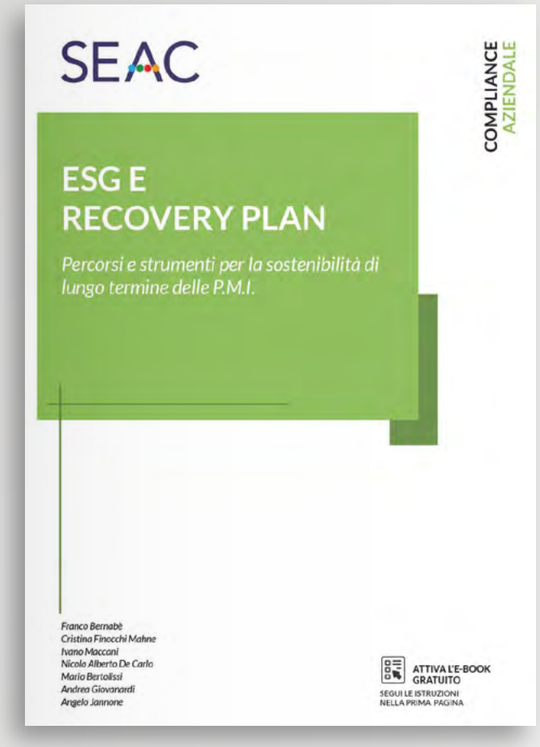
ISSN 2784-8213

COMPLIANCE

Marzo 2022 – n. 3 Anno II – Mensile

Poste Italiane S.P.A. – Spedizione in abbonamento postale- Aut. n°mipa/cn-ne/128/a.p./2021 - Periodico Roc – C.I.

SEAC



Passione per semplificare le cose

Il testo offre un' accurata analisi su come il Recovery Plan e i criteri ESG - se utilizzati al meglio - possano stimolare ed accelerare i processi di cambiamento di enti, professionisti ed imprese e pubbliche amministrazioni.

Autori del calibro di Franco Bernabè, Cristina Finocchi Mahne, Ivano Maccani, Nicola Alberto De Carlo, Mario Bertolissi, Andrea Giovanardi ed Angelo Jannone analizzano in modo chiaro e rigoroso come cogliere le opportunità ed operare correttamente nel panorama dei finanziamenti previsti dal Recovery Fund.

Il testo fornisce gli strumenti e le indicazioni utili per utilizzare al meglio gli ingenti fondi pubblici messi a disposizione dal PNRR, sbloccare gli assetti amministrativi/normativi e soprattutto riuscire a promuovere una nuova stagione di iniziative: dalla trasformazione dei processi alla transizione digitale, passando per innovazione sostenibile, smart working, conciliazione vita-lavoro, energie rinnovabili, ecc.

Direttore responsabile: Giovanni Bort
Product Manager: Giuliano Testi e Tullio Zanin
Comitato di redazione: Ivano Maccani, Anna Maria Carbone, Luigi Fruscione, Maurizio Block, Mario Bertolissi, Denise Boriero
Coordinatrici di redazione: Maria Chiara Volpi e Elisabetta Arcuri
Indirizzo della Redazione:
Via dei Solteri, 74 – 38121 Trento
Telefono 0461/805326 – email: compliance@seac.it
Editore: SEAC S.p.A. – Via dei Solteri, 74 – 38121 Trento
Telefono 0461/805111 – Fax 0461/805161 – email: seacspa@sicurezzapostale.it
C.F. 00865310221 – P.IVA 01530760220
Repertorio ROC n. 4275
Grafica ed impaginazione: Vulcanica.net
Tipografia: Litotipografia Alcione – Via Galilei, 47 – Lavis (TN)
Iscrizione al tribunale di Trento numero 4 del 19/02/2021

Hanno contribuito alla realizzazione di questo numero

Giulia Bontempini: Avvocato del Foro di Verona, nell'ambito del diritto civile si occupa in particolare del diritto d'impresa e di contrattualistica, esperta in diritto della privacy e nel settore del diritto dell'energia.

Olga Bussinello: Laureata in giurisprudenza, giornalista-pubblicista, dopo importanti esperienze nell'amministrazione pubblica e nel settore privato, è impegnata nella consulenza strategica per il settore agroalimentare.

Elisa Chizzola: Abilitata all'esercizio della professione di avvocato. Esperta compliance privacy. Giornalista-pubblicista ed autrice di numerosi articoli pubblicati su Riviste di settore specializzate nell'ambito del diritto civile, del diritto amministrativo e della protezione dei dati personali.

Silvia Crocelli: Laureata in Giurisprudenza alla Università Sapienza di Roma. Compliance Manager ex lege 4/2013 e svolge la pratica forense presso uno studio legale a Terni che si occupa principalmente di diritto del lavoro e diritto previdenziale. Consulente legale di ADIC UMBRIA, un'associazione a favore del cittadino consumatore.

Giovanni Finetto: Fondatore e presidente Fidem srl – Cyber Security e Intelligence, già ufficiale NATO, innovation manager (MiSE), senior security manager, perito sistemi informativi.

Paola Finetto: Avvocato, Partner di Andersen, esperta nella costruzione e implementazione di Modelli Organizzativi ex D.Lgs. 231/2001 e di procedure per la protezione dei dati, oltre che per la prevenzione e la gestione delle minacce cyber; presidente e componente di Organismi di Vigilanza, DPO/RPD.

Luigi Fruscione: Avvocato nel Foro di Roma, si occupa di Modelli 231 e diritto doganale con particolare riferimento al risparmio costi, collabora con importanti enti di formazione.

Ivano Maccani: Generale di Divisione della Guardia di Finanza, docente in materia di trasparenza e prevenzione dei rischi di reato all'Università di Padova e all'Università Cattolica del Sacro Cuore.

Matteo Montagner: Laurea Magistrale in Scienze Filosofiche e Master in Gestione e Strategia d'Impresa, negli anni attraverso collaborazioni con l'Università Ca' Foscari di Venezia e Società di Consulenza Internazionali ha accompagnato in processi di trasformazioni di piccole, medie e grandi imprese. Nel corso degli ultimi anni ha approfondito sul campo modalità di revisione degli assetti organizzativi aziendali e accompagnamento al cambiamento delle organizzazioni complesse.

Diletta Mora: Psicologo del lavoro e delle organizzazioni, esperta di benessere organizzativo e prevenzione mediante tecnologie di realtà virtuale, dottoranda di ricerca presso l'Università di Roma-Lumsa.

Sebastiano Rapisarda: Psicologo del lavoro e delle organizzazioni, esperto di benessere organizzativo e prevenzione mediante tecnologie telematiche, dottorando di ricerca presso l'Università di Roma-Lumsa.

Pier Luca Toselli: Luogotenente della Guardia di Finanza, docente nell'ambito del Master Executive di II livello in Criminologia e cyber Security – Modulo 7: Lotta al Crimine organizzato (Master Sida - Fondazione INUIT Tor Vergata), docente OSINT, First- Responder e Digital Forensic.

Stefano-Francesco Zuliani: ingegnere elettronico, esperto in diritto della privacy e in direzione di sistemi informativi aziendali. Si occupa inoltre di formazione professionale accreditata ed è CTU presso il Tribunale di Verona.

Arriva la primavera con il suo mantra: riparta l'economia dopo il torpore pandemico

di Olga Bussinello

L'avvicinarsi della bella stagione ed il desiderio di rinascita che porta con sé, aprono finalmente un nuovo capitolo dopo mesi, anzi anni, di incertezza e di chiusura, preoccupati solo di vedere una luce alla fine della galleria. L'informazione pubblica, che ci ha abituato a numeri, conteggi e percentuali per stabilire tante o poche limitazioni alla nostra libertà di agire, inizia ad affrontare il vero scoglio del prossimo futuro post pandemia: la crisi economica. Una crisi che già si stava preparando e che le preoccupazioni sanitarie hanno solo temporaneamente offuscato, con l'effetto placebo di bonus, sussidi e ristori in luogo di un serio incentivo alla libertà di impresa. Un torpore che, complice la scossa della partita Ucraino-Russa, sembra finire, per lasciare il posto alle questioni reali, come la crisi energetica, l'assenza delle materie prime, la competitività internazionale sulla questione climatico-ambientale, le nuove tecnologie e i loro rischi. In questo numero della rivista, trattiamo, quindi, molti argomenti legati all'attualità e alle nuove sfide per il mondo imprenditoriale. In relazione agli scambi commerciali fra Europa e Area Mediterranea, viene analizzata la recente modifica della Convenzione Paneuromediterranea (PEM) sull'origine doganale delle

merci, nell'ottica di favorire l'integrazione dell'approvvigionamento fra Europa e paesi aderenti all'Accordo, attraverso l'uniformazione di regole che attualmente richiedono l'utilizzo combinato di 60 diversi protocolli. Cambiano anche le norme sul cumulo delle diverse origini dei prodotti ed i criteri per stabilire la percentuale di tolleranza per poter dichiarare di origine italiana prodotti trasformati in Italia, ma con materie prime di provenienza diversa, nonché le modalità per la restituzione del dazio e la regola di non modificazione. Quest'ultima sarà attenuata, prevedendo, così, una movimentazione più agile dei prodotti, a patto che siano soddisfatti i requisiti della loro origine doganale.

Sempre in materia di competitività, si toccano due settori strategici per il nostro paese, come il turismo e l'agricoltura (biologica). Pensato per un possibile rilancio del comparto turistico, il decreto attuativo del PNNR n. 152/2021, pubblicato nella G.U. n.265/2021 ed in vigore dal 7 novembre scorso, rende disponibili 2,4 miliardi di euro attraverso un credito di imposta dell'80% cumulabile con un contributo a fondo perduto, la creazione di una sezione speciale dedicata del fondo di garanzia delle PMI, un credito di imposta per la digitalizzazione di agenzie di viaggio e tour operator, l'istituzione di un fondo rotativo attraverso cui saranno riconosciuti contributi a fondo perduto a sostegno di interventi di riqualificazione energetica, sostenibilità ambientale e innovazione digitale. Per consentire il rush finale dell'Italia verso gli obbiettivi del Green Deal Europeo al 2030, la Camera ha approvato in via definitiva il 9 febbraio scorso, il Testo Unico sulla produzione biologica in agricoltura e acquacoltura. Fra le novità, oltre ad un riassetto dei sistemi di tracciabilità e controllo, un nuovo fondo per finanziare lo sviluppo del sistema, un Marchio Unico Nazionale e l'accreditamento del metodo biodinamico quale parte integrante del sistema biologico.

Sempre in tema di PNNR, un articolo è dedicato ai sistemi di controllo e gestione dei finanziamenti del Piano. E', infatti, previsto che ogni dicastero responsabile di gestire direttamente uno o più interventi previsti, debba organizzare risorse tecniche ed umane per occuparsi del coordinamento delle attività di gestione, del loro monitoraggio, della rendicontazione, del controllo degli investimenti ed eventuali riforme. Dovrà, inoltre, garantire tutte le misure finalizzate alla prevenzione, all'individuazione e rettifica delle frodi, dei casi di corruzione, di conflitti di interessi e di duplicazione dei finanziamenti.

Con la riduzione del ricorso allo smart working ed il ritorno al lavoro in ufficio, sia per il pubblico che per il privato, diventa importante riconsiderare aspetti temporaneamente accantonati come i rischi connessi a segnalazioni di illeciti o reati da parte di dipendenti che, per questo, dovranno essere tutelati (whistleblowing), la prevenzione dei rischi di illeciti amministrativi o reati - grazie alla presenza in azienda di un buon modello organizzativo ai sensi del D.lgs n. 231/2001 – e la gestione dei possibili problemi connessi al rientro da una maternità.

Mentre Zuckerberg crea Metaverso, la piattaforma virtuale dove comunicare, giocare e divertirsi come nel mondo reale, ma senza le sue limitazioni, la tecnologia dovrà fare i conti anche con i suoi "ma", come il sottile confine fra la tutela della privacy e il diritto d'informazione e di pubblicità nella videosorveglianza o la tutela delle informazioni e dell'identità digitale dei dispositivi collegati ad una rete in un mondo sempre più connesso. Parliamo di *endpoint security*, che è un concetto ampio, di grande interesse per tutte le aziende che operano collegate ad una rete di dispositivi tecnologici (pc, smartphone, stampanti, telecamere, fax, ecc.) dei quali va garantita quell' integrità che il semplice antivirus non riesce ad assicurare. La protezione riguarda i processi, i dati sensibili, gli archivi di storage e i dispositivi connessi alla rete in questione e al web.

Terza ed ultima parte dell'analisi della circolare n.1/2018 della Guardia di Finanza dedicata alla prova digitale nell'attività di polizia giudiziaria del Corpo. Si analizzano le differenze nella scelta di acquisire il "contenitore" (intero contenuto di un supporto di memorizzazione) ovvero il "contenuto" (estrazione di dati digitali singolarmente identificabili come file, cartelle, ecc.) sia sotto il profilo della "migliore" opportunità probatoria, che varia a seconda dell'obbiettivo finale, sia sotto quello della fattibilità tecnologica delle ricerche ispettive, che richiede più valutazioni informatiche contestuali all'acquisizione e duplicazione delle prove digitali.

Sicuramente, se non interviene qualche fastidiosa variante, i prossimi mesi serviranno principalmente per impostare una possibile ripartenza dell'economia, con moderato entusiasmo e, speriamo - grazie al contributo di questa rivista - un po' più preparati.

PNNR: sistemi di controllo sulle spese

di Ivano Maccani

Il PNRR identifica lo strumento principale con cui rilanciare lo sviluppo e la crescita del nostro Paese, tramite un articolato programma costituito da riforme e investimenti strumentali, per affrontare alla radice le cause che più di altre hanno determinato ritardi ed inefficienze al sistema nel suo complesso.
Tre, in particolare, sono gli assi strategici su cui stanno convergendo i maggiori sforzi, coerentemente alle priorità fissate: digitalizzazione e innovazione, transizione ecologica e inclusione sociale.
Le modalità di attivazione dei progetti e l'accesso ai finanziamenti del PNRR da parte dei Soggetti attuatori e dei destinatari finali prevedono un numero significativo di procedure e strumenti, quale la partecipazione a bandi e avvisi pubblici, la presentazione di domande/progetti in risposta ad avvisi pubblici e la presentazione di singole istanze/richieste.
Risulta fondamentale che gli interventi individuati possano dispiegarsi in maniera efficace e all'interno di una cornice di piena legalità.
I controlli dovranno essere calibrati avendo riguardo alle caratterizzazioni delle varie realtà territoriali, alle fenomenologie di frode e alle tipologie di progetti di spesa ed essere il più possibile tempestivi rispetto al momento dell'erogazione dei servizi pubblici, per intercettare eventuali frodi sin dalla loro genesi, anche in ragione dell'ordine temporale previsto per la realizzazione del PNRR fissato al 31 dicembre 2026.
È opportuno sottolineare che l'articolo 22 del Regolamento UE 2021/241 prevede che gli Stati membri, nell'ambito dei rispettivi Piani nazionali per la ripresa e la resilienza, garantiscano *"la presenza di un sistema di controllo interno efficace ed efficiente finalizzato a prevenire, individuare e rettificare le frodi, i casi di corruzione e i conflitti di interessi, nonché a recuperare le somme erroneamente versate o utilizzate in modo non corretto"*.

Sempre in tema di controlli, le Linee guida UE sul Dispositivo per la Ripresa e la Resilienza, raccomandano agli Stati membri di avvalersi dei sistemi di gestione e controllo nazionali già esistenti, nonché delle strutture ed organismi già utilizzati per altri fondi dell'UE, suggerendo, di fatto, la soluzione di combinare processi e procedure di controllo in essere con controlli "aggiuntivi", al fine di monitorare non solo la regolarità della spesa, ma anche il conseguimento dei *milestone* e *target*, nonché il rispetto delle priorità trasversali e dei principi del *Next Generation EU*.
Il sistema di gestione e controllo adottato per il PNRR italiano, ufficialmente trasmesso alla Commissione europea lo scorso 30 aprile, è descritto nella parte 3 del documento e trova la sua fonte normativa nel DL 31 maggio 2021, n. 77 (convertito dalla Legge 29 luglio 2021, n. 108), che prevede un meccanismo che combina controlli "ordinari", previsti dall'ordinamento amministrativo vigente, con controlli "specifici" per il PNRR pertinenti per ogni struttura coinvolta nel flusso di rimborso comunitario, secondo il sistema multilivello di seguito descritto:

Per consentire che i fondi PNRR vengano utilizzati per soddisfare i bisogni reali della società e soprattutto che i soldi non finiscano nelle "tasche" sbagliate, è pertanto necessario poter contare su un sistema efficiente ed efficace di controlli.

CONTROLLI "ORDINARI" E "SPECIFICI"

Partendo dai Soggetti attuatori, vale a dire le Amministrazioni responsabili della realizzazione operativa degli interventi previsti dal PNRR sulla base delle specifiche competenze istituzionali ovvero della diversa titolarità degli interventi definita dal PNRR (ad esempio, Amministrazioni centrali, Regioni, Province autonome di Trento e Bolzano e gli enti locali), i controlli previsti a questo livello ricomprendono:
• controlli interni di regolarità amministrativa e contabile, che hanno l'obiettivo di garantire la legittimità, la correttezza e la regolarità dell'azione amministrativa, l'analisi e la valutazione della spesa;
• controlli di gestione, volti a ottimizzare il rapporto tra costi e risultati, anche mediante tempestivi interventi di correzione, nonché a verificare efficacia, efficienza ed economicità dell'azione amministrativa.
I Soggetti attuatori assicurano, inoltre, la completa tracciabilità delle operazioni e la tenuta di una apposita codificazione contabile per l'utilizzo delle risorse del PNRR e sono tenuti a conservare tutti gli atti e la relativa documentazione giustificativa su supporti informatici adeguati, nonché a renderli disponibili per le attività di controllo e di *audit*.
In tale contesto, la Corte dei Conti esercita il controllo sulla gestione di cui all'art. 3, comma 4, della Legge n. 20/1994, svolgendo, in particolare, valutazioni di economicità, efficienza ed efficacia circa l'acquisizione e l'impiego delle risorse finanziarie provenienti dai fondi di cui al PNRR. Tale controllo si informa a criteri di cooperazione e coordinamento con la Corte dei Conti Europea. Ai sensi dell'art. 3, comma 6, della citata Legge, inoltre, la Corte dei Conti riferisce, almeno semestralmente, al Parlamento sullo stato di attuazione del PNRR.
In base a quanto previsto dall'art. 7, comma

8[1], del DL n. 77/2021, al fine di migliorare l'efficacia complessiva delle misure volte a prevenire, ricercare e contrastare le violazioni in danno degli interessi economico-finanziari dell'Unione Europea, dello Stato, delle Regioni e degli Enti locali, connessi alle misure di sostegno e finanziamento del PNRR, è stato sottoscritto uno specifico protocollo d'intesa tra la Ragioneria Generale dello Stato e la Guardia di Finanza.

Per quanto concerne le Amministrazioni centrali titolari di interventi previsti nel PNRR, va innanzitutto precisato che le stesse operano da raccordo per i Soggetti attuatori e svolgono, sulla base delle informazioni ricevute da questi ultimi sull'avanzamento dei progetti, ulteriori attività di controllo, distinte in:

- verifiche formali sulla regolarità delle spese e delle relative procedure rendicontate dai Soggetti attuatori, a campione estratte sulla base di un'accurata analisi di rischio. Tali verifiche consistono in controlli amministrativo-contabili *on desk*, accompagnati da eventuali approfondimenti *in loco*, aventi l'obiettivo di accertare la correttezza e la conformità alla normativa di riferimento riguardo alle procedure di gara/affidamento adottate per l'attuazione dell'intervento, nonché l'effettività, la legittimità, l'ammissibilità e l'assenza di doppio finanziamento delle spese stesse;
- verifiche sul raggiungimento dei *target* e dei *milestones* previsti dai progetti, svolte mediante l'esame della documentazione ricevuta dai Soggetti attuatori;
- verifiche sul rispetto delle priorità trasversali[2] e dei principi *DNSH*[3], *Tagging* clima e digitale.

Altro soggetto di rilievo, inquadrabile nel sistema di controllo, si identifica nel Servizio Centrale per il PNRR che riceve, con cadenza almeno bimestrale, le rendicontazioni dalle Amministrazioni centrali titolari degli interventi e pone in essere attività di controllo aggiuntive sui dati comunicati, propedeutiche all'invio delle richieste di pagamento alla Commissione Europea, avvalendosi del supporto dell'Unità di Missione, istituita dall'art. 1, comma 1050, della Legge n. 178/2020[4].

Altro ruolo importante è riservato all'Unità di *Audit*, istituita[5] presso il Ministero dell'Economia e delle Finanze – Dipartimento della Ragioneria Generale dello Stato – Ispettorato Generale per i Rapporti con l'Unione Europea (IGRUE)[6], che attua specifiche procedure, coerenti con gli *standard* e i principi di *audit* internazionalmente riconosciuti, tese a garantire l'efficacia del Sistema di Gestione e Controllo del PNRR ed in particolare:

- verifiche di sistema, finalizzate a valutare la validità delle procedure adottate dai soggetti preposti alla gestione, realizzazione e verifica delle progettualità del PNRR mediante *test* di conformità su specifiche operazioni selezionate (*audit* sulle strutture amministrative coinvolte ed eventuali controlli trasversali su temi ritenuti rilevanti ai fini del PNRR);
- verifiche sulle operazioni, finalizzate a verificare la correttezza e la coerenza dei progetti in relazione ad un campione di operazioni, selezionate sulla base di un'analisi di rischio e di specifiche metodologie.

Per lo svolgimento di tali attività, l'Unità individua una precisa strategia di *audit*, formalizzata in un apposito *Audit planning memorandum*. A conclusione dell'*iter,* viene invece predisposta una sintesi degli *audit* che, insieme alla dichiarazione di gestione, viene allegata alla richiesta di pagamento semestrale con lo scopo di aggiornare la Commissione Europea sulla regolarità delle procedure poste in essere e sui risultati raggiunti con i progetti realizzati.

Le attività di controllo fin qui descritte vengono "registrate" in un sistema informatico unitario denominato "ReGiS", che si avvale di appositi strumenti (*check-list*) utili ai vari soggetti per tenere traccia degli esiti delle operazioni realizzate, consultabile da tutti gli organismi coinvolti nelle attività di verifica e controllo[7].

Proprio l'implementazione di sistemi informatici integrati in grado di combinare dati eterogenei risulta di estremo interesse, in quanto strumenti utili ai fini della prevenzione, individuazione e contrasto delle irregolarità. Attraverso tali strumenti è infatti possibile effettuare un monitoraggio completo dei progetti, con particolare attenzione sui casi di conflitto di interessi, rischio di frode e doppio finanziamento. Al riguardo si segnalano:

a) il sistema informativo comunitario antifrode "Arachne IT System", che permette l'interrogazione di specifici indicatori e classifiche di rischio connessi ai possibili casi di conflitto di interesse (frequenza di interrelazioni di codici fiscali e partite IVA associati e di fornitori e contraenti), nonché analisi di rischio utili a orientare i controlli verso progetti e soggetti potenzialmente più esposti al rischio di frode;

b) il sistema "ReGiS", che in relazione al ri-

1 *"Ai fini del rafforzamento delle attività di controllo, anche finalizzate alla prevenzione ed al contrasto della corruzione, delle frodi, nonché ad evitare i conflitti di interesse ed il rischio di doppio finanziamento pubblico degli interventi, ferme restando le competenze in materia dell'Autorità nazionale anticorruzione, le amministrazioni centrali titolari di interventi previsti dal PNRR possono stipulare specifici protocolli d'intesa con la Guardia di Finanza senza nuovi o maggiori oneri per la finanza pubblica".*

2 *Rispetto e promozione della parità di genere, protezione e valorizzazione dei giovani teso a garantire l'attuazione di interventi e riforme a beneficio diretto e indiretto per le future generazioni e superamento dei divari territoriali.*

3 *Acronimo di "Do Not Significant Harm", testualmente "non arrecare un danno significativo". Si fa riferimento, in particolare, al rispetto di requisiti di sostenibilità ambientale.*

4 *"Con decorrenza dal 1° gennaio 2021, è istituita, presso il Dipartimento della Ragioneria generale dello Stato del Ministero dell'economia e delle finanze, un'apposita unità di missione con compiti di coordinamento, raccordo e sostegno delle strutture del medesimo Dipartimento a vario titolo coinvolte nel processo di attuazione del programma Next Generation EU (...)".*

5 *Ai sensi dell'art. 7 del DL n. 77/2021.*

6 *Quindi in posizione di separazione funzionale rispetto alle strutture amministrative coinvolte nella gestione attuativa del PNRR.*

7 *Commissione Europea, Ufficio europeo per la Lotta Antifrode, Corte dei conti europea ecc.*

schio del doppio finanziamento, consente di avere una visione completa della distribuzione dei fondi nei vari territori e delle relative fonti di finanziamento (si possono monitorare, in un unico *database*, sia i progetti legati al PNRR, che quelli finanziati dalle altre politiche di investimento comunitarie e nazionali);
c) la Piattaforma Integrata Anti-Frode (PIAF-IT), la cui entrata in funzione è prevista entro dicembre 2021, consentirà di aggregare dati provenienti da fonti nazionali ed europee, costituendo un patrimonio informativo utile alla prevenzione delle frodi (si potranno, in particolare, ottenere informazioni su un determinato soggetto e/o fenomeno senza dover ricorrere a diverse e distinte interrogazioni su differenti banche dati).
d) la Dorsale Informatica della Guardia di Finanza che consente, tra l'altro, l'interrogazione "*per elenchi predefiniti*", con acquisizione istantanea delle informazioni presenti in ciascuna banca dati disponibile su una serie multipla di entità di interesse fornendo, inoltre, *link* ai portali tematici delle diverse risorse, con possibilità di esplorare le connessioni eventualmente emergenti tra due o più *target* selezionati[8];
e) il nuovo applicativo INPS "MoCOA" che consente di agevolare le verifiche di congruità occupazionale;
f) il sistema di business intelligence nel settore degli appalti denominato "MO. CO.P." – monitoraggio dei contatti pubblici - che a regime permetterà di sviluppare analisi di rischio e di contesto automatizzate. In particolare, il sistema consentirà di rendere fruibili per la consultazione elementi puntuali e aggregati concernenti gli appalti aggiudicati dalle diverse stazioni appaltanti pubbliche, attraverso una correlazione ragionata, sul piano oggettivo e soggettivo, delle informazioni complessivamente disponibili.

RISCHI DI INFILTRAZIONI DELLA CRIMINALITA' ORGANIZZATA ED ECONOMICO-FINANZIARIA

Nel tempo, le organizzazioni criminali hanno progressivamente desistito dalla ricerca di forme immediate e dirette di accaparramento degli appalti preferendo, piuttosto, esercitare il controllo sulla loro gestione "*a valle*", cioè nella sola fase esecutiva, grazie all'autonoma capacità di intimidazione presente a livello territoriale, così rinunciando, di fatto, a collusioni o infiltrazioni nelle strutture pubbliche.
I controlli di carattere sostanziale, in relazione alle potenziali infiltrazioni della criminalità nell'utilizzo dei fondi stanziati dal PNRR può assumere a seconda del momento cronologico di aggiudicazione della commessa pubblica per la realizzazione dell'opera finanziata, un carattere preventivo o repressivo:
• nel primo caso, il sistema di prevenzione del rischio di infiltrazione mafiosa si basa sull'individuazione di eventuali cause impeditive e ostative alla partecipazione alla gara pubblica, ossia sulla verifica, da parte delle amministrazioni appaltanti, della non ricorrenza di ulteriori cause impeditive e ostative, attraverso l'acquisizione della documentazione e delle informazioni previste dal *Codice delle leggi antimafia* (D.Lgs. n. 159/2011);
• il secondo, viceversa, poggia su un sistema di controlli *in itinere* presso i cantieri (al fine di verificare le imprese effettivamente operanti e di monitorare il personale e i mezzi impiegati), nonché di cautele sulla tracciabilità dei flussi finanziari per la ricostruzione dei percorsi seguiti dalle risorse pubbliche, dal committente sino all'ultimo dei beneficiari.
Il controllo criminale delle commesse pubbliche ha registrato una progressiva estensione anche alla fase di esecuzione dell'opera, attraverso interventi volti all'imposizione coattiva di contratti di guardiania ai cantieri, ovvero di forniture di opere, materiali e prestazioni a vantaggio

8 Nel dettaglio, a fronte di un intero insieme di identificativi (più codici fiscali, partite IVA o targhe di automezzi) censiti in un'unica consultazione, è possibile verificarne il censimento o meno in un elenco di banche dati e/o sistemi operativi - predefinito dall'utente - interrogabili tramite la Dorsale.

di imprese riconducibili al medesimo circuito criminale, all'assunzione come manodopera di personale "raccomandato", ecc.
A tal fine, appare opportuno instaurare un canale di collaborazione con i Soggetti attuatori, per monitorare le iniziative finanziate dai fondi del PNRR e poter, anche in fase embrionale, sottoporre ad analisi preventiva i dati comunicati ovvero pianificare successivamente all'avvio della cantierizzazione dell'opera, mirate attività ispettive.
In tale contesto, devono essere tenute in considerazione le novità introdotte dal DL 31 maggio 2021, n. 77 (c.d. Decreto "*Semplificazioni-bis*"), convertito nella Legge 29 luglio 2021, n. 108, recante le disposizioni finalizzate a semplificare le procedure di affidamento concernenti la realizzazione di opere che rientreranno nel PNRR (Piano Nazionale di Ripresa e Resilienza)[9], al fine di velocizzarne i tempi di realizzazione[10].
Più in particolare, con specifico riferimento alle distinzioni tra le due citate tipologie di controlli, si evidenzia quanto segue.
a) Controlli di natura preventiva
In tale contesto assumono rilevanza i gruppi interforze antimafia, pool provinciali coordinati dalle Prefetture e composti da rappresentanti territoriali delle forze di Polizia e dei Centri operativi della DIA, nel cui ambito viene promosso il controllo di appalti e sub-appalti allo scopo di escludere in partenza quelli potenzialmente interessati da infiltrazioni della criminalità.
Per dare una dimensione del fenomeno, le interdittive antimafia attivate nel solo 2020 sono state circa un migliaio, in netto aumento rispetto al passato.
Ciò dà la misura di quanto sia necessario non sottovalutare il tema delle infiltrazioni criminali, emerso sia nei tentativi di illecita acquisizione delle provvidenze e commes-

9 Le novità introdotte non incidono esclusivamente sul Codice degli appalti (D.Lgs. n. 50/2016) ma vanno a modificare anche il DL 18 aprile 2019, n. 32 (c.d. "Sblocca-cantieri") e la disciplina transitoria del DL 16 luglio 2020, n. 76 (c.d. Decreto "Semplificazioni"). Tali modifiche si applicano alle procedure i cui bandi o avvisi di indizione della gara siano pubblicati dopo il 1° giugno 2021.

10 A tale scopo, è stata altresì prevista, a mente dell'art. 5 del DL n. 77/2021, l'istituzione dell'Unità per la razionalizzazione e il miglioramento dell'efficacia della regolazione presso la Presidenza del Consiglio dei Ministri, che ha il compito di superare ostacoli normativi, regolamentari e burocratici che possano rallentare l'attuazione del piano.

se pubbliche, sia nella gestione diretta o indiretta di imprese operanti in settori produttivi oggi e, soprattutto, in prospettiva più attrattivi, oppure andati in crisi a causa della pandemia.
La storia, infatti, insegna come gli scenari di difficoltà socioeconomica siano sempre stati molto allettanti per la criminalità di ogni genere, rappresentando essi, con tutto il loro portato di dolore, debolezze e insicurezza, anche una deprecabile, ma enorme, opportunità di arricchimento illecito per taluni.
b) Controlli di natura repressiva
L'accesso ai cantieri, soprattutto in fase di realizzazione dell'opera, costituisce uno strumento operativo particolarmente utile per rilevare l'effettiva situazione che si presenta a "cantiere aperto" e per verificare la corrispondenza fra quanto dichiarato dall'imprenditore riguardo alle ditte affidatarie e subappaltatrici – le uniche autorizzate a essere presenti, secondo il piano di affidamenti, con le proprie maestranze e i propri mezzi sul luogo di esecuzione dell'opera – e lo stato dei fatti, riscontrando, così, eventuali anomalie più o meno indizianti.

A tal fine, il legislatore ha introdotto lo strumento del controllo dei cantieri, realizzato attraverso un potere di accesso assegnato, in origine, all'Alto Commissario Antimafia e, successivamente, ai Prefetti, i quali si avvalgono dei i cc.dd. "Gruppi Interforze", coordinati da un funzionario dell'Ufficio Territoriale del Governo e composti da un funzionario della Polizia di Stato, un ufficiale dell'Arma dei Carabinieri e della Guardia di Finanza, un rappresentante del Provveditorato alle Opere Pubbliche, un rappresentante dell'Ispettorato del lavoro, nonché un funzionario delle articolazioni periferiche della Direzione Investigativa Antimafia.

Le nuove norme di origine della Convenzione Paneuromediterranea: le norme transitorie per facilitare il commercio

di Luigi Fruscione

Premessa

Per comprendere l'importanza della Convenzione PanEuroMediterranea (PEM) nell'ambito del commercio dell'Unione Europea basta visionare l'elenco dei Paesi sottoscrittori che vanno, tra gli altri, dallo Stato di Israele al Regno di Giordania, dalla Repubblica del Libano al Regno del Marocco, dalla Repubblica tunisina alla Repubblica di Turchia.

Nel 2020 il 40% del commercio di natura preferenziale dell'Unione, si è svolto con valori pari a 385 miliardi di euro per le esportazioni e 294 miliardi di euro per le importazioni[1].

Proprio in considerazione dell'importanza commerciale si è lavorato per giungere alla predisposizione di norme di origine che favorissero, ancora di più, il commercio tra le parti contraenti, giungendo all'elaborazione di un nuovo testo.

La Convenzione Paneuromediterranea

La Convenzione PEM, entrata in vigore il 1° maggio 2012, costituisce il quadro normativo di riferimento per l'applicazione del sistema paneuromediterraneo di cumulo dell'origine tra le Parti contraenti della Convenzione stessa, che sono: l'Unione europea, gli Stati EFTA[2], Le Isole Fær Øer, i Paesi partecipanti al processo di Barcellona[3], i Paesi dei Balcani occidentali che partecipano al processo di stabilizzazione e di associazione dell'UE[4], Ucraina, Georgia e Moldavia.

Il sistema PEM di cumulo dell'origine si basa su una rete di accordi di libero scambio e stabilisce norme di origine identiche che consentono di applicare il cumulo diagonale.

In considerazione delle criticità operative nella gestione delle diverse norme inserite nella rete di protocolli bilaterali esistenti tra i Paesi o territori dell'area paneuromediterranea, si era resa necessaria la redazione di un unico quadro.

Tale impostazione determinò la scelta di redigere una convenzione regionale relativa alle norme di origine preferenziali, cui gli accordi di libero scambio individuali vigenti tra i Paesi della zona facessero riferimento; infatti l'art.1 della Convenzione stabilisce le "*disposizioni sull'origine delle merci scambiate nell'ambito dei pertinenti accordi conclusi tra le parti contraenti*".

1 *Si veda la "Guidance transitional PEM rules of origin" (v1.0 – 16 august 2021) - della Commissione europea, DG Taxation and Customs Union;*

2 *Islanda, Liechtenstein, Norvegia, Svizzera;*

3 *Algeria, Egitto, Giordania, Israele, Libano, Marocco, Palestina, Siria, Tunisia, Turchia;*

4 *Albania, Bosnia-Erzegovina, Kosovo, Macedonia del Nord, Montenegro, Serbia;*

I terzi - ovverosia qualsiasi Paese o territorio limitrofo che non è una parte contraente - possono diventare parti contraenti della Convenzione purché tra il Paese o il territorio candidato e almeno una delle parti contraenti sia in vigore un accordo di libero scambio che preveda norme di origine preferenziali.

La Convenzione stabilisce la definizione della nozione di «prodotti originari» (prescrizioni generali, cumulo dell'origine, prodotti interamente ottenuti, prodotti sufficientemente lavorati o trasformati, lavorazioni o trasformazioni insufficienti, accessori, pezzi di ricambio e utensili, etc.), i requisiti territoriali (principio di territorialità, trasporto diretto, etc), i casi di restituzione o esenzione, la prova dell'origine e i metodi di cooperazione amministrativa.

Ai fini dell'applicazione dell'accordo, i seguenti prodotti si considerano originari di una parte contraente quando sono esportati in un'altra parte:

a) i prodotti interamente ottenuti nella parte contraente;

b) i prodotti ottenuti nella parte contraente utilizzando materiali non interamente ottenuti sul suo territorio, a condizione che detti materiali siano stati oggetto nella parte contraente di lavorazioni o trasformazioni sufficienti;

c) le merci originarie dello Spazio economico europeo (SEE) ai sensi del protocollo n. 4 dell'accordo sullo Spazio economico europeo. Tali merci sono considerate originarie dell'Unione europea, dell'Islanda, del Liechtenstein o della Norvegia («parti SEE») quando sono esportate, rispettivamente, dall'Unione europea, dall'Islanda, dal Liechtenstein o dalla Norvegia in una parte contraente diversa dalle parti contraenti del SEE.

Fermo quanto appena evidenziato, sono considerati originari della parte esportatrice, quando sono esportati, i prodotti fabbricati all'interno della prima utilizzando materiali originari:

- della Svizzera (compreso il Liechtenstein), dell'Islanda, della Norvegia, della Turchia o dell'Unione europea, a condizione che tali materiali siano stati sottoposti nella parte contraente esportatrice a lavorazioni o trasformazioni più complesse rispetto alle

operazioni individuate quali insufficienti all'art. 6 della Convenzione;
- delle Isole Faerøer o di qualsiasi partecipante al processo di Barcellona, esclusa la Turchia, o qualsiasi altra parte contraente diversa da quelle indicate al punto precedente, a condizione che tali materiali siano stati sottoposti nella parte contraente esportatrice a lavorazioni o trasformazioni più complesse rispetto alle operazioni insufficienti di cui all'art.6 della Convenzione.
In entrambi i casi non è necessario che i materiali siano stati oggetto di lavorazioni o trasformazioni sufficienti.
Da ciò deriva che i prodotti originari delle parti contraenti che non sono sottoposti ad alcuna lavorazione o trasformazione nella parte esportatrice, conservano la loro origine quando vengono esportati in una delle altri parti contraenti.
Ulteriormente si prevede che, ai fini dell'attribuzione dell'origine, il cumulo possa trovare applicazione qualora:
a) un accordo commerciale preferenziale sia in vigore tra le parti contraenti che partecipano all'acquisizione del carattere originario e la parte contraente di destinazione;
b) i materiali e i prodotti abbiano acquisito il carattere originario con l'applicazione di norme di origine identiche a quelle previste dalla Convenzione;
c) siano stati pubblicati avvisi da cui risulti che sussistono i requisiti necessari per l'applicazione del cumulo nella Gazzetta ufficiale dell'Unione europea (serie C) e nelle parti contraenti che sono parte degli accordi pertinenti.
Si considerano interamente ottenuti in una parte contraente quando sono esportati in un'altra parte contraente:
a) i prodotti minerari estratti dal suolo o dal fondo marino della parte contraente esportatrice;
b) i prodotti del regno vegetale ivi raccolti;
c) gli animali vivi, ivi nati e allevati;
d) i prodotti che provengono da animali vivi ivi allevati;
e) i prodotti della caccia o della pesca ivi praticate;
f) i prodotti della pesca marittima e altri prodotti estratti dal mare, al di fuori delle acque territoriali della parte contraente esportatrice, con le sue navi;
g) i prodotti ottenuti a bordo delle sue navi officina, esclusivamente a partire dai prodotti di cui alla lettera f);
h) gli articoli usati, a condizione che siano ivi raccolti e possano servire soltanto al recupero delle materie prime, compresi gli pneumatici usati che possono servire solo per la rigenerazione o essere utilizzati come cascami;
i) gli scarti e i residui provenienti da operazioni manifatturiere ivi effettuate;
j) i prodotti estratti dal suolo o dal sottosuolo marino ubicato fuori delle sue acque territoriali, purché essa eserciti a fini di sfruttamento diritti esclusivi su tale suolo o sottosuolo;
k) le merci ivi ottenute esclusivamente a partire dai prodotti di cui alle lettere da a) a j).
Per quel che attiene ai prodotti sufficientemente lavorati, la Convenzione richiama delle regole specifiche per prodotto trasfuse nell'allegato II.
Dette condizioni stabiliscono la lavorazione o la trasformazione cui devono essere sottoposti i materiali non originari impiegati nella fabbricazione e si applicano unicamente a detti materiali. Ne consegue pertanto che, se un prodotto che ha acquisito il carattere originario - perché soddisfa le condizioni indicate nell'elenco - è impiegato nella fabbricazione di un altro prodotto, le condizioni applicabili al prodotto in cui esso è incorporato non gli si applicano e non si tiene alcun conto dei materiali non originari eventualmente impiegati nella sua fabbricazione.
Ad esempio: Capitolo 8 del Sistema Armonizzato (Frutta commestibili; scorze di agrumi o di meloni) - la regola primaria prevede per il conferimento dell'origine la fabbricazione in cui tutta la frutta utilizzata è interamente ottenuta, e il valore di tutti i materiali del capitolo 17 utilizzati (zuccheri e prodotti a base di zuccheri) non ecceda il 30 % del prezzo franco fabbrica del prodotto.
Ulteriore esempio: capitolo 46 del Sistema Armonizzato (Lavori di intreccio, da panieraio o da stuoiaio) - la regola primaria prevede la fabbricazione a partire da materiali di qualsiasi voce, esclusi quelli della stessa voce del prodotto.
La Convenzione prevede anche un regime di tolleranze - strumento utilizzato per rendere maggiormente flessibili le regole di conferimento dell'origine specifiche - stabilendo che i materiali non originari che, in base alle condizioni indicate nell'elenco dell'Allegato II, non devono essere utilizzati nella fabbricazione di un prodotto, possono essere ugualmente utilizzati a condizione che:
a) il loro valore totale non superi il 10 % del prezzo franco fabbrica del prodotto;
b) in virtù del presente paragrafo non si superi alcuna delle percentuali indicate nell'elenco con riguardo al valore massimo dei materiali non originari[5].

Le norme transitorie

Come evidenziato in precedenza, le singole autorità dei Paesi sottoscrittori della Convenzione hanno avvertito la necessità di rendere maggiormente facile l'accesso alle regole di origine così si sono iniziati dei negoziati che si sono sviluppati nel corso di un decennio.
Nel dicembre del 2020 il Consiglio dell'Unione Europea ha approvato 21 decisioni finalizzate all'aggiornamento degli accordi di libero scambio; l'entrata in vigore era fissata per il 1° settembre 2021.
Le nuove disposizioni trovano applicazione in parallelo con quelle della Convenzione e ciò fino alla sua revisione completa; infatti, non tutte le parti hanno approvato le modifiche.
A partire dal 1° settembre 2021, le nuove norme sono diventate applicabili, in una fase iniziale, tra l'UE ed i seguenti Paesi partner: Albania, Isole Farøer, Georgia, Giordania, Islanda, Macedonia del Nord, Norvegia, Palestina, Repubblica di Moldova, Serbia e Svizzera.
La Direzione TAXUD della Commissione europea aggiornerà man mano la ratifica delle nuove disposizioni da parte di altri Paesi rientranti nella Convenzione PEM.

5 Il regime delle tolleranze non trova applicazione ai prodotti contemplati dai capitoli da 50 a 63 del sistema armonizzato (materie tessili e loro manufatti);

Quindi, gli operatori economici possono scegliere se utilizzare le norme di origine contenute nella Convenzione originaria oppure le regole di origine revisionate - cd. norme transitorie - con le parti contraenti PEM che hanno deciso di procedere alla loro applicazione.
Sotto l'aspetto operativo tale scelta determina che, in caso di utilizzo delle nuove disposizioni, potrà essere applicato il cumulo dell'origine tra le parti contraenti richiedenti solo se l'origine dei materiali e dei componenti utilizzati nel cumulo ha acquisito l'origine conformemente alle norme transitorie.
Le principali novità introdotte dalle norme di origine rivedute attengono alla semplificazione delle disposizioni di origine, al cumulo, alla clausola del no-drawback, alle tolleranze, alla separazione contabile e alle prove di origine.
Ad esempio in tema di tolleranze, in deroga all'articolo 4 (lavorazioni sufficienti) - e fatti salvi i paragrafi 2 e 3 dell'articolo 5 (tolleranze) - si prevede che i materiali non originari che, secondo le condizioni stabilite nell'elenco di cui all'allegato II, non devono essere utilizzati nella fabbricazione di un determinato prodotto possono comunque essere utilizzati, a condizione che il loro peso netto totale o il valore valutato per il prodotto non ecceda:
a) il 15 % del peso netto del prodotto di cui ai capitoli 2 e da 4 a 24, altri rispetto ai prodotti della pesca trasformati di cui al capitolo 16;
b) il 15 % del prezzo franco fabbrica del prodotto per i prodotti diversi da quelli contemplati al punto (a)[6].
Non è consentito il superamento di alcuna delle percentuali per il contenuto massimo di materiali non originari come specificato nelle regole previste nell'elenco nell'allegato II.
Quindi, in pratica, per i prodotti agricoli, il 15 % è fissato al peso netto del prodotto, mentre per il resto dei prodotti, questa percentuale è applicata al prezzo franco fabbrica del prodotto finale.
Parimenti, rispetto alle disposizioni vigenti, viene offerta maggiore flessibilità per quanto riguarda i prodotti tessili per i quali si applicano le tolleranze indicate nelle note introduttive.
Applicando la tolleranza nella lavorazione di un prodotto, non è consentito superare la percentuale massima di materiali non originari nella regola dell'elenco. Ciò significa che le percentuali non possono essere cumulate per soddisfare la regola dell'elenco.
Tra gli interventi di maggior rilievo occorre segnalare anche l'introduzione di regole per rendere il cumulo regionale maggiormente flessibile. La disposizione di riferimento è l'art. 7 delle disposizioni transitorie attraverso il quale:
1) si conferma il cumulo per tutti i prodotti a condizione che vengano applicate regole di origine identiche tra i Paesi partner coinvolti nel cumulo;
2) si stabilisce il cumulo completo generalizzato per tutti i prodotti salvo i casi dei tessili e dell'abbigliamento (capitoli 50-63 del sistema armonizzato di classificazione delle merci per queste merci si prevede il cumulo bilaterale completo).
Nell'ambito dell'applicazione delle norme transitorie, i Paesi partner potranno concordare l'estensione del cumulo integrale anche ai prodotti dei capitoli 50-63 del Sistema Armonizzato; in tal caso la parte informerà l'altra parte e la Commissione europea.
Ulteriore aspetto su cui le nuove disposizioni sono intervenute riguarda la clausola del no-drawback, ovverosia l'impossibilità di ottenere il duplice vantaggio della preferenza tariffaria e della restituzione o la sospensione dei dazi (ad esempio, nel traffico di perfezionamento attivo); infatti le disposizioni della Convenzione PEM stabiliscono il principio generale del divieto di restituzione ai materiali utilizzati nella fabbricazione di qualsiasi prodotto, mentre in base alle norme transitorie - art. 16 - il divieto è eliminato per tutte le merci salvo i casi dei materiali utilizzati nella fabbricazione dei prodotti che rientrano nell'ambito di applicazione dei capitoli da 50 a 63 del Sistema Armonizzato.
Ulteriore intervento di semplificazione è relativo alla regola del trasporto diretto che viene sostituita con la non manipolazione prevista dall'art.14 delle disposizioni transitorie; il principio rimane lo stesso di quello contenuto nella Convenzione, ossia che le merci devono essere trasportate direttamente dal territorio di una Parte contraente all'altra affinché sia garantito che le merci che giungono nel Paese di importazione siano le stesse che hanno lasciato quello di esportazione.
Ulteriori interventi attengono ad una maggiore flessibilità delle regole di separazione contabile previste dall'art.12 delle norme transitorie e dalle disposizioni sulla prova di origine (art.17), campo, questo, in cui le norme transitorie prevedono l'utilizzo dell'EUR 1 (o dichiarazione di origine rilasciata dall'esportatore) al posto del EUR 1/EUR MED semplificando così il sistema di prova dell'origine.
È inoltre prevista la possibilità di provare l'origine attraverso il sistema degli esportatori registrati (REX), che è il sistema informatico attraverso il quale gli esportatori registrati in una apposita banca dati, dal 2017, possono attestare direttamente l'origine preferenziale delle merci nell'ambito dell'SPG, degli Accordi preferenziali che prevedono tale strumento e del PTOM (Paesi e territori d'oltremare).

6 E' prevista una eccezione per i prodotti di cui ai capitoli da 50 a 63 del Sistema Armonizzato per cui trovano applicazione le tolleranze di cui alle note 6 e 7 dell'allegato I.

Le linee guida della Guardia di Finanza nella gestione della fonte di prova digitale. Parte III

di Pier Luca Toselli

Con questa ultima parte si conclude la disamina della circolare 1/2018 della Guardia di Finanza da me affrontata in altre due parti già pubblicate nel mese di gennaio e febbraio u.s.
Prima di affrontare il tema di quelle che definiremo nel prosieguo "acquisizioni informatiche/estrazione di quanto d'interesse", la Circolare 1/2018, si richiama ad un principio espresso in una giurisprudenza di legittimità [1] evidenziando che a seguito delle attività di ricerca possono verificarsi distinte situazioni rispetto alle quali l'acquisizione probatoria può riguardare il dato informatico in sé, ovvero il medesimo dato quale mero "recipiente" di informazioni. Una distinzione tra "contenuto" e "contenitore" che ha sostanziali implicazioni sulle modalità di ricerca, individuazione ed acquisizione dei documenti informatici di interesse, anche per quanto concerne i risvolti amministrativo-giuridici che ne derivano.

Sul piano pratico, si presenta quindi a seconda degli specifici "casi" la possibilità di:
• effettuare l'estrazione di mirate informazioni digitali, ove l'interesse degli operanti risulti circoscritto a particolari contenuti informatici specificamente individuabili – quali a titolo di esempio: file, email, traffico di rete o qualunque altro dato digitale singolarmente identificabile;
• effettuare l'acquisizione dell'intero contenuto di un supporto di memorizzazione, prelevandone una "copia immagine", cosiddetta "copia bit to bit" o "bit stream image", al fine di preservarne l'integrità e l'identità alle condizioni in cui si trovava al momento della sua acquisizione e consentire successive verifiche, esami ed accertamenti.
È evidente come sul piano strategico, operativo ed investigativo, le due possibilità riverberano in maniera alquanto differente. Nel primo caso pur assicurando attraverso idonei strumenti il rispetto delle *best-practices* in materia di digital forensics, è evidente come l'assenza di una "bit stream image" costringa gli operatori a rinunciare alla possibilità di:
• poter esaminare con riferimento al "contenitore" la presenza di eventuali files cancellati - non allocati - che in determinati contesti potrebbero invece assurgere per l'appunto ad elementi strategici e di interesse per l'indagine;
• procedere ad un accurato e minuzioso esame di tutti i files raccolti e non solo di quelli "frutto" delle ricerche viziate, dalle problematiche già evidenziate nella seconda parte di questa serie di miei articoli.
Invero, per quanto accurate possano essere le "indicizzazioni", le ricerche effettuate sul posto, tenuto anche conto delle fallibilità già in precedenza evidenziate, potrebbero risultare incomplete ed inefficaci.
Non a caso, la circolare evidenzia che, qualora si sospetti fondatamente che il contribuente possa aver cancellato file di interesse, sarà necessario procedere ad una bit stream image del supporto che di fatto permetta poi successive operazioni di "carving" volte al recupero dei dati cancellati.
Proprio con riferimento ai dati cancellati laddove ritenuto utile o necessario rispetto alle finalità dell'intervento e/o al profilo soggettivo del contribuente, i militari operanti possono acquisire anche l'intero contenuto di supporti di memoria (HDD interni o esterni, USB drive, schede SD etc.), avendo cura, ovviamente, di effettuare quello che le best practices in materia internazionale definiscono una copia forense degli stessi, cioè un archivio in formato EWF o simili (AFF, DD, RAW). Tale modalità permette al pari di un "clone" la creazione di una copia bit a bit del supporto, con possibilità di poter esaminare ed anche recuperare (qualora non sovrascritto) quello spazio del disco cosiddetto non allocato ove trovano conservazione anche quei files che risultano "cancellati" dal contribuente ed ancora non sovrascritti da altri dati.
Va evidenziato in merito che l'avvento di nuovi supporti di memoria e nuove tecnologie rendono più difficoltose le operazioni cd. di "carving", ossia il recupero dei files cancellati. Senza entrare in temi non contesto di questa trattazione, mi permetto tuttavia di sollecitare il lettore ad un approfondimento sul cd. "garbage collection and TRIM" dei dischi SSD[2], che aiuta a comprendere quali siano le sfide introdotte da queste "ormai non più nuove" tecnologie.
Altra considerazione attiene, invece, sempre con riferimento al tema della cd. "copia integrale/copia bit a bit/ bit stream image", all'impossibilità, attesi i nuovi "limiti" di storage raggiunti dalle aziende, di poter realizzare copie integrali di "mainserver" che hanno raggiunto capacità di storage quasi mai replicabili in tempi accettabili.
Alternativa all'acquisizione dell'intero "contenitore" è l'acquisizione del suo contenuto o meglio l'estrazione di mirate informazioni digitali, ove l'interesse degli

1 *Cass., Sez. Un., 7 settembre 2017, n. 40963.*

2 *https://www.secureforensics.com/blog/computer-forensics-on-ssds-with-trim-and-garbage-collection.*

operanti risulti circoscritto a particolari contenuti informatici.
In tale contesto si aprono però due scenari. Il primo si sostanzia in quella che possiamo considerare una soluzione "intermedia" tra l'efficacia della bit-stream image e l'acquisizione "mirata" di singole tipologie di files individuati e selezionati sul posto (che scontano le problematiche di "ricerca" sopra tratteggiate). Il riferimento è all'acquisizione di quello che nel gergo operativo viene definito "profilo/i users". Si tratta di effettuare una copia logica della cartella e relative sottocartelle "User/Utenti" di Windows o MacOS. Tale soluzione presenta alcuni vantaggi rispetto all'acquisizione mirata che possiamo riassumere in:
• una riduzione dei tempi di acquisizione rispetto alla "copia raw" del disco;
• viene solitamente ben accettata dal soggetto ispezionato che vede ridotta la permanenza degli operatori all'accesso e subisce minori disagi alla propria operatività. Invero la ricerca per parole chiave e altri elementi risulta maggiormente dispendiosa in termini di tempo. Inoltre la soluzione è accettata di buon grado in quanto si tratta di "cristallizzare" uno stato riservando poi l'esame dei singoli file in una fase successiva del controllo;
• si evita di acquisire i files del sistema operativo che generalmente in questa tipologia di controlli raramente risultano strategici;
• è un'acquisizione molto più ampia ed anche invasiva (non al pari della bit stream image) ma che tende a mitigare parte delle criticità della ricerca finalizzate all'individuazione di specifici files.
Il secondo attiene quella che viene definita sempre nel gergo "acquisizione selettiva"; pur presentando le criticità già ampiamente evidenziate, in taluni contesti continua ad essere al pari delle due precedenti ampiamente utilizzata. Si pensi a quelle situazioni in cui le ricerche vengono estese a server e NAS caratterizzati da elevate capacità di "storage" nei confronti dei quali non è sempre possibile procedere ad acquisizioni bit stream image e la soluzione "Users" non è percorribile (cartelle condivise di rete).
Passiamo ora ad una panoramica degli strumenti utilizzati per le diverse ricerche e tipologie di estrazioni, tracciando nel contempo le migliori pratiche, nell'ulteriore considerazione che la circolare non indica mai particolari software o apparecchi da utilizzare.
Per le ricerche sono da preferire gli strumenti di indicizzazione già presenti sul sistema o previsti da particolari software in utilizzo al controllato (anche a livello aziendale si presenta molto spesso l'esigenza di effettuare ricerche attraverso l'utilizzo di diverse chiavi) e laddove richiesto dal particolare contesto investigativo si potrà ricorrere anche all'utilizzo, con il consenso della parte di software in versione "portable" che non preveda l'installazione e la conseguente modifica dei dispositivi del soggetto sottoposto a controllo, vanno bene anche le soluzioni da linea di comando quali GREP, FIND, LOCATE su sistemi LINUX o FINDSTR in Windows e MDFIND in MacOS. Le soluzioni software GUI "portable" di maggior utilizzo sono: AGENT RANSACK, FILE LOCATOR, SEARCH MY FILE. Sono soluzioni alquanto intuitive e presentano il vantaggio di poter individuare i file ed anche di esportarli direttamente senza fare ricorso ad altri software ed anche di creare diversi tipi di report molto utili per quanto riguarda la redazione del verbale delle operazioni tecniche compiute. Va anche precisato che il Corpo ha fornito i militari CFDA anche di altre soluzioni che si presentano quali soluzioni "ALL IN ONE" (portable) capaci di effettuare "preview" approfondite ed efficaci, ricerche a seguito di indicizzazione ed anche l'esportazione "forense" in vari formati dei target individuati – immagini bit to bit – immagini logiche di files e cartelle. Il loro ricorso è riservato a quei contesti operativi che consiglino l'adozione di particolari attenzioni o allorquando ci si trovi in quelle situazioni che pur essendo avviate come contesto "amministrativo" di lì a poco possano sfociare in contesti "penalmente-rilevanti".
Qualora gli strumenti ALL IN ONE non siano disponibili, le soluzioni andranno ricercate come vedremo nel prosieguo attraverso l'utilizzo delle distro linux forensi.
Quanto all'acquisizione o duplicazione dei dati occorre precisare che la definizione di duplicato informatico viene fornita dall'art. 1, comma 1, lettera i-quinquies del D.Lgs. 7 marzo 2005, n. 82[3] ove viene definito come il documento informatico ottenuto mediante la memorizzazione sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario, avendo cura di preservare i cosiddetti "metadati"[4].
Il D.P.C.M. 13 novembre2014[5], stabilisce che il duplicato informatico di un documento informatico deve essere prodotto mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine. Tale procedura consente di conferire al duplicato informatico il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui lo stesso è tratto. Cosa ben diversa dal più comune e conosciuto copia/incolla che non permettere l'acquisizione dei metadati originari ed altera anche quelli presenti sul filesystem se non vengono adottate specifiche precauzioni nella lettura dei dati.
Qualsiasi modalità di acquisizione e duplicazione dei dati dovrà quindi garantire nel rispetto delle *best-practice*s internazionali, che il metodo adottato sia capace di garantire l'integrità, immodificabilità e genuinità dell'evidenza acquisita e questo nel reciproco interesse delle "parti" coinvolte.
Ciò è essenzialmente assicurato dal calcolo di un'impronta logico-matematica detta *hash*[6], non a caso la circolare a pag. 31 del Volume 2, recita testualmente: *"in ogni caso, e quale regola generale cui conformarsi anche in assenza dei militari CFDA, anche per*

3 Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale (CAD).

4 Nell'ambito degli archivi digitali i metadati sono le informazioni di cui bisogna dotare il documento informatico per poterlo correttamente formare, gestire e conservare nel tempo. Vengono anche definiti dati sui dati e descrivono il contenuto, la struttura e il contesto dei documenti e la loro gestione nel tempo. Si pensi all'importanza per gli investigatori di dati quali, la data di creazione ed ultima modifica dei documenti o dei cd. "header" di posta elettronica che forniscono informazioni spesso strategiche in ordine al loro invio, server utilizzati, contenuto del messaggio.

5 Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici.

6 Sequenza di bit di lunghezza predefinita creata attraverso l'utilizzo di una funzione matematica (hash), utile a generare una ed una sola impronta / stringa partendo da qualunque file o testo.

l'acquisizione di singoli documenti informatici, è opportuno, ove tecnicamente possibile in relazione alle competenze degli operanti, calcolare un'impronta logico-matematica detta hash. La determinazione dell'impronta (rectius valore di hash e funzione di verifica) del documento informatico attraverso gli algoritmi di hash consente, infatti, unitamente alla documentazione delle attività svolte, di ricostruire le azioni svolte sui documenti informatici di interesse". Vedremo come al di là dell'eterogeneità dei metodi e delle tecniche, tutti si soffermino in particolare su detto aspetto che potrebbe portarci ad affermare che nella digital-forensic affinché un file possa dirsi compiutamente identificato deve essere accompagnato dalla corrispondente impronta logico matematica di *hash*, la quale funge a ben rifletterci anche quale "sigillo" elettronico dell'evidenza in riferimento[7] . Tale funzione permette una volta calcolato l'*hash* di assicurare con riferimento a quel contenuto che ogni modifica a quest'ultimo comporterà di lì in avanti un diverso *hash.* Di qui il concetto di MATCH e MISMATCH laddove i file in occasione del loro controllo di integrità, immodificabilità e genuinità dovranno possedere l'identico *hash* calcolato all'atto della loro acquisizione e riportato in calce al verbale o allegato in appositi Report (MATCH) o viceversa evidenziare che sono intervenute modifiche (MISMATCH).

I duplicatori e i software che si definiscono "forensi" prevedono tutti nelle diverse modalità di acquisizione il calcolo dell'*hash* della sorgente e della destinazione e il loro "confronto" che ne assicura identicità, genuinità e di lì in avanti immodificabilità.

Di default le procedure prevedono oggi il calcolo dell'*hash* con algoritmo Md5 + Sha1 o Sha 256 per quanto attiene le acquisizioni effettuate nel corso di accessi fiscali.

Le migliori prassi a livello internazionale impongono, poi, soprattutto nel caso della duplicazione di unità di memoria, l'utilizzo di specifici dispositivi write-blocker o specifici duplicatori ovvero l'utilizzo di software di acquisizione forense capaci di garantire l'integrità e l'identicità dell'evidenza acquisita.

Per quanto concerne il Corpo lo stesso ha dotato ed istruito, da tempo, le unità CFDA sia sull'uso di duplicatori (nello specifico LOGICUBE FALCON) che di Write-Blocker – TABLEAU entrambe le soluzioni permettono una volta smontato l'hard-disk cd. "Source" di essere acquisito quale copia bit to bit sia in formato RAW DD che in formati proprietari quali E01 (Encase) ed altri, assicurando che le operazioni avvengono in modalità "Read Only" ovvero senza apportare alcuna modifica al disco sorgente[8].

Quale destinazione vengono utilizzati dischi messi a disposizione dall'unità CFDA ovvero dal contribuente stesso, atteso che qualsiasi modalità di estrazione venga adottata, a fattor comune, si prevede sempre che i dati devono essere estratti almeno in duplice copia di cui una andrà a costituire la cd. "Copia lavoro" utilizzata dai verificatori nel prosieguo dell'attività di controllo per i necessari, approfondimenti e riscontri , l'altra andrà invece, debitamente cautelata e conservata quale "Copia Garanzia" e per l'intero iter procedurale che interesserà il controllo, finanche alla successiva fase contenziosa, seppur conservata dagli operatori stessi con modalità che dovranno risultare sempre a verbale di verifica, non verrà mai utilizzata, costituendo per l'appunto, copia garanzia di quanto acquisito agli atti della verifica. È inoltre facoltà del contribuente richiederne una ulteriore terza copia. Sempre con riferimento alle bit stream image dei supporti occorre considerare che pur essendo dotati di strumenti specifici come quelli sopra indicati per svariate ragioni[9] può accadere che si debba ricorrere a soluzioni alternative. Tra

7 Ogni minima modifica del file o del testo produrrà una diversa stringa in uscita. La caratteristica fondamentale di queste funzioni è la loro difficile invertibilità: in questo modo, dato un valore di hash, non si può facilmente risalire al messaggio che l'ha generato ed inoltre è molto difficile produrre un messaggio che fornisca una stringa predeterminata.

8 Di recente per quanto concerne il mondo MacOs diffuso in specifici settori sono stati forniti software ed hardware MACQUISITION per acquisizioni fisiche e logiche su dispositivi della mela.

9 Le ragioni sono solitamente riconducibili all'assenza del personale adeguatamente formato o alla mancanza delle apparecchiature necessarie, impegnate in altre e prioritarie esigenze operative.

queste le principali risiedono nell'utilizzo di distro-live LINUX quali ad esempio (TSURUGI, DEFT, CAINE, PALADIN ed altre) che spesso risultano addirittura indispensabili laddove risulti difficoltoso l'accesso e lo smontaggio del disco "Source" (sistemi cd. Unibody, dischi con attacchi particolari ed assenza di idonei adattatori per collegare il disco al write-blocker o apparecchio duplicatore). Anche all'utilizzo di queste il personale è addestrato e presentano oltre al vantaggio testé indicato di rispettare le *best-practice*s in termini di accesso al "target" con modalità read -only, l'ulteriore e non secondario vantaggio di presentare una "suite" completa di programmi che permettono oltre all'effettuazione della bit stream image dei dispositivi collegati di effettuare numerose altre operazioni sempre nel rispetto delle *best-practice*.[10] Inoltre seguito della cd. "preview" del target sarà comunque possibile poi procedere alla individuazione dei file d'interesse attraverso programmi quali CATFISH o RECOLL capaci di effettuare indicizzazioni e ricerche. Infine la maggior parte di queste distro prevede anche una componente "Windows oriented" che permette di operare anche su sistemi Windows in modalità "Live"[11], il che permette di utilizzarle anche su sistemi Windows accesi. In merito va precisato che la maggior parte delle operazioni di cui stiamo trattando avviene su sistemi accessi ovvero con modalità LIVE in quanto all'atto dell'accesso come già ricordato le attività risultano nel loro normale orario di esercizio e quasi sempre la quasi totalità dei dispositivi risulta a quell'ora già in funzione. Qualora in tali casi risulti necessario procedere ad operazioni che prevedono lo spegnimento del dispositivo si farà ricorso a seconda della tipologia di target alle migliori pratiche consigliate sul metodo di spegnimento, evidenziando che se le stesse oggi risultano ben delineate per quanto concerne il mondo "mobile" ove dipendono molto dalla marca e modello del dispositivo o meglio dai sistemi di sicurezza insiti nello stesso, per quanto concerne PC DESKTOP e LAPTOP permangono ancora dubbi sulle scelte tra procedure standard ed altre tecniche che variamente presentano vantaggi e svantaggi nella loro applicazione.

10 Dette distro Forensics Oriented sono utilizzabili nell'attività di digital forensics in quanto, durante il loro utilizzo, garantiscono l'inalterabilità della struttura dei file o del sistema sottoposto ad analisi, non utilizzano le partizioni di swap presenti nel sistema sottoposto ad analisi; non effettuano o creano automatismi di mount delle memorie di massa all'avvio del sistema; e non vi sono automatismi di alcun tipo durante l'attività di analisi delle evidenze. Il tutto è rimesso dopo il boot alle capacità e competenze dell'operatore il quale può avvalersi, per le successive operazioni, di mount e analisi di software sia GUI (Graphical User Interface) che CLI (Command Line Interface). Il livello di eccellenza raggiunto da tali distro_linux_forensics è testimoniato dall'adozione delle stesse da parte di molti Law Enforcement nazionali ed esteri. Del resto la "suite" di programmi e funzioni di cui sono corredate ne fa dei piccoli "laboratori digital forensics" portatili, in quanto tale corredo è in grado di coprire buona parte delle esigenze di indagini digitali richieste all'operatore.

11 Il riferimento è a BENTO per quanto concerne il progetto TSURUGI; a DART per quanto concerne il progetto DEFT e a WINDOWS SIDE IR/Live di CAINE.

Va sempre ricordato che nella fase di identificazione e acquisizione delle evidenze digitali è opportuno assegnare una priorità ai dati da acquisire secondo criteri che tengano conto del loro valore investigativo e, a seguire, del grado della loro volatilità, posto che i dati potrebbero risultare indisponibili o alterati a seguito di una non immediata preservazione. Per questo facendo riferimento a quei dispositivi informatici che risultano in esercizio e che non possono essere interrotti, disconnessi dalla rete o spenti per effettuare un'acquisizione "post-mortem", i militari operanti programmeranno opportunamente le attività in maniera tale da essere portate a termine senza interruzioni, con appropriata documentazione degli esiti. A tal proposito andrà posta la massima attenzione a quei processi attivi ed eventualmente di interesse (collegamenti "cloud", collegamenti a volumi "criptati", altri processi attivi strategici all'indagine) che a seguito dello spegnimento vedrebbero pregiudicate le loro possibilità di acquisizione.[12]

Allorquando la scelta degli investigatori ricade invece sull'estrazione dei profili USERS ovvero su di un'acquisizione selettiva di files ben individuati, allora le opportunità e le possibilità si allargano. Qui gli elementi essenziali da salvaguardare ove possibile sono i medesimi previsti per le bit stream image.

Una procedura collaudata consiste qualora si debbano esportare intere cartelle nel comprimerle talché in un file compresso e quindi calcolare l'*hash* sul singolo file così ottenuto. Di seguito l'archivio può essere

12 Contrariamente a quanto avviene nei normali contesti di digital forensic ove l'acquisizione della RAM di un PC acceso, viene sempre fortemente consigliata dalle best-practice, in tali contesti pur non giungendo a quella che si definisce una "capture RAM" è sempre bene porre grande attenzione prima dello spegnimento del target che lo stesso non presenti informazioni strategiche che potrebbero andare disperse a seguito dello spegnimento.

tranquillamente spostato da un supporto all'altro mantenendo inalterati i dati (anche i metadati) all'interno del proprio archivio che andranno ogni volta scompattati[13]. Tale procedura viene spesso applicati per gli archivi di posta elettronica (pst/ost) e ciò al fine di preservare ulteriormente da accidentali modifiche i file, che all'atto della loro apertura potrebbero essere modificati.

A questo punto i file compressi accompagnati dall' *hash* possono essere masterizzati anche su supporti riscrivibili ovvero copiati su HDD di più grandi dimensioni.

Si ricorda che la circolare a seguito dell'individuazione dei file di interesse contempla anche possibilità più elementari di duplicazione del dato che tuttavia rispettano le *best-practice*[14]. Una fa riferimento alla possibilità di masterizzazione su CD/DVD/Blu-ray purchè non riscrivibili dei dati di interesse, anche senza il calcolo dell'*hash* per singolo file o cartelle compresse, e la realizzazione di tre copie dei supporti ottici, che andranno siglate dai verbalizzanti e dalla parte ed andranno a costituire una copia "garanzia" una "lavoro" ed una per la parte. La possibilità di avere tre copie confrontabili nella loro identicità e su supporti immodificabili si ritiene sufficiente a garantire quanto verrebbe garantito dall'*hash* calcolato su ogni singolo file o cartella compressa. Tuttavia tale procedura a cagione di più sempre elevati volumi che richiedono l'impegno di "storage" mediamente di centinaia di Gigabyte è stata abbandonata nel tempo a favore di software che di fatto permettono lo svolgimento di dette operazioni in pochi passaggi ed assicurano più elevati standard forensi. Il riferimento è al programma FTK IMAGER della ACCES DATA pur non consentendo nella versione IMAGER l'effettuazione di ricerche, permette al pari delle soluzioni ALL IN ONE prima accennate di accedere ad un volume ed individuati (questa volta attraverso altre soluzioni) i files/cartelle/partizioni di interesse, procedere ad una RAW COPY del supporto in vari formati forensi (DD, E01, AFF) o all'effettuazione di copie logiche in formato .AD1 di intere cartelle e sottocartelle con la possibilità anche di combinare in un'unica immagine logica più cartelle e sottocartelle appartenenti a diverse radici e device. Il suo utilizzo risulta alquanto comodo nell'acquisizione dei profili Users già prima accennati ma anche in una creazione di una "custom image" costituita da diverse cartelle e sottocartelle individuate o ritenute di interesse all'interno della rete aziendale. Il "valore aggiunto" è costituito oltre che dalle specifiche che ne fanno un vero e proprio programma "forense" nel fatto che è possibile:

- avere un calcolo del MATCH "*hash*" tra l'immagine sorgente e quella di destinazione;
- compila nel caso di immagini logiche un file .csv relativo a tutti i file contenuti nell'immagine riportandone per ciascuno i metadati e il relativo *hash* MD5;
- redige un analitico REPORT delle operazioni contenente nel rispetto delle *best-practice* data e ora di inizio e fine delle operazioni – dati identificativi e specifiche del supporto /percorso /path del sorgente e della destinazione – *hash* del sorgente e destinazione e loro MATCH/MISMATCH ma anche un apposito log indicante eventuali errori, file non copiati, errori rilevati nei settori del disco.

Quando si ha a che fare con "dati digitali" in qualsiasi contesto, vige un principio generale per cui tutte le operazioni devono essere verificabili e valutabili anche da terze parti e a posteriori attraverso la documentazione delle attività svolte che deve permettere la successiva valutazione della metodologia tecnico-scientifica e delle procedure seguite. Per questo tutte le operazioni svolte devono trovare dettagliata descrizione negli atti compilati (verbale di verifica) e nel caso di partecipazione diretta alle attività dei militari qualificati CFDA, si deve anche dare atto negli atti compilati

13 Occorrerà poi tenere a mente che all'atto dell'estrazione dei file su altro supporto le date di creazione e di ultimo accesso saranno modificate nel file estratto e saranno impostate all'istante di esecuzione dell'operazione, ma avremo sempre salvaguardato l'integrità del file contenuto nell'archivio.

14 La circolare ricorda anche la possibilità di stampare i dati ritenuti maggiormente d'interesse, avendo cura di far apporre la firma per copia conforme ai verificatori stessi e al contribuente, nonché di riportare la data della stampa. In tal modo, si ottiene una copia analogica di documento informatico, secondo le modalità e le garanzie previste dall'art.23 del citato CAD.

delle operazioni tecniche poste in essere e delle relative modalità di esecuzione, precisando quanto più possibile chi vi ha materialmente partecipato, chi per conto del contribuite ha assistito i militari, eventuali eccezioni poste e tutte le procedure tecniche adottate specificando la strumentazione e i software utilizzati con indicazione delle loro specifiche e con riferimento a quest'ultimi quando possibile, anche l'*hash* dell'eseguibile onde permettere eventualmente in caso di contestazioni la ripetizione delle medesime operazioni nelle medesime condizioni. Dal verbale dovranno rilevarsi le modalità di accesso ai dispositivi, percorsi di rete, chi e con l'assistenza di chi se ne è occupato le eventuali tecniche di ricerca adottate (parole chiave, indicazioni del direttore della verifica, indicate spontaneamente dalla parte etc.), l'elenco delle evidenze acquisite con le modalità di acquisizione /esportazione scelte e con indicazione dei supporti utilizzati ed indicazione nel verbale degli *hash* (comprensivo della funzione di calcolo utilizzata) relativi alle stesse (*hash* della bit stream image, *hash* dei file, etc.) le modalità ulteriori di assicurazione adottate a tutela dell'integrità delle stesse oltre all' *hash* (sigilli fisici utilizzati) e non ultimo ai fini della catena di custodia indicazione del luogo e responsabile della custodia degli stessi e degli eventuali passaggi di consegne. Qualora si abbia avuto l'accortezza di produrre video o foto delle operazioni svolte anche queste in formato file con il corrispondente *hash* troveranno citazione nel verbale.

Quanto all' "assicurazione" di quanto raccolto dell'importanza dell'*hash* o di altre tecniche dirette allo scopo (tre copie dei supporti non riscrivibili) già si è detto, tuttavia chi scrive ritiene che ciò venga assolto anche dalla catena di custodia. In conclusione alle attività di acquisizione/ estrazione che abbiamo appena visto, occorre conservare quanto acquisito proteggendone l'integrità da alterazioni naturali, colpose e finanche dolose. Il riferimento in tal caso non è ricondotto unicamente ai files o alle bit stream image acquisite ma anche ai supporti che ora le contengono e che vanno a costituire le copie garanzia e lavoro di cui si è già detto. Assume quindi fondamentale importanza la catena di custodia che documenta i movimenti e le interazioni che vi sono state con le evidenze digitali. Il documento che ben può essere costituito dal verbale redatto all'atto dell'accesso e dai successivi verbali di verifica che andranno a prendere in considerazione di giorno in giorno i supporti e dati raccolti deve essere sempre in grado attraverso la sua lettura storica di indicare in ogni momento chi avesse la disponibilità materiale delle evidenze raccolte.

Paradossalmente, l'ambito amministrativo-penale nel quale si confronta quotidianamente il Corpo evidenzia aspetti di complessità e difficoltà di quelli che possono rilevarsi in quelle che per distinzione definiamo attività di polizia- giudiziaria. Bene ha fatto la circolare, con la lungimiranza che viene riconosciuta anche al legislatore in questa materia, a non imporre metodi, strumenti e tecniche in un mondo dove "domani è già ieri" per l'investigatore e dove incombe il rischio che prescrizioni troppo stringenti possano essere facilmente superate dalla controparte (*antiforensic*) o risultare nel giro di breve tempo inadatte ed anacronistiche.

Se è vero che una maggior presenza di "reti" e la necessità di operare su quantità di dati enormi non rende sempre possibile il raggiungimento di quell' "optimum" rappresentato dalla bit-stream image che sempre più riveste il ruolo di "regina" (seppur con recenti temperamenti) nel processo, è altrettanto vero che la *digital-evidence* in ogni caso richieda nuove attenzioni nella sua complessiva gestione dall'individuazione finanche alla sua "presentazione" nel processo.

Di qui una rinnovata e maggiore attenzione verso la cd. "prova digitale" che ne vari contesti e contenziosi è oggi sempre più presente e spesso costituisce "l'ago della bilancia" che fa propendere per una responsabilità o assoluzione. In tale ambito risulta allora fondamentale il ricorso ad un "set" di regole condivise, capaci di assicurare le legittime prerogative e diritti (quasi sempre divergenti) in capo alle parti.

Concludo ritenendo che per quanto il tema possa apparire alquanto specialistico, una lettura effettuata dalle "parti" coinvolte, saprà fornire a ciascuna elementi di riflessione, approfondimento e confronto che non possono che riverberare "positivamente" in quel rapporto tra contribuente e investigatore oggi più che un tempo chiamato a nuove sfide in un nuovo mondo, quello "tecnologico" che ormai pervade la nostra quotidianità e vita.

Compliance: il modello organizzativo 231 e la gestione del rischio. Un esempio applicativo. Seconda parte

di Matteo Montagner

Premessa

Il Decreto Legislativo 8 giugno 2001, n. 231 (di seguito D.Lgs. n. 231/2001) ha delineato la responsabilità amministrativa degli Enti che scaturisce in corrispondenza alla commissione di un reato da parte di una persona fisica che sia riconducibile all'Ente da un rapporto funzionale.

Ne consegue che l'Ente, per evitare di essere investito di tale responsabilità amministrativa, deve aver messo in atto, prima che sia commesso l'illecito contestato, un Modello Organizzativo di gestione e controllo previsto dal D.Lgs. n. 231/2001. La responsabilità amministrativa in conseguenza di tali reati comporta per l'Ente la possibilità di vedersi irrogare pesanti sanzioni di carattere patrimoniale che incideranno anche sull'immagine e sull'attività dell'Azienda.

In conseguenza della commissione dei c.d. reati presupposto, il D.lgs. 231/01 prevede sia sanzioni pecuniarie (commisurate per quote e valore di ogni quota) che sanzioni interdittive (interdizione dell'esercizio e delle attività, divieto di contrattare con la Pubblica Amministrazione e di pubblicizzare beni e servizi, sospensione o revoca di autorizzazioni, licenze e concessioni funzionali alla commissione dell'illecito, nonché, esclusione e revoca di finanziamenti, sussidi, agevolazioni e contributi).

Il Modello 231 è uno strumento che consente alle Imprese di tutelarsi dalla responsabilità amministrativa derivante dalla commissione di comportamenti illeciti compiuti da soggetti collegati alla Società.

Il Modello Organizzativo di gestione e controllo stabilisce mediante procedure organizzative, codici di comportamento, protocolli operativi, attività di verifica, di formazione e di comunicazione un sistema di gestione preventiva del rischio che minimizzi la possibilità del verificarsi la commissione di determinati illeciti (i reati presupposto).

Il Modello Organizzativo deve essere tarato in base alle caratteristiche dell'Impresa, alle attività svolte, ai processi produttivi e alle operazioni commerciali effettuate, alla struttura organizzativa dei contesti in cui opera e dei soggetti con cui interagisce; è necessario attuare e applicare diligentemente il Modello Organizzativo nell'attività aziendale.

Importante è che il Modello Organizzativo sia costantemente verificato e tenuto sempre aggiornato in base alle modifiche della normativa di settore.

Il Modello Organizzativo di cui al D.Lgs. n. 231/2001 si articola nelle seguenti parti

principali:
• Parte Generale**:** contiene la descrizione degli aspetti e dei principi generali conoscitivi e applicativi del Modello, i principi e le procedure di controllo, l'adozione di un codice etico, l'adozione di un sistema disciplinare e sanzionatorio e l'istituzione e la definizione dei poteri di un Organismo di Vigilanza.
• Parte Speciale: individua i reati ipotizzabili e le aree di rischio, le funzioni coinvolte, le modalità di commissione dei reati, le procedure di controllo adottate finalizzate alla riduzione dei rischi.
Il Modello Organizzativo 231 deve essere appositamente approvato dall'Organo Amministrativo della Società, che deve nominare contestualmente anche l'Organismo di Vigilanza.

Un esempio applicativo di Modello Organizzativo 231
Prima di proporre un esempio di schema applicativo è necessario premettere che è impossibile delineare un Modello Organizzativo che possa essere applicato a tutte le Imprese in modo generalizzato e diretto a prescindere dal settore merceologico, dalla soglia dimensionale e dall'organizzazione aziendale.
Il settore merceologico e la consistenza dimensionale dell'Impresa sono tra i fattori che possono determinare un maggiore fattore di rischio rispetto ad altre situazioni, in quanto possono aumentare la possibilità di commettere i reati contemplati dal D.lgs. n. 231/2001. Pertanto, un Modello Organizzativo 231 non può essere direttamente generalizzato anche se l'attività svolta da Società diverse è molto simile, in quanto ogni Azienda ha caratteristiche organizzative specifiche che devono essere attentamente valutate e recepite nel Modello.
Infatti, solo un'attenta analisi di dettaglio può stabilire i rischi di illeciti e le reali ricadute di efficacia in termini di tutela e prevenzione del Modello Organizzativo che si intende adottare.
L'aspetto dimensionale e della conseguente diversificazione della struttura organizzativa invece è una problematica che può interessare in generale tutte le Imprese indipendentemente dal settore merceologico in cui operano, in quanto può influire sull'aspetto della complessità del Modello Organizzativo da adottare.
Pertanto, si deve porre particolare attenzione agli aspetti relativi all'organizzazione aziendale, alle deleghe di funzioni e alle procedure decisionali e operative in particolare in situazioni come quelle riguardanti le PMI nelle quali tali funzioni fanno capo spesso ad un numero limitato di soggetti.
È opportuno, pertanto, valutare attentamente il ruolo effettivo che un modello deve rivestire in relazione alle esigenze, alla struttura e alle risorse di una PMI.

In una piccola impresa è essenziale la struttura interna gerarchica e funzionale piuttosto che i parametri quantitativi. Resta comunque confermato anche per le PMI, al pari delle realtà più grandi, l'esigenza di dotarsi di un Modello Organizzativo di gestione e controllo per cautelarsi rispetto alla possibilità di essere implicate in procedimenti giudiziari a causa dei reati previsti dal D.Lgs. n. 231/2001. Con l'attuazione di un Modello Organizzativo l'Impresa può minimizzare le gravi conseguenze sanzionatorie in cui può incorrere.
Fatte queste debite premesse l'esempio di applicazione di un Modello Organizzativo che si andrà ad illustrare di seguito in modo sintetico ha lo scopo di rappresentare, a titolo esemplificativo, le indicazioni delineate nel D.Lgs. n. 231/2001 con particolare attenzione alle PMI. In merito ai Modelli adottabili è di importante rilevanza il documento di indirizzo emanato da Confindustria; tale documento, a seguito delle modifiche normative intervenute, è stato più volte adeguato e da ultimo Confindustria ha diffuso un'edizione aggiornata delle "*Linee Guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ai sensi del Decreto Legislativo 8 giugno 2001, n. 231*" datata giugno 2021.

Parte Generale del Modello Organizzativo di gestione e controllo
La Parte Generale del Modello contiene come premessa una descrizione del quadro normativo di riferimento, una presentazione sintetica dell'attività esercitata e degli aspetti strutturali dell'impresa, nonché delle modalità di attuazione e di funzionamento del Modello Organizzativo e dell'Organismo di Vigilanza.

La Parte Generale, che può avere una premessa che riporti Glossario e Definizioni dei termini utilizzati, si può articolare secondo i seguenti punti:

• Quadro normativo di riferimento
In questo punto è riportata una sintesi del quadro normativo di riferimento di cui al Decreto Legislativo 8 giugno 2001, n. 231 e successive integrazioni e modificazioni e dei principi ai quali deve uniformarsi il Modello.

• Presentazione della Società, dell'attività aziendale e dell'Assetto Organizzativo (sistema di Governance e dell'Organigramma Aziendale)
Devono essere descritti gli strumenti e i sistemi di Governance e di funzionamento dell'impresa, nonché l'assetto organizzativo, le responsabilità attribuite alle diverse funzioni ed unità organizzative che afferiscono al sistema gestionale dell'impresa, la ripartizione dei poteri e il sistema delle deleghe e quindi l'organigramma ricavato dall'ordinamento e dalla documentazione costitutiva della società.

• Attività di Comunicazione, Formazione e Informazione del Modello
Questo punto prevede le indicazioni per quanto riguarda le attività di formazione, comunicazione finalizzate alla prevenzione dei reati, nonché il flusso informativo verso l'Organismo di Vigilanza da parte del personale dell'organizzazione aziendale e viceversa.
In proposito è importante istituire un sistema di segnalazione "Whistleblowing" che consenta alle figure apicali, ai sottoposti e a terzi di presentare, nel rispetto della riservatezza dell'identità, segnalazioni di condotte anche solo potenzialmente illecite, rilevanti sia ai sensi del D.Lgs. n. 231/2001 che ai sensi di altre normative applicabili.

• Organismo di Vigilanza (OdV)
Contiene la descrizione della composizione e del funzionamento dell'Organismo di Vigilanza, nonché e prerogative, dei poteri e dei compiti che esercita.
L'adozione e il funzionamento dell'Organismo di Vigilanza è presupposto necessario perché il Modello Organizzativo di gestione e controllo possa escludere effettivamente la responsabilità amministrativa dell'impresa in caso di reato. Lo stesso deve essere costituito da uno o più soggetti che siano in possesso di requisiti specifici in termini di competenza e professionalità. L'Organi-

smo di Vigilanza è deputato al controllo ed al monitoraggio in merito alla corretta applicazione del Modello Organizzativo.
All'Organismo di Vigilanza devono essere assicurati poteri autonomi di iniziativa e di controllo in modo tale che possa efficacemente senza vincoli:
• provvedere alla verifica del rispetto dei principi del Codice Etico
• vigilare sull'osservanza e funzionamento delle prescrizioni e delle procedure previste dal Modello Organizzativo
• curare l'aggiornamento periodico del Modello.
Pertanto, l'Organismo di Vigilanza deve essere caratterizzato da:
• autonomia e indipendenza
• professionalità
• continuità di azione.
Al Modello Organizzativo va allegato il Regolamento dell'Organismo di Vigilanza come parte integrante del Modello stesso.
Per quanto riguarda l'Organismo di Vigilanza la normativa per le piccole Imprese consente una deroga rispetto a quanto previsto in via generale in considerazione del fatto che tali realtà imprenditoriali, in base alle dimensioni e alla semplicità della struttura organizzativa, non dispongono di una funzione o di personale da assegnare all'attività di monitoraggio del sistema di controllo interno. Per tali piccole Imprese l'istituzione di una posizione specifica risulterebbe oltretutto un onere economicamente non sostenibile. In riferimento a questa problematica l'art.6 del D.Lgs. n. 231/2001 consente all'organo dirigente di svolgere direttamente i compiti indicati. Tuttavia in questi casi è opportuno, se possibile, affidarsi per le verifiche periodiche sul rispetto e l'efficacia del Modello a professionisti esperti, posto che la responsabilità di vigilanza prevista per Legge resta in capo all'organo interno.

• Codice Etico
Il Codice Etico o di comportamento esprime i principi di deontologia aziendale secondo i quali l'Impresa indirizza la propria attività. Essi si fondano in particolar modo sulla trasparenza gestionale e sulla correttezza etica a cui la Società dovrà adeguare la propria attività. Il Codice Etico è strutturato con riferimento ad un insieme di principi e di linee guida recepite da quanto previsto dal D.Lgs. n. 231/2001. Tali principi, sulla base dei quali dovrà essere condotta l'attività dell'Impresa, prevedono sostanzialmente il rispetto delle norme vigenti, il monitoraggio di ogni attività effettuata e riguardano il comportamento non solo dei propri dipendenti, ma anche di coloro con i quali l'Ente entra in contatto nell'ambito dell'attività commerciale.
La predisposizione e l'adozione di un Codice Etico non dovrebbe destare particolari difficoltà di adattamento per le PMI.

• Sistema Disciplinare
In questa sezione sono comprese le procedure sanzionatorie da assumere nel caso siano commessi illeciti, violate regole e procedure previste dal Modello Organizzativo. E' importante che il Sistema Disciplinare vieti espressamente di compiere atti di ritorsione o discriminatori nei confronti di coloro che effettuino segnalazioni in buona fede come previsto nella procedura "Whistleblowing".

• Approvazione, aggiornamento e attuazione del Modello
La competenza per l'approvazione del Modello Organizzativo di gestione e controllo è, ai sensi dell'art. 6, comma I, lett. a) del D.Lgs. n. 231/2001, in capo all'Amministratore; è pertanto rimessa a quest'ultimo la responsabilità di approvare ed adottare, mediante apposita determina, il Modello Organizzativo di gestione e controllo.
Le successive modifiche e integrazioni dei principi di riferimento del Modello, finalizzate a consentire la continua rispondenza dello stesso alle eventuali successive prescrizioni del Decreto, sono anch'esse rimesse alla competenza dell'Amministratore.
L'Amministratore deve altresì garantire l'attuazione del Modello Organizzativo assumendo i provvedimenti necessari per consentirne l'implementazione avvalendosi del supporto dell'Organismo di Vigilanza.
L'Amministratore anche dopo l'adozione del Modello Organizzativo deve comunque garantire di provvedere agli aggiornamenti o adeguamenti del Modello che si rendessero necessari in base ad esigenze organizzative o a modifiche normative anche attraverso l'intervento dell'Organismo di Vigilanza.

Parte Speciale del Modello Organizzativo – Protocolli
La seconda Parte Speciale contiene l'individuazione delle aree di rischio di reato, le fattispecie di reato che sono suscettibili di essere commesse, le modalità di commissione, le funzioni coinvolte, il sistema di controllo interno e di gestione dei rischi per la prevenzione dei reati.

La Parte Speciale del Modello Organizzativo di gestione e controllo si può articolare secondo i seguenti punti:

• Fattispecie di reato applicabili
In questo punto sono elencati i reati previsti dal D.Lgs. n. 231/2001 suscettibili di essere commessi dai soggetti in posizione apicale, dai sottoposti o dai collaboratori interni ed esterni (collaboratori, consulenti, fornitori e partner).
Le tipologie di reato previste dal D.Lgs. n. 231/2001 sono molto ampie e coprono potenzialmente tutte le attività aziendali. Anche a seguito di successivi interventi legislativi le fattispecie di reato sono via via aumentate. Da ultimo sono state ampliate dal D.Lgs. n. 184/2021. Tale normativa introduce con l'art. 25-octies.1 nel D.Lgs. 231/2001 dei reati relativi a pagamenti diversi dai contanti.
Si riportano di seguito come esempio i reati-presupposto che più comunemente sono potenzialmente rapportabili alle attività della generalità delle Imprese:
- reati contro la Pubblica Amministrazione (art. 24 D.Lgs. n. 231/2001)
- delitti informatici e trattamento illecito di dati (art. 24-bis D.Lgs. n. 231/2001)
- reati societari (art. 25-ter D.Lgs. 231/2001)
- reati in materia di tutela della salute e sicurezza sul lavoro (art. 25-septies D.Lgs. n. 231/2001)
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25 octies D.Lgs. n. 231/2001)
- reati ambientali (art. 25-undecies D.Lgs. n. 231/2001)
- impiego di cittadini di paesi-terzi il cui soggiorno è irregolare (art. 25-duodecies D.Lgs. n. 231/2001)
- reati Tributari (art. 25- quinquiesdecies D.Lgs. n. 231/2001).

• Mappatura delle aree di rischio
In questo punto vengono descritte ed individuate le aree aziendali funzionali e operative nell'ambito delle quali è ipotizzabile che possano verificarsi condotte illecite. Tale mappatura è indirizzata alla realizzazione di un sistema di gestione e controllo finalizzata a minimizzare il rischio della commissione di reati. La metodologia

utilizzata deve evidenziare le "aree sensibili" o "a rischio" cioè quei processi e quelle attività aziendali che rientrano nelle condizioni per le quali potrebbe determinarsi in via presuntiva la possibilità che si possano commettere degli illeciti espressamente previsti dal D.Lgs. n. 231/2001. Un fattore importante della mappatura da evidenziare per le aree a rischio è il cosiddetto "*Gap analysis"* (o analisi comparativa) che consiste in un'attenta operazione di valutazione che, in base alle carenze rilevate nella gestione dei controlli e nelle procedure utilizzate dalla Società, ha lo scopo di individuare un idoneo sistema di prevenzione. Tale sistema deve essere calibrato in funzione di prevenire potenzialmente la commissione di reati o comunque di ridurre i rischi dei reati individuati in ciascuna area.

• Procedure e protocolli per evitare la commissione di reati

In questo punto sono analizzati e descritti i protocolli adottati per prevenire la commissione di illeciti. La Società elabora e adotta procedure, già in essere o da integrare, funzionali a prevenire i rischi di illeciti nell'ambito delle aree di rischio individuate.

In base alle categorie di reato a rischio i contenuti sono articolati in specifici capitoli in cui sono riportati i reati ipotizzabili, le funzioni coinvolte, le modalità di commissione del reato, le procedure di controllo adottate per ridurre i rischi.

Le informazioni possono essere rappresentate in tabelle che riportino per i rischi di reato indicati dal D.Lgs. n. 231/2001 le seguenti informazioni:

a) descrizione delle fattispecie di reato

b) modalità e forme attraverso le quali tali reati potrebbero effettivamente verificarsi

c) analisi delle aree e processi organizzativi sensibili

d) analisi delle funzioni/posizioni organizzative sensibili

e) l'indicazione dei protocolli di controllo per la prevenzione del rischio di reato (dettagliati in protocolli già in essere al momento della pubblicazione del Modello e protocolli da integrare).

In aggiunta ai protocolli definiti per il Modello Organizzativo di gestione e controllo di cui al D.Lgs. n. 231/2001 sono da considerare anche le procedure relative alle attività aziendali. Tali documenti devono costituire parte integrante del Modello Organizzativo di gestione e controllo e possono essere presenti come allegati o appendici.

Tali procedure ad esempio possono riguardare: acquisto beni e servizi, reclutamento e gestione delle risorse umane, attività finanziaria, sponsorizzazioni, gestione rete informatica, procedura deleghe di funzioni, finanziamenti pubblici, ecc.

Il regolamento per il corretto utilizzo dei Sistemi Informativi aziendali: inquadramento generale e alcuni esempi pratici

di Giulia Bontempini e Stefano-Francesco Zuliani

Il regolamento per il corretto utilizzo dei Sistemi Informativi Aziendali (SIA) è una delle misure di sicurezza più importanti per la protezione dei dati aziendali. Se ben redatto, da esso discendono quasi tutte le altre misure di sicurezza, con lo scopo primario di mantenere la business continuity aziendale attraverso la riduzione del rischio di compromissione del patrimonio informativo, anche al fine di evitare sanzioni o profili di responsabilità penale.

Il quadro normativo

Nel redigere un Regolamento SIA bisogna misurarsi con la normativa cogente, ovvero GDPR, Codice della Privacy e principali provvedimenti del Garante[1] [2] [3] [4] [5] o di altri organismi europei[6] [7] [8], senza tralasciare il Job Act[9] e i c.d. "Reati 231"[10]. Tali fattispecie di reato sono più diffuse di quan-

1 GPDP Linee guida sul trattamento di dati personali dei lavoratori privati - 23 novembre 2006 [1364939] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1364939;

2 GPDP Lavoro: le linee guida del Garante per posta elettronica e internet [1387522] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1387522;

3 GPDP Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499;

4 Videosorveglianza https://www.garanteprivacy.it/temi/videosorveglianza;

5 GPDP Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9126951;

6 Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica di violazione dei dati https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en;

7 Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 https://ec.europa.eu/newsroom/article29/items/612052/en;

8 I provvedimenti e gli interventi del Garante in tema di Data Breach https://www.garanteprivacy.it/home/ricerca/-/search/tipologia/Data%20breach;

9 Art. 23 D. Lgs.151/2015 (c.d.Jobs Act) "Modifiche all'art.4 delle legge 300/70" Statuto dei Lavoratori;

10 D.lgs. 231/2001 Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300;

to si creda: tra i tanti[11], un caso classico è quello dell'ex impiegato commerciale che detiene ancora le vecchie credenziali di accesso al sistema informatico, utilizzando le quali carpisce informazioni sui clienti del suo precedente datore di lavoro[12]. Un altro esempio è rappresentato dall'Amministratore di Sistema che utilizza le password di accesso alle caselle email dei dipendenti al fine di controllarne l'attività[13]. Infine, il caso più diffuso rimane quello dell'installazione di software privo di licenza con lo scopo di evitarne i costi di acquisto[14] [15]. L'accesso ad un sistema informatico con le credenziali di un altro utente potrebbe inoltre configurare il reato di sostituzione di persona (494 c.p.) o frode informatica (640 ter c.p.), mentre la cancellazione di email potrebbe integrare altri reati legati alla violazione della corrispondenza[16] [17]. Ancora, un utilizzo improprio di social e strumenti di comunicazione potrebbe configurare il reato di diffamazione (595 c.p.) o, anche involontariamente, una violazione degli artt. 98 e 99 del Codice della Proprietà Industriale (norme relative alle informazioni coperte da segreto) o degli obblighi di fedeltà di cui all'art. 2105 c.c. ("*il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio*"). In taluni casi, vanno poi considerate le normative particolari di settore, i codici deontologici, ad esempio per la categoria degli Avvocati e dei Giornalisti, nonché l'adesione a standard di certificazione (ad esempio quelli della famiglia ISO/IEC 27000 - Sistemi di Gestione per la Sicurezza delle Informazioni).

Il Regolamento SIA risponde anche agli obblighi inerenti alla formazione e all'informazione dei collaboratori sanciti dal GDPR[18] [19] [20] e dal Jobs Act. La contravvenzione alle regole in esso contenute da parte di un lavoratore configura una violazione degli obblighi di diligenza, di osservanza e di fedeltà e "*può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione*"[21] a carico del datore di lavoro, oltre al risarcimento del danno e al profilo di responsabilità penale.

I criteri di fondo

Nel redigere un Regolamento per i Sistemi Informativi Aziendali (Regolamento SIA) si cade spesso in alcuni gravi errori.

Purtroppo, anche per motivi culturali, l'attenzione che di prassi il top management rivolge a questa tematica è molto bassa. La perdita della riservatezza, integrità e disponibilità (RID) delle informazioni è generalmente ancora estranea all'esperienza diretta personale e, conseguentemente, per convincimento diffuso, è considerata o trattata come un rischio remoto.

Il Regolamento SIA viene inoltre spesso erroneamente considerato come un "regolamento IT" o comunque afferente ai soli sistemi informatici. Nulla di più sbagliato. Si tratta invero di un regolamento inerente ai sistemi informativi in generale, intesi come tutti quei sistemi aziendali che contengono informazioni, su qualsiasi supporto e, paradossalmente, anche sotto forma di capitale umano. Conseguentemente, impattando sui rischi aziendali e sulle politiche di governance in generale, non può essere considerato di pertinenza delle figure tecniche ma deve essere approvato dai vertici. Deve valere inoltre per tutti gli utenti che accedono a sistemi informativi, non solo pertanto ai dipendenti, ma anche ai collaboratori e talvolta ai fornitori.

In altri casi, il Regolamento SIA viene trattato come una "*scartoffia privacy*" da redigersi in quanto suggerito dal consulente "di turno", mal digerito a livello aziendale e il più delle volte redatto senza una conoscenza approfondita dell'azienda o, ancor peggio, acquistato già pronto online. Impattando sulla governance, il Regolamento SIA deve vestire l'azienda come un abito sartoriale, cucito su misura sulla base di processi, prassi e necessità aziendali. Talvolta si leggono regolamenti degni della NASA applicati a piccole medie aziende nei quali i livelli di sicurezza in esso descritti sono non applicabili, troppo costosi, sconosciuti o bloccanti per il lavoro quotidiano. La cattiva prassi di "vietare tutto", magari in contrasto con pratiche quotidiane adottate dalla stessa dirigenza va (forse) a tutelare unicamente l'autore o l'approvatore interno del documento che in caso di data breach potrà

11 Art. 491 bis c.p. Falsità in un documento informatico; art. 615 quinquies c.p. diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico; art. 617 quater c.p. intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; art. 617 quinquies installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche; art. 617-quinquies c.p. installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche; art. 635 bis c.p. danneggiamento di informazioni, dati e programmi informatici; art. 635 ter c.p. danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; art. 635 quater c.p. danneggiamento di sistemi informatici o telematici; art. 635 quinquies c.p. danneggiamento di sistemi informatici o telematici di pubblica utilità; art. 640 quinquies c.p. frode informatica del certificatore di firma elettronica; art. 1, comma 11, D.L. 21 settembre 2019, n. 105 Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica;

12 Art. 615 ter c.p. accesso abusivo ad un sistema informatico o telematico;

13 Art. 615 quater c.p. detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;

14 Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009];

15 Art. 171-bis l. 633/41.Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità;

16 616 c.p. Violazione, sottrazione e soppressione di corrispondenza;

17 617 sexies c.p. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche;

18 GDPR C.81 Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento. L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento (..);

19 GDPR Art. 29 Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento (C81) Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri;

20 GDPR Art. 32.4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri;

21 Art. 2106 c.c;

scaricare eventuali responsabilità verso i soggetti colpevoli di inosservanza, ma mai l'azienda nel suo complesso che si trova ad avere commissionato la redazione di un documento disapplicato sistematicamente e talvolta esposto nella bacheca aziendale unicamente per finalità estetiche. In funzione della tipologia di dipendenti, del grado di sensibilità al tema e della loro alfabetizzazione informatica, talvolta al posto di tanti complessi manuali, formalmente incontestabili ma ignorati da tutti è preferibile dettare poche semplici regole pianificando contestualmente un loro lento ma costante inasprimento. La via formale poi per accertarsi della corretta applicazione del Regolamento SIA risiede nella formazione e nelle attività di Audit periodiche, volte a verificarne la corretta comprensione ed applicazione ad ogni livello, andando anche a sanzionare in modo rigoroso il suo mancato rispetto. Una via informale e meno strutturata è quella di inserire nel testo degli "*easter egg*" e aspettare che qualcuno li segnali agli uffici competenti.
I regolamenti più strutturati e le misure di sicurezza più avanzate non sono in grado di resistere all'anello debole della catena: l'uomo. L'esperienza[22] e gli studi concordano sul fatto che semplici operazioni di ingegneria sociale possono portare gli attaccanti alla violazione di sistemi anche complessi: talvolta basta una telefonata di un finto addetto dei sistemi informativi o una email di phishing particolarmente ben strutturata. Bisogna sganciarsi dal formalismo della mera responsabilità burocratica ed evitare di semplificare la discussione imputando al solo fattore umano ogni responsabilità. "*L'opinione generale è che la maggior parte degli utenti sia negligente e demotivata quando si tratta di sistema sicurezza. (..) Una analisi più approfondita, tuttavia, ha rivelato che tale comportamento è spesso causato dal modo in cui sono implementati i meccanismi di sicurezza e la mancanza di conoscenza degli utenti.*"[23]
Considerato quindi che questi problemi sono noti e statisticamente diffusi, scaricare formalmente ogni colpa sul c.d. "*utonto*" significa non tenere in debito conto la sostanza di un rischio strutturale. Chi redige i Regolamenti SIA e le conseguenti linee guida per l'implementazione delle misure di sicurezza dei sistemi informativi aziendali deve considerare il fattore umano, non solo impedendo che possano essere create password tipo "1 2 3 4 5" ma mettendo al riparo i sistemi dagli attacchi di ingegneria sociale attraverso l'introduzione nei sistemi più critici di ulteriori livelli di sicurezza.
Senza la pretesa di poter compiere un'analisi esaustiva del tema, formuliamo di seguito alcuni suggerimenti riguardo alcuni temi ricorrenti.

Dalla password alla passphrase

Una delle principali regole da definirsi nel Regolamento SIA è la policy aziendale in tema di credenziali di autenticazione.
La più antica password che si conosca è la parola ebraica "**שבולת**" (shibboleth o scibbolet /ʃiˈbɔlɛt/): per la sua complessità fonologica è praticamente impronunciabile correttamente da un non madrelingua ebraico e pertanto come da narrazione biblica[24] assunse la funzione di segno di riconoscimento o parola d'ordine. Per estensione, ancora oggi il termine *shibbòleth* in linguistica indica una parola o espressione che, per la sua complessità fonologica è molto difficile da pronunciare per chi parla un'altra lingua o un altro dialetto. Nei secoli a venire le parole d'ordine furono sempre usate in ambito militare, ma è solo negli anni '60 e con l'avvento dell'informatica che vengono create le prime password propriamente dette. La prima è relativa ad un sistema del 1960 dell'IBM utilizzato per creare e mantenere prenotazioni di viaggi denominato Semi-Automatic Business Research Environment (SABRE). Di tale sistema purtroppo oggi non è rimasto nulla ed effettivamente non è provato che fosse dotato di credenziali di autenticazione, pertanto generalmente si attribuisce l'introduzione delle password al prof. Fernando Corbato del Massachusetts Institute of Technologyil quale nel 1961 dovette risolvere il problema di assegnare un tempo di elaborazione massimo prestabilito a numerosi utenti, ognuno con un set di dati personali da elaborare che accedevano ad computer centrale denominato "CTSS" tramite terminali condivisi. Le password erano però salvate sul server in chiaro, così che lo studente di dottorato Allan Scherr riuscì a carpirle ottenendo più tempo macchina per le sue elaborazioni. L'invenzione stessa della password è collegata conseguentemente all'importante insegnamento per cui non devono mai essere salvate in chiaro.
Oltre a ciò le password devono avere una loro complessità.
Correva l'anno 1987 quando Mel Brooks definì "*1 2 3 4 5*" come "*la combinazione che un idiota userebbe per la sua valigia*"[25], e sono numerosi gli esempi della filmografia americana che già dagli anni '80 ci insegnano di non utilizzare come password nomi facilmente intuibili come quello dei nostri partner, animali domestici o dei figli[26]. Ciò nonostante dopo decenni di alfabetizzazione informatica rimangono fra le password più diffuse al mondo[27]. È altrettanto sconsigliabile aggirare l'obbligo di inserire quale password un numero postponendo semplicemente un "1"[28] o un anno. Secondo una recente analisi[29] basata su dati forniti dal britannico National Cyber Security Centre condotta da Dojo, un'azienda che si occupa della gestione di sistemi di pagamento tramite carta, la maggior parte di password violate sono nomi di animali domestici o soprannomi vezzeggiativi, mentre i nomi propri sono classificati come la seconda categoria di password più comunemente violata. E' buona prassi infatti che la password non sia prevedibile. Se "juventus"

22 *15 Examples of Social Engineering: Real-World Attacks https://www.tessian.com/blog/examples-of-social-engineering-attacks/;*

23 *Users are not the enemy - Anne Adams & Martina Angela Sasse Department of Computer Science University College London (1999) https://discovery.ucl.ac.uk/id/eprint/20247/2/CACM%20FINAL.pdf;*

24 *Libro dei Giudici, 12,5-6 [5] I Galaaditi intercettarono agli Efraimiti ai guadi del Giordano; quando uno dei fuggiaschi di Efraim diceva: "Lasciatemi passare", gli uomini di Gàlaad gli chiedevano: "Sei un Efraimita?". Se quegli rispondeva: "No", [6] i Galaaditi gli dicevano: "Ebbene, dì Scibbolet", e quegli diceva Sibbolet, non sapendo pronunciare bene. Allora lo afferravano e lo uccidevano presso i guadi del Giordano. In quella occasione perirono quarantaduemila uomini di Efraim;*

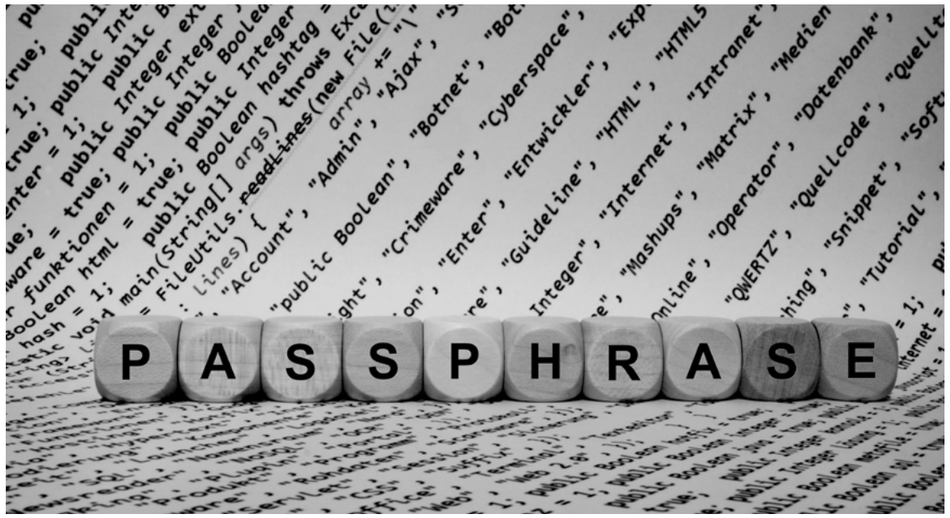
25 *Dal film "Balle spaziali" (1987) di Mel Brooks https://www.imdb.com/title/tt0094012/;*

26 *Dal film "Wargames - Giochi di guerra" di John Badham https://www.imdb.com/title/tt0086567/ David: «Come si chiamava?» Jennifer: «Mio padre?» David: «No, no. Il figlio di Falken» Jennifer: «Ah. Joshua» David: «Non può essere così semplice...» [inserisce la backdoor password "joshua"];*

27 *Secondo uno studio di NordPass https://nordpass.com/it/most-common-passwords-list/;*

28 *Dal film "Una notte da leoni 2" di Todd Phillips https://www.imdb.com/title/tt1411697/ Phil: «Your password is baloney1?» Mr. Chow: «Well, used to be just baloney, but now they make you add number»;*

29 *Top most hacked passwords & how to make yours more secure https://dojo.tech/blog/worlds-most-hacked-passwords/;*



è una delle password italiane più diffuse, è comunque altrettanto diffusa la cattiva prassi di utilizzare frasi celebri o password contenute in romanzi o film famosi.[30] [31] Altrettanto singolare il caso della password "*Hellas1903*", dal nome e dall'anno di fondazione della squadra di calcio "Hellas Verona": ha più di 8 caratteri, maiuscole e numeri e apparentemente è una password sicura, ma da una analisi compiuta dagli autori del presente su un database utenti con password in chiaro (SIC!) è risultata fra le più usate nella provincia di Verona, dove chiaramente i tifosi *gialloblù* sono numerosi.

Un'altra buona prassi è quella di utilizzare password differenti per servizi differenti. Il motivo è che i data breach, così come i cigni neri, capitano. Negli anni sono stati violati colossi quali LinkedIn, Adobe, Facebook, e una miriade di siti web minori. Chi utilizzava coppie di e-mail/password anche per altri servizi potrebbe aver avuto violazioni ancora più gravi. Fortunatamente esistono servizi online[32] che "collezionano" gli indirizzi e-mail dei profili oggetto di data breach: si può pertanto verificare se si è stati oggetto di violazione.

A livello normativo, nell'abolito Allegato B del Codice della Privacy si sanciva che "*La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.*"[33] Oggi questo disciplinare tecnico è stato abolito in quanto in contrasto col principio di accountability sancito dal GDPR, ma per la basicità delle sue indicazioni può essere ancora considerato una utile baseline per ogni ragionamento in materia di sicurezza.

Oggi il consiglio più diffuso è quello di usare password complesse, come per primo proposto da un documento del 2003 del National Institute of Standards and Technology (NIST)[34] nel quale si suggeriva di creare password con "*lower case letters, upper case letters, and non-alphabetic symbols (e.g.:"~!@#$%^&*()_-+={}[]|\:;'<,>.?/1234567890*". Per l'autorevolezza della pubblicazione questa regola venne presa come riferimento da generazioni di esperti di sicurezza informatica e di Data Protection Officer, compreso il nostro Garante nel suo vademecum sulle password[35] realizzato nel quadro delle attività di educazione digitale di base.

Il problema di avere molte password complesse e di doverle cambiare spesso è che sono fisicamente impossibile da ricordare, portando inevitabilmente gli utenti a doverle salvarle nel browser o su un supporto alternativo, tipicamente un foglietto sotto il tappetino del mouse, un appunto in agenda o un classico Post-It sul monitor. Questa pratica, da sempre deprecata, è ancora molto diffusa, come dimostrato dal recente episodio di un post su Twitter pubblicato da un membro del Congresso degli Stati Uniti (membro inoltre del Comitato per i servizi armati e di una sottocommissione di sicurezza informatica) contenente la foto del suo monitor con tanto di Post-It con la sua password. *Ça va sans dire* il post è diventato immediatamente virale[36].

Un altro aspetto critico su cui soffermarci è l'individuazione del luogo dove salvare le numerose credenziali di accesso. Oggi un impiegato medio detiene numerose password: posta elettronica, profili social aziendali, portali aziendali online, sistemi di reportistica, etc. In assenza di un sistema centralizzato di autenticazione, che appartiene a realtà più strutturate, l'utente medio tenderà a salvare le credenziali nel browser del PC di lavoro, tipicamente su Google Crome. Queste credenziali saranno poi salvate sui server di Google e accessibili da qualunque dispositivo dell'utente, talvolta anche personale, rendendo così agevole il lavoro dell'utente anche in mobilità. Queste credenziali saranno pertanto tanto sicure quanto sarà sicuro il profilo Google dell'utente, sul quale l'Amministratore di Sistema aziendale difficilmente avrà controllo.

Non è detto però che una password complessa sia anche sicura. Recentemente William Burr, l'autore del succitato documento del 2003 del NIST, ha ammesso[37] [38] non solo di non esser stato all'epoca né un esperto di sicurezza né un esperto di password in generale, ma che la difficoltà di memorizzare password redatte secondo le regole da lui all'epoca ipotizzate le rende intrinsecamente insicure. Il suggeritore automatico di Google Chrome suggerisce password di 15 caratteri del calibro di "*HW64Ze.ag6NòDhq*", ma come dimostrano vari studi[39] e le più recenti linee guida[40] una "*passphrase*" formata da quattro distinte parole di dizionario separate da un carattere speciale a scelta[41] è enormemente più facile da ricordare e molto più difficile da hackerare con un attacco informatico.

In molti casi poi la password, per quanto

30 *Speak Friend and Enter – Do people actually use movie passwords? https://kobikobi.wordpress.com/2018/03/03/speak-friend-and-enter-do-people-actually-use-movie-passwords/;*

31 *12 famous passwords used through the ages https://www.idginsiderpro.com/article/3335121/12-famous-passwords-used-through-the-ages.html;*

32 *https://haveibeenpwned.com/;*

33 *D. lgs. 196/2003 – Allegato B. Disciplinare tecnico in materia di misure minime di sicurezza (abolito dal d.lgs 101/2018);*

34 *Electronic Authentication Guideline NIST SP 800-63 Version 1.0.1 https://csrc.nist.gov/publications/detail/sp/800-63/ver-10/archive/2004-06-30;*

35 *GPDP Suggerimenti per creare e gestire password a prova di privacy [Doc-Web 4248578] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9709765;*

36 *While ranting like a lunatic and claiming to be a victim because his wife was handed a piece of paper, Mo Brooks accidentally tweeted his Gmail password and pin numbers https://twitter.com/Josh_Moon/status/1401678401946243073?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1401678401946243073%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.kaspersky.it%2Fblog%2Fsecurity-2021-year-in-memes%2F26257%2F;*

37 *The Wall Street Journal 07/08/2017 – "The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!" https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118;*

38 *The Guy Who Invented Those Annoying Password Rules Now Regrets Wasting Your Time https://gizmodo.com/the-guy-who-invented-those-annoying-password-rules-now-1797643987;*

39 *Are Your Passwords in the Green? https://www.hivesystems.io/blog/are-your-passwords-in-the-green;*

40 *Oregon FBI Tech Tuesday: Building a Digital Defense with Passwords https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-with-passwords;*

41 *XKCD - Password Strength https://xkcd.com/936/;*

complessa, non è una misura di sicurezza sufficiente, in quanto può essere carpita. Per i sistemi più critici è necessario pertanto aggiungere altri livelli di sicurezza mediante l'autenticazione a più fattori, affiancando così a "*qualcosa che si conosce*" (la password) anche "*qualcosa che si possiede*" (es: SPID, firma digitale, le vecchie chiavette della banca, l'SMS di conferma sul cellulare, etc.) o "*qualcosa che si è*" (es: identificazione biometrica con impronta o iride). Anche in questi casi però la sicurezza non è mai assoluta: sono infatti in aumento le c.d. "*SIM swap fraud*", nelle quali la scheda telefonica della vittima viene duplicata rivolgendosi, con un documento falso e una falsa denuncia di smarrimento, direttamente a un negozio di telefonia mettendo l'attaccante nelle condizioni di intercettare gli SMS della banca. La crescente potenza delle fotocamere digitali, unita all'abitudine di condividere sui social ogni momento della nostra vita sta inoltre compromettendo la riservatezza delle nostre impronte digitali che oramai possono essere carpite anche da un semplice post su Facebook.[42] Anche le firme digitali vanno conservate con diligenza: è addirittura di narrazione biblica la consegna da parte del re Assuero del suo sigillo regale all'infedele consigliere Aman che lo usò per redigere ordini per suoi scopi personali.

Esempi di esigenze contrapposte

Il problema del salvataggio delle credenziali aziendali su un profilo Google privato pone l'attenzione sul connesso tema dell'interconnessione degli strumenti e servizi aziendali con quelli privati. Aziende molto strutturate pongono serie barriere all'utilizzo per scopi personali di strumenti aziendali, e viceversa. Aziende meno strutturate, di contro, troverebbero tali limitazioni troppo bloccanti per l'attività quotidiana. Un problema tipico è quello della connessione a reti Wi-Fi non aziendali. Collegarsi ad una rete non nota, soprattutto quelle pubbliche di bar, stazioni e aeroporti, espone i dispositivi aziendali al rischio del c.d. attacco "*man in the middle*". Ad un attaccante *sarà sufficiente* recarsi con un PC portatile in stazione e condividere una finta rete con un nome, tipo "Grandi Stazioni Libera". Dopodiché con opportuni software *basta* ascoltare tutto il traffico in passaggio, intercettare le password inserite talvolta in chiaro e iniziare ad analizzare quello che si è pescato. Tra i molti studenti e disoccupati che ruotano attorno a questi luoghi, con un po' di tempo e fortuna si potrebbe riuscire ad entrare nell'account di posta o nel portatile di qualche professionista o imprenditore e con un po' di pazienza riuscire a scoprire il suo numero di cellulare e le credenziali della banca. Non è pesca a strascico, è caccia alla preda importante. Dal punto di vista della sicurezza informatica sarebbe meglio imporre ai collaboratori di collegarsi ad internet utilizzando esclusivamente connessioni 4G con telefoni aziendali, ma con l'aumento delle video call è evidente l'importante impatto sulle bollette telefoniche aziendali. Di contro, anche le reti Wi-Fi casalinghe, in quanto al di fuori del perimetro controllato, potrebbero essere fonte di rischio.

Un altro tema sono le porte USB. Qui i rischi sono vari: il primo è che un dipendente infedele copi della documentazione aziendale; il secondo è che inavvertitamente infetti il PC con un virus contenuto nella chiavetta; il terzo è che mediante l'installazione di una periferica, ad esempio anche solo una tastiera, un attaccante possa ottenere i privilegi di Amministratore locale della macchina.[43] Ovviamente l'esigenza di avere le porte USB abilitate è quella di potersi copiare i file semplicemente con una chiavetta e di poter aggiungere periferiche senza troppe preoccupazioni.

Un altro tema importante è legato agli smartphone in quanto oggi dai dispositivi mobili è praticamente possibile accedere in mobilità a quasi tutti i dati aziendali. Il controllo degli smartphone può avvenire mediante strumenti di Mobile Device Management (MDM) garantendo così la gestione da remoto del dispositivo, compresa la cancellazione dei dati in esso contenuto, il blocco dell'intero dispositivo e la gestione delle autorizzazioni inerenti al download delle applicazioni consentite (e in questi casi tipicamente Whats App e gli altri social network non sono tra queste). Di contro, è diffusa tra i lavoratori la prassi di utilizzare per comodità gli strumenti di messaggistica istantanea o altri sistemi collaborativi, magari non validati dall'azienda: secondo uno studio di Veritas Technologies "*il 71% dei dipendenti a livello globale ammette di condividere dati sensibili e business-critical utilizzando la messaggistica istantanea e gli strumenti di collaborazione aziendale*"[44]. L'immediata conseguenza è il rischio di data breach. Il DPA finlandese ha stabilito che un'impresa di pulizie ha violato il GDPR utilizzando i servizi di messaggistica istantanea di WhatsApp con i propri dipendenti come mezzo per condividere informazioni sui propri clienti, inclusi nomi, indirizzo, codice della porta o codice della cassetta delle chiavi. Tra l'altro, il titolare del trattamento non aveva i mezzi per vigilare sull'uso dei dati personali tramite WhatsApp, o altrimenti imporre restrizioni su un possibile ulteriore utilizzo.[45] Un caso simile si era verificato anche nel 2020, quando una banca rumena è stata multata dal locale Garante a causa di un impiegato che per sua comodità operativa si faceva mandare le fotocopie dei documenti via WhatsApp[46] [47].

Conclusioni

Gli esempi fin qui citati non possono essere chiaramente esaustivi delle molteplici complessità e aspetti da affrontare nel redigere un Regolamento SIA ma hanno lo scopo di porre in rilievo la circostanza per cui in materia di sicurezza delle informazioni non esiste una risposta o una posizione corretta in senso assoluto. I responsabili della sicurezza richiederanno sempre più budget e più restrizioni, gli operativi più libertà, il DPO sarà in contrasto con le esigenze del marketing e l'Organismo di Vigilanza 231 dovrà garantire la compliance. La *coperta è corta* e ogni singola realtà deve adattarla alle proprie peculiari esigenze, senza dimenticare la premessa: il regolamento SIA serve a supportare la continuità del Business, non è un'opera d'arte fine a sé stessa.

42 È possibile rubare le impronte digitali da una foto su Facebook https://qds.it/24135-possibile-rubare-impronte-digitali-da-una-foto-su-facebook-htm/;

43 Need local admin and have physical access? https://twitter.com/jOnh4t/status/1429049506021138437;

44 https://www.veritas.com/en/au/news-releases/2021-03-10-71-percent-of-employees-globally-admit-to-sharing-sensitive-and-business-critical-data-using-instant-messaging-and-business-collaboration-tools-according-to-new-research-from-veritas;

45 Tietosuojavaltuutetun toimisto (Finland) - 9024/181/19 https://gdprhub.eu/index.php?title=Tietosuojavaltuutetun_toimisto_(Finland)_-_9024/181/19&mtc=today;

46 Impiegato di banca usava WhatsApp per farsi inviare documenti dai clienti, violato il Gdpr https://www.federprivacy.org/informazione/primo-piano/impiegato-di-banca-usava-whatsapp-per-farsi-inviare documenti-dai-clienti-violato-il-gdpr;

47 Sancțiune pentru încălcarea RGPD https://www.dataprotection.ro/?page=Sanctiune_pentru_incalcarea_RGPD_BCR&lang=ro.

Sistemi di videosorveglianza nel mirino del Garante privacy

di Elisa Chizzola

Rischi della videosorveglianza: è sempre più difficile restare anonimi

I sistemi di videosorveglianza rappresentano strumenti di sicurezza e di controllo sempre più diffusi.

I dispositivi video si inseriscono prepotentemente nella vita delle persone, caratterizzando sia contesti pubblici che privati, e sono in grado di influenzare fortemente i comportamenti dei cittadini sottoposti all'occhio dell'obbiettivo.

Questo inarrestabile processo richiede necessariamente una gestione dei sistemi di rilevazione delle immagini conforme alle norme dell'ordinamento giuridico: si può oggi parlare di una vera e propria "video-governance", contesto non solo complesso e critico ma anche normativamente "stratificato".

Infatti, l'utilizzo e la gestione di sistemi di videosorveglianza richiede il rispetto, oltre che della disciplina in materia di trattamento e protezione dei dati personali, anche delle altre normative applicabili: ad esempio, le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata (tra cui art. 615-bis, Codice penale), o in materia di controllo a distanza dei lavoratori (art. 4, Statuto dei lavoratori).

Non solo. L'utilizzo sempre più massiccio, dal punto di vista quantitativo, di strumenti video vede, parallelamente, un inarrestabile processo di sofisticazione degli strumenti utilizzati grazie all'evoluzione delle tecnologie, situazione che aumenta in modo esponenziale tutte le criticità e le complessità legate ad una gestione *compliance* del fenomeno.

La videosorveglianza è diventata un sistema ad alte prestazioni grazie alla crescente applicazione di tecnologie di analisi dei video "intelligenti", che rinviano al concetto di "sorveglianza intelligente" effettuata con telecamere dotate di tecniche di *artificial intelligence* anche attraverso il riconoscimento facciale con tecniche biometriche.

Se è vero, infatti, che la videosorveglianza, sotto il profilo della materia della protezione dei dati personali, rappresenta un tema che potremmo definire "tradizionale", occorre sottolineare come esso sia un ambito sempre in "evoluzione": oltre alle tecnologie di AI, si diffondono droni, *bodycam*, e altre sofisticate strumentazioni. È chiaro come ormai la videosorveglianza, anche senza "scomodare" le tecniche di AI, vada ben oltre la ripresa di un luogo fisico che entra nel raggio d'azione della telecamera.

È evidente come tali strumentazioni si rivelano molto intrusive e aumentano vertiginosamente, lato *data protection*, i rischi legati ai diritti e alle libertà delle persone riprese. Se infatti il diritto alla riservatezza, come noto, storicamente nasce dall'inviolabile "diritto ad essere lasciati soli" (*right to be alone*) che porta con sé il correlato "diritto all'anonimato", è evidente come le "memorie" della videosorveglianza mettano seriamente in pericolo tali diritti. Resta-

re anonimi e preservare la propria privacy rappresentano esigenze sempre più difficili da soddisfare per l'individuo.
Siamo consapevoli che tutto ciò non si può arrestare, anzi, è inevitabile che tale fenomeno caratterizzerà sempre più intensamente le nostre vite.
Se ciò è inconfutabile, tuttavia, il rischio per i diritti e le libertà delle persone fisiche può essere mitigato da una gestione sempre più "governata" dei sistemi di videosorveglianza esistenti ed in procinto di essere installati; tale *governance* deve necessariamente basarsi sulla conoscenza approfondita di tutte le normative coinvolte.
Tali normative fanno riferimento a discipline tutte molto specialistiche che si intrecciano, come spesso accade, e in questo caso sono caratterizzate da competenze che derivano dalla conoscenza della normativa civilistica e penale in tema, dell'ambito gius-lavoristico collegato, nonché naturalmente della conoscenza e applicazione delle norme e principi privacy.
Ecco che allora è essenziale seguire e conoscere gli adempimenti che società, enti ed imprese devono mettere in atto al fine di installare e utilizzare correttamente le tecnologie in questione.

La videosorveglianza nel piano ispettivo del Garante privacy nel primo semestre 2022

È quanto mai importante riprendere ed analizzare gli adempimenti privacy legati ai sistemi di videosorveglianza in questo momento, considerando che il Garante per la protezione dei dati personali ha stabilito che per il primo semestre 2022 l'attività ispettiva si focalizzerà anche su tale settore. Quindi in questo periodo il Garante privacy "punta il faro" anche sul trattamento di dati personali nell'ambito della videosorveglianza attraverso le attività ispettive curate dallo stesso Ufficio dell'Autorità di controllo italiana, affiancato dalla Guardia di finanza con il suo Nucleo speciale tutela privacy e frodi tecnologiche.
L'esigenza di concentrare i controlli in tale ambito deriva dal fatto che nell'ultimo periodo l'Autorità di controllo è stata subissata di reclami e segnalazioni riguardanti, oltre che al settore del telemarketing, anche potenziali trattamenti di dati illeciti nell'ambito della gestione dei dispositivi video. Infatti, ultimamente i settori più "caldi", oggetto di reclami e segnalazioni da parte degli interessati, sono tre: il telemarketing, la videosorveglianza, oltre che il mancato soddisfacimento dei diritti in capo agli interessati. In particolare, le segnalazioni e i reclami in tema di videosorveglianza vengono inviati all'Autorità di controllo da cittadini, da condomini, da clienti-consumatori, ma anche da dipendenti e relative organizzazioni sindacali aziendali. I rappresentanti dei lavoratori spesso lamentano che le telecamere costituiscano più strumenti di controllo dei lavoratori piuttosto che misure a difesa della proprietà e sicurezza aziendale. È chiaro quindi che la grande attenzione che negli ultimi mesi è stata

data dai cittadini al tema della videosorveglianza ha portato il Garante a voler approfondire tale ambito programmando controlli mirati per il primo semestre del 2022.

Evoluzione normativa in tema di videosorveglianza

Occorre fare innanzitutto il punto sulla normativa applicabile al contesto della videosorveglianza che, rispetto all'ambito della protezione dei dati personali, rinvia *in primis* al GDPR e al Codice privacy, ma che comprende anche i provvedimenti emanati – nel 2000, nel 2004 e nel 2010 e, più recentemente nel 2020 in forma di FAQ – dall'Autorità di controllo italiana, capace di esprimere importanti criteri interpretativi delle norme in argomento, per poi arrivare alla Linee guida adottate il 29 gennaio 2020 dall'European data protection board (n. 3/2019).
Sinteticamente, ripercorrendo l'evoluzione normativa e provvedimentale citata, in assenza di una specifica normativa, con il Provvedimento del 29 novembre 2000, il Garante privacy italiano ha deciso di fissare un "decalogo" di regole, costituito da indicazioni sintetiche ma interessanti, per aiutare i soggetti a rendere conforme alle norme sulla privacy l'installazione di telecamere in luoghi pubblici e privati.
Successivamente, con il Provvedimento generale del 29 aprile 2004 è stato introdotto l'obbligo di sottoporre alla verifica preliminare del Garante i trattamenti che prevedono l'intreccio delle immagini con dati biometrici e voce o in caso di digitalizzazione delle immagini.
Il provvedimento generale dell'8 aprile 2010, invece, ha imposto il rispetto di garanzie ancor più stringenti per l'introduzione di sistemi integrati di videosorveglianza. In particolare, tale provvedimento aveva previsto l'obbligo di sottoporre alla preventiva autorizzazione del Garante i sistemi che presentavano rischi per i diritti e le libertà fondamentali delle persone, come i sistemi tecnologicamente avanzati o "intelligenti".
Il meccanismo della preventiva autorizzazione del Garante a seguito di una verifica preliminare (cd. "prior checking") era previsto dall'ormai abrogato art. 17, Codice privacy.
L'applicazione delle norme e dei principi contenuti nel GDPR, vincolanti per tutti gli Stati membri dell'Ue a partire dal 25 maggio 2018, ha avuto un'importanza fondamentale anche sul versante della corretta gestione della videosorveglianza: la nuova volontà del Legislatore europeo segna il passaggio, tra le altre cose, dalla verifica preliminare dell'Autorità (ex art. 17 Codice privacy, oggi abrogato) al principio di accountability.
Si sottolinea che il provvedimento del 2010 risulta ancora valido nella misura in cui le disposizioni e i criteri interpretativi in esso contenuti non risultano superati dal GDPR e dalle Linee guida n. 3/2019 dell'EDPB.
Infatti, a questo proposito, il 29 gennaio 2020 l'European Data Protection Board ha adottato le Linee guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video, che comprendono anche la cd. videosorveglianza. Le Linee guida forniscono importanti indicazioni circa l'approccio basato sul rischio nei trattamenti che includono la videosorveglianza, con una particolare attenzione rivolta alle nuove tecnologie.
Inoltre, il Garante per la protezione dei dati personali il 5 dicembre 2020 ha messo a punto delle interessanti Faq sulle questioni concernenti il trattamento dei dati personali nell'ambito dell'installazione di impianti di videosorveglianza da parte di soggetti pubblici e privati. Tali chiarimenti si sono resi necessari in ragione delle nuove previsioni introdotte dal GDPR, alla luce delle quali va valutata la validità dell'ultimo provvedimento del Garante in materia sopra citato, che risale al 2010 e che evidentemente contiene prescrizioni in parte superate. Le Faq tengono conto anche delle citate Linee guida dell'EDPB e contengono un modello di informativa semplificata redatto proprio sulla base dell'esempio proposto dall'EDPB.
Da ultimo, si sottolinea che recentemente, nel corso del mese di gennaio 2022, il Garante privacy, data l'effettiva e sentita esigenza di sicurezza personale dei cittadini che ricorrono sempre più spesso a telecamere "private", ha diffuso una pratica e chiara scheda informativa che fissa sinteti-

camente le condizioni da seguire nel caso in cui le persone fisiche siano interessate ad attivare sistemi di videosorveglianza a tutela della sicurezza di persone o beni, nell'ambito di attività di carattere personale o domestico.
Peraltro, è in fase di definizione presso il Garante un nuovo provvedimento in tema di videosorveglianza che aggiorna il provvedimento citato del 2010 in quanto l'Autorità di controllo sente ormai l'esigenza di allineare le disposizioni della fonte provvedimentale alle Linee guida del Board e, in generale, ai tutti i principi del GDPR, eliminando in questo modo potenziali sovrapposizioni tra fonti e rischi di errata interpretazione.

Definizione di videosorveglianza e dati personali oggetto del trattamento

Il RGPD non contiene una definizione dei sistemi di videosorveglianza, tuttavia una descrizione tecnica è disponibile, ad esempio, nella norma EN 62676-1-1:2014.
È l'EDPB con le Linee guida citate n. 3/2019 che prova a definire, dal punto di vista terminologico, un sistema di videosorveglianza (VVS), concependolo come sistema costituito da "*dispositivi analogici e digitali nonché da software per acquisire immagini, gestirle e mostrarle a un operatore*". Il Board abbraccia una definizione "tecnica" descrivendo gli elementi che devono comporre tale sistema, categorizzabili con riferimento:
• ad un ambiente video: l'attività del sistema comprende, in generale, l'acquisizione di immagini, l'interconnessione e la gestione delle immagini;
• alle funzioni logiche di gestione del sistema, le quali implicano la gestione dei dati, delle attività e delle interfacce/connessioni con altri sistemi;
• alla sicurezza di un sistema, la quale consiste nella riservatezza, nell'integrità e nella disponibilità del sistema e dei dati, contesto che comprende la sicurezza fisica di tutti i componenti del sistema e il controllo dell'accesso al VVS, nonché la prevenzione della perdita o della manipolazione dei dati.
Sotto il profilo della tipologia dei dati personali che possono entrare nel raggio d'azione della telecamera, si evidenzia che la sorveglianza sistematica e automatizzata di uno spazio specifico con mezzi ottici o audiovisivi comporta la raccolta e la conservazione di informazioni grafiche o audiovisive su tutte le persone fisiche che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici. L'identità di tali persone può essere stabilita sulla base delle informazioni così raccolte. Questo tipo di sorveglianza consente, inoltre, un ulteriore trattamento dei dati personali per quanto riguarda la presenza e il comportamento delle persone nello spazio considerato. È sulle possibili "correlazioni" di dati che si insinuano la maggior parte dei rischi per la riservatezza degli individui, senza dimenticare che il rischio potenziale di un uso improprio di tali dati aumenta in rapporto alla dimensione dello spazio monitorato e al numero di persone che lo frequentano.
Non solo. Come detto, i sistemi di videosorveglianza raccolgono enormi quantità di dati personali che possono rivelare dati di natura altamente personale e persino categorie particolari di dati ai sensi dell'art. 9 GDPR. Infatti, dati apparentemente non significativi, all'origine raccolti tramite video, possono essere utilizzati per ricavare altre informazioni e raggiungere uno scopo diverso da quello iniziale (ad esempio, per mappare le abitudini di un individuo). Naturalmente se le riprese video sono trattate allo scopo di ricavare categorie particolari di dati si applica l'art. 9, pertanto tale finalità va innanzitutto dichiarata nell'informativa e richiede una delle deroghe al divieto generale di trattamento di tali categorie di dati previste dalla norma citata. A questo proposito, le FAQ del Garante privacy del 2020 evidenziano come il trattamento di categorie particolari di dati personali attuato attraverso sistemi video richieda una vigilanza rafforzata e continua, ad esempio attuata con elevati livelli di sicurezza e attraverso una DPIA.

Sistemi di videosorveglianza: principi generali e adempimenti

Naturalmente per installare impianti di videosorveglianza correttamente, in conformità alla normativa *data protection*, occorre innanzitutto rispettare i principi cardine previsti dal GDPR, vale a dire *in primis* il principio di privacy by design e by default, i principi generali applicabili al trattamento dei dati personali ex art. 5 DGPR (principio di liceità, correttezza e trasparenza, principio di limitazione della finalità, principio di minimizzazione dei dati – si veda *infra* il paragrafo dedicato – principio di esattezza, principio di limitazione della conservazione, principio di integrità e riservatezza), compreso il principio di accountability.
Più nello specifico, per quanto riguarda gli step da seguire per l'installazione di sistemi di videosorveglianza compliance privacy, si elencano di seguito gli adempimenti necessari:
• individuazione della finalità del trattamento e della relativa base giuridica ex art. 6 GDPR;
• previsione del periodo di conservazione dei dati personali;
• predisposizione delle misure di sicurezza tecniche ed organizzative;
• previsione del processo di gestione dei diritti dell'interessato;
• predisposizione delle informative privacy (composta da cartello ed informativa completa), che deve contenere sinteticamente le decisioni relative ai 4 punti sopra citati;
• regolamento tecnico per l'utilizzo del sistema di videosorveglianza e controllo datoriale nel rispetto dell'art. 4, Statuto dei lavoratori, nel caso di inserimento del sistema in ambito lavorativo (art. 114 Codice privacy);
• predisposizione della DPIA ex art. 35 GDPR, nel caso di rischio elevato per i diritti e le libertà degli interessati (ed eventuale consultazione preventiva del Garante privacy ex art. 36 GDPR);
• istruzione agli autorizzati al trattamento dei dati personali/immagini raccolte derivanti dagli impianti di videosorveglianza;
• eventuale nomina dei responsabili per il trattamento dei dati personali ex art. 28 GDPR, nel caso in cui l'attività di videosorveglianza venga gestita da un soggetto terzo per conto del titolare del trattamento.

Finalità del trattamento e base giuridica

La videosorveglianza può servire per molti scopi che sinteticamente rinviano a finalità di sicurezza di persone o beni, nonché di controllo di persone o beni.
In particolare, le finalità che possiamo definire "tipiche" perseguite dal titolare del trattamento in occasione dell'installazione della relativa strumentazione fanno riferimento all'esigenza di:
• protezione della vita e dell'integrità fisica degli individui;
• protezione della proprietà (mobiliare o immobiliare);
• rilevazione, prevenzione e controllo delle

possibili infrazioni, in ambito civilistico e amministrativo;
• rilevazione, prevenzione e controllo in relazione alla commissione di reati;
• acquisizione di elementi di prova in vista di procedimenti giudiziari e stragiudiziali;
• identificazione biometrica di soggetti sospetti.
Ogni finalità del monitoraggio, che deve essere specifica per ogni telecamera di sorveglianza in uso, va documentata per iscritto ai sensi dell'art. 5, par. 2, GDPR (principio di accountability), nonché va comunicata all'interessato ex art. 13 GDPR.
Si ricorda, che l'art. 5, par. 1, lett. b), GDPR stigmatizza il principio di limitazione delle finalità, secondo il quale i dati personali devono essere raccolti per finalità "*determinate, specifiche e legittime*", pertanto la semplice menzione di uno scopo di "*sicurezza*" o "*per la vostra sicurezza*" con riguardo alla videosorveglianza non è sufficientemente specifica. Tali locuzioni peraltro contrastano con il principio secondo il quale i dati personali devono essere "*trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*" (principio di liceità, correttezza e trasparenza ex art. 5, par. 1, lett. a), GDPR).
Il ragionamento giuridico legato all'individuazione della finalità, in ambito *data protection*, è strettamente collegato alla scelta della corretta base giuridica ex art. 6 GDPR che supporta la liceità del trattamento stesso. Nella pratica, nel contesto della videosorveglianza, le condizioni di liceità più suscettibili di essere utilizzate sono il legittimo interesse (art. 6, par. 1, lett. f), la necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6, par. 1, lett. e), e, in casi marginali, il consenso (art. 6, par. 1, lett. a).
In relazione, in particolare, alla base giuridica del legittimo interesse, tale condizione di liceità si configura legittima se la videosorveglianza è necessaria per conseguire la finalità di soddisfare un legittimo interesse (che può avere natura giuridica, economica o immateriale) perseguito da un titolare del trattamento o da un terzo, a meno che su tale interesse non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato. Il legittimo interesse, inoltre, deve esistere ed essere attuale e non quindi fittizio od ipotetico.

Principio di minimizzazione con criterio cardine

Come anticipato, la corretta installazione di sistemi di videosorveglianza deve avvenire nel rispetto dei principi generali previsti dal GDPR, innanzitutto conformemente al principio di minimizzazione dei dati personali ex art. 5, par. 1, lett. c), GDPR, secondo il quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
Tale principio cardine in materia di privacy, nell'ambito della videosorveglianza si traduce nell'obbligo per il titolare del trattamento di valutare criticamente, prima di installare il sistema, se questa misura sia in primo luogo idonea a raggiungere l'obiettivo desiderato e, in secondo luogo, se sia adeguata e necessaria per i suoi scopi.
La logica è quella della misura di *extrema ratio*: il titolare del trattamento deve optare per la videosorveglianza esclusivamente se la finalità non si possa ragionevolmente raggiungere con altri mezzi meno invasivi per i diritti e le libertà fondamentali degli interessati.
Per esplicitare meglio il concetto, l'EDPB esemplifica considerando il caso di un titolare che abbia l'esigenza di prevenire reati legati al patrimonio: invece di installare un sistema di videosorveglianza potrebbe scegliere di adottare misure di sicurezza alternative, come la recinzione della proprietà, una migliore illuminazione, l'installazione di serrature di sicurezza, finestre e porte a prova di manomissione o l'applicazione di rivestimento anti-graffiti o lamine alle pareti (oltre che valutare, nelle realtà più complesse, l'opzione dell'utilizzo di personale di sicurezza e di custodi). Tali misure, infatti, possono essere efficaci quanto i sistemi di videosorveglianza contro furti e vandalismi e, dato che sono meno invasive rispetto alla videosorveglianza, rispettano a pieno il principio di minimizzazione in esame.
È chiaro che l'applicazione del principio di minimizzazione richiede un'attività di bilanciamento degli interessi in gioco: il contemperamento va fatto tenendo presente, da una parte, i legittimi interessi e le finalità del titolare del trattamento e, dall'altro, i diritti e le libertà fondamentali delle persone fisiche. Tale ragionamento giuridico deve essere effettuato specificatamente, caso per caso.
In questo contesto, criterio decisivo è rappresentato dalla "misura" della potenziale invasività della videosorveglianza rispetto ai diritti ed alle libertà dell'individuo. Il "calcolo" di tale "misura" dipende da diversi fattori: dal tipo di informazioni raccolte (contenuto delle informazioni), dalla portata (densità delle informazioni, estensione territoriale e geografica), dal numero di interessati coinvolti – come numero specifico o come percentuale della popolazione interessata – dalla situazione specifica, dagli interessi effettivi del gruppo di interessati, dalla disponibilità di strumenti mezzi alternativi nonché dalla natura e dalla portata della valutazione dei dati. Quindi importanti elementi di bilanciamento si rivelano essere le dimensioni della zona e il numero di interessati sotto sorveglianza.
Oltre a ciò, sempre in virtù del principio di minimizzazione, occorre interrogarsi sulla necessità del trattamento anche sotto il profilo delle modalità di conservazione delle immagini. In alcuni casi potrebbe essere necessario utilizzare soluzioni tipo scatola nera, nelle quali il filmato viene registrato, conservato e automaticamente cancellato dopo un determinato periodo di tempo, con la possibilità di accedervi solo in caso in cui si verifichino eventi problematici. Invece, in altre situazioni, potrebbe non essere necessario registrare il materiale video, essendo magari sufficiente il monitoraggio in tempo reale, senza registrazione. L'opzione per tale seconda soluzione, se si ritiene non indispensabile la registrazione delle immagini, rispetta a pieno il principio di minimizzazione nei termini sopra descritti. Naturalmente la scelta tra le due soluzioni dipende dallo scopo perseguito.

Informative di primo livello (cartello) e di secondo livello (informativa privacy completa)

Un altro adempimento che richiede un focus particolare è quello legato all'obbligo di trasparenza in capo al titolare del trattamento: l'attività di videosorveglianza solitamente è segnalata all'interessato, attraverso un approccio scalare/granulare, con un'informativa di primo livello (cd. cartello) e con un'informativa di secondo livello, vala a dire completa di tutti gli elementi ex art. 13 GDPR.
L'informativa semplificata fornita attraverso il consueto cartello (si ricorda che le FAQ del Garante privacy hanno fornito un fac-simile di cartello, in linea con il modello fornito dalle Linee guida dell'EDPB citate) deve contenere, tra le altre informazioni, le indicazioni sul titolare del trattamento e sulla finalità perseguita.
Il cartello va collocato prima di entrare nella zona sorvegliata, in quanto l'interessato

deve poter capire in anticipo, prima di accedervi, quale zona sia coperta da una telecamera: in questo modo, se lo ritiene, può consapevolmente scegliere di evitare la sorveglianza oppure può decidere di adeguare il proprio comportamento alla presenza del sistema video.
Non è necessario che il cartello riporti la precisa ubicazione della telecamera, purché non vi siano dubbi su quali zone sono soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza.
L'informativa semplificata deve rinviare all'informativa completa contenente tutti gli elementi obbligatori ex art. 13 GDPR, indicando chiaramente le modalità per accedere al testo esteso: ad esempio, è possibile rinviare al sito Internet del titolare del trattamento, oppure alle bacheche aziendali, oppure - sfruttando la tecnologia esistente - il cartello potrebbe riportare un QR Code (codice QR) che rimanda direttamente al testo dell'informativa estesa e completa.

Periodo di conservazione delle immagini registrate

La questione dei tempi di conservazione delle immagini registrate dai sistemi di videosorveglianza rappresenta un tema molto delicato e complesso, che implica attente e motivate valutazioni in capo al titolare del trattamento.
Come anticipato, per strutturare un sistema di videosorveglianza compliance privacy è necessario rispettare, tra gli altri, anche il principio di limitazione della conservazione (art. 5, par. 1, lett. e), GDPR), in virtù del quale le immagini non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite.
In base al principio di accountability, spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.
Le FAQ del Garante per la protezione dei dati personali fanno proprio questo ragionamento, al netto di specifiche norme di legge che prevedono espressamente determinati tempi di conservazione dei dati. Ad esempio, l'art. 6, co. 8, D.L. 11/2009, nell'ambito dell'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, dispone che "*la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione*".
In via generale, le FAQ citate, allineandosi ai ragionamenti dell'EDPB, sottolineano che spesso gli scopi della videosorveglianza sono la sicurezza e la protezione del patrimonio. Se questo è lo scopo, solitamente è possibile individuare eventuali danni entro uno o due giorni. Pertanto, tenendo conto dei principi di minimizzazione dei dati e di limitazione della conservazione, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve a rilevare atti vandalici) – cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione.
Per orientale i titolari, il Garante privacy descrive una fattispecie concreta: occorre considerare che normalmente un piccolo esercizio commerciale si accorgerebbe di eventuali atti vandalici il giorno stesso in cui si verificano; pertanto in questo caso un periodo di conservazione di 24 ore si dimostra, in linea generale, sufficiente. Tuttavia, la chiusura nei fine settimana o in periodi festivi più lunghi potrebbe giustificare un periodo di conservazione più prolungato.
Infine, a chiosa del tema, si sottolinea che in particolari casi potrebbe essere necessario prolungare i tempi di conservazione delle immagini inizialmente fissati dal titolare o previsti dalla legge: ad esempio, nel caso in cui tale prolungamento si renda necessario a dare seguito ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria in relazione ad un'attività investigativa in corso.

Che cos'è il *whistleblowing?*

di Silvia Crocelli

Il *whistleblowing* è un sistema di derivazione anglosassone, tramite il quale viene regolamentata la possibilità per l'intraneo, di un'organizzazione pubblica o privata, di segnalare potenziali condotte illecite o irregolarità di cui sono venuti a conoscenza nello svolgimento della propria attività lavorativa. Tratto dall'inglese "*to blow the whistle*" – letteralmente "soffiare il fischietto", il *whistleblower* è, infatti, colui che scopre un comportamento illecito o fatti che accusano o possono causare un pregiudizio all'ente di appartenenza o a terzi (i.e. consumatori, clienti e/o azionisti) e, perciò, lo segnala al soggetto a ciò deputato internamente dall'organizzazione di appartenenza (*whistleblowing* interno) o alle autorità competenti (*whistleblowing* esterno).
Finalizzato all'accertamento ed alla repressione della condotta illecita, l'istituto in esame mira a prevenire i rischi di illiceità per l'ente in cui opera il *whistleblower* e, in linea di massima, vuole reprimere rischi e delle situazioni pregiudizievoli per l'interesse pubblico generale. Inizialmente introdotto in ambito pubblico con riferimenti al contrasto dei fenomeni corruttivi (cfr. più approfonditamente *infra*), nel tempo l'istituto è stato esteso ad altri ambiti, così come è stato ampliato il novero dei soggetti legittimati ad effettuare la segnalazione.
Molteplici sono le normative che prevedono questo sistema di contrasto al crimine: il D.Lgs. n. 165/2001 (T.U. pubblico impiego), il D.Lgs. n. 231/2001 (responsabilità da illecito amministrativo dipendente da reato dell'ente), il D.Lgs. n. 231/2007 (antiriciclaggio), il D.Lgs. n. 209/2005 (codice delle assicurazioni private), il D.Lgs. n. 385/1993 (Testo Unico bancario), il D.Lgs. n. 58/1998 (Testo Unico della Finanza).
L'essere previsto e collocato in articolati diversi, fa sì che il sistema della segnalazione presenti, in ciascuno di essi, caratteristiche peculiari, rilevando un gap di coordinamento (ad esempio, cambia l'oggetto della segnalazione così come cambia il soggetto designato a ricevere la segnalazione).

Il quadro normativo

L'istituto era quasi del tutto sconosciuto in Italia prima della legge n. 190/2012 (c.d.

legge anticorruzione o legge Severino), che ha inserito nel T.U. del Pubblico Impiego, l'art. 54-*bis* del D.Lgs. n. 165/2001, intitolato "*Tutela del dipendente pubblico che segnala illeciti*", (poi modificato dalla L. n. 178/2017), il quale stabilisce che "*il pubblico dipendente [...] non può essere sanzionato, dimensionato, licenziato, trasferito o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti sulle condizioni di lavoro determinata dalla segnalazione [...] L'adozione di misure ritenute ritorsive, di cui al primo periodo, nei confronti del segnalante è comunicata in ogni caso all'ANAC dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere [...].*

In seguito, con l'entrata in vigore della Legge 30 novembre 2017 n. 179 che ha profondamente modificato la disciplina del *whistleblowing*, l'ambito di operatività dell'art. 54-*bis* del D.Lgs. n. 165/2001 è stato innovato, rendendo tra l'altro necessaria l'emanazione da parte dell'ANAC di nuove linee guida nel 2021 in sostituzione a quelle del 2015. In particolare, in merito all'oggetto della segnalazione ai fini della tutela prevista dall' art. 54-*bis*, l'ANAC stabilisce che "*i fatti oggetto delle segnalazioni whistleblowing comprendono [...] tutte le situazioni in cui, nel corso dell'attività amministrativa, si riscontri un abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati.*" Vediamo inoltre che secondo quanto stabilito dal comma 1 del riformato art. 54-*bis* la segnalazione può essere fatta o al responsabile della prevenzione della corruzione e della trasparenza, o all'autorità nazionale anticorruzione (ANAC), o all'autorità giudiziaria ordinaria o, infine, all'autorità giudiziaria contabile.

Per quanto concerne il settore privato, la L. n. 179/2017, ha novellato, altresì, l'art. 6, D. Lgs. n. 231/2001, riguardante la responsabilità amministrativa degli enti (si veda più diffusamente *infra*) terminando il suo intervento nell'esame del rapporto tra il segreto d'ufficio aziendale e l'obbligo di fedeltà del dipendente con la denuncia degli illeciti.

Molte le novità, dunque, apportate: dalla più puntuale previsione di regole specifiche per tutte le pubbliche amministrazioni, nonché fornitori per le PP.AA., all'estensione della disciplina del *whistleblowing* anche al settore privato nel sistema 231, dall'ampliamento della tutela nei confronti dei segnalanti in presenza di condotte ritorsive e/o discriminatorie all'assoluta necessità di munirsi di canali alternativi, dei quali è necessario che almeno uno sia strutturato con modalità informatiche.

Da ultimo, si segnala che entro il 17 dicembre 2021 dovrà essere recepita la direttiva UE 2019/1937 nel nostro ordinamento, con la quale verrà imposto a tutte le imprese con un numero di dipendenti superiore a 50 di implementare un sistema di *whistleblowing*.

In ultimo, si segnala la revisione delle Linee Guida di Confindustria e di ANAC, pubblicate nel giugno 2021, nonché, tra le altre, quelle emanate dall'Ordine dei Commercialisti nel febbraio 2021, tutte finalizzate a fornire indicazioni specifiche ed organiche su come realizzare, attraverso la definizione di apposite regole, un sistema di *whistleblowing*.

La Legge n. 179/17 nel settore privato in particolare nei Modelli 231

Come anticipato, la legge n. 179/17 ha introdotto l'obbligo di previsione del *whistleblowing* anche all'interno dei modelli di organizzazione, gestione e controllo, tramite una novella all'art. art. 6 del D.Lgs. n. 231/2001, aggiungendo i commi 2-*bis*, 2-*ter* e 2-*quater*. Se da un lato i modelli devono prevedere canali alternativi - tra cui mail, lettera, piattaforme digitali, telefono - attraverso i quali i soggetti apicali o dipendenti possano segnalare le condotte illecite, ai sensi del D. Lgs. n. 231/01, dall'altro è necessario che la segnalazione sia fondata su elementi di fatto precisi, non arbitrari, puntuali e concordanti, evitare una *non gestione* della segnalazione ovvero l'erogazione di sanzioni disciplinari in caso di segnalazione che si riveli infondata, effettuata con dolo e colpa grave.

La disposizione, così come le Linee Guida di Confindustria, esplicita la necessità di almeno un canale alternativo di segnalazione che sia idoneo a garantire, con modalità informatiche, la "riservatezza" dell'identità del segnalante. Su tutto, la normativa interviene a stabilire una tutela rafforzata verso il whistleblower, vietando atti discriminatori o ritorsivi nei confronti del segnalante per motivi che anche indirettamente possano ricollegarsi alla segnalazione (così l'art. 6, co. 2-*bis*, del D.Lgs. 231/2001).

Quanto al soggetto destinatario, è necessario che la segnalazione, se non in prima battuta, venga comunque inoltrata all'Organismo di Vigilanza.

Quanto all'oggetto, oltre alle ipotesi di reato c.d. presupposto che compongono il Catalogo 231, si ritiene che la "denuncia" possa concernere anche violazioni di procedure, protocolli, policy adottate a presidio della prevenzione di reati, nonché in tutti quei comportamenti che in qualche modo possano rientrare all'interno della nozione di "*mala gestio*", in quanto sintomo di un atteggiamento che in un futuro potrebbe estrinsecare in condotte illecite ai sensi della responsabilità amministrativa degli enti.

La revisione 2021 delle Linee Guida di Confindustria recepisce al proprio interno la Legge n. 179/2017, fornendo precise indicazioni sull'attuazione dell'istituto all'interno del modello.

In particolare, vengono fornite indicazioni sul canale di segnalazione, non escludendo la possibilità di prevedere anche canali per effettuare segnalazioni in forma anonima, con espresso rinvio alle Linee Guida ANAC n. 6/2015.

Confindustria sottolinea, inoltre, l'importanza che la definizione delle policies proceda a pari passo con la predisposizione degli strumenti informatici di supporto e che, in ogni caso, l'implementazione tenga conto dei dettati del GDPR.

Importanti indicazioni vengono, quindi, fornite sul destinatario della segnalazione, offrendo una serie di esemplificazioni che prevedono: l'OdV o altro soggetto/comitato/struttura specificamente individuata, il responsabile della funzione di compliance, un comitato rappresentato da soggetti appartenenti a funzioni quali area legale, compliance, HR, internal audit, il datore di lavoro nelle PMI, un ente o soggetto esterno dotato di comprovata professionalità, che si occupi di gestire la prima fase di ricezione delle segnalazioni, in coordinamento con l'ente.

Nel caso in cui non venga individuato come diretto referente l'Odv, andrà comunque prevista una reportistica, affinché il flusso di informazioni non sfugga al suo controllo e monitoraggio, che spiega i suoi riflessi sul funzionamento del modello, rimesso *ex lege* in capo all'Organismo di vigilanza.

Le Linee Guida concludono la disamina, riportandosi alla necessità di adeguamento alle prescrizioni della Direttiva 2019/1937.

Integrazione del *whistleblowing* con altre normative

Una corretta gestione del sistema del *whistleblowing* impone il rispetto di altre norme. In tema di protezione dei dati personali, vediamo come il *whistleblowing* debba essere oggetto di valutazione d'impatto e necessiti di una – apposita – informativa privacy. Qualora per le segnalazioni vengano utilizzati canali esterni, nella specie piattaforme digitali esterne, occorre procedere alla nomina di un responsabile esterno

per il trattamento dei dati ai sensi dell'art. 28 del GDPR. Il Garante per la protezione dei dati personali, con uno specifico provvedimento del 15 giugno 2021 n. 236, ha ribadito che in virtù della delicatezza delle informazioni contenute all'interno della segnalazione, è necessario tutelare l'identità del *whistleblower* attraverso un regime di riservatezza previsto dalla normativa di settore, ciò al fine di scoraggiare e precludere qualsiasi azione ritorsiva nei confronti del medesimo all'interno del contesto lavorativo di riferimento, spetta poi al titolare del trattamento garantire la conformità rispetto ai principi in materia di protezione dati.
Si segnala, inoltre, che nella normativa antiriciclaggio (D.Lgs. n. 2231/2007), a differenza e rispetto alle altre normative, si chiede di assicurare l'"anonimato" e non la riservatezza.
Di norma la piattaforma, ovvero il portale di segnalazione, è gestita da un soggetto specializzato, terzo e indipendente, e dovrebbe garantire la possibilità di effettuare la segnalazione senza che il soggetto segnalante abbia l'obbligo di palesarsi. Tuttavia, alcune società richiedono a quest'ultimo di fornire le proprie generalità per potersi iscrivere alla piattaforma, altre invece adottano un portale che consente di nasconderne il nominativo e solo nell'eventualità in cui ricorrano determinate circostanze, il responsabile *whistleblowing* potrà chiedere al segnalante di svelare la sua identità. Ciò è consentito dalla legge quando si parla di riservatezza e non di anonimato. In questo secondo caso, infatti, non è possibile venire a conoscenza del nominativo del segnalante, contrariamente, nel primo caso, l'azienda può anche pretendere di conoscerne l'identità nel rispetto di tutti quegli obblighi di riservatezza previsti dalle varie normative. La piattaforma digitale dovrebbe funzionare in modo semplice, attraverso un percorso guidato, che consenta ai dipendenti, ma anche a terzi (fornitori, collaboratori), di segnalare eventuali condotte illecite, irregolarità, violazioni del Codice Etico, violazioni di norme, di procedure o anche del Modello 231.
In materia di salute e sicurezza sul lavoro l'art. 20 del Testo Unico Salute e Sicurezza (D.Lgs. n. 81/2008) stabilisce l'obbligo di "*Segnalare immediatamente al datore di lavoro, al dirigente o al proposto le deficienze dei mezzi e dei dispositivi [...], nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia ala rappresentante dei lavoratori per la sicurezza*". In questo contesto, vi sono anche altre attività di prevenzione da attuare sui luoghi di lavoro, difatti l'art. 18 del D.Lgs. n. 81/2008 prevede in capo al datore di lavoro numerosi obblighi da rispettare come ad esempio fornire ai lavoratori i necessari dispositivi di protezione individuale, ma anche adempiere agli obblighi di formazione, informazione e addestramento di cui agli artt. 36-37 del decreto e così via. La mancata osservanza di queste disposizioni e di altre prescrizioni va ad integrare fattispecie di illecito di varia natura che quindi possono essere segnalate da un soggetto, il *whistleblower*, che andrà tutelato da eventuali ritorsioni.

ISO 37002:2021 per la gestione del *whistleblowing*

L'ISO ha pubblicato nel mese di luglio le Linee Guida 37002:2021 che costituiscono il primo standard completamente dedicato alla gestione del *whistleblowing*, in particolare fornirà le "*linee guida per l'attuazione, l'implementazione, la gestione, la valutazione, la manutenzione e il miglioramento di un solido ed efficace sistema di gestione del whistleblowing nell'ambito di un'organizzazione*". La norma si rivolge a tutti i tipi di organizzazioni, pubbliche, private, PMI, associazioni, aziende quotate, ecc., e assume la forma di Linee Guida recanti numerose raccomandazioni dirette a garantire la gestione delle segnalazioni ma non ha carattere di standard certificabile come, ad esempio, la ISO 37001:2016 o la ISO 37301:2021. La norma 37002 fornisce alle organizzazioni delle direttive pratiche, ma non individua prescrizioni. È stata elaborata secondo la struttura ad Alto Livello (*HLS- High Level Structure*) che consente una integrazione automatica con i sistemi di gestione già esistenti all'interno dell'organizzazione. L'*High Level Structure* si compone di dieci principi che devono essere rispettati ed utilizzati da tutti gli standard relativi ai sistemi di gestione ISO, al fine di assicurare coerenza tra i vari sistemi. Elemento caratteristico è la protezione dei segnalanti - informatori - attraverso la progettazione di un sistema di *whistleblowing* che si articola in quattro fasi: ricevere, valutare e affrontare le segnalazioni di illeciti, concludere casi di whistleblowing. Questo sistema si fonda sui principi di fiducia, imparzialità e protezione.
Si segnala che sia lo Standard ISO 37001 sui sistemi di Gestione Anticorruzione del 2016, sia la recente ISO 37301:2021 sui sistemi di gestione della Compliance, avevano già, in qualche modo, rilevato questo tema. La norma ISO 37301:2021 "*Compliance management systems – Requirements with guidance for use*" in particolare prevede degli specifici requisiti per progettare e mantenere, attraverso un miglioramento costante, un sistema di gestione della Compliance; è rivolta a tutti i tipi di organizzazioni, pubbliche, private, no profit, è certificabile ed infine conformemente ai nuovi standard ISO, ha una struttura HLS. All'interno vi sono richiami e principi relativi alla ISO 37001, Sistemi di gestione per la prevenzione della corruzione e alla ISO 37002:2021, norma che riguarda la gestione del nostro *whistleblowing*.

In conclusione

Affinché il canale di segnalazione possa ritenersi idoneo è necessario che sia riservato e inaccessibile sia all'interno che all'esterno dell'organizzazione e sia in grado di garantire la criptazione dei flussi informativi. Deve, inoltre, essere predisposto per consentire una comunicazione tra il segnalante ed il responsabile del *whistleblower* sullo stato della segnalazione. In particolar modo per tutelare la riservatezza è auspicabile che le segnalazioni siano conosciute da un numero ridotto di persone e, ancor meglio, che si proceda alla nomina di un responsabile del canale *whistleblowing* a cui venga accentrato il compito di analizzarle. A chi può essere attribuita questa responsabilità? Si tratta di una scelta che spetta all'azienda stessa, di norma è auspicabile affidare questa funzione internamente. Prendendo spunto dai modelli adottati negli Stati Uniti o in UK, si potrebbe pensare anche ad incentivare le segnalazioni attraverso ricompense. Diffusa, negli ordinamenti citati, è, ad esempio, la promessa di una promozione piuttosto che una ricompensa monetaria, il che potrebbe portare ad incentivare l'uso del meccanismo, recuperando effettivamente molte più notizie e informazione su condotte illecite, violazioni o irregolarità, e tale esigenza, si auspica, potrà essere ponderata, sempre di più, con una maggiore garanzia, sia per il segnalante così come per il segnalato.
Si tratta di assicurare il giusto equilibrio tra due contrapposte esigenze: la riservatezza del segnalante e il diritto di accesso al materiale raccolto contro di lui in capo al segnalato.

Il rientro al lavoro dopo la maternità: sfide e obiettivi

di Diletta Mora e Sebastiano Rapisarda

La nascita di un figlio rappresenta un momento unico e molto intenso nella vita di una donna, destinato a cambiare per sempre la vita. Oltre alla gioia della lieta notizia, spesso le future mamme si trovano ad affrontare una sfida importante, ovvero coniugare la maternità con il lavoro.
Diverse sono le difficoltà che possono emergere di carattere biologico, sociale e relazionale, nonché un notevole aumento dello stress, alterazione dell'umore e del ritmo sonno veglia.
Spesso capita che l'ambiente lavorativo attribuisca alla maternità caratteristiche negative, contribuendo a rendere il rientro al lavoro dopo il congedo di maternità un momento particolarmente delicato per le madri.
In virtù del loro status, le donne in dolce attesa e le neomamme dovrebbero godere di particolari tutele in ambito lavorativo. Per salvaguardare la loro salute e quella del bambino, ed evitare loro stress che potrebbe rivelarsi dannoso sul posto di lavoro, esistono numerosi strumenti a loro supporto, tra i quali la possibilità di modificare l'orario di lavoro, il congedo di maternità e il divieto di licenziamento.
In questo breve estratto ci concentreremo su un argomento tanto importante quanto discusso ovvero il ritorno al lavoro dopo la maternità.
Oggi come oggi, la vita lavorativa è fondamentale per evidenziare i diversi ruoli delle madri lavoratrici e per creare un'identità integrata che coniughi l'essere madre e al contempo lavoratrice[1]. Il rientro al lavoro dopo il congedo di maternità è una transizione comune nella vita delle donne che rappresenta una sfida importante sotto il profilo personale e lavorativo di ognuna di esse[2]. Tuttavia, la maternità è spesso considerata problematica dai datori di lavoro all'interno delle organizzazioni, motivo per cui spesso le donne hanno timore nell'annunciare la propria gravidanza al lavoro - o addirittura rimandano la scelta di diventare madri - perché hanno interiorizzato i messaggi più o meno impliciti di supervisori e colleghi sull'inadeguatezza della maternità nel contesto lavorativo e su ciò che questa potrebbe comportare[3].

1 *Kuleshova, 2015.*
2 *Wiese & Heidemeier, 2012.*
3 *Stumbitz et al., 2018.*

Le madri lavoratrici devono necessariamente dividere i loro sforzi tra l'essere una "buona madre", ovvero conformarsi alle norme sociali e alle aspettative condivise, ed essere una "lavoratrice efficiente", cioè mostrare competenze, impegno e attuare delle buone performance. Le madri che rientrano al lavoro dopo un congedo di maternità più o meno lungo, però, possono sperimentare sentimenti di inadeguatezza, domandandosi se saranno in grado di affrontare questa condizione sfidante che vede necessaria una riorganizzazione della vita familiare, nonché il riposizionamento all'interno della nuova situazione lavorativa, accogliendo eventuali nuovi membri del team o adattandosi a un ruolo diverso da quello svolto precedentemente[4].

In uno studio condotto nel 2018[5] alcune mamme lavoratrici nel settore sanitario, in riferimento al loro rientro al lavoro, hanno segnalato di aver sperimentato disturbi del sonno, demansionamento e atteggiamento ostile da parte dei colleghi. Tutte queste sfide rendono il rientro molto complesso, influendo negativamente sul benessere fisico e mentale nonché sullo sviluppo della propria carriera.

Dal punto di vista organizzativo le donne che scelgono di avere una gravidanza vengono tutt'oggi percepite come meno performanti, affidabili e degne di fiducia[6].

Un ruolo chiave e di supporto può svolgerlo il supervisore, il quale se assume comportamenti positivi rispetto al rientro al lavoro delle madri, è in grado di facilitare tale momento.

Il ritorno al lavoro è un processo in continua evoluzione che inizia quando la lavoratrice prende in considerazione l'idea di diventare mamma. Durante la gravidanza e in seguito al parto, le difficoltà diventano più concrete e prevedono necessariamente importanti scelte. Quando sono in congedo, alcune madri lavoratrici mantengono i contatti con il proprio supervisore e colleghi, anche per riuscire a preparare in maniera efficace il proprio rientro. A differenza di ciò che si potrebbe pensare, il ritorno al lavoro non termina con i primi giorni di rientro, ma quando le madri percepiscono (e vengono percepite) come completamente reintegrate nella vita organizzativa.

Un rientro al lavoro fallimentare porterebbe a conseguenze negative sia per le madri che per le organizzazioni: le prime sarebbero costrette a rinunciare sia alla soddisfazione sul lavoro che ai guadagni, le seconde si occuperebbero dei costi del turnover.

Una migliore pianificazione del rientro al lavoro dopo la maternità renderà semplice per l'organizzazione la gestione efficace del congedo[7].

4 *Greenberg et al., 2016.*

5 *Gottenborg et al., 2018.*

6 *Stumbitz et al., 2018.*

7 *Grether & Wiese, 2016.*

Le madri che percepiscono un maggiore sostegno da parte delle loro organizzazioni hanno maggiori probabilità di tornare effettivamente al lavoro dopo il congedo di maternità[8]. Un altro aspetto che influisce significativamente sul rientro riguarda la proposta di lavoro ridotto, suggerite dal supervisore; infatti, se le madri percepiscono che la proposta di lavoro flessibile non sia adeguatamente supportata, potrebbero mostrarsi titubanti nell'usufruire di tale opportunità nonostante rappresenti un vero e proprio diritto[9].

Esistono naturalmente molteplici fattori che possono influenzare il rientro al lavoro: lo stato di salute psicofisica del bambino e della madre, le problematiche economiche, la presenza di strutture che facilitino l'equilibrio tra lavoro e vita privata[10]. In uno studio del 2019 di Juengst e colleghi (2019), che analizzava le esperienze di rientro al lavoro di madri lavoratrici nel settore sanitaria, è stato evidenziato come la maggior parte di loro sentiva che il tempo di congedo fosse insufficiente. Inoltre, anche se molte madri avevano percepito il sostegno dei colleghi, hanno anche ricordato esperienze negative di rientro al lavoro associate alla mancanza di strutture per l'allattamento, nonché mancanza di opportunità di assistenza all'infanzia.

Esistono forti evidenze scientifiche rispetto all'importanza dei comportamenti positivi da parte del supervisore nella promozione del benessere dei dipendenti[11], del work engagement, della soddisfazione nel lavoro e nella vita e della performance lavorativa[12]. Esiste un'associazione positiva tra prudenza, temperanza, umanità, coraggio e giustizia da parte del supervisore e soddisfazione sul lavoro dei lavoratori[13]. Il supporto del supervisore risulta essere uno dei più importanti facilitatori del rientro al lavoro[14]; infatti, i supervisori che gestiscono efficacemente il rientro al lavoro influenzano sia la durata dell'assenza che le ricadute economiche per l'organizzazione. Tuttavia, la gestione di tale delicato momento non è un'attività semplice. Le competenze e le caratteristiche personali del supervisore sono molto importanti nella gestione di questa importante fase della vita per le madri; dovrebbero infatti mostrarsi empatici e onesti, cercando di comprendere quanto più possibile il punto di vista e le esigenze del dipendente. *Conditio sine qua* è la conoscenza dei processi e delle procedure, anche dal punto vista giuridico e legislativo relative al rientro al lavoro.

Come sopra delineato, la letteratura scientifica suggerisce come i comportamenti positivi del supervisore promuovano i processi motivazionali e l'impegno lavorativo, i quali, a loro volta, si associano positivamente alle buone performance lavorative e a una maggiore percezione di opportunità delle madri lavoratrici. I manager svolgono quindi un ruolo essenziale per la gestione dello stress lavoro-correlato ed è importante posseggano competenze che permettano loro di garantire un ambiente di lavoro positivo e di promuovere il benessere nella piena positività in modo efficace. Donaldson-Feilder e colleghi (2011) hanno individuato quattro competenze che ogni manager dovrebbe avere.

La prima competenza che un "buon manager" dovrebbe possedere è definita *Rispettoso e Rispettabile* ovvero il gestire le emozioni e avere l'integrità e si riferisce al modo in cui è necessario trattare i propri collaboratori. Quando si verificano situazioni di stress, il manager dovrebbe agire con calma, prevenendo ed eventualmente gestendo le situazioni critiche: è importante che assicuri delle scadenze realistiche fornendo al contempo dei feedback ai collaboratori e dipendenti.

L'approccio rispettoso è una delle carat-

8 *Coulson et al., 2012.*

9 *Kossek & Buzzanell, 2011; Shanmugam & Agarwal, 2019.*

10 *Van Niel et al., 2020.*

11 *He et al., 2019; Shin & Hur, 2020.*

12 *De Carlo, Dal Corso et al., 2020.*

13 *Hendriks et al., 2020.*

14 *Ansoleaga et al., 2015; Janssen et al., 2003; Jetha et al., 2018.*

teristiche più importanti che un manager positivo deve possedere e consiste nell'elogiare il buon lavoro, riconoscendo l'impegno del lavoratore.
La seconda competenza, *Gestire e comunicare il lavoro esistente e quello futuro*, si riferisce alla gestione proattiva del manager, il quale dovrebbe essere in grado di gestire il lavoro proprio e dei suoi dipendenti, coinvolgendoli il più possibile nel processo decisionale e nelle problematiche interne. Per comportamento proattivo s'intende lo sviluppo di piani d'azione, comunicando con chiarezza gli obiettivi; il monitoraggio del carico di lavoro del team, spronandolo a rivedere l'organizzazione del proprio lavoro e a dare le adeguate priorità ai futuri carichi di lavoro. Inoltre, individuare il problema e le cause, indentificare le possibili soluzioni e metterle in atto.
La gestione del singolo all'interno del team è la terza competenza che un manager dovrebbe possedere. Quest'ultimo, deve mostrarsi: accessibile personalmente, ovvero cercare di essere disponibile e accessibile per i propri dipendenti; socievole, essere sufficientemente amichevole nei confronti del proprio team al fine di ottenere maggiore fiducia; empatico, sforzarsi di comprendere come si sente l'altra persona e cosa la spinge a comportarsi in un determinato modo.
L'ultima competenza proposta dagli autori è definita *Comprensione/gestione delle situazioni difficili* e ne fanno parte comportamenti non quotidiani, ma che possono venire attuati in presenza di situazioni complesse come conflitti, presenza di mobbing o vessazione. È fondamentale che il manager sappia gestire tali situazioni utilizzando le risorse organizzative e assumendosi la responsabilità e laddove necessario chiedendo l'intervento e l'aiuto degli altri dirigenti o usufruendo dei servizi messi a disposizione, ad esempio, il servizio di Risorse Umane o quelli afferenti alla Psicologia del lavoro.
Una volta chiarite le competenze necessarie, i manager hanno il compito di modificare il loro approccio manageriale al fine di includere i comportamenti utili a rendere l'organizzazione positiva e promuovere il benessere organizzativo.
All'interno di un'organizzazione funzionale il supervisore dovrebbe mostrare dunque disponibilità a considerare gli adattamenti lavorativi e a rendere il rientro al lavoro il meno stressante possibile, promuovendo uno spirito di squadra nei confronti delle madri lavoratrici; anche il saper ascoltare eventuali loro preoccupazioni contribuirà a renderle più coinvolte e performanti.
Il presente articolo vuole fornire una panoramica delle buone prassi relative al rientro al lavoro dopo la maternità, suggerendo alle organizzazioni come pianificare al meglio il rientro e il lavoro delle madri. Ad esempio, la condivisione dei bisogni e delle aspettative tra supervisore e madre lavoratrice, così come una comunicazione positiva e regolare, è un aspetto cruciale per gestire un rientro al lavoro efficace, in particolare in termini di impegno lavorativo, prestazioni lavorative e opportunità occupazionali percepite.
La formazione per i supervisori è consigliabile, ma non sufficiente: è importante che la cultura si diffonda in tutta l'organizzazione e che, come una cascata, coinvolga ogni stakeholder, dal top management alla bottom line. Nessun intervento organizzativo può essere efficace senza il coinvolgimento del top management[15].
Trattandosi di un periodo cruciale per molte donne, è fondamentale sviluppare le risorse personali che permettano di affrontare il rientro al lavoro in modo efficace. Particolarmente utili possono essere gli interventi volti a migliorare le capacità di gestione dello stress[16]. Al giorno d'oggi, questi interventi possono sfruttare tecnologie innovative, come la realtà virtuale[17]. Ulteriori strategie utili sono il networking, fondamentale per condividere le difficoltà nell'integrazione tra il lavoro, la vita privata e le prospettive di carriera futura, concedendosi la possibilità di parlare e confrontarsi con altre persone significative per cercare di sfatare i miti legati a ciò che una "buona madre" dovrebbe e non dovrebbe fare[18]. Più in generale, interventi efficaci dovrebbero mirare a rafforzare le risorse a disposizione delle lavoratrici ai vari livelli, prendendo in considerazione non solo l'individuo e il supervisore, ma anche il gruppo, l'organizzazione e il contesto sociale complessivo, sia lavorativo e che familiare.

15 *Girardi et al., 2018.*
16 *Dal Corso et al., 2013.*
17 *De Carlo, Carluccio et al., 2020.*
18 *Greenberg et al., 2016.*

BIBLIOGRAFIA

Ali, M., Aziz, S., Pam, T. N., Babalola, M. T., & Usman, M. (2020). A positive human health perspective on how spiritual leadership weaves its influence on employee safety performance: The role of harmonious safety passion. *Safety Science, 131*, 104923.
Ansoleaga, E., Garrido, P., Domínguez, C., Castillo, S., Lucero, C., Tomicic, A., & Martínez, C. (2015). Facilitadores del reintegro laboral en trabajadores con patología mental de origen laboral: Una revisión sistemática [Return to work enablers for workers with work-related mental illness]. *Revista Médica de Chile, 143*, 85-95.
Coulson, M., Skouteris, H., & Dissanayake, C. (2012). The role of planning, support, and maternal and infant factors in women's return to work after maternity leave. *Family Matters, 90*(1), 33-44.
Dal Corso, L., Floretta, P., Falco, A., Benevene, P., & De Carlo, A. (2013). The repertory grid technique in a research-intervention on work-related stress. *TPM – Testing, Psychometrics, Methodology in Applied Psychology, 20*(2), 155-168.
Dal Corso, L., Carluccio, F., Barbieri, B., & De Carlo, N. A. (2020, April). *Positive motherhood at work: The role of supervisor support in return to work after maternity leave* [Paper presentation]. Proceedings of the International Psychological Applications Conference and Trends – InPACT2020, Madeira, Portugal.
De Carlo, A., Dal Corso, L., Carluccio, F., Colledani, D., & Falco, A (2020). Positive supervisor behaviors and employee performance: The serial mediation of workplace spirituality and work engagement. *Frontiers in Psychology, 11*, 1834.
De Carlo, A., Carluccio, F., Rapisarda, S., Mora, D., & Ometto, I. (2020). Three uses of Virtual Reality in work and organizational psychology interventions - A dialogue between Virtual Reality and organizational well-being: Relaxation techniques, personal resources, and anxiety/depression treatments. *TPM – Testing, Psychometrics, Methodology in Applied Psychology, 27*(1), 129-143.
Donaldson-Feilder, E., Yarker, J., & Lewis, R. (2011). *Preventing Stress in Organizations: How to Develop Positive Managers*. John Wiley and Sons Ltd.
Girardi, D., Falco, A., De Carlo, A., Dal Corso, L., & Benevene, P. (2018). Perfectionism and workaholism in managers: The mod-

erating role of workload. *TPM – Testing, Psychometrics, Methodology in Applied Psychology, 25(*4), 571-588.
Gottenborg, E., Maw, A., Ngov, L. K., Burden, M., Ponomaryova, A., & Jones, C.D. (2018). You can't have it all: The experience of academic hospitalists during pregnancy, parental leave, and return to work. *Journal of Hospital Medicine, 13*(12), 836-839.
Greenberg, D.N., Clair, J.A., & Ladge, J. (2016). Identity and the transition to motherhood: Navigating existing, temporary, and anticipatory identities. In C. Spitzmueller & R.A. Matthews (Eds.), *Research Perspectives on Work and the Transition to Motherhood* (pp. 33-55). Springer International Publishing.
Grether, T., & Wiese, B.S. (2016). Stay at home or go back to work? Antecedents and consequences of mothers' return to work after childbirth. In C. Spitzmueller & R.A. Matthews (Eds.), *Research Perspectives on Work and the Transition to Motherhood* (pp. 105-128). Springer International Publishing.
He, J., Morrison, A. M., & Zhang, H. (2019). Improving millennial employee well-being and task performance in the hospitality industry: The interactive effects of HRM and responsible leadership. *Sustainability, 11,* 4410.
Hendriks, M., Burger, M., Rijsenbilt, A., Pleeging, E., & Commandeur, H. (2020). Virtuous leadership: A source of employee well-being and trust. *Management Research Review, 43*(8), 951-970.
Janssen, N., Van Den Heuvel, W.P.M., Beurskens, A.J.H.M., Nijhuis, F.J.N., Schröer, C.A.P., & Van Eijk, J.T.M. (2003). The demand-control-support model as a predictor of return to work. *International Journal of Rehabilitation Research, 26*(1), 1-9.
Jetha, A., LaMontagne, A.D., Lilley, R., Hogg Johnson, S., Sim, M., & Smith, P. (2018). Workplace social system and sustained return-to-work: A study of supervisor and co-worker supportiveness and injury reaction. *Journal of Occupational Rehabilitation, 28,* 486-494.
Juengst, S.B., Royston, A., Huang, I., & Wright, B. (2019). Family leave and return-to-work experiences of physician mothers. *JAMA Network Open, 2*(10), e1913054.
Kuleshova, A. (2015). Dilemmas of modern motherhood (based on research in Russia). *Economics and Sociology, 8(*4), 110-121.
Kossek, E. E., & Buzzanell, P. M. (2011). Women's career equality and leadership in organizations: Creating an evidence-based positive change. *Human Resources Management, 57*, 813-822.
Mukaihata, T., Fujimoto, H., & Greiner, C (2020). Factors influencing work engagement among psychiatric nurses in Japan. *Journal of Nursing Management, 28(*2), 306-316.
Shanmugam, M.M., & Agarwal, B. (2019). Support perceptions, flexible work options and career outcomes. A study of working women at the threshold of motherhood in India. *Gender in Management, 34*(4), 254-286.
Shin, Y., & Hur, W.M. (2020). Supervisor incivility and employee job performance: The mediating roles of job insecurity and amotivation. *The Journal of Psychology Interdisciplinary and Applied, 154*(1), 38- 59.
Stumbitz, B., Lewis, S., & Rouse, J. (2018). Maternity management in SMEs: A transdisciplinary review and research agenda. *International Journal of Management Reviews, 20*, 500-522.
Van Niel, M.S., Bhatia, R., Riano, N.S., De Faria, L., Catapano-Friedman, L., Ravven, S., Weissman, B., Nzodom, C., Alexander, A., Budde, K., & Mangurian, C. (2020). The impact of paid maternity leave on the mental and physical health of mothers and children: A review of the literature and policy implications. *Harvard Review of Psychiatry, 28*(2), 113-126.
Wiese, B.S. & Heidemeier, H. (2012). Successful return to work after maternity leave: Self-regulatory and contextual influences. *Research in Human Development, 9(*4), 317-336.
Yang, C., Chen, Y., Zhao, X., & Hua, N. (2020). Transformational leadership, proactive personality and service performance: The mediating role of organizational embeddedness. *International Journal of Contemporary Hospitality Management, 32*(1), 267-287.

Endpoint Protection e protezione dell'identità digitale: le nuove sfide della security in un mondo digitale diffuso

di Giovanni Finetto e Paola Finetto

Fino all'avvento della cosiddetta "Era Covid" abbiamo beneficiato di una netta separazione tra ciò che si trovava all'interno di una rete aziendale, considerato affidabile, e ciò che era al di fuori di essa, considerato un rischio. Questa separazione era favorita anche da una sorta di sicurezza fisica del perimetro: le risorse di rete erano accessibili esclusivamente dall'interno dell'azienda: senza entrare fisicamente nei locali aziendali, non c'era possibilità di accesso alla rete, se non per rare eccezioni, tramite Virtual Private Network (VPN), normalmente per compiti di supervisione da parte degli IT aziendali.

La pandemia, unitamente alle possibilità date dalle nuove tecnologie di trasformazione digitale, ha cambiato radicalmente l'architettura dei sistemi. Dall'uso ormai esteso degli accessi tramite VPN alle applicazioni e infrastrutture ospitate nel cloud, i confini del perimetro della rete sono svaniti così rapidamente che non ha quasi più senso limitare la protezione aziendale al perimetro fisico della rete aziendale. An-

che l'uso di dispositivi personali per scopi lavorativi (*Bring Your Own Device*) contribuisce al dissolversi dei confini delle reti aziendali e a richiedere ulteriori misure di sicurezza, con due priorità per gli IT Manager in termini di tutela dell'accesso remoto:
• autenticazione;
• autorizzazione degli utenti.

Utilizzando tunnel sicuri e criptati, l'azienda permette al dipendente di accedere alle risorse aziendali e trasferire dati al sicuro da attacchi *Man In The Middle* (MITM). Il compito di identificare e autenticare i dipendenti, invece, è gestito tramite strumenti di connettività remota e soluzioni *Multi Factor Authentication*. Esiste inoltre un modello, denominato *zero trust*, in cui si verifica fondamentalmente tutto: accessi, identità e permessi in ogni punto di accesso alla rete, anche qualora l'utente si trovi all'interno della rete aziendale. Se l'utente si autentica come previsto dalle procedure adottate, è considerato "affidabile". Alcuni professionisti del settore sono addirittura dell'opinione che questo sistema di verifica non sia sufficiente: secondo questo orientamento, l'approccio *zero-trust* non può limitarsi solo all'accesso alla rete aziendale; è l'intera strategia di protezione che deve necessariamente includere l'identificazione di utenti e dispositivi, l'autenticazione a più fattori e la gestione degli accessi. I permessi di accesso andrebbero assegnati in base al tipo di dispositivo in uso, dotazione professionale o personale, al software utilizzato, al livello di attualità della soluzione di sicurezza sul dispositivo, o anche in base alla posizione dell'utente (casa, ufficio, in viaggio, ecc.).

Per le ragioni sopra esposte, le soluzioni di protezione delle *workstation* devono supportare politiche di sicurezza contestuali ed essere in grado di adattare dinamicamente all'ambiente il livello di sicurezza fornito: l'identità diventa quindi il nuovo perimetro di sicurezza.

Un primo sistema di protezione è il software antivirus: un'applicazione o una suite di programmi che trova e rimuove virus su computer e reti. Oltre ai virus, quasi tutti i programmi antivirus odierni sono anche in grado di rilevare e rimuovere altri tipi di software malevolo, tra cui *worm, trojan, adware, spyware, ransomware, browser hijacker, keylogger* e *rootkit*.
Poiché i virus informatici rappresentano una minaccia costante su tutte le piattaforme, i software antivirus di oggi sono pensati per proteggere tutti i sistemi operativi e tutti i dispositivi connessi a Internet, tra cui computer desktop e portatili con Microsoft Windows e macOS, nonché smartphone con iOS e Android. Tutti i programmi antivirus possono essere organizzati nelle seguenti categorie:

a) Software antivirus *free*:
• Molte persone cercano soluzioni online per spendere il meno possibile; effettivamente, online vengono pubblicizzati numerosi sistemi gratuiti, che spesso, tuttavia, non proteggono affatto, ma sono solo "*banner*" pubblicitari e servono alle aziende produttrici per testare sul campo qualche specifica caratteristica del sistema. Recentemente due storici brand produttori di software hanno iniziato a proporre un servizio dalle caratteristiche discutibili: da qualche mese questi player stanno integrando nelle installazioni un "*cryptominer*" per generare una moneta chiamata *Ethereum*, pubblicizzando potenziali guadagni da parte dei clienti ma, in realtà, nascondendo la notevole spesa aggiuntiva nelle bollette di energia elettrica.
b) Software antivirus a pagamento:
• Software antivirus *standalone*: il software antivirus *standalone* è uno strumento specializzato, progettato per rilevare e rimuovere determinati virus. Viene comunemente indicato come software antivirus portatile, perché l'amministratore del sistema può installarlo su una unità USB per eseguire una scansione di emergenza di un sistema infetto. Tuttavia, quasi nessun programma portatile è pensato per fornire protezione in tempo reale e scaricare quotidianamente nuove definizioni di virus, motivo per cui non può sostituire le suite di sicurezza Internet, che includono numerose funzionalità aggiuntive.
• Suite di sicurezza: le suite di sicurezza, oltre a essere in grado di rilevare e rimuovere i virus, sono anche equipaggiate per contrastare tutti gli altri software malevoli e per fornire protezione continua al computer e ai file. La maggior parte di questi pacchetti di programmi include *antispyware*, *firewall* e controllo parentale; alcune suite dispongono anche di funzionalità aggiuntive, come password manager, VPN e perfino programmi antivirus *standalone*.
• Software antivirus basato sul cloud: il software antivirus basato su cloud è una tecnologia antivirus relativamente nuova, che analizza i file nel cloud piuttosto che sul computer, in modo da liberare le risorse di calcolo e consentire una risposta più rapida. Questi programmi di solito sono costituiti da due parti: il *client* installato sul computer, che esegue scansioni periodiche di virus e *malware* senza occupare troppa memoria, e il servizio web che elabora i dati raccolti dal *client* e li ispeziona alla ricerca di corrispondenze nel suo database di *malware* e virus.
• Software antivirus sul cloud e suite di sicurezza centralizzati (*Endpoint protection Systems*): permette di integrare le tecnologie sopra citate e di avere una console centralizzata per controllare da remoto l'andamento delle operazioni di sicurezza.
• Software antivirus sul cloud e suite di sicurezza centralizzati (*Endpoint protection Systems*) gestiti da un *Cyber Security Operation Centre* (C-SOC): permette di integrare le tecnologie sopra citate e di avere una console centralizzata per monitorare da remoto l'andamento delle operazioni di sicurezza. Le attività di verifica vengono effettuate in outsourcing in tempo reale da un C-SOC con analisti in grado di effettuare interventi tempestivi e analisi forensi di 1° livello per comprendere l'origine dell'eventuale attacco informatico. È necessario che la suite di *Endpoint Protection* scelta per la propria organizzazione abbia la possibilità di fornire i seguenti servizi, ormai considerati come essenziali e irrinunciabili ai fini di una completa dotazione di sicurezza:
- protezione in tempo reale: consente di rilevare le minacce nei file aperti e di esaminare le app durante l'installazione nel dispositivo in tempo reale;
- rimozione dei *malware/spyware/adware*: capacità di rilevare, rimuovere e bloccare *ransomware*, trojan, virus e altri elementi dannosi o indesiderati;
- protezione da *ransomware* appositamente progettata: la maggior parte dei *ransomware* non colpisce due volte, nel senso che se un PC è già stato infettato (e i documenti criptati), quel PC non verrà infettano nuovamente. Il software di Anti-Ransomware inganna i controlli dei *ransomware* in modo che questi rilevino il PC come già infettato e, quindi, si disattivino o, comunque, non inizino a criptare i documenti della vittima;
- anti-phishing/anti-frode: sistemi di filtraggio anti-phishing e anti-frode che impediscono di accedere a siti dannosi;
- modalità recupero: quando l'antivirus ri-

leva una minaccia, che non può essere rimossa, richiede il riavvio del computer in modalità Soccorso per la pulizia e il ripristino. Basta fare "clic" su Riavvia in Ambiente soccorso al termine della scansione;
- EDR: la capacità di *Endpoint Detection and Response* estende le capacità di analisi e correlazione degli eventi oltre i confini di un singolo endpoint per consentire di affrontare con maggiore efficacia attacchi informatici complessi, che interessano più endpoint. Fornendo una visualizzazione delle minacce a livello organizzativo, aiuta a concentrare le indagini e a rispondere in maniera più efficace;
- VPN: una *Virtual Private Network* veloce che protegga l'identità e le attività online da attacchi malevoli;
- banking online sicuro: è un browser protetto, un ambiente isolato, progettato per mantenere le operazioni bancarie, gli acquisti e altri tipi di transazioni online assolutamente sicuri e privati;
- protezione Webcam: garantisce un monitoraggio continuo di tutti i processi e le applicazioni aperti nel computer e ne controlla l'accesso alla webcam. Nel caso in cui un processo e/o un'applicazione cerchino di accedere alla webcam, la funzione avviserà e sarà possibile bloccarli;
- avvertenze sui contenuti non adatti ai minori: un controllo genitoriale avanzato per monitorare con discrezione le attività online dei minori;
- scanner di vulnerabilità: programma progettato per ricercare e mappare le debolezze di un'applicazione, di un computer o di una rete;
- *firewall*: componente hardware e/o software di difesa perimetrale di una rete, originariamente passivo, che può anche svolgere funzioni di collegamento tra due o più segmenti di rete, fornendo dunque una protezione in termini di sicurezza informatica della rete stessa;
- modalità silenziosa: è un tipo di modalità che blocca temporaneamente i processi in background e sopprime le notifiche o avvisi di sicurezza in esecuzione. Il software antivirus sarà ancora la protezione del computer da malware, mentre è in modalità silenziosa, ma non riceverà alcun popup, e il software non condurrà le scansioni in background;
- protezione sui social network e identità digitale: consente agli utenti di proteggersi dal sempre maggior numero di ladri di dati e truffatori, che usano le informazioni personali, reperibili nel web, per danneggiare la reputazione, prendere il controllo degli account personali o sottrarre denaro;
- strumenti per la gestione delle password: sono programmi e app che archiviano in modo sicuro e crittografato le credenziali (username e password) di accesso ai servizi web (e non solo) in una sorta di cassaforte ("*Vault*") virtuale, rendendola disponibile all'utente quando ne avrà bisogno;
- antifurto: è possibile localizzare, bloccare, cancellare o inviare un messaggio in remoto al dispositivo in caso di smarrimento o furto. Inoltre, il telefono Android è in grado di autodifendersi: scattare una foto segnaletica di chiunque cerchi di manometterlo in sua assenza e invio per e-mail;
- cancellazione definitiva dei dati: permette di eseguire questa procedura senza possibilità di recupero degli stessi;
- modalità batteria: il profilo "Modalità Batteria" è stato progettato appositamente per gli utenti di computer portatili e tablet. Il suo scopo è ridurre al minimo l'impatto del sistema sul consumo energetico, quando il livello di carica della batteria è inferiore a quello predefinito o selezionato;
- *Patch management*: *Patch*, in informatica, indica una porzione di software progettata per aggiornare o migliorare un programma. Ciò include la risoluzione di vulnerabilità di sicurezza e altri bug generici: tali *patch* vengono anche chiamate *fix* o *bugfix*. Il termine è solitamente associato a un piccolo aggiornamento;
- IDS/IPS: gli *Intrusion Detection/Prevention systems*, sono componenti software attivi sviluppati per incrementare la sicurezza informatica di un sistema informatico, individuando e registrando le informazioni relative e tentando di segnalare e bloccare le attività dannose;
- supporto telefonico: assistenza in caso di misconfigurazioni o problemi;
- chat dal vivo: gli operatori si occupano dal vivo della richiesta, accesso rapido con tempi di risposta molto veloci;
- Mac/Windows/Linux/Android/iOS: interoperabilità per un parco dispositivi variegato.

La sicurezza informatica – delle reti, dei sistemi, dei dati – è sicuramente il tema dei prossimi decenni, poiché ancora oggi essa identifica l'insieme degli asset tecnologici, che hanno il fine di proteggere le strutture telematiche in termini di disponibilità, confidenzialità e integrità. In questo ambito rientrano, oltre agli apprestamenti tecnici sopra descritti, anche procedure, protocolli e comportamenti, che siano tutti conformi a standard di sicurezza quantomeno essenziali. Il punto di partenza, per identificare le misure di sicurezza in concreto necessarie per la specifica organizzazione, è pur sempre costituito dall'attività di *risk assessment*: è necessario mappare i rischi, valutare la superficie di attacco e ricercare eventuali minacce ai sistemi informativi, al fine di creare un perimetro di sicurezza, che li protegga da attacchi sia esterni che interni, che potrebbero provocare impatti importanti all'organizzazione o ad organizzazioni terze (si pensi, ad esempio, al rischio residuo economico, sociale, di *brand reputation*). A questo riguardo, indicazioni anche operative significative provengono dal Garante europeo per la protezione dei dati (*European Data Protection Supervisor* – EDPS), così come dall'Agenzia europea per la cybersicurezza (*European Union Agency for Cybersecurity* – ENISA).

Il 28 giugno 2021, l'ENISA ha pubblicato la relazione "*Cybersicurezza per le PMI: sfide e raccomandazioni*", accompagnandola con un decalogo di 12 buone pratiche per proteggere sistemi e attività:
1) sviluppare una solida cultura della cybersicurezza;
2) fornire una formazione appropriata;
3) garantire un'efficace gestione dei terzi;
4) sviluppare un piano di risposta agli incidenti;
5) rendere sicuro l'accesso ai sistemi;
6) rendere sicuri i dispositivi (e, in questo contesto, con specifico riferimento alle soluzioni antivirus, *si consiglia di attuare una soluzione antivirus gestita a livello centrale su tutti i tipi di dispositivi e aggiornarla per assicurarne l'efficacia continua e di evitare di installare un software pirata perché potrebbe contenere malware*);
7) rendere sicura la propria rete;
8) migliorare la sicurezza fisica;
9) rendere sicuri i backup;
10) lavorare con il cloud;
11) rendere sicuri i siti online;
12) cercare e condividere le informazioni.
L'osservanza di queste buone pratiche può senz'altro sviluppare le caratteristiche di robustezza, capacità di reazione e resilienza, che ciascun sistema tecnologico-informativo deve possedere *by design* per affrontare attacchi cyber mirati.

Il Garante europeo, da parte sua, si propone di operare ed effettivamente opera, anche a supporto dei Garanti Privacy nazionali, al fine precipuo di:
• monitorare lo sviluppo tecnologico, in particolare laddove esso possa incidere sulla

protezione dei dati personali (*cloud computing*, PIMS, Big Data, *malicious* software);
• analizzare e identificare il potenziale impatto di politiche centrate sulla tecnologia e delle relative misure di carattere normativo;
• segnalare ogni nuova funzionalità tecnologica che possa riguardare la protezione dei dati e favorire il confronto e il dibattito al riguardo;
• supportare le istituzioni europee, i Garanti privacy nazionali e, più in generale, il pubblico degli utenti, nel fornire chiarimenti in merito a questioni afferenti le nuove tecnologie e la protezione dei dati;
• disporre della conoscenza e delle risorse tecnologiche, che consentano un check specifico su sistemi IT e altre soluzioni tecnologiche, che possano, per le loro caratteristiche, comportare un trattamento di dati personali;
• dare indicazioni, accrescere la consapevolezza e fornire chiarimenti con riferimento a qualsivoglia sviluppo tecnologico, che possa incidere sulla protezione dei dati personali, così da favorire l'applicazione corretta dei principi della *privacy by design* e della *privacy by default*.

Si comprende, dunque, come la gestione del rischio informatico richieda una visione omnicomprensiva della sicurezza, che permetta di spostare l'attenzione da un problema contingente ad una visione ben più ampia, nella quale devono essere presi in considerazione e valutati costantemente molteplici fattori. È importante proteggere ogni segmento della operatività, anche e soprattutto aziendale, che, se compromesso, possa portare a una perdita economica, di immagine o di reputazione. Come già si è sopra evidenziato, i sistemi e le reti, che sono utilizzati nella quotidianità operativa aziendale, sono naturalmente esposti a molte e diverse vulnerabilità, l'analisi delle quali costituisce una criticità nel processo di valutazione e mitigazione dei rischi. A fronte della sempre maggiore diffusione di tecnologie e modelli di business basati sulla rete, dove vengono possedute e scambiate informazioni anche sensibili o riservate, l'adozione di efficienti ed efficaci strumenti di *vulnerability management* assume rilevanza cruciale, in quanto da essa possono dipendere le sorti stesse dell'organizzazione. Con specifico riferimento alla protezione dei dati personali, ad esempio, è l'art. 32 del GDPR (Regolamento UE 679/2016) a imporre al titolare del trattamento di dotarsi di misure tecnico-organizzative, che garantiscano la sicurezza dei trattamenti effettuati e, conseguentemente, degli stessi dati trattati; l'imprenditore dovrà, dunque, dotarsi di strumenti tecnologici, applicativi, software che soddisfino i requisiti di cui alla norma citata. È fondamentale, infatti, essere preparati ad affrontare e, all'occorrenza, gestire un attacco informatico. Tutto ciò fa comprendere l'importanza di affidare ad un C-SOC esterno le operazioni di security della rete, al fine di esternalizzare il rischio, ma pure per avere risorse specializzate nella gestione in tempo reale di situazioni critiche onde ottenere una *Common Operational Picture* del nostro stato di sicurezza.

Testo Unico sul Biologico: Marchio Volontario Nazionale, un Fondo a sostegno dello sviluppo della pratica agricola e un po' di disciplina anche sul biodinamico

di Olga Bussinello

In lavorazione dal 2018 e approvato definitivamente alla Camera il 9 febbraio scorso, il TU sul biologico si pone quale sintesi ragionata della regolamentazione preesistente e frammentata di questa pratica di produzione agricola. Grazie alla crescente richiesta da parte dei consumatori di cibi green e più salutari, la disciplina tocca ogni ambito e settore agroalimentare per preservare la fiducia di chi compra e la qualità finale del prodotto.

Il comparto italiano della produzione biologica da alcuni anni gioca un ruolo importante nell'agroalimentare nazionale, favorendo lo sviluppo del "Made in Italy" nel mondo. In 21 articoli, il legislatore italiano riorganizza e in parte rinnova la regolamentazione di un sistema complesso qual è quello biologico in agricoltura e acquacoltura. Complesso, perché frutto di una stratificazione normativa, che, negli anni, ha prodotto zone grigie ed interpretazioni "non autentiche". La produzione biologica è definita "un sistema globale di gestione dell'azienda agricola e di produzione alimentare, che utilizza le migliori prassi in materia di ambiente, di azione per il clima e di salvaguardia delle risorse naturali". Essa applica norme rigorose di produzione, contribuendo alla qualità dei prodotti, alla sicurezza alimentare, al benessere degli animali, allo sviluppo rurale, alla tutela dell'ambiente e dell'ecosistema, alla salvaguardia della biodiversità e al raggiungimento degli obiettivi di riduzione dell'intensità delle emissioni di gas a effetto serra previsti dagli obiettivi dell'Agenda 2030 per lo sviluppo sostenibile. Il punto di partenza sono i soggetti che fanno parte del sistema singoli ed aggregati, l'inclusione della produzione Biodinamica, le competenze delle autorità di controllo e l'operatività della filiera. Il punto di arrivo è il Marchio Unico Nazionale.

Autorità Nazionali, Locali e Organismi Competenti

L'attività di indirizzo e di coordinamento spetta al MIPAAF quale Autorità Nazionale di riferimento, mentre, quella tecnico-scientifica ed amministrativa relativa alla produzione biologica spetta alle Regioni e Province Autonome. Questo significa che, a differenza di quanto previsto nella disciplina normativa precedente, le Autorità locali si occuperanno delle attività amministrative relative alla pratica del metodo biologico, ma anche di quelle tecnico-scientifiche che, invece, prima venivano gestite dal CREA e dal CNR, Enti vigilati e controllati dallo Stato, per le rispettive competenze. Questo, non solo assicurava una visione di ampio respiro alle attività di ricerca e sperimentazione, spesso supportata dalla collaborazione dell'Università, ma garantiva anche un controllo centralizzato di tali attività e programmi, che sono sempre finanziati con risorse pubbliche Nazionali o europee. Il Governo dovrà poi, entro 18 mesi dall'entrata in vigore del TU, riassettare il sistema dei controlli, attraverso molteplici Decreti Legislativi che ridefiniscano più puntualmente la materia delle verifiche ufficiali, della tracciabilità nel processo produttivo e le garanzie di trasparenza sull'informazione dei consumatori. Fra gli obbiettivi principali ci sarà: una integrazione delle norme del decreto legislativo n. 20/2018 per adeguarlo alle nuove disposizioni; una disciplina più stringente nei rapporti fra controllori e controllati per evitare conflitti di concorrenza; maggiori informazioni circa la provenienza, la qualità e la tracciabilità dei prodotti biologici, anche mediante l'impiego di piattaforme digitali a tutela dei consumatori; riordino della normativa in materia di frodi alimentari, ridefinendo e risistemando i confini fra le fattispecie delittuose, contravvenzionali e di illecito amministrativo, con contestuale revisione della disciplina sanzionatoria vigente. Se lo sviluppo tecnologico del sistema di controlli, in uno con una necessaria crescita culturale delle aziende produttrici, incontra il favore delle Autorità Nazionali e degli Enti di Certificazione, questi ultimi ritengono essenziale far confluire tutte le specifiche sulla Certificazione del metodo biologico all'interno del decreto legislativo n. 20/2018. Le ragioni non sono solo di comodità esegetica, ma anche di organizzazione e chiarezza operativa.

Distretti Biologici, Aggregazioni tra i Produttori e gli Altri Soggetti della Filiera

L'articolo 13 del TU si occupa dei distretti biologici, già disciplinati dall'articolo 13 del decreto legislativo 18 maggio 2001, n. 228, che annovera i distretti biologici e i biodistretti tra i distretti del cibo. Secondo la nuova definizione, anche i sistemi produttivi locali, sia di carattere sovracomunale, che interprovinciale, o interregionale, purché a spiccata vocazione agricola, possono essere considerati distretti biologici purché la componente biologica sia significativa nella coltivazione, nell'allevamento, nella trasformazione o nella preparazione alimentare, all'interno del territorio individuato dal biodistretto. Essi devono godere, al loro interno, di una situazione di integrazione con le altre attività economiche pre-

senti nell'area del distretto stesso e della presenza di aree paesaggisticamente rilevanti, comprese le aree naturali protette nazionali e regionali (vedi legge n. 394/1991) o le aree comprese nella rete «Natura 2000» (vedi DPR 8 settembre 1997, n. 357). Nel biodistretto è limitato o vietato l'uso dei prodotti fitosanitari e l'utilizzo di diserbanti per la pulizia delle strade e delle aree pubbliche, prevedendo agevolazioni compensative per le imprese. Gli agricoltori convenzionali che si trovano nell'area amministrativa del biodistretto devono adottare ogni pratica necessaria per impedire l'inquinamento accidentale delle coltivazioni biologiche. Con successivo DM del MIPAAF, ne verrà disciplinata l'operatività, a partire dai requisiti e dalle condizioni per la loro costituzione. Gli scopi del biodistretto sono ampi e riguardano tutti i soggetti che risultano coinvolti dal comprensorio: i produttori, a cui si chiede di impegnarsi nella promozione della conversione alla produzione biologica e nell'uso sostenibile delle risorse naturali e locali nei processi produttivi agricoli, ma anche nel garantire la tutela degli ecosistemi e di un'economia circolare; gli abitanti e le aziende del biodistretto, perché convertano le proprie abitudini e le proprie attività alla conservazione delle risorse naturali, dell'ambiente della salute e delle diversità locali; le autorità locali, perché semplifichino i processi di certificazione biologica, ambientale e territoriale, favoriscano la crescita delle attività multifunzionali collegate, incentivino la commercializzazione dei prodotti bio. Molte parti del TU approvato alla Camera sono in linea con le richieste delle Associazioni Nazionali Biologiche preoccupate di cristallizzare fina da subito i requisiti minimi di indirizzo per la disciplina di dettaglio che verrà fissata nei decreti attuativi che seguiranno. Fra i temi più caldi su cui, in tre anni di lavoro, si è trovata la sintesi ci sono: la "significatività" della produzione primaria bio nel territorio del Distretto Biologico con criteri che evitino disomogeneità dannose al sistema; l' uso "parsimonioso" dei pesticidi in campo e dei diserbanti per la pulizia delle strade e delle aree pubbliche, stabilendo norme premianti per chi non vi ricorre; l'attenzione da parte degli agricoltori convenzionali, con misure tecniche e/o meccaniche, per impedire l'inquinamento accidentale delle coltivazioni biologiche; la riduzione generalizzata dell'uso dei pesticidi e della plastica; nessun compenso o rimborso di spesa ai membri del Comitato Direttivo del Distretto perché ruolo politico e non manageriale; l'inserimento dei biodistretti fra i soggetti beneficiari con priorità di accesso nei finanziamenti pubblici. Tema in divenire, non con qualche perplessità, è quello delle organizzazioni professionali biologiche e di filiera. Per il riconoscimento, a cura del MIPAAF, l'oggetto sociale deve prevedere il miglioramento della conoscenza e della trasparenza della produzione e del coordinamento delle modalità di immissione dei prodotti sul mercato, nonché la valorizzazione dei prodotti biologici. Sarà possibile una sola organizzazione interprofessionale a livello nazionale o una a livello di circoscrizione economica. I requisiti per ottenere il riconoscimento prevedono: una quota dell'attività economica pari ad almeno il 30% del valore dei prodotti della filiera biologica nazionale, ovvero, se il criterio è la circoscrizione economica, il 40% del valore dell'area per operare nello stesso ambito e il 25% del valore a livello nazionale per andare oltre. Tema caldo sono gli accordi siglati dalle organizzazioni interprofessionali. Queste, infatti, possono richiedere che alcune condizioni siano rese obbligatorie anche nei confronti dei non aderenti alla stessa organizzazione, ovvero, le OI possono chiedere l'istituzione di contributi obbligatori. Si tratterà comunque di condizioni che devono aver avuto il placet di almeno l'85% degli aderenti alle stesse. Competente a decidere sull'estensione delle regole e sulla richiesta di istituzione di contributi obbligatori è il MIPAAF. La legge prevede anche sistemi di integrazione degli operatori della filiera biologica, finanziati dallo Stato, come i contratti di rete fra le imprese, le cooperative e i contratti di filiera tra gli operatori del settore. Lo scopo è favorire l'aggregazione imprenditoriale e l'integrazione tra i diversi anelli della filiera dei prodotti biologici. Secondo le principali associazioni e federazioni di settore, non risultava necessario dedicare una disciplina specifica all'interprofessione nel settore biologico essendo il tema già normato da altra legge, mentre esistono molti dubbi sulla possibilità di costituire una filiera operativa ed efficiente, soprattutto per quanto riguarda la distribuzione della remuneratività e l'equilibrio fra le posizioni di forza dei suoi componenti. Il quadro attuale è popolato da marchi privati, pubblicizzati "furbescamente" come filiere, e da contratti di coltivazione in mano a pochi commercianti che escludono i produttori non solo dalla condivisione degli utili, ma soprattutto dalla determinazione del prezzo. Per quanto riguarda l'equiparazione dell'agricoltura biodinamica a quella biologica, prevista al comma 3 dell'art. 1, va, innanzitutto, chiarito che essa opera secondo metodologie più restrittive di quelle biologiche nella produzione, escludendo l'uso di molte sostanze (concimi, ammendanti, antiparassitari e prodotti fitosanitari) che sono, invece, autorizzate nel biologico dalla normativa Comunitaria. Il metodo però, non risulta disciplinato da alcuna normativa specifica ufficiale com'è invece, quella dedicata al biologico. Secondo le Associazioni di settore, pur restando nell'alveo del biologico, è indispensabile che la nuova legge faccia sempre specifico riferimento agli standard di produzione che identificano il metodo biodinamico, citando, quindi, espressamente, la biodinamica nei punti chiave, per evitare ambiguità di interpretazione in sede di future applicazioni, ma anche da parte di enti ed organizzazioni terze, potendo l'omissione di una esplicita menzione essere interpretata per implicita esclusione. Fra i nodi cruciali per far crescere la pratica biodinamica: la formazione e ricerca (art. 8 e art. 9), che potrebbe accreditare la biodinamica nei corsi universitari, scolastici, regionali e nei piani di ricerca-sviluppo; il "Piano d'azione nazionale per la produzione biologica" che le garantirebbe una promozione istituzionale; il Tavolo tecnico per la produzione biologica, dove potrà contribuire alle decisioni del sistema; avere un posto fra i beneficiari del nuovo Fondo per lo sviluppo della produzione biologica. Nella versione approvata dalla Camera, la biodinamica si è aggiudicata un posto al tavolo e nel piano sulle sementi biologiche. D'altronde, la perplessità maggiore, rilevata dagli OdC, nasce in fase certificativa, dove occorrono precise codificazioni normative del processo produttivo a garanzia del prodotto, del produttore e del consumatore. Se, infatti, il biologico risulta regolamentato in ogni sua fase, dalla produzione sino all'etichettatura, attraverso Regolamenti Comunitari, lo stesso, attualmente, non può dirsi per il biodinamico.

Operatività del Sistema

A supportare le Amministrazioni Pubbliche nell'organizzazione della disciplina di det-

taglio sulla produzione biologica, in linea con le esigenze ed i bisogni delle aziende, ci sarà il Tavolo tecnico per la produzione biologica, istituito presso il MIPAAF. I compiti affidati sono centrali per il sistema. Dovrà, infatti: determinare le priorità per il comparto nell'organizzazione del Piano d'azione nazionale per l'agricoltura biologica; formulare pareri sui provvedimenti di carattere nazionale ed europeo in merito alla produzione biologica; occuparsi di promozione del biologico proponendone le attività; individuare come incrementare la percentuale di operatori del comparto attraverso strategie che favoriscano la conversione delle aziende convenzionali. Circa la sua composizione, oltre all'inclusione di un rappresentante del Ministero della transizione ecologica, si è prevista la larga partecipazione di portatori di interessi vari e, talora, in conflitto, lasciando così spazio a più di una perplessità sulla sua efficienza. Le modalità di funzionamento del suddetto Tavolo saranno definite con DM del MIPAAF. Per i partecipanti non sono previsti compensi, indennità, gettoni di presenza, rimborsi di spese o altri emolumenti.
Entro 90 giorni dall'entrata in vigore della presente Legge, il MIPAAF dovrà adottare il Piano d'azione nazionale per la produzione biologica e i prodotti biologici. Gli obiettivi degli interventi del Piano, previsti dal 2 comma dell'art. 10, spaziano per target di destinatari ed ambiti di competenza (vedi tabella). Sullo stato di attuazione del Piano, il MIPAAF dovrà annualmente informare il Parlamento.

OBIETTIVI PIANO D'AZIONE NAZIONALE SUL BIOLOGICO
• agevolare la conversione al biologico, con particolare riferimento alle imprese agricole convenzionali con reddito non superiore a 7.000 euro; • sostenere la costituzione di forme associative e contrattuali per rafforzare la filiera del biologico; • incentivare il consumo dei prodotti biologici attraverso iniziative di informazione, formazione ed educazione, anche ambientale ed alimentare, con particolare riferimento alla ristorazione collettiva; • monitorare l'andamento del settore; • sostenere e promuovere i distretti biologici; • favorire l'insediamento di nuove aziende biologiche nelle aree rurali montane; • migliorare il sistema di controllo e di certificazione a garanzia della qualità dei prodotti biologici attraverso la semplificazione della normativa, l'utilizzo di strumenti informatici e la predisposizione di interventi di formazione; • stimolare gli enti pubblici ad utilizzare il biologico nella gestione del verde e a prevedere il consumo di prodotti biologici nelle mense pubbliche e in quelle private in regime di convenzione; • incentivare e sostenere la ricerca e l'innovazione in materia; • promuovere progetti di tracciabilità dei prodotti biologici provenienti dai distretti biologici, finalizzati alla condivisione dei dati relativi alle diverse fasi produttive, nonché all'informazione sulla sostenibilità ambientale, sulla salubrità del terreno, sulla lontananza da impianti inquinanti, sull'utilizzo di prodotti fitosanitari ecocompatibili e sulle tecniche di lavorazione e di imballaggio dei prodotti utilizzate; • valorizzare le produzioni tipiche italiane biologiche; • promuovere la sostenibilità ambientale con azioni per l'incremento della fertilità del suolo, l'uso di metodi di conservazione, confezionamento e distribuzione rispettosi dell'ambiente.

Un capitolo a sé è quello sulle sementi biologiche. L'articolo 8 della legge stabilisce, a cura del MIPAAF, l'adozione, entro 6 mesi dalla sua entrata in vigore, di un Piano Nazionale per aumentare la disponibilità delle sementi biologiche per le aziende, migliorandone l'aspetto quantitativo e qualitativo con riferimento a varietà adatte all'agricoltura biologica e biodinamica. Il Piano, di durata triennale, vuole promuovere il miglioramento genetico nel selezionare piante che rispondano ai bisogni degli agricoltori e che si adattino alle diversità ambientali, climatiche e colturali. Tema di particolare attenzione è quello della loro commercializzazione intra ed extra UE che, avendo riguardo a materiale riproduttivo vegetale eterogeneo biologico come lo sono piante, parti di piante e bulbi, dovrà rispettare precise condizioni e garanzie. Sarà, infatti, importante verificarne i requisiti di registrazione e certificazione previsti da norme specifiche, ovvero, accertare che sia possibile fare riferimento a norme vincolanti nella produzione che consentano di individuare, tracciare e rintracciare detto materiale.

L'articolo 9 della legge prevede che presso il MIPAAF sia istituito un Fondo per lo sviluppo della produzione biologica in sostituzione dell'attuale Fondo per la ricerca nel settore dell'agricoltura biologica e di qualità (Legge 23 dicembre 1999, n. 488) che sarà contestualmente soppresso. Le risorse residue confluiranno nel nuovo fondo, con apposita variazione di Bilancio. Seguirà a breve giro il DM attuativo del MIPAAF (2 mesi dall'entrata in vigore della Legge) per definire le modalità di funzionamento, i requisiti ed i criteri di chi e di cosa può essere finanziato dal Fondo. Ogni anno il MIPAAF deciderà quanto di ciò destinare: a sostegno della realizzazione del marchio biologico italiano, al finanziamento del piano nazionale delle sementi biologiche e ai programmi di ricerca ed innovazione del comparto. Le dotazioni per ogni singola destinazione dovranno essere tracciate con separata voce contabile nel bilancio ministeriale. La dotazione del Fondo è parametrata sulle entrate del contributo previsto dall'articolo 59, comma 1, della legge 23 dicembre 1999, n. 488, a favore della sicurezza alimentare, che in questo caso è assicurata dallo sviluppo di una produzione biologica ed ecocompatibile con l'obiettivo prioritario di ridurre i rischi per la salute degli uomini e degli animali e per l'ambiente. Il contributo è previsto nella misura del 2% del fatturato annuo realizzato dalle aziende che commercializzano: prodotti fitosanitari autorizzati secondo la normativa vigente; fertilizzanti da sintesi; prodotti fitosanitari e coadiuvanti di prodotti fitosanitari che, nelle indicazioni in etichetta, non presentano frasi di rischio pericolose per uomini, animali ed ambiente ovvero ammessi dagli elenchi nazionali. Il contributo avrà rate semestrali, con modalità stabilite dal MIPAAF entro trenta giorni dalla data di entrata in vigore del presente provvedimento. Il DM prevede le sanzioni amministrative e le modalità per la riscossione (vedi tabella) pari al doppio del dovuto.

Contributo annuo a sostegno Fondo per lo sviluppo produzione Biologica	
Mancato versamento	si applica la sanzione amministrativa pecuniaria pari al doppio del contributo dovuto
Versamento in misura inferiore	la sanzione è pari al doppio della differenza tra quanto versato e quanto dovuto
Ritardato versamento	la sanzione è pari allo 0,1 per cento del contributo dovuto per ogni giorno di ritardo

Se entrambi i Fondi, quello previsto dalla presente legge e quello dalla legge n. 488, condividono i medesimi criteri di sostegno annuo, conservano anche gli stessi limiti, sia economici che di programmazione. L'imposta applicata a chi vende fitofarmaci produce, infatti, un gettito che oscilla fra i 10 ed i 12 milioni annui. Poca cosa se si pensa che, con lo stesso capitolo di bilancio, si dovrebbe finanziare sia la ricerca e sperimentazione, che la formazione ed i servizi tecnici di supporto agli agricoltori.

Marchio Nazionale Volontario

Entro 90 giorni dall'entrata in vigore del TU il MIPAAF dovrà adottare un DM che preveda le condizioni ed i criteri per attribuire il marchio biologico italiano ai prodotti biologici ottenuti da materia prima italiana. Il Marchio, disciplinato dall'art. 6 della legge in commento, grazie alla sua apposizione in etichetta o nel packaging del prodotto, potrà garantire sia la massima visibilità e riconoscibilità alle materie prime agricole italiane, sia una effettiva trasparenza per il consumatore delle informazioni riportate in etichetta. Attualmente la normativa Comunitaria in materia di etichettatura dei prodotti biologici prevede, infatti, che sia riportato obbligatoriamente in etichetta il codice dell'organismo di controllo dell'operatore che ha effettuato l'ultima operazione dove è presente la sigla del paese di appartenenza dell'OdC. Se il prodotto è preconfezionato, il logo sarà quello Comunitario, mentre, se è composto, per ogni materia prima dovrà comparire se il paese di origine se è UE o ExtraUE. È, infine, possibile indicare il paese di produzione al posto della dicitura UE, solo quando tutte le materie prime sono ottenute in quel paese. Quest'ultimo solo è il caso che consente l'apposizione del Marchio Biologico Italiano. Considerando il valore crescente del prodotto "griffato" Made in Italy e l'abuso della regola sull'origine doganale della merce, che consente di apporre il marchio italiano anche a ciò che è solo trasformato entro i confini nazionali, si tratta di una prescrizione di forte impatto commerciale.

I Numeri del Biologico

Ettari e aziende agricole

Nel 2020 gli ettari a biologico sono 2.095.380 milioni che corrispondono al 16,6% della SAU (Superficie Agricola Utilizzata) nazionale (nel 2010 era l'8,7%) e 81.731 operatori (+71% rispetto al 2010). In Europa, l'Italia è il terzo paese in termini di superficie, dopo Francia e Spagna, ed il primo in termini di operatori, di quantità prodotta e di volume di prodotti esportati. La superficie media Europea è superiore ai 20 ha mentre quella italiana è pari a 8 ha. Più di un terzo degli operatori è concentrato in tre regioni: Puglia, Sicilia e Calabria. La categoria che ha avuto maggiore incremento dal 2010 (+ 300%) è quella dei produttori/trasformatori. L'età media degli agricoltori Ue è di 40 anni mentre in Italia si avvicina ai 65.

Vendite

Nel 2021 la domanda domestica ha superato i 4,6 miliardi di euro, con un incremento del 5% rispetto al 2020. Il canale di acquisto principale è la Distribuzione Moderna con il 56% del totale dei consumi casalinghi (+2% rispetto al 2020) ed un valore di 2,2 miliardi di euro. Seguono i negozi bio specializzati che rappresentano il 26% del totale delle vendite (+8% rispetto all'anno precedente) con un valore che sfiora il miliardo di euro (996 milioni di euro). Infine, gli altri canali di vendita (negozi di vicinato, farmacia, parafarmacie, mercatini e GAS) con un +5% rispetto al 2020 e vendite per oltre 720 milioni di euro. Nella Grande distribuzione, il canale Iper+Super detiene la leadership del mercato bio con 1,4 miliardi di euro di vendite, stabile rispetto al 2020. Seguono in ordine decrescente: il canale Discount (205 milioni di euro; +11%), l'eCommerce (75 milioni di euro; 67%) e degli Specialisti Drug, con 2 milioni di euro.

Fonti: Sinab, Nielsen, Nomisma

Il ruolo delle clausole sociali nei cambi appalto

di Mauro Petrassi

Studio Legale PROIA & PARTNERS

Premessa

Il processo di globalizzazione e terziarizzazione dell'economia che caratterizza da diversi decenni i mercati occidentali ha favorito la tendenza delle imprese a frazionare il ciclo produttivo in molteplici realtà organizzative, con evidenti ripercussioni sulle modalità di organizzazione dell'impresa e sulle condizioni di lavoro, inevitabilmente schiacciate sotto il peso della competizione tra ordinamenti e condizionate dalla crisi che ha investito molti settori.

Fenomeni come il decentramento produttivo e le trasformazioni dei modelli di impresa hanno fatto emergere l'inadeguatezza degli apparati giuridici tradizionali a mediare tra i diversi e contrapposti interessi coinvolti: da un lato, le richieste di flessibilità e di contenimento dei costi dei datori di lavoro e, dall'altro lato, le esigenze di tutela dei diritti dei lavoratori, che rischiano di rimanere disattese da un mercato sempre più liberalizzato e connotato da una forte concorrenza internazionale.

Nella cornice così sinteticamente delineata, uno dei fenomeni più complessi da governare è quello del cosiddetto cambio appalto.

L'avvicendamento di più appaltatori nel contratto: il cosiddetto cambio appalto

Le vicende commerciali definite "cambio appalto" consistono – principalmente – nel mutamento dell'affidatario di un appalto a seguito di cessazione del contratto stipulato dal committente con un precedente appaltatore.

Si tratta di una fattispecie complessa a formazione progressiva che può essere idealmente scomposta in due fasi tra loro correlate: la cessazione del rapporto contrattuale che lega l'appaltante all'appaltatore con conseguente risoluzione del contratto di lavoro stipulato tra quest'ultimo e i suoi dipendenti e l'assegnazione dell'appalto ad un nuovo imprenditore.

Questa seconda fase può a sua volta dar luogo a due scenari differenti: al licenziamento dei dipendenti quale conseguenza della cessazione dell'appalto, ovvero alla prosecuzione dei rapporti di lavoro, senza soluzione di continuità, alle dipendenze del nuovo appaltatore.

Dottrina e giurisprudenza, nazionale e sovranazionale, si sono a lungo soffermate sui criteri distintivi tra "trasferimento di azienda o di ramo di azienda" e mero "cambio appalto" e sul conseguente ambito di applicazione dell'art. 2112 Cod. Civ. – applicabile soltanto nella ipotesi del trasferimento di azienda o di ramo di azienda – e delle clausole cosiddette di seconda generazione o di riassorbimento, contenute in norme di legge, capitolati di appalto o contratti collettivi.

La questione ha profonde implicazioni pratiche, nella misura in cui solo laddove si configuri un trasferimento d'azienda, il lavoratore conserva la totalità dei diritti connessi al pregresso rapporto di lavoro, e quindi, l'anzianità maturata, le mansioni, le qualifiche e i livelli retributivi in atto al momento del trasferimento dell'azienda, con tutte le conseguenze che ne derivano, compresa l'impossibilità di variazioni in *pejus* delle mansioni e delle retribuzioni. Diversamente, laddove non si configuri un'ipotesi di trasferimento d'azienda, il grado di tutela riconosciuto al lavoratore dipende esclusivamente dall'applicazione e dalla relativa portata delle cosiddette "clausole sociali" di riassorbimento laddove, peraltro, dai contratti collettivi.

Ed infatti, ai sensi dell'art. 29, comma 3, D.Lgs 10 settembre 2003, n. 276, "*l'acquisizione del personale già impiegato nell'appalto a seguito di subentro di nuovo appaltatore dotato di propria struttura organizzativa e operativa, in forza di legge, di contratto collettivo nazionale di lavoro o di clausola del contratto d'appalto, ove siano presenti elementi di discontinuità che determinano una specifica identità di impresa, non costituisce trasferimento d'azienda o di parte d'azienda*".

In pratica, secondo il dettato normativo, il caso di mero subentro di un nuovo imprenditore nello svolgimento di attività preordinate all'esecuzione di un'opera o di un servizio con immutata organizzazione, configura una ipotesi di trasferimento di azienda implicante, in favore dei lavoratori impiegati dal precedente appaltatore, l'applicazione delle garanzie e delle tutele previste dall'art. 2112 Cod. Civ. Diversamente, nel caso in cui l'appaltatore subentrante vanti una propria autonoma struttura organizzativa e operativa, nonché siano ravvisabili elementi di discontinuità tali da porre in evidenza che si tratta di una nuova e distinta organizzazione delle attività appaltate, fa sì che non possa trovare applicazione l'apparato protettivo delineato dall'art. 2112 Cod. Civ., ma solamente quello eventualmente previsto dalle clausole sociali di seconda generazione.

Le clausole sociali di seconda generazione

La dottrina definisce "di seconda generazione" (per distinguerle dalle clausole di equo trattamento anche dette di prima generazione) le clausole sociali che impongono all'impresa aggiudicataria di un appalto, pubblico o privato, di garantire la conservazione dell'impiego per i lavoratori già adibiti all'attività oggetto del contratto, attraverso la riassunzione, di tutto o parte, del personale ivi impiegato, o solo tramite la previsione di procedure di coinvolgimento dei loro rappresentanti nella gestione delle vicende legate all'avvicendamento contrattuale.

La *ratio* delle clausole sociali è principalmente rinvenibile nella tutela della stabilità occupazionale del personale utilizzato dall'impresa uscente nell'esecuzione del contratto e, dunque, nella finalità di contrastare dinamiche di concorrenza al ribasso del costo del lavoro.

Tali clausole, previste da alcune norme di legge (cfr. ad esempio l'art. 50 del Codice dei Contratti Pubblici) o dai capitolati di appalti pubblici, sono frequenti nei contratti collettivi applicati in quei settori in cui fenomeni di decentramento produttivo sono particolarmente diffusi.

In alcuni casi, esse impongono all'azienda subentrante la conservazione di tutto o parte del personale già impiegato dall'azienda cedente. In base a tali prescrizioni, il nuovo aggiudicatario non sarebbe libero di scegliere quali lavoratori adibire alla realizzazione dell'attività svolta in favore dell'appaltante, risultando vincolato alle scelte organizzative poste in essere da un'altra impresa sulla base di differenti strategie.

In considerazione della potenziale incompatibilità di tali clausole con i principi di libera concorrenza e di libertà economica delle imprese, è frequente che le clausole prevedano obblighi di assunzione per così dire modulati ovvero condizionati dal numero di lavoratori interessati, dalle loro professionalità o anzianità di servizio, oppure dalla possibilità che i termini, le modalità e le prestazioni contrattuali risultino più o meno invariati.

In tal senso, il grado di protezione offerto ai lavoratori impiegati nell'appalto differisce a seconda che il subentro avvenga o meno a parità di termini, modalità e prestazioni contrattuali. Tale distinzione è frutto dell'opportunità di garantire, a parità di condizioni dell'appalto, parità di lavoro, onde evitare che i guadagni dell'impresa subentrante possano aumentare a discapi-

to delle condizioni di lavoro. Solo a titolo esemplificativo, l'art. 4 CCNL Multiservizi prevede che *"in caso di cessazione di appalto a parità di termini, modalità e prestazioni contrattuali l'impresa subentrante si impegna a garantire l'assunzione senza periodo di prova degli addetti esistenti in organico sull'appalto"*; diversamente in caso di cessazione di appalto con modificazioni di termini, modalità e prestazioni contrattuali, l'impresa subentrante è solamente tenuta ad un esame congiunto della situazione occupazionale con la rappresentanza sindacale aziendale e le Organizzazioni sindacali stipulanti territorialmente competenti.
Resta tuttavia fermo che la circostanza che, oggetto e termini del contratto di appalto restino immutati, non implica affatto che l'imprenditore subentrante adotti i medesimi modelli organizzativi dell'appaltatore uscente. Attraverso scelte gestionali differenti, il nuovo appaltatore potrebbe infatti avere interesse ad utilizzare un numero minore di lavoratori o profili professionali differenti. In tali circostanze, l'imposizione di un obbligo rigido al mantenimento di tutti i lavoratori potrebbe pertanto essere in contrasto con il principio di libertà di iniziativa economica privata.
Sul punto, la giurisprudenza amministrativa è pressoché unanime nell'affermare che le clausole sociali – perseguendo la prioritaria finalità di garantire la continuità dell'occupazione in favore dei medesimi lavoratori già impiegati dall'impresa uscente nell'esecuzione dell'appalto – risultano costituzionalmente legittime, quali forme di tutela occupazionale ed espressione del diritto al lavoro se si contemperano con l'organigramma dell'appaltatore subentrante e con le sue strategie aziendali, frutto, a loro volta, di quella libertà di impresa pure tutelata dall'art. 41 Cost..
In una logica di contemperamento fra valori di rilievo costituzionale, la compressione del diritto di libertà economica e di libera organizzazione imprenditoriale non può essere predicata in modo incondizionato, incontrando piuttosto specifici limiti nella compatibilità con le strategie aziendali dell'operatore subentrante e, più in generale, nell'identità di *ratio* e di oggetto di tutela (cfr. Cons. Stato, Sez. V, 12 febbraio 2020, n. 1066)
Alcune clausole sociali anziché prevedere un obbligo generalizzato di riassunzione, definiscono in modo dettagliato le posizioni dei lavoratori assunti dalle imprese subentranti, specificando, ad esempio, che essi devono essere riassunti, con la costituzione di un nuovo rapporto e l'estinzione del precedente. Alcuni accordi, invece, garantiscono anche la conservazione delle posizioni di cui i dipendenti erano titolari, riconoscendo, pertanto, i livelli retributivi in godimento e l'anzianità pregressa. Altri ancora prevedono la possibilità di escludere il periodo di prova.
Non è peraltro infrequente che siano definiti criteri specifici per identificare i lavoratori destinati a confluire nell'organico dell'impresa aggiudicataria, per esempio, escludendo dalla tutela il personale con qualifica apicale e con più elevata professionalità, o estendendo il diritto al mantenimento dell'impiego in favore dei lavoratori part-time, ovvero con l'indicazione dei requisiti di anzianità necessari.
In molte clausole, la riassunzione è poi condizionata al verificarsi di eventi e/o circostanze che risultano inscindibilmente correlate al precedente contratto di lavoro. Esemplificativa in questo senso è la previsione secondo cui la riassunzione del lavoratore presso il nuovo appaltatore si realizza solo nel momento in cui cessano le cause che avevano legittimato la sospensione del rapporto presso il precedente appaltatore. Analogamente può essere richiamata la clausola sulla base della quale il contratto a tempo determinato sottoscritto con l'appaltatore subentrante terminerà alla scadenza originariamente concordata con il precedente appaltatore.
Vi possono poi essere clausole che, a differenza di quelle fin qui evocate, incidono solo marginalmente sulla libertà di impresa, limitandosi ad imporre alle parti l'avvio di una procedura di informazione e/o consultazione sindacale (per esempio per individuare eventuali soluzioni alternative al licenziamento).
L'adempimento a tali obblighi è finalizzato ad "*armonizzare le mutate esigenze tecnico-organizzative dell'appalto con il mantenimento dei livelli occupazionali, tenuto conto delle condizioni professionali e di utilizzo del personale impiegato, anche facendo ricorso a processi di mobilità da posto di lavoro a posto di lavoro nell'ambito dell'attività dell'impresa ovvero a strumenti quali part-time, riduzione orario di lavoro, flessibilità delle giornate lavorative, mobilità*" (cfr. art. 4 CCNL Multiservizi).
All'impresa uscente potrà essere imposto di fornire informazioni sulla consistenza numerica degli addetti all'appalto, sul rispettivo orario e anzianità di servizio e all'impresa entrante di fornire informazioni sulla nuova gestione. In taluni casi, anche l'azienda appaltante è tenuta ad informare le organizzazioni sindacali sulle problematiche relative al subentro ed in particolare sulle questioni di organizzazione del lavoro e sicurezza (cfr. art. 42-bis CCNL logistica).
Per quanto tali obblighi possano apparire mere formalità, non sono tuttavia mancate letture giurisprudenziali che ne hanno rafforzato la portata al punto da sostenere che tali clausole non si limiterebbero a prevedere "un mero obbligo a trattare", ma introdurrebbero *"un compiuto obbligo di assunzione in quanto attestanti la concorde volontà di apprestare lo strumento contrattuale idoneo a garantire la continuità occupazionale"* (cfr. Cass. civ. 3 ottobre 2011, n. 20192).
In tal senso, alcuni contratti prevedono che il mancato assolvimento degli obblighi procedurali comporti l'obbligo di riassunzione di tutti i lavoratori impiegati nell'appalto (cfr. artt. 42 e 42-bis CCNL Logistica).

L'efficacia delle clausole di fonte contrattuale

Di ampia portata sono i problemi legati all'efficacia soggettiva delle clausole sociali previste dai contratti collettivi di lavoro.
Ed infatti, secondo l'indirizzo consolidato della dottrina e della giurisprudenza, a causa della nota inattuazione della seconda parte dell'art. 39 Cost., gli effetti delle clausole dei contratti collettivi di lavoro sono regolati sulla base dei principi generali dell'ordinamento in materia di contratti e, quindi, anche le clausole sociali previste da quei contratti collettivi di lavoro, producono effetti soltanto nei confronti dell'imprenditore che si è vincolato all'applicazione del contratto collettivo di lavoro che prevede la specifica clausola sociale.
Più nel dettaglio, le previsioni relative al coinvolgimento delle organizzazioni sindacali, richiedono, per essere efficaci, l'affiliazione sindacale, quantomeno, dell'appaltatore uscente e di quello subentrante.
Ciò non significa tuttavia che l'applicazione da parte dei due imprenditori di contratti collettivi differenti comporti una disapplicazione *tout court* degli obblighi imposti dalle clausole sociali in essi contenute. Ad esempio, laddove tali prescrizioni, per quanto differenti, non siano del tutto incompatibili, non è escluso che le imprese coinvolte possano adempiere alle indicazioni dei rispettivi contratti ponendo in essere processi di coinvolgimento efficaci, al di là delle più specifiche prescrizioni formali.
Rispetto alle clausole sociali che prevedono più stringenti obblighi di assunzione, è possibile prospettare tre diverse ipotesi:
1) i due appaltatori applicano il medesimo contratto collettivo, con il conseguente obbligo in capo all'imprenditore subentrante di adempiere agli obblighi dedotti nella clausola sociale;
2) il contratto collettivo applicato dall'appaltatore subentrante non prevede alcuna clausola di riassorbimento, con la conseguenza che i lavoratori non potranno rivendicare alcun diritto all'assunzione o ad altre posizioni giuridiche di tutela;
3) i contratti collettivi applicati dai due appaltatori prevedono clausole di riassorbimento di differente contenuto. In queste circostanze risulta risolutiva l'autonomia negoziale individuale delle due imprese, le quali, per essere adempienti agli obblighi derivanti dalla rispettiva affiliazione associativa, devono elaborare una previsione del contratto di appalto che costituisca una sintesi tra i contenuti delle due clausole collettive, laddove ciò sia possibile, in quanto le diverse previsioni non evidenzino contrasti insanabili.
Ulteriori problemi insorgono in merito alla posizione dei lavoratori non iscritti al sindacato che ha sottoscritto il contratto collettivo di lavoro in cui è contenuta la clausola sociale. Infatti, l'appaltatore subentrante potrebbe sostenere di non aver assunto al-

cuna obbligazione in loro favore. Tuttavia, in ragione dell'applicazione alle assunzioni della disciplina antidiscriminatoria per ragioni sindacali, anche tali lavoratori possono rivendicare il diritto ad essere assunti, perché un eventuale rifiuto si tradurrebbe in un trattamento pregiudizievole motivato dalla loro adesione o non adesione a un'organizzazione collettiva (cfr. art. 15 St. Lav.).

Rimedi e tutela in caso di violazione delle clausole sociali

Il dibattito dottrinale e giurisprudenziale si è poi soffermato sui possibili rimedi individuali e collettivi attivabili dai lavoratori e dalle organizzazioni sindacali al fine di pretendere l'adempimento delle clausole sociali.

In particolare, è controverso se il lavoratore, una volta accertato il diritto ad essere assunto dal nuovo appaltatore, possa ottenere una sentenza che, accertato l'inadempimento dell'imprenditore subentrante nell'appalto all'obbligo di assunzione, abbia l'effetto di costituire essa il rapporto di lavoro.

Difatti, la Cassazione in più occasioni si è pronunciata nel senso che l'art. 2932 Cod. Civ. – che disciplina l'esecuzione in forma specifica dell'obbligo di concludere il contratto mediante emanazione di sentenza che produca gli effetti del contratto non concluso – trova applicazione anche nel caso di inadempimento all'obbligo di stipulazione di un contratto di lavoro subordinato, purché risultino compiutamente indicati tutti gli elementi del contratto, anche nei dettagli, non essendo ammissibile alcun tipo di intervento del giudice che tenga luogo della volontà delle parti ai fini della concreta specificazione del suo contenuto in ordine ad elementi essenziali (cfr. ad esempio Cass. n. 8568/2004 e Cass n. 12516/2003).

Tale orientamento è stato ribadito con specifico riferimento ad ipotesi di subentro nell'appalto, precisandosi che l'oggetto del contratto di lavoro possa ritenersi sufficientemente determinato, in tutti i casi in cui le parti abbiano concordato in sede sindacale, oltre che l'obbligo di assunzione, anche ulteriori elementi, quali il contratto collettivo applicabile ai nuovi dipendenti, la relativa categoria di inquadramento, il riconoscimento dell'anzianità pregressa e il superminimo individuale, conseguendone che il lavoratore, in caso di inadempimento, potrà richiedere, ai sensi dell'art. 2932 Cod. Civ., l'esecuzione in forma specifica dell'obbligo di concludere il contratto, senza che rilevi la mancata predeterminazione della concreta assegnazione della sede lavorativa e delle mansioni (cfr. Cass. n. 27841/2009; n. 28415/2020).

D'altra parte, il lavoratore potrebbe non avere più interesse all'esecuzione in forma specifica della clausola di riassorbimento, ad esempio per aver acquisito un nuovo impiego, mantenendo tuttavia interesse ad ottenere un risarcimento del danno. In proposito, la dottrina segnala il consolidato orientamento della giurisprudenza a quantificare il nocumento subito dal lavoratore sulla base del parametro retributivo, che nel caso di cambio appalto consiste nel trattamento economico che il lavoratore avrebbe percepito laddove fosse stato assunto dall'appaltatore subentrante, nel rispetto degli obblighi previsti dalla clausola sociale.

Peraltro, il diritto al risarcimento del danno può essere fatto valere anche nel caso in cui sussistano le condizioni per addivenire ad una sentenza costitutiva del rapporto di lavoro. Ciò si verifica, ad esempio, quando, nelle more del giudizio, la mancata assunzione abbia arrecato al lavoratore ulteriori svantaggi, patrimoniali o non patrimoniali, diversi dalla intempestiva acquisizione del nuovo impiego. Per questi profili, il ricorso al parametro retributivo è ingiustificato, e la quantificazione del risarcimento deve avvenire sulla base dell'effettiva entità del danno, in ragione degli elementi probatori prodotti.

Quando le clausole sociali prevedono, invece, obblighi di informazione o consultazione, il mancato adempimento da parte delle imprese rileva sul piano delle relazioni sindacali e può essere denunciato dalle organizzazioni sindacali mediante il procedimento di repressione della condotta antisindacale *ex* art. 28 St. Lav..

SEAC

Passione per semplificare le cose

Reati tributari, infortuni sul lavoro, riciclaggio, reati informatici ed ambientali, reati societari, etc. comportano necessariamente, per le imprese, anche le più piccole, l'esposizione ai rischi previsti dal D.Lgs. n. 231/01 per gli illeciti penali commessi dai propri dirigenti, lavoratori, etc.

Il rischio è di pagare multe salatissime ma anche di chiudere con la revoca di autorizzazioni e licenze o l'interdizione ad operare con la Pubblica Amministrazione.

Il volume ha l'ambizione di costituire una guida pratica per professionisti, soprattutto commercialisti, consulenti del lavoro e avvocati - quali consulenti e/o membri dell'Organismo di Vigilanza, "gestori" delle strategie difensive, etc. – e per le attività imprenditoriali, professionali, commerciali, etc. sottoposte alla c.d. responsabilità amministrativa, di fatto penale. L'originalità si sostanzia nell'approfondire non solo gli aspetti di natura preventiva, a cominciare dalla costruzione del modello, ma anche patologici e di gestione della crisi (ispezioni e/o indagini esterne, segnalazioni del whistleblower, indagini difensive, etc.). Nell'ultimo capitolo viene affrontato analiticamente, sempre con taglio pratico, il recente ingresso tra i reati presupposto delle fattispecie tributarie.

Disponibili su shop.seac.it o nelle librerie specializzate. Per informazioni: editoria@seac.it