rispettivamente, 20 luglio, 14 agosto e 12 dicembre 2012) con le quali si lamentava che presso la sede del Liceo Scientifico Statale "Giuseppe Battaglini" di Taranto sarebbe stato installato un sistema biometrico di rilevazione delle presenze dei dipendenti, al fine di acquisire elementi necessari alla valutazione della complessiva liceità dei trattamenti effettuati, ha disposto accertamenti in loco che sono stati eseguiti dal Nucleo Privacy della Guardia di finanza in data 28 e 29 novembre 2012.

1.2 In particolare, in sede ispettiva, è emerso che:

a. secondo quanto dichiarato dal dirigente scolastico del Liceo, nel dicembre 2011 sarebbe stata avanzata la proposta di installare "un sistema di rilevazione di impronte digitali per attestare l'orario di entrata e […] di uscita del personale ATA [amministrativo tecnico e ausiliario]", oggetto peraltro di una "ipotesi di accordo" con le rappresentanze sindacali (cfr. all. 1 al verbale del 28.11.2012);

b. con circolare del 7 luglio 2012 (prot. n. 8572/C1) indirizzata a tutto il personale A.T.A. – successiva "all'installazione dell'apparecchio" – il dirigente scolastico ha comunicato che "dal giorno 10 luglio 2012 l'accertamento della presenza sarà effettuato in tempo reale attraverso il sistema di rilevazione automatica […]. Il riconoscimento del dipendente avverrà attraverso un lettore di impronte digitali" (cfr. verbale 28.11.2012, All. 3);

c. a seguito della presentazione – da parte di due dipendenti e di una rappresentanza sindacale – di alcune richieste di chiarimenti, il dirigente scolastico ha inviato una nota di risposta (successivamente inoltrata anche al Garante in data 7 agosto 2012) nella quale si precisa che "la suddetta modalità di rilevazione [delle presenze] è stata oggetto di confronto con la RSU di questo istituto", ciò alla luce di quanto stabilito dall'art. 92, comma 3, lett. g), del Ccnl 2006-2009 relativo al comparto scuola; nella nota si è altresì affermato che "il software di gestione […] ha solo la

possibilità di ricevere […] le informazioni riguardanti gli orari di passaggio dei dipendenti e non i loro dati biometrici" (cfr. verbale 28.11.2012, p. 2 e All. 4);

d. le operazioni di trattamento dei dati personali dei lavoratori sarebbero iniziate nel mese di settembre 2012, data in cui "sono state acquisite le impronte digitali dei dipendenti ATA per testare il sistema. Tutt'ora il sistema è in fase di sperimentazione e verifica del funzionamento, anche in attesa della definizione dell'argomento da parte del Garante"; ad ogni buon conto "modalità ufficiale di rilevazione degli orari di entrata e di uscita del personale ATA" sarebbe costituita dall'apposizione della firma nell'apposito registro (cfr. verbale 28.11.2012, p. 2);

e. i dipendenti sarebbero stati informati "sulle caratteristiche dell'impianto e sulle modalità di utilizzo dello stesso" in sede di designazione degli incaricati del trattamento avvenuta in data 9 ottobre 2012 (cfr. verbale 28.11.2012, p. 2);

f. quanto alle finalità perseguite con l'installazione del menzionato sistema, il dirigente ha rappresentato che "si è pensato di sostituire il registro delle firme al fine di avere una puntuale ed attendibile verifica delle presenze e degli ingressi nel luogo di lavoro; è stato escluso l'utilizzo del classico tesserino magnetico in quanto cedibile tra i dipendenti" (cfr. verbale 28.11.2012, p. 3);

g. con riferimento alle caratteristiche del sistema installato – che consentirebbe di estrarre "i principali dati caratteristici dell'immagine dell'impronta digitale, generando un «modello caratteristico» criptato, necessario per identificare l'utente, e senza conservare l'immagine dell'impronta digitale" – ed al suo funzionamento, a seguito dell'accesso al software di gestione effettuato nel corso dell' ispezione, è risultato che a partire dal mese di settembre 2012 sono stati raccolti e archiviati dati personali dei dipendenti (cfr. verbale 29.11.2012, p. 2);

h. secondo quanto dichiarato dal dirigente scolastico, il Liceo non ha provveduto ad effettuare la notificazione del trattamento di dati biometrici previsto dall'art. 37 del Codice ritenendo dubbia la sussistenza dell'obbligo di notificazione posto "che il sistema non conserva le immagini dell'impronta digitale"; tuttavia "[q]ualora si dovesse accertare che tale trattamento possa configurarsi come trattamento di dati biometrici, provvederemo ad effettuare la notificazione al Garante prima dell'adozione di tale sistema, quale modalità di rilevazione ufficiale ed esclusiva delle presenze dei dipendenti. […] in attesa di sciogliere i prefati dubbi, il Liceo […] sospenderà l'utilizzo del sistema di rilevazione delle presenze" (cfr. verbale 29.11.2012, p. 3).

1.3. Ad integrazione degli elementi acquisiti in sede di accertamento, su richiesta dell'Ufficio, con comunicazione dell'8 luglio 2013 il Liceo ha inviato copia degli atti con i quali, in data 9 ottobre 2012, diciotto dipendenti sono stati designati incaricati delle operazioni di trattamento, contenenti altresì informazioni sintetiche sulle caratteristiche del sistema biometrico installato e, con riguardo a quindici lavoratori, anche l'assenso a che "l'apparecchiatura […] installata presso la scuola, preved[a] il rilevamento dell'impronta digitale allo scopo di poter registrare le […] entrate e uscite dall'istituto".

2.1. Sulla base delle risultanze istruttorie risulta accertato che presso il Liceo sono stati effettuati trattamenti di dati biometrici riferiti al personale A.T.A. per finalità di rilevazione delle presenze con conseguente applicazione della disciplina posta a tutela della protezione dei dati personali.

Come più volte ribadito dall'Autorità, infatti, le operazioni concernenti le impronte digitali nonché i dati biometrici dalle stesse ricavati, sia con riguardo alla fase della raccolta che in relazione alla successiva memorizzazione ed utilizzo per le conseguenti operazioni di verifica e raffronto

nell'ambito di procedure di autenticazione, integrando forme (distinte) di trattamento dei dati personali (cfr. art. 4, comma 1, lett. a) e b), del Codice), sono soggette alla disciplina del Codice (sul punto cfr., tra i tanti, Provv. 19 novembre 1999, doc. web n. **42058**; 26 maggio 2011, doc. web n. **1832558**). Ciò anche nel caso in cui il rilievo dattiloscopico, temporaneamente raccolto ai soli fini del completamento della fase di enrollment, venga successivamente utilizzato (sotto forma di codice numerico) per le menzionate operazioni di verifica e raffronto (Provv. n. 265 del 4 ottobre 2012, doc. web n. **2059743**; Provv. 23 gennaio 2008, doc. web n. **2059743**; v. anche il Gruppo dei Garanti europei previsto dall'art. 29 della direttiva 95/46/Ce (di seguito "Gruppo art. 29") dapprima nel Documento di lavoro sulla biometria, WP 80, adottato il 1° agosto 2003, punto 3.1, ed ancora nel Parere 3/2012 sugli sviluppi nelle tecnologie biometriche, WP193, adottato il 27 aprile 2012, p. 5 s.).

2.2. Ciò premesso, deve rilevarsi che in relazione alla valutazione di liceità dei trattamenti dei dati biometrici riferiti a lavoratori, il Garante ha in più occasioni individuato le condizioni in presenza delle quali i trattamenti medesimi possono ritenersi leciti.

In particolare, l'Autorità ha precisato che tali dati possono essere di regola utilizzati solo in casi particolari, tenuto conto delle finalità perseguite dal titolare e del contesto in cui il trattamento viene effettuato, nonché – con specifico riguardo ai luoghi di lavoro – per presidiare l'accesso ad "aree sensibili" in considerazione della natura delle attività ivi svolte (cfr. , tra le decisioni più risalenti, Provv. 21 luglio 2005, doc. web n. **1150679** e da ultimo, con ulteriori richiami, Provv. del 31 gennaio 2013 n. 38, doc. web n. **2304669**).

A mente della prescrizione contenuta nella Regola 2 dell'allegato B) al Codice, il Garante ha poi talvolta prescritto, in relazione a particolari operazioni di trattamento di dati personali, il ricorso a tecniche biometriche di autenticazione quale necessaria misura di sicurezza (cfr., ad esempio, in relazione ad operazioni concernenti i dati di traffico telefonico e telematico, il Provv. 17 gennaio 2008, doc. web n. **1482111**; Provv. 14 febbraio 2013, n. 64).

Da ultimo, l'Autorità ha altresì riconosciuto la legittimità nonché la proporzionalità del trattamento di dati biometrici per finalità di autenticazione dell'utente nell'ambito di servizi di firma digitale remota (cfr. Provv. 31 gennaio 2013, doc. web n. **2311886**).

2.3. Tali presupposti non risultano tuttavia ricorrere nella fattispecie in esame, posto che il sistema biometrico risulta essere stato installato presso il Liceo allo scopo di effettuare la rilevazione delle presenze dei dipendenti. A tale proposito, con riferimento all'applicazione dei principi di necessità nonché di pertinenza e non eccedenza (art. 11, comma 1, lett. d), del Codice) dei trattamenti effettuati in relazione alle finalità perseguite, il Garante ha di regola ritenuto sproporzionato l'impiego generalizzato di dati biometrici per finalità di rilevazione delle presenze dei lavoratori (cfr. Provv. del 31 gennaio 2013 n. 38, doc. web n. 2304669; v. già le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico del 14 giugno 2007, punto 7.1, doc. web n. **1417809**; questo orientamento è stato condiviso, proprio in sede di impugnazione di un'ordinanza-ingiunzione dell'Autorità, dal Trib. Prato, 19 settembre 2011). Tale valutazione tiene conto della possibilità di utilizzare idonee modalità alternative – adottando soluzioni tecnico-organizzative che non incidano sulla libertà e la dignità stessa dei lavoratori interessati (art. 2 del Codice) – preordinate all'accertamento parimenti efficace e rigoroso dell'effettiva presenza dei dipendenti in servizio.

Il titolare del trattamento, infatti, allo scopo di verificare il puntuale rispetto dell'orario di lavoro ben può disporre di altri (più "ordinari") sistemi, meno invasivi della sfera personale nonché della libertà individuale del lavoratore, che non ne coinvolgano la dimensione corporale (cfr. Provv. 31 gennaio 2013, n. 38, doc. web n. **2304669**; con specifico riferimento all'impiego di analoghi sistemi di rilevazione in ambito scolastico cfr. Provv.ti 30 maggio 2013, doc. web n. **2502951** e doc. web n. **2503101**). Aspetti, questi, costitutivi della dignità personale, a presidio della quale sono dettate le discipline di protezione dei dati personali, come emerge dall'art. 2 del Codice. I sistemi basati sull'utilizzo di tecnologie biometriche, infatti, possono operare solo con l'attiva collaborazione personale dei lavoratori interessati in assenza di puntuali disposizioni che la impongano (v. anche Gruppo art. 29, WP193, Parere 3/2012, cit., p. 12, secondo cui "il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico").

2.4. Alla luce di tali orientamenti e degli elementi in atti, non risulta che nel caso specifico ricorrano i suindicati presupposti di legittimità, non essendo stati addotti circostanziati elementi, strettamente rapportati alla specifica realtà lavorativa in esame, da cui si possa effettivamente arguire l'inidoneità di ordinarie misure di controllo e, correlativamente, la reale indispensabilità del trattamento dei dati biometrici dei lavoratori per la finalità suindicata.

Al contrario, risulta che la scelta a favore del sistema biometrico sia stata effettuata in ragione dell'astratta possibilità di utilizzo abusivo dei più tradizionali strumenti automatici di rilevazione delle presenze d'uso comune (quali i badge) (cfr. verbale del 28 novembre 2012, p. 3), né il titolare del trattamento ha riferito che gli ordinari controlli, se del caso a campione, circa la presenza dei lavoratori presso l'istituto scolastico, effettuati per il tramite del personale direttivo (sul quale anzitutto incombe la verifica quotidiana, peraltro di immediata evidenza e comunque di agevole accertamento all'interno di un istituto scolastico), siano risultati insufficienti.

Peraltro tali verifiche appaiono di agevole realizzazione con riguardo ai dipendenti dell'Istituto – rispetto ai quali non sono stati evidenziati comportamenti abusivi né ipotesi di inadempimento rispetto all'esecuzione della prestazione dovuta.

Più in generale, va poi considerato che il trattamento dei dati biometrici per la finalità qui considerata, oltre ad essere in linea di principio (nonché, per quanto detto, nel caso di specie) sproporzionato, potrebbe comunque in concreto rivelarsi di scarsa utilità nel contrasto di eventuali casi di allontanamento dal servizio atteso che tale modalità di rilevazione delle presenze, in difetto di efficaci sistemi di controllo e vigilanza sull'effettiva (operosa) presenza dei lavoratori durante l'arco dell'intera giornata lavorativa, non è di per sé in grado di assicurare l'effettiva presenza sul luogo di lavoro di dipendenti infedeli.

2.5. Nel caso considerato il trattamento risulta altresì essere stato effettuato in violazione della disciplina di protezione dei dati con riferimento al principio di correttezza (art. 11, comma 1, lett. a), del Codice) – atteso che nel corso dell'interlocuzione con i lavoratori che ha preceduto l'installazione del sistema non sono state chiaramente evidenziate le modalità peculiari del trattamento che si sarebbe effettuato (consistenti nell'impiego di tecnologie biometriche), rappresentandosi, in sede di redazione dell'ipotesi di accordo relativo alla stipula del contratto collettivo integrativo d'Istituto del 29.12.2011 (all. 1, verbale 28.11.2012 cit.), che "l'accertamento della presenza [risulterà] attraverso un sistema di rilevazione automatica" (art. 25, lett. b) – nonché in ragione dell'inidoneità delle informazioni rese agli interessati ai sensi dell'art. 13 del Codice.

A quest'ultimo proposito, infatti, non è risultato comprovato che le necessarie informazioni richieste dall'art. 13 del Codice siano state rese preventivamente al personale: in atti risultano copie delle designazioni di personale A.T.A. ad incaricati del trattamento (cfr. all. 6 al verbale 28.11.2012 e nota dell'8 luglio 2013) contenenti altresì (con l'esclusione di tre lavoratori) l'"accettazione" della rilevazione della presenza tramite sistema biometrico e la contestuale indicazione di talune informazioni riferite all'apparecchiatura già installata presso l'istituto. Atteso, tuttavia, che tali designazioni recano la data del 9 ottobre 2012 e che le operazioni di trattamento dei dati biometrici dei dipendenti, secondo quanto dichiarato dal Liceo, sono iniziate nel mese di settembre 2012, non risulta essere stata fornita agli interessati l'informativa – completa degli elementi indicati nell'art. 13 del Codice – anteriormente all'installazione del sistema biometrico e alla sua effettiva attivazione.

2.6. Deve infine rilevarsi che non consta che l'Istituto abbia provveduto alla dovuta notificazione del trattamento ai sensi dell'art. 37, comma 1, lett. a), del Codice, profilo per il quale l'Autorità si riserva di contestare, con autonomo procedimento, la relativa violazione amministrativa.

2.7. Tanto premesso, il Garante, ritenuto che il trattamento effettuato dall'Istituto nel caso di specie sia avvenuto in violazione dei principi di liceità, correttezza, necessità, pertinenza e non eccedenza rispetto agli scopi perseguiti (artt. 11, comma 1, lett. a) e d) del Codice), nonché in violazione dell'art. 13 del Codice dichiara illecito il trattamento dei dati biometrici riferiti ai lavoratori e ne dispone il divieto ai sensi degli artt. 154, comma 1, lett. d), 144 e 143, comma 1, lett. c), del Codice.

2.8. L'Autorità si riserva di valutare con autonomo procedimento la sussistenza di violazioni amministrative, con particolare riferimento all'omessa notificazione al Garante del trattamento dei dati biometrici (art. 37, comma 1, lett. a), del Codice) nonché all'inidonea informativa agli interessati rispetto al trattamento effettuato (art. 13 del Codice).

TUTTO CIÒ PREMESSO, IL GARANTE

in relazione ai descritti trattamenti di dati personali effettuati dal Liceo Scientifico Statale "Giuseppe Battaglini" di Taranto dichiara illecito, nei termini di cui in motivazione, il trattamento dei dati biometrici riferiti ai lavoratori e, ai sensi degli artt. 154, comma 1, lett. d), 144 e 143, comma 1, lett. c), del Codice, ne vieta l'ulteriore trattamento.

Ai sensi degli artt. 152 del Codice e 10 del d.lg. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

2. [Elenchi telefonici on line: illegittimi se la fonte dei dati non è il d.b.u. (archivio elettronico unico)]

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Daniele De Paoli, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice");

VISTI le numerose segnalazioni e reclami, pervenuti all'Autorità, con i quali è stata lamentata la diffusione sul sito www.pronto.it - nella titolarità della Mother s.r.l. (già Mother Technologies di G. Vinci), di seguito indicata come "la società" - di un elenco telefonico on line contenente vari dati (nome e cognome, indirizzo, recapito telefonico, numero della partita IVA) degli interessati, alcuni dei quali hanno anche evidenziato il carattere "riservato" dell'utenza telefonica pubblicata;

CONSIDERATO che è stato segnalato che il sito in questione consente anche la *c.d.* "*ricerca inversa*", ossia la ricerca del nominativo di un abbonato sulla base del suo numero telefonico, senza il consenso espresso dell'interessato;

TENUTO CONTO che alcune delle segnalazioni hanno anche lamentato che la procedura prevista per l'eliminazione dei dati degli interessati dal detto elenco telefonico non sia agevole, essendo richiesta come presupposto necessario la registrazione al detto sito;

CONSIDERATO che - dal verbale redatto dal Nucleo Speciale Privacy della Guardia di Finanza in data 21 aprile 2010, ad esito della notificazione alla società di alcune richieste di informazione formulate dall'Ufficio ex art 157 del Codice, e dalle note del 5 maggio 2010 e del 16 luglio 2010, inviate dalla medesima in risposta a ulteriori richieste di informazioni di questa Autorità – risulta che la società gestisce il detto sito web e possiede una "*banca dati on line*", i cui dati, riferiti sia a persone fisiche sia ad imprese, sono stati acquisiti con le due seguenti modalità: "*mediante elenco telefonico digitale, fornito da Telecom Italia S.p.a. e successivi decadali di aggiornamento, contenenti nuovi inserimenti, modifiche e cancellazioni dei contatti presenti in elenco, acquisiti a partire dall'anno 2002, giusta scrittura privata stipulati con Telecom Italia S.p. a ….*", e "*mediante registrazione di nuovi utenti visitatori del sito, che desiderano rendere visibili i propri contatti….*";

RILEVATO, altresì, che la società – la quale risulta titolare del trattamento dei dati - ha affermato di aver acquisito i dati di alcuni degli interessati che si sono rivolti all'Autorità dal suindicato elenco fornitole da Telecom Italia S.p.a., il quale, in base alla scrittura privata stipulata al fine dell'acquisizione, sarebbe "all'origine e per definizione privo delle utenze riservate per cui il cliente non ha prestato il consenso alla pubblicazione in elenco";

RILEVATO che Telecom Italia S.p.a., nella nota del 18 febbraio 2011, in risposta ad apposita richiesta di informazioni dell'Autorità, ha affermato che il suindicato rapporto contrattuale decorrente dal settembre 2000 con la società è venuto meno con l'attivazione nel 2005 della base di dati unica (di seguito, d.b.u.) e che non ha stipulato con la medesima società alcun contratto di cessione del d.b.u.;

VISTO, altresì, il provvedimento del 15 luglio 2004 (in www.garanteprivacy.it, doc. *web* n. **1032381**) in materia di elenchi telefonici "alfabetici" del servizio universale, con cui l'Autorità ha chiarito che "*è consentita la sola formazione, distribuzione e diffusione degli elenchi, in qualunque forma realizzati, basati sulla consultazione e accesso*" al d.b.u. già previsto dalla delibera Agcom n. 36/02/CONS;

CONSIDERATO, conseguentemente, che non è legittimo formare un elenco telefonico con dati che non siano tratti dal d.b.u., né consentire tramite tale elenco la funzione di *c.d.* "*ricerca inversa*", ossia la ricerca del nominativo di un abbonato sulla base del suo numero telefonico, rilevandosi per di più la mancanza di un consenso espresso dell'interessato a tale funzione;

RILEVATO, altresì, che dall'accertamento condotto con specifico riguardo al predetto sito risulta anche che nel relativo form di registrazione è previsto un unico consenso per diversi trattamenti dei dati, ossia "*per la memorizzazione informatica*" dei dati e per l'invio di "*informazioni di servizio e promozionali*" di interesse dell'utente registrato, in violazione dell'art. 23, comma 3, il quale prevede invece che il trattamento di dati personali da parte dei privati è ammesso solo previa acquisizione di un consenso dell'interessato libero, informato e specifico, con riferimento a un trattamento chiaramente individuato, e da documentare per iscritto;

CONSIDERATO, al riguardo che, come già rilevato da questa Autorità, gli interessati devono essere messi in grado di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei dati che li riguardano, manifestando il proprio consenso - allorché richiesto per legge - per ciascuna distinta finalità perseguita dal titolare (cfr. provv. 24 febbraio 2005, punto 7, in www.garanteprivacy.it, doc. *web* n. **1103045**);

RILEVATA, inoltre, l'inidoneità dell'informativa ex art. 13 del Codice, prevista per il detto *form* di registrazione, che non indica la finalità di diffusione *on line* di dati personali, che invece risulta svolta dalla società;

VISTO l'art. 10 del Codice, in base al quale "*per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare…a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente*", mentre il sito www.pronto.it prevede una procedura complessa per l'esercizio dei suddetti diritti, essendo necessaria a tal fine la registrazione al sito stesso;

RILEVATO che la società, alla luce di un ulteriore accertamento sul sito www.pronto.it, svolto il 28 marzo u.s., risulta svolgere ancor oggi il predetto trattamento dei dati e che questo presenta carattere sistematico;

RITENUTO, inoltre, che l'art. 11, comma 2, del Codice prevede che i dati trattati in violazione della normativa in materia di protezione dei dati personali non possono essere utilizzati;

CONSIDERATO che il Garante, ai sensi degli artt. 143, comma 1, lett. c) e 154, comma 1, lett. d), del Codice, ha il compito di vietare anche d'ufficio il trattamento illecito o non corretto dei dati o di disporne il blocco e di adottare, altresì, gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;

RILEVATA la necessità di adottare nei confronti della società un provvedimento di divieto del trattamento illecito di dati personali - ai sensi degli artt. 143, comma 1, lett. c), e 154, comma 1, lett. d), del Codice – correlato alla costituzione e diffusione on line di un elenco telefonico i cui dati non sono stati tratti dal d.b.u. e utilizzato anche per la funzione di c.*d.* "*ricerca inversa*", in violazione del provvedimento 15 luglio 2004, nonché alla memorizzazione informatica, alla diffusione *on line* di dati personali raccolti sul *web* e all'invio di informazioni di servizio e promozionali in assenza di un'idonea informativa ex art. 13 del Codice e di un consenso libero, specifico e documentato degli interessati ex art. 23, comma 3, del Codice;

TENUTO CONTO che, ai sensi dell'art. 170 del Codice, chiunque, essendovi tenuto, non osserva il presente provvedimento di divieto è punito con la reclusione da tre mesi a due anni e che, ai sensi dell'art. 162, comma 2-ter del Codice, in caso di inosservanza del medesimo provvedimento, è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila a centottantamila euro;

RITENUTA altresì la necessità di adottare nei confronti della società un provvedimento prescrittivo ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice qualora la società intenda continuare ad effettuare il trattamento dei dati personali in questione;

RISERVATA, con autonomo procedimento, la verifica dei presupposti per contestare le violazioni amministrative concernenti il rilascio di inidonea informativa e l'omessa acquisizione del consenso (artt. 13, comma 4 e 161; 23, commi 1 e 3 e 162, comma 2-*bis* del Codice);

RILEVATO, altresì, che resta impregiudicata la facoltà per gli interessati di far valere i propri diritti in sede civile in relazione alla condotta accertata (cfr. anche art. 15 del Codice), con specifico riguardo agli eventuali profili di danno;

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 del 28 giugno 2000;

RELATORE il dott. Giuseppe Fortunato;

TUTTO CIÒ PREMESSO IL GARANTE:

a) dichiara illecito il trattamento di dati personali posto in essere da Mother s.r.l., con sede legale in Siracusa, via Nizza n. 21, tramite la costituzione e diffusione *on line* di un elenco telefonico i cui dati non sono stati tratti dal d.b.u. e utilizzato anche per la funzione di "ricerca inversa", in violazione del provvedimento 15 luglio 2004, nonché tramite la memorizzazione informatica, la diffusione on line di dati personali raccolti sul web e l'invio di informazioni di servizio e

promozionali in assenza di un consenso libero, specifico e documentato degli interessati ex art. 23, comma 3, del Codice;

b) vieta a Mother s.r.l., ai sensi degli artt. 143, comma 1, lett. c) e 154, comma 1, lett. d), del Codice, l'ulteriore trattamento di qualunque dato personale già acquisito consistente:

1) nella costituzione e diffusione *on line* di un elenco telefonico i cui dati non sono stati tratti dal d.b.u., e utilizzato anche per la funzione di *c.d.* "*ricerca inversa*", in violazione del suindicato provvedimento;

2) nella memorizzazione informatica, nella diffusione *on line* di dati personali raccolti sul *web* e nell'invio di informazioni di servizio e promozionali, senza che sia stata rilasciata un'idonea informativa e che risulti documentato per iscritto uno specifico consenso;

c) prescrive a Mother s.r.l., ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c), del Codice, di adempiere - fornendo adeguata documentazione all'Autorità entro trenta giorni dalla comunicazione del presente provvedimento – a quanto di seguito indicato:

1) qualora la società intenda continuare a raccogliere on line dati personali degli utenti, modificare il form di raccolta dei dati personali sul sito www.pronto.it, previsto per la registrazione al servizio di consultazione dell'elenco telefonico digitale, inserendo, nell'informativa ex art. 13 del Codice, la finalità della diffusione *on line* dei dati personali raccolti sul *web* e formulando la richiesta agli interessati di un preventivo consenso distinto e facoltativo per ciascuna delle finalità perseguite dalla società (memorizzazione informatica, diffusione on line di dati personali, invio di informazioni di servizio, invio di comunicazioni promozionali);

2) qualora la società intenda continuare a inviare comunicazioni promozionali, adottare le misure necessarie e opportune, tramite il rilascio di un'idonea informativa e l'acquisizione di un consenso libero, specifico e documentato per iscritto;

3) semplificare le modalità previste per l'esercizio dei diritti ex artt. 7 ss. del Codice, in particolare eliminando l'obbligo della previa registrazione al detto sito.

Si ricorda che avverso il presente provvedimento è possibile, ai sensi dell'art. 152 del Codice, proporre opposizione con ricorso all'autorità giudiziaria ordinaria, in particolare al Tribunale del luogo ove risiede il titolare del trattamento, entro il termine di trenta giorni dalla data di comunicazione del medesimo provvedimento, e che l'opposizione non sospende l'esecuzione del provvedimento (v. art. 152, comma 5 del Codice).