A gentile richiesta

Modifica contrattuale della percentuale lavorativa e gestione vacanze residue

"Come deve essere gestito dal datore di lavoro il saldo dei giorni di vacanza residui nel momento in cui il grado di occupazione del dipendente viene contrattualmente modificato?"
Il datore di lavoro ed il lavoratore hanno la possibilità di concordare una modifica contrattuale volta a diminuire, rispettivamente ad aumentare, la percentuale lavorativa del dipendente. Il datore di lavoro è altresì libero di intimare unilateralmente al dipendente una modifica di questa portata, tramite la procedura di modifica-disdetta del contratto di lavoro. Nel caso in cui vi siano dei giorni di ferie di cui il dipendente non ha usufruito, questi vengono riportati nella nuova versione del contratto di lavoro, comprensiva della modifica del grado di occupazione. Si pone di conseguenza la questione a sapere come debbano essere conteggiati tali giorni di vacanza dal datore di lavoro, in virtù del nuovo grado occupazionale.
L'art. 329a CO sancisce che il datore di lavoro deve accordare al lavoratore, ogni anno di lavoro, almeno quattro settimane di vacanza; ai lavoratori sino ai 20 anni compiuti, almeno cinque settimane. L'unità di calcolo previsto dal CO, fissata in settimane, dipende dalla durata ordinaria di lavoro di ogni lavoratore, variando per ciascuno di essi in funzione del numero dei giorni lavorativi in ogni settimana. Rispetto a tale unità, ogni lavoratore dispone del medesimo diritto alle ferie. Sia in caso di lavoro a tempo parziale, sia in caso di lavoro a tempo pieno, qualunque sia il numero di giorni alla settimana su cui è ripartito il tempo di lavoro, il diritto minimo alle vacanze sarà di quattro o cinque settimane all'anno. A seconda del tasso di attività, rispettivamente del numero di giorni lavorati alla settimana, le quattro (o cinque) settimane di vacanza non corrisponderanno al medesimo numero di ore o giorni di lavoro. Al fine di convertire in giorni il diritto annuale alle ferie è necessario tenere conto del numero di giorni in cui il dipendente è di consueto occupato.
Ne consegue che per un dipendente occupato al 50%, ovvero per due giorni e mezzo alla settimana, le quattro settimane di vacanza non corrispondono a venti giorni pieni di vacanza, bensì a dieci giorni pieni. Nel calcolo dei giorni residui di vacanza in caso di modifica del grado di occupazione del dipendente, occorre di conseguenza tenere in considerazione che il numero di giorni di vacanza con un grado di occupazione al 100% non corrisponde al medesimo numero di giorni per un grado di occupazione, ad esempio, al 50%. Prendiamo l'esempio di un dipendente occupato al 50% che, a seguito di una modifica contrattuale, presta servizio al 100%, con due giorni di vacanza residui, intesi come due mezze giornate nell'arco di due giorni. Con l'aumento della percentuale lavorativa al 100% egli avrà diritto a un giorno pieno di ferie. Nella situazione inversa invece, se il dipendente dispone di un saldo vacanze residuo di due giorni pieni, con la riduzione della percentuale lavorativa al 50% egli avrà diritto a usufruire di quattro mezze giornate nell'arco di quattro giorni. Tali esempi mostrano come il datore di lavoro debba convertire con attenzione le quattro settimane di vacanza in giorni di ferie effettivi, a seconda del numero di giorni concretamente lavorati dal dipendente nell'arco della settimana lavorativa, i quali possono effettivamente variare a seconda della percentuale lavorativa stabilita contrattualmente.

Simone Beraldi, avvocato - Studio Delogu

Modifiche del contratto - Disdetta-modifica: Manuale 3.3.1
Vacanze: Manuale 3.2.4.1

Giurisprudenza

Disdetta senza preavviso da parte del lavoratore causa insolvenza del datore di lavoro. *Sentenza della Seconda Camera civile del Tribunale d'appello 12.2019.72 del 14 maggio 2020.*
In caso di ritardi nel pagamento degli stipendi il lavoratore può rifiutare di lavorare se ha preventivamente diffidato il datore di lavoro, avvertendolo che in caso di mancato pagamento degli arretrati si asterrà dal lavoro. In questa evenienza il contratto di lavoro rimane in vigore ed il lavoratore non può essere rimproverato per abbandono del posto di lavoro. L'insolvenza del datore di lavoro può giustificare, secondo l'art. 337a CO, il licenziamento immediato da parte del lavoratore, con la possibilità di chiedere il risarcimento del danno (art. 337b CO). D era direttore del controllo qualità di un'industria, con un salario mensile lordo di fr. 7'000.- per tredici mensilità. Il datore di lavoro, in grave crisi economica, lo ha licenziato il 27 marzo 2013 con effetto dal 31 maggio 2013. Il 4 aprile 2013 D ha diffidato la ditta dal versargli gli stipendi arretrati di dicembre, gennaio e febbraio entro le ore 12.00 del giorno seguente, avvertendo che in caso di mancato pagamento sarebbe stato libero di disdire con effetto immediato il contratto. Allo scadere infruttuoso del termine D si è licenziato con effetto immediato e ha poi promosso causa contro il datore di lavoro chiedendo il versamento di fr. 56'032.90 lordi per crediti salariali e fr. 32'206.30 netti in risarcimento del danno. L'azione giudiziaria è stata respinta dal Pretore, secondo il quale i crediti salariali effettivamente maturati erano già stati pagati, mentre non vi era il diritto al risarcimento del danno, mancando le condizioni poste dall'art. 337a CO. Su ricorso di D, la Seconda Camera civile del Tribunale d'appello ha confermato la sentenza del Pretore. I giudici di appello hanno esaminato le condizioni alle quali il lavoratore può licenziarsi con effetto immediato in caso di insolvenza del datore di lavoro. L'insolvenza è data dopo l'apertura di un fallimento o l'ordine di pignoramento, o una domanda di moratoria concordataria (provvisoria), o la prova di un massiccio ritardo di pagamento da parte del datore di lavoro o di un sovraindebitamento. Problemi temporanei di liquidità non sono invece sufficienti. Il lavoratore deve fissare al datore di lavoro un termine adeguato (di regola 3-5 giorni, 10 giorni in casi particolari) entro il quale prestare una garanzia per il pagamento degli stipendi futuri. La garanzia può avere diverse forme: garanzia bancaria, blocco del conto, fideiussione, messa in pegno di beni facilmente realizzabili, ecc., ma in ogni caso copre solo i crediti futuri, non quelli già maturati. Nel caso concreto, D aveva assegnato al datore di lavoro un termine troppo breve e non aveva chiesto garanzie per i salari futuri, ma il pagamento di quelli arretrati. Il licenziamento senza preavviso in applicazione dell'art. 337a CO non era quindi giustificato e il lavoratore non poteva quindi vantare alcun risarcimento del danno.

Emanuela Colombo Epiney,
avvocato, già giudice

Disdetta immediata per insolvenza del datore di lavoro: Manuale 4.4.4

IMPRESSUM
NewsletterLavoro è la pubblicazione mensile del sistema d'informazione **Il diritto del lavoro applicato**.
Editore: Boss Editore SA.
Resp. Newsletter: Gian Luigi Trucco.
Hanno collaborato: Alessandro Trivilini, Gianni Cattaneo, Simone Beraldi ed Emanuela Colombo Epiney.
Boss Editore SA - CH 6900 Lugano
tel. +41(0)91 600 93 03
Amministrazione: info@boss-editore.ch
© www.boss-editore.ch

BOSS conoscenza applicata
NEWSLETTER LAVORO
Maggio 2021

Editoriale

Gli attacchi informatici sono in aumento ed il periodo di pandemia ne ha accresciuto l'impatto. Colpiscono privati ed aziende di ogni dimensione e settore economico. Provengono da dilettanti ed "artigiani" del crimine o da organizzazioni strutturate fino ai livelli più elevati. Puntano alla truffa, all'estorsione finanziaria o alla raccolta di dati e informazioni sensibili, su prodotti, programmi di sviluppo, alla ricerca di "scorciatoie" per le strategie societarie, tanto più quanto il comparto è avanzato. Possono anche puntare ad informazioni sulle persone, fornitori e clienti, così come manager ed amministratori, da condizionare in modo illecito secondo la vecchia tecnica del "kompromat" sovietico (e non solo).
Tutto questo può nascere da un momento di disattenzione o da una negligenza del collaboratore, dall'aprire incautamente una e-mail o inoltrare con disinvoltura una comunicazione. Ma al di là dei comportamenti del singolo, l'azienda è chiamata a regolamentare l'ambito informatico, attribuendo responsabilità definite, controllando, prevedendo procedure per prevenire e soprattutto affrontare tempestivamente ed efficacemente gli "incidenti" quando essi si verifichino. E l'estensione dell'home working impone controlli ancora più severi, naturalmente nei limiti della legge. Se la regolamentazione aiuta l'azienda, l'evoluzione normativa, sempre più standardizzata a livello internazionale, ne accresce responsabilità e potenziali danni, legali, operativi, finanziari e di immagine. Temi ampi e complessi, sui quali presentiamo i contributi di due esperti: Alessandro Trivilini, docente e ricercatore della SUPSI, e l'Avv. Gianni Cattaneo.

Gian Luigi Trucco

All'interno:

Aziende e Ciberattacchi

Fattore umano e responsabilità

Intervista ad Alessandro Trivilini, docente e ricercatore, Responsabile del Servizio di informatica forense della SUPSI

Si dice che spesso dietro ai "problemi" informatici, anche in azienda, vi siano errori e comportamenti umani inadeguati. Di cosa si tratta?
Gli errori riconducibili al fattore umano sono dovuti alla capacità di inganno di messaggi che, ad esempio come e-mail, possono arrivare in azienda a tutti i livelli, dall'Amministratore Delegato alla segretaria. Messaggi truffaldini costruiti con finalità di phishing, che recano contenuti testuali, immagini, multimediali, volti ad ingannare i sensi cognitivi delle persone cui si rivolgono, sfruttando tre elementi di ingegneria sociale, vecchi e caratteristici dell'essere umano nel rispondere a certi stimoli, determinanti se arrivano nel momento opportuno e alla persona giusta. Rivolti al target scelto e controllato attraverso i social media, si rivelano cruciali, convincono e persuadono la persona in tre secondi (ce lo indicano le ricerche) a "credere o non credere" a quello che legge e che vede.
Pescando in un universo di milioni di persone cui queste e-mail si rivolgono in base alla tipologia di profilo, non stupisce che le statistiche dei crimini informatici siano molto alte. Questi tre elementi sono la memoria, li linguaggio e l'attenzione. Lo scopo è ingannare, far credere che il contenuto sia vero, indurre a fare "clic", "send" o "download", trasformare cioè l'intenzione in azione. Si opera sullo stile comunicativo del testo e dell'istituzione, su logo, foto, linea grafica ed altri elementi che danno la percezione di fiducia e trasparenza, perfino su espressioni tipiche che sollecitano la memoria del destinatario e catturano la sua attenzione. Queste azioni si rivelano tanto più efficaci quando colgono il collaboratore in un momento di pressione psicologica, di stress, di fretta, di fragilità, e lo fanno cadere nella trappola. Così si cedono dati, un "trojan" bypassa i privilegi del sistema e gli eventuali controlli e le informazioni vengono trasmesse.
Quanto è importante la password ed il cambiarla per la sicurezza informatica?
La stessa password non va tenuta per molto tempo, ma ogni realtà è diversa e non c'è una regola precisa. Si può dire che se la password è semplice, composta solo di numeri o solo di lettere, esistono algoritmi che, provando e riprovando, riescono a trovare la combinazione. Se invece usiamo almeno 12 caratteri alfanumerici, quindi mescolando lettere, numeri e caratteri speciali, gli algoritmi faticano molto di più e, impiegando tempo e risorse, tendono alla fine a rinunciare.
Quali sono in generale le aziende più prese di mira, e con quali tipi di attacchi?
Il mercato del crimine informatico è vasto e variopinto. Vi sono attori provinciali e pasticcioni, ma vi è un mercato sempre

più organizzato, perché ha risorse, infrastrutture, non deve seguire linee-guida e regolamenti. E' estremamente pragmatico e si rivolge a quei luoghi aziendali, privati o semiprivati (come nel caso del lavoro da casa in cui le due realtà si mescolano), alla ricerca di "valore". Non solo denaro o cryptovalute, ma *segue a pag. 2→*

segue da pag. 1→

Fattore umano e responsabilità

anche dati, brevetti, informazioni strategiche e più o meno confidenziali, risultati di ricerche e di nuovi prodotti, quale che sia la dimensione aziendale, perché anche un'impresa piccola può essere parte di un circuito aziendale grande e diventare un canale di accesso.
Fra i "valori" ricercati vi sono anche quelli reputazionali, persone rappresentative, membri del management medio ed alto, che possono essere posti sotto ricatto con un malware. Il loro comportamento viene analizzato per esercitare un ricatto al momento opportuno, non necessariamente a scopo monetario, ma per tenerlo sotto scacco ed usare le informazioni magari in futuro, al momento di una nomina o di una votazione.

L'home working ha aumentato i rischi informatici aziendali?

L'home working ha mescolato e complicato le situazioni, accelerando processi come quello di delegare il lavoro da casa in responsabilità e sicurezza e controllando le attività con dei protocolli ben definiti. Molte aziende non erano pronte per questo. Vi era tutto un sistema di valori da costruire sulla base della fiducia e della trasparenza, attraverso la tecnologia a distanza. Si sono create situazioni diverse. Pensiamo al discusso bossware, algoritmi di monitoraggio dei collaboratori a casa. Si può arrivare a situazioni di paranoia per eccesso di controllo laddove non c'è un sistema di valori fra azienda e collaboratori tale da definire condivisione del tempo ed obiettivi. Oggi c'è bisogno di un nuovo sistema di valori, di regole e protocolli chiari.

In generale, le aziende sono attrezzate nei riguardi degli attacchi informatici?

Fino all'arrivo del Covid la percezione di sicurezza informatica era riconducibile alla voce "altri ed eventuali" nelle riunioni dei top management e dei Consigli di Amministrazione, perché l'approccio era verticale, realizzato essenzialmente in termini di antivirus, anti-intrusione, il tutto delegato ad un tecnico specialista, spesso invisibile e costoso, ma comunque non determinante per il business aziendale.
Ora lo scenario è cambiato radicalmente, anche in termini di responsabilità, visto che lo scorso 20 settembre è stata votata dal Parlamento svizzero la nuova legge sulla protezione dei dati, allineata sul General Data Protection Regulation (GDPR) europeo. Ma c'è di più, in quanto dal 2018 la Confederazione ha adottato uno standard di cybersecurity che arriva dall'America, si chiama National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), già adottato da due anni in Europa e a cui la Svizzera si è anche in questo caso allineata.
A luglio 2020 è stato creato un nuovo centro svizzero di cybersecurity (NCSC, www.ncsc.admin.ch), MELANI (Centro di Annuncio ed Analisi per la Sicurezza dell'Informazione) si è ampliato ed è stato raggiunto un chiaro livello di coordinamento, per cui la gestione della sicurezza è legata alla trattazione dei dati, nuove responsabilità emergono, non più rinviabili, a vari livelli aziendali, per cui l'assetto verticale nell'uso degli strumenti di difesa oggi diventa un processo che coinvolge tutto il personale, suggerisce un numero preciso di ore per identificare l'attacco, scoprire il tipo di attacco ed i dati che sono stati contaminati, quali danni ha arrecato, ed impone di comunicarli ai clienti nel minor tempo possibile. In base alla normativa e a questo standard perfino Facebook, per la prima volta nella sua storia, ha dovuto fare un comunicato stampa sull'attacco in meno di 24 ore, invece che l'incidente emergesse dopo anni anni.
La gestione è strutturata e coordinata, sempre più anche in Svizzera. E definito il dato personale ed il suo trattamento in un'ottica transnazionale, e la scelta è logica, perché il dato non è in un luogo fisico, e lo strumento legale della rogatoria non è più sufficiente, ha tempi troppo lunghi, i danni sono stati fatti e, se magari il "valore" è finanziario, i soldi sono già stati monetizzati.
Ormai prevenzione e gestione degli incidenti vanno gestite secondo protocolli uniformi proattivi e le aziende devono essere in grado di rilevare la minaccia ed essere preparate a rispondere. L'azienda non compliant va incontro a grosse responsabilità. Non potrà dire "non sapevo". Il processo è trasversale e si estende a tutta la filiera, dalla produzione alla vendita fino ai contatti post-vendita ed a tutte le altre attività aziendali.

La videoconferenza oggi così diffusa è una fonte ulteriore di rischio?

Abbiamo due elementi su cui misurare il rischio: la trattazione del dato e la risposta agli incidenti, che devono diventare i nostri due pilastri di riferimento.
Quindi nella video conferenza, la prima domanda da porsi è: ho acquistato una licenza oppure no? Nell'ultimo caso il prodotto sono io e devo leggere le condizioni d'uso. La sede dell'azienda che offre il servizio è in Svizzera o all'estero? I dati vengono lasciati nel Paese in cui li uso, oppure no? Zoom segue le norme GDPR ma i suoi server non sono in Svizzera, e questo potrebbe essere un problema. Altri operatori americani stanno invece portando server e data center in Svizzera. In azienda possiamo avere specialisti disponbiili, ma la questione è più delicata quando lavoriamo da casa, usando reti gratuite ma meno affidabili, con rischi reputazionali elevati per l'azienda. La scelta della tecnologia, in questo come in altri casi, diventa il fattore determinante.

A maggio il Canton Ticino ha promosso la settimana di sensibilizzazione sulla sicurezza digitale. I dati indicano come gli "incidenti", frodi, malware, phishing, furti di identità ed altro, siano in aumento ed abbiano registrato una forte crescita nel periodo della pandemia.
Ogni mese sono mediamente 25.000 gli "attacchi" in Svizzera. Il fattore umano è critico e la prima norma da adottare è quella della sana diffidenza. Fra i consigli operativi, mettere al sicuro i dati su almeno due supporti, "ripulire" periodicamente i dispositivi ed aggiornare i software, usare antivirus e password alfanumeriche complesse. A livello globale il trend si rivela allarmante, con un incremento sensibile dei casi definibili "gravi".
L'e-mail aziendale rimane uno dei principali veicoli di cyber-criminalità, con fini estorsivi, di spionaggio ed "information warfare" in generale. Target particolari il settore governativo, sanità e ricerca, finanza ed infrastrutture, oltre agli attacchi alle "supply chain" di molte aziende.
Nessuna impresa può sentirsi al sicuro, soprattutto alla luce dell'incidenza di nuovi trend, come i cosiddetti "big data", l'"internet delle cose", l'uso esteso degli apparati mobili e dei social media. I dati aziendali sono ovunque in pericolo, a fronte della nuova normativa GDPR che ha sovvertito e regolamentato il panorama in tema di privacy e gestione dei dati personali, ad iniziare da quelli della clientela. Il tema della cybersecurity va quindi posto in primo piano con opportuni investimenti, non solo in tecnologie ma anche in formazione dei dipendenti. (GLT)

Tutte le edizioni di *NewsletterLavoro* sono consultabili nell'area riservata ai clienti sul sito:
www.boss-editore.ch
Diversi indici facilitano la ricerca per parola chiave.

Informatica ed impresa: aspetti legali

Intervista all'Avv. Gianni Cattaneo, LL.M. Studio CBM Cattaneo Bionda Mazzucchelli di Lugano, docente SUPSI di diritto della privacy e della protezione dei dati personali (www.cbm-lex.ch)

Molti "incidenti" in campo informatico sono attribuibili a manchevolezze e negligenze umane. Ma in pratica di cosa si tratta?

Per iniziare, occorre definire "cosa" sia un incidente informatico.
Mutuando la definizione di violazione della sicurezza contenuta nella futura Legge federale sulla protezione dei dati, si tratta di un evento, in seguito al quale, *"in modo accidentale o illecito, dati vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate"*.
Ciò è il caso quando risultano violate, a seguito di un attacco esterno o interno, oppure di un banale errore di un collaboratore, poco importa, l'integrità, la disponibilità oppure la confidenzialità dei dati.

Semplice negligenza e disattenzione, come nel caso delle e-mail di phishing, possono comportare responsabilità legali per il lavoratore?

Certamente. Il lavoratore è responsabile del danno che cagiona intenzionalmente o per negligenza al datore di lavoro. È il caso, in particolare, se commette un atto illecito oppure una violazione del contratto di lavoro.
Riferendoci alle e-mail "trappola", occorre tuttavia che il dipendente sia stato preventivamente sensibilizzato sui rischi "cyber", e correttamente istruito su come comportarsi se si materializza un rischio.
Inoltre, occorre che l'e-mail sia riconoscibile come dannosa (spam) oppure che la richiesta veicolata dall'e-mail rientri nel novero dei comportamenti vietati dal datore di lavoro (es. inserire i dati della carta di credito in un sito "linkato" in una e-mail non richiesta).
Da ultimo, occorre che l'azienda si sia protetta in maniera diligente. Solo in un caso del genere è possibile imputare una responsabilità chiara e completa al dipendente.

Quale è il limite di demarcazione fra responsabilità "istituzionale" dell'azienda e del singolo dipendente?

L'azienda è al fronte poiché ha tutti i mezzi per prevenire gli attacchi e per minimizzare le conseguenze nocive degli stessi. L'azienda assume integralmente il rischio imprenditoriale, incluso il rischio di attacco informatico, che difficilmente, salvo il dolo (attacco insider), può essere imputato interamente al dipendente.
Anche in caso di pacifica violazione delle

normative interne, un giudice valuterebbe con attenzione se, e in quale misura, l'azienda sia stata diligente nell'implementare misure preventive adeguate al rischio e allo stato della tecnica, onde escludere, rispettivamente minimizzare, le conseguenze negative dell'attacco (es. back-up e piano di disaster recovery, firewall, anti-virus ecc.).

Di cosa si deve, o dovrebbe, dotare l'azienda, per essere al riparo?

L'azienda deve a mio avviso:

a) scegliere in maniera adeguata i propri dipendenti attribuendo ruoli adatti al profilo personale;
b) sorvegliare i dipendenti in maniera lecita e, ove necessario, sanzionare le violazioni;
c) istruire i dipendenti tramite direttive chiare e complete sull'uso di internet e dei mezzi informatici;
d) sensibilizzare regolarmente ed in maniera comprovabile i dipendenti sui rischi di sicurezza;
e) adottare tutte le misure tecniche ragionevolmente disponibili secondo il livello di rischio per prevenire le violazioni e le loro conseguenze.

L'ideale sarebbe iniziare da subito un percorso di messa in conformità alla futura Legge sulla protezione dei dati (che entrerà in vigore non prima di 12-18 mesi), nell'ambito della quale le tematiche organizzative e di sicurezza in genere vengono affrontate e risolte in maniera sistematica e coerente.

Quali sono le modalità ed i limiti della sorveglianza dei collaboratori?

È vietata la sorveglianza del comportamento sul luogo di lavoro. È per contro ammissibile una sorveglianza giustificata da motivi oggettivi, la quale deve essere retroattiva (non in tempo reale), proporzionata (ossia limitata allo stretto necessario) e svolta in maniera depersonalizzata (in maniera anonimizzata o sotto pseudonimo).
Solo in presenza di una violazione conclamata è possibile analizzare i dati raccolti per identificare le persone colpevoli. Resta inteso che nel regolamento sulla sorveglianza destinato ai dipendenti occorre illustrare i meccanismi impiegati, le regole di accesso ai dati, il periodo di conservazione e le sanzioni disciplinari in caso di violazione delle direttive interne.

L'home working modifica questo quadro giuridico?

L'home office non modifica tale quadro giuridico. Semmai rende ancora più urgente e necessario un piano di sicurezza e delle regole ad hoc da parte del datore di lavoro.
Faccio alcuni esempi. L'abitazione è in genere condivisa con altre persone, per cui non è accettabile che le telefonate con i clienti siano effettuate in viva voce davanti a estranei, oppure che i dossier professionali siano abbandonati in cucina alla mercé di chiunque, che le stampe di documenti aziendali finiscano nella raccolta della carta oppure che il computer professionale sia condiviso con i familiari. Non si tratta di questioni banali, bensì di aspetti fondamentali da regolare in una direttiva speciale.

Come si muove la normativa sul tema dei rischi informatici aziendali e della privacy?

La futura Legge federale sulla protezione dei dati prevede l'obbligo di garantire la sicurezza dei dati personali, istituendo per giunta standard minimi la cui violazione comporterà la punibilità dei dirigenti responsabili con la multa fino a CHF 250'000.-.
Inoltre, è previsto l'obbligo di comunicazione all'Incaricato federale della protezione dei dati di ogni violazione della sicurezza che comporta verosimilmente un rischio elevato per le persone interessate, come pure l'obbligo di informare queste ultime sulla violazione della sicurezza dei dati, se ciò è necessario per proteggerle o se lo esige l'IFPDT (Incaricato federale della protezione dei dati e della trasparenza).
La reputazione è un asset fondamentale, da cui dipende non solo la fiducia dei clienti, bensì il successo dell'azienda.