Provvedimento del Garante

Navigazione internet dei lavoratori e tutela della privacy

Paolo Johan Natali - Avvocato

Il presente contributo ha per oggetto un intervento provvedimentale del Garante Privacy, in particolare il provvedimento inibitorio e prescrittivo del 5 febbraio 2015 (doc. web. 3813428), relativamente al tema del trattamento dei dati personali dei dipendenti, mediante il controllo occulto da parte del datore di lavoro (1).

É interessante considerare, almeno per linee sintetiche, tale provvedimento poiché la disciplina di tale fattispecie (e quindi, conseguentemente, l'orientamento del Garante) rimane invariata anche a dispetto della nuova normativa del Jobs Act, vale a dire l'art. 23 dello Schema di decreto legislativo n. 176, rubricato «Impianti audiovisivi e altri strumenti di controllo»), contenuto nel Titolo II («Disposizioni in materia di rapporto di lavoro e pari opportunità»), Capo I (Disposizioni in materia di rapporto di lavoro), prevede la integrale sostituzione del vigente art. 4 dello Statuto dei Lavoratori.

In particolare, come noto, la nuova formulazione dell'articolo in questione mira a distinguere tra controlli sugli impianti, che dovrebbero restare vietati salvo autorizzazioni particolari, da quelli sugli strumenti di lavoro, i quali, invece, sono stati liberalizzati e comunque sganciati da un'apposita procedura da seguire.

In sostanza, pc, tablet, telefonini aziendali potranno essere oggetto di controlli a distanza senza dover passare attraverso l'accordo con i sindacati o attraverso l'autorizzazione dell'ex ispettorato del lavoro, purché però il datore di lavoro predisponga un'informativa sulla policy di controllo che l'impresa intenda implementare, tale da consapevolizzare adeguatamente i lavoratori interessati.

Anche tale nuova norma non consente, tuttavia, il monitoraggio da parte del datore di lavoro della navigazione web effettuata dai lavoratori mediante i suddetti strumenti.

La fattispecie concreta

La fattispecie vede protagonista un lavoratore che, dopo aver subito il licenziamento, ha adito l'Autorità Garante per la protezione dei dati personali affermando l'illecito trattamento dei dati personali dei lavoratori da parte dell'ex datore di lavoro, e in particolare il "monitoraggio" abusivo del traffico in rete, tramite il conteggio del tempo trascorso e l'analisi delle pagine web visitate, nonché delle attività svolte sui programmi di scrittura (come i file salvati sul pc), ma anche sul contenuto dei messaggi di posta elettronica ricevuti e inviati dal lavoratore mediante il suo account personale.

Dagli accertamenti effettuati dall'Autorità non venivano comprovate tutte le doglianze del lavoratore, pertanto la pronuncia del Garante viene a investire il solo profilo del monitoraggio del traffico internet del lavoratore.

Dall'analisi del testo del provvedimento dell'Autorità, a seguito dell'istruttoria preliminare condotta dalla stessa, emerge che il datore di lavoro, a seguito di attacchi alla rete da parte di hacker stranieri, aveva installato un sistema di proxy al fine di monitore e tener traccia per 24 ore di tutto il traffico entrante e uscente dalla rete web azien-

(1) Per un primo commento dello stesso, v. quello di C. Vicarelli, *Privacy e protezione dei dati personali*, in *www.cristinavicarelli.it/blog/*, del quale nel presente contributo si ripropongono alcune considerazioni.

dale, con esclusivo riferimento all'attività delle singole macchine.
Il Garante ha ritenuto il controllo del traffico effettuato dal lavoratore sulla rete Internet illecito in base alla seguente argomentazione logica-giuridica.

Iter argomentativo del provvedimento del Garante

Ebbene, andando in concreto, il sistema informatico aziendale è risultato configurato in modo da permettere la memorizzazione sistematica dell'indirizzo di dettaglio delle singole pagine web (c.d. URL) digitate e visitate dagli utenti (dipendenti e collaboratori della società), ed idoneo a consentire un controllo della navigazione web individualmente effettuata da soggetti identificabili.
Si evidenzia che «la specifica e accertata funzionalità del sistema, configurata in modo da consentire la registrazione, con una significativa profondità temporale, dei dati relativi alla navigazione web effettuata dalla singola macchina (IP) e quindi dal lavoratore cui la stessa è stata attribuita in via esclusiva», permetteva all'azienda «agevolmente (…) di estrapolare i dati di dettaglio relativi a URL visitata, IP sorgente e orario di connessione».
Inoltre - elemento senz'altro decisivo nella valutazione del Garante - è emerso che il datore di lavoro poteva risalire, peraltro in ogni momento, all'identità del lavoratore utilizzatore della singola macchina.

Sotto il profilo strettamente normativo

II trattamento dei dati personali dei dipendenti effettuato dalla società è stato ritenuto illecito in base alla violazione delle seguenti norme:
• art. 11, comma 1, lett. a) del Codice Privacy;
• art. 114 del Codice Privacy;
• art. 4, legge 20 maggio 1970, n. 300.
• Linee guida del Garante Privacy, 1° luglio 2007, in materia di posta elettronica e internet.
In particolare, nell'ambito del divieto di cui all'art. 4, rientrano - anche dopo l'adozione della nuova norma del Jobs Act che liberalizza il controllo a distanza dei lavoratori che utilizzano pc, cellulari e tablet aziendali - le strumentazioni hardware e software che, se configurate in modo da trattare (e conservare) dati di dettaglio in ordine alla risorsa internet visitata (URL) ed in presenza di un collegamento univoco tra i dati relativi alla connessione e il lavoratore che le utilizza, consentono di ricostruirne l'attività.
Per l'Autorità, il trattamento dei dati personali dei dipendenti operato dal datore di lavoro si svolgeva in contrasto con l'articolo 4 dello Statuto dei Lavoratori, nella versione non modificata dalla novella di cui sopra (e che la novella ha lasciato invariata sul punto), che vieta l'impiego di apparecchiature idonee al controllo a distanza dell'attività dei lavoratori, fatti salvi alcuni casi di deroga, in presenza di determinati presupposti e adempimenti.

Violazione delle Linee guida del Garante Privacy del 2007

Per l'Autorità la condotta datoriale in ordine al trattamento dei dati personali dei dipendenti ha violato peraltro quanto stabilito dalle 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), per i seguenti elementi:
• mancanza di un'informativa completa circa le effettive caratteristiche del sistema aziendale ai sensi dell'art. 13 del Codice Privacy
• mancanza di una policy volta a disciplinare in modo puntuale l'utilizzo degli strumenti elettronici affidati in dotazione ai lavoratori inclusa la navigazione sulla rete Internet degli stessi.
L'Autorità non ha ritenuto sufficiente, ad evitare l'illegittimità del trattamento, la comunicazione ai dipendenti pur operata dal datore, in quanto la suddetta:
«non recava gli elementi essenziali del trattamento, né informava in merito all'eventualità di controlli anche su base individuale volti a verificare il corretto uso degli strumenti di lavoro e alle modalità degli stessi, limitandosi a specificare che il sistema fosse idoneo a tracciare la navigazione effettuata dalle "singole macchine"».

Il diritto all'identità digitale del lavoratore

Occorre, peraltro notare, anche se non rilevato dal Garante, la navigazione sul web da parte dei lavoratori va tutelata, a dispetto di nuove eventuali ulteriori proposte di riforma della normativa

sul controllo a distanza dei lavoratori, anche perché coinvolge altri fondamentali diritti del lavoratori. Fra questi emerge quello alla libertà personale e quello all'"identità digitale" che si affianca a quella fisica e che non è affatto virtuale ma altrettanto reale, fondando e legittimando così un nuovo concetto di privacy.

La tesi del datore di lavoro

Il datore di lavoro basa la sua difesa sull'argomento del controllo posto in essere a scopo difensivo, che, tuttavia, pone il problema in sé della sua legittimità.

L'apposita istruttoria del Garante Privacy

Tuttavia, secondo quanto accertato dal Garante, le informazioni rese dal medesimo datore si limitavano a consapevolizzare i lavoratori che era possibile tracciare la navigazione delle singole macchine, mentre non veniva adeguatamente esplicitata (e spiegata!) la possibilità di ricostruire l'attività dei singoli dipendenti/collaboratori.
Inoltre, il Garante Privacy evidenzia:
• che le esigenze difensive del datore di lavoro non consentono di sacrificare l'obbligo di informare compiutamente i dipendenti dei trattamenti operati dal medesimo;
• nel caso di specie, in particolare, non era stato adottato un regolamento informatico che definisse con precisione le modalità e i limiti dell'utilizzo della strumentazione informatica, con particolare riferimento alla navigazione sul web.

Alcuni precedenti dell'Autorità riguardo al controllo del datore di lavoro sui lavoratori

Consideriamo ora alcuni precedenti su analoghe fattispecie affrontati dall'Autorità Garante, al fine di verificare come è stato declinato l'orientamento del Garante su altri simili casi concreti.
Per esempio, può farsi riferimento alla decisione dell'Autorità su un ricorso presentato da un dipendente che era stato licenziato senza preavviso dalla propria azienda, che ha condotto all'adozione di un provvedimento il 18 ottobre 2012 [doc. web n. 2149222], secondo il quale una società non può controllare il contenuto del pc di un dipendente senza averlo prima adeguatamente informato di questa possibilità, in modo tale da garantire, per quanto possibile, la sua libertà e dignità.

Decisione e relativa argomentazione del Garante Privacy

Secondo l'Autorità, il datore di lavoro può effettuare dei controlli mirati (direttamente o attraverso la propria struttura) al fine di verificare l'effettivo e corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.). Ciò, evidentemente, potremmo aggiungere, anche per garantire ulteriori fondamentali beni giuridici, come la sicurezza dei lavoratori.
Tuttavia, al contempo, il Garante evidenzia che, nell'esercizio di tale prerogativa, occorre rispettare la libertà e la dignità dei lavoratori, nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali, i principi di correttezza, (secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori), di pertinenza e non eccedenza di cui all'art. 11, comma 1, del Codice. Tali controlli, infatti, come ricorda l'Autorità, possono determinare il trattamento dati personali anche non pertinenti, o di dati di carattere persino sensibile.
Analizzando la documentazione in atti, l'Autorità ha ritenuto che, nel caso concreto, il lavoratore non risultava essere stato previamente informato in riferimento al trattamento di dati personali che avrebbe potuto essere effettuato in attuazione di eventuali controlli sull'utilizzo del pc concessogli in uso per esclusive finalità lavorative, con particolare riferimento alle modalità e alle procedure da seguire per gli stessi.
Il Garante ha evidenziato infatti che nel «regolamento per l'utilizzo delle risorse informatiche e telematiche» messo a disposizione dei dipendenti, e nel «documento recante istruzioni agli incaricati del trattamento», pur sottoscritto per accettazione dall'interessato, la società aveva fatto riferimento alla necessità di effettuare - almeno settimanalmente - il salvataggio dei dati su copie di sicurezza con conseguente verifica del buon fine dell'operazione effettuata.
Però, il datore di lavoro non aveva fornito un'idonea informativa ex art. 13 del Codice in ordine al trattamento di dati personali connesso ad eventuali attività di verifica e controllo effettuate dal-

la società stessa sui p.c. concessi in uso ai dipendenti, come invece espressamente previsto dalle Linee Guida del Garante del 1° marzo 2007 «Lavoro: le linee guida del Garante per posta elettronica e internet» (pubblicate in G.U. n. 58 del 10 marzo 2007, punto 3).
Il Garante Privacy, ben consapevole del suo ruolo e dei limiti delle sue competenze, ha espressamente fatte salve le autonome determinazioni spettanti all'autorità giudiziaria riguardo all'utilizzabilità della documentazione venuta in rilievo nell'ambito del ricorso presso l'Autorità.
Ciò, fermo restando che chiaramente è sempre l'autorità giudiziaria ad essere competente per valutare la legittimità del licenziamento del lavoratore nonché l'eventuale risarcimento del danno spettante a quest'ultimo a causa dell'illecito trattamento dei suoi dati da parte del datore di lavoro.

Cessione aziendale: l'uso della casella di posta elettronica del lavoratore ex dipendente

Fra i precedenti dell'Autorità Garante, val la pena ricordare anche il provvedimento del 22 aprile 2010 (doc. web 1727692), con il quale il Garante della Privacy è intervenuto su una fattispecie molto delicata, in quanto caratterizzata da più profili di disciplina (diritto del lavoro, diritto della privacy, diritto del lavoro e diritto civile): quella dell'uso della casella di posta elettronica del lavoratore ex dipendente in caso di cessione aziendale.
In particolare, il provvedimento prescrittivo in questione ha sollecitato l'azienda, destinataria del medesimo, nel modo seguente:
a) procedere alla disattivazione di tutti gli account di posta elettronica appartenenti al dominio aziendale, attribuiti a soggetti che non fanno parte dell'attuale organizzazione imprenditoriale della società, entro un determinato termine perentorio decorrente dalla notifica del provvedimento;
b) predisporre, durante il suddetto periodo, un sistema informativo di tutti i mittenti di comunicazioni inviate agli account di posta della prossima disattivazione degli stessi, con contestuale invito all'inoltro della corrispondenza ad un indirizzo di posta elettronica alternativo.
Come già affermato dall'Autorità nel provvedimento del 25 giugno 2002 (doc. web 29864), anche l'indirizzo e-mail di una persona fisica è da considerarsi un dato personale. Difatti, gli indirizzi di posta elettronica, pur rappresentando un mezzo utilizzato dall'impresa per raccogliere gli ordini della clientela, contengono il nome e cognome del lavoratore. Tuttavia, precisa il Garante, l'indirizzo e-mail attribuito al singolo lavoratore per lo svolgimento delle sue mansioni non garantisce la confidenzialità dei messaggi inviati e ricevuti tramite lo stesso, qualora l'accesso del datore di lavoro si renda necessario per improrogabili esigenze aziendali.
Ciò emerge chiaramente anche nella deliberazione del 1° marzo 2007 (doc. web n. 1387522), con la quale l'Autorità ha indicato le citate Linee guida per un corretto uso della posta elettronica e di Internet nell'ambito dei rapporti lavorativi.
Secondo il Garante, l'esigenza di tutela si estende anche nei confronti di coloro che inviano i messaggi (di qualunque contenuto, privato o lavorativo) esclusivamente nei confronti di una determinata persona.
Per l'Autorità, l'interesse alla tutela dei dati personali delle persone coinvolte (ex dipendenti e terzi mittenti di e-mail) deve, tuttavia, in una corretta ottica di bilanciamento, essere contemperato con l'interesse aziendale a gestire le informazioni indispensabili all'efficiente attività imprenditoriale.
Inoltre, si evidenzia l'esigenza di dare attuazione, anche nella fattispecie, ai seguenti fondamentali parametri normativi, che è opportuno enucleare precisamente:
• art. 3 del Codice Privacy, che prevede che i sistemi informativi e i programmi informatici siano configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali;
• art. 11, comma 1 lett. e) Codice Privacy, che sancisce che i dati siano conservati «per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati».

Riflessioni conclusive

Abbiamo, pur sinteticamente, visto come il Garante Privacy di volta in volta abbia effettuato un bilanciamento di diritti dei lavoratori e dei diritti dell'impresa-datore di lavoro, assicurandone un ragionevole contemperamento.

Tornando al tema principale oggetto del recente provvedimento del 5 febbraio scorso, come sopra considerato, va detto che la navigazione sul web da parte dei lavoratori va tutelata, a dispetto di nuove eventuali ulteriori proposte di riforma della normativa sul controllo a distanza dei lavoratori, anche perché coinvolge altri fondamentali diritti dei lavoratori, come quello all'"identità digitale", di cui si è già detto sopra.
Privacy, che, in una società interconnessa, non può essere più né mero "right to be alone" né più il solo complesso di diritti e tutele connesse al fondamentale diritto alla protezione dei dati personali, perché gli "interessati" del Codice sono inevitabilmente immersi in un mondo interconnesso.
Non va trascurato che, a tale nuova concezione di privacy, considerata dall'angolo visuale dell'interessato corrisponde, inevitabilmente, una nuova dimensione della stessa, contraddistinta da una diversa posizione giuridica dei titolari del trattamento, che si deve necessariamente arricchire e rafforzare di nuovi obblighi e responsabilità.
In questo senso, occorre far riferimento, anche per i datori di lavoro, ai concetti di:
• "privacy by design", ossia essenzialmente la necessità di considerare e garantire gli aspetti privacy fin dalla fase della progettazione di apparecchiature di telecomunicazione, anche assicurando la disponibilità di meccanismi adeguati per informare ed educare l'utente finale, quale il lavoratore, riguardo a quello che le applicazioni possono fare e a quali dati sono in grado di accedere, nonché offrendo agli utenti le opportune impostazioni per modificare i parametri del trattamento, ma è esigenza riferibile comunque ad ogni attività che comporti operazione di trattamento di dati;
• "privacy by default", in base al quale il titolare del trattamento è chiamato a garantire che, di default, possano essere trattati solo i dati personali realmente necessari al raggiungimento di ciascuna specifica finalità del trattamento indicata agli interessati ed, in particolare, che la quantità dei dati raccolti e la durata della loro conservazione o diffusione non vadano oltre il minimo necessario al perseguimento di tali scopi (in quest'ottica si distinguono alcuni pareri del Gruppo ex art. 29).
Principi, comunque, ormai acquisiti a livello di diritto europeo, se non ancora propri dell'*acquis communautaire*, e infatti contemplati anche dal testo attuale dell'approvando nuovo Regolamento Ue in materia di protezione dei dati personali (in dottrina, v. Panetta 2014).

Garante privacy – Provvedimento 5 febbraio 2015

Trattamento dei dati personali riferiti alla navigazione internet dei dipendenti - 5 febbraio 2015 •doc. web n. 3813428•

Registro dei provvedimenti n. 65 del 5 febbraio 2015
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");
Vista la segnalazione presentata da XY, concernente il trattamento di dati personali a sé riferiti effettuato da Estrogeni s.r.l. con sede legale in Napoli (via Libertà II trav. a sinistra, 3) con riferimento ad asseriti controlli eseguiti sulla propria postazione di lavoro presso la società, in assenza delle condizioni previste dall'art. 4, l. n. 300/1970;
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 degli accertamenti *in loco* effettuati in data 22 maggio 2013 presso la sede legale della società in Roma, via Nomentana 222;
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 dott.ssa Augusta Iannini.

Premesso

1.1. XY ex dipendente (con mansioni di copywriter) di Estrogeni s.r.l. – società che fornisce servizi di comunicazione e promozione commerciale – ha lamentato la violazione della disciplina in materia di protezione dei

dati personali con riguardo all'asserito controllo posto in essere dal datore di lavoro in ordine all'utilizzo dei sistemi di comunicazione elettronica effettuato dalla propria postazione lavorativa. In particolare, a detta del segnalante, la società avrebbe operato ai danni dell'interessato un "monitoraggio" del "traffico in rete"("con il conteggio del tempo trascorso e l'analisi dei siti visitati") nonché delle "attività svolte sui programmi di scrittura (word)" (ad esempio, delle "azioni svolte sul pc" e dei "file salvati sul pc") e sul "contenuto dei messaggi di posta elettronica" ricevuti e inviati dall'account personale (cfr. segnalazione 7 dicembre 2012, pp. 2-4).
1.2. In data 16 aprile 2012 all'interessato veniva recapitata una lettera di licenziamento per giustificato motivo oggettivo dovuto alla necessità di ridurre il personale; successivamente, manifestata dallo stesso l'intenzione di impugnare il licenziamento, la società gli notificava in data 28 maggio 2012 una lettera di contestazione disciplinare per "l'uso improprio e indebito dei mezzi di lavoro […] nonché lo svolgimento di attività […] in concorrenza" con la società (segnatamente l'inserimento del proprio profilo professionale su un sito operante "in palese concorrenza con" la società). In particolare, con la menzionata comunicazione si contestava lo svolgimento "durante l'orario di lavoro" di "una costante e massiccia attività di copywriter e blogger in rete" su siti il cui indirizzo completo veniva espressamente riportato nella nota disciplinare. Più in dettaglio, il datore di lavoro asseriva che, da "una prima e parziale analisi del traffico sulla rete e sul computer di proprietà aziendale affidato alla sua cura", sarebbe emersa "una quantità media giornaliera costante di tempo speso dal suo computer aziendale su domini web che presentano alcuna attinenza con la sua attività lavorativa" e contestava la circostanza che l'interessato avrebbe effettuato "screenshot della [propria] postazione lavorativa riportanti progetti e materiali lavorativi da inserirsi nel nostro flusso produttivo" (cfr. nota del 28 maggio 2012, allegato a)-bis alla segnalazione). A tale comunicazione faceva seguito, in data 13 giugno 2013, provvedimento di licenziamento per giusta causa nei confronti dell'interessato (cfr. all. d) alla segnalazione).
1.3. Il segnalante lamenta che le operazioni di controllo sopra descritte sarebbero avvenute in assenza delle garanzie previste dall'art. 4 l. n. 300/70 (cfr. altresì, le precisazioni del rappresentante CGIL-SLC Roma Est contenute nel "processo verbale" redatto ai sensi dell'art. 7, comma 2, l. n. 300/1970, all. c) alla segnalazione). La società si sarebbe limitata a comunicare ai propri dipendenti l'installazione, a seguito di attacchi alla rete da parte di hacker stranieri, di un sistema di proxy che avrebbe "monitor[ato] e te[nuto] traccia per 24 ore di tutto il traffico entrante e uscente dalla rete" aziendale con esclusivo riferimento all'"attività delle singole macchine" (cfr., all. e) alla segnalazione).
2. Al fine di verificare la fondatezza dei comportamenti ascritti alla società e l'osservanza dei principi e delle disposizioni in materia di protezione dei dati personali con specifico riguardo all'utilizzo dei sistemi di comunicazione elettronica, il 22 maggio 2013 sono stati effettuati dal Nucleo speciale privacy della Guardia di Finanza – su delega conferita da questa Autorità – accertamenti presso la sede operativa della società, titolare del trattamento (ai sensi ai sensi degli artt. 4, comma 1, lett. f) e 28 del Codice), nell'ambito dei quali sono state acquisite informazioni dal legale rappresentante e dall'amministratore di sistema, nonché l'ulteriore documentazione attinente al caso.
3.1 Quanto all'asserito controllo delle caselle di posta elettronica, di servizio e personale, lamentato dal segnalante, le dichiarazioni acquisite nel corso dell'istruttoria hanno consentito di escludere la fondatezza delle affermazioni in questione; secondo l'amministratore di sistema, infatti:
- "ogni utente (che "utilizza il servizio gratuito gmail associato al nome del nostro dominio estrogeni.net") è dotato di una propria casella di posta elettronica cui accede tramite web o client" (cfr., pp. 4 e 5 verbale in atti);
- la società non ha effettuato controlli in ordine all'utilizzo della posta elettronica dei propri dipendenti, atteso che "le credenziali di autenticazione della macchina e della posta elettronica sono ad esclusiva conoscenza dell'incaricato" (cfr., p. 5 verbale cit.);
- non è mai stato effettuato alcun controllo su account di posta elettronica di tipo personale, "non essendo quell'account di posta presente sulla rete aziendale" (cfr., p. 6 verbale cit.).
Non sono emersi, poi, elementi tali da poter confutare le dichiarazioni predette, in relazione alla veridicità delle quali i dichiaranti hanno assunto piena responsabilità penale ai sensi dell'art. 168 del Codice.
3.2. Quanto, invece, al monitoraggio del traffico in rete, si ritiene che lo stesso presenti alcuni profili di violazione di legge, discostandosi, altresì, dalle indicazioni fornite dal Garante nelle Linee guida per posta elettronica e internet, cit., adottate con provvedimento confermato da Trib. Roma, sez. I., 10 dicembre 2012, n. 12826.
In primo luogo, il trattamento in esame è stato posto in essere in assenza di un'informativa completa circa le effettive caratteristiche del sistema ai sensi dell'art. 13 del Codice, nonché di una policy volta a disciplinare in modo puntuale l'utilizzo degli strumenti elettronici affidati in dotazione ai lavoratori ed in particolare con riguardo alla navigazione web degli stessi. Non può infatti ritenersi a tal fine esaustiva la comunicazione ai dipendenti del 24 maggio 2011 (cfr. all. e) alla segnalazione, cit.), che non recava gli elementi essenziali del trattamento, né informava in merito all'eventualità di controlli anche su base individuale volti a verificare il corretto uso degli strumenti di lavoro e alle modalità degli stessi, limitandosi a specificare che il sistema fosse idoneo a tracciare la navigazione effettuata dalle "singole macchine".
3.3. In base a quanto verificato, altresì, in ordine alle specifiche caratteristiche del sistema, deve ritenersi che questo, configurato con funzionalità tali da permettere la memorizzazione sistematica dell'indirizzo di dettaglio

delle singole pagine web (c.d. URL) richieste e visitate dagli utenti (dipendenti e collaboratori della società), sia idoneo a consentire un controllo della navigazione web individualmente effettuata da soggetti identificabili. Come avvenuto nel caso di specie, infatti, il datore di lavoro ha la possibilità di risalire in ogni momento all'identità dell'utilizzatore della singola macchina. La specifica ed accertata funzionalità del sistema, configurata in modo da consentire la registrazione, con una significativa profondità temporale, dei dati relativi alla navigazione web effettuata dalla singola macchina (IP) e quindi dal lavoratore cui la stessa è stata attribuita in via esclusiva, consente agevolmente, infatti – come avvenuto nel caso di specie generando report su base individuale per il tramite dell'amministratore di sistema (cfr. nota della società del 5 giugno 2013) –, di estrapolare i dati di dettaglio relativi a "URL visitata, IP sorgente e orario di connessione" (cfr. altresì, pp. 3, 4 e 5 verbale cit.; all. 5 verbale cit., recante "report e screenshot proxy").
Per tali ragioni il descritto trattamento risulta, anche sotto questo diverso profilo, in contrasto con il principio di liceità per violazione della rilevante disciplina di settore che vieta l'impiego di apparecchiature idonee al controllo a distanza dell'attività dei lavoratori (artt. 11, comma 1, lett. a) e 114 del Codice e art. 4, l. 20 maggio 1970, n. 300). Tra queste sono ricomprese anche le strumentazioni hardware e software che, se configurate in modo da trattare dati di dettaglio in ordine alla risorsa internet visitata (URL) ed in presenza di un collegamento univoco tra i dati relativi alla connessione e la persona utilizzatrice, consentono di ricostruirne l'attività (cfr., par. 4 Linee guida cit.; nonché, Provv. 21 luglio 2011 doc. web n. 1829641, confermata da Trib. Roma, sez. I, 21 marzo 2013 n. 4766; cfr. anche Provv.ti 2 aprile 2009, doc. web n. 1606053 e 1° aprile 2010 doc. web n. 1717799).

Tutto ciò premesso il Garante
1. dichiara illecito il trattamento effettuato da Estrogeni s.r.l. in violazione degli artt. 11, comma 1, lett. a), 13, 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 su base individuale dei dati personali riferiti alla navigazione internet dei dipendenti, con conservazione di quelli finora trattati ai fini della eventuale acquisizione da parte dell'autorità giudiziaria;
3. dispone che sia data comunicazione al Garante, entro 90 giorni dalla data di comunicazione del presente provvedimento, dell'avvenuta attuazione dello stesso.
Ai sensi degli artt. 152 del Codice e 10 d.lgs. n. 150 del 2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria, 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.