AXERTA®
INDAGA. DOCUMENTA. ACCERTA.

IL PUNTO

Rassegna Giurisprudenziale

Controlli e indagini nel rapporto di lavoro

Luglio-Agosto 2019

Axerta S.p.A.
Nord-ovest Piazza Duomo 17 - 20121 Milano
Centro-sud Viale Giulio Cesare 71 - 00192 Roma
Nord-est Vicolo Vincenzo Bellini 4 - 35131 Padova

800 800 007
P.IVA 10239431009 | **www.axerta.it**

L'editoriale del Presidente

Digital Forensics e Cybersecurity nella lotta all'illegalità in azienda

Gen. Michele Franzé - Presidente di Axerta S.p.a.

Periodicamente, con monotona ripetitività, ci siamo ritrovati a parlare di illeciti in ambito lavorativo, pubblico e privato, e di possibili strade da seguire per contrastare ed arginare il fenomeno, odioso sia per i contenuti di chiara illegalità, sia per il danno che si arreca ai datori di lavoro e, forse ancor di più, agli stessi lavoratori onesti.

Eppure, ancora una volta, ci ritroviamo a parlare di primari, medici ed altri dipendenti di una ASL che non esitano a timbrare il cartellino per poi abbandonare il posto di lavoro, per recarsi al mare o dedicarsi ad altre incombenze, sicuramente più gratificanti e allettanti.

È il caso, come riportato dagli organi di informazione il 15 maggio scorso, di ben otto dipendenti dell'ospedale di San Severo (Foggia), tratti in arresto a seguito di specifiche indagini della Guardia di Finanza, che ha riscontrato come gli indagati, per mascherare l'assenza dal posto di lavoro, non si limitassero a non timbrare il badge al momento dell'allontanamento, ma provvedessero ad alterare le informazioni contenute nel sistema informatico di registrazione delle presenze.

Di qui la conferma, ove mai ve ne fosse bisogno, della sempre più pressante esigenza di conciliare al meglio indagini tradizionali e digital forensics, volte alla ricerca e all'analisi dei dati contenuti nei dispositivi elettronici oggetto di quotidiano utilizzo (talvolta truffaldino, come nel caso dell'ospedale di San Severo) da parte del personale dipendente.

Da anni, ormai, il dipartimento di Digital Forensics & Cybersecurity di Axerta viene frequentemente chiamato ad indagare su accessi abusivi al sistema informatico, anche al fine di contrastare casi di spionaggio industriale e trafugamento di informazioni sensibili.

Ecco quindi che l'analisi degli strumenti informatici resta una componente fondamentale dell'indagine aziendale, ogni qualvolta vi sia la necessità di provare fatti aventi una valenza giuridica in sede civile o penale.

Ed al riguardo acquista cruciale rilevanza la recente sentenza della Cassazione numero 8541/2019, che meglio definisce gli estremi dell'accesso abusivo ad un sistema informatico, affermando come per integrare il reato di cui all'art. 615-ter c.p. sia sufficiente che l'utilizzo dello strumento non sia in linea con le autorizzazioni di chi effettua l'accesso.

"E – aggiunge la Corte – poiché lo scopo della norma è quello di inibire gli ingressi abusivi nel sistema informatico, non assume rilievo ciò che l'agente ebbe a carpire indebitamente (se notizie riservate o altrimenti recuperabili) ma l'ingresso stesso non sorretto da ragioni collegate al servizio (pubblico o privato) svolto".

Dalla consapevolezza, pertanto, che non esiste più alcun ambito lavorativo che non veda coinvolto un dispositivo digitale, risulta evidente quali e quanti siano i campi di applicazione per le indagini in materia, indagini la cui importanza ci viene confermata in ogni settore di attività, sia pubblico che privato, e che ci consente di affermare con legittimo orgoglio la valenza del nostro contributo nelle indagini tese a prevenire accessi abusivi e ad individuare i punti deboli della catena di sicurezza posta a protezione dell'informazione.

Gen. Michele Franzé
Presidente di Axerta S.p.a.

Sicurezza informatica

Quali fattispecie sono tutelate a livello legislativo e quale interpretazione ne dà la giurisprudenza

Accesso a sistema informatico: la Cassazione precisa le ragioni che lo rendono abusivo

Cass. pen. Sez. V, Sent., (ud. 09/11/2018) 27-02-2019, n. 8541

La Suprema Corte ha rigettato il ricorso di un dipendente che affermava la legittimità del proprio accesso al sistema informatico dell'azienda per scaricare alcuni documenti, che gli servivano per la causa civile in corso. Premesso che in appello l'imputato non aveva contestato l'ingresso nel sistema informatico e aveva sollevato censure unicamente con riguardo alla qualificazione del fatto dal punto di vista penale, va rilevato che, nel frattempo, è intervenuta un'altra pronuncia delle Sezioni Unite (n. 41210/2017) nella quale è stato chiarito che "integra il delitto previsto dall'art. 615-ter c.p. la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni impartite dal titolare di un sistema protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli è attribuita".

Dunque, visto che, indipendentemente dai limiti "formali" posti dall'amministratore, il lavoratore si era introdotto nel sistema per ragioni ontologicamente diverse da quelle per cui il potere gli era stato conferito, e poiché lo scopo della norma è quello di inibire "ingressi abusivi" nel sistema informatico, "non assume rilievo cosa l'agente ebbe a carpire indebitamente (se notizie riservate o altrimenti recuperabili), ma l'ingresso stesso, non sorretto da ragioni collegate al servizio (pubblico o privato) svolto".

La norma che sanziona l'accesso abusivo a sistema informatico configura un reato di pericolo. Il reato, cioè, si concretizza ogniqualvolta l'ingresso abusivo riguardi un sistema informatico in cui sono contenute notizie riservate, indipendentemente dal tipo di notizia eventualmente appresa. E non c'è dubbio che il sistema contenga notizie della più varia natura, tra cui anche notizie e dati destinati a rimanere segreti o riservati.

GDPR

La brand reputation passa per la protezione dei dati ed il risarcimento dei danni conseguenti ad una violazione

Come cambia il risarcimento del danno da violazione della Privacy

Parlamento Europeo Reg. (CE) 27/04/2016, n. 2016/679/UE, art. 82

L'articolo 82 del GDPR disciplina il diritto al risarcimento e la responsabilità del titolare del trattamento, a seguito dell'abrogazione espressa dell'art. 15 ("danni cagionati per effetto del trattamento") del D.lgs. 196/2003 ("Codice Privacy") da parte del D.lgs. 101/2018 (la norma italiana di raccordo con il GDPR).
L'articolo afferma che l'interessato possa richiedere il risarcimento dei danni materiali e immateriali, in pratica dovrà essere risarcito ogni tipo di danno che l'interessato possa subire dalla violazione dei suoi dati personali.
Il senso è ovviamente quello di attribuire all'interessato il diritto ad essere risarcito per ogni tipo di danno che quest'ultimo possa subire dalla lesione dalla violazione dei suoi dati personali; ciò anche se le definizioni di danni materiali e immateriali non sono letteralmente identiche a quelle del codice civile italiano ove il riferimento è ai danni patrimoniali e non patrimoniali.
Inoltre il Considerando 46 specifica che il concetto di danno dovrebbe essere interpretato alla luce della giurisprudenza della Corte di Giustizia ai fini di ripristino del pregiudizio subito dall'interessato.
Ciò apre la possibilità di estendere al campo della protezione dei dati personali (quale diritto fondamentale dell'UE) numerose tipologie di danni enucleate negli anni dalla Corte in questione.

Il diritto al risarcimento del danno da violazione del GDPR è la norma cardine del Regolamento UE sulla responsabilità civile nel trattamento dei dati personali e rappresenta un incentivo per titolare e responsabile del trattamento a predisporre le misure di sicurezza idonee a impedire la violazione dei dati personali.

Quanto può costare un data breach aziendale?

Cybersecurity360.it, Avv. Alessandro Ronchi – Digital and data protection lawyer

Gli articoli 32 e seguenti del GDPR indicano alcuni strumenti tecnici ritenuti validi per garantire la sicurezza dei dati, prevenendo i danni tipici conseguenti ad un evento di data breach (pseudonimizzazione e cifratura, procedure di testing periodiche dei sistemi informatici, formazione del personale ecc.).
In questo contesto non deve, peraltro, essere dimenticato che un ruolo fondamentale è rivestito dall'adozione di opportune misure organizzative da parte del Titolare del trattamento sia sul fronte interno (la propria organizzazione) sia sul fronte esterno (ad esempio, i propri fornitori).
Pensiamo, ad esempio, al danno reputazionale che può subire un'azienda operante nel mercato digitale a causa di un data breach sui dati dei propri clienti affidati ad un fornitore esterno, divenuto quindi responsabile del trattamento ex art. 28 non adeguatamente verificato o controllato (o che ha mentito in merito alle misure di protezione che avrebbe dovuto adottare e che non ha, nella realtà, messo in atto): il fatto che l'evento lesivo sia da attribuirsi alla responsabilità di un soggetto terzo rispetto al brand non è sufficiente ad impedire il formarsi di un'opinione negativa circa l'inaffidabilità del brand stesso a tutelare i propri clienti. La quantificazione economica di questo danno dovrà necessariamente essere calcolata su base probabilistica, ma si possono, comunque, utilizzare dati certi ed oggettivi, quali quelli statistici– per esempio, le attese di vendite di un certo periodo secondo il loro andamento storico – confrontati con il fatturato (minore) realizzato effettivamente dopo l'evento lesivo.

Monitoraggio e difesa della reputazione sono prioritari per gestire la competitività sul mercato: un'adeguata protezione dei dati in accordo col GDPR può scongiurare "incidenti" in grado di provocare ingenti perdite economiche. Il danno reputazionale, nella sua componente on-line, può essere verificato anche tramite un'indagine affidata ad una società specializzata nella valutazione della web reputation.

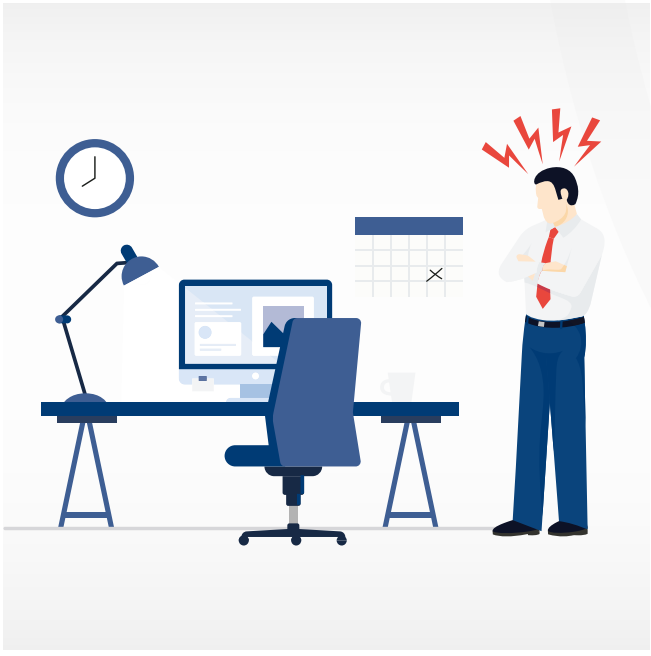
Assenteismo

La buona fede non è ragione di revoca dei licenziamenti intimati ai “furbetti del cartellino”

Furbetti del Cartellino, comune di Sanremo: la corte di Appello conferma il licenziamento.

Corte d’Appello Genova, sez. Lavoro, sent. 20 maggio 2019, n. 250

La Corte d’appello di Genova, con la sentenza in commento, ha respinto il ricorso presentato da un dipendente che aveva chiesto la revisione della sentenza di primo grado con la quale era già stata respinta la domanda di annullamento del licenziamento intimatogli per via delle oltre 50 assenze. Il dipendente del comune approfittava della propria posizione per assentarsi, naturalmente senza timbrare l’uscita, ma lamentava l’illegittimità del licenziamento poiché non era stato tenuto conto della sua convinzione che il consenso verbale del proprio responsabile all’allontanamento dall’ufficio fosse sufficiente.
La sentenza di merito ha precisato che la presunta buona fede del c.d. “furbetto del cartellino” non può portare all’annullamento del licenziamento per giusta causa.



Il lavoratore era alle dipendenze del comune da molti anni e non poteva non essere a conoscenza dell’obbligo, imposto da sempre da leggi e contratti collettivi, di timbrare il cartellino presenze sia in entrata che in uscita.

La sentenza conferma la legittimità dei licenziamenti in caso di assenteismo. Ricordiamo che ai dipendenti pubblici che sono “pescati” nell’alterare i sistemi di controllo delle presenze viene irrogata da subito la sanzione della sospensione del 50% del trattamento economico. Nei loro confronti matura anche responsabilità amministrativa per danno alla immagine dell’ente.