prorevi auditing S.r.l.

NOTA INFORMATIVA N. 17/2021

PROTEZIONE DEL PATRIMONIO INFORMATIVO AZIENDALE E LAVORO AGILE

1. Il lavoro agile emergenziale

Tra gli aspetti ai quali la normativa emergenziale dedica particolare attenzione vi è, senza dubbio, il tema del lavoro agile. Invero, si registra l'aumento esponenziale del numero di lavoratori che hanno iniziato a svolgere la propria prestazione professionale da remoto.
Se il fenomeno di dematerializzazione del lavoro non è venuto a esistenza con il COVID-19, la nuova normalità con la quale siamo costretti a convivere ha sostanzialmente eroso ogni differenza tra lavoro dentro e fuori dall'ufficio, per lo meno con riguardo a quelle professioni che già in passato venivano svolte tramite strumenti informatici. Tale rivoluzione culturale impone di interrogarsi in merito a nuove situazioni di pericolo, per lavoratori e imprese, sorte in ragione del mutato contesto sociale, prima ancora che lavorativo. Tra le più note, possiamo ricordare:

- **i.** la diminuzione delle interazioni fisiche – sia esterne alle singole aziende sia all'interno della stessa azienda – con spostamento di numerose operazioni, anche di natura finanziaria, in un ambiente esclusivamente digitale;
- **ii.** la maggiore trasmissione di dati e informazioni nell'etere: se una riunione interna di gruppi di lavoro poteva essere svolta in una stanza chiusa, ora le interazioni tra membri dello stesso gruppo di lavoro impongono, spesso, una fuoriuscita di dati dal perimetro aziendale;
- **iii.** la maggiore difficoltà a trasmettere informazioni e valori aziendali a dipendenti che operano da remoto, soprattutto ai dipendenti più giovani, o a coloro i quali hanno avviato una nuova esperienza lavorativa interamente da remoto;
- **iv.** l'aumento di rischi che provengono dall'interno dell'impresa stessa: casi nei quali lo stesso dipendente, in violazione degli obblighi di diligenza e di fedeltà, realizza condotte illecite nei confronti del proprio datore di lavoro;
- **v.** l'incremento di minacce che provengono dall'esterno: l'accesso a dati o informazioni aziendali da parte di soggetti terzi che sfruttano i dipendenti dell'impresa come *ponte* (i c.d. *cyber attack*) ecc. ecc.

2. La fedeltà del dipendente e i rischi di furto di dati e appropriazione indebita

La nuova modalità di fruizione del lavoro agile comporta un duraturo distacco fisico tra lavoratore e datore di lavoro, poiché il lavoro agile comporta lo svolgimento dell'attività:

- **i.** in parte nei locali aziendali e in parte al di fuori di essi;
- **ii.** senza una postazione fissa;
- **iii.** senza vincoli di orario e di luogo di lavoro;
- **iv.** con il necessario utilizzo di strumenti tecnologici.

In questo contesto, il lavoratore agile può effettuare telefonate, inviare *e-mail* o organizzare incontri (in presenza o virtuali) per finalità diverse da quelle dell'impresa per la quale opera, così violando il proprio dovere di fedeltà. Il distanziamento fisico tra datore di lavoro e lavoratore incentiva tali comportamenti opportunistici, atteso che gli stessi possono essere svolti dal lavoratore:

prorevi auditing s.r.l.

- più facilmente, perché non vincolato dalla presenza presso la sede aziendale o perché favorito da un orario di lavoro flessibile;
- senza essere sottoposto a controlli diretti o indiretti (da parte di colleghi), che nella prassi renderebbero difficile svolgere attività infedeli durante un rapporto di lavoro.

Ciò premesso, uno dei beni che, con lo sviluppo di diverse modalità di esecuzione della prestazione lavorativa rischia di essere maggiormente esposto a fenomeni di appropriazione è il patrimonio informativo aziendale.

Nonostante l'imprescindibile ruolo dell'informazione nella dinamica aziendale, sul versante penalistico la tutela del patrimonio informativo dell'impresa non ha ancora trovato una disciplina unitaria, e sconta un deficit tecnologico molto elevato. A tale proposito, si ricorda la recente sentenza della Suprema Corte secondo cui «*i dati informatici (files) sono qualificabili cose mobili ai sensi della legge penale e, pertanto, costituisce condotta di appropriazione indebita la sottrazione da un personal computer aziendale, affidato per motivi di lavoro, dei dati informatici ivi collocati, provvedendo successivamente alla cancellazione dei medesimi dati e alla restituzione del computer "formattato"*» (Cass. Pen., 10 aprile 2020, n. 11959). Tale sentenza porta alla luce tutte le difficoltà di adattamento delle tradizionali fattispecie delittuose rispetto al passaggio dalla società industriale alla società dell'informazione. Del resto, l'informazione continua a non esser vista come valore in sé da tutelare, ma solo in quanto incorporata in una cosa mobile.

Predetta necessaria fisicità dell'informazione, per essere potenziale oggetto di furto e appropriazione, permette di comprendere, sotto il profilo tecnico, l'inadeguatezza di tali figure delittuose a intervenire nelle situazioni più comuni nella pratica: si pensi a tutti quei casi in cui l'autore della condotta si limiti a creare una copia di un documento informatico senza l'autorizzazione del legittimo titolare, che quindi non perde la disponibilità del file illegittimamente copiato, o, casi nei quali ci si appropri del contenuto del documento (per esempio copiandolo e incollandolo su un nuovo *file*) senza neppure creare una copia del medesimo. In tutte queste ipotesi, si rientra in quella che la Suprema Corte etichetta come mera presa di conoscenza non sanzionabile ai sensi degli articoli 624 e 646 c.p.

3. La rivelazione di segreti scientifici o commerciali

Nondimeno, le già menzionate situazioni non appaiono oggi completamente sprovviste di tutela penale, anche se disorganica. Nell'attuale panorama, la disposizione che più di altre tutela l'informazione aziendale è la nuova formulazione di cui all'art. 623 c.p., in tema di rivelazione di segreti scientifici o commerciali, così come ridisegnato dal d. lgs. 11 maggio 2018 n. 63.
La principale novità del nuovo art. 623 c.p. consiste proprio nella estensione della tutela del patrimonio immateriale dell'azienda, affiancando alla tutela delle notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche anche quella dei segreti commerciali; il bene giuridico tutelato dalla nuova formulazione normativa è da individuarsi, pertanto, nel c.d. segreto scientifico-commerciale che, simmetricamente a quello disciplinato in ambito civilistico, rappresenta una speciale figura del segreto professionale, costituita da tre elementi:

I. la segretezza;
II. il valore economico;
III. la protezione.

L'ultima novità è da individuarsi nel nuovo terzo comma, che interviene quando il fatto è commesso tramite qualsiasi strumento informatico*:* tale ampia formulazione porta a suppore una sua applicazione generalizzata, perché, attualmente, appare difficile ipotizzare una condotta di

prorevi auditing s.r.l.

acquisizione, divulgazione e uso di segreti commerciali commessa interamente senza l'uso di alcun strumento informatico.
Da un confronto tra l'art. 646 c.p., così come interpretato dalla Suprema Corte nella sentenza precedentemente menzionata, e l'art. 623 c.p., le due norme, pur presentando una parziale sovrapponibilità, mantengono zone di intervento distinte. Le differenze sono da ricondurre:

- all'oggetto materiale del reato (cosa mobile dotata di una fisicità vs segreto scientifico o commerciale);
- alla condotta (appropriazione vs divulgazione o utilizzo).

Le due fattispecie, peraltro, potrebbero concorrere: si pensi, per esempio, se, in un caso come quello analizzato nella sentenza, i *files* illecitamente appresi dall'ex dipendente contengano segreti scientifici o commerciali e gli stessi siano successivamente rivelati o utilizzati nell'ambito della nuova società presso la quale il medesimo viene assunto, al fine di conseguire un profitto (per il dipendente e/o per il nuovo datore di lavoro).

4. La responsabilità dell'impresa

Nel sistema di tutele così delineato vi è un grande assente. Né il reato di appropriazione indebita né il reato di rivelazione di segreti scientifici o commerciali sono inclusi nel catalogo dei reati presupposto di cui al d. lgs. 231/2001. Una assenza, soprattutto quella dell'art. 623 c.p., che suscita profonde critiche se si consideri che, nell'attuale contesto economico, non è certamente situazione residuale che un furto di informazioni aziendali (*rectius* di segreti scientifici o commerciali) sia commesso nell'interesse o a vantaggio di una impresa, la quale potrà beneficiarne, in termini di sviluppo di nuovi prodotti, di identificazione di nuovi potenziali clienti, ecc. ecc.
Nondimeno, tale vuoto normativo può essere parzialmente compensato dalla possibilità di ricondurre condotte di appropriazione di informazioni (anche riguardanti segreti) a talune fattispecie rilevanti per la responsabilità delle imprese, quali la corruzione tra privati o l'accesso abusivo a sistemi informatici (presenti nel decalogo dei reati presupposto 231). Per quanto concerne l'accesso abusivo a un sistema informatico o telematico, questo può essere considerato un reato che fornisce una tutela anticipata rispetto a condotte infedeli quali il furto di dati o la rivelazione di segreti: tale reato, infatti, punisce il semplice accesso abusivo a un sistema informatico altrui protetto da misure di sicurezza – quale, per esempio, un *server* condiviso aziendale – indipendentemente da qualsiasi atto concreto lesivo del patrimonio informativo aziendale.

Di particolare interesse appaiono le definizioni di sistema informatico e di abusività dell'accesso.
Le Sezioni Unite, dirimendo un contrasto giurisprudenziale circa il *locus commissi delicti* in casi di accessi abusivi effettuati da postazioni remote, nel concludere che «*il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615 ter c.p., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente*», hanno fornito indicazioni sulla nozione di sistema informatico. Nello specifico, la Corte osserva come «*un dispositivo elettronico assurge al rango di sistema informatico o telematico se si caratterizza per l'installazione di un software che ne sovrintende il funzionamento, per la capacità di utilizzare periferiche o dispositivi esterni, per l'interconnessione con altri apparecchi e per la molteplicità dei dati oggetto di trattamento*», facendo rientrare nell'ambito della protezione di cui all'art. 615 *ter* c.p., «*anche i sistemi di trattamento delle informazioni che sfruttano l'architettura di rete denominata Client-Server, nella quale un computer o terminale (il client) si connette tramite rete ad un elaboratore centrale (il server) per la condivisione di risorse o di informazioni, che possono essere rese disponibili a distanza anche ad altri utenti*» (Cass. Pen., 26 marzo 2015, n. 17325).

prorevi auditing s.r.l.

Nel ricondurre i sistemi di tipo *Client-Server* alla nozione di sistema informatico rilevante, la Corte mostra esplicitamente di riconoscere lo sviluppo di una nuova dimensione aterritoriale, incrementata dalla diffusione di dispositivi mobili e dalla tecnologia del *cloud computing*, che permettono di memorizzare, elaborare e condividere informazioni su piattaforme delocalizzate alle quali è possibile accedere da qualunque parte del globo. Di conseguenza, in presenza di una banca dati ubiquitaria, circolare o diffusa sul territorio, o contestualmente compresente e consultabile in condizioni di parità presso tutte le postazioni remote autorizzate all'accesso, la Cassazione ritiene arbitrario scomporre i singoli componenti dell'architettura di rete: *server* e *client* sono parte integrante di un complesso meccanismo strutturato in modo da esaltare la funzione di immissione e di estrazione dei dati da parte del client.
Tale ultima pronuncia ha avallato una concezione di sistema informatico caratterizzato da una dimensione illimitata, e una profondità spaziale che perde ogni connotazione fisica per diventare virtuale rimanendo, però, assolutamente reale, distribuita intorno alla banca dati centrale lungo raggi indefinibili che la rendono sostanzialmente ubiquitaria, circolare, diffusa.
Tale processo di dematerializzazione appare ancora più evidente nella recente giurisprudenza di legittimità che ritiene integrativo del reato di cui all'art. 615-*ter* c.p. l'accesso all'altrui casella di posta elettronica, trattandosi di uno spazio di memoria, protetto da una password personalizzata, di un sistema informatico destinato alla memorizzazione di messaggi, o di informazioni di altra natura, nell'esclusiva disponibilità del suo titolare, identificato da un account registrato presso il provider del servizio, sottolineando come «*l'accesso a questo spazio di memoria concreta un accesso a sistema informatico, giacché la casella è una porzione della complessa apparecchiatura – fisica e astratta – destinata alla memorizzazione delle informazioni, quando questa porzione di memoria sia protetta, in modo tale da rivelare la chiara volontà dell'utente di farne uno spazio a sé riservato, con la conseguenza che ogni accesso abusivo allo stesso concreta l'elemento materiale del fatto*» (Cass. Pen. 2 maggio 2019, n. 18284).

A differenza del reato di appropriazione indebita, il reato di cui all'art. 615-*ter* c.p., prevedendo quale oggetto materiale un sistema informatico, si adatta con maggiore facilità alla nuova realtà dematerializzata: la locuzione sistema informatico si conforma all'attuale contesto tecnologico, non prestando il fianco a sostanziali vuoti di tutela.

5. Le misure preventive per l'impresa

Nonostante i numerosi passi in avanti, sia in ambito legislativo sia giurisprudenziale, si è visto che si è ancora lontani da una disciplina unitaria per la tutela del patrimonio informativo dell'impresa.
In tale ottica, per garantire una effettiva tutela alle informazioni aziendali, occorre agire in via preventiva:

- **I.** adottando modalità di gestione delle informazioni idonee a mantenerne il carattere riservato, o, prevedendo nei contratti, con dipendenti o collaboratori esterni, specifiche clausole di confidenzialità, c.d. *non disclosure agreements;*
- **II.** implementando sistemi di sicurezza informatica che limitino l'accesso ai medesimi solo a un ristretto e determinato numero di soggetti;
- **III.** monitorando ogni accesso, *download*, inoltro o anche stampa di tali documenti informatici, in conformità con le disposizioni *privacy* e del diritto del lavoro.

Questa tematica si interseca con quella del controllo dell'attività dei lavoratori attraverso impianti audiovisivi e altri strumenti di controllo, previsti dall'art. 4, l. 20 maggio 1970, n. 300. In forza di tale norma «*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».
A titolo esemplificativo, ci si chiede: sarebbe possibile analizzare i file di *log* nel caso vi fossero indizi di una possibile infedeltà del dipendente?
La risposta sembra essere positiva: a tacer del fatto che un controllo *ex post* di dati informatici non appare immediatamente sussumibile nella categoria degli strumenti dai quali derivi anche la possibilità di controllo a distanza, una tale attività di controllo potrebbe rientrare nella disciplina dei c.d. controlli difensivi, e quindi inerente alla difesa in giudizio di un proprio diritto, essendo quindi liceizzata dall'art. 51 c.p. In ogni caso, al fine di evitare successive contestazioni in termini di violazione dell'art. 4, si potrebbe procedere a un accordo collettivo con le rappresentanze sindacali.
In tale contesto, appare opportuno prevedere, all'interno dell'accordo, le modalità tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore al di fuori dell'orario lavorativo e un'idonea informativa ai sensi della normativa *privacy*.

Diverso, in termini di invasività, potrebbe essere il caso nel quale il controllo venisse effettuato attraverso veri e propri sistemi di videosorveglianza: si pensi, per esempio, alle telecamere del portatile aziendale accese in maniera ininterrotta, che andassero a riprendere la vita del lavoratore nel proprio contesto domestico.
Una tale ipotesi non solo potrebbe essere sanzionata ai sensi dell'art. 38 dello Statuto dei Lavoratori ma, ma anche configurare una responsabilità per interferenze illecite nella vita privata ai sensi dell'art. 615 *bis* c.p., che punisce «*chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614*».

6. Manovre di infrastrutture informatiche e lavoro da remoto

I rischi legati alla sicurezza cibernetica delle imprese non sono certo sorti in epoca Covid. È sufficiente guardare indietro negli anni per osservare come i rapporti annuali pubblicati da vari enti, pubblici o privati, attivi nel campo della *cybersecurity* registrano ogni anno un incremento notevole di attacchi *hacker* delle più svariate tipologie. Tale *trend* si è andato a consolidare nel 2020. Richiamando il recentissimo rapporto Avira, il medesimo esordisce osservando come nel periodo di riferimento si è assistito al maggior numero di minacce *malware* di sempre, superando il precedente *record* del 2019.

Anche nell'esperienza giudiziaria, un altissimo numero di truffe perpetrate nei confronti di imprese avviene con la formula del *Fake CEO*. Si tratta di una truffa molto semplice: un dipendente di una società riceve una e-mail da parte di un indirizzo di posta elettronica apparentemente riconducibile a quello del proprio responsabile, il quale chiede al dipendente di effettuare un pagamento a un determinato conto correte, necessario per un'operazione urgente.
Una variante di questo meccanismo è la truffa del c.d. *man in the middle*: un soggetto riesce a frapporsi nelle comunicazioni tra cliente e fornitore relative al pagamento di un determinato ordine. Indicando che i riferimenti bancari solitamente utilizzati non possono essere momentaneamente utilizzati in ragione di disfunzioni tecniche del conto, chiede di effettuare il pagamento su un diverso iban.
Tali tipologie di truffe beneficiano evidentemente delle nuove modalità lavorative da remoto: minore confronto tra colleghi, proliferarsi di richieste di trasmissione dati e pagamenti in assenza di interazione fisica.

Con uno sguardo al domani – ipotizzando un sempre maggiore ricorso al lavoro agile e una sempre crescente informatizzazione delle relazioni – queste truffe potrebbero trovare maggiore solidità tecnica attraverso l'utilizzo di tecniche avanzate quali il *deep Fake* (clonazione del viso di un soggetto ai fini anche del furto di identità) e del *voice mimicking* (furto della voce).

prorevi auditing s.r.l.

prorevi auditing s.r.l.

Se alla *e-mail* del finto responsabile segue una *video call* dove il dipendente crede di parlare con il vero responsabile, un fornitore o un cliente, identico al soggetto reale nei lineamenti e nella voce, è evidente che il rischio di essere vittima di frodi non potrà che aumentare.
Con riferimento alla tutela penalistica di tali situazioni, possiamo trovarci davanti a una condotta di sostituzione di persona e a ipotesi di truffa sia canonica, sia, nel caso di intervento sul funzionamento del flusso di comunicazione, di truffa informatica con la nuova aggravante del furto dell'identità digitale. Condotte che, peraltro, sono ulteriormente aggravate dalla c.d. minorata difesa.
La giurisprudenza identifica le condizioni della minorata difesa nella costante distanza tra venditore e acquirente che gestiscono trattative che si svolgono interamente sulle piattaforme web: tale modalità di contrattazione pone l'acquirente in una situazione di debolezza in quanto è costretto ad affidarsi alle immagini che non consentono una verifica della qualità del prodotto.

7. Quali tutele?

Un primo aspetto che deve essere tenuto in debita considerazione è la poca effettività di una tutela successiva, in ragione delle caratteristiche della criminalità informatica e delle difficoltà investigative che caratterizzano questi tipi di reati. Per identificare alcune caratteristiche comuni, si segnala:

a) l'alta possibilità che i proventi del reato siano resi irrintracciabili con numerose operazioni (per esempio con conti esteri);
b) l'attaccante può utilizzare tecnologie tali da camuffare la propria identità digitale (con tecniche – non necessariamente illecite – con le quali è possibile apparire con un indirizzo IP diverso rispetto al proprio: *proxy*, *VPN*, *Tor*);
c) i dati conservati all'estero rende difficile per i pubblici ministeri ricorrere a procedure di cooperazione internazionale o all'ordine di indagine europeo.

Per questi motivi, la modalità più efficace di contenere il rischio di attacchi da parte di terzi appare la prevenzione:

- a livello formativo: istruendo i dipendenti sui pericoli che le diverse minacce informatiche rivestono e su come possono essere individuati, sia attraverso la predisposizione di politiche aziendali finalizzate a un corretto uso degli strumenti informatici, sia attraverso specifici investimenti nella formazione dei dipendenti;
- a livello tecnico: predisponendo protocolli antifrode, con i dipendenti formati su come poter identificare una telefonata o un video truffaldini, e autenticazione multifattore per l'accesso a tutti i sistemi aziendali.

13 aprile 2021

A cura di Avv. Bruna Capparelli