C O M U N E D I B I T E T T O

Medaglia d'Oro al Merito Civile

COPIA DELIBERAZIONE ORIGINALE DELLA GIUNTA COMUNALE

N.ro 83 del reg.
Data 10.10.2007

OGGETTO: Linee guida per proteggere la sicurezza dell'ente e la riservatezza dei dipendenti-approvazione disciplinare

L'anno 2007, il giorno 10 del mese di OTTOBRE alle ore 17.00 con il prosieguo nella sala delle adunanze del Comune suddetto, convocata con appositi avvisi, la Giunta Comunale si è riunita nelle persone dei signori:

	Giovanni Iacovelli	Sindaco
.	Donato Calamita	Vice Sindaco
	Anna Paladino	Assessore assente
	Tommaso Troccoli	Assessore
	Matteo Soranno	Assessore
	Martire Proscia	Assessore
	Mario Rutigliano	Assessore

Con l'assistenza del Segretario Generale ff dott.Vincenzo Marcario

Il Sindaco, constatato che gli intervenuti sono in numero legale, dichiara aperta la riunione ed invita i convocati a deliberare sull'oggetto sopraindicato.

IL RESPONSABILE DEL SERVIZIO INTERESSATO
UDE
Ai sensi dell'art.49 del D. Lgs. 18.08.2000, n.267
esprime parere:

FAVOREVOLE

In merito alla regolarità tecnica

Giorgio Gatti

LA GIUNTA COMUNALE

Il Sindaco sulla base dell'istruttoria operata dall'ufficio competente, confermata dal capo settore UDE

Premesso che con deliberazione del garante n. 13 del 1° marzo 2007 (pubblicata sul sito dell'Autorità come doc. web. n. 1387522) sono state elaborate linee guida per l'uso di internet e della posta elettronica che qui di seguito si trascrivono alcune interpretazioni su:

Linee guida per proteggere la sicurezza dell'ente e la riservatezza dei dipendenti

Spiare il lavoratore è vietato, i controlli indiretti e graduali sull'uso della posta elettronica e di internet, invece, no. Il bilanciamento degli opposti interessi (salvare la privacy e non impedire i controlli interni ente) ha spinto il garante a elaborare le linee guida per l'uso di internet ed e-mail sui luoghi di lavoro pubblici e privati. La deliberazione n. 13 del 1° marzo 2007 (pubblicata sul sito dell'Autorità come doc. web. n. 1387522) definisce in maniera precisa il confine del controllo lecito da quello illecito. Il controllo lecito ha le seguenti caratteristiche: è indiretto, contrattato con i sindacati, è oggetto di una informazione preventiva al lavoratore, è graduale, è effettuato da soggetti appositamente designati, è preceduto da una disciplina interna dei controlli diffusa tra i lavoratori.

Il controllo illecito è invece a distanza, a sorpresa, diretto, realizzato senza la consapevolezza del lavoratore. Ma al di là della definizione dei controlli leciti, la deliberazione del garante chiama gli enti ad uno sforzo organizzativo: non solo disciplinare i controlli interni con una circolare o un ordine di servizio), ma anche porre in essere quelle barriere tecniche in grado di arginare il problema:

abilitazioni specifiche all'uso di internet, oscuramento di siti, messa a disposizione di caselle di posta elettronica personali, liberamente utilizzabili,creazione di indirizzi di posta elettronica di ufficio.

Si obietterà chequesto sforzo organizzativo si traduce in oneri economici per le pubbliche amministrazioni. La risposta è che una rimodulazione organizzativa dell'ente pubblico potrà essere proficua in se stessa, a prescindere dalla esigenza di garantire controlli privacy compatibili e che una verifica delle autorizzazioni di accesso alla rete libererà le risorse che sono necessarie a finanziare gli adempimenti prefigurati dal provvedimento del garante.

Verificando i contenuti della deliberazione, non senza specificare che con la stessa diventano sorpassati alcuni orientamenti giurisprudenziali di merito che si sono pronunciati nel senso di una piena liceità dell'accesso del datore di lavoro alla casella di posta elettronica del lavoratore. Il provvedimento riconosce ai datori di lavoro pubblici e privati alcune prerogative, tra le quali assicurare la funzionalità e il corretto impiego di internet e della posta elettronica da parte dei lavoratori e tutelare la sicurezza e l'integrità dei

sistemi informativi e di dati, anche per prevenire utilizzi indebiti (anche da parte degli stessi lavoratori). Di fronte a questa prerogativa si collocano i diritti dei lavoratori.

L'utilizzo di internet significa esporsi a un possibile costante e penetrante monitoraggio, in quanto la navigazione può formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, come descrive nelle sue premesse lo stesso provvedimento del garante, da un proxy server o da un altro strumento di registrazione delle informazioni.

Peraltro questo aspetto potrebbe non essere noto a tutti i lavoratori e una diffusione di tale informazione potrà di per sé disincentivare utilizzi non consentiti.

Lo stesso vale per i servizi di posta elettronica, suscettibili (anche attraverso la tenuta di log file di traffico e-mail e archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza. Insomma usare internet e la posta elettronica significa esporsi allo sguardi di tanti, anche se la convinzione di un profano può essere di segno contrario e cioè di navigare in canali strettamente confidenziali. H provvedimento del garante si occupa in specifico di disciplinare i diritti e i doveri del datore di lavoro rispetto al controllo sull'uso della rete da parte del lavoratore: l'uso di internet e dell'e-mail costituisce ai sensi del codice della privacy trattamento di dati personali (del lavoratore) e bisogna capire fino a che punto questo trattamento può avvenire senza violare la legge. Anzi in gioco ci sono anche i dati personali di terzi, come per esempio i destinatali di messaggi di posta elettronica inviati dal lavoratore.

Un freno alla commistione tra sfera lavorativa e privata

Il primo aspetto toccato dalla deliberazione è il potere del datore di lavoro di disciplinare l'uso di internet e della posta elettronica da parte dei lavoratori. Per arginare la possibile commistione tra sfera lavorativa e sfera privata (possibile oggetto di invasioni di campo da parte del lavoratore) il garante sottolinea che diversi datori di lavoro hanno prefigurato modalità d'uso che assegnano aree di lavoro riservate per appunti strettamente personali, o consentono usi moderati di strumenti per finalità private. È evidente che una scelta di questo tipo deve fare i conti con la dimensione dell'impresa e le compatibilità economiche della stessa. H provvedimento del garante traccia linee guida per la ricostruzione normativa del bilanciamento tra l'interesse del datore di lavoro di ottenere la prestazione lavorativa e preservare gli strumenti ente e l'interesse del lavoratore di non subire illeciti trattamenti di dati personali. La prima misura indicata nel provvedimento del garante è la disciplina interna e cioè la redazione di un codice, un provvedimento richiama i datori di lavori all'onere di indicare in ogni caso,

chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali. Peraltro va anche sottolineato che non solo questa informazione costituisce un obbligo a carico del datore di lavoro, ma è anche un suo interesse, perché si mettono nero su bianco le regole per l'uso dei computer in ente. La disciplina interna può essere adottata con un vero e proprio codice, ma si può pensare anche a circolari o a ordini di servizio. Il disciplinare interno va pubblicizzato adeguatamente: comunicazione diretta ai singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavori e va sottoposto ad aggiornamento periodico.

Il provvedimento del garante si spinge a individuare il contenuto del disciplinare interno sull'uso di internet e della posta elettronica, indicando che in esso va per esempio specificato:

1) se determinati comportamenti non sono tollerati rispetto alla «navigazione» in internet (per esempio, il download di software o di file musicali), oppure alla tenuta di file nella rete interna;

2) in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di webmail, indicandone le modalità e l'arco temporale di utilizzo (per esempio, fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);

3) quali informazioni sono memorizzate temporaneamente (per esempio, le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;

4) se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log);

5) se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime, specifiche e non generiche, per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);

6) quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;

7) le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;

8) se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
9) quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
10) le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché allegato B), in particolare regole 4,9,10).
Alla disciplina interna (da diffondere tra i lavoratori) si aggiunge, per il datore di lavoro, l'obbligo di fornire l'informativa ai sensi dell'articolo 13 del Codice).
Nell'informativa privacy vanno illustrate le modalità di controllo, le finalità dei controlli (specifiche esigenze organizzative, produttive e di sicurezza del lavoro, esercizio di un diritto in sede giudiziaria). Va specificato anche soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i diritti garantiti dal codice della privacy

La posta elettronica

In ente si usano caselle di posta elettronica del tipo m.rossi@ente.it, rossi@societa.com, mario.rossi@società.it. Non sempre è esplicito se i messaggi riguardano le incombenze lavorative o piuttosto la sfera privata.
Se non c'è un disciplinare interno all'ente vale la regola per cui il lavoratore ha la legittima aspettativa sulla confidenzialità dell'email.
Per poter effettuare controlli indiretti sulla posta elettronica deve quindi disciplinare l'uso della posta elettronica stessa. In secondo luogo è opportuno che il datore di lavoro ponga in essere alcuni accorgimenti che diminuiscono l'entità del problema:

- rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori (per esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@societa.com, urp@ente.it ecc.), eventualmente affiancandoli a quelli individuali;
- valutare la possibilità di attribuire al lavoratore un diverso indirizzo destinato a uso privato del lavoratore;
- mettere a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le «coordinate» (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura;
- prescrivere ai lavoratori di avvalersi delle modalità di risposta automatica, prevenendo così

l'apertura della posta elettronica;

- in caso di eventuali assenze non programmate (per esempio per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), perdurando l'assenza oltre un determinato limite temporale, disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (l'amministratore di sistema oppure, se presente, un incaricato dell'ente per la protezione dei dati), l'attivazione dell'accorgimento della risposta automatica, avvertendo gli interessati;
- in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, se si debba conoscere il contenuto dei messaggi di posta elettronica, consentire al lavoratore di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa (con la compilazione di un apposito verbale e informazione al lavoratore interessato alla prima occasione utile;
- inserimento nei messaggi di posta elettronica di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla policy datoriale.

I controlli consentiti

I controlli consentiti sono i cosiddetti controlli «indiretti» e cioè quelli che derivano dall'utilizzo di sistemi informativi per esigenze produttive o organizzative (quelli per rilevare anomalie o per manutenzioni) o, comunque, necessari per la sicurezza sul lavoro. Resta, certamente, ferma in questi casi la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati così come in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. Peraltro prima di arrivare all'utilizzo dei controlli indiretti il garante richiama a una rimodulazione organizzativa dell'ente, che si articola su quattro piani:

1) valutazione dell'impatto delle apparecchiature sui diritti dei lavoratori
2) individuazione preventiva (anche per tipologie) dei lavoratori ai quali è accordato l'utilizzo della posta elettronica e l'accesso a internet;
3) individuazione della ubicazione riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo;

4)adozione di tutte le misure tecnologiche volte a minimizzare l'uso di dati identificativi (privacy enhancing technologies-PETs).

In ogni caso i controlli devono essere non solo indiretti, ma anche graduati. Deve essere per quanto possibile innanzi tutto realizzato un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo a un rilevato utilizzo anomalo degli strumenti dell'ente e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale. Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati. In seconda battuta si passa ai controlli individuali. Per i controlli ammessi non è necessario il consenso del lavoratore. Per i controlli, inoltre, il datore di lavoro può designare facoltativamente uno o più responsabili del trattamento. In ogni modo in caso di eventuali interventi per esigenze di manutenzione del sistema, va evitato l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti, con l'obbligo degli incaricati della manutenzione di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa. Adempimento connesso è quello della formazione del personale sui rischi collegati all'uso degli elaboratori. Infine i dati personali relativi agli accessi ad internet e al traffico telematico, la cui conservazione non sia necessaria, non devono essere conservati senza limite di tempo. Anzi gli stessi sistemi software devono essere programmati e configurati in modo da cancellare periodicamente e automaticamente i dati.

Un eventuale prolungamento dei tempi di conservazione è ammesso in via eccezionale solo in relazione:

- a esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare a una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Il controllo a distanza

La regola iniziale è il divieto di installare «apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori», tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica. Il divieto opera anche se i lavoratori sono esattamente informati della natura degli apparecchi e delle modalità di controllo, li principio si sviluppa nei divieti specifici di:

•lettura e registrazione sistematica dei messaggi di posta elettronica e dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio -mail;
•riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
•lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo dell'analisi occulta di computer portatili affidati in uso.

Peraltro il divieto di controllo a distanza, precisa lo stesso garante, riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. Come ha precisato, infatti, la giurisprudenza, il divieto del controllo a distanza dell'attività dei lavoratori posto dall'articolo 4 Statuto lavoratori non si estende ai cosiddetti controlli difensivi, i quali, peraltro, non costituiscono una categoria a sé esentata, a priori, dall'applicabilità delle previsioni dell'articolo 4, ma semplicemente un modo per definire controlli finalizzati all'accertamento di condotte illecite del lavoratore che non rientrano nell'ambito di applicazione del divieto perché non comportano la raccolta anche di notizie relative all'attività lavorativa. È stato così ritenuto che stanno al di fuori della previsione della norma il controllo cosiddetto difensivo al fine di verificare condotte illecite dei lavoratori, quali sono le telefonate ingiustificate.

L'uso di internet

II lavoratore non può tenere condotte illecite in contrasto con il disciplinare tecnico elaborato dal datore di lavoro: visione di siti non pertinenti, upload e download di file, uso di servizi di rete con finalità ludiche o estranee all'attività.

Il datore di lavoro può reagire senza violare la privacy del lavoratore.

In particolare, il datore di lavoro può:

•individuare categorie di siti considerati correlati o meno con la prestazione lavorativa;
•configurare di sistemi o utilizzo di filtri che prevengano determinate operazioni, incoerenti con l'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
•trattare di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni;
•conservare nel tempo i dati sui controlli in maniera strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza

Considerato che il Comune di Bitetto non ha mai adottato un disciplinare per l’uso di internet e della posta elettronica;

che a fronte di quanto sopra, occorre provvedere all'approvazione e dotazione di un disciplinare, di seguito riportato, da notificare a tutti i dipendenti che usufruiscono di internet e che sono titolari di posta elettronica;

Ritenuto pertanto fare proprie le su esposte considerazioni del Garante ed approvare il relativo disciplinare :

DISCIPLINARE

Al Sig.

In relazione alle disposizioni a tutela della riservatezza del lavoratore e in osservanza della deliberazione del garante per la protezione dei dati personali n. 13 dell'1/3/2007; con la presente comunicazione si comunicano le modalità di utilizzo di internet e della posta elettronica, alle quali tutti coloro che hanno una postazione con accesso ad internet dovranno attenersi.

Computer

- È vietato installare programmi non autorizzati
- È vietato modificare le configurazioni impostate, se non preautorizzate dal Responsabile Informatico
- È vietato installare modem o altri apparecchi non autorizzati
- Tutti i supporti magnetici devono essere utilizzati previa autorizzazione dell'ente

Internet

- Non è consentito navigare in siti o registrarsi a siti non attinenti allo svolgimento delle mansioni
- non è consentito il download di programmi o di file musicali, anche se gratuiti, salvo autorizzazione preventiva ed espressa
- è vietato partecipare a forum e utilizzare chat line, se non strettamente inerente l'attività istituzionale.
- è vietata la conservazione di file a contenuto offensivo, discriminatorio

E-mail

- è vietato l'uso della posta elettronica per motivi non attinenti allo svolgimento delle mansioni
- è consentito utilizzare l'uso della posta elettronica anche per ragioni personali,

esclusivamente dalla seguente postazione...

- è consentito utilizzare l'uso della posta elettronica anche per ragioni personali fuori dall'orario di lavoro o durante le pause, o altro
- è vietato inviare o memorizzare messaggi a contenuto offensivo, discriminatorio
- è vietato usare la posta elettronica per documenti riservati o confidenziali
- è vietato l'uso della posta elettronica per la partecipazione a dibattiti, forum o mail-list a contenuto offensivo, discriminatorio
- in caso di sua assenza la continuità dell'attività lavorativa sarà garantita da sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;

In caso di assenza non programmata Lei è tenuto a indicare un fiduciario prontamente reperibile per la lettura dei messaggi di posta elettronica.

Si precisa inoltre che le informazioni sono memorizzate e a essi può accedere il personale debitamente autorizzato. Inoltre, il Responsabile del S.I.C. si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali. La non osservanza delle prescrizioni comporterà l'applicazione delle sanzioni disciplinari previste dal vigente contratto di lavoro.

Per ogni chiarimento Lei potrà rivolgersi al Responsabile del Servizio Informatico Comunale

Si prega di restituire la presenta debitamente sottoscritta per presa visione e accettazione.

Data e firma

DELIBERA

Per i motivi in narrativa esposti e che qui si intendono riprodotti

1. di approvare il disciplinare per l'utilizzo di internet e della posta elettronica
2. di fare proprie tutte le considerazioni del Garante;
3. di dichiarare che la presente non comporta impegno di spesa;
4. di demandare al Responsabile del Servizio Informatico Comunale ogni adempimento consequenziale alla presente;
5. Di rendere la presente immediatamente eseguibile, ai sensi dell'art.134 - 4° comma – del D. Lgs. 18.8.2000, n.267.

Approvato e sottoscritto:

Il Segretario Generale ff **Il Sindaco**
F.to: Dott.Vincenzo MArcario **F.to: Giovanni IACOVELLI**

ATTESTATO DI INIZIO PUBBLICAZIONE

Si attesta che copia della presente deliberazione è in corso di pubblicazione all'Albo Pretorio di questo Comune per quindici giorni consecutivi dalla data _____

Il Capo Settore AA.GG.

PUBBLICAZIONE

Pubblicata per 15 giorni dal _____ al _____ e contestualmente comunicata ai capi gruppi consiliari.

- Immediatamente eseguibile
- Non soggetta a controllo
- Soggetta a controllo di iniziativa dell'Organo
- Soggetta a controllo di iniziativa di 1/5 dei consiglieri (istanza del _____)
- Inviata alla Sezione di controllo il _____
- Ricevuta dalla Sezione di Controllo il _____
- Ordinanza interlocutoria n._____ del _____
- Controdeduzioni del Comune n._____ del _____

ESECUTIVITA'

- Divenuta esecutiva per decorrenza dei termini il _____
- Divenuta esecutiva a seguito di comunicazione del Comitato di Controllo Regione Puglia – Bari il _____.

Bitetto lì_____ **Il Capo Settore AA.GG.**

E' copia conforme all'originale per uso amministrativo.

Dalla residenza comunale lì _____ **Il Capo Settore AA.GG**