COMPLIANCE IT E PUBBLICA AMMINISTRAZIONE[1]

di Marco Bufacchi, dottore in Giurisprudenza

SOMMARIO: 1.1 La Direttiva sull'uso di *internet* e della posta elettronica sul luogo di lavoro. – 1.2 I rapporti con la protezione dei dati personali e i diversi profili di responsabilità del dipendente pubblico.

1.1 La Direttiva sull'uso di *internet* e della posta elettronica sul luogo di lavoro

Il Ministro per la Pubblica Amministrazione e l'Innovazione ha emanato, in data 26 maggio 2009, una Direttiva[2] (c.d. "Brunetta") recante "*Utilizzo di internet e della casella di posta istituzionale sul luogo di lavoro*". Tale interesse per l'impiego in ambito pubblico delle nuove tecnologie, non rappresenta certamente una novità. Infatti, da alcuni anni il Ministero della Funzione Pubblica e il soppresso Ministero per l'Innovazione e le Tecnologie[3], hanno assunto un atteggiamento ambivalente nei confronti dell'uso della posta elettronica nelle pubbliche amministrazioni[4].

Da un lato si auspicava un utilizzo sempre più diffuso delle nuove tecnologie nel settore della pubblica amministrazione, e, in particolare, dell'uso della posta elettronica, con l'obiettivo anche di attivare per ogni dipendente una apposita casella istituzionale. Tale obiettivo, già oggetto di interesse negli anni passati in provvedimenti quali le "*Linee guida per lo sviluppo della società dell'informazione nella legislatura*"[5] e richiamato dall'art. 27[6], comma 8, lettera e), della legge n. 3/2003[7], è stato poi ribadito nella Direttiva del Ministro per l'Innovazione e le Tecnologie del 27 novembre 2003 recante "*Direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni*"[8] nonché nella Direttiva

[1] Estratto dell'elaborato finale discusso nel febbraio 2010 nell'ambito del Master di II livello in "*Diritto dell'Informatica e Teoria e Tecnica della Normazione"* – Facoltà di Giurisprudenza dell'Università "La Sapienza" di Roma.

[2] Direttiva n. 2/2009 in data 26 maggio 2009, registrata alla Corte dei conti in data 10 giugno 2009, registro n. 6, foglio n. 293, su: http://www.innovazione.gov.it .

[3] Con D.P.C.M. 28 aprile 2009 recante "*Modifiche agli articoli 2, 21 e 22 del decreto del Presidente del Consiglio dei Ministri 23 luglio 2002, recante «Ordinamento delle strutture generali della Presidenza del Consiglio dei Ministri»*" (pubblicato nella *Gazzetta Ufficiale n. 128 del 5 giugno 2009*) il Dipartimento innovazione e tecnologie ha assunto la denominazione di "Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica" e rappresenta la struttura di cui si avvale il Ministro per la Pubblica Amministrazione e l'Innovazione ai fini del coordinamento e dell'attuazione delle politiche di promozione dello sviluppo della società dell'informazione, nonché delle connesse innovazioni per le amministrazioni pubbliche, i cittadini e le imprese.

[4] **C. e F. SARZANA DI SANT'IPPOLITO**, *Il dipendente e la posta elettronica*, 05/2009, su: http://punto-informatico.it/2633789/PI/Commenti/dipendente-posta-elettronica.aspx .

[5] Su: www.cnipa.gov.it/site/_files/Linee%20guida%20Governo%20sviluppo%20Informazione%20legislatura.pdf .

[6] L'art. 27 rubricato "*Disposizioni in materia di innovazione tecnologica nella pubblica amministrazione*", è inserito nel Capo VI "*Disposizioni in materia di innovazione*".

[7] Legge 16 gennaio 2003, n. 3 recante "*Disposizioni ordinamentali in materia di pubblica amministrazione*" (pubblicata nella *Gazzetta Ufficiale n. 15 del 20 Gennaio 2003 - Supplemento Ordinario n. 5*).

[8] Pubblicata nella *Gazzetta Ufficiale n. 8 del 12 gennaio 2004.*

del Ministro per l'Innovazione e le Tecnologie del 18 novembre 2005 recante "*Linee guida per la Pubblica amministrazione digitale*"[9], per poi essere richiamato anche nella Direttiva n. 2/2009 in argomento.

Dall'altro, però, si tende a penalizzare il dipendente che ecceda nell'uso di questo strumento. Secondo l'indicazione della Direttiva "Brunetta", infatti, fermo restando i richiami in ordine alle tutele del lavoratore e della protezione dei dati personali, il dipendente che utilizzi *internet* per scopi personali si porrebbe[10] in contrasto con il dovere di lealtà verso il potere datoriale. Si fa riferimento, infatti, sia al Codice di comportamento del pubblico dipendente sia agli illeciti di natura disciplinare nonché penale.

Inoltre, non si farebbe esplicito riferimento in alcun passo della Direttiva al caso dei *social network*[11], ma il richiamo sembrerebbe abbastanza evidente e ciò risulta confermato anche dagli articoli selezionati nella rassegna stampa[12] del Ministero. In particolare, vengono evidenziati taluni aspetti relativi al *social network* denominato "*Facebook*"[13]. Al riguardo, risulta opportuno considerare il possibile rischio derivante dalla possibilità di uso improprio di un *account* utente attivo in un *social network*, con conseguenti profili di danno anche in capo all'amministrazione interessata; infatti, l'estrema facilità con cui è possibile generare un indirizzo di posta elettronica[14] inserendo dati fittizi, potrebbe ad esempio consentire l'integrazione di una vera e propria "sostituzione di persona". Su tale

[9] Pubblicata nella *Gazzetta Ufficiale n. 16 del 20 gennaio 2006*.

[10] Salvo attività contenute nei tempi strettamente necessari allo svolgimento di circoscritti adempimenti di natura burocratica (punto 3, ultimo capoverso della Direttiva).

[11] Si tratta di un fenomeno estremamente diffuso, basato su piattaforme di aggregazione sulle quali le persone possono entrare in contatto, condividere contenuti, stabilire nuovi legami o riprodurre quelli della vita reale. Nei *social network* è esaltata una delle caratteristiche chiave del *web* 2.0 (l'insieme delle applicazioni *online* che permettono un significativo livello di interazione sito-utente), cioè la partecipazione, l'interesse attivo dei membri di un gruppo che interagiscono con altri individui per intrattenimento, lavoro, condivisione di contenuti multimediali o semplicemente per instaurare nuove relazioni.

[12] Rassegna stampa su http://www.innovazione.gov.it: 03/01/2010 - Il Gazzettino Ed. Padova *Niente Facebook mentre si lavora*; 10/11/2009 - Il Giorno Ed. Legnano *Cari dipendenti, così si utilizza internet*; 30/10/2009 - Il Secolo XIX Ed. Imperia Sanremo *Oscurato Facebook sui pc del Comune*; 09/10/2009 - Corriere dell'Alto Adige *Siti "vietati". I sindacati sono d'accordo*; 08/10/2009 - Media Duemila *Social working. Distrazione o beneficio sul lavoro?*; 05/10/2009 - Il Sole 24 Ore *In ufficio la tentazione di Facebook*; 22/09/2009 - Il Messaggero Ed. Abruzzo *E la Regione vieta Facebook ai dipendenti*; 18/09/2009 - L'Unione Sarda Ed. Sassari *Decreto Brunetta: Facebook censurata per i dipendenti*; 16/09/2009 - La Sicilia Ed. Agrigento *Niente Internet per i dipendenti*; 06/09/2009 - Il Mattino Ed. Padova *Il Comune ha "spento" Facebook*.

[13] In generale il problema di *Facebook*, come delle altre *social network*, risiederebbe nel favorire la comunicazione e la diffusione di una elevata quantità di dati personali quali fotografie, interessi, abitudini e amicizie, con l'alto rischio che queste informazioni circolino senza l'effettiva consapevolezza dell'utente.

[14] Durante la fase di generazione dell'indirizzo di posta elettronica, viene memorizzato l'indirizzo IP assegnato nella circostanza all'utente. Durante tale generazione, ancorché l'I.S.P. (*Internet Service Provider*) nelle condizioni generali del contratto rese disponibili *online* richieda generalmente al cliente di garantire la veridicità dei dati personali forniti al momento dell'attivazione del servizio (ad esempio "*Il Cliente si impegna a non utilizzare il servizio per effettuare comunicazioni che arrechino danni o turbative alla rete o a terzi utenti o che violino le leggi ed i regolamenti vigenti*"), è possibile inserire generalità non reali (impersonificando ad esempio altri soggetti) e nel contempo rendere anonima la navigazione (indirizzo IP non riconducibile) adottando una serie di opportuni accorgimenti tecnici.

questione giuridica relativa al furto d'identità *online*, si è pronunciata la Suprema Corte[15], in un caso di un soggetto che aveva creato un *account* di posta elettronica apparentemente intestato ad altro soggetto, sancendo come tale "furto di identità"[16] debba essere inquadrato nella fattispecie delittuosa prevista dall'articolo 494 c.p. . In sostanza, "*nonostante vi sia la possibilità di attivare un account di posta elettronica recante un nominativo diverso dal proprio, anche di fantasia, perfeziona il reato ex art. 494 c.p. chiunque, utilizzando un account di posta elettronica apparentemente intestato ad un'altra persona, induce in errore gli utenti della Rete, i quali, ritenendo di interloquire con una determinata persona, in realtà inconsapevolmente si sono trovati ad avere a che fare con una persona diversa*". Una conferma alle criticità rappresentate, perviene dal Servizio Polizia Postale e delle Comunicazioni del Ministero dell'Interno, che illustra[17] come si ricevano segnalazioni quotidiane per i *social network*: "*Ci si sostituisce ad una persona usando le sue generalità e cercando di ottenerne un profitto. Posso mettermi in contatto con i suoi conoscenti, tentando una truffa*". "*Non solo, con una falsa identità posso anche provocare un grave danno d'immagine, pubblicando informazioni false e diffamatorie; o mettere in atto comportamenti molesti, turbando l'emotività e la vita sociale delle persone con cui entro in contatto*".

Ciò posto, l'adozione delle misure[18] *compliant* IT da parte delle amministrazioni pubbliche, ribadite dalla Direttiva n. 2/2009, dovrebbe innanzi tutto partire da criteri di gradualità e trasparenza. La presenza nel Master di partecipanti appartenenti a diverse realtà della Pubblica Amministrazione Centrale (PAC)[19], ha fornito l'occasione per effettuare un risconto dei contesti in cui sono inseriti tali dipendenti. Al riguardo, è stato di interesse osservare come l'attività volta a rendere trasparente le modalità di utilizzo e di controllo delle risorse informatiche – con conseguente riduzione dei rischi derivanti da un uso inconsapevole degli strumenti informatici impiegati – messe a disposizione degli utenti, sia stata posta in essere, in parte, unicamente in ambito ACI; nelle altre

[15] Cassazione penale, Sez. V, sentenza n. 46674 del 14 dicembre 2007.

[16] Sulla rete *internet* possono integrarsi generalmente tre diverse tipologie di furto di identità:
a) *Financial Identity Theft*: per ottenere credito con le credenziali di un'altra persona;
b) *Criminal Identity Theft*: quando il furto di identità viene adottato per porre in essere una frode. Un altro caso è la vendetta/ricatto verso colui che si vuole danneggiare;
c) *Identity Cloning*: consiste in una vera e propria sostituzione di persona con l'obiettivo di creare una nuova identità.

[17] Nell'articolo dal titolo "*FACEBOOK*: MA QUAL È IL PREZZO DA PAGARE?", pubblicato su http://www.ilsalvagente.it/Sezione.jsp?idSezione=1806 in data 07/01/2009.

[18] Non ultime quelle afferenti la sicurezza informatica.

[19] Quali: Ministero dell'Istruzione, dell'Università e della Ricerca; Ministero dell'Economia e delle Finanze – Agenzia Monopoli di Stato; Ministero della Giustizia – Dipartimento Amministrazione Penitenziaria; Automobile Club d'Italia (ACI).

amministrazioni gli interessati hanno rappresentato di non aver preso visione di disciplinari tecnici o avvisi informativi volti a regolamentare la fruizione delle risorse informatiche nonché responsabilizzare i dipendenti nei casi di eventuale utilizzo non conforme alle norme che disciplinano il lavoro alle dipendenze delle pubbliche amministrazioni.

1.2 I rapporti con la protezione dei dati personali e i diversi profili di responsabilità del dipendente pubblico

Dal punto di vista della *privacy*, la Direttiva n. 2/2009 richiama le linee guida 1° marzo 2007 del Garante in materia di uso di *internet* e della posta elettronica[20]da parte dei lavoratori pubblici e privati. Tale provvedimento fornisce una serie di indicazioni generali secondo le quali compete innanzitutto ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di *internet* e della posta elettronica nonché sulla possibilità che vengano effettuati controlli. Ma quali sono in particolare le norme che regolano l'uso della posta elettronica e la navigazione *internet* da parte dei dipendenti pubblici[21] ?

Per la sfera pubblica, invero, era presente una disposizione normativa relativa all'uso privato delle linee telefoniche d'ufficio, contenuta nel decreto del Ministro della Funzione Pubblica del 31/03/1994[22], con il quale fu adottato il Codice di comportamento dei dipendenti della pubblica amministrazione ai sensi dell'art. 58 *bis* del D.lgs. 3 febbraio 1993, n. 29[23]. Si trattava dell'art. 10 che, al primo capoverso del comma 5, prevedeva che "*salvo casi eccezionali dei quali informa il dirigente dell'ufficio, il dipendente non utilizza le linee telefoniche dell'ufficio per effettuare chiamate personali*".

La necessità di ampliare questa limitata facoltà di deroga collegata al requisito dell'eccezionalità ha indotto successivamente il Ministro della Funzione Pubblica a rivedere l'impostazione iniziale dell'art. 10 e, infatti, il nuovo Codice di comportamento dei dipendenti delle pubbliche amministrazioni di cui al D.M. del 28/11/2000 ha previsto al comma 3, art. 10, che il dipendente "*salvo casi d'urgenza, non utilizza le linee telefoniche dell'ufficio per esigenze personali*". Tale disposizione di carattere puramente amministrativo, a parte il riferimento alle sole apparecchiature telefoniche, non appare comunque tale da escludere, totalmente, la responsabilità civile e penale nel caso di uso illecito delle linee telefoniche da parte del dipendente pubblico.

Per quanto riguarda l'orientamento dottrinale e giurisprudenziale in materia, va rilevato che la dottrina penalistica[24] è divisa in ordine alla definizione della natura giuridica della posta elettronica

[20] Linee guida pubblicate in *Gazzetta Ufficiale n. 58 del 10 marzo 2007*.
[21] **C. e F. SARZANA DI SANT'IPPOLITO**, *cit.* .
[22] Recante "*Codice di comportamento dei dipendenti delle pubbliche amministrazioni*" (pubblicato nella *Gazzetta Ufficiale n. 149 del 28 giugno 1994*). Il presente decreto è stato abrogato dall'art. 14, D.M. 28 novembre 2000.
[23] "*Razionalizzazione dell'organizzazione delle amministrazioni pubbliche e revisione della disciplina in materia di pubblico impiego, a norma dell'articolo 2 della L. 23 ottobre 1992, n. 421*". (pubblicato nella *Gazzetta Ufficiale n. 30 del 6 febbraio 1993, Supplemento Ordinario*). Il presente decreto è stato abrogato dall'art. 72, D.lgs. 30 marzo 2001, n. 165.
[24] Con riferimento al problema della qualificazione della posta elettronica d'ufficio in termini di corrispondenza "chiusa" o meno ai fini dell'applicazione dell'art. 616 c.p.: **F. TOFFOLETTO**, *Nuove tecnologie informatiche e tutela del lavoratore*, Giuffré, 2006; **A. MAGGI**, *Il controllo della posta elettronica aziendal*e, in Guida al lav., 2005, n. 36, p. 22; **L. NOGLER**, *Posta elettronica aziendale: conta anche la privacy del lavoratore?*, in Guida al lav, 2002, n. 22, p. 10; **F. ROTONDI, F. COLLIA**, *Il controllo a distanza dei dipendenti*, in Dir. e prat. lav., n. 36, 2001, p. 2423. In ordine alla più generale questione dell'operatività dell'esimente di cui all'art. 51 c.p. con riferimento ai rapporti di

e alla possibilità dei dirigenti dell'ufficio di controllare l'uso che i dipendenti fanno, in genere, degli strumenti tecnologici posti a loro disposizione. Parte della dottrina[25] ritiene che, almeno sino a quando il dipendente non acceda alla sua casella ed apra il messaggio di posta elettronica, il messaggio stesso debba considerarsi come "corrispondenza chiusa" e come tale tutelata ai sensi dell'art. 616 c.p. . Tale orientamento è stato sostenuto in giurisprudenza implicitamente da una decisione del T.A.R. Lazio[26], in relazione ad una *mailing-list* in ambiente pubblico secondo cui "*la corrispondenza trasmessa per via informatica o telematica, c.d. posta elettronica, deve essere tutelata alla stregua della corrispondenza epistolare o telefonica ed è quindi caratterizzata dalla segretezza*". La tesi in questione è stata, in passato, sostenuta anche dal Garante per la protezione dei dati personali nel comunicato 12 luglio 1999[27], secondo cui, appunto, la posta elettronica sarebbe protetta ai sensi dell'art. 616, comma 4, c.p. . Tale affermazione, nel tempo, ha incontrato un forte ridimensionamento avendo, il datore di lavoro, secondo le "Linee guida per posta elettronica e *internet*"[28], il legittimo accesso alle informazioni di lavoro diffuse attraverso le *e-mail* dei propri dipendenti[29]. In caso contrario, dovrà essere garantita la riservatezza[30] delle comunicazioni degli stessi dipendenti. In tale contesto la posta elettronica d'ufficio può essere equiparabile ad uno strumento lavorativo, e come tale ricadere nella pertinenza del datore di lavoro cui è consentito, a determinate condizioni, senza rilievi dal punto di vista penale, né di violazione della disciplina sulla protezione dei dati personali, il legittimo accesso.

Secondo la Suprema Corte (Cass. pen., Sez. V, 19/12/2007, n. 47096), qualora non si configuri sottrazione o distrazione, la condotta di colui che prende semplicemente cognizione della corrispondenza informatica è punibile solo se riguarda "corrispondenza chiusa" ovvero quella che attiene a soggetti che non siano legittimati all'accesso dei sistemi informatici di invio o di ricezione del singolo messaggio. Chi prende cognizione di "corrispondenza aperta" è punito solo se l'abbia a tale scopo sottratta al destinatario ovvero distratta dalla sua destinazione[31]. E come porsi, inoltre,

---

subordinazione: **V. MANZINI**, *Trattato di diritto penale italiano*, Utet, 1948; **F. ANTOLISEI**, *Manuale di diritto penale*. Parte speciale, 1, Giuffré, 2008. Con riferimento al problema dell'accesso del datore di lavoro alla casella di posta elettronica messa a disposizione del lavoratore: **E. BARRACO, A. SITZIA**, *La tutela della privacy nei rapporti di lavoro*, Ipsoa, 2008.

[25] **F. MANTOVANI**, *Diritto penale,* Parte spec., Delitti contro la persona, Padova, Cedam, 2008.

[26] Sezione I *ter*, sentenza n. 9425 del 15/11/2001.

[27] Su http://www.garanteprivacy.it/garante/doc.jsp?ID=47997 (Bollettino n. 9/1999, pag. 96).

[28] Su http://www.garanteprivacy.it/garante/doc.jsp?ID=1387978 .

[29] **F. SANTINI**, *La corrispondenza elettronica tra diritto alla riservatezza e potere di controllo del datore di lavoro,* in Argomenti Dir. Lav., n. 3, 2007, p. 747.

[30] Ciò, nelle intenzioni dell'Autorità garante, dovrebbe restare vero solo se, l'utilizzo della casella di posta d'ufficio non venga limitato ad usi esclusivamente professionali, lasciando al prestatore la legittima aspettativa di confidenzialità delle comunicazioni.

[31] Infatti, prosegue la Suprema Corte, diversamente da quanto avviene per la corrispondenza cartacea, di regola accessibile solo al destinatario, è appunto la legittimazione all'uso del sistema informatico o telematico che abilita alla conoscenza delle informazioni in esso custodite. Sicché tale legittimazione può dipendere non solo dalla proprietà, ma soprattutto dalle norme che regolano l'uso degli impianti. E quando in particolare il sistema telematico sia protetto da

nei casi di utilizzo della crittografia[32] da parte del dipendente che abbia involontariamente o meno perso la *passphrase*[33], in modo tale da impedire, di fatto, l'accesso del datore di lavoro? Su tale problematica si rileva come, oggi, nella maggior parte dei paesi non esistono particolari controlli sull'uso della crittografia[34]: le tecniche crittografiche possono essere impiegate senza restrizioni ed i sistemi di crittografia sono prodotti, esportati ed importati liberamente[35]. Da un lato sussiste una generale tendenza a ridurre i controlli e le limitazioni relative alla crittografia ed a contrastare le c.d. politiche di "*key escrow*"[36] e "*key recovery*"[37], mentre dall'altro persiste un certo numero di paesi in cui il controllo delle attività crittografiche è particolarmente elevato (in maggioranza nei paesi in cui vigono regimi autoritari).

Per quanto riguarda la giurisdizione contabile, la Corte dei conti, attraverso le competenti sezioni giurisdizionali regionali, si è occupata del problema dell'utilizzo improprio delle risorse informatiche sotto il profilo del danno erariale.

Infatti, la Corte dei conti, Sezione Giurisdizionale per la Regione Sicilia, con la sentenza n. 390/05[38] ha condannato al risarcimento dei danni un dipendente di un'Agenzia fiscale che, avendo lasciata incustodita la postazione informatica assegnata, aveva consentito che altro soggetto effettuasse sgravi di imposta non dovuti a favore di terzi. Nel qualificare colpa grave il comportamento del dipendente, la Corte ha precisato che "*la negligenza del convenuto è consistita nella violazione delle disposizioni di servizio impartite dalla direzione centrale Audit e sicurezza dell'agenzia delle entrate agli operatori incaricati del trattamento di dati sensibili mediante procedura informatica, acquisite agli atti del giudizio, che impongono lo spegnimento del personal computer al termine della giornata di lavoro, eseguendo l'apposita procedura di spegnimento e,*

---

una *password*, deve ritenersi che la corrispondenza in esso custodita sia lecitamente conoscibile da parte di tutti coloro che legittimamente dispongano della chiave informatica di accesso. Anche quando la legittimazione all'accesso sia condizionata, l'eventuale violazione di tali condizioni può rilevare sotto altri profili, ma non può valere a qualificare la corrispondenza come "chiusa" anche nei confronti di chi sin dall'origine abbia un ordinario titolo di accesso.

[32] Secondo A. MONTI, "*in realtà, la crittografia sembra essere l'unico mezzo in grado di garantire il rispetto di alcuni diritti assoluti sanciti dalla Costituzione*", su http://www.ictlex.net .

[33] In ambito informatico e crittografico con il termine *passphrase* si intende indicare un insieme di parole o di stringhe alfanumeriche (usualmente separate da caratteri non alfabetici quali numeri, caratteri speciali o il carattere "spazio") utilizzato per l'autenticazione ad un sistema, ad un programma, ad una base dati o ad una rete come anche per effettuare operazioni di cifratura (http://it.wikipedia.org/wiki/Passphrase).

[34] Al riguardo si osserva come siano presenti disciplinari sull'uso di *internet* e della posta elettronica, che prevedono specifici divieti di applicare sistemi di crittografia, codificazione e simili ai dati trattati, se non espressamente autorizzato dai soggetti competenti (ad esempio su: http://portale.asl3.umbria.it/MEDIACENTER/FE/CategoriaMedia.aspx?idc=332).

[35] Per una panoramica sulla possibilità di impiego e importazione di prodotti crittografici a livello internazionale si veda il portale recante "*Summary of International crypto controls*", raggiungibile all'indirizzo *web* http://rechten.uvt.nl/koops/cryptolaw .

[36] "Deposito della chiave": è un concetto giuridico che implica la consegna volontaria della chiave (ovvero parte di essa) ad una terza parte fidata, in modo da consentire l'accesso al testo in chiaro partendo da dati cifrati al ricorrere di condizioni prestabilite.

[37] "Recupero della chiave": sistema realizzato per consentire la generazione della chiave al fine di accedere al testo in chiaro partendo da dati cifrati a prescindere dalla volontà dell'originatore del dato.

[38] Su http://bddweb.corteconti.it/bdddaccessibile/ricerca.aspx .

nell'ipotesi di momentaneo allontanamento, l'attivazione della funzione di blocco della postazione oppure, ove non sia possibile il blocco, lo spegnimento dell'apparecchiatura".

Ancora la Corte dei conti, Seconda Sezione Giurisdizionale Centrale d'Appello, con la recente sentenza n. 250/2009 in data 10 marzo 2009, nel confermare la condanna già pronunziata in primo grado, ha disposto un ulteriore pagamento a titolo di risarcimento del danno non patrimoniale. Tale decisione, fa seguito alla sentenza della Sezione Giurisdizionale Piemonte n. 1856/03 in data 13 novembre 2003, in cui un dirigente pubblico era stato condannato a risarcire i danni patrimoniali e di immagine subiti dall'amministrazione di appartenenza per aver effettuato oltre 250 ore di navigazione su siti *web* non afferenti l'attività istituzionale. Nella fattispecie il soggetto era stato, per detta condotta, rinviato a giudizio dinanzi al Tribunale Penale di Verbania per i delitti di cui agli artt. 314, 323 e 640, 2° comma, c.p. .

Tale decisione appare di particolare interesse poiché analizza la legittimità, sia pure incidentalmente, dell'uso da parte della pubblica amministrazione di strumenti di analisi del traffico di rete per finalità di sicurezza. Nella circostanza il giudice contabile "*non ravvisa nell'operato del Comune di Arona alcun comportamento invasivo preordinato al controllo recondito dell'attività del proprio dipendente, ma semplicemente l'impiego, con verifiche svolte ex post, di un tipo di software in uso a molte Pubbliche Amministrazioni in grado di registrare i dati inerenti agli accessi degli utenti collegati alla rete, non solo per finalità di repressione di comportamenti illeciti, ma anche per esigenze statistiche e di controllo della spesa*".

Affermando il principio ribadito nella citata sentenza della Sezione Giurisdizionale per la Regione Sicilia, anche nel presente caso si afferma la responsabilità per danni del dipendente che non rispetta le misure di sicurezza informatica, con particolare riguardo alla fase di autenticazione. Rileva, infatti, il giudice: "*Sulla specifica questione, il Collegio, non condivide le conclusioni prospettate dalla difesa, relativamente all'asserita possibilità per la quale chiunque avrebbe potuto navigare in internet con il p.c. in dotazione all'odierno convenuto e la "password" avrebbe potuto essere conosciuta da altri soggetti, quali gli addetti al C.E.D., sul rilievo che, se ciò non si può certamente escludere in via di fatto, residua, tuttavia, un comportamento negligente, inescusabile e gravemente colposo del Dr. .., il quale, per sua espressa ammissione, si allontanava dal proprio ufficio per diverse ore al giorno lasciando il locale aperto ed il p.c. acceso, incustodito e con la parola chiave inserita. Il contegno serbato con sistematicità dal citato Dirigente, connotato dal mancato esercizio di quelle minime, possibili e semplici cautele procedimentali che la situazione richiedeva, da considerarsi oltremodo censurabile, poiché posto in essere da una figura lavorativa che ricopriva un ruolo di vertice nell'organigramma dell'Ente locale, depone a favore di una diretta imputabilità del danno, sotto il profilo eziologico, all'odierno convenuto*".

Sempre la Corte dei conti, Sezione Giurisdizionale per la Regione Basilicata, con la sentenza n. 83/06 in data 17 gennaio 2006, ha pronunziato una condanna al risarcimento dei danni subiti da un ente pubblico a seguito della diffusione di *virus* informatico[39] contratto dal dipendente che aveva visitato siti *web* non legati all'attività istituzionale. Secondo la sentenza *"... la condotta serbata dal Tizio nella fattispecie in esame si manifesta come connotata da colpa grave in quanto, pur non essendo evidentemente preordinata alla contrazione del "virus", è tuttavia segnata dalla piena e consapevole volontà di utilizzare uno strumento informatico in dotazione dell'Ufficio presso il quale egli prestava servizio, e quindi annoverabile tra i beni strumentali all'ottimale esecuzione ed adempimento di compiti strettamente istituzionali, per realizzare invece scopi e finalità di carattere eminentemente personale: l'evento dannoso in questo modo verificatosi – contrazione e propagazione successiva del virus con i conseguenti ingiustificati costi – rappresenta così la conseguenza prossima, prevedibile ed evitabile, della iniziale condotta volitiva. Il Tizio poteva e doveva astenersi dall'eseguire operazioni non pertinenti con l'attività lavorativa propria tanto in ragione del generalizzato dovere di osservanza delle regole organizzative dell'Ufficio che non consentono lo svolgimento di operazioni diverse da quelle riconducibili alle mansioni assegnate, quanto, e soprattutto, in virtù della conoscibilità dei pericoli derivanti dalla non corretta utilizzazione del sistema informatico, conoscibilità resa possibile dall'intervento di specifiche comunicazioni diramate dalla Direzione Prov.le del Lavoro di Potenza in data 8.11.2000 e 22.3.2002, ed indirizzate al personale tutto della sede locale*".[40]

Da un punto di vista più strettamente penalistico è da osservare che si rinvengono, allo stato, rare decisioni giudiziarie relative all'abuso della posta elettronica e della navigazione su *internet* da parte del dipendente pubblico mediante le dotazioni d'ufficio. Esistono, tuttavia, più cospicue pronunzie relative all'uso delle apparecchiature telefoniche in ambito lavorativo pubblico, che potrebbero applicarsi[41] anche all'uso illegittimo della posta elettronica nonché alla navigazione *internet* non autorizzata. La Suprema Corte, in realtà, è stata divisa sul punto, pur ritenendo applicabile in materia l'art. 314 c.p. relativo al peculato. Più in particolare, mentre talune decisioni hanno ritenuto che il fatto debba essere inquadrato nell'ipotesi prevista dal primo comma del citato articolo, punita con la grave pena della reclusione da tre a dieci anni (*ex plurimis*, Cass. Pen, Sez. VI, 07/03/2003, n. 10671; Cass. Pen, Sez. VI, 31/05/2007, n. 21335), altre hanno invece affermato che si trattava di "peculato d'uso", fatto punito con la più lieve pena della reclusione da sei mesi a tre anni (Cass. Pen., Sez. VI, 14/02/2000, n. 788). Tuttavia, la Suprema Corte, di fronte alla scarsa

[39] Il celebre *worm* denominato "*Blaster*", in grado di sfruttare le vulnerabilità descritte nei bollettini di sicurezza informatica *Microsoft* n. MS03-06 e MS03-039.
[40] **A. MONTI**, *Responsabilità del dipendente e mancato rispetto delle regole sull'uso della postazione di lavoro*, in ICTLEX BRIEFS, n. 3/2006, su www.ictlex.com .
[41] Ed in tal senso si muove l'iniziativa della Procura della Repubblica di Verbania.

rilevanza dei reati commessi dal soggetto imputato, non ha ritenuto di affermare la grave responsabilità derivante dall'applicazione dell'art. 314 c.p. ed ha, con la suddetta decisione n. 788/2000, compiuto un'attività interpretativa della norma, ammettendo il fatto che la condotta dell'imputato appariva caratterizzata dalla eccezionalità prevista dal citato art. 10 dell'allora vigente Decreto del Ministro della Funzione Pubblica del 31/03/1994. Di interesse, è un ulteriore caso relativo alla condotta di un dipendente di un ente locale consistita nell'aver utilizzato il *computer* d'ufficio per navigare su siti non istituzionali, scaricando su archivi personali circa diecimila *file* a carattere prevalentemente pornografico (Cass. Pen., Sez. VI, 21/05/2008, n. 20326)[42].

Al riguardo, la Suprema Corte ha rinviato al giudice *a quo* l'ordinanza impugnata per un nuovo esame, osservando che "*l'art. 314 c.p., oltre a tutelare il patrimonio della pubblica amministrazione, mira ad assicurare anche il corretto andamento dei pubblici uffici, basato su un rapporto di fiducia e lealtà col personale dipendente*"; ha inoltre ritenuto non sufficientemente dimostrata l'assenza di danno patrimoniale per la stessa pubblica amministrazione. Appare evidente, quindi, che la mancanza di danno patrimoniale non esclude automaticamente la sussistenza del reato in questione, allorché l'uso del bene pubblico da parte del dipendente che ne abbia la disponibilità sia tale da ledere comunque il buon andamento degli uffici.

Tutto ciò premesso, l'intera problematica, nei suoi riflessi giuridici e normativi, andrebbe esaminata anche alla luce degli orientamenti della coscienza sociale. Appare infatti *illusoire et irrealiste*, - come affermato in Francia dalla CNIL, organo posto a tutela della *privacy*, in un rapporto denominato "*La cybersurveillance des salariés dans l'entreprise*" del marzo 2001[43] - una proibizione rigorosa dell'uso per scopi personali degli strumenti tecnologici in ambiente lavorativo.

Ciò che appare di interesse, dinanzi alla diffusione del fenomeno, è riesaminare l'inquadramento tradizionale dell'ipotesi di abuso nell'ambito penalistico per evitare soluzioni giurisprudenziali oggettivamente inique di fronte alla scarsa rilevanza della condotta, tenendo conto, da un lato le esigenze di sicurezza e di correttezza amministrativa, dall'altro la necessità di evitare frustrazioni in ambiente lavorativo le cui conseguenze potrebbero anche cagionare come effetto una minore produttività. È pacifico, comunque, che le risorse produttive appartengano al datore di lavoro per il perseguimento della propria attività istituzionale. Tale consapevolezza, tuttavia, sfuma progressivamente quando si considerano i mezzi di comunicazione, un settore in cui si è visto affermare un principio contrario: l'uso per fini privati è consentito fino a contraria disposizione e il dirigente non può violare la sfera afferente la protezione dei dati personali del dipendente anche se per esigenze di servizio.

[42] Per la configurabilità del reato di abuso d'ufficio a seguito dell'indebito utilizzo di *internet* da parte del pubblico dipendente, si veda Cass. Pen., Sez. VI, 09/04/2008, n. 31688.
[43] Su http://www.cnil.fr/ .

Tale erroneo luogo comune, è spesso accompagnato da una distorta percezione della violazione delle *policy* di sicurezza previste, tale da ingenerare la non implicazione di alcuna conseguenza in termini di sanzioni disciplinari.

La percezione del reato commesso con le nuove tecnologie, soprattutto da parte dell'utente comune, è di vitale importanza poiché fornisce informazioni e conferme sulla diffusione di stereotipi e atteggiamenti relativi a determinate azioni improprie. La percezione sociale di alcuni crimini legati a tali tecnologie può risultare a tal punto distorta che sarebbe possibile non considerare reato ciò che è ritenuto tale dalle norme. Molti utenti, infatti, pur consapevoli che alcuni comportamenti integrano un comportamento non consentito, trovano giustificazione per il fatto di praticarli in quanto li percepiscono come impersonali.

Alla luce di quanto rappresentato, appare evidente come approcciare in modo efficace con l'adozione e la partecipazione delle misure *compliant* IT in ambito pubblico, costituisca basilare fondamento anche per il perseguimento del buon andamento della pubblica amministrazione. Tale osservazione, tuttavia, non può trascurare come dovrebbe accrescere lo sforzo da parte dei soggetti pubblici coinvolti a predisporre provvedimenti che tengano preliminarmente in maggior considerazione l'analisi sull'impatto organizzativo e tecnico derivante dall'adozione delle misure di sicurezza che si intendono implementare. Ciò, infatti, porterebbe a indubbi benefici di applicabilità di disposizioni che faticano non poco a integrarsi con l'ordinario fluire dell'attività amministrativa.