“ Controlli a distanza sui lavoratori in azienda: I provvedimenti del Garante per la protezione dei dati personali “

Torino, Palazzo di Giustiziam 18 ottobre 2013

Avv. Mauro Alovisio, Fellow Nexa

Presidente Centro Studi di Informatica Giuridica di Ivrea-Torino

Obiettivi e agenda del seminario

- il rapporto fra Statuto dei lavoratori e Codice privacy

- i provvedimenti del Garante privacy in materia di videosorveglianza, internet e posta elettronica sul posto di lavoro

- utilizzo del p.c. aziendale

- cenni su Gps e Rfid negli ambienti di lavoro

- sanzioni e responsabilità

Nexa Center for Internet & Society

Politecnico di Torino

Il Centro Nexa su Internet e Società del Politecnico di Torino (Dipartimento di Automatica e Informatica) fondato nel novembre 2006, è un centro di ricerca indipendente che studia le componenti della forza di Internet e i suoi effetti sulla società.

Il Centro Nexa interagisce con la Commissione europea, organismi regolatori, governi locali e nazionali, nonché con imprese e altre istituzioni - attento a preservare la sua indipendenza accademica e intellettuale e con una specifica attenzione per gli aspetti di policy delle proprie ricerche

Web nexa.polito.it

@nexacenter

facebook.com/nexa.center

Nexa Center for Internet & Society

Politecnico di Torino

Csig di Ivrea-Torino

Il Centro Studi di Informatica Giuridica di Ivrea-Torino è un' **associazione indipendente** senza finalità di lucro **interdisciplinare** (rivolta a giuristi, informatici, etc.) attiva dal 2005

Mission: **aggiornamento professionale**, studio, approfondimento dell'evoluzione dei diritti digitali, dell'ICT e dell'Informatica Giuridica a livello locale e nazionale

Aderisce alla rete nazionale www.cisig.it, alla relativa mailing **list (900 professionisti)**

A livello piemontese: ha due sedi una storica a Ivrea e una a Torino, un blog http://csig-ivrea-torino.blogspot.it/

ed un Comitato Scientifico di magistrati, professori e avvocati

Csig di Ivrea-Torino

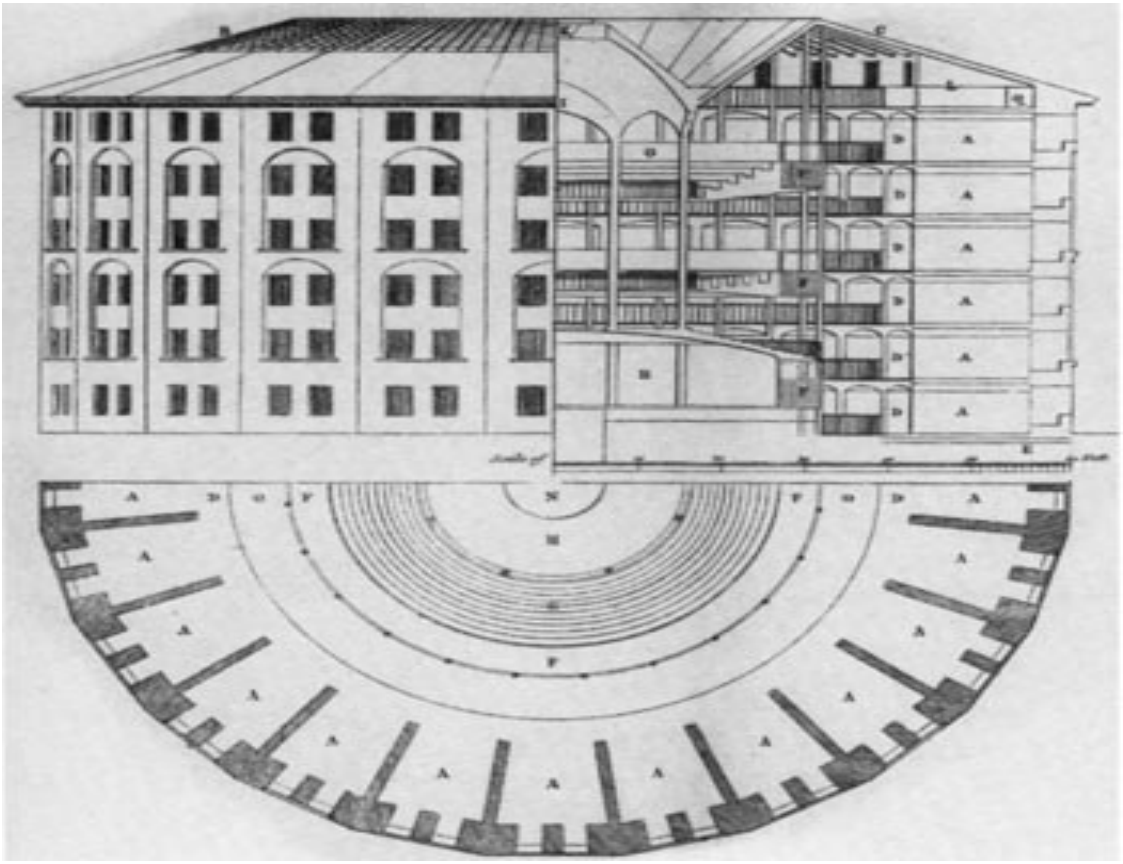
-Partecipazione ai lavori dell'agenda digitale di Torino e alle consultazioni su **mozione software libero e open** data del comune di Torino (Comitato di Torino Digitale)

-Audizione e contributi in Consiglio Regionale (legge sul wi-fi; legge regionale open data in sinergia con Centro di ricerca su Internet Nexa)

-Partecipazione a consultazione nazionale dell'Agenzia Digitale su **smart city,** open data,

-Partecipazione a consultazione del Garante privacy su Tlc e data breach,, partecipazione a tavolo tecnico con Garante sui **cookie** e a consultazione su codice dei giornalisti

Bentham Panopticon, 1791



Che cos’è la privacy?

-“Diritto ad essere lasciati soli” **Right to be let alone** (articolo di Warren e Brandeis, Right to Privacy 1890): diritto alla riservatezza della propria sfera privata, a non subire intrusioni indesiderate nella propria vita intima (**privacy statica)**

evoluzione tecnologica

- Diritto alla protezione dei dati personali: diritto sui propri dati, di controllare la diffusione dell’informazione circa se stessi (**privacy dinamica)**

Convenzione Europea dei Diritti dell'Uomo

Art. 8 "Ogni persona ha diritto al rispetto della sua **vita privata e familiare,** del suo domicilio e della sua corrispondenza

Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non laddove tale ingerenza sia contemplata dalla legge in quanto provvedimento, che in una società democratica, risulti necessario per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui"

Art. 10 " Ogni persona ha diritto alla libertà di espressione"

n.b **vita privata comprende anche il diritto di stabilire e sviluppare relazioni con altri esseri umani, l'attività di natura professionale e commerciale** (caso Niemetiz contro Germania su perquisizione dell'ufficio del ricorrente) (caso Halford contro Regno Unito)

Statuto dei Lavoratori e Codice della Privacy (a)

-**Norme complementari e sovrapponibili**, devono essere rispettate in modo cumulativo in un'ottica di integrazione

- Il rispetto delle disposizioni dell'art. 4 dello Statuto è presupposto di liceità del trattamento di dati personali. Il codice della Privacy si aggiunge alla normativa dello Statuto dei lavoratori

-"La disciplina sulla protezione dei dati personali **non agisce in modo disgiunto** dalla legislazione sul lavoro e viceversa la disciplina e le prassi lavoristiche non operano in modo disgiunto dalla legislazione sul lavoro" Gruppo dei Garanti europei rapporto di coordinamento fra lo Statuto dei lavoratori e Codice della privacy

Statuto dei Lavoratori e Codice della Privacy (b)

Le disposizioni dello statuto dei lavoratori (legge 300 del 1970) trovano applicazione solo nei confronti dei lavoratori subordinati **e non verso anche i lavoratori autonomi** che svolgono attività in qualche modo coordinata con l'organizzazione dell'imprenditore (es. lavoratori a progetti)

-Ruolo strategico del Codice privacy nella tutela della dignità di tutti i lavoratori, i provvedimenti del Garante in materia sui casi **contengono prescrizioni concrete e e sono strumenti giuridici adeguati, flessibili e di messa in sicurezza a garanzia dei lavoratori**

Lo Statuto dei lavoratori e la privacy (c)

L’art. 114 del Codice privacy stabilisce che :

“Resta fermo quanto disposto dall’articolo 4 della legge 20 maggio 1970”

“Le attività di controllo implicano un trattamento di dati che deve svolgersi nel rispetto dei principi di necessità, liceità, finalità e proporzionalità del codice in materia di protezione dei dati personali “

Art. 171 del Codice privacy stabilisce che:

- “ La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300”

Videosorveglianza

- **Tecnica di controllo a distanza** che registra il maggior numero di segnalazioni; ispezioni e verifiche da parte del Garante per la protezione dei dati personali
- 202 segnalazioni e reclami
- 4% del totale degli accertamenti del Garante
- fonte: Relazione Garante per la protezione dei dati personali del 2011
- Settori lavorativi eterogenei:
- alberghi; centri commerciali, call center
- ospedali, case di cura, scuole, aziende di trasporti, enti pubblici

Videosorveglianza

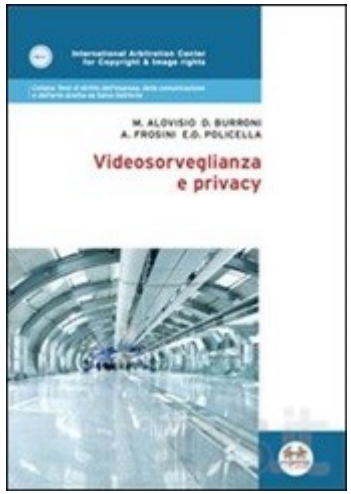
- Principi del Codice privacy (D.Lvo n. 196 del 2003)

- Provvedimento generale del 8 aprile 2010

il precedente provvedimento del 29 aprile 2004

- Il decalogo del 2000

- Normativa di settore



Principi generali

- ✓ Principio di liceità
- ✓ Principio di necessità
- ✓ Principio di proporzionalità
- ✓ Principio di finalità

- Nel caso di mancato rispetto dei sopra citati principi**: il trattamento delle immagini non è lecito, le immagini sono inutilizzabili** (art. 11, comma 2, C.Privacy); sanzioni v. blocco immagini;

Rapporti di lavoro: provv. gen. videosorveglianza del 2010 (a)

- Rapporti di lavoro (punto 4.1) del provvedimento generale del Garante in materia di protezione dei dati personali
- Nelle attività di sorveglianza occorre rispettare il **divieto di controllo a distanza dell'attività lavorativa**, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: **non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza** stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge).

Criticità emerse nelle ispezioni

- Il Garante Privacy ha rilevato nelle ispezioni nel settore lavorativo:
- **violazione delle disposizioni dello Statuto dei lavoratori** (v. relativa trasmissione atti all'autorità giudiziaria)
- carenze di informative privacy semplificate agli interessati della presenza di telecamere (mancanza di trasparenza)
- mancanza di designazione di responsabili ed incaricati al trattamento delle immagini
- definizione di tempi di conservazione eccessivi in violazione del principio di proporzionalità

Videosorveglianza e supermercato

- *Provvedimento del Garante Privacy del 17 gennaio 2013*
- Telecamere ad alta risoluzione, brandeggiabili, con possibilità di effettuare ingrandimenti
- Presenza di accordo sindacale per installazione delle telecamere per finalità di anti-rapina e anti-taccheggio
- Sistema di videosorveglianza integrato –collegamento con addetti esterni, che visionano le immagini sia presso la sala monitor del centro commerciale sia da remoto
- Telecamere che inquadrano il dispositivo di rilevazione delle presenze dei dipendenti

Criticità accordo sindacale

- Il testo dell'accordo sindacale prevedeva che "Le immagini memorizzate sono custodite in un apposito armadio di sicurezza con accesso a doppia chiave (una nella disponibilità del responsabile della sicurezza; una di un rappresentante sindacale aziendale)"
- Il Nucleo ispettivo del Garante ha invece verificato che: l'accesso alle immagini veniva effettuato con modalità diverse da quelle stabilite nell'accordo sindacale, in violazione dei principio di liceità e correttezza del trattamento
- *L'accesso alle immagini era infatti consentito esclusivamente all'azienda esterna che effettuava operazioni di manutenzione all'impianto, previo contattato ed invio password di accesso da parte del responsabile della sicurezza dell'azienda (sistema di videosorveglianza integrato)*

Telecamere negli alberghi (a)

Provvedimento del Garante privacy del 25 ottobre 2012

- Dichiarazione del rappresentante legale dell'albergo: le telecamere non inquadrano direttamente postazioni fisse di lavoro
- Verifica Garante :
- i dipendenti possono in realtà essere ripresi nell'esecuzione delle proprie mansioni dalle telecamere lungo il corridoio di servizio dietro la hall che conduce alla cucina (aree riservate ai dipendenti)

Telecamere negli alberghi (b)

Provvedimento del Garante privacy del 4 ottobre 2011

- il divieto di controllo a distanza dell'attività lavorativa non viene meno dalla circostanza che lo stesso possa essere discontinuo (Cass. 6 marzo 1986, n. 1490)
- Il divieto di controllo a distanza non viene meno dal fatto che i lavoratori siano al corrente dell'esistenza del sistema di videosorveglianza e del suo funzionamento (Cass. 18 febbraio 1983, n. 1236; Cass. Sez.lav. 16 settembre 1997, n. 9211)

Provvedimenti del Garante

Garante privacy, nei casi in esame:

- ha dichiarato illecito il trattamento effettuato a mezzo di sistemi di videosorveglianza

ha disposto il blocco del trattamento dei dati , nell'attesa dell'eventuale espletamento delle procedure previste dall'art. 4 della legge 300 del 1970

ha trasmesso gli atti all'autorità giudiziaria

Obiettivi e agenda del seminario

-il rapporto fra Statuto dei lavoratori e Codice privacy

- i provvedimenti del Garante privacy in materia di videosorveglianza, internet e posta elettronica sul posto di lavoro

- **utilizzo del p.c. aziendale**

- cenni su Gps e Rfid negli ambienti di lavoro

- sanzioni e responsabilità

PC e portatili aziendali, supporti removibili (a)

- *provvedimento del Garante privacy del 18 ottobre 2012*
- - Una società accede ai file contenuti nella cartella personale del dipendente nel corso delle operazioni di salvataggio dei dati **(back up)** sul pc portatile del dipendente, accerta la presenza di file estranei alle attività professionali e di possibile concorrenza sleale
- -L'azienda procede alla contestazione disciplinare-licenziamento del dipendente
- - Il dipendente presenta richiesta art. 7 Codice privacy e successivamente ricorso al Garante per la protezione dei dati personali

PC e portatili aziendali, supporti removibili (b)

Il Garante ha verificato sul campo :

- la policy aziendale in materia di strumenti informatici
- l'informativa privacy al dipendente,
- le istruzioni agli incaricati al trattamento.

-La società non ha fornito un'idonea informativa in ordine al trattamento di dati personali connesso ad eventuali attività di verifica e controllo effettuate dalla società stessa sui p.c.

-Una società non può controllare il contenuto del pc di un dipendente senza averlo prima informato di questa possibilità e senza il pieno rispetto della libertà e della dignità del lavoratore

PC e portatili aziendali, supporti removibili (c)

- Il datore di lavoro può effettuare dei controlli mirati (direttamente o attraverso la propria struttura) al fine di verificare **l'effettivo e corretto adempimento della prestazione lavorativa** e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.)
- nell'esercizio di tale prerogativa, occorre rispettare la **libertà e la dignità dei lavoratori,** nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali, i principi di correttezza, (secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori), di pertinenza e non eccedenza di cui all'art. 11, comma 1, del Codice;
- i controlli possono determinare il trattamento di informazioni personali, anche non pertinenti, o di dati di carattere sensibile;

PC e portatili aziendali, supporti removibili (d)

- Il Garante ha **accolto il ricorso e ha vietato** alla società resistente di trattare ulteriormente i dati oggetto del ricorso a partire dalla data di ricezione del provvedimento del Garante
- La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale. (art. 160, comma 6, del Codice privacy con riferimento alle autonome)

Linee guida del Garante per la protezione dei dati su posta e internet in azienda

-**Deliberazione adottata,** ai sensi dell'art. 154 comma 1 lett. C) del Codice Privacy **dal Garante Privacy il 1 marzo 2007**

-Le linee guida impongono al datore di strutturare i **propri poteri di organizzazione e di direzione** in modo da garantire il corretto utilizzo degli strumenti di lavoro; posta elettronica e rete internet

-contengono prescrizioni di carattere organizzativo, informatico e giuridico rivolte sia

ai datori di lavoro privati e pubblici,

Prescrizioni linee guida

- adozione di **misure disciplinari** adozione e affissione di un disciplinare interno (punto 3.2.)
- adozione di **misure di tipo organizzativo** (punto 5.2.)
- adozione di **misure di tipo tecnologico**

Criteri individuati dal Gruppo dei Garanti europei e ripresi dalle linee guida

- Principi:
- di necessità
- di correttezza
- di legittimità
- di finalità determinate, esplicite
- di proporzionalità
- di cura e conservazione dei dati
- art.11 del Codice privacy nel caso di violazione-inutilizzabilità dei dati

Controlli diretti su internet e posta vietati

Divieto di installare “apparecchiature per finalità di controllo a distanza dell’attività dei lavoratori”

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 di e-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 un uso

Principio di non eccedenza conservazione dei dati

- In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una **finalità specifica e comprovata e limitata al tempo necessario –e predeterminato– a raggiungerla** (v. art. 11, comma 1, lett. e) codice
- Un eventuale **prolungamento dei tempi di conservazione** va valutato come eccezionale e secondo l'Autorità può aver luogo solo in relazione:

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

Internet

- l'individuazione di **categorie di siti considerati correlati** o non correlati con la prestazione lavorativa
- la configurazione di sistemi o l'utilizzo di **filtr**i che prevengano determinate operazioni
- **trattamento di dati in forma anonima** o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni
- l'eventuale **conservazione di dati** per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza
- la graduazione dei controlli (punto 6.1.)

Posta elettronica Soluzioni possibili

Il Garante suggerisce al datore due ipotesi:

1) disponibilità di un **indirizzo di posta elettronica aziendale** condivisa tra più lavoratori (es. ufficio vendite@nome azienda.it) affiancata eventualmente da un indirizzo individuale (m.rossi@ente.it)

2) disponibilità di **un indirizzo di posta elettronica aziendale + possibilità di e- mail** con diverso indirizzo destinato ad uso privato del lavoratore

Oneri specifici del datore

1) adottare e pubblicizzare il "**disciplinare tecnico"** che regolamenti:

-**Uso dei mezzi** (internet e posta elettronica)

-**Controlli**

2) dovere di **informare** i dipendenti ai sensi dell'art 13 del codice privacy

1+2 = Circolo virtuoso

Disciplinare aziendale contenuto (1)

- **Comportamenti non consentiti** (ad es., il download di software di i files musicali, conservazione di files personali)
- **Utilizzo personale** della posta elettronica (uso della webmail)
- **File di log** eventualmente registrati e diritti di accesso
- **Tempi e modalità di conservazione** delle informazioni (back up)

Disciplinare contenuto (2)

- indicare le **ragioni** legittime –specifiche e non generiche– (es. per verifiche sulla funzionalità e sicurezza del sistema) dei **controlli**
- 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)
- **conseguenze,** anche di tipo disciplinare
- **divieto** di controlli prolungati, costanti o indiscriminati

Disciplinare contenuto (3)

- Il disciplinare interno deve essere adottato, laddove ne ricorrano i presupposti, rispettando le previsioni **dell'art. 4 dello Statuto dei Lavoratori:**

  a) Informazione, concertazione, consultazione delle **Organizzazioni Sindacali**

  b) in caso di mancato accordo: **Ricorso al servizio ispettivo della DPL**

Informativa dei dipendenti

gli interessati hanno il diritto di essere informati preventivamente, e in modo chiaro

- sui **trattamenti di dati** che possono riguardarli (dati su internet, posta elettronica)
- sull'eventualità dei **controlli**
- indicazione del soggetto o unità al quale rivolgersi per **l'esercizio dei diritti privacy**
- indicazione della **finalità del controllo** (specifiche esigenze organizzative, produttive e di sicurezza del lavoro (art. 4 dello statuto) possono riguardare anche l'esercizio di un diritto in sede giudiziaria

Principio di pertinenza graduazione dei controlli

- la **graduazione dei controlli**
- **-** attraverso 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 ad un rilevato utilizzo anomalo degli strumenti aziendali 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.**

Caso accesso a siti porno in azienda (a)

- Provvedimento del Garante della Privacy del 14 febbraio 2006 su lavoratore che naviga in internet
- Un dipendente di un casa di cura presenta ricorso al Garante contro il datore di lavoro che aveva contestato la navigazione in siti Internet a contenuto religioso, politico e **pornografico,** durante l'orario di lavoro attraverso una lettera con elenco dettagliato dei siti in oggetto.
- Il provvedimento afferma il diritto del datore di lavoro a controllare il corretto utilizzo di internet ma senza indagare sui contenuti dei siti (da cui si possono dedurre dati sensibili, idonei a rilevare orientamento politico, adesione a sindacati e tendenze sessuali esempio: siti di partiti politici o sindacati)

Accesso a siti porno in azienda (b)

Ricorso dell'azienda contro il provvedimento del Garante privacy

-Tribunale di Palermo (sentenza del 26.6.2008)

-Corte di Cassazione sentenza del 19 giugno- 1 agosto 2013 n. 18443 hanno l'orientamento del Garante privacy

-illegittimo il trattamento dei dati posto in essere da un'azienda che, nell'operare, dapprima una contestazione disciplinare, e poi l'intimazione del licenziamento, ai danni di un proprio dipendente, ha documentato il contenuto degli accessi ai siti internet, non autorizzati, e compiuti dal medesimo durante l'orario di lavoro.

Accesso a siti porno in azienda (c)

- «la società ricorrente avrebbe potuto dimostrare l'illiceità della condotta del prestatore, "in rapporto al corretto uso degli strumenti affidati sul luogo di lavoro", limitandosi a dar prova **degli accessi indebiti ad internet e i relativi tempi di collegamento, attraverso una modalità differente da quella nei fatti utilizzata.**
- Secondo la Corte, la società ha posto in essere "un trattamento diffuso di numerose altre informazioni indicative anche degli specifici contenuti degli accessi dei singoli siti web visitati […], operando […] un trattamento di dati eccedente rispetto alle finalità perseguite […]".
- La società ha operato in modo non trasparente

Accesso a siti porno in azienda (d)

- Garante privacy
- «Il trattamento di dati sensibili relativi allo stato di salute e alla vita sessuale può essere fatto senza consenso solo per far valere o difendere in giudizio un diritto di rango pari a quello dell'interessato ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile. Anche tale circostanza non ricorre nel caso di specie, nel quale sono stati fatti valere solo diritti legati allo svolgimento del rapporto di lavoro (cfr. art. 26, comma 4, lett. c), del Codice; punto 3, lett. d), della autorizzazione; cfr. Provv. Garante 9 luglio 2003)» .

Accesso a siti porno in azienda (d)

la società ha operato - «**in modo peraltro non trasparente un trattamento di dati eccedente rispetto alle finalità perseguite**, tenuto conto che, sebbene i dati personali siano stati raccolti nell'ambito di controlli informatici volti a verificare l'esistenza di un comportamento illecito, le informazioni di natura sensibile possono essere trattate dal datore di lavoro senza il consenso **quando il trattamento necessario per far valere o difendere un diritto in sede giudiziaria sia "indispensabile"** e tale indispensabilità, non ricorre nel caso di specie»

Telefono e cellulare aziendale (a)

- controllo aziendale- rispetto art. 4 Statuto e del Codice privacy
- dati delle telefonate: contenuti, data, durata, numeri composti destinatari (art. 8 della convenzione europea dei diritti dell'uomo) - sentenza della Corte dei Diritti dell'Uomo, Case of Copland/The united Kingdom del 3 aprile 2007
- casi concreti della giurisprudenza diritto del lavoro:
- legittimi i controlli del datore di lavoro diretti ad accertare le condotte illecite dei dipendenti attraverso gli apparecchi di rilevazione di telefonate ingiustificate (Cass. 3 aprile 2002, n. 4746) – caso della guardia giurata
- legittimo il licenziamento di dipendente per abuso di cellulare aziendale per ragioni estranee al lavoro (Cass. 9 luglio 2007, n. 15334)

Telefono e cellulare aziendale (b)

l'installazione di software Blue's 2002 di controllo delle telefonate dei lavoratori in assenza di accordo sindacale costituisce violazione dell'art. 4 dello Statuto (Trib. Milano 30 marzo 2006; Tribunale di Cagliari decreto 3 del 15 marzo 2011)

- Ministero del lavoro risposta interpello del 6 giugno 2006 per installazione di sistemi di controllo telefonate su singole utenze occorre una rigorosa verifica caso per caso se tale controllo implichi un controllo indiretto sull'attività lavorativa dei dipendenti (es. casi di attività di telemarketing) con conseguente applicazione del secondo comma dell'art. 4 Stat.

Obiettivi e agenda del seminario

- il rapporto fra Statuto dei lavoratori e Codice privacy

- i provvedimenti del Garante privacy in materia di videosorveglianza, internet e posta elettronica sul posto di lavoro

- utilizzo del p.c. aziendale

- cenni su **Gps** e Rfid negli ambienti di lavoro

- sanzioni e responsabilità

Gps

-illustrare il rapporto fra i sistemi Gps e dati

- prescrizioni e misure previsti dal provvedimento generale del Garante del 2011: informativa; scelta delle tipologie dei dati, definizione della durata di conservazione dei dati, designazione responsabile

- notificazione e verifica preliminare

- casi concreti e applicazione dei Gps in ambito lavorativo

Sistemi di Gps e i dati

-L’utilizzo di sistemi di Gps determina un **trattamento di dati personali** in quanto i dati relativi all’ubicazione dei veicoli consente di acquisire, archiviare informazioni personali che si riferiscono, seppur solo in modo indiretto, **ai lavoratori** assegnatari dei veicoli(Cfr. WP nr. 4/2007; n. 5/2005 del Gruppo dei Garanti europei):n questa materia trova cosi **applicazione il codice privacy**

-Il Garante privacy in data 4 ottobre 2011ha emanato , ai sensi degli artt. 154, lett. c) e 162, comma 2-t un **provvedimento generale**, ad oggetto: “*Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro “* in cui definisce **regole, misure e adempimenti**

Provvedimento del Garante del 2011

-**ambito**: utilizzo di GPS per **finalità organizzative, produttive oppure per la sicurezza nell'ambito del rapporto di lavoro**.
-Il provvedimento in esame è **di bilanciamento degli interessi**
-non sé necessario per il datore di lavoro titolare del trattamento, raccogliere il consenso dei soggetti interessati (esimente del consenso ai sensi dell''art. 24, comma 1 lett. g) del D.lgs. 196/2003)
-si ribadisce **l'obbligo di adempiere all'art. 4, comma 2, della Legge 300/1970,**

Finalità

L'uso del GPS è lecito per soddisfare:
- esigenze organizzative e produttive ovvero per la sicurezza del lavoro, per esigenze logistiche (consente di impartire tempestive istruzioni al conducente del veicolo oggetto di localizzazione);
-**per elaborare rapporti di guida** allo scopo di commisurare il tempo di lavoro del conducente con la conseguente determinazione della retribuzione dovuta dell'adempimento degli obblighi previsti dal D.M. del 9 luglio 2008 recante norme in materia di "*Modalità di tenuta e conservazione del libro unico del lavoro e disciplina del relativo regime transitorio"*
ovvero per commisurare i costi da imputare alla clientela, nonché **per assicurare una più efficiente gestione e manutenzione del parco veicoli,** con effetti vantaggiosi anche **sulla sicurezza sul lavoro e per la sicurezza della collettività.**

Principi di pertinenza e non eccedenza

Il provvedimento ha il merito di individuare alla luce delle finalità lecite ammesse, solo i **seguenti dati pertinenti e non eccedenti** che, secondo il Garante privacy possono essere trattati:

- **ubicazione del veicolo;**
- **distanza percorsa;**
- **tempi di percorrenza;**
- **carburante consumato**;
- **velocità media del veicolo** (no dati su frenate)

La posizione del veicolo non dovrebbe, nel rispetto del principio di necessità, essere monitorata continuativamente dal titolare (*divieto di monitoraggio continuo)*

La conservazione dei dati (a)

Il provvedimento richiama i principi generali previsti dall'art. 11 del Codice privacy : i **tempi di conservazione delle diverse tipologie di dati eventualmente trattati devono essere commisurati tenendo conto di ciascuna delle finalità in concreto perseguite**

Finalità connesse alla prestazione contrattuale, i dati devono essere anonimizzati o cancellati successivamente all'esecuzione del contratto.

La conservazione dei dati (b)

-finalità connesse agli adempimenti previsti all'art. 6 DM 9 luglio 2008 “Libro unico”
La conservazione dei dati per **il periodo di cinque anni limitatamente alle informazioni da annotare** ai sensi dell'art. 39, d.l. 25 giugno 2008, n. 112 (convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 6 agosto 2008, n. 133), con particolare riferimento ai dati dei lavoratori relativi alle presenze nonché ai tempi di lavoro, anche straordinario, e di riposo (cfr. anche art. 8, d.lg. 19 novembre 2007, n. 234 come modificato dall'art. 40, comma 3, d.l. n. 112/2008 nonché la risposta al quesito n. 20 resa dal Ministero del lavoro e delle politiche sociali nel Vademecum sul libro unico del lavoro).

Oneri per il datore di lavoro

Il datore di lavoro deve definire:
- le **tipologie di dati** da trattare nel rispetto dei principi di pertinenza e non eccedenza
- **differenti periodi di conservazione dei dati** a seconda delle finalità del sistema

Attenzione: nel caso di violazione del principio di pertinenza e non eccedenza e di durata, l'impresa potrà essere sanzionata con la pena da euro **30.000 ad euro 180.000** (v. art. 162, comma 2 ter, art. 154, comma 1 lett. c.)

Informativa

Il Garante privacy ha previsto, nel provvedimento, l'obbligo:
- di fornire una completa informativa ai dipendenti sull'installazione di un sistema di geolocalizzazione sul veicolo
-fonire unitamente a **ragguagli sulla natura dei dati e sulle caratteristiche del sistema Gps** utilizzato dall'impresa
I datori di lavoro sono tenuti ad apporre all'interno dei veicoli vetrofanieche con la dicitura "*Veicolo sottoposto a geolocalizzazione"* o, comunque, avvisi chiari e visibili che segnalino la possibilità di procedere alla geolocalizzazione del veicolo. Al fine di agevolare questo obbligo il Garante privacy ha predisposto **uno specifico facsimile** allegato al provvedimento

Responsabili

I sistemi di geolocalizzazione sono usualmente gestiti da soggetti **terzi, società esterne** che forniscono all'azienda servizi di localizzazione e trasmissione dei dati

Il provvedimento prescrive espressamente **la designazione obbligatoria di tali società** quali responsabili esterni del trattamento ai sensi dell'art. 29 del Codice della Privacy

I titolari del trattamento sono tenuti ad impartire alla società esterne le necessarie **istruzioni** in ordine all'utilizzo legittimo dei dati raccolti per le sole finalità previste dall'accordo che regola la fornitura del servizio di localizzazione,e a determinare altresì le tipologie di dati da trattare nonché le modalità e i tempi della loro eventuale conservazioni.

Incaricati

I titolare del trattamento sono tenuti a designare, ai sensi dell’art. 30 del Codice, **gli incaricati al trattamento** del Codice privacy tutti i dipendenti (ma anche collaboratori) che, per motivi lavorativi hanno necessità di accedere ai dati raccolti per il tramite del sistema di GPS (es. personale incaricato di gestire la logistica, i servizi di magazzino e di manutenzione del parco veicoli, ovvero quello operante nell'ambito della gestione delle risorse umane).

Notificazione e verifica preliminare

Notificazione: il Garante conferma l'obbligo di procedere alla **notificazione preventiva telematica** allo stesso del sistema di geolocalizzazione (art. 34 del Codice della privacy)

Interpello: i **sistemi non conformi al provvedimento generale devono essere sottoposti ad una verifica** preliminare da parte dello stesso Garante Privacy, mediante la presentazione di un atto di interpello

La Radio Frequency Identification (RFID)

- La tecnologia RFID richiede l'utilizzo
- - di un "**tag",** ossia un **circuito elettronico** miniaturizzato che contiene memorizzate alcune informazioni ed è unito ad un'**antenna** in grado di comunicare queste informazioni attraverso onde radio;
- un lettore (dotato a sua volta di un'antenna di trasmissione/ricezione);
- un decodificatore che traduce i dati in entrata in dati digitali potenzialmente trattabili da un computer.

Rfid e provvedimenti

-WP art. 29 parere n. 105 del 19 Gennaio 2005

-**Provvedimento del Garante italiano del 2005** dedicato all'analisi della tecnologia RFID, che riprende e sviluppa le linee del Parere del WP 29

-Consultazione pubblica promossa da WP art. 29

Provvedimento del Garante del 2005 (a)

Principio di necessità (art. 3 del Codice)
I sistemi di RFID devono essere configurati in modo tale da evitare l'utilizzazione di dati personali oppure, a seconda dei casi, l'identificabilità degli interessati, quando non siano strettamente necessarie in relazione alla finalità perseguita.
• **Liceità** (art. 11, comma 1, lett. a), del Codice)
In ambito lavorativo, l'uso di tecniche RFID deve in particolare rispettare il divieto di controllo a distanza del lavoratore (art. 4 l. 20 maggio 1970, n. 300; art. 114 del Codice)
-**Finalità e qualità dei dati**
-proporzionalità (es. rfid attivo fuori dal supermercato)

Informativa privacy e diritti sui dati (a)

L'informativa privacy attraverso **appositi avvisi agevolmente visionabili** nei luoghi in cui le tecniche RFID sono adoperate, con un formato ed un posizionamento tale da risultare chiaramente visibile e **un'idonea informativa** sugli oggetti o sui prodotti recanti le "etichette intelligenti", qualora le stesse rimangano attive dopo che è stato reso possibile associarle con dati relativi a terzi identificati o identificabili, in particolare al di fuori dei luoghi (ad esempio esercizi commerciali) in cui si fa uso della RFID.
Esercizio sui diritti sui dati (art. 7)con modalità semplificate in fase di progettazione

Disattivazione etichetta

All'interessato deve essere riconosciuta la possibilità di **ottenere, gratuitamente e in maniera agevole, la rimozione o la disattivazione delle etichette RFID** al momento dell'acquisto del prodotto su cui è apposta l'etichetta o al termine dell'utilizzo del dispositivo.
Le etichette devono essere posizionate in modo tale da risultare, per quanto possibile, facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto o dell'oggetto a cui si riferiscono (ad esempio, disponendone la collocazione sulla sola confezione).

Etichette Rfid e art. 4 Statuto

-utilizzo in ambito lavorativo di Rfid

se il tag è passivo e non trasmette dati non abbiamo problemi di applicazione dell'art. 4 dello statuto
se il tag è attivo e trasmette dati , consente di identificare il lavoratore e monitorare tutti i movimenti scatta l'art. 4 dello Statuto sia divieto del primo comma (es. stazione ricevente nascosta) sia procedura codeterminativa del secondo comma (installazione Rfid per finalità di sicurezza: no duplicazione di badge, identificazione dipendenti in luoghi pericolosi come miniere, cantieri, in caso di incidenti

Caso concreto Rfid e lavoro (a)

- Caso di **ricorso** presentato al Garante da un lavoratore per l'introduzione in azienda di "un nuovo sistema di rilevamento delle presenze a radiofrequenza (RFID)" in cui i dati raccolti erano relativi all'entrata o all'uscita dei lavoratori, attraverso l'accostamento del badge al lettore.,
il Garante (v. provvedimento del 1 marzo del 2012) ha verificato che:
- il datore di lavoro **aveva informato i dipendenti** dell'introduzione del nuovo sistema di rilevamento delle presenze mediante affissione in bacheca della descrizione della nuova modalità;

Caso concreto Rfid e lavoro (b)

Il Garante ha verificato che la timbratura con terminali a prossimità rileva le sole informazioni pertinenti e non eccedenti, ossia il codice del cartellino e l'orario di ingresso e di uscita, né più e né meno di quanto non faccia un sistema a timbratura per la verifica dell'esatto adempimento della prestazione, la commisurazione dell'importo della retribuzione, anche per lavoro straordinario, o dei premi da corrispondere, la quantificazione di ferie e permessi;

Caso concreto RFID e lavoro (c)

- la lettura del dispositivo necessita una **distanza minima tra il badge e il lettore,** oltre la quale non è possibile rilevare il movimento di entrata o uscita del dipendente e lo stesso conferma la transazione mediante un suono e la visualizzazione a display di una risposta scritta.

Caso concreto (d)

- L'Autorità ha concluso che il trattamento dei dati così effettuato **non risulta violare la legge perché non raccoglie dati personali eccedenti rispetto alle finalità di gestione** del rapporto di lavoro, essendo raccolti esclusivamente i dati relativi all’entrata o all’uscita del lavoratore attraverso l’accostamento del badge al lettore, il quale segnala, in modo evidente, la registrazione dei dati medesimi ed evita pertanto la raccolta di dati all’insaputa del lavoratore

Sanzioni e responsabilità

Il mancato rispetto delle prescrizioni contenute nel provvedimento in esame determina l'applicazione di **sanzioni pecuniarie amministrative**: pagamento di una somma da **trentamila euro a centottantamila euro**

(art.162, comma 2-ter, del Codice della privacy)

Obiettivi e agenda del seminario

- il rapporto fra Statuto dei lavoratori e Codice privacy

- i provvedimenti del Garante privacy in materia di videosorveglianza, internet e posta elettronica sul posto di lavoro

- utilizzo del p.c. aziendale

- cenni su Gps e Rfid negli ambienti di lavoro

- **sanzioni e responsabilità**

Responsabilità trattamento dati

- responsabilità amministrativa
art. 161-166

- responsabilità civile
art. 15

- responsabilità penale
art. 167-172

Responsabilità amministrativa
Sanzioni privacy

- ambito di applicazione: trattamento dati personali in **ambito pubblico e in ambito privato**

-costerà caro alle aziende non rispettare la normativa privacy

- Omessa ed inidonea informativa

-Illegittima cessione di dati

-Illegittima comunicazione di dati sanitari

-Omessa ed incompleta notificazione

-Omessa informazione o esibizione al Garante

-Violazione misure minime

Omessa o inidonea informativa (a)

Sensibile inasprimento della sanzione (art. 161)

-prima del decreto importi dal minimo di 3.000 euro a 18.000 ; 5.000 a 36.000 per dati sensibili

-dopo decreto un sensibile dal minimo di **6.000** euro a **36.000**

il decreto prevede che gli importi possono raddoppiare in caso di violazione di maggiore gravità o quadruplicare se la sanzione può risultare inefficace in ragione delle **condizioni economiche del contravventore.** (esempio grandi aziende / enti pubblici).

Violazione di divieti o prescrizioni del Garante

Nelle ipotesi **di violazione dei provvedimenti di prescrizione del Garante** di misure necessarie o divieti adottati, ai sensi dell'art. 154, comma 1, lett.c) o d) dal garante privacy (v.art.142 codice)

Sanzione da **30.000 a 180.000** euro

Esempi : linee guida internet e posta elettronica del 1 marzo 2007; provvedimento videosorveglianza del 29 aprile 2004; provvedimento amministratore di sistema del 27 novembre 2008

Responsabilità civile (I)

- art. 15 del codice Danni cagionati per effetto del trattamento

"*Chiunque cagiona danno ad altri per effetto del trattamento di dati è tenuto al risarcimento ai sensi dell'art. 2050 c.c.*"

Il danno non patrimoniale *è risarcibile anche in caso di violazione dell'art. 11 del Codice (Modalità del trattamento)*

Responsabilità civile (II)

art 2050 c.c. : **Responsabilità per l'esercizio di attività pericolose "** *Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno*"

- inversione onere della prova
- prova positiva di avere adottato tutte le misure di prevenzione
- casi di giurisprudenza su attività pericolosa attività edilizia, produzione e distribuzione di energia

Sanzioni penali

- **Trattamento illecito di dati personali** da parte di soggetti pubblici (salvo che il fatto non costituisca più grave reato) Se ne deriva un danno:fine è quello di trarre per sé o altri profitto o di recare ad altri un danno.

Sanzioni previste: Reclusione da 6 a 18 mesi; 24 mesi (vedi diffusione e comunicazione)

Art. 167, comma 1 del Codice

Falsità nelle dichiarazioni e notificazioni

1. Chiunque, nelle comunicazioni e nella notificazione di cui all'articolo 37 o in comunicazioni, atti,
-documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti,
dichiara o attesta falsamente notizie o circostanze
o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, **con la reclusione**
- da sei mesi a tre anni. (art. 168 codice della Privacy)

Per approfondimenti

Alovisio M., Privacy nel rapporto di lavoro in Russo C, Carbone L. Formulario del lavoro. Contratti, sicurezza e privacy, Utet, 2008

Alovisio M, .Burroni D., Frosini A., Policella E.O., «Videosorveglianza e privacy», Experta, 2011

Favalli G., Stanchi A., Favalli, «Privacy e lavoro Il nuovo Testo Unico sulla privacy e la disciplina del rapporto di lavoro» Etas, 2004

Grazie per l’attenzione!!!

Avv. Mauro Alovisio

blog in materia di privacy

http://www.serviziweb.unito.it/blog/?area=Blog&action=ReadForm&id=40524

slide edite creative commons 2.5 no commercial

mauro.alovisio@gmail.com