Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro - 13 luglio 2016

Registro dei provvedimenti
n. 303 del 13 luglio 2016

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

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

VISTE le segnalazioni e i reclami con le quali è stata lamentata la illiceità di trattamenti effettuati dall'Università degli studi "G. D'Annunzio" di Chieti e Pescara mediante strumenti elettronici;

VISTE le Linee guida per posta elettronica e internet, adottate dal Garante con provvedimento n. 13 del 1° marzo 2007 (G.U. n. 58 del 10 marzo 2007 e www.garanteprivacy.it, doc. web n. 1387522);

ESAMINATE le risultanze istruttorie e la documentazione in atti;

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

RELATORE la dott.ssa Augusta Iannini;

PREMESSO

1. E' stata lamentata da parte del personale dell'Università degli studi "G. D'Annunzio" di Chieti e Pescara la violazione della disciplina in materia di protezione dei dati personali con riguardo, tra l'altro, all'asserito controllo posto in essere dal datore di lavoro in ordine all'utilizzo di sistemi di comunicazione elettronica e di videosorveglianza.

2.1. Nel dare riscontro alle richieste di informazioni formulate dall'Ufficio al fine di verificare la fondatezza delle doglianze e l'osservanza dei principi e delle disposizioni in materia di protezione dei dati personali l'Ateneo, in qualità di titolare del trattamento, ha dichiarato ai sensi dell'articolo 168 del Codice che, con riguardo al trattamento posto in essere mediante il sistema di videosorveglianza il trattamento è effettuato nel rispetto delle indicazioni fornite dalla "Direzione territoriale del lavoro di Chieti-Pescara, con nota prot. n. 12078 del 2/4/2015, acquisita al protocollo di Ateneo al n. 16330 del 7/4/2015" (cfr. nota 22 maggio 2015, in atti).

2.2. Con specifico riguardo all'utilizzo dei sistemi di comunicazione elettronica l'Ateneo ha dichiarato che:

1. "i log delle attività di rete sono anonimi: vengono raccolti e conservati i dati relativi ai Mac Address ed agli indirizzi IP dei personal computer […]" e "non vengono raccolti dati personali contenuti nella comunicazione di rete, eccezion fatta per il Mac Address (legato alla postazione utilizzata per l'attività lavorativa) e l'indirizzo IP dinamico ottenuto nella sessione di lavoro" (cfr. nota 22 maggio 2015, in atti);

2. "non è stata fornita nessuna informativa ai sensi dell'articolo 13 del Codice […] in quanto non è possibile[trattare] dati personali […] per cui l'informativa è superflua";

3. "i dati riferibili ai log delle attività di rete in senso lato vengono conservati per 5 anni: su apposito server per arco temporale di 3 anni on line e cancellati automaticamente dopo tale arco temporale; i restanti 2 anni su nastro di backup in modalità off line. La motivazione è quella di fornire alle forze dell'ordine che su mandato della magistratura debbano compiere indagini su attività illecite che hanno avuto come sorgente o come destinatario i sistemi informatici dell'Ateneo" (l'art. 14 del citato regolamento indica invece la conservazione per 36 mesi);

4. "i dati sono acquisiti in maniera automatica dalla rete […] i dati oggetto di backup [sono conservati in un locale protetto e ad accesso riservato]. L'accesso logico è impedito a tutti, eccezion fatta per il responsabile e gli incaricati [...] i quali accedono mediante una VPN" e con proprie credenziali; "ogni accesso viene memorizzato su un log file. L'attività svolta dagli amministratori di sistema viene registrata";

5. "l'associazione tra il mac address della postazione e del dipendente che lo utilizza non viene in alcun modo effettuata" e "il mac address non [è] un dato identificativo tale da rendere necessaria l'informativa"; nella normale attività nessuno è in grado di associare l'utilizzatore con il mac address. Solo l'amministratore di rete […può farlo] previa legittima richiesta" (cfr. nota del 14 ottobre 2015, in atti);

6. il Senato accademico ed il Consiglio di amministrazione dell'Ateneo hanno approvato il "Regolamento di utilizzo della rete internet e della posta elettronica" pubblicato sul sito web di cui è "stata data comunicazione a tutto il personale docente e non docente";

7. l'art. 14 del menzionato regolamento prevede la registrazione delle "attività di accesso ai servizi internet" e "l'utilizzo della posta elettronica" al fine "precipuo di garantire la integrità e disponibilità dei dati" e per "l'ulteriore fine statistico necessario a conoscere la tipologia del traffico […] indesiderato" o "illegale" nonché "in caso di richieste investigative dell'Autorità giudiziaria";

8. le operazioni di "controllo, filtraggio, monitoraggio e tracciatura delle connessioni e dei collegamenti ai siti internet esterni" (art. 15, comma 2, Regolamento cit.) vengono svolte "su segnalazione del Network Operating Center (NOC) del Gruppo Armonizzazione Reti della Ricerca (GARR) in caso di violazione del diritto d'autore […] di diffusione di malware ed in generale di software maligno che possa avere ripercussioni sulla rete";

9. in tali casi si procede al "monitoraggio dei dati scambiati […] successivamente si attua un filtraggio dei dati o un loro blocco e, quindi, si procede all'individuazione fisica della postazione sulla rete e alla sua bonifica".

2.3. Alla luce della documentazione in atti e delle dichiarazioni, talora contraddittorie, rese dal titolare del trattamento nel corso dell'istruttoria, emerge che l'Ateneo effettua operazioni che consistono nella raccolta e conservazione, per un periodo di 5 anni (successivamente ha dichiarato di voler ridurre tale tempo di conservazione a 12 mesi), dei file di log relativi al traffico internet contenenti, tra gli altri, il MAC Address (Media Access Control Address), l'indirizzo IP nonché informazioni relative all'accesso ai servizi internet, all'utilizzo della posta elettronica e alle connessioni di rete (cfr. nota 22 maggio 2015, in atti e art. 14, comma 1, Reg., cit.). Tale raccolta e conservazione prolungata di informazioni sarebbe effettuata, asseritamente in forma anonima, per esclusive finalità "di monitoraggio del servizio nonché di sicurezza e […] integrità dei sistemi" (art. 14, comma 3, Reg., cit.) nonché in caso di richieste investigative dell'Autorità giudiziaria (cfr. nota 22 maggio 2015, cit.: "[…] fornire alle forze dell'ordine che su mandato della magistratura debbano compiere indagini su attività illecite che hanno avuto come sorgente o come destinatario i sistemi informatici dell'Ateneo").

Stando a quanto dichiarato, l'associazione tra il MAC Address della postazione e il dipendente che lo utilizza non sarebbe effettuata (in fase di raccolta e nelle successive elaborazioni) se non in relazione alle richieste dell'Autorità giudiziaria (cfr. nota 14 ottobre 2015, cit., art. 14, comma 2, Reg., cit.).

Tramite il personale tecnico del "Settore competente" sarebbe effettuata attività di "controllo, filtraggio, monitoraggio e tracciatura delle connessioni e dei collegamenti ai siti internet esterni" (artt. 2 e 15, comma 2, Reg. cit.).

Sebbene sia stato dichiarato nella nota dell'ottobre 2015 che le predette operazioni vengono svolte solo "su segnalazione del Network Operating Center (NOC) del Gruppo Armonizzazione Reti della Ricerca (GARR) in caso di violazione del diritto d'autore […] di diffusione di malware ed in generale di software maligno che possa avere ripercussioni sulla rete" (cfr. nota 14 ottobre 2015, cit.), il regolamento evidenzia invece che le stesse vengono effettuate in modo costante e che, in presenza di "violazione delle regole" vengono informate le Autorità competenti e successivamente consentite le operazioni di identificazione dell' "utente utilizzatore" (arg. art. 15, commi 2 e 5, Reg., cit.).

L'associazione tra il MAC Address della postazione (comunque raccolto e conservato, unitamente agli altri dati relativi all'utilizzo dei servizi di rete) e la persona utilizzatrice verrebbe effettuata "esclusivamente su precisa richiesta delle Autorità competenti" e "la consultazione dei suddetti file di tracciatura in maniera non aggregata [sarebbe] diritto esclusivo dell'Autorità giudiziaria" (art. 15, comma 5, Reg., cit.; nota del 14 ottobre 2015, ove si legge: "nella normale attività nessuno è in grado di associare l'utilizzatore con il mac address. Solo l'amministratore di rete […può farlo] previa legittima richiesta").

RILEVATO

3. In base ad una complessiva valutazione degli elementi sopra richiamati, deve ritenersi che, contrariamente a quanto sostenuto dall'Ateneo, le descritte operazioni di trattamento, effettuate per il tramite del personale incaricato e degli amministratori di sistema, diano luogo ad un trattamento di dati personali, peraltro riferiti ad un novero assai ampio di soggetti definiti "utenti" della rete di Ateneo (in particolare, i docenti, i ricercatori, il personale tecnico amministrativo e bibliotecario, gli studenti, i dottorandi, gli specializzandi e gli assegnisti di ricerca, ma anche professori a contratto e visiting professors; cfr. artt. 2 e 3 Reg., cit.). Ciò in quanto il MAC Address della "interfaccia" di rete di una postazione è da considerarsi "dato personale" ai sensi della disciplina comunitaria e nazionale in materia di protezione dei dati (art. 4, comma 1, lett. b) del Codice). Infatti, il MAC Address è costituito da una sequenza numerica (48 cifre binarie) associata in modo univoco dal produttore a ogni scheda di rete ethernet o wireless prodotta al mondo e rappresenta l'indirizzo fisico identificativo di quel particolare dispositivo di rete da cui è possibile desumere l'identità del produttore, la tipologia di dispositivo e, in taluni casi, anche risalire all'acquirente o utilizzatore dell'apparato: è infatti sostanzialmente immodificabile e, date le caratteristiche (in particolare, la sua univocità su scala globale), consente di risalire, anche indirettamente, alla postazione corrispondente e di conseguenza all'utente che su di essa sta operando. Per tutto ciò il suo trattamento impone il rispetto della normativa sulla protezione dei dati personali (cfr., Gruppo Art. 29, Parere n. 4/2007 - WP 136 sul concetto di dato personale; sul carattere di dato personale del MAC Address stante la relativa univocità, cfr. Gruppo Art. 29, Parere n. 13/2011 - WP 185 sui servizi di geolocalizzazione su dispositivi mobili intelligenti, spec. p. 11; segnalazione del Garante a Governo e Parlamento del 9 luglio 2013 con particolare riferimento all'art. 10, d.l. n. 69 del 21 giugno 2013. c.d. "decreto del fare"; Provv.ti 10 luglio 2014, doc. web n. 3283078, spec. punto 2; 19 marzo 2015, doc. web n. 3881513, punto 3; 12.03.2015, doc. web n. 3881392; 23.04.2015, doc web n. 4015426).

CONSIDERATO

4.1.Tanto premesso, l'assoggettabilità del trattamento dell'Ateneo alla disciplina di protezione dei dati personali consente di rilevare alcuni profili di violazione della stessa, con particolare riferimento al principio di liceità (art. 11, comma 1, lett. a) del Codice).

Ciò assume particolare rilievo con riguardo alla possibilità di risalire all'identità dell'utilizzatore della postazione, ancorché tramite l'intervento dell'amministratore di sistema, circostanza che è ancor più evidente con specifico riferimento ai dipendenti dell'Ateneo: tra gli "utenti" della rete figura infatti il

personale tecnico-amministrativo e docente cui è abitualmente assegnata una specifica postazione (atteso che, contrariamente a quanto sostenuto dal titolare del trattamento, la presenza di eventuali postazioni condivise fra più persone è da considerarsi circostanza residuale).

4.2. In primo luogo, l'Ateneo (sulla scorta dell'erroneo presupposto che il MAC Address non costituisca "dato personale") non ha reso la dovuta informativa in favore degli utilizzatori della rete, anche con riguardo alle effettive caratteristiche delle operazioni di trattamento effettuate (artt. 11, comma 1, lett. a) e 13 del Codice; Linee guida, cit., punto 3).

Il menzionato Regolamento di Ateneo che pur detta regole in merito al corretto utilizzo degli strumenti elettronici in dotazione agli utenti, non è comunque idoneo a sostituire l'adempimento all'art. 13 del Codice in quanto non reca gli elementi essenziali richiesti dalla legge per l'informativa da rendere agli interessati, né è idoneo a renderli edotti in modo esaustivo in merito alle operazioni di trattamento effettuate, con particolare riferimento alla raccolta, alla conservazione e alle altre operazioni di trattamento dei dati relativi ai MAC Address e agli indirizzi IP dei personal computer a loro messi a disposizione o assegnati in uso.

Sotto quest'ultimo profilo, peraltro, sebbene l'art. 14 del Regolamento precisi che "le attività di accesso ai servizi internet ed in particolare l'utilizzo della posta elettronica sono registrati in forma elettronica" per il tramite del personale del "settore competente", il riferimento in esso contenuto alla gestione "in maniera anonima" e all'utilizzo di queste informazioni "esclusivamente in relazione alle attività di monitoraggio del servizio, alla sicurezza e all'integrità dei sistemi" (art. 14, comma 3, Reg., cit.) risulta, oltre che non corrispondente a quanto dichiarato nel corso dell'istruttoria dal titolare del trattamento, non idoneo, in applicazione dei principi di liceità e correttezza dei trattamenti (artt. 11, comma 1 lett. a) del Codice), ad informare in modo chiaro e dettagliato circa la raccolta e le caratteristiche dell'effettivo trattamento dei dati personali degli utenti (quale emerge all'esito dell'attività istruttoria condotta, cfr. descrizione al punto 2.3.), nonché in ordine all'eventuale utilizzo degli stessi per controlli anche su base individuale (arg. art. 15, Reg., cit.).

4.3. Quanto alle specifiche caratteristiche del trattamento dei dati derivante dalla configurazione del sistema, si ritiene che questo, articolandosi anche in operazioni di controllo, filtraggio, monitoraggio e tracciatura delle connessioni e dei collegamenti ai siti internet esterni, peraltro registrati in modo sistematico e conservati per un ampio arco temporale, sia idoneo a consentire un controllo dell'attività e dell'utilizzo dei servizi della rete individualmente effettuato da soggetti identificabili.

Ciò, nei casi in cui il trattamento sia posto in essere nei confronti dei dipendenti e in presenza del menzionato collegamento tra i dati relativi alla connessione e la persona utilizzatrice, consente di ricostruirne anche indirettamente l'attività e risulta, anche sotto questo profilo, in contrasto con il principio di liceità nonché con la rilevante disciplina di settore in materia di lavoro (artt. 11, comma 1, lett. a) e 114 del Codice e art. 4, l. 20 maggio 1970, n. 300). Tanto, sia con riguardo alla disciplina in materia di impiego di apparecchiature idonee al controllo a distanza dell'attività dei lavoratori vigente all'epoca in cui il trattamento è stato iniziato (cfr., Linee guida cit. par. 4; nonché, con riguardo a software di controllo della navigazione in internet, Provv.ti 5 febbraio 2015, doc. web n. 3813428; 21 luglio 2011 doc. web n. 1829641, confermato da Trib. Roma, sez. I, 21 marzo 2013 n. 4766, ma già, 2 aprile 2009, doc. web n. 1606053 e 1° aprile 2010 doc. web n. 1717799), sia con riguardo al quadro normativo risultante dalle modifiche intervenute per effetto dell'art. 23 del decreto legislativo 14 settembre 2015, n. 151.

Quanto a quest'ultimo profilo, in particolare, il trattamento è effettuato, attualmente, per il tramite di apparati (differenti dalle ordinarie postazioni di lavoro) e di sistemi software che consentono, con modalità non percepibili dall'utente (c.d. in background) e in modo del tutto indipendente rispetto alla normale attività dell'utilizzatore (cioè senza alcun impatto o interferenza sul lavoro del dipendente), operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" costanti ed indiscriminati degli accessi a internet o al servizio di posta elettronica.

Tali software non possono essere considerati "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (ai sensi e per gli effetti dell'art. 4, comma 2, l. n. 300/1970, come modificato dall'art. 23 del d.lg. n. 151/2015; sul punto, cfr. nota del Ministero del Lavoro e delle Politiche Sociali, del 18 giugno 2015; v. altresì la definizione di "attrezzatura" e "post[azione] di lavoro" di cui all'art. 173 d.lg. n. 81/2008).

In tale nozione, infatti - e con riferimento agli strumenti oggetto del presente provvedimento, vale a dire servizio di posta elettronica e navigazione web - è da ritenere che possano ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza. Da questo punto di vista e a titolo esemplificativo, possono essere considerati "strumenti di lavoro" alla stregua della normativa sopra citata il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un account personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio, per una breve durata non superiore comunque ai sette giorni; sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso).

Altri strumenti pure utili al conseguimento di una elevata sicurezza della rete aziendale, invece, non possono normalmente consentire controlli sull'attività lavorativa, non comportando un trattamento di dati personali dei dipendenti, e di conseguenza non sono assoggettati alla disciplina di cui all'art. 4 Stat. lav. (ad es. sistemi di protezione perimetrale – firewall – in funzione antintrusione e sistemi di prevenzione e rilevamento di intrusioni – IPS/IDS – agenti su base statistica o con il ricorso a sorgenti informative esterne).

Ciò considerato, i sistemi ed applicativi in uso presso l'Università esulano senza dubbio dal perimetro degli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" e comportano, quindi, un trattamento in contrasto con quanto previsto dal predetto art. 4.

5. Il trattamento effettuato si pone altresì in violazione dei principi di necessità, pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. d) del Codice) che non consentono controlli massivi, prolungati, costanti e indiscriminati, quali, come nel caso di specie, la registrazione sistematica dei dati relativi al MAC Address e i dati relativi alla connessione ai servizi di rete (sul punto, Consiglio di Europa, Raccomandazione del 1 aprile 2015, CM/Rec(2015)5, ma già, Linee guida cit., spec. par. 4, 5.2. lett. b) e 6.1; sulla minimizzazione nel trattamento dei dati, Provv. 2 febbraio 2006, doc. web n. 1229854, confermato da Cass., sez. I civ., 1° agosto 2013, n. 18443).

Anche su tale aspetto si è soffermato il Garante nelle menzionate audizioni chiarendo che i principi di necessità e proporzionalità impongono di privilegiare misure preventive ed, in ogni caso, gradualità nell'ampiezza del monitoraggio "che renda assolutamente residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie" quali, ad esempio, la riscontrata presenza di virus e "comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori" (cfr. audizione del Garante, cit., spec. punto 2, lett. e)).

In particolare, la memorizzazione dei dati relativi al MAC Address e i dati relativi alla connessione ai servizi di rete in modo massivo ed anelastico, in presenza della menzionata associabilità in via univoca all'utente, non risulta strettamente necessaria per la generica finalità di protezione e sicurezza informativa ovvero per astratte finalità derivanti da possibili indagini giudiziarie (cfr. art. 14 Reg., cit.; nota 14.10.2015, cit.), dando luogo ad un trattamento di dati eccedente rispetto agli scopi dichiarati (artt. 3 e 11, comma 1, lett. d) del Codice). L'Ateneo non ha infatti addotto la ricorrenza di specifici episodi "anomali" ovvero la presenza di idonei presupposti che possano legittimare sotto il profilo della proporzionalità il trattamento (quali, ad esempio, incidenti di sicurezza occorsi o la presenza di indagini in corso da parte dell'autorità giudiziaria).

RITENUTO

6. Ciò considerato, ritenuto illecito il trattamento effettuato dell'Università degli studi "G. D'Annunzio" di Chieti e Pescara nei termini sopra indicati per violazione degli articoli 3, 11, comma 1, lett. a) e d), 13 e 114 del Codice, il Garante, ai sensi degli articoli 143, comma 1, lett. c), e 154, comma 1, lett. d), del Codice, ritiene di dover vietare con effetto immediato dalla data di ricezione del presente provvedimento, il trattamento descritto in motivazione, con conservazione dei dati finora trattati ai fini di un'eventuale acquisizione degli stessi da parte dell'autorità giudiziaria, nonché per esigenze di tutela dei diritti in sede giudiziaria.

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

L'Autorità si riserva di valutare, con autonomo procedimento, la sussistenza di violazioni amministrative in capo al titolare del trattamento.

TUTTO CIÒ PREMESSO IL GARANTE

nei confronti dell'Università degli studi "G. D'Annunzio" di Chieti e Pescara:

1. dichiara illecito il trattamento descritto in motivazione in violazione degli articoli 3, 11, comma 1, lett. a) e d), 13 e 114 del Codice nonché dell'art. 4, l. n. 300/1970 con la conseguente inutilizzabilità dei dati trattati in violazione di legge, ai sensi dell'art. 11, comma 2 del Codice;

2. ai sensi degli artt. 143, comma 1, lett. c), e 154, comma 1, lett. d), del Codice, dispone, con effetto immediato dalla data di ricezione del presente provvedimento, il divieto dell'ulteriore trattamento dei dati personali sopra indicati con conservazione di quelli finora trattati ai fini di un'eventuale acquisizione degli stessi da parte dell'autorità giudiziaria, nonché per esigenze di tutela dei diritti in sede giudiziaria;

3. dispone che sia data comunicazione al Garante, entro 30 giorni dalla data di comunicazione del presente provvedimento, dell'avvenuta attuazione dello stesso;

4. dispone, ai sensi dell'art. 171 del Codice, la trasmissione degli atti e di copia del presente provvedimento all'autorità giudiziaria per le valutazioni di competenza in ordine agli illeciti penali che riterrà eventualmente configurabili.

Avverso il presente provvedimento, ai sensi dell'art. 152 del Codice e dell'art. 10 del d.lg. n. 150/2011, può essere proposta opposizione davanti al tribunale ordinario del luogo ove ha sede il titolare del trattamento entro il termine di trenta giorni dalla notificazione del provvedimento stesso.

Roma, 13 luglio 2016

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia