GIURISPRUDENZA PENALE

Lavoro *"dematerializzato"* e tutela penale del patrimonio informativo aziendale.

di ***Andrea Alfonso Stigliano***

Sommario: 1. Premessa. - **2.** Lavoro da remoto e fedeltà del dipendente. - **2.1** Appropriazione indebita e furto di dati. - **2.2** La responsabilità dell'ente: tra accesso abusivo e corruzione tra privati. - **2.3** Prevenire è meglio che curare. - **3.** Lavoro da remoto ed attacchi informatici. - **3.1** Nuove minacce esterne - **3.2** Strumenti di tutela. - **4.** Conclusioni.

1. Premessa.

Quando, il 9 marzo 2020, l'allora Presidente del Consiglio Giuseppe Conte annunciava restrizioni in tutta Italia per fermare l'esplosione di casi dovuti dell'emergenza epidemiologica da Covid-19, contestualmente prendeva avvio ad un processo di profonde mutazioni dello stile di vita della popolazione italiana.

Tra gli aspetti ai quali la normativa emergenziale dedicava particolare attenzione vi erano, senza dubbio, le tematiche del *"lavoro agile"*. Lasciando da parte ogni questione giuridica in merito alle differenze tra lavoro agile o *smart working* e il, più tradizionale, telelavoro, l'effetto pratico delle misure adottate è stato l'aumento esponenziale del numero di lavoratori che hanno iniziato a svolgere la propria prestazione professionale *"da remoto"*.

Se tale fenomeno di *"dematerializzazione"* del lavoro non è venuto ad esistenza con il COVID-19, la nuova normalità con la quale siamo – ancora oggi, ad oltre un anno dall'inizio della pandemia – 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 all'emersione di eventuali nuove situazioni di pericolo, per lavoratori ed imprese, sorte in ragione del mutato contesto sociale, prima ancora che lavorativo.

Cercando di identificare alcune caratteristiche del lavoro in *smart working* o del telelavoro, possiamo elencare: i) 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) maggiore trasmissione di dati ed 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) maggiore difficoltà a trasmettere informazioni e valori aziendali a dipendenti che operano da remoto, soprattutto con riferimento ai dipendenti più giovani ovvero a coloro i quali hanno avviato una nuova esperienza lavorativa interamente da remoto.
Questi elementi, che non sono i soli, ma che forniscono una buona approssimazione dell'attuale contesto socio-lavorativo, possono essere considerati un importante substrato culturale e sociologico dell'incremento, da più parti osservato, di minacce cibernetiche nei confronti sia delle imprese (quali datori di lavoro) sia dei lavoratori.
La presente analisi si concentra su due distinti profili.
Nella prima parte, sarà analizzato l'aumento di minacce che provengono dall'interno dell'impresa stessa: ovverosia casi nei quali lo stesso dipendente, in violazione degli obblighi di diligenza (ma ancor prima) di fedeltà, pone in essere condotte illecite nei confronti del proprio datore di lavoro.
Nella seconda parte, sarà approfondito l'incremento di minacce che provengono dall'esterno, ovverosia dall'accesso a dati o informazioni aziendali da parte di soggetti terzi che sfruttano i dipendenti dell'impresa come *"ponte"* (i *cyber attack* nell'accezione più comune del termine).

2. Lavoro da remoto e fedeltà del dipendente.

2.1 Appropriazione indebita e furto di dati.

La nuova modalità di fruizione del lavoro agile comporta un fisiologico e duraturo distacco fisico tra lavoratore e datore di lavoro.
Il lavoro agile comporta lo svolgimento dell'attività: i) in parte nei locali aziendali ed 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 possibile (*rectius "necessario"*) utilizzo di strumenti tecnologici.
Il dipendente in *"lavoro agile"* può effettuare telefonate, inviare *email* ovvero organizzare veri e propri incontri (di persona come online) per finalità diverse da quelle dell'impresa per la quale opera, così violando il proprio dovere di fedeltà.
Il distacco fisico tra datore di lavoro e lavoratore *"incentiva"* tali comportamenti opportunistici atteso che gli stessi possono essere svolti dal lavoratore: i) molto più agevolmente, perché non vincolato dalla presenza presso la sede aziendale o perché favorito da un orario di lavoro flessibile; ii) senza essere sottoposto ai classici *"controlli"*, diretti come indiretti (da parte di colleghi), che nella prassi renderebbero difficile svolgere attività *"infedeli"* durante un rapporto di lavoro; iii) avendo modo di fornire una falsa rappresentazione della realtà, magari anche utilizzando i device del datore di lavoro.

In tale contesto, uno dei beni che, con l'avvento delle nuove modalità di lavoro rischia di essere maggiormente esposto a fenomeni di *"appropriazione"* è il patrimonio informativo aziendale.
Nonostante tale 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.
È stata di recente accolta con favore una sentenza della Suprema Corte di Cassazione[1] la quale affermava che *"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"*.
Tale sentenza – che ha l'indiscusso merito, per la prima volta, di fornire una interpretazione adeguatrice che permette di sussumere il dato informatico nel concetto di *"cosa"* suscettibile di furto e appropriazione indebita, laddove in passato il *"furto di dati"* era punito esclusivamente quando era realizzato il furto di un supporto contenente i dati (cartaceo o informatico) – porta alla luce tutte le difficoltà di adattamento delle tradizionali fattispecie delittuose rispetto al passaggio dalla società industriale alla società dell'informazione: l'informazione continua a non esser vista come valore in sé da tutelare ma solo in quanto incastonata in una "*cosa mobile*".
Predetta necessaria fisicità dell'informazione, per essere potenziale oggetto di *"furto"* e *"appropriazione"*, permette di comprendere l'inadeguatezza di tali figure delittuose ad intervenire nelle situazioni più comuni, da un punto di vista tecnico, nella pratica: si pensi a tutti quei casi nei quali 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, ovvero, casi nei quali ci si appropri del contenuto del documento (per esempio copiandolo ed 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.[2].

---

[1] Cass. Pen., 10 aprile 2020, n. 11959. Per un commento alla sentenza, CASTAGNO - STIGLIANO, *La tutela penale del patrimonio informativo aziendale tra appropriazione indebita di files e "presa di conoscenza" di informazioni, in Diritto di Internet*, Vol. III, 2020.

[2] Diversamente, sul versante processuale, non sottoposto ai medesimi vincoli interpretativi imposti del principio di stretta legalità in materia penale, la giurisprudenza ha ormai equiparato l'estrazione di una copia di dati informatici, restituendo il sistema informatico al legittimo proprietario, al sequestro dei dati

2.2 Rivelazione di segreti scientifici o commerciali.

Tali situazioni, tuttavia, non appaiono oggi completamente sprovviste di tutela penale, anche se la stessa appare disorganica e riconducibile a diverse figure di reato.

Nell'attuale panorama, la disposizione che, più di tutte, tutela l'*"informazione"* aziendale appare essere la nuova formulazione – in vigore successivamente ai fatti di cui alla sentenza in commento e, pertanto, agli stessi non applicabili – dell'art. 623 c.p. in tema di rivelazione di segreti scientifici o commerciali, così come ridisegnato dal d. lgs. 11 maggio 2018 n. 63, al fine di adeguare la disciplina interna ai contenuti della direttiva UE 2016/943 sulla protezione del *know-how* riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti.

Secondo la originaria previsione normativa la tutela penale del segreto era ancorata ad una dimensione industriale, configurando la fattispecie di cui all'art. 623 c.p. la condotta di *"chiunque, venuto a cognizione per ragione del suo stato o ufficio, o della sua professione o arte, di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche o applicazioni industriali, le rivela o le impiega a proprio o altrui profitto, è punito con la reclusione fino a due anni*.[3] La norma si caratterizzava sia per la ristretta cerchia di soggetti che potevano commettere il reato sia per il forte legame con il contesto economico, prettamente produttivo[4], dovendo il segreto tutelabile, necessariamente, estrinsecarsi in una notizia suscettibile di potenziale applicazione tecnica.

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*"[5]; il bene

---

medesimi. In un primo momento, le corti di merito, in particolare in contesti cautelari, avevano fermamente negato che l'effettuazione di una copia potesse costituire una ablazione di un bene e quindi che si potesse parlare di sequestro anche in assenza di sottrazione dell'involucro contenente i dati informatici. Più di recente, la giurisprudenza di legittimità ha finalmente riconosciuto come la apprensione della stessa copia costituisca una privazione e quindi possa essere oggetto di riesame anche nel caso di intervenuta restituzione (Cass. Pen. 24 febbraio 2015, n. 24617; Cass. Pen. Sez. Un., 20 luglio 2017, n. 40963).

[3] Si vedano sul punto FIANDACA-MUSCO, *Diritto Penale. Parte speciale*, Vol. II, tomo I, Bologna 2006; CIANFARINI, *La responsabilità penale in materia di proprietà industriale*, Bologna, 2007.

[4] Cass. Pen. 18 maggio 2001, n. 25008.

[5] L'ampia formula descrittiva del segreto commerciale prevista dalla norma incriminatrice induce, ora, a ritenere che entrambe le figure distinte del segreto scientifico-industriale (metodi di lavorazione, macchinari utilizzati, prodotti realizzati)

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, e che si compone dei tre elementi costitutivi del requisito della segretezza, del valore economico e della protezione[6].
L'ultima novità consiste nella previsione dell'aggravante, prevista dal nuovo terzo comma, che interviene quando il fatto è *"commesso tramite qualsiasi strumento informatico"*: tale ampia formulazione porta a suppore una sua applicazione generalizzata in quanto, attualmente, appare difficile ipotizzare una condotta di acquisizione, divulgazione ed 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) e alla condotta (appropriazione *vs* divulgazione o utilizzo). Le due fattispecie, peraltro, potrebbero concorrere: si pensi 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 (per esempio) 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).

---

e del segreto scientifico-commerciale (contratti in corsa, organizzazione della produzione, della distribuzione, della pubblicità) siano comprese nell'area di tutela assicurata dalla disposizione.

[6] Per quanto attiene il primo requisito, la segretezza, pur se la sussistenza del medesimo non può essere rimessa alla esclusiva valutazione dell'imprenditore o di altro beneficiario, dovendo pur sempre scaturire da oggettive ragioni giustificatrici del divieto di conoscenza da parte dei terzi, tuttavia, la presenza di procedure di gestione di tali informazioni nonché di specifiche clausole contrattuali di confidenzialità appare un utile strumento al fine di rafforzare tale carattere di segretezza. Il valore economico, in linea con il dettato di cui all'art. 98 c.p.i., non fa riferimento ad una quotazione di mercato quanto, piuttosto, a un oggettivo quanto concreto vantaggio per il suo utilizzatore esclusivo rispetto alla concorrenza, idoneo ad assicurare o addirittura accrescere la posizione di mercato. Per quanto concerne l'elemento costitutivo della protezione, assicurando il precetto la tutela penale soltanto al titolare del diritto al segreto che possa dimostrare di avere positivamente assolto ad un onere di diligenza nella protezione dei dati da altrui intrusioni, è di preminente importanza che tali protezioni siano state correttamente individuate e predisposte correttamente. Cfr. GALLI, *Il Nuovo Diritto del know-how e dei segreti commerciali Prima lettura sistematica delle novità introdotte dal D.Lgs. 11 Maggio 2018*, n. 63 ss.

2.3 La responsabilità dell'ente: tra accesso abusivo e corruzione tra privati.

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 son inclusi nel catalogo dei reati presupposto di cui al d. lgs. 231/2001. Una assenza, soprattutto quella dell'art. 623 c.p., che non può che suscitare 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.)[7].

Tale vuoto normativo può, tuttavia, essere parzialmente compensato dalla possibilità di ricondurre condotte di appropriazione di informazioni (anche riguardanti segreti) a talune fattispecie rilevanti per la responsabilità degli enti, quali la corruzione tra privati o l'accesso abusivo a sistemi informatici (inserite nel decalogo dei reati presupposto 231[8]).

---

[7] Non può peraltro sfuggire che, con le modifiche operate dalla l. n. 179/2017 in tema di *whistleblowing*, è stato necessario un coordinamento tra la tutela dei soggetti segnalanti e le altre disposizioni poste a presidio della non circolazione di informazioni che è interesse delle aziende mantenere riservate, fra le quali figurano i segreti commerciali. Il legislatore ha risolto tale possibile contrasto configurando nelle ipotesi di segnalazione effettuata "*nelle forme e nei limiti previsti nel comma 2-bis*", il riconoscimento del perseguimento dell'interesse all'integrità dell'ente, costituendo la "*giusta causa*" di rivelazione di notizie coperte formalmente dall'obbligo di segreto. In tal modo, le norme che sanzionano la rivelazione dei segreti vedranno un restringimento della loro area di operatività non potendosi incriminare quali *"rivelazioni illecite"* le segnalazioni effettuate per il tramite del canale predisposto dal modello 231. In merito, si è osservato come, in considerazione della operatività limitata della giusta causa, ancorata ai soli casi delle segnalazioni effettuate correttamente ai sensi della normativa 231, occorre domandarsi quali conseguenze discendano qualora le segnalazioni, una volta effettuate, si rivelino *"improprie"*. In tal caso, la segnalazione sarà potenzialmente in grado di arrecare un danno ai beni giuridici tutelati dalle norme di cui agli artt. 622 e 623 c.p. e quindi giustificare l'operatività delle due fattispecie incriminatrici.

[8] Una ulteriore opzione attiene alla possibilità che condotte riconducibili ai reati di appropriazione indebita (di *file*) o di rivelazione o utilizzo di segreti scientifici o commerciali si configurino quali reati fine di una associazione per delinquere. Il discorso appare molto simile a quanto avvenuto nell'ambito dei delitti tributari prima che questi venissero inseriti nei reati presupposto della responsabilità degli enti. Prima del c.d. "*decreto fiscale*" – d.l. 26 ottobre 2019 n. 124 la giurisprudenza di legittimità prevedeva, seppur in via indiretta, la possibilità di confisca di beni della persona giuridica, quale profitto dei reati fiscali (reati fine) compiuti dall'associazione

Per quanto concerne l'accesso abusivo ad 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 ad un sistema informatico altrui protetto da misure di sicurezza – quale, per esempio, un *server* condiviso aziendale – precedentemente (ed 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*", fornivano importanti indicazioni sulla nozione di sistema informatico; si osservava 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 offerta dall'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*"[9].
Nel ricondurre i sistemi di tipo *client - server* alla nozione di sistema informatico rilevante, la Suprema Corte mostrava 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*"[10]. Di conseguenza, in presenza di una banca dati "*ubiquitaria, circolare o diffusa sul territorio, nonché contestualmente compresente e consultabile in condizioni di parità presso tutte le postazioni remote autorizzate all'accesso*", la Suprema Corte riteneva 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*

per delinquere (reato presupposto). Si veda anche sul punto Cass. 14 ottobre 2015, n. 46162.

[9] Cass. Pen. 26 marzo 2015, n. 17325, in *Riv. Pen.*, 2015, 521.

[10] Cass. Pen. 26 marzo 2015, n. 17325, cit.

funzione di immissione e di estrazione dei dati da parte del client"[11]. Si è osservato come tale ultima pronuncia abbia avallato una concezione di sistema informatico caratterizzato da "*una dimensione – o almeno una capacità di 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*"[12].

Tale processo di dematerializzazione appare ancora più evidente nella recente giurisprudenza di legittimità che riteneva 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*"[13].

A differenza del reato di appropriazione indebita – fattispecie delittuosa inserita già nell'originario assetto codicistico ancorata al concetto di *"cosa"* – il reato di cui all'art. 615 *ter* c.p., prevedendo quale oggetto materiale un *"sistema informatico"*, si presta con maggiore facilità ad adattarsi alla nuova realtà dematerializzata: se è vero che i sistemi informatici dell'epoca dell'introduzione del reato (1993) e le relative modalità di utilizzo degli stessi sono incredibilmente mutati nel corso degli ultimi trent'anni, la locuzione *"sistema informatico"* pare potersi quasi integralmente adattare all'attuale contesto tecnologico, non prestando il fianco a sostanziali vuoti di tutela.

Passando al concetto di abusività, anch'esso presenta una accezione piuttosto lata:

un accesso abusivo può ricorrere in caso di originaria mancanza di autorizzazione o di sua successiva revoca[14] ma altresì quando, alla luce dei

[11] Cass. Pen. 26 marzo 2015, n. 17325, cit.. Negli stessi termini anche Cass. 22 luglio 2015 n. 37343; Cass. Pen. 20 gennaio 2016, n. 12951.

[12] SCIUBA, *Osservazioni a Cass. Pen., 26 marzo 2015, sez. UU, n. 17325*, in *Cass. Pen.*, 2015, 3507 s..

[13] Cass. Pen. 2 maggio 2019, n. 18284.

[14] Cass. Pen. 25 ottobre 2018, n. 48895, secondo la quale *"La preposizione ad una branca o un settore autonomo dell'impresa del dipendente con qualifica dirigenziale non implica necessariamente l'accesso indiscriminato a tutte le informazioni in*

principi espressi dalle Sezioni Unite dalle note sentenze *"Casani"*[15] e *"Savarese"* [16], l'agente "*violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema*" ovvero "*ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito*". Con riferimento a tale ultima situazione, la Suprema Corte, con la recente sentenza della Quinta Sezione della Suprema Corte n. 18284 del 2 maggio 2019[17], qualificava come accesso abusivo la condotta di "*accesso, mediante abusivo utilizzo della password*" ad una casella di posta elettronica, della lettura della corrispondenza privata e della modifica apportata alle credenziali d'accesso rendendo, in tal modo, inaccessibile la casella da parte del titolare. In tale arresto, la Suprema Corte estendeva per la prima volta i principi enunciati nella sentenza "*Savarese*" anche al settore privato – "*nella parte in cui vengono in rilievo i doveri di fedeltà e lealtà del dipendente che connotano indubbiamente anche il rapporto di lavoro privatistico*" – qualificando come illecito e abusivo qualsiasi comportamento del dipendente che si ponga in contrasto con i suddetti doveri manifestandosi in tal modo la "*ontologica incompatibilità*" dell'accesso al sistema informatico, connaturata ad un utilizzo dello stesso estraneo alla *ratio* del conferimento del relativo potere.
Nel caso in cui il *"furto"* e la successiva rivelazione dell'informazione/segreto da parte di un esponente aziendale, sia esso apicale o subordinato, si manifestino quale diretta conseguenza di una precedente promessa o

possesso dell'imprenditore preponente, perché una compartimentazione dell'accesso informativo è pienamente compatibile, sul piano logico e giuridico, con il carattere settoriale della preposizione. Ne consegue che risponde di accesso abusivo a sistema informatico il dirigente che non provi di avere accesso illimitato ai dati del datore e superi i limiti della suddetta compartimentazione".

[15] Cass. Pen. Sez. Un., 27 ottobre 2011, n. 4694: "*Integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-ter cod. pen., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema*".

[16] Cass. Pen. Sez. Un., 18 maggio 2017, n. 41210: *"Integra il delitto previsto dall'art. 615-ter comma 2 n. 1 c.p. la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un servizio informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita*".

[17] CASTAGNO - STIGLIANO, *L'accesso abusivo a sistema informatico nell'era delle tecnologie dell'informazione e della comunicazione*, in Diritto di Internet, Vol. IV, 2019.

ricezione di denaro o di altra utilità, tale condotta potrebbe rilevare in termini di violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà di cui alla fattispecie della corruzione tra privati, disciplinata dall'art. 2635 c.c..
In merito, se gli obblighi inerenti all'ufficio disciplinati dall'art. 2635 c.c. sono quelli rilevabili da precetti civilistici che regolano e disciplinano i singoli doveri dei soggetti qualificati, in tale categoria andrebbero inseriti tutti quegli gli obblighi di portata ampia e generica (a patto che trovino concretizzazione in una fonte scritta o in negozi giuridici ed atti formali) assumendo quindi rilevanza le violazioni di qualunque obbligo finalizzato ad assicurare la tutela degli interessi patrimoniali della società[18], inclusi quelli derivanti da beni immateriali quali informazioni rilevanti e/o segrete. Peraltro, a norma del terzo comma, alla responsabilità del dipendente *"infedele"*, si andrebbe ad aggiungere quella del corruttore.
In entrambe le ipotesi sopra descritte, quindi, qualora il reato venisse commesso nell'interesse o a vantaggio di una persona giuridica – il nuovo datore di lavoro per esempio –, quest'ultimo potrebbe essere chiamato a rispondere per gli illeciti di cui agli articoli 24 *bis* comma 1 (reati informatici) e 25 *ter* comma 1 lett. s-*bis*) (reati societari) del d. lgs. 231/2001. A tal fine, sarà sempre necessario che il reato presupposto sia commesso in concorso dal dipendente che si appropri delle informazioni/*file* aziendali (il quale, al momento del fatto, sarà ancora formalmente legato alla società vittima del reato) con un esponente della società beneficiaria, quale istigatore del reato di accesso abusivo ovvero quale corruttore.

2.3 Prevenire è meglio che curare

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 in una duplice direzione.
Da una parte, per garantire una tutela efficace del patrimonio informatico dell'impresa occorre adottare delle modalità di gestione delle informazioni idonee a mantenerne il carattere riservato ovvero prevedere nei contratti, con dipendenti o collaboratori esterni, specifiche clausole di confidenzialità, c.d. *non disclosure agreements*: in tal modo, in primo luogo, viene prevista una obbligazione contrattuale di riservatezza a carico delle persone che sottoscrivono il contratto e, in secondo luogo, si preserva il carattere riservato delle informazioni ai fini della loro protezione in sede civile e penale.
Dall'altra parte, al fine di evitare l'apprensione, finanche massiva, di *files* aziendali, occorre implementare sistemi di sicurezza informatica che limitino

[18] AMATI, *Infedeltà a seguito di dazione o promessa di utilità*, in ROSSI (a cura di), *Reati societari*, Torino, 2005, 441.

l'accesso ai medesimi solo ad un ristretto e ben determinato numero di soggetti, così come monitorare 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 gli Impianti audiovisivi e altri strumenti di controllo, previsti dall'Art. 4, L. 20 maggio 1970, n. 300, in forza del quale "*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*".
Per fare un esempio, sarebbe possibile analizzare i file di *log* nel caso vi fossero indizi di una possibile infedeltà del dipendente? La risposta appare 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 ad 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, ad 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 – che punisce con l'ammenda *"da lire 100.000 a lire un milione"* o con l'arresto da 15 giorni ad un anno la violazione dell'art. 4 dello Statuto dei Lavoratori – ma, inoltre, potrebbe 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, è punito con la reclusione da sei mesi a quattro anni*".

3. Lavoro da remoto ed attacchi informatici.

3.1. Nuove minacce esterne.

I rischi legati alla sicurezza cibernetica delle imprese non sono certo sorti in epoca Covid.

Basta andare a ritroso 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.

Solo per fare un esempio, il rapporto Clusit 2020 (relativo all'anno 2019) evidenziava come *"Nell'anno appena passato si è consolidata una discontinuità, si è oltrepassato un punto di non ritorno, tale per cui ormai ci troviamo a vivere ed operare in una dimensione differente, in una nuova epoca, in un "altro mondo", del quale ancora non conosciamo bene la geografia, gli abitanti, le regole e le minacce"*[19].

Se il 2019, allora, già presentava una rottura con il passato, tale *trend* si è andato a consolidare nel 2020. Richiamando il recentissimo rapporto Avira sul 2020[20], il medesimo esordisce osservando come nel 2020 si è assistito al maggior numero di minacce *malware* di sempre, superando il precedente *record* del 2019.

È, pertanto, evidente che i rischi di sicurezza informatica, già molto accentuati nel periodo precedente alla pandemia, hanno conosciuto una vera e propria impennata causata, soprattutto, dalla nuova normalità lavorativa alla quale abbiamo dovuto abituarci.

Volendo cercare una principale ragione a tale incremento delle minacce, il medesimo non è dipeso, o per lo meno non in maniera rilevante, da un aumento nell'utilizzo di sistemi informatici nell'ambito dell'attività lavorativa ma, in realtà, dalla *"vulnerabilità umana"* connessa all'utilizzo delle medesime.

Questo fenomeno è efficacemente riassunto da una frase e da una statistica. La frase è di un rappresentante di una società di sicurezza che in maniera provocatoria sentenziava che non avrebbe senso per un *hacker* spendere centinaia di migliaia di dollari per creare un proprio *malwere* quando avrebbe potuto, più semplicemente, convincere qualcuno a fare qualcosa di stupido[21].

---

[19] Rapporto Clusit 2020 sulla sicurezza ICT in Italia, https://d110erj175o600.cloudfront.net/wp-content/uploads/2020/03/Rapporto-Clusit-2020.pdf.

[20] Aviva plc - Annual Report and Accounts 2020, https://www.avira.com/en/state-of-cybersecurity-2020.

[21] La frase originale di Adam Meyers, Crowdstrik, recita: *"The whole idea is why invest hundreds of thousands of dollars to build your own malware when you can just convince someone to do something stupid?"*.

La statistica fa riferimento al numero degli attacchi informatici in Inghilterra nel 2018: di questi solo il 12% era un vero attacco informatico realizzato attraverso un programma *malwere*, mentre il restante 88% consisteva in una frode informatica attuata attraverso lo sfruttamento di una vulnerabilità umana[22].

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 *email* da parte di un indirizzo di posta elettronica che appare essere quello del proprio responsabile il quale chiede al dipendente di effettuare un pagamento ad un determinato conto correte necessario al fine di effettuare una 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 o quant'altro, chiede di effettuare il pagamento su un diverso conto.

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, (aggiungerei anche) ansia a volte causata da una percepita pressione dovuta dall'emergenza della situazione.

Con uno sguardo al domani – ipotizzando un sempre maggiore ricorso al lavoro agile ed una sempre crescente informatizzazione delle relazioni – queste truffe *naive* potrebbero trovare maggiore solidità tecnica attraverso l'utilizzo di tecniche avanzate quali il *deepfake* (clonazione del viso di un soggetto ai fini anche del furto di identità) e del *voice mimiking* (furto della voce)[23].

Se alla *mail* del finto responsabile segue una *videocall* dove il dipendente crede di parlare con il vero responsabile, identico in tutto e per tutto al soggetto reale nei lineamenti e nella voce – ma un discorso analogo vale con un fornitore o un cliente – 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 ad ipotesi di truffa sia

[22] L. Ingram, "88% of UK data breaches caused by human error, not cyberattacks", Verdict, 3 September 2018, https://www.verdict.co.uk/uk-data-breaches-human-error/.

[23] Vademecum Garante della Privacy - Deepfake Il falso che ti «ruba» la faccia (e la Privacy), https://www.garanteprivacy.it/documents/10160/0/Deepfake+-+Vademecum.pdf/478612c7-475b-2719-417f-869e5e66604e?version=2.0.

"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, come anche di recente ribadito dalla Suprema Corte di Cassazione in tema di truffe su piattaforme *online*, sono ulteriormente aggravate dalla c.d. *"minorata difesa"*.
Sussiste l'aggravante della minorata difesa, con riferimento alle circostanze di luogo, note all'autore del reato e delle quali egli, ai sensi dell'art. 61, n. 5, cod. pen., abbia approfittato, nell'ipotesi di truffa commessa attraverso la vendita di prodotti online, poiché, in tal caso, la distanza tra il luogo ove si trova la vittima, che di norma paga in anticipo il prezzo del bene venduto, e quello in cui, invece, si trova l'agente, determina una posizione di maggior favore di quest'ultimo, consentendogli di schermare la sua identità, di non sottoporre il prodotto venduto ad alcun efficace controllo preventivo da parte dell'acquirente e di sottrarsi agevolmente alle conseguenze della propria condotta[24].
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; a ciò si aggiunge che la trattativa telematica consente di vendere (ed acquistare) sotto falso nome rendendo difficile anche l'identificazione del contraente e difficile il controllo sulla sua affidabilità.

3.2. Strumenti di tutela.
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 tali tipi di reati.
Per identificare alcune caratteristiche comuni: i) vi è una alta possibilità che i proventi del reato siano resi irrintracciabili attraverso numerose operazioni, anche coinvolgendo conti esteri, con una rapidità tale da rendere inefficaci le successive indagini; ii) l'attaccante può utilizzare tecnologie tali da "camuffare" la propria identità digitale. È a tutti noto il concetto di "indirizzo IP" che può essere paragonato alla "targa" dell'auto con la quale un soggetto si immette nella rete. Esistono numerose tecniche – non necessariamente illecite – attraverso le quali un soggetto può apparire con un indirizzo IP diverso rispetto al proprio: *proxy*, *VPN*, *Tor*, sono tutti strumenti tecnici che possono, almeno in una prima battuta, ingannare l'investigatore; iii) nel caso

[24] *Ex multis*, Cfr. Cass Pen., 22 marzo 2017 n. 17937; Cass. Pen. 29 settembre 2916, n. 43705.

in cui, poi, i dati siano effettivamente conservati all'estero, non può non considerarsi anche la difficoltà data dalla necessità per i pubblici ministeri di adire a procedure di cooperazione internazionale, oggi facilitate dall'ordine di indagine europeo (in attesa di strumenti più efficaci quali l'ordine di produzione europeo).
Per questo motivo, la modalità maggiormente efficace di contenere il rischio di attacchi da parte di terzi appare quella della prevenzione.
Da un punto di vista *"umano"*, i dipendenti delle aziende devono essere istruiti sui pericoli che le diverse minacce informatiche rivestono e su come possono essere individuati, sia attraverso la predisposizione di politiche aziendali finalizzate ad un corretto uso degli strumenti informatici, sia attraverso specifici investimenti nella formazione dei dipendenti. Così l'azienda dovrebbe approntare protocolli anti-frode, con i dipendenti formati su come poter identificare una telefonata o un video truffaldini e che sappiano aderire, senza eccezioni di sorta, a un processo di approvazione in due fasi, per qualsiasi richiesta di trasferimento di denaro
Da un punto di vista tecnico, fondamentale è l'autenticazione multifattore per l'accesso a tutti i sistemi aziendali.
Da ultimo, sotto un profilo economico, le società dovrebbero dotarsi di una c.d *"ciberassicurazione"* che, affiancata ad una solida strategia di sicurezza informatica, potrebbe mitigare, per lo meno economicamente, le conseguenze di un eventuale attacco.

4. Conclusioni

Dall'analisi delle minacce alle imprese in epoca Covid – *id est* minacce che provengono dall'interno dell'impresa stessa ovvero minacce che provengono dall'esterno – emergono due principali riflessioni.
Da una parte, la tutela penale dell'informazione e del dato informatico appare frammentaria e non sempre in grado di cogliere le mutazioni tecnologiche e sociali sottese ai fenomeni criminali. Peraltro, la aterritorialità e la immediatezza delle minacce informatiche appaiono trarre giovamento dalle caratteristiche della repressione giudiziaria di tali fenomeni: una repressione "territoriale", in quanto svolta da autorità nazionali ancorché in "cooperazione" tra di loro, e con delle tempistiche assolutamente inadeguate a fornire una risposta concreta.
Dall'altra parte, proprio tali inadeguatezze impongono una attività di prevenzione che agisca su differenti fattori: predisposizione di strumenti contrattuali o di normativa interna finalizzati alla tutela dell'informazione; investimento sul "fattore umano", inteso come corretta informazione circa possibili condotte illecite (minacce interne) e possibili rischi (minacce esterne) e predisposizione di appositi *training* per testare l'effettiva comprensione; investimento nello sviluppo tecnologico, per essere al passo con l'incessante evolversi della modalità di lesione del patrimonio informatico aziendale.