Decreto n. 94/2021

Tribunale ordinario di Taranto

Taranto, 27 luglio 2021

OGGETTO: Disposizioni in materia di privacy, sicurezza informatica, integralità e disponibilità dei dati.

La Presidente del Tribunale

considerato che il "Documento programmatico della sicurezza dei dati trattati con strumenti elettronici", adottato il 2 dicembre 2019 ai sensi del D.lgs. 196/203 ("Codice in materia di protezione dei dati personali" (di seguito D.P.S.) deve essere aggiornato alla luce delle modifiche normative intervenute;

visto il regolamento (UE) 2016/679 del Parlamento europeo (*Generai Data Protection Regulation*) di seguito G.D.P.R., e il regolamento del Consiglio d'Europa in data 27 aprile 2016 in tema di protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati che ha abrogato la direttiva 95/46/CE;

viste le direttive (UE) 2016/680 del Parlamento europeo e del Consiglio d'Europa in data 27 aprile 2016 relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle Autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, che ha abrogato la decisione quadro 2008/977/GAI del Consiglio d'Europa;

visto il decreto legislativo 18 maggio 2018, n. 51 (recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (EU) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"), che ha abrogato la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), modificato il d. lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), ed ha dato attuazione alla direttiva (UE) 2016/680, regolamentando il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzioni di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse sia da parte dell'Autorità giudiziaria che da parte delle Forze di Polizia;

visto il decreto legge 9 febbraio 2012, n. 5, convertito con modificazioni, dalla legge 4 aprile 2012, n. 35, che ha apportato semplificazioni anche in materia di protezione di dati personali e ha abolito l'obbligo di adozione o di aggiornamento, entro il 31 marzo di ogni anno, del D.P.S (art. 45 che ha abrogato il punto 19 dell'Allegato B, nonché l'art. 34, comma 1, lett. g, e comma 1 bis);

letto il provvedimento del Garante per la protezione dei dati personali in data 5 dicembre 2013 n.

545 ("Trasmissione ai terzi di dati personali del dipendente da parte dei datore di lavoro") che fa seguito ai provvedimenti emessi dalla medesima Autorità il 1° marzo 2007 ("Utilizzo degli strumenti elettronici da parte dei lavoratori"), il 13 ottobre 2008 ("Dismissione di apparecchiature elettriche ed elettroniche contenenti dati personali"), il 27 novembre 2008 ("Funzioni dell'amministratore di sistema"), il 2 dicembre 2010 ("Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità d'informazione giuridica"), il 2 marzo 2011 ("Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web");

letta la nota del Ministero della Giustizia - Dipartimento Organizzazione Giudiziaria n. 26/18 reg. circolari del 28 giugno 2018, con cui è stata trasmessa la nota prot. n. 21611 del 27 giugno 2018 a firma del capo di Gabinetto, ove si specifica che, a norma dell'art. 4, punto 7 G.D.P.R («titolare del trattamento» è *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*) la titolarità del trattamento dei "dati giudiziari appartiene agli stessi Uffici giudiziari";

visto il decreto 7 agosto 2018 con il quale il Ministro della Giustizia ha designato il Responsabile della protezione dei dati con riferimento ai dati trattati dagli Uffici giudiziari nell'esercizio di funzioni non giurisdizionali;

vista la nota in data 13 dicembre 2018, n. 41553 della Direzione Generale Sistemi Informativi Automatizzati in materia di "Piano strategico della sicurezza";

rilevato che il regolamento (UE) 2016/679 (entrato in vigore il 25 maggio 2016 e applicabile in tutti gli Stati membri a partire dal 25 maggio 2018) intende garantire e bilanciare la protezione dei dati di carattere personale (incrementati in maniera esponenziale nella condivisione e raccolta a seguito della rapida evoluzione tecnologica), costituente un diritto fondamentale (art. 8, par. 1, Carta dei diritti fondamentali dell'Unione europea e art. 16, par. 1, TFUE), con la libera circolazione dei dati stessi (art. 1 del regolamento UE 2016/679);

PREMESSO CHE IL PRESENTE DOCUMENTO SI PROPONE DI:

- attuare, in ciascuna fase procedimentale, i principi di protezione dei dati di carattere personale, tenuto conto della loro natura, del loro oggetto, delle finalità del trattamento, delle specifiche caratteristiche delle operazioni compiute;
- scongiurare forme di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta;
- contemperare le esigenze di protezione dei dati di carattere personale con quelle della loro libera circolazione (art. 1 regolamento UE 2016/679);
- elaborare specifici modelli organizzativi.

DATO ATTO CHE:

il capo 4 del regolamento (UE) 2016/679 disciplina l'attuazione del principio di "responsabilizzazione" e prevede le seguenti figure:

1. "titolare del trattamento" quale persona fisica o giuridica, autorità pubblica, organismo che, singolarmente o insieme ad altri, detta le finalità e i mezzi del trattamento dei dati personali (4.7);
2. "responsabile del trattamento", persona fisica o giuridica, autorità pubblica o altro organismo che tratta i dati personali per conto del titolare del trattamento (4.8);
3. "responsabile della protezione dei dati" (*data protection officer*, DPO, art. 37), responsabile per il trattamento di tutti i dati giudiziari operati dagli Uffici e effettuati nell'esercizio di funzioni giurisdizionali (capo 4 Sezione 4 del Regolamento UE 2016/679 e art. 37, paragrafo 1, lettera A,

del medesimo regolamento).

Pertanto, in base all'organizzazione interna:

1. Titolare del trattamento è il presidente pro tempore del Tribunale, che detta le finalità e i mezzi del trattamento dei dati personali (art. 4.7 del Regolamento EU 2016/679) e assolve agli obblighi previsti dalle fonti sovranazionali e dalle norme interne che vi hanno dato attuazione (capo III della Direttiva (UE) 2016/680) in relazione all'attività giudiziaria e agli incombenti ad essa connessi, alle attribuzioni riservate dalla disciplina ai magistrati o ad essi delegati da altri organismi, eccezion fatta per i dati relativi all'attività amministrativa svolta negli Uffici giudiziari, rientranti nella titolarità del Ministero della Giustizia (cfr. nota del Capo di Gabinetto del Ministero della Giustizia in data 27.06.2018 e Decreto Ministeriale del 7.08.2018).
2. Responsabile del trattamento è il presidente vicario del Tribunale pro tempore incaricato di trattare i dati personali per conto del titolare del trattamento (art. 4.8 del regolamento (UE) 679 e art. 2.2 lett. I del d.lgs. n. 51/2018) e di seguire le attività di trattamento dei dati riconducibili all'esercizio delle funzioni giurisdizionali.
3. Responsabile della protezione dati, per i trattamenti di dati non effettuati nell'esercizio delle funzioni giurisdizionali, è il soggetto nominato con D.M. 7 agosto 2018 quale responsabile per la protezione dei dati per il Ministero della Giustizia, dr.ssa Doris Lo Moro, fatta salva la nomina di altro RPD da parte dello stesso Ministero, come previsto dalla citata nota del capo di Gabinetto n. 21611 del 27.06.2018.
4. Incaricati del trattamento dei dati sono: tutti i magistrati, professionali e non; tutti i dipendenti amministrativi in servizio nell'ufficio, che accedono ad affari di pertinenza dell'ufficio medesimo per l'esecuzione materiale di operazioni di trattamento, ciascuno in relazione all'attività istituzionalmente svolta.
5. Tenuto conto della posizione all'interno della struttura e in stretta correlazione con le specifiche responsabilità che afferiscono alla posizione stessa, anche sotto il profilo della distinzione tra attività giurisdizionale e attività amministrativa, i magistrati presidenti di sezione, i direttori o i funzionari cui è affidata la direzione di un servizio svolgono anche attività di vigilanza sul rispetto delle misure di sicurezza da parte degli incaricati del trattamento e di coordinamento delle attività, funzionale alla osservanza uniforme delle regole che presiedono alla *privacy* e alla sicurezza informatica.
6. Amministratori dei servizi informatici ex art. 4 del D.M. 27 aprile 2009 sono quelli individuati, a livello distrettuale ed interdistrettuale, per ciascun sistema in uso sulla rete RUG, dalla Direzione Generale per i Sistemi Informativi Automatizzati del Ministero della Giustizia.

   Collaboratori degli ADSI, attualmente in servizio presso il tribunale, sono il funzionario CISIA dr. Giuseppe De Bellis, l'esperto informatico CISIA Massimiliano Pavone e gli addetti sistemisti del consorzio SIRFIN P.A. Catucci Licia, Buonfrate Roberto e Montanaro Giuseppe. Costoro svolgono i compiti ad essi contrattualmente assegnati per garantire il funzionamento del sistema informatico, sotto la direzione del direttore CISIA di Napoli e in collaborazione con il titolare ed il responsabile del trattamento, verificando altresì che non siano effettati collegamenti non autorizzati alla LAN.

7. L'attivazione delle nuove utenze ADN, con contestuale comunicazione di nome utente, password e relativo Pin di sicurezza è di competenza della dr.ssa Mariangela Eramo, direttore della segreteria di presidenza

DISPONE

1. Gli incaricati del trattamento devono osservare puntualmente le disposizioni contenute nel presente provvedimento nonché le vigenti prescrizioni in materia di sicurezza.
2. I predetti direttori e funzionari, con riguardo ai programmi utilizzati, verificano a campione, con cadenza almeno semestrale e con l'eventuale collaborazione del personale assegnato ai rispettivi servizi, la correttezza e l'aggiornamento dei dati immessi nei programmi informatici e segnalano al capo dell'ufficio eventuali disfunzioni non eliminabili con le risorse e conoscenze a disposizione delle cancellerie.
3. In relazione all'attività di trattamento dei dati ciascun soggetto autorizzato si impegna a:
   - trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
   - conservare i supporti informatici e/o cartacei contenenti dati personali in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati medesimi o siano facilmente oggetto di danneggiamenti intenzionali o accidentali;
   - restituire al termine delle operazioni affidate gli atti e documenti cartacei contenenti dati personali e loro copie;
   - effettuare copie dei dati personali oggetto di trattamento esclusivamente se necessario e previa autorizzazione del titolare o responsabile del trattamento o suo soggetto designato;
   - effettuare le operazioni di trattamento dei dati personali nel rispetto della normativa vigente e delle misure tecniche e organizzative adeguate al livello sicurezza a cui può essere esposto il trattamento;
   - segnalare al titolare o responsabile del trattamento o suo soggetto designato eventuali circostanze che rendano necessario od opportuno aggiornare le predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta;
   - dare immediata comunicazione al titolare o responsabile del trattamento in tutti i casi in cui si rilevi o si sospetti una violazione dei dati personali;
   - effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal titolare o dal responsabile del trattamento o suo soggetto designato e secondo le modalità stabilite dai medesimi;
   - mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente ad esso;
   - fornire al titolare o responsabile del trattamento o suo soggetto designato, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo;

- prestare la più ampia e completa collaborazione al titolare o responsabile del trattamento o suo soggetto designato, al fine di compiere quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

4. **Elenco dei trattamenti.** L'art. 5 del Reg. n. 679/2016 elenca i *"principi applicabili al trattamento di dati personali"*: a) liceità, correttezza e trasparenza; b) limitazione della finalità; c) minimizzazione dei dati; d) esattezza; e) limitazione della conservazione; f) integrità e riservatezza; g) responsabilizzazione.

4.1- Il personale amministrativo è abilitato, in funzione esclusiva dei compiti svolti da ciascuno, al trattamento dei dati personali nell'ambito di:

a) iscrizioni e annotazioni - anche informatiche - nei registri ufficiali generali, nelle rubriche prescritte, nei registri di comodo e nei registri di passaggio; dette annotazioni e iscrizioni devono peraltro essere corrette e complete;
b) iscrizioni e annotazioni sulle copertine dei fascicoli;
comunicazioni su supporto cartaceo, telematico e/o con mezzi di comunicazione a distanza con altri uffici giudiziari e nell'ambito dell'ufficio;
c) comunicazioni relative all'informazione processuale;
d) archiviazione di atti e documenti;
e) ricezione e inoltro della corrispondenza di ufficio, anche in via telematica;
f) attività amministrativa relativa alla gestione del personale di magistratura e amministrativo;
g) attività residuale concernente i compiti istituzionali dell'ufficio.

Le attività di cui ai punti a), b), c), e d) riguardano prevalentemente od esclusivamente le cancellerie; l'attività di cui al punto e) riguarda sia le cancellerie che le segreterie della presidenza e della dirigenza amministrativa; i punti f), g) ed h) riguardano le appena citate segreterie.

4.2- Gli incaricati del trattamento, con riguardo all'attività posta in essere senza l'ausilio di strumenti elettronici, si atterranno alle seguenti prescrizioni:

- i fascicoli cartacei, nella fase di trasporto all'interno dell'ufficio, devono permanere nei corridoi il tempo strettamente necessario per la loro consegna;
- gli incaricati devono avere accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
- nessuno può accedere all'archivio se non autorizzato; il trasporto di atti da e per l'archivio deve essere eseguito in modo da evitarne l'accesso da parte di persone non autorizzate; analogamente si procederà nella produzione di copie di atti;
- i fascicoli, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati, curati personalmente e riservatamente dagli stessi o comunque da dipendenti dell'ufficio per l'eventuale attività finalizzata alla riproduzione fotostatica di atti, e restituiti al termine delle operazioni affidate;
- il materiale elettorale deve essere conservato in ambienti chiusi a chiave, ben custoditi e l'accesso ai quali sia controllato dal responsabile del servizio;
- nel caso in cui i documenti o l'archivio contengano dati afferenti ai procedimenti civili o penali (cosiddetti *dati giudiziari,* secondo la terminologia utilizzata dal testo previgente del D. Lgs. n. 196/2003), oppure dati appartenenti ad una delle *particolari categorie* di cui all'art. 9 Reg. n. 679/2016 (già *dati sensibili,* ferma restando la non completa

sovrapponibilità): gli atti e i documenti contenenti detti dati, se affidati agli incaricati del trattamento, devono essere conservati, fino alla restituzione, in armadi muniti di serratura; particolare attenzione deve essere prestata ai fascicoli e agli atti relativi alle intercettazioni provenienti dalle Procure della Repubblica, che devono essere trattati e movimentati esclusivamente dal personale incaricato di eseguire i prescritti adempimenti e conservati in armadi chiusi a chiave sino alla restituzione alle Procure stesse con registro di passaggio, fatto salvo il rispetto del Protocollo di intesa sottoscritto il 9.09.2020 dal Procuratore della Repubblica f.f. e dal Presidente della sezione gip, relativo alla gestione dei fascicoli riguardanti le intercettazioni a seguito della entrata in vigore del d.l. 161/2019, convertito con modifiche dalla L. n. 7/2020.

- i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento devono essere conservati e custoditi con le modalità suddette; in particolare le cassette di fonoregistrazione devono essere custodite, a cura del cancelliere del dibattimento a ciò addetto, in armadio accuratamente chiuso a chiave e sito in ambiente non facilmente accessibile al pubblico in assenza del personale dell'ufficio.

4.3-Trattamento dei dati personali relativo all'utilizzo di strumenti elettronici; disciplinare interno ex provvedimento del Garante per la protezione dei dati personali in data 1° marzo 2007.

Il richiamato provvedimento 1.3.2007 del Garante per la protezione dei dati personali ha segnalato la necessità di preservare adeguatamente la riservatezza dei lavoratori con riguardo all'utilizzo della posta elettronica e della rete *internet* e l'opportunità che sia redatto un disciplinare interno alla struttura.

Preliminarmente è bene ribadire il contenuto del provvedimento della scrivente in data 20.07.2020, nonché formalizzare il seguente disciplinare:

a) la posta elettronica, cui hanno accesso i soggetti formalmente abilitati per ragioni di servizio, deve essere utilizzata - avendo l'accortezza di non divulgare notizie riservate o dati personali il cui trattamento si riveli eccedente o non pertinente - per motivi direttamente riconducibili alla prestazione lavorativa, o dalla medesima prestazione occasionati nel senso sopra precisato; in tale ultima ipotesi l'utilizzo avviene sotto la personale responsabilità dell'intestatario dell'utenza di posta elettronica;
b) l'utilizzo della rete internet, per i soggetti formalmente abilitati per ragioni di servizio, è finalizzato alla acquisizione, attraverso la connessione a siti prevalentemente istituzionali e comunque di sicura affidabilità, di notizie e conoscenze necessarie o utili per il servizio svolto;
c) la finalità istituzionale che connota l'utilizzo della rete e la non inerenza alla specificità dell'utente-persona fisica esclude la possibilità del download di file musicali o multimediali;
d) è necessario che i file di lavoro, non inerenti a programmi informatici, siano dallo stesso utente salvati e conservati, anche con riguardo alla posta elettronica e ad internet, in quantità tendenzialmente limitata, onde evitare, nell'interesse proprio e dell'ufficio, che la sovrabbondanza di dati contenuti nei file di ordinario lavoro comprometta le operazioni di back-up;
f) i limiti istituzionali di utilizzo della posta elettronica e della rete internet sono assistiti dai controlli effettuabili, dal personale a ciò autorizzato dall'Amministrazione centrale, sulla base dell'analisi dei tracciamenti preordinati dal sistema adottato dall'Amministrazione stessa, ai quali l'ufficio non ha possibilità di autonomo e diretto accesso.

4.4-Pubblicità dei dati di debitori nelle esecuzioni immobiliari (prescrizione ex art. 154, comma 1, D.

Lgs. 196/2003 del Garante per la protezione dei dati personali del 7.2.2008).

E' necessario non riportare nell'avviso di vendita e nelle copie pubblicate delle ordinanze e delle relazioni di stima l'indicazione delle generalità del debitore e di ogni altro dato personale idoneo a rivelare l'identità di quest'ultimo e di eventuali soggetti terzi non previsto dalla legge e comunque eccedente e non pertinente rispetto alle procedure di vendita in corso.

La prescrizione, dettata per le **esecuzioni immobiliari,** è estesa anche alle analoghe attività relative alle **esecuzioni mobiliari** ed alle **procedure concorsuali.**

Con specifico riguardo ai fascicoli delle **procedure concorsuali,** occorre avere cura che gli atti all'interno degli stessi siano suddivisi in cartelle differenziate a seconda della qualificazione degli utenti per la consultazione.

4.5-Deliberazione del C.S.M. in data 28.1.2015: "*Notificazione di una convocazione per testimoniare - riservatezza dei dati personali*".

Con tale delibera il C.S.M., ritenuta eccedente la finalità del trattamento la indicazione cumulativa, nei decreti di convocazione, dei dati anagrafici e dei luoghi di residenza delle persone chiamate a testimoniare, ha indicato due possibili, valide alternative:

- predisposizione di una citazione *individuale*, nel corpo della quale non compariranno nominativi e dati diversi da quelli del singolo teste citato;
- emissione di decreto di citazione cumulativo con oscuramento delle generalità e degli altri dati identificativi dei testi non destinatari della comunicazione, in modo da pervenire, in fatto, al confezionamento di un provvedimento individuale.

Di tali principi dovrà tenersi conto nelle attività di notificazione ai testi effettuata, su disposizione del giudice, ad opera delle cancellerie, nonché nelle notifiche degli ordini di traduzione.

4.6-Trattamento dei dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica.

Con la citata deliberazione del Garante per la protezione dei dati personali del 2.12.2010 sono state dettate prescrizioni sul trattamento dei dati riguardanti la riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica.

Sebbene tragga spunto dall'art. 47 del codice della *privacy* ora abrogato, detta delibera può considerarsi ancora attuale, in relazione alle disposizioni di cui all'art. 2-*duodecies* del D.Lgs. 101/2018, commi 1 e 3.

Le linee guida in parola riguardano esclusivamente l'attività di informazione giuridica perciò esse:

- non riguardano i trattamenti non effettuati per ragioni di giustizia (a norma dell'art. 2-*duodecies,* comma 4, *si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività' ispettive su uffici giudiziari*)
- non incidono sulle norme processuali.

Tanto premesso, il contenuto di dette linee-guida può essere così essere precisato:

- presupposto per l'applicazione delle misure prescritte è l'avvenuta pubblicazione del provvedimento dell'Autorità Giudiziaria (dal Garante definita, a tal fine, < *onere* >);
- a norma dell'art. 52, commi 1 e 2 del codice della *privacy* (tuttora in vigore), *l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria*

dell'ufficio ... che sia apposta a cura della cancelleria o segreteria ... un 'annotazione volta a precludere ... l'indicazione delle generalità e di altri dati identificativi;

- la competenza a decidere sull'istanza spetta all'Autorità Giudiziaria presso cui pende il giudizio, che provvederà con decreto;
- *l'annotazione in discorso può essere disposta dal magistrato anche di ufficio (comma 2);*
- *in caso di accoglimento della richiesta, spetta alla cancelleria o segreteria giudiziaria darvi esecuzione; in attesa della eventuale acquisizione del timbro cui fa riferimento la deliberazione del Garante, gli addetti provvederanno ad annotare per iscritto la formula indicata* "In caso di diffusione, omettere, a norma dell'art. 52 d. Igs. 196/2003, le generalità e gli altri dati identificativi di ... *";*
- *non sussistono a carico della cancelleria o segreteria ulteriori obblighi; in particolare, non sussiste l'obbligo di cancellare materialmente i dati dell'interessato sulle copie dei provvedimenti rilasciate a chi ne abbia diritto e che riportino la menzionata annotazione;*
- *in caso di accoglimento della richiesta o di decisione d'ufficio da parte del magistrato, la prescrizione in ordine alla* anonimizzazione *vincola tutti i soggetti che svolgono attività di diffusione e riguarda anche le massime giuridiche;*
- con riferimento a quanto previsto dal comma 5 dell'art. 52 codice *privacy*[1], il Garante ha precisato, in particolare, quanto segue: *"In relazione a quesiti che sono stati posti con riferimento ad alcuni particolari profili del divieto posto dal comma 5 dell'art. 52, deve essere, in primo luogo, chiarito che il divieto di diffusione delle generalità, degli altri dati identificativi e degli ulteriori dati che consentano di identificare i minori o le parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone non può, ovviamente, trovare applicazione ove la lettura della sentenza o di altro provvedimento non permetta, facendo applicazione dell'ordinaria diligenza, di individuare il coinvolgimento di un minore o delle parti dei menzionati procedimenti. Ciò chiarito, si precisa che: - la disposizione intende fare riferimento non solo alla sentenza o altro provvedimento emessi nel procedimento in cui è coinvolto il minore o in materia di rapporti di famiglia e di stato delle persone, ma anche a qualsiasi sentenza o altro provvedimento che contenga dati personali, anche di terzi, che consentono, "anche indirettamente ", di svelare l'identità delle persone tutelate; - la norma richiede ai soggetti che diffondono i provvedimenti per finalità di informazione giuridica di esercitare un'ordinaria diligenza nell'esame del testo delle sentenze e degli altri provvedimenti. In particolare, rientrano nell'oggetto del divieto le informazioni che, nella valutazione della fattispecie concreta, permettano di risalire agevolmente all'identificazione del minore o delle parti nei giudizi in questione (ad esempio, i nominativi dei genitori del minore o la scuola da questo frequentata, o l'indirizzo dell'abitazione delle parti processuali)".*

4.7-<u>Sicurezza del trattamento dei dati dei magistrati.</u>

---

[1] Il citato comma 5 così recita: *"Fermo restando quanto previsto dall'articolo 734-bis del codice penale relativamente alle persone offese da atti di violenza sessuale, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell'annotazione di cui al comma 2, le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone".*

I fascicoli personali dei magistrati ordinari, anche in tirocinio, e onorari sono custoditi in armadi chiusi a chiave e con ante non trasparenti; i dati sensibili devono essere conservati separatamente rispetto alle altre informazioni negli stessi contenute (il Garante per la tutela dei dati ha chiarito che il suddetto principio non fa venir meno l'unitarietà del fascicolo e risponde all'esigenza di garantire la protezione dei dati sensibili) in apposita stanza chiusa a chiave.

I fascicoli relativi ad esposti, congedi ordinari e straordinari, procedimenti disciplinari e pre-disciplinari dei magistrati sono custoditi in armadi chiusi a chiave e con ante non trasparenti in apposita stanza chiusa a chiave.

I responsabili/coordinatori di settore verificano che gli incaricati del trattamento, durante le relative operazioni di gestione dei dati, compresa la fase di archiviazione, utilizzino tutte le misure idonee a mantenere la riservatezza dei dati personali.

4.8-Sicurezza del trattamento dei dati dei dipendenti.

I fascicoli personali dei dipendenti sono custoditi in armadi chiusi a chiave e con ante non trasparenti; i dati sensibili devono essere conservati separatamente rispetto alle altre informazioni negli stessi contenute (il Garante per la tutela dei dati ha chiarito che il suddetto principio non fa venir meno l'unitarietà del fascicolo e risponde all'esigenza di garantire la protezione dei dati sensibili).

Le cartelle sanitarie e di rischio (art. 41 d.lgs. 9 aprile 2008 n.81 e succ. integrazioni/modificazioni) relative ai lavoratori sottoposti a sorveglianza ai sensi del d.lgs. 81/2008 sono conservate in armadi chiusi a chiave.

La documentazione relativa alla fissazione delle visite mediche deve essere conservata in armadi chiusi a chiave - a cura dei dipendenti incaricati di collaborare con il datore di lavoro.

L'accesso ai suddetti documenti è consentito esclusivamente agli organi di vigilanza ed al medico competente.

Eventuali elenchi contenenti la tipologia delle assenze dei dipendenti e relativa documentazione sono analogamente conservati in spazi riservati ed i relativi dati possono essere diffusi solo in forma anonima/aggregata, per adempimenti statistici.

I dati riguardanti l'attribuzione dei buoni pasto sono custoditi in luogo riservato ed accessibile solo agli incaricati del trattamento dei dati ed utilizzati esclusivamente per le richieste di fornitura e per eventuali adempimenti statistici.

I "fogli-firma" devono essere mantenuti in cartelle chiuse che non ne consentano la visione agli utenti, così come la cartella nella quale i dipendenti depositano le loro istanze, in attesa che vengano acquisite dal dipendente che gestisce il sistema di rilevazione delle presenze.

I dati relativi alla gestione delle presenze del personale vengono trattati esclusivamente dagli addetti, sotto la vigilanza del responsabile, compreso l'accesso al sistema informatizzato di gestione, dal quale ciascun dipendente deve poter ricavare esclusivamente le informazioni che lo riguardano.

4.9-Direttive impartite dalla D.G.S.I.A. ai sensi dell'art. 8 del D.M. 27 aprile 2009 in tema di controllo degli accessi al sistema informatico della giustizia.

Con tale direttiva la Direzione Generale S.I.A. ha raccomandato in generale di "sensibilizzare il personale nel porre la dovuta attenzione nell'attività di inserimento dei dati nei sistemi informatici, giacché buona parte degli interventi di assistenza applicativa risultano dovuti ad errori e/o inesattezze nell'attività di data-entry effettuata dal personale dell'amministrazione e non a problematiche tecniche del sistema informatico".

Nello specifico le direttive suddette possono riassumersi come segue.

- L'inserimento della password di accesso alla postazione di lavoro va effettuato esclusivamente a cura dell'utente.
- Nome utente e password sono strettamente personali. Il nome utente e la password sono le chiavi accesso a molti degli applicativi ministeriali e a tutte le risorse a cui l'utente ha accesso.
- Pertanto l'utente è tenuto a:
  - non comunicare a terzi le password.
  - non annotare le password su supporti posti in vicinanza della propria postazione di lavoro, o comunque incustoditi.
  - attenersi a tutte le indicazioni contenute nel manuale per la sicurezza.
- In occasione degli interventi sistemistici, non deve essere effettuata la comunicazione della password dell'utente a chi effettua le operazioni tecniche.
- Sui personal computer desktop assegnati ai magistrati e al personale amministrativo non può essere configurata una utenza con i privilegi di amministratore.
- L'utenza con privilegi di amministratore viene configurata esclusivamente sui portatili assegnati ai magistrati dall'Amministrazione, previa sottoscrizione del modulo di assunzione delle responsabilità, prodotto dalla D.G.S.I.A.

Con particolare riferimento al settore penale, la successiva circolare a firma dei Direttori Generali della Giustizia Penale e dei Sistemi Informativi Automatizzati prot. n. 78341.U dell'11.6.2013, ha inoltre raccomandato agli uffici l'immediatezza, l'esaustività e la correttezza delle annotazioni e dell'inserimento dei dati, così da realizzare il loro allineamento e corrispondenza e rendere possibile lo scambio di informazioni provenienti dai diversi uffici.

DISPONE

che il presente provvedimento sia comunicato:

- a tutti i magistrati professionali ed onorari in servizio in questo Tribunale e ad esso destinati;
- a tutti i giudici di pace in servizio nel circondario del Tribunale di Taranto;
- a tutto il personale amministrativo in servizio nei predetti Uffici;
- ai magistrati di riferimento per l'informatica di questo Tribunale;
- ai referenti informatici distrettuali per il Distretto della Corte di Appello di Lecce;
- al funzionario CISIA in sede, anche per la comunicazione alla competente Direzione Generale del Ministero ed al personale addetto all'assistenza sistemica;
- al Presidente del Consiglio dell'Ordine degli Avvocati di Taranto.

La Presidente del Tribunale
Rosa Anna Depalo