I CONTROLLI DATORIALI E LE ATTIVITÀ DI CONSULENZA TECNICA SUGLI STRUMENTI INFORMATICI AZIENDALI IN USO AL DIPENDENTE "INFEDELE"

Paolo Dal Checco,
Consulente
Informatico Forense

Jacopo Giunta

Francesco Meloni

INTRODUZIONE

Una delle domande ricorrenti che vengono poste a Consulenti Tecnici e Giuristi riguarda il comportamento da tenere nei confronti del "dipendente infedele", cioè nella situazione in cui l'azienda venga a scoprire o tema che uno dei propri dipendenti stia portando avanti attività di concorrenza sleale o comunque stia causando danni all'azienda. La domanda, tipicamente, verte sulle modalità con le quali i titolari possono commissionare un'analisi del PC e degli altri strumenti informatici in uso al dipendente sui quali, si presume, siano presenti le prove dell'infedeltà o della condotta lesiva. Gli autori dell'articolo, ricoprendo appunto i ruoli di Consulenti Tecnici e Giuristi, risponderanno al quesito esaminando aspetti, modalità tecniche di acquisizione dei dati e limiti dei cosiddetti "controlli datoriali" sugli strumenti informatici aziendali, tentando di districare la matassa e ragionando in termini di tutela del patrimonio aziendale, di difesa dei propri diritti, senza trascurare l'importanza delle policies nello svolgimento delle attività di controllo da remoto in tempo reale o in differita, del rispetto della Privacy e delle modalità tecniche di acquisizione e di conservazione delle evidenze probatorie.

CONTROLLI DATORIALI SUGLI STRUMENTI INFORMATICI AZIENDALI IN USO AI DIPENDENTI

I controlli datoriali sugli strumenti informatici aziendali in uso ai dipendenti (acquisizione e analisi di archivi mail, analisi di account Skype o di messaggistica istantanea, acquisizione e analisi di cellulari, pc e tablet aziendali) nonché le modalità e gli strumenti con cui i medesimi vengono effettuati, costituiscono uno dei temi maggiormente delicati nello scenario dell'organizzazione aziendale, in quanto costituiscono il risultato di un'equazione le cui contrapposte espressioni devono necessariamente trovare un punto d'incontro; da una parte l'imprescindibile esigenza di tutela del patrimonio aziendale e l'interesse del datore di lavoro – che può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempi-

> I CONTROLLI DATORIALI SUGLI STRUMENTI INFORMATICI AZIENDALI IN USO AI DIPENDENTI COSTITUISCONO UNO DEI TEMI MAGGIORMENTE DELICATI NELLO SCENARIO DELL'ORGANIZZAZIONE AZIENDALE

Paolo Dal Checco svolge attività di Consulenza Tecnica in ambito forense collaborando con Procure, Tribunali e Forze dell'Ordine oltre che con aziende, privati e Avvocati. Insieme al socio Giuseppe Dezzani è socio fondatore dello studio di consulenza informatica forense "Digital Forensics Bureau" di Torino. Professore a Contratto del corso di Sicurezza Informatica per l'Università degli Studi di Torino, nel C.d.L. in Scienze Strategiche, socio IISFA, CLUSIT, AIP e Tech & Law è tra i fondatori dell'Osservatori Nazionale per l'Informatica Forense, dell'Associazione DEFT che sviluppa la piattaforma DEFT Linux per acquisizioni e analisi forensi.
Jacopo Giunta, Legal & IT Counsultant @ Studio Legale Associato Ambrosio & Commodo. Si occupa di responsabilità civile, privacy e data protection. Consulente informatico forense, certificato CIFI, socio CLUSIT, IISFA e DFA, nella sua attività ha maturato specifiche competenze in materia di, infortunistica stradale, responsabilità medica, disastri aerei e marittimi, danni da contagio, danni da farmaci, danni ambientali, privacy & data retention.
Francesco Meloni, Avvocato penalista del Foro di Torino, Studio Legale Associato Ambrosio & Commodo. Si occupa di diritto penale societario e di impresa, con particolare riferimento agli ambiti della responsabilità amministrativa degli Enti e delle persone giuridiche ai sensi del D.Lgs. n. 231 del 2001 e della salute e sicurezza sui luoghi di lavoro.

mento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 c.c) e, dall'altro, la tutela dei dati personali dei dipendenti (art. 11 D.Lgs 196/2003).
Se da un lato i controlli datoriali, sia preventivi che successivi, danno la possibilità all'azienda di verificare l'operato dei dipendenti e, in ipotesi di c.d. "infedeltà", di raccogliere riscontri probatori tali da giustificare l'allontanamento del dipendente – e idonei a essere producibili innanzi le competenti autorità giudiziarie - dall'altro gli stessi devono essere adottati e adeguatamente strutturati in una policy interna (di cui gli interessati devono essere compiutamente informati) che ne definisce le modalità ed i limiti nei minimi termini, nel rispetto dei generali principi di necessità, finalità, legittimità, correttezza, proporzionalità e non eccedenza.
Tali controlli, comportando anche deroghe a diritti e a garanzie di rango costituzionale poste a tutela dei lavoratori (in particolar modo ogni qualvolta i controlli coinvolgano la corrispondenza elettronica), indipendentemente dalla fondata sussistenza di profili di "infedeltà", devono essere limitati nel tempo e nell'oggetto, mirati e fondati su presupposti tali da legittimarne l'esecuzione, pena l'inutilizzabilità dei risultati, l'esposizione a pesanti sanzioni pecuniarie per violazione del trattamento dei dati nonché a eventuali conseguenze di natura penale.

I CONTROLLI DEVONO ESSERE LIMITATI NEL TEMPO E NELL'OGGETTO, MIRATI E FONDATI SU PRESUPPOSTI TALI DA LEGITTIMARNE L'ESECUZIONE, PENA L'INUTILIZZABILITÀ DEI RISULTATI, L'ESPOSIZIONE A SANZIONI PECUNIARIE NONCHÉ A EVENTUALI CONSEGUENZE PENALI

I controlli devono essere limitati nel tempo e nell'oggetto, mirati e fondati su presupposti tali da legittimarne l'esecuzione, pena l'inutilizzabilità dei risultati, l'esposizione a sanzioni pecuniarie nonché a eventuali conseguenze penali.

La costante casistica desumibile dai provvedimenti del Garante Privacy, relativa alle procedure di controllo sull'ope-

LE RISULTANZE DEGLI ACCERTAMENTI E DELLE ATTIVITÀ DI SORVEGLIANZA SONO UTILIZZABILI SIA IN SEDE DISCIPLINARE, SIA NELL'AMBITO DEL PROCEDIMENTO PENALE QUALE PROVA DOCUMENTALE

rato dei dipendenti, è conforme nell'accordare all'azienda ampi spazi di movimento, sia nelle procedure ordinarie che in quelle mirate a individuare comportamenti illeciti, purché:

- le procedure di controllo vengano cristallizzate in una policy aziendale (formata secondo le linee guida per la protezione dei dati personali n. 13 dell'1 marzo 2007 secondo cui, giova ribadirlo, "*i dirigenti dell'azienda accedono legittimamente ai computer – ed agli altri dispositivi - in dotazione ai propri dipendenti, quando delle condizioni di tale accesso sia stata loro data piena informazione*"), il cui ruolo rimane centrale per disciplinare in modo puntuale l'utilizzo degli strumenti elettronici affidati in dotazione ai lavoratori.
- che vengano rispettati i principi generali in materia di trattamento dei dati sopra enucleati, la cui importanza intrinseca è stata peraltro recentemente ribadita anche dopo la riforma dei controlli datoriali operata dal Jobs Act (e anche rispetto agli strumenti di lavoro che, pur sottratti alla procedura concertativa, restano comunque soggetti alla disciplina del Codice Privacy).
- che le risultanze investigative o di controllo vengano acquisite secondo le best practices della Digital Forensics – di cui si parlerà infra – in quanto le sole a garantire l'immodificabilità del dato originale e quindi la piena valenza probatoria. Tale aspetto assume rilevanza estrema, in particolare nel caso in cui la raccolta dei dati sia prodromica a un'azione giudiziale, sia civile che penale.

IL D.LGS N. 151/2015, LO STATUTO DEI LAVORATORI E L'UTILIZZABILITÀ DEI DATI RACCOLTI

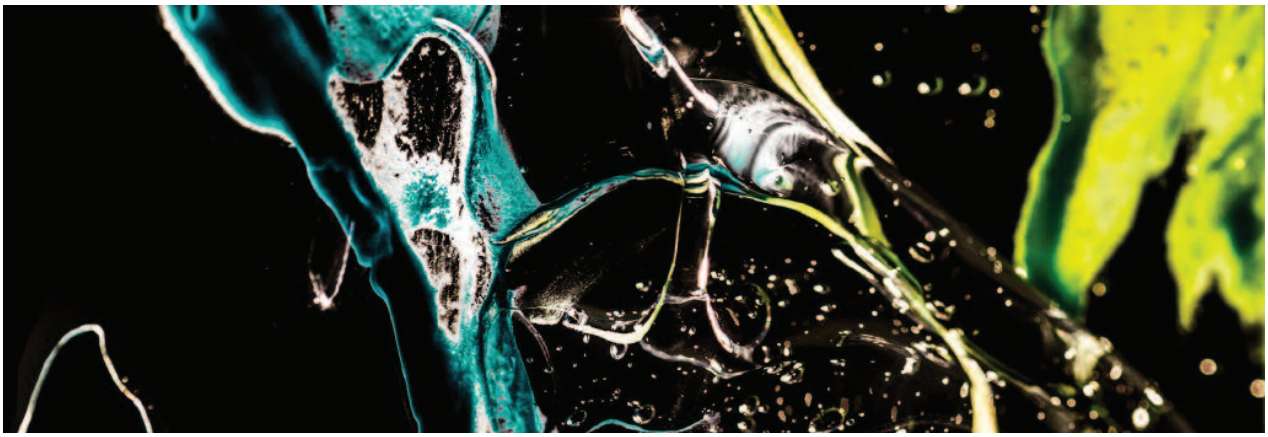
La recente entrata in vigore del D.Lgs. n. 151/2015, emanato in attuazione della delega contenuta nel Jobs Act, ha sensibilmente innovato l'originaria cornice normativa dei controlli datoriali a distanza sul luogo di lavoro.

Secondo la precedente formulazione dell'art. 4, Statuto dei lavoratori, gli impianti di controllo potevano essere installati dal datore di lavoro esclusivamente in presenza di specifiche esigenze organizzative, produttive o di prevenzione di infortuni sul luogo di lavoro.

Traducendo in dato normativo un orientamento ermeneutico recentemente ribadito dalla giurisprudenza della Corte di Cassazione (si veda, da ultimo, Cass., Sez. Lav., 17 febbraio 2015, n. 3122), la riforma del 2015 ha ampliato il novero dei requisiti oggettivi sottesi all'installazione di impianti audiovisivi sul luogo di lavoro o di apparecchi di controllo a distanza, includendovi espressamente la finalità di tutela del patrimonio aziendale.

Allo stato attuale, pertanto, hanno trovato pieno ed espresso riconoscimento i controlli di natura difensiva, volti a prevenire e ad accertare l'eventuale realizzazione di attività illecite poste in essere dai propri lavoratori o da soggetti terzi.

Permane, nella vigente formulazione dell'art. 4, Statuto dei lavoratori, l'obbligo di rispettare taluni adempimenti for-



mali, quali il raggiungimento di un accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali o, in alternativa, il conseguimento della prescritta autorizzazione rilasciata dalla competente Direzione territoriale del lavoro.
L'estensione del potere di sorveglianza del datore di lavoro si affianca a un'ulteriore importante novità, prevista dall'ultimo comma dell'art. 4, Statuto dei lavoratori.
Quest'ultima disposizione, facendo seguito a un costante orientamento interpretativo elaborato dalla Corte di Cassazione, ha espressamente sancito l'utilizzabilità delle informazioni e dei dati acquisiti mediante le attività di controllo a distanza a qualsiasi fine connesso al rapporto di lavoro.
A tal fine, è in ogni caso imprescindibile il rispetto degli adempimenti imposti dal Codice della Privacy e delle raccomandazioni impartite dall'Autorità Garante per la protezione dei dati personali. Primi fra tutti, l'adozione e l'attuazione di idonee policies aziendali e l'adeguata informazione ai lavoratori in merito alle modalità di esecuzione dei controlli.
Le risultanze degli accertamenti e delle attività di sorveglianza, dunque, sono pacificamente utilizzabili sia in sede disciplinare, sia nell'ambito del procedimento penale, quale prova documentale di eventuali condotte penalmente rilevanti.

Le risultanze degli accertamenti e delle attività di sorveglianza sono utilizzabili sia in sede disciplinare, sia nell'ambito del procedimento penale quale prova documentale.

Per contro, i requisiti oggettivi e gli adempimenti formali prescritti dall'art. 4 dello Statuto dei lavoratori non si applicano in relazione ai controlli datoriali esercitati sugli strumenti di lavoro in uso ai dipendenti per lo svolgimento della prestazione lavorativa.
Trattasi di una novità di grande rilievo, introdotta dallo stesso D.Lgs. n. 151/2015: in tali casi l'installazione è libera, fermo restando, naturalmente, l'obbligo di rispettare gli adempimenti imposti dalla normativa sulla Privacy.
Sul piano dell'utilizzabilità, nell'ambito del processo penale, dei dati e delle informazioni acquisite tramite l'espletamento di controlli datoriali a distanza, occorre richiamare i seguenti principi, da ultimo confermati all'interno di una recentissima pronuncia della Corte di Cassazione (Cass. Pen., Sez. II, 16 giugno 2015, n. 24998):

- sul piano normativo, non esiste ad oggi uno standard prestabilito per la metodologia di trattamento e di analisi delle prove informatiche;
- l'estrazione dei dati informatici archiviati su un computer o su altri dispositivi informatici non costituisce accertamento tecnico irripetibile ai sensi dell'art. 360 c.p.p., trattandosi di operazione meramente meccanica, riproducibile per un numero di volte indefinito;
- nell'effettuare le operazioni di estrazione dei dati, è necessario adottare mi-

sure tecniche idonee ad assicurare la conservazione dei dati originali e a impedirne l'alterazione;
- ove possibile, è opportuno procedere alla duplicazione dei dati su adeguati supporti informatici, mediante procedure idonee ad assicurarne la conformità della copia all'originale e la sua immodificabilità.

MODALITÀ TECNICHE DI ACQUISIZIONE DEL DATO INFORMATICO

Dal punto di vista tecnico, per l'acquisizione del dato informatico valgono le *best practices* della *digital forensics*, il ramo della scienza forense che studia le fasi d'identificazione, acquisizione, conservazione, analisi e reportistica nell'ambito dei dispositivi digitali. E' importante, quando possibile, per il Consulente Tecnico muoversi in accordo con un eventuale Studio Legale che assista l'Azienda, a seguito di nomina ad esempio per l'espletamento di indagini difensive. In genere la nomina può essere motivata dall'esigenza di proteggere asset/informazioni aziendali, eventualmente rafforzata da elementi che diano adito a credere che sia in corso una *data exfiltration* o comunque un comportamento scorretto da parte di un dipendente. Si raccomanda anche il rilascio, da parte dell'Azienda, di una lettera d'incarico che specifichi l'ambito dell'attività, obblighi del cliente e del fornitore, autorizzazioni, condizioni e termini del trattamento dei dati personali, oltre alle opportune considerazioni in merito all'impianto recato dal Modello Organizzativo 231, ove presente, con riferimento alle disposizioni di parte generale e di parte speciale.
Una volta chiariti gli aspetti formali, l'attività di acquisizione segue l'iter standard che prevede innanzitutto l'identificazione del dispositivo di cui deve essere eseguita copia forense, con verbalizzazione e possibilmente documentazione fotografica della postazione di lavoro, del computer e del disco o dei dischi in esso contenuti. La copia forense – ricordiamo – consiste nella duplicazione integrale di tutto il contenuto del dispositivo, a livello di *bit* e non di file, partendo dal primo settore del disco fino all'ultimo, coinvolgendo quindi aree contenenti file ancora presenti sul sistema e aree dove invece ci sono informazioni rimaste intatte di file ormai cancellati.
Se il Consulente possiede un *write blocker* (strumento che permette il collegamento di un hard disk a un computer in modo "sicuro" senza rischi di scritture accidentali) può aprire il *case* del PC, estrarre il disco e collegarlo al suo computer per avviare la fase di copia. Spesso al posto dei *write blocker* si utilizzano *copiatori forensi*, strumenti più evoluti che permettono la copia ad alta velocità di un disco sorgente su di uno di destinazione, senza bisogno di un computer che si ponga da interfaccia.
Nel caso in cui tali strumenti non siano disponibili, oppure sia difficile estrarre fisicamente l'hard disk dal PC, ci si può avvalere di sistemi software per avviare il computer del dipendente mediante un Sistema Operativo esterno che permetta l'accesso e la copia del disco interno senza comprometterne l'integrità. Il sistema infatti funge da *write blocker* e *copiatore forense* software, con la differenza che non si sta utilizzando uno strumento esterno ma è lo stesso PC contenente il disco che provvede ad accederne al contenuto in maniera sicura. Esistono al mondo diversi sistemi di questo genere, definiti per tradizione "Live CD" ma che ora possono essere utilizzati anche sotto forma di pendrive USB: in Italia abbiamo DEFT o CAINE e all'estero PALADIN o RAPTOR, basate su sistema Linux, ma esistono altre varianti come WinFE basate su OS Windows o persino vecchie versioni di RAPTOR.
Il risultato della copia sarà un file, grande quanto il disco acquisito, che contiene ciò che viene comunemente definito "immagine forense", poiché contiene una copia speculare detta "immagine" creata a fini "forensi", cioè per diventare una potenziale "prova" in ambito giudiziario penale o civile.
Sulla copia dovranno essere calcolati almeno due codici, chiamati "valori hash", che costituiscono una sorta di firma univoca o meglio d'impronta digitale del di-

IL TEMPO È UN ELEMENTO CHE VA "CONGELATO" TRAMITE SERVIZI DI APPOSIZIONE DATA CERTA, ATTI AD ATTESTARE L'ESISTENZA E L'INTEGRITÀ DELLE EVIDENZE ACQUISITE IN UN CERTO PERIODO

sco così come è stato acquisito, finalizzata ad attestarne l'integrità nel tempo. Il tempo è proprio un elemento che va "congelato", apponendo a questi due valori una data certa, o *timestamp* digitale, impresso ad esempio tramite il servizio offerto da operatori come Infocert, Aruba, etc... che può essere arricchito da eventuale firma digitale di chi ha eseguito l'operazione di copia.

Il tempo è un elemento che va "congelato" tramite servizi di apposizione data certa, atti ad attestare l'esistenza e l'integrità delle evidenze acquisite in un certo periodo.

Il *timestamp* serve per poter attestare in maniera incontrovertibile che il disco è stato acquisito in una tale data, con i contenuti anch'essi certificati a catena e che quindi a tale data esistevano. In passato si usava stampare i valori hash su carta e fare apporre data certa presso il Servizio Postale, così come si usava procedere per certificare i DPS: fortunatamente l'evoluzione digitale permette ora di eseguire la procedura dal proprio PC, opportunamente connesso alla rete e a un servizio di marca temporale.
Chi non possiede un servizio di *timestamping* può utilizzare, più semplicemente, la PEC, inviando al proprio indirizzo una messaggio di posta elettronica certificata contenente i valori hash calcolati sull'immagine forense acquisita.
Una volta duplicato il contenuto del disco, è consigliabile conservare comunque quello originale e, nel caso in cui non fosse possibile interromperne l'utilizzo, eseguirne un'immagine su un nuovo disco e inserire quest'ultimo nel computer. Questa precauzione talvolta può sembrare eccessiva, ma in caso di contenzioso poter disporre anche del supporto originale può essere un punto a favore dell'Azienda.

CONCLUSIONI

Come da premessa, la tematica dei controlli datoriali è stata trattata in modo da offrire una panoramica delle possibilità, dei limiti e dei campi d'azione tecnici e giuridici, con l'obiettivo di guidare le aziende e i datori di lavoro nella scelta della migliore strategia difensiva funzionale alla tutela del patrimonio e dell'organizzazione aziendale.
Ovviamente, tali valutazioni non possono in alcun modo prescindere da un'analisi attenta e accurata, che tenga conto delle peculiarità e delle caratteristiche del singolo caso concreto, specialmente per ciò che attiene agli aspetti prettamente giuridici della liceità e dell'utilizzabilità dei controlli e delle risultanze acquisite.
Sotto il profilo più propriamente tecnico, infatti, occorre dare atto che le procedure sono ormai piuttosto consolidate e condivise nella comunità scientifica.
Raccomandiamo quindi, a chi dovesse trovarsi nell'esigenza di eseguire controlli datoriali finalizzati a rilevare eventuali comportamenti scorretti o illeciti di un proprio dipendente, di rivolgersi al proprio Studio Legale di fiducia per condividere una linea di condotta che consenta di non incorrere in eventuali sanzioni penali o amministrative, nonché, ultimo aspetto ma non meno importante, di acquisire dati ed elementi probatori pienamente utilizzabili nell'ambito di procedimenti disciplinari, civili e penali. ■