

Garante per la protezione dei dati personali, provvedimento 21 luglio 2011

Il Garante privacy al Poligrafico: più tutele per i lavoratori - 21 luglio 2011

Registro dei provvedimenti
n. 308 del 21 luglio 2011

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Daniele De Paoli, segretario generale;

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

VISTA l'Autorizzazione del Garante n. 1/2009 al trattamento dei dati sensibili nei rapporti di lavoro del 16 dicembre 2009, pubblicata sulla G.U. n. 13 del 18 gennaio 2010 - suppl. ord. n. 12;

VISTE le "Linee guida per posta elettronica e internet" adottate dal Garante con deliberazione n. 13 del 1° marzo 2007, pubblicate sulla G.U. n. 58 del 10 marzo 2007;

VISTE le "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" adottate dal Garante con provvedimento del 27 novembre 2008 (pubblicate sulla G.U. n. 300 del 24 dicembre 2008), come modificato dal provvedimento del 25 giugno 2009 (in www.garanteprivacy.it, doc. web n. 1577499);

ESAMINATE le risultanze istruttorie degli accertamenti in loco effettuati in data 12 e 13 maggio 2011 presso la sede dell'Istituto Poligrafico e Zecca dello Stato s.p.a. in Roma;

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

RELATORE il prof. Francesco Pizzetti;

PREMESSO

1. Accertamenti relativi all'utilizzo dei servizi di comunicazione elettronica

In data 12 e 13 maggio 2011 sono stati effettuati presso la sede dell'Istituto Poligrafico e Zecca dello Stato s.p.a. (interloquendo con i responsabili dell'area "ICT e business solutions", "Risorse umane", con il "responsabile privacy" e con il responsabile "Information security e assicurazione qualità" nonché con alcuni amministratori di sistema) accertamenti finalizzati alla verifica dell'osservanza dei principi e delle disposizioni in materia di protezione dei dati personali relativi all'utilizzo dei sistemi di comunicazione elettronica, in particolare:

- i. internet (punto 2),
- ii. posta elettronica aziendale (punto 3),
- iii. sistemi di telefonia su protocollo IP (sistemi di telefonia VoIP) (punto 4) da parte dei dipendenti della società, nonché
- iv. le correlate modalità di attuazione delle misure prescritte ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema in relazione ai menzionati sistemi di comunicazione elettronica (punto 5).

2. La navigazione in internet

2.1. L'uso di Internet da parte degli utenti (per lo più dipendenti della società) – disciplinato dalla società nell'ambito di più ampie istruzioni impartite ai propri dipendenti per il tramite di un opuscolo (in larga misura incentrato sulle diverse misure di sicurezza da adottare) denominato "*Istruzioni agli Incaricati al trattamento di dati personali*", consegnato agli stessi e reso disponibile sulla rete intranet dell'Istituto, nelle quali si prevede che "l'attività in internet dei singoli utenti viene registrata in appositi log mantenuti dai Sistemi Informativi" (cfr. all. 5 al verbale delle attività del 12.5.2011, p. 16) – è regolato da appositi filtri di navigazione. Questi ultimi sono implementati mediante uno specifico software, denominato XY, che opera congiuntamente a un sistema proxy/web gateway, "per finalità di tutela aziendale e per poter eventualmente riferire all'Autorità Giudiziaria comportamenti anomali registrati dai sistemi" (cfr. verb. 12.5.2011, p. 7). In tal modo la società intende prevenire il libero accesso ai siti presenti in rete da parte della generalità dei lavoratori, confinandolo ai soli siti web ritenuti conferenti con lo svolgimento delle attività lavorative (salva diversa valutazione da effettuarsi caso per caso).

Il sistema di filtraggio della navigazione web come configurato presso la società non si limita però a rifiutare la connessione a (categorie di) siti reputati ex ante inconferenti con lo svolgimento delle attività lavorative, ma memorizza "*l'accesso e i tentativi di accesso di ogni singolo dipendente ai domini selezionati e registra i log che contengono le seguenti informazioni: la macchina utilizzata per l'accesso ad Internet, data e ora dell'accesso (c.d. timestamp), indirizzo (url) di destinazione e utente richiedente*" (cfr. verb. 12.5.2011). Dalle verifiche effettuate sui diversi componenti del menzionato sistema di filtraggio proxy/web gateway è risultato che lo stesso consente di:

- a. generare, su base giornaliera, report individuali relativi ai siti web visitati da ciascun lavoratore, indicandolo nominativamente (cfr. verb. 12.5.2011, all. 8, p. 3). Gli esempi visualizzati nel corso delle operazioni di verifica "*hanno confermato la presenza nei suddetti file di log delle URL complete relative ai siti visitati dai dipendenti attraverso il server proxy aziendale, comprensive di data e ora della visita e dell'indirizzo IP della postazione utilizzata dal dipendente*" (cfr. verb. 12.5.2011);
- b. eseguire interrogazioni dei log relativi alla navigazione in Internet effettuata da ciascuno degli utenti;
- c. fornire, inoltre, statistiche della navigazione di tipo aggregato (ad esempio, per categoria di siti web permessi/bloccati, per indirizzo del sito web ovvero per postazione utilizzata).

Ancorché la società disponga dei dati relativi alla navigazione Internet riconducibili ad ogni singolo utente – la cui conservazione riguarda circa 1200 persone ed oscilla tra "un periodo minimo di sei mesi e massimo di un anno", essendo vincolata "alla disponibilità di spazio per l'archiviazione" predefinito dalla società nella misura di circa 1500 MB (cfr. verb. 12.5.2011, p. 7) –, gli stessi non sono stati mai richiesti dall'autorità giudiziaria, né la società ha effettuato segnalazioni sulla base di tali dati o se ne è altrimenti avvalsa per finalità disciplinari (cfr. verb. 12.5.2011, p. 4).

Per giustificare la prolungata conservazione dei dati relativi agli accessi, nonché di quelli semplicemente oggetto di tentativo, sono state rese dichiarazioni contraddittorie da parte di diversi rappresentanti della società: a fronte dell'affermazione secondo cui "i dati della navigazione Internet contenuti nei log [del proxy] vengono conservati dalla società per individuare accessi a siti reputati pericolosi o inconferenti non ancora censiti da XY e, in pari tempo, per verificare il buon funzionamento del sistema di filtraggio di quest'ultimo" (cfr. verb. 13.5.2011), non solo la società non è stata in grado di dimostrare quali fossero "i siti web [da bloccare] inseriti ex novo a seguito dei controlli sui log [del proxy] e quindi non già presenti nell'ambito dei filtri preimpostati dal prodotto", ma è stato altresì dichiarato che non sono mai avvenute "attività di verifica sui dati presenti nei log [del proxy] al fine di affinare, attraverso opportune personalizzazioni, i filtri [utilizzati]" (cfr. verb. 13.5.2011).

Nell'ambito dell'attività ispettiva svolta, è altresì emerso che XY "categorizza le pagine filtrate ricorrendo ad una molteplicità di classi di siti visitati, tra i quali, si trovano indicizzati quelli raggruppati nella dizione entertainment, vehicles, marketing, sex, sport, ecc." e che tale indicizzazione determina altresì la categorizzazione, su base individuale, della navigazione effettuata da ciascun utente secondo le categorie predefinite dal sistema medesimo, quali, ad esempio, quelle denominate *adult material, advocacy groups, business and economy, entertainment, abortion, drugs, militancy and extremist* (cfr. all. 1, verb. 13.5.2011).

Peraltro, dalla documentazione acquisita in atti, e segnatamente dal documento dedicato all'"Utilizzo delle risorse informatiche e di rete" – redatto dalla funzione interna deputata al "Sistema di gestione per la qualità" e approvato dal direttore ICT (all. 12, 2 al verb. 12.5.2011), nonché richiamato nel documento programmatico sulla sicurezza - DPS (all. 6 al verb. 12.5.2011, punto 6.5, p. 122) –, risulta che, con l'intento di "provvedere ad un'efficiente attività di monitoraggio e controllo", "si rende necessario attivare una serie di norme, restrizioni e controlli per garantire la sicurezza dei sistemi e definire le responsabilità degli utilizzatori delle risorse" (cfr. all. 6, p. 4). In questa prospettiva, tra le varie misure previste, si precisa che "gli amministratori di sistema sono obbligati [...] a garantire la massima riservatezza nella trattazione dei dati personali anche desunti dal software di analisi di traffico, a mantenere riservate le informazioni relative al collegamento degli utenti fatti salvi i casi di interessamento della Magistratura a fronte di ipotesi di reato" (all. 6, p. 7).

Nel menzionato DPS è poi specificato che "i log della navigazione internet dei singoli dipendenti sono mantenuti ed archiviati su supporti magnetici custoditi in cassaforte. La loro archiviazione è dovuta al fatto che tutti i log prodotti dai sistemi debbono essere mantenuti, ma nessuno ha accesso a queste informazioni. Gli unici abilitati alla consultazione sono i sistemisti che amministrano l'applicativo, ma vista la loro natura e secondo le direttive del Garante nessuno utilizza queste informazioni per finalità legate al controllo della persona od altro" (cfr. DPS, p. 122). Nel corso degli accertamenti è invece risultato che tutti i dati relativi alle navigazioni individuali sono oggetto di conservazione su XY.

È stato infine accertato che rispetto alle operazioni di raccolta, memorizzazione e conservazione dei dati relativi alla navigazione web dei dipendenti non è stato stipulato "nessun accordo con le organizzazioni sindacali [...], né esiste un'autorizzazione della Direzione provinciale del lavoro" (cfr. verb. 12.5.2011, p. 4). Tale circostanza è stata confermata anche dal responsabile delle risorse umane della società, il quale ha ulteriormente precisato (cfr. verb. 13.5.2011, p. 5) che:

i. la scelta dei sistemi e della funzionalità degli stessi in relazione alle potenzialità di "filtraggio" nell'utilizzo dei servizi Internet non viene effettuata dalla Direzione risorse umane, e che tale direzione non ha concordato le modalità d'uso del sistema esistente presso la direzione ICT;

ii. rilevate le potenzialità di controllo dei dipendenti proprie del sistema di filtraggio in uso, in un prossimo futuro la società intenderebbe interloquire al riguardo con le rappresentanze sindacali aziendali.

2.2. In base ad una complessiva valutazione degli elementi sopra indicati, deve ritenersi che il trattamento di dati personali riferito a ciascun utente ed effettuato dalla società mediante la sopra descritta configurazione del sistema di filtraggio – con funzionalità tali da consentire la memorizzazione sistematica (per un arco temporale assai ampio) dei domini web richiesti dagli utenti, la cui visualizzazione sia stata consentita o meno dal sistema – presenti più profili di violazione di legge, e in particolare della disciplina di protezione dei dati personali (ed inoltre si discosti dalle indicazioni fornite dal Garante nelle menzionate Linee guida; v. altresì il Provv. 2 aprile 2009, doc. web n. [1606053](#)).

In primo luogo, risulta che il descritto trattamento sia effettuato in violazione dell'art. 4, comma 1, l. 20 maggio 1970, n. 300 che vieta l'impiego di apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Ciò, come si è visto al punto 2.1, in ragione:

a. della configurazione del sistema di filtraggio, tale da consentire un controllo a distanza della navigazione web individualmente effettuata dagli utenti;

b. della specifica funzionalità di XY atta a categorizzare, nelle modalità in uso presso la società, su base individuale e con una significativa profondità temporale nella memorizzazione dei dati, la navigazione web effettuata (o, come detto, solo tentata) dai singoli utenti;

c. delle modalità operative e delle direttive impartite agli incaricati del trattamento (in particolare, agli amministratori di sistema) circa la "policy" della società in relazione al trattamento dei dati relativi alla

navigazione *web* degli utenti (cfr. quanto riferito al punto 2.1. in relazione alla riconosciuta possibilità di "consultazione dei dati relativi ai *log* di navigazione" per i "sistemisti", nonché degli obblighi di confidenzialità per gli amministratori in ordine alla "trattazione dei dati personali anche desunti dal *software* di analisi di traffico").

Inoltre, anche a volere, in ipotesi, far confluire la fattispecie in esame in quella astrattamente prevista dal secondo comma del menzionato art. 4, l. n. 300/1970 – in relazione a funzionalità che, ricorrendo "*esigenze organizzative e produttive*", legittimamente potrebbero essere perseguite mediante il sistema di filtraggio opportunamente installato e configurato – egualmente l'installazione del sistema di filtraggio (e il conseguente trattamento di dati) sarebbe vietata, in quanto la società non ha provveduto a dare attuazione agli adempimenti previsti dalla disposizione richiamata (nel senso della violazione dell'art. 4, l. n. 300/1970 per il tramite di software che consentono il monitoraggio della posta elettronica e degli accessi a internet cfr. anche Cass., Sez. lav., 23 febbraio 2010, n. 4375).

A ciò deve altresì aggiungersi che la categorizzazione di ciascun utente realizzata tramite la configurazione di XY in essere presso la società consente, oltre alla menzionata possibilità di un controllo a distanza dell'attività effettuata, anche una vera e propria "profilazione" degli utenti, in grado di rivelare, con immediatezza, dati sensibili ad essi riferiti, ivi comprese informazioni il cui trattamento è precluso dall'art. 8 l. n. 300/1970, disposizione che vieta al datore di lavoro, anche nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale dello stesso.

Nella prospettiva appena raffigurata, il trattamento dei dati personali relativi ai log delle navigazioni *web* degli utenti risulta quindi effettuato in violazione del principio di liceità di cui all'art. 11, comma 1, lett. a) e degli artt. 113 e 114 del Codice che richiamano espressamente le anzidette disposizioni della legge n. 300/1970.

Con riferimento ai principi di protezione dei dati personali di cui all'art. 11 del Codice, il trattamento dei dati in questione non risulta poi essere lecitamente effettuato anche sotto ulteriori profili, e segnatamente:

a. con riguardo alla qualità dei dati trattati (art. 11, comma 1, lett. c), del Codice), giacché il sistema memorizza non solo gli accessi e i tentativi di accesso ai domini *web* effettivamente richiesti dall'utente, "*ma anche [i] frame comunque presenti sulle pagine visualizzate*", vale a dire qualsiasi dominio *web* comunque richiamato, indipendentemente dalla volontà dell'utente, all'interno della pagina *web* visitata (quali box, *banner* e *pop up*) (cfr. verb. 13.5.2011): i dati memorizzati in XY possono quindi ben essere inesatti, in quanto relativi a siti *web* non espressamente visitati su richiesta dell'utente;

b. con riguardo alla pertinenza e non eccedenza dei dati trattati (art. 11, comma 1, lett. d), del Codice), tenuto conto:

i. del monitoraggio prolungato e costante effettuato sui singoli utenti dalla società, parametrato, come si è visto, sulla mera capienza del supporto di memorizzazione (in merito cfr. anche le citate *Linee guida*, punto 6);

ii. della memorizzazione di tutte le pagine *web* visitate e finanche dei tentativi di accesso a pagine *web* inibiti a priori dal sistema di filtraggio (che ne impedisce quindi la visualizzazione al dipendente).

In relazione ad entrambi tali profili, come detto al punto 2.1, gli elementi forniti dalla società sono risultati contraddittori e comunque nessuna attività di quelle dichiarate (a fondamento della rilevata conservazione) risulta essere stata effettuata. Peraltro, anche ove si intendesse, come dichiarato, verificare la funzionalità del prodotto XY, ben potrebbero essere a tal fine utilizzati i dati delle navigazioni effettuate previa loro anonimizzazione. Anche in questa prospettiva risulta, quindi, che il trattamento effettuato si ponga in violazione della disciplina di protezione dei dati personali (art. 11, comma 1, lett. d) del Codice).

Infine, a fondare ulteriormente l'illiceità del trattamento così effettuato, deve rilevarsi che la descritta attività di profilazione degli utenti:

a. non ha formato oggetto di informativa agli interessati (ai sensi dell'art. 13 del Codice);

b. non è consentita nell'Autorizzazione del Garante n. 1/2009 al trattamento dei dati sensibili nei rapporti di lavoro del 16 dicembre 2009, né rispetto ad essa è stato raccolto il consenso scritto dei lavoratori interessati (art. 26 del Codice);

c. non ha formato oggetto di notificazione al Garante (art. 37, comma 1, lett. d), del Codice).

2.3. Tanto premesso, limitatamente al monitoraggio degli accessi a Internet, il Garante:

a. ai sensi degli artt. 143, comma 1, lett. c), e 154, comma 1, lett. d), del Codice, con effetto immediato dalla data di ricezione del presente provvedimento, vieta l'ulteriore trattamento, nella forma della conservazione e della categorizzazione su base individuale, dei dati personali riferiti alla navigazione internet dei dipendenti, con conservazione di quelli finora trattati in vista di un'eventuale acquisizione degli stessi da parte dell'autorità giudiziaria, cui atti e copia del presente provvedimento verranno trasmessi per le valutazioni di competenza (cfr. punto 7), nonché per esigenze di tutela dei diritti in sede giudiziaria;

b. si riserva di valutare con autonomo procedimento la sussistenza delle violazioni di cui agli artt. 161, 162, comma 2-bis e 163 del Codice.

3. Il servizio di posta elettronica

3.1. Le modalità di utilizzo dei sistemi di posta elettronica non hanno formato oggetto di apposito disciplinare da parte della società – che tuttavia nelle menzionate Istruzioni agli incaricati ha previsto che non debba essere utilizzata *"la casella postale assegnata per fini privati e personali"* (p. 15) –, né specifica informativa ai sensi dell'art. 13 del Codice è stata fornita all'utenza in ordine al funzionamento del servizio e alle modalità di archiviazione ed eventuale accesso da parte di incaricati o responsabili del trattamento ai messaggi di posta elettronica.

Dalle dichiarazioni rese, *"l'uso della posta aziendale non è sottoposto ad alcun controllo. I sistemi informativi conservano, attraverso JH, solo traccia dei dati necessari (header) per l'esecuzione del servizio. La società non accede in ogni caso al contenuto delle e-mail inviate e ricevute dai dipendenti"* e *"i dipendenti possono utilizzare tutte le caselle di posta elettronica privata, purché sia consentito l'accesso alle stesse via web"* (cfr. verb. 12.5.2011, p. 4). Inoltre, all'interno della società risultano avere accesso ai sistemi per l'erogazione e la gestione dei servizi di posta elettronica solo "una parte degli amministratori di sistema risultanti dall'elenco allegato al dps", pari a 7 unità (cfr. All. C al DPS in atti).

Nel corso delle verifiche volte ad accertare l'eventuale archiviazione dei messaggi di posta elettronica presso il server della società (e le modalità attraverso cui ciò avviene) – circostanza che uno degli amministratori del servizio di posta elettronica, peraltro quello incaricato di assicurare l'ordinaria funzionalità del servizio, ha dichiarato di non conoscere (verb. 13.5.2011, p. 3) –, è emerso che:

a. i messaggi di posta elettronica riferiti agli utenti che si avvalgono di programmi configurati per mantenere la posta permanentemente archiviata sul server sono memorizzati *"in chiaro"* in una specifica cartella del menzionato server e, conseguentemente,

b. tutti gli amministratori abilitati ad un accesso sistemistico al suddetto server sono potenzialmente in grado di visualizzare i messaggi di posta, come accertato con riferimento alla casella del "responsabile privacy" della società, utilizzata a scopo dimostrativo e con il consenso dell'interessata (cfr. verb. 13.5.2011, p. 4 e all. 12 al medesimo verbale).

Rilevata la presenza della cartella contenente i messaggi di posta elettronica, un altro amministratore di sistema partecipante alle verifiche ha precisato che *"la memorizzazione e l'archiviazione dei messaggi di posta elettronica sul server non è regolata da alcuna policy specifica della società, al di là di quelle predisposte per lo spazio massimo occupato dalle caselle, e pertanto ogni utente può liberamente scegliere di mantenere la propria posta elettronica nel disco del server [...] o in alternativa di cancellarla dal server memorizzandola sul disco fisso locale del computer usato per accedere alla posta [...]"* (cfr. verb. 13.5.2011, p. 4).

3.2. Nel corso degli accertamenti è stato altresì verificato che la menzionata cartella destinata all'archiviazione di tutta la posta elettronica degli utenti è accessibile soltanto agli amministratori di sistema mediante l'uso della specifica utenza di amministratore (c.d. "root") e che il file di log dal quale possono desumersi gli ultimi comandi eseguiti dall'utente "root" sul server di posta (c.d. file di history del sistema operativo), ivi inclusi quelli relativi a eventuali accessi alla cartella contenente i messaggi di posta, è stato azzerato e inizializzato nel mese di aprile 2011 in occasione di un aggiornamento software. Dagli accertamenti eseguiti, limitati quindi ad un intervallo temporale di circa un mese, non sono emersi profili di rilevanza per l'attività di controllo.

3.3. Alla luce degli accertamenti effettuati, deve ritenersi che la società non abbia fornito agli utenti un'informativa conforme alla previsione contenuta nell'art. 13 del Codice con riguardo all'utilizzo del servizio di posta elettronica atteso che la stessa si è limitata a rendere noto ai dipendenti il divieto di *"utilizzare la casella postale per fini privati e personali"* (cfr. all. 5, verb. 12.5.2011, Istruzioni agli incaricati, p. 15), senza esplicitare però né le modalità del trattamento (art. 13, comma 1, lett. a) del Codice), non essendo stato chiarito agli stessi che la società, qualora l'utente si avvalga di programmi configurati per mantenere la posta permanentemente archiviata sul server, conserva tutti i messaggi di posta elettronica scambiati, né quali siano i soggetti che, in qualità di incaricati o responsabili, a tali messaggi possono (come dimostrato) accedere (art. 13, comma 1, lett. d) del Codice). Tanto, anche alla luce della prescrizione impartita dal Garante nel menzionato provvedimento del 27 novembre 2008 (al n. 2, lett. c), del dispositivo) secondo cui *"qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 [...]; in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini)"*.

Alla luce delle precedenti considerazioni, ai sensi degli artt. 143, comma 1, lett. b), e 154, comma 1, lett. c), del Codice, si prescrive alla società di fornire una compiuta informativa ai sensi dell'art. 13 del Codice con riguardo al trattamento effettuato per rendere il servizio di posta elettronica.

4. Sistema di telefonia VoIP

4.1. Con riguardo all'utilizzo di sistemi di comunicazione elettronica, la società ha altresì rappresentato che è in corso di realizzazione un piano di migrazione della rete telefonica dalla tecnologia tradizionale (a circuito) a quella su protocollo IP (VoIP): allo stato, circa 300 utenze (su 1800) – parte delle quali configurate anche a beneficio di altri enti e società (allo stato Editalia, Bimospa e Ministero dell'economia e delle finanze) – si avvalgono di questa tecnologia.

Un solo utente della società è abilitato ad operare, con privilegi di amministratore, sui sistemi di telefonia VoIP comprensivi di (cfr. verb. 13.5.2011, p. 6):

a. una piattaforma di gestione delle utenze telefoniche (QZ) usata per la configurazione di nuove utenze, con l'attribuzione dei servizi di telefonia decisi dalla società per ciascuna tipologia di utente;

b. un secondo sistema grazie al quale la "società effettua il trattamento dei dati di traffico generati dalle centrali telefoniche" nel quale gli stessi sono conservati (denominato HH) ed ai quali è possibile accedere "attraverso un'applicazione web denominata XZ", sistema di analisi e controllo del traffico telefonico tramite il quale sono visualizzati i dettagli delle chiamate in uscita che il sistema, in fase di implementazione, provvede a memorizzare per un intervallo temporale non ancora stabilito. Con l'eccezione di una perdita di informazioni nella fase iniziale di implementazione del sistema, tutti i dati relativi alle chiamate effettuate sono quindi conservati a far data dalla sua installazione (avvenuta nel dicembre 2010). Considerato che la società fornisce un servizio di telefonia VoIP anche a soggetti terzi, in relazione ad essi si è ravvisata la "necessità di conservare tali dati per finalità di fatturazione sulla base della periodicità di fatturazione stabilita" (su base trimestrale e, in un caso, annuale: cfr. verb. 13.5.2011, p. 6).

Dagli accertamenti effettuati è inoltre emerso che la società:

a. non ha stabilito regole o policy interne relative all'utilizzo del sistema di telefonia VoIP, con particolare riferimento all'autorizzazione all'uso anche per finalità personali dello stesso né, nell'ipotesi affermativa, che gli eventuali costi delle comunicazioni vengano imputati in capo ai dipendenti;

b. non ha fornito all'utenza apposita informativa circa le categorie di soggetti ai quali gli stessi possono eventualmente essere comunicati o che, in qualità di responsabili o incaricati del trattamento, possono comunque venirne a conoscenza (art. 13, comma 1, lett. d), del Codice);

c. non ha provveduto a dare attuazione agli adempimenti previsti dall'art. 4, comma 2, l. n. 300/1970 in relazione al menzionato sistema "XZ" di analisi e controllo del traffico telefonico dei dipendenti realizzato su base individuale;

d. può in astratto avvalersi, in relazione al sistema di telefonia VoIP installato, di una funzione di "alert" – che si è dichiarato non essere stata utilizzata – in grado "di configurare l'invio automatico di un messaggio di posta elettronica ad un indirizzo e-mail a scelta ogni qual volta un numero interno effettua una chiamata verso determinati numeri esterni configurabili dall'amministratore" (cfr. verbale 13.5.2011, p. 7).

4.2. Anche il trattamento di dati personali connesso al servizio di telefonia VoIP presenta profili di illiceità.

Anzitutto, considerata la potenzialità del controllo a distanza sull'attività dei dipendenti realizzata attraverso il menzionato sistema di analisi del traffico telefonico (le cui funzionalità di controllo si sono sopra descritte) tramite il quale sono acquisite le numerazioni delle utenze chiamate e la durata delle comunicazioni senza che siano stati posti in essere gli adempimenti previsti dall'art. 4, comma 2, l. n. 300/1970, il trattamento risulta essere effettuato in violazione degli artt. 114 e 11, comma 1, lett. a) del Codice.

Per ulteriori ragioni, poi, il trattamento presenta profili di illiceità: da un lato, non essendo stata fornita idonea informativa agli utenti circa i soggetti che, anche in qualità di incaricati o responsabili del trattamento, possono venire a conoscenza dei dati trattati (art. 13, comma 1, lett. d), del Codice); tanto anche alla luce della menzionata prescrizione impartita dal Garante nel provvedimento del 27 novembre 2008 (al n. 2, lett. c), del dispositivo).

D'altro canto, rispetto ai dati riferiti ai dipendenti, allo stato non risulta giustificata, alla luce del principio di pertinenza e non eccedenza (art. 11, comma 1, lett. d), del Codice) la conservazione dei dati relativi alle telefonate effettuate mediante il sistema VoIP, atteso che nessun corrispettivo viene agli stessi richiesto nell'eventualità in cui il servizio sia fruito per finalità personali, né sono state indicate dalla società ragioni ulteriori per la conservazione di tali informazioni (come invece accaduto rispetto a soggetti terzi cui sono forniti i servizi di telefonia VoIP). Rispetto a tali dati (parte dei quali, peraltro, è andata perduta nella fase di prima implementazione del servizio) deve pertanto disporsi il divieto dell'ulteriore trattamento, fino all'eventuale espletamento delle procedure all'uopo previste dall'art. 4, comma 2, l. n. 300/1970 e previa idonea informativa degli utenti ai sensi dell'art. 13 del Codice, con conservazione di quelli finora trattati in vista di un'eventuale acquisizione degli stessi da parte dell'autorità giudiziaria, cui atti e copia del presente provvedimento verranno trasmessi per le valutazioni di competenza (cfr. punto 7), nonché per esigenze di tutela dei diritti in sede giudiziaria.

Resta salvo il loro eventuale trattamento ricorrendo ad opportune tecniche di anonimizzazione – con modalità da comunicare a questa Autorità – per eventuali esigenze di analisi statistica delle direttrici di chiamata (ad es. verso particolari archi di numerazione o verso determinati operatori), finalità per la quale non è necessario disporre di dati (direttamente o indirettamente) nominativi, specie se per tempi prolungati e, come nel caso di specie, non ancora definiti.

In relazione ai tempi di conservazione dei dati riferiti ad utenze altre rispetto ai soli dipendenti della società, risulta giustificata una limitata conservazione dei dati a fini di fatturazione. Considerata la fase di prima introduzione del servizio e anche al fine di omogeneizzare i tempi di conservazione per finalità di fatturazione, si invita tuttavia codesta società a valutare attentamente i tempi di conservazione e si prescrive, quale misura opportuna, che tali tempi di conservazione siano contenuti entro il limite dei sei mesi, salva l'ulteriore conservazione dei dati ove gli stessi formino oggetto di contestazione e la società sia chiamata a tutelare le proprie pretese (cfr. in tal senso, per la fattispecie della conservazione dei dati di traffico da parte del fornitore dei servizi di comunicazione elettronica, l'art. 123, comma 2, del Codice).

Con riguardo infine, alla funzionalità di "alert" sopra descritta al punto c) – che allo stato, in base alle dichiarazioni rese, non ha formato oggetto di utilizzo da parte della società –, risolvendosi la stessa nella possibilità di un controllo

a distanza dei lavoratori, la stessa si pone in contrasto con la disposizione contenuta nell'art. 4, comma 1, l. n. 300/1970.

4.3. Alla luce delle precedenti considerazioni, ai sensi degli artt. 143, comma 1, lett. c), e 154, comma 1, lett. d), del Codice, con effetto immediato dalla data di ricezione del presente provvedimento, si dispone nei confronti della società il divieto dell'ulteriore trattamento, nella forma della conservazione dei dati personali relativi alle utenze telefoniche chiamate dai singoli dipendenti, fino all'eventuale espletamento delle procedure all'uopo previste dall'art. 4, comma 2, l. n. 300/1970 e previa idonea informativa degli utenti ai sensi dell'art. 13 del Codice, con conservazione di quelli finora trattati in vista di un'eventuale acquisizione degli stessi da parte dell'autorità giudiziaria, nonché per esigenze di tutela dei diritti in sede giudiziaria.

Inoltre, ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c), del Codice si prescrive alla società:

a. quale misura necessaria, di provvedere a disattivare la menzionata funzione di "alert" senza ritardo, e comunque entro e non oltre tre mesi dal ricevimento del presente provvedimento dandone contestuale comunicazione a questa Autorità;

b. quale misura opportuna, limitatamente ai tempi di conservazione dei dati riferiti ad utenze del servizio di telefonia VoIP altre rispetto ai soli dipendenti della società, di contenere i medesimi entro i limiti dei sei mesi, salva l'ulteriore conservazione dei dati ove gli stessi formino oggetto di contestazione e la società sia chiamata a tutelare le proprie pretese.

5. I trattamenti effettuati dagli amministratori di sistema

5.1. Nell'ambito delle complessive attività di verifica correlate all'utilizzo dei sistemi di comunicazione elettronica in uso presso l'Istituto è stata altresì verificata la modalità di attuazione delle misure prescritte ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, acquisendo le dichiarazioni dei rappresentanti della società (punto a) nonché effettuando verifiche dirette – aventi ad oggetto il sistema KW, sistema di registrazione appositamente configurato per il tracciamento degli accessi degli amministratori di sistema ed installato dalla società per dare attuazione al provvedimento del Garante del 27 novembre 2008 citato in premessa (punto b) – e indirette – mediante opportuni riscontri sui sistemi oggetto di monitoraggio (punto c) –.

a) In proposito la società ha dichiarato che *"vengono registrati in un apposito sistema [...] i dati relativi a login, logout, timestamp e utenza di accesso (username); non viene, invece, registrato il dettaglio dell'attività svolta dagli amministratori (attività sistemistica) successivamente al login"* (cfr. verb. 12.5.2011, p. 5).

b) Effettuate le verifiche su KW è risultato che:

i. il sistema è stato configurato per registrare il log degli accessi degli amministratori (conformemente a quanto sopra riferito) per un periodo massimo di 1 anno e che in esso confluiscono i log di accesso di tipo sistemistico degli amministratori ai sistemi proxy, ai sistemi firewall, ai server di posta elettronica e a tutti gli altri sistemi informatici gestiti dal gruppo ICT;

ii. in aggiunta a tale misura (prevista dal provvedimento del Garante), l'accesso al sistema KW viene altresì segnalato automaticamente, con un'apposita e-mail di *alert* sia all'indirizzo e-mail dell'amministratore del sistema medesimo, sia a quello del responsabile "Information security e assicurazione qualità";

iii. il sistema consente di generare statistiche dettagliate sugli accessi effettuati dagli amministratori ai singoli sistemi e una ulteriore reportistica riassuntiva preordinata alla predisposizione di "relazioni periodiche redatte a cura del direttore ICT ed inviate al responsabile privacy, il quale ne rende informativa all'amministratore delegato" (verb. 12.5.2011, p. 5).

c) Al fine di riscontrare la completezza delle attività di tracciamento realizzate tramite il descritto sistema di registrazione degli accessi degli amministratori (nonché l'idoneità dello stesso a consentire le necessarie verifiche sulle attività di *log in/out* degli amministratori medesimi), sono stati quindi effettuati ulteriori accessi a XY e al sistema di telefonia VoIP, entrambi oggetto di monitoraggio mediante KW.

Da tale ulteriore attività sono emersi esiti discordanti.

Infatti, le registrazioni degli eventi di accesso di tipo sistemistico effettuati dagli amministratori a XY e al sistema di gestione della telefonia VoIP sono rinvenibili nella reportistica generata da KW (cfr. all. 7 al verb. 12.5.2011, p. 13-14 e all. 13 al verb. 13.5.2011, p. 2).

Tuttavia le registrazioni degli eventi di accesso ai medesimi sistemi effettuate mediante interfaccia di tipo applicativo (ad es. interfaccia web) non sono invece rinvenibili nella medesima reportistica (cfr. all. 10 al verb. 12.5.2011 e dichiarazioni contenute nello stesso verbale, p. 6, dal quale risulta che l'accesso con interfaccia web a XY *"non veniva evidenziato dalla reportistica standard di KW attualmente predisposta"*, nonché verb. 13.5.2011, p. 6).

La rilevata discordanza nel sistema di tracciamento KW degli accessi degli amministratori di sistema ai XY e al sistema VoIP è stata peraltro confermata nel corso degli accertamenti dalle dichiarazioni rese in atti da rappresentanti della società, secondo le quali:

i. i log memorizzati nel sistema di registrazione degli accessi *"includono soltanto accessi di tipo sistemistico (accessi fatti da un amministratore al sistema operativo ...), mentre la citata reportistica [...] utilizzata per il controllo degli amministratori non include gli accessi degli amministratori effettuati dal pannello generale di*

gestione del prodotto XY tramite il quale è possibile controllare la navigazione web effettuata dai dipendenti" (cfr. verb. 12.5.2011, p. 6);

ii. *"gli accessi al sistema XY effettuati dagli amministratori in possesso di credenziali interne al sistema stesso non vengono registrati da KW in quanto [...] sussistono ostacoli di natura tecnica nella raccolta di tali log. Diversamente, in caso di accesso al sistema XY da parte degli amministratori tramite credenziale di dominio, il log dell'accesso effettuato viene registrato dal sistema di monitoraggio e raccolta log KW" (cfr. verb. 12.5.2011, p. 8);*

iii. *identica (anomala) modalità di funzionamento caratterizza anche le attività di tracciamento degli accessi al sistema VoIP e della relativa interfaccia web (denominata QZ) (cfr. verb. 13.5.2011, p. 6): si è al riguardo precisato, infatti, che i "log interni della piattaforma di gestione delle utenze telefoniche (QZ) non confluiscono nel sistema KW per problemi di natura tecnica del sistema stesso" (cfr. verb. 13.5.2011, p. 6).*

5.2. Dal complesso delle verifiche così effettuate emerge, pertanto, che la società ha dato solo parziale attuazione alle misure prescritte dal Garante ai sensi dell'art. 154, comma 1, lett. c), del Codice con il provvedimento relativo agli amministratori di sistema del 27 novembre 2008 nel quale, alla lett. f), si è stabilito che *"devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste [...]".*

Orbene, atteso che gli accessi di tipo applicativo alla strumentazione utilizzata per l'amministrazione dei sistemi informativi della società non vengono censiti sul sistema KW (come descritto al punto 5.1. lett. c), il richiesto requisito della completezza non risulta soddisfatto, con la conseguenza che i soggetti preposti a sovrintendere alla regolarità nello svolgimento delle attività effettuate dagli amministratori di sistema – sia a livello di unità organizzativa, che a livello apicale – hanno potuto disporre di un'informazione incompleta rispetto all'operato degli amministratori di sistema.

Pertanto potrebbero non rappresentare fedelmente l'operato degli amministratori di sistema sia il report inviato dal responsabile dell'area "ICT e Business solutions" al responsabile privacy (cfr. all. 6 al verb. del 13.5.2011) – nel quale si attesta che *"dall'analisi dei report dei log prodotti con l'ausilio del sistema KW Logger non è emersa nessuna anomalia né intrusione non autorizzata ai sistemi da parte degli amministratori di sistema, ma solo attività lavorativa nell'ambito della loro professione e del proprio profilo organizzativo" –*, sia la conseguente *"comunicazione al consiglio di amministrazione"* dell'amministratore delegato il quale, alla luce delle informazioni disponibili, ha potuto attestare che *"dal primo controllo annuale risulta che tutti gli amministratori di sistema hanno svolto la loro attività nei limiti dei rispettivi profili autorizzativi; pertanto non è stata rilevata nessuna irregolarità"* (cfr. all. 7 al verb. del 13.5.2011).

A tale inconveniente, derivante dalla rilevata incompletezza del tracciamento effettuato, va aggiunto che proprio l'accesso di tipo applicativo, nel caso in esame non tracciato, permette a chi ad esso ricorre un'immediata accessibilità alle informazioni personali presenti nei sistemi senza gli ostacoli di natura strutturale propri invece delle informazioni estratte mediante un accesso di tipo sistemistico (oggetto invece di tracciamento).

5.4. Tanto premesso, il Garante, ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice:

a. prescrive a codesta società di dare integrale attuazione alla prescrizione di cui alla lett. f) del provvedimento di questa Autorità del 27 novembre 2008 richiamato nelle premesse, assicurando in particolare la completezza del tracciamento delle attività effettuate dagli amministratori di sistema;

b. si riserva di valutare con autonomo procedimento la sussistenza della violazione di cui all'art. 162, comma 2-ter del Codice.

6. Gli accertamenti complessivamente effettuati hanno altresì evidenziato, al di là della mancata attuazione delle misure di garanzia previste dall'ordinamento, un difetto di coordinamento tra i diversi centri di responsabilità, di cui pure la società si è dotata (nel caso di specie, le aree "ICT e business solutions", "Risorse umane", "legale" nonché la figura del "responsabile privacy") e, nonostante siano state intraprese da tempo iniziative volte a monitorare l'implementazione del c.d. modello di gestione della privacy presso l'Istituto (cfr. Relazione finale attività di audit 2008, all. 5, verb. 13.5.2011), in ordine a scelte tecnologico-organizzative che riguardano un numero rilevante di dipendenti e che, opportunamente, avrebbero dovuto comportare una previa valutazione di impatto sulla protezione dei dati personali e la riservatezza degli interessati con la conseguente adozione delle garanzie dettate dall'ordinamento.

Ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c), del Codice si prescrive pertanto, quale misura opportuna, che, in caso di introduzione o potenziamento di sistemi informativi che possono avere un impatto sulla protezione dei dati personali e la riservatezza degli interessati, vengano introdotte idonee misure organizzative, quali forme di coordinamento e cooperazione tra le pertinenti unità organizzative presenti all'interno della società, volte ad assicurare un corretto processo decisionale, rispettoso delle garanzie previste dall'ordinamento.

7. Infine, considerati gli esiti degli accertamenti effettuati, il Garante dispone 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.

TUTTO CIÒ PREMESSO IL GARANTE

1. dichiara illeciti i trattamenti effettuati dall'Istituto Poligrafico e Zecca dello Stato s.p.a. in violazione degli artt. 11, comma 1, lett. a), c) e d), 113 e 114 del Codice nonché 4 e 8, 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. con riguardo al trattamento dei dati personali relativi agli accessi a Internet effettuato dai dipendenti (punto 2.3.), 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, nella forma della conservazione e della categorizzazione su base individuale, dei dati personali riferiti alla navigazione internet dei dipendenti, con conservazione di quelli finora trattati in vista di un'eventuale acquisizione degli stessi da parte dell'autorità giudiziaria, nonché per esigenze di tutela dei diritti in sede giudiziaria;

3. con riguardo al trattamento dei dati personali relativi allo svolgimento del servizio di posta elettronica (punto 3.3.), ai sensi degli artt. 143, comma 1, lett. b), e 154, comma 1, lett. c), del Codice, prescrive di fornire idonea informativa agli utenti, ai sensi dell'art. 13 del Codice con riguardo al trattamento effettuato per rendere il servizio;

4. con riguardo al trattamento di dati personali connesso al servizio VoIP (punto 4.3):

a. 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, nella forma della conservazione dei dati personali relativi alle utenze telefoniche chiamate dai singoli dipendenti, fino all'eventuale espletamento delle procedure all'uopo previste dall'art. 4, comma 2, l. n. 300/1970 e previa idonea informativa agli utenti ai sensi dell'art. 13 del Codice, con conservazione di quelli finora trattati in vista di un'eventuale acquisizione degli stessi da parte dell'autorità giudiziaria, nonché per esigenze di tutela dei diritti in sede giudiziaria;

b. ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c), del Codice, prescrive:

i. quale misura necessaria, di provvedere a disattivare la menzionata funzione di "alert" senza ritardo, e comunque entro e non oltre tre mesi dal ricevimento del presente provvedimento, dandone contestuale comunicazione a questa Autorità;

ii. quale misura opportuna, limitatamente ai tempi di conservazione dei dati riferiti ad utenze del servizio di telefonia VoIP altre rispetto ai soli dipendenti della società, di contenere i medesimi entro il limite dei sei mesi, salva l'ulteriore conservazione dei dati ove gli stessi formino oggetto di contestazione e la società sia chiamata a tutelare le proprie pretese;

5. con riguardo al trattamento di dati personali effettuato dagli amministratori di sistema, ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c) del Codice, prescrive, quale misura necessaria, di dare integrale attuazione senza ritardo, e comunque entro e non oltre tre mesi dal ricevimento del presente provvedimento, alla prescrizione di cui alle lett. c) ed f) del provvedimento del 27 novembre 2008, contenente *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*, assicurando in particolare che sia resa nota o conoscibile l'identità degli amministratori di sistema nell'ambito della società (punto 3.3 e 4.2) nonché la completezza del tracciamento delle attività effettuate dagli amministratori di sistema (punto 5.3);

6. ai sensi dell'art. 157 del Codice, prescrive di dare comunicazione a questa Autorità, senza ritardo, e comunque entro e non oltre tre mesi dal ricevimento del presente provvedimento delle misure adottate per conformarsi alle prescrizioni impartite con il presente provvedimento;

7. si riserva di valutare con autonomo procedimento la sussistenza delle violazioni di cui agli artt. 161, 162, comma 2-bis, 162, comma 2-ter e 163 del Codice (punti 2.3 e 5.4);

8. ai sensi degli artt. 143, comma 1, lett. b) e 154, comma 1, lett. c), del Codice, prescrive, quale misura opportuna, che, in caso di introduzione o potenziamento di sistemi informativi che possono avere un impatto sulla protezione dei dati personali e la riservatezza degli interessati, vengano introdotte idonee misure organizzative, quali forme di coordinamento e cooperazione tra le pertinenti unità organizzative presenti all'interno della società, volte ad assicurare un corretto processo decisionale, rispettoso delle garanzie previste dall'ordinamento (punto 6);

9. dispone 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 (punto 7).

Avverso il presente provvedimento, ai sensi dell'art. 152 del Codice, 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, 21 luglio 2011

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti
IL SEGRETARIO GENERALE
De Paoli