VEDI ANCHE Newsletter del 17 febbraio 2017

[doc. web n. 5958296]

Accesso alla posta elettronica dei dipendenti - 22 dicembre 2016

Registro dei provvedimenti
n. 547 del 22 dicembre 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");

VISTO il reclamo presentato da XY concernente il trattamento di dati personali riferiti all'interessato effettuato da AON S.p.A.;

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

VISTE le "Linee guida per posta elettronica e internet", adottate con provvedimento n. 13 del 1° marzo 2007 (pubblicato nella G.U. 10 marzo 2007, n. 58);

ESAMINATA 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 prof.ssa Licia Califano;

PREMESSO

1.1. Il reclamo nei confronti della società.

Con reclamo del 22 giugno 2015 il Sig. XY, lamentando l'illegittimità del trattamento di dati personali effettuato da AON S.p.A. (di seguito: la società) nell'ambito di un rapporto di lavoro allo stato non più in essere, ha chiesto all'Autorità di disporre il blocco nonché il divieto del trattamento effettuato dalla società. Il reclamante ha chiesto altresì di ordinare la cancellazione dei dati trattati in violazione di legge - "previa trasmissione in forma intellegibile […] della corrispondenza personale presente nell'account [di posta elettronica] e dei files personali contenuti nel telefono aziendale" - e la "restituzione di tutto ciò che fosse presente nella stanza" all'epoca assegnatagli.

Con l'istanza, in particolare, è stata lamentata la violazione di alcune disposizioni del Codice (segnatamente degli artt. 11, comma 1, lett. a), b) e d); 13; 23; 24; 26; 31 e ss.) in relazione:

a. alla persistente operatività, successivamente alla risoluzione del rapporto di lavoro con la società (a seguito di licenziamento intimato in data 17.2.2015), dell'account di posta elettronica aziendale, con conseguente possibilità per la società di "accedere a tutte le e-mail, in entrata e in uscita […] senza […] predisporre alcun sistema idoneo ad informare i terzi mittenti della circostanza che le comunicazioni inviate a quell'indirizzo di posta non venivano più ricevute" dal reclamante (cfr. reclamo 22.6.2015, p. 2 e 3);

b. alla circostanza che la società non avesse reso nota "la possibilità […] di acquisire e conservare dati personali contenuti nella casella di posta elettronica e nel personal computer dei dipendenti (anche per effetto di copie di backup), né sulle caratteristiche di eventuali controlli" (cfr. reclamo cit., p. 6);

c. all'accesso "per il tramite dell'area IT al dispositivo Blackberry, già prima del luglio 2014, affidato in uso esclusivo [al reclamante] prendendo visione e «scaricando» numerosi files personali (es. fotografie) attinenti alla vita privata […] sul pc dello stesso senza che [il medesimo] ne fosse informato o avesse autorizzato una simile attività. I suoi dati venivano poi sottoposti a backup"(cfr. reclamo cit., p. 3);

d. all'accesso, avvenuto dopo l'interruzione del rapporto di lavoro, nei locali dell'ufficio assegnato in via esclusiva al reclamante al fine di apprendere tutti gli effetti personali, collocarli all'interno di scatole e successivamente consegnarli all'ex dipendente, "senza

che [lo stesso] fosse presente o ne fosse stato preventivamente informato o avesse autorizzato una simile operazione" (cfr. reclamo cit., p. 4 e 11).

1.2. La società, in risposta alla richiesta di elementi formulata dall'Ufficio, ha dichiarato che:

a. "le dotazioni informatiche affidate […] ai dipendenti nell'ambito del rapporto di lavoro dovrebbero essere esclusivamente utilizzate per fini lavorativi […]. è possibile tuttavia che, nell'ambito delle autonomie di gestione degli apparati, un dipendente utilizzi […] tali strumenti anche per archiviare dati privati" (cfr. nota 3.2.2016, p. 2);

b. con riferimento ai dati contenuti nel pc e nel Blackberry assegnati al reclamante, la società non effettua alcun trattamento, posto che il personal computer è stato restituito dopo l'interruzione del rapporto di lavoro "totalmente e irreversibilmente cancellato, sia per quanto riguarda i file (aziendali e non) sia per i messaggi della casella di posta elettronica"; per quanto riguarda il Blackberry, avendo il reclamante inserito una password di accesso "non prevista dalle procedure IT aziendali", la società "non può accedere ai contenuti del telefono" (cfr. nota cit., p. 3 e 4);

c. la policy interna "non prevede l'esecuzione sistematica di copie di backup dei dispositivi assegnati ai dipendenti, e nelle cartelle di rete di AON non risultano archiviati documenti contenenti dati personali relativi" al reclamante (cfr. nota cit., p. 3);

d. per quanto riguarda i dati contenuti nell'account di posta elettronica "una copia della casella postale aziendale è archiviata sui server Aon EMEA, il cui accesso è […] subordinato ad una procedura di autorizzazione a livello di gruppo […] attraverso l'utilizzo di parole chiave" (cfr. nota cit., p. 4);

e. la casella di posta elettronica assegnata al reclamante "è stata disabilitata dalla funzione IT di Aon il giorno stesso della cessazione del rapporto di lavoro. Per policy aziendale di gruppo, l'account di posta viene immediatamente disabilitato e segue una fase di cancellazione gestita a livello centralizzato dalla funzione IT Aon EMEA (Europe, Middle East e Africa) […]. In tale fase la casella resta attiva solamente per i messaggi in entrata fino alla data di cancellazione definitiva - entro un termine di sei mesi - e viene poi mantenuto solo l'archivio dei messaggi sui server Aon EMEA" (cfr. nota cit., p. 4 e 5);

f. a seguito della "disabilitazione" dell'account e dell'archiviazione sul server "nessuno in Aon può accedervi in assenza di una specifica disposizione da parte della Società. […] Gli unici soggetti che hanno la possibilità di accedervi sono gli Amministratori di sistema della funzione IT EMEA salvo eventuali autorizzazioni all'accesso ad altri utenti concesse dal titolare della casella di posta" (cfr. nota cit., p. 5);

g. a seguito della richiesta del reclamante di accedere ed avere copia dei dati contenuti nella casella di posta "la funzione IT di Aon ha avviato una procedura di autorizzazione […] per l'accesso all'account email sui server EMEA (cd. Security Investigation Request) […].Tale procedura prevede: i. la compilazione di un form dove indicare in dettaglio le motivazioni dell'investigazione; ii. il form deve essere inviato dall'ufficio HR o Legal al Security Risk Management Team; iii. 3 livelli di approvazione da parte del Security Risk Management Team"; la ricerca effettuata sulla base di parole chiave fornite dal reclamante ha tuttavia dato "esito negativo" (cfr. nota cit., p. 5);

h. la società "conferma che per quanto di sua conoscenza non sono stati raccolti e trattati dati personali [del reclamante] contenuti negli strumenti elettronici aziendali dopo la sua uscita e prima della cessazione del rapporto con AON, con l'unica eccezione della procedura di Security Investigation Request […]. In tale ambito l'accesso all'account email sui server EMEA è stato eseguito dagli amministratori di sistema dell'Unità IT di Aon sotto la supervisione del Responsabile IT" (cfr. nota cit., p. 9);

i. la società ha reso nota a tutti i dipendenti la "Guida all'uso degli strumenti informatici Aon", adottata nel 2012, ed ha fornito al reclamante due informative individualizzate (cfr. nota cit., p. 9 e All. 1);

j. la società "non effettua controlli sistematici sull'utilizzo degli strumenti elettronici dei dipendenti ma si riserva la facoltà di effettuare accessi o controlli mirati ex post in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività aziendale, di sicurezza del sistema, o sospetto di attività illecite" (cfr. nota cit., p. 11).

1.3. Con nota di replica pervenuta il 5.4.2016 il reclamante ha ribadito le richieste già avanzate all'Autorità ritenendo, tra l'altro, che dal documento contenente la policy interna sugli strumenti informatici "emerge chiaramente che la società esegue il backup dei dati in relazione alle cartelle condivise e alla posta" (cfr. nota cit., p. 2). Inoltre è stato rappresentato all'Autorità che nell'ambito del procedimento giurisdizionale in corso tra le parti, incardinato dinnanzi al giudice del lavoro, l'interessato ha depositato dichiarazioni effettuate da altri dipendenti della società relative alla presunta circolazione all'interno della compagine aziendale di immagini private a lui riferite che sarebbero state estratte dal Blackberry affidatogli. A ciò si aggiungerebbe anche il trattamento, da parte della società, dei dati di traffico e dei dati relativi alla localizzazione geografica del dispositivo telefonico mobile, circostanza che si evincerebbe da documentazione prodotta in atti (cfr. nota cit., p. 4).

1.4. Con successiva nota pervenuta il 22.6.2016, la società – rispondendo ad una richiesta di integrazioni e chiarimenti formulata dall'Ufficio – ha precisato che:

a. dopo la cessazione del rapporto di lavoro "le caselle di posta elettronica […] vengono mantenute attive […] al fine di garantire l'operatività aziendale e la comunicazione a terzi dell'avvenuta cessazione del rapporto"; il tempo di conservazione "non può in ogni caso superare i sei mesi" anche se "nella prassi locale di AON s.p.a. […] il periodo […] di norma è di due mesi" (cfr. nota cit., p. 2);

b. "i tempi di ulteriore conservazione sui server AON EMEA sono i medesimi che valgono in via generale per il trattamento delle

email aziendali (anch'esse conservate sui medesimi server). In particolare, i messaggi di posta elettronica sono conservati per dieci anni dalla data di invio o ricezione" (cfr. nota cit., p. 3);

c. "l'entità «AON EMEA» è in realtà AON Service Corporation, una società del gruppo AON" che fornisce servizi di Information Technology alle altre società del gruppo AON, compresa AON S.p.A.; tra i servizi offerti vi è "la gestione (in particolare l'hosting) della posta elettronica che, per le affiliate AON a livello EMEA, avviene su server europei" (cfr. nota cit., p. 3);

d. la società ha informato i propri dipendenti, compreso il reclamante, "che i dati connessi alle attività di lavoro possono essere trattati da altre società del gruppo, anche in altri paesi europei e non" (cfr. nota cit., p. 3);

e. al momento della cessazione del rapporto di lavoro "AON invita ogni dipendente uscente ad attivare un messaggio di risposta automatica sulla propria casella che avvisi della chiusura dell'account in corso e inviti i terzi a inoltrare le comunicazioni a un indirizzo email aziendale differente […]. Inoltre la società permette altresì ai dipendenti di scegliere un […] collega […] autorizzato a consultare la sua casella email in caso di necessità" (cfr. nota cit., p. 4);

f. mentre "il salvataggio dei dati in locale è […] sconsigliato", i dati contenuti "negli spazi condivisi, sui server aziendali" sono soggetti, quanto alla conservazione, ad una policy differente, che "prevede copie di backup e altre misure di sicurezza" (cfr. nota cit., p. 5);

g. "eventuali backup dei dispositivi personali possono essere effettuati esclusivamente nell'ambito di interventi di assistenza della funzione IT" (cfr. nota cit., p. 6);

h. per quanto riguarda, invece, i "telefoni [questi], attraverso un'applicazione installata al momento del rilascio al dipendente, inviano periodicamente alcuni dati relativi alle soglie di consumo impostate dalla funzione IT di AON e il loro punto di origine. Tali soglie, una volta raggiunte, fanno scattare delle comunicazioni di allarme presso il personale preposto alla gestione dei contratti, garantendo un puntuale controllo su eventuali problematiche di consumo nei confronti del gestore del servizio. Non sono invece previsti controlli e sanzioni rispetto ai lavoratori per aver ecceduto soglie di traffico" (cfr. nota cit., p. 6);

i. la società, al momento della consegna del Blackberry, fornisce ai dipendenti un'informativa e un "modulo di consenso" relativi al programma "Global Mobility Freedom", all'interno dei quali è rappresentata "la possibilità […] di dover accedere o verificare i dati del dispositivo" (cfr. nota cit., p. 6);

j. nell'ambito dell'informativa resa con la "Guida all'uso degli strumenti informatici AON" la società ha inteso sottolineare "che la funzione IT [può] procedere a controlli sul corretto uso degli strumenti elettronici. Ma si tratta esclusivamente di controlli ex post e mirati, in caso di sospetti di attività illecite o comunque di condotte a danno del patrimonio aziendale, attuabili senza l'uso di particolari apparecchiature e tecnologie, bensì attraverso il semplice accesso ai sistemi o dispositivi elettronici aziendali ed eventualmente all'uso di comuni strumenti di analisi dei dispositivi" (cfr. nota cit., p. 7).

2. L'esito dell'istruttoria.

All'esito dell'esame delle dichiarazioni rese all'Autorità nel corso del procedimento - della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice - nonché della documentazione acquisita, emerge che la società in qualità di titolare ha effettuato (e tutt'ora effettua) operazioni di trattamento di dati personali riferiti al reclamante - nonché ad altri dipendenti - sia in costanza del rapporto di lavoro che successivamente alla sua cessazione, che risultano per alcuni profili non conformi alla disciplina in materia di protezione dei dati personali, nei termini di seguito descritti.

3. Trattamenti di dati effettuati attraverso l'account di posta elettronica aziendale.

Con riferimento ai trattamenti di dati effettuati attraverso l'account di posta elettronica aziendale – individualizzato con nome e cognome del reclamante – risulta che la società ha raccolto i dati contenuti nelle comunicazioni elettroniche in transito sul menzionato account sia nel corso del rapporto di lavoro che successivamente alla sua cessazione, quantomeno fino all'esaurimento della procedura di cancellazione dell'account medesimo. L'effettiva disattivazione, infatti, secondo quanto dichiarato all'Autorità, avviene di regola entro il termine di sei mesi, allo scopo di "garantire l'operatività aziendale e la comunicazione a terzi dell'avvenuta cessazione del rapporto di lavoro" (v. precedente punto 1.2., lett. e. e, in termini parzialmente diversi circa i tempi, punto 1.4., lett. a.).

Tale procedura di cancellazione ed effettiva disattivazione è gestita da AON Service Corporation (v. punto 1.2., lett. e.), la quale gestisce anche il server aziendale sul quale sono conservati per un periodo di dieci anni i dati raccolti (v. punto 1.4., lett. b.). Risulta altresì da quanto dichiarato che in relazione ai dati così memorizzati è possibile attivare una procedura di autorizzazione all'accesso (Security Investigation Request) gestita dalla medesima AON Service Corporation, che consente l'accesso ai dati archiviati anche alla società AON S.p.A. (quantomeno, come nel caso di specie, attraverso gli amministratori di sistema ed il responsabile della struttura di Information Technology: v. punto 1.2., lett. h.).

3.1. L'informativa all'interessato.

In relazione ai descritti trattamenti, in primo luogo, non risulta che la società abbia informato il reclamante - e gli altri dipendenti - circa modalità e finalità della descritta attività di raccolta e conservazione dei dati, né all'interno delle informative individualizzate (cfr. informativa resa al reclamante in data 12.1.2004 e 26.2.2009, nota Aon 3.2.2016, All. 9 e 10) né con i documenti informativi resi noti alla generalità dei dipendenti, in particolare la Guida all'uso degli strumenti informatici Aon (cfr. punto 1.2., lett. i.) e il Codice di condotta commerciale, sia nella versione del 2013, in atti, sia nella versione 2015 reperibile sul sito internet della società.

All'interno di tali documenti non v'è infatti traccia di riferimenti alla conservazione sui server aziendali - per un lungo periodo di tempo (sul quale vedi infra punto 3.3.) - di tutte le email scambiate nell'ambito del rapporto di lavoro (e delle finalità e modalità di conservazione), né dell'esistenza di una procedura di cancellazione dell'account dopo l'interruzione del rapporto ed il persistente trattamento delle comunicazioni per un periodo che può arrivare a sei mesi, né dell'esistenza di una procedura di autorizzazione all'accesso dei dati conservati nei server aziendali (e delle relative finalità).

Ciò risulta in contrasto con l'obbligo posto in capo al titolare del trattamento di fornire una preventiva informativa all'interessato in ordine alle caratteristiche essenziali dei trattamenti effettuati nonché con il principio di correttezza (in relazione agli articoli 11, comma 1, lett. a) e 13 del Codice).

L'informativa ai dipendenti deve inoltre indicare le operazioni di trattamento che possono essere effettuate dall'amministratore di sistema per finalità connesse alla fornitura del servizio (cfr. anche Provv. 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008, modificato con provvedimento del 25 giugno 2009, "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", doc. web n. 1577499, spec. n. 2, lett. c) e f) del dispositivo. In base a tale provvedimento il titolare è altresì tenuto ad adottare sistemi che registrino gli "accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema").

3.2. Trattamenti effettuati sulla posta elettronica aziendale dopo la cessazione del rapporto di lavoro. Disattivazione account.

Con riferimento ai trattamenti effettuati sulla posta elettronica aziendale dopo la cessazione del rapporto di lavoro, come già precisato dal Garante in precedenti occasioni, in conformità ai principi in materia di protezione dei dati personali, gli account riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento. L'interesse del titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività, pertanto, deve essere contemperato con la legittima aspettativa di riservatezza sulla corrispondenza da parte dei dipendenti nonché dei terzi (v. provv.ti 30 luglio 2015, n. 456, doc. web n. 4298277; 5 marzo 2015, n. 136, doc. web n. 3985524 e 27 novembre 2014, n. 551, doc. web n. 3718714).

Non risulta invece conforme ai suesposti principi la procedura adottata dalla società, consistente nel mantenere attive le caselle di posta elettronica per un periodo che può arrivare fino a sei mesi dalla data della cessazione del rapporto. Ciò indipendentemente dall'attivazione di un messaggio di risposta automatico (cfr. punto 1.4., lett. e.). Sotto questo profilo, peraltro, la formula standard che sarebbe stata adottata anche di recente dalla società (v. e-mail del 10.6.2016, All. 17 nota 22.6.2016) risulta fuorviante in quanto reca l'indicazione (ai terzi) che la casella "non è più attiva", mentre l'effettiva disattivazione è prevista solo all'esito di un'ulteriore fase nel corso della quale i messaggi sono raccolti e memorizzati.

3.3. Conservazione dei dati.

Risulta inoltre non conforme ai principi di necessità, pertinenza e non eccedenza (in relazione agli artt. 3 e 11, comma 1, lett. d) e e) del Codice) la conservazione per dieci anni su server aziendali sia dei dati esterni che dei contenuti delle comunicazioni elettroniche. Tale esteso tempo di conservazione applicato indistintamente a tutte le e-mail scambiate (in relazione al quale la società non ha fornito elementi in ordine alle specifiche ragioni che lo renderebbero necessario in relazione agli scopi perseguiti) non appare infatti commisurato alle ordinarie necessità di gestione dei servizi di posta elettronica, comprese le esigenze di sicurezza dei sistemi.

3.4. Flussi di informazioni.

Risulta altresì che la società AON Service Corporation effettua operazioni di trattamento di dati personali raccolti attraverso l'utilizzo degli account di posta elettronica aziendale (conservazione dei dati su server ed accesso ai dati memorizzati, procedura di disattivazione e cancellazione degli account dopo la cessazione del rapporto di lavoro: cfr. punto 1.2., lett. d., e. e f. e punto 1.4., lett. c.), pur essendo entità distinta da AON S.p.A. (e dalle altre società del gruppo AON in Italia).

Diversamente da quanto ritenuto dalla società, pertanto, la trasmissione di dati personali tra i due soggetti è qualificabile come comunicazione di dati. In assenza di un autonomo criterio di legittimazione (allo stato non rinvenuto) AON S.p.A. avrebbe dovuto designare in qualità di responsabile del trattamento ai sensi dell'articolo 29 del Codice la società che fornisce servizi di posta elettronica, impartendo altresì specifiche istruzioni in proposito (cfr. quanto chiarito dal Garante in relazione ai gruppi di imprese con il Provv. 23.11.2006, doc. web n. 1364939, Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati, par. 3.2.).

Anche sotto tale profilo, dunque, i trattamenti effettuati attraverso la posta elettronica non risultano conformi alla disciplina in materia di protezione dei dati personali.

3.5. La disciplina lavoristica.

Infine, la raccolta sistematica delle comunicazioni elettroniche in transito sugli account aziendali dei dipendenti in servizio, la loro memorizzazione per un periodo di dieci anni e la possibilità di accedervi all'esito di una procedura di Security Investigation Request consente alla società di effettuare il controllo dell'attività dei dipendenti.

Ciò risulta in contrasto con la disciplina di settore in materia di controlli a distanza (cfr. artt. 11, comma 1, lett. a) e 114 del Codice e art. 4, legge 20.5.1970, n. 300). Tale disciplina infatti, pure a seguito delle modifiche disposte con l'art. 23 del decreto legislativo 14 settembre 2015, n. 151, non consente l'effettuazione di attività idonee a realizzare (anche indirettamente) il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore (v. Linee guida per posta elettronica e internet citate in premessa, spec. par. 4, 5.2. lett. b) e 6; Consiglio di Europa, Raccomandazione del 1 aprile 2015, CM/Rec(2015)5, spec. princ. 14).

Inoltre il datore di lavoro, pur avendo la facoltà di verificare l'esatto adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, deve in ogni caso salvaguardarne la libertà e la dignità e, in applicazione dei principi di liceità e correttezza dei trattamenti di dati personali, informare in modo chiaro e dettagliato circa le consentite modalità di utilizzo degli strumenti aziendali e l'eventuale effettuazione di controlli anche su base individuale (v., tra gli altri, Provv. n. 139 del 7 aprile 2011, doc. web n. 1812154; Provv. n. 308 del 21.7.2011, doc. web n. 1829641; Provv. 23 dicembre 2010, doc. web n. 1786116). L'assenza di una esplicita policy al riguardo può determinare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione (cfr. Provv. n. 13 del 1° marzo 2007, Linee guida per posta elettronica e internet, doc. web n. 1387522, spec. 3; 5.2. lett. b), e 6.1.).

Considerato inoltre che la società consente - in sé ragionevolmente - "l'uso di e-mail a scopo privato in orario non lavorativo" (cfr. Guida all'uso degli strumenti informatici Aon, par. 4), le descritte operazioni consentono l'eventuale trattamento di dati "non rilevanti ai fini della valutazione dell'attitudine professionale" del dipendente nonché di dati sensibili in violazione dell'articolo 8 della legge 20 maggio 1970, n. 300 e 10 del d. lgs. 10 settembre 2003, n. 276 (si veda sul punto Corte Cass., 19.9.2016, n. 18302 che con riferimento alla violazione del menzionato art. 8 ha ritenuto che "acquisire e conservare dati che contengono (o possono contenere) simili informazioni importa già l'integrazione della condotta vietata").

3.6. Conclusioni: illiceità del trattamento.

Per i suesposti motivi, considerato che il trattamento dei dati effettuato dalla società attraverso gli account di posta elettronica aziendale risulta illecito per violazione degli artt. 3, 11, comma 1, lett. a), d) ed e), 13, 23 e 24, 113 e 114 del Codice, si dispone il divieto di ulteriore trattamento dei predetti dati, fatta salva la conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria, nei limiti posti dall'art. 160, comma 6, del Codice, in base al quale "la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali, ancorché non conforme a disposizioni di legge o di regolamento, restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale".

4. Trattamenti di dati mediante dispositivi assegnati al reclamante.

La società ha dichiarato, sotto propria responsabilità, di non detenere dati personali raccolti attraverso l'uso dei dispositivi affidati al reclamante (personal computer e Blackberry). In proposito si ritiene che dalla documentazione in atti non emergano evidenze dell'avvenuto trattamento da parte della società dei dati di traffico e dei dati di localizzazione geografica del dispositivo telefonico mobile. Non risultano, parimenti, evidenze del lamentato trattamento di dati (in particolare fotografie) tratte dal suddetto Blackberry, circostanza smentita dalla società; si rileva che, ad ogni buon conto, il relativo accertamento è stato devoluto alla cognizione del giudice ordinario.

Risulta tuttavia che i dati archiviati sulle cartelle di lavoro condivise sono conservati sul server aziendale previa effettuazione di copie di backup e "altre misure di sicurezza" (cfr. punto 1.4., lett. f.). Sotto questo profilo emerge che la società ha trattato (e presumibilmente tutt'ora tratta) dati riferiti al reclamante (e agli altri dipendenti), ma in base ai documenti in atti non sono emersi specifici profili di illiceità.

5. Trattamenti di dati contenuti nel Blackberry in dotazione ai dipendenti.

Dall'istruttoria è tuttavia emerso che - in termini generali - la società si riserva di trattare i dati contenuti nel Blackberry fornito in dotazione ai dipendenti (oltre che in occasione di operazioni di manutenzione), sia attraverso l'installazione di un'applicazione preordinata alla rilevazione dell'eccedenza delle soglie di traffico, sia con le modalità stabilite nel programma "Global Mobility Freedom" (cfr. punto 1.4., lett. h. e i.).

Al momento della consegna del Blackberry, infatti, al dipendente è consegnata copia delle "Conditions for Participation" al programma "Global Mobility Freedom" ed un modulo da sottoscrivere (cfr. nota 22.6.2016, All. 18 e 18 bis, disponibile in lingua inglese). All'interno del documento relativo alle condizioni di partecipazione al programma è rappresentata la possibilità per la società di accedere, con diverse modalità, ai contenuti del dispositivo e trattare ulteriormente i dati ivi contenuti:

> accesso da remoto e cancellazione dei dati contenuti sia nell'area (virtuale) riservata ai contenuti aziendali (corporate container) che in qualsiasi altra area del dispositivo (punto 8, Remote Data Clearing: "Aon retains the right to wipe the entire device if there is evidence of a policy violation or an extraordinary failure in the technology to wipe only the corporate container");
>
> accesso ed altre operazioni di trattamento - compresa la comunicazione a (non meglio specificati) soggetti terzi - dei dati contenuti nel dispositivo (punto 9, Right to Access: "Subject to applicable privacy and/or local laws, Aon maintains the right, at any time, to temporarily take possession of your phone, to image, and/or access your device or the container, in the event of a corporate need, such as a legal or internal investigation. All contents of the device may be subject to discovery by third parties");
>
> effettuazione di una pluralità di operazioni di trattamento dei dati contenuti nel dispositivo (indicate esemplificativamente in: raccolta, conservazione, cancellazione, utilizzo, incrocio e comunicazione), alcune delle quali previo trasferimento negli Stati Uniti (punto 11, Processing of Your Information: "[…] you are providing Aon with permission to process your information including, but not limited to, collecting, storing, deleting, using, combining and disclosing information necessary for the participation in the Mobility Freedom 2 program. Some processing activities may take place outside of your home country. […] If you reside outside the United States, your information may be transferred to the U.S. and processed there under U.S. privacy standards and Aon privacy and security standards").

Alcune delle modalità di trattamento previste dalle citate condizioni di partecipazione, ancorché rese note in termini generali all'interessato e sottoposte alla sua accettazione (pur con riserva di compatibilità con la legge applicabile, anche in materia di riservatezza), non risultano conformi ai principi di protezione dei dati, nei termini di seguito indicati.

5.1. L'informativa all'interessato.

Per quanto riguarda l'applicazione informatica - configurata in modo tale da consentire la riferibilità al singolo utente dei dati relativi alle "soglie di consumo" - non risulta che la società abbia informato, come dovuto ai sensi dell'articolo 13 del Codice, i dipendenti interessati circa l'esistenza, le finalità e le concrete caratteristiche dei trattamenti così effettuati.

Inoltre, l'informativa non indica specificamente tipologia, finalità e modalità delle operazioni di trattamento che possono essere effettuate sui dispositivi, nonché gli elementi identificativi dei soggetti che possono trattare i dati e a cui i dati stessi possono essere comunicati.

L'informativa resa appare quindi carente sotto questo specifico aspetto.

5.2. Necessità del trattamento e pertinenza dei dati.

La prevista facoltà per il titolare di accedere da remoto all'area ove sono archiviati i documenti creati nel corso dell'attività lavorativa e cancellarli, nonché la facoltà di accedere, raccogliere, conservare (senza individuare tempi di conservazione proporzionati allo scopo della raccolta), comunicare e cancellare le informazioni comunque presenti all'interno del dispositivo (dunque, in ipotesi, anche di natura privata), in occasione del verificarsi di eventi genericamente indicati ed in assenza della predisposizione di alcuna procedura di garanzia, non è conforme ai principi di liceità, necessità, pertinenza e non eccedenza dei trattamenti (artt. 3, 11, comma 1, lett. a), d) ed e) del Codice).

5.3. La disciplina lavoristica.

Con specifico riferimento alla liceità del trattamento, ciò risulta in contrasto con quanto stabilito dai già citati articoli 4 e 8, l. 20.5.1970, n. 300 e 10, d. lgs. 10.9.2003, n. 276, stante la possibilità per la società di effettuare in tal modo il controllo sistematico e massivo dell'attività del dipendente ed accedere a dati "non rilevanti ai fini della valutazione dell'attitudine professionale" dello stesso nonché, in ipotesi, a dati sensibili.

5.4. Conclusioni: illiceità del trattamento.

Per i suesposti motivi, considerato che il trattamento dei dati effettuato dalla società attraverso i dispositivi Blackberry risulta illecito per violazione degli artt. 3, 11, comma 1, lett. a), d) ed e), 13, 113 e 114 del Codice, si dispone il divieto di ulteriore trattamento dei predetti dati, fatta salva la conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria, nei limiti posti dal già citato articolo 160, comma 6, del Codice.

6. Controlli sull'uso di strumenti informatici.

In relazione all'effettuazione di controlli sui dispositivi elettronici che la società si riserva espressamente di effettuare in base al paragrafo 6 della Guida all'uso degli strumenti informatici AON (par. 6, "Controlli e verifiche": "L'infrastruttura dei Sistemi Informativi ha gli strumenti necessari al monitoraggio delle attività informatiche. Tali attività sono comunque regolamentate dal Garante per la protezione dei dati personali […]"), si prende atto di quanto dichiarato sotto propria responsabilità dalla società (cfr. punto 1.4., lett. j). Si rammenta che in proposito l'Autorità si è pronunciata sulle condizioni di liceità di alcuni trattamenti di dati tratti dall'utilizzo di strumenti di lavoro (v. Provv. n. 303 del 13.7.2016, doc. web n. 5408460, spec. par. 4.2., 4.3. e 5).

7. Trasferimento di dati in Paesi terzi.

Con riferimento ai trattamenti effettuati da AON Service Corporation - società che risulta avere sede in un paese terzo (Stati Uniti) - ed ai trasferimenti in paesi terzi (compresi gli Stati Uniti) dei dati tratti dai dispositivi Blackberry, l'Autorità si riserva di verificarne con autonomo procedimento la conformità alle disposizioni sui trasferimenti di dati all'estero (artt. 43, 44 e 45 del Codice).

8. Restituzione degli effetti personali.

Relativamente alla richiesta volta ad ottenere la restituzione "di tutto ciò che fosse presente nella stanza" a suo tempo assegnata al reclamante, si prende atto che la società ha dichiarato di aver già provveduto alla restituzione dei documenti ed altro materiale rinvenuto nell'ufficio assegnato (cfr. nota della società 3.2.2016, p. 11).

In applicazione del principio di correttezza dei trattamenti (art. 11, comma 1, lett. a) del Codice) e a tutela della dignità della persona (art. 2 del Codice) si invita la società, tenuto conto delle circostanze del caso concreto, ad adottare di regola - in occasione dell'interruzione del rapporto di lavoro (o comunque di trasferimento) del dipendente - procedure che consentano all'interessato di partecipare alla ricognizione (e, se del caso, alla consegna) di documenti o di oggetti collocati all'interno degli uffici, soprattutto in caso di assegnazione di spazi e postazioni ad uso di un singolo e per un periodo significativo di tempo.

9. Aspetti sanzionatori.

L'Autorità si riserva di valutare, con autonomo procedimento, la sussistenza dei presupposti per la contestazione di violazioni amministrative nei confronti della società, in relazione all'omessa informativa agli interessati per i trattamenti effettuati attraverso il servizio di posta elettronica e l'utilizzo dei dispositivi Blackberry (v. punti 3.1. e 5.1., in relazione all'art. 13 del Codice), nonché alla comunicazione di dati ad AON Service Corporation in assenza dei presupposti di legge (v. punto 3.4., in relazione agli artt. 23 e 24 del Codice).

Si ricorda che, ai sensi dell'articolo 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'articolo 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.

TUTTO CIÒ PREMESSO, IL GARANTE

1. ritenuto illecito, nei termini di cui in motivazione (punto 3.6.), il trattamento effettuato dalla società sulle e-mail dei dipendenti ed ex dipendenti in violazione degli artt. 3, 11, comma 1, lett. a), d) ed e), 13, 23 e 24, 113 e 114 del Codice, ai sensi degli artt. 143, comma 1, lett. c) e 154, comma 1, lett. d), del Codice vieta l'ulteriore trattamento dei dati indicati in premessa, salva la loro conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria, nei limiti di cui all'art. 160, comma 6 del Codice;

2. ritenuto illecito, nei termini di cui in motivazione (punto 5.4.), il trattamento effettuato dalla società attraverso i dispositivi Blackberry per violazione degli artt. 3, 11, comma 1, lett. a), d) ed e), 13, 113 e 114 del Codice, ai sensi degli artt. 143, comma 1, lett. c) e 154, comma 1, lett. d), del Codice vieta l'ulteriore trattamento dei dati indicati in premessa, salva la loro conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria, nei limiti di cui all'art. 160, comma 6 del Codice;

3. ai sensi dell'art. 157 del Codice, invita, altresì, entro 30 giorni dalla data di ricezione presente provvedimento, a comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto vietato e prescritto nel presente provvedimento e di fornire comunque riscontro adeguatamente documentato. Si ricorda che il mancato riscontro alla richiesta ai sensi dell'art. 157 è punito con la sanzione amministrativa di cui all'art. 164 del Codice.

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

Roma, 22 dicembre 2016

IL PRESIDENTE
Soro

IL RELATORE
Califano

IL SEGRETARIO GENERALE
Busia