Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 6.1.1.

Principii generali in materia di privacy e controllo dei lavoratori

Avv. Michele Gallucci

I riferimenti normativi di carattere generale

Prima di accennare a quelle che sono le norme di legge fondamentali di riferimento specifico al potere datoriale di controllo su accessi e presenze, occorre citare due norme di legge a carattere generale, contenute nel Codice Civile:

- **Articolo 2086 Codice Civile → *«l'imprenditore è capo dell'impresa e da lui dipendono gerarchicamente i suoi collaboratori»***
- **Articolo 2087 Codice Civile → *«l'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro».***

I riferimenti normativi di carattere speciale sul controllo del datore di lavoro sui propri dipendenti.

L'art. 4 dello Statuto dei Lavoratori – Legge n° 300/1970 – prima dell'entrata in vigore dell'art. 23 comma 1, D.Lgs. n° 151/2015 (Jobs Act) – disponeva espressamente in materia di impianti audiovisivi e controllo a distanza dei lavoratori quanto segue:

«è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. 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, dettando, ove occorra, le modalità per l'uso di tali impianti. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali o con la commissione interna, l'ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti. Contro i provvedimenti dell'ispettorato del lavoro, di cui ai precedenti commi, il datore di lavoro, le rappresentanze sindacali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro trenta giorni dalla comunicazione del provvedimento al Ministero per il lavoro e la previdenza sociale.

La modifica all'art. 4 dello Statuto dei Lavoratori

Con la modifica dell'art. 4 legge n° 300/1970 attuata con l'art. 23, comma 1, del Decreto Legislativo n° 151/2015, il legislatore, alla luce dei mutamenti organizzativi apportati all'uso delle tecnologie telematiche (personal computer; tablets, smartphone, badge ecc.) ha cercato di aggiornare le modalità per il loro uso legittimo, chiarendo in particolare che la necessità di un preventivo accordo sindacale (o in mancanza di questo, della preventiva autorizzazione dell'Ispettorato del Lavoro) non sussiste per gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

ARTICOLO 4 Legge 20 maggio 1970 n° 300 – riformato dall'art. 23 del D.Lgs. n° 151/2015
«Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo comma possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.

La modifica all'art. 4 dello Statuto dei Lavoratori

Il decreto legislativo n° 151/2015 con la modifica apportata all'art. 4 dello Statuto dei Lavoratori nel disciplinare la materia dei controlli a distanza del datore di lavoro sul dipendente ha stabilito un regime diverso a seconda del tipo di strumento adottato:

- **strumenti che consentono il controllo dei lavoratori (ad esempio: videosorveglianza);**
- **strumenti di lavoro (personal computer, smartphone, tablets).**

principio generale → **L'installazione di impianti audiovisivi e di altri strumenti dai quali deriva anche la possibilità di controllo a distanza dell'attività dei lavoratori è di norma vietata.**

Impiego di tali strumenti alla presenza delle seguenti condizioni

- **Esigenze organizzative, produttive, di sicurezza del lavoro e tutela del patrimonio aziendale**
- **preventivo accordo sindacale**

La novità della riforma dell'art. 4 dello Statuto dei Lavoratori

La novità della riforma apportata con il Decreto Legislativo n° 115/2015 all'art. 4 dello Statuto dei Lavoratori è data dal secondo comma della disposizione in commento il quale prevede che: *«le garanzie non si applicano agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. In tali casi l'installazione non richiede alcun accordo sindacale. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità di uso degli strumenti e di effettuazione dei controlli nel rispetto di quanto disposto dal D.Lgs. n° 196/2003.*

TIPOLOGIA DEGLI STRUMENTI DI REGISTRAZIONE DEGLI ACCESSI E DELLE PRESENZE.
L'accesso delle persone, siano esse lavoratori o terzi, ai locali aziendali e la loro presenza negli stessi costituiscono aspetti importanti sotto vari punti di vista, legati:

- **alla sicurezza intesa come tutela del patrimonio aziendale (security);**
- **alla sicurezza del lavoro (safety);**
- **all'obbligo di calcolare l'orario di lavoro ai fini retributivi;**
- **al rispetto dei limiti previsti dalla legge e dalla contrattazione collettiva in materia di orario di lavoro;**
- **al rispetto delle normative aziendali in materia di orario di lavoro, ai fini disciplinari.**

Controllo accessi

Badge
Smartphone
Sistemi di rilevazione antropobiometrici (impronte digitali, scansione dell'iride biometria facciale)

La posizione del Garante della Privacy

In materia di controllo tecnologico dei lavoratori vanno tenute presenti alcuni provvedimenti adottati dal Garante della Privacy, quali:

- **Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro del 14 giugno 2007;**
- **Provvedimento del 16 marzo 2017;**
- **Provvedimento del 16 febbraio 2017;**
- **Provvedimento del 15 settembre 2016 e 15 marzo 2016;**
- **Provvedimento 8 settembre 2016**

L'art. 88 del Regolamento GDPR

L'art. 88 del Regolamento GDPR n° 679/2016 stabilisce che gli Stati possono emanare regole particolari atte a garantire la protezione dei diritti e delle libertà dei dipendenti durante i trattamenti dei dati nel contesto del rapporto di lavoro. Questo può avvenire tramite accordi collettivi o disposizioni legislative. Il GDPR prevede, quindi, che le attività di controllo dei lavoratori siano svolte in un contesto di trasparenza e di adeguata protezione dei dati personali. Il controllo del datore di lavoro e, in genere il trattamento di dati del lavoratore, può, infatti, avvenire in una molteplicità di fasi: valutazione dei candidati e assunzione, valutazione delle prestazioni lavorative, pianificazione ed organizzazione delle prestazioni lavorative, di salute e sicurezza dell'ambiente di lavoro, protezione dei beni del dipendente, conclusione del rapporto di lavoro.

Casi pratici individuati dal WP29

- **Trattamento dei dati dei candidati pubblicati sui social network;**
- **Trattamento dei dati dei lavoratori pubblicati sui social network;**
- **Monitoraggio della strumentazione informatica dei lavoratori;**
- **Rilevazione della presenza dei lavoratori;**
- **Trattamenti di dati mediante sistemi di videosorveglianza;**
- **Geolocalizzazione dei veicoli;**
- **Trasferimento dei dati personali dei lavoratori a terzi.**

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Moduli 6.1.2. – 6.1.3.

Videosorveglianza e altri sistemi di potenziale controllo

La giurisprudenza dei Tribunali italiani e del Garante Privacy

Avv. Michele Gallucci

La videosorveglianza come strumento di controllo – riferimenti normativi.

L'uso di telecamere di sorveglianza per controllare il personale è contro le disposizioni di legge – riferimento alla legge 300/1970 art. 4, così come modificato dall'art. 23 del D.Lgs. n° 151/2015 e del Codice Privacy (nella sua previsione originaria D.Lgs. n° 196/2003)

Art. 4 dello Statuto dei Lavoratori – Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.

III COMMA – deroga introdotta dalla disposizione di cui all'art. 23 D.Lgs. n° 151/2015 – La disposizione di cui al primo comma non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

I provvedimenti del Garante della Privacy sulla materia della videosorveglianza.

L'Autorità Garante per la protezione dei dati personali ha adottato un Provvedimento in materia di videosorveglianza (Provvedimento 8 aprile 2010 – pubblicato in G.U. n° 99 del 28 aprile 2010) nel quale ha chiarito che nel contesto dei rapporti di lavoro debbano essere comunque rispettate tutte le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro, previo accordo collettivo sindacale o, in alternativa, tramite provvedimento autorizzativo ministeriale e comunque previa adeguata informativa.

Gli interventi della giurisprudenza di legittimità

Corte di Cassazione Sezione Terza Penale sentenza del 30 gennaio 2014 n° 4331 si è stabilito il seguente principio di diritto: «l'installazione di una telecamera sul posto di lavoro diretta verso il luogo in cui i propri dipendenti svolgono le proprie mansioni o su spazi dove essi hanno accesso anche sporadicamente deve essere preventivamente autorizzata dall'Ispettorato del Lavoro o deve essere autorizzata da un particolare accordo con i sindacati».

Corte di Cassazione Sezione Terza Penale sentenza del 17 aprile 2012 n° 22611 si è stabilito il seguente principio di diritto ossia ha introdotto l'esimente del valido consenso dei prestatori di lavoro: «quale ulteriore condizione di liceità del trattamento dei dati personali relativi all'utilizzo dei sistemi di videosorveglianza vi deve esserci il consenso espressamente prestato da tutti i lavoratori e non solo da parte del titolare del bene protetto (diretto interessato)».

A conclusioni diametralmente opposte è giunta la pronuncia della Corte di Cassazione, Sezione Terza Penale con la sentenza del 8 maggio 2017 n° 22148 negando l'efficacia scriminante del consenso acquisito dalla totalità dei lavoratori e richiamando proprio il concetto del bene giuridico protetto dalla norma penale in esame (art. 171 del previgente Codice Privacy) ossia la tutela non solo di posizioni giuridiche individuali bensì anche di interessi di carattere collettivo, quale la tutela della dignità dei lavoratori sul luogo di lavoro durante lo svolgimento della prestazione lavorativa, cui sono titolari ex lege proprio le rappresentanze sindacali il cui intervento è espressamente previsto.

Gli interventi della giurisprudenza di legittimità

Corte di Cassazione, Sezione Terza Penale, sentenza del 26 ottobre 2016 n° 45198 ha stabilito che è reato la predisposizione, da parte del datore di lavoro, di apparecchiature idonee, nella specie telecamere, a controllare a distanza l'attività dei lavoratori e per la sua punibilità non è richiesta la messa in funzione o il concreto utilizzo delle attrezzature essendo sufficiente l'idoneità al controllo a distanza dei lavoratori e la sola installazione dell'impianto.

La Corte di Cassazione Sezione Lavoro con la sentenza del 5 ottobre 2016, n° 19922 ha stabilito che i dati dell'impianto GPS di controllo a distanza non possono essere utilizzati per provare l'inadempimento contrattuale del lavoratore e risulta illegittimo il provvedimento disciplinare di licenziamento. Il datore di lavoro non ha la possibilità di controllare (a distanza) i propri dipendenti mediante l'apparecchiatura GPS, in quanto trattasi di sistema di controllo generalizzato predisposto prima ancora dell'emergere di ogni e qualsiasi sospetto. Da ciò ne consegue che il datore non può utilizzarlo ai fini dei c.d. controlli difensivi al fine di verificare la violazione degli obblighi contrattuali.

Gli interventi dell'Ispettorato del Lavoro

Con circolare n° 5 del 19 febbraio 2018, avente ad oggetto *«indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della legge n° 300/1970»,* l'Ispettorato Nazionale del Lavoro fornisce una serie di indicazioni operative che mirano, sulla scia dei più o meno recenti interventi normativi in materia, ad adeguare le procedure previste dalla norma alle innovazioni tecnologiche degli strumenti dai quali derivi la possibilità di controllo a distanza dell'attività lavorativa.

Tali indicazioni, relative alle modalità e condizioni di espletamento delle procedure previste dall'art. 4 della Legge n° 300/1970 rappresentano un'importante novità per le aziende che intendono installare e utilizzare lecitamente «impianti audiovisivi e altri strumenti di controllo» negli ambienti lavorativi.

Aspetti innovativi della circolare

- **Il focus delle istruttorie, finalizzate al rilascio dei provvedimenti autorizzativi in materia – che non deve essere una valutazione tecnica dei dispositivi, bensì una valutazione delle motivazioni che ne giustificano e legittimano l'utilizzo nonché della correlazione tra tali motivazioni e lo strumento da utilizzare. Si legge nella circolare: «l'oggetto dell'attività valutativa, infatti, va concentrata sulla effettiva sussistenza delle ragioni legittimanti l'adozione del provvedimento, tenendo presente in particolare la specifica finalità per la quale viene richiesta la singola autorizzazione e cioè le ragioni organizzative, produttive, quelle di sicurezza sul lavoro e quelle di tutela del patrimonio aziendale».**

Le possibilità di inquadrare direttamente i lavoratori, in presenza di ragioni giustificatrici, è un ulteriore elemento di novità della Circolare in commento.

La circolare n° 5 del 2018 Ispettorato Nazionale del Lavoro.

Si legge nella circolare quanto segue: «è bene precisare che i principii di legittimità e determinatezza del fine perseguito nonché della sua proporzionalità, correttezza e non eccedenza, impongono una gradualità nell'ampiezza e tipologia del monitoraggio, che rende assolutamente residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori».

Quanto all'accesso alle immagini registrate si osserva come questo sia da remoto che «in loco» deve necessariamente essere tracciato anche tramite apposite funzionalità che consentano la conservazione dei «log di accesso» per un congruo periodo di tempo, non inferiore a sei mesi. In considerazione di ciò, lo stesso Ispettorato Nazionale del Lavoro ha ritenuto che l'utilizzo del sistema della «doppia chiave fisica o logica» non sia più una condizione necessaria nell'ambito dei provvedimenti autorizzativi da rilasciare.

La circolare in questione – in conclusione – rappresenta una forte svolta non solo nell'applicazione della norma, ma, soprattutto, nell'approccio alla stessa. Il rilievo di tale circolare è, infatti, rappresentato non solo, come è ovvio, dalla semplificazione dei processi di richiesta e rilascio dei provvedimenti autorizzativi e dalla evidente volontà di adeguamento ai cambiamenti tecnologici in corso ma soprattutto dalla volontà di responsabilizzare le aziende demandando loro la scelta circa le modalità con cui tutelare un proprio interesse legittimo (controllo dei luoghi di lavoro e sicurezza degli stessi) pur rispettando la normativa applicabile. Elemento del tutto coerente con la responsabilizzazione prevista dal Regolamento UE 2016/679 in materia di protezione dei dati personali, la c.d. accountability.

Le conseguenze in caso di violazione delle disposizioni in materia di controlli a distanza – decreto di adeguamento n° 101/2018.

Il decreto di adeguamento conferma i reati già previsti dall'art. 171 del previgente Codice per le violazioni delle norme dello Statuto dei lavoratori in materia di controlli a distanza dei lavoratori e indagini sulle loro opinioni politiche, religiose o sindacali.

Le violazioni connesse al controllo a distanza dei lavoratori sono oggetto di un numero sempre maggiore di segnalazioni inviate dal Garante all'autorità giudiziaria, e i precedenti giurisprudenziali certo non mancano in questo campo. Ad esempio, come si è già visto, la Cassazione ha recentemente stabilito con la pronuncia n° 22148/2017 che l'installazione di un sistema di videosorveglianza in grado di controllare a distanza l'attività dei lavoratori in mancanza di accordo con le rappresentanze sindacali integra reato anche se la stessa sia stata preventivamente autorizzata per iscritto da tutti i dipendenti.

La riformulazione delle norme sul controllo a distanza dei lavoratori da parte del Jobs Act ha però creato non poche difficoltà interpretative (in particolare rispetto all'uso dei moderni sistemi digitali di controllo) al punto di sollevare dubbi di compatibilità con il principio di tassatività. A questo proposito si sarebbe potuto pensare di intervenire ulteriormente, sulle norme in questione proprio durante l'adeguamento del nostro ordinamento al GDPR, ma i tempi stretti dettati dall'entrata in vigore del Regolamento Europeo hanno sicuramente lasciato poco spazio a riflessioni di più ampio respiro.

L'art. 114 del D.Lgs. n° 101/2018 in materia di garanzie in tema di controllo a distanza dei lavoratori stabilisce espressamente che restano ferme le disposizioni contenute nell'art. 4 della legge 20 maggio 1970 n° 300 in termini di garanzie per i trattamenti connessi ai controlli a distanza dei lavoratori.

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo VI

Dott. Marco La Diega

M6.1.4 - Le possibilità, i limiti e le modalità con cui effettuare controlli sull'uso di Internet e della posta elettronica da parte dei dipendenti.

USO DI INTERNET: INIZIAMO CON TRE DOMANDE - (PROFILO INFORMATICO)

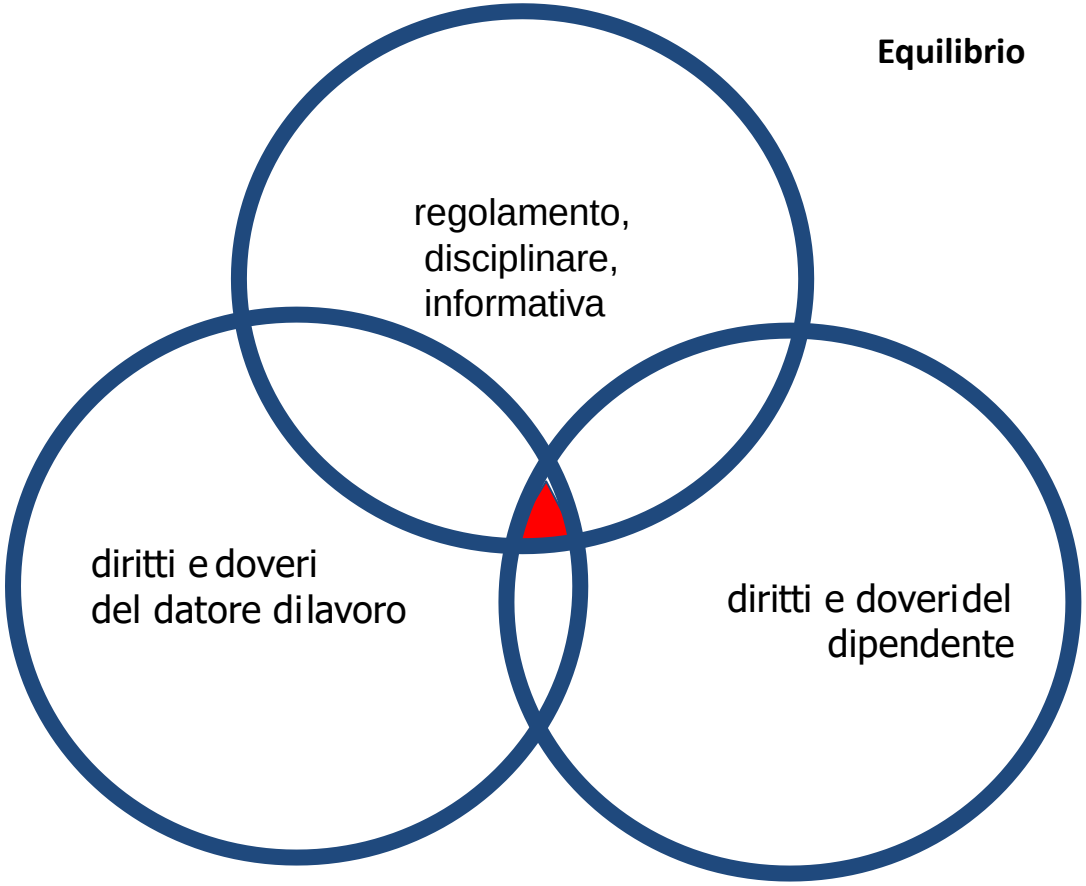
- **Tecnicamente è <u>possibile sempre accedere</u> al traffico** da e verso la postazione di lavoro, per attività connesse all'utilizzo della connettività. ?

- **E' possibile tecnicamente limitare**, la consultazione del traffico dati, eliminando elementi che possono violare la privacy?

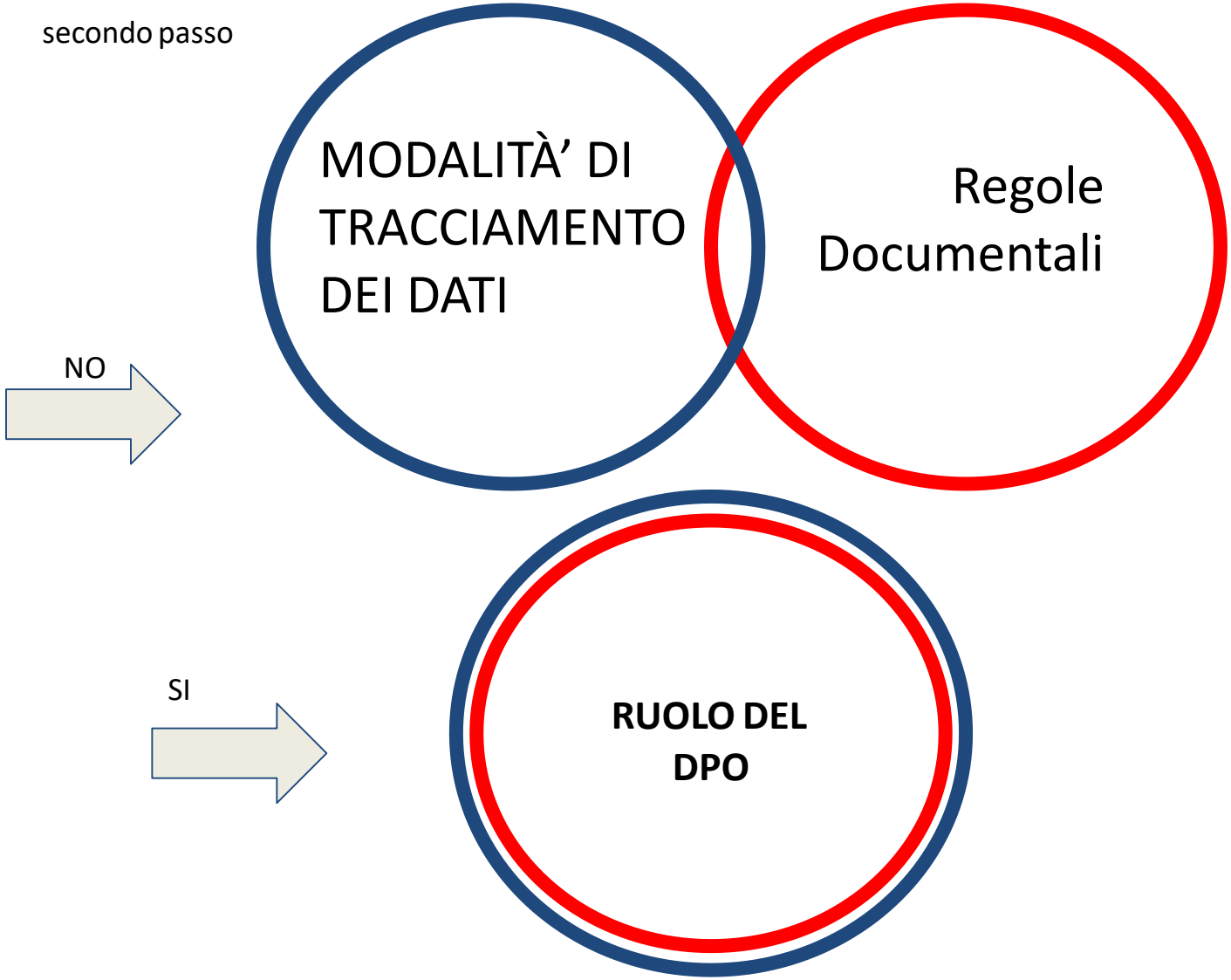
- **E' lecito controllare in modo costante** il flusso di dati personali relativo al comportamento del soggetto da parte di un incaricato alla sicurezza?

Equilibrio

primo passo



secondo passo



Ci troviamo in una zona di passaggio

Un famoso film di alcuni anni fa racconta una storia di un uomo che si trova a vivere un'avventura particolarmente singolare.

Sto parlando del film The Terminal. Tom Hanks è l'attore principale, impersona proprio bene la disavventura realmente accaduta al protagonista. In breve quest'uomo parte dalla città nel suo piccolo paese della Federazione Russa per andare a New York ma, dopo Il lungo viaggio, al momento di passare l'ultimo gate ed accedere alla città della Grande Mela, viene bloccato.

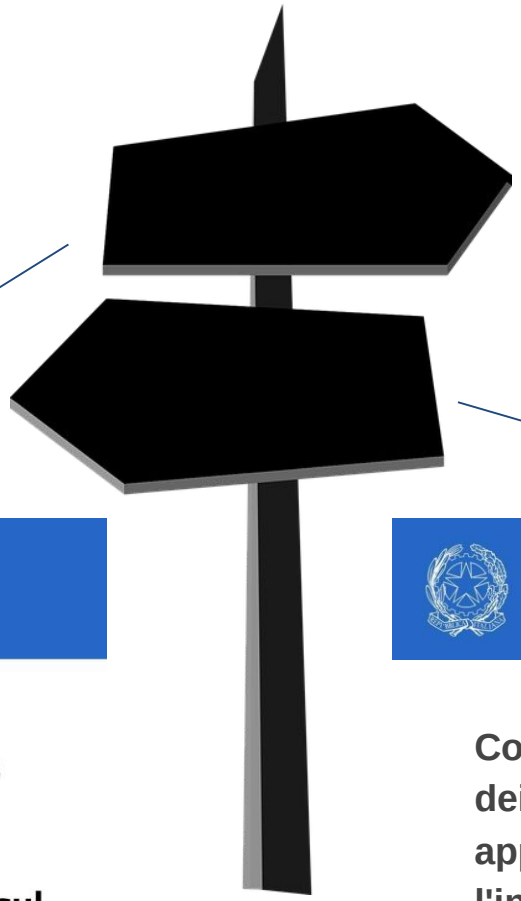
Il suo passaporto risulta non valido a causa del fatto che il suo paese proprio da poche ore era stato protagonista di un colpo di stato.

Victor quindi rimane all'interno del terminal dell'aeroporto di New York per 9 mesi.

Rimane all'interno di una zona destinata al passaggio ed al transito di persone, un luogo che non è stato studiato né pensato per far vivere una persona per tanti mesi.

Victor quindi **vive in un "non luogo"**. Né casa né lavoro, la sua vita si svolge in una **zona di passaggio**.
Forse ti starai chiedendo che c'entra la storia di Victor con la Pubblica Amministrazione digitale.

LE DUE STRADE PRINCIPALI (GLI SCENARI POSSIBILI)



MENU Ministro per la Pubblica Amministrazione

Home › Dipartimento della funzione pubblica › Articoli

Direttiva n. 2/09 relativa all'utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro

•it Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione

Con decreto del Presidente del Consiglio dei ministri 31 maggio 2017 e' stato approvato il Piano triennale per l'informatica 2017-2019.

Direttiva 2/2009

1. **Esercizio del potere di controllo e doveri di comportamento dei dipendenti delle pubbliche amministrazioni**

2. **I principi contenuti nelle linee guida del Garante della protezione dei dati personali**

3. **Utilizzo della rete internet**

4. **Utilizzo della posta elettronica istituzionale**

Direttiva 2/2009

1. Esercizio del potere di controllo e doveri di comportamento dei dipendenti delle pubbliche amministrazioni

Le Pubbliche Amministrazioni, in quanto datori di lavoro, sono tenute ad **assicurare la funzionalità ed il corretto impiego degli strumenti ICT** da parte dei propri dipendenti, **definendone le modalità di utilizzo** nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi.

rispettando principio di proporzionalità, che si concreta nella pertinenza e non eccedenza delle attività di controllo

in ogni caso esclusa l'ammissibilità di **controlli prolungati, costanti e indiscriminati;**
l'introduzione di tecnologie e di strumenti per il controllo sull'uso della rete e della posta elettronica deve essere fatto **rispettando le procedure di informazione/consultazione** delle rappresentanze dei lavoratori previste dai contratti collettivi;

lavoratori **devono essere preventivamente informati dell'esistenza di dispositivi di controllo atti a raccogliere i dati personali.**

Direttiva 2/2009

2. I principi contenuti nelle linee guida del Garante della protezione dei dati personali

LINEE GUIDA GARANTE

il datore di lavoro (secondo i poteri a lui affidati dalle norme del codice civile, articoli 2086, 2087 e 2104), può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro.

Nell'esercizio di tali prerogative, tuttavia, deve **rispettare la libertà e la dignità dei lavoratori.** […]

I mezzi e **l'ampiezza del controllo** devono essere proporzionati allo scopo: in base a tale considerazione il datore di lavoro potrebbe, ad esempio, **verificare se vi è stato indebito utilizzo della connessione ad internet da parte del dipendente attraverso il controllo degli accessi e dei tempi di connessione**, **senza però indagare sul contenuto dei siti visitati.**

Quali sono le attività consentite, a quali controlli sono sottoposti, le modalità del trattamento dei dati e in quali sanzioni possono incorrere nel caso di abusi. Al riguardo, viene raccomandata l'adozione di un **disciplinare interno adeguatamente pubblicizzato** e di idonee **misure di tipo organizzativo.**

Direttiva 2/2009

3. Utilizzo della rete internet

In capo all'Amministrazione datore di lavoro, alla cui proprietà è riconducibile il Sistema informativo, è posto l'onere di predisporre misure per ridurre il rischio di usi impropri di internet, quali la visione di siti non pertinenti, l'upload e il download di files, l'uso di servizi di rete con finalità estranee all'attività lavorativa.

A tale proposito, si raccomanda alle Amministrazioni di dotarsi di software idonei ad **impedire l'accesso** a siti internet aventi contenuti e/o finalità vietati dalla legge.

4. Utilizzo della posta elettronica istituzionale

ART 49 DEL CAD

La connettività Internet della PA deve essere finalizzata a:

- garantire accesso alla rete Internet a **tutti i dipendenti della PA,** indipendentemente dal ruolo o dai compiti assegnati, e senza limiti di tempo o orari. Internet oggi deve essere considerato a tutti gli effetti uno strumento di lavoro indispensabile ed efficace per svolgere ogni tipo di attività: dal trovare numeri di telefono, all'identificare persone e relazioni tra queste persone, riferimenti di un concorso o normativi, documentazione tecnica, strumenti di produttività (traduzioni, orari nel mondo, ecc.), servizi di emergenza, o notizie di ogni tipo.
- garantire accesso non solo agli strumenti ed alle applicazioni utilizzati dalla PA, ma -previa analisi delle necessità organizzative in relazione agli obiettivi da raggiungere- a **tutti i contenuti e gli strumenti che Internet mette a disposizione**, inclusi strumenti per la condivisione di file e contenuti, social network, nonché siti come forum, chat o altri strumenti di comunicazione.

PA che fanno uso di firewall o altre tipologie di filtri applicativi devono quindi configurarli per consentire accesso ad internet a tutti i dipendenti, e limitare il filtraggio esclusivamente a siti e contenuti direttamente pericolosi (malware, virus, *phishing*), illegali, o chiaramente non appropriati per un ambito lavorativo. Siti di condivisione file, social network, chat o altro, non dovrebbero quindi essere filtrati di principio, per quello che sono, ma solo ed esclusivamente in funzione della tipologia di contenuti normalmente scambiati.

Nel caso la PA abbia chiare e documentate esigenze di sicurezza superiori alla norma (materiale riservato, servizi critici e sicurezza nazionale) è raccomandato l'utilizzo di filtri stringenti che blocchino l'utilizzo di strumenti di comune utilizzo **solo ed esclusivamente** a quei dipendenti e quei sistemi che hanno accesso a questo tipo di informazioni, ed a fronte di forti politiche di sicurezza che istruiscano i dipendenti su come individuare e trattare informazioni riservate, sui pericoli del *phishing*, l'utilizzo di chiavette USB, ecc. ed a fronte della configurazione di strumenti di logging e auditing per mantenere la rete sicura.

Le linee di azione nel capitolo 8, dedicato alla sicurezza, si occuperanno di fornire linee guida chiare e dettagliate.

USO DELLA POSTA ELETTRONICA

ART 49 DEL CAD

Segretezza della corrispondenza trasmessa per via telematica

1.Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, **duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica,** salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

2.Agli effetti del presente codice, **gli atti, i dati e i documenti trasmessi per via telematica si considerano,** nei confronti del gestore del sistema di trasporto delle informazioni, **di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.**

APPLICAZIONE PRATICA

I LIMITI DELLA RISERVATEZZA DELLA CORRISPONDENZA VIA POSTA ELETTRONICA

Perchè la riservatezza della Posta Elettronica è labile.

a. Fattore organizzativo
b. La natura dello strumento digitale

l'esempio delle procedure E-Procurement

L'**e-procurement** (**electronic procurement**) è un neologismo di lingua inglese con cui si intende il processo di "approvvigionamento elettronico",

caso pratico

- una misura semplice ma molto efficace da adottare a costo zero - "la cifratura dei contenuti".

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

Trattamento di dati personali effettuato sugli account di posta elettronica aziendale - 1° febbraio 2018

Con reclamo pervenuto il 23 dicembre 2016 il Sig. XX ha chiesto all´Autorità di disporre il blocco o il divieto del trattamento della società …. con particolare riferimento ai dati esterni ed al contenuto di alcune email conservate e utilizzate al fine di elevare una contestazione disciplinare (…) Quanto al contenuto delle email, questo sarebbe stato caratterizzato "dagli evidenti toni personali […] espressione di goliardia e […] ironia fra colleghi" (cfr. reclamo cit., p. 2).

Tale attività di raccolta (e successivo trattamento) delle email da parte della società sarebbe inoltre avvenuto in assenza di informativa circa le specifiche politiche aziendali adottate in proposito.

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

Trattamento di dati personali effettuato sugli account di posta elettronica aziendale - 1° febbraio 2018

La azienda dichiara che:

le comunicazioni e-mail successivamente utilizzate per la contestazione disciplinare […] sono state rinvenute in occasione di un accesso tramite server aziendale alla casella di posta elettronica di un altro dipendente allo scopo di verificare rilevanti non conformità nella tenuta della contabilità.

La società ha conseguentemente proceduto alla "ricerca della documentazione necessaria …

in occasione di tale consultazione […] sono state rinvenute le e-mail poste, in uno ad altre rilevanti circostanze, a base della contestazione disciplinare e del licenziamento" […], a denigrare pesantemente l´azienda [e] dimostrano che il reclamante con la sua condotta […] ha consentito il perseverare di gravi errori nella redazione dei bilanci […]"(cfr. nota cit., p. 6);

il trattamento effettuato sarebbe pertanto legittimo in quanto preordinato "alla tutela degli interessi dell´impresa (anche di protezione del patrimonio aziendale) e all´esercizio del potere disciplinare del datore di lavoro" …

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

Trattamento di dati personali effettuato sugli account di posta elettronica aziendale - 1° febbraio 2018

La azienda dichiara che:

a seguito del licenziamento del reclamante la società "ha provveduto ad attivare un sistema di risposta automatica che invitava il mittente a inviare future comunicazioni" ad un diverso indirizzo aziendale;

inoltre in vista delle "richiamate ragioni di tutela aziendale e di difesa giudiziale […] sono state effettuate operazioni di sola lettura sulle e-mail in ingresso sull´account aziendale del [reclamante] per un periodo […] inferiore a sei mesi (oggi del tutto terminato), dopo la sospensione cautelare del rapporto di lavoro e il successivo licenziamento"

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

Trattamento di dati personali effettuato sugli account di posta elettronica aziendale - 1° febbraio 2018

La azienda dichiara che:

la società ha fornito una "informativa personalizzata inserita nella lettera di designazione quale incaricato del trattamento" nonché reso noto il menzionato "Disciplinare interno sull´utilizzo delle risorse informatiche aziendali"

con il menzionato Disciplinare interno la società ha "vieta[to] la tenuta nella rete interna di file non attinenti all´attività lavorativa […] e prescri[tto] che i dispositivi hardware e software concessi in uso dalla società – e quindi anche gli account e-mail aziendali – devono essere utilizzati solo per scopi aziendali";

quanto alla normativa in materia di controlli a distanza (art. 4, legge 20.5.1970, n. 300) la società ha dichiarato di "non [aver] attivato alcun tipo di controllo o controllo automatizzato del lavoratore"; pertanto le procedure ivi previste non sono state attivate (cfr. nota cit., p. 11).

L'interessato replica.

Con nota di replica pervenuta il 19.6.2017 il reclamante ha ribadito le richieste già avanzate all´Autorità, rappresentando - tra l´altro - che "il range di ricerca sulle email contestate", inizialmente individuato tra i mesi di luglio/ottobre 2015 (con lettera di contestazione disciplinare), è stato successivamente esteso dalla società "a tutto l´anno 2015" (…)

inoltre "nel merito, il contenuto delle mail […] non appare avere alcuna rilevanza disciplinare, trattandosi di comunicazioni private scambiate tra colleghi con tono scherzoso e senza che ne emerga alcun intento destabilizzante o denigratorio, anche in considerazione del fatto che dovevano essere lette solo dai destinatari che partecipavano alla conversazione […]"

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

Trattamento di dati personali effettuato sugli account di posta elettronica aziendale - 1° febbraio 2018

(...) g. il "Disciplinare interno sull´utilizzo delle risorse informatiche aziendali" è stato adottato il 4 marzo 2010 e in pari data "trasmesso […] alla scrivente società e precisamente alla casella di posta elettronica [assegnata al reclamante] in ragione del ruolo rivestito in azienda"; il documento è stato "affisso in bacheca" ed ha "costituito uno degli argomenti trattati durante i corsi di formazione e di aggiornamento che la società organizza periodicamente per i propri dipendenti" (cfr. nota cit., p. 6 e 7);

h. per quanto riguarda la procedura relativa agli account di posta elettronica aziendale assegnati ai dipendenti dopo l´interruzione del rapporto di lavoro, le "nuove misure oggi attuate […] prevedono che alla data della cessazione del rapporto di lavoro venga disattivato l´account […].

Pertanto, nel caso di tentativo di invio di una comunicazione alla casella disattivata il mittente riceve un messaggio di mancato recapito"; diversamente, all´epoca dei fatti oggetto di reclamo, "la disattivazione […] avveniva ancora in due distinte fasi: in un primo momento veniva transitoriamente attivato un sistema di autoreply al fine di rendere noto ai mittenti un altro indirizzo e-mail a cui inviare le future comunicazioni; in una seconda fase veniva definitivamente disattivato l´account e, a quel punto, in caso di tentato invio il mittente riceveva un messaggio di mancato recapito" (cfr. nota cit., p. 7).

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

Trattamento di dati personali effettuato sugli account di posta elettronica aziendale - 1° febbraio 2018

L´esito dell´istruttoria.

All´esito dell´esame delle dichiarazioni rese all´Autorità nel corso del procedimento risulta che la società in qualità di titolare ha effettuato (e tutt´ora effettua) operazioni di trattamento di dati personali riferiti al reclamante

- nonché agli altri dipendenti - che risultano per alcuni profili non conformi alla disciplina in materia di protezione dei dati personali, nei termini di seguito descritti.

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

Primo punto - *L´informativa all'interessato data attraverso la policy aziendale.*

In relazione ai descritti trattamenti, in primo luogo, non risulta che la società abbia informato il reclamante - e gli altri dipendenti - circa modalità e finalità della descritta attività di raccolta e conservazione dei dati relativi all´utilizzo della posta elettronica, né con informativa individualizzata né con la messa a disposizione della policy aziendale.

All´interno di tali documenti non v´è dunque alcun riferimento alla conservazione sui server aziendali - per tutta la durata del rapporto di lavoro ed anche oltre la cessazione dello stesso (si veda infra punto 3.2.) - di tutte le email scambiate nel corso dell´attività lavorativa, né delle finalità e modalità di conservazione e di accesso della società a tale database.

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

Secondo punto - *L´informativa all'interessato data attraverso la policy aziendale.*

Non sono state rese note le specifiche attività di controllo - indicando dettagliatamente modalità e procedure adottate - che il datore di lavoro si riserva di effettuare sui dati raccolti nel corso dell´attività lavorativa (con particolare riferimento alla possibilità di accedere al contenuto di tutte le comunicazioni elettroniche scambiate).

"Linee guida per posta elettronica e internet", citate in premessa, spec. punto 3.1.

"Grava […] sul datore di lavoro l´onere di indicare […], 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";

Terzo punto - *L´informativa all'interessato data attraverso la policy aziendale.*

…. si rammenta che l´informativa ai dipendenti deve altresì indicare le operazioni di trattamento che possono essere effettuate dall´amministratore di sistema per finalità connesse alla fornitura del servizio (cfr. anche Provv. 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008, modificato con provvedimento del 25 giugno 2009, "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", doc. web n. 1577499, spec. n. 2, lett. c) e f) del dispositivo. In base a tale provvedimento il titolare è altresì tenuto ad adottare sistemi che registrino gli "accessi logici ...

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

QUARTO PUNTO

Liceità, necessità e proporzionalità del trattamento. Conservazione dei dati.

La conservazione sistematica dei dati esterni e del contenuto di tutte le comunicazioni elettroniche scambiate dai dipendenti, non risulta altresì conforme ai principi di liceità, necessità e proporzionalità del trattamento.

(…) L'AZIENDA è TENUTA AD individuare i documenti che nel corso dello svolgimento dell´attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile (si veda quanto stabilito dal D.P.C.M. 3 dicembre 2013, recante le Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell´amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

… i documenti che rivestano la qualità di "scritture contabili" devono essere memorizzati e conservati con modalità determinate: artt. 2214 c.c.; artt. 43 e 44, d. lgs. 7 marzo 2005, n. 82, "Codice dell´amministrazione digitale"). I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche.

Pertanto lo scopo di predisporre strumenti per l´ordinaria ed efficiente gestione dei flussi documentali aziendali può ben essere perseguito - conformemente alle disposizioni vigenti oltre che più efficacemente - con strumenti meno invasivi per il diritto alla riservatezza dei dipendenti e dei terzi, rispetto alla sopra descritta attività di sistematica ed estesa conservazione delle comunicazioni elettroniche, che risulta pertanto non necessaria né proporzionata rispetto allo scopo.

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

QUINTO PUNTO

Liceità, necessità e proporzionalità del trattamento. Conservazione dei dati.

La raccolta sistematica delle comunicazioni elettroniche in transito sugli account aziendali dei dipendenti in servizio, la loro memorizzazione per un periodo non predeterminato e comunque, allo stato, amplissimo e la possibilità per il datore di lavoro di accedervi per finalità indicate in astratto e in termini generali – quali la difesa in giudizio o il perseguimento di un legittimo interesse – consente alla società di effettuare il controllo dell´attività dei dipendenti.

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

QUINTO PUNTO

laddove si afferma che qualora "siano attivate caselle di posta elettronica – protette da password personalizzate – a nome di uno specifico dipendente, quelle «caselle» rappresentano il domicilio informatico proprio del dipendente […].

La casella rappresenta uno «spazio» a disposizione – in via esclusiva – della persona, sicché la sua invasione costituisce, al contempo, lesione della riservatezza").

Tanto più che l´assenza di una esplicita policy al riguardo può determinare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione (cfr. Linee guida per posta elettronica e internet, cit., spec. 3; 5.2. lett. b), e 6.1.).

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

SESTO PUNTO - DISATTIVAZIONE ACCOUNT

Non risulta conforme ai suesposti principi la procedura adottata dalla società a seguito del licenziamento del reclamante, consistente nella raccolta e accesso alle "e-mail in ingresso sull´account aziendale […] per un periodo […] inferiore a sei mesi" (v. precedente punto 1.2., lett. g.). Ciò indipendentemente dall´attivazione di un messaggio di risposta automatico che indicava al mittente un diverso account aziendale da contattare, considerato che la formula adottata risulta per di più fuorviante in quanto reca l´indicazione (ai terzi) che la casella "è stata disattivata" (v. e-mail 6.3.2017, All. 10 nota del reclamante 19.6.2017).

Si prende altresì atto che, allo stato, la società avrebbe invece adottato un sistema coerente con quanto indicato in proposito dall´Autorità, posto che in caso di cessazione del rapporto di lavoro l´account viene "disattivato" con attivazione di un "messaggio di mancato recapito" in caso di tentato invio di una comunicazione elettronica sull´account (v. precedente punto 1.4., lett. h.).

tali da inibire in via definitiva la ricezione in entrata di messaggi diretti al predetto account, nonché la conservazione degli stessi su server aziendali" (v. Provv. 5 marzo 2015, n. 136, doc. web n. **3985524**).

doc. web n. 8159221 - Registro dei provvedimenti n. 53 del 1° febbraio 2018

CONCLUSIONI

3.5. Conclusioni: illiceità del trattamento.

Per i suesposti motivi, considerato che il trattamento dei dati personali effettuato dalla società sugli account di posta elettronica aziendale risulta illecito, si dispone il divieto di ulteriore trattamento dei predetti dati, fatta salva la conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria.

LA TECNOLOGIA VA CONFIGURATA SEGUENDO I REGOLAMENTI

MENU Ministro per la Pubblica Amministrazione

Home › Dipartimento della funzione pubblica › Articoli

Direttiva n. 2/09 relativa all'utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro

.it Piano Triennale 2017-2019 per l'informatica nella Pubblica Amministrazione

Con decreto del Presidente del Consiglio dei ministri 31 maggio 2017 e' stato approvato il Piano triennale per l'informatica 2017-2019.

Sistemi di controllo/protezione/ connettività

FIREWALL/PROXY

Sistemi di controllo/protezione/ connettività

FIREWALL/PROXY

NEGA/ACCONSENTE/FILTRA/TRACCIA/VPN Canali sicuri punto-punto

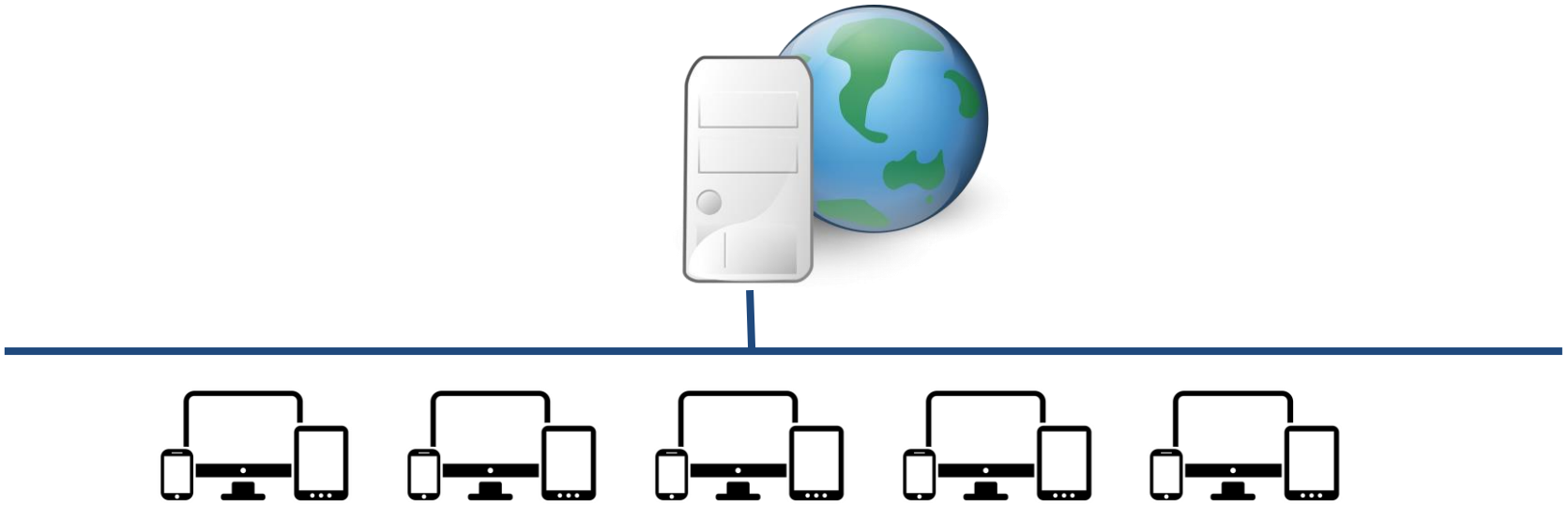
Cos'è un firewall?

Un firewall è uno strumento, hardware o software, che funge da schermo protettivo, un vero e proprio muro (da qui il nome) che garantisce protezione alla rete informatica. Il firewall, in particolare, blocca l'accesso al sistema alle risorse esterne, applicando filtri di protezione **che agiscono secondo determinate regole, a loro volta definite dall'amministratore della rete.**

Sistemi di controllo/protezione/ connettività

PROXY

OTTIMIZZA, TRACCIA, MEMORIZZA



Configurazioni Firewall

"tutto no tranne che" o "tutto si tranne che" ? (deny e allow)

Il firewall viene impostato con le cosiddette "regole", che sono, essenzialmente, di due tipologie: deny e allow.
Nel primo caso posso impostare il firewall in modo tale che questo vieti tutto, tranne quello che gli dico di non vietare.
Nel secondo caso il meccanismo è esattamente l'opposto: il firewall concederà l'accesso a tutto tranne a ciò che gli chiedo di bloccare.

Tutti i firewall, per garantire una maggiore sicurezza, seguono di prassi la policy del default-deny.
In ogni caso, l'ENTE decide come configurare il firewall nel rispetto del REGOLAMENTO INTERNO.

LA GESTIONE DEI MESSAGGI/POSTA ELETTRONICA PER UNA PA

IL LUOGO MIGLIORE PER DEFINIRE LE POLICY GDPR è IL REGOLAMENTO DELLA GESTIONE DEL PROTOCOLLO INFORMATICO

CHE VA ALLINEATO ALL'EFFETTIVO FUNZIONAMENTO DEL SISTEMA INFORMATIVO COMUNALE

IL RUOLO DEL DPO E'

VERIFICARE L'EFFETTIVA CORRISPONDENZA TRA LE REGOLE DESCRITTE DAI REGOLAMENTI

CON L'EFFETTIVA CONFIGURAZIONE DEI SISTEMI DI GESTIONE

NEL RISPETTO DEL **GDPR**

ESEMPI DI REGOLAMENTO CHE TENGONO IN CONSIDERAZIONE LO STATO DELL'ARTE

MODALITÀ' DI UTILIZZO (ESEMPI VOCI DI REGOLAMENTO)

UTILIZZO DELLA POSTA ELETTRONICA

a) La casella di posta elettronica assegnata dall'azienda al dipendente è uno strumento di lavoro il cui utilizzo per fini personali non è consentito se non nei limiti di cui al successivo art. X del presente regolamento.

I dipendenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

b)Le caselle di posta elettronica aziendale di tipo "cognome@comune.it' vanno utilizzate esclusivamente per l'invio di messaggi attinenti il rapporto di lavoro.

Ne è vietato l'utilizzo per la partecipazione a dibattiti, forum, chat o mail-list, salvo diversa esplicita autorizzazione dall'Amministratore del Sistema.

Per la trasmissione di files attinenti l'attività lavorativa è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e allegati ingombranti.

c)E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di files eseguibili o documenti di siti Web o Ftp non conosciuti).

d)E' vietato inviare catene telematiche. Non si devono in alcun caso attivare gli allegati ai messaggi in questione.

e)La casella di posta elettronica, in quanto avente le caratteristiche di cui alla precedente lett. a), non è da intendersi come corrispondenza privata del singolo dipendente ma esclusivamente quale corrispondenza e documentazione di lavoro di stretta pertinenza aziendale.

Qualora l'Amministratore di Sistema nell'espletamento delle proprie funzioni individui comportamenti anomali potenzialmente pericolosi per i sistemi informativi aziendali, il datore di lavoro potrà inviare un avviso generalizzato o circoscritto a dipendenti afferenti l'area o il settore in cui stato rilevato il comportamento anomalo con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite, contrariamente il datore di lavoro potrà effettuare controlli sulla singola casella di posta elettronica, anche tramite propri incaricati, con identificazione del mittente, del destinatario e dell'oggetto di ogni mail.

f)E' vietato l'invio di messaggi di posta elettronica interna ad un numero indistinto di utenti (tutti gli utenti o liste di distribuzione), salvo i casi di comprovata necessità organizzativa che andranno appositamente e preventivamente autorizzati.

g)I dipendenti sono responsabili del contenuto delle proprie comunicazioni e della riservatezza dei dati ivi contenuti, la cui impropria colpevole diffusione potrebbe integrare L'illecito di violazione del segreto d'ufficio e/o della normativa in materia di tutela dei dati personali.

MODALITA' DI UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI (ESEMPI)

a)II PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento dell'attività lavorativa ed il suo utilizzo per fini personali o comunque non attinenti alle mansioni svolte vietato. E' proibita la navigazione in Internet per motivi diversi da quelli legati alla prestazione lavorativa del dipendente assegnatario del PC abilitato se non nei limiti di cui alla sezione successivo UTILIZZO PERSONALE CONSENTITI del presente regolamento.

b)E' fatto divieto all'utente di effettuare il download di software anche se gratuito (freeware) e shareware prelevato da siti internet non certificati dall'Amministratore di Sistema, se non espressamente autorizzato dallo stesso.

c)E' vietata l'effettuazione di ogni genere di transazione finanziaria se non nei limiti di cui al successivo UTILIZZO PERSONALE CONSENTITI ivi comprese le operazioni di remote banking, acquisti on line e simili, salvo i casi direttamente autorizzati dal Responsabile dell'aera di competenza e con il rispetto delle normali procedure di acquisto.

d) Non è consentita ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa

e)E' vietata la partecipazione a forum non professionali, social network, gaming on line, l' utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (nickname).

f) E' vietato l'accesso a siti a pagamento, salvo per necessità esclusivamente aziendali.

g)Il dipendente non e in ogni caso autorizzato a produrre ed a pubblicare siti web personali mediante la rete aziendale.

h)L'utilizzo di Internet per scopi attinenti le mansioni di lavoro è ammesso ed autorizzato solo attraverso la rete di trasmissione dati aziendale.

i) L'Amministratore di Sistema provvedere a monte, tramite apposite procedure, ad impedire l'accesso ai siti internet di consultazione comune, ai social network (facebook o similari), etc, tranne per specifici compiti assegnati.

L'indebito utilizzo del servizio internet da parte del dipendente abilitato comporterà l'avvio di ogni procedura e/o procedimento inerente

QUALI VOCI FONDAMENTALI DEVE CONTENERE UN REGOLAMENTO

UTILIZZI PERSONALI CONSENTITI (ESEMPI)

Nel convenire che internet e posta elettronica fanno ormai parte della vita quotidiana e che sempre più servizi vengono gestiti con la modalità web, L'ENTE riconosce la possibilità ai destinatari del presente Regolamento di utilizzare le dotazioni aziendali assegnate, anche per fini personali, purché nel rispetto delle prescrizioni sotto indicate:

a) le connessioni ad internet di carattere non strettamente lavorativo dovranno avvenire fuori orario di lavoro e quindi durante la pausa pranzo ovvero dopo la fine del servizio; b) per i lavoratori che non hanno l'obbligo di timbratura ci si riferisce, per la determinazione dell'orario di lavoro, a quello standard;

c)sono consentite le connessioni per consultazioni varie, la possibilità di effettuare transazioni bancarie nonché di stampare documenti e/o atti purché in misura ragionevole e non indiscriminata e sempre nei limiti di cui al punto a);

d)l'utilizzo personale della posta elettronica aziendale è consentito sempreché il numero di mail inviate a titolo personale risulti essere di modesta entità rispetto a quelle gestite a livello lavorativo. Tutte le attività sopra indicate dovranno ispirarsi ai principi di buona fede contrattuale, non dovranno superare la soglia della ragionevolezza né procurare danni e/o costi ulteriori alle dotazioni aziendali. L'utilizzatore risponderà di eventuali danni arrecati o di un uso ingiustificatamente esteso delle citate attività.

MODALITA' DI TRACCIAMENTO DEI DATI

a)L'Ente è dotato di appositi programmi di tracciabilità e conservazione dei dati e delle operazioni che vengono eseguite dagli Amministratori di Sistema, opportunamente Designati dal Titolare del Trattamento, come indicato nei registri di trattamento vigente, su tutti i server/PC, collegati alla rete aziendale.

Le operazioni compiute da tutti gli utenti (dipendenti/collaboratori, etc.), memorizzate dal sistema operativo, vengono conservate per le finalità di cui alle disposizioni normative in materia e al fine di essere rese disponibili a fronte di richieste da parte dell'Autorità Giudiziaria.

Unicamente agli Amministratori di Sistema è consentito effettuare operazioni sui dati memorizzati.

b)Considerata l' importanza strategica dei server, che costituiscono la banca dati della Società e quindi il patrimonio imprescindibile per il corretto svolgimento delle attività aziendali che deve essere adeguatamente preservato, l' Amministratore di Sistema è autorizzato ad intervenire immediatamente al verificarsi di qualsiasi anomalia causata da comportamenti ed usi impropri da parte degli operatori .

c)Le operazioni difformi compiute dall'operatore in seguito individuato, saranno oggetto di segnalazione all'ufficio Risorse Umane e Organizzazione per i conseguenti procedimenti disciplinari.

d)Le operazioni collegate all'utilizzo della casella di posta elettronica aziendale vengono altresì monitorate tramite apposito log da parte del fornitore del servizio, nel rispetto delle disposizioni di legge in materia. La tracciabilità riguarda solamente i dati identificativi del mittente, destinatario, data e ora di spedizione/ricezione del messaggio e oggetto della missiva.

e)Ogni nuovo accesso a internet deve essere richiesto ed autorizzato da parte del Responsabile competente. L'Amministratore di Sistema provvede all'attivazione del servizio.

f)Ad ogni nuovo dipendente abilitato al servizio internet e/o alla casella di posta elettronica sarà preventivamente consegnata una nota informativa della Direzione contenente "Diritti e Doveri del dipendente" in materia di utilizzo del servizio internet aziendale (Allegato "A" al presente Regolamento), da sottoscriversi per ricevuta. La sottoscrizione vale quale presa d'atto delle informazioni e delle disposizioni normative e di legge a presupposto del presente Regolamento. La mancata sottoscrizione non esonera dalle responsabilità previste per ogni utilizzatore da dette disposizioni normative e/o da norme generali e specifiche adottate dall'Azienda.

g)Ogni nuovo accesso alla rete aziendale a favore di personale NON dipendente (collaboratori, consulenti, stagisti, etc.) dovrà essere espressamente richiesto dal Responsabile competente.

M6.1.5 Geolocalizzazione mezzi aziendali – GPS

LE APPLICAZIONI DI QUESTI SISTEMI

esempi

1. SALVAGUARDIA DEI BENI STRUMENTALI DELL'AZIENDA/ENTE NEL CASO DI FURTI
2. GESTIONE DELLA LOGISTICA NELLE CONSEGNE
3. ELIMINARE GLI SPRECHI DI CARBURANTE
4. VELOCIZZARE GLI INTERVENTI SULLA SICUREZZA

SENSORI PER INTERNI

ATTENZIONE ALL'USO PROMISCUO

ANALISI DEL RISCHIO E IMPATTO (A)

DPIA - VALUTAZIONE D'IMPATTO
SULLA PROTEZIONE DEI DATI PERSONALI
Art.35, art.24 del Regolamento Europeo GDPR - UE 679/2016

Relativo ai seguenti servizi e/o trattamenti

NOME TRATTAMENTO
NOME TRATTAMENTO
NOME TRATTAMENTO
NOME TRATTAMENTO
NOME TRATTAMENTO

DESCRIZIONE STATO DELL'ARTE
(INSERIRE SINTESI DELLA VOSTRA OSSERVAZIONE E VERIFICA DOCUMENTALE)

ANALISI DEL RISCHIO E IMPATTO (B)

Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità.

- E' STATA EFFETTUATA LA VERIFICA DEI DATI RICHIESTI IN FASE DI ISTANZA E/ ACQUISIZIONE DATI PERSONALI IN MERITO ALLA PROPORZIONALITÀ, LA VALUTAZIONE RISULTA '

[ ] CONGRUA [ ] NON CONGRUA

MOTIVAZIONE

ANALISI DEL RISCHIO E IMPATTO (C)

RISCHI RILEVATI

Nome Trattamento	ACCESSO ILLEGITTIMO	INDISPONIBILITÀ' DEI DATI	MODIFICHE INDESIDERATE
	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO
	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO
	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO
	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO
	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO	[ ] BASSO [ ] MEDIO [ ] ALTO

ANALISI DEL RISCHIO E IMPATTO (D)

INDIVIDUAZIONE DELLE MISURE PREVISTE PER LIMITARE I RISCHI IN RELAZIONE ALL'IMPATTO.

STRUMENTI IN USO

ORGANIZZAZIONE

NUOVE TECNOLOGIE IN ARRIVO

LA GEO-LOCALIZZAZIONE IN LUOGHI CHIUSI CON SENSORI

L'ESEMPIO DELLA METROPOLITANA DI MILANO

PRIVACY BY DEFAULT BY DESIGN - VERIFICARE PRIMA DI COMPRARE O REALIZZARE

CONSIDERANDO 78 GDPR

(78)La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in **particolare i principi della protezione dei dati fin dalla progettazione** e della protezione dei dati per i**mpostazione predefinita.**.

IN PRATICA:

- **Proattivo non reattivo**, preventivo non correttivo: le minacce alla privacy dovrebbero essere anticipate e prevenute, piuttosto che corrette dopo che queste si sono verificate.
- **Privacy come impostazione predefinita:** la privacy dovrebbe essere lo standard. I dati personali dovrebbero essere protetti automaticamente, anche senza alcuna azione esplicita da parte dell'individuo interessato.
- **Privacy incorporata nella progettazione:** la privacy non dovrebbe essere considerata un elemento aggiuntivo, ma dovrebbe essere integrata nella progettazione e nell'architettura dei sistemi software e delle attività di business in generale.
- **Piena funzionalità** la privacy dovrebbe coesistere con altri interessi di business. Dovrebbero tuttavia essere evitati compromessi non necessari (ad esempio privacy vs. sicurezza o privacy vs. performance). Si dovrebbe cercare di ottenere una somma positiva.
- **Sicurezza end-to-end -** Tutela dell'intero ciclo di vita: la privacy richiede sicurezza durante l'intero ciclo di vita dei dati personali, garantendo una gestione sicura e completa di tutti i dati.
- • V**isibilità e trasparenza:** gli obiettivi di privacy dichiarati dall'organizzazione e conseguentemente adottati dai sistemi, devono essere visibili e trasparenti agli utenti. • Rispetto per la privacy degli utenti: devono essere applicate misure adeguate per responsabilizzare l'utente nel trattamento dei propri dati.

PONIAMO ATTENZIONE AL GESTORE DEL SISTEMA e APPLICHIAMO IL GDPR

- Chi è Il Gestore Del Sistema?
- Che software utilizza?
- Quali sono le caratteristiche del software?
- Dove risiedono i dati?
- E' sotto il nostro controllo stretto?
- Esiste un designato ben istruito e competente?
- Le interfacce prevedono policy di accesso multilivello sulla consultazione del dato?
- Il data base è sotto il nostro controllo.
- Esistono politiche di conservazione, archiviazione e uso dei dati raccolti?
- Esistono limitazioni alla durata della conservazione?
- Il sistema è customizzabile?
- Il contratto di servizio prevede le misure di sicurezza dei dati adeguate al trattamento?
- La natura dei dati raccolti è proporzionata alle finalità?
- Esistono misure tecniche organizzative per garantire i diritti agli interessati.
- Sono stabiliti gli obblighi e istruzioni aziendali

….

L'ARGINE NORMATIVO DELLE FINALITA' TRATTAMENTO DEI DATI RACCOLTI DAI MEZZI AZIENDALI E' IL GDPR

N.B. IL GDPR e' un Regolamento normativo non tecnico specifico, dobbiamo cercare i riferimenti

Le linee guida di **AGID - LINEE GUIDA PER LA MODELLAZIONE DELLE MINACCE ED INDIVIDUAZIONE DELLE AZIONI DI MITIGAZIONE CONFORMI AI PRINCIPI DEL SECURE/PRIVACY BY DESIGN - Presidenza Consiglio dei Ministri.**

La privacy si riferisce alla relazione tra un'organizzazione che raccoglie informazioni e il proprietario delle informazioni raccolte. Per stabilire e gestire questa relazione, è necessario creare una politica di riservatezza formata da diverse istruzioni. Un'istruzione della politica di riservatezza definisce:

- I tipi di informazioni raccolte e quelle accessibili;
- Chi può accedere alle informazioni raccolte;
- Per quali scopi è possibile accedere alle informazioni.

attività di base dannose: -(TRATTO DALLE LINEE GUIDA DI AGID)

•**Raccolta dei dati.** Include due tipi di violazioni della privacy: il controllo inteso come "osservazione, ascolto o registrazione delle attività di un individuo", e, l'investigazione che consiste in varie forme di sondaggio per ottenere informazioni.

•**Trattamento dei dati**. Include cinque tipi di violazioni dei dati raccolti al punto precedente:
aggregazione (ovvero combinazione di dati relativi a un individuo),
identificazione (ovvero collegamento dei dati per identificare un individuo),
negligenza (poca attenzione nella protezione dei dati memorizzati),
uso secondario (ovvero utilizzo dei dati per scopi diversi da quelli per i quali sono stati raccolti) ed
esclusione (ovvero quando l'interessato non è a conoscenza dei dati che gli altri hanno su di esso).

• **Diffusione dei dati**. Include sette categorie di violazioni:
violazione della riservatezza (ovvero non mantenere riservate le informazioni di una persona),
divulgazione (cioè rivelare informazioni "sensibili" veritiere su una persona),
esposizione (cioè rivelare le nudità, il dolore o le caratteristiche fisiche di una persona),
maggiore accessibilità (cioè amplificare l'accessibilità dei dati),
appropriazione (cioè l'uso della propria identità per perseguire un'altra finalità).

•**Invasione.** A differenza dei gruppi precedenti, non riguarda necessariamente le informazioni personali, ma degli elementi che limitano la sfera personale e decisionale (ad esempio atti invasivi che violano la tranquillità di una persona e atti invasivi che impattano sulle decisioni private di una persona)

I LOG - NEI SISTEMI DI CONTROLLO ACCESSI

Non utilizzare un meccanismo di log vuol dire non poter provare nulla.

- **Assicurarsi di tracciare tutte le informazioni rilevanti dal punto di vista della sicurezza.**
- **Esposizione dei Logs a eventuali attacchi**
- **Documentare la progettazione del log sin dall'inizio del processo di sviluppo.**

M6.1.6 Biometria

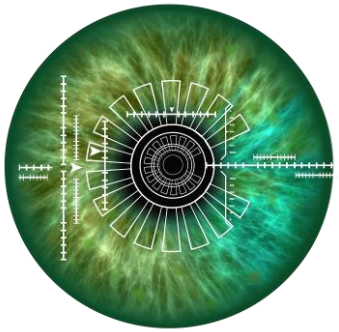
M6.1.7 Rilevazione della presenza dei lavoratori

- **I metodi per l'autenticazione delle persone possono coinvolgere uno qualsiasi dei seguenti elementi:**

1. Qualcosa che sai, come ad esempio una password,
2. Qualcosa che hai, come una card di accesso,
3. Qualcosa che sei, come ad esempio un dispositivo biometrico, comprese le fotografie,
4. Qualcuno che conosci e che può autenticarti.

LA BIOMETRIA

Attualmente, il termine “biometria” si riferisce a una vasta gamma di tecnologie che possono essere utilizzate per verificare l’identità di un soggetto, misurando e analizzando **caratteristiche umane proprie dell’individuo** stesso (riconoscimento biometrico).



LA BIOMETRIA E' LA PASSWORD CHE NON PUOI CAMBIARE

BIOMETRIA E GDPR

GDPR - Verifichiamo sempre la sicurezza HW,SW E DB

L' art. 4, paragrafo 1, n. 14) del GDPR, definisce i dati biometrici come quei "dati personali ottenuti da un trattamento tecnico specifico, **relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica** e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".

In concreto, la raccolta di questi particolari dati personali è possibile ricorrendo all'impiego di sistemi informatici di riconoscimento biometrico, il cui funzionamento è basato essenzialmente su due elementi.

In primo luogo, una **componente hardware** acquisisce il dato biometrico (si pensi, ad esempio, al sensore per il riconoscimento dell'impronta digitale integrato in molti modelli di smartphone di ultima generazione).

In secondo luogo, interviene un **software** che consente, attraverso l'impiego di algoritmi matematici, di analizzare i dati raccolti e di confrontarli con quelli acquisiti in precedenza e conservati nel **database del sistema,** al fine di ricondurre il dato raccolto ad una determinata persona e di riconoscerla da tali informazioni.

TIPI DI BIOMETRIA

IMPRONTE DIGITALI

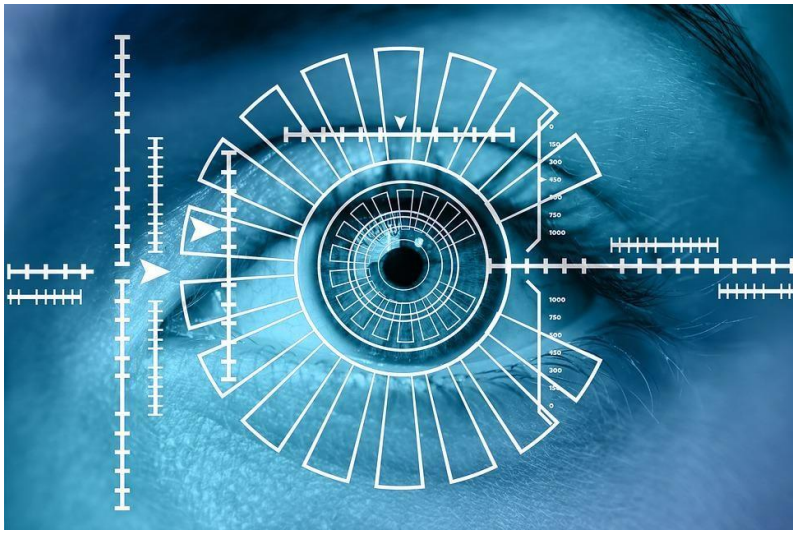
RICONOSCIMENTO FACCIALE

GEOMETRIA DELLE VENE

IRIDE

DNA

VALORI VITALI COME LA PRESSIONE DEL SANGUE



LETTORI BIOMETRICI PER RILEVAMENTO PRESENZA AD IMPRONTA

CRITICITA' - SISTEMI ED INTEGRAZIONI LABILI CON IL SISTEMA INFORMATIVO

UTILIZZAZIONE : SEMPRE PIU' UTILIZZATI IN COMBINATO A SISTEMI FISICI DI RICONOSCIMENTO (BADGE - OTP - ETC)

RFID - Radio-Frequency IDentification;
M6.1.9 Analisi di casi specifici (cartellini identificativi, comunicazioni di dati e bacheche aziendali, controllo accessi e badge)

RFID - Radio-Frequency IDentification;

La radiotecnologia Rfid.

La Radio Frequency Identification (Rfid) è un sistema che usa onde elettromagnetiche per l´identificazione automatica di cose o persone. Il sistema si compone di un Tag (cioè di un´etichetta costituita da una memoria elettronica leggibile e talvolta scrivibile, nonché da antenne) e di un lettore. I Tag Rfid possono contenere un codice identificativo unico o anche ulteriori informazioni. I lettori Rfid sono utilizzati, appunto, per leggere le informazioni contenute nei Tag.

Con sempre maggiore frequenza i sistemi Rfid comportano il trattamento di dati personali nella misura in cui nei Tag vengono registrate anche informazioni idonee a identificare, direttamente o indirettamente, gli interessati quali nome, cognome, data di nascita, numero di targa, etc..

In considerazione della peculiarità di questi sistemi - molto diffusi e praticamente invisibili-, deve essere prestata particolare attenzione, sia nella fase della loro creazione che del relativo utilizzo, alla tutela dei diritti e delle libertà fondamentali, nonché della dignità dell´interessato, con particolare riferimento alla riservatezza, all´identità personale e al diritto alla protezione dei dati personali.

RFID - Radio-Frequency IDentification;

Qual è la differenza tra tag attivi e passivi?

Quando si parla di tag RFID, un'altra distinzione ricorrente è quella tra tag RFID attivi e passivi.

i tag RFID attivi sono dotati di un trasmettitore e di una propria fonte di alimentazione integrata che alimenta il circuito del tag specifico per l'applicazione e viene utilizzata anche per trasmettere un segnale dall'antenna del tag a un dispositivo di lettura RFID.

I tag RFID passivi non dispongono di batteria o alimentazione integrata; **traggono energia da un lettore RFID che emette onde elettromagnetiche.** Queste onde inducono una corrente nell'antenna del tag RFID e consentono la comunicazione reciproca tra il lettore e il medesimo tag. Inoltre, sul mercato sono disponibili tag RFID semi-passivi che utilizzano una batteria per far funzionare il circuito integrato del tag, mentre la comunicazione vera e propria avviene tramite l'alimentazione del lettore RFID.

RFID - Radio-Frequency IDentification;

Perché sono disponibili così tanti tag RFID passivi?

Pensando a un sistema RFID come possibile soluzione applicativa, si potrebbe rimanere colpiti dalla vasta scelta di tag disponibili sul mercato. Da dove viene? La tecnologia RFID è molto versatile e flessibile, pertanto anche i tag si adattano facilmente ai diversi casi applicativi.

Qualche esempio:

RFID - Radio-Frequency IDentification;

QUALI SONE LE APPLICAZIONE DEL RFID ? (stanno sostituendo i codici a barre e le barre magnetiche)

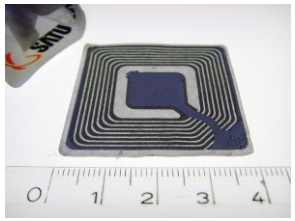
SISTEMA DI RICONOSCIMENTO A RADIO FREQUENZA ?

ALCUNI ESEMPI - per la tracciabilità degli animali, i tag sono molto piccoli per poter essere implementati sottopelle, per l'identificazione di alberi/oggetti in legno, i tag sono a forma di vite o chiodo per le applicazioni di controllo accessi, i tag sono simili a portachiav**i … o anche**

- ETICHETTE ANTITACCHEGGIO
- BIGLIETTI METROPOLITANA RICARICABILI (AD ESEMPIO QUELLO DI LISBONA)
- NEI NUOVI PASSAPORTI è INSERITO UN CHIP RFID
- CARTE DI CREDITO CONTACTLESS
- TELEPASS (semi attivo)

come funzionano ?

etichetta emettitore di segnale attivato da un chip



costo 0,2 cent

emettitore o ricevitore di Onde a Radio Frequenza

antenna

RFID - Radio-Frequency IDentification;

COMUNE DI VERONA -

doc. web n. 1875840

Il Comune di Verona ha richiesto la verifica preliminare del Garante, ai sensi dell´art. 17 del Codice, in relazione al trattamento di dati personali che intende effettuare attraverso un sistema Rfid per la registrazione dell´"orario di ingresso e il successivo orario di uscita dalla Ztl" (zona a traffico limitato) dei veicoli adibiti al trasporto delle merci.

Con riferimento alle finalità che intende perseguire tramite l´istallazione del predetto sistema, il Comune di Verona ha rappresentato che "il primo obbiettivo (…) è quello di impedire che i veicoli autorizzati allo scarico-carico merci in Ztl rimangano all´interno dell´area oltre il limite concesso dalle ordinanze".

… è composto "da un'antenna posta su un palo collegata ad una piccola unità locale che registra una sola informazione e cioè il numero univoco", con cui il Tag è identificato dal produttore. "Tali antenne sono poste sia in corrispondenza degli ingressi (varchi ZTL esistenti) sia in corrispondenza di tutte le uscite dove è presente un varco elettronico".(…). Per sapere a chi appartiene il veicolo/permesso associato occorre abbinare il Tag alla targa/permesso, associazione già presente nel gestionale dei permessi, ..

RFID - Radio-Frequency IDentification;

COMUNE DI VERONA -

doc. web n. 1875840

Il Comune, rappresentando le modalità di funzionamento del sistema, ha evidenziato che esso è composto "da un'antenna posta su un palo collegata ad una piccola unità locale che registra una sola informazione e cioè il numero univoco", con cui il Tag è identificato dal produttore. "Tali antenne sono poste sia in corrispondenza degli ingressi (varchi ZTL esistenti) sia in corrispondenza di tutte le uscite dove è presente un varco elettronico".(…). Per sapere a chi appartiene il veicolo/permesso associato occorre abbinare il Tag alla targa/permesso, associazione già presente nel gestionale dei permessi, già soggetto a rigorose misure di sicurezza informatica sotto il profilo della privacy". Il Comune ha precisato, inoltre, che il sistema potrebbe essere attivo 24 ore su 24, registrare i Tag (ingresso e uscita) e consentire di penalizzare i veicoli che risulteranno essere usciti dalla Ztl oltre l´orario consentito. Al riguardo, è stato evidenziato che le sanzioni da applicare ai trasgressori sono "ancora oggetto di discussione, ma che un´ipotesi potrebbe essere la sospensione dell´autorizzazione per un periodo di tempo a seguito della reiterata uscita oltre i limiti (per esempio alla terza volta). Successivamente (…), il trasgressore verrebbe sanzionato solo se accedesse comunque alla Ztl nel periodo di sospensione".

Il Comune ha precisato, altresì, che non avrà la "possibilità di tracciare in modo continuativo i veicoli da monitorare, perché non viene registrata alcuna informazione sul percorso seguito e l´unica informazione restituita dal sistema è il Tag".

RFID - Radio-Frequency IDentification;

COMUNE DI VERONA -

2.2. Il sistema Rfid che il Comune di Verona intende installare.

In tale quadro, con riferimento all´ipotesi generale di cui all´art. 17 del Codice, si rileva che il trattamento di dati personali che il Comune di Verona intende effettuare tramite il sistema Rfid descritto in premessa non necessita della verifica preliminare del Garante, non presentando rischi specifici per i diritti e le libertà fondamentali degli interessati. Ciò, innanzitutto in considerazione delle garanzie rappresentate dal titolare in relazione alle modalità del trattamento che verranno di seguito illustrate (cfr. infra punto 3); inoltre, perché il trattamento riguarda unicamente dati personali -diversi da quelli sensibili e giudiziari- non direttamente identificativi degli interessati e, infine, perché le uniche operazioni di trattamento che il Comune di Verona intende effettuare sono la rilevazione e la conservazione di dati personali che non determinano, sulla base di quanto rappresentato, alcun effetto particolare sulla vita privata degli interessati, nel caso di specie gli intestatari delle targhe dei veicoli utilizzati per il trasporto delle merci nella Ztl.

Il predetto trattamento di dati personali non rientra, inoltre, nelle particolari ipotesi, puntualmente individuate dal Garante nei provvedimenti generali del 9 marzo 2005 e dell´8 aprile 2010 sopra citati, per le quali è stato prescritto ai titolari l´obbligo di richiedere una verifica preliminare.

RFID - Radio-Frequency IDentification;

COMUNE DI VERONA -

si rileva, in primo luogo, che il trattamento dei dati personali in esame attiene alle funzioni istituzionali del Comune, in quanto è finalizzato ad individuare i trasgressori delle regole concernenti gli orari di ingresso e di uscita dalla Ztl dai veicoli adibiti al trasporto merci. Il Codice della strada, infatti, prevede che nei centri abitati i comuni possono, con ordinanza del Sindaco, prescrivere orari e riservare spazi per i veicoli autorizzati per il carico e lo scarico delle cose (cfr. artt. 11, comma 1, lett. a) e 18 del Codice; art. 7, comma 1, lett. g) del Codice della strada).

Inoltre, in conformità ai principio di necessità, il sistema Rfid descritto in premessa consente l´identificazione dell´interessato solo in caso di necessità (cfr. art. 3 del Codice). Il sistema, invero, non comporta il trattamento sistematico di dati identificativi diretti, ma di soli numeri di identificazione personali che non consentono di risalire immediatamente all´identità dell´interessato. Il sistema, infatti, effettua la rilevazione e la registrazione delle targhe, associate al codice univoco con cui il Tag è identificato dal produttore, dei veicoli autorizzati all´accesso alla Ztl per il carico e lo scarico delle merci. In tale modo, quindi, l´identificazione dell´interessato può avvenire solo nel momento in cui, attraverso la targa, si intende risalire all´intestatario del veicolo, unicamente quando sia necessario individuare il trasgressore delle regole concernenti gli orari di ingresso e di uscita dalla Ztl dei veicoli adibiti al trasporto merci.

RFID - Radio-Frequency IDentification;

COMUNE DI VERONA -

Si rileva, inoltre, la pertinenza e non eccedenza delle informazioni trattate rispetto alla finalità perseguita (cfr. art. 11, comma 1, lett. d) del Codice). Da una parte, infatti, le targhe dei veicoli autorizzati all´accesso alla Ztl sono indispensabili al Comune di Verona per identificare i trasgressori delle regole concernenti gli orari di ingresso e di uscita dalla Ztl dei veicoli adibiti al trasporto merci; dall´altra non risulta, sulla base di quanto rappresentato, che il predetto Comune intenda trattare ulteriori informazioni.

A tutela della libertà e dignità degli interessati, nonché a garanzia del divieto di controllo a distanza dell´attività dei lavoratori, il Comune di Verona ha rappresentato, infine, che il sistema Rfid in esame non consente "di tracciare in modo continuativo i veicoli da monitorare, perché non viene registrata alcuna informazione sul percorso seguito".

RFID - Radio-Frequency IDentification;

COMUNE DI VERONA -

4.1. Informativa.

Preliminarmente, si richiama l´obbligo per il Comune di Verona di fornire idonea informativa agli interessati in relazione al trattamento di dati personali che intende effettuare attraverso il sistema Rfid descritto in premessa (cfr. art. 13 del Codice).

A tal fine, si prescrive al Comune di Verona di informare, ai sensi dell´art. 13 del Codice, gli intestatari delle targhe dei veicoli utilizzati per il trasporto delle merci nella Ztl, sul trattamento dei dati personali che intende effettuare tramite il sistema Rfid, all´atto della richiesta del permesso per l´accesso alla Ztl per il trasporto merci e comunque prima dell´istallazione del sistema Rfid sui veicoli autorizzati ovvero, qualora tali sistemi siano già stati installati, prima della loro attivazione.

RFID - Radio-Frequency IDentification;

COMUNE DI VERONA -

4.3. Conservazione dei dati.

Con riferimento al tempo di conservazione dei dati trattati nell´ambito del sistema Rfid in esame, si ritiene che possano essere applicati i medesimi principi di garanzia previsti, al riguardo, per i sistemi di controllo degli accessi alla Ztl sia nella normativa di settore (d.P.R. 22 giugno 1999, n. 250), sia nel provvedimento generale del Garante in materia di videosorveglianza dell´8 aprile 2010 (cfr. in particolare punto 5.3).

In tale quadro, pertanto, il Comune di Verona nel rilevare, tramite l´impianto in esame, il numero di targa dei veicoli che entrano ed escono dalla Ztl per il trasporto delle merci, può conservare tali informazioni solo per il tempo a tale scopo necessario. A tal fine, si prescrive al Comune di Verona:

a)in caso di ingresso e di uscita di un veicolo nei tempi consentiti, di cancellare subito dopo l´uscita il numero di targa e le altre informazioni raccolte -secondo le modalità di seguito descritte (cfr, punto 4.4., lett. b);

b)in caso di infrazione, di conservare le informazioni rilevate, per il periodo necessario alla contestazione dell´infrazione stessa, all´applicazione dalla sanzione e alla definizione dell´eventuale contenzioso.

RFID - Radio-Frequency IDentification;

COMUNE DI VERONA

5. Incaricati del trattamento.

Si richiama, infine, l´obbligo per il Comune di Verona di:

a)designare, anche per il tramite del responsabile, per iscritto le persone fisiche, incaricate del trattamento delle informazioni raccolte e, nei casi in cui sia indispensabile per lo scopo perseguito, autorizzate anche a identificare gli interessati (art. 30 del Codice);

b)individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, ivi compresi gli addetti alla gestione e alla manutenzione del sistema, distinguendo coloro che sono unicamente abilitati ad accedere ai dati trattati dai soggetti che, invece, possono anche effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, identificare gli interessati attraverso l´incrocio con ulteriori informazioni, al fine di applicare le sanzioni previste) (cfr. punti 13 e 15, Allegato B al Codice).

+

CONCLUSIONE

“Il problema non è la tecnologia, ma l'uso che se ne fa. Ogni cosa comporta dei rischi, l'importante è esserne consapevoli e valutare se il prezzo che paghiamo (meno privacy) è adeguato a quanto riceviamo in cambio.” - cit. S. Nasetti