Utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche

Approvazione Disciplinare
Delibera n. 1037 del 07/05/2010

Utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche - Approvazione Disciplinare.

PROVINCIA AUTONOMA DI TRENTO
Pag. di 6 RIFERIMENTO: 2010-S007-00357

Reg.delib.n. 1037
Prot. n.

VERBALE DI DELIBERAZIONE DELLA GIUNTA PROVINCIALE

O G G E T T O:
Utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche - Approvazione Disciplinare.

Il giorno 07 Maggio 2010 ad ore 10:05 nella sala delle Sedute
in seguito a convocazione disposta con avviso agli assessori, si è riunita

LA GIUNTA PROVINCIALE

sotto la presidenza del

PRESIDENTE
Lorenzo Dellai

Presenti:
VICE PRESIDENTE
Alberto Pacher

ASSESSORI
Mauro Gilmozzi

Lia Giovanazzi Beltrami

Tiziano Mellarini

Alessandro Olivi

Ugo Rossi

Assenti:

Marta Dalmaso

Franco Panizza

Assiste:
LA DIRIGENTE
Patrizia Gentile

Il Presidente, constatato il numero legale degli intervenuti, dichiara aperta la seduta
Il Relatore comunica:
L'art. 46 bis della l.p. n. 7/1997, come introdotto dall'art. 23, c. 8 della l.p. n. 4/2009, dispone che per assicurare la funzionalità, la sicurezza e il corretto impiego degli strumenti informatici e delle reti telematiche da parte degli utilizzatori, la Giunta provinciale adotti, con proprio provvedimento, un disciplinare che definisca le misure di tipo organizzativo e tecnologico e individui le condotte e le forme di controllo ammissibili.
Con tale norma, diretta al perseguimento degli interessi generali cui l'organizzazione e l'azione amministrativa sono indirizzate (art. 36, c. 1, l.p. n. 7/1997 e s.m.), il legislatore provinciale prende atto di come l'uso delle tecnologie informatiche implichi notevoli rischi sia dal punto di vista della sicurezza nei luoghi di lavoro che di quello della funzionalità e del corretto impiego delle reti telematiche e degli strumenti informatici, fatti oggetto di specifiche previsioni in sede penale e fonti di possibile responsabilità dell'Amministrazione, con conseguente necessità, peraltro prevista dalle stesse fonti normative in svariati settori (contrasto al terrorismo, reati pedopornografici, illeciti finanziari e così via), di adottare le opportune misure volte a limitare e contenere i rischi predetti.
Tali misure si traducono nella necessaria adozione di strumenti di filtraggio e monitoraggio delle comunicazioni tali da consentirne il tracciamento tecnologico cui può potenzialmente accompagnarsi la possibilità di controllo indiretto della attività dei lavoratori. A salvaguardia dei diritti del lavoratore e, in primis, del diritto alla dignità e riservatezza, opera dunque un complesso normativo richiamato dall'art. 46 bis cit., ossia:
il d.lgs. n. 82/2005 (Codice dell'amministrazione digitale), con particolare riferimento all'art. 2, c. 5 che riconosce il diritto dei cittadini a che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché alla dignità dell'interessato;
il d.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali), che sancisce il diritto alla protezione dei dati personali e dispone che ogni trattamento garantisca un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2); il legislatore prescrive, inoltre, che i trattamenti di dati siano effettuati per finalità determinate, esplicite e legittime, oltre a dover rispondere al principio di necessità e correttezza: ogni dato trattato in violazione della disciplina in materia non può essere utilizzato (artt. 11, 3);
la l. n. 300/1970 (Statuto dei Lavoratori), con particolare richiamo all'art. 4 che, nel contemperamento tra le esigenze del datore di lavoro e quelle dei dipendenti, svolge a tutt'oggi un ruolo fondamentale, vietando da un lato il controllo diretto dei lavoratori e, dall'altro, ammettendo per esigenze organizzative produttive ovvero di sicurezza del lavoro, l'installazione di impianti e apparecchiature di controllo dalle quali possa anche derivare un controllo a distanza dell'attività dei lavoratori (c.d. controllo preterintenzionale). Nel settore privato si prevede per tali casi non la determinazione unilaterale del datore di lavoro ma il previo accordo con le OO.SS. o, in mancanza, l'autorizzazione dell'Ispettorato del lavoro.
Recentemente, anche l'Amministrazione statale, con la direttiva n. 2/2009 avente ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro", ha fornito indicazioni utili a facilitare, nell'ambito del settore pubblico, da un lato il corretto utilizzo degli strumenti ICT (postazioni di lavoro, connessioni di rete e posta elettronica) e, dall'altro il proporzionato esercizio del potere datoriale di controllo da parte delle Amministrazioni pubbliche.
Specifica rilevanza assume poi in materia la deliberazione n. 13/2007 del Garante per la protezione dei dati personali, che prescrive ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e di internet.
In particolare, il Garante, alla luce della normativa sopra richiamata, evidenzia la necessità che i trattamenti di dati si uniformino al principio di necessità e di correttezza e che siano sempre effettuati per finalità determinate, esplicite e legittime; sottolinea, inoltre, a tutela della libertà e dignità dei lavoratori, il divieto di installare apparecchiature preordinate al controllo a distanza dei dipendenti, ammettendo invece l'utilizzo di programmi e tecnologie che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale), a condizione che ciò sia necessario per esigenze produttive o organizzative o, comunque, quando sia necessario per la sicurezza sul lavoro; evidenzia ancora come eventuali controlli

sull'utilizzo degli strumenti informatici debbano ispirarsi al principio di pertinenza e non eccedenza, nell'equo bilanciamento di interessi tra le parti coinvolte.
Sono poi fortemente sottolineati dal Garante gli accorgimenti tecnici volti a prevenire comportamenti del lavoratore pericolosi per la sicurezza aziendale, di cui viene data ampia esemplificazione.
Il disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche, di cui si propone l'approvazione, è dunque volto a garantire, in ossequio a quanto previsto dal legislatore, la sicurezza nei luoghi di lavoro, assicurare la funzionalità e il corretto impiego delle reti telematiche e degli strumenti informatici e di comunicazione, fermo restando il divieto di utilizzo di sistemi hardware e software esclusivamente preordinati al controllo a distanza dell'attività lavorativa del dipendente.
A tal fine il documento raccoglie, innanzitutto, una serie di elementari prescrizioni per il corretto utilizzo degli strumenti di lavoro (per es.: verificare l'assenza di virus dei supporti magnetici in input; mantenere la segretezza delle password; non lasciare incustodito e accessibile il PC durante la sessione di lavoro e così via). Il Disciplinare ribadisce poi il generale divieto, per i dipendenti provinciali, di utilizzare per ragioni personali Internet, la posta elettronica e le attrezzature informatiche; in deroga e solo al di fuori dell'orario di lavoro, consente, previa autorizzazione del dirigente, di avvalersi dei servizi Internet e di posta elettronica per motivi personali, nelle fasce orarie dalle 07.45 alle 09.00, dalle 12.45 alle 14.30 e dopo le 18.30 (prima e/o dopo l'orario di lavoro, per il personale a part-time orizzontale). Il Disciplinare regolamenta anche i controlli previsti per verificare il generale rispetto delle norme organizzative e di sicurezza. Tali controlli si svolgono, in prima istanza, in forma anonima (anche a campione) e, solo in caso di reiterazione o nei casi espressamente indicati (per gli illeciti civili, penali e amministrativi), in forma specifica e mirata, ossia mediante identificazione del singolo dipendente. Le verifiche possono riguardare anche il corretto utilizzo delle linee telefoniche dell'ufficio: in deroga al generale divieto di effettuare telefonate personali, sono ammesse brevi e limitate chiamate tra il personale provinciale e, solo in casi eccezionali e urgenti, verso soggetti esterni. Il Disciplinare indica, inoltre, le misure di garanzia di tipo organizzativo e tecnologico che l'Amministrazione adotta, attraverso le strutture competenti, per assicurare il perseguimento delle predette finalità prevedendo, ad esempio: l'ubicazione dei server in luogo protetto, la periodica sostituzione della password su richiesta del sistema; l'individuazione di categorie di siti considerati non correlati con la prestazione lavorative (black list) e così via.
Il Disciplinare vieta, ovviamente, i controlli esclusivamente diretti all'attività del lavoratore nonchè, salvo diversa previsione dei contratti collettivi, l'utilizzo dei sistemi e dei dati al fine della valutazione quantitativa e qualitativa della prestazione del lavoratore nonché ai fini dell'accertamento del rispetto degli obblighi di comportamento del lavoratore nell'esecuzione del contratto di lavoro estranei all'ambito di regolazione del disciplinare e sempre che tale comportamento non costituisca più grave illecito civile, penale o amministrativo. Non è inoltre previsto l'utilizzo di software di controllo.
Il Disciplinare, in coerenza con le finalità perseguite, si applica non solo ai dipendenti provinciali ma anche, in quanto compatibile, agli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture della Provincia; costituisce inoltre linea guida per il corretto utilizzo tecnico delle strumentazioni informatiche per coloro che, a qualunque titolo, utilizzano il sistema informativo provinciale; infine, si rivolge anche agli enti pubblici strumentali della Provincia, fatta salva la possibilità di adottare un proprio disciplinare.
L'inosservanza delle prescrizioni in esso contenute può comportare, oltre all'irrogazione di sanzioni disciplinari nei confronti dei dipendenti, la sospensione o la revoca dell'autorizzazione ad accedere ai sistemi.
Sullo schema di Disciplinare sono state raccolte e recepite le osservazioni del Servizio semplificazione e sistemi informativi, del Servizio Reti e telecomunicazioni e del Servizio Edilizia pubblica e logistica.
Lo schema di Disciplinare è stato altresì comunicato alle Organizzazioni sindacali per eventuali osservazioni. Ha riscontrato la sola FENALT con nota d.d. 3 marzo 2010. Sulla base delle relative osservazioni si è innanzitutto meglio precisato all'art. 1 il divieto di controllo a distanza laddove esclusivamente diretto all'attività del dipendente, vietato dall'art. 4, c. 1, l. n. 300/1970; all'art. 12.2 lett. m) si è poi subordinato l'accesso del dirigente alla casella di posta elettronica del dipendente assente a improrogabili ragioni di ufficio.
La FENALT rileva inoltre che la recente sentenza della Corte di Cassazione n. 4375 del 23 febbraio 2010 stabilisce che i controlli a distanza preterintenzionali (funzionali a esigenze organizzative, produttive o di sicurezza) ricadono nell'art. 4, c. 2, l. n. 300/1970, che ammette il controllo a distanza solo in presenza di accordo sindacale, con il quale ultimo, dunque, non deve essere confuso il presente Disciplinare, restando l'accordo con le RSA presupposto imprescindibile di eventuali controlli.
Il punto merita specifica attenzione, dovendosi osservare come:
il Disciplinare ribadisce il divieto di controllo diretto dei lavoratori;

il Disciplinare presuppone l'utilizzo dei dati coessenziali al funzionamento dello strumento di lavoro (e non di controllo) utilizzato dallo stesso lavoratore (per es. sistema operativo) e non già di software applicativi di controllo a tutela di esigenze produttive, organizzative o di sicurezza del lavoro muniti della concreta potenzialità, attraverso opportuni algoritmi di elaborazione dei predetti dati, di monitorare a distanza l'attività lavorativa individuale dei lavoratori, di rappresentarne cioè il minuto svolgimento e consentirne dunque, in modo meccanico, continuo e anelastico (come descritto nella Relazione Ministeriale all'art. 4), la precisa analisi critico-valutativa di conformità della prestazione resa alla prestazione attesa (micropause, assenze temporanee; ritmi di lavoro, errori operativi, modalità esecutive e così via: situazione questa efficacemente descritta con la locuzione "lavoratore di vetro"); di qui, secondo taluni orientamenti, la radicale estraneità, in difetto di previsione di tali strumenti, all'art. 4, l. n. 300/1970;
a prescindere da quanto sopra, la sentenza citata, appunto relativa ad un contesto aziendale ove era stato adottato un apposito software di controllo (Super Scout), non reca in ogni caso, nella materia, particolari novità rispetto alla precedente giurisprudenza, subordinando ad accordo "i controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso". L'accordo è dunque richiesto solo laddove il controllo consenta la verifica del diligente adempimento della prestazione lavorativa sotto il profilo quali-quantitativo e dell'osservanza delle connesse norme aziendali, restando invece estranei alla necessità dell'accordo i controlli "difensivi" diretti a prevenire e reprimere gli ulteriori illeciti civili nonchè gli illeciti penali e amministrativi posti a presidio di beni estranei all'ambito del diligente adempimento della prestazione;
anche a voler ulteriormente prescindere, l'art. 46-bis, l.p. n. 7/1997, norma diretta al perseguimento degli interessi generali cui l'organizzazione e l'azione amministrativa sono indirizzate (art. 36, c. 1, l.p. n. 7/1997 e s.m.), rimette il disciplinare a "provvedimento" della Giunta provinciale e non ad accordo con le RSA, sul punto derogando dunque alla norma comune di cui all'art. 4, c. 2, l. n. 300/1970.
Per migliore chiarezza, in linea con quanto sopra osservato sub n. 3) si è in ogni caso provveduto ad integrare lo schema di Disciplinare (art. 10, lett. E) e 18, lett. D)) con il già visto espresso divieto - salvo diversa previsione dei contratti collettivi - di utilizzo dei sistemi e dei dati ai fini della valutazione quantitativa e qualitativa della prestazione del lavoratore nonchè ai fini dell'accertamento del rispetto degli obblighi di comportamento del lavoratore nell'esecuzione del contratto di lavoro estranei all'ambito di regolazione del disciplinare e sempre che il comportamento non costituisca diverso illecito civile, penale o amministrativo.
L'entrata in vigore dell'allegato Disciplinare è fissata per il Capo I il giorno successivo al relativo invio per posta elettronica ai dipendenti e, per il Capo II, il quindicesimo giorno successivo a quello di approvazione della presente delibera.

Tutto ciò premesso
LA GIUNTA PROVINCIALE

udita la relazione,
visto l'art. 46 bis della l.p. n. 7/1997,
vista la precitata normativa nazionale,
vista la deliberazione del Garante per la protezione dei dati personali e la citata direttiva,
a voti unanimi espressi nelle forme di legge,

delibera

di approvare il Disciplinare per l'utilizzo della rete internet, della posta elettronica, delle attrezzature informatiche e telefoniche, allegato alla presente deliberazione quale parte integrante e sostanziale della stessa;
2. di dare atto che il Disciplinare è pubblicato sul sito Web della Provincia autonoma di Trento ed entra in vigore nel Capo I il giorno successivo al relativo invio per posta elettronica ai dipendenti e, nel Capo II, il quindicesimo giorno successivo a quello di approvazione della presente delibera;.
di disporre la pubblicazione del Disciplinare nel sito Web della Provincia autonoma di Trento.

AM - SD