SMARTPHONE SUL POSTO DI LAVORO: VALUTAZIONE DEI RISCHI E MISURE GIURIDICHE DI PROTEZIONE DELL'AZIENDA

Avv. Gianni Cattaneo, Lugano
www.infodiritto.net
contatto@infodiritto.net

Indice tematico

A) Imperativi aziendali
B) Nuove opportunità e nuovi rischi
C) Misure regolamentari di contenimento dei rischi
D) La sorveglianza elettronica
E) Follow-up
F) Conclusioni

A) Imperativi aziendali

- Sicurezza
  - Dati aziendali, furto d'identità, accesso indebito
- Segreti d'affari e commerciali, informazioni confidenziali
- Tutela dei partner
  - clienti, fornitori, consulenti e dipendenti
- Funzionalità
  - Piattaforma interna, accesso remoto, e-mail, sito web
- Reputazione e fiducia

B) Nuove opportunità

- Disponibilità 24/7
- Produttività
- Accesso all'informazione
- Flessibilità del lavoro
- Soddisfazione dell'utente

B) Nuovi rischi

- Tracciabilità del comportamento (web, e-mail)
- Geolocalizzazione
- Sicurezza
  - intercettazione e furto di dati, furto d'identità, compromissione piattaforma aziendale (accesso indebito, diffusione malware ecc.)
- Furto / perdita del dispositivo
- Perdita di controllo IT manager
- Scarso rigore nelle comunicazioni
- Errori di valutazione
- Dipendenza?

C) Strumenti giuridici

IT governance

Direttiva tecnica sul settore IT

Direttiva sull'uso dell'informatica, di Internet e degli altri mezzi di comunicazione

Informativa in tema di sorveglianza del dipendente sul posto di lavoro

C) Strumenti giuridici

Premessa: misure tecniche di protezione dell'azienda e di tutela dei dipendenti e degli altri partner giocano un ruolo fondamentale e preminente in questo campo:

- autenticazione dell'utente: password;
- protezione contro accessi non autorizzati: attribuzione diritti d'accesso;
- protezione da attacchi esterni: firewall (HW/SW);
- cifratura dati e comunicazioni confidenziali;
- antivirus client e server;
- backup.

Omissione: colpa concomitante del datore di lavoro (riduzione risarcimento), responsabilità per omessa tutela nel caso di una lesione della personalità arrecata al dipendente

C) Direttiva sull'uso dell'informatica, di Internet e degli altri mezzi di comunicazione

Base legale

Art. 321 d CO

Osservanza di direttive e di istruzioni

1 Il datore di lavoro può stabilire direttive generali sull'esecuzione del lavoro e sul comportamento del lavoratore nell'azienda o nella comunione domestica e dargli istruzioni particolari.

2 Il lavoratore deve osservare secondo le norme della buona fede le direttive generali stabilite dal datore di lavoro e le istruzioni particolari a lui date.

Errore concettuale da evitare: non è un contratto, bensì una serie di regole di condotta stabilite dal datore di lavoro. «Ricevute, lette e comprese» e non «accettate».

C) Direttiva sull'uso dell'informatica, di Internet e degli altri mezzi di comunicazione

Dovere del datore di lavoro: comportamento proattivo

Art. 328 CO

Protezione della personalità del lavoratore

1 Nei rapporti di lavoro, il datore di lavoro deve rispettare e proteggere la personalità del lavoratore, avere il dovuto riguardo per la sua salute e vigilare alla salvaguardia della moralità. In particolare, deve vigilare affinché il lavoratore non subisca molestie sessuali e, se lo stesso fosse vittima di tali molestie, non subisca ulteriori svantaggi.

2 Egli deve prendere i provvedimenti realizzabili secondo lo stato della tecnica ed adeguati alle condizioni dell'azienda o dell'economia domestica, che l'esperienza ha dimostrato necessari per la tutela della vita, della salute e dell'integrità personale del lavoratore, in quanto il singolo rapporto di lavoro e la natura del lavoro consentano equamente di pretenderlo.

C) Direttiva sull'uso dell'informatica, di Internet e degli altri mezzi di comunicazione

Art. 4 LPar

Divieto di discriminazione in caso di molestia sessuale

Per comportamento discriminante si intende qualsiasi comportamento molesto di natura sessuale o qualsivoglia altro comportamento connesso con il sesso, che leda la dignità della persona sul posto di lavoro, in particolare il proferire minacce, promettere vantaggi, imporre obblighi o esercitare pressioni di varia natura su un lavoratore per ottenerne favori di tipo sessuale.

TF: mostrare, esporre, mettere a disposizione e inviare materiale pornografico (anche per via elettronica), osservazioni allusive e «barzellette» sessiste, contatti fisici molesti e palpeggiamenti, ecc. tra / a dipendenti costituiscono molestie sessuali.

C) Direttiva sull'uso dell'informatica, di Internet e degli altri mezzi di comunicazione

Conseguenze per l'azienda:

art: 5 cpv. 3 LPar: nel caso di discriminazione mediante molestia sessuale, il tribunale o l'autorità amministrativa può parimenti condannare il datore di lavoro ed assegnare al lavoratore un'indennità, a meno che lo stesso provi di aver adottato tutte le precauzioni richieste dall'esperienza e adeguate alle circostanze, che ragionevolmente si potevano pretendere da lui per evitare simili comportamenti o porvi fine. L'indennità è stabilita considerando tutte le circostanze, in base al salario medio svizzero;

art. 5 cpv. 4 LPar: qualora la discriminazione avvenga … mediante molestie sessuali, l'indennità prevista ai capoversi 2 o 3 non eccede l'equivalente di sei mesi di salario.

C) Direttiva sull'uso dell'informatica, di Internet e degli altri mezzi di comunicazione

Contenuto della Direttiva:
- destinatari
- informativa sui rischi e principio di precauzione
- regole di comportamento

Tematiche classiche:
a) uso privato vs. uso professionale
b) segretezza dati d'accesso
c) politica password
d) legalità
e) sicurezza
f) gestione dei dati aziendali confidenziali
g) sensibilizzazione sui rischi
h) comportamento in caso di catastrofe o compromissione sicurezza
i) dati personali e fine del rapporto di lavoro

C) Direttiva sull'uso dell'informatica, di Internet e degli altri mezzi di comunicazione

Smartphone: direttiva generale o specifica?

- destinatari
- telefono personale o professionale?
- uso privato vs. uso professionale
- servizi attivi da remoto: vpn, e-mail, cloud ecc.
- certificazione e collaudo del device
- dati aziendali: partizione protetta, restrizioni e divieti (dati confidenziali)
- procedura in caso di furto e perdita: reporting immediato
- procedure speciali in caso di viaggi all'estero (es. Cina e Russia)
- avvertenza: cancellazione da remoto: quid dei file personali?
- educazione alla sicurezza
- regole d'uso:
  - gps / wifi / blutooth disattivati
  - divieto jailbreak sistema operativo
  - antivirus e password d'accesso
  - divieto di accesso account personali privati (es. google / gmail)

D) La sorveglianza elettronica del dipendente

Nozione:

Analisi delle comunicazioni e delle registrazioni a giornale al fine di ricostruire il comportamento del dipendente in relazione all'utilizzo dei mezzi informatici e di telecomunicazione aziendali (e-mail, web, telefono, stampante, ecc.).

Scopi:

a) garantire la sicurezza e la funzionalità del sistema informatico aziendale
b) verificare un sospetto di abuso o un abuso delle normative interne (uso privato web / e-mail, ad esempio)
c) verificare un sospetto di reato penale (furto o modifica di dati, diffamazione, molestia sessuale sul posto di lavoro, diffusione di materiale razzista o pornografico, sabotaggio, spionaggio industriale, ecc.)

Quesito di fondo:

A quali condizioni ed entro quali limiti il datore di lavoro può analizzare le tracce elettroniche lasciate da un dipendente per controllare il suo comportamento in azienda?

D) La sorveglianza elettronica del dipendente

Magic Tool: KidLogger.net, versione di base gratuita

Smartphone: Mobile phone tracking

a) SMS / MMS: *record all incoming/outgoing SMS messages with phone number and recipient name.*

b) keystrokes: *soft Keyboard PRO keylogger for Android phones allows to record keystrokes typed in the phone on-screen keyboard and text copied into clipboard;*

c) photos: *allows to record and upload fact of taken photos created with phone camera;*

d) calls: *record calls incoming/outgoing – make reports of the most often used contacts;*

e) coordinates: *records point to point navigation during the day, by GPS or WiFi coordinates. Register location in real time mode;*

f) Wi-Fi, USB, SD card and GSM connection: *will help you to supervise most important connections on phone (with Android software). Connection to Wi-Fi network. SD card usage by USB cable. GSM states like ON\Off or airplane mode;*

g) used applications: *record the list of applications that user use on the mobile phone based on Android;*

h) visited web sites history: *record and save visited web sites history (only default phone browser).*

D) La sorveglianza elettronica del dipendente

Magic Tool: KidLogger.net

Un tale sistema può essere legalmente utilizzato in Svizzera per sorvegliare i dipendenti?

No! **Divieto generale dei programmi spia**. Violazione grave della privacy, con valenza sia civile, sia penale

Forse non nella Repubblica di Moldavia?

Abuse

If you noticed KidLogger application running on your device without your consent, you may inform us about this case. We do not support illegal usage of KidLogger service and prevent this. Please send us a message with Your name and Device ID (Device ID can be found in the application options or settings dialog box). We will block the account holder and delete all information about your device.

D) La sorveglianza elettronica del dipendente

Limiti di diritto privato:

A) Art. 328 CO

Protezione della personalità del lavoratore

1 Nei rapporti di lavoro, il datore di lavoro deve rispettare e proteggere la personalità del lavoratore, avere il dovuto riguardo per la sua salute e vigilare alla salvaguardia della moralità. In particolare, deve vigilare affinché il lavoratore non subisca molestie sessuali e, se lo stesso fosse vittima di tali molestie, non subisca ulteriori svantaggi.

2 Egli deve prendere i provvedimenti realizzabili secondo lo stato della tecnica ed adeguati alle condizioni dell'azienda o dell'economia domestica, che l'esperienza ha dimostrato necessari per la tutela della vita, della salute e dell'integrità personale del lavoratore, in quanto il singolo rapporto di lavoro e la natura del lavoro consentano equamente di pretenderlo.

B) Segreto delle comunicazioni: emanazione della personalità protetta (art. 28 e segg. CC, art. 7 e 10 cpv. Costituzione federale)

D) La sorveglianza elettronica del dipendente

C) Art. 328*b* CO

Nel trattamento di dati personali

Il datore di lavoro può trattare dati concernenti il lavoratore soltanto in quanto si riferiscano all'idoneità lavorativa o siano necessari all'esecuzione del contratto di lavoro. Inoltre, sono applicabili le disposizioni della legge federale del 19 giugno 1992 sulla protezione dei dati.

NB *dati personali*: tutte le informazioni relative a una persona identificata o identificabile (art. 3 a. LPD)

DTF 136 II 508 c. 3.2: principio di determinabilità relativa

D) Principio di proporzionalità: obbligo di minimizzazione del trattamento dei dati personali

D) La sorveglianza elettronica del dipendente

Limiti di diritto pubblico:

A) Art. 6 Legge sul lavoro

Obblighi del datore di lavoro e del lavoratore

1 A tutela della salute dei lavoratori, il datore di lavoro deve prendere tutti i provvedimenti, che l'esperienza ha dimostrato necessari, realizzabili secondo lo stato della tecnica e adeguati alle condizioni d'esercizio. Deve inoltre prendere i provvedimenti necessari per la tutela dell'integrità personale dei lavoratori.

2 Egli deve segnatamente apprestare gli impianti e ordinare il lavoro in modo da preservare il più possibile i lavoratori dai pericoli per la salute e dagli spossamenti.

2bis Il datore di lavoro veglia affinché il lavoratore non debba consumare bevande alcoliche o altri prodotti psicotropi nell'esercizio della sua attività professionale. Il Consiglio federale disciplina le eccezioni.

3 Egli fa cooperare i lavoratori ai provvedimenti sulla protezione della salute nel lavoro. Questi devono secondare il datore di lavoro quanto alla loro applicazione.

4 I provvedimenti sulla protezione della salute nel lavoro necessari nelle aziende sono definiti mediante ordinanza

D) La sorveglianza elettronica del dipendente

B) Art. 26 OLL3

1 Non è ammessa l'applicazione di sistemi di sorveglianza e di controllo del comportamento dei lavoratori sul posto di lavoro.

2 I sistemi di sorveglianza o di controllo, se sono necessari per altre ragioni, devono essere concepiti e disposti in modo da non pregiudicare la salute e la libertà di movimento dei lavoratori.

Attenzione: interpretazione restrittiva del TF (Sentenza TF 6B_536/2009)

D) La sorveglianza elettronica del dipendente

Strumenti di interpretazione:

1. «Guida al trattamento dei dati personali nell'ambito del lavoro» (trattamento da parte di persone private);
2. «Sorveglianza dell'utilizzazione di Internet e della posta elettronica sul posto di lavoro» (per le amministrazioni pubbliche e l'economia privata);
3. Commentario SECO LL / OLL;
4. Dottrina e giurisprudenza.

D) La sorveglianza elettronica del dipendente

Regole di base (posizione dell'IFPD):

i. misure preventive d'ordine tecnologico e organizzativo
ii. direttiva sull'uso dell'informatica, di Internet e degli altri mezzi di comunicazione
iii. informativa in tema di sorveglianza del dipendente sul posto di lavoro:
   a. strumenti di controllo elettronico
   b. tipologie di dati personali oggetto di trattamento
   c. sanzioni in caso di violazione del regolamento (DTF 119 II 162 c. 2: determinabili in anticipo e proporzionate)
   d. persone incaricate del controllo
iv. no ai programmi spia
v. sì alle misure di controllo costanti se anonime o sotto pseudonimo
vi. sì alle misure di controllo personalizzate se:
   a. dai controlli anonimi / sotto pseudonimo è emersa una violazione della normativa interna
   b. denuncia circostanziata di terzi
   c. sospetto fondato di comportamento illecito, anti-contrattuale o penalmente rilevante

Attenzione: controllo su base personalizzata non è giustificabile retroattivamente se viene accertato un abuso.

E) Follow-up

Follow up:

1. consegnare copia delle direttive al dipendente
2. illustrare le disposizioni nel corso di conferenze o colloqui personali
3. richiedere conferma scritta: ricezione, lettura e comprensione
4. mettere a disposizione una persona per ulteriori spiegazioni o altre necessità
5. organizzare periodicamente seminari e conferenze su tematiche inerenti la normativa sul contratto di lavoro, la sicurezza informatica, il cybercrime ecc.;
6. sanzionare in maniera documentabile la violazione delle disposizioni aziendali sul contratto di lavoro

Attenzione: divieto dell'uso privato di Internet e della posta elettronica: emettere formali diffide, rispettivamente comminare adeguate sanzioni disciplinari, onde evitare che dalla tolleranza possa essere dedotta una rinuncia ad opporre il divieto.

F) Conclusioni

Opinione personale (azienda con esigenze elevate di tutela della confidenzialità):

1. adottare un regolamento professionale sull'informatica e sulla cybersorveglianza
2. l'uso dello smartphone va regolato in un documento speciale
3. «coltivare» la normativa interna: seminari di informazione / sensibilizzazione e verifiche anonimizzate costanti sul rispetto del medesimo;
4. no all'integrazione di dispositivi mobili personali e/o di tipo consumer (no mescolanza tra ciò che è personale e ciò che è professionale);
5. sì all'integrazione di dispositivi mobili basati su tecnologia professionale con le seguenti limitazioni:
    1. verifica rigorosa della cerchia di destinatari (necessità e affidabilità);
    2. delimitazione rigorosa / restrittiva dei servizi informatici utilizzabili da remoto;
    3. implementazione di misure tecniche di sicurezza e con effetto preventivo;
    4. uso privato escluso o ristretto al minimo;
    5. divieto di installare software senza l'approvazione dell'IT manager;
    6. password, software di cancellazione da remoto, antivirus.