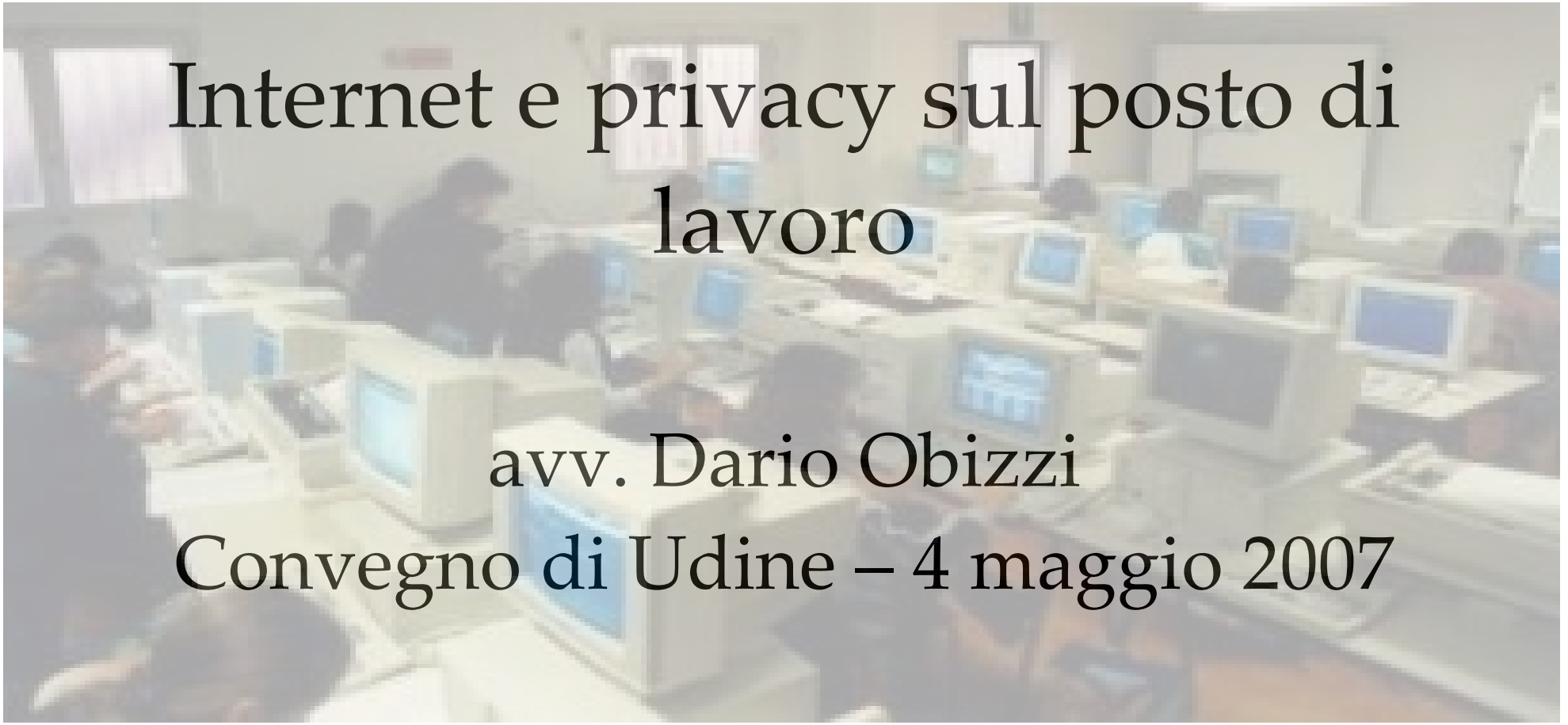

Internet e privacy sul posto di lavoro

avv. Dario Obizzi

Convegno di Udine – 4 maggio 2007

Caso: un dirigente pubblico si collegava, tramite il PC situato all'interno dell'ufficio, a siti Internet non istituzionali, per un totale di circa 250 ore in sei mesi!!!

La Pubblica Amministrazione si accorgeva di ciò del tutto casualmente operando dei controlli a seguito di ripetuti attacchi di virus informatici.

Il caso veniva discusso dinanzi alla Corte dei Conti.

Il dirigente negava gli addebiti sostenendo:

- Violazione della privacy da parte del datore di lavoro
- L'utilizzo del PC poteva essere stato effettuato da chiunque in quanto il dirigente, nei momenti di assenza, era solito lasciare l'ufficio aperto ed il PC incustodito con la PW inserita (!).

La Corte, censurando il comportamento assolutamente negligente ed imprudente del dirigente (che aveva lasciato incustodito il PC del proprio ufficio), rigettava la eccezione relativa ad una presunta violazione della privacy in quanto i controlli effettuati dalla P.A. erano avvenuti solo a causa degli attacchi dei virus e non erano preordinati al controllo dell'attività del lavoratore.

La Corte, quindi, condannava il dirigente al pagamento della somma di € 5.000,00, determinata in via equitativa.
(Corte dei Conti, sez. giurisdizionale, 13.11.2003, n. 1856)

Come emerge nell'esempio, l'utilizzo del PC e la navigazione in Internet sul posto di lavoro possono creare notevoli problemi.
Da un lato il datore di lavoro ha l'esigenza di controllare gli strumenti lavorativi. Ciò permette infatti di:

- Verificare l'**esatto adempimento** della prestazione lavorativa;
- Evitare **abusi** degli strumenti lavorativi;
- Ridurre al minimo il rischio che il dipendente commetta **illeciti civili e/o penali**, cui possa essere chiamato a rispondere anche il datore di lavoro (vd. art. 171 sexies L.633/41).

Dall'altro lato i lavoratori hanno il diritto di non essere controllati (se non entro certi limiti) sul posto di lavoro. Tali diritti trovano fondamento nelle seguenti fonti:

- STATUTO DEI LAVORATORI (L.n. 300/1970)

- CODICE PRIVACY (D.Lvo 196/2003), nonché tutti i provvedimenti, pareri, newsletter del Garante per la Privacy

(tra cui L'AUTORIZZAZIONE GENERALE N. 1/05, la DELIBERAZIONE n. 53 del 23.11.2006 in tema di trattamento dei dati dei lavoratori e la DELIBERAZIONE del 01.03.2007 in tema di e-mail ed internet)

LO STATUTO DEI LAVORATORI

- **DIVIETO ASSOLUTO**

Art. 4, comma 1, "*E' vietato l'uso di* ***impianti audiovisivi ed altre apparecchiature*** *per finalità di controllo a distanza dell'attività dei lavoratori.*"

La vigenza di tale divieto è confermata dal rinvio operato dall'art. 114 CODICE PRIVACY *"Resta fermo quanto disposto dall'articolo 4 della legge 300/70"*

- **DIVIETO RELATIVO**

Art. 4, comma 2, "***Gli impianti e le apparecchiature di controllo*** *che siano richiesti da* ***esigenze organizzative*** *e* ***produttive*** *ovvero dalla* ***sicurezza del lavoro****, ma dai quali derivi* ***anche la possibilità di controllo a distanza dell'attività dei lavoratori****, possono essere installati soltanto* ***previo accordo*** *con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la Commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'ispettorato del lavoro [...]*".

Con tali norme il legislatore del 1970 non ha voluto vietare il potere di controllo del datore di lavoro sull'operato del dipendente ma ha voluto *impedire*, attraverso l'art. 4, *l'abuso di tale potere*.

Si è voluto cioè impedire che il datore di lavoro operi una indiscriminata ingerenza nell'attività lavorativa (intesa in senso lato, comprendente anche le cd. Licenze comportamentali) tramite strumenti di controllo a distanza (sia in senso spaziale che temporale)

In estrema sintesi, si può dire che lo Statuto dei Lavoratori considera:

- **VIETATO** utilizzare (ma anche il semplice installare) apparecchiature di controllo a distanza dell'attività lavorativa;
- **LECITO** utilizzare apparecchiature di controllo a distanza per finalità di organizzazione, produzione e sicurezza del lavoro purché **non sia possibile alcun controllo dell'attività dei lavoratori;**
- **LECITO** utilizzare apparecchiature di controllo a distanza per finalità di organizzazione, produzione e sicurezza del lavoro anche se rende **possibile il controllo dell'attività dei lavoratori** purché: **previo accordo** con le RSU oppure Commissione interna oppure ispettorato del lavoro.

VIOLAZIONE DEL DIVIETO

Dal punto di vista penale, la violazione dell'art. 4 è sanzionata con una contravvenzione punita alternativamente con l'arresto o l'ammenda.
Tale pena nei casi più gravi può essere applicata congiuntamente e, in considerazione delle condizioni economiche del reo, puo' essere aumentata fino al quintuplo e può essere disposta la pubblicazione della sentenza di condanna.

Da un punto di vista processualcivilistico, le prove raccolte in violazione del divieto sono considerate inutilizzabili.

LA PRIVACY

Riprendendo principi già espressi nella quasi totalità dalla L. 675/96 e successive modifiche ed integrazioni, il codice Privacy consente il trattamento dei dati in capo al titolare-datore di lavoro a condizione che:

- il trattamento venga fatto nel rispetto dei principi di necessità e liceità (artt. 3 e 13);
- vi sia un'adeguata e preventiva informativa (art. 13);
- qualora previsto, l'interessato presti il proprio consenso (art. 23);
- trattandosi di dati sensibili, sia stata rilasciata l'autorizzazione da parte del Garante (art. 26);
- venga effettuata la notificazione al Garante (art. 37);
- vengano adottate le misure perlomeno minime (meglio se idonee) di sicurezza (art. 31).

CONTROLLO SUL COMPUTER: la situazione sino al marzo 2007

Secondo alcune pronunce, i controlli effettuati sul PC del dipendente sono leciti nei limiti dei cd. **controlli difensivi,** diretti cioè ad accertare condotte illecite del lavoratore. (In questo orientamento si inseriscono la pronuncia della Corte dei Conti (la n. 1856/2003 citata all'inizio, Cassazione n.4746/2002 e, da ultimo, Tribunale di Perugia ordinanza del 20 febbraio 2006).

Altre pronunce hanno invece ritenuto, anche nel caso di indagini difensive, sussistere l'obbligo di ricorrere alla procedura di autorizzazione di cui all'art. 4, secondo comma, Statuto Lavoratori (Cass. n. 8250/2000; Cass. 14671/2000; Corte Appello Milano n. 668/2005).

Per controllare i files (in particolare quelli di log, per verificare la navigazione in Internet) sarebbe necessario quindi ottenere il previo accordo della RSU, della Commissione Interna o dell'Ispettorato del Lavoro.

La soluzione corretta: il controllo difensivo non necessita della autorizzazione delle RSU tutte le volte in cui si sostanzia in un **controllo ex post** diretto a fronteggiare un atto illecito del dipendente. Naturalmente i controlli, ex art. 11 Codice Privacy, devono essere proporzionati, pertinenti, leciti, corretti ed eseguiti in modo trasparente.

Questa interpretazione sembra essere confermata anche dal provvedimento del 9.11.2006 del Garante che ha ritenuto leciti i controlli difensivi del datore di lavoro attuati mediante un'agenzia investigativa che aveva accertato che il dipendente svolgeva, nei lunghi periodi di malattia, un secondo lavoro.

Qualora il controllo difensivo venga effettuato **in via preventiva ed in maniera sistematica**, allora si rientra nel caso previsto e disciplinato dall'art. 4, 2° comma, Statuto dei Lavoratori (cd. Controllo preterintenzionale)

Sul punto è intervenuto di recente il Garante per la protezione dei dati personali che, con due ravvicinati provvedimenti, ha dato delle importanti indicazioni. Con il primo **provvedimento del 2 febbraio 2006**, ha stabilito che "*Ancorché al lavoratore dipendente possa essere contestato l'uso indebito del computer, è illegittimo il monitoraggio del contenuto dei siti visitati, idoneo a rilevare dati sensibili*"

Il Garante ha cioè statuito che il datore di lavoro può effettuare dei controlli sui PC del dipendente, a condizione però che:

- Vi sia stata una **previa informativa** al dipendente.
- Venga rispettato l'**art. 11 Codice Privacy**: i dati devono essere trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle finalità perseguite.
- Nel caso di dati sensibili (opinioni religiose, filosofiche, politiche, stato di salute e vita sessuale) sia stato raccolto il **consenso** del dipendente.

Con il secondo provvedimento del **18 maggio 2006** il Garante ha ribadito:

- La necessità di una **previa informativa** al dipendente.
- Il rispetto dell'**art. 11 Codice Privacy**: i dati devono essere trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle finalità perseguite.

A conclusioni analoghe era già giunto il gruppo dei Garanti Europei, che, oltre a sottolineare la necessità della previa informativa, aveva anche distinto due livelli di controllo elettronico sui dipendenti.

IL CONTROLLO DELLA POSTA ELETTRONICA: la situazione sino al marzo 2007

La posta elettronica è equiparata alla posta epistolare e, pertanto, i messaggi via e-mail sono soggetti alle **medesime regole di riservatezza e inviolabilità che tutelano la posta**.

Tale equiparazione è stata espressamente sancita dal d.lgs. 513/97, dalla l. 547/1993 nonché da un parere e da una *Newsletter* del Garante per la Privacy.

Bisogna distinguere due ipotesi:

- **<u>Utilizzo da parte del dipendente di un proprio indirizzo e-mail</u>**:

in questo caso è chiaro che il datore di lavoro non potrà controllare la posta del dipendente, ma potrà contestare l'inadempimento contrattuale da parte del lavoratore (sanzioni disciplinari fino al licenziamento)

- **<u>Utilizzo da parte del dipendente di un indirizzo e-mail aziendale fornito dal datore di lavoro:</u>**

in questa ipotesi la soluzione appare ben più complessa. Da un lato vi è il diritto del datore di lavoro di verificare che il lavoratore non abusi della e-mail:

→Diminuzione produttività;
→Aumento costi aziendali;
→Diffusione materiale interno all'azienda;
→Commissione di reati (pedopornografia, legge diritto autore, etc.)

Dall'altro lato vi è il diritto del lavoratore a veder tutelata la propria sfera personale.

La soluzione deve tener conto di un dato testuale: gli artt. 31-34 Codice della Privacy prevedono espressamente che i dati oggetti di trattamento devono essere **custoditi** in maniera tale da evitare "**accessi non autorizzati**" e "**trattamenti non consentiti**". Inoltre il trattamento dei dati con strumenti elettronici è consentito solo se vengono adottate alcune **misure minime di sicurezza**, tra cui, "protezione degli strumenti elettronici e dei dati" e "copie di sicurezza".

L'allegato B, infine, prevede che vengano impartite istruzioni scritte: a) agli incaricati per non lasciare accessibile lo strumento elettronico; b) per individuare le modalità per assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato.

Tutto ciò sembra confermare il **potere di controllo da parte del datore di lavoro**.

Quanto riportato, dimostra che il datore di lavoro, quale titolare del trattamento dei dati, non ha solo un diritto ma addirittura un dovere di controllo sui dati e sugli strumenti elettronici aziendali. E come tutti i mezzi forniti dal datore di lavoro, rimane nella completa e totale disponibilità del medesimo, senza limitazioni.

Tale soluzione è però in netto contrasto con quanto espresso dal gruppo dei Garanti Europei. Il Gruppo ha infatti ritenuto lecito l'accesso al contenuto della e-mail solo in determinati e specifici casi di controlli difensivi.

In Italia vi è un famoso precedente giurisprudenziale sul punto **(ordinanza del GUP di Milano del 10 maggio 2002**). Il provvedimento del Giudice riguardava il caso di una dipendente che, licenziata a seguito di controlli effettuati sulla propria casella di posta elettronica aziendale, al cui interno erano stati rinvenuti progetti lavorativi estranei all'azienda presso cui lavorava, aveva presentato querela per il reato di cui all'art. 616 c.p.(violazione di corrispondenza).
Successivamente il PM aveva presentato richiesta di archiviazione, cui la lavoratrice aveva fatto opposizione, innestando così il giudizio del GUP.

Quest'ultimo disponeva l'archiviazione del procedimento, rilevando che **la posta elettronica aziendale, quale strumento di lavoro, assolve una funzione aziendale e deve quindi considerarsi accessibile al datore di lavoro**.

Neppure l'utilizzo di uno username e di una password da parte del lavoratore comporterebbe la segretezza dei dati personali dello stesso lavoratore in quanto tali procedure hanno come finalità la protezione dei dati da accessi di persone non autorizzate e, quindi, estranee all'azienda.

Di recente anche il **Tribunale di Torino, sezione distaccata di Chivasso (20 giugno 2006)**, è intervenuto sul punto, stabilendo che "i messaggi inviati tramite l'indirizzo di posta elettronica aziendale del lavoratore rientrano nel normale scambio di corrispondenza che l'impresa intrattiene" e "devono ritenersi relativi a quest'ultima". Ha altresì affermato che "la personalità dell'indirizzo di posta elettronica attribuito ad un dipendente non comporta la segretezza dei messaggi" in quanto l'uso dell'e-mail si sostanzia solo in "un uso di beni aziendali affidati ai dipendenti esclusivamente per ragioni di servizio".

Deliberazione del Garante n. 13 del 1° marzo 2007: **Linee guida per la posta elettronica ed internet**.

Il Garante, dimostrando particolare attenzione al mondo del lavoro e facendo seguito alla deliberazione in tema di trattamento di dati per finalità di lavoro di data 23.11.2006, è nuovamente intervenuto sulla materia con la succitata deliberazione.
Con tale provvedimento il Garante entra nel merito dello spinoso problema dell'uso e dei controlli sugli strumenti elettronici in ambito lavorativo, dettando precise regole da osservare.

Si tratta di un provvedimento reso sulla base dei poteri conferiti al Garante dal codice per la Privacy (art. 154, primo comma, lett. c) e d)).
Evidenzia, già ad una prima lettura, una forte tutela per il lavoratore dipendente, lasciando in secondo piano i diritti e gli interessi del datore di lavoro. Anzi proprio a quest'ultimo sono imposte una serie di attività e di doveri molto pregnanti e con ricadute anche di tipo economico.
Il provvedimento, dopo una parte introduttiva e motivazionale, termina con una parte precettiva. Quest'ultima, in particolare, prevede tre punti fondamentali.

Il primo punto: **LE PRESCRIZIONI**

Il datore di lavoro deve indicare in modo chiaro e particolareggiato quali sono le **modalità corrette di utilizzo** degli strumenti messi a disposizione (posta elettronica ed internet) e se ed in che misura e con quali modalità vengono effettuati dei **controlli**.

Il secondo punto: **LE LINEE GUIDA**

E' opportuno che il datore di lavoro adotti e pubblicizzi un **disciplinare interno (cd. policy)**.

Il datore di lavoro, inoltre, deve adottare delle **misure di tipo organizzativo**:

- per valutare l'impatto sui diritti dei lavoratori;
- per individuare i lavoratori cui è consentito l'accesso a Internet e l'uso dell'e-mail;
- per individuare quale ubicazione è riservata alle postazioni di lavoro.

Il datore di lavoro deve anche adottare delle **misure di tipo tecnologico** per:

Navigazione in Internet:

individuare le categorie di siti correlati con la prestazione lavorativa (black list);

configurare sistemi o utilizzare filtri per prevenire determinate operazioni (opere ingegno);

trattare i dati in forma anonima (log);
eventuale conservazione di dati per il tempo strettamente necessario al perseguimento delle finalità organizzative, produttive e di sicurezza;
graduazione dei controlli.

<u>Utilizzo della posta elettronica:</u>
messa a disposizione di indirizzi e-mail condivisi tra più lavoratori (es. info@nomeazienda oppure indirizzi personalizzati)
eventuale attribuzione al lavoratore di un diverso indirizzo ad uso privato (!?);

messa a disposizione dei lavoratori di funzionalità di sistema che consentano di inviare automaticamente messaggi di risposta in caso di assenza del lavoratore (autoresponder);
consentire, in caso di assenza improvvisa del lavoratore e per improrogabili esigenze lavorative, che il lavoratore deleghi un altro lavoratore (fiduciario [!?]) a leggere l'e-mail e ad inoltrare al lavoratore quelle rilevanti per l'attività lavorativa. Di tale attività deve essere redatto verbale ed informato il lavoratore interessato;

informare i destinatari dell'eventuale natura non personale del messaggio (disclaimer), specificando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
graduazione dei controlli.

Il terzo punto: **I DIVIETI**
E' vietato ai datori di lavoro effettuare trattamenti di dati personali mediante sistemi HW e SW che mirano al controllo a distanza dei lavoratori mediante:
la lettura e la registrazione sistematica dei messaggi di posta elettronica;

la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visitate dal lavoratore;
la lettura e la registrazione dei caratteri inseriti tramite la tastiera;
l'analisi occulta dei portatili affidati in uso.

Vi è un quarto punto, non molto chiaro, che individua i casi nei quali il **trattamento** di dati non sensibili possono essere effettuati anche *senza il consenso* degli interessati:
debbono ricorrere i presupposti di cui all'**art. 4, 2° comma Stat. Lav.** ed il datore di lavoro deve: 1. **esercitare un diritto in sede giudiziaria**; 2. o avere il **consenso**; 3. o vi deve essere un **bilanciamento interessi**.

CONCLUSIONE

Il provvedimento del Garante, seppur opportuno e per certe soluzioni condivisibile (vd. disciplinare interno), sembra essere troppo improntato alla tutela del lavoratore.

Il datore di lavoro deve dare al lavoratore una serie di informazioni che, francamente, appaiono eccessive. Non si comprende, inoltre, la creazione della figura del “fiduciario”. Parimenti inspiegabile il motivo per cui il datore di lavoro dovrebbe mettere a disposizione un indirizzo e-mail privato per il dipendente.

Il datore di lavoro, per contro, appare quasi svilito dei suoi poteri. Ciò comporta, a ben vedere, anche un contrasto con quanto stabilito dallo stesso Codice della Privacy in merito alle misure di sicurezza: il datore di lavoro deve proteggere gli strumenti elettronici (artt. 31-34 Codice Privacy ed Allegato B e, soprattutto, deve rispettare quanto previsto dall'art. 2214, II° comma, c.c.) ma il controllo degli stessi gli è quasi precluso dalla deliberazione n. 13.

L'ultimo aspetto riguarda il valore “normativo” della presente deliberazione: potrà essa avere conseguenze ed influenze sulle future pronunce giurisprudenziali, soprattutto in riferimento alle norme penali?