

Decreto n. 184 /2019

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



## Tribunale Ordinario di Bari

### IL PRESIDENTE DEL TRIBUNALE

- **visto** il Regolamento europeo n. 679/2016, in vigore dal 25.5.2018, e che ha abrogato la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- **considerato** che a norma dell'art. 2 par. 2 lett. d) del predetto Regolamento, esso non si applica al settore penale, di cui si occupa la direttiva UE 2016/680, come attuata dal D.Lgs. n. 51/2018;
- **visto** il D.Lgs. n. 196/2003 (*"codice in materia di protezione di dati personali"*), come modificato dal D.Lgs. n. 101/2018, contenente disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del 27.4.2016, in vigore dal 19.9.2018;
- **visto** il D.M. 27.3.2000 n. 264 (*"Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari"*) nonché il D.M. 27.4.2009 (*"Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia"*), che *"fissa le regole procedurali per la gestione del sistema informatico del Ministero della Giustizia e per la tenuta informatizzata dei registri informatizzati tenuti, a cura delle cancellerie o delle segreterie, presso gli uffici giudiziari, ovvero dei registri previsti da codici, da leggi speciali o da regolamenti, comunque connessi all'espletamento delle attribuzioni e dei servizi svolti dall'Amministrazione della giustizia, come previsti dall'art. 1 del Decreto Ministeriale 27 marzo 2000, n. 264"*;
- **visti** i provvedimenti del Garante per la protezione dei dati personali in data 1.3.2007 (*linee guida del Garante per posta elettronica e internet*) e in data 27.11.2008, modificato dal successivo provvedimento del 25.6.2009 (*misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*);
- **visto** il D.M. 7.8.2018, con il quale il Ministero della Giustizia ha disposto, ai sensi dell'art. 37, par. 1 lett. a) del Regolamento europeo 2016/679, la nomina del responsabile della protezione dei dati per il Ministero della Giustizia;
- **letta** la circolare n. 21611.U del 27.6.2018, con la quale il Ministero della Giustizia ha ritenuto, con riguardo alla titolarità dei dati, che *"tutti i dati trattati relativi all'attività amministrativa svolta negli uffici giudiziari dovrebbero rientrare nella titolarità di questa Amministrazione"*, e che *"altro è da dirsi, invece, per i dati giudiziari, la cui titolarità [...] appartiene all'ufficio giudiziario"*;

- **preso atto** che l'art. 45 del D.L. n. 5/2012, convertito in Legge 4.4.2012, n. 35 (in G.U. n. 82 del 6.4.2012), ha abrogato la lett. g) del comma 1 dell'art. 34 del D.Lgs. n. 196/2003 citato - che prevedeva, quale "misura minima", la tenuta di un aggiornato documento programmatico sulla sicurezza, nell'ambito dei trattamenti che si avvalgono di strumenti informatici - e i paragrafi da 19 a 19.8 e 26 del disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B del sopra richiamato D.Lgs. 196/2003;
- **visto** il Reg. Min. Giustizia 12.12.2006, n. 306 ("*disciplina del trattamento dei dati sensibili e giudiziari da parte del Ministero della Giustizia, adottato ai sensi degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196*");
- **dato atto** che le misure concernenti il trattamento dei dati, con e senza l'ausilio degli strumenti elettronici, ad opera degli incaricati appartenenti all'organico del personale amministrativo sono state adottate dopo aver sentito al riguardo il dirigente amministrativo del Tribunale e dell'Ufficio del Giudice di Pace di Bari, responsabili del trattamento dei dati con riguardo agli organici del personale amministrativo;
- **considerato** che, in virtù dell'art. 40, comma 2, del D.L. 6.12.2011 n. 201, convertito in Legge 22.12.2011 n. 214, per "*dato personale*" devono intendersi soltanto le informazioni riferite alle persone fisiche e non più anche alle persone giuridiche, enti o associazioni, essendo state queste ultime parole - già contenute all'art. 4, comma 1, lett. b) del D. Lgs. n. 196/2003 - soppresse dall'art. 40 del D.L. n. 201/2011;
- **ritenuto** che le intervenute modifiche legislative fanno apparire necessario, o quantomeno opportuno, procedere alla redazione di un documento che abbia contenuti - ricognitivi e programmatici - che riproducano sinteticamente, nei tratti essenziali, quelli del pur soppresso *documento programmatico sulla sicurezza* in materia di privacy, sicurezza informatica, integralità e disponibilità dei dati sia in considerazione dell'attuale assetto organizzativo sia per l'oggettiva utilità di riproporre le regole che attengono a dette correlate materie, sia ancora per la circostanza che esigenze formali di aggiornamento periodico sono comunque tuttora previste con riguardo alla individuazione dell'ambito del trattamento consentito agli incaricati (art. 34, comma 1, lett. d) D.Lgs. 196/2003 e paragrafo 15 dell'allegato B, con riguardo ai trattamenti con strumenti elettronici, e art. 35 del medesimo D.Lgs. e paragrafo 27 dell'allegato B, con riguardo ai trattamenti che prescindono da strumenti elettronici);
- **letto** l'art. 47 del D.Lgs. n. 196/2003, che esonera gli uffici giudiziari dalla notificazione al Garante per la protezione dei dati personali;

**Nella qualità di titolare del trattamento dei dati ex art. 46 D.Lgs. n. 196/2003, sia come Presidente del Tribunale che come Coordinatore dei vari Uffici del Giudice di Pace operanti nel Circondario;**

## DISPONE

### 1) - Persone autorizzate al trattamento dei dati personali<sup>1</sup>.

---

<sup>1</sup> L'art. 4, paragrafo 1, n. 2), Reg. 679/2016 ("*Definizioni*") così recita: "*Ai fini del presente regolamento s'intende per: [...] 2) «trattamento»: qualsiasi operazione o insieme di operazioni,*



Sono autorizzati al trattamento dei dati giudiziari e, quindi, incaricati del trattamento stesso, tutti i magistrati, professionali e non, e 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 e nell'ambito dei trattamenti consentiti di cui al successivo paragrafo 6.

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 ovvero quelli referenti nei vari Uffici del Giudice di Pace, i dirigenti amministrativi, i direttori o i funzionari cui è affidata la direzione di un reparto 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.

Gli incaricati del trattamento devono osservare puntualmente le disposizioni contenute nel presente provvedimento nonché le vigenti prescrizioni in materia di sicurezza.

Sarà cura della segreteria della presidenza e della dirigenza amministrativa, per quanto di rispettiva competenza, fornire copia del presente atto ai magistrati e ai dipendenti che, assunto servizio nell'ufficio successivamente alla data della sua emanazione, risulteranno automaticamente designati, in virtù dell'atto stesso, quali incaricati del trattamento.

A norma dell'art. 13 del D.M. 27.4.2009, "*Il dirigente o responsabile dell'ufficio è responsabile della qualità dei dati e ne verifica periodicamente, anche attraverso il personale dell'ufficio all'uopo incaricato ed anche utilizzando strumenti automatici, correttezza ed aggiornamento, assumendo le conseguenti iniziative.*" Pertanto i predetti responsabili dei reparti, con riguardo ai programmi utilizzati, **verificano a campione, con cadenza almeno semestrale** e con l'eventuale collaborazione del personale assegnato ai rispettivi reparti, **la correttezza e l'aggiornamento dei dati immessi nei programmi informatici** e segnalano al capo dell'ufficio e al dirigente amministrativo (ove esistente) eventuali disfunzioni non eliminabili con le risorse e conoscenze a disposizione delle cancellerie. Tale attività di controllo riveste **particolare importanza** anche in considerazione della delicatezza e complessità dei programmi in uso, e della necessità di realizzare e conservare **l'integrità** e correttezza dei dati ai fini della efficace **digitalizzazione** della giustizia.

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;

---

*compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".*

- 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 l'aggiornamento delle 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.

## **2) - Amministratori dei servizi informatici (ADSI)**

Al riguardo, malgrado la richiesta ed il relativo sollecito di cui alle note prot. 6757 del 26.9.2019 e 7104 dell'8.10.2019 trasmesse al Dirigente C.I.S.I.A. di Bari e da questi inoltrate alla D.G.S.I.A. del Ministero della Giustizia, non sono stati forniti i nominativi degli amministratori di sistema e del personale addetto all'assistenza sistemica in quanto la richiesta ed il relativo sollecito sono "*all'attenzione della Direzione Generale*", così come risulta dalla nota pervenuta il 28.10.2019 a firma del predetto Dirigente C.I.S.I.A.

Pertanto, in mancanza di nuove indicazioni, non può che farsi riferimento ai nominativi indicati nel decreto n. 29/2011 del 31.3.2011, a firma congiunta del Presidente del Tribunale di Bari e del Dirigente Amministrativo del medesimo ufficio, trasmesso ai vari responsabili con nota prot. 686 del 28.4.2011 a firma del Dirigente Amministrativo.

Tanto premesso, deve sottolinearsi che gli amministratori di sistema - rientrando necessariamente tra i soggetti autorizzati al trattamento dei dati - hanno il compito di *“porre in essere le iniziative necessarie per il rispetto degli standard di sicurezza e della normativa sulla tenuta informatizzata dei registri”*, come previsto dal D.M. 27.4.2009.

A norma dell'art. 4, comma 5, del D.M. 27.4.2009, *“L'amministratore dei servizi informatici, se nominato responsabile del trattamento da parte dei titolari delle banche dati, pone in essere le iniziative necessarie per il rispetto degli standard di sicurezza e della normativa sulla tenuta informatizzata dei registri, anche alla luce delle direttive concordemente emanate dai titolari delle banche dati.”*; tale compito è da intendersi invariato nell'attuale assetto normativo, in base al quale la figura dell'ADSI è assimilabile a quella di un *responsabile esterno* alla struttura (ma non all'Amministrazione giudiziaria) e, comunque, è pur sempre un *incaricato del trattamento* che svolge le proprie funzioni al servizio della struttura cui è stato destinato.

Le suddette unità di personale assicurano il supporto tecnico nell'analisi del fabbisogno informatico, il monitoraggio delle dotazioni *hardware* e *software* e la tenuta della relativa documentazione, l'aggiornamento della banca dati interna, della verifica e valutazione delle disfunzioni relative al funzionamento delle apparecchiature informatiche, le relazioni con le ditte incaricate dell'assistenza, del supporto nell'attività di destinazione/distribuzione dell'*hardware* in dotazione.

### **3) - Magistrati di riferimento per l'informatica.**

Magistrati di riferimento per l'informatica nel Tribunale di Bari sono il dott. Francesco Cavone, per il settore civile, e il dott. Francesco Mattiace, per il settore penale.

### **4) - Assistenza sistemistica ed applicativa. Incaricati del servizio di assistenza.**

Vale in questo caso quanto già detto all'inizio del precedente paragrafo 2 e quindi che, malgrado la richiesta ed il relativo sollecito di cui alle note prot. 6757 del 26.9.2019 e 7104 dell'8.10.2019 trasmesse al Dirigente C.I.S.I.A. di Bari e da questi inoltrate alla D.G.S.I.A. del Ministero della Giustizia, non sono stati forniti i nominativi degli amministratori di sistema e del personale addetto all'assistenza sistemistica in quanto la richiesta ed il relativo sollecito sono *“all'attenzione della Direzione Generale”*, così come risulta dalla nota pervenuta il 28.10.2019 a firma del predetto Dirigente C.I.S.I.A.

Pertanto, in mancanza di nuove indicazioni, non può che farsi riferimento ai nominativi indicati nel decreto n. 29/2011 del 31.3.2011, a firma congiunta del Presidente del Tribunale di Bari e del Dirigente Amministrativo del medesimo ufficio, trasmesso ai vari responsabili con nota prot. 686 del 28.4.2011 a firma del Dirigente Amministrativo. Detti nominativi vanno integrati con quello del dott. Antonio Lepore, atteso che lo stesso Dirigente del C.I.S.I.A. di Bari ha comunicato - con altra nota a sua firma pervenuta pure il 28.10.2019 - che il dott. Antonio Lepore *“dal 28 ottobre '19 sarà inserito temporaneamente nel gruppo di tecnici esterni che operano nella sede di Via Dioguardi, a supporto delle attività sistemistiche ed applicative dei sistemi informatici”*.

Tanto premesso, occorre ribadire che gli interventi finalizzati a preservare l'operatività e la sicurezza del sistema possono essere effettuati in assenza o impedimento dell'utente solo nel

caso in cui presentino carattere di indispensabilità e indifferibilità; tale valutazione sarà previamente effettuata dal vertice giudiziario o amministrativo dell'ufficio, al quale dovrà essere tempestivamente richiesta specifica autorizzazione; all'interessato sarà data prontamente notizia dell'effettuato intervento a cura del responsabile della segreteria della dirigenza amministrativa, su impulso del soggetto che ha autorizzato l'intervento.

Alcuni interventi dei sistemisti sono realizzati in remoto, attraverso lo strumento BOMGAR.

Nello svolgimento dei loro compiti, i sistemisti terranno altresì presente quanto prescritto al paragrafo 9), lett. d).

I sistemisti, come tutti gli incaricati del trattamento, sono obbligati al segreto d'ufficio.

#### **5) - Informazioni in ordine alla fruizione del servizio di assistenza sistemistica e applicativa.**

Per richiedere l'assistenza sistemistica, occorre seguire le istruzioni riportate nell'apposita pagina *intranet* da cui risultano:

numero verde: 800.868.444

e-mail: spocgiustizia@telecomitalia.it

Va qui inoltre ricordato che con nota 23444.U del 15.10.2013, la D.G.S.I.A. ha fatto presente che il contratto di assistenza sistemistica e applicativa prevede, su richiesta dell'utente interessato, la possibilità di accedere da remoto sulla singola postazione di lavoro con le modalità indicate nella medesima nota.

#### **6) - 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.

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;

c) comunicazioni su supporto cartaceo, telematico e/o con mezzi di comunicazione a distanza con altri uffici giudiziari e nell'ambito dell'ufficio;

d) comunicazioni relative all'informazione processuale;

e) archiviazione di atti e documenti;

f) ricezione e inoltro della corrispondenza di ufficio, anche in via telematica;

g) attività amministrativa relativa alla gestione del personale di magistratura e amministrativo;

h) 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.

#### **7) - Prescrizioni riguardanti i trattamenti senza l'ausilio di strumenti elettronici.**

Con riguardo all'attività posta in essere senza l'ausilio di strumenti elettronici, gli incaricati del trattamento 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 sovrapposibilità): 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.

L'accesso agli archivi è consentito solo al personale che per disposizione di servizio è addetto ad essi e a soggetti diversi che operano sotto la vigilanza del suddetto personale.

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.

#### **8) - Trattamento dei dati personali e udienze civili e penali; accesso dei difensori nelle cancellerie.**

Per quanto riguarda la materia civile, giova riportare un breve stralcio, della deliberazione del C.S.M. 24.7.2007, che argomenta sulla base degli artt. 83, 84, 116 e 117 disp. att. c.p.c. e ai cui suggerimenti è opportuno prestare particolare attenzione:

*“se un problema di affissione del ruolo di udienza non si pone per le cause istruttorie, essendo le stesse chiaramente non pubbliche, ragion per cui per esse il ruolo non deve essere reso pubblico, diversamente esso si pone per quelle di discussione. ... Ne consegue, chiaramente, che gli accorgimenti suggeriti già nella delibera del 16 luglio 2003 possono ancora essere considerati come quelli minimi cui riferirsi per un accettabile temperamento tra le esigenze, se non contrapposte perlomeno coesistenti, sopra rappresentate. E, dunque, è opportuno ribadire che l'affissione del ruolo sulla porta della sala destinata alla pubblica udienza non contenga necessariamente i nomi delle parti e l'oggetto delle specifiche cause, potendo ben essere sufficiente la mera indicazione del numero di registro generale della controversia”.*

In ordine alla problematica relativa all'accesso dei difensori in cancelleria, la deliberazione citata del C.S.M., sulla scorta del parere dell'ufficio studi e documentazione n. 294/2007, ha osservato che *“il quadro normativo vigente, pur consentendo alcune deroghe all'applicazione della normativa sulla privacy, atteso che la predisposizione dei ruoli di udienza e l'accesso dei difensori alle cancellerie rientrano tra le attività svolte “per ragioni di giustizia”, comunque impone adeguati accorgimenti finalizzati a tutelare la riservatezza delle parti nei confronti di chi non abbia alcun interesse processuale sulle controversie che riguardano queste ultime”.*

E' dunque necessario: evitare in tutti i modi che *“trapelino notizie sui processi a favore di persone non espressamente portatrici di interessi processuali sugli stessi”*; attivarsi in modo che *“le scrivanie degli operatori siano sistemate in modo da non rendere immediatamente accessibile a chicchessia l'accesso alle scansie contenenti i fascicoli non ancora definiti”*; aver cura nella custodia degli archivi; *“rilasciare informazioni solo ai difensori muniti di mandato ed ai loro stretti collaboratori”*. Per quanto riguarda le udienze penali, è necessario e sufficiente fare qui riferimento agli artt. 471 (*pubblicità dell'udienza*) e 472 (*casi in cui si procede a porte chiuse*) c.p.p.

#### **9) - 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 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.

Premesso che la posta elettronica, per gli utenti abilitati in ragione del servizio svolto, è funzionale ad una maggiore rapidità ed efficacia della comunicazione, sia tra addetti all'ufficio, sia tra addetti e soggetti allo stesso estranei; che la finalità istituzionale non può non costituire connotato assolutamente preminente dell'utilizzo di detta modalità elettronica di comunicazione; che, peraltro, non può essere sottaciuto che la posta elettronica ha natura e sostanza di *“corrispondenza”*, con tutte le inevitabili implicazioni in termini di pregnante

riferimento del contenuto dei messaggi elettronici alla persona umana in quanto tale; che messaggi, formalmente o apparentemente avulsi da un contesto propriamente prestazionale, sono, tuttavia, spesso occasionati immediatamente dall'attività lavorativa e contribuiscono a realizzare quel clima di serenità e di virtuosa confidenzialità capace di favorire una collaborazione più efficace per il servizio; che non è preventivabile con certezza che, con riguardo a ciascun utente abilitato, il collegamento a soli siti istituzionali esaurisca le esigenze connesse con il servizio; che non sussistono esigenze particolari che consiglino controlli ulteriori rispetto a quelli che già prevede il sistema, si ritiene opportuno 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) i sistemisti hanno l'obbligo (come espressamente raccomandato dal provvedimento 1°.3.2007 del Garante) di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità specifiche di manutenzione e sicurezza, senza realizzare attività di controllo a distanza, anche di propria iniziativa;

e) 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.

#### **10) - 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 secondo della qualificazione degli utenti per la consultazione<sup>2</sup>.

**11) - Deliberazione del C.S.M. in data 28.1.2015: “Notificazione di una convocazione per testimoniare - riservatezza dei dati personali”.**

Con nota prot. n. P1957/2015 del 30.1.2015 il C.S.M. ha trasmesso la delibera del precedente 28.1.2015 concernente la problematica, segnalata dal Garante per la protezione dei dati personali, della tutela della riservatezza dei dati personali di coloro che sono convocati a testimoniare nell'ambito dei procedimenti penali.

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 dai 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.

**12) - Trattamento dei dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica.**

Con nota prot. n. 34296.U del 10.3.2011, il Ministero della Giustizia ha trasmesso la deliberazione del Garante per la protezione dei dati personali del 2.12.2010, con la quale sono state dettate prescrizioni sul trattamento dei dati riguardanti la riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica.

Per quanto la normativa sia stata oggetto di importanti modifiche e per quanto l'art. 47 del codice della *privacy* dal quale traeva spunto detta deliberazione sia stato abrogato dal D. Lgs. 101/2018 (le norme di riferimento, in luogo dell'art. 47 predetto, possono ora essere

---

<sup>2</sup> Si riporta il testo dell'art. 90 l. fall. (*fascicolo della procedura*): 1 - *Immediatamente dopo la pubblicazione della sentenza di fallimento, il cancelliere forma un fascicolo, anche in modalità informatica, munito di indice, nel quale devono essere contenuti tutti gli atti, i provvedimenti ed i ricorsi attinenti al procedimento, opportunamente suddivisi in sezioni, esclusi quelli che, per ragioni di riservatezza, debbono essere custoditi separatamente.* 2 - *Il comitato dei creditori e ciascun suo componente hanno diritto di prendere visione di qualunque atto o documento contenuti nel fascicolo. Analogo diritto, con la sola eccezione della relazione del curatore e degli atti eventualmente riservati su disposizione del giudice delegato, spetta anche al fallito.* 3 - *Gli altri creditori ed i terzi hanno diritto di prendere visione e di estrarre copia degli atti e dei documenti per i quali sussiste un loro specifico ed attuale interesse, previa autorizzazione del giudice delegato, sentito il curatore.*

considerate quelle contenute nell'art. 2-duodecies del D.Lgs. 101/2018, commi 1 e 3 ), le prescrizioni del Garante sono da considerarsi vigenti.

Premesso che le *linee guida* adottate dal Garante del trattamento dei dati personali riguardano esclusivamente l'attività di informazione giuridica e che restano pertanto esclusi dal relativo ambito di afferenza i trattamenti non effettuati per ragioni di giustizia (*"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."*, comma 4 dell'art. 2-duodecies richiamato); e che *"le presenti linee guida non incidono sulle norme processuali"*, come dichiara la deliberazione del Garante, 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. lgs. 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*<sup>3</sup>, 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*

<sup>3</sup> 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."*

*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)".*

### **13) - Raccomandazioni della D.G.S.I.A.**

Con nota 9353.U, in data 23.3.2009, la Direzione Generale S.I.A. ha raccomandato 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”*; in particolare per quanto concerne il settore penale, con circolare a firma dei Direttori Generali della Giustizia Penale e dei Sistemi Informativi Automatizzati prot. n. 78341.U dell'11.6.2013, diramata in sede di informatizzazione dei registri penali tramite il S.I.C.P., sono state raccomandate agli uffici l'immediatezza, l'eshaustività 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.

L'inserimento dei predetti passi delle richiamate note ministeriali nel presente provvedimento è finalizzato all'ulteriore sensibilizzazione del personale sulla **necessità di svolgere con attenzione l'attività di data-entry**. Si richiama anche l'**attività di controllo sull'utilizzo dei programmi informatici, di cui al paragrafo 2), demandata ai responsabili delle cancellerie**.

## **DISPONE**

che, a cura della segreteria, il presente provvedimento sia immediatamente comunicato:

- a tutti i magistrati professionali ed onorari in servizio nel Tribunale di Bari;
- a tutti i Giudici di Pace in servizio nel Circondario del Tribunale di Bari;
- al Sig. Dirigente amministrativo del Tribunale di Bari e, a cura di quest'ultimo, al personale amministrativo in servizio nel medesimo Tribunale;

- al Sig. Dirigente amministrativo dell'Ufficio del Giudice di Pace di Bari e, a cura di quest'ultimo, al personale amministrativo in servizio nel medesimo Ufficio;
- a tutto il personale amministrativo in servizio negli altri Uffici del Giudice di Pace operanti nel Circondario del Tribunale di Bari, diversi da quello indicato al punto precedente;
- ai magistrati di riferimento per l'informatica del Tribunale di Bari;
- ai referenti informatici distrettuali per il Distretto della Corte di Appello di Bari;
- al Sig. Dirigente del CISIA di Bari anche per la comunicazione, a sua cura, alla competente Direzione Generale del Ministero ed al personale addetto all'assistenza sistemica;
- al Sig. Presidente del Consiglio dell'Ordine degli Avvocati di Bari;
- ai Sigg.ri Presidenti di tutti gli Ordini professionali di Bari, i cui iscritti possono essere inseriti negli albi dei periti o dei consulenti tecnici di ufficio.

Bari, 29 ottobre 2019.

Il Presidente del Tribunale  
(Domenico De Facendis)

