Note sulla *privacy* negli uffici giudiziari.

Indice-sommario: 1 - Fonti di disciplina; 2 – I dati personali; 3 - Titolari del trattamento; 4 - Responsabile della Protezione dei dati (R.P.D.); 5 - Registri dei trattamenti; 6 - La figura del responsabile del trattamento e quella degli incaricati; 7 - La valutazione d'impatto sulla protezione dei dati (DPIA); 8 - Il trattamento dei dati nell'ambito dei rapporti di lavoro; 9 – L' informativa ex artt. 13 e 14 Reg. 679/2018; - 10 - La figura dell'amministratore dei sistemi informatici.

1 - Fonti di disciplina.

La materia del trattamento dei dati personali è stata modificata, nel corso del 2018, da alcuni interventi normativi – innanzitutto, dal Regolamento Europeo 2016/679, immediatamente applicabile in tutti gli stati dell'Unione Europea ed entrato in vigore il 25.5.2018 – dai quali è scaturito un quadro particolarmente complesso.

Prendendo in considerazione anche il tema della sicurezza informatica e delle importanti questioni correlate al trattamento dei dati effettuato, sempre più frequentemente, a mezzo delle nuove tecnologie e, sotto il profilo delle fonti di disciplina, anche dei decreti e dei provvedimenti del Garante italiano della *privacy*, con riguardo agli uffici giudiziari vanno considerati i testi normativi sotto indicati.

- Regolamento Europeo sulla *privacy* 2016/679 ("*Regolamento* […] *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati*)"), di seguito: Reg. 679), entrato in vigore in data 25.5.2018.

A norma dell'art. 2, par. 2, lett. d) Reg. 679, il Regolamento predetto non si applica al settore penale, di cui si occupa la direttiva UE 2016/680 e il D. Lgs attuativo n. 51/2018, di cui si dirà successivamente.

Gli artt. 2, par. 1 Reg. 679, e 1, c. 2 D. Lgs. 51/2018, di cui anche si dirà in seguito, con norme sostanzialmente identiche, stabiliscono che entrambi i provvedimenti normativi si applicano al "*trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*" (così il Reg. 679). Pertanto l'applicazione di tale composita normativa ha come presupposto la presenza di un *ausilio tecnologico* o di un *archivio strutturato*, di "*uno strumento, cioè, che consenta una facile, efficiente*

e sistematica interazione tra il soggetto e i dati personali, perché in quei casi sorgono i maggiori rischi per le libertà e i diritti delle persone"[1].

- Codice della privacy (D. Lgs. 196/2003, come modificato dal D. Lgs. 101/2018 - "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati*", entrato in vigore il 19.9.2018[2])**.**

- Disposizioni di legge o di Regolamento che regolano i procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado, richiamate espressamente dall'art. 2-*duodecies*, c. 1 del D. Lgs. 101/2018 ("*in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonchè dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di*

[1] Cfr. "*Manuale per il trattamento dei dati personali*", a cura di G. Comandè e G. Malgieri, *Gruppo 24 ore*, pag. 8. Per archivio si intende "*qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico*;" (art. 4, n. 6, Reg. 679). In base al Considerando 15 del Reg. 679, "*Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.*".

2 "Il decreto legislativo contiene un corpus di norme complesso e interviene con abrogazioni e modificazioni sulla quasi totalità dei 186 articoli del codice della privacy vigente. In particolare, articoli 1 e 2 del provvedimento modificano la Parte I del Codice della privacy dedicata alle disposizioni generali. Gli attuali 46 articoli che compongono la Parte I sono infatti abrogati dalla riforma e ridotti a 16: le disposizioni generali sul trattamento dei dati personali sono infatti ora prevalentemente contenute nel Regolamento. Sono introdotte nella I parte del Codice 14 nuove disposizioni (articoli da 2-bis a 2-quinquiesdecies) che integrano quanto disposto dal Regolamento in materia di fondamento giuridico del trattamento, limitazioni ai diritti degli interessati, titolare e responsabile del trattamento, regole deontologiche e categorie particolari di dati.". (www.camera.it; link: https://temi.camera.it/leg18/provvedimento/la_protezione_dei_dati_personali.html)

Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento.").

Il richiamato art. 2-*duodecies* D. Lgs. 101 è stato formulato "*in applicazione dell'art. 23, par. 1, lett. f), del Regolamento*" (Reg. 679): pertanto, a rigore, non si riferisce al settore penale, cui è dedicato espressamente il D. Lgs. 51/2018 - di cui si dirà al punto successivo - come confermato dalla precisazione di cui al successivo comma 4 del medesimo art. 2-*duodecies*, in base alla quale le "*ragioni di giustizia*" sono riferite agli "*affari e controversie*" (nonché "*i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonche' i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari*").

- D. Lgs. 51/2008, attuativo della direttiva UE 2016/680 ("*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa 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 e che abroga la decisione quadro 2008/977/GAI del Consiglio*"), che detta una disciplina speculare rispetto a quella del Reg. 679 e concerne il trattamento dei dati in ambito penale, prevedendo alcune norme specifiche per i dati trattati nei procedimenti penali[3].

---

[3] Monica A. Senor (in www.ictsecuritymagazine.com, link: https://www.ictsecuritymagazine.com/articoli/una-overview-sulla-data-protection-in-ambito-di-polizia-e-giustizia-penale/): "*Nel suo insieme il decreto, così come la direttiva, presenta la stessa struttura del Regolamento con il quale, non a caso, ha sempre viaggiato abbinato nel suo iter approvativo. In particolare, all'art. 3 sono previsti gli stessi sei principi posti a presidio di qualsiasi trattamento di dati personali, al netto di due peculiarità: 1) è escluso, rispetto al GDPR, il principio di trasparenza e 2) è stato aggiunto, con riferimento al principio di conservazione, un obbligo di analisi periodica dei dati al fine di verificare la persistente necessità di conservazione dei dati, a cui è associato un obbligo di cancellazione o di anonimizzazione decorso il termine di conservazione*. […] *A fronte di queste linee comuni, il decreto si discosta, invece, sensibilmente dal GDPR in relazione a sei profili: categorizzazione dei dati e degli interessati, liceità del trattamento, trasferimenti all'estero, sicurezza, decisioni automatizzate e sanzioni. L'art. 4 del decreto, in attuazione degli artt.6 e 7 della direttiva, introduce un'importante disposizione che impone al titolare del trattamento, tenuto conto delle finalità e per quanto possibile (locuzione invero un po' generica), di tenere distinti i dati personali a seconda che siano fondati su fatti o su valutazioni nonché di differenziarli in relazione ai soggetti interessati, categorizzati, sulla scorta della terminologia tecnica adottata dal codice di procedura penale, in: persone sottoposte ad indagine, imputati (anche in relazione a procedimenti connessi o collegati), condannati in via definitiva, persone offese, parti civili, persone informate sui fatti e testimoni. L'art.5, in tema di liceità del trattamento, prevede, coerentemente col fatto che si tratta di trattamenti effettuati da autorità pubbliche, che l'unica valida base giuridica, oltre al diritto*

- DM 27.3.2000, n. 264 ("*Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari"*) e dal 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"*[4].

- Provvedimento del Garante per la protezione dei dati personali in data 1° marzo 2007 (del. n. 13), con il quale il predetto Garante ha prescritto ai datori di lavoro privati e pubblici di "*adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l´onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli*;", e ha indicato inoltre, ai medesimi datori di lavoro, alcune linee guida a garanzia degli interessati, in particolare per ciò che riguarda l´adozione e la pubblicizzazione di un disciplinare interno alla struttura.

Il provvedimento suddetto è tuttora in vigore, in considerazione di quanto previsto dall'art. 22, c. 4 del d. Lgs. 101/2018 ("*A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento* [Reg. 679] *e con le disposizioni del presente decreto*."), nonchè dall'art. 88 Reg.

---

dell'Unione europea, sia costituita dalla fonte normativa, legislativa o regolamentare, italiana, salvo che per le decisioni basate su trattamenti automatizzati in ordine ai quali viene imposta, attesi gli elevati rischi per i diritti e le libertà degli interessati sottesi a tale tipologia di trattamenti, una riserva di legge. […] *In punto sicurezza l'art.25, 1° co., del decreto prevede, come regola generale, lo stesso meccanismo di* accountability *introdotto dal GDPR con riferimento all'ampia discrezionalità lasciata al titolare del trattamento nella scelta delle misure tecnico-organizzative da adottare, purché idonee a garantire un livello di sicurezza adeguato al rischio di violazione dei dati; tuttavia, la tutela della sicurezza nella specifica materia risulta rafforzata dalla previsione (art.25, 2° co.), con riferimento ai trattamenti automatizzati, di una serie di misure obbligatorie volte a garantire il controllo dell'accesso alle attrezzature ed ai dati, dei supporti, dell'utente, dell'introduzione (inteso come inserimento), del trasporto (inteso come trasmissione), della trasmissione (inteso come comunicazione) e della conservazione dei dati, nonché misure atte ad assicurare la recovery, l'affidabilità e l'integrità dei sistemi.*".

[4] Il D.M. 28.12.2015 indica, poi, le specifiche tecniche per l'adozione, nel processo civile e penale, delle tecnologie dell'informazione e della comunicazione.

679 ("*Trattamento dei dati nell'ambito dei rapporti di lavoro*"; unica norma dettata in materia), in base al quale "*Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro* […]".

- D.M. 7.8.2018, con il quale il Ministero della Giustizia ha disposto, ai sensi del richiamato art. 37, par. 1 lett. a) Reg. 679, la nomina del "*Responsabile della Protezione dei Dati per il Ministero della Giustizia*" nella persona di un magistrato, affidandogli, "*nel rispetto di quanto previsto dall'art. 39, par. 1 Reg. 679*", "i *compiti e funzioni*" indicati dal medesimo articolo, nonché della *"tenuta del registro delle attività di trattamento*" (in applicazione - è da ritenersi - dell'art. 38, par. 6 Reg. 679, citato nella indicazione dei motivi in diritto del decreto, in base al quale articolo "*Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.*").

2 – I dati personali.

La definizione di *dato personale* è fornita dall'art. 4, par. 1, Reg. 679: "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)*" (identica la definizione data dall'art. 1, c. 1, lett. a) del D. Lgs. 51/2018).

Il medesimo art. 4 introduce il concetto di *identificativo*: "*si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*.".

Con il Reg. 679, la categoria dei *dati sensibili,* già prevista dall'art. 4, c. 1, lett. d) del testo originario del D. Lgs. 196/2003*,* è stata assorbita nella definizione di *categorie particolari di dati personali,* che godono di protezione rafforzata: "*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare*

dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona." (art. 9 Reg. 679)[5].

In ambito penale, in particolare, l'art. 7 del D. Lgs. 51/2018 prevede che il trattamento dei dati di cui al citato art. 9 reg. 679 "*è autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le liberta' dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge […] ovvero, ferme le garanzie dei diritti e delle liberta', se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato*.".

Ai sensi dell'abrogato art. 4, c. 1, lett. e) del testo del D. lgs. 196/2003 precedentemente vigente, erano considerati "*"dati giudiziari" i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;*".

Come rilevato dal Servizio Studi della Camera dei Deputati, il concetto di *dati giudiziari*, con l'entrata in vigore del Reg. 679, è stato sostituito da quello, in verità non del tutto sovrapponibile, di *dati relativi a condanne penali e reati*[6], categoria che è presa in considerazione dalla normativa al solo effetto di prevedere che il relativo trattamento può essere svolto (D. Lgs. 101/2018, art. 2-*octies*) solo sotto il controllo dell'Autorità pubblica, con le garanzie ulteriori previste in ambito penale dal D. Lgs. 51/2018, o laddove sia autorizzato da norme nazionali (in assenza di tali norme, i trattamenti e le garanzie "*sono individuati con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante*." - art. 2-*octies* D. Lgs. 101/2018).

---

[5] A norma dell'art. 22, c. 2 D. Lgs. 101/2018, "*A decorrere dal 25 maggio 2018 le espressioni «dati sensibili» e «dati giudiziari» utilizzate ai sensi dell'articolo 4, comma 1, lettere d) ed e), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del Regolamento (UE) 2016/679 e ai dati di cui all'articolo 10 del medesimo regolamento.*". (La rubrica dell'art. 10 reg. 679 è la seguente: "*Trattamento dei dati personali relative a condanne penali e reati*".)

[6] "[…] *con riguardo alla categoria dei dati giudiziari, essa è sostituita dai dati relativi a condanne penali e reati, il cui trattamento può essere svolto in base alle specifiche norme del Regolamento e al nuovo articolo 2-octies del Codice*.".

3 - Titolari del trattamento.

Con circolare n. 21611.U, in data 27.6.2018, 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, in forza della richiamata previsione dell'art. 4, appartiene all'ufficio giudiziario*" e, con riguardo alla nomina del Responsabile della Protezione dei dati (RPD), che è opportuno procedere alla nomina di un *unico* Responsabile a livello nazionale, sia per il trattamento dei dati c.d. *amministrativi*, sia per quello dei *dati giudiziari*.

Dunque, i titolari del trattamento sono stati individuati sulla base della *summa divisio* tra *dati relativi all'attività amministrativa* (anche definiti, nel testo della riferita circolare, senz'altro *amministrativi*) svolta negli uffici giudiziari e *dati giudiziari*, attribuendone la titolarità, rispettivamente, allo stesso Ministero e agli uffici giudiziari, in forza della previsione dell'art. 4 Reg. 679 ("[…] *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*") e della circostanza che "*al Ministero della Giustizia compete l'organizzazione e il funzionamento dei servizi relativi alla giustizia*" (come precisato dalla circolare richiamata).

La individuazione di tali due distinte categorie di dati è stata concepita per comprensibili motivi di ordine istituzionale, in quanto funzionale alla individuazione dei due distinti titolari del trattamento sulla base dell'attività, amministrativa o giudiziaria, svolta e al formale riconoscimento dell'autonomia della funzione giudiziaria.

Tuttavia, come si è visto sopra, l'espressione *dati giudiziari*, con l'entrata in vigore del Reg. 679, è stata espunta dall'ordinamento e sostituita da quella di *dati relativi a condanne penali e reati* (individuata dall' art. 2-*octies*, D. Lgs. 101/2018 e dall'art. 10 Reg. 679).

Quest'ultima categoria di dati, ovviamente, non esaurisce il complesso dei dati trattati nei processi penali e nelle attività amministrative dell'ufficio strettamente connesse agli esiti di quei processi. D'altro canto, l'accezione lata, e ormai atecnica e informale, di cui alla riferita circolare (*dati giudiziari*), in quanto utilizzata in contrapposizione con quella di *dati relativi all'attività amministrativa svolta negli uffici giudiziari* (insieme, le due categorie di dati "devono" esaurire l'interezza dei dati trattati dall'ufficio giudiziario nel complesso di tutti i suoi compiti istituzionali) non può che essere ritenuta comprensiva anche di tutti i dati personali trattati nell'attività giurisdizionale civile e penale: si tratta dei dati che, pur sempre, in base alle definizioni dettate

dalle norme, costituiscono dati personali *tout court*, del tutto assimilabili ai dati a loro volta latamente definibili, e dalla riferita circolare definiti, *amministrativi* (categoria o, meglio, definizione utilizzata dalla circolare per circoscrivere, si ribadisce, i dati trattati nell'ambito dell'attività amministrativa – tra i predetti dati, peraltro, possono essere presenti i dati riconducibili alle *categorie particolari di dati personali* di cui al predetto art. 9 Reg. 679).

Inoltre, giova ricordare che, come sopra anticipato, il citato art. 2-*duodecies* del D. Lgs. 196/2003, come modificato dal D. Lgs. 101/2018*,* al comma 4, prevede che *"Ai fini del presente articolo 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, nonchè i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari. Le ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti."*): la *trattazione giudiziaria di affari e di controversie* concerne lo svolgimento dei procedimenti civili e di volontaria giurisdizione e per i relativi dati, non inerendo gli stessi all'attività amministrativa dell'ufficio, il titolare del trattamento è l'ufficio giudiziario (non anche per i dati trattati in occasione delle attività amministrative indicate dall'art. 2-*duodecies* predetto).

In conclusione, appare opportuno ricondurre la titolarità del trattamento al singolo ufficio giudiziario in riferimento a tutti i dati personali trattati nei procedimenti civili - contenziosi e volontari - e penali, nell'ambito dei quali si evidenziano, per la loro autonoma categorizzazione e la loro correlata accentuata delicatezza, i dati afferenti a condanne penali e reati e le categorie particolari di cui all'art. 4 Reg. 679.

L'*ufficio giudiziario*, per i c.d. *dati giudiziari* come intesi dalla circolare ministeriale riferita - è opportuno precisare - è individuato quale titolare in linea con il dettato normativo europeo, per quanto, se è pur vero che la responsabilità del corretto trattamento è in capo al singolo magistrato o impiegato amministrativo che lo pone in essere, il soggetto nel quale si concentra il potere decisionale nell'ufficio con riguardo alle misure adottande non può essere che il capo dello stesso, come ebbe a ritenere senz'altro il Ministero della Giustizia, vigente il codice *privacy* 196/2003 nella sua originaria formulazione.

4 - Responsabile della Protezione dei dati (R.P.D.)

La predetta circolare ministeriale del 27.6.2018 delinea chiaramente la esaustività della soluzione consistente nella nomina di un unico R.P.D. per tutti gli uffici del territorio nazionale, in relazione ad ogni tipo di trattamento e ad ogni tipo di dato.

La unicità del R.P.D., in particolare, è chiaramente fatta discendere dalle "*difficoltà che potrebbero insorgere nella qualificazione della natura del dato, sia per la difficoltà pratica degli uffici di reperire l'idonea professionalità interna o le risorse necessarie per la nomina di RPD esterno*".

Per quanto concerne l'ambito delle competenze del R.P.D., va detto che la composita normativa vigente registra una contraddizione tra l'art. 37 Reg. 679/2018, in base al quale "*Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta* […] *eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali*;", e l'art. 2-*sexiesdecies* del riformato codice della *privacy*, a norma del quale, "*Il responsabile della protezione dati è designato, a norma delle disposizioni di cui alla sezione 4 del capo IV del Regolamento, anche in relazione ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni*.".

Al contrasto tra le due citate norme, tra le quali la prevalenza andrebbe riconosciuta alla norma nazionale in ragione del carattere ulteriormente protettivo rispetto a quella del regolamento europeo, si aggiunge la difformità tra il testo della circolare citata, che estende tale competenza sia al trattamento dei dati c.d. *amministrativi*, sia a quello dei c.d. *dati giudiziari* trattati dagli uffici giudiziari, e il testo del D.M. 7.8.2018 citato, che, tra le norme indicate a fondamento della parte dispositiva, non richiama il par. 3 dell'art. 37 Reg. 679 ("*Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione*."), citato, invece, dalla circolare a fondamento dell'analisi svolta e delle relative conclusioni; sottolinea la obbligatorietà della nomina ai sensi del par. 1, lett. a) stesso articolo (che, come sopra evidenziato, sancisce la non obbligatorietà per i trattamenti effettuati dalle "*autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali*"), e, nella parte dispositiva, riferisce la nomina alla "*protezione dei dati per il Ministero della Giustizia*" e i compiti "*all'insieme del trattamento dei dati effettuati dal Ministero della Giustizia*", mostrando di escludere senz'altro i dati trattati nell'attività

giurisdizionale e di potersi riferire, tutt'al più, ai dati personali trattati dagli uffici giudiziari nella loro attività amministrativa[7].

Ad ogni modo, non può non prendersi atto che, allo stato - per via del contenuto della circolare richiamata, della quale vanno di necessità valorizzati i contenuti e gli effetti *organizzatori* pur in una condizione di recessività, quanto a valenza *normativa*, della circolare stessa rispetto al decreto - gli uffici giudiziari, in ordine alle funzioni della figura del R.P.D., non possono che fare riferimento al R.P.D. che il Ministro della Giustizia ha designato con il suo D.M. 7.8.2018, restando altrimenti privi di tale figura normativamente necessaria.

5 - Registri dei trattamenti.

L'art. 30, par. 1 lett. a) reg. 679 e l'art. 20 del D. Lgs. 51/2018[8], sostanzialmente identici, prevedono, a cura del titolare del trattamento, la tenuta di *Registri delle attività di trattamento*; come sopra si è visto, il Ministero della Giustizia ha individuato, con D.M. 7.8.2018, un R.P.D. al quale ha affidato anche la *"tenuta del registro delle attività di trattamento*; con lo stesso D.M., il Ministro ha precisato che "*i compiti del RPD attengono all'insieme del trattamento dei dati effettuati dal ministero della Giustizia"*.

Le incertezze in ordine alla portata delle competenze del R.P.D., cui si è fatto cenno sopra, si ripercuotono sulla individuazione dei registri dei trattamenti da tenere presso gli uffici giudiziari.

La circostanza che titolare del trattamento dei dati relativi all'attività amministrativa degli uffici giudiziari è il Ministero della Giustizia indurrebbe a ritenere che il singolo ufficio giudiziario non

[7] Nella informativa resa ai sensi degli artt. 13 e 14 Reg. 679 sul sito del Ministero ("*La presente sezione contiene le informazioni sul trattamento dei dati personali degli utenti che consultano il sito* web *del Ministero della Giustizia o che, interagendo con il sito forniscono i propri dati personali. La presente informativa è resa, comunque, in generale per il trattamento dei dati personali da parte del titolare. Le informazioni rese non riguardano altri siti, pagine o servizi* online *raggiungibili tramite link ipertestuali eventual*mente *pubblicati nel sito, ma riferiti a risorse esterne al dominio del Ministero della giustizia*."), il R.P.D. rappresenta che "*I dati personali sono trattati dal Ministero della giustizia nell'esecuzione dei propri compiti pubblici o comunque connessi all'esercizio dei propri pubblici poteri e per le finalità connesse a questi compiti*.").

[8] L'art. 30 ("*Registri delle attività di trattamento*"), par. 1 lett. a) reg. 679, dispone che "*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità*.". L'art. 20 ("*Registri delle attività di trattamento*") del D. Lgs. 51/2018 dispone che "*I titolari del trattamento tengono un registro di tutte le categorie di attività di trattamento sotto la propria responsabilità.*".

debba tenere un registro per il trattamento di tali dati, atteso che la normativa prevede che sia il titolare del trattamento a dover tenere il registro (o il R.P.D., su incarico del titolare).

Tuttavia, evidenti ragioni di opportunità inducono a ritenere che presso ciascun ufficio debba essere tenuto un registro dei trattamenti che includa sia i dati trattati in occasione dell'attività amministrativa, sia quelli trattati nel corso dei procedimenti civili e penali.

Quanto alla disciplina, occorre tener conto di quanto previso dal Reg. 679 (art. 30), salvo che per i dati personali afferenti ai procedimenti penali, per i quali vigono le regole, simili ma non identiche, dettate dall'art. 20 D. Lgs. 51/2018.

Il registro delle attività di trattamento dei dati personali afferenti all'attività giudiziaria e a quella amministrativa dell'ufficio è tenuto, opportunamente, con apposito foglio *excel* e contiene le indicazioni di cui ai riferiti artt. 30 Reg. 679/2018, per l'attività giudiziaria civile e per l'attività amministrativa, e 20 D. Lgs. 51/2018, per l'attività giudiziaria penale.

In particolare, è opportuno che tale registro indichi: informazioni di carattere preliminare, (dati di contatto del titolare, del DPO - per dati di contatto si intendono indirizzo, e-mail, PEC, numero di telefono); tipologie di trattamento (in relazione a ciascuna finalità, occorre indicare se siano effettuati e quali le seguenti operazioni di trattamento: raccolta, registrazione, organizzazione, conservazione, modifica, estrazione, consultazione, uso, comunicazione, archiviazione); finalità (ad es.: gestione degli ordini) e base giuridica; categorie di interessati (anche solo identificabili); categorie di dati trattati (occorre indicare, in questo campo, se vengono trattati, ad esempio, dati anagrafici, ovvero dati relativi allo stato di salute - importante è riferire i trattamenti ex artt. 9 e 10 Reg. 679); categorie di destinatari dei dati (non sono considerati destinatari le autorità pubbliche che possono ricevere comunicazioni di dati personali in ambiti di indagine); misure di sicurezza (l'art. 30, par. 1, lett. g) Reg. 679 prevede, al riguardo, "*ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'art. 32, par. 1*.")[9].

[9] Si è tenuto particolarmente presente, nella indicazione dei contenuti del registro, di quanto pubblicato da Luca Morini sul sito www.cybersecurity360.it. Se ne trascrivono, qui di seguito, le "*considerazioni finali*": "*Il trattamento di dati è fisiologicamente collegato a violazioni ed altri incidenti di percorso. Il GDPR non richiede che non si verifichino problemi relativi ai trattamenti, non lo richiede neppure la nostra Autorità Garante, forse per prima consapevole dei pericoli cui ogni trattamento è naturalmente esposto. Quello che è realmente imposto, è che il titolare istituisca un ambiente lavorativo che offra idonee garanzie, che tenga conto del contesto, dei continui pericoli collegati ai trattamenti (non si pensi solamente al classico attacco informatico: è una violazione anche la perdita di un supporto USB) e predisponga una serie di misure collegate sia alla minimizzazione (ad esempio, raccolta dei soli dati realmente necessari, cosiddetto need-to-*

6 - La figura del responsabile del trattamento e quella degli incaricati.

In ordine alla figura del *responsabile del trattamento* – di cui si è molto discusso se possa ritenersi conservata, nel diritto nazionale italiano, anche quella del responsabile *interno*, o se debba ritenersi sussistente soltanto quella del responsabile *esterno* – va detto che, sulla base di quanto previsto dagli artt. 4, n. 8 (*definizione*), 28 (*responsabile del trattamento*) e 30, par. 2 (*registro di tutte le categorie di attività*) Reg. 679 e di quanto indicato dal Considerato 81 del Reg. 679, e tenuto conto della avvenuta abrogazione, ad opera del d.Lgs. 101/2018, dell'art. 29 del codice *privacy* come precedentemente disciplinato, il ruolo del responsabile delineato dalla normativa europea appare essere quello tipico di un soggetto *esterno* alla struttura.

Il citato Considerando 81 prevede che "*Per garantire che siano rispettate le prescrizioni del presente regolamento […] quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento.[…] Dopo il completamento del trattamento per conto del titolare del trattamento, il responsabile del trattamento dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione dei dati personali*.": è evidente, "*per definizione, che non può sussistere alcun flusso di dati personali dal titolare verso i propri dipendenti (che compongono quell'assetto organizzativo deputato al trattamento dei dati nell'ambito dello svolgimento delle funzioni*

---

know only) dei rischi (anche tramite puntuale definizione di compiti e ruoli interni, come quello del soggetto designato di cui all'art 2-quaterdecies del D.lgs. 101/18, ed esterni tra responsabili che prestino idonee garanzie di conformità), che alla reale garanzia dei diritti esercitabili dagli interessati. Diritti che occorre preservare e garantire tramite procedure idonee, anche in assenza di loro esercizio.".

dell'ente pubblico), che agiscono sotto l'autorità del titolare, flusso che - al contrario - caratterizza il rapporto di quest'ultimo con il Responsabile"[10].

Discorso diverso va fatto per gli incaricati del trattamento, figure contemplate, o quanto meno non escluse, sia dall'art. 4, n. 10 Reg. 679, sia dall'art. 2-*quaterdecies* codice *privacy* attualmente vigente, in forza dei quali è ben possibile designare, per il trattamento dei dati personali sotto l'autorità diretta del titolare, nell'ambito del proprio assetto organizzativo – e, quindi, tenendo conto del grado di responsabilità loro ascritto dall'ordinamento generale o interno – determinate persone fisiche, per l'attribuzione di specifici compiti e funzioni, correlati alla loro posizione nella struttura.

7 - La valutazione d'impatto sulla protezione dei dati (DPIA).

Tale procedimento, previsto dagli artt. 35 Reg. 679 e 23 d. lgs. 51/2018, è finalizzato alla gestione dei rischi che un determinato trattamento può comportare per i diritti e le libertà degli interessati. Il contenuto del documento in cui deve sostanziarsi la valutazione in discorso, sostanzialmente identico per il settore civile (Reg. 679) e quello penale (D. Lgs. 51), consiste in una descrizione sistematica dei trattamenti previsti e delle relative finalità, nella valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità, nella valutazione dei rischi per i diritti e le libertà degli interessati, nella indicazione delle relative misure previste per affrontare tali rischi.

Rilevante, nel quadro normativo vigente, è anche l'art. 22, c. 3 del D. Lgs. 101/2018, in virtù del quale "*Sino all'adozione dei corrispondenti provvedimenti generali di cui all'articolo 2-quinquiesdecies del codice […] i trattamenti di cui al medesimo articolo, gia' in corso alla data di entrata in vigore del presente decreto, possono proseguire qualora avvengano in base a espresse disposizioni di legge o di regolamento* […]".

Giova ricordare che il Considerando 89 del reg. 679 prevede quanto segue: "*La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati*

[10] Gilberto Ottaviani, "GDPR nella P.A., responsabile interno od esterno?", www.altalex.com. Che così prosegue: "*non potendosi assumere in capo ai dipendenti dell'ente stesso, pur con responsabilità dirigenziali, quei profili di conoscenza specialistica, affidabilità e disponibilità di risorse per mettere in atto adeguate misure tecniche ed organizzative, ed in definitiva di autonomia gestionale caratterizzanti la figura del Responsabile del trattamento, il quale - giova ricordarlo - assume responsabilità proprie nei confronti degli interessati, e ne risponde all'autorità di controllo ed alla magistratura.*".

personali. […] *tale obbligo non ha sempre contribuito a migliorare la protezione dei dati personali. È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale*.": l'obbligo di notificazione al Garante viene dunque sostituito, in base al Reg.679, dal procedimento di valutazione in discorso (tale obbligo, già previsto dall'art. 47 del d. Lgs. 196/2003 - vecchio codice della *privacy* - era, in verità, escluso per gli uffici giudiziari).

L'obbligo della valutazione di impatto è collegato ad una ipotesi generale (l'uso di nuove tecnologie) e ad alcune ipotesi speciali, come il trattamento su larga scala di particolari categorie di dati personali o di dati relativi a condanne penali e a reati o la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (quest'ultima ipotesi interessa gli uffici giudiziari requirenti, competenti in materia di sicurezza antiintrusione).

Tenuto conto della raccomandazione del *Gruppo di Lavoro Articolo 29*[11], per la quale è pur sempre consigliabile – in via di principio - l'adozione di un documento di valutazione di impatto, e del fatto che, sino a pochi anni fa, gli uffici giudiziari hanno normalmente adottato un documento, denominato "*Piano della Sicurezza dei Sistemi informatici*" - già obbligatorio a norma dell'art. 34 del D. Lgs. 196/2003, sino alla abrogazione di detto articolo ad opera dell'art. 45 del d.l. n. 5/2012, convertito in l. 4.4.2012, n. 35 - recante la individuazione dei rischi e le misure ritenute adeguate per scongiurare eventi sfavorevoli in campo informatico, appare ragionevole – necessario e sufficiente - procedere ad una rielaborazione di tale documento, onde aggiornarlo e adattarlo alle disposizioni sopra richiamate.

[11] Il gruppo di cui all'articolo 29 è composto da rappresentanti dei garanti della protezione dei dati degli Stati membri. Il gruppo ha carattere consultivo e indipendente che, tra l'altro, ha il compito di esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della direttiva relativa alla tutela dei dati per contribuire alla loro applicazione omogenea.

Tale atto è necessario che contenga, in linea con le previsioni del D.M. Giustizia 27.4.2009, indicazioni precise in ordine ai rischi e alla adeguatezza delle misure atte a scongiurare i rischi stessi, con particolare riferimento all'inventario delle risorse, alla protezione fisica delle aree e dei locali, al controllo degli accessi informatici, al monitoraggio del sistema, alla integralità e disponibilità dei dati, alla continuità degli applicativi, alla copia storica dei dati e all'archiviazione ottica degli stessi, alla sicurezza delle reti e alle norme di comportamento degli utenti.

Non necessari appaiono i contenuti, di cui al Reg. 679 e al d. Lgs. 51/2018, consistenti nella "*descrizione sistematica dei trattamenti previsti e delle finalità del trattamento*" e nella "*valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità*" (art. 35, par. 7 Reg. 679), atteso che i trattamenti, le finalità e la proporzionalità predetti, per gli uffici giudiziari, sono previsti normativamente, attengono pertanto ai compiti istituzionali degli uffici stessi, e sono, sul piano operativo, vincolati alla configurazione e strutturazione dei *software* con i quali sono gestiti i registri istituzionalmente previsti.

8 - Il trattamento dei dati nell'ambito dei rapporti di lavoro – il Reg. 679 (art. 88) si limita a stabilire che "*Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro* […]".

Il codice della *privacy*, così come modificato dal D. Lgs. 101/2018, prevede: "*Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato*." (art. 111).

Queste essendo le norme più importanti che vengono in rilievo, è evidente che, allo stato attuale, resta confermato il quadro normativo già esistente. E, in tale quadro, particolare attenzione va dedicata all'evoluzione tecnologica, per i maggiori rischi che possono derivarne in riferimento, ad esempio, ai controlli tramite videosorveglianza e al controllo remoto delle comunicazioni elettroniche o dei programmi utilizzati[12] (a tal proposito, si dirà in seguito del già citato

[12] Cfr. "*Manuale per il trattamento dei dati personali*", a cura di G. Comandè e G. Malgieri, *Gruppo 24 ore*, pag. 120.

provvedimento del Garante per la protezione dei dati personali in data 1° marzo 2007 (del. n. 13), in materia *di utilizzo della posta elettronica e della rete Internet*.).

Giova anche considerare le ulteriori regole della nuova normativa che vanno ad incidere anche sulla gestione dei dati personali dei lavoratori e, quindi, "*i principi di minimizzazione (a norma dell'art. 5, par. 1, lett. c): i dati personali sono* […] *limitati a quanto necessario rispetto alle finalità per le quali sono trattati*".*), di data protection by design* [si tratta dell'obbligo di protezione dei dati sin dalla progettazione del loro processo di gestione] *e di privacy by defoult* [*si tratta del*'obbligo di tutelare la privacy dei cittadini di default, cioè come impostazione predefinita]*, che consentono di gestire già a livello tecnologico ed organizzativo molti degli strumenti di intrusione nelle attività dei lavoratori sui luoghi di lavoro*."[13].

Degne di essere evidenziate sono, poi, le indicazioni del *Gruppo* Articolo 29, che, in particolare, ha raccomandato che i datori di lavoro dovrebbero sempre tenere presenti i seguenti principi generali: finalità, trasparenza, legittimità, proporzionalità (*i dati personali devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o successivamente trattati.*), esattezza e conservazione dei dati, sicurezza (*sul luogo di lavoro il datore di lavoro deve adottare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dei propri lavoratori. Una particolare protezione deve essere accordata rispetto alla diffusione o all'accesso non autorizza*), consapevolezza del personale.

Riguardo al consenso, il "*Il gruppo di lavoro "articolo 29" ritiene che, se un datore di lavoro deve trattare dati personali come conseguenza necessaria e inevitabile del rapporto di lavoro, sbaglia se cerca di legittimare il trattamento mediante il consenso. Il ricorso al consenso va limitato ai casi in cui il lavoratore è effettivamente libero di scegliere e può successivamente ritirare il proprio consenso senza pregiudizio*. […] *Il gruppo di lavoro ritiene preferibile contare su un'adeguata protezione del paese destinatario piuttosto che sulle deroghe di cui all'articolo 26, come ad esempio il consenso dei lavoratori. Quando ci si affida al consenso, questo deve essere inequivocabile e dato liberamente. Sbagliano i datori di lavoro che si affidano esclusivamente al consenso, eccettuato il caso in cui un suo eventuale ritiro successivo non causi problemi*.". Quanto alla sorveglianza e al controllo, "*Il controllo e la sorveglianza dei lavoratori rispetto all'uso della posta elettronica, all'accesso a Internet, alle riprese televisive o ai dati sulla localizzazione sono*

[13] "*Manuale per il trattamento dei dati personali*", cit., pag. 121.

soggetti alle norme che tutelano i dati. Ogni controllo deve essere una risposta proporzionata del datore di lavoro ai rischi che corre nel tener conto della riservatezza e di altri interessi legittimi dei lavoratori. Tutti i dati personali detenuti o utilizzati durante i controlli devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità che giustificano il controllo. I controlli devono essere eseguiti nel modo meno intrusivo possibile.".

Devono, inoltre, essere ricordate alcune regole dettate dal Garante con l'autorizzazione generale n. 1/2016, in sintonia con il documento elaborato dal *Gruppo Articolo 29*, con riguardo anche all'utilizzo di mezzi cartacei e alla materia delle assenze del personale e dei relativi titoli, regole ispirate soprattutto al principio di necessità ed essenzialità:

- *in tutte le comunicazioni all'interessato che contengono categorie particolari di dati devono essere utilizzate forme di comunicazione anche elettroniche individualizzate nei confronti di quest'ultimo o di un suo delegato, anche per il tramite di personale autorizzato. Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo dovrà essere trasmesso, di regola, in plico chiuso, salva la necessità di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto;*
- *i documenti che contengono dati categorie particolari di dati, ove debbano essere trasmesse ad altri uffici o funzioni in ragione delle rispettive competenze, devono contenere esclusivamente le informazioni necessarie allo svolgimento della funzione senza allegare, ove non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo;*
- *quando per ragioni di organizzazione del lavoro, e nell'ambito della predisposizione di turni di servizio, si proceda a mettere a disposizione a soggetti diversi dall'interessato (altri colleghi) dati relativi a presenze ed assenze dal servizio, il datore di lavoro non deve esplicitare, nemmeno attraverso acronimi o sigle, le causali dell'assenza dalle quali sia possibile evincere la conoscibilità di particolari categorie di dati personali (es. permessi sindacali o dati sanitari).*

Con il richiamato provvedimento in data 1° marzo 2007 (del. n. 13), il Garante per la protezione dei dati personali ha prescritto ai datori di lavoro privati e pubblici precise regole concernenti l'utilizzo di *internet* e della posta elettronica, prevedendo l'adozione di un disciplinare interno alla struttura. Al riguardo, giova evidenziare che la posta elettronica 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 "*corrispondenz*a", 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.

Il disciplinare in argomento, in ultima analisi, potrebbe avere il seguente contenuto normativo-dichiarativo:

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 umana 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.

9 – L' informativa ex artt. 13 e 14 Reg. 679/2018.

L'informativa è una comunicazione con la quale sono portate a conoscenza del cittadino, anche prima che diventi interessato, le finalità e le modalità dei trattamenti operati dal titolare del trattamento.

Essa costituisce un obbligo dei titolari del trattamento "*propedeutico alla legittimità del trattamento stesso*"[14].

Il diritto di ricevere informazioni durante il trattamento è disciplinato dall'art. 15 Reg. 679/2018.[15]

I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13, par. 1, e 14, paragrafo 1, Reg. 679.

Tenuto conto anche della normativa vigente, di quanto indicato dal Garante e di quanto pubblicato dal sito del Ministero della Giustizia, l'informativa da rendere a cura degli uffici giudiziari è necessario che contenga:

- le fonti normative in materia di privacy,
- l'identità e i dati di contatto del titolare del trattamento del responsabile della protezione dei dati (RPD),
- la base giuridica e le finalità del trattamento (individuate già a livello normativo, in riferimento ai compiti istituzionali),

---

[14] "*Manuale per il trattamento dei dati personali*", a cura di G. Comandè e G. Malgieri, *Gruppo 24 ore*, pag. 45.

[15] "*Per quanto la tipologia e l'elenco di informazioni che il soggetto interessato può ricevere siano pressocché gli stessi per gli articoli 13, 14 e 15, ciò che cambia è il momento dell'esercizio del diritto, ma soprattutto l'attività del soggetto interessato: per il solo diritto d'accesso è richiesta un'attività del soggetto, che dovrà dunque esplicitamente richiedere informazioni sul proprio trattamento. Al contrario, per i diritti di informativa (artt. 13 e 14), è il titolare che spontaneamente deve fornire tutte le informazioni rilevanti*.", "*Manuale per il trattamento dei dati personali*", a cura di G. Comandè e G. Malgieri, *Gruppo 24 ore*, pag. 46.

- le modalità di trattamento (con indicazioni particolari riguardanti le procedure selettive – tirocinanti, partecipanti a gare indette per la fornitura di beni e servizi);
- i diritti degli interessati in relazione all'accesso ai propri dati, alla cancellazione, alla limitazione del trattamento, alla opposizione al trattamento, al diritto di reclamo;
- informazioni in ordine ai *cookies* e ai dati di navigazione (i *cookies* sono piccoli *file* di testo che alcuni siti, durante la navigazione, invia al terminale dell'utente, dove vengono memorizzati, per poi essere ritrasmessi allo stesso sito alla visita successiva.);
- la data di aggiornamento dell'informativa.

E' opportuno riportare il testo del Considerando 58 del Reg. 679/2018: "*Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.*".

Da tener presente, infine, che l'attività di informazione va resa gratuitamente[16].

10 - La figura dell'amministratore dei sistemi informatici.

La disciplina di protezione dei dati previgente al Codice del 2003 definiva l´amministratore di sistema, individuandolo quale "*soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l´utilizzazione*" (art. 1, comma 1, lett. c) d.P.R. 318/1999).

Il Codice della privacy del 2003 non includeva questa figura tra le proprie definizioni normative.

[16] "*salvo che le richieste dell'interessato siano considerate infondate o eccessive: in tal caso l'interessato è obbligato a contribuire e il titolare può rifiutarsi di evadere la richiesta qualora le informazioni richieste siano già state fornite. L'onere della prova grava in ogni caso sul titolare*"., "*Manuale per il trattamento dei dati personali*", cit., pag. 46.

Il Garante per la protezione dei dati personali, nel provvedimento del 27.11.2008, osservava che "*con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.* […] *Il codice non ha … incluso questa figura tra le proprie definizioni normative. Tuttavia le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema …* ".

Abrogato l'allegato B di cui sopra, pur nel mutato quadro normativo dominato dai principi di *accountability*[17], *privacy by design* e *privacy by defoult*, il provvedimento del Garante del 2008 conserva la propria efficacia e continua a trovare esplicazione, con riguardo agli uffici giudiziari, nelle disposizioni di cui al D.M. 27.4.2009[18], che, all'art. 4, prevede e disciplina la figura dell'*amministratore di sistema*, divenuta nel frattempo *amministratore dei sistemi informatici* (ADSI).

Giulio BRUNO

---

[17] Stefano Aterno, in www.agendadigitale.eu: "*In italiano è stato tradotto con il termine "responsabilizzazione" ma il concetto non è chiaramente interpretabile solo come "responsabilità*". […] *Il concetto di "accountability" è legato al rendere conto dell'azione fatta o fatta fare, al rispondere e al rendere conto dei risultati ottenuti, delle cose fatte (fatte bene e fatte male).* […] *Il punto fondamentale del concetto di accountability è in realtà posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità*. […] *Saper anticipare il verificarsi di situazioni critiche, l'accadimento di eventi rischiosi possibili o molto probabili e trovare soluzioni che, ex ante in concreto, forniscano un certo margine di sicurezza, significa forse essere accountable*."

[18] L'art. 4 citato prevede, in particolare, che "*L'amministratore dei servizi informatici (ADSI) assicura la conduzione operativa di specifiche componenti del sistema informatico, effettuando, anche mediante accesso remoto, tutte le operazioni necessarie a garantire i requisiti di cui all'art. 2*." (comma 1) e che "*Il Responsabile S.I.A., su proposta del dirigente informatico competente per territorio o per settore, designa i soggetti di cui ai commi 1, 2 e 3 individuandoli fra gli esperti informatici dell'Amministrazione ovvero, se non sono disponibili tali risorse, ricorrendo a personale esterno qualificato.*" (comma 4).