ISSN 2784-8213

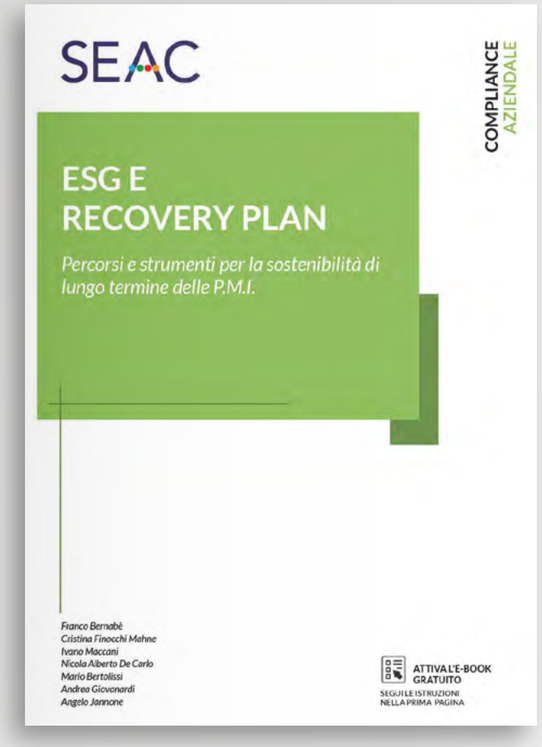
COMPLIANCE

Gennaio 2022 – n. 1 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

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.

Denise Boriero: Avvocato del Foro di Trento, collabora con l'Università degli Studi di Trento. Si occupa di sicurezza e criminalità, nonché di compliance aziendale.

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.

Alessandro De Carlo: Founder di Sygmund – Il tuo psicologo online, responsabile tecnico-scientifico per il Gruppo CISES di IF Informazione&Fiducia e realtà virtuale. Psicologo – psicoterapeuta, docente universitario.

Giorgia Farella: Executive MBA, ingegnere energetico, imprenditrice, esperta di servizi energetici avanzati

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.

Simone Franzò: PhD, ingegnere gestionale, senior assistant professor della School of Management Politecnico di Milano

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.

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

Manlio d'Agostino Panebianco: Adjunct professor of Economic Crime and Cybercrime (Limec), consulente aziendale.

Giulia Sulpizi: Praticante avvocato del Foro di Padova e Cultrice della materia di ELP-Global English for Legal Studies (Università di Padova). Già autrice di contributi scientifici in tema di diritto costituzionale, si occupa prevalentemente di diritto amministrativo e civile.

Elisabetta Torzuoli: Iscritta all'Ordine degli Avvocati di Perugia, esercita la propria attività professionale nell'ambito del diritto civile e penale, svolge consulenza legata ai temi della compliance aziendale, anche con riguardo al D.Lgs. 231/2001. È formatore qualificato in ambito di salute e sicurezza sui luoghi di lavoro, oltrechè data protection officer ai sensi del Regolamento europeo 16/679/CE. Coordina il dipartimento di compliance aziendale di Aiga – Sezione di Perugia. È consulente dell'Assessorato regionale dell'Umbria alle politiche agricole e agroalimentari ed alla tutela e valorizzazione ambientale.

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.

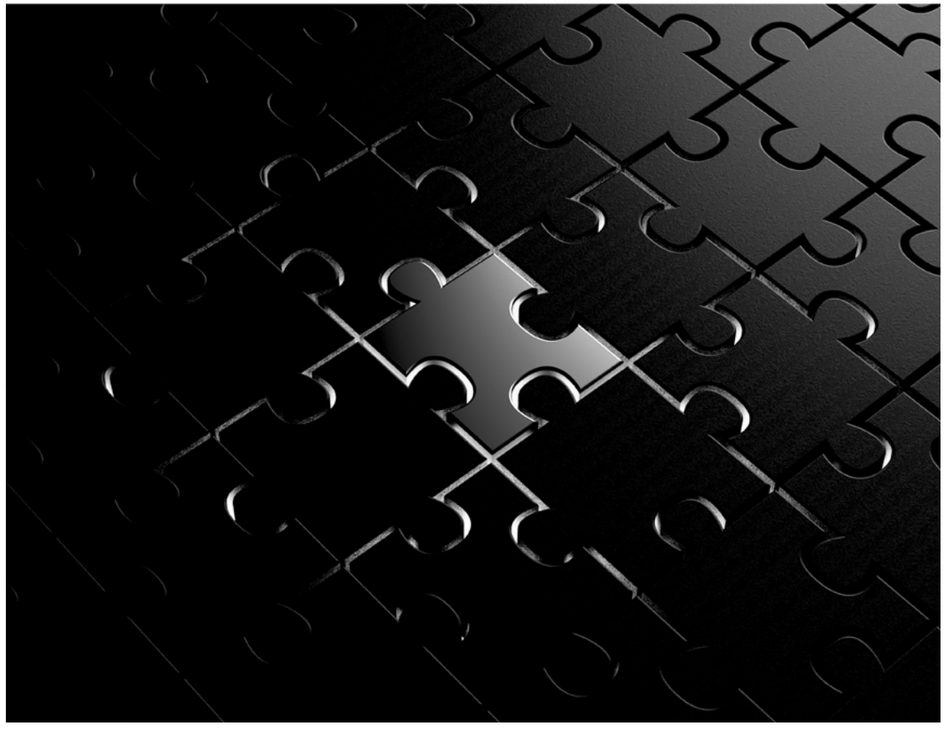
Compliance aziendale: per la nuova economia i valori vengono prima del valore

di Ivano Maccani e Denise Boriero

Il modo di fare impresa sta cambiando progressivamente e non si può fare a meno di considerarne l'impatto ambientale, etico e sociale. Per chiarire cosa vuol dire fare buona impresa e soprattutto per ispirare gli imprenditori di domani è indispensabile conoscere, rispettare ed utilizzare strumenti come il benessere organizzativo, lo *smart working*, i modelli organizzativi 231, la *privacy* e la tutela dei dati, la sicurezza informatica e sui luoghi di lavoro, la finanza sostenibile, la *green economy* e gli obblighi antiriciclaggio. Queste, solo per fare alcuni esempi, sono tutte tematiche che rappresentano il filo conduttore della rivista Compliance! É a questa prospettiva che si ispirano i contenuti del primo numero del nuovo anno, fornendo delle indicazioni operative e stimolando l'adozione di efficaci strategie di gestione di eventi che hanno o possono avere un impatto interno e/o esterno, quali i controlli e le ispezioni, il giudizio cautelare, le indagini difensive, il benessere del personale, la transizione ecologica, l'innovazione tecnologica, la preven-

zione dagli attacchi informatici, eccetera. In effetti, il rischio compliance, ossia di disallineamento tra le procedure aziendali e l'insieme delle regole interne ed esterne, comporta per le aziende il pericolo di incorrere in sanzioni penali e amministrative, perdite finanziarie e di immagine. Per fare buona impresa ed evitare tali rischi occorre necessariamente definire in via continuativa specifici meccanismi di coordinamento e collaborazione tra i principali attori aziendali come il dirigente preposto, la funzione compliance, l'*internal audit*, il datore di lavoro, il collegio sindacale, l'organismo di vigilanza e tutti i protagonisti interni ed esterni a vario titolo coinvolti. La gestione integrata del rischio aziendale rappresenta infatti un tema di fondamentale rilevanza non solo in termini finanziari ma anche secondo una visione allargata economico-organizzativa. Possiamo pertanto affermare che sussiste la necessità di un cambiamento culturale nel *management* societario che deve essere sempre più indirizzato su aspetti di natura ambientale, sociale e di *governance*.

Partendo da tali premesse, nel saggio d'apertura annuale della rivista viene affrontato il tema della sicurezza sul lavoro con approfondimenti sui concetti di interesse e vantaggio in materia antinfortunistica nonché sulla recente stretta (Decreto legge n. 146/2021) del relativo arsenale sanzionatorio, che in taluni casi può comportare la sospensione del cantiere o addirittura la chiusura dell'azienda. Ulteriori argomenti trattati riguardano le linee guida della Guardia di Finanza nella gestione della fonte di prova digitale, l'impatto del Covid sulle organizzazioni e sulla salute psicologica dei lavoratori, la tutela della *privacy*, la transizione energetica, i divieti e sanzioni per chi svende i prodotti agroalimentari o non rispetta i termini di pagamento dei fornitori, il "modello organizzativo 231" incentrato sulla prevenzione del reato di contrabbando, le nuove linee guida Confindustria per il Sistema 231, l'intelligenza artificiale e tecnologie di *cyber security*, i rapporti tra imprese e pubblica amministrazione e il registro dei titolari effettivi in ambito anti riciclaggio.



I reati in materia di sicurezza lavoro e le violazioni che comportano l'obbligo di sospensione immediata dell'attività aziendale ex D.Lgs n. 146/2021 e circolare Inl n. 4 del 9 dicembre 2021

di Denise Boriero e Ivano Maccani

Premessa

Il Decreto legislativo n. 231/2001 costituisce una novità dirompente e una vera e propria rivoluzione ordinamentale.

Il fatto che l'illecito formalmente amministrativo dipendente da reato sia accertato e perseguito con le regole del procedimento penale e che all'ente o società si applichino le disposizioni processuali relative all'imputato, in quanto compatibili, comporta un indubbio ampliamento dello spazio di azione per le investigazioni e le indagini della polizia giudiziaria nonché del Pubblico Ministero.

In effetti, a fronte della commissione da parte di un soggetto apicale o subordinato di un reato presupposto ex D.Lgs n. 231/2001, nell'ambito delle rispettive attribuzioni, la PG e l'AG che svolgono le indagini sono tenute ad accertare, avvalendosi pure delle disposizioni del codice di procedura penale, anche la cosiddetta responsabilità amministrativa della società.

In particolare, in tali casi, ogni volta che all'esito delle indagini emergono fondati indizi di un reato presupposto in capo a un soggetto apicale o sottoposto:

- la polizia giudiziaria dovrà denunciare sia la persona fisica autrice del reato commesso nell'interesse o a vantaggio della società, sia la società stessa per la cosiddetta responsabilità amministrativa;
- il pubblico ministero dovrà aprire due procedimenti, che normalmente sono poi riuniti, uno per il reato nei confronti della persona fisica indagata e l'altro per il cosiddetto illecito amministrativo della società.

Anche a seguito della progressiva e costante implementazione dei reati presupposto assistiamo ad un continuo aumento delle indagini, dei procedimenti e delle misure cautelari ex D.Lgs n. 231/2001.

A tal proposito va rilevato che la responsabilità penale di enti e società, innescata dai delitti di omicidio colposo e di lesioni gravi e gravissime conseguenti a violazioni delle norme sulla sicurezza lavoro, di fatto rappresenta un fenomeno assai diffuso che viene facilmente ad emergere a fronte delle precarie condizioni lavorative e di una legislazione particolarmente ricca di prescrizioni verso l'impresa.

I settori più esposti a tale rischio risultano essere le costruzioni, i trasporti e il magazzinaggio, il commercio e la riparazione di veicoli, la lavorazione dei metalli e l'agricoltura.

Possiamo peraltro osservare che proprio tale tipologia di illeciti rappresenta uno dei principali capi di imputazione per enti e società. In effetti, nei soli primi 8 mesi dell'anno 2021 risultano essere ben 772 le

sole denunce di infortunio mortale.
Si tiene inoltre a sottolineare che i reati collegati alla sicurezza sul lavoro comportano seri rischi per enti e società, considerato che anche per tali illeciti sono applicabili, oltre le sanzioni pecuniarie, anche quelle interdittive.
Si immagini quanto possa essere pesante per un'impresa che opera prevalentemente nel settore dei pubblici appalti l'applicazione della sanzione di non contrattare con la pubblica amministrazione, che costituisce una delle cause di esclusione dalla procedura di affidamento delle concessioni e degli appalti di lavori, forniture e servizi. La società colpita da tale sanzione, vedendosi pregiudicata la possibilità di partecipare a gare pubbliche, corre evidentemente seri e concreti rischi di chiudere l'attività. L'impatto dell'articolo 25 *septies* del D.Lgs n. 231/2001 assume pertanto una rilevanza particolarmente significativa sia in termini quantitativi che qualitativi.

I reati collegati alla sicurezza sul lavoro e i criteri dell'interesse o vantaggio

Prima di approfondire l'aspetto della compatibilità tra reati colposi e criteri dell'interesse o vantaggio, vediamo la differenza tra lesioni gravi e gravissime.
Si considerano gravi le lesioni quando dal fatto derivi una malattia che possa mettere in pericolo la vita della persona offesa o una malattia o una incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai 40 giorni, oppure il fatto produca l'indebolimento permanente di un senso o un organo.
Le lesioni si considerano gravissime se dal fatto derivi una malattia certamente o probabilmente insanabile, la perdita di un senso, la perdita di un arto o una mutilazione che possa rendere l'arto inservibile, ovvero la perdita dell'uso di un organo o della capacità di procreare ovvero una permanente e grave difficoltà della favella oppure la deformazione, ovvero lo sfregio permanente del viso.
Ricordate queste definizioni, passiamo ora ad affrontare, anche alla luce di recenti posizioni di dottrina e giurisprudenza, i concetti di interesse e vantaggio.

Va innanzitutto precisato che la formula contenuta nell'articolo 5 del D.Lgs n. 231/2001, *"nel suo interesse o a suo vantaggio"*, individua il cosiddetto presupposto oggettivo di attribuzione della responsabilità penale di enti e società.
Si osserva, inoltre, che i requisiti dell'interesse o vantaggio devono essere riferiti alla condotta e non all'evento; gli stessi sono alternativi e concorrenti tra loro. In effetti, trattasi di due autonomi e distinti concetti. In particolare, l'interesse, che riguarda la sfera soggettiva, va valutato ex ante mentre il vantaggio ex post.
La Corte di Cassazione ha peraltro avuto modo di chiarire che l'interesse è un criterio soggettivo, che rappresenta l'intento del reo di arrecare un beneficio all'ente o società mediante la commissione di un reato. Diversamente, quello del vantaggio è un criterio oggettivo ancorato all'effettiva realizzazione di un profitto in capo all'ente quale conseguenza della commissione di un reato presupposto.
Nell'evidenziare che in linea generale il presupposto oggettivo ex articolo 5, D.Lgs n. 231/2001 si integra con il mero risparmio economico derivante dalla mancata o non adeguata predisposizione delle salvaguardie necessarie allo svolgimento in sicurezza dell'attività lavorativa, procediamo ora ad un'analisi più approfondita dei due concetti di interesse e vantaggio.
Si può ipotizzare un interesse prefigurato come discendente da un indebito arricchimento e magari non realizzato, e, invece, un vantaggio obiettivamente conseguito tramite la commissione di un reato, così come si può avere un reato commesso nell'interesse dell'ente, senza procurargli di fatto alcun vantaggio.
In particolare, il requisito dell'interesse ricorre ogni volta che il soggetto apicale o subordinato dell'azienda, pur non volendo il verificarsi dell'evento morte o lesioni del lavoratore, agisce con consapevolezza per conseguire un'utilità a favore della stessa, violando la normativa cautelare. Ad esempio quando la mancata adozione delle previste cautele antinfortunistiche risulti essere l'esito, non di una semplice sottovalutazione dei rischi, ma di una scelta finalizzata a risparmiare sui costi dell'azienda; l'interesse può peraltro sussistere anche a fronte di una violazione isolata, causata da una iniziativa estemporanea, a condizione che altre evidenze fattuali dimostrino il collegamento finalistico tra la violazione e l'interesse della società, neutralizzando in tal modo il valore probatorio riconducibile alla sistematicità (in tal senso, la recente pronuncia di Cassazione n. 12149 del 31 marzo 2021).
Per il sussistere del requisito del vantaggio è necessario che l'apicale o il subordinato, agendo per conto della società, pur non volendo il verificarsi dell'evento morte o lesioni del lavoratore, violi le norme prevenzionistiche, realizzando una politica d'impresa disattenta alla sicurezza sul lavoro con conseguente riduzione dei costi ed un risparmio in termini di spesa. In sostanza, è necessario che la persona fisica, agendo per conto dell'azienda, decida di violare sistematicamente le norme prevenzionistiche, con conseguente riduzione dei costi ed un contenimento della spesa tali da massimizzare il profitto.
Relativamente alla consistenza del vantaggio, deve trattarsi di un importo non irrisorio, che deve essere valutato dal giudice di merito. Occorre sottolineare che tale valutazione è insindacabile ove congruamente ed adeguatamente motivata.
Soffermandoci sempre sul concetto di vantaggio, osserviamo inoltre che lo stesso, così come stabilito con sentenza n. 33595 della Cassazione in data 10 settembre 2021, può consistere anche in una velocizzazione degli interventi per la predisposizione di misure di sicurezza che sia tale da incidere sui tempi di lavorazione. In sostanza, al risparmio di tempo corrisponde un conseguente risparmio di spesa. Possiamo pertanto affermare che con tale pronuncia viene ampliato il criterio di interpretazione fondato sul risparmio dei costi, includendo anche il risparmio determinato dalla accelerazione degli interventi.
Va comunque sottolineato che a fronte di un sinistro sul lavoro la società non ne risponde in mancanza della prova dell'oggettiva prevalenza delle esigenze della produzione e del profitto su quella della tutela della salute dei lavoratori. Ne consegue che la prova dell'effettivo vantaggio, vale a dire del risparmio di spesa, non è desumibile dalla mera omessa adozione della misura di prevenzione (Cassazione, sentenza n. 22256/2021).
Anche in presenza di una sentenza di applicazione, ex articolo 131 bis c.p., della particolare tenuità del fatto e conseguen-

te esclusione della punibilità del soggetto apicale o sottoposto che ha commesso il reato presupposto, il giudice è in ogni caso tenuto a procedere all'autonomo e distinto accertamento ex D.Lgs n. 231/2001 nei confronti della società nel cui interesse o vantaggio l'illecito è stato commesso. In effetti, l'applicazione alla persona fisica del citato articolo 131 bis c.p. non esclude la distinta responsabilità di enti e società.
Si osserva, infine, che il datore di lavoro viene esonerato dalla responsabilità solo in presenza di un comportamento abnorme (causato da un'autonoma iniziativa del dipendente e in un ambito che esula dalle mansioni affidate) del lavoratore oppure nel caso in cui un comportamento riconducibile alle mansioni che gli sono proprie sia consistito in qualcosa di radicalmente lontano dalle ipotizzabili scelte del lavoratore (Ex multis, Cassazione, sentenza n. 2848/2021).

Vincoli più stringenti e rafforzamento delle sanzioni

Tra le novità introdotte dal D.Lgs n. 146 del 21 ottobre 2021, che impattano sulla sicurezza lavoro, sono contemplate anche la sospensione obbligatoria e non più discrezionale dell'attività d'impresa a fronte di gravi violazioni alle disposizioni in materia di sicurezza sul lavoro nonché dell'abbassamento dal 20% al 10% della soglia massima di lavoratori irregolari.
Relativamente all'obbligo di sospensione immediata dell'attività (in precedenza la sospensione scattava solo nel caso di reiterazione delle violazioni), anche alla luce delle indicazioni presenti nella circolare n. 4/2021 dell'Ispettorato nazionale del lavoro, possiamo distinguere due ipotesi: sospensione dell'attività interessata dalle violazioni e sospensione limitata all'attività dei lavoratori interessati. A tal proposito, va innanzitutto precisato che il provvedimento di sospensione immediata dell'attività d'impresa va adottato solo in caso di mancata redazione del DVR. Qualora, invece, il DVR risulti essere custodito in un luogo diverso, ferma restando la contestazione dell'illecito, il provvedimento di sospensione potrà essere adottato a decorrere dalle ore 12 del giorno lavorativo successivo, a meno che il datore di lavoro, entro tale termine, provveda all'eventuale esibizione di un DVR con data certa antecedente al provvedimento di sospensione, che in tal caso verrà annullato.
Altre violazioni che comportano il provvedimento di sospensione dell'attività sono:

• la mancata elaborazione del piano di emergenza ed evacuazione (in tal caso il provvedimento di sospensione trova applicazione solo per l'omessa redazione del piano e ai fini della revoca del provvedimento il piano dovrà essere successivamente esibito);
• la mancata formazione ed addestramento (la sospensione va applicata solo quando è prevista la partecipazione del lavoratore sia ai corsi di formazione sia all'addestramento);
• la mancata costituzione del servizio di prevenzione e protezione e nomina del relativo responsabile (nei soli casi in cui il datore di lavoro non abbia costituito il servizio di prevenzione e protezione e non abbia altresì nominato il RSPP ex articolo 17, comma 1, lettera b), D.Lgs n. 81/2008 o assunto lo svolgimento diretto dei relativi compiti dandone preventiva informazione al rappresentante dei lavoratori per la sicurezza);
• la mancata elaborazione del piano operativo di sicurezza (Pos);
• la mancata fornitura del dispositivo di protezione individuale contro le cadute dall'alto;
• la mancanza di protezioni verso il vuoto;
• la mancata applicazione delle armature di sostegno, fatte salve le prescrizioni desumibili dalla relazione tecnica di consistenza del terreno;
• i lavori in prossimità di linee elettriche in assenza di disposizioni organizzative e procedurali idonee a proteggere i lavoratori dai conseguenti rischi;
• la presenza di lavori non elettrici effettuati in vicinanza di linee elettriche o di impianti elettrici con parti attive non protette durante i quali i lavoratori operino a distanza inferiore ai limiti previsti;
• la mancanza di protezione contro i contatti diretti ed indiretti (impianto di terra, interruttore magnetotermico, interruttore differenziale) e l'omessa vigilanza in ordine alla rimozione o modifica dei dispositivi di sicurezza o di segnalazione o di controllo.

Si tratta di violazioni di massima trasversali per un gran numero di attività che implicano l'impiego di lavoratori intesi in senso ampio.
Si evidenzia che la sospensione ha come conseguenza l'impossibilità di contrattare con la pubblica amministrazione e, oltre all'applicazione delle sanzioni penali previste dal testo unico sulla sicurezza, può anche comportare la responsabilità patrimoniale qualora la società non sia conseguentemente nelle condizioni di adempiere alle proprie obbligazioni verso il proprio committente o subappaltatore.
A tal proposito sorge spontaneo il riferimento ai cantieri per gli interventi previsti nei condomini per il cosiddetto super bonus o per le facciate. Poiché anche in tal caso la rilevazione delle citate violazioni comporta il provvedimento di sospensione dell'attività d'impresa, le conseguenze per il condominio, in caso di sospensione prolungata nel tempo, possono addirittura impedire la realizzazione dell'opera e il conseguimento dei benefici fiscali.

BIBLIOGRAFIA

Alessio Scarcella, "L'interesse o il vantaggio vanno verificati nell'ambito della complessiva condotta tenuta dall'ente", rivista 221.
Marco Dell'Antonia e Alessandro De Nicola, "Tagliare i tempi dei lavoratori per la sicurezza riduce i costi e può far scattare le sanzioni 231", il Sole24ore.
Giuseppe Amato, "Interesse e vantaggio per l'ente in materia antinfortunistica", rivista 231.
Daniele Cirioli, "Sigilli all'azienda non sicura", Italia oggi.
Gabriele Taddia, "Sicurezza sul lavoro, subito la mappa dei rischi per non inciampare nei nuovi stop all'attività", Il Sole24ore.
Giulio Benedetti, "Scarsa sicurezza e lavoro nero, si rischia la sospensione del cantiere", Il Sole24ore.
Giorgio Pogliotti e Claudio Tucci, "Sicurezza sul lavoro, stretta sulle sanzioni", Il Sole24ore.
Ivano Maccani, Piero Burla e Enrico Cieri, "La responsabilità da reato delle società" a cura del Sole24ore.

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

di Pier Luca Toselli

L'inarrestabile progresso tecnologico ed informatico che ci sta accompagnando ed in particolare, lo sviluppo delle reti telematiche e sempre più efficienti mezzi di comunicazione dei dati e controllo, permette oggi ai diversi operatori economici, di gestire ed amministrare i loro affari da ogni angolo del mondo, senza l'obbligo di collocare una propria presenza fisica in un determinato territorio. Tale contesto ha enormemente incrementato ed accelerato diversi fenomeni quali, per l'appunto, la delocalizzazione, quasi sempre giustificata da motivi di risparmio (ricomprendendovi ovviamente anche quelli relativi all'imposizione fiscale[1]) e la "dematerializzazione" dei documenti. Questi fenomeni insieme ad altri, accompagnati da un inarrestabile progresso tecnologico permettono di affermare che oggi non esiste processo produttivo/economico che non abbia una qualche implicazione diretta o indiretta

1 Alcune giurisdizioni si vedono sottratte ingenti quantità di imponibile fiscale a seguito della delocalizzazione che si sostanzia nel trasferire la sede della società o del gruppo in paesi che hanno regimi impositivi fiscali più convenienti.

con uno strumento digitale e conseguentemente con dati digitali. Soprattutto i processi di continua dematerializzazione del documento cartaceo, con l'obbiettivo di migliorare ed ottimizzare quelli che sono i processi di conservazione, gestione e consultazione, ha profondamente modificato le più elementari metodologie di controllo e verifica degli stessi. Di pari passo con questa evoluzione tecnologica, si sono allora modificate le regole, le tecniche e le procedure che oggi gli investigatori della Guardia di Finanza, calati in questi nuovi e particolari scenari operativi devono non solo conoscere, ma obbligatoriamente rispettare al fine di non inficiare le proprie attività d'indagine. In particolare, in questi articoli, verranno descritte, a seguito dell'emanazione della circolare 1/2018 del Comando Generale della Guardia di Finanza[2], quali siano le linee guida emanate dal Corpo per una corretta gestione delle "evidenze digitali" che pervadono quotidianamente le comuni attività d'istituto demandate al Corpo e quali siano gli strumenti tecnici generalmente utilizzati per il rispetto delle migliori pratiche in materia di *digital forensics*.

La Guardia di Finanza e i suoi poteri in materia economico-finanziaria

Per meglio comprendere l'importanza strategica delle linee guida emanate dal Corpo con la circolare in esame occorre preliminarmente conoscere i compiti di questo particolare Corpo di Polizia.

I compiti sono essenzialmente connessi alla repressione della criminalità economica e la Guardia di Finanza costituisce, ancora, un caso unico in Europa di organismo di polizia ad ordinamento militare con attribuzioni così vaste e specializzate.

Dette attribuzioni sono sancite dalla legge di ordinamento del 23 aprile 1959, n. 189 e si possono riassumere nella prevenzione, ricerca e denunzia delle evasioni e delle violazioni finanziarie, nella vigilanza sull'osservanza delle disposizioni di interesse politico-economico e nella sorveglianza in mare per fini di polizia finanziaria.

Il Corpo concorre anche al mantenimento dell'ordine e della sicurezza pubblica e la difesa politico militare delle frontiere.

Il decreto legislativo 19 marzo 2001, n. 68, in attuazione dei principi direttivi della legge n. 78/2000 ha ridisegnato, ormai da oltre 20 anni, la missione della Guardia di Finanza come forza di polizia a competenza generale su tutta la materia economica e finanziaria. Ciò ha di fatto esteso le facoltà e i poteri riconosciuti per legge ai militari del Corpo in campo tributario a tutti i settori in cui si esplicano le proiezioni operative della polizia economica e finanziaria. In pratica, le funzioni connesse ai compiti di polizia economico-finanziaria vedono la coesistenza del tradizionale ruolo di polizia tributaria (negli ultimi 20 anni, economico-finanziaria) con le attribuzioni tipiche della polizia giudiziaria, consentendo così, agli appartenenti, di contrastare in maniera trasversale ogni fenomeno illecito sia sul piano "amministrativo" che "penale". Quest'ultimo ultimo aspetto assume particolare rilevanza, laddove nell'ambito delle attività d'istituto, ed in particolare nel corso delle attività ispettive, che vedremo, siano acquisite risultanze tali da configurare una violazione penalmente rilevante.

Per quanto attiene ai poteri riconosciuti al Corpo, con riferimento allo specifico comparto, il legislatore ha attribuito alla Guardia di Finanza i medesimi poteri concessi agli Uffici finanziari dagli artt. 51 e 52 del D.P.R. n. 633/72 e dagli artt. 32 e 33 del D.P.R. n. 600/73, in materia, rispettivamente, di IVA e di imposte sui redditi. Tra questi prenderò in considerazione in modo particolare l'accesso e le ricerche, che costituiscono la fase preliminare a seguito delle quali si perviene a contatto con fonti prova digitali. L'accesso è un atto amministrativo di natura autoritativa che consiste nel potere di accedere e di permanere, anche senza o contro il consenso di chi ne ha la disponibilità, se eseguito dalla Guardia di Finanza ha quasi sempre la natura di atto a "sorpresa" (al momento in cui scrivo) e come meglio si può apprendere da un esame della normativa sopra richiamata sottostà ad un preciso regime di autorizzazioni a seconda delle motivazioni e luoghi in cui viene svolto. In particolare , l'art. 52, comma 1, del D.P.R. n. 633/72 prevede, infatti, la possibilità per gli organi dell'Amministrazione Finanziaria di accedere nei locali destinati all'esercizio di attività commerciali, agricole, artistiche o professionali, nonché in quelli utilizzati dagli enti non commerciali per procedere ad ispezioni documentali, verificazioni e ricerche e ad ogni altra rilevazione ritenuta utile per l'accertamento dell'imposta e per la repressione dell'evasione e delle altre violazioni e su autorizzazione del Procuratore della Repubblica territorialmente competente può estendersi anche a quei locali che oltre ad essere adibiti all'esercizio di attività economiche, agricole e professionali, sono anche adibite ad abitazione.

L'elemento di attenzione va riposto nel termine "ricerche" ed è facile comprendere come l'accesso sia per sua natura strumentale e propedeutico all'esercizio di altri poteri come per l'appunto quello di effettuare ricerche volte all'individuazione e alla conseguente raccolta di libri, registri, scritture, documenti ed altri elementi, anche di natura informatica, potenzialmente utili alla ricostruzione dell'effettiva capacità contributiva del soggetto controllato. Invero a seguito dell'accesso il contribuente ha l'obbligo di esibire tutti i libri, registri, scritture e documenti richiesti dai verificatori, l'eventuale inottemperanza da parte del contribuente determina gravi conseguenze e preclusioni, mi limito qui a ricordare che secondo il disposto dell'art. 52, comma 5, del D.P.R. n. 633/72, applicabile anche in materia di imposte sui redditi, per effetto del rinvio operato dall'art. 33 del D.P.R. n.600/73, i libri, i registri, le scritture e i documenti di cui venga rifiutata l'esibizione non possono essere presi in considerazione a favore del contribuente ai fini dell'accertamento in sede amministrativa e contenziosa, intendendosi per rifiuto di esibizione anche la dichiarazione di non possedere libri, registri, documenti e scritture e/o la sottrazione degli stessi al controllo. Oltre alla documentazione sopra evidenziata assumono particolare importanza nell'ambito di quanto trattato nel prosieguo anche i documenti definiti "extracontabili", anticipando già qui che la circolare 1/2018 specifica che tale documen-

2 http://www.gdf.gov.it/documenti-e-pubblicazioni/circolari/circolare-1-2018-manuale-operativo-in-materia-di-contrasto-allevasione-e-alle-frodi-fisca.

tazione pur non rientrando nella categoria dei "libri, registri e scritture obbligatorie" risulta comunque riconducibile al disposto dell'art. 22, 3° comma del D.P.R. 600/73 in cui è previsto che, per ciascun affare devono essere ordinatamente conservati ai sensi del Codice Civile (2220 c.c.) gli originali delle lettere, dei telegrammi e delle fatture ricevuti e le copie delle lettere e dei telegrammi spediti e delle fatture emesse (qui il riferimento che ci accompagnerà è evidente sia riferito alla cd. "corrispondenza" oggi ormai solo elettronica). Ma a rafforzare l'importanza della documentazione "extracontabile" interviene altra norma ovvero l'art. l'art. 52, comma 4, del D.P.R. n. 633/72, il quale dispone che l'ispezione documentale si estende a tutti i libri, registri, documenti e scritture che si trovano nei locali in cui si esercita l'attività, ivi compresi quelli la cui tenuta e conservazione non sono obbligatorie.

Infine, sempre con riferimento all'accesso, va precisato che lo stesso viene eseguito da un numero tale di militare capaci di impedire al contribuente modifiche allo stato delle cose. Ciò trova applicazione anche nei confronti delle apparecchiature informatiche, tant'è che in taluni casi si può anche arrivare per motivate situazioni ad "isolare la rete" aziendale dalla possibilità di subire modifiche da remoto o molto più semplicemente il singolo dispositivo di interesse viene "isolato" dalla rete aziendale. Vige un principio generale di arrecare minor pregiudizio possibile all'attività sottoposta a controllo, che si sostanzia nel piantonare i dispositivi e i soggetti di interesse, pur permettendo loro l'operatività sotto la stretta vigilanza di un militare. Ad ogni buon conto nel prosieguo vedremo anche quali ulteriori tecniche tendono ad impedire/evitare che il contribuente apporti modifiche, accesso durante, allo stato delle cose.

La circolare 1/2018

La circolare è stata pubblicata per la prima volta il 4 dicembre 2017 e rappresenta lo sforzo compiuto per aggiornare ed innovare le metodologie ispettive demandate al Corpo. Ad un decennio di distanza fa seguito alla precedente circolare 1/2008 e costituisce pertanto il necessario aggiornamento adottato dal Corpo per delineare le nuove metodologie di controllo ed ispettive già utilizzate dagli operatori per l'espletamento delle verifiche e dei controlli che oggi si sviluppano in evoluti e nuovi contesti connaturati dalla onnipresenza di dati digitali. A tal proposito basti pensare alla rivoluzione apportata in questi contesti dalla introduzione della cd. "fatturazione elettronica"[3]. La circolare in esame è alquanto corposa e suddivisa in 4 volumi per complessive 1.251 pagine che trattano ad ampio spettro il contrasto all'evasione e alle frodi fiscali. Un indice di massima, può aiutare a comprendere meglio la vastità dell'elaborato, che potremo così riassumere:

VOLUME I

PARTE I: L'azione della Guardia di Finanza a contrasto dell'evasione e delle frodi fiscali. Direttive generali e moduli operativi;

PARTE II: L'attività di polizia giudiziaria a contrasto dell'evasione e delle frodi fiscali;

VOLUME II

PARTE III: Esecuzione delle verifiche e dei controlli;

PARTE IV: Valorizzazione delle informazioni acquisite nell'ambito delle attività investigative, di vigilanza e di controllo dei flussi finanziari;

VOLUME III

PARTE V: Principali metodologie di controllo;

VOLUME IV

Modulistica e documentazione di supporto.

Va dato atto a questa circolare, seppur dopo 10 anni di aver preso seriamente in considerazione quegli aspetti di *digital-forensics* già delineati dalla legge 48/2008 che, trovato recepimento in specifiche modifiche apportate al codice di procedura penale, non avevano ancora trovato "indirizzo" nelle attività amministrative demandate al Corpo.

Proprio la particolarità della "mission" riconosciuta al Corpo, fa sì che questo più di altri corpi di Polizia del nostro Paese, sia oggi chiamato a confrontarsi in un mondo digitale a cavallo tra ambiti amministrativi e penali di non sempre facile qualificazione e specificazione ma che anzi, spesso, risultano profondamente compenetrati tra loro. Sul tema per quanto qui di interesse preme evidenziare che la stessa circolare dispone:

"Infatti, l'individuazione, nel corso dell'attività di verifica fiscale, di elementi che possano indicare l'esistenza di un fatto costituente reato determina l'obbligo di rispettare il disposto di cui all'art. 220 delle disposizioni di attuazione, coordinamento e transitorie del codice di procedura penale, a mente del quale "quando nel corso di attività ispettive o di vigilanza previste da leggi o decreti emergano indizi di reato, gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale, sono compiuti con l'osservanza delle disposizioni del codice".[4]

Pertanto, qualora nel corso di un controllo emergano indizi di reità assisteremo ad un cambio di paradigma anche in ordine alle modalità di ricerca, acquisizione ed assicurazione delle fonti di prova digitali. Una delle criticità maggiori è rappresentata da talune fattispecie delittuose che prevedono delle "soglie"[5], che spesso vengono determinate al termine del controllo ed in ogni caso quasi sempre in una fase di molto successiva all'accesso fiscale che ha visto l'acquisizione delle evidenze digitali. È qui

3 La legge 27 dicembre 2017, n. 205 (legge di Bilancio 2018) , in luogo del previgente regime opzionale, ha previsto sia nel caso in cui la cessione del bene o la prestazione di servizio è effettuata tra due operatori Iva (operazioni B2B,cioè Business to Business), sia nel caso in cui la cessione/prestazione è effettuata da un operatore Iva verso un consumatore finale (operazioni B2C, cioè Business to Consumer) l'obbligo di emettere soltanto fatture elettroniche attraverso il Sistema di Interscambio a partire dal 1° gennaio 2019.

4 Pag. 122 – Volume II.

5 Il reato tributario di dichiarazione infedele si verifica al superamento congiunto di due soglie di punibilità:
• Evasione d'imposta di 100.000,00 euro per ogni singola imposta (IRPEF o IVA).
• Elementi attivi sottratti all'imposizione (ricavi o costi) di almeno 3.000.000,00 euro. Tuttavia, se gli elementi fittizi indicati in dichiarazione (ricavi o costi) supera il 10% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione il reato è consumato anche se gli elementi sottratti ad imposizione sono inferiori a 3.000.000,00 euro.
Tuttavia con riferimento a quei reati che richiedono il superamento di una soglia la circolare richiama la si richiama (Cass. pen., 3 febbraio 2015, n. 4919) secondo la quale per rendere operante l'art. 220 disp. att. c.p.p. non occorre che sia stata già raggiunta la prova del superamento della soglia di punibilità, ma è sufficiente che vi sia una concreta probabilità che lo possa essere.

evidente come la circolare, tenuto conto della doppia veste amministrativo-panale indossata dal militare addetto ai controlli sia dovuta ricorrere a specifiche istruzioni che prendessero anche in considerazione il delicatissimo aspetto rivestito dalla *digital-evidence,* che rilevata in un ambito squisitamente "amministrativo", di lì a poco potrebbe assurgere a prova strategica in un processo penale. Come appena detto, accade spesso, che l'attività amministrativa svolta dal Corpo sia propedeutica all'emersione di fatti ben più gravi e penalmente rilevanti. In tale evoluzione la *digital-evidence,* deve necessariamente essere trattata e presentare specifiche caratteristiche onde non inficiarne la sua validità probatoria[6].
Bisogna anche premettere ed evidenziare come non esista una metodologia ufficiale che descriva le procedure di acquisizione forense. Come ben sappiamo, la *digital-forensics* nel panorama nazionale si basa essenzialmente su *best practices,* standard ISO, ed alcuni adeguamenti legislativi, in particolare la già citata Legge n. 48 del 2008 che, ratificando la Convenzione di Budapest del 2001, ha introdotto una serie di requisiti formali che l'operatore che opera sulla cd. "scena del crimine" deve conoscere e saper rispettare.

La ricerca di documenti informatici

Il tema viene trattato nel Volume II – Capitolo 2 – punto 2 lettera c. (5), la ricerca in questo particolare ambito è finalizzata all'individuazione dei dati digitali di interesse, ai fini del controllo fiscale, e consiste essenzialmente nella possibilità per gli operatori di svolgere per l'appunto ricerche anche contro la volontà e senza il consenso dell'interessato finalizzate alla individuazione di documenti digitali.
Rispetto le canoniche fasi della *digital-forensics* il documento ne ricalca alcune, prendendo essenzialmente in considerazione le seguenti: la ricerca (vedremo molto simile alla canonica fase di "Individuazione"); l'estrazione, (del tutto simile all'"Acquisizione") e l'assicurazione; delle evidenze digitali.
La ricerca preliminarmente, si sostanzia al di là di quanto spontaneamente esibito dal contribuente e di facile individuazione da parte dei militari (PC in uso, smartphone, tablet, altri supporti collegati al momento ed in uso) nella scoperta di quei dispositivi informatici occulti o comunque non facilmente individuabili a seguito di una preliminare ricognizione della postazione di lavoro. L'esperienza operativa conferma che molto spesso le cd. "contabilità parallele" / "contabilità occulte", vengono conservate (oltre a quanto vedremo nel prosieguo) su dispositivi facilmente occultabili[7], trasportabili e spesso non conservati in prossimità della normale strumentazione di lavoro proprio per essere più facilmente sottratti, all'attenzione dei militari operanti[8]. A ciò si aggiunga poi la sempre più capillare diffusione di micro-computer poco più grandi di un pacchetto di sigarette *(Raspberry)* oggi capaci non solo di essere gestiti da remoto ma anche capaci di supportare ingenti quantità di storage[9]. La ricerca quindi va estesa a seconda dei casi non solo ai classici spazi di custodia di tali dispositivi ma anche a spazi spesso impensabili[10]. Giova qui ricordare che l'apertura coattiva di determinati luoghi e oggetti (cassetti chiusi, casseforti, armadi, borse, valigie) richiede l'autorizzazione del Pubblico Ministero solo di fronte all'espressa opposizione da parte del contribuente. Tale approccio viene confermato dalla circolare in esame volume II – parte III – capitolo 2 *"Poteri esercitabili",* pag. 24. Con particolare riferimento all'esame di pieghi sigillati, borse, casseforti, mobili e ripostigli, il citato documento di prassi evidenzia, richiamando la giurisprudenza di legittimità, che l'autorizzazione del Procuratore della Repubblica è richiesta solo nel caso di *"apertura coattiva"* e non anche, quindi, quando l'attività di ricerca si svolga con la collaborazione del contribuente o nel caso in cui cassetti e armadi non siano chiusi a chiave (cfr. Corte di cassazione, sentenza n. 3204 del 18.02.2015). Di recente poi, la suprema Corte di cassazione con l'ordinanza n. 24306 del 4.10.2018 ha confermato che il provvedimento del magistrato non si rende necessario qualora il contribuente acconsenta spontaneamente all'apertura, ad esempio, di una borsa di un dipendente aziendale.
Ritornando alle ricerche ciò che in tale ambito fa la differenza tra un successo ed un fallimento da parte dei militari operanti è l'esperienza operativa ed a volte la fortuna[11], fermo restando che è logico ritenere che ciò è occultato, sarà il primo target da esaminare con particolare attenzione. In conclusione qualsiasi supporto e dispositivo può potenzialmente costituire "interesse" ai fini investigativi sia quelli rilevabili a colpo d'occhio sia quelli rinvenuti a seguito delle ricerche. Tuttavia, giova qui ricordare e precisare che la ricerca non esaurisce la sua azione nell'individuazione del dispositivo/supporto (contenitore) ma allarga sempre la propria attività anche al suo contenuto (files contenuti sul supporto).
Occorre anche evidenziare che:
- dette ricerche si rendono necessarie non solo con riferimento ai dati di natura contabile, quanto, soprattutto, a quelli di carattere extracontabile sviluppati dal contribuente per finalità di controllo gestionale ovvero per altre esigenze interne che, tuttavia, possono rivelarsi comunque utili ai fini di una compiuta comprensione e determinazione della capacità contributiva del soggetto e di conseguenza ad una esatta determinazione delle imposte dovute all'Erario;

6 Sul punto la circolare pag. 124 - Volume II – ricorda che: "sono processualmente inutilizzabili i verbali redatti successivamente all'insorgere degli indizi di reato, qualora non siano state rispettate le disposizioni del codice di procedura penale, così come è privo di rilevanza di prova, ai sensi dell'art. 234 c.p.p., il processo verbale di constatazione nella parte in cui recepisce i contenuti di atti di acquisizione probatoria effettuati senza l'osservanza delle disposizioni del codice di rito (Cass. pen., 30 gennaio 2015, n. 7930)".

7 Oggi con poche decine di euro si possono acquistare per drive USB di piccole dimensioni ma con capacità di 128GB o superiori, ben capaci di conservare una moltitudine di file.

8 Il personale viene addestrato anche a simulazioni nel corso delle quali si apprendono le principali tecniche di mimetizzazione dei dispositivi man mano che vengono scoperte nel corso dei controlli.

9 Il progetto Raspberry è in continua evoluzione e si tratta di un microcomputer al quale oggi possono essere collegati via USB3 dischi della capacità di alcuni Terabyte, oltre alla microSD dedicata al sistema operativo che oggi possono raggiungere dimensioni di 128 Gigabyte e superiori.

10 Anche l'utilizzo di App specifiche per la ricerca di reti ed hotspot (Fing, OpenSignal, Wi-Fi Map) possono aiutare nell'individuazione di reti ad hoc create dal soggetto controllato per scopi estranei all'ordinaria gestione aziendale.

11 Manager che recava nella stecca del colletto della camicia una microSD da 128GB contenente i dati di una gestione parallela di magazzino; Raspberry nel controsoffitto dell'ufficio rilevata solo grazie all'acume del militare che individuava un "collegamento" sul Desktop "dati da non inviare" e centinaia di altri.

- devono essere svolte con la continua assistenza del contribuente o suo delegato e dove possibile, tutte le operazioni di acquisizione di materiale e/o supporti informatici devono svolgersi con l'assistenza di personale specializzato del soggetto sottoposto a controllo, arrecando ove possibile minor pregiudizio alle attività svolte;

Quanto alla prima precisazione è evidente come al di là del mero dato contabile (si pensi per esempio, ad una fattura relativa ad una operazione economica) possano rilevare in maniera determinante quei documenti cd. "extracontabili" che tuttavia potrebbero confermare, smentire, rettificare, delineare nei suoi tratti effettivi, la stessa operazione (si pensi alle email, appunti, lettere, conversazioni via Skype etc. relative a quel fatto economico). La stessa giurisprudenza di legittimità, ha precisato che i documenti informatici estrapolati legittimamente dai computer nella disponibilità dell'imprenditore, nei quali sia contenuta contabilità non ufficiale, costituiscono, in quanto scritture dell'impresa stessa, elemento probatorio, sia pure meramente presuntivo, utilmente valutabile, salva la verifica della loro attendibilità[12].
Circa la seconda precisazione, nel sancire il divieto di eseguire operazioni direttamente sugli apparati in uso al contribuente in assenza di un suo espresso consenso[13], il personale che può fornire assistenza qualificata può identificarsi nel responsabile dei sistemi IT, o dove non presente nell'utilizzatore del dispositivo. Vanno evitate se non per specifici casi più gravi (accessi in assenza di personale, mancata collaborazione) azioni che vedano ricerche effettuate dai soli militari in totale autonomia e senza consenso. La collaborazione da parte del responsabile dei sistemi IT o suoi delegati, va precisato, è quasi sempre necessaria anche a poter svolgere le operazioni più elementari che richiedono il superamento delle misure di sicurezza, oltre che per evidenti motivi di controllo circa l'operato dei verificatori sulle metodologie, tecniche ed eventuali software utilizzati per le ricerche[14]. Evidente è poi l'indispensabile collaborazione laddove vi sia la necessità di accedere ai server aziendali[15] o ancora ai personal computer oggi più che un tempo a seguito del GDPR sottoposti ad un più stringente regime di sicurezza finalizzato alla "protezione dei dati ivi contenuti" che richiedono spesso l'intervento di detto personale in possesso delle necessarie user e password per accedere quali "amministratori" al dispositivo; ma anche più banalmente alla necessità di avviare specifici software per la ricerca/individuazione dei files di interesse e loro acquisizione qualora gli stessi richiedano per l'appunto privilegi amministrativi. Capita poi che il "centro" di controllo della rete IT aziendale spesso non coincida con la sede dell'accesso e sempre più spesso risulti collocato fisicamente all'estero. In questi casi il personale IT presente presso il luogo dell'accesso non ha poteri amministrativi tali da poter consentire l'accesso all'intera rete e a sua volta deve interfacciarsi con chi è in possesso di questi poteri per poter accedere a determinati servizi. Questo è uno dei casi più complessi ma sempre più frequente ed oltre a presentare notevoli difficoltà tecniche vede molto spesso comportamenti reticenti giustificati da diversi motivi spesso di difficile se non impossibile accertamento soprattutto in assenza di condizioni di reciprocità nell'applicazione della normativa fiscale tra il nostro Paese e quello di ubicazione del server. Data la complessità ed alto livello di tecnologia ormai posseduto dalle aziende di rilevanti dimensioni il Corpo ha previsto con lungimiranza la presenza nella pattuglia operante di personale in possesso di adeguate cognizione tecniche, ancorché non munito di specifiche qualifiche, ma comunque capace di "interfacciarsi" efficacemente con i responsabili IT dell'azienda ispezionata. Ciò anche al fine di ottimizzare e rendere attuabili le operazioni di ricerca, individuazione ed acquisizione del dato digitale nel rispetto delle necessità investigative e quelle di privacy, tutela del segreto, ed altre eventualmente avanzate dal soggetto ispezionato.
In merito al proprio personale, il Corpo ha avviato da tempo iniziative dirette alla formazione di due figure:
- First Responder;
- C.F.D.A. – Computer Forensic Data Analysis.
Queste due figure traggono la loro origine nella ISO/IEC 27037 – Guidelines for identification, collection, acquisition, and preservation of digital evidence – Annex A[16] ed intervengono su diversi gradi di com-

12 Cass. civ., 9 marzo 2016, n. 4600; Cass. civ., 3 ottobre 2014, n. 20902; Cass. civ., 30 marzo 2012, n. 5226.

13 In caso di diniego è concesso ai verificatori di procedere all'elaborazione dei dati ivi contenuti successivamente, al di fuori dei locali del contribuente, con ciò attribuendo agli stessi, evidentemente, anche la facoltà di adottare gli accorgimenti necessari a tale scopo. Ovviamente di tale rifiuto alla collaborazione deve essere fatta esplicita menzione nei processi verbali redatti, con indicazione delle modalità specifiche con cui i dati del contribuente sono stati successivamente elaborati e delle misure adottate per garantirne la conservazione e la genuinità.

14 Si pensi alle conseguenze insite nell'utilizzo di tecniche o software che potrebbero se non danneggiare creare anche solo disservizi temporanei non preavvisati all'intera linea produttiva. Di questi tempi sono le difficoltà legate ad accessi in aziende che sopravvivono grazie al telelavoro smart-working e per un attimo si pensi a quali problemi potrebbe creare il distacco di una VPN allo scopo adibita effettuata da personale non esperto e non debitamente assistito.

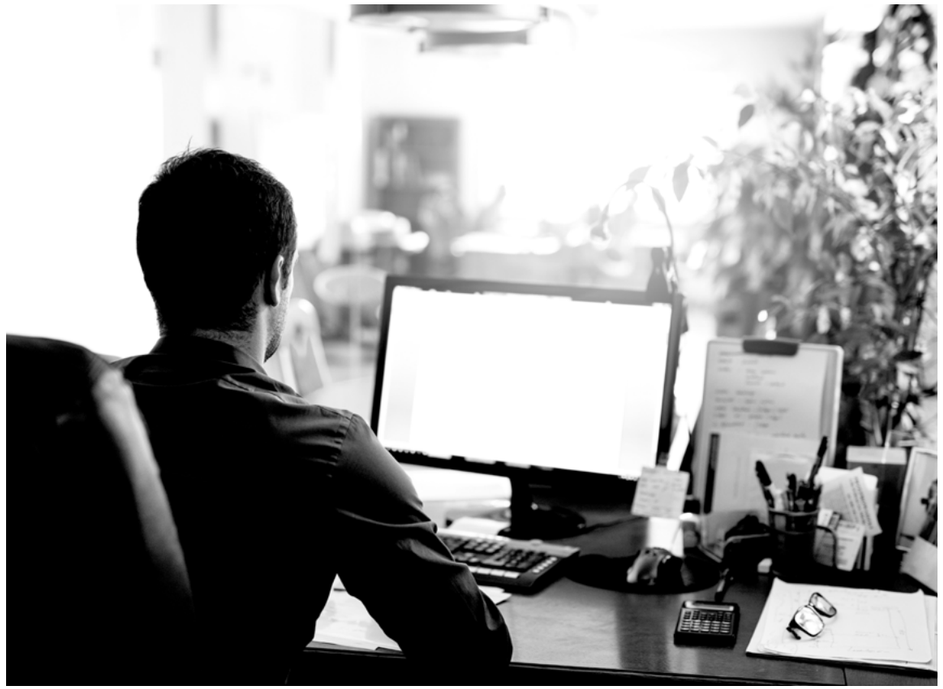
15 È evidente come la conoscenza del server sia "patrimonio" dell'amministratore IT e come sia importante conoscerne a fondo i sistemi di difesa. Al fine di proteggere un server da accessi non autorizzati i server sono solitamente isolati dalle reti pubbliche con firewall e zone demilitarizzate (DMZ).Vi sono poi i sistemi di rilevamento degli attacchi, i cosiddetti Intrusion Detection System (IDS), che servono a monitorare automaticamente i server e le reti e a lanciare l'allarme, non appena vengano registrati tentativi di accesso non autorizzati o attacchi automatici tramite software dannosi e gli Instrusion Prevention Systems (IPS).

16 L'ISO (Organizzazione Internazionale per la Standardizzazione) e l'IEC (Commissione Elettrotecnica Internazionale) formano il sistema specializzato per la standardizzazione delle procedure a livello mondiale, in materia di Digital Forensics. Tra i vari standard promossi dall'ISO vi sono quelli che riguardano l'informatica forense che si candidano a norme tecniche di riferimento effettivamente discusse e riconosciute a livello internazionale. L'unico standard attualmente emanato in versione definitiva è lo standard ISO/IEC 270372012. È un documento che contiene le linee guida di riferimento nel settore dell'informatica forense per le fasi di identificazione, raccolta, acquisizione e conservazione delle prove digitali necessarie in una qualsiasi indagine che deve mantenere l'integrità delle stesse. Il documento prevede che i soggetti responsabili gestiscano le potenziali prove digitali con metodologie che risultino adeguate su scala mondiale, con l'obiettivo di facilitare le investigazioni riguardanti i dispositivi e le prove digitali in maniera sistematica e imparziale, preservandone al contempo l'integrità e l'autenticità. Il documento individua i seguenti soggetti:

• Digital Evidence First Responders (DEFR), soggetto autorizzato, preparato e qualificato per intervenire per primo sulla scena di un incidente raccogliendo ed acquisendo le prove digitali con la responsabilità della loro gestione;

• Digital Evidence Specialists (DES), soggetto che svolge le mansioni di un DEFR ed ha conoscenze specialistiche, capacità ed abilità nella gestione di una grande varietà di questioni tecniche;
• specialisti di Incident Response (IR);

• specialisti di laboratori di informatica forense.
Il Corpo della Guardia di Finanza individua una corrispondenza tra DEFR e DES con i soggetti qualificati CFDA riconoscendo invece le residue figure previste dalla ISO (IR e specialità di laboratorio) alla Polizia Postale e al R.I.S. dei Carabinieri.



plessità se il First Responder risulta pressoché ormai necessario in ogni situazione, il supporto del personale C.F.D.A. è invece riservato a quegli accessi rivolti a imprese appartenenti a gruppi multinazionali che potrebbero impiegare sistemi di comunicazione e di memorizzazione delle informazioni condivisi al proprio interno, così che l'estrazione informatica presso la singola entità in verifica potrebbe anche avere riverberi sulle altre consociate ovvero sul sistema nel suo complesso.
È facile comprendere come la globalizzazione abbia tra le tante conseguenze anche un enorme diffondersi di aziende che oggi presentano le complessità sopra delineate, ovvero sistemi informatici sempre più interconnessi tra società e realtà economico produttive appartenenti non solo a paesi diversi ma nei confronti delle quali si applicano anche giurisdizioni differenti. In tali ultimi casi, l'elevato tasso di dematerializzazione delle operazioni economiche e la difficoltà di applicare i tradizionali criteri di collegamento, fisici e territoriali, per stabilire il luogo di tassazione degli utili delle imprese che vi ricorrono, rende imprescindibile l'acquisizione dei dati informatici, ovunque presenti e di qui la necessità di adibire ad operazioni così complesse personale adeguatamente addestrato sul piano tecnico e giuridico ad affrontare problematiche di tale natura. Invero la circolare in diversi punti, a fattor comune consiglia l'impiego di dette unità quando la verifica riguardi contribuenti che adottano sistemi digitali complessi e così anche nei casi in cui siano in corso attività di polizia giudiziaria ovvero nell'ambito di interventi che possano verosimilmente condurre all'individuazione di elementi di prova di responsabilità penali.
Sperando di aver suscitato interesse, rinvio ad una seconda parte, il prosieguo di questo lavoro che per la complessità dei temi affrontati non può qui esaurirsi.

L'impatto del Covid sulle organizzazioni e sulla salute psicologica dei lavoratori: un anno dopo

di Diletta Mora e Alessandro De Carlo

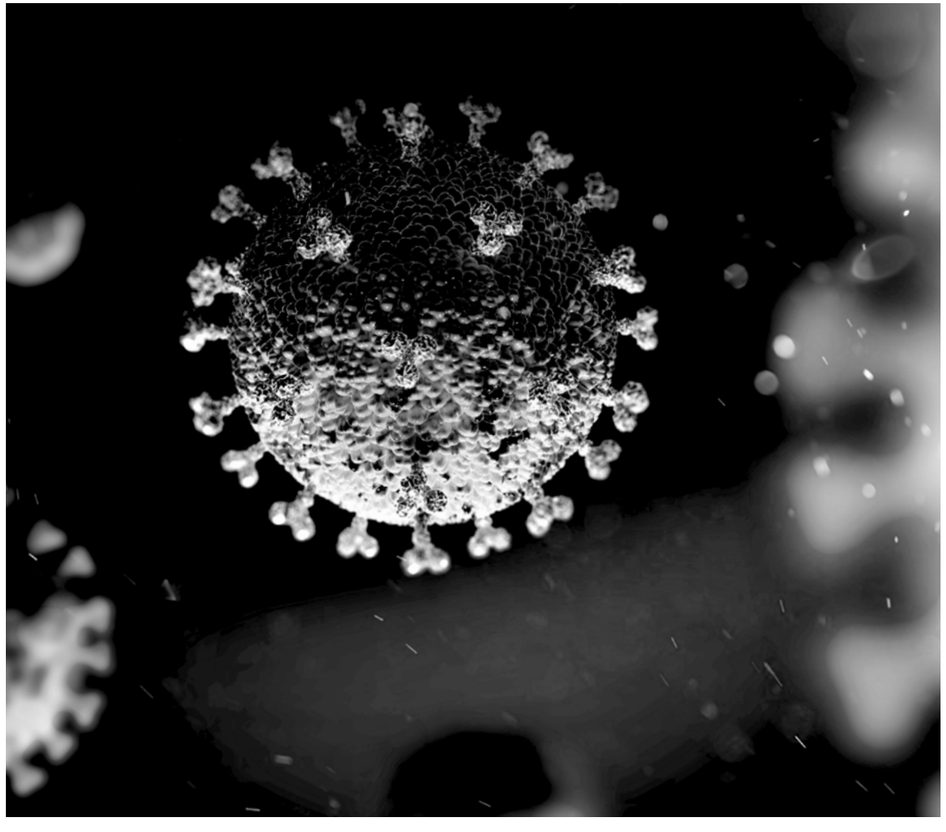
Fin dal suo esordio nella città di Wuhan (Cina) alla fine del 2019, la malattia COVID-19, causata da un nuovo coronavirus denominato SARS-CoV-2, ha drasticamente alterato le strutture sociali di tutto il mondo. L'11 marzo 2020, l'Organizzazione Mondiale della Sanità (OMS) ha annunciato che il COVID-19 può essere definito una pandemia per via dell'elevato numero di contagi in tutto il mondo. In Italia, il 21 febbraio 2020, l'Istituto Superiore di Sanità (ISS) ha confermato il primo caso di COVID-19, e nell'arco di un mese il Paese si è reso protagonista di una rapida ondata di contagi, diventando rapidamente il secondo Paese più colpito al mondo dal coronavirus. La prima linea di difesa contro questa pandemia è stata la riduzione dell'interazione fisica, a discapito delle relazioni sociali. Il governo italiano ha stabilito un blocco nazionale che ha permesso alle persone di lasciare le loro abitazioni solo per comprovate esigenze lavorative, di salute o di estrema necessità. Questo ha costretto la maggior parte delle aziende, pubbliche e private, a ricorrere allo smart working. Da allora, il COVID-19 ha afflitto milioni di persone in tutto il mondo, con gravi ripercussioni non solo sulla salute psicofisica di ognuno, ma anche nei settori economico e lavorativo. Ad oggi, secondo un recente rapporto dell'OMS, il numero di casi globali di COVID-19 è cresciuto oltre i 260 milioni, con più di 5 milioni di morti. In Italia i casi confermati sono circa 5 milioni, con poco più di 130.000 decessi (Organizzazione Mondiale della Sanità, 2021).
Ad oltre un anno dal suo esordio, molti sono gli studi che analizzano l'impatto che tale pandemia ha avuto per il mondo organizzativo e i suoi lavoratori. Di seguito verrà presentata una rassegna delle principali conseguenze relative al COVID-19.

La sicurezza nei luoghi di lavoro: una risorsa contro l'esaurimento emotivo
Ad oggi grande attenzione è stata dedicata alla salute e sicurezza degli operatori sanitari sul lavoro, che si sono trovati in prima linea a dover gestire la situazione emergenziale. Quest'ultimi sono stati esposti a diversi rischi psicofisici e sociali non indifferenti, basti pensare al carico di lavoro eccessivo, all'impatto emotivo, alle severe restrizioni al fine di contrastare i contagi, ad esempio i contatti ridotti con pazienti e fa-

miliari, nonché alla percezione del rischio di essere contagiati e di contagiare i propri cari, con notevoli conseguenze in termini di stress e riduzione del benessere individuale. Inoltre, a queste preoccupazioni, per gli operatori sanitari si aggiunge un'atra fonte di stress e sofferenza, ovvero essere vittima di stigma sociale. Si tratta di mettere in atto comportamenti discriminatori, di attribuire connotazioni negative a una persona (o gruppo di persone) che hanno in comune una specifica malattia o, come in questo caso, hanno a che fare con una malattia altamente contagiosa. Molti operatori sanitari sono stati, dunque, etichettati e stereotipati a causa del legame percepito con il COVID-19. Ovviamente, le ripercussioni negative dello stigma si riversano sia su coloro che sono affetti dal virus, inibendone l'accesso all'assistenza sanitaria, sia sui professionisti che lavorano sul campo, aumentando la percezione di stress.

Tuttavia, non solo gli operatori sanitari, ma tutti i lavoratori operanti in diversi settori professionali stanno tutt'oggi affrontando il rischio di essere contagiati dal virus nei luoghi di lavoro: i contesti organizzativi, a causa della vicinanza fisica e dello stretto contatto sociale con colleghi e utenti, possono facilitare la diffusione del COVID-19. Pertanto, oggi più che mai, la sicurezza nei luoghi di lavoro svolge un ruolo centrale nelle organizzazioni: in termini di prevenzione e promozione della salute, i fattori organizzativi associati al COVID-19, che possono avere un impatto psicofisico, devono essere considerati con attenzione. A tal proposito, Falco e collaboratori (2021) si sono focalizzati sulla sicurezza, sia fisica che psicologica, nei luoghi di lavoro. Gli autori hanno fatto riferimento al *Job Demands-Resources Model* (JD-R Model) di Bakker e Demerouti (2017), che prevede due dimensioni principali:

• *job-demands* (richieste lavorative) – definite come gli aspetti fisici, sociali, psicologici o organizzativi del lavoro che richiedono uno sforzo (fisico e psicologico) tale per



cui vengono associati a costi fisiologici e/o psicologici; alcuni esempi di richieste sono il sovraccarico lavorativo e l'ambiguità di ruolo;

• *job-resources* (risorse lavorative) – definite come gli aspetti fisici, sociali, psicologici o organizzativi del lavoro che sono funzionali al raggiungimento degli obiettivi, alla promozione della crescita personale e alla riduzione delle richieste lavorative; alcuni esempi di risorse lavorative sono l'autonomia, il sostegno sociale e i feedback chiari.

Seguendo il JD-R Model, gli autori considerano la percezione del rischio di essere contagiati dal COVID-19 come una richiesta lavorativa, dunque un fattore di rischio per il benessere dell'individuo, mentre le condizioni che aiutano i lavoratori a gestire tale rischio, ad esempio i sistemi di sicurezza, la comunicazione chiara, la corretta gestione della fatica e la partecipazione ai processi decisionali, vengono considerate come risorse lavorative. Coerentemente con il modello teorico di riferimento, dopo aver analizzato i questionari self-report di oltre 350 partecipanti, gli autori hanno rilevato che la percezione del rischio di essere contagiati sul lavoro è positivamente associata all'esaurimento emotivo. Tuttavia, le risorse lavorative si associano negativamente all'esaurimento emotivo e moderano la relazione tra quest'ultimo e la percezione del rischio di essere contagiati: maggiori sono le risorse percepite, meno intensa è la relazione tra la percezione del rischio e il distress emozionale. Inoltre, è stato rilevato che anche l'affettività negativa, una dimensione disposizionale che riflette le differenze individuali pervasive nell'emotività negativa e nel concetto di sé, modera la relazione tra la percezione del rischio e lo stress psicofisico, intensificandola quando vengono registrati elevati livelli del costrutto (Girardi et al., 2021). Nella prospettiva di prevenzione e promozione della salute e del benessere, i risultati evidenziano la necessità di ridurre la percezione di rischio di essere contagiati, rafforzando, ad esempio, quelle caratteristiche organizzative che permettono ai lavoratori di meglio gestire il rischio percepito.

Lo smart working nel periodo emergenziale: vantaggi e criticità

Come già evidenziato, un altro importante cambiamento per i contesti organizzativi è stato l'utilizzo dello smart working. Il termine fa riferimento a una modalità di lavoro subordinato caratterizzato dall'assenza di vincoli orari o spaziali e da un'organizzazione per fasi, cicli e obiettivi, stabilita mediante accordo tra dipendente e datore di lavoro. Si tratta di una modalità di lavoro che permette da una parte la conciliazione vita-lavoro, dall'altra la crescita della produttività. In letteratura troviamo quattro requisiti fondamentali che determinano la corretta esecuzione dello smart working (De Carlo & Maccani, 2021):

1) l'attività lavorativa deve essere svolta in modo adeguato per via informatica/telematica;
2) la strumentazione tecnologica e informativa deve essere idonea;
3) il conseguimento degli obiettivi deve guidare la valutazione della prestazione, portando a una responsabilizzazione del lavoratore;
4) la garantita disponibilità di un luogo adeguato dove svolgere la propria attività.

Oltre ai requisiti, è bene evidenziare i principali obiettivi dello smart working: 1) andare oltre la mera esecuzione dei compiti, focalizzandosi e promuovendo la logica del *Management by Objectives* (MBO), prefissando e condividendo con i lavoratori degli obiettivi specifici; 2) promuovere una maggiore autonomia e gestione proattiva della propria attività lavorativa; 3) migliorare la qualità, la produttività e la performance attraverso la promozione di una crescente responsabilizzazione dei lavoratori, tutelando, allo stesso tempo, la salute e il benessere individuale e organizzativo.

Lo smart working, tuttavia, non è stato applicato allo stesso modo nei diversi contesti organizzativi: in ambito privato, tale modalità di lavoro è stata applicata solo quando fossero presenti i requisiti fondamentali descritti ai punti 1 e 2 (cercando comunque di perseguire anche i requisiti 3 e 4); in gran parte dell'ambito pubblico, invece, lo smart working è stato praticato senza tenere in considerazione alcun requisito sopracitato. Inoltre, in entrambi i

settori non si è potuto tenere molto conto dell'integrazione tra i principali obiettivi dello smart working e i requisiti fondamentali per via della crescente pressione esercitata dalla situazione emergenziale. Tuttavia, le esperienze riportate da alcuni lavoratori operanti sia in ambito pubblico che privato sono positive. Nell'ultimo anno un gruppo di psicologi operanti in ambito sanitario ed educativo hanno raccolto le percezioni di diversi lavoratori sulle opportunità e sui limiti dello smart working (Rapisarda et al., 2021).
Tra i principali vantaggi si riportano:
• riduzione dei costi e dei tempi per recarsi a lavoro;
• riduzione dei costi per il rifornimento del proprio mezzo di trasposto e per il parcheggio;
• riduzione dei costi per la ristorazione;
• ampliamento della sfera della vita familiare;
• riduzione del conflitto vita-lavoro.
Le principali criticità vengono di seguito riportate:
• difficoltà nella conciliazione vita-lavoro, soprattutto per le donne;
• percezione di solitudine e isolamento;
• ambienti della propria abitazione da dedicare al lavoro ristretti e da condividere con il resto della famiglia;
• riduzione della percezione del tempo libero;
• difficoltà nella comunicazione con colleghi e superiori.
I risultati evidenziano una necessaria maggiore organizzazione dello smart working, integrando in maggior misura i requisiti necessari e gli obiettivi fondamentali sopra definiti, ampliando il supporto ai lavoratori con interventi di benessere organizzativo attraverso, ad esempio, sportelli e servizi di ascolto attivo.

L'impatto del COVID-19 sulla salute psicologica dei lavoratori

L'esperienza emergenziale vissuta è considerata un trauma collettivo, il quale si verifica quando un'intera società avverte un'intensa minaccia che non è in grado di gestire; allo stesso modo, il COVID-19 è stato percepito da molti come una minaccia per sé stessi o per i propri cari. Inoltre, si aggiungono le preoccupazioni relative alla capacità di accedere alle risorse, mantenere l'occupazione, prendersi cura dei propri cari e gestire le attività di prevenzione del contagio. A tutto ciò si aggiunge il trauma per la perdita e il dolore: perdita di persone care, di opportunità, di risorse, di controllo e di molto altro. I professionisti che si occupano di salute psicologica e gli altri lavoratori che operano nel sociale percepiscono una maggiore sofferenza: da una parte vivono le esperienze di perdita personali, dall'altra vivono i traumi degli utenti con distress emotivo associato al periodo emergenziale a cui forniscono assistenza.
Holmes e collaboratori (2021) in un loro studio hanno esplorato l'entità dello stress post traumatico, del dolore e del burnout percepiti dai professionisti operanti nel sociale che durante il periodo pandemico hanno prestato il loro supporto. Allo studio hanno partecipato 181 lavoratori, per lo più donne. I risultati dello studio hanno evidenziato che più del 25% dei partecipanti ha riportato sintomi di stress post-traumatico. Nello specifico, i sintomi maggiormente riportati facevano riferimento a pensieri intrusivi e ad alterazioni dell'umore e della reattività. Inoltre, sono stati riportati percezioni di dolore e vulnerabilità associate al lutto e alla perdita. Sebbene la quasi totalità dei partecipanti abbia riportato livelli medio-alti di soddisfazione per la propria attività lavorativa, il 68% ha manifestato livelli medi di burnout.
Lo studio ha inoltre esaminato la capacità organizzativa di affrontare lo stress prima e durante la pandemia di COVID-19 (Fig. 1). Sebbene la promozione di interventi volti al benessere organizzativo (es. yoga, meditazione) e le opportunità per i colleghi di fornirsi supporto reciproco siano diminuite significativamente durante la pandemia di COVID-19, non ci sono state variazioni significative tra le altre aree valutate nello studio (debriefing promossi dall'organizzazione, sessioni di supporto organizzativo dopo eventi importanti o stressanti, supervisori che offrivano opportunità di discutere e/o gestire l'esposizione a traumi).

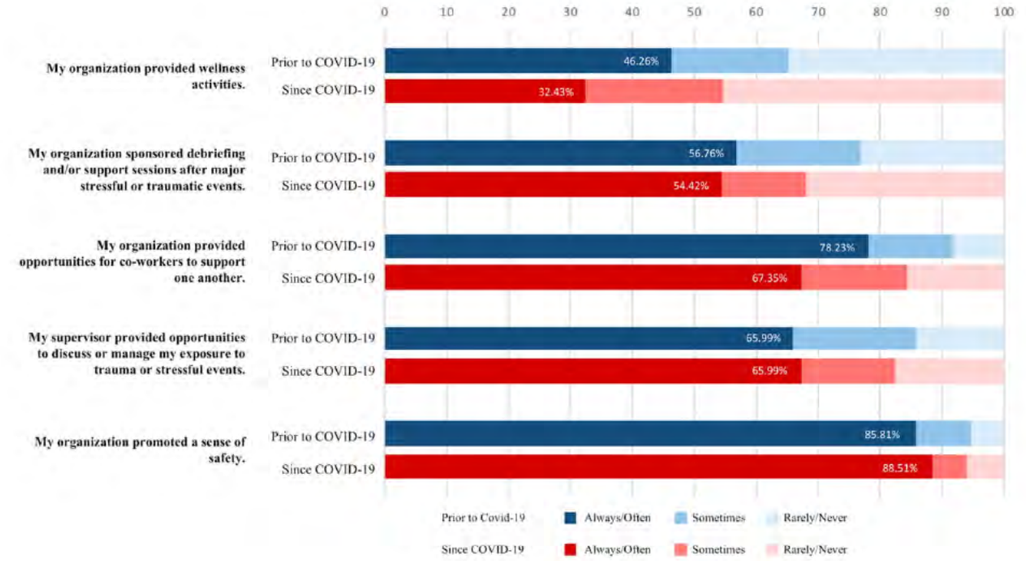


Fig. 1 Percezione del supporto organizzativo prima e durante la pandemia di COVID-19 (Holmes et al., 2021, p. 501)

Le nuove tecnologie per la promozione della salute organizzativa e individuale

I diversi studi analizzati evidenziano l'importante ruolo delle organizzazioni nel supporto ai lavoratori. Chi si occupa della gestione delle risorse umane ha la responsabilità di potenziare le risorse lavorative e individuali di ogni lavoratore, al fine di creare un serbatoio di risorse utili a fronteggiare i momenti difficili che causano disagio psicologico e abbassamento della performance organizzativa. È necessario operare interventi mirati ed efficaci, che promuovono la salute organizzativa e individuale.
Ad oggi, la tecnologia può essere una valida alleata per la costruzione di strumenti e protocolli per il supporto psicologico ai lavoratori, permettendo di intervenire nelle condizioni di disagio venutesi a creare a seguito della pandemia di COVID-19. Nello specifico, negli ultimi anni diversi studi hanno analizzato e confermato l'efficacia di interventi erogati attraverso gli strumenti della realtà virtuale. Tali interventi, grazie alla capacità della realtà virtuale di massimizzare l'esperienza di chi ne usufruisce, si rivelano particolarmente adatti alla promozione di tecniche utili alla gestione dell'ansia e dello stress, ormai fenomeni percepiti quotidianamente nei contesti organizzativi. Grazie alla possibilità di essere immersi in un ambiente virtuale, sicuro e gestito totalmente dal professionista, i lavoratori possono vivere un'esperienza unica, che promuove l'apprendimento di diverse tecniche e strategie (es. mindfulness), rendendo l'intervento maggiormente efficiente ed efficace (Mora et al., 2021). Altri studi, hanno valutato l'efficacia della telehealth. Nello specifico, il supporto psicologico online si è dimostrato efficace tanto quanto l'intervento face-to-face. Questo ha permesso a molti professionisti di continuare a supportare i propri utenti anche durante il periodo emergenziale, che costringeva la maggior parte della popolazione a operare dalla propria abitazione. L'intervento psicologico online non solo viene percepito ugualmente efficace da quello in presenza, ma porta con sé diversi vantaggi: il superamento delle barriere architettoniche e di quelle legate alla distanza; il mantenimento della relazione terapeutica con l'utente; la possibilità di supportare i lavoratori anche al di fuori del contesto organizzativo;

una maggiore flessibilità e miglior gestione dei tempi e degli spazi (De Carlo et al., 2021).
Grazie alle tecnologie è possibile far fronte a diversi disagi che ancora oggi, purtroppo, incidono sulla salute organizzativa e individuale dei lavoratori. Si rendono sempre più necessari interventi di ascolto attivo, supporto professionale e assistenza al lavoratore, i quali permettono di meglio fronteggiare situazioni difficili e stressanti, monitorando al contempo il rischio di stress lavoro-correlato. Gli interventi psicologici, coadiuvati dalle nuove tecnologie, oggi più che mai si trovano a dover supportare le aziende per fronteggiare i disagi percepiti e superare le situazioni di criticità.

Bibliografia

De Carlo, A., Mora, D., Di Sipio, A., & Girardi, D. (2021, settembre). *Essere psicologi online: uno studio qualitativo.* XVIII Congresso Nazionale AIP – Sezione di Psicologia per le Organizzazioni, Verona.
De Carlo, N. A., & Maccani, I. (2021). *Codice smart working.* Trento: SEAC.
Falco, A., Girardi, D., Dal Corso, L., Yildirim, M., & Converso, D. (2021). The perceived risk of being infected at work: An application of the job demands–resources model to workplace safety during the COVID-19 outbreak. *Plos One, 16*(9), e0257197. https://doi.org/10.1371/journal.pone.0257197
Girardi, D., De Carlo, A., Dal Corso, L., Di Sipio, A., & Falco, A. (2021, April). *Risk of Covid-19 infection at work and psycho-physical strain: The moderating role of negative affectivity.* [Paper presentation]. International Psychological Applications Conference and Trends – InPact 2021.
Holmes, M. R., Rentrope, C. R., Korsch-Williams, A., & King, J. A. (2021). Impact of COVID-19 pandemic on posttraumatic stress, grief, burnout, and secondary trauma of social workers in the united states. *Clinical Social Work Journal, 49,* 495-504.
Mora, D., Falco, A., Di Sipio, A., & De Carlo, A. (2021, aprile). *4 steps for fighting covid-related anxiety: An application of virtual reality in a small company.* International Psychological Applications Conference and Trends – InPact 2021.
Organizzazione Mondiale della Sanità (2021). *Coronavirus (COVID-19).* https://www.salute.gov.it/
Rapisarda, S., Ghersetti, E., Girardi, D., De Carlo, N. A., & Dal Corso, L. (2021, aprile). *Smart working and online psychological support during the COVID-19 pandemic: Work-family balance, well-being, and performance.* International Psychological Applications Conference and Trends - InPACT 2021.

I ruoli della privacy: titolare, contitolare, responsabile, autorizzato, DPO: casi particolari di nomina

Giulia Bontempini e Stefano-Francesco Zuliani

Come noto, l'approccio del GDPR alla disciplina della privacy è basato sulla c.d. "accountability", ovvero la "responsabilizzazione" del titolare del trattamento in punto privacy basata sulla gestione dei rischi. Con la cogente normativa europea la privacy è diventata infatti una attività "risk based" e come tutte le best practice in ambito di risk management parte anch'essa dal principio portante della corretta definizione di ruoli e responsabilità. La difficoltà in questo caso è la corretta individuazione non solo formale ma anche funzionale dei soggetti centro di imputazione giuridica della governance dei dati.

I ruoli secondo la normativa

Quando si parla di *privacy* la prima questione da affrontare è l'individuazione del Titolare del Trattamento, ovvero la persona o l'ente che individua le "*finalità e i mezzi del trattamento*"[1] e valuta il "*rischio per i diritti e le libertà delle persone fisiche*"[2]; è inoltre colui nei cui confronti l'interessato può esercitare i suoi diritti. Per spiegare il suo ruolo centrale, il Titolare del Trattamento è stato paragonato ad un "*mandante dell'omicidio*"[3]. Per la sua individuazione non è previsto alcun atto di nomina, in quanto la sua identificazione deriva automaticamente dall'effettivo potere decisorio esercitato nella pratica o, in altri casi, discende uno specifico obbligo normativo ad effettuare un determinato trattamento. Come già ribadito in passato dal Garante[4] [5], quando il trattamento è effettuato da una persona giuridica il Titolare è l'ente nel suo complesso (es: la società, il ministero, l'ente pubblico, l'associazione) e non taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all´esterno (es: l´amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante). Allo stesso modo, anche se un particolare dipartimento o unità di un'organizzazione ha una responsabilità operativa non può assumere il ruolo di Titolare.

L'importanza della corretta attribuzione del ruolo del Titolare è dovuta al fatto che rappresenta la principale figura destinataria delle pesanti sanzioni comminate negli ultimi tre anni dai Garanti europei e che in caso di ispezione è colui che deve dimostrare, con l'inversione dell'onere della prova, di aver garantito la *privacy by design e by default* in ogni suo trattamento. Infatti anche se con la novellazione del 2018[6] il Codice della Privacy ha rimosso l'inclusione del trattamento dei dati personali tra le attività pericolose[7] [8], il GDPR, nonostante la diversa formulazione[9], continua ad ispirarsi allo stesso modello.

Nello svolgimento delle attività di trattamento di dati personali che gli sono proprie, il titolare potrebbe trovarsi a comunicare i dati personali degli interessati a varie tipologie di destinatari, con lui legati con-

1 *GDPR art. 4.7 «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*

2 *(GDPR C.74) È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.*

3 *Avv Luca Bolognini, presidente dell'Istituto Italiano Privacy*

4 *GPDP Titolare, responsabile e incaricato - Individuazione del 'titolare del trattamento' - 9 dicembre 1997 [30915] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/30915*

5 *GPDP Titolare, responsabile, incaricato - Precisazioni sulla figura del 'titolare' - 9 dicembre 1997 [39785] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39785*

6 *D.Lgs. 101/2018*

7 *Art. 15 d.lgs 196/2003 Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.*

8 *Art. 2050 CC. Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno*

9 *GDPR art. 82 - 1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. 2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. 3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.*

trattualmente a vario titolo e la cui esatta qualificazione è uno degli elementi fondanti della legittimità della comunicazione effettuata e della corretta ripartizione delle responsabilità. Dal Titolare discendono, infatti, per nomina o contratto, gli altri ruoli: contitolare, responsabile, autorizzato e DPO.

Quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento vengono qualificati dal GDPR come "contitolari". Le rispettive responsabilità, soprattutto nei confronti degli interessati, devono essere determinate in modo trasparente da un accordo contrattuale.[10]

Il responsabile del trattamento è invece "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*"[11] e che deve offrire "*garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate*"[12], in assenza delle quali, in caso di infrazione, il Titolare risponderà per *culpa in eligendo*. Il responsabile non può mai determinare le finalità del trattamento in quanto il Titolare "*must decide on both purpose and means*"[13]. La sua individuazione non è un atto di nomina unilaterale del Titolare ma è un addendum contrattuale, denominato "Data Processing Agreement" (DPA), con obbligo di forma scritta, redatto secondo le specifiche dettate dall'art. 28 del GDPR quali specifici obblighi in merito alle garanzie da fornire, istruzioni da impartire e attività di supervisione. Queste ultime purtroppo vengono spesso citate solo sulla carta ma in caso di data breach la loro omissione espone il Titolare alla responsabilità per *culpa in vigilando*. Sul suo contenuto la Commissione Europea si è recentemente espressa emanando un documento di clausole contrattuali tipo[14]. Anche se il GDPR esclude la figura del responsabile *interno* del trattamento, talvolta per questo ruolo si specifica il fatto che sia *esterno* in quanto l'abrogata normativa italiana ante GDPR consentiva sia la nomina del responsabile interno che del responsabile esterno a seconda della sua individuazione tra dipendenti e collaboratori del Titolare oppure nei riguardi di un soggetto terzo. Un responsabile, se debitamente autorizzato dal Titolare, può a sua volta nominare dei sub responsabili[15] del trattamento con riferimento a specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano Titolare e responsabile primario.

Per l'ipotesi di trasferimenti di dati all'estero da parte di titolari, responsabili o sub responsabili (es: presso un data center posto al di fuori dei confini dello Spazio Economico Europeo), conseguentemente alla nota sentenza Shrems II già analizzata su queste pagine[16] [17], la Commissione Europea il 04/06/2021 ha emanato le nuove Clausole Contrattuali Standard (SCC)[18], mentre l'EDPB ha pubblicato le *Guidelines 04/2021 on codes of conduct as tools for transfers*[19].

Infine, anche le persone fisiche, siano esse dipendenti o consulenti esterni che operano sotto l'autorità diretta del Titolare e hanno accesso a dati personali, devono ricevere una specifica designazione corredata da adeguate istruzioni completate dall'attività formativa. Anche se il GDPR prevede solo indirettamente l'esistenza della figura dell'autorizzato[20] [21] [22] [23], il Codice della Privacy ne impone invece espressamente la designazione[24]. L'autorizzazione deve essere nominativa, specifica dei trattamenti effettuati e, come misura di sicurezza prevista dal GDPR[25], essere affiancata da adeguate istruzioni operative. L'accesso effettivo ai dati personali aziendali dovrà poi, nei fatti, rispecchiare il livello di autorizzazione ricevuto. Anche il professionista potrebbe essere talvolta un semplice autorizzato al trattamento, ad esempio quando la sua attività viene svolta presso il Titolare, agendo nei fatti similarmente ad un impiegato e da

10 *GDPR art. 26*

11 *GDPR art. 4.8*

12 *GDPR art. 28.1*

13 *GDPR art. 4.7 nella sua formulazione originaria è più comprensibile*

14 *Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio (Testo rilevante ai fini del SEE) https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32021D0915*

15 *GDPR art. 28.4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.*

16 *"Il trasferimento dei dati extra UE e i principi del GDPR" di Anna Maria Carbone in "Compliance", giugno 2021 - n. 1, ISSN 2784-8213, Editore: SEAC S.p.A.*

17 *"Dalla sentenza Schrems II al Provvedimento BayLDA su Mailchimp: il problema aperto del trasferimento dei dati personali verso gli USA" di Giulia Bontempini e Stefano-Francesco Zuliani in "Compliance", luglio 2021 - n. 2, ISSN 2784-8213, Editore: SEAC S.p.A.*

18 *DECISIONE DI ESECUZIONE (UE) 2021/914 DELLA COMMISSIONE del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=it&uri=CELEX:32021D0914*

19 *EDPB https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_it*

20 *GDPR C 29 (..) Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate nell'ambito dello stesso titolare del trattamento*

21 *GDPR art. 4.10 (..) le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;*

22 *GDPR art. 28.3.b (il responsabile del trattamento) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;*

23 *GDPR 34.3.a Il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi.*

24 *D.lgs 196/2003 Art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati) 1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. 2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.*

25 *GDPR 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.*

quest'ultimo differenziandosi solamente per la tipologia di rapporto contrattuale in essere col Titolare. Anche se in linea di principio il Titolare è sempre responsabile per i danni causati dall'autorizzato[26], in epoca ante GDPR anche l'autorizzato è stato individuato come soggetto tenuto al risarcimento[27].

Le più importanti linee guida in merito alla distinzione tra Titolare, Contitolare e Responsabile sono le "*Guidelines 07/2020 on the concepts of controller and processor in the GDPR*"[28], emesse dall'European Data Protection Board (EDPD) in sostituzione di un precedente parere ante GDPR del Working Party art. 29[29]. Come tutte le linee guida dell'EDPB vanno tenute in massima considerazione in quanto, pur non essendo prevista nel GDPR alcuna prescrizione che in via diretta ne imponga l'obbligo di osservanza, tra i poteri che il GDPR attribuisce[30] all'EDPB vi è quello di monitorare il Regolamento e assicurarne "*l'applicazione corretta*"[31]. Se dunque le linee guida dell'EDPB sono atti giuridici finalizzati a circostanziare, a livello meramente interpretativo, come nella pratica vada rispettato il principio di correttezza[32], il loro mancato rispetto potrebbe essere sanzionato al pari di una violazione dell'art. 5 del GDPR. Nelle *Guidelines* vengono analizzate nel dettaglio le definizioni dettate dalla normativa europea andando ad esemplificare una pluralità di casistiche di natura generale, estremamente utili al fine di un inquadramento della materia.

Non direttamente applicabili sono invece le linee guida[33] del 2019 dell'European Data Protection Supervisor (EDPS[34]), l'organismo che controlla l'applicazione delle norme in materia di protezione dei dati personali da parte delle istituzioni europee. In ogni caso, per quanto riguardino specificatamente le istituzioni e gli organi comunitari nell'adempimento degli obblighi loro imposti dal GDPR, contengono comunque indicazioni utili in via generale a tutte le organizzazioni che affrontano il problema della qualificazione dei ruoli soggettivi come previsti dal GDPR.

Alcuni casi pratici

Nella "*messa a terra*" delle nomine accade talvolta ci si ponga dei dubbi interpretativi sulla corretta identificazione di un destinatario di dati personali.

Un caso classico di contitolarità si ha nei c.d. "contratti di rete", introdotti nel nostro ordinamento nel 2009 con la c.d. *Rete-Contratto* in cui "*due o più imprese si obbligano ad esercitare in comune una o più attività economiche rientranti nei rispettivi oggetti sociali allo scopo di accrescere la reciproca capacità innovativa e la competitività sul mercato*"[35]. Le imprese che si riuniscono in una rete stabiliscono degli obbiettivi comuni mantenendo la propria autonomia e il contratto, avente mera natura negoziale, è presente nella Sezione del Registro Imprese presso cui è iscritto ciascun partecipante alla Rete. In questo caso ogni retista rimane titolare autonomo dei propri trattamenti specifici, divenendo al contempo contitolare di quelli rientranti nel contratto di rete. Nel 2012 la normativa si è evoluta ed è stata introdotta[36] la "rete soggetto", nuovo soggetto autonomo centro di imputazione sul piano giuridico e tributario, dotato conseguentemente di partita IVA, fondo patrimoniale e iscrizione nel Registro delle Imprese della Camera di Commercio. In questo caso la rete è "titolare autonomo".

A capo di molte categorie professionali sussistono degli obblighi di legge di tenuta con riguardo a determinate tipologie di dati (si pensi ad esempio agli atti stipulati e conservati dai Notai).

Vediamone alcune.

Consulente del lavor**o:** il Garante ha specificato[37] che opera come responsabile quando tratta i dati dei dipendenti dei suoi clienti sulla base dell'incarico professionale ricevuto, mentre rimane titolare autonomo quando gestisce i dati dei suoi dipendenti e clienti persone fisiche (es. liberi professionisti);

Avvocato**:** il Consiglio Nazionale Forense lo individua come "*titolare del trattamento di tutte le informazioni che vengono allo stesso fornite dagli assistiti in virtù o in correlazione del mandato ricevuto*" [38] limitando la figura del Responsabile ai soli casi di domiciliatario. Su quest'ultima interpretazione potrebbero esserci però dei dubbi in virtù dell'effettivo margine discrezionale che i domiciliatari hanno in sede di udienza, facendo così ricadere anche quest'ultimo

26 *Art. 2049 c.c. (Responsabilità dei padroni e dei committenti). I padroni e i committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti.*

27 *Tribunale d Pordenone, H. L. // Azienda Ospedaliera Santa Maria Degli Angeli Di Pordenone sentenza 16/04/2010 https://studylibit.com/doc/2552056/clicca-qui-testo-integrale-sentenza*

28 *EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_it qui una traduzione non ufficiale in Italiano https://www.lentepubblica.it/wp-content/uploads/2021/09/20210905-EDPB-LG7-2020.pdf*

29 *WP 169 Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento" https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1791922*

30 *GDPR Articolo 70 - Compiti del comitato (C139) 1. Il comitato garantisce l'applicazione coerente del presente regolamento. A tal fine, il comitato, di propria iniziativa o, se del caso, su richiesta della Commissione, in particolare: (..) pubblica linee guida, raccomandazioni e migliori pratiche.*

31 *GDPR art. 70.1.a*

32 *GDPR 5.1 I dati personali sono: (C39) a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);*

33 *EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 https://edps.europa.eu/data-protection/our-work/publications/guidelines/concepts-controller-processor-and-joint_en*

34 *https://edps.europa.eu/_en*

35 *art. 3.4 ter, D.L. 10/02/2009, n° 5, convertito con L. 09/04/2009, n° 33*

36 *art. 45 D.L. n° 83/2012 (Decreto Crescita), convertito con modificazioni dalla L. 07/08/2012, n° 134, art. 36 D.L. n. 179/2012 (Decreto Crescita-bis), convertito con modificazioni dalla L. 17/12/2012, n° 221.*

37 *GPDP Risposta a un quesito relativo al ruolo del consulente del lavoro dopo la piena applicazione del Regolamento (UE) 679/2016 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9080970*

38 *CNF Il GDPR e l'Avvocato https://www.consiglionazionaleforense.it/documents/20182/445621/IL+GDPR+E+L%27AVVOCATO/ef231b75-2066-43df-8d88-570bf0ea98b3*

caso nella fattispecie generale dei Titolari Autonomi.
Commercialista: è Titolare autonomo nei casi in cui svolge attività professionale nei confronti di persone fisiche, opera come revisore dei conti[39], o nello svolgimento di incarichi disciplinati da leggi o regolamenti che prevedano il rilascio di pareri, relazioni, perizie asseverate o visti da parte del professionista, mentre è "Responsabile" quando svolge attività più operative quali il data entry o elaborazioni contabili che non richiedano decisioni professionali o assumendo decisioni minime esclusivamente nell'ambito di precise istruzioni ricevute dal Titolare.
Analoghe considerazioni possono essere svolte allo stesso modo per gli Ingegneri e per molti altri professionisti.
Il Garante ha stabilito che l'Organismo di Vigilanza (OdV) ex d.lgs 231/2001 "*nel suo complesso, a prescindere dalla circostanza che i membri che lo compongano siano interni o esterni, debba essere considerato "parte dell'ente". Il suo ruolo - che si esplica nell'esercizio dei compiti che gli sono attribuiti dalla legge, attraverso il riconoscimento di "autonomi poteri di iniziativa e controllo" - si svolge nell'ambito dell'organizzazione dell'ente, titolare del trattamento, che, attraverso la predisposizione dei modelli di organizzazione e di gestione, definisce il perimetro e le modalità di esercizio di tali compiti.*"[40] Il parere del Garante dichiaratamente non si applica al "*nuovo e diverso ruolo che l'organismo potrebbe acquisire in relazione alle segnalazioni effettuate nell'ambito della normativa di whistleblowing (art. 6, comma 2-bis, 2-ter, 2-quater cit., d.lgs. n. 231/2001)*"[41] evidenziando che "*allo stato, il d.lgs n. 231/2001 non attribuisce necessariamente all'OdV la gestione delle segnalazioni in questione, ma rimette alla discrezionalità dell'ente la scelta di individuare in un soggetto diverso il destinatario di tali segnalazioni che avrà il compito di istruirle e adottare ogni conseguente provvedimento*". Per tale trattamento è pertanto lecito delineare una autonoma titolarità. L'importanza del whistleblowing è stata in più ri-

39 Documento di Ricerca n.227 Assirevi di Febbraio 2019 http://webappassirevi.azurewebsites.net/DocumentiSito/DownloadFile?file=/DocumentiRicerca/Doc%20227.pdf

40 GPDP Parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9347842

41 Introdotto in Italia dalla L. 190/2012 per i pubblici dipendenti e rafforzata ed estesa al settore privato dalla L. 179/2017

prese ribadita dal Garante[42] ed è in fase di definizione la sua riforma con emanazione da parte del Governo[43] di un Decreto Legislativo di recepimento della direttiva UE 2019/1937 "*riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*".
Sul ruolo del Collegio Sindacale il Garante non si è ancora espresso, ma essendo ad esso applicabile la maggior parte dei ragionamenti svolti per l'OdV, per analogia può essere corretto considerarlo parte dell'ente.
Sulla corretta individuazione del ruolo del medico del lavoro in ordine al trattamento dei dati personali posto in essere da parte del medico competente, ai sensi della disciplina in materia di igiene e sicurezza sul luogo di lavoro (se come titolare o responsabile), si è molto dibattuto in passato [44] [45].
Un orientamento del Garante alla sua individuazione come titolare autonomo poteva indirettamente essere desunto da vari pregressi provvedimenti[46] [47] [48] [49] ma è stato solo a seguito di una specifica risposta formulata in riscontro ad un quesito posto dalla Società Italiana di Medicina del Lavoro (SIML) che il Garante ha precisato che la disciplina di settore[50] individua la funzione del medico competente come titolare autonomo. Gli accertamenti volti a verificare l'idoneità alla mansione dei dipendenti sono obblighi di legge posti a carico del datore di lavoro, che ne sostiene anche i relativi oneri. Essi però possono essere effettuati esclusivamente per il tramite del medico competente, unico soggetto legittimato ex lege a trattare in piena autonomia e competenza tecnica i dati personali di natura sanitaria dei lavoratori per le finalità indicate dalle normative di settore[51].
Le sole informazioni nella disponibilità del datore di lavoro sono il "giudizio di idoneità alla mansione" e le eventuali prescrizioni che il professionista individua come condizioni di lavoro, ovvero un atto medico ufficiale che il medico competente deve consegnare anche al lavoratore, in assenza del quale non può essere impiegato[52].
"*Tale obbligo rende "pubblico", ovviamente sempre in condizioni di riservatezza, il giudizio di idoneità e le eventuali prescrizioni o limitazioni per tutta la linea gerarchica che ha responsabilità nella gestione del lavo-*

42 GPDP Segnalazione al Parlamento e al Governo sull'individuazione, mediante sistemi di segnalazione, degli illeciti commessi da soggetti operanti a vario titolo nell'organizzazione aziendale [Doc-Web 1693019] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1693019

43 L. 22704/2021, n. 53 - Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020.

44 Agenda Digitale: GDPR e medici del lavoro: titolari autonomi o responsabili esterni? https://www.agendadigitale.eu/sicurezza/privacy/gdpr-e-medici-del-lavoro-titolari-autonomi-o-responsabili-esterni/

45 Cybersecurity 360: Il medico competente nel sistema privacy aziendale: quale ruolo per la compliance GDPR https://www.cybersecurity360.it/legal/privacy-dati-personali/il-medico-competente-nel-sistema-privacy-aziendale-quale-ruolo-per-la-compliance-gdpr/

46 GPDP "Trattamento di dati sanitari del personale navigante da parte del medico competente del vettore aereo" del 27 aprile 2016, punto 3.2; https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5149198

47 GPDP "Linee guida sul trattamento di dati personali dei lavoratori privati" del 23 novembre 2006, punto 33; https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1364939

48 GPDP "Autorizzazione n. 1/2005 al trattamento dei dati sensibili nei rapporti di lavoro" del 21 dicembre 2005, punto 1 ambito di applicazione lettera c); https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1203930

49 GPDP "Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice del 13 dicembre 2018 ", punto 1 ambito di applicazione lettera g). https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9068972

50 d.lgs. 09/04/2008, n° 81

51 GPDP par. 13.14. Relazione 2019 https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2019.pdf/4fcc5ca8-5ca7-432f-c3f8-4e9e69181a23?version=1.1

52 Art. 18.1 del d.lgs 81/2008 "Il datore di lavoro, che esercita le attività di cui all'articolo 3, e i dirigenti, che organizzano e dirigono le stesse attività secondo le attribuzioni e competenze ad essi conferite, devono: (..) bb) vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità.

ratore (dirigente, preposto). In mancanza, il superiore gerarchico, soprattutto se "delegato", non potrebbe adempiere agli obblighi di salvaguardia della salute del lavoratore".[53]
Anche in merito alle vaccinazioni aziendali il Garante ha attribuito[54] al medico competente il compito di raccogliere i nominativi dei dipendenti interessati alla vaccinazione, sottolineando come tale raccolta non possa essere delegata al datore di lavoro. Al termine della raccolta delle adesioni al programma vaccinale, il medico competente comunicherà al datore di lavoro il numero complessivo di lavoratori interessati, ma non i relativi nominativi.
Qualora la sede aziendale o dello studio professionale del Titolare fosse situata in un condominio, l'Amministratore di Condominio potrebbe trattare i dati personali dei condomini per la finalità di gestione ed amministrazione del condominio (cfr Relazione Annuale del Garante anno 2019[55]). Tali dati possono essere condivisi all'interno della compagine condominiale in quanto i condòmini devono essere considerati contitolari di un medesimo trattamento dei dati di cui l'amministratore, agendo in eventuale veste di responsabile esterno del trattamento, ha la concreta gestione.
Il caso della nomina dei "procacciatori" presenta diversi profili di analisi in quanto a seconda del caso concreto si possono delineare come titolari, autorizzati o responsabili. Ad esempio, un agente di commercio che opera esclusivamente presso la sede del titolare, utilizza esclusivamente strumenti informatici di quest'ultimo e ha limitata libertà operativa, potrebbe essere facilmente considerato un incaricato. Questo perché, nel caso specifico appena analizzato, gli agenti di commercio non si troverebbero nelle condizioni oggettive di determinare né le finalità né i mezzi del trattamento e, più per esteso, di assumersi qualsivoglia responsabilità in merito al trattamento effettuato (se non, ovviamente, nei confronti dell'azienda mandante o del diritto penale).
Diversamente il caso di un procacciatore che utilizza contatti derivanti da sue relazioni personali ma che agisce come libero professionista, utilizza mezzi propri (auto, computer, casella di posta elettronica, etc.) e organizza in modo autonomo il proprio tempo : i) se l'invio dei contratti avviene in modo unidirezionale (es: email/fax/posta) i procacciatori sono considerati titolari autonomi senza necessità di alcuna nomina poiché procacciatore e azienda definiscono diverse finalità e mezzi. Dunque, il procacciatore opera per l'adempimento del contratto di vendita col cliente e di tutte le misure precontrattuali, l'azienda per altre finalità (es: marketing diretto, gestione del parco clienti acquisito, etc.). In questo caso il procacciatore è tenuto a fornire al cliente, oltre alla propria, anche l'informativa del Titolare e (se del caso) la richiesta di consenso dell'azienda mandante che risulterà al contempo destinataria per quanto concerne la transazione presente e titolare per quanto riguarda i trattamenti futuri. ii) Se i procacciatori hanno accesso ad un data base aziendale nel quale vengono inseriti i dati dei clienti e attraverso il quale possono essere visualizzati anche lo storico dei clienti inseriti, vanno nominati come Responsabili Esterni, in quanto le "finalità e mezzi" sono definite dal Titolare. iii) Vi è infine l'eventualità nella quale venga impedito all'azienda di ricontattare il cliente una volta conclusa la transazione; siamo in presenza di un rapporto titolare-destinatario per cui non è necessario alcun adempimento, salvo l'obbligo per l'agenzia di segnalare l'azienda mandante nel novero dei destinatari dell'informativa resa al cliente.
Lo stesso procacciatore libero professionista se utilizza invece liste di clienti o prospect fornite dal Titolare (e magari si presenta telefonicamente come il titolare), va nominato "responsabile esterno"[56]. In questo caso la proprietà del portafogli clienti è del titolare, il procacciatore ha libertà decisionale ed operativa riguardo ai mezzi del trattamento ma non ne ha alcuna riguardo le finalità del trattamento. Vi è ad ultimo il caso di contitolarità[57] con il procacciatore: è il caso di un agente di commercio o procacciatore che concluda un accordo con la propria azienda mandante inerente all'acquisto congiunto di immobili, sistemi informativi e altri beni strumentali con condivisione di costi e anagrafiche clienti.
Le compagnie di assicurazione operano sotto la vigilanza di un'autorità di controllo di settore. La loro attività è disciplinata da una specifica normativa[58], individuando gli obblighi che ricadono su ognuna delle parti contraenti. Non ponendo in essere pertanto un trattamento di dati per conto dell'ente aggiudicante rispetto al quale persegue interessi separati e distinti si configura come titolare autonomo[59].
In linea di massima le imprese di pulizie e di facchinaggio non dovrebbero trattare dati personali. In un mondo ideale e in una azienda perfettamente aderente alle norme cogenti del GDPR come noto non dovrebbero essere lasciati fascicoli nominativi liberamente accessibili a chiunque, dovrebbe vigere la regola del "*clean desk*" e nei cestini della spazzatura non dovrebbero potersi rinvenire stampe di cedolini di dipendenti. Nell'esercizio del servizio prestato a favore del Titolare, l'Impresa non svolge pertanto nessun ruolo, funzione o attività di responsabile del trattamento dei dati o di autorizzato al trattamento, rimanendo titolare autonomo ed in quanto tale responsabile ex art. 24 del GDPR. Pur non essendo la "nomina a titolare" soggetta a contratto, è comunque opportuno ai fini dell'accountability formalizzare questo aspetto in un addendum contrattuale che formalizzi che gli addetti alle pulizie

53 Associazione nazionale medici d'Azienda e Competenti http://www.anma.it/anma-risponde/giudizio-di-idoneita-alla-mansione-e-privacy/

54 GPDP Provvedimento del 13 maggio 2021 - Documento di indirizzo "Vaccinazione nei luoghi di lavoro: indicazioni generali per il trattamento dei dati personali" [9585300] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9585300

55 GPDP Relazione annuale 2019, par. 15 https://www.garanteprivacy.it/home/attivita-e-documenti/documenti/relazioni-annuali

56 GPDP Ordinanza ingiunzione nei confronti di Merlini s.r.l. - 9 luglio 2020 [9435774] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435774

57 GDPR art. 26 Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.

58 artt. 1882 ss. c.c.; d.lgs. n. 209/2005, codice delle assicurazioni; regolamento Ivass n. 40/2018

59 GPDP Ruolo soggettivo dell'impresa assicurativa nell'ambito dei bandi di gara per l'affidamento dei servizi assicurativi [9169688] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9169688

nell'espletamento delle loro funzioni non sono autorizzati a trattare dati personali e indichi quale procedura questi devono adottare in caso di reperimento fortuito di materiale (es: un cedolino di un dipendente rivenuto casualmente sul pavimento). È inoltre consigliabile inserire in tale addendum regole specifiche di comportamento al fine di garantire la sicurezza fisica dei dati (es: gestione accessi, spazi accessibili, obblighi di comunicazione, etc.).
Bisogna invece prestare particolare attenzione ai fornitori con incarichi di distruzione di dati personali, si pensi a vecchi archivi cartacei o a vecchi computer: in questi casi è necessaria la nomina della ditta incaricata a responsabile esterno del trattamento.
Nel caso di quotidiani o riviste il Titolare del Trattamento è normalmente l'Editore e non i singoli giornalisti, seppur con alcuni piccoli distinguo in caso di attività lavorativa indipendente e in caso di archivi giornalistici personali. Infatti, come espresso dal Garante[60] a seguito dell'analisi del Contratto di lavoro giornalistico, "p*oiché la disposizione sulla notificazione in forma semplificata da parte dei giornalisti, dei pubblicisti e dei praticanti pone l´accento soprattutto sul piano funzionale anziché su quello soggettivo, ai fini dell´individuazione della figura del titolare in ambito giornalistico, cui spettano le decisioni di fondo sulle finalità e sulle modalità del trattamento, è necessario appurare se le scelte di ordine generale sulle complessive modalità dei trattamenti competano ai singoli giornalisti ovvero all´editore. All´esito di un´analisi del modo d´esplicazione dell´attività giornalistica e del rapporto giornalisti-editori, deve ritenersi corretto identificare nell´editore il titolare del complesso dei dati che ruota attorno all´impresa editoriale e che, pertanto, è tenuto ad effettuare la notificazione semplificata, senza che a ciò possa ritenersi di ostacolo la prassi adottata nel settore per effetto del contratto di lavoro giornalistico concluso tra la Federazione italiana editori giornali (F.i.e.g.) e la Federazione nazionale della stampa italiana (F.n.s.i.), che ribadisce soltanto alcuni principi a garanzia della sfera soggettivo-professionale del giornalista*".[61]
Conseguentemente le istanze di esercizio dei diritti dell'interessato possono essere proposte, "*oltre che al direttore responsabile della testata giornalistica, nella qualità di responsabile del trattamento dei dati personali, anche al titolare del trattamento per il tramite di una articolazione centrale o periferica della struttura che fa capo a quest'ultimo (nella specie, una redazione periferica del quotidiano). L'istanza, infatti, deve presumersi conosciuta dal titolare ove giunga in un luogo che rientra nella sua sfera di dominio e controllo*".[62] Vi è però una eccezione, il caso del "*giornalista che, operando in una condizione di completa autonomia dall'editore ed al di fuori di quelle particolari modalità di lavoro previste dal contratto collettivo con riferimento alla struttura editoriale, crei una distinta base di dati destinati alla diffusione, assume in prima persona la veste di titolare del trattamento*"[63]. È il caso ad esempio dei free lance o degli archivi personali.
In merito agli obblighi di nominare specificatamente (o meglio "autorizzare") le figure descritte nei provvedimenti ante GDPR del Garante di natura generale[64], quali gli Amministratori di Sistema[65], gli Incaricati alla Videosorveglianza[66] e i Custodi Fiduciari delle Password[67], questi adempimenti permangono solo laddove non in contrasto[68] con il GDPR (considerando inoltre che il d.lgs 101/2018 ha abrogato le sanzioni[69] in caso di loro inosservanza). Ad esempio, l'obbligatorietà della nomina dell'"Amministratore di sistema" che all'epoca era considerata una misura minima di sicurezza, oggi parrebbe incompatibile con il principio di accountability dettato dal GDPR ed ad una prima lettura si potrebbe valutare di poterne liberamente ometterne l'adozione. Questi "vecchi" provvedimenti del Garante vanno però oggi considerati al pari delle attuali linee guida[70] per cui la loro mancata adozione verrebbe verosimilmente valutata in ottica di mancato rispetto dei principi generali di accountability con il conseguente rischio di sanzione ex art. 83.5 GDPR. Riprendendo l'esempio dell'Amministratore di Sistema, se nel 2008 il Garante la reputava una misura di sicurezza così importante da renderla obbligatoria, oggi difficilmente, alla luce di un parere così fermo, si potrebbe sostenere fondatamente nell'ambito di un contenzioso la sua inutilità[71], anche solo relativamente a talune situazioni. In conclusione, sono nomine da mantenersi attualmente.

Infine, il DPO

Dall'analisi dei provvedimenti sanzionatori finora pubblicati, i Garanti europei in

60 *"Massimario 1997 - 2001. I principi affermati dal Garante nei primi cinque anni di attività" | "Massimario 2002" | "Massimario 2003" di Fabrizia Garri*, Luigi Pecora, Giuseppe Staglianò cura editoriale di Maurizio Leante [doc. web n. 1510100]*

61 *GPDP 24 marzo 1998, in Bollettino n. 4, pag. 50 [doc. web n. 41822]*

62 *GPDP 25 ottobre 2001, in Bollettino n. 23, pag. 19 [doc. web n. 40739]*

63 *GPDP 24 marzo 1998, in Bollettino n. 4, pag. 50 [doc. web n. 41822]*

64 *https://www.garanteprivacy.it/web/guest/home/ricerca/-/search/tipologia/Provvedimenti%20a%20carattere%20generale*

65 *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*

66 *GPDP Provvedimento in materia di videosorveglianza - 8 aprile 2010 [1712680] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1712680*

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

68 *d.lgs 101/2018 art. 22.4. A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto.*

69 *art. 162 comma 2-ter d.lgs 196/2003, ora abolito: In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro.*

70 *D.lgs 196/2003 art. 154-bis 1. Oltre a quanto previsto da specifiche disposizioni, dalla Sezione II del Capo VI del Regolamento e dal presente codice, ai sensi dell'articolo 58, paragrafo 6, del Regolamento medesimo, il Garante ha il potere di: a) adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento;*

71 *Se alla parola "inutilità" il lettore ha pensato all'obbligo per tutti i titolari del backup dei log degli accessi dell'Amministratore di Sistema sappia che non è solo.*

questi anni hanno colpito pesantemente le mancate nomine, soprattutto quando conseguenza di una conclamata accidia dei titolari, dimostrandosi invece più clementi di fronte ad una motivata e documentata scelta supportata dal parere del proprio Data Protection Officer - DPO (Responsabile della Protezione dei Dati - RPD[72]), figura che il Garante considera di garanzia quale organo indipendente[73]. La sua nomina è obbligatoria per tutti gli enti pubblici e, in taluni casi, anche nel settore privato[74] [75], mentre rimane sempre fortemente consigliato, se non addirittura obbligatorio nei fatti, "*documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un RPD, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti. Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione. Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario (..).*"[76]
Ancora una volta la parola chiave è *accountability*.

72 GPDP Il Responsabile della Protezione dei Dati (RPD) https://www.garanteprivacy.it/regolamentoue/rpd

73 Cybersecurity 360 Conflitto di interessi del DPO, maxi multa del Garante belga a un'azienda https://www.cybersecurity360.it/legal/privacy-dati-personali/conflitto-di-interessi-del-dpo-maxi-multa-del-garante-belga-a-unazienda/

74 GDPR Articolo 37 Designazione del responsabile della protezione dei dati (C97) 1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

75 GPDP Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico [9589104] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9589104

76 WP art. 29 - Linee guida sui responsabili della protezione dei dati - WP 243 rev. 01 13/12/2016 https://ec.europa.eu/newsroom/article29/items/612048

Transizione (energetica) o estinzione: questo è il dilemma!

di Giorgia Farella e Simone Franzo

Questo articolo potrebbe interessare perché parla di:
• cosa sta accadendo nel settore energetico;
• quali sono le soluzioni emergenti abilitanti la decarbonizzazione e i nuovi modelli di business;
• in che modo le utenze energetiche – in ambito residenziale, terziario o industriale – possono cogliere le nuove opportunità generate in questo contesto, rendendosi non solo parte attiva e consapevole ma addirittura protagoniste della transizione energetica.

Lo scenario energetico
L'evoluzione in atto che ha caratterizzato il sistema elettrico in Italia negli ultimi anni, e che va sotto il nome di "transizione energetica", ne sta promuovendo la progressiva decarbonizzazione ed elettrificazione.

1. Sistema elettrico nazionale e quadro normativo a supporto
Gli impianti alimentati a fonte rinnovabile rappresentano oggi una componente strutturale del sistema elettrico italiano, con una capacità installata che supera oggi i 56 GW (Figura 1), grazie soprattutto all'aumento nell'ultimo decennio degli impianti fotovoltaici ed eolici.
Se il numero assoluto di per sé può non dire nulla, basti sapere che questa capacità ha quasi raggiunto quella relativa agli impianti termoelettrici (ovvero alimentati da fonti fossili), che invece si è gradualmente ridotta: essa oggi è pari a circa 60 GW, rispetto ai 77 GW del 2012. Di questi 60 GW, il 77% fa riferimento a impianti alimentati a gas naturale, che rappresentano pertanto gli impianti su cui il sistema elettrico fa maggiormente leva e che – di conseguenza – contribuiscono maggiormente a determinare il prezzo dell'energia (ossia il cosiddetto PUN o "Prezzo Unico Nazionale").
Com'è noto, negli ultimi mesi le forti tensioni sull'approvvigionamento di gas naturale (dalla Russia *in primis*) hanno determinato un forte incremento dei prezzi di mercato del gas e, di conseguenza, un'impennata storica dei prezzi dell'energia elettrica in Italia. Ciò fa capire, da un lato, quanto sia necessario per il Paese promuovere l'ulteriore sviluppo delle fonti rinnovabili, al fine di affrancarsi sempre più dalla dipendenza dall'approvvigionamento di fonti energetiche dall'estero. Dall'altro lato, risulta evidente l'importanza di agire sui consumi energetici, rendendoli sempre più efficienti.
Infine, gli impianti a carbone ad oggi rappresentano il 17% della capacità di generazione termoelettrica e dovranno essere dismessi nel corso dei prossimi 5 anni, così come definito all'interno del PNIEC (Piano Nazionale Integrato per l'Energia e il Clima).

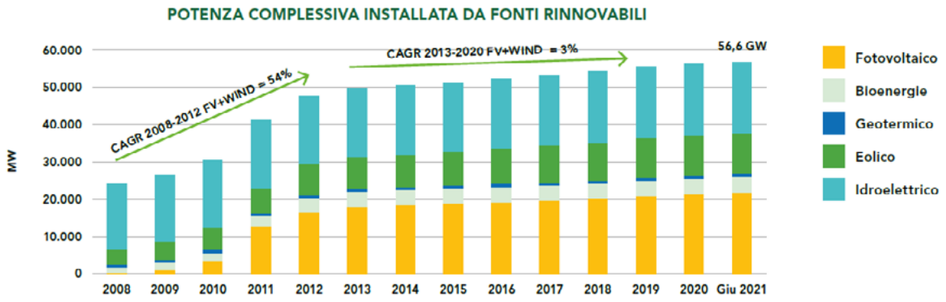


Figura 1 – Fonte: Energy&Strategy, Electricity Market Report 2021

Se poi passiamo all'elettrificazione dei consumi (ovvero il consumo finale da energia elettrica rispetto all'energia finale richiesta), essa nell'ultimo decennio si è sostanzialmente mantenuta costante, nell'intorno del 20% dei consumi finali. Gli scenari e le politiche energetiche prevedono però una crescente elettrificazione dei consumi, grazie a tecnologie quali le autovetture elettriche (già oggi le immatricolazioni presentano un andamento esponenziale, ancorché su valori assoluti limitati) in sostituzione delle tradizionali autovetture alimentate prevalentemente a benzina o diesel e alle rinnovabili termiche (quali le pompe di calore) in luogo del gas naturale per il soddisfacimento dei fabbisogni termici.
La diffusione delle rinnovabili e l'elettrificazione dei consumi sono peraltro trainate dall'evoluzione del quadro normativo a livello internazionale e nazionale in tema di decarbonizzazione, che ha imposto obiettivi sempre più sfidanti fino a una completa decarbonizzazione attesa per il 2050.
A **livello europeo**, s'è molto sentito parlare di *Green Deal*, *Next Generation EU* e *Fit for 55*. Questi sono i programmi attraverso i quali la Commissione Europea ha recentemente proposto di elevare l'obiettivo della riduzione delle emissioni di gas serra per il 2030 ad almeno il 55% rispetto ai livelli del 1990 e ha promulgato un pacchetto di finanziamenti pari a 1.800 miliardi di euro – il più grande mai stanziato dall'Unione Europea – al fine di creare un'Europa post Covid-19 più verde, digitale, resiliente e adeguata alle sfide future.
A **livello italiano**, c'è invece l'ormai noto Piano Nazionale di Ripresa e Resilienza (PNRR), piano italiano di spesa dei fondi stanziati dal *Next Generation EU* presentato il 30 aprile 2021 e che vede "*green*" e "digitale" come ambiti cui sono dedicate la maggior parte delle linee di finanziamento. Se questi obiettivi e obblighi possono lasciare perplessi, è fondamentale sapere che c'è un'ottima notizia: essi sono affiancanti dall'introduzione di una serie di provvedimenti atti a favorirne il raggiungimento, quali ad esempio incentivi all'acquisto di determinate tecnologie e nuovi modelli di produzione e consumo *smart* dell'energia.

2. Nuove soluzioni abilitanti la decarbonizzazione

L'evoluzione tecnologica sta portando alla ribalta nuove soluzioni abilitanti la decarbonizzazione, in grado di stravolgere il mercato energetico facendogli fare passi da gigante verso i succitati obiettivi.
Ma di che evoluzione tecnologica stiamo parlando? Si tratta di tecnologie più o meno nuove, più o meno innovative, con applicazioni a tutti i livelli della filiera energetica, come mostrato in Figura 2.

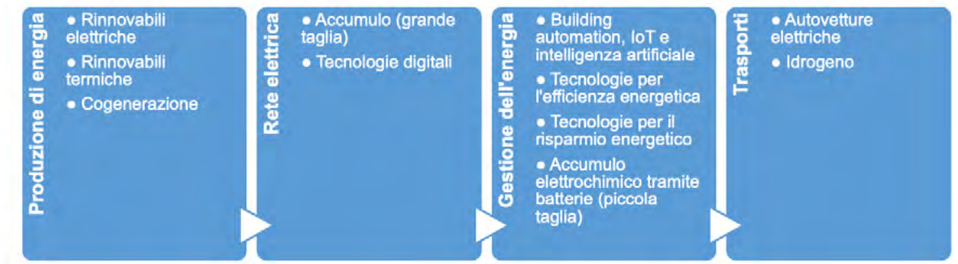


Figura 2 – Soluzioni abilitanti la decarbonizzazione, clusterizzate in funzione del livello nella filiera energetica

Di seguito facciamo una rapida panoramica, sicuramente non esaustiva, ma speriamo quantomeno esplicativa.

Produzione di energia

• Rinnovabili elettriche

Parliamo ad esempio di un impianto solare fotovoltaico che produce energia elettrica sfruttando l'irraggiamento solare, oppure dell'utilizzo di altre fonti rinnovabili quali l'eolico, il geotermico e le bioenergie.

• Rinnovabili termiche

Si tratta ad esempio di pompe di calore elettriche, che tramite energia elettrica (preferibilmente rinnovabile) estraggono il calore da una fonte naturale (aria, acqua o terra) e lo trasportano alla temperatura idonea all'interno di un edificio o in un processo. E questo può valere sia per il riscaldamento che per il raffrescamento. Secondo la normativa europea in tema di energia, se l'energia catturata da una pompa di calore eccede in maniera significativa la quantità di energia necessaria al suo funzionamento, essa è considerata rinnovabile.

• Cogenerazione

La cogenerazione è la produzione combinata di energia elettrica e calore, generati da una singola fonte energetica, che garantisce il miglioramento dell'efficienza dovuta alla produzione combinata dell'energia rispetto a produzioni separate. Le tecnologie più diffuse in ambito cogenerativo prevedono la combustione di gas naturale, GPL, gasolio, biogas, biometano, olio vegetale o biomassa.

Rete elettrica

• Accumulo (grande taglia)

Si tratta dell'utilizzo di accumulo elettrochimico (ovvero batterie di grande taglia) o di idrogeno al fine di stoccare l'energia elettrica prodotta da fonti rinnovabili e utilizzarla quando necessaria e/o quando la rete non è congestionata e quindi è in grado di distribuirla.

• Tecnologie digitali

Sono le tecnologie *hardware-software* che permettono di ottimizzare il funzionamento dei diversi asset all'interno della rete elettrica. Si fa riferimento, ad esempio, alla possibilità per una moltitudine di soggetti in forma aggregata – quali ad esempio piccoli impianti di generazione di energia, sistemi di accumulo elettrochimico, batterie di auto elettriche, pompe di calore etc. – di fornire servizi che consentono un esercizio in sicurezza del sistema elettrico (le cosiddette "Unità Virtuali Abilitate Miste" o UVAM).

Gestione dell'energia

• *Building automation,* IoT e intelligenza artificiale

Sono le tecnologie *hardware-software* per la gestione ottimizzata di impianti ed elettrodomestici all'interno degli edifici (residenziali e non). Per esempio, algoritmi evoluti all'interno di un termostato che utilizzano il wi-fi di casa e il GPS del cellulare per accendere il riscaldamento quando si sta tornando a casa (ma per tenerlo spento quando si è in trasferta).

• Tecnologie per l'efficienza energetica

Tecnicamente parlando, "efficienza energetica" significa consumare meno... ottenendo "uguale". Ad esempio, questo si può ottenere passando da una lampadina ad

incandescenza a una lampadina a LED: la stanza è ugualmente illuminata, ma il consumo di energia elettrica si riduce notevolmente.

• Tecnologie per il risparmio energetico

Tecnicamente parlando, "risparmio energetico" significa invece consumare meno... ottenendo meno. Ad esempio, si può decidere deliberatamente di spegnere l'impianto d'illuminazione o di riscaldamento, talvolta determinando un peggioramento del comfort abitativo.

• Accumulo elettrochimico tramite batterie (piccola taglia)

Per esempio, quando un impianto fotovoltaico residenziale produce energia che le utenze energetiche in casa non sono in grado di assorbire istantaneamente, allora la si stocca nell'accumulo. Viceversa, quando, di notte, serve l'energia ma l'impianto fotovoltaico non la produce... si usa quella stoccata nell'accumulo.

Trasporti

• Autovetture elettriche

Si fa riferimento ad autovetture caratterizzate dalla presenza di un motore elettrico e di una batteria, dove la propulsione elettrica rappresenta l'unica disponibile (cosiddetti "veicoli elettrici puri" o BEV – *Battery Electric Vehicle*) o dove la propulsione elettrica affianca il tradizionale motore a combustione interna (cosiddetti veicoli ibridi plug-in o PHEV – *Plug-in Hybrid Electric Vehicle*, i quali sono in grado di ricaricarsi dalla rete elettrica). La diffusione delle auto elettriche richiede la presenza di un'opportuna infrastruttura di ricarica, sia in ambito privato (ad esempio domestico) che pubblico (ad esempio su strade e autostrade).

• Idrogeno

Parliamo dell'uso di celle a combustibile che sfruttano l'idrogeno come combustibile, auspicabilmente prodotto utilizzando energia prodotta da fonti rinnovabili (cosiddetto "idrogeno verde").

Per completezza d'informazione, è giusto evidenziare che tutte le tecnologie (escluse quelle applicabili alla rete elettrica) descritte qui sopra possano essere applicate tanto nel settore residenziale, quanto nel settore terziario e industriale.

3. Evoluzione dei player del mercato

Se volessimo riassumere tutto in una frase, potremmo dire che... i grandi si stanno comprando i piccoli.

Uno dei trend rappresentativi degli ultimi anni è infatti l'interesse da parte di molteplici attori della filiera nel valutare la possibilità di acquisire società, al fine di cogliere le opportunità emergenti associate ai trend sopracitati. Di fatto, si registra la tendenza di grandi soggetti in termini di fatturato (principalmente *utility*, fondi di *private equity*, società di *facility management* e società coinvolte nella trasmissione dell'energia elettrica o nella distribuzione del gas) ad acquisire i principali (ma piccoli, se rapportati alla dimensione dei grandi soggetti) fornitori di servizi e tecnologie energetici specializzati in determinati settori. Parliamo ad esempio di *Energy Service Company*, fornitori tecnologici, società di progettazione e di costruzioni.

Questo è sintomatico di un crescente e trasversale interesse per energia e transizione energetica, non più circoscritto solamente ad aziende specializzate su un preciso prodotto o servizio, bensì integrate in ottica olistica. E perché dovrebbero farlo?

In primo luogo, l'obiettivo degli acquirenti è proprio quello di integrare in ottica complementare le proprie risorse e competenze con quelle di soggetti esterni che hanno una buona visibilità e copertura del mercato, seppur con minore potenza di fuoco.

In secondo luogo, l'interesse è trainato dall'evoluzione normativa in atto che – supportata anche da obblighi e incentivi – sta rivoluzionando il mondo dell'energia. Ad esempio, l'introduzione di cessione del credito d'imposta e bonus rafforzati (superbonus) gioca a favore di soggetti caratterizzati da una forte capacità finanziaria e da un elevato numero di clienti, che attraverso acquisizioni strategiche possono entrare prepotentemente in mercati prima meno presidiati.

Conseguenze di questo scenario e modelli di business emergenti

All'alba del 2022, in un mondo digitalizzato che permette di essere costantemente informati su cosa accade nel mondo (anche quello energetico!) e valutare e contattare qualunque impresa, è più che mai importante cogliere le opportunità della transizione energetica da protagonisti. Le opportunità, ormai è chiaro, ci sono infatti a tutti i livelli: come *player* del settore energetico, come utente, e come professionista informato che supporti i propri clienti.

1. Utente attivo e consapevole: il prosumer

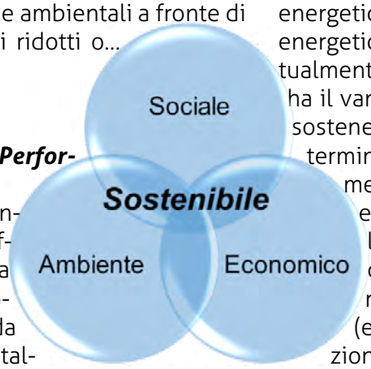
Se si cerca nel dizionario il significato di "*prosumer*", si troverà questa definizione: "Il destinatario di beni e di servizi che non si limita al ruolo passivo di consumatore (*consumer*), ma partecipa attivamente alle diverse fasi del processo produttivo". Se quindi si applica questo concetto al mondo energetico, si ottiene un utente consapevole, attivo, protagonista.

In pratica, il *prosumer* è colui che possiede un proprio impianto di produzione di energia, della quale ne consuma (almeno) una parte. La rimanente quota di energia può essere immessa in rete, scambiata con i consumatori fisicamente prossimi al *prosumer* o anche stoccata in un apposito sistema di accumulo e dunque restituita alle unità di consumo nel momento più opportuno. Tra l'altro, l'utilizzo e la cessione dell'energia alla rete elettrica possono seguire varie logiche di ottimizzazione, alcune delle quali volte a supportare la gestione del sistema elettrico nazionale. Pertanto, il *prosumer* è un protagonista attivo nella gestione dei flussi energetici, e può godere non solo di una relativa autonomia ma anche di benefici economici. Se fino a pochi anni fa la figura del *prosumer* rappresentava un'eccezione all'interno del sistema elettrico, oggi è un protagonista indiscusso: basti pensare che in Italia sono presenti circa un milione di piccoli impianti fotovoltaici connessi ad utenze residenziali.

2. Nuovi modelli di business e servizi energetici avanzati

Tornando a quanto ci siamo detti all'inizio dell'articolo, si comprende perché la transizione energetica sta abilitando una progressiva evoluzione dei modelli di business (quali la fornitura di servizi energetici avanzati) attraverso cui tecnologie e soluzioni sono portate a mercato. L'evoluzione tecnologica è infatti (spesso) una condizione

necessaria ma non sufficiente per abilitare la transizione energetica. Essa deve essere affiancata da un'evoluzione dei modelli di business, in una chiave di sostenibilità.
La sensibilità collettiva dev'essere in grado di coniugare la sostenibilità economica delle iniziative con quella ambientale e sociale (la cosiddetta triple bottom line, si veda Figura 3).
In questa sede, tralasciamo quella sociale (che richiederebbe una trattazione *ad hoc*) e ci focalizziamo su quelle economica e ambientale. Da esse, infatti, derivano i principali nuovi modelli di business, che permettono di veicolare a mercato i servizi energetici avanzati, intesi come quei servizi integrati che permettono al consumer di diventare *prosumer* – protagonista della transizione energetica – massimizzando i benefici economici e ambientali a fronte di investimenti iniziali ridotti o...
nulli.
Per esempio?



E.P.C. – Energy Performance Contract
Questo tipo di contratto si basa sull'efficienza energetica e il risparmio economico generati da una tecnologia installata presso l'utente a spese di un *player* energetico.
In accordo alla definizione data dal Decreto Legislativo 102/2014, l'E.P.C. è "un accordo contrattuale tra il beneficiario o chi per esso esercita il potere negoziale e il fornitore di una misura di miglioramento dell'efficienza energetica, verificata e monitorata durante l'intera durata del contratto, dove gli investimenti (lavori, forniture o servizi) realizzati sono pagati in funzione del livello di miglioramento dell'efficienza energetica stabilito contrattualmente o di altri criteri di prestazione energetica concordati, quali i risparmi finanziari".
In altri termini, l'E.P.C. affida al *player* energetico l'onere degli investimenti (lavori, servizi, forniture) necessari per la riqualificazione degli edifici/impianti, che saranno ripagati restituendo al *player* energetico una percentuale del risparmio energetico conseguito stabilita contrattualmente (come mostrato in Figura 4). Ciò ha il vantaggio per il cliente di non dover sostenere alcun investimento iniziale. Al termine del contratto (che tendenzialmente dura dai 5 ai 12 anni), il *player* energetico si fa da parte cedendo la proprietà della tecnologia al cliente, che beneficerà in toto dei risparmi generati dalla tecnologia (e avrà l'onere della sua manutenzione).

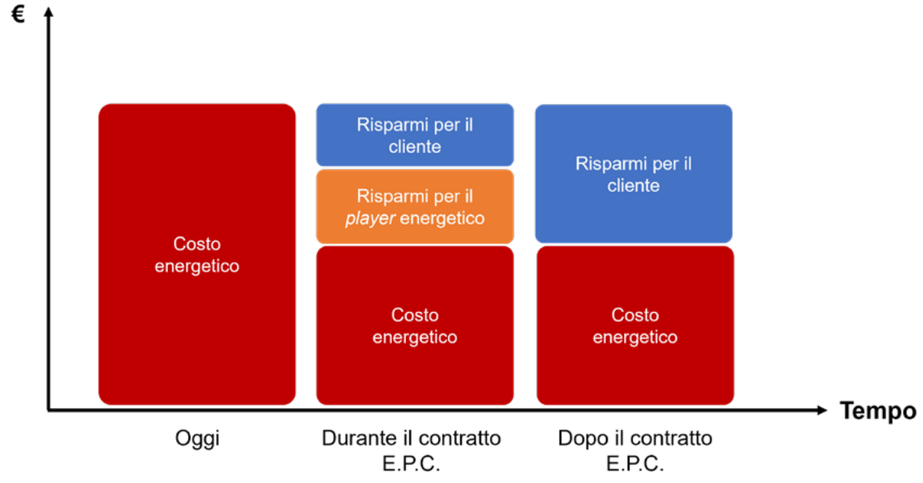


Figura 4 – Energy Performance Contract

Pay Per Use
Un po' come alcuni contratti di noleggio auto, si paga solo ciò che si usa.
Questo tipo di contratto – che, come per l'E.P.C., prevede fornitura, installazione e manutenzione della tecnologia a spese del *player* energetico – viene generalmente utilizzato con tecnologie che permettono di produrre energia in modo più sostenibile (dal punto di vista ambientale ed economico). Ad esempio, un impianto fotovoltaico o di cogenerazione.
Nel Pay Per Use, il *player* energetico si ripaga dell'investimento vendendo all'utente l'energia prodotta dalla tecnologia. La convenienza per il cliente sta nel fatto che l'energia acquistata gli costerà meno rispetto a quella acquistata normalmente.

Autoconsumo collettivo e Comunità Energetiche
Parliamo di aggregazioni di utenti energetici – all'interno di uno stesso edificio o in una determinata area geografica – che condividono l'energia prodotta da impianti alimentati da fonti rinnovabili, presenti sull'edificio o sull'area geografica di cui sopra. I principali benefici derivanti da questa tipologia di aggregazioni di utenze sono molteplici: autoconsumo fisico dell'energia prodotta (ovvero mancato acquisto della stessa), valorizzazione a mercato dell'energia immessa in rete, riduzione degli oneri, incentivi statali.
Questa tipologia di configurazione può essere veicolata a mercato tramite diversi modelli di business; ad esempio, un *player* energetico esterno all'aggregato può investire nello sviluppo degli impianti rinnovabili e condividere con le utenze energetiche i benefici derivanti dall'iniziativa.

Cessione del credito e Sconto in fattura
Parliamo in questa sede di detrazioni fiscali derivanti da interventi di miglioramento dell'efficienza energetica o di consolidamento sismico, quali Ecobonus, Sismabonus, Superbonus, ...
Lo **sconto in fattura** consiste in uno sconto sul corrispettivo dovuto, fino a un importo massimo pari al corrispettivo stesso, anticipato dal fornitore che ha effettuato gli interventi e da quest'ultimo recuperato sotto forma di credito d'imposta, con facoltà di successiva cessione del credito ad altri soggetti, ivi inclusi gli istituti di credito e gli altri intermediari finanziari (Figura 5).
La **cessione del credito** di imposta permette la trasformazione del corrispondente importo legato ai lavori di riqualificazione edilizia in credito d'imposta, con facoltà di successiva cessione ad altri soggetti, ivi inclusi istituti di credito e altri intermediari finanziari.

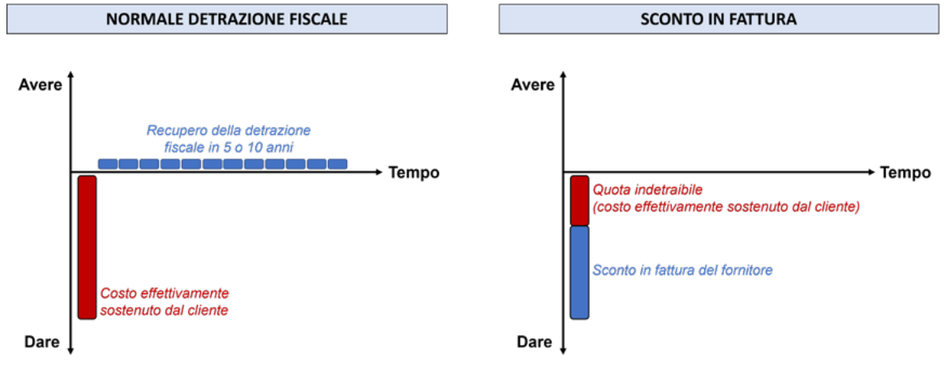


Figura 5 – Sconto in fattura

La differenza tra uno e l'altro sistema è – tendenzialmente – che lo sconto in fattura prevede il solo pagamento della quota non incentivata tramite la detrazione (es: per detrazione pari al 65%, si paga solo il 35%); l'importo detraibile è infatti anticipato dal fornitore, che fa appunto uno "sconto" al cliente finale. La cessione del credito invece prevede l'esborso totale da parte del cliente finale, che successivamen-

te cede l'importo incentivato, retrocessogli al netto degli oneri finanziari, a un terzo.
Tutte le pratiche necessarie per la formalizzazione della cessione del credito sono in linea di massima in carico al fornitore del servizio di cessione o sconto.

Come il nostro attento lettore avrà notato, abbiamo volutamente tralasciato alcuni modelli che l'utente può realizzare in autonomia senza il coinvolgimento di player del settore energetico (ma con esborso economico maggiore), quali ad esempio industria 4.0, iperammortamento, ...

E quindi? Come muoversi per cogliere queste opportunità

1. Se già non lo si fa, iniziare ad approcciare i propri consumi energetici in modo attivo invece che passivo. La consapevolezza dei consumi energetici è la *conditio sine qua non* per avviare iniziative volte a efficientare e ottimizzare i propri consumi energetici.
2. Imparare a cambiare il proprio *mindset*, ovvero accogliere modelli di business nuovi senza pregiudizi o diffidenze. Può sembrare scontato, ma purtroppo non è così! Per qualunque tipologia di utente infatti, come abbiamo visto, la transizione energetica può riservare varie opportunità, che per le imprese si traducono anche in un vantaggio competitivo.
3. Trovare un professionista serio a cui affidarsi, che aiuti a comprendere al meglio i propri consumi energetici e le proprie esigenze. Questo passaggio è necessario perché l'abbondanza di opportunità connesse alla transizione energetica ha fatto esplodere l'offerta sul mercato, ma è fondamentale comprendere quali siano i *player* adatti alle specifiche esigenze dell'utente (nonché in grado di offrirgli con serietà e continuità quanto promesso).

Bibliografia essenziale

• Energy&Strategy (2021), Electricity Market Report
• Piano Nazionale Integrato per l'Energia e il Clima (PNIEC)
• Piano Nazionale di Ripresa e Resilienza (PNRR)
• D.L. 102/2014
• L. 302/2017, DL. 63/2013, L. 302/2017, L. 145/2018, Legge n. 58/2019, L. 160/2019, L. 178/2020
• RED II
• Guide ENEA e GSE

Divieti e sanzioni per chi svende i prodotti agroalimentari o non rispetta i termini di pagamento dei fornitori. All'ICQRF il compito di vigilare sulle condotte borderline

di Olga Bussinello

Dallo scorso dicembre, con l'entrata in vigore del Decreto Legislativo n. 198 dell'8 novembre 2021, pubblicato in G.U. serie speciale n. 41/L del 30 novembre 2021, sarà garantito un livello minimo di tutela a tutti gli agricoltori e le PMI Europei che lavorano con la Grande Distribuzione rispetto alle pratiche commerciali adottate in passato da quest'ultima. Per orientare gli operatori sono definite varie tipologie di condotte sanzionabili distinte per gravità, mentre vengono, altresì, suggerite quelle auspicabili. Deroghe e nuove regole sono previste per i contratti di cessione nel settore della somministrazione di alimenti e bevande e per chi lavora con la PA.

Dopo due anni dall'entrata in vigore della direttiva UE 2019/633, anche l'Italia si è allineata alla nuova disciplina in materia di accordi per la commercializzazione dei prodotti agricoli che dovrebbe porre fine alla posizione di forza dei grandi player della distribuzione moderna nella definizione degli accordi di fornitura con produttori agricoli o piccole aziende di prima trasformazione. Un problema che, tradotto in cifre, dà luogo in Europa ad un danno di 10 miliardi di euro ogni anno e a 4.4 miliardi di costi aggiuntivi per chi lo subisce (Fonte parlamento Europeo). La normativa, tuttavia, introduce un livello minimo di tutela, frutto della mediazione occorsa fra le parti sociali, puntando a conformare ai principi di buona fede, proporzionalità e trasparenza le clausole contrattuali sottoscritte dalle parti. Viene, infatti, fornito un elenco di pratiche commerciali sleali vietate ed uno di pratiche che potranno essere autorizzate se concordate in termini chiari e univoci tra le parti al momento della conclusione dell'accordo di fornitura. Interessati sono solo i rapporti BtoB, cioè quelli fra produttori e operatori commerciali. Restano esclusi, quindi, quelli in cui uno dei contraenti è il consumatore finale. Il punto di partenza è la "naturale" debolezza dei produttori nelle relazioni con gli altri attori della filiera dovuta, sia alla deperibilità e alla stagionalità delle produzioni, sia alla ridotta dimensione aziendale, fattori questi che insieme determinano la costante fluttuazione dei costi di produzione. Da segnalare che lo schema di decreto, a differenza di quanto dispone il quadro giuridico Europeo, prevede una disciplina unica per tutti gli scambi commerciali aventi ad oggetto prodotti agricoli e alimentari, a prescindere dal fatturato dei contraenti. L'art. 7 della legge n. 53 del 2021 (legge di delega Europea), non accoglie l'opportunità lasciata aperta dalla direttiva UE, ed impone di mantenere ferma l'opzione di applicare la disciplina a tutte le cessioni di prodotti agricoli e agroalimentari, indipendentemente dal fatturato aziendale, in considerazione della peculiarità del sistema agroalimentare italiano, estremamente frammentato e popolato da microaziende familiari. In questo senso, si prosegue il percorso iniziato ancora nel 2012 con l'art. 62 del decreto-legge 24 gennaio 2012, n. 1, che è abrogato con l'entrata in vigore del presente Decreto Legislativo. Sono altresì abrogati: i commi 1, 3, 4 e 5 dell'art. 10 quater del DL n. 27/2019, il comma 6-bis dell'art. 36 della legge n. 221 del 2012 e il Decreto Mipaaf n. 199/2012.

Ambito di operatività e definizioni

Con l'art. 1 viene definito l'oggetto del decreto, vale a dire le pratiche commerciali vietate in quanto contrarie ai principi di buona fede e correttezza che vengano decise unilateralmente da un contraente e imposte *sic et simpliciter* alla sua controparte. Interessate dalla nuova disciplina sono solo le cessioni di prodotti agricoli ed alimentari indipendentemente dal fatturato dei fornitori e degli acquirenti fra soggetti che siano stabiliti nel territorio nazionale. Essa non riguarda i contratti di cessione direttamente conclusi tra fornitori e consumatori, benché anche per queste transazioni commerciali sarebbe utile prevedere un sistema di tutela e regole di trasparenza analoghe a quelle qui introdotte. La norma ha natura ordinamentale, ed in quanto tale, provvede all'attuazione, adeguamento e coordinamento a livello nazionale della disciplina della direttiva n. 633/2019. Fra i punti salienti della norma UE si evidenziano 3 principi ritenuti irrinunciabili e matrici delle disposizioni in commento:

- definire più dettagliatamente i principi di buone pratiche commerciali di trasparenza, buona fede, correttezza, proporzionalità e reciproca corrispettività a cui occorre attenersi nelle transazioni commerciali;
- coordinare la normativa vigente in materia di termini di pagamento del corrispettivo con le previsioni relative alla fatturazione elettronica;
- prevedere che il pagamento oltre i termini indicati dalla direttiva, inquadrato come pratica commerciale vietata, si applichi pur con i necessari distinguo, anche alle pubbliche amministrazioni, in particolare quelle scolastiche e sanitarie, o, quantomeno, si applichi il divieto di pagamento entro un termine superiore a sessanta giorni già previsto a legislazione vigente.

A tal fine, per alcune prescrizioni del decreto si opta per renderle imperative e prevalenti rispetto ad una pregressa differente disciplina di settore. È il caso degli articoli 3 (Principi ed elementi essenziali dei contratti di cessione), 4 (Pratiche commerciali sleali vietate), 5 (Altre pratiche commerciali sleali) e 7 (Disciplina delle vendite sot-

tocosto di prodotti agricoli ed alimentari).
Le definizioni di cui all'articolo 2 riprendono lo stesso impianto della normativa previgente con qualche accenno di novità: la descrizione di acquirente che include anche le autorità pubbliche e i gruppi di persone fisiche e giuridiche che procedono agli acquisti; la definizione del Dipartimento dell'Ispettorato Centrale della tutela della Qualità e Repressione Frodi dei prodotti agroalimentari del Ministero delle politiche agricole, alimentari e forestali, quale autorità nazionale di controllo e vigilanza e la delimitazione di cosa si intende per disciplina applicabile in caso di ritardato pagamento. Utile e vincente per rendere applicabile la nuova disciplina sui termini di pagamento, creare un esplicito collegamento fra "accordo quadro" e "contratti di cessione con consegna pattuita su base periodica", soprattutto quando il rapporto fra venditore e acquirente risulta qualificato.

Requisiti dei contratti di cessione
L'impianto è quello già esistente nella previgente normativa circa i requisiti essenziali di forma e sostanza con la premessa che i contratti di cessione dovranno essere informati a principi di trasparenza, correttezza, proporzionalità e reciproca corrispettività delle prestazioni. Devono avere forma scritta e l'accordo (scritto) andrà concluso prima della consegna dei prodotti ceduti riportando chiaramente:
• la durata, le quantità e le caratteristiche del prodotto venduto;
• il prezzo, che può essere fisso o determinabile sulla base di criteri stabiliti nel contratto;
• le modalità di consegna e di pagamento.
L'obbligo della forma scritta in alcuni casi specifici può essere assolto anche a mezzo forme equipollenti quali: documenti di trasporto o di consegna, fatture e ordini di acquisto.
In ogni caso, gli elementi contrattuali devono risultare concordati tra acquirente e fornitore mediante un accordo quadro. La durata minima è di 12 mesi, ad eccezione:
• di diverso accordo motivato fra le parti contraenti che risulti da un contratto stipulato con l'assistenza delle rispettive organizzazioni professionali maggiormente rappresentative a livello nazionale;
• di contratti di cessione nel settore della somministrazione di alimenti e bevande (ristoranti, bar e altri pubblici esercizi), poiché spesso le forniture non possono essere programmate annualmente, ma seguono stagionalità e mutevoli preferenze dei clienti.
Restano valide:
• le condizioni contrattuali, comprese quelle relative ai prezzi, che siano compatibili con gli accordi quadro sulla fornitura dei prodotti agricoli e alimentari stipulati dalle organizzazioni professionali rappresentate in almeno cinque camere di commercio, industria, artigianato e agricoltura, ovvero nel Consiglio nazionale dell'economia e del lavoro (CNEL), anche per il tramite delle loro articolazioni territoriali e di categoria;
• le competenze e le funzioni dell'Autorità garante della concorrenza e del mercato (AGCM).
Una prima criticità evidenziata durante gli incontri fra le parti sociali riguarda la durata minima di 12 mesi generalizzata per tutti i contratti di cessione, salvo che non intervenga un accordo scritto fra i contraenti assistiti dalle reciproche sigle sindacali nazionali. Trascurando la discutibile limitazione della libertà contrattuale degli operatori, che non è peraltro contemplata dalla stessa Direttiva (UE) 2019/633, né dai criteri di delega di cui alla legge n. 53/2021, il procedimento di deroga risulta macchinoso e fuori tempo. La varietà e variabilità delle esigenze dei diversi comparti dell'agroalimentare che intersecano altrettante specificità presenti nelle filiere, rendono talora difficile se non impossibile rispettare la norma, ma anche soddisfare le necessità del contesto operativo e commerciale o tenere conto delle caratteristiche della catena di produzione e approvvigionamento. Desta perplessità anche la assistenza necessaria delle Associazioni sindacali di riferimento, che rallenterebbe, o addirittura bloccherebbe, il funzionamento di molte filiere con complessità ingestibili per le migliaia di Operatori del settore. Per completezza va osservato che, nell'era della digitalizzazione, forse valeva la pena di includere nelle forme equipollenti al contratto scritto le risorse informatiche ormai nell'uso quotidiano, come l'e-mail certificata e i supporti digitali informatici.

Black list, Grey list e pratiche consigliate
In tre articoli, il legislatore nazionale definisce 31 diversi comportamenti da stigmatizzare, con alcune deroghe per 6 di questi e alcuni esempi di condotte che rappresentano un modus corretto di negoziazione già in sé per sé. Lo stile è puntuale e manicheo, distinguendo fra quello che è sempre vietato e quello che può diventare lecito solo se vi è un accordo in termini chiari ed univoci fra le parti. Fra i comportamenti ritenuti sleali, si annovera il ritardato versamento del corrispettivo, dettagliando varie ipotesi: dai casi di consegna pattuita su base periodica a quelli di cessione occasionale e, all'interno di questi, fra prodotti deperibili e non. Per i prodotti agricoli e alimentari deperibili, il termine di pagamento non può superare i trenta giorni dal termine della data di consegna. Per i prodotti non deperibili, il termine, invece, non può eccedere i sessanta giorni dalla consegna. Esenzioni, motivate e condivise, sono previste per la distribuzione di prodotti ortofrutticoli e di latte destinati alle scuole, per gli enti pubblici che forniscono assistenza sanitaria, nell'ambito di contratti di cessione tra fornitori di uve o mosto per la produzione di vino e i loro acquirenti diretti. Non è possibile annullare, da parte dell'acquirente, l'ordine di prodotti agricoli e alimentari deperibili con un preavviso inferiore a 30 giorni, salvo eccezioni che definirà un successivo Decreto del Ministro delle politiche agricole, alimentari e forestali.
Altri casi di comportamenti sleali, sono:
• la modifica unilaterale, da parte dell'acquirente o del fornitore, delle condizioni di un contratto di cessione di prodotti agricoli e alimentari in relazione ad elementi sostanziali quali: frequenza, metodo, luogo, tempi o volume della fornitura o della consegna, norme di qualità, termini di pagamento, prezzi, servizi accessori rispetto alla cessione dei prodotti;
• la richiesta al fornitore, da parte dell'acquirente, di pagamenti che non sono connessi alla vendita dei prodotti agricoli e alimentari;
• l'inserimento, da parte dell'acquirente, di clausole contrattuali che obbligano il fornitore a farsi carico dei costi per il deterioramento o la perdita di prodotti agricoli e alimentari che si verifichino presso i locali dell'acquirente o comunque dopo che tali prodotti siano stati consegnati;
• l'acquisizione, l'utilizzo o la divulgazione

illecita, da parte dell'acquirente, di segreti commerciali del fornitore;
• la messa in atto o la minaccia di mettere in atto ritorsioni commerciali nei confronti del fornitore quando quest'ultimo esercita i diritti contrattuali e legali di cui gode.
Per il ritardo nei pagamenti il saggio di interessi è aumentato di 4 punti percentuali rispetto alla disciplina in vigore ed è inderogabile. Sono, inoltre, vietate le clausole precontrattuali che spostino rischi ed oneri economici dal venditore al fornitore, salvo che non siano state concordate espressamente fra le parti in un accordo quadro o nel contratto di cessione. Esemplificando, non possono essere accollati al fornitore i costi:
• per l'immagazzinamento, l'esposizione, e la messa in commercio dei prodotti;
• per gli sconti sui prodotti venduti come parte di una promozione, salvo che non si tratti di una fornitura specificamente destinata;
• per pubblicità e marketing dei prodotti;
• per il personale incaricato di organizzare gli spazi destinati alla vendita dei prodotti.
L'acquirente dovrà fornire al venditore una stima per iscritto dei pagamenti unitari o dei pagamenti complessivi e una valutazione, per iscritto, dei costi a carico del fornitore e i criteri alla base di tale calcolo.
Per le pubbliche amministrazioni è possibile fissare termini di pagamento superiori a quelli previsti in ragione della particolarità del contratto e/o dalle sue caratteristiche mantenendo valide le prescrizioni dell'articolo 4, comma 4, del decreto legislativo n. 231 del 2002.
Vanno sempre bene i contratti triennali, in linea con gli accordi quadro o concordati con le sigle sindacali.
Restano confermati i divieti già esistenti a livello nazionale (articolo 62, comma 2, del decreto legge n. 1 del 2012 e decreto del Ministro delle politiche agricole, alimentari e forestali 19 ottobre 2012, n. 199) con qualche novità, quali: l'acquisto di prodotti agricoli e alimentari con gare e aste elettroniche a doppio ribasso; l'imposizione di condizioni contrattuali eccessivamente gravose per il venditore, come a prezzo inferiore ai costi di produzione o non rispettare le prescrizioni di cui all'articolo 168, paragrafo 4 del regolamento (UE) n. 1308/2013 (contratto stipulato prima della consegna e requisiti essenziali dello stesso).
Per quanto riguarda i prezzi medi a cui fare riferimento nella fissazione del quantum contrattuale, il riferimento ufficiale sono le elaborazioni mensili di ISMEA. Si considera pratica sleale un corrispettivo con un 15% in meno dei costi medi rilevati da ISMEA.
Infine, per gli accordi in linea con le prescrizioni del Decreto è possibile utilizzare nelle campagne pubblicitarie e nel confezionamento dei prodotti della dicitura: "Prodotto conforme alle buone pratiche commerciali nella filiera agricola e alimentare".
Alcune osservazioni risultano opportune. *In primis*, l'annullamento degli ordini non oltre i 30 giorni di preavviso, se soddisfa alcune situazioni, lascia aperte questioni importanti legate al commercio di prodotti freschi e freschissimi che seguono processi e traffici commerciali e giuridici autonomi e delicati. In questo senso, diventa essenziale l'adozione in termini rapidi del Decreto Mipaaf sulle deroghe alla norma generale, prevista dalla norma in commento, per salvaguardare prodotti e settori con necessità atipiche. Presumendo l'impossibilità per il fornitore di trovare un'alternativa di commercializzazione dei prodotti, per specifici casi potrebbe essere opportuno introdurre a livello nazionale una salvaguardia anche per l'acquirente, come la possibilità di provare che l'annullamento dell'ordine non ha impedito al fornitore di collocare con successo in altro luogo la merce.
Altra questione riguarda i prezzi medi stabiliti dall'ISMEA. Essi rappresentano una questione già dibattuta in passato che è stata oggetto di analisi e valutazione sia da parte del Consiglio di Stato che dell'Antitrust. Entrambe hanno riconosciuto come il riferimento a tale parametro costituisca di fatto una disposizione di difficile attuazione, che non porta efficienza nella filiera agricola. Il Tribunale Amministrativo aveva ritenuto contraria alla tutela della concorrenza l'illiceità generalizzata ed inderogabile dei prezzi inferiori ai costi di produzione, essendo questi ultimi variabili da fornitore a fornitore, secondo criteri soggettivi e non oggettivi, con il risultato di penalizzare il consumatore con un incremento del prezzo al mercato. L'Antitrust, nello specifico, ha sottolineato che un prezzo regolatorio applicabile ad un intero settore che possa definirsi equo dovrebbe tenere conto anche di un costo medio di produzione ufficiale che invece nel caso dei prodotti agricoli non esiste, perché legato a fattori contingenti variabili e non regolabili come clima, territorio, patologie e altre variabili che possono portare ad un'offerta eccessiva o ad una scarsa produzione. In questo senso, pare opportuno ritenere il parametro come indicativo e quindi utile per valutare l'opportunità di procedere ad una sanzione, escludendo da una fattispecie così delicata ogni ipotesi di automatismo.

Vendite sottocosto
Non sarà più possibile vendere prodotti agricoli ed alimentari sottocosto, salvo che non vi sia il placet del fornitore, perché rientra in una precisa strategia commerciale, ovvero la merce sia fresca e soggetta a facile e rapido deperimento. L'accordo fra le parti deve essere in forma scritta. In caso di assenza di tale accordo, il prezzo stabilito dalle parti è sostituito di diritto dal prezzo calcolato sulla base dei costi medi di produzione rilevati da ISMEA ovvero, in mancanza di quest'ultimo, dal prezzo medio praticato per prodotti similari nel mercato di riferimento. La competenza resta in capo all'Autorità garante della concorrenza e del mercato (AGCM).
Due precisazioni. La legge di delega Europea non prevede espressamente la surrogazione della normativa sui prezzi agli accordi sottoscritti dalle parti, ma solo tutela il fornitore da eventuali oneri derivanti da perdite di business a lui non imputabili. La stessa legge in commento consente deroghe concordate fra le parti in relazione a situazioni particolari e necessarie.

Autorità di controllo
L'ICQRF (ossia il Dipartimento dell'Ispettorato Centrale della tutela della Qualità e Repressione Frodi dei prodotti agroalimentari del Ministero delle politiche agricole, alimentari e forestali) sarà l'autorità nazionale di contrasto deputata all'attività di accertamento delle violazioni delle disposizioni del decreto ed all'irrogazione delle relative sanzioni. La pubblicità dei provvedimenti sanzionatori inflitti, delle denunce ricevute, delle indagini avviate o concluse nel corso dell'anno precedente e della relazione annuale è garantita con la pubblicazione nell'apposita sezione del sito internet del Mipaaf. Entro il 15 marzo

di ogni anno, il Dipartimento trasmette alla Commissione europea una relazione sulle pratiche commerciali sleali. Per vigilare, l'ICQRF può avvalersi del Comando Carabinieri per la tutela agroalimentare e della Guardia di finanza. Le attività sono svolte d'ufficio o su denuncia di qualunque soggetto interessato, ferme restando le competenze dell'Autorità garante della concorrenza e del mercato per l'accertamento pratiche commerciali sleali. Il denunciante può chiedere di restare anonimo e la PA provvederà in tal senso. A livello procedurale, entro 30 giorni dalla denuncia il Dipartimento comunica come intende procedere. Se la denuncia viene ritirata può comunque decidere di procedere d'ufficio, ovvero ricorrere a procedure di mediazione o di risoluzione alternativa delle controversie.

Sanzioni

L'articolo 10 si occupa delle sanzioni. Stabilisce, quale criterio principe di commisurazione dell'entità della pena, il *quantum* fra il beneficio ricevuto dal soggetto che ha commesso la violazione rispetto all'entità del danno provocato all'altro contraente. Se si accerta la reiterazione o la prosecuzione, da parte dell'autore della violazione, della pratica sleale inibita con provvedimento emanato dell'ICQR, si applica la sanzione amministrativa pecuniaria nella misura massima prevista per la violazione commessa, fermo restando il limite massimo del 10 per cento del fatturato realizzato nell'ultimo esercizio precedente all'accertamento. È prevista una sanzione amministrativa accessoria nel caso di reiterazione delle violazioni di legge con la sospensione dell'attività di impresa fino a trenta giorni. I proventi del pagamento delle sanzioni amministrative pecuniarie saranno assegnati al Dipartimento dell'Ispettorato centrale della tutela della qualità e repressione frodi dei prodotti agroalimentari (ICQRF). L'ICQRF collaborerà con le Autorità di contrasto degli altri Stati membri e con la Commissione europea, anche al fine della reciproca assistenza nelle indagini che presentano una dimensione transfrontaliera.

Entrata in vigore e *tempus regit actus*

All'articolo 14 sono previste le disposizioni transitorie e finali, in base alle quali le disposizioni, di cui allo schema di decreto, si applicano ai contratti di cessione di prodotti agricoli e alimentari conclusi a far data dal 15 dicembre 2021. Mentre, i contratti di cessione in corso di esecuzione prima di tale data, sono resi conformi alle disposizioni del decreto entro sei mesi dalla stessa data.

Contrabbando e Modello 231/01: destinatari e presidi di controllo

di Luigi Fruscione

La normativa doganale: cenni

La disciplina che regola gli scambi doganali è prevista sia da una normativa unionale che nazionale, nella prima rientrano il Codice doganale dell'Unione - regolamento (UE) n.952/2013 - con due ulteriori provvedimenti di integrazione (il regolamento (UE) n.2446/2015) ed applicazione (regolamento (UE) n.2447/2015).

I tre provvedimenti indicati vanno letti in connessione tra loro in quanto il primo rappresenta il vero e proprio codice mentre il secondo integra le disposizioni del 952/2013 ed il terzo stabilisce le regole applicative.

Complessivamente si tratta di XX articoli.

Di particolare importanza sono i capi che affrontano i temi dell'origine delle merci, dell'obbligazione doganale, dei regimi.

A livello nazionale vi è il D.P.R. 23/11/1973 n. 43 - Testo Unico delle disposizioni legislative in materia doganale («TULD») - che disciplina aspetti quali l'organizzazione dei servizi doganali, le prescrizioni ai fini della vigilanza e dei controlli e poteri degli organi doganali, l'obbligazione tributaria doganale, le procedure di accertamento, l'impugnazione e revisione dell'accertamento, etc.

Nell'ambito del tema oggetto di trattazione nell'ambito del TULD rileva l'art. 34 che, nell'ambito del rapporto doganale ed in particolare dell'obbligazione tributaria doganale, pone la definizione di diritti doganali e di confini stabilendo che si considerano "diritti doganali" tutti quei diritti che la dogana è tenuta a riscuotere in forza di una legge, in relazione alle operazioni doganali.

Fra i diritti doganali costituiscono "diritti di confine": i dazi di importazione e quelli di esportazione, i prelievi e le altre imposizioni all'importazione o all'esportazione previsti dai regolamenti comunitari e dalle relative norme di applicazione ed inoltre, per quanto concerne le merci in importazione, i diritti di monopolio, le sovrimposte di confine ed ogni altra imposta o sovrimposta di consumo a favore dello Stato.

I dazi doganali trovano applicazione a tutti quei prodotti importati da Paesi extra Unione europea e rappresentano una delle risorse dell'Unione Europea che confluisce direttamente nel bilancio dell'UE; infatti con la Decisione n.70/243 del Consiglio, del 21 aprile 1970, relativa alla sostituzione dei contributi finanziari degli Stati membri con risorse proprie delle Comunità, "*ha consentito alla Commissione di iniziare a riscuotere risorse proprie per finanziare il bilancio dell'UE anziché affidarsi interamente ai contributi finanziari degli Stati membri. Le prime risorse proprie del bilancio dell'UE sono state i prelievi agricoli, i dazi doganali e una risorsa basata sull'IVA.*

I dazi doganali sono definiti risorse proprie

tradizionali (RPT) in quanto sono sempre esistiti come fonte diretta di entrate per il bilancio dell'UE, a differenza dell'imposta sul valore aggiunto e dei contributi nazionali, che sono messi a disposizione del bilancio dell'UE dagli Stati membri.
I dazi doganali derivano dalle politiche commerciali. Vengono imposti sulle importazioni di prodotti da paesi non appartenenti all'UE secondo aliquote determinate nella tariffa doganale comune.
Con l'abolizione dei contributi zucchero nel 2017, i dazi doganali sulle importazioni provenienti da paesi terzi sono le uniche risorse proprie tradizionali rimaste nel bilancio dell'UE". [1]
L'art. 36 del TULD stabilisce che quando si realizza il presupposto dell'obbligazione doganale, ovverosia per le merci soggette a diritti di confine, il presupposto dell'obbligazione tributaria è costituito, relativamente alle merci estere, dalla loro destinazione al consumo entro il territorio doganale e, relativamente alle merci nazionali e nazionalizzate, dalla loro destinazione al consumo fuori del territorio stesso.
Si intendono destinate al consumo entro il territorio doganale le merci estere dichiarate per l'importazione definitiva e si intendono destinate al consumo fuori del predetto territorio le merci nazionali e nazionalizzate dichiarate per l'esportazione definitiva; l'obbligazione sorge alla data apposta sulla dichiarazione, in presenza dell'operatore, dal funzionario incaricato dell'accettazione.
Stabilire il presupposto è essenziale al fine della configurabilità del contrabbando.

Il contrabbando
Il contrabbando è tra quelle fattispecie di natura finanziaria in quanto, realizzandosi una sottrazione di merci al pagamento dei diritti di confine, si determina una lesione, in particolare, degli interessi dell'Unione europea.
Nel Testo Unico delle Leggi Doganali ("TULD") agli artt. 36 e seguenti si leggono i presupposti che danno origine al delitto di contrabbandando, inteso come: "*la condotta di chi introduce nel territorio dello Stato, in violazione delle disposizioni in materia doganale, merci che sono sottoposte ai diritti di confine*".
La fattispecie in esame si distingue in due tipologie: contrabbando extraispettivo (la prima fattispecie si realizza qualora la merce non si presenta agli Uffici doganali) e intraispettivo (si verifica all'atto della presentazione delle merci ma realizzando quegli artifici che deviano gli accertamenti dell'amministrazione doganale).
Gli artt. 282-291 del D.P.R. n. 43/1973 elencano le singole fattispecie di reato stabilendo per ognuna di esse le condotte alle quali viene collegata la violazione; in particolare abbiamo: art.282 (contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali); art. 283 (contrabbando nel movimento delle merci nei laghi di confine); art. 284 (contrabbando nel movimento marittimo delle merci); art. 285 (contrabbando nel movimento delle merci per via aerea); art. 286 (contrabbando nelle zone extra-dogana); art. 287 (contrabbando per indebito uso di merci importate con agevolazioni doganali); art. 288 (contrabbando nei depositi doganali); art. 289 (contrabbando nel cabotaggio e nella circolazione); art. 290 (contrabbando nell'esportazione di merci ammesse a restituzione di diritti); Articolo 291 (Contrabbando nell'importazione od esportazione temporanea); art. 291-bis (contrabbando di tabacchi lavorati esteri); art. 291-ter (circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri); art. 291-quater (associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri); art. 292 (altri casi di contrabbando); art. 294 (pena per il contrabbando in caso di mancato o incompleto accertamento dell'oggetto del reato).
La Cassazione penale, sentenza n. 33213/2014, ha evidenziato come sia configurabile "*il delitto di contrabbando cosiddetto intraispettivo, previsto dall'art. 292 del D.P.R. 23 gennaio 1973, n. 43, e non l'illecito amministrativo previsto dall'art. 303 del medesimo decreto, qualora la discordanza tra i valori denunciati e quelli accertati delle merci importate derivi non da una semplice dichiarazione ma da un comportamento fraudolento, volto a sottrarre in tutto o in parte la merce al dovuto diritto di confine*".
L'art. 303 del TULD è disciplinato nel capo II nell'ambito delle contravvenzioni ed illeciti amministrativi derivanti dall'applicazione della normativa doganale.
La norma prende in esame il caso delle differenze rispetto alla dichiarazione di merci destinate alla importazione definitiva, al deposito o alla spedizione ad altra dogana; in particolare essa prevede che qualora le dichiarazioni relative alla qualità, alla quantità ed al valore delle merci destinate alla importazione definitiva, al deposito o alla spedizione ad altra dogana con bolletta di cauzione, non corrispondano all'accertamento, il dichiarante è punito con la sanzione amministrativa da euro 103 a euro 516 a meno che l'inesatta indicazione del valore non abbia comportato la rideterminazione dei diritti di confine nel qual caso si applicano le diverse e ben più rilevanti sanzioni indicate all'ultimo comma.
Se i diritti di confine complessivamente dovuti secondo l'accertamento sono maggiori di quelli calcolati in base alla dichiarazione e la differenza dei diritti supera il cinque per cento, la sanzione amministrativa, qualora il fatto non costituisca più grave reato, è applicata come segue:
a) per i diritti fino a 500 euro, si applica la sanzione amministrativa da 103 a 500 euro;
b) per i diritti da 500,1 a 1.000 euro, si applica la sanzione amministrativa da 1.000 a 5.000 euro;
c) per i diritti da 1000,1 a 2.000 euro, si applica la sanzione amministrativa da 5.000 a 15.000 euro;
d) per i diritti da 2.000,1 a 3.999,99 euro, si applica la sanzione amministrativa da 15.000 a 30.000 euro;
e) per i diritti pari o superiori a 4.000 euro, si applica la sanzione amministrativa da 30.000 euro a dieci volte l'importo dei diritti.

Il D.Lgs. n. 231/01
Con l'entrata in vigore del D.Lgs. n. 231 del 2001 nel nostro sistema giuridico si è sancita la responsabilità dei soggetti collettivi in sede penale.
La normativa, pur essendo qualificata come amministrativa, ha una struttura strettamente connessa al penale; basti pensare infatti alla disciplina di accertamento della responsabilità in base alla quale trovano

1 *Si veda il sito internet della Commissione europea - sezione dazi doganali.*

applicazione le norme del codice di procedura penale (art. 34), è prevista l'estensione della disciplina relativa all'imputato all'ente (art.35), l'attribuzione al giudice penale della competenza a conoscere degli illeciti 231 (art.36), etc.
L'ente è ritenuto responsabile per i reati commessi nel suo interesse o a suo vantaggio da due categorie di soggetti:
a) le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonchè da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
b) le persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).
Affinchè si possa giungere ad una condanna dell'ente occorre che il reato 231 non sia stato commesso dal soggetto agente nell'interesse esclusivo proprio o di terzi.
Pur in presenza di un reato il soggetto collettivo potrà andare esente da responsabilità qualora abbia adottato un modello di organizzazione e gestione del rischio connesso ai reati che astrattamente si possono verificare nello svolgimento della propria attività di business.
Infatti l'art. 6 precisa che "*se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che...*" a significare che la verificazione della fattispecie criminosa di per sé non rende inefficace l'esimente.
Quali sono gli elementi che si dovranno dimostrare esistenti per l'applicazione del Modello sono:
a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi. Qualora il Modello sia adottato successivamente alla realizzazione del reato la normativa prevede una diminuzione della pena da un terzo alla metà qualora prima della dichiarazione di apertura del dibattimento di primo grado l'ente:
1. abbia risarcito integralmente il danno ed abbia eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
2. abbia, per l'appunto, adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; tale organismo dovrà compiere le proprie attività di vigilanza in maniera sufficiente (requisito sub lett. d, art.6, co.1);
c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione.
Affinchè il modello sia idoneo occorre che siano:
a) individuate le attività nel cui ambito possono essere commessi reati;
b) predisposti specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
c) individuate le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
d) posti obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
e) introdotto un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.
L'art. 7 del D.Lgs. n.231/01 si occupa delle prescrizioni che il modello deve contenere rispetto ai soggetti sottoposti stabilendo che, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, devono essere previste misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.
L'efficace attuazione del modello richiede:
a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il D.Lgs. n. 231/01 ed il contrabbando
Nell'ambito dell'imponente attività di implementazione delle fattispecie incriminatrici che comportano una responsabilità 231 con il D.Lgs. n.75/2020 - con cui è stata data attuazione alla Direttiva UE 2017/1371 sulla protezione degli Interessi finanziari della Unione europea (Direttiva «PIF») - si è stabilito l'introduzione dell'art. 25 sexiesdecies relativo al reato di contrabbando doganale attraverso il quale si cerca di interviene sull'elusione dei diritti doganali che rappresentano una risorsa propria dell'UE.
Le sanzioni previste sono quella pecuniaria fino a duecento quote; quando i diritti di confine dovuti superano centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote.
Oltre alle sanzioni pecuniarie si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e) ovverosia:
c) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
d) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
e) il divieto di pubblicizzare beni o servizi.
Nell'ambito di un protocollo di riduzione del rischio di verificazione del reato di contrabbando occorrerà richiamare anche il rispetto dei protocolli relativi al rapporto con funzionari della pubblica amministrazione in considerazione del fatto che l'Agenzia delle Dogane è un ente pubblico dotato di personalità giuridica che dipende direttamente dal Ministero dell'Economia e delle Finanze. Da ciò deriva che i funzionari sono pubblici ufficiali.
A ciò si aggiunga che l'altra Autorità che svolge compiti in materia doganale è rappresentata dalla Giardia di Finanza. Quindi i rapporti con i pubblici ufficiali dovranno seguire gli specifici protocolli predisposti dal soggetto collettivo.
Il codice doganale è fondato sul criterio dell'affidamento su quanto contenuto nella dichiarazione doganale. Vigono quindi tre generici obblighi in capo al soggetto

che presenta i documenti in dogana:
a) esattezza e completezza delle informazioni;
b) autenticità dei documenti e dati ivi contenuti;
c) osservanza degli obblighi di legge.
Quindi tutta la documentazione necessaria alla presentazione della dichiarazione in dogana deve essere oggetto di attenta verifica da parte del soggetto importatore, in tal senso assume rilievo la qualifica dei fornitori extra UE, della gestione del ciclo passivo, il riscontro dell'avvenuto pagamento dei dazi doganali con la riconciliazione con la dichiarazione doganale, la verifica delle attività svolte da parte del rappresentante in dogana.
Deve essere individuato all'interno dell'organizzazione del soggetto collettivo il soggetto che è deputato alla individuazione del valore in dogana.
Presidio fondamentale è dato dalla tracciabilità dell'intero flusso passivo dall'ordine all'arrivo delle merci in magazzino con la corrispondenza dell'intera documentazione che va riconciliata con la documentazione doganale, in tal senso istituire anche una procedura di controllo a campione è senz'altro auspicabile.
A tali controlli si aggiungono quelli che ogni ordine deve essere formalizzato così come ogni operazione doganale delegato ad un fornitore di servizi doganali.
Particolare importanza è data da una attività di formazione sul momento doganale al fine di chiarire gli aspetti maggiormente importanti della gestione di classificazione, origine e valore delle merci importate.
Per quanto fin qui evidenziato si ritiene di consigliare l'organizzazione di personale che sia chiamato funzionalmente alla gestione degli aspetti doganali (amministrazione, logistica e magazzino su tutte).
In tal senso appare rilevante l'ottenimento dell'autorizzazione AEO attraverso la quale l'operatore economico sarà ritenuto da parte dell'Agenzia delle Dogane quale partner affidabile o molto affidabile in seguito ad una attività di audit da questa svolta.

"Sistema 231": le nuove Linee Guida Confindustria

di Elisabetta Torzuoli

Correva l'anno 2002, quando Confindustria accettava la sfida lanciata da un sistema legislativo che puntava a prevenire i reati nello svolgimento dell'attività di impresa, favorendo la cultura dei controlli interni e della trasparenza gestionale.
È noto agli addetti ai lavori che il D.Lgs. 231/2001 ha introdotto nel nostro panorama normativo una specie di responsabilità formalmente amministrativa, ma sostanzialmente penale, a carico degli enti, in conseguenza della commissione, nel loro interesse o vantaggio, di un reato, sanzionando una colpa c.d. d'organizzazione.
Deflagrato, così, il noto brocardo "*societas delinquere non potest*", è stata invece riconosciuta l'opposta capacità dell'ente che, come correttamente ha rilevato il giurista Carlo Piergallini, "*...ha la capacità di indurre la criminalità di impresa: la scelta dell'illegalità non costituisce mai un'episodica degenerazione individuale, ma il frutto di un'azione organizzata che non ha interiorizzato (intenzionalmente o per carenze organizzative) la cultura della legalità.*".
Diversamente detto, rifacendosi ad una nota elaborazione giurisprudenziale della Suprema Corte, nella sua massima composizione, la c.d. colpa d'organizzazione si traduce in una "*inottemperanza da parte dell'ente dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenire la commissione dei reati previsti tra quelli idonei a fondare la responsabilità del soggetto collettivo, dovendo tali accorgimenti essere consacrati in un documento che individua i rischi e delinea le misure atte a contrastarli* (Cass. Pen, Sez. Un., 24.4.2014, n. 38343).
Introducendo una logica preventiva e premiale, l'ente non risponde allorquando: abbia adottato ed efficacemente attuato un modello organizzativo, di gestione e controllo idoneo a prevenire reati della specie di quello verificatosi, il compito di vigilare sul funzionamento e l'osservanza del modello sia stato affidato ad un organismo di vigilanza e non ci si sia stata omessa o insufficiente vigilanza ed il reato sia stato commesso eludendo fraudolentemente il modello (nel caso in cui l'autore sia un apicale) ovvero in caso di inosservanza di obblighi di direzione e vigilanza (nel caso in cui il reo sia un sottoposto).
In questa impostazione, è stata prevista sin dall'inizio la possibilità di adozione dei modelli, assicurando le esigenze prima descritte, sulla base di codici di comportamento redatti dalle associazioni maggiormente rappresentative degli enti: la prima edizione delle Linee Guida viene, quindi, pubblicata nel marzo 2002 ed è revisionata dapprima nell'aprile 2008, quindi nel marzo 2014 e, da ultimo, nel giugno 2021.

Rimane la struttura bipartita tra parte generale e parte speciale: la prima, suddivisa in lineamenti della responsabilità 231, analisi delle componenti del modello (rischi e protocolli, codice etico e sistema disciplinare, organismo di vigilanza), la seconda, concentrata su *case study* per le singole fattispecie di reato presupposto, oramai diventato un ricco e diversificato catalogo.

Finalità
Prima di procedere alla rassegna delle principali novità apportate, piace riportare le finalità conclamate in esordio delle linee guida, dalla stessa Confindustria, perché in essa si compendia lo spirito che deve animare l'ente nell'adozione di un modello ed il monito che il sistema preventivo adottato non rimanga un mero adempimento burocratico, un'apparenza di organizzazione, ma che viva nell'impresa e si conformi alle sue esigenze.
"Confindustria si propone, mediante le presenti Linee Guida, di offrire alle imprese che abbiano scelto di adottare un modello di organizzazione e gestione una serie di indicazioni e misure, essenzialmente tratte dalla pratica aziendale, ritenute in astratto idonee a rispondere alle esigenze delineate dal decreto 231. Tuttavia, data l'ampiezza delle tipologie di enti presenti nella realtà associativa di Confindustria e la varietà di strutture organizzative di volta in volta adottate in funzione sia delle dimensioni sia del diverso mercato geografico o economico in cui essi operano, non si possono fornire riferimenti puntuali in tema di modelli organizzativi e funzionali, se non sul piano metodologico. Le Linee Guida, pertanto, mirano a orientare le imprese nella realizzazione di tali modelli, non essendo proponibile la costruzione di casistiche decontestualizzate da applicare direttamente alle singole realtà operative. Pertanto, fermo restando il ruolo chiave delle Linee Guida sul piano della idoneità astratta del modello che sia conforme ad esse, il giudizio circa la concreta implementazione ed efficace attuazione del modello stesso nella quotidiana attività dell'impresa è rimesso alla libera valutazione del giudice. Questi compie un giudizio sulla conformità e adeguatezza del modello rispetto allo scopo di prevenzione dei reati da esso perseguito. In questa prospettiva, è di fondamentale importanza, affinché al modello sia riconosciuta efficacia esimente, che l'impresa compia una seria e concreta opera di implementazione delle misure adottate nel proprio contesto organizzativo. Il modello non deve rappresentare un adempimento burocratico, una mera apparenza di organizzazione. Esso deve vivere nell'impresa, aderire alle caratteristiche della sua organizzazione, evolversi e cambiare con essa.
L'auspicio che sospinge il presente lavoro e, in particolare, la revisione compiuta nel 2014, è che le soluzioni indicate nelle Linee Guida continuino a ispirare le imprese nella costruzione del proprio modello e che, d'altra parte, la giurisprudenza valorizzi i costi e gli sforzi organizzativi sostenuti dalle imprese per allinearsi alle prescrizioni del decreto 231".
Un invito, dunque, quello formulato da

Confindustria e rivolto alla giurisprudenza a valorizzare gli sforzi compiuti dall'ente, a fronte dell'adempimento ad una prescrizione, l'adozione del modello, ad oggi non obbligatoria, in ordine alla quale comunque le stesse imprese riconoscono una serie di vantaggi, consacrati anche da diverse disposizioni normative.
Oltre alla possibile esclusione della responsabilità dell'ente ed ai vantaggi sul piano edittale ex D.Lgs. 231/2001, oggi la predisposizione è ritenuta conveniente perché:
• consente l'individuazione di gap organizzativi, favorisce la chiarezza organizzativa, la razionalizzazione dei presidi di controllo, la ripartizione di poteri e responsabilità, incentivando un business trasparente;
• assicura il rispetto di normative, con conseguente riduzione del rischio di sanzioni da non-conformità e del relativo *cost-saving*;
• agevola l'accesso ai bandi di gara indetti dalla Pubblica Amministrazione, con indubbio vantaggio reputazionale;
• assicura un miglior posizionamento riguardante il *rating* di impresa e di legalità, migliorando i rapporti con le pubbliche amministrazioni e incrementando, nelle gare di appalto, le *chance* di aggiudicazione.
Anche diversi corpi di norme, riconoscono ormai un valore significativo al modello 231, vediamoli:
• Il codice della crisi di impresa, ove l'integrazione del modello 231 con quanto previso dal D.Lgs. 14/2019 può essere una scelta efficace e sintomatica di una realtà sicura e affidabile, poiché il modello 231 è ascritto tra quelle previsioni che assicurano il principio di adeguatezza dell'assetto societario;
• T.U. 81/2008 che ha stabilito un esimente del dovere di vigilanza del datore di lavoro in caso di adozione di un modello 231;
• Terzo settore: l'art. 4, comma 1, lett. g), L. 106/2016 suggerisce l'adozione del modello 231, nel disciplinare gli obblighi di controllo interno e di accountability nei confronti dei diversi stakeholder, mentre la delibera ANAC 20.01.2016, n. 32 (recante "*Linee Guida per l'affidamento di servizi a enti del terzo settore e alle cooperative sociali*"), prevede che l'appaltante debba verificare l'applicazione del D.Lgs. 231/2001, in capo agli enti no-profit;
• tra le misure di *self-cleaning* significative ai sensi dell'art. 80 del codice degli appalti, le Linee Guida Anac 16.11.2016, n. 6, individuano l'adozione di idonei modelli di organizzazione, gestione e controllo che prevengono reati della specie di quello verificatosi, come misura per superare l'esclusione dalla partecipazione alle gare pubbliche per gli operatori economici;
• in ambito previdenziale, sono previsti rilevanti sgravi contributivi INAIL per l'ente munito di modello, che sia efficacemente attuato nell'ambito dell'organizzazione di impresa.
In definitiva, sebbene la scelta del nostro legislatore in ambito 231, sia ancor oggi quella di mantenere come facoltativa l'adozione del *compliance programs*, la sua mancanza, nell'ambito di una organizzazione aziendale complessa, rischia di apportare riflessi negativi.

Le principali novità apportate dall'edizione 2021
L'approccio integrato nella gestione del rischio, la disciplina del whistleblowing, una miglior caratterizzazione dell'organismo di vigilanza costituiscono le principali novità da segnalare con riguardo alla parte generale, mentre, per quanto concerne la parte speciale, questa si arricchisce dell'analisi (con lo studio approfondito di aree a rischio, potenziali modalità di commissione, protocolli e presidi da predisporre in via preventiva per evitare commissione del rischio) riferita alle nuove fattispecie – presupposto, che nel tempo hanno arricchito il catalogo dei reati-presupposto (ossia corruzione privata, falso in bilancio/autoriciclaggio/riciclaggio/abusi di mercato, caporalato, reati ambientali, impiego di cittadini terzi il cui soggiorno è irregolare, traffico di influenze illecite, illeciti tributari, frode nelle pubbliche forniture, contrabbando, peculato e abuso di ufficio).
La presente disamina procede ora, concentrandosi sulle novità della parte generale.

Approccio integrato nella gestione del rischio

"*...la gestione dei numerosi obblighi di compliance, secondo un approccio tradizionale, può risultare connotata da una pluralità di processi, informazioni potenzialmente incoerenti, controlli potenzialmente non ottimizzati, con conseguente ridondanza nelle attività.*
Il passaggio ad una compliance integrata potrebbe permettere invece agli Enti di:
• razionalizzare le attività (in termini di risorse, persone, sistemi, ecc.);
• migliorare le attività (in termini delle attività di compliance;
• facilitare la condivisione delle informazioni attraverso una visione integrata delle diverse esigenze di compliance, anche attraverso l'esecuzione di risk assessment congiunti, e la manutenzione periodica dei programmi di compliance (ivi incluse le modalità di gestione delle risorse finanziarie, in quanto rilevanti ed idonee ad impedire la commissione di molti dei reati espressamente previsti come fondanti la responsabilità degli enti)."
Il *rischio di compliance*, ossia di non conformità alle norme, comporta per le imprese il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni reputazionali in conseguenza di violazioni di norme imperative ovvero di autoregolamentazione, molte delle quali rientrano nel novero dei reati di cui al D.Lgs. 231/2001.
Un approccio tradizionale nella gestione degli obblighi di *compliance* può portare sfasamenti, pluralità di processi, informazioni potenzialmente incoerenti, controlli potenzialmente non ottimizzati, con conseguente ridondanza nelle attività.
Proseguono, perciò le linee guida: "*In quest'ottica, un approccio integrato dovrebbe, quindi, contemplare procedure comuni che garantiscano efficienza e snellezza e che non generino sovrapposizione di ruoli (o mancanza di presidi), duplicazioni di verifiche e di azioni correttive, in termini più ampi, di conformità rispetto alla copiosa normativa di riferimento, laddove tali ruoli rispettivamente incidano e insistano sui medesimi processi.*"
Quali azioni vanno, dunque, poste in essere per realizzare un'integrazione nella gestione del rischio?
prevedere procedure comuni che assicurino efficienza e snellezza ed evitino sovrapposizione di ruoli (o mancanza di presidi), duplicazioni di verifiche e di azioni correttive, in termini più ampi, di conformità rispetto alla normativa di riferimento, laddove tali ruoli rispettivamente incidano e insistano sui medesimi processi; predisporre o integrare le procedure tenendo conto delle peculiarità sottese a ciascuna di esse, portando a sintesi gli adempimenti, individuando le modalità per intercettare e verificare gli eventi economici e finanziari dell'impresa nell'ottica del corretto agire; definire specifici e continui meccanismi di coordinamento e collaborazione tra i principali soggetti aziendali interessati tra i quali, a titolo esemplificativo, il Dirigente

Preposto, la funzione Compliance, l'Internal Audit, il Datore di lavoro, il Collegio sindacale, il Comitato per il controllo interno e la revisione contabile (ai sensi dell'art.19, d.lgs. n. 39/2010) e l'OdV; implementare i sistemi di controllo già esistenti (*tax control framework* / reati tributari – *SGSL* ex d. lgs. n. 81 del 2008 e standards internazionali / reati in materia di salute e sicurezza dei lavoratori) attraverso la loro integrazione nel Modello 231 (con conseguente previsione di poteri di monitoraggio in capo all'OdV, flussi informativi nei confronti dell'OdV, applicazione del sistema disciplinare, meccanismi di tutela del segnalante); armonizzare i sistemi esistenti ed obbligatori con quelli c.d. "volontari" (es. ISO 14001, ISO 27001, ISO 37001) e valorizzare gli esiti delle attività di audit interno e delle verifiche funzionali al conseguimento e al mantenimento delle relative certificazioni.

Il whistleblowing

Le linee guida dedicano un apposito capitolo alla procedura volta ad introdurre il whistleblowing, all'interno del modello. È noto che l'art. 6, comma 2-bis, D.Lgs. 231/2001 stabilisce che:

"I modelli di cui alla lettera a) del comma 1 prevedono:

a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;

c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;

d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate."

Con riguardo all'ambito soggettivo, questo è individuato negli enti che intendono istituire un sistema di prevenzione 231, il cui modello dovrà prevedere: appositi canali per segnalare eventuali illeciti rilevanti ai sensi del decreto 231, nonché violazioni del modello stesso; i canali devono garantire la riservatezza dell'identità del segnalante e almeno uno deve prevedere modalità informatiche; indicare il "destinatario" delle segnalazioni e le caratteristiche dimensionali e organizzative; stabilire il divieto di atti di ritorsione o discriminatori nei confronti dei whistleblowers e misure sanzionatorie in caso di violazione degli obblighi di riservatezza e/o atti ritorsivi o discriminatori. Le linee concludono raccomandando l'adeguamento alle prescrizioni di cui alla direttiva 2019/1937, di prossimo, si auspica, recepimento. Per quanto concerne la riservatezza dell'identità del segnalante, si evidenzia che, rispetto ad altre normative che prevedono l'istituto del whistleblowing, in ambito 231 non è richiesto l'anonimato, poiché per garantire al denunciante una tutela adeguata, anche in termini di riservatezza dell'identità, è necessario che costui sia riconoscibile. Pur tuttavia, i modelli organizzativi possono prevedere anche canali per effettuare segnalazioni in forma anonima, ma con delle cautele, onde evitare di compromettere la necessaria verifica della fondatezza della denuncia, al fine di arginare il rischio di denunce infondate. A tal fine, è possibile adottare degli *escamotage*, prevedendo che le segnalazioni siano documentate adeguatamente ovvero rese con dovizia di particolari e "*in grado di far emergere fatti e situazioni relazionandoli a contesti determinati*", come precisato dall'Anac (avendo riguardo alle segnalazioni che è tenuta a gestire). Una precisazione, infine, quanto al destinatario. Vista la rosa di possibilità offerte da Confindustria (Organismo di Vigilanza ovvero un altro soggetto, comitato, struttura specificamente individuato; responsabile della funzione *compliance*; un comitato rappresentato da soggetti appartenenti a varie funzioni, ad esempio legale, *internal audit*, *compliance*, HR; 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; il datore di lavoro nelle PMI), va precisato che se il destinatario è individuato in un soggetto diverso dall'Organismo di Vigilanza, questo andrà coinvolto in via concorrente ovvero successiva, per evitare il rischio che il flusso di informazioni generato dal meccanismo di whistleblowing sfugga del tutto al suo monitoraggio, prevedendo un'apposita reportistica nei suoi confronti.

Organismo di vigilanza

Le linee guida esaminano dunque il fulcro del sistema di vigilanza, riconosciuto come perno soggettivo del sistema di contenimento del rischio penale, centro di riferimento del sistema gestorio per la valutazione e verifica costante dell'adeguatezza del modello e della sua effettiva implementazione. Viene analizzata, dunque, la sua composizione variabile, monosoggettivo, plurisoggettivo, con esame della composizione di membri interni ed esterni, sono ribaditi i requisiti di autonomia, indipendenza, professionalità, l'importanza dell'effettivo funzionamento di flussi informativi, nonché i rapporti tra organismo di vigilanza e collegio sindacale.

Conclusioni

L'arresto di Confindustria, tanto atteso a seguito delle continue novelle in un'ottica di ampliamento dei reati - presupposto, segna un fondamentale passaggio verso la valorizzazione dell'organizzazione di impresa. Nonostante l'adozione del modello rientri comunque in una scelta gestoria dell'ente, è evidente la crescente centralità che assume la compliance nell'organizzazione aziendale, anche a seguito della ventennale applicazione del D.lgs. 231/2001. Fermo l'impegno delle imprese nell'adeguarsi ai dettami normativi e nel revisionare le procedure e protocolli già esistenti facendo propri i preziosi focus apportati dalle linee guida, si attende ora un riconoscimento premiale in sede giudiziale, il superamento delle incertezze sul giudizio di idoneità concreta, una valorizzazione dei presidi di gestione e controllo del rischio esistenti nelle imprese di grandi dimensioni (sistemi di compliance integrata, certificazioni ISO, programmi anticorruzione, procedure e controlli societari).

Più di tutti, è forse atteso ed auspicato un ritocco al testo di legge, al fine di attribuire determinatezza ai parametri sui contenuti e modalità di costruzione del modello in ottica di esimente. La prassi, dunque, recepita dalla maggiore associazione rappresentativa degli enti, sembra ora voler cedere il passo al Legislatore.

Intelligenza artificiale e tecnologie cyber: opportunità o limite?

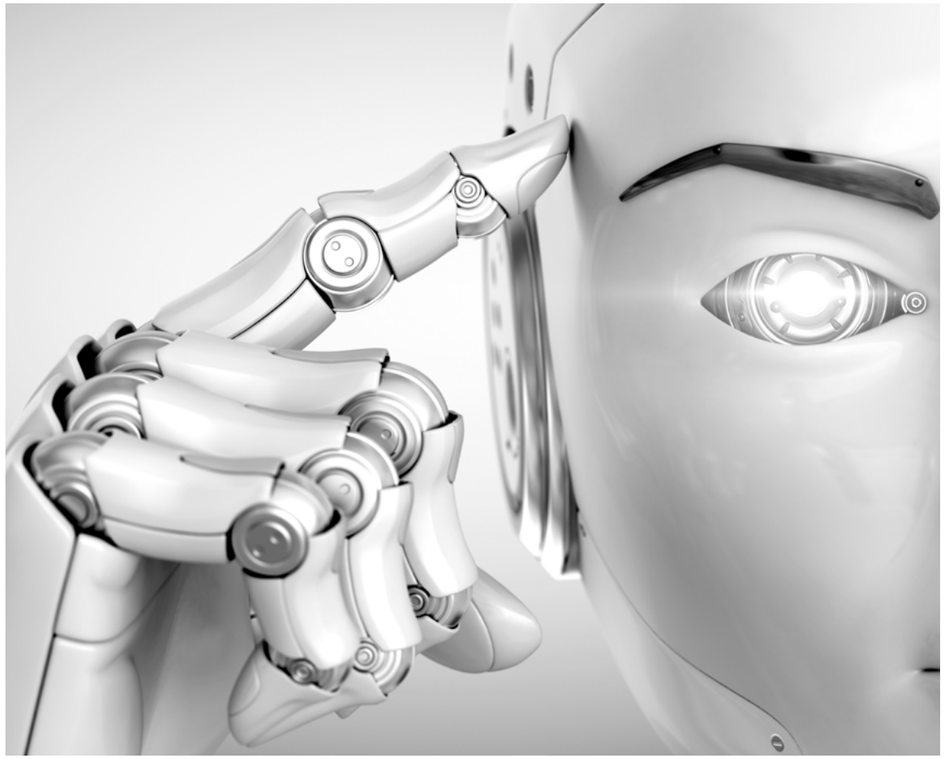
di Giovanni Finetto e Paola Finetto

Lo scorso 9 novembre 2021 è stato pubblicato il rapporto, datato 2 novembre 2021, della Commissione del Parlamento Europeo sulla Intelligenza Artificiale in un'Era Digitale (*Special Committee on Artificial Intelligence in a Digital Age*), nel quale si evidenzia come l'Unione Europea dovrebbe fornire agli Stati Membri gli strumenti – e, primo fra tutti, una normativa uniforme – per agevolare il migliore impiego della intelligenza artificiale (IA). Tanto più che le tecnologie basate sulla intelligenza artificiale potrebbero avere un ruolo determinante in settori strategici delle politiche comunitarie, quali quello dell'ambiente, della salute e della competitività. A questo riguardo, nel rapporto in esame si legge che l'IA è la vera e propria chiave del sistema tecnologico scaturente dalla quarta rivoluzione industriale, anzi, l'IA costituisce essa stessa un quinto elemento che permea la nostra esistenza dopo l'aria, la terra, l'acqua, il fuoco.

Avendo riguardo a studi presentati dal Parlamento Europeo[1] e ripresi dal legislatore italiano[2], l'IA può essere definita come *l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività; tali caratteristiche consentono all'IA la comprensione del proprio ambiente, l'elaborazione di ciò che viene percepito e l'individuazione di soluzioni per un obiettivo specifico. In particolare, il sistema è in grado di ricevere i dati (già preparati o raccolti tramite sensori), di processarli e di indicare la risposta richiesta.* Le applicazioni delle tecnologie basate sulla intelligenza artificiale sono effettivamente numerose e spaziano in settori tra loro anche molto diversi: si pensi ai software di assistenza virtuale, agli strumenti di videosorveglianza con riconoscimento facciale, agli strumenti di analisi di immagini o di riconoscimento vocale. Molto spesso, poi, le tecnologie di IA vengono integrate in altri sistemi, come robot, droni, veicoli a guida autonoma e, più in generale, strumenti riconducibili all'IoT (Internet of Things).

Negli ultimi anni le istituzioni europee hanno avviato un percorso volto a sostenere e promuovere una serie di azioni tese a favorire maggiori applicazioni della IA ma, allo stesso tempo, garantirne l'affidabilità. In questo contesto, il 16 giugno 2020 è stata costituita, su iniziativa del Parlamento Europeo, la Commissione AIDA allo scopo di studiare lo sviluppo delle tecnologie *AI-based*, monitorare la loro incidenza sulla economia europea ed elaborare proposte per una legislazione comunitaria uniforme in questa materia. Nel dettaglio, alla Commissione AIDA è stato affidato, tra l'altro, il compito di:

- analizzare gli impatti futuri della IA sulla economia europea, con particolare riferimento ai settori lavoro, istruzione, salute, fintech, trasporti, turismo, agricoltura, ambiente, difesa, industria, energia, e-government;
- monitorare lo sviluppo della IA e il suo contributo ai valori di business e alla crescita economica;
- elaborare strategie di medio e lungo termine per favorire il transito europeo verso un'era autenticamente digitale.

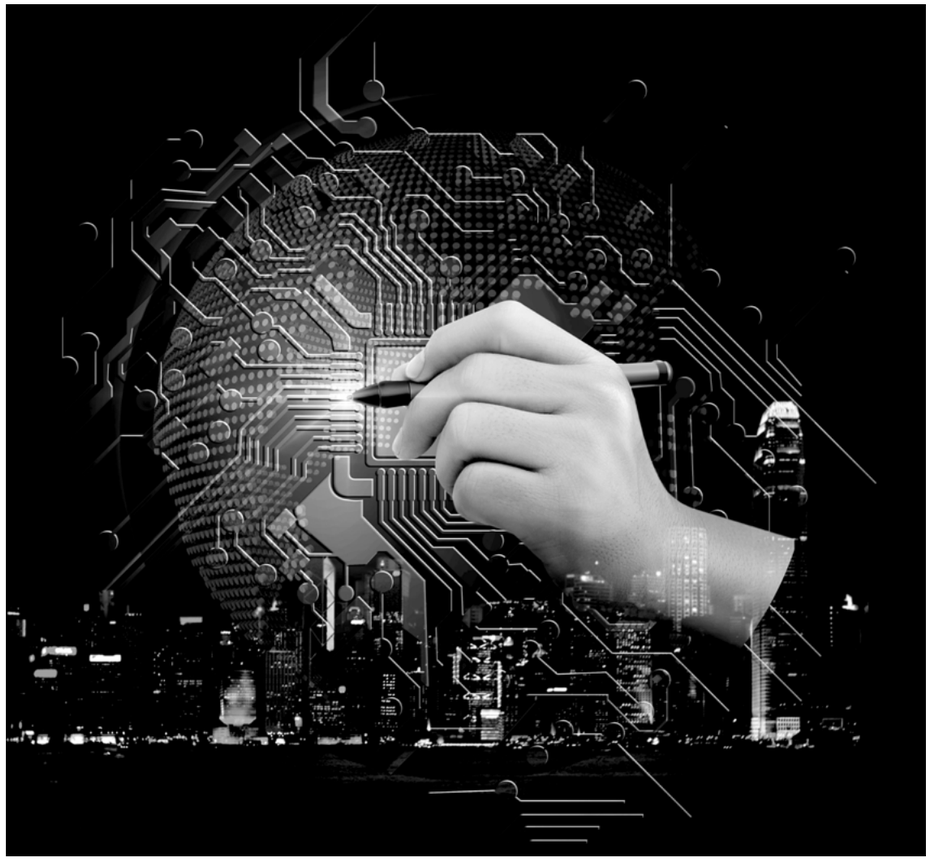


L'interesse delle istituzioni europee per il settore della intelligenza artificiale viene da lontano. Il Trattato sul funzionamento dell'Unione Europea prevede specifiche competenze in capo all'Unione Europea nel settore della ricerca e dello sviluppo tecnologico, dunque anche nell'ambito digitale e della IA: in tal senso, gli artt. 4, 13, 16, 26, 173, 179, 180, 181, 182, 186 e 187 del Trattato medesimo. Nel corso degli ultimi due anni, tuttavia, si sono intensificate, in ambito europeo, le iniziative volte a evidenziare gli aspetti più concreti, operativi e applicativi della IA: è del 28 luglio 2020 uno studio della Commissione Europea relativo all'uso da parte delle imprese delle tecnologie basate sull'intelligenza artificiale. Da questo studio emerge come il 42% delle imprese europee partecipanti al sondaggio utilizzi sistemi e applicazioni basati sulla IA; si tratta soprattutto di grandi imprese che, comunque, risultano dotate, al più, di due tecnologie di IA. Il sondaggio condotto dalla Commissione Europea rileva, tuttavia, come il 40% delle imprese in-

1 *https://www.europarl.europa.eu/news/it/headlines/priorities/intelligenza-artificiale-nell-ue/20200827STO85804/che-cos-e-l-intelligenza-artificiale-e-come-viene-usata*

2 *https://documenti.camera.it/Leg18/Dossier/Pdf/RI070.Pdf*

tervistate non solo non utilizzi tecnologie *AI-based* ma, soprattutto, non sia neppure intenzionato a farlo nel prossimo futuro. Questa presa di posizione di imprese per lo più medio-piccole sconta, probabilmente, le incertezze che, ancora oggi, caratterizzano le tecnologie di intelligenza artificiale; non a caso nel rapporto pubblicato dalla Commissione AIDA il 9 novembre 2021 si fa riferimento espresso all'impatto che l'uso dell'intelligenza artificiale può avere sui diritti fondamentali, quali, a titolo meramente esemplificativo, i diritti alla protezione dei dati personali e il diritto alla riservatezza. A quest'ultimo riguardo lo stesso Parlamento Europeo, con una risoluzione del 20 ottobre 2020, aveva invitato la Commissione Europea a presentare una proposta di regolamento sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale; in questa risoluzione si metteva in evidenza il ruolo cruciale dei sistema di IA nella società, nei luoghi di lavoro e nell'economia degli Stati membri, potendo le tecnologie basate sulla IA migliorare la qualità di vita in ogni settore, dai trasporti all'istruzione, dalla sanità alla concessione di credito, dall'ambiente al lavoro. Al contempo, tuttavia, la risoluzione rilevava come "*la complessità, la connettività, l'opacità, la vulnerabilità, la capacità di modifica mediante aggiornamenti, l'autoapprendimento e la potenziale autonomia dei sistemi di IA, come pure la molteplicità degli attori coinvolti nel settore*" e la consapevolezza che "*tutte le attività, i dispositivi o i processi fisici o virtuali che sono guidano da sistemi di IA possono essere tecnicamente la causa diretta o indiretta di danni o pregiudizi*", rendano inevitabile una regolamentazione uniforme in materia di responsabilità derivante dall'uso di sistemi di IA. A questa risoluzione ne sono seguite molte altre, soprattutto nel corso dell'ultimo anno: si



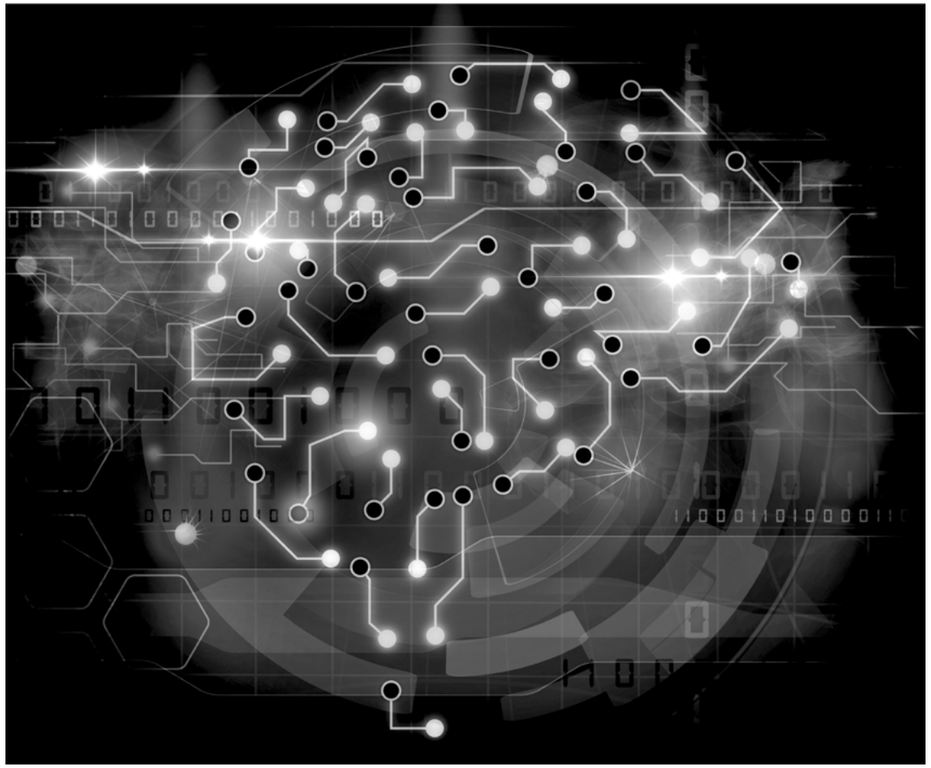
pensi alle risoluzioni del 25 marzo 2021 su una strategia europea per i dati, del 19 maggio 2021 sulla IA nella istruzione, nella cultura e nel settore audiovisivo, del 6 ottobre 2021 sulla IA nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale. In particolare, con quest'ultima risoluzione, il Parlamento europeo si è espresso a favore di una "*governance dell'IA a livello europeo con una valutazione indipendente*", ritenendo che soltanto questa metodologia consenta "*la necessaria attuazione operativa dei principi riguardanti i diritti fondamentali*".

In definitiva, è chiaro come le tecnologie basate sull'intelligenza artificiale possano alleggerire la quotidianità, semplificare operazioni complesse di natura finanziaria, rendere meglio e più velocemente accessibili servizi alle persone, favorire la transizione verso una economia realmente digitale. Tutte queste applicazioni della IA, tuttavia, non sono esenti da rischi di manipolazione e malfunzionamenti, che potrebbero compromettere, anche significativamente, i diritti fondamentali delle persone, tra cui il diritto alla protezione dei dati personali. Alcuni dei sistemi basati sulla IA e già in uso hanno evidenziato questi limiti, tanto più che si tratta di tecnologie comunque vulnerabili ed esposte ad attacchi hacker. Per quanto innovativi, anche i sistemi *AI-based* sono esposti ai rischi della rete e del web e, al contrario, sempre più spesso l'IA viene utilizzata dagli hacker malevoli per mettere a punto sofisticati attacchi informatici. La stessa IA può anche essere utilizzata dai "protettori della rete" come ausilio nella ormai conclamata "guerra tra macchine". Facciamo però un passo indietro e torniamo nel 1988, quando Robert Tappan Morris, laureato ad Harvard, effettuò quello che da tutti viene considerato il primo attacco hacker della storia tramite un worm, ovvero un malware capace di moltiplicarsi all'interno della rete vittima, in quel caso quasi il 10% della rete internet che all'epoca contava circa 60.000 computer online. Questo attacco cominciò a instillare i primi dubbi sulla sicurezza di una rete che nasce per definizione libera e con la finalità di mettere a disposizione di tutti le informazioni condivise all'interno della rete stessa. Se si interpretano questi dubbi con la consapevolezza odierna, ci si rende conto che la rete globale è una realtà quasi "fuori controllo", dove la sicurezza rappresenta una rincorsa continua, dati i tempi velocissimi di sviluppo di nuove applicazioni firmware e software e lo sviluppo, d'altra parte, di tecniche di hacking sempre più complesse e fantasiose. Le realtà statuali, da parte loro, hanno cominciato, da un lato, a comprendere la dimensione cyber come una nuova dimensione da dominare e un nuovo luogo dove esercitare conflitti e pressioni tramite tecniche tipiche degli hacker malevoli, dall'altro, soprattutto dopo i disastrosi attacchi *WannaCry* e *NotPetya* del 2017 (che hanno dimostrato a tutti come i tradizionali metodi di difesa come i firewall possano essere bypassati e come si possano colpire infrastrutture critiche in più di 150 paesi del mondo, superando il concetto di "perimetro digitale sicuro"), si sono seriamente attivati per difendere i "confini" tecnologici nazionali, dando vita ad agenzie dedicate alla salvaguardia del patrimonio essenziale dello Stato. L'IA in ambito difensivo è dunque oggi utilizzata per coadiuvare l'analista a filtrare le segnalazioni di pericolo che pervengono al C-SOC (*Cyber Security Operations Centre*), non sulla base della storicità degli attacchi e delle tecniche passate (che abbiamo visto evolvere in maniera esponenziale), bensì sulla base di comportamenti umani e tecnologici non standard rilevati su ogni specifica rete (ogni rete si comporta, infatti, in modo diverso, essendo caratterizzata da comportamenti umani e tecnologici non standardizzabili ma estremamente personalizzati). A questo punto l'IA, una volta comprese le "abitudini" standard della rete sarà capace di discernere gli indicatori devianti, segnalando all'operatore solamente le situazioni a rischio e scartando i falsi positivi. Ma chi assicura che un hacker malevolo, ovvero una compagine di hacker malevoli, che in alcuni contesti potrebbero addirittura contare sul "supporto economico" statuale, non riescano a creare una IA dedicata a ingannare le rilevazioni della nostra IA "buona" e, quindi, permettere la penetrazione della rete obiettivo

senza che la stessa venga rilevata, così come accaduto nel 2017 con gli attacchi citati? Effettivamente, se venissero utilizzati massivamente algoritmi di *machine learning*, che migliorano in maniera continua imparando i modi di scrivere, parlare e comportarsi degli umani, per ingannare i moderni sistemi di rilevazione, saremmo di fronte ad un cambiamento importante nelle tecniche di attacco, ovvero attacchi basati di fatto sull'IA: questo è lo scenario che gli esperti cyber di tutto il mondo si aspettano! Nel frattempo, si moltiplica l'impiego di sistemi e di tecnologie basati sull'intelligenza artificiale, molti dei quali hanno tuttavia già iniziato a manifestare vulnerabilità significative.

Un primo esempio di sistemi basati su tecnologie di IA caratterizzati da enormi potenzialità d'uso ma, al contempo esposti a rischi, è dato dai sistemi di videosorveglianza con riconoscimento facciale per fini di contrasto alla criminalità e di supporto al settore giudiziario. Si tratta di sistemi che consentono di identificare o confermare l'identità di una persona a partire dal suo viso. In alcune città italiane (Udine, Torino e Como) sono già stati introdotti simili sistemi, in grado di collegare il volto ripreso ad una banca dati o black-list, ma pure di generare alert in tempo reale in caso di illeciti. Il Garante per la Protezione dei Dati Personali e il Parlamento europeo hanno espresso al riguardo molte riserve: è stato tra l'altro evidenziato che i sistemi di riconoscimento facciale potrebbero essere utilizzati impropriamente e per scopi altri e diversi, rispetto a quelli per cui sono stati installati, il che potrebbe tradursi in compromissioni ingiustificate del diritto alla privacy. Anche per queste ragioni il Garante italiano per la Protezione dei Dati Personali, con un provvedimento del 26 febbraio 2020, ha bloccato il sistema di videosorveglianza con riconoscimento facciale introdotto dal Comune di Como e, con un parere del 25 marzo 2021, si è espresso negativamente riguardo al sistema SARI Real Time proposto dal Ministero dell'Interno, che avrebbe consentito alle telecamere delle forze dell'ordine di confrontare in tempo reale i volti di chiunque fosse passato in determinate aree con un database specifico. Il Parlamento europeo, con la Risoluzione del 6 ottobre 2021 "*L'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziaria in ambito penale*", ha assunto una posizione ancora più nettamente contraria all'uso generalizzato della videosorveglianza biometrica in luoghi e spazi pubblici, considerando invasive queste tecniche di prevenzione e di contrasto del crimine, nella misura in cui esse comportano una serie di rischi potenzialmente elevati, e in alcuni casi inaccettabili, per la protezione dei diritti e delle libertà fondamentali degli individui.

Un'altra interessante applicazione della IA riguarda la giustizia predittiva, che in prima battuta fa riferimento alla possibilità di prevedere l'esito di un procedimento con l'ausilio di algoritmi. In realtà, i sistemi di IA permetterebbero anche di agevolare attività di segreteria e cancelleria negli uffici giudiziari, oltre che velocizzare specifiche attività dei vari operatori del diritto (inclusi magistrati e avvocati), come la redazione di atti, il controllo di atti e documenti, la ricerca legale, finalizzati alla possibilità, cui si è accennato poc'anzi, di prevedere l'esito di una controversia. Negli ultimi anni sono stati avviati in Italia numerosi progetti volti a introdurre l'intelligenza artificiale negli uffici giudiziari, confidando che sistemi così tecnologicamente avanzati (e tendenzialmente esenti da discrezionalità e da errori umani) possano garantire una maggiore applicazione del principio della certezza del diritto ed anche un maggior risparmio in termini di tempi e costi processuali. Si pensi al progetto, cui hanno collaborato a vario titolo anche il Tribunale di Genova e il Tribunale di Pisa, che ha portato allo sviluppo della piattaforma di giustizia predittiva nella Scuola Superiore Sant'Anna di Pisa, basata su una metodologia di raccolta e studio dei casi di giurisprudenza unendo tecniche di *machine learning* e analisi dei *big data*. Un altro interessante progetto è stato promosso dalla Corte d'Appello di Brescia, in collaborazione e con il supporto dell'Università di Brescia, allo scopo, anzitutto, di raccogliere in una banca dati, da cui estrarre poi orientamenti e casistiche,



tutti i provvedimenti emessi, in primo e secondo grado, dal 2018 in settori specifici (principalmente nelle materie assegnate alla competenza della sezione specializzata in materia di impresa e alla sezione lavoro). Interessante, infine, è anche l'accordo-quadro in materia di intelligenza artificiale e giustizia predittiva sottoscritto il 29 settembre 2021 tra il Centro Elettronico di Documentazione della Corte di Cassazione e la Scuola Universitaria Superiore IUSS di Pavia, allo scopo di avviare una collaborazione per la ricerca avanzata in ambito tecnologico per la raccolta e la migliore organizzazione di materiale giuridico digitale (normativa e giurisprudenza).

Anche le applicazioni nell'ambito della *Business Intelligence* destano interesse e curiosità. La *Business Intelligence* (BI) si riferisce alle capacità che consentono alle organizzazioni di prendere decisioni migliori, intraprendere azioni informate e implementare processi aziendali più efficienti, consentendo di:

- raccogliere dati aggiornati;
- presentare i dati in formati di facile comprensione (come tabelle e grafici);
- fornire i dati in modo tempestivo.

Una soluzione di BI è una combinazione di strategia e tecnologia per la raccolta, l'analisi e l'interpretazione dei dati da fonti interne ed esterne, con il risultato finale di fornire informazioni e *analytics* sullo stato passato, presente e futuro del target esaminato. I dati vengono creati a partire da un numero crescente di dispositivi: i dati e la capacità di trarne intuizioni sono la risorsa più preziosa per sostenere e far crescere le aziende. L'utilizzo di un approccio opportunamente selezionato alla BI può aiutare l'organizzazione a ottenere un vantaggio in termini di competitività, riducendo il tempo e gli sforzi necessari per acquisire, integrare, distribuire, esaminare e rispondere ai nuovi dati: la BI rappresenta il cuore di ogni impresa *data-driven*. Le informazioni così ottenute possono essere utilizzate in azienda, ad esempio, per le seguenti attività:

- misurazione dei risultati delle campagne di marketing;

• aumento della visibilità sul flusso di cassa, sui margini lordi e sulle spese operative;
• acquisizione di insight su dipendenti e potenziali clienti per ottimizzare i processi e il recruiting delle risorse umane;
• monitoraggio delle tendenze dei componenti e dei materiali e delle performance dei fornitori;
• previsione del fatturato e delle transazioni;
• ottimizzazione dei livelli di personale del call center e del deposito;
• visualizzazioni interaziendali;
rilevamento di nuovi modelli e nuove opportunità di guadagno;
• screening dei business partner.

Soffermiamoci ora su un nuovo concetto, che trae le basi dalla BI e la integra con la IA: si tratta della *Continuous Intelligence* (CI), ovvero un nuovo modo di intendere gli *analytics*, in cui l'osservazione dei dati in tempo reale si integra con i processi di business in modo diretto, col risultato che diventa possibile supportare le decisioni, o addirittura automatizzarle, al verificarsi di eventi rilevanti. È un approccio innovativo e guidato dall'intelligenza artificiale e dal *machine learning* che permette di raccogliere grandi volumi di dati e di accelerare l'analisi, indipendentemente dal numero e tipo delle fonti e dai loro formati. Si tratta di una metodologia che va oltre l'analisi descrittiva, diagnostica e predittiva, ossia quella che risponde alle classiche questioni "cosa è accaduto" e "cosa accadrà". Esso fornisce indicazioni prescrittive, suggerendo la migliore azione da intraprendere nel contesto dato ("cosa devo fare adesso"). Per questo si applica a situazioni in cui i dati in tempo reale possono migliorare le decisioni aziendali in misura significativa: questo è il concetto di *time sentitive data*. La CI accresce la consapevolezza della situazione in cui il business si sta muovendo (*situation awareness*) e fornisce una visione integrata tra le funzioni aziendali. Non da sottovalutare è la capacità di innescare risposte automatiche, inviando input alle macchine o avviando processi aziendali laddove le decisioni possono essere automatizzate. La *Continuous Intelligence* si basa sull'intelligenza artificiale (AI) e usa il *machine learning* per processare e interpretare un flusso continuo di dati disgregati, scoprire modelli complessi ed estrarre conoscenze preziose che possono essere immediatamente e automaticamente tradotte in azioni. In termini pratici, la *Continuous Intelligence* porta la consapevolezza della situazione in tempo reale e guida le azioni in modo che le persone, i processi e le macchine rispondano più efficacemente agli eventi aziendali importanti nell'esatto momento in cui accadono.

Sono, le precedenti, soltanto alcune delle applicazioni dell'IA nei sistemi e nelle tecnologie che caratterizzano anche la nostra quotidianità. Non si deve tuttavia dimenticare che, anche nel caso di utilizzo di tecnologie di IA, non si può prescindere dal rispetto del fondamentale diritto alla protezione dei dati personali, il che presuppone, tra l'altro, di operare in conformità all'art. 32 GDPR (General Data Protection Regulation, UE Reg. 2016/679): il titolare del trattamento è sempre tenuto a definire, nell'ambito della sua organizzazione, i dati personali trattati, le modalità di trattamento e le relative finalità, nonché le responsabilità e le modalità con cui gestire la protezione dei dati personali secondo i princìpi fondamentali sanciti dal GDPR, oltre che a individuare le procedure tecnico-organizzative e relative modalità di gestione, al fine di garantire un livello di sicurezza per i dati personali adeguato ai rischi. Inoltre, il titolare del trattamento è chiamato a effettuare la valutazione dell'impatto dei trattamenti mediante sistemi di IA sulla protezione dei dati trattati, così da assicurare che il trattamento sia esente da insidie e rischi per gli interessati, quali fughe di dati, violazioni della sicurezza dei dati, accesso non autorizzato ai dati personali. A questo riguardo, uno strumento particolarmente utile per testare l'affidabilità dei sistemi di IA utilizzati può essere ALTAI, acronimo di *Assessment List on Trustworthy Artificial Intelligence*, portale online creato dalla Commissione Europea, che permette a imprese e organizzazioni di auto-effettuare un check di affidabilità dei sistemi di IA.

Le novità sui "Titolari Effettivi": l'attivazione del Registro nazionale ed il B.R.I.S.

di Manlio d'Agostino Panebianco

Introduzione
La costante e continua evoluzione della normativa per la prevenzione ed il contrasto al riciclaggio, autoriciclaggio e finanziamento del terrorismo, sebbene sia fondata prevalentemente sul recepimento di Direttive europee (che a loro volta, fanno proprie alcune conclusioni di Organismi internazionali), non è sempre temporalmente omogenea tra i diversi Paesi; infatti, è possibile notare come, negli anni, le normative nazionali si sono – non solo - diversificate in ragione di specifiche peculiarità territoriali ma, soprattutto, hanno avuto alterne accelerazioni e rallentamenti, creando – in taluni casi – degli inspiegabili disallineamenti.
Un aspetto - direttamente correlato ad un obbligo - riguarda, ad esempio, l'attuazione della disposizione[1] in materia di istitu-

1 Contenuta già nella cosiddetta IV Direttiva, ossia la Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione (Testo rilevante ai fini del SEE).

zione, implementazione e funzionamento del "*Registro dei titolari effettivi*", sia nella parte nazionale che internazionale.
Già, la IV Direttiva Europea in materia Antiriciclaggio, infatti, prevedeva che l'adozione di questo strumento si sviluppasse in due fasi: una prima, per quella locale, ossia legata a ciascun paese membro; ed una seconda, con la interconnessione delle stesse, in una rete di collegamento e interscambio, agevolando così la relativa consultazione di dati relativi a persone fisiche di altra cittadinanza e/o censite in altro Stato membro.
Allo stato attuale, sembra opportuno ricordare come lo scorso 22 marzo 2021, sia entrato in vigore il Regolamento di esecuzione (UE) 2021/369[2], che ha istituito il B.R.I.S. (*Business Registers Interconnection System*), ossia il sistema di interconnessione tra i *Registri nazionali dei titolari effettivi*, che favorisce e consente l'accesso da parte degli Stati membri alle informazioni relative alla titolarità effettiva di ogni singolo Paese.

Il «*Registro nazionale dei titolari effettivi*»

Essenzialmente, il "*Registro*" non è altro che un "*database centralizzato on-line*", dove sono raccolte, accentrate e conservate le informazioni relative alle persone fisiche (qualificabili come "*titolari effettivi*" sulla base degli elementi *infra* descritti), normato in particolar modo dalle modifiche introdotte dal Decreto Legislativo 25 maggio 2017, n. 90 al Decreto Legislativo 21 novembre 2007, n. 231: chiaramente questa modalità e soluzione tecnologica, in prospettiva, può garantire un costante e continuo aggiornamento di questa tipologia di informazioni, favorendo l'accurata verifica e riscontro da parte dei destinatari obbligati[3].
In Italia, la scelta del Legislatore nazionale è stata di non creare un nuovo strumento "*stand-alone*", bensì è previsto che sia una "*sezione, ad accesso riservato*" in seno al Registro delle imprese del sistema delle Camere di Commercio, per ovvie e ragionevoli motivazioni di economicità ed efficienza.
L'alimentazione di questo strumento è legata all'istituito obbligo di comunicazione delle informazioni e dati da parte delle imprese dotate di personalità giuridica tenute all'iscrizione nel Registro delle imprese; delle persone giuridiche private; dei trust produttivi di effetti giuridici rilevanti ai fini fiscali.
Tale scelta sembra opportuna e motivata poiché il Registro delle imprese (al pari dell'anagrafe civile per i residenti) raccoglie già tutti i dati delle imprese, con qualsiasi forma giuridica e settore di attività economica, con sede o unità locali sul territorio nazionale, nonché gli altri soggetti previsti dalla legge. Ne deriva che l'implementazione di una specifica sezione consente in modo efficace non solo di raccordare tutti i dati già presenti con i nuovi ma anche di poter utilizzare la gran parte delle procedure e strutture informatiche di scambio informativo già esistenti.[4]

D'altro canto, la sua consultazione è prevista oltre che per i destinatari della normativa di prevenzione antiriciclaggio, alle *Financial Intelligence Units*[5], anche ad una serie di Autorità ed Istituzioni che hanno un legittimo interesse nel contrasto di quei reati economico finanziari, direttamente correlati e/o presupposto di riciclaggio, autoriciclaggio e finanziamento del terrorismo[6].

Registro dei «titolari effettivi»: entra in funzione nei primi mesi del 2022?

A quanto sembra, il lungo percorso per l'avvio del Registro è giunto – finalmente – al traguardo: infatti, dopo ormai quasi cinque anni, è stato acquisito l'ultimo parere (Consiglio di Stato n. 01835/2021 del 06/12/2021) per la definitiva emanazione e pubblicazione in Gazzetta Ufficiale, e messa in funzione (si spera) già dai primi mesi del 2022.
A tal uopo, sembra opportuno ricordare che il nostro Paese è rimasto uno dei tre (insieme ad Ungheria e Lituania) a non avere ancora un proprio Registro nazionale, dopo che anche Malta e Cipro (che fino a qualche mese fa, erano tra i maggiori ritardatari) ne hanno introdotto uno nei loro ordinamenti.
A questo punto, l'urgenza di dare operatività al "Registro nazionale"[7], non riguarda solo un aspetto di *compliance formale*, ma anche uno di natura *sostanziale* e molto pragmatica: questo ritardo, infatti, non consente al nostro Paese di integrarsi nel B.R.I.S. (precedentemente citato), sia nella

2 Regolamento di esecuzione (UE) 2021/369 della Commissione del 1° marzo 2021 che stabilisce le specifiche tecniche e le procedure necessarie per il sistema di interconnessione dei registri centrali di cui alla direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio.

3 Un punto di forza è che questo Registro metterà tutti i destinatari di accedere alle medesime informazioni, annullando una asimmetria oggi riscontrabile: infatti, alcuni destinatari hanno stipulato costosi contratti di accesso a database per la consultazione di queste informazioni, che spesso hanno una portata limitata al territorio nazionale. D'altro canto, si evidenzia che l'accesso e la consultazione al Registro è a titolo oneroso, e prevedendo il pagamento dei diritti di segreteria, fissati con le modalità di cui all'art. 18 della legge 29 dicembre 1993, n. 580, e successive modificazioni. Per cui, de facto, poco o nulla cambierà per quanti abbiano già in essere i citati contratti, ed al contrario viene introdotto un costo legato all'assolvimento dell'obbligo per tutti gli altri.

4 M. d'Agostino Panebianco, Antiriciclaggio - Vademecum per l'Operatore, Bancaria Editrice, 2020, p. 144.

5 in Italia: la UIF, Unità di Informazione Finanziaria della Banca d'Italia.

6 M. d'Agostino Panebianco, Antiriciclaggio - Vademecum per l'Operatore, Bancaria Editrice, 2020, pp. 146-147: «il d.lgs. n. 231/2007 [...] consente l'accesso ai soggetti obbligati, a supporto dell'assolvimento dei relativi obblighi di Adeguata Verifica della Clientela (previo accreditamento), nonché senza alcuna restrizione al Ministero dell'Economia e delle Finanze, alle Autorità di vigilanza di settore (Banca d'Italia, IVASS, ecc.), alla UIF, alla Direzione Investigativa Antimafia (DIA), alla Guardia di Finanza (che opera, nei casi previsti dal decreto, attraverso il Nucleo Speciale di Polizia Valutaria). A queste si aggiungono la Direzione Nazionale Antimafia e Antiterrorismo (DNAA) e l'Autorità giudiziaria in relazione alle proprie attribuzioni istituzionali. [...] L'accesso è, altresì, consentito alle Autorità preposte al contrasto dell'evasione fiscale, secondo modalità idonee a garantire il perseguimento di tale finalità, stabilite in apposito decreto del Ministro dell'Economia e delle Finanze, di concerto con il Ministro dello Sviluppo Economico».

7 Infatti, in caso di prolungato ritardo, l'Italia potrebbe essere sanzionata.

fase di conferimento che di consultazione delle informazioni. Per completezza ed andando con ordine, sembra opportuno tracciare il lungo percorso, evidenziando gli aspetti salienti nonché le principali difficoltà e perplessità emerse, poiché sono certamente utili a comprendere il contorno e lo spirito di attuazione.

Il primo "atto" specifico - post emanazione del Decreto Legislativo 25 maggio 2017, n. 90 - fu la consultazione pubblica (con scadenza di risposta al 28 febbraio 2020) della bozza di schema di decreto del Ministro dell'economia e delle finanze, di concerto con il Ministro dello sviluppo economico in materia di "*Registro della titolarità effettiva delle imprese dotate di personalità giuridica, delle persone giuridiche private, dei trust e degli istituti e soggetti giuridici affini*", individuando sia i soggetti che le modalità tecniche di accesso, tanto per l'alimentazione quanto per la consultazione, ponendo una particolare enfasi sulle previste scadenze e sulle relative sanzioni. Un interessante aspetto che si evidenzia[8] che il Decreto (nella sua versione ancora non definitiva) è già volto a dare attuazione alla Direttiva UE 2018/843 (c.d. "*V Direttiva Antiriciclaggio*")[9], modificando la Direttiva UE 2015/849 (c.d. "*IV Direttiva Antiriciclaggio*") appena recepita.

In secondo luogo, in conseguenza di una serie di richieste di modifiche e chiarimenti, l'Autorità Garante per la protezione dei dati personali in data 14 gennaio 2021 ha emanato un proprio parere[10] essenzialmente favorevole, poiché nel complesso non presenta specifiche criticità, ed evidenziando in particolar modo, che il previsto termine di *data-retention* di 10 anni rispetta il principio di limitazione della conservazione dei dati[11], nonché la previsione di verifica a cadenza annuale delle medesime informazioni raccolte dal Registro delle Imprese, é rispondente ai principi di esattezza ed aggiornamento[12]. Inoltre, il Garante, valuta come appropriate la previsione di adozione di quelle misure finalizzate a trattare gli eventuali dati "*particolari*"[13] e/o "*giudiziari*", ed in particolare la conservazione separata e l'adozione di specifiche misure tecniche ed organizzative volte ad assicurare accessi selettivi ai dati personali da parte dei soli soggetti autorizzati dalle Camere di commercio a valutare le istanze di accesso da parte del pubblico o di portatori di interessi giuridici rilevanti e differenziati; nonché a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi attraverso l'adozione di tecniche crittografiche. In ultimo, l'Autorità valuta come adeguata la gestione della eventuale segnalazione di difformità da parte di un soggetto obbligato, garantendo l'anonimato del segnalante, fatto salvo per le specifiche previsioni relative all'accesso da parte delle autorità di controllo preposte.

Quindi, il terzo step significativo ha riguardato la valutazione di merito del Consiglio di Stato, che è avvenuta con l'emanazione di due distinti pareri, di cui il primo di natura interlocutoria (n. 428 del 19 marzo 2021, reso nelle adunanze del 23 febbraio 2021 e del 9 marzo 2021) era sostanzialmente *negativo*, avendo evidenziato alcune perplessità e criticità di impostazione, e per cui veniva sospesa l'adozione del parere medesimo, in attesa che il Ministero dell'Economia e delle Finanze potesse fornire delle valutazioni, dei chiarimenti e degli elementi di approfondimento.
Infatti, in questo parere "interlocutorio" il Supremo Consiglio evidenziava - tra gli altri - come indebitamente vi fosse, in generale, una struttura del documento non adeguata, in particolare poiché molte materie non avrebbero dovuto essere ricomprese in un "allegato tecnico" che, a parere dello stesso, avrebbe dovuto essere rivisto integralmente.
Inoltre, nel parere viene evidenziato come emerga «l'inammissibile duplicazione delle norme di rango primario e secondario, in una con la previsione di prescrizioni attuative aggiuntive rispetto a quelle individuate nello schema di decreto, incide quantomeno sulla semplicità e chiarezza, cui dovrebbero mirare le disposizioni, soprattutto se di carattere attuativo; tanto più che i richiami dagli articoli dello schema di decreto all'allegato sono molteplici».
Il Consiglio di Stato entra anche nel merito di una questione prettamente tecnico-giuridica circa la forma espressiva (che in effetti modifica la sostanza nell'esercizio dei diritti e nell'assolvimento degli obblighi) riguardante chi richieda l'accesso (previa verifica dei requisiti) o ne abbia un diritto incondizionato. Tra l'altro, viene altresì evidenziato come il processo sanzionatorio (richiamando espressamente l'art. 2630 codice civile) di quelle imprese che omettessero comunicare entro i termini prestabiliti, dovrebbe essere completato con più chiari riferimenti legislativi in materia di accertamento ed irrogazione di sanzioni, pena la contestabilità dello stesso.

Ultimamente, il Consiglio di Stato, nell'adunanza della Sezione Consultiva per gli Atti Normativi del 23 novembre 2021, alla luce della relazione con la quale il Ministero dell'economia e delle finanze ha trasmesso un nuovo schema di decreto accompagnato da adeguate relazioni, tutte modificate alla luce delle risultanze del

8 Espressamente dichiarato, peraltro, dall'Autorità Garante per la Protezione dei Dati personali.

9 Relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo, è adottato ai sensi dell'articolo 21, comma 5, del decreto legislativo 21 novembre 2007, n. 231, come modificato dai decreti legislativi 25 maggio 2017 n. 90 e 4 ottobre 2019, n. 125.

10 Registro dei provvedimenti n. 2 del 14 gennaio 2021 «Parere su uno schema di decreto del MEF, di concerto con il MISE in materia di comunicazione, accesso e consultazione dei dati e delle informazioni relativi alla titolarità effettiva di imprese dotate di personalità giuridica, di persone giuridiche private, di trust produttivi di effetti giuridici rilevanti ai fini fiscali e di istituti giuridici affini al trust».

11 Di cui all'articolo 5, par. 1, lett. e), del Regolamento UE n.679/2016, meglio noto come GDPR.

12 Di cui all'articolo 5, par. 1, lett. d), del GDPR.

13 In precedenza, prima dell'entrata in vigore del Regolamento, erano definiti dalla normativa italiana, i "dati sensibili".

precedente parere interlocutorio di marzo 2021, ha sintetizzato la propria nuova posizione nel parere n.01835/2021 del 06/12/2021.
Rispetto a quest'ultimo, la prima considerazione riguarda l'ancora attuale validità dell'unico parere del Garante per la protezione dei dati personali, considerando che le innovazioni apportate al Decreto non hanno uno specifico impatto in materia, salvo la puntuale precisazione di limitare il trattamento, nel rispetto dei principi di necessità e minimizzazione.
La seconda è, di ampia e generale portata, ed evidenzia come «lo schema modificato, come suffragato dalle esplicazioni nelle relazioni, ha consentito il superamento di ogni profilo di criticità direttamente incidente sul rispetto delle disposizioni legislative attuative delle direttive comunitarie».
Inoltre, le precedenti incertezze interpretative in merito alla identificazione della seconda categoria di soggetti che possono accedere al Registro, sono oramai «superate dall'attuale utilizzo della più esaustiva formula "qualunque persona fisica o giuridica, ivi compresa quella portatrice di interessi diffusi"», e l'Amministrazione, con il nuovo schema di regolamento si è adeguata, proponendo una riformulazione idonea a chiarire i dubbi interpretativi segnalati nella sede interlocutoria.
Oltre ad una serie di raccomandazioni - che hanno di certo rilevanza ed importanza – sono ormai di minore portata e non di certo ostative, e sembra chiaro ed evidente che - a questo punto – il legislatore italiano sia finalmente nella condizione di dare finalmente avvio al Registro Nazionale nei prossimi mesi, invitando le imprese, i trust ed i soggetti aventi personalità giuridica ad effettuare le relative comunicazioni dei propri titolari effettivi, così da consentire nella successiva immediatezza, ai soggetti destinatari degli obblighi antiriciclaggio di poter accedere al database, e confrontare quanto da loro raccolto direttamente dal cliente, con le informazioni centralizzate.

L'obbligo di "individuazione" del *titolare effettivo*

Il quadro sinottico relativo all'entrata in vigore delle nuove disposizioni, non può non essere completato: per tale ragione, sembra opportuno, sintetizzare i cardini dell'adempimento a carico dei destinatari del Decreto Legislativo 21 novembre 2007, n.231 modificato negli anni.
In seno all'Adeguata Verifica della Clientela, uno dei principali obblighi è quello della individuazione del *beneficial owner*, ossia «*la persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l'operazione è eseguita*»[14].
Il primo aspetto - che opportunamente va evidenziato – è che la vigente normativa, esplicita come nel caso di "*cliente diverso da persona fisica*" è sempre da individuare uno o più titolari effettivi, sulla base dei criteri pubblicati, e che il Decreto declini[15] tale obbligo con riferimento a "*persone giuridiche, trust e altri istituti e soggetti giuridici affini*", attraverso un idoneo "approccio basato sul rischio".
In secondo luogo, sempre la vigente normativa[16], in tal senso, fornisce i criteri per la determinazione della titolarità effettiva di clienti diversi dalle persone fisiche, suddividendoli essenzialmente tra: a) società di capitali; b) fondazioni; c) trust; d) altre *persone giuridiche private*.
Inoltre, sembra opportuno sottolineare - proprio per agevolare l'adempimento in un contesto di *compliance formale* e *sostanziale* - come a differenza dell'obbligo di identificazione della persona fisica che chiede di instaurare il rapporto continuativo (ovvero la singola operazione o prestazione professionale), per quanto attiene il titolare effettivo sarebbe più opportuno riferirsi al *processo di loro individuazione*[17], attraverso la raccolta di informazioni, dichiarazioni e documenti ottenute dal cliente, riscontrate e verificate con fonti attendibili. Tra queste ultime, la principale è di certo il "*Registro dei titolari effettivi*".

14 Definizione di cui all'art. 1 del Decreto Legislativo 21 novembre 2007, n. 231, aggiornato a seguito delle modifiche introdotte dal Decreto Legislativo 25 maggio 2017, n. 90.

15 Si vedano articoli 18 e seguenti.

16 Si vedano sia in generale l'articolo 20 del Decreto, ma anche il Provvedimento di Banca d'Italia in materia di Adeguata Verifica della Clientela del 30 luglio 2019.

17 M. d'Agostino Panebianco, Antiriciclaggio - Vademecum per l'Operatore, Bancaria Editrice, 2020, p.135: «In primo luogo, occorre evidenziare come anche il Provvedimento di Banca d'Italia sull'Adeguata Verifica della Clientela confermi la precedente interpretazione secondo cui l'identificazione del titolare effettivo possa avvenire anche senza che sia necessaria la sua presenza fisica (pur contestualmente all'identificazione del cliente), sulla base dei dati identificativi da questo forniti, in conseguenza di una richiesta dell'intermediario. Seguendo tale indicazione espressa ed esplicita, il termine "identificazione" viene utilizzato lato sensu: per la coesistenza delle due condizioni poste (la non necessaria presenza della persona fisica e l'ottenimento delle informazioni da parte del cliente) sarebbe più opportuno parlare di "individuazione" (piuttosto che di identificazione, stricto sensu)».

Note a margine della recente sentenza della corte di giustizia dell'Unione Europea in tema di avvalimento

di Giulia Sulpizi

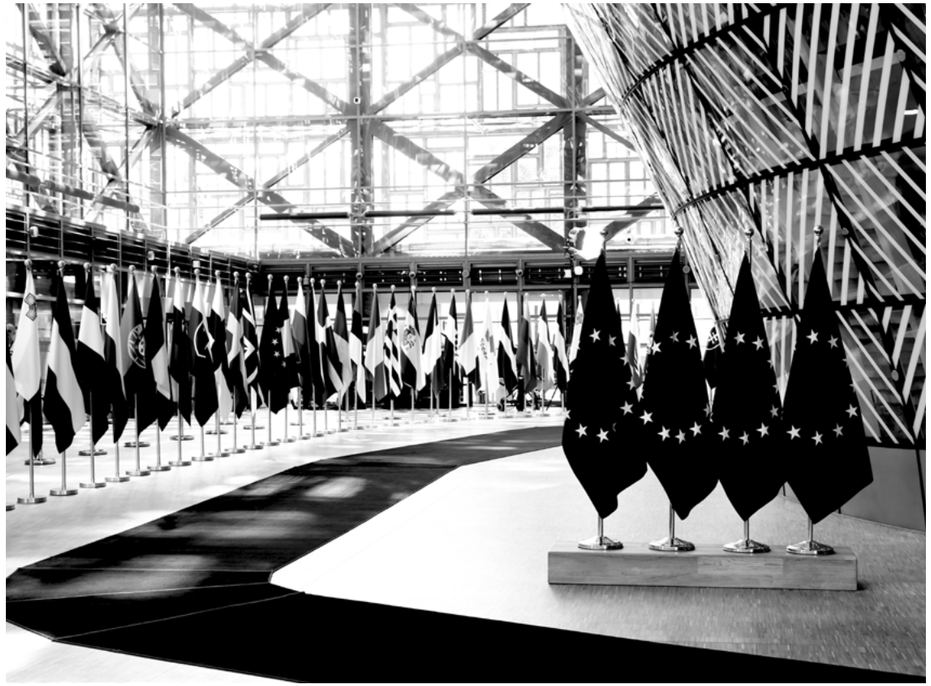
Premessa: la normativa del Codice degli appalti e del diritto comunitario

Nell'ambito dei rapporti tra privati e pubbliche amministrazioni è intervenuta, di recente, la Corte di giustizia dell'Unione europea con un'importante pronuncia.
Per comprendere il caso sottoposto all'attenzione del giudice comunitario è necessario, innanzitutto, indagare il contenuto dell'art. 89, 1° co., d.lgs. n. 50/2016. Questa disposizione si occupa dell'ipotesi del c.d. avvalimento, fattispecie di derivazione comunitaria che permette al concorrente di partecipare anche alle procedure ad evidenza pubblica per le quali non possiede tutti i requisiti di capacità economico-finanziaria e tecnico-professionale previsti dal bando di gara, assicurando la possibilità di avvalersi di altri soggetti che possiedono tali requisiti. La norma in questione, infatti, statuisce che "*L'operatore economico, singolo o in raggruppamento (...), per un determinato appalto, può soddisfare la richiesta relativa al possesso dei requisiti di carattere economico, finanziario, tecnico e professionale (...) necessari per partecipare ad una procedura di gara (...) avvalendosi delle capacità di altri soggetti, anche partecipanti al raggruppamento, a prescindere dalla natura giuridica dei suoi legami con questi ultimi. (...) Nel caso di dichiarazioni mendaci, ferma restando l'applicazione dell'articolo 80, comma 12, nei confronti dei sottoscrittori, la stazione appaltante esclude il concorrente e escute la garanzia*".
In particolare, ciò che rileva primariamente attiene alla presentazione di "*documentazione o dichiarazioni non veritiere*" da parte degli operatori economici, ipotesi sanzionata dal combinato disposto degli artt. 80, 5° co., lett. f-*bis*) e 80, 12° co., d.lgs. n. 50/2016 con l'esclusione dell'operatore economico.
L'importanza della succitata normativa è ben testimoniata nel nostro ordinamento dall'ampio ricorso da parte dei privati all'istituto in esame. La sua *ratio* si identifica nella volontà di ampliare la platea dei possibili contraenti della pubblica amministrazione, obiettivo che, però, deve essere bilanciato con l'esigenza di garantire alla stazione appaltante un aggiudicatario affidabile. Esso trova la sua scaturigine in Corte giust., Sez. V, Sent. 14 aprile 1994, C-389/92, laddove la Corte di giustizia ha

stabilito che una holding potesse dimostrare la sussistenza dei requisiti di qualificazione tramite una società del suo gruppo di appartenenza. È, poi, intervenuto il legislatore europeo attraverso, da ultimo, la Direttiva 2014/24.
Nel caso sottoposto all'attenzione della Corte di giustizia rilevano, dunque, le norme del d.lgs. n. 50/2016 (il Codice degli appalti) e l'art. 63 della Direttiva del 2014 il quale, nell'ipotesi di avvalimento, al paragrafo 1, 2° co. prevede che, in caso di false dichiarazioni o di mendaci dichiarazioni, "*l'amministrazione aggiudicatrice impone che l'operatore economico sostituisca un soggetto che non soddisfa un pertinente criterio di selezione o per il quale sussistono motivi obbligatori di esclusione. L'amministrazione aggiudicatrice può imporre o essere obbligata dallo Stato membro a imporre che l'operatore economico sostituisca un soggetto per il quale sussistono motivi non obbligatori di esclusione*".
Tale norma ha il chiaro intento di non sanzionare con l'automatica esclusione quegli operatori economici che non presentino alcuni dei requisiti richiesti, al fine di ampliare il più possibile la platea dei concorrenti alle procedure ad evidenza pubblica.

La giurisprudenza amministrativa nazionale sul tema delle omesse, reticenti e false dichiarazioni da parte degli operatori economici e nei casi di avvalimento

Per comprendere il rapporto sussistente tra il diritto interno e comunitario è opportuno, in primo luogo, delineare la portata applicativa dell'art. 80 d.lgs. n. 50/2016 e della disciplina sanzionatoria ivi prevista ricorrendo alle più importanti e recenti pronunce della giurisprudenza amministrativa sul punto.
In particolare, si può, in questa sede, segnalare quanto sostenuto dal T.A.R. Sicilia, Catania, con sent. n. 693/2020. Qui è stata ripresa una celebre distinzione tra omessa, reticente e falsa dichiarazione. La prima si ha quando "*l'operatore economico non riferisce di alcuna pregressa condotta professionale qualificabile come 'grave illecito professionale'*"; la seconda quando "*le pregresse vicende sono solo accennate senza la dettagliata descrizione necessaria alla stazione appaltante per poter compiutamente apprezzarne il disvalore nell'ottica dell'affidabilità del concorrente*"; la terza, infine, quando "*l'operatore rappresenta una circostanza di fatto diversa dal vero*".
Questa tripartizione appare centrale sul



piano degli effetti giuridici che ne conseguono. È, infatti, lo stesso T.A.R. a precisare, riprendendo un consolidato orientamento del Consiglio di Stato[1], che "*solo alla condotta che integra una falsa dichiarazione consegue l'automatica esclusione dalla procedura di gara poiché depone in maniera inequivocabile nel senso dell'inaffidabilità e della non integrità dell'operatore economico, mentre ogni altra condotta, omissiva o reticente che sia, comporta l'esclusione dalla procedura solo per via di un apprezzamento da parte della stazione appaltante che sia prognosi sfavorevole sull'affidabilità dello stesso*".

La sopraccitata differenziazione non è stata, però, considerata come esaustiva dalla giurisprudenza amministrativa nazionale. Ciò ha comportato la rimessione all'Adunanza Plenaria del Consiglio di Stato della questione relativa alla consistenza, alla perimetrazione e agli effetti degli obblighi dichiarativi gravanti sugli operatori economici in sede di partecipazione alla procedura evidenziale, con particolare riguardo ai presupposti per l'imputazione della falsità dichiarativa di cui all'art. 80 d.lgs. n. 50/2016. Tale è stato l'oggetto dell'ordinanza n. 2332 della Sez. V del Consiglio di Stato del 2020.

Partendo, infatti, dalla considerazione che "*le irregolarità di carattere dichiarativo sono normalmente definite nel quadro delle 'situazioni' concretanti 'gravi illeciti professionali', idonei, come tali, a 'rendere dubbia' l''integrità' e l''affidabilità' del concorrente*" si può comprendere il generale obbligo, in capo ad ogni operatore economico, di fornire alla stazione appaltante ogni dato o informazione rilevante perché quest'ultima possa acquisire e valutare tutte le circostanze e gli elementi determinanti ai fini dell'ammissione al confronto competitivo.

Tale impostazione è giustificata dalla logica relazionale del c.d. "*contatto sociale qualificato*", che sorge in conseguenza della partecipazione alla procedura ad evidenza pubblica, di cui al combinato disposto degli artt. 1337 e 1338 c.c., il quale impone un vero e proprio dovere di chiarezza e di correttezza informativa. In tale contesto, marcatamente pubblicistico, ciò si traduce nell'obbligo – espressione del "*principio di correttezza*" di cui all'art. 30 d.lgs. n. 50/2016 – di professionalità imposto agli operatori economici. Quest'obbligo è, in ogni caso, di natura strumentale, essendo "*finalizzato (...) a mettere in condizione la stazione appaltante di conoscere tutte le circostanze rilevanti per l'apprezzamento dei requisiti di moralità e meritevolezza soggettiva*".

La pronuncia in esame (l'ordinanza n. 2332) sostiene, però, che non a caso il legislatore nazionale è intervenuto su questa previsione. Quest'ultima, infatti, introduce uno specifico, legittimo e autonomo motivo di esclusione, come testimonia il d.l. n. 135/2018, convertito dalla l. n. 12/2019. Da ciò discende la "*sua attitudine a concretare, in sé, una forma di grave illecito professionale*". Queste considerazioni hanno importanti ripercussioni sul piano giuridico: "*il necessario nesso di strumentalità rispetto alle valutazioni rimesse alla stazione appaltante finisce per dislocarsi dal piano del concreto apprezzamento delle circostanze di fatto (...) al piano astratto di una illiceità meramente formale e presunta, operante de jure*".

Il giudice amministrativo enuncia, dunque, la necessità di una puntuale perimetrazione della portata dei suddetti obblighi informativi, in relazione ai quali si bilanciano, necessariamente, opposti interessi. Da una parte, infatti, si afferma la doverosità dell'estromissione dalla gara dei soggetti non affidabili sotto il profilo dell'integrità morale, della correttezza professionale, della credibilità imprenditoriale e della lealtà operativa. Dall'altra, non si può dimenticare l'esigenza di non indebolire la garanzia della massima partecipazione alla gara e di non compromettere la necessaria certezza sulle regole di condotta imposte agli operatori economici, presidiate dai principi di tipicità e tassatività.

Il problema della delimitazione dell'alveo applicativo dell'art. 80 d.lgs. n. 50/2016 – e della sanzione che da esso consegue – investe, in particolare, le c.d. "omissioni dichiarative", le dichiarazioni reticenti. Con riferimento a queste ultime, infatti, bisogna distinguere tra il mero – e non rilevante – "*nihil dicere*" dal "*non dicere quod debetur*". Quest'ultimo soltanto postula una violazione di un dovere giuridico di parlare e giustifica di per sé – in quanto illecito professionale in sé considerato – l'operatività, in chiave sanzionatoria, della misura espulsiva. Il contegno censurabile consiste, appunto, nella lesione – potenziale o effettiva – dell'integrità e dell'affidabilità dell'operatore economico.

In questa prospettiva, dunque, "*gli obblighi informativi decampano dalla logica della mera strumentalità, diventando obblighi finali, dotati di autonoma rilevanza*". Di conseguenza, "*l'omissione, la reticenza, l'incompletezza divengono – insieme alle più gravi decettività e falsità – forme in certo senso sintomatiche di grave illecito professionale in sé e per sé*".

Seguendo, quindi, tale opzione ricostruttiva, l'interpretazione assegnata all'art. 80 del Codice degli appalti ha assunto il contorno di una vera e propria norma di chiusura, "*che impone agli operatori economici di portare a conoscenza della stazione appaltante tutte le informazioni relative alle proprie vicende professionali, anche non costituenti cause tipizzate di esclusione*".

Ciò ha messo in luce, però, la necessità di individuare un generale limite di operatività a tale disposizione, il cui contenuto risulterebbe, altrimenti, eccessivamente oneroso per i privati "*imponendo loro di ripercorrere a beneficio della stazione appaltante vicende professionali ampiamente datate o (...) del tutto insignificanti nel contesto della vita professionale di un'impresa*".

Non è un caso, dunque, che sia maturata – nella giurisprudenza più recente – una diversa prospettiva, che verte sulla distinzione tra due fattispecie. In un caso, infatti, si tratterà dell'ipotesi dell'omissione delle informazioni dovute ai fini del corretto svolgimento della procedura di selezione, che comprende anche la reticenza. In un altro caso, invece, si configurerà l'ipotesi di falsità delle dichiarazioni, ovvero la presentazione, nella procedura di gara in corso, di dichiarazioni non veritiere, rappresentative di una circostanza in fatto diversa dal vero cui conseguirebbe l'automatica esclusione dalla procedura di gara.

Questa ricostruzione è foriera di diverse conseguenze sul piano normativo ed operativo. Mentre le ipotesi di dichiarazioni omesse, reticenti e fuorvianti hanno rilie-

1 *Cons. Stato, Sez. V, sent. n. 5171/2019.*

vo solo in quanto si manifestino nel corso della procedura, la falsità è più gravemente sanzionata, determinando, non a caso, l'obbligo di segnalazione all'ANAC e della possibile iscrizione destinata ad operare anche nelle successive procedure evidenziali, nei limiti del biennio.

Alla luce di queste considerazioni si può arrivare ad affermare che solo la falsità – sia essa informativa, documentale o dichiarativa – presenta un'attitudine espulsiva automatica e potenzialmente ultrattiva. Al contrario, le informazioni semplicemente fuorvianti giustificano solo l'estromissione dalla procedura nella quale si collocano.

In conclusione, ad avviso del Consiglio di Stato, la falsità e la manipolazione fuorviante sarebbero, di per sé, dimostrative di "*pregiudiziale inaffidabilità*", mentre l'omissione e la reticenza informativa sarebbero insuscettibili di legittimare l'automatica esclusione dalla gara, "*dovendo sempre e comunque rimettersi all'apprezzamento di rilevanza della stazione appaltante, ai fini della formulazione di prognosi in concreto sfavorevole sull'affidabilità del concorrente*".

I giudici di Palazzo Spada sostengono, infatti, al termine del loro *iter* logico-argomentativo, che la falsità delle dichiarazioni "*costituisce frutto del mero apprezzamento di un dato di realtà, cioè di una situazione fattuale per la quale possa alternativamente porsi l'alternativa logica vero/falso, accertabile automaticamente*", mentre la semplice mancanza delle stesse "*non potrebbe essere apprezzata in quanto tale, dovendo essere (...) valutate le circostanze taciute, nella prospettiva della loro idoneità a dimostrare l'inaffidabilità del concorrente*".

In forza di questi ragionamenti, è stata chiamata a pronunciarsi l'Adunanza Plenaria, che si è espressa, infine, con sentenza n. 16/2020.

In questa sede, il giudice amministrativo ha assunto un diverso punto di vista, ripercorrendo la distinzione tra omesse e false dichiarazioni, ma giungendo ad approdi differenti rispetto alla Sez. V, da cui era scaturita l'ordinanza di rimessione predetta.

In tale pronuncia la Plenaria ha sottolineato che l'esclusione per omissioni dichiarative del concorrente in relazione a reati c.d. "*non ostativi*" non può mai essere automatica. Parifica, infatti, le ipotesi di omissione e di falsità delle informazioni, laddove quest'ultima, sanzionata dall'art. 80 d.lgs. n. 50/2016, non è soggetta ad un automatismo espulsivo, necessitando sempre di una valutazione di integrità e affidabilità del concorrente. Si argomenta, infatti, che tanto "*il fornire, anche per negligenza, informazioni false o fuorvianti suscettibili di influenzare le decisioni sull'esclusione, la selezione o l'aggiudicazione*", quanto "*l'omettere le informazioni dovute ai fini del corretto svolgimento della procedura di selezione*" sono qualificabili come "*gravi illeciti professionali*", in grado di incidere sulla "*integrità o affidabilità*" dell'operatore economico, le quali necessitano, in ogni caso, di una valutazione in concreto da parte della stazione appaltante.

Alla luce, quindi, di questi recenti e fondamentali approdi giurisprudenziali si deve, ora, passare all'analisi del disposto dell'art. 89 d.lgs. n. 50/2016, che, in tema di avvalimento, richiama l'art. 80, richiedendo che anche l'impresa ausiliatrice dimostri di essere in possesso dei requisiti prescritti dalla normativa del Codice degli appalti. Anche in questo caso si sanziona la mancanza di questi elementi con l'esclusione automatica dell'operatore economico ausiliato dalla gara.

Anche questa disposizione è stata presa in esame dal Consiglio di Stato con un'ordinanza di rimessione[2], questa volta indirizzata alla Corte di giustizia dell'Unione europea. Appare, infatti, in questo caso centrale il richiamo alla disciplina comunitaria.

Occorre, ad ogni buon conto, premettere che il giudice nazionale si è pronunciato su una gara bandita nel gennaio 2018, quando l'art. 80 del Codice degli appalti era applicabile nella sua formulazione antecedente al d.l. n. 135/2018 e ancora non si era espressa l'Adunanza Plenaria del Consiglio di Stato con la pronuncia n. 16/2020. Muovendo, dunque, da tale cornice normativa e giurisprudenziale, il Consiglio di Stato ha ritenuto astrattamente applicabile la norma ad un caso in cui l'ausiliaria aveva

2 *Cons. Stato, Sez. III, ord. n. 2005/2020.*

omesso di dichiarare una sentenza di patteggiamento a carico del titolare dell'impresa, giudicato responsabile di lesioni colpose commesse con violazione delle norme in materia di salute e sicurezza sul lavoro. In particolare, si è affermato che, sulla base della normativa nazionale, "*la dichiarazione non veritiera resa dal rappresentante legale dell'impresa ausiliaria in gara comporta, quale conseguenza automatica, il dovere della stazione appaltante di escludere il concorrente ausiliato, senza possibilità di provvedere alla sostituzione dell'impresa*".

In caso, dunque, di dichiarazione mendace, dovrebbe ritenersi preclusa la facoltà di sostituzione dell'ausiliaria ammessa dall'art. 89, 3° co., d.lgs. n. 50/2016, applicabile ad altre ipotesi. Tale regime potrebbe essere giustificato "*dalla esigenza di sanzionare coloro che si sono resi responsabili di dichiarazioni mendaci, o dolosamente reticenti, responsabilizzando l'operatore economico in ordine alla genuinità delle attestazioni compiute dall'impresa ausiliaria*".

Questa soluzione, sebbene risulti rispondente sia alla normativa nazionale che all'orientamento giurisprudenziale consolidato sul punto, è stata, però, ritenuta di dubbia compatibilità con l'ordinamento comunitario.

A tal proposito, si è argomentato che il diritto dell'Unione europea nulla dispone riguardo all'ipotesi di esclusione del concorrente a seguito di dichiarazioni mendaci da parte dell'ausiliaria ed è stata sottolineata la centralità del disposto dell'art. 63 della Direttiva 2014/24, che, in una prospettiva pro-concorrenziale, impone solamente la sostituzione dell'impresa ausiliaria.

Alla luce di tali prospettazioni, la causa di esclusione di cui all'art. 89 d.lgs. n. 50/2016, da una parte, contrasterebbe con

la norma sovranazionale, introducendo un automatismo espulsivo non contemplato dalla direttiva UE, che persegue opposte finalità e, dall'altra, appare inconciliabile con il principio per cui il concorrente ausiliato, "*non disponendo di speciali poteri di verifica circa l'attendibilità delle credenziali della controparte, non può che affidarsi alle dichiarazioni o alla documentazione da quest'ultima fornitegli*", con il corollario che "*all'operatore concorrente non può richiedersi una diligenza maggiore di quella richiesta ad un comune operatore negoziale*"[3].
Sulla scorta di tali argomenti, il Consiglio di Stato ha, quindi, rimesso alla Corte di giustizia il quesito interpretativo inerente al rapporto tra l'art. 63 della Direttiva 2014/24 e le disposizioni del Codice degli appalti.

3 *Cons. Stato, Sez. V, sent. n. 69/ 2019.*

4 *Corte giust., Sez. IX, Sent. 3 giugno 2021, C-210/20.*

La pronuncia della Corte di giustizia dell'Unione europea: il combinato disposto degli artt. 80 e 89 d.lgs. n. 50/2016 in relazione alla Direttiva 24/2014

Ad avviso del giudice comunitario[4], dalla formulazione dell'art. 63 della Direttiva 2014/24 emergerebbe che, per le sole ipotesi in cui ricorrano in capo all'ausiliaria motivi di esclusione non obbligatori, agli Stati membri è consentito di rendere l'obbligo di sostituzione – prescritto per tutte per le cause di esclusione obbligatoria – una facoltà, ma non possono, in ogni caso, privare le amministrazioni aggiudicatrici della possibilità di esigere, di propria iniziativa, tale sostituzione.
Quest'opzione interpretativa, oltre ad essere conforme al dato testuale della disposizione, è volta ad assicurare, altresì, il rispetto del principio di proporzionalità, esprimendo in specie il divieto di c.d. *gold plating*[5].
La Corte ha, poi, condotto un'analisi sistematica della disciplina contenuta nella Direttiva 2014/24, definendo anche le modalità di esercizio del potere di valutazione da parte delle amministrazioni aggiudicatrici nelle ipotesi in cui sussistano in capo all'ausiliaria motivi di esclusione.
Partendo dalla considerazione preliminare che l'obiettivo del diritto europeo degli appalti pubblici è quello di "*consentire all'amministrazione aggiudicatrice di garantire l'integrità e l'affidabilità di ciascuno degli offerenti e, di conseguenza, la mancata cessazione del rapporto di fiducia con l'operatore economico interessato*", la normativa comunitaria consente agli operatori economici, che si trovino in situazioni ostative alla partecipazione alle gare pubbliche, di dimostrare di aver adottato misure idonee a comprovare la propria affidabilità, nonostante l'esistenza di motivi di esclusione.
In tal senso dispongono il Considerando n. 102 della Direttiva, laddove si evidenzia l'opportunità di riconoscere agli operatori economici la possibilità di "*adottare misure per garantire l'osservanza degli obblighi a porre rimedio alle conseguenze di reati o violazioni e a impedire efficacemente che tali comportamenti scorretti si verifichino di nuovo*", e l'art. 57 della Direttiva stessa, che prevede l'applicazione di tale facoltà sia al ricorrere di motivi di esclusione obbligatori, sia in presenza di quelli facoltativi. Si tratta del c.d. principio di *self cleaning,* che trova una sua corrispondenza, a livello interno, nell'art. 80, comma 7, d.lgs. n. 50/2016, alla luce del quale l'operatore non viene escluso se è in grado di provare che ha adottato misure riabilitative sufficienti e adeguate a dimostrare la sua affidabilità.
La Corte giunge, quindi, ad estendere le regole di cui *supra* anche ai casi di avvalimento. L'amministrazione aggiudicatrice, dunque, ancor prima di esigerne la sostituzione da parte dell'offerente, dovrebbe far presentare all'ausiliaria (o all'offerente medesimo) le misure correttive che la stessa ha adottato al fine di rimediare alle irregolarità contestate e, solo in subordine, farla sostituire. Tale regola opera, ad avviso del giudice comunitario, anche in presenza di sentenze definitive.
Queste considerazioni si radicano, inoltre, sul rispetto del principio di proporzionalità. Qualora, infatti, l'esclusione colpisca l'offerente per una violazione imputabile al soggetto sulle cui capacità l'amministrazione intenda fare affidamento e nei confronti del quale non disponga di alcun potere di controllo, la stessa p.a. deve prestare attenzione all'applicazione dei motivi di esclusione ed effettuare una valutazione specifica e concreta dell'atteggiamento del soggetto interessato, tenendo conto dei mezzi di cui quest'ultimo dispone per verificare l'esistenza di una violazione in capo all'impresa ausiliaria.
In attuazione, poi, dei principi di trasparenza e parità di trattamento, l'amministrazione aggiudicatrice deve assicurarsi che la sostituzione dell'ausiliaria non conduca ad una modifica sostanziale dell'offerta iniziale presentata in gara.
Alla luce di tali prospettazioni, i giudici europei hanno conclusivamente affermato che "*l'articolo 63 (...) in combinato disposto con l'articolo 57 (...) e alla luce del principio di proporzionalità, deve essere interpretato nel senso che esso osta a una normativa nazionale in forza della quale l'amministrazione aggiudicatrice deve automaticamente escludere un offerente da una procedura di aggiudicazione di un appalto pubblico qualora un'impresa ausiliaria, sulle cui capacità esso intende fare affidamento, abbia reso una dichiarazione non veritiera quanto all'esistenza di condanne penali passate in giudicato, senza poter imporre o quantomeno permettere, in siffatta ipotesi, a tale offerente di sostituire detto soggetto*".

Conclusioni

La soluzione prospettata dalla Corte di giustizia appare di particolare rilievo per diverse ragioni.

5 *Tale divieto "comporta che non si possano stabilire oneri a carico degli operatori economici ulteriori rispetto a quelli previsti dalle direttive europee": così, la Segnalazione del Prof. Avv. Enrico Michetti della sentenza del Consiglio di Stato Sez. III del 19.1.2018 del 21.01.2018.*

In primo luogo, essa risulta coerente con la *ratio* della disciplina europea dei contratti pubblici, basata sulla volontà di garantire ai privati il più ampio accesso possibile alle gare e di assicurare ai medesimi condizioni di parità e trasparenza nello svolgimento delle procedure di aggiudicazione. Per questa ragione il giudice europeo è arrivato a censurare la normativa nazionale: quest'ultima, infatti, è stata ritenuta eccessivamente restrittiva, ricollegando conseguenze fortemente diversificate a fattispecie che, in forza della loro natura e della comune disciplina di matrice comunitaria, dovrebbero essere trattate in modo analogo.

La sanzione, poi, dell'esclusione automatica, prevista dall'art. 89 sopraccitato, non risulta idonea a consentire la realizzazione delle finalità perseguite dal Codice degli appalti di selezionare operatori economici affidabili, comportando, al contrario, il rischio che vengano estromessi dal mercato soggetti virtuosi per fatti ad essi non imputabili.

L'applicazione di questa disposizione non permette, inoltre, alle imprese di prevedere con sufficiente certezza se la propria partecipazione alle procedure ad evidenza pubblica sarà considerata ammissibile, potendo le stesse essere escluse in maniera automatica anche per violazioni riconducibili ad altri soggetti, non sottoposti al loro controllo. Tale meccanismo pregiudica, tra l'altro, in particolar modo le piccole e medie imprese, che si ritrovano più di frequente costrette a ricorrere all'istituto dell'avvalimento.

La volontà della Corte di giustizia, dunque, è volta ad attribuire maggiore discrezionalità e capacità di scelta alle stazioni appaltanti in merito alle modalità di selezione dei contraenti, adottando un approccio che tenga in considerazione le specificità delle singole fattispecie concrete invece di ricorrere ad automatismi normativi.

La recente pronuncia, in definitiva, costituisce un importante approdo giurisprudenziale e, altresì, un centrale punto di partenza per il legislatore italiano. Quest'ultimo, infatti, dovrà tenere conto delle indicazioni rese a livello comunitario nell'ambito della generale riforma della disciplina dei contratti pubblici. Riforma che, si auspica, dovrebbe incoraggiare sempre più una vera e propria apertura da parte delle pubbliche amministrazioni nei confronti dei privati.

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