ISSN 2784-8213

Aprile 2023 – n. 04 Anno III – Mensile

COMPLIANCE

La compliance secondo Barilla

La compliance al diritto dell'Unione Europea

SEAC

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

SEAC

Passione per semplificare le cose

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

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

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

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

Direttore responsabile:
Giovanni Bort
Product Manager:
Giuliano Testi e Tullio Zanin
Responsabili scientifici:
Ivano Maccani e Denise Boriero.
Redazione: Alessandro Butticé,
Alessandro De Carlo, Luigi Fruscione,
Mario Bertolissi, Matteo Macilotti,
Pierpaolo Rossi
Coordinatori di redazione:
Maria Chiara Volpi e Mattia Guadagnini
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

Indice

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 il Centro di Scienze della Sicurezza e della Criminalità dell'Università degli Studi di Trento e di Verona. Si occupa di *security e safety*, nonché di *compliance aziendale*.

Alessandro Butticé: giornalista, Generale di Brigata (c.a.) della Guardia di Finanza, capo unità emerito della Commissione Europea, già portavoce dell'Ufficio Europeo per la lotta alla Frode (OLAF) e creatore della Rete dei Comunicatori Anti-Frode dell'OLAF. Laureato in Giurisprudenza, Economia e commercio, Scienze della sicurezza economico-finanziaria. Specializzato in Giornalismo e comunicazioni di Massa. (le opinioni espresse sono a titolo prettamente personale, e non rappresentano necessariamente le posizioni ufficiali delle Istituzioni dell'Ue).

Ernesto Cotugno: Ispettore della Guardia di Finanza, Computer Forensic & Data Analysis Digital Evidence Specialist, Investigatore Economico Finanziario, Esperto d'Area – PNRR, GDPR nella PA, autore per IISFA, Docente First Responder e Digital Forensic, Relatore Istituzioni Scolastiche Cyberbullismo e Sicurezza delle Informazioni.

Ilaria De Vito: Maresciallo Capo della Guardia di Finanza – Psicologa iscritta all'Albo A dell'Ordine degli Psicologi dell'Emilia Romagna. Laureata in Psicologia Clinica e in Scienze della Comunicazione. Ha conseguito un Master di I Livello in: "L'insegnamento delle materie filosofiche ed umanistiche negli Istituti secondari di II grado" presso l'Università telematica e-campus ed un Master di II Livello in: "Psicologo di Base e Counselling Sanitario" presso l'Università Cattolica del Sacro Cuore di Roma.

Luca Faiella: Luogotenente della Guardia di Finanza - Specializzazione di "Verificatore Fiscale".

Matteo Faiella: Avvocato nel Foro di Milano, si occupa principalmente di contenzioso tributario, anche stragiudiziale e consulenza in materia fiscale presso Studio Associato dei Dottori Moroni di Milano

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 nel Foro di Verona, esperta in modelli conformi al Regolamento UE 2016/679 e ex D. Lgs. 231/2001, presidente di vari organismi di vigilanza e DPO/RPD.

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

Federico Fuga: laureato in Ingegneria Elettronica a Padova nel 2000 e dal 2004 ingegnere libero professionista. Si occupa di sviluppo di elettronica e software per Sistemi Embedded e Mobili, ma anche di Cybersecurity e Digital Forensics. Appassionato Maker e lettore vorace di Fantascienza, da qualche anno scrive di Tecnologie Digitali, provando a interpretare per il grande pubblico un mondo sempre più complesso.

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.

Luisa Malagola: Avvocato del Foro di Milano con competenze specifiche nel settore penale.

Paolo Marzano: Capitano della Guardia di Finanza, laureato in Giurisprudenza e specializzato in Professioni Legali. Frequentatore di numerosi corsi e di una Summer School universitaria in "Economia e Legislazione Antiriciclaggio", negli anni ha maturato una vasta competenza in materia di reati tributari, antiriciclaggio, appalti e anticorruzione. Formatore qualificato in attività di contrasto alle frodi comunitarie e nazionali.

Gianluigi Miglioli: Generale di Corpo d'Armata della Guardia di Finanza (della riserva), laureato in Giurisprudenza, Scienze Politiche e Scienza della Sicurezza Economico-Finanziaria. Docente in materie giuridiche e tecnico professionali, nonché frequentatore di numerosi corsi di formazione.

Matteo Montagner: Direttore Generale presso Innovabay, start up tecnologica del progetto Sygmund per l'erogazione di servizi psicologici online rivolta a privati e imprese. Negli anni, attraverso collaborazioni con l'Università Ca' Foscari di Venezia e Società di Consulenza Internazionali, ha accompagnato piccole, medie e grandi imprese nei processi di trasformazione degli assetti organizzativi.

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

Marcovalerio Pozzato: Presidente Aggiunto, Sezione giurisdizionale Emilia-Romagna della Corte dei conti. Professore a contratto di Contabilità pubblica e Diritto dei Contratti Pubblici presso l'Università di Trento

Pierpaolo Rossi: Consigliere Bilancio, Dogane e Fiscalità presso il Servizio giuridico della Commissione. Generale di brigata (r) della Guardia di Finanza. Avvocato Cassazionista, docente di diritto tributario europeo presso l'Università di Marsiglia/Aix-en-Provence. Laureato in Scienze della Sicurezza Economico-Finanziaria e Giurisprudenza. Specializzato presso la Law School della New York University (International Tax Program, LL.M.). (le opinioni espresse sono a titolo prettamente personale, e non rappresentano necessariamente le posizioni ufficiali delle Istituzioni dell'Ue).

Camilla Speriani: sustainability addicted e advisor per aziende, ha fondato la società di consulenza Collectibus Società Benefit nel 2015. Collabora alla nascita di startup e ad operazione di venture per la sostenibilità, ha ideato il Sustainable Open Agent e si occupa.

Diego Tatulli: Ex allievo della Scuola Militare Nunziatella, Ufficiale Superiore nella Guardia di Finanza ed appassionato di sicurezza economico-finanziaria, nel corso della sua ventennale carriera militare ha maturato una significativa esperienza operativa nel contrasto al riciclaggio di proventi illeciti e nella repressione di fenomeni corruttivi.

Pier Luca Toselli: Luogotenente della Guardia di Finanza, docente nell'ambito del Master Execu- tive 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.

Carlo Zadra: Direttore dell'équipe Giustizia Affari Interni – Servizio giuridico del Consiglio dell'Unione Europea.

Filippo Zemignani: dottorando in Studi Giuridici Comparati ed Europei presso la Facoltà di Giurisprudenza di Trento, si occupa principalmente di responsabilità civile di fronte alle sfide dell'intelligenza artificiale e della guida autonoma. È avvocato presso il Foro di Trento.

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.

Editoriale

di Denise Boriero e Ivano Maccani

Il 23 e il 24 marzo si è tenuta a Roma l'ottava Assemblea del Network della rete europea delle Autorità a tutela dei *whistleblower (NEIWA).* Tale Network è la rete delle 29 autorità europee finalizzate a promuovere e salvaguardare l'integrità pubblica nei rispettivi Paesi e responsabili della gestione delle segnalazioni e della tutela dei segnalatori da possibili comportamenti ritorsivi.
L'appuntamento è stato da subito molto sentito sia perché mirava ad approvare la costituzione della Rete, sia perché si svolgeva a ridosso di quello che può essere definito un grande traguardo per l'Italia, ossia l'approvazione del decreto legislativo proprio in materia di *whistleblowing*. Con questo decreto, approvato dal Consiglio dei Ministri il 9 marzo c.a., il nostro Paese recepisce finalmente la Direttiva europea del 2019, la numero 1937. Lo schema di decreto è già stato oggetto di plurimi approfondimenti in questa Rivista, così come lo è nel numero attuale, e continuerà ad esserlo, data la rilevante importanza.
ANAC, che ha ospitato presso la propria sede l'Assemblea NEIWA, ha da sempre fortemente voluto l'approvazione della normativa in parola al fine di garantire una tutela effettiva ai segnalatori.
In Italia c'è ora bisogno di un cambiamento culturale, in primis, poiché questo istituto non si è mai diffuso molto, anzi è sempre stato visto con sospetto. In altre realtà, invece, sia europee che extraeuropee – in particolare negli Stati Uniti – la gestione delle segnalazioni è considerata una forma di controllo diffuso, sia in ambito pubblico che privato, e oltre ad essere tutelata, è estremamente incentivata.
Il cambio culturale, però, di fatto non potrà tardare nemmeno nel nostro Paese in quanto le disposizioni del decreto legislativo entrano in vigore a breve, ossia dal 15 luglio 2023 per tutte le Pubbliche Amministrazioni e per le imprese e le società con un numero di lavoratori subordinati – indipendentemente dalla durata del loro contratto – pari o superiore a 250. Le realtà che impiegano invece fino a 249 dipendenti, ed un minimo di 50, hanno l'obbligo di istituire il canale di segnalazione interna dal 17 dicembre 2023.
Per essere *compliant*, enti e imprese devono adottare una serie di misure e accorgimenti che favoriscano il ricorso agli strumenti di segnalazione e soprattutto garantiscano la massima tutela ai *whistleblowers*.
È stato previsto un doppio canale per le segnalazioni: uno interno messo a disposizione dall'azienda e uno esterno, normalmente indirizzato ad ANAC.
Le tipologie di condotte da segnalare variano in base all'ambito privato o pubblico, al numero del personale e al fatto che la realtà in oggetto sia tenuta o meno alla redazione di un modello organizzativo ai sensi del decreto legislativo 231 del 2001.
Negli enti pubblici possono essere segnalati comportamenti che potenzialmente integrano illeciti amministrativi, civili e penali, dunque violazioni di diritto interno ma anche di norme europee. Nell'ambito privato, le aziende con più di 50 dipendenti prive del modello 231, possono segnalare condotte che violano il diritto europeo.
Infine, per le imprese private dotate di modello 231, in caso di un numero di lavoratori subordinati inferiore a 50, possono essere segnalate solo internamente le condotte che violano il modello organizzativo e la normativa prevista dal d.lgs. 231/2001, così come per quelle che presentano un numero superiore di dipendenti, con la differenza che queste ultime possono segnalare anche esternamente le violazioni di norme di derivazione europea.
Vale dunque la pena di evidenziare la portata di questa nuova adozione, pur senza entrare in questa sede nelle numerose conseguenze pratiche che ne derivano, non solo a livello culturale ma anche per l'apparato sanzionatorio previsto per coloro che non si adeguano e non tutelano i propri segnalatori.

Diversity in azienda, l'Italia fa il punto con la certificazione di genere (UNI/PdR 125:2022)

di Camilla Speriani

A che punto siamo in Europa
Con un tweet di marzo 2020, la Presidente della Commissione Europea Ursula von der Leyen riassumeva in poche righe tutta l'importanza di progredire nella parità di genere all'interno dell'Unione Europea (e a livello globale) a partire da una situazione tutt'altro che idilliaca: *"La parità di genere è un principio fondamentale dell'Unione Europea, ma non è ancora una realtà. Nel mondo degli affari, in politica e nella società nel suo complesso potremo raggiungere il nostro pieno potenziale solo utilizzando tutti i nostri talenti e la nostra diversità. Impiegare soltanto la metà della popolazione, la metà delle idee e la metà dell'energia non è sufficiente."*

https://twitter.com/vonderleyen/status/1235525914836033539?lang=en

Secondo l'Istituto Europeo per l'uguaglianza di genere (*European Institute for Gender Equality* — EIGE) che produce il Gender Equality Index, nei dodici anni del suo monitoraggio sullo stato dell'Unione è registrabile un andamento migliorativo, ma molto, molto lento. Al ritmo attuale al quale si registrano progressi, restano ancora almeno 60 anni prima che la completa uguaglianza di genere sia conseguita, quasi un secolo di storia, dal Trattato di Maastricht, per raggiungere finalmente una situazione di uguaglianza e dare pari diritti alla metà della popolazione europea.

Secondo i dati dell'Istituto, infatti, dal 2010 al 2022 è stato registrato un incremento di 5,5 punti sul Gender Equality Index che oggi registra un punteggio complessivo di 68,6 punti su 100. I paesi best performer sono la Svezia, Danimarca e Olanda che superano o sfiorano gli 80 punti mentre sette paesi i membri (Polonia, Repubblica Ceca, Cipro, Ungheria, Romania, Slovacchia, Grecia) che hanno avuto un

punteggio al di sotto del 60 dimostrando quindi una grande difficoltà a garantire un processo di miglioramento sul tema. L'Italia, con i suoi 65 punti, nel 2022 ha registrato un incremento significativo dalla prima rilevazione, più 11,7 punti, attestandosi comunque al quattordicesimo posto vicino a Slovenia, Portogallo, Malta e Lettonia.
I dati italiani sono estremamente noti:
• un tasso di occupazione femminile che non raggiunge neppure il 53%, abbassando la media Ue (superiore al 67%);
• un 38% delle donne che modifica la struttura del proprio lavoro per far fronte alle esigenze della famiglia (gli uomini? Si fermano al 12%);
• tempo dedicato alla cura non retribuita cui si dedica quotidianamente l'81% di donne contro il 20% degli uomini (la media europea è del 79% delle donne a fronte del 34% degli uomini).

L'Istituto ha anche segnalato che la pandemia COVID-19 ha avuto un impatto drammatico sulle dimensioni considerate nella costruzione dell'Indice, al punto che il miglioramento registrato è dovuto unicamente all'ambito della rappresentatività negli organi di governo nazionali che, pur migliorato, registra comunque una performance molto bassa: le donne rappresentano solo il 33% dei membri dei parlamenti europei. Mentre, per la prima volta, la disparità di genere nel lavoro (*full-time equivalent employment rate (FTE), duration of working life*), nell'educazione (*tertiary graduation and participation in formal or informal education and training*) e nello stato di salute e nell'accesso ai servizi sanitari è addirittura cresciuta, anziché diminuire.
Non stupisce quindi che, all'interno degli impegni del Green New Deal Europeo, sia stata avvertita la necessità di configurare una Strategia per la parità di genere 2020-2025 che definisce gli obiettivi politici e le azioni chiave da intraprendere per conseguire la parità di genere e per integrare maggiormente la dimensione in tutti gli ambiti politico-economici, ovvero inserendo tale prospettiva in ogni fase dell'elaborazione delle politiche europee.
Obiettivi essenziali della Strategia sono sicuramente:
• il liberarsi dalla violenza e dagli stereotipi (in attuazione della Convenzione di Istanbul), anche con riferimento alle molestie in ambito lavorativo come già indicato l'ILO (International Labor Organization);
• il realizzarsi di una economia basata sulla partita di genere, colmando il divario nell'accesso alle materie STEM (solo il 36% dei laureati è donna), attuando una direttiva sull'equilibrio tra attività professionale e vita familiare, fino al risolvere il fondamentale problema dovuto al divario retributivo e pensionistico generando una nuova dimensione di genere nella finanza (sostegno all'imprenditorialità femminile, accesso al credito, etc.);
• un approccio che riverbera su un obbligo per ciascuno Stato membro di disporre di un quadro strategico nazionale per la parità di genere quale presupposto essenziale per l'utilizzo dei Fondi comunitari.

Parità, diversità, inclusione, equità
La parità di genere ricade nel più ampio tema della diversità, inclusione ed equità (DI&E) per la quale a livello internazionale il dibattitto è ampio e sempre più circostanziato per quel che riguarda le soluzioni da implementare in azienda in connessione al l vantaggio competitivo conseguibile.
In questo ambito a maggio 2021 è stata pubblicata la norma ISO 30415:2021 - *Human Resources Management – Diversity and Inclusion*. Come per molti altri aspetti della gestione responsabile d'azienda, l'International Organization for Standardization è intervenuta per definire uno standard internazionale a disposizione delle aziende per dimostrare il proprio impegno sulla gestione e capacità di valorizzazione della diversità negli ambienti di lavoro favorendone l'inclusione. Uno stimolo ad adottare un orientamento strategico a supporto della diversità quale elemento differenziante per conseguire creazione di valore per l'azienda con l'idea che la diversità esiste sempre, quindi va gestita, mentre l'inclusione deve essere creata, attraverso una gestione consapevole.

Non solo quindi parità di genere ma uno sguardo più allargato per comprendere il tema, ovvero:
• diversità, comprensione, accettazione e valorizzazione della diversità delle persone includendo età, etnicità, genere, identità di genere, differenze di lingua, nazionalità, stato della genitorialità, abilità e sviluppo fisico e mentale, razza, religione, orientamenti sessuali, colore della pelle, status socioeconomico, stili di comportamento e lavoro, prospettive dovute all'identità nazionale, all'esperienza e alla cultura;
• inclusione, capacità di creare inclusione ovvero ambienti di lavoro collaborativi, rispettosi, valorizzanti che accrescano la partecipazione e il contributo di ciascun collaboratore;
• equità, corretto trattamento per tutte le persone, affinché norme, pratiche e politiche assicurino che l'identità non sia pregiudiziale per la vita lavorativa, ovvero non costituiscano ostacolo né automatica opportunità.

La ISO 30415 ha quindi l'obiettivo di rappresentare una guida sulla DI&E e costituisce un ottimo punto di riferimento anche per la sola parità di genere perché, come tutte le ISO, si rivolge a tutti i tipi di organizzazione. Sia che si tratti di organizzazioni pubbliche, private, non profit, indipendentemente dalle dimensioni o tipologia di attività la norma supporta nell'identificare una serie di principi, ruoli e responsabilità, azioni, politiche, processi, pratiche e misure per consentire e sostenere un'effettiva gestione della DI&E attraverso l'adozione di un approccio Plan-Do-Check-Act e di miglioramento continuo.

Su quali processi aziendali incide?
Sicuramente ha grande impatto sulla gestione delle risorse umane, dalla pianificazione del personale al recruiting e selezione, dalla formazione, ai processi di sviluppo e performance management, ai piani di sviluppo alle politiche retributive.
La norma non esaurisce in questo il suo portato di azione incidendo anche sull'offerta di prodotti e servizi, ovvero quali scelte sono operate nella progettazione, produzione, commercializzazione dei prodotti e dei servizi aziendali, così come nelle relazioni lungo la catena di fornitura per il monitoraggio dello stato di integrazione del tema e la definizione di impegni condivisi e nelle relazioni in generale con gli stakeholder.
Punti cardini della norma sono:
• riconoscere la diversità, valorizzando tutte le persone sia come individui, sia come gruppi, apprezzandone il modo di rapportarsi e riconoscendo che le caratteristiche demografiche e personali possono essere protette da leggi e regolamenti;
• governare in modo efficace, promuovendo l'impegno del management nei confronti di diversità e inclusione attraverso l'uso di sistemi, politiche, processi e prassi inclusive;
• agire in modo etico e socialmente responsabile, promuovendo un'occupazione produttiva e un lavoro dignitoso per tutti;
• lavorare in modo inclusivo, consentire e sviluppare un ambiente di lavoro accessibile e rispettoso che favorisca l'inclusione e il senso di appartenenza;
• comunicare in modo inclusivo, rispondendo ai bisogni specifici delle persone che entrano nell'organizzazione, relazionandosi e comunicando anche con modalità differenti;
• sostenere e diffondere la diversità e l'inclusione, influenzare e promuovere attivamente pratiche organizzative e relazioni con gli stakeholder inclusive.

A livello di governance, una volta definito il commitment dei vertici e definito il processo di delega alle funzioni e persone competenti in materia, la norma definisce come essenziale l'individuazione delle risorse necessarie alla attuazione dei programmi e delle politiche di D&I (diversity & inclusion). Questo per l'azienda si traduce necessariamente nella produzione di un quadro di principi e obiettivi (es. Policy D&I) e poi delle procedure operative connesse sia per la promozione di modelli di riferimento coerenti con i principi D&I ma anche per la valutazione

e gestione di comportamenti non coerenti con essi e quindi la protezione e il supporto di coloro i quali subiscono un comportamento inappropriato.
Ulteriore tassello è quello di chiedere agli alti dirigenti di rendere conto della valutazione di opportunità e rischi di D&I dell'organizzazione, e revisionare le prestazioni e i progressi nel raggiungimento degli obiettivi di D&I e l'impatto dei relativi risultati.
Per guardare ad un esempio nazionale, a novembre 2022, Poste Italiane ha comunicato di aver conseguito la certificazione quale prima azienda italiana nell'FTSE Mib, indice di borsa dedicato al segmento degli investimenti sostenibili, ed importante è il perimetro indicato come focus del sistema di gestione implementato: "Integrare i principi di diversità e inclusione in tutti i processi di progettazione, indirizzo, controllo, coordinamento e fornitura dei servizi postali, finanziari, assicurativi e digitali". Le dichiarazioni arrivano poi dai vertici che riconoscono in questo percorso un valore di reputazione e competitività: "La cultura d'impresa espressa da Poste Italiane, ispirata alla inclusione, risulta ancora più radicata e viene avvertita sempre meglio, anche all'esterno dell'azienda e sul piano internazionale - ha dichiarato l'amministratore delegato Matteo Del Fante -. L'attestazione riconosce quindi questa percezione frutto del lavoro compiuto negli ultimi anni dal Gruppo sull'inclusione attraverso la valorizzazione della diversità in tutte le sue forme e su ogni piano organizzativo e rafforza il nostro impegno nel candidarci come riferimento nazionale sulla diversity & inclusion". "L'affermazione di una cultura inclusiva - commenta Giuseppe Lasco, condirettore generale di Poste Italiane - genera benefici individuali e collettivi ed è in grado di arricchire ad ogni livello di responsabilità l'esperienza di tutte le persone di Poste Italiane"..

Parità di genere, la certificazione in Italia
Specificatamente circoscritta all'ambito della parità di genere, invece, il 16 marzo 2022 è stata pubblicata la Prassi di Riferimento UNI/PdR 125:2022 che introduce in Italia un Sistema di Gestione della Parità di Genere e la relativa certificazione.
La norma UNI/PdR 125:2022 stabilisce le linee guida per un Sistema di Gestione per la Parità di Genere con lo scopo di incoraggiare la misurazione, la rendicontazione e la valutazione dei dati relativi al genere all'interno delle organizzazioni, con l'obiettivo di ridurre le differenze di genere e promuovere un cambiamento duraturo e sostenibile. La UNI/PdR 125 è correlata alla linea guida ISO 30415:2021 e ne riprende i contenuti del sistema di gestione per la diversità e l'inclusione, ma si focalizza principalmente sulla parità di genere.
La norma è derivata da un Tavolo di lavoro sulla certificazione di genere delle imprese come previsto dal PNRR Missione 5 e coordinata dai Dipartimenti per le Pari Opportunità, per le politiche della famiglia, dal Ministero dell'Economia e delle Finanze, del Lavoro e delle Politiche Sociali, dello Sviluppo Economico e dalla Consigliera Nazionale di Parità. Tale prassi è inoltre disciplinata dalla Legge Gribaudo e dalla Legge di Bilancio 2022 e collegata alla Strategia Nazionale sulla Parità di Genere 2021-2025 (ispirata alla Gender Equality Strategy 2020-2025 europea), di cui uno dei dispositivi legislativi è la Legge 5 novembre 2021 n. 162 sulla parità salariale.
Quest'ultima, in vigore dal 3 dicembre 2021, modifica gli articoli 46 e 47 del Codice delle Pari Opportunità (D.lgs. 198/2006) e prevede strumenti normativi volti a favorire la partecipazione femminile al mercato del lavoro in Italia e a ridurre le differenze sul piano retributivo e di crescita professionale tra i due generi.
La legge introduce nel Codice delle pari opportunità una nuova nozione di discriminazione: è discriminazione ogni trattamento o prassi, anche organizzativa, concernente le condizioni e i tempi di lavoro che mette o può mettere il/la lavoratore/lavoratrice, in ragione del sesso, dell'età, di esigenze di cura personale o familiare, in condizione di svantaggio, di limitazione delle opportunità di partecipare alla vita o alle scelte aziendali, di limitazione nell'accesso ai meccanismi di progressione nella carriera rispetto alla generalità del resto del personale aziendale.
«*Abbiamo scelto con chiarezza di investire nel lavoro femminile e di accompagnare concretamente le imprese: la certificazione per la parità di genere, strumento fortemente innovativo, attiverà nuove pratiche di carattere aziendale e darà opportunità alle donne*– spiega la Ministra Elena Bonetti -. *Non possiamo più permetterci di lasciare in panchina le competenze e i talenti femminili: liberarli non è soltanto giusto ma necessario ed è la strada che il governo ha deciso di percorrere per far crescere tutto il Paese*».
Tra le azioni concrete introdotte dalla Legge 261/2021, troviamo la redazione del rapporto biennale sulla situazione del personale e la certificazione della parità di genere in azienda.
Il rapporto biennale è previsto per le aziende con più di 50 dipendenti che dovranno redigere, ogni 2 anni, e trasmettere alle rappresentanze sindacali un rendiconto sulla situazione del personale con il numero dei lavoratori occupati e/o assunti suddivisi per sesso (senza indicazione di dati identificativi ulterio-

ri), l'inquadramento contrattuale, le funzioni svolte, l'importo della retribuzione complessiva e dei bonus riconosciuti e le eventuali differenze tra le retribuzioni iniziali dei lavoratori di ciascun sesso. Le aziende sotto 50 dipendenti potranno redigere il rapporto su base volontaria. Il rapporto ha una forte valenza ai fini del coinvolgimento degli stakeholder interni ed esterni quali le rappresentanze sindacali, i consiglieri territoriali e regionali di parità i quali, in possesso di tale informativa aziendale possono esercitare il controllo e la verifica del rispetto dei requisiti necessari al mantenimento dei parametri minimi per il conseguimento della parità di genere alle imprese e collaborare con il datore di lavoro per la progettazione degli interventi necessari.
La Certificazione di Parità di Genere, invece, oltre a rafforzare l'immagine e reputazione aziendale, ha in previsione l'accesso, per le organizzazioni che la adottino, a sgravi fiscali e premialità nella partecipazione a bandi italiani ed europei.

Come misurare la Parità di genere: i KPI
La UNI/PdR 125 tiene conto della presenza di disparità di genere in alcuni settori produttivi e richiede un confronto basato sulla media della categoria aziendale per definire i KPI quantitativi che necessitano di un raffronto con indicatori esterni all'azienda. Sono previste semplificazioni per le organizzazioni di dimensioni minori, mentre per le organizzazioni di media e grande dimensione sono applicati tutti gli indicatori. La norma è progettata per una certificazione di parte terza e individua sei aree di indicatori che contraddistinguono un'organizzazione inclusiva.
Le aree coperte dagli indicatori sono:
• Cultura e strategia;
• Governance;
• Processi HR;
• Opportunità di crescita ed inclusione;
• Equità remunerativa;
• Tutela genitorialità e conciliazione vita-lavoro.

Ogni area ha un peso percentuale specifico, che contribuisce alla valutazione generale dell'organizzazione. Ogni indicatore ha un punteggio associato e il raggiungimento o meno di ogni indicatore è ponderato in base al peso dell'area di appartenenza. Per ottenere la certificazione, che ha validità triennale, l'organizzazione deve raggiungere uno score di sintesi complessivo almeno del 60%. Gli indicatori per la certificazione possono essere di natura qualitativa o quantitativa e variano a seconda delle dimensioni aziendali.
A titolo di esempio, nella linea guida sono riportati gli indicatori:
• Processi HR ;
- Presenza di meccanismi di analisi del Turnover in base al genere (qualitativo);
- Presenza di politiche in grado di garantire la partecipazione equa e paritaria a percorsi di formazione e di valorizzazione, con la presenza di entrambi i sessi, inclusi corsi sulla leadership (qualitativo);
- Presenza di politiche di mobilità interna e di successione a posizioni manageriali coerenti con i principi di un'organizzazione inclusiva e rispettosa della parità di genere;
• Opportunità di crescita ed inclusione;
- Percentuale di donne nell'organizzazione con qualifica di dirigente (in caso di impresa familiare considerare anche le donne con ruoli dirigenziali espressione della proprietà) (quantitativo);
• Equità remunerativa;
- Percentuale di differenza retributiva per medesimo livello inquadramentale per genere e a parità di competenze (quantitativo);
• Tutela della genitorialità e conciliazione vita-lavoro;
- Rapporto tra il numero dei beneficiari uomini effettivi sul totale dei beneficiari potenziali dei congedi di paternità nei primi dodici anni di vita del bambino obbligatori (quantitativo);

L'iter per il conseguimento della certificazione comprende:
• Una fase iniziale di analisi dello stato dell'arte dell'azienda, un assessment condotto internamente o con il supporto di un consulente esterno;
• Un gap analysis che, a partire dall'esistente, e sulla base delle sei aree coperte da indicatori evidenzi i punti di interventi necessari;
• La definizione della politica aziendale sulla parità di genere, del riesame della Direzione e dell'organigramma aziendale;
• La stesura di procedure specifiche per la parità di genere (Whistleblowing, Assunzioni, Formazione, Bonus, etc.);
• L'individuazione di obiettivi tangibili di miglioramento per tutti gli aspetti coinvolti dalla prassi, con relative tempistiche di attuazione e correlazione con gli indicatori di performance;
• Organizzazione della formazione obbligatoria ai collaboratori;
• Organizzazione della prima visita certificativa e poi degli audit di controllo semestrali/annuali;
• Assistenza, se richiesta, durante l'audit da parte dell'Ente di Certificazione;

È importante nell'attivazione dell'intero processo, come per ogni impegno strategico aziendale, avere una precisa idea dell'impegno che l'azienda ha deciso di profondere sul tema sia per scegliere le corrette risorse da attivare internamente ed esternamente sia per utilizzare l'intero processo in ottica di miglioramento delle performance aziendale a tutto campo e dal punto di vista competitivo. Un approfondimento rispetto ai rischi legali e di vantaggio competitivo per la mancata applicazione così come dei rischi di una applicazione parziale all'interno dell'organizzazione per resistenze culturali, immaturità organizzativa può essere di aiuto nella definizione del percorso più corretto di azione.

Infine, anche la comunicazione interna ed esterna è un tassello importante della gestione nell'ottica di diffondere una cultura della parità di genere e del farlo sia utilizzando un linguaggio rispettoso delle differenze di genere sia con il coinvolgimento delle parti interessate e, naturalmente, allineando la comunicazione istituzionale e commerciale dell'azienda ai nuovi principi. Lo sviluppo di una nuova sensibilità porterà inevitabilmente a riconsiderare alcune prassi comunicative interne ed esterne (es. circolari interne su maternità/paternità, scelta dei soggetti per le pubblicità, etc.) per un sicuro miglioramento del modo con cui comunichiamo (e pensiamo) nelle aziende rispetto alla parità di genere.

Il Piano Nazionale di Ripresa e Resilienza prevedeva che, entro il 2026, sarebbero state circa 800 le aziende italiane che avrebbero portato a compimento il processo di certificazione per la parità di genere, grazie anche al supporto economico derivato dalle risorse del Piano. Con l'introduzione della certificazione erano state introdotte anche alcuni incentivi quali il poter usufruire di un esonero dal versamento dei contributi previdenziali e ottenere un punteggio premiale per la valutazione di proposte progettuali ai fini della concessione di aiuti di Stato. Inoltre, nei bandi di gara per appalti pubblici erano previste clausole per la parità di genere e l'assunzione di giovani e donne, e la premialità per le aziende che adottano specifiche misure per promuovere la parità di genere, come l'utilizzo di strumenti di conciliazione delle esigenze di cura, di vita e di lavoro. Le aziende in possesso della certificazione della Parità di Genere beneficiano anche di una riduzione della garanzia fideiussoria nei contratti di servizi e forniture. È recente però la notizia che, nella trasmissione del nuovo Codice degli Appalti il nuovo testo non contiene alcun riferimento alla certificazione per la parità di genere così come prevista dall'art. 46 bis del Codice delle pari opportunità mancando una forte opportunità di incentivazione alla sua applicazione.

Sicuramente il Paese Italia non potrà che beneficiare da questa prassi sia per l'annoso problema della qualità e quantità dell'occupazione femminile, sia come precursore di una migliore cultura della diversità e inclusione nelle aziende e nella società tutta.

Legge di bilancio 2023: la tassazione delle cripto-attività

di Luca Faiella e Matteo Faiella

Introduzione

La legge di Bilancio 2023[1] ha introdotto per la prima volta nel nostro ordinamento una disciplina specifica con riguardo al trattamento dei redditi e degli oneri di monitoraggio connessi a fattispecie relative alla detenzione e al trasferimento a vario titolo delle c.d. *cripto-attività*.

Le modifiche e le integrazioni disposte dai commi dal 126 al 146 della L. 197/2022 si inseriscono all'interno di un sistema che è stato, fino ad oggi, come s'è detto, sprovvisto di una disciplina specifica in materia e che ha regolato il fenomeno, per questa ragione, sulla base di un *framework* di riferimento, sviluppatosi sulla scorta di svariati interventi di prassi[2].

Sebbene la stessa Amministrazione Finanziaria si sia più volte espressa attraverso risoluzioni ed in sede di risposta ad istanze di interpello su svariati temi collegati al trattamento fiscale delle c.d. *cripto-attività*, il complesso delle indicazioni fornite non ha potuto certamente assolvere all'arduo compito di delineare un quadro completo e organico della materia, lasciando in tal senso numerosi e forse troppi dubbi interpretativi per consentirne una gestione puntuale.

La necessità, ormai sempre più attuale per via della progressiva diffusione del fenomeno, che il legislatore nazionale provvedesse ad introdurre nel nostro ordinamento un *corpus* normativo dedicato, perlomeno in materia fiscale, al trattamento delle c.d. *cripto-attività*, ha certamente trovato, nella novella richiamata, un primo importante riscontro.

Il contenuto del dettato normativo, se da un lato si è posto in continuità con taluni orientamenti e interpretazioni già avallati da parte dell'Amministrazione Finanziaria, dall'altro si è completamente discostato da altre precedenti indicazioni, talvolta anche in maniera radicale, aprendo la strada, in taluni casi, ad un trattamento delle richiamate fattispecie del tutto differente rispetto al passato.

La novella normativa costituisce senza dubbio una tappa fondamentale nel trattamento del fenomeno, che, a parere di chi scrive, delinea un decisivo punto di svolta nell'*iter* formativo di una chiara disciplina fiscale in materia, seppur ancora non del tutto compiuta.

Tale carattere trova conferma e si riflette in una serie di disposizioni ulteriori introdotte dalla legge di Bilancio rispetto a quanto previsto in relazione ai vari regimi fiscali applicabili alle cripto-attività e alle norme in materia di monitoraggio, essendo state previste anche disposizioni di carattere agevolativo e premiale, collegate alla rideterminazione ai fini fiscali del valore delle attività detenute al 01/01/2023 e alla possibilità di regolarizzare l'omesso monitoraggio delle cripto-attività detenute e non dichiarate in passato nel modello RW della dichiarazione dei redditi.

Il presente contributo esaminerà, nel prosieguo, il

1 *Legge 29 dicembre 2022, n. 197 - Bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023-2025.*

2 *Si riportano i riferimenti delle principali risoluzioni e risposte a istanze di interpello fornite dall'Amministrazione Finanziaria in materia di imposte sui redditi relative al trattamento di vari e differenti aspetti delle criptovalute: Ris. 2.9.2016 n. 72, Risposta a interpello 24.11.2021 n. 788, Risposta a interpello 1.8.2022 n. 397, Risposte a interpello 24.8.2022 n. 433 e 26.8.2022 n. 437, Risposte a interpello 12.10.2022 n. 508 e 17.10.2022 n. 515.*

disposto normativo richiamato illustrando quanto previsto secondo le direttrici poc'anzi descritte ed in particolare:
- le norme relative al regime fiscale introdotto per il trattamento delle fattispecie rilevanti collegate alle cripto-attività;
- le modifiche intervenute in materia di monitoraggio delle cripto-attività;
- la disciplina agevolativa per la rideterminazione del valore delle cripto-attività detenute al 01/01/2023;
- la procedura per la regolarizzazione dell'omessa indicazione nel quadro RW delle cripto-attività non dichiarate.

Ambito di applicazione: definizione di Cripto-Attività

Un primo elemento di sicuro interesse è l'introduzione di una definizione, perlomeno ai fini fiscali[3], di "cripto-attività", identificate dal nuovo disposto della lett. c sexies dell'art. 67 comma 1 del Testo Unico delle Imposte dirette come una "*rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga.*"
Tale definizione ha senza dubbio una portata ampia, suscettibile di uno svariato numero di applicazioni e quindi in grado di includere nel perimetro applicativo della norma un vasto spettro di casi.
L'individuazione di un criterio di selezione delle fattispecie inquadrabili all'interno della categoria delle c.d. *cripto – attività*, sulla base del comun denominatore identificato nell'infrastruttura tecnologica utilizzata per "documentare" le operazioni concernenti i valori o i diritti oggetto delle stesse cripto-attività, ha certamente il pregio di prevenire una serie di difficoltà definitorie e di inquadramento che si genererebbero dal confronto con fattispecie analoghe, ma già previste dal nostro ordinamento

Sulla scorta di queste indicazioni ben possono essere ascritte alla categoria delle cripto-attività i c.d.:
- Utility token;
- *Asset-referenced token;*
- *E-money tokens;*
- Security token;
- Equity token;
- NFT – Non fungible token;
- Criptovalute in senso stretto.

Regimi fiscali

Venendo dunque al primo tema da analizzare con riguardo al trattamento ai fini delle imposte sul reddito, le disposizioni della legge di bilancio hanno introdotto delle modifiche, provvedendo all'inserimento di nuovi specifici commi agli artt. 67, 68 e 110 del TUIR e agli artt. 5, 6, 7 e 10 del D.lgs n. 461/97.
Con riguardo ai soggetti operanti non in regime di impresa l'art. 67, con la disposizione introdotta al comma 1 lett. c sexies, riconduce alla categoria dei *redditi diversi di natura finanziaria le plusvalenze e gli altri proventi realizzati mediante rimborso o cessione a titolo oneroso, permuta o detenzione di cripto-attività, comunque denominate, non inferiori complessivamente a 2.000 euro nel periodo d'imposta, escludendo dalle fattispecie fiscalmente rilevanti la permuta tra cripto-attività aventi eguali caratteristiche e funzioni.*
Dalla lettura della norma emerge come sia stata esclusa qualsiasi distinzione collegata alla fattispecie realizzativa del presupposto impositivo ai fini dell'individuazione della categoria alla quale risulti ascrivibile reddito generato nelle ipotesi descritte. La disposizione richiamata riconduce all'unica categoria dei redditi diversi di natura finanziaria sia fattispecie nelle quali sia riscontrabile l'emersione di redditi imponibili collegati al trasferimento delle cripto-attività e dunque fattispecie realizzative, che anche ipotesi "ordinariamente" riconducibili alla categoria dei redditi di capitale, individuando espressamente tra le ipotesi previste anche la percezione di *altri proventi* in particolare derivanti dalla detenzione delle cripto-attività.
In tal senso è bene sottolineare come si possa cogliere sin d'ora un primo elemento di discontinuità rispetto alle indicazioni ricavabili in relazione agli interventi di prassi forniti dall'Amministrazione finanziaria in epoca precedente all'introduzione delle nuova disciplina: con risposta ad interpello n. 433/2022 in merito all'attività di *staking* l'Amministrazione Finanziaria aveva infatti ricondotto i proventi dalla stessa rinvenienti alla categoria dei redditi di capitale, circostanza non riscontrabile alla luce della normativa attuale. Allo stesso modo si deve rilevare come non sia previsto alcuna distinzione di trattamento in ordine al contenuto e alla tipologia di cripto-attività detenuta e nemmeno si rinvenga alcuna assimilazione al trattamento di altra fattispecie analoga, essendo previsto in questo senso un sistema autonomo. Come si è detto all'interno della categoria delle cripto-attività si possono distinguere svariate tipologie di *token* come anche le stesse criptovalute, senza che però, ai fini fiscali, tale distinzione si traduca in un differente trattamento. In questo senso si può notare il superamento e dunque la non applicabilità della soglia di rilevanza fiscale per le plusvalenze individuata nella detenzione di importo superiore a 51.645,69 euro per almeno 7 giorni come previsto al comma 1 lett. c ter dell'art. 67, ritenuto applicabile dall'Amministrazione finanziaria in virtù dell'assimilazione delle criptovalute alle valute estere come indicato nella risposta all'interpello n. 397/2022.
La norma prevede in ogni caso una soglia di rilevanza generale al di sotto della quale la fattispecie che venga a verificarsi non acquisisce rilievo fiscale e tale soglia è individuata in euro 2000,00.[4]
La norma, infine, prevede l'esclusione dalle fattispecie fiscalmente rilevanti delle operazioni di permuta tra cripto-attività aventi eguali caratteristiche e funzioni. Questa fattispecie presenta sicuramente delle difficoltà di carattere interpretativo ravvisabili nella necessità di identificare l'identità di caratteristiche e funzioni necessaria per poter far rientrare l'operazione permutativa nel perimetro applicativo di esenzione previsto dalla norma.
Con riguardo al tema della valorizzazione delle cripto-attività per la determinazione della base imponibile collegata sia alle ipotesi relative a plusvalenze che ad altri proventi comunque rinvenibili dalla detenzione delle stesse, la novella normativa ha disposto l'introduzione del comma 9 bis dell'articolo 68, con il quale è stato previsto che:
- *"Le plusvalenze di cui alla lettera c-sexies) del comma 1 dell'articolo 67 sono costituite dalla differenza tra il corrispettivo percepito ovvero il valore normale delle cripto-attività permu-*

3 È da notare come lo stesso articolo 67 del TUIR, comma 1 lett. c sexies, circoscriva il perimetro applicativo della definizione introdotta alle finalità della stessa norma, senza attribuirne esplicitamente una portata generale, non essendo peraltro nemmeno richiamata esplicitamente da altre norme introdotte dalla L. 197/2022 come, ad esempio, il comma 3 bis dell'art. 110 TUIR. E' parere di chi scrive, in ogni caso, che detta definizione possa ben essere estesa e ritenersi applicabile ai fini fiscali a tutte le ipotesi afferenti le cripto-attività attesa peraltro la continuità rilevabile tra questa stessa definizione e le indicazioni fornite anche a livello europeo per esempio dalla Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo ai mercati delle cripto-attività, che modifica la direttiva (UE) 2019/1937 - COM/2020/593 final – c.d. regolamento MiCA o nell'ambito del Crypto Asset Reporting Framework, pubblicato dall'Ocse il 10 ottobre 2022, con lo scopo di integrare la disciplina per lo scambio di informazioni ai fini fiscali in relazione a operazioni collegate alle cripto-attività rispetto a quanto previsto e riconducibile al perimetro applicativo del c.d. Common Reporting Standard.

4 Sul punto si deve sottolineare come al momento non vi siano chiarimenti circa i termini di operatività di questa franchigia, dal momento che la norma non chiarisce se il superamento della soglia comporti il recupero a tassazione di tutti i redditi ovvero solo della parte eccedente detto livello di esenzione.

tate e il costo o il valore di acquisto;
- Le plusvalenze di cui al primo periodo sono sommate algebricamente alle relative minusvalenze[5]*; se le minusvalenze sono superiori alle plusvalenze, per un importo superiore a 2.000 euro, l'eccedenza è riportata in deduzione integralmente dall'ammontare delle plusvalenze dei periodi successivi, ma non oltre il quarto, a condizione che sia indicata nella dichiarazione dei redditi relativa al periodo di imposta nel quale le minusvalenze sono state realizzate*[6]*;*
- Nel caso di acquisto per successione, si assume come costo il valore definito o, in mancanza, quello dichiarato agli effetti dell'imposta di successione;
- Nel caso di acquisto per donazione si assume come costo il costo del donante. Il costo o valore di acquisto è documentato con elementi certi e precisi a cura del contribuente; in mancanza il costo è pari a zero;
- I proventi derivanti dalla detenzione di cripto-attività percepiti nel periodo di imposta sono assoggettati a tassazione senza alcuna deduzione."
Con riguardo invece ai soggetti operanti in regime di impresa, la legge 197/2022 ha previsto l'inserimento del comma 3 bis all'articolo 110 del TUIR, che espressamente ha previsto "*In deroga alle norme degli articoli precedenti del presente capo e ai commi da 1 a 1-ter del presente articolo, non concorrono alla formazione del reddito i componenti positivi e negativi che risultano dalla valutazione delle cripto-attività alla data di chiusura del periodo di imposta a prescindere dall'imputazione al conto economico*".

Tale previsione introduce un elemento di importante discontinuità rispetto all'orientamento precedentemente avallato dall'Amministrazione finanziaria, che assimilando le cripto-valute alle valute tradizionali, avrebbe dedotto la necessaria imputazione a conto economico delle variazioni di valore, per quanto non realizzate, basate sull'applicazione del cambio in vigore al termine dell'esercizio.
In tema di IRAP per quanto relativo alle valutazioni delle cripto-attività, la norma ha parimenti disposto l'irrilevanza ai fini fiscali.

5 In relazione alla compensazione di plusvalenze e minusvalenze è bene sottolineare che la norma, a differenza di quanto previsto al comma 5 dell'art. 68, circoscriva tali possibilità a rapporti tra operazioni omogenee dal punto di vista della categoria di riferimento, dovendo avere ad oggetto esclusivamente cripto-attività. A differenza di quanto previsto in tema di esenzione per operazioni di carattere permutativo non è prevista, a fini della possibilità di applicazione del meccanismo compensativo, la necessità che ricorra alcuna identità di caratteristiche e funzioni delle cripto-attività oggetto delle operazioni in esame. In tal senso dunque pare non sussista alcuna limitazione alla possibilità di scomputo delle minusvalenze da plusvalenze lucrate anche con riferimento a differenti tipologie di cripto-attività purché si rinvenga la medesima natura degli asset trasferiti riconducibile appunto a quella delle cripto-attività.

6 È stato previsto un regime transitorio che consente la deduzione delle minusvalenze relative a cripto-attività maturate sino al 2022 "per masse", in sostanza consentendone la compensazione anche con plusvalenze derivanti da redditi di natura finanziaria differenti, pur sempre nei limiti del quarto esercizio successivo.

Con riguardo al disposto degli artt. 5, 6, 7 e 10 del D.lgs n. 461/97 si deve evidenziare come l'articolo 5, appositamente integrato, preveda ora espressamente l'applicazione dell'aliquota del 26% per la determinazione dell'imposta relativa ai redditi di cui all'art. 67 comma 1 lett. c sexies del Tuir, mentre gli artt. 6 e 7 consentano l'estensione della facoltà di esercitare l'opzione per i regimi di risparmio amministrato e gestito anche in relazione ai redditi collegati alle operazioni relative a cripto-attività. Allo stesso modo per le stesse operazioni l'articolo 10 ha esteso l'obbligo di rilascio delle certificazioni da parte di intermediari che vi intervengano anche in qualità di controparti, nonché l'obbligo per gli stessi di comunicazione all'Amministrazione finanziaria dei dati relativi alle singole operazioni effettuate.

In conclusione si segnala l'estensione alle cripto-attività dell'imposta IVAFE qualora esse siano oggetto di detenzione per il tramite di un intermediario non residente ovvero archiviate tramite chiavette pc o *smartphone* e dell'imposta di bollo nella misura del 2 per mille per la comunicazione relativa ai prodotti finanziari, indipendentemente dal fatto che essa ricorra o meno, essendo previsto ora nella tariffa di cui al D.lgs. n. 642/1972 che "*si considera in ogni caso inviata almeno una volta nel corso dell'anno quando non sussiste un obbligo di invio di redazione*".

Monitoraggio
Con riguardo al tema del monitoraggio, la legge di Bilancio ha introdotto delle modifiche al Decreto Legge n. 167/1990, in particolare prevedendo l'ingresso nel novero dei soggetti destinatari delle previsioni di seguito indicate:
- all'art. 1, in tema di comunicazione delle operazioni di trasferimento di importo pari o superiore a 5.000 euro;
- all'art. 2, per quanto riguarda la richiesta nell'ambito dell'attività investigativa svolta dall'Unità Speciale costituita ai sensi dell'articolo 12, comma 3, del decreto legge 1° luglio 2009, n. 78, convertito, con modificazioni, dalla legge 3 agosto 2009, n. 102, e dai reparti speciali della Guardia di finanza, di cui all'articolo 6, comma 2, del regolamento di cui al decreto del Presidente della Repubblica 29 gennaio 1999, n. 34 dell'identità dei titolari effettivi rilevata in applicazione dei criteri di cui all'articolo 1, comma 2,lettera pp), e all'articolo 20 del D.lgs n. 231/2007 con riferimento a specifiche operazioni con l'estero o rapporti ad esse collegate;
- dei c.d. prestatori di servizi di portafoglio digitale di cui all'art. 3 co. 5 lett. i) e i-bis) del D.Lgs. n. 231/2007, ampliando altresì il perimento dell'oggetto del monitoraggio stesso, estendendolo alle cripto-attività nel loro complesso.

Per quanto riguarda invece le disposizioni in materia di quadro RW la novella normativa ha interessato il disposto dell'articolo 4, prevedendo espressamente l'inserimento delle cripto-attività tra i valori che devono esse oggetto di monitoraggio. Tale indicazione si pone in linea con il precedente orientamento dell'Amministrazione finanziaria che aveva rilevato la necessità di indicare nel quadro RW anche le criptovalute, in virtù di un'assimilazione di queste alle valute estere, pur evidenziando l'assenza del predetto obbligo nei casi di detenzione per il tramite di intermediari residenti[7].
La formulazione attuale della norma non prevede alcuna distinzione tra cripto-attività localizzate in Italia o estere, in assenza peraltro di qualsivoglia criterio di collegamento territoriale normativamente previsto, dovendosi pertanto ritenere suscettibile di una portata applicativa estesa a tutte le cripto-attività anche quelle detenute in Italia.
In relazione al tema della valorizzazione delle predette attività la legge di bilancio non detta alcuna regola ed in assenza di indicazioni normative in tal senso occorrerà fare riferimento a quanto ordinariamente previsto ed in particole alle indicazioni fornite con il provvedimento dell'Agenzia delle Entrate n. 151663/2013, fermo restando che, nell'analisi dei criteri previsti , pare che l'unica indicazione che possa fornire dei riscontri oggettivi non possa che essere ravvisata nel prezzo di acquisto.
Quanto poi all'individuazione del tasso di cambio da applicare, anche in questo caso occorre riferirsi a quanto suggerito in sede di risposta ad interpello da parte di Agenzia delle Entrate che ha individuato il cambio di riferimento nel valore al 31/12 rinvenibile sul sito sul quale è stato effettuato l'acquisto della cripto-attività.[8]

Rivalutazione delle cripto-attività
Con riguardo poi al tema del valore riconosciuto ai fini fiscali per le cripto-attività detenute al 01/01/2023 la novella normativa ha introdotto, ai soli fini dei redditi diversi di natura finanziaria, una disposizione agevolativa che prevede la possibilità di

7 Risposta a interpello n. 433/2022 e n. 437/2022.

8 Risposta a interpello n. 788/2011.

rideterminarne il valore fiscale da realizzarsi mediante il pagamento di un'imposta sostitutiva, nella misura del 14%, entro il 30.06.2023, in unica soluzione ovvero in massimo 3 rate annuali di pari importo con applicazione dei relativi interessi nella misura del 3% annuo sulle rate successive alla prima.

Il valore oggetto di rideterminazione, in relazione al quale calcolare l'imposta dovuta, deve essere individuato nel valore normale delle cripto-attività al 1 gennaio 2023 determinato in basi ai criteri previsti all'articolo 9 del TUIR[9].

Con riguardo all'ambito di applicazione soggettivo della richiamata disciplina, dalla lettura del testo della norma si rinviene come l'operatività della predetta ipotesi venga circoscritta alla determinazione delle plusvalenze di cui comma 1 lettera c) sexies, andando dunque ad escludere qualsivoglia altra forma di reddito non ascrivibile alla categoria dei redditi diversi di natura finanziaria e dunque per l'effetto la possibilità che del regime agevolativo ne beneficino soggetti operanti in regime di impresa.

Quanto invece alla portata dell'opzione e alla facoltà di operare una scelta selettiva delle cripto-attività, sulle quali effettuare la rideterminazione del valore fiscale, dalla lettera del disposto della norma non sembrano evincersi indici negativi in tal senso atteso che la formulazione letterale non pare porre vincoli alla necessità di trattamento unitario e omogeneo per tutte le cripto-attività detenute[10].

Cripto-attività - procedura di "disclosure"

Da ultimo il legislatore ha altresì previsto, come si è anticipato, una procedura di emersione agevolata delle cripto-attività delle quali sarebbe stata omessa l'indicazione nel modello RW.

La disposizione introdotta prevede in tal senso una disciplina premiale caratterizzata dalla significativa diminuzione degli importi dovuti a titolo di sanzione per la regolarizzazione dell'omissione rispetto alla procedura ordinaria regolata attraverso l'applicazione del c.d. ravvedimento operoso nelle ipotesi di emendabilità della dichiarazione presentata attraverso dichiarazione integrativa, fuori dai casi di omissione.

Tale procedura, peraltro, in assenza di contrarie indicazioni nel testo della norma, e in assenza di chiarimenti di prassi sul punto, non pare essere condizionata alla presentazione del modello Unico e dunque applicabile estensivamente ai casi in cui si riscontri una dichiarazione omessa.

Oggetto della regolarizzazione sono le cripto-attività detenute entro il 31/12/2021, da parte dei soggetti tenuti alla compilazione del quadro RW.

La procedura viene introdotta dalla presentazione di un'istanza da inoltrare su modello approvato con provvedimento dell'Agenzia delle Entrate e perfezionata attraverso il pagamento di una sanzione ridotta determinata:

- nella misura del 3,5% del valore delle attività detenute al termine di ciascun anno o al momento del realizzo in caso di realizzazione di redditi nel periodo di riferimento e
- nella visura del 0,5% a titolo di sanzione ridotta per il monitoraggio fiscale.

9 *L'art. 9 del Tuir al comma 3 e 4 espressamente prevede: "3. Per valore normale, salvo quanto stabilito nel comma 4 per i beni ivi considerati, si intende il prezzo o corrispettivo mediamente praticato per i beni e i servizi della stessa specie o similari, in condizioni di libera concorrenza e al medesimo stadio di commercializzazione, nel tempo e nel luogo in cui i beni o servizi sono stati acquisiti o prestati, e, in mancanza, nel tempo e nel luogo più prossimi. Per la determinazione del valore normale si fa riferimento, in quanto possibile, ai listini o alle tariffe del soggetto che ha fornito i beni o i servizi e, in mancanza, alle mercuriali e ai listini delle camere di commercio e alle tariffe professionali, tenendo conto degli sconti d'uso. Per i beni e i servizi soggetti a disciplina dei prezzi si fa riferimento ai provvedimenti in vigore.*
4. Il valore normale è determinato:
a) per le azioni, obbligazioni e altri titoli negoziati in mercati regolamentati italiani o esteri, in base alla media aritmetica dei prezzi rilevati nell'ultimo mese;
b) per le altre azioni, per le quote di società non azionarie e per i titoli o quote di partecipazione al capitale di enti diversi dalle società, in proporzione al valore del patrimonio netto della società' o ente, ovvero, per le società' o enti di nuova costituzione, all'ammontare complessivo dei conferimenti;
c) per le obbligazioni e gli altri titoli diversi da quelli indicati alle lettere a) e b), comparativamente al valore normale dei titoli aventi analoghe caratteristiche negoziati in mercati regolamentati italiani o esteri e, in mancanza, in base ad altri elementi determinabili in modo obiettivo."

10 *Resta inteso che in merito occorrerebbe un preciso chiarimento da parte dell'Amministrazione Finanziaria dal momento che il riferimento testuale a "ciascuna cripto-attività" posseduta, per individuare l'ambito applicativo del norma, può non essere di immediata comprensione .*

Dal Bring Your Own Device (BYOD) al Corporate Owned Business Only (COBO): tra mode, rischi e opportunità – seconda parte

di Giulia Bontempini e Stefano-Francesco Zuliani

Le linee guida di riferimento

Il "quadruplo bypass" è lo scenario peggiore del BYOD: un dispositivo di livello consumer che utilizza dati aziendali e accede direttamente a servizi cloud personali per la loro condivisione, archiviazione e modifica. Questo approccio, purtroppo molto comune, aggira completamente ogni possibilità di controllo da parte dell'IT aziendale sui dati e sulla loro sicurezza con rischio di violazione delle normative cogenti[1] [2]. Pur non essendoci norme o regolamenti specifici sulla corretta implementazione di una politica BYOD, nel corso degli anni varie istituzioni hanno emesso utili linee guida.

i) L'European Union Agency for Cybersecurity (ENISA) ha emanato nel 2012 le linee guida "*Consumerization of IT: Top Risks and Opportunities*"[3] [4]. Sebbene il documento non presenti soluzioni, rimane un utile strumento per l'individuazione di rischi e opportunità.

ii) Il Clusit - Associazione Italiana per la Sicurezza Informatica, nel marzo 2012 ha pubblicato la guida "Mobile e Privacy"[5].

iii) Nel marzo 2013 l'Information Commissioner's Office (ICO), la DPA del Regno Unito, ha pubblicato la "*Bring Your Own Device (BYOD) Guidance*" [6]. Tale guida è stata pubblicata in seguito alle polemiche legate ad un data breach subito nel 2012 dal Royal Veterinary College (RVC) come conseguenza del furto di una scheda di memoria di una fotocamera personale di un dipendente, utilizzata per motivi di lavoro e contenente immagini di documenti personali di candidati[7]. L'ICO considera ancora oggi questo evento come un importante *caso di scuola*, tanto da citarlo anche nelle sue linee guide sulla crittografia[8], anch'esse parzialmente applicabili.

iv) L'European Data Protection Supervisor (EDPS) del 2015 ha pubblicato le "*Mobile devices guidelines*" [9], le quali nonostante si rivolgano alle istituzioni UE, costituiscono un importante punto di riferimento per qualunque organizzazione interessata all'uso del BYOD al proprio interno.

v) Il National Institute of Standards and Technology (NIST) nel 2016 ha revisionato due linee guida preesistenti, ovvero "*Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*" e "*User's Guide to Telework and Bring Your Own Device (BYOD) Security*", rivolte rispettivamente alle aziende[10] e ai lavoratori remoti[11].

vi) Il tema del BYOD è stato affrontato nel 2017 dal WP29, che con l'Opinion 2/2017[12] ha aggiornato le precedenti linee guida sul trattamento dei dati personali dei lavoratori[13] [14].

vii) Alcune best practice sono state esemplificate nel 2019 in un articolo pubblicato sul sito web del Commission Nationale de l'Informatique et des Libertés (CNIL)[15].

viii) La norma volontaria ISO/IEC 27001:2022 presenta vari punti di controllo applicabili[16] [17] [18] [19] [20].

ix) Il Communications-Electronic Security Group

1 *Ad esempio: GDPR, art 4 Statuto dei Lavoratori, d.lgs 231/01, Legge sul Diritto d'Autore, etc.*

2 *Ad esempio negli Stati Uniti: Sarbanes-Oxley Act (SOX) sulla protezione delle informazioni finanziarie; Health Insurance Portability and Accountability Act (HIPAA) sulla protezione dei dati sanitari.*

3 *ENISA Consumerization of IT: Top Risks and Opportunities https://www.enisa.europa.eu/publications/consumerization-of-it-top-risks-and-opportunities*

4 *Ruch, Thierry Jean and Gregory, Robert Wayne, "CONSUMERIZATION OF IT – WHERE IS THE THEORY?" (2014). PACIS - 2014 Proceedings. 139. http://aisel.aisnet.org/pacis2014/139 https://core.ac.uk/download/pdf/301362759.pdf*

5 *Mobile e Privacy https://privacycloudmobile.clusit.it/index.php*

6 *ICO - Bring your own device (BYOD) https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf*

7 *RVC 'disappointed' after breaching data protection law https://www.vettimes.co.uk/news/rvc-disappointed-after-breaching-data-protection-law/*

8 *Encryption scenarios https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/encryption-scenarios/*

9 *Guidelines on the protection of personal data in mobile devices used by European institutions (Mobile devices guidelines) https://edps.europa.eu/data-protection/our-work/publications/guidelines/mobile-devices_en*

10 *SP 800-46 Rev. 2 - Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final*

11 *SP 800-114 Rev. 1 - User's Guide to Telework and Bring Your Own Device (BYOD) Security https://csrc.nist.gov/publications/detail/sp/800-114/rev-1/final*

12 *Opinion 2/2017 on data processing at work - wp249 - 5.4.2 BRING YOUR OWN DEVICE (BYOD) - https://ec.europa.eu/newsroom/article29/items/610169*

13 *ARTICLE 29 - DATA PROTECTION WORKING PARTY - WP 48 - Opinion 8/2001 on the processing of personal data in the employment context https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1365969*

14 *WP 55 - Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro - 29 maggio 2002 [1609517] https://www.garante-privacy.it/home/docweb/-/docweb-display/docweb/1609517*

15 *BYOD: quelles sont les bonnes pratiques ? https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques*

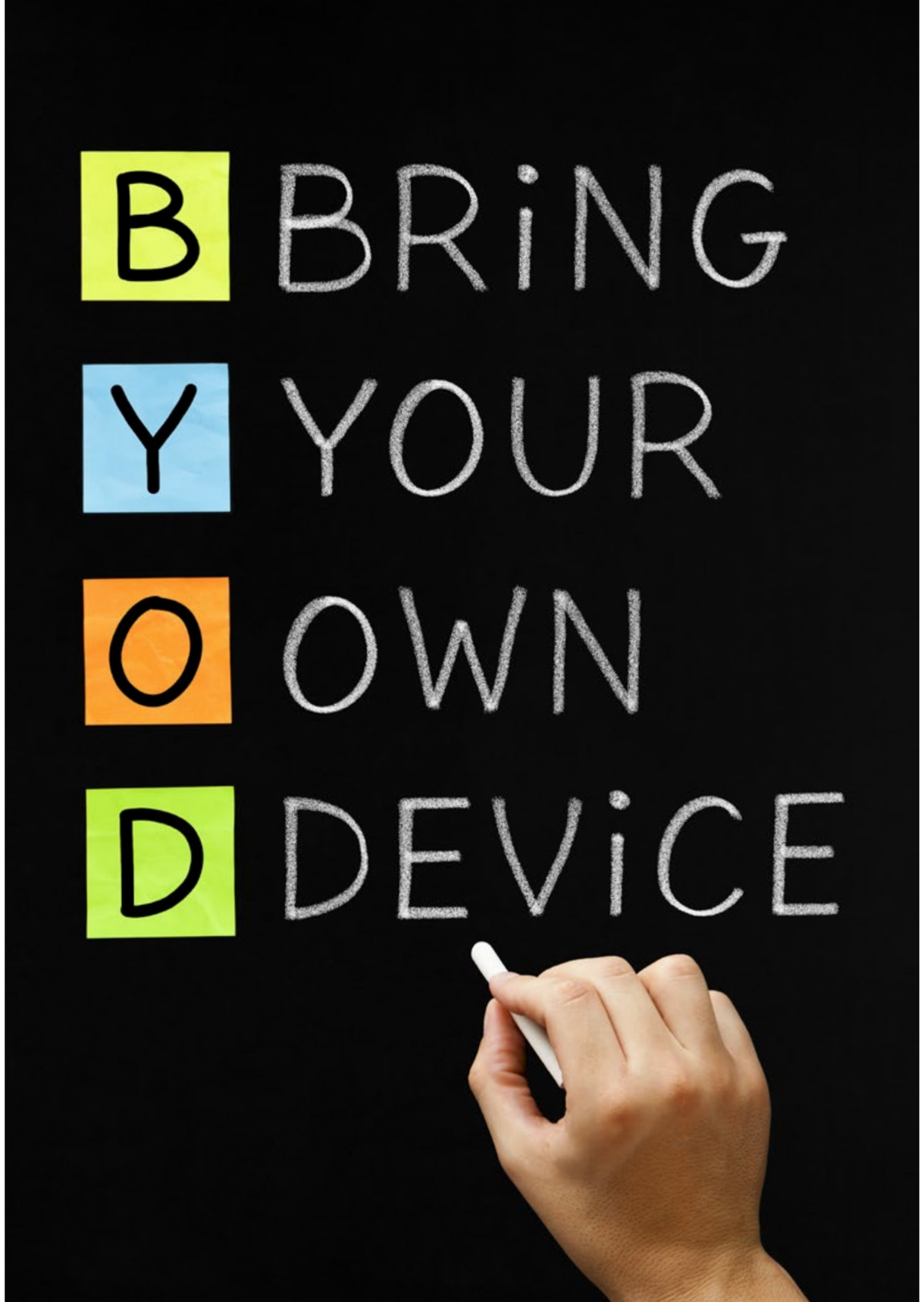
16 *ISO/IEC 27002 6.2.1 Mobile device policy*

17 *ISO/IEC 27002 6.2.2 Teleworking*

18 *ISO/IEC 27002 8.1.3 Acceptable use of assets*

19 *ISO/IEC 27002 13.2.1 Information transfer policies and procedures*

20 *ISO/IEC 27002 13.2.3 Electronic messaging*



(CESG), l'autorità nazionale UK per la sicurezza informatica, nel 2022 ha aggiornato le proprie linee guida "*Device Security Guidance*" che vertevano su come scegliere, configurare e utilizzare i dispositivi in modo sicuro[21]. Si tratta del documento più recente e maggiormente dettagliato, di cui un capitolo è dedicato al BYOD. Precedentemente il CESG aveva pubblicato altre due linee guida, ora ritirate[22] [23].
Da questi documenti, anche se in taluni casi datati, si possono ricavare dei suggerimenti di carattere generale. Vediamone alcuni.

Le misure organizzative

Gli IT manager aziendali sono spesso portati a considerare le misure tecniche come le più importanti. In realtà, come evidenziano sia il GDPR che le normative ISO/IEC, queste devono essere frutto di apposite riflessioni, policy aziendali e accettazione dei rischi residui da parte della governance aziendale. Le misure più importanti sono pertanto sempre quelle organizzative, che, come sancito dal Codice dell'Amministrazione Digitale[24], nel caso dell'adozione del BYOD nella Pubblica Amministrazione sono addirittura obbligatorie.
È necessario, prima di autorizzare l'uso del BYOD, coinvolgere "*tempestivamente e adeguatamente*"[25] il DPO[26] e redigere un apposito Data Protection Impact Assessment (DPIA)[27] [28], talvolta in letteratura specificato come BYOD Impact Assessment (BIA)[29], andando ad individuare le misure di sicurezza adeguate a minimizzare il rischio specifico senza al contempo invadere la privacy dei dipendenti con ingiustificati trattamenti dei loro dati personali.
Il primo aspetto da analizzare è se il BYOD rappresenti una soluzione provvisoria (come ad esempio nel caso dell'improvviso *lock down* dei tempi del COVID) o di lungo termine[30]. Le soluzioni emergenziali vengono implementate per motivi di necessità, in deroga ad importanti principi di sicurezza e possono diventare rapidamente implementazioni a lungo termine non adatte allo scopo e difficili da rimuovere, soprattutto se utilizzate da un ampio volume di personale. All'opposto, le pratiche a lungo termine richiederanno approfondite analisi iniziali ed una revisione regolare. "N*on c'è nulla di più definitivo del provvisorio e nulla di più provvisorio del definitivo*"[31].
La misura organizzativa più importante è il censimento degli apparati BYOD (SIM e account personali compresi) con la loro preventiva autorizzazione alla connessione ai sistemi aziendali, la verifica periodica delle misure di sicurezza in essi implementate[32] [33] [34] e delle licenze del software installato[35]. Applicando il principio di *accoutability*, oltre ai vantaggi è opportuno effettuare una adeguata valutazione dei rischi connessi all'applicazione del BYOD sulla base delle diverse tipologie di dipendenti coinvolti[36], delle diffe-

21 Device Security Guidance https://www.ncsc.gov.uk/collection/device-security-guidance

22 End User Devices Security and Configuration Guidance https://www.gov.uk/government/collections/end-user-devices-security-guidance

23 Bring Your Own Device Guidance https://www.gov.uk/government/collections/bring-your-own-device-guidance

24 Codice dell'amministrazione digitale. (CAD) d.lgs 7 marzo 2005, n. 82 - Art. 12.3-bis. I soggetti di cui all'articolo 2, comma 2, favoriscono l'uso da parte dei lavoratori di dispositivi elettronici personali o, se di proprietà dei predetti soggetti, personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo. In caso di uso di dispositivi elettronici personali, i soggetti di cui all'articolo 2, comma 2, nel rispetto della disciplina in materia di trattamento dei dati personali, adottano ogni misura atta a garantire la sicurezza e la protezione delle informazioni e dei dati, tenendo conto delle migliori pratiche e degli standard nazionali, europei e internazionali per la protezione delle proprie reti, nonché ((a condizione che sia data al lavoratore adeguata informazione)) sull'uso sicuro dei dispositivi, anche attraverso la diffusione di apposite linee guida, e disciplinando, tra l'altro l'uso di webcam e microfoni ((, previa informazione alle organizzazioni sindacali)).

25 GDPR 38.1 - Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

26 EDPS Mobile devices guidelines – III. Recommendations – 18 – R1 devices in the EU institutions.

27 EDPS Mobile devices guidelines – III. Recommendations – 18 – R2-R5, R7.

28 GPDP Valutazione d'impatto della protezione dei dati (DPIA) https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-

29 BYOD, necessario gestire e pianificare l'uso dei dispositivi per mettersi in salvo https://www.federprivacy.org/strumenti/accesso-ristretto/byod-necessario-gestire-e-pianificare-l-uso-dei-dispositivi-per-mettersi-in-salvo

30 NCSC - Is BYOD intended to be an interim or long-term solution? https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-1-determine-your-objectives

31 Giuseppe Prezzolini

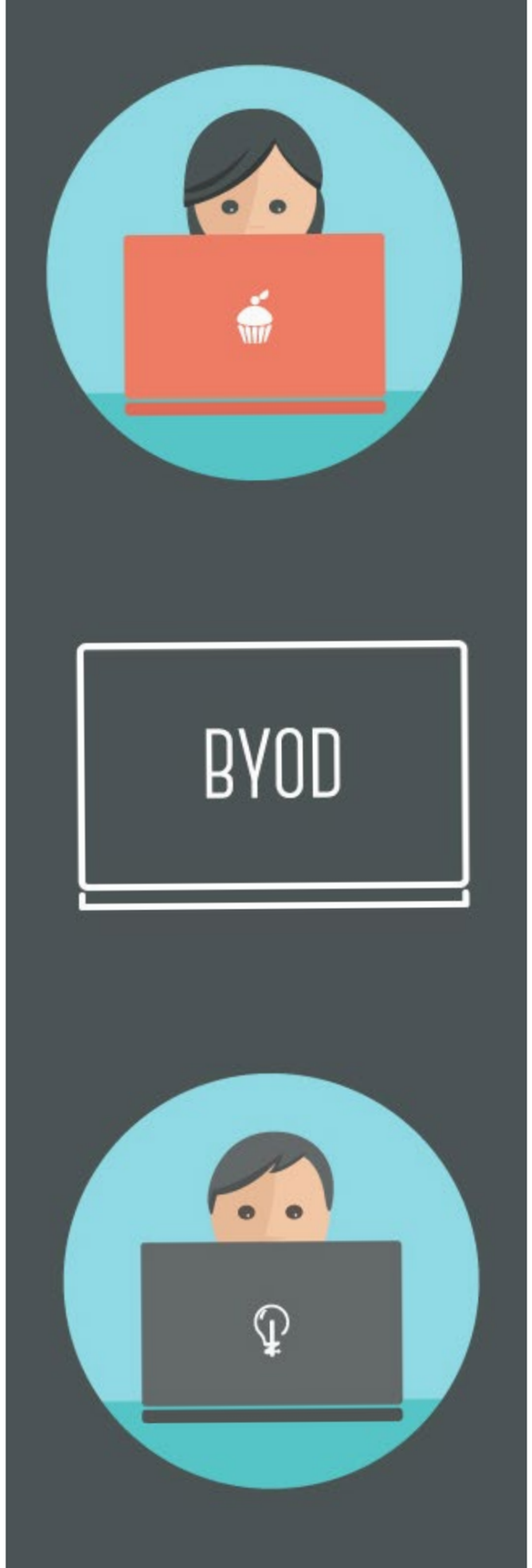
32 EDPS Mobile devices guidelines - IV.1.1.Life-cycle management of the mobile device

33 BYOD: quelles sont les bonnes pratiques ? https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques

34 Vedi anche linee guida ICO

35 ISO/IEC 27002 6.2.2 Teleworking i) software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees or external party users;

36 EDPS Mobile devices guidelines - VI. Risks for personal data processed by mobile devices



renti tipologie di dispositivi utilizzati, delle reali casistiche d'utilizzo e dei dati personali accessibili da tali dispositivi[37] [38]. Dovranno poi essere aggiornate le opportune policy aziendali di utilizzo, il cui mancato rispetto comporta sanzione disciplinare per il lavoratore. Saranno pertanto adeguati il "*Regolamento sul corretto uso dei sistemi informativi aziendali*", le procedure interne sullo smaltimento dei dispositivi aziendali, di off-boarding[39] [40] [41] e di Data Breach[42] [43] [44]. Nel caso in cui vi siano copie locali di dati personali su dispositivi BYOD è necessario aggiornare le procedure di risposta alle istanze degli interessati (es: rettifica, blocco o cancellazione) in modo da comprendere anche questa casistica[45]. Questi regolamenti dovranno essere modificati nel corso del tempo a seconda degli effettivi casi d'uso e delle relative criticità emerse[46], come dimostra il recente caso di spionaggio mediante TikTok[47] [48] [49] e la conseguente decisione della Commissione Europea[50] di vietarne l'istallazione su dispositivi aziendali e BYOD (è dibattito corrente se vietarlo anche all'interno della Pubblica Amministrazione italiana[51]). Conseguentemente, bisognerà procedere alla redazione di apposite istruzioni per i soggetti autorizzati e alla loro sensibilizzazione attraverso l'aggiornamento dei piani di formazione[52]. Gli utenti spesso infatti non sono consapevoli che l'utilizzo dei BYOD può comportare un trattamento di dati personali (di cui il datore di lavoro è titolare e conseguentemente soggetto ai dettami e alle sanzioni del GDPR) anche da parte di soggetti terzi fornitori di servizi, siano essi servizi cloud (magari con trasferimento all'estero dei dati), o riparatori locali troppo curiosi[53].

Le misure organizzative, tenuto in debito conto il fattore umano, dovranno al loro interno prevedere anche adeguate misure tecniche.

Politiche e procedure per il trasferimento delle informazioni

I titolari del trattamento dovrebbero mettere in atto politiche, procedure e controlli per proteggere il trasferimento delle informazioni da e verso i dispositivi utilizzati dai dipendenti, soprattutto se BYOD, facendo proprie le indicazioni delle linee guida ICO, i punti di controllo della norma ISO/IEC 27001[54] [55] [56] [57] e le linee guida del CNIL[58].

Nel rispetto del principio di minimizzazione, è opportuno progettare l'infrastruttura tecnologica al fine di evitare o ridurre quanto possibile la memorizzazione dei dati nei dispositivi BYOD. Ad esempio, le informazioni accessibili da tali dispositivi potrebbero by design essere memorizzate solo online, mediante l'utilizzo di webapp, webmail o sistemi documentali cloud[59] , quali Office 365 o Google G Suite Business. In varie aziende i PC portatili personali sono utilizzati solo per il collegamento in mobilità mediante Virtual Private Network (VPN) e Remote Desktop Protocol (RDP)[60] ai PC fissi aziendali, con disabilitazione della copia dei dati tra PC remoto e PC locale. In questo modo lo smarrimento di un dispositivo o le dimissioni del dipendente comportano rischi inferiori, oltre a garantire un certo grado di sicurezza anche in caso di utilizzo di connessioni WiFi non affidabili[61].

Il rischio residuo è una esfiltrazione di dati mediante fotografia dello schermo. È un caso estremo, ma verificatosi realmente nei Paesi Bassi, dove due persone sono state arrestate per aver venduto dati esfiltrati in siffatto modo dai sistemi del Ministero della Salute[62].

Un'ulteriore soluzione potrebbe essere l'adozione di un sistema di Cloud Access Security Brokers (CASB)[63]. È simile ad una VPN, ma è gestito da una terza parte in grado di filtrare e controllare tutto il traffico in entrata ed in uscita da un dispositivo (anche quello personale), verificando così che non vi siano esfiltrazioni di dati, accessi non consentiti o attacchi man-in-the-middle in corso. Le soluzioni CASB verificano anche l'utilizzo non autorizzato di piattaforme cloud di storage di dati (es: Google Drive).

In molti casi le aziende non possono fidarsi del comportamento dei propri dipendenti e degli apparati connessi alla rete. È la conclusione alla quale è giunta il Dipartimento della Difesa degli Stati Uniti che nel 2022 ha pubblicato "*The DoD Zero Trust Strategy*"[64]. "Zero trust" (Fiducia Zero) è un modello di sicurezza basato sulla convinzione che la fiducia implicita sia sempre una vulnerabilità. La sicurezza viene progettata col principio di "non fidarsi mai, verificare sempre" adottando microperimetri di contenimento attorno ad ogni apparato per oltrepassare i quali gli utenti e i client devono dimostrare la propria affidabilità in modo continuo nel tempo, ad esempio me-

37 *Vedi anche linee guida ICO*

38 *NCSC What tasks will employees be permitted or encouraged to do from their own devices? What will they not be permitted to do? https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-2-develop-the-policy*

39 *ISO/IEC 21964 con titolo "Destruction of data carriers")*

40 *GPDP Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008 [1571514] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1571514*

41 *Vedi anche linee guida ICO*

42 *EDPS Mobile devices guidelines – III. Recommendations – 18 – R6; IV.1.5. Security breaches/security incidents*

43 *GPDP Violazioni di dati personali (data breach) in base alle previsioni del Regolamento (UE) 2016/679 https://www.garanteprivacy.it/regolamentoue/databreach*

44 *Vedi anche linee guida ICO*

45 *EDPS Mobile devices guidelines – III. Recommendations – 18 – R8.*

46 *NCSC Increased reliance on procedural controls https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-3-understand-additional-costs-and-implications*

47 *EXCLUSIVE: TikTok Spied On Forbes Journalists https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=1a74b0197da5*

48 *Can TikTok convince the world it is not a tool for China? https://www.ft.com/content/c8903308-4da1-4a13-a50a-fe96bbf9b5a2*

49 *TikTok ammette: app utilizzata per spiare i giornalisti https://www.corrierecomunicazioni.it/privacy/tiktok-ammette-app-utilizzata-per-spiare-i-giornalisti/*

50 *Commission strengthens cybersecurity and suspends the use of TikTok on its corporate devices https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1161*

51 *TikTok, il governo apre il dossier. Zangrillo: "Tra le opzioni c'è il blocco per i dipendenti pubblici". No di Salvini: "Niente censure" https://www.repubblica.it/politica/2023/02/25/news/tiktok_vietato_nel_pubblico_proposta_zangrillo-389482367/*

52 *EDPS Mobile devices guidelines - IV.1.3.Training*

53 *No Privacy in the Electronics Repair Industry https://arxiv.org/abs/2211.05824*

54 *ISO/IEC 27002 6.2.2 Teleworking c) the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system*

55 *ISO/IEC 27002 6.2.2 Teleworking f) the use of home networks and requirements or restrictions on the configuration of wireless network services;*

56 *ISO/IEC 27002 13.2.1 Information transfer policies and procedures*

57 *ISO/IEC 27002 13.2.3 Electronic messaging*

58 *BYOD: quelles sont les bonnes pratiques ? https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques*

59 *NCSC Web browsers https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-4-deployment-approaches https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-5-put-technical-controls-in-place#section_2*

60 *NCSC Virtual Desktop Infrastructure (VDI)/Remote Desktop/Remote Apps https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-4-deployment-approaches*

61 *EDPS Mobile devices guidelines - IV.2.2.Other technical measures – T9*

62 *Dutch Insider Attack on COVID-19 Data https://www.schneier.com/blog/archives/2021/01/dutch-insider-attack-on-covid-19-data.html*

63 *Mitigare i rischi di sicurezza nel Cloud pubblico con i Cloud Access Security Brokers (CASB) https://www.ictsecuritymagazine.com/articoli/mitigare-rischi-sicurezza-nel-cloud-pubblico-cloud-access-security-brokers-casb/*

64 *https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf*

diante l'autenticazione a due fattori, con un certificato digitale[65] o una smart card.

Dal Mobile Device Management (MDM) all'Unified Endpoint Management (UEM)

Gli strumenti di Mobile Device Management (MDM) sono software di proprietà di terze parti che, installati su uno smartphone, ne consentono la gestione amministrativa in modalità remoto. Possono essere utilizzati per monitorare e controllare l'utilizzo dei dispositivi mobili dei dipendenti in modo da garantire che se ne compia un uso appropriato e sicuro. Un ausilio alla corretta configurazione di un MDM può provenire dalla lista dei controlli previsti dalla norma ISO/IEC 27001[66] e dalle linee guida ICO[67], NCSC[68] [69], EDPS[70] e CLUSIT [71]. Un MDM può aiutare ad incrementare il livello di sicurezza dei dati imponendo ad esempio la crittografia del dispositivo[72], l'attivazione del Personal Identification Number (PIN)[73], il blocco automatico del dispositivo[74] o l'installazione automatica degli aggiornamenti di sistema e delle app installate[75]. In merito a queste ultime, può essere redatta la white list delle App installabili al di fuori della quale il dipendente dovrà chiedere l'autorizzazione all'installazione, in modo similare ai sistemi di parental control sugli smartphone dei minorenni. In caso di furto o smarrimento, consentono di rendere inaccessibile il dispositivo e di cancellarne i contenuti. La gestione remotizzata del backup[76] del dispositivo consente la continuità operativa. Normalmente questi strumenti vengono installati sui dispositivi aziendali, ma, previa autorizzazione del lavoratore, possono tecnicamente essere installati anche su quelli personali. Si potrebbero quindi utilizzare soluzioni di protezione supplementari quali il "*sandboxing*"[77] [78] [79], che prevede la conservazione dei dati non lavorativi in un'area specifica, con specifici criteri di salvaguardia, o viceversa un sistema di Mobile Application Management (MAM)[80] dove il dipendente gestisce tutti gli aspetti del dispositivo, ad eccezione delle applicazioni di lavoro che vengono conservate in un contenitore sul dispositivo e gestite dall'organizzazione. "*Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device), sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l´area di memoria dedicata all´applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l´azione di eventuali agenti malevoli (malware)*"[81].

Per l'ipotesi di PC portatili, una soluzione potrebbe essere quella di fornire al dipendente un supporto esterno di avvio, in genere una chiavetta USB, in modo da gestire l'apparato in modalità diverse a seconda del tipo di utilizzo, personale o lavorativo. La versione lavorativa potrebbe poi essere gestita aziendalmente[82].

L'adozione di uno strumento quale Windows Server Update Services (WSUS) consente agli amministratori IT di gestire la distribuzione degli aggiornamenti disponibili in Microsoft Update nei computer connessi, garantendone così la sicurezza.

Il massimo della gestione si raggiunge con l'Unified Endpoint Management (UEM), evoluzione del MDM, una classe di strumenti software[83] che fornisce un'unica interfaccia di gestione per tutte le tipologie di endpoint, quali ad esempio smartphone (iOS e Android), PC fissi e portatili (Windows, MAC e Linux), stampanti, dispositivi IoT e dispositivi indossabili. Oltre a verificare l'aggiornamento del Sistema operativo, questi sistemi consentono di verificare quali pacchetti software sono installati in ogni dispositivo e di gestirne da remoto l'installazione, l'aggiornamento o la rimozione, Per contrastare attacchi man-in-the-middle, possono essere disabilitate o limitate nell'uso le varie interfacce di connessione quali Near Field Communication (NFC), WiFi e Bluetooth[84] [85].

WhatsApp – verifica in due passaggi

WhatsApp ha *de facto* sostituito nell'immaginario collettivo l'utilizzo degli SMS, divenendo un insostituibile strumento di comunicazione, anche di dati sanitari[86] [87]. Conseguentemente è divenuto obiettivo di attacchi informatici ed involontari data breach. Come noto, WhatsApp più che uno strumento di messaggistica è un mezzo di profilazione pubblicitaria di massa attuato da una società privata statunitense soggetta all'*Executive Order 12333*[88] e al *FISA Foreign Intelligence Surveillance Act*[89]. Indipendentemente dalle riflessioni in punto privacy sull'opportunità o meno del suo utilizzo, il suo grado di penetrazione di mercato obbliga perlomeno all'implementazione di alcune basiche misure di sicurezza. In particolare, meritano una menzione specifica i rischi connessi alla mancata adozione della verifica in due passaggi.

Il primo rischio è quello del furto dell'identità da parte di soggetti criminali. Potrebbe capitare di ricevere un messaggio da un proprio contatto, anche tra le persone strette, del seguente tenore: "*Ciao, ti ho inviato un codice per sbaglio, potresti rimandarmelo?*". La truffa sfrutta il meccanismo di WhatsApp che permette di trasferire l'account su di un nuovo dispositivo. Normalmente la procedura è attuata dal legit-

65 *EDPS Mobile devices guidelines - IV.2.2.Other technical measures – T8*

66 *ISO/IEC 27002 6.2.1 Mobile device policy*

67 *ICO - Bring your own device (BYOD) punti 30) e 31).*

68 *NCSC Mobile Device Management (MDM) https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-4-deployment-approaches*

69 *NCSC Mobile Device Management https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/mobile-device-management*

70 *EDPS Mobile devices guidelines - IV.2.1.Mobile device management ("MDM")*

71 *Mobile e Privacy https://privacycloudmobile.clusit.it/index.php*

72 *EDPS Mobile devices guidelines - IV.2.2.Other technical measures - T2*

73 *EDPS Mobile devices guidelines - IV.2.2.Other technical measures - T4*

74 *EDPS Mobile devices guidelines - IV.2.2.Other technical measures - T6*

75 *EDPS Mobile devices guidelines - IV.2.2.Other technical measures - T7*

76 *EDPS Mobile devices guidelines - IV.2.2.Other technical measures - T3*

77 *Cfr ICO - Bring your own device (BYOD) punto 22)*

78 *Opinion 2/2017 on data processing at work - wp249 - 5.4.2 BRING YOUR OWN DEVICE (BYOD) - https://ec.europa.eu/newsroom/article29/items/610169*

79 *EDPS Mobile devices guidelines - IV.2.2.Other technical measures - T1*

80 *NCSC Mobile Application Management (MAM) https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-4-deployment-approaches*

81 *GPDP Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3556992*

82 *NCSC Bootable OS https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device/action-4-deployment-approaches*

83 *Gartner - Unified Endpoint Management Tools Reviews and Ratings https://www.gartner.com/reviews/market/unified-endpoint-management-tools*

84 *Cfr ICO - Bring your own device (BYOD) punto 26)*

85 *EDPS Mobile devices guidelines - IV.2.2.Other technical measures - T5*

86 *Whatsapp è diventato uno strumento di lavoro del medico. Il 50% lo usa per ricette e consigli http://www.quotidianosanita.it/toscana/articolo.php?articolo_id=111198*

87 *La Messaggistica Istantanea nell'esercizio della Professione Medica. Presentazione della survey OMCeO Firenze sui propri iscritti https://www.ordine-medici-firenze.it/formazione/eventi/promossi-dall-ordine/516-consenso-informato-e-disposizioni-anticipate-di-trattamento-2*

88 *Executive Order 12333--United States intelligence activities https://www.archives.gov/federal-register/codification/executive-order/12333.html*

89 *The Foreign Intelligence Surveillance Act of 1978 (FISA) https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286*

timo proprietario, mentre in questo caso è attivata da un criminale informatico[90]. Una volta in possesso dell'SMS col codice di 6 cifre, l'attaccante è in grado di impossessarsi del profilo WhatsApp della vittima[91]. Non vedrà i contenuti delle chat antecedenti al furto dell'identità digitale, ma potrà vedere l'elenco dei contatti, i gruppi, i messaggi da quel momento in poi ed usarli per propagare la truffa. Preso il controllo di un account, in genere l'attaccante richiede a parenti ed amici il loro numero di carta di credito con la scusa di piccoli acquisti emergenziali. "*Oggi è il compleanno di Matteo. Ho preso un regalo da Internet ma la mia carta di credito è scaduta. Posso usare la tua e ti faccio un bonifico oppure in contanti se preferisci. Spendo 125 euro. La posso usare?*"[92] Con un minimo di ingegneria sociale incrociata con le informazioni presenti su LinkedIn ed altri social network, l'attaccante cercherà di ottenere anche i numeri delle carte aziendali. In questi casi è importante contattare subito telefonicamente il malcapitato per comunicargli la violazione suggerendogli di avvisare tutti i suoi contatti.

Un secondo scenario è quello del cambio di numero telefonico. Dato che riutilizzare le numerazioni è una prassi piuttosto comune per gli operatori di telefonia mobile, è possibile che il nuovo proprietario dell'utenza, loggandosi per la prima volta su WhatsApp, acceda alla lista di contatti del precedente proprietario. Questo è un problema noto da tempo[93], tanto che WhatsApp disabilita i profili non usati per più di 45 giorni[94]. La misura non è purtroppo sempre efficace in quanto molte persone per non perdere tutti i contatti e i gruppi ai quali si sono iscritti[95] [96] utilizzano sulla nuova linea telefonica il profilo WhatsApp appoggiato alla numerazione precedente.

Per entrambi gli scenari la misura di sicurezza è quella di attivare preventivamente la verifica in due passaggi di WhatsApp[97], in modo che il profilo non possa essere trasferito senza la conoscenza dell'ulteriore codice segreto. Tra l'altro questa misura di sicurezza viene sempre subito attivata dai criminali informatici che si impossessano di profili altrui, impedendone così il reimpossesso e lasciando come unica soluzione la non rapida disattivazione del profilo[98].

Nello scenario del cambio di numerazione telefonica, la misura di sicurezza è la disattivazione del profilo.

Misure similari dovrebbero essere attuate in qualunque piattaforma di messaggistica, ove disponibili.

COPE, CYOD e COBO

Per mitigare o rimuovere i rischi del BYOD vi sono varie soluzioni organizzative alternative.

Con il Company-Owned, Personally-Enabled (COPE) i dispositivi sono di proprietà e gestiti dall'azienda (la quale può quindi adottare tutte le restrizioni e misure di sicurezza che reputa opportune) e i dipendenti hanno la facoltà di utilizzarli per scopi personali ben delineati. In genere è una politica adottata nel caso degli smartphone. In questo caso l'Azienda può mantenere un controllo più stretto sul livello di sicurezza dell'apparato, installarci senza problemi un MDM/UEM e gestire con meno difficoltà l'integrazione con l'ecosistema aziendale. Può essere ristretto il numero e la tipologia di app scaricabili, evitando il rischio di utilizzi non appropriati di sistemi cloud che potrebbero causare esfiltrazione di dati. Viene lasciato spesso libero l'utilizzo per scopi personali del traffico voce e della messaggistica.

Il Choose Your Own Device (CYOD) è invece un programma di gestione dei dispositivi mobili che consente ai dipendenti di accedere a una scelta limitata di dispositivi approvati per il lavoro dell'azienda, che ne sostiene il costo di acquisto, e di utilizzarli come se fossero BYOD. In questo modo l'azienda ha la certezza che i dispositivi di per sé superino i livelli minimi di sicurezza e il lavoratore ha maggiore flessibilità nel loro utilizzo. COPE CYOD possono essere considerate lecite anche alla luce delle "*linee guida del Garante per posta elettronica e internet*"[99] del 2007. Queste non contemplavano ancora il concetto di BYOD, ma ipotizzavano già che potessero esservi "*usi moderati di strumenti per finalità private*" e che il datore di lavoro potesse valutare "*la possibilità di attribuire al lavoratore un diverso indirizzo [email] destinato ad uso privato*".

L'opposto del BYOD è il Corporate Owned Business Only (COBO), che mediante la completa segregazione tra la sfera aziendale e quella privata permette al dipartimento IT di tenere sotto controllo la maggior parte dei rischi. In questo scenario i dispositivi sono di proprietà del Titolare del Trattamento e i dipendenti possono utilizzarli esclusivamente per gli scopi lavorativi autorizzati, senza possibilità di modificare le impostazioni di base. Se soggetti a specifiche normative di certificazione aziendale, è l'unica soluzione adottabile. In taluni casi i regolamenti aziendali vietano persino di portare dispositivi personali in alcune aree aziendali (si pensi ad esempio agli archivi cartacei vigilati delle aziende che si occupano di conservazione sostitutiva).

I rischi per i lavoratori

Nell'imporre un modello organizzativo e le relative misure di sicurezza, il datore di lavoro dovrà tenere conto anche dei rischi per le libertà dei dipendenti, nonché il rispetto del novellato art. 4 dello Statuto dei lavoratori, che andrà considerato anche nella redazione della DPIA.

Il semplice utilizzo di dispositivi BYOD, COPE, CYOD o COBO e la loro interconnessione agli apparati aziendali comporta automaticamente per il datore di lavoro un trattamento di dati personali del dipendente (ad esempio nei log di rete) e delle persone con le quali è entrato in contatto, anche per motivi personali. Tali trattamenti dovranno essere specificati nell'apposita sezione dell'informativa ai lavoratori[100].

Il controllo dei dispositivi mediante CASB, MDM o UEM è sicuramente molto invasivo e nel caso di BYOD anche limitante rispetto alla sperimentazione e alla competizione interna alla base della sua giustificazione filosofica. "*Il monitoraggio dell'ubicazione e del traffico di tali dispositivi può essere considerato rientrare nel legittimo interesse di proteggere i dati personali per i quali il datore di lavoro è responsabile in qualità di titolare del trattamento; tuttavia potrebbe essere illecito quando riguarda un dispositivo personale di un dipen-*

90 *Ho ricevuto il codice di verifica senza averlo richiesto https://faq.whatsapp.com/479314433984258/?helpref=hc_fnav&locale=it_IT*

91 *Furto dell'account https://faq.whatsapp.com/1131652977717250/?helpref=hc_fnav&locale=it_IT*

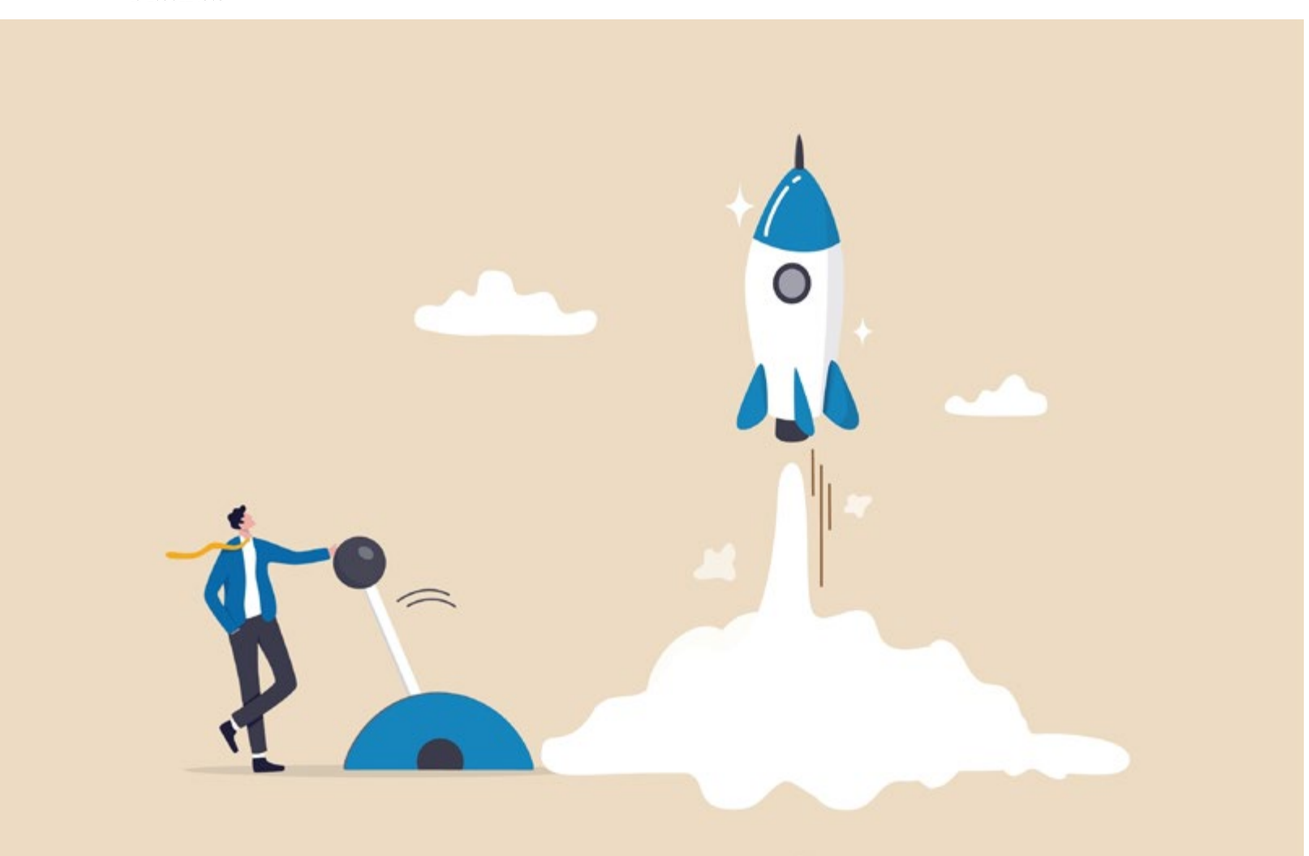
92 *Messaggio reale. Era veramente il compleanno di Matteo.*

93 *How I Accidentally Hijacked Someone's WhatsApp https://www.vice.com/en/article/bv8mqd/how-i-hacked-whatsapp-account*

94 *Se il tuo numero di telefono è già su WhatsApp https://faq.whatsapp.com/3347469605523961?cms_id=3347469605523961*

95 *Accidental WhatsApp account takeovers? It's a thing https://www.theregister.com/2023/02/21/accidental_whatsapp_account_takeover/*

96 *WhatsApp Has a Years-Old Security Problem. Here's How to Solve It. https://gizmodo.com/whatsapp-new-phone-number-account-problem-group-chats-1850124309*



97 *Come gestire le impostazioni della verifica in due passaggi https://faq.whatsapp.com/1920866721452534?helpref=faq_content*

98 *Telefono rubato o smarrito https://faq.whatsapp.com/1007324800132703/?locale=it_IT*

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

100 *EDPS Mobile devices guidelines - 67*

dente e permette di acquisire anche dati relativi alla vita privata e familiare del dipendente"[101]. "*I dipendenti i cui dispositivi sono inseriti in tali servizi di gestione dei dispositivi mobili devono essere pienamente informati sul tipo di tracciamento attuato e sulle sue conseguenze nei loro confronti*" [102].

Con riferimento al lavoro da remoto la normativa ISO/IEC 27001 prevede un apposito controllo, specificando quali misure di sicurezza debbano essere previste all'interno delle policy aziendali[103]. Trova piena applicazione alle politiche di BYOD in quanto è soprattutto in questo caso che i dipendenti utilizzano strumenti personali per finalità lavorative. Fra i controlli presenti vi è anche la definizione degli orari di lavoro[104], concetto già presente ovviamente in consolidata normativa giuslavorista e di antica cogenza: "*Ricordati del giorno di sabato per santificarlo: sei giorni faticherai e farai ogni tuo lavoro; ma il settimo giorno è il sabato (..)*"[105]. È però esperienza comune che durante il lock down la barriera tra la sfera privata e quella professionale si sia in molti casi infranta. Questa situazione, peggiorata ed amplificata dalle politiche di BYOD emergenziali, ha portato alla sbagliata abitudine, in molti casi perdurante ancora oggi, di controllare la posta elettronica anche durante il proprio tempo libero e, spesso, di rispondere anche in assenza di urgenza specifica. "Always on", essere sempre connessi, non è salutare per il lavoratore. Comporta sicuramente per l'azienda vantaggi nel breve periodo ma svantaggi per tutti su quello lungo. La prassi si è così estesa da spingere il Legislatore ad introdurre il concetto di "obbligo di disconnessione"[106] [107], la possibilità per i lavoratori di staccarsi completamente dal lavoro al termine della giornata lavorativa, "*senza cui si rischia di vanificare la necessaria distinzione tra spazi di vita privata e attività lavorativa, annullando così alcune tra le più antiche conquiste raggiunte per il lavoro tradizionale*"[108]. Il concetto alla base di questo nuovo obbligo è la necessità che "*tutte le persone abbiano la possibilità di disconnettersi e godano di garanzie per l'equilibrio tra vita professionale e vita privata in un ambiente digitale*"[109]. Il benessere psico-fisico dei lavoratori deve essere garantito mediante un lavoro sano e sostenibile e evitando il rischio di burnout (stress lavoro-correlato), vale a dire il collasso fisico e mentale dei lavoratori a causa di un eccessivo carico di lavoro, secondo l'OMS seconda causa più comune di malattie lavorative, dopo i disturbi muscolo-scheletrici. Una buona politica BYOD deve tenere in considerazione anche questo rischio aziendale ed attuare le opportune policy di contromisura.

Conclusioni

Non è possibile offrire una risposta univoca in merito all'opportunità dell'adozione del BYOD. In alcuni casi potrebbe risultare assolutamente sconsigliabile mentre in altri potrebbe rappresentare la soluzione, se ben regolamentata. Come visto è una politica con pro e contro. Come è errato criminalizzarla a priori, pare altrettanto sbagliato abbracciarla solo perché "va di moda" o adottata da aziende di successo. Bisogna sicuramente evitare l'adozione di policy prestampate, anche se ottimamente redatte[110], in quanto ogni regolamento deve essere *taylor made*: va valutato, adattato e aggiornato nel tempo per tenere conto dei cambiamenti tecnologici, del livello di alfabetizzazione informatica dei dipendenti e delle peculiari esigenze e criticità aziendali. Vale, come per tutte le tematiche di privacy e di sicurezza delle informazioni, il vecchio adagio "*an ounce of prevention is worth a pound of cure*"[111].

101 *Opinion 2/2017 on data processing at work - wp249- 5.4.2 BRING YOUR OWN DEVICE (BYOD) - https://ec.europa.eu/newsroom/article29/items/610169*

102 *Opinion 2/2017 on data processing at work - wp249- 5.4.3 GESTIONE DEI DISPOSITIVI MOBILI (MOBILE DEVICE MANAGEMENT) - https://ec.europa.eu/newsroom/article29/items/610169*

103 *ISO/IEC 27002 6.2.2 Teleworking*

104 *ISO/IEC 27002 6.2.2 Teleworking (..) The guidelines and arrangements to be considered should include: (..) b) (..) the hours of work(..)*

105 *Esodo, 20:8-10*

106 *L. 22 maggio 2017, n. 81*

107 *DL n. 30 del 13 marzo 2021*

108 *GPDP Audizione del Presidente del Garante per la protezione dei dati personali sull'affare assegnato atto n. 453 relativo al tema di Ricadute occupazionali dell'epidemia da Covid-19, azioni idonee a fronteggiare le situazioni di crisi e necessità di garantire la sicurezza sanitaria nei luoghi di lavoro - 13 maggio 2020 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9341993*

109 *Dichiarazione europea https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52022DC0028&from=EN sui diritti e i principi digitali per il decennio digitale*

110 *A titolo meramente esemplificativo: BYOD policy (Bring your own device)- ISO27001 https://iso-docs.com/products/byod-policy-bring-your-own-device-iso27001*

111 *Benjamin Franklin, Pennsylvania Gazette 04/02/1735, criticando lo stato del servizio antincendio della città di Philadelphia.*

Il trattamento dei dati nella mobilità autonoma e connessa: alla ricerca di basi condivise

di Filippo Zemignani

La trasformazione tecnologica in atto

Anche i meno avvezzi a confrontarsi con i ritrovati tecnologici che equipaggiano i veicoli di più recente concezione non avranno difficoltà a riconoscere che il settore *automotive*, nell'ultimo decennio, ha intrapreso un percorso di profonda trasformazione, capace di ridefinire completamente – se non qui ed ora, perlomeno sul lungo periodo – l'esperienza di bordo dell'automobilista.

Sono tre gli ambiti che possiamo individuare quali sintomatici di questa evoluzione. In primo luogo, le istanze di contenimento dell'impatto ambientale hanno incentivato la transizione a tappe forzate verso la propulsione elettrica, costringendo il conducente non solo a prendere maggiore consapevolezza dell'impronta ecologica degli spostamenti, ma anche a mutare l'approccio alla pianificazione dei viaggi e al rifornimento (*rectius*, alla ricarica) del veicolo.

In seconda battuta, il diffondersi di sempre più sofisticati sistemi di *infotainment*, spesso progettati per integrarsi con gli *smartphone*, ha trasformato le plance delle automobili in veri e propri computer, capaci di aumentare sia il livello di informazioni di cui può disporre il conducente – pensiamo al meteo, al traffico, allo stato di pressione degli pneumatici: gli esempi sono molteplici – che le opzioni di intrattenimento di cui possono godere i passeggeri.

Da ultimo, la vena tecnologica della vettura moderna si concretizza non solo nella capacità di connettersi ad internet o di dialogare con altri *device*, ma anche e soprattutto nella presenza di numerosi dispositivi di assistenza alla guida in grado di controllare autonomamente direzione e velocità del veicolo. Questi dispositivi, noti con l'acronimo di ADAS (*Advanced Driver Assistance Systems*), coadiuvano il conducente – talvolta su sua esplicita richiesta, talaltra con interventi automatici al manifestarsi di situazioni di pericolo – nelle operazioni di marcia, con il duplice obiettivo di aumentare tanto la sicurezza quanto il confort di bordo.

Non si tratta – sebbene i fraintendimenti siano frequenti, anche tra gli addetti ai lavori[1] – di sistemi di guida autonoma: il conducente non è mai rimpiazzato dal sistema, bensì meramente affiancato dallo stesso. Tuttavia, gli ADAS stanno lentamente abituando l'uomo a concedere alla tecnologia spazi di intervento sempre maggiore, in un contesto – quello della conduzione di un veicolo – che fino a pochi anni orsono era del tutto manuale e meccanico.

Sono i prodromi di quella rivoluzione *driverless* che, più volte impropriamente annunciata come imminente, ha iniziato negli ultimissimi anni a fare timidamente capolino nei listini di alcune case automobilistiche, seppur solamente in pochi selezionati mercati (tra i quali, al momento, non è incluso quello italiano)[2].

1 L'esempio più eclatante riguarda, come sarà noto, il sistema Autopilot dei veicoli prodotti da Tesla, spesso spacciato dai mezzi di informazione per un vero e proprio sistema di guida autonoma, quando invero è un semplice – seppur avanzato – sistema ADAS.

2 A partire dall'aprile 2021, Honda Motor Co. ha iniziato la vendita, in serie limitata, di una versione della sua ammiraglia Legend dotata di sistema di guida autonoma di livello 3. Ad oggi, il sistema è stato omologato solo in Giappone. Similmente, a partire dall'estate del 2022 Mercedes-Benz ha avviato la commercializzazione, su un numero limitato di modelli di alta gamma, di un analogo sistema, dopo aver ottenuto in patria l'omologazione. Nei primi mesi del 2023, la casa tedesca ha iniziato a chiedere (ed ottenere) l'omologazione anche in alcuni stati federati statunitensi.

Il tema della responsabilità da circolazione di veicoli a guida autonoma è stato ampiamente sviscerato in dottrina, rappresentando chiaramente l'interrogativo più pressante in vista di una possibile transizione verso una mobilità dominata da questa tipologia di mezzi: non meno importanza riveste tuttavia il tema del trattamento dei dati, dal momento che l'enorme mole di informazioni che tali mezzi raccolgono – e ancor più raccoglieranno, se effettivamente giungeranno a piane maturazione le tecnologie di guida autonoma – può ingenerare preoccupazioni in relazione alla loro conservazione, circolazione e sfruttamento economico.

L'interconnessione V2X come volano della mobilità del futuro

La premessa è d'obbligo: un sistema di guida autonoma non può operare se non per il tramite di una vasta, pervasiva e costante opera di raccolta, scambio e analisi di dati provenienti dall'interno e dall'esterno del veicolo.

L'automobile raccoglie, semplicemente osservando la realtà che la circonda per il tramite dell'*hardware* di cui è equipaggiata, un cospicuo quantitativo di informazioni: telecamere, sensori, GPS e LiDAR registrano la posizione del veicolo, le condizioni del meteo, la distanza dagli oggetti circostanti e i loro movimenti, fornendo al *software* le coordinate più rilevanti affinché possa orientarsi nello spazio.

Se l'obiettivo futuro è quello di realizzare in pienezza la filosofia *driverless*, tuttavia, i tecnici del settore sono sostanzialmente concordi nel ritenere che l'automobile dovrà andare oltre questa raccolta ed elaborazione interna di dati provenienti da sensori e camere. La *self-driving car* si appresta infatti a diventare l'ennesima pedina nel mosaico dell'*Internet of Things* (IoT): l'interazione con altri veicoli, infrastrutture *smart* e singoli *device* permetterebbe infatti al *software* di acquisire un numero di informazioni infinitamente superiore, mediante le quali migliorare la sicurezza della circolazione e sviluppare soluzioni di trasporto non implementabili quando i singoli veicoli si comportano come monadi. Si pensi alla tecnologia del *platooning*, ove l'interconnessione tra veicoli e infrastruttura consente di far viaggiare lunghe file di vetture – e soprattutto, di mezzi pesanti deputati al trasporto merci – delegando il controllo solo al primo veicolo del convoglio; si pensi, ancora, alla possibilità di concepire reti di navette che, offrendo soluzioni di trasporto pubblico, possano comunicare tra di loro e con una piattaforma che coordini la domanda degli utenti, per dirigersi autonomamente ove è più alta la domanda e per ottimizzare lo sfruttamento della capienza dei singoli mezzi.

Lo sviluppo di queste soluzioni di mobilità passa per l'interconnessione e per il costante scambio di dati. I veicoli a guida autonoma sfrutteranno *vehicle-to-vehicle communications* (V2V), *vehicle-to-infrastructure communications* (V2I) e *vehicle-to-device communications* (V2D), alimentando le conoscenze del proprio *software* e degli oggetti con cui entreranno in contatto: è ormai invalsa la locuzione *vehicle-to-everything* (V2X) per sintetizzare questa capacità del veicolo di connettersi e comunicare con qualsiasi oggetto, rete o infrastruttura che possa fornirgli un supporto operativo, sia questo indispensabile o solamente utile per il suo funzionamento.

I rischi dell'interconnessione e della proliferazione dei dati

Se queste sono le dinamiche della circolazione stradale del futuro, è chiaro che l'automobile si appresta a trasformarsi in un *database* su ruote, ricco di dati di svariata natura accessibili da più parti.

Ciò induce ovviamente a chiedersi se siano necessario contornare detto *database* di specifiche cautele, soprattutto quando i dati movimentati sono dati personali. È evidente che a questa mole di dati possono essere interessati più soggetti, intenzionati a sfruttarli con svariate finalità.

In assenza di un quadro normativo ben definito, i rischi sono molteplici. Il più evidente è quello che l'utente perda radicalmente il controllo dei propri dati, anche di quelli volontariamente prestati: s'è già detto, infatti, che molte delle informazioni raccolte dal veicolo vengono scambiate, inviate all'infrastruttura e/o a dispositivi terzi, articolandosi in rivoli che lasciano desumere che un singolo dato possa, di passaggio in passaggio, essere utilizzato per finalità sempre più lontane da quelle originariamente autorizzate dal titolare.

In secondo luogo, i dati prodotti da un veicolo a guida autonoma hanno un grande e immediato potenziale economico. Conoscere quanto tempo il proprietario passa a bordo del veicolo, che strade percorre, la condotta di guida che tiene: sono tutte informazioni che produttori, assicuratori e fornitori di servizi multimediali possono sfruttare per predisporre offerte specifiche per il singolo utente, per operare discriminazioni di prezzo o comunque per migliorare il proprio prodotto o servizio sulla base dei dati di utilizzo dello stesso.

Sono dati che possono avere un importante valore economico per i soggetti più impensabili: ad esempio, conoscere in quale momento della giornata il conducente di un veicolo elettrico è più propenso a fermarsi a ricaricare il proprio mezzo, e sapere altresì quanto tempo detto conducente si ferma in media per la ricarica, è un informazione che potrebbe essere sfruttata dal *software* di navigazione per indirizzare verso una colonnina di ricarica dove è presente un ristorante o, al contrario, un distributore automatico di caffè, a seconda del tipo di utenza intercettata. Se l'informazione fosse sfruttata a fini puramente commerciali, il conducente potrebbe essere indirizzato dal sistema di navigazione del veicolo verso un punto di ricarica ove sono presenti negozi di un *partner* commerciale del produttore, anche se magari ciò gli risulta meno comodo: anche qui, gli esempi sarebbero molteplici.

È un tema, è evidente, direttamente connesso a quello della profilazione, attività senz'altro utile agli interessi economici di chi la pone in essere, ma che incide sulle libertà personali del singolo e può financo coartare la sua capacità di autodeterminarsi in alcune scelte: l'esempio dei punti di ricarica e dei

loro servizi connessi è illuminante in tal senso.
Va peraltro sottolineato che, a bordo di un'automobile, la profilazione è attività che non passa necessariamente per l'impiego di dati personali: o meglio, i dati tecnici prodotti dal veicolo possono essere così esplicativi relativamente alle caratteristiche di un certo utente da arrivare ad identificarlo, diventando a loro volta dati personali. Dati in apparenza banali – come può essere il livello dell'olio, del liquido refrigerante, o il rispetto degli intervalli di manutenzione – possono facilmente essere ricondotti ad un conducente specifico, del quale vengono identificate determinate caratteristiche, come la propensione a curare o trascurare il veicolo, e quindi a spendere o meno in prodotti ad esso dedicati.
Il dato tecnico ha pertanto una natura ibrida che può renderlo insidioso, qualora – non essendo esplicitamente qualificato come dato personale – sfugga alle discipline protettive per questi approntate.

I perchè di una normazione difficoltosa

È innanzitutto opportuno chiarire che la raccolta e il trattamento di dati personali operato dall'automobile rappresenta già da anni una realtà: l'esempio più concreto è rappresentato dal Regolamento (UE) 2015/758, che ha reso obbligatoria, per tutti i veicoli omologati successivamente al 31 marzo 2018, la presenza a bordo di un sistema *eCall*, incaricato di effettuare una chiamata al 112 qualora rilevasse il coinvolgimento del veicolo in un sinistro di una certa gravità. Il funzionamento del sistema presuppone – servisse precisarlo – la costante geolocalizzazione del veicolo, la quale viene condivisa, in caso di necessità, con gli operatori del soccorso. L'art. 6 del summenzionato regolamento disciplina in maniera particolarmente rigida la sorte dei dati trattati, garantendo che essi vengano utilizzati esclusivamente per lo scopo prefissato, conservati solo per il lasso di tempo necessario a gestire l'emergenza e infine cancellati: un modello funzionale, ma difficilmente replicabile come modello universale nel futuro contesto dei veicoli autonomi e connessi.
Tale conclusione è imposta da una serie di ragioni. In primo luogo, come s'è accennato, la pervasività, omnidirezionalità e vastità delle operazioni di raccolta e trattamento rende impensabile elaborare multiple normative *ad hoc* che possano circoscrivere con puntualità, per ogni operazione e per ogni tipologia di dato, i limiti dello sfruttamento, giacché le potenzialità sono molteplici e gli sviluppi difficilmente prevedibili.
Ciò dipende anche dal fatto che la natura stessa dei dati che saranno generati dai veicoli a guida autonoma potrebbe essere sfuggente: s'è già detto, in proposito, della polivalenza del dato tecnico. La questione – è evidente – è di grande rilevanza, dal momento che dall'esatta qualificazione del dato dipende la possibilità di applicare la disciplina di cui al Regolamento (UE) 679/2016[3].
Similmente, non va sottovalutata la capacità del *software* di guida autonoma di estrarre da un dato, magari fornito dallo stesso utilizzatore del veicolo, più di quanto esso stesso significhi se preso all'infuori del contesto in cui fornito: in relazione alla geolocalizzazione, ad esempio, è del tutto ragionevole pensare che il *software* di guida autonoma, col tempo e la reiterazione di certi percorsi e certe destinazioni, possa autonomamente dedurre che una certa posizione equivale alla residenza del proprietario del mezzo, al suo luogo di lavoro, alla sua stazione di ricarica preferita.

3 *D'ora in avanti, GDPR.*

Da ultimo, va segnalato che alcuni dispositivi, peraltro spesso sviluppati con l'intento di migliorare sensibilmente i livelli di sicurezza della circolazione stradale, potrebbero financo fare utilizzo di quelli che l'art. 9 del GDPR qualifica come dati particolari, prevedendo la necessità di un consenso esplicito per il loro trattamento: è noto infatti che una delle strade più efficaci per vincere la tendenza a distrarsi che manifestano i conducenti di veicoli dotati di basici sistemi di automazione – i quali richiedono l'interazione e la supervisione umana per operare – sarebbe quella di monitorare costantemente alcuni suoi parametri vitali (anche in uno con le espressioni facciali e il movimento oculare) per valutarne l'effettivo grado di coinvolgimento. Più semplicemente, è ormai comune che i veicoli di alta gamma riconoscano la voce del proprietario, o prevedano l'attivazione di alcune funzionalità del sistema di *infotainment* dopo la lettura dell'impronta digitale.
Sono quindi le molteplici sfaccettature e combinazioni di questo quadro che rendono difficile ragionare secondo la classica dicotomia tra dato personale (da proteggere) e dato non personale (verso il quale essere più permissivi); soprattutto, queste articolazioni mettono in difficoltà capisaldi consolidati della materia quali il principio di finalità del trattamento (art. 5 GDPR) e la possibilità di individuare basi giuridiche univoche che tale trattamento giustifichino.

Le linee guida dell'European Data Protection Board

Se è vero che il tema tecnologico è complesso e ancora del tutto in divenire, non sorprende che a livello europeo il dibattito sia sfociamento al più in documenti di *soft law*.
In assenza di un quadro normativo definito, è opportuno soffermarsi sugli spunti che emergono dalle *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications* elaborate dall'*European Data Protection Board* (EDPB) il 29 marzo 2021.
La prima osservazione da svolgere è che tali linee guida ricomprendono i veicoli a guida autonoma

nel campo di applicazione dell'art. 5, par. 3 della Direttiva (CE) 2002/58 (c.d. *Direttiva ePrivacy*), relativa alla protezione dei dati nel campo delle comunicazioni elettroniche: la conseguenza è che per archiviare informazioni o avere accesso alle informazioni archiviate nel veicolo sia necessario, in ogni caso, il consenso dell'utente, e non una qualsiasi delle basi di trattamento di cui all'art. 6 del GDPR. Tale limite viene meno solo nel caso in cui l'archiviazione o la trasmissione sia "*strettamente necessaria*" per la fornitura del servizio. È una locuzione che le linee guida non precisano ulteriormente, ma che, in assenza di casistica, sarebbe opportuno riempire di significato: la concatenazione di servizi di mobilità e di intrattenimento che potrebbe essere in grado di offrire l'automobile autonoma e connessa si presta a facili abusi, attraverso i quali i dati necessariamente raccolti dal sistema di bordo per l'operatività di una sua determinata funzione possono poi essere sfruttati, nel medesimo contesto, per funzioni connesse per le quali detti dati non sarebbero strettamente necessari.

Ad ogni modo, l'approccio suggerito dall'EPBD sembra rivolto all'individuazione del rischio e alla sua gestione preventiva, anche imponendo al titolare del trattamento dei dati (la casa produttrice del veicolo, o il produttore di un dispositivo del quale il veicolo è equipaggiato) degli oneri di natura procedurale, i quali declinano i noti concetti di *privacy by design* e *privacy by default* di cui all'art. 25 del GDPR.

Quel che lascia perplessi, in questo quadro, è il tornare al consenso come chiave di volta del sistema, anche e soprattutto per la trasmissione dei dati dal titolare del trattamento ad un *partner* commerciale. Di fronte alla mole, alla sensibilità e alla complessità dei dati elaborati costantemente da una *driverless car*, è questionabile che l'utente possa davvero fornire un consenso "*libero, specifico e informato*" in relazione ad ogni singola operazione di trattamento. Non viene agevole neppure immaginare le modalità attraverso le quali detto consenso possa essere prestato. È ipotizzabile che, sul sistema *infotainment* dell'auto, possano essere generate continue schermate di consenso simili a quelle che da anni vediamo – e critichiamo – su *smartphone* e computer: sarebbe tuttavia una soluzione macchinosa, oltre che incapace di garantire l'effettività di detto consenso.

È ipotizzabile che le linee guida assegnino nuovamente grande rilevanza al consenso proprio in ragione della circostanza che si teme un'estensione sconfinata e di difficile governo delle operazioni di raccolta e trattamento di dati. Effettivamente, le linee guida rendono esplicita la preoccupazione per il fatto che "*il continuo aumento del numero di sensori integrati nei veicoli connessi comporta il rischio assai elevato di una raccolta di dati eccedenti rispetto a quelli necessari allo scopo*", col rischio di contravvenire ai principi di *privacy by default* e di minimizzazione. È una preoccupazione del tutto ragionevole, anche in considerazione del possibile sfumare della distinzione tra dato personale e non personale: resta invero il fatto che il consenso non sembra incidere significativamente su detto quadro.

A completamento del quadro, le linee guida si soffermano anche sul tema – invero attuale già da diversi anni – dell'installazione, da parte delle assicurazioni, di *telematic boxes* a bordo del veicolo, specie qualora il contrente opti per una polizza "*pay as you drive*" o "*pay how you drive*". Le linee guida riconoscono che esiste un rischio che i dati raccolti in detto contesto possano essere utilizzati per profilare l'utente, ma si limitano a raccomandare che le *telematics boxes*, invece che trasferire direttamente i dati grezzi al titolare del trattamento, li elaborino per arrivare ad uno *score relating to driving habits*, che potrà essere poi inviato all'assicuratore.

Pur nella necessità di trattare questi dati per dare esecuzione al contratto, sembra che, in assenza di un quadro di contorno ben definito sui limiti di utilizzazione e conservazione di questo *score*, si apra un'autostrada per la futura attuazione di discriminazioni di prezzo sui premi assicurativi, anche qualora l'utente optasse in seguito per una diversa formula assicurativa.

In questo contesto, manca un riferimento diretto alla fattispecie forse più interessante, e cioè l'eventuale utilizzo dei dati raccolti dal veicolo per accertare cause e responsabilità in caso di sinistro. In proposito, si ricorda che in Italia, ai sensi dell'art. 145 bis cod. ass., le risultanze della scatola nera formano piena prova, nei procedimenti civili, dei fatti a cui esse si riferiscono. Oggigiorno, tuttavia, un'automobilista può scegliere di sua sponte di installare la scatola nera sul proprio veicolo, mentre una *driverless car* raccoglierà di *default* dei dati di utilizzo che potranno poi facilmente essere ricondotti all'utente, se si rinvenisse una base legale che autorizza al loro trattamento. Può forse immaginarsi che in una prima fase di diffusione della tecnologia, la base legale di cui all'art. 6, lett. e) del GDPR possa venire in rilievo, nel caso di grandi incidenti involgenti anche infrastrutture *smart*, sotto forma di interesse pubblico

al miglioramento della sicurezza dei trasporti e della circolazione.

Possibili prospettive de iure condendo

Detto delle direttrici di *soft law* tracciate dall'EDPB, così come delle loro criticità, è possibile indicare quelle che sembrano poter essere le fondamenta di una possibile futura disciplina del trattamento dei dati nel contesto della circolazione di veicoli a guida autonoma.

Sono due gli aspetti, connessi tra loro, che maggioramente spiccano nel contesto dell'automazione della circolazione. Il primo è l'attenuarsi, in alcune specifiche situazioni, della differenza tra dato non personale e dato personale, aspetto ben esemplificato da quanto s'è esposto in relazione ai dati tecnici. Il secondo è l'immediata sfruttabilità economica, per un numero crescente e imprecisato di soggetti, di questi dati dalla natura ibrida, e quindi non necessariamente protetti delle cautele legislative prettamente riservate ai dati personali.

Imporre una chiara definizione della natura di ogni singolo dato trattato sarebbe senz'altro positivo, ma è un obiettivo probabilmente irrealizzabile, stante la genuina opacità di alcuni di questi. D'altro lato, almeno per quanto attiene ai dati chiaramente tecnici e/o non personali, non sembra neppure opportuno assumere una posa illiberale e restrittiva, giacché è proprio grazie alla circolazione di questi dati che è possibile ragionare di una mobilità che vada oltre le forme attuali per sviluppare modelli cooperativi: sono dati che servono, per un obiettivo generalmente meritevole.

Nella ricerca di un equilibrio, in una fase in cui è ancora ignota quella che sarà l'effettiva portata del fenomeno, non resta che richiamarsi a tre concetti consolidati, i quali possono rappresentare basi di partenza utili, condivise e ragionevoli: *accountability*, limitazione delle finalità e anonimizzazione.

Partendo da quanto appare più pacifico, non v'è dubbio che la protezione del dato personale debba basarsi, anche nel contesto oggetto delle presenti riflessioni, su meccanismi di prevenzione, e quindi *in primis* su quei principi di *privacy by default* e *privacy by design*, portati dall'art. 25 del GDPR, con cui ormai imprese e operatori del diritto hanno grande familiarità.

La minimizzazione dei dati non varrà – si sarà ormai chiarito – a contenerne significativamente la raccolta, giacché tale attività è intrinseca alla natura e al funzionamento dei veicoli autonomi e connessi: in questo senso, sarà allora opportuno valorizzare adeguatamente il principio di finalità del trattamento, pur al netto della difficoltà di assicurarne il rispetto, assicurando che taluni dati – in specie quelli personali – necessariamente raccolti per l'espletamento di una determinata funzione (si può pensare alla memorizzazione dell'indirizzo di residenza del proprietario del veicolo operata dal *software* di guida autonoma, corredata da immagini raccolte dai sensori affinché il veicolo impari a muoversi con sempre maggior confidenza in un luogo battuto quotidianamente) non vengano anche impiegati sì nel contesto del funzionamento del veicolo, ma per *feature* che possono prescindere dall'utilizzo di tali dati.

Da ultimo, l'interconnessione e l'inevitabile uscita dei dati dal veicolo impone che questi siano perlomeno pseudonimizzati, e quando possibile anonimizzati. Esigenze di pubblica sicurezza potrebbero impedire una totale anonimizzazione del dato, ed è opportuno prevedere che talune informazioni siano, in casi specifici e determinati, ricollegabili alla persona fisica: non va dimenticato che nelle indagini sugli incidenti che avverranno nella mobilità interconnessa i dati potranno rappresentare un ausilio per ricostruire dinamiche e allocare responsabilità. Sarà tuttavia opportuno delimitare con precisione le fattispecie nelle quali si potrà procedere con la riconduzione del dato al singolo, di modo che l'interesse pubblico, pur previsto dall'art. 6, lett. e) del GDPR, non diventi una scappatoia in grado di legittimare indebite intrusioni.

Si tratta, chiaramente, di semplici petizioni di principio. Tuttavia, non va sottovalutata l'utilità di approcciare gli sviluppi tecnologici in divenire – che porteranno senz'altro all'esplosione del tema che abbiamo trattato – partendo dalla condivisione di poche fondamenta solide e non contestate, preferibilmente condivise tanto dai giuristi quanto dagli sviluppatori: da qui, si costruirà la disciplina una volta avuti più chiari gli sviluppi in divenire.

Riferimenti bibliografici

E. FIALOVA, J. MATEJKA, *Data protection and privacy issues in the use of autonomous vehicles*, in *The Lawyer Quarterly*, 2022, 12, 408

M.C. GAETA, *La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi*, in *Diritto dell'informazione e dell'informatica*, 2018, 1, 147

B. GRUSH, J. NILES, *The End of Driving: Transportation Systems and Public Policy Planning for Autonomous Vehicles*, Elsevier, Amsterdam, 2018

N. MINISCALCO, *Il diritto alla protezione dei dati personali al tempo della mobilità intelligente*, in *Forum di Quaderni Costituzionali*, 2020, 1

A.C. NAZZARO, *Privacy e smart mobility*, in D. CERINI, A. PISANI TEDESCO, *Smart mobility, smart cars e intelligenza artificiale: responsabilità e prospettive*, G. Giappichelli Editore, Torino, 2019

F. VAN DEN BOOM, *Regulating Telematics Insurance – Enabling Car Data-Driven Innovations*, in *European Business Law Review*, 2023, 34, 157.

Frodi nel settore dei Bonus edilizi: fattispecie penali ipotizzabili, primi approdi giurisprudenziali e questioni ancora aperte

di Gianluigi Miglioli e Paolo Marzano

I bonus edilizi rappresentano un argomento dibattuto da tempo e oggi, più che mai, sono al centro di accesi confronti. Dalla loro prima comparsa - nel 1997 - sono stati sempre di più oggetto di diversi interventi normativi, da ultimo - nel 2020 - per sostenere le imprese del settore edile gravemente danneggiate dalla pandemia da COVID-19 e favorire l'occupazione, incentivando ancora di più i cittadini nella realizzazione di interventi sui propri immobili. Le misure messe in campo dal Legislatore, nonostante abbiano dato una forte spinta al settore, con le correlate positive conseguenze in termini di P.I.L., recupero del patrimonio edilizio e incremento del numero di lavoratori occupati, sono state anche teatro per la realizzazione di condotte fraudolente volte alla creazione, circolazione, commercializzazione e monetizzazione di crediti di imposta "inesistenti", realizzate soprattutto sfruttando la possibilità di optare - in luogo della "classica" detrazione di imposta - per lo "sconto in fattura" o la "cessione del credito".
Le Autorità Giudiziarie italiane hanno accertato in tutta Italia la commissione di reati di *"Truffa"*, *"Emissione di fatture o altri documenti per operazioni inesistenti"*, *"Indebita compensazione"*, *"Riciclaggio"*, che hanno finora portato al sequestro di crediti d'imposta inesistenti per quasi 4 miliardi di euro.
Il presente contributo - che si compone di tre parti - cercherà di tracciare un quadro d'insieme normativo, fattuale e giurisprudenziale, focalizzando l'attenzione su alcune questioni che appaiono ancora aperte, come ad esempio le fattispecie di reato che potrebbero essere contestate e i temi legati alla "tutela del terzo cessionario" che ritiene di essere "estraneo ai reati" ed "in buona fede".

Parte prima

Premessa
La materia delle agevolazioni fiscali per interventi di recupero del patrimonio edilizio è da tempo all'attenzione del Legislatore.
Dal lontano 1997 - dopo l'emanazione della Legge n. 449, istitutiva delle detrazioni - la normativa di settore è stata particolarmente prolifera e si è assistito a continue modifiche, proroghe e ampliamenti del novero delle spese agevolabili[1], con approdo ad una vera e propria stabilizzazione delle misure in argomento attraverso l'introduzione dell'articolo 16-*bis*[2]

1 *Ad esempio, nel 2006 sono state introdotte quelle finalizzate ad aumentare il livello di efficienza energetica degli edifici esistenti (L. n. 296/2006, art. 1, commi dal 344 al 349, cd. finanziaria 2007). Più tardi (2013) quelle concernenti l'adozione di misure antisismiche (D.L. n. 63/2013).*

2 *Ad opera dell'art. 4, comma 1, lett. c), del D.L. n. 201/2011.*

nel D.P.R. n. 917 del 1986 (*Testo unico delle imposte sui redditi*), che ha confermato non solo l'ambito di applicazione delle detrazioni (soggettivo e oggettivo), ma anche le condizioni di spettanza del beneficio fiscale così consolidando l'orientamento di prassi formatosi in materia.

Al fine di fronteggiare i devastanti effetti negativi subiti dal settore edile a causa della pandemia da COVID-19, il Governo è intervenuto con normativa emergenziale (cc.dd. Decreti "Cura Italia" e "Rilancio", rispettivamente D.L. n. 18/2020 e D.L. n. 34/2020) attuando imponenti misure di sostegno aventi il duplice scopo di: 1) ampliare l'ambito applicativo delle agevolazioni esistenti: 2) favorire la loro fruizione; prevendendo a più ampio raggio, in alternativa alla genetica detrazione d'imposta da parte del beneficiario, la possibilità di optare per: lo "*sconto in fattura*"[3] ovvero la "*cessione del credito a terzi*"[4].

Ed è proprio in queste "pieghe" che si sono annidate perniciose condotte fraudolente, consistenti nell'artificiosa creazione di crediti di imposta inesistenti con finalità di monetizzazione, sì da dare luogo a un vero e proprio "mercato" costituente la struttura portante di un vasto fenomeno truffaldino caratterizzato, in buona parte, dalla mancanza di collegamento tra i crediti e i lavori che li hanno originati (con sicuro impatto in un già delicato contesto di Finanza Pubblica)[5].

Le modalità di esercizio della "*opzione di cessione*"[6], l'assenza di limiti alle cessioni (sia dal punto di vista numerico che soggettivo), la mancanza di obblighi certificativi tesi ad asseverare la veridicità della documentazione presentata e la congruità delle spese sostenute, l'assenza di limiti di spesa e la possibilità di fruizione da parte di soggetti cd. incapienti[7], certamente hanno favorito siffatte condotte illecite.

Sicché il legislatore è intervenuto nuovamente - e più volte - con l'adozione di provvedimenti normativi "antifrode"[8]: mettendo fine alla "libera circolazione dei crediti" (stabilendo precisi adempimenti e procedure), introducendo i "codici univoci identificativi dei crediti" e prevedendo, in caso di esercizio delle ridette opzioni, specifici obblighi documentali (visto di conformità e asseverazioni tecniche).

Aggiungasi che, a febbraio ultimo scorso, il Governo è - ancora - intervenuto mediante emanazione del D.L. n. 11/2023 (entrato in vigore il 17/02/2023), con il quale ha eliminato la possibilità, per il tratto a venire, di esercizio delle menzionate opzioni (con salvezza delle pregresse situazioni al verificarsi di determinati presupposti).

Il presente contributo, pertanto, si pone l'obiettivo di provare a dare risposte ad una serie di domande su diverse questioni, alcune delle quali appaiono ancora aperte, in particolare se:

tali fatti illeciti siano sussumibili nel delitto tributario di "*Indebita compensazione*" previsto dall'art. 10-*quater*, del D.Lgs. n. 74/2000 e non nella fattispecie di reato di "*Truffa*"[9], dovendosi applicare il principio di specialità sancito dall'art. 15 del c.p.;

sia possibile ipotizzare il concorso fra i predetti reati; con l'ulteriore necessaria verifica se trattasi di: "*Truffa ex* art. 640, comma 1, del c.p."; "*Truffa ai danni dello Stato o di altro ente pubblico e dell'Unione Europea ex* art. 640, commi 1 e 2, n. 1, del c.p.; "*Truffa per il conseguimento di erogazioni pubbliche ex* art. 640-*bis* del c.p.";

sia applicabile ed in quali circostanze il principio della "tutela del terzo in buona fede", nel caso di sequestro dei crediti d'imposta inesistenti;

sussista la compatibilità del "dolo eventuale" in relazione alle condotte del "terzo cessionario finale", che ritiene abbia agito in "buona fede".

La natura dei crediti d'imposta

Il punto di partenza è certamente quello di verificare la natura dei crediti d'imposta e, quindi, se la loro "veste di *agevolazione fiscale*" sia idonea a integrare un fatto commesso a danno dello Stato o di altro Ente Pubblico (si vedrà che in quest'ultimo caso il riferimento corre a Poste Italiane s.p.a. ovvero a Cassa Depositi e Prestiti, quali cessionari finali) e se possano rientrare nella nozione di: <<*...contributi, sovvenzioni*[10]*(...) ovvero altre erogazioni dello stesso tipo, comunque denominate (...)*>> rilevabile *ex* art. 640-*bis* del c.p..

Secondo la dottrina[11], "erogazione pubblica" (in generale) deve essere intesa qualsiasi attribuzione agevolata "*concessa*" o "*erogata*" dallo Stato, da altri Enti Pubblici o dall'Unione Europea, la cui *ratio* si rinviene nella rilevanza pubblica degli interessi sottostanti. Detta prospettazione è richiamata e condivisa anche dalla giurisprudenza[12].

Dal testo della Sentenza n. 36859/2013 emessa dalla

3 *Consistente nella detrazione del contributo dall'imponibile della fattura: in sostanza l'appaltatore "sconta" l'importo al committente per poi rivalersi nei confronti del Fisco.*

4 *Con possibilità di monetizzarlo.*

5 *La stima del Superbonus e degli altri bonus edilizi è stata aumentata a circa 110 miliardi di euro, con uno scostamento complessivo di 37,75 miliardi di euro rispetto alle previsioni iniziali sull'intero orizzonte temporale. Stime che determinerebbero per gli anni 2023-2026 un peggioramento della previsione delle imposte dirette per importi compresi tra gli 8 e i 10 miliardi di euro in ciascun anno (fonte: relazione del Direttore Dipartimento delle Finanze del MEF, Giovanni Spalletta, nell'intervento del 2 febbraio 2023 presso la Commissione Finanze del Senato).*

6 *Accesso all'apposita area, sul portale web dell'Agenzia delle Entrate, denominata "Piattaforma cessione crediti", con inserimento del cessionario (persona fisica o giuridica), il quale, poi, con autonoma procedura può accettare la cessione (che pertanto si perfeziona) oppure rifiutarla (in tal caso, il credito per essere ceduto ad altro soggetto deve essere nuovamente inserito da parte del beneficiario).*

7 *È questo il caso del c.d. "Bonus facciate" di cui all'art. 1, comma 2019, l. n. 160/2019 (cd. Legge di bilancio 2020).*

8 *D.L. n. 157/2021, D.L. n. 13/2022, D.L. n. 17/2022, D.L. n. 50/2022.*

9 *Con riguardo all'eventuale ipotesi di cui all'art. 316-ter del c.p. in luogo di quella di Truffa, nelle concrete fattispecie in trattazione appare integrata "l'induzione in errore" (cfr., ex plurimis, Cassazione penale, Sez. II, sentenza n. 47064 del 13 ottobre 2017).*

10 *Parola inserita dal dall'art. 28-bis, comma 1, lett. d), D.L. 27 gennaio 2022, n. 4, convertito, con modificazioni, dalla L. 28 marzo 2022, n. 25, a decorrere dal 29 marzo 2022.*

11 *F. ANTOLISEI, Manuale di diritto penale. Parte speciale, I, Milano, Giuffrè, 2016, p. 384.*

12 *Cassazione penale, Sezione VI, Sentenza n. 7963/2020.*

Corte di Cassazione penale, Sezione V, si ricava - per quanto di interesse in *parte qua* - la seguente posizione: non sembra affatto che il riconoscimento di un credito d'imposta possa essere assimilato alle categorie di atti di disposizione patrimoniale elencati dall'art. 316-*ter* del c.p. (n.d.r.: ed evidentemente dall'art. 640-*bis* del c.p.). Gli ermellini muovono dall'analisi del precetto disegnato dall'art. 10-*quater* del D.Lgs. n. 74/2000, affermando che quella di non versare all'Erario somme dovute, utilizzando in compensazione crediti non spettanti o inesistenti, appare *latu sensu* fraudolenta, ma a tale elemento in fatto (ai fini della consumazione del reato) non è richiesto debba aggiungersi un atto di disposizione patrimoniale da parte della Pubblica Amministrazione.

Risulta utile richiamare, sul tema, anche il "Documento n. 9" redatto dal "Tavolo di coordinamento fra Banca d'Italia, Consob ed Ivass in materia di applicazione degli IAS/IFRS", relativo al <<*Trattamento contabile dei crediti d'imposta connessi con i Decreti Legge "Cura Italia" e "Rilancio" acquistati a seguito di cessione da parte dei beneficiari diretti o di precedenti acquirenti*>>, dove viene evidenziato che: << *Per il soggetto beneficiario tali crediti sembrano potersi assimilare alla fattispecie dei crediti d'imposta sugli investimenti (investment tax credits). Una volta acquistati da un soggetto terzo, le peculiarità dei crediti non permettono una loro immediata riconducibilità a uno specifico principio contabile internazionale. Sono infatti esclusi dalle disposizioni dello IAS 12 "Imposte sul reddito" in quanto non rientrano tra le imposte che vanno a colpire la capacità dell'impresa di produrre reddito e non rientrano tra la definizione di contributi pubblici (government grants) stabilita dallo IAS 20 "Contabilizzazione dei contributi pubblici e informativa sull'assistenza pubblica" in quanto la titolarità del credito verso l'Erario sorge solo a seguito del pagamento di un corrispettivo al cedente. Non risultano inoltre direttamente applicabili l'IFRS 9 "Strumenti finanziari" in quanto le attività costituite dai crediti di imposta acquistati non originano da un contratto tra il cessionario e lo Stato italiano, né lo IAS 38 "Attività immateriali" in quanto i crediti d'imposta in questione possono essere considerati attività monetarie, consentendo il pagamento di debiti d'imposta usualmente estinti in denaro. Pertanto, è necessario richiamare quanto previsto dallo IAS 8 "Principi contabili, cambiamenti nelle stime contabili ed errori" nei casi in cui vi sia una fattispecie non esplicitamente trattata da un principio contabile IAS/IFRS. In questi casi il principio richiede che la direzione aziendale definisca un trattamento contabile (accounting policy) che sia idoneo a fornire un'informativa rilevante e attendibile (...)*>>.

Ulteriori elementi si possono trarre anche dalla lettura del "Manuale sul disavanzo e sul debito pubblico, secondo il nuovo sistema dei conti nazionali (Sec 2010)", pubblicato dall'Ufficio statistico dell'Unione Europea (EUROSTAT), nel quale si evidenzia che la spesa e la relativa passività del Governo devono essere rilevate all'inizio, cioè quando il credito d'imposta viene maturato. Un credito d'imposta può essere trasferito ad altri beneficiari o può essere utilizzato per saldare un'ampia gamma di passività fiscali del contribuente, compreso il suo debito fiscale totale. In questi casi, il credito d'imposta è considerato esigibile quando vi è un'altissima probabilità (ossia prossima al 100%) che venga eventualmente utilizzato per intero (o quasi per intero) in futuro, quindi, quel governo perderà effettivamente risorse equivalenti. Sulla trasferibilità del credito, EUROSTAT chiarisce che << *se il credito d'imposta può essere trasferito a terzi, tale credito d'imposta deve quindi essere considerato un credito d'imposta pagabile e deve essere registrato nei conti nazionali come un'attività del contribuente e una passività del governo*>>. Destino diverso, invece, se il credito di imposta è trasferibile, ma a un numero limitato di soggetti. In quel caso, <<*quando il credito d'imposta può essere trasferito solo a parti correlate (ad esempio, solo al fornitore dei beni/servizi che hanno attivato il credito d'imposta, familiari o società dello stesso gruppo), può essere necessaria una valutazione per esaminare se, in pratica, tali crediti d'imposta possano andare perduti per importi non trascurabili (nel qual caso il credito d'imposta rimarrebbe inesigibile)*>>.

Orbene, che il credito d'imposta in argomento sia una agevolazione tributaria[13] che il Legislatore riconosce al contribuente sotto forma di "*detrazione diretta*" oppure di utilizzo mediante "*sconto in fattura*" o "*cessione del credito a terzi*" per l'unica finalità "compensativa" (è escluso il rimborso), non sembra in discussione. Si tratta di strumenti che consentono di ritenere classificabile il beneficio in maniera automatica: l'Erario fa affidamento nella correttezza del contribuente che in concreto gestisce il proprio credito (il controllo eventuale si avrà *ex post*).

Sul tema della qualificazione della natura dei crediti di imposta derivanti da lavori edili, pregevole si ritiene la Sentenza n. 45558/2022 della Terza della Corte di Cassazione penale, che in motivazione affronta la questione ponendo l'interrogativo se essi (crediti) possano o meno essere considerati agevolazioni tributarie e di riflesso quali siano le conseguenze derivanti dal loro utilizzo fraudolento (in tema di "*Superbonus* 110% e sequestro di crediti effettuato nei confronti del cessionario Poste Italiane s.p.a.). Iniziando dal-

13 Nozione che tuttavia non si rinviene nel diritto tributario.

la considerazione che la loro qualificazione li rende sia diretti a risparmiare imposta abbattendola, che finalizzati ad agevolare il mercato immobiliare e il mondo del lavoro aumentando la richiesta di interventi edilizi; ripercorrendo, poi, le diverse modalità di utilizzo dell'agevolazione; e non collocandoli, infine, nel concetto di "rimborso", li ritiene riferibile alla nozione di "*agevolazione tributaria*" perché nulla hanno a che fare con il presupposto d'imposta e la relativa capacità contributiva del beneficiario. Pertanto, ponendo quale presupposto <<*(...) cui commisurare l' "aiuto", l'interesse politico economico, sociale o ambientale, inequivocabilmente costituzionalmente rilevante, ma che quindi è evidentemente di natura extrafiscale*>> (ndr.: cfr. pag. 27 della Sentenza), evidenzia <<*l'esistenza di una "passività" in capo all'Erario derivante proprio dall'inesistenza del credito che, ove lo si ritenesse opponibile in compensazione nonostante la mancanza del suo presupposto, genererebbe un indubbio danno alle casse dell'Erario, in quanto consentirebbe al cessionario di compensare crediti (inesistenti) con quanto (realmente) dovuto al Fisco, con indubbio "arricchimento senza causa" (...) a favore del cessionario (...)*>> (ndr.: cfr. pagg. 28 e 29 della Sentenza). Sul piano delle conseguenze e del rapporto tra le ipotesi di *Truffa* e il reato tributario di *Indebita compensazione*, i giudici di legittimità - qualificati detti crediti come "agevolazione tributaria" - ritengono senz'altro applicabile l'art. 10-*quater* del D.Lgs. n. 74/2000 (sul punto ritorneremo nella Parte seconda, di prossima pubblicazione).

Merita menzione, sempre per la pregnanza delle argomentazioni, un'altra recentissima pronuncia della Cassazione[14], che - in relazione alla fattispecie di *Truffa ex* art. 640, commi 1 e 2, n. 1, del c.p., contestata proprio con riferimento alla creazione e commercializzazione di "crediti d'imposta fittizi" originati da sottostanti lavori edili documentati da fatture per operazioni inesistenti - ha, tra l'altro, riconosciuto la natura di "*erogazione pubblica*" al credito d'imposta.

Traendo le conclusioni sull'argomento, come si vede non è agevole rispondere all'interrogativo circa la natura dei crediti d'imposta originati da lavori edili.

A parere di chi scrive, se *prima facie* sembrerebbe esclusa la loro riconducibilità alla categoria dei contributi, sovvenzioni e/o erogazioni pubbliche, sulla constatazione dell'assenza di una vera e propria disposizione patrimoniale della Pubblica Amministrazione, ad una più attenta e critica analisi - invero - si potrebbe annoverarla, aggiungendo, quale ulteriore spunto di riflessione, la considerazione che proprio la specificità di questi crediti d'imposta - dunque la rilevanza pubblica delle operazioni che sempre di più hanno incentivato l'esecuzione dei lavori edili, che giustifica l'onerosità unilaterale per chi dà le condizioni di favore[15] - induce a ragionare anche puntando alla valorizzazione della violazione dei richiamati doveri e obblighi di correttezza sui quali fa affidamento l'Erario - e dalla quale deriva un danno conseguente ai mancati introiti tributari - per ricavare l'inferenza indiretta della citata riconducibilità dei crediti (*rectius*: una sorta di disposizione patrimoniale qualificabile "in negativo").

Del resto, tale ragionamento appare congruente con le motivazioni (per la specifica parte di rilevanza) espresse nella richiamata Sentenza n. 7963 del 2020, la quale fa rientrare nel concetto di "*agevolazione*" anche un "*risparmio di spesa*": <<*(...) Le erogazioni di cui all'art. 316-ter c.p., quindi, non devono necessariamente consistere nel conseguimento diretto di una somma di denaro, ben potendo anche consistere nell'esenzione dal pagamento di una somma altrimenti dovuta, ovvero in un risparmio (...)*>>.

Ma già in precedenza - e nello stesso solco - anche la nota Sentenza delle Sezioni Unite n. 7537/2011 (Pizzuto): <<*(...) nel concetto di conseguimento indebito di una "erogazione" (...) rientrano tutte le attività di "contribuzione" (...) non soltanto attraverso l'elargizione precipua di una somma di danaro ma pure attraverso la concessione dell'esenzione dal pagamento di una somma (...), perché anche in questo secondo caso il richiedente ottiene un vantaggio e beneficio economico che viene posto a carico della comunità*>>.

14 *Cassazione penale, Sezione Terza, Sentenza n. 42012/2022 (ud. 13 ottobre 2022).*

15 *Sul principio: Fratini Marco-Lucrezia Fiandaca, Manuale sistematico di diritto penale. Parte speciale.*

Il controllo concomitante della Corte dei conti sugli investimenti del PNRR

di Marcovalerio Pozzato

Il controllo concomitante costituisce, come noto, un elemento di peculiare novità nel quadro dei controlli di gestione effettuati dalla Corte dei conti.
La genesi di tale controllo va ricercata nell'art. 11 della L. n. 15/2009, cui si ricollega, nell'attualità ordinamentale, l'art. 22 del D.L. n. 76/2020.
Lo scenario oggetto del nostro esame è da porre in relazione agli sviluppi normativi legati alla necessità del rilancio delle infrastrutture nazionali e dell'economia, particolarmente sensibili alle negatività e alla situazione di conseguenti alla nota emergenza pandemica.
L'impulso agli interventi legati a tali finalità, a sua volta, è garantito dagli investimenti relativi al Piano Nazionale di Ripresa e Resilienza (PNRR), la cui importanza postula un percorso collaborativo di verifiche pubbliche.
A tale itinerario di riscontri appartiene pienamente il Collegio del controllo concomitante della Corte dei conti, chiamato dalla legge ad accelerare gli interventi di sostegno e di rilancio dell'economia nazionale, imprimendo dunque un effetto propulsivo all'azione di governo del sistema.
L'inquadramento della tematica del controllo concomitante richiede tuttavia, preliminarmente, una breve disamina con riferimento alla collocazione di quest'ultimo nell'ambito generale dei controlli svolti dalla Corte dei conti.

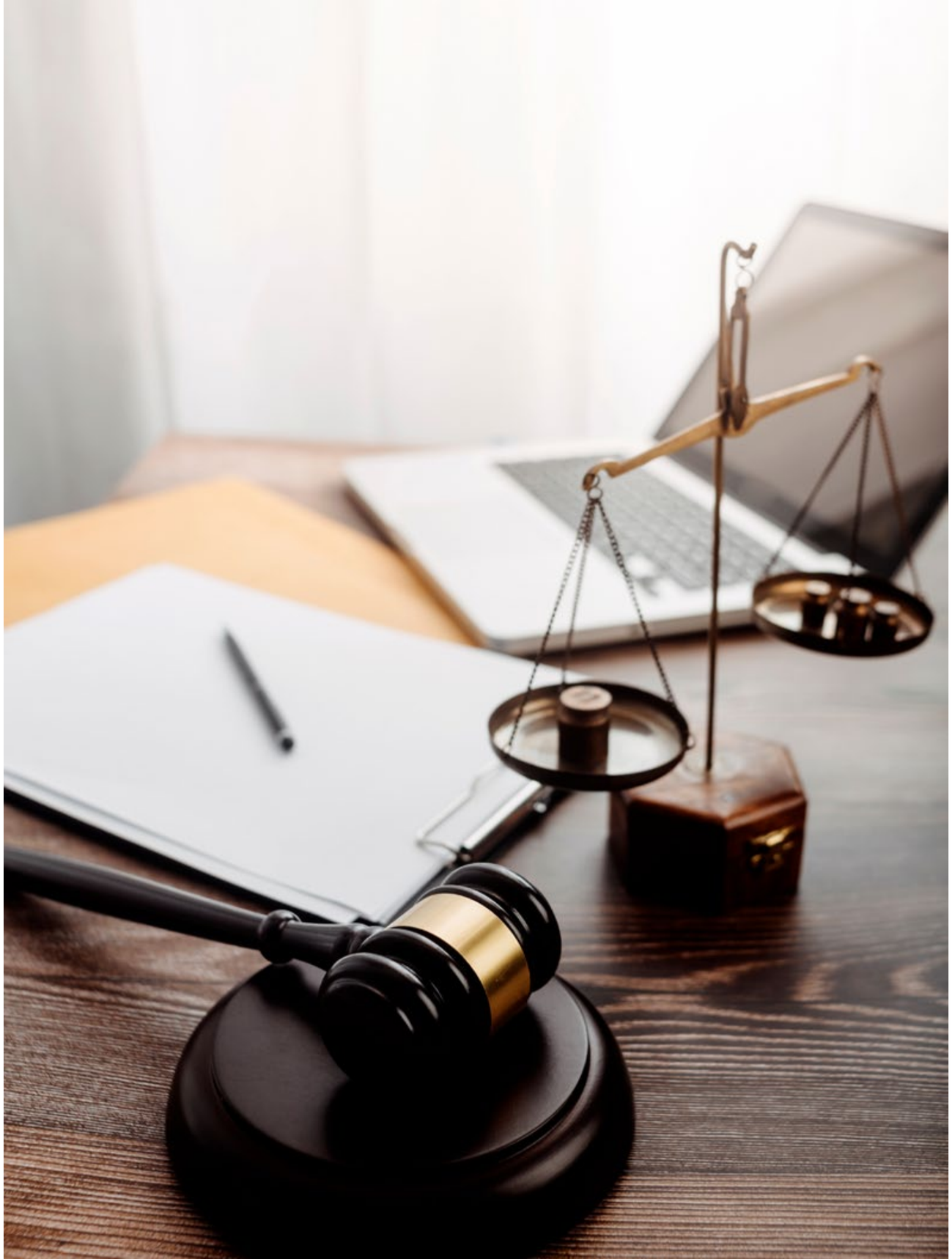
Occorre all'uopo premettere che questi ultimi rappresentano attività tipiche di verifica, caratterizzate dalla terzietà, profondamente modificatesi nel tempo.
La c.d. "funzione di controllo" si ricollega, *ab origine*, al riscontro proprio del controllo preventivo di legittimità sugli atti ministeriali e successivo sul bilancio consuntivo dello Stato, in affiancamento alla c.d. "funzione giurisdizionale", ricollegata nel medesimo contesto primigenio ai *giudizi di conto*.
Ambedue le funzioni si ricollegano a un'idea centrale, quella di un medesimo Organo – connotato da indipendenza, imparzialità e specifica competenza tecnica - deputato al loro svolgimento, caratterizzato dall'essere il "Guardiano del Pubblico Erario": la Corte dei conti.
Questa figura, responsabile della diretta protezione del pubblico denaro svolgeva quindi, nell'originario disegno cavouriano, compiti aventi conseguenze impeditive (per quanto concerne il c.d. controllo preventivo di legittimità) - con inserimento del competente Ufficio di controllo nell'*iter* procedimentale, nella fase cosiddetta integrazione dell'efficacia dell'atto amministrativo - ovvero conseguenze eventualmente sanzionatorie, con riferimento alla pronuncia ripristinatoria a carattere patrimoniale nei giudizi di conto.
Nella disamina odierna i nostri riferimenti saranno

peraltro indirizzati al *genus* dei controlli amministrativi, volendo intendere tutte le attività di verificazione della conformità di un atto, di un'attività o di un comportamento a determinati canoni o prescrizioni, onde esprimere un giudizio e adottare le misure conseguenti.
Se il quadro normativo sino agli novanta (in primo luogo, la Costituzione; la Legge di contabilità generale dello Stato, il Testo unico delle Leggi sulla Corte dei conti, Leggi comunali e provinciali) evidenziava un primario ruolo dei controlli preventivi - caratterizzati dall'essere di natura "susseguente" rispetto a atti emanati ma non ancora efficaci, aventi la specifica funzione di intervenire nella fase c.d. "integrativa dell'efficacia", il centro di gravità degli itinerari di verifica va a spostarsi, dagli anni novanta, al momento successivo dell'adozione degli atti, in un percorso evolutivo che prende in esame l'attività amministrativa nel suo complesso (come insieme coordinato e omogeneo dei singoli provvedimenti), privilegiando al sistema dell'asettica e preventiva comparazione con il parametro legale, la ponderazione dell'efficacia, economicità e efficienza dell'agire amministrativo (il sistema delle c.d. "3 E").
La variazione nel baricentro del sistema di controllo della Corte dei conti si pone quindi in una scia di maturazione dell'attività della P.A., riconoscendo il superamento di uno schema ottocentesco fondato sulla sanzione e sull'effetto impeditivo delle verifiche (imperniate sul modello del "visto" e della "registrazione").
L'introduzione del c.d. "controllo concomitante" a partire dai primi anni del nuovo millennio costituisce un ulteriore *step* nella maturazione della consapevolezza dell'azione amministrativa e nel sistema di affinamento della stessa: se nel caso del controllo preventivo l'atto non può essere emanato o comunque non diviene efficace, nell'applicazione del controllo concomitante il soggetto controllato dovrà conformare la sua attività agli esiti del controllo (per esempio snellendo le procedure, o verificando l'impegno dei fondi).
In questo quadro, il controllo concomitante costituisce un momento a cavallo tra i più tradizionali controlli preventivi e successivi (nel quadro di questi ultimi, ricordiamolo, l'atto ha già spiegato i suoi effetti e l'Amministrazione può solo intervenire per rimuoverli, eventualmente sanzionando il soggetto responsabile).
La valutazione dell'attività della P.A., in altre parole, si pone non solo in termini di corrispondenza o meno ad uno specifico modello regolato dalla Legge,

ma si modella anche alla luce degli ulteriori profili sopra delineati (secondo i princìpi di economicità, efficienza ed efficacia).
Le grandi riforme della P.A. che hanno contrassegnato i primi anni novanta non vanno considerate, in questo scenario, fenomeni isolati, ma elementi coerenti di una strategia unica: la semplificazione e la trasparenza dei procedimenti amministrativi, le forme partecipative, nel quadro dell'attività procedimentale, devono coniugarsi a una nuova concezione di Amministrazione, operante non per schemi e archetipi legali, ma alla ricerca del risultato, ovverossia della *perfomance* pubblica.
Il concetto di responsabilità del dirigente, sempre in questo scenario, va ricollegato quindi non più solo alla possibile applicazione di misure sanzionatorie per la violazione di regole di condotta in collegamento agli obblighi di servizio, ma anche e soprattutto al mancato raggiungimento dei risultati previsti in termini giuridico-socio-economici.
Il sindacato esercitato dalla Corte dei conti in quest'ultima sede si esprime in termini di referto agli organi assembleari, operando in funzione propulsiva, essendo volto a indirizzare il potere autocorrettivo da parte dell'Amministrazione, in un quadro in cui il potere gestionale non viene compartecipato, né viene attuata alcuna valutazione preliminare in ordine a possibili danni erariali.
L'art. 17, c. 30 quater, del D.L. n. 78/2009 (convertito dalla L. n. 102/2009) ha peraltro costituito un *turning point* ordinamentale, giacché introduce l'esonero da responsabilità amministrativo-contabile per gli atti ammessi al visto nell'esercizio del controllo.
Il Codice di giustizia contabile (c.g.c.), entrato in vigore nel 2016, ha per altro verso introdotto un ulteriore fattore di sicura novità, tenuto conto che l'art. 69, c. 2, prevede che *"Il pubblico ministero dispone altresì l'archiviazione per assenza di colpa grave quando l'azione amministrativa si è conformata al parere reso dalla Corte dei conti in via consultiva, in sede di controllo e in favore degli enti locali nel rispetto dei presupposti generali per il rilascio dei medesimi"*.
A sua volta, l'art. 95, c. 4, c.g.c., dispone che *"Il giudice, ai fini della valutazione dell'effettiva sussistenza dell'elemento soggettivo della responsabilità e del nesso di causalità, considera, ove prodotti in causa, anche i pareri resi dalla Corte dei conti in via consultiva, in sede di controllo e in favore degli enti locali, nel rispetto dei presupposti generali per il rilascio dei medesimi"*.
Ciò posto, l'allontanamento del sindacato di controllo della Corte dei conti dai parametri della stretta legalità postula invece l'avvicinamento a un giudizio di carattere empirico, ispirato, più che a precisi parametri normativi, a canoni di comune esperienza che trovano la loro razionalizzazione nelle conoscenze tecnico-scientifiche proprie delle varie discipline utilizzabili ai fini della valutazione dei risultati dell'azione amministrativa.
Nel medesimo contesto di evoluzione ordinamentale emerge il nuovo *genus* di controllo "concomitante", mutuato dalle procedure in essere durante lo svolgimento delle operazioni aziendali, allo scopo di monitorare l'andamento della gestione aziendale e di garantire, entro i limiti del possibile, il rispetto degli obiettivi che erano stati fissati in sede di programmazione, consentendo, ove i risultati intermedi rilevati non risultino coerenti con quelli attesi, interventi di correzione tempestivi.
Dal punto di vista teorico-aziendalistico tale forma di riscontro presuppone l'analisi periodica degli indicatori, attraverso la rilevazione dei costi diretti e indiretti sostenuti per il raggiungimento dei risultati predeterminati.
L'approccio di *"pre-azione"* presuppone che le eventuali "correzioni di rotta" si verifichino nel corso della gestione, senza dovere attendere il completamento delle attività.
In questo quadro il giudizio va riconnesso a quattro fasi fondamentali, identificate in 1) fissazione degli obiettivi, 2) rilevazione periodica dei risultati, 3) analisi causale, 4) interventi correttivi.
Per quanto concerne la fissazione degli obiettivi (1), è opportuno rammentare la necessità di individuare entità realistiche e chiaramente definite, onde non ritrovarsi in situazioni di scarsa comprensibilità (in termini di proficuità dell'indirizzo aziendale). In questo quadro, un obiettivo non in linea con la fattibilità tecnica o la domanda del mercato potrebbe, ad esempio, determinare non solo strozzature o blocchi nei procedimenti, ma causare stress nel personale interessato.
Circa la rilevazione periodica dei risultati (2), il fattore tempestività nell'elaborazione e nella distribuzione dei dati si rivela decisivo ai fini della correzione utile delle attività interessate.
L'analisi causale (3) è correlata all'esigenza di indicare le specifiche cause dell'eventuale divaricazione fra gli obiettivi e i risultati; costituisce il momento centrale della valutazione tecnica, in quanto affianca gli uni e gli altri evidenziando le non concordanze e le criticità a queste associabili, individuando la necessità di percorsi correttivi.
Gli interventi correttivi (4) possono rivolgersi tanto alle prestazioni all'interno dell'ente, che agli obiettivi; nel primo caso, riallineano le attività con la programmazione, senza variare gli obiettivi, nel secondo caso, modificano gli obiettivi armonizzandoli con le attività in concreto esigibili all'interno dell'organizzazione.

Il sistema normativo

Il controllo concomitante è stato, come già accennato, originariamente introdotto nell'Ordinamento dall'art. 11, c. 2, della L. n. 15/2009.
L'art. 22 del D.L. n. 76/2020, convertito, con modificazioni, dalla L. n. 120/2020, novella questa attività sindacatoria inquadrandola organicamente nel più vasto ambito delle funzioni di controllo sulle Amministrazioni dello Stato, attribuite in via generale alla Corte dei conti dall'art. 100, c. 2, Cost.
Il controllo concomitante evidenzia ampie aree in comune con il controllo sulla gestione, condividendone ambiti e principi ispiratori ma differenziandosene per finalità, tempi, modalità ed esiti. In particolare, nell'ambito delle funzioni intestate alla Corte dei conti, il Legislatore ha avvertito la necessità di introdurre, intensificandone l'efficacia, nuove forme di controllo in grado di assicurare –assieme alle consolidate verifiche di legittimità sui singoli atti e alle valutazioni ex post sulle gestioni condotte dai soggetti pubblici al fine, non rinunciabile, di orientarne e correggerne l'attività – una verifica tempestiva e un'azione propulsiva finalizzate al corretto impiego delle risorse disponibili, in parte provenienti anche dall'Unione europea e rimesse alla gestione pubblica.
La finalità è quella di intercettare e, ove possibile, prevenire, attraverso un dialogo aperto con le stesse Amministrazioni, gravi irregolarità gestionali o gravi deviazioni da obiettivi, procedure o tempi di attuazione stabiliti da norme, nazionali o euro-unitarie, ovvero da direttive del Governo.
Il ruolo del controllo concomitante si rivela, in tal senso, inedito e incisivo, in un contesto di garanzia, con tempi e modalità più immediati e stringenti, di quell'efficacia dell'azione amministrativa radicata nel principio di buon andamento di cui all'art. 97 del-



la Costituzione.
Tale ruolo si declina non tanto nel riscontro della legittimità dei singoli atti e nella verifica di una corretta gestione delle Amministrazioni centrali o locali al fine di indicarne *ex post* i correttivi; trova piuttosto corrispondenza in un controllo che affianca, passo dopo passo, l'azione amministrativa nei singoli segmenti di attuazione delle diverse misure e interventi voluti dal Legislatore e bisognosi di trovare, per essere efficaci, corretta e tempestiva attuazione presso le Amministrazioni competenti (cfr. Corte dei conti, Coll. contr. concomitante, del. n. 8/2023).
Il sindacato di tipo "concomitante" si riferisce, in questo quadro, a un controllo su gestioni "in corso di svolgimento", cioè "... gestioni non ancora concluse, in ordine alle quali sono possibili interventi correttivi tali da poter determinare il mancato avverarsi, o quanto meno l'interruzione, di situazioni illegittime o pregiudizievoli" attraverso correttivi "in corso d'opera, mirati anche alla prevenzione, come tali più efficaci di quelli essenzialmente preordinati a misure di riparazione del danno o all'indicazione di correttivi" (cfr. Corte dei conti, SS.RR. in sede di controllo, del. n. 29/CONTR/09).
Gli esiti dell'attività di controllo concomitante possono trovare formale categorizzazione nei sensi che seguono:
• casi previsti dall'art. 11, c. 2, della L. n. 15/2009 (gravi irregolarità gestionali o gravi deviazioni da obiettivi, procedure o tempi di attuazione), con espresso richiamo all'art. 22 del D.L. n. 76/2020 e riferimento alla comunicazione, per il tramite del Presidente della Corte dei conti, al Ministro, il quale può disporre la sospensione dell'impegno delle somme; casi di rilevanti ritardi nella realizzazione di piani e di programmi, di erogazione di contributi, ovvero nel trasferimento di fondi, con comunicazione al Ministro competente, che provvede alla rimozione degli impedimenti o adotta gli atti previsti dalla norma;
• casi previsti dall'art. 22 del D.L. n. 76/2020 (gravi irregolarità gestionali o rilevanti e ingiustificati ritardi nell'erogazione di contributi), con comunicazione all'Amministrazione ai fini della responsabilità dirigenziale, ai sensi e per gli effetti di cui all'art. 21, c. 1, del D. Lgs. n. 165/2001.
Qualora, nell'esercizio delle funzioni di controllo concomitante, venga altresì accertata la presenza di ritardi o di carenze gestionali non tali da integrare la soglia di gravità prevista dalle soprarriferite disposizioni ex L. n. 15/2009 e D.L. n. 76/2020, il competente Collegio del controllo "può indirizzare all'Amministrazione specifiche raccomandazioni e avvisi (warning), affinché venga stimolato un percorso auto-correttivo che l'Amministrazione stessa potrà declinare sia sul piano delle modifiche delle decisioni normative, dell'organizzazione amministrativa, delle attività gestionali, sia sul piano dei "controlli interni", al fine di pervenire ad una più efficace ed efficiente gestione delle risorse finanziarie" (cfr. Corte dei conti, Coll. Contr. concomitante, del. n. 2/2022).
Nel quadro ordinamentale è manifesta la necessità di intensificare e prevedere un controllo tempestivo con intenti propulsivi ("acceleratori"), in correlazione al corretto impiego delle risorse disponibili, in parte provenienti anche dall'Unione europea e rimesse alla gestione pubblica, al fine di intercettare e, ove possibile, prevenire, attraverso un dialogo aperto con le stesse Amministrazioni, gravi irregolarità gestionali o gravi deviazioni da obiettivi, procedure o tempi di attuazione stabiliti da norme, nazionali o comunitarie, ovvero da direttive del Governo.
Il controllo concomitante è chiamato, pertanto, ad attenzionare in *itinere* deviazioni e scostamenti in grado di compromettere investimenti di rilievo anche strategico per il Paese, lasciando al contempo all'Amministrazione la responsabilità di attivarsi per evitare il "fallimento" della propria azione.
In questo contesto, il Collegio intende continuare ad avvalersi dello strumento della "raccomandazione" – oltre che degli esiti normativamente previsti – che risulta particolarmente adatto a stimolare un percorso auto-correttivo – declinabile dall'Amministrazione sia sul piano delle proposte di atti normativi, dell'organizzazione amministrativa e delle attività gestionali, sia sul piano dei "controlli interni" – in modo da portare ad una più efficace ed efficiente gestione delle risorse finanziarie (Corte dei conti, Coll. Contr. Concomitante, del. n. 1/2023).

Gli interventi del PNRR

A questo punto, ci si rivolgerà quindi alla più specifica tematica in trattazione, concernente il controllo concomitante sugli interventi del PNRR.
La funzione di controllo concomitante è esercitata sui principali piani, programmi e progetti relativi agli interventi di sostegno e di rilancio dell'economia nazionale di cui risultano titolari le Amministrazioni, sulla base di un programma annuale deliberato dallo stesso Collegio del controllo concomitante.
In questo quadro deve essere quindi esaminato il fondamentale documento di programmazione dei controlli espresso dal Collegio del controllo concomitante per l'anno 2023 (cfr. cit., del. n. 1/2023), in cui il Consesso evidenzia la necessità di "dare continu-

ità alle attività di controllo già avviate nella fase di start-up della struttura, conferma la scelta di concentrare, anche per il presente anno, l'attività istruttoria prevalentemente sui "piani, programmi e progetti" già individuati nel corso del 2022" (cfr. del. n. 1/2023; del. n. 1/2022 e 12/2022).
Il Collegio conferma, altresì, la scelta di porre particolare attenzione agli interventi oggetto del PNRR e del Piano nazionale complementare, attesa la rilevanza strategica che occupa questo Piano – ed i correlati interventi nazionali - nel quadro delle iniziative di rilancio e sviluppo economico-sociale del nostro Paese, essendo caratterizzati da maggiore rilevanza finanziaria, impatto socio-economico su cittadini e imprese, nonché dalla possibilità di colmare i tanti gap, anche di natura infrastrutturale, accumulati dal nostro Paese negli ultimi decenni. Fermo restando che, come previsto dallo stesso art. 22 del D.L. n. 76 del 2020, il Collegio potrà essere attivato "anche a richiesta del Governo o delle competenti Commissioni parlamentari".
Al contempo ritiene, tuttavia, di dover aggiungere a questi ultimi, alcuni progetti oggetto di recenti interventi normativi e della legge di bilancio per il 2022, finalizzati, in particolare, al contrasto delle emergenze idriche ed energetiche verificatesi nell'ultimo periodo e tuttora di stretta attualità, avviando in tal modo il fisiologico spostamento del baricentro del controllo concomitante di competenza di questo Collegio verso l'area "extra PNRR".
"Quanto agli strumenti del controllo concomitante (nel rinviare anche in questo caso alla del. n. 1 del 2022), l'attività istruttoria sarà svolta, nel rispetto del principio del contraddittorio con le amministrazioni, con le consuete metodologie del controllo sulla gestione – in questo caso in itinere o real time – auspicando peraltro, con riferimento ai progetti oggetto del PNRR, il superamento del perdurante insufficiente popolamento dei dati, e soprattutto dei documenti, sul sistema ReGis, ossia sull'applicativo che dovrebbe costituire "lo strumento unico attraverso cui le Amministrazioni interessate a livello centrale e territoriale adempiono agli obblighi di monitoraggio, rendicontazione e controllo delle misure e dei progetti finanziati dal PNRR" (cfr. Circolare MEF-RGS 21 giugno 2022, n. 27). A tale ultimo riguardo, si ribadisce, anche in questa sede, come la completezza, la tempestività e l'esaustività della documentazione (e non dei soli dati) disponibile online, in forma digitale, sul ReGis, consentirebbe una maggiore celerità della prima fase istruttoria di competenza di questo Collegio, evitando in tal modo di onerare le amministrazioni con eccesive richieste istruttorie (in omaggio al "principio di non aggravamento istruttorio", già richiamato nella citata deliberazione n. 1/2022)" (cfr. cit., del. n. 1/2023).
Nell'allegato 1 alla sopra riferita delibera n. 1/2023 sono evidenziati, per ciascuna area tematica di interesse, i piani, programmi e progetti statali le cui attività prevedono tappe intermedie di attuazione già nel corso del 2023 e che, pertanto, saranno oggetto di controllo concomitante nell'anno in corso, la maggior parte dei quali, come detto, già oggetto di controllo concomitante nel corso del 2022, con espressa riserva di integrazione o modifica relazione all'eventuale evoluzione del quadro normativo relativo agli interventi di sostegno e rilancio dell'economia nazionale.

Un caso pratico, la tutela del verde nel territorio urbano e extraurbano

Nel quadro dei riscontri in esame è stato segnalato, da parte del Collegio (del. n. 8/2023, depositata il 15 marzo 2023), il ritardo nella realizzazione dei progetti sulla tutela verde nel territorio urbano e extraurbano. Il riferimento è all'allocazione di risorse PNRR nel quadro della realizzazione degli obiettivi europei concernenti la piantumazione.
Il progetto prevede una serie di azioni, rivolte ai territori di 14 città metropolitane, particolarmente esposte a problemi legati all'inquinamento atmosferico, all'impatto dei cambiamenti climatici e alla perdita di biodiversità, con effetti negativi sul benessere e sulla salute dei cittadini. La misura include lo sviluppo di boschi urbani e periurbani, attraverso la piantumazione di almeno n. 6.600.000 alberi (per 6.600 ettari di foreste urbane).
Gli obiettivi principali dell'intervento si correlano a 1) miglioramento della qualità dell'aria e della vita in 14 città metropolitane (Bari; Bologna; Cagliari; Catania; Palermo; Firenze; Genova; Milano; Messina; Napoli; Reggio Calabria; Roma; Torino; Venezia) e 2) tutela della biodiversità.
L'investimento prevede, a valere sulle risorse stanziate per il PNRR, un importo complessivo di euro 330.000.000,00, tra "Progetti in essere" e "Progetti nuovi" (di cui euro 300.000.000,00 per i "Progetti nuovi").
Per l'attuazione dell'Investimento è stata costituita presso il Ministero dell'Ambiente e della Sicurezza Energetica una "Cabina di Regia", con la partecipazione di ISPRA (Istituto Superiore per la Protezione e la Ricerca Ambientale), CUFA (Arma dei Carabinieri, Comando Unità Forestali Ambientali e Agroalimentari) e ISTAT (Istituto Nazionale di Statistica) e con il supporto del CIRBISES (Centro di Ricerca Interuniversitario Biodiversità, Servizi ecosistemici e sostenibilità), che ha il compito di seguire tutto il percorso operativo, a partire dal necessario sostegno tecnico e scientifico, fino alle fasi di monitoraggio degli effetti diretti e indiretti dei nuovi boschi urbani.
Il monitoraggio dell'avanzamento procedurale e fisico degli interventi si ricollega all'utilizzo dei sistemi informativi RGS.
I riscontri sul territorio sono stati effettuati dall'Arma dei Carabinieri, la quale ha riferito che, in senso difforme da quanto programmaticamente previsto, sono stati piantati in vivaio semi originari, anziché innestare (nei luoghi individuati) piante già sviluppate.
Nella sostanza, le criticità rilevate hanno riguardato sia il grande ritardo nella realizzazione degli interventi (perlopiù ancora allo stadio progettuale, o addirittura solo svolti nell'*iter* documentale amministrativo), sia difetti strutturali negli innesti (le piante si sono seccate, per incuria o per inadeguatezza).
Il Collegio ha segnalato, tecnicamente, la discrepanza sussistente fra la coltivazione dei semi e l'innesto di piante già in fase di sviluppo, suggerendo al Ministero dell'Ambiente e della Sicurezza Energetica di verificare la corretta e tempestiva implementazione delle attività previste in ognuna delle città interessate dalla piantumazione dei 6.600.000 alberi in totale programmati.
Al termine delle verifiche della prima fase istruttoria condotte sulla misura "Rimboschimento urbano e tutela del verde PNRR M2 C4 - 3.1" il Collegio del controllo concomitante ha quindi 1) formalmente accertato che non sussistono criticità tali da implicare allo stato le conseguenze di cui all'art. 11 della L. n. 15/2009 e dell'art. 22 del D.L. n. 76/2020 e, nel contempo, 2) formulato diverse raccomandazioni al Ministero dell'Ambiente e della Sicurezza Energetica.

In particolare:
• per i Progetti in essere, ha raccomandato di a) adottare le opportune iniziative per accertare la sussistenza dei requisiti progettuali e procedimentali previsti dal PNRR per l'ammissione a finanziamento; b) vigilare sulla corretta ed efficace esecuzione dei lavori presso ciascuna Città metropolitana;
• per i Progetti nuovi, di c) assumere ogni iniziativa idonea ad acquisire un pronunciamento certo della Commissione europea circa l'effettiva equiparabilità della semina o della coltivazione in vivaio alla messa a dimora in situ delle piante; d) adottare un cronoprogramma dettagliato sui tempi del *"planting"* e del *"transplanting"* necessari per ogni tipologia di specie arborea, ai fini del rispetto di entrambi i target europei Q4 2022 e Q4 2024.
Per entrambe le tipologie di progetto, ha raccomandato di monitorare con continuità l'attuazione, da parte dei Soggetti attuatori, delle ulteriori fasi del Piano (al fine di scongiurare eventuali ritardi che possano pregiudicare il raggiungimento del secondo target Q4 2024).
Il Collegio ha invitato l'Amministrazione a riferire, nel termine di trenta giorni dal ricevimento della delibera, in merito alle eventuali misure che ha inteso adottare per superare le criticità segnalate, avvisando che, alla mancata comunicazione nel termine assegnato sarebbe stato attribuito il significato di mancata adozione di ogni misura.
Le criticità segnalate in fase di controllo concomitante sono state recepite nel senso che l'Amministrazione riferisce di avere avviato processi di correzione al fine di implementare l'effettiva piantumazione.
Il quadro complessivo del Piano di Resilienza induce a lamentare, peraltro, ripetuti ritardi; la visione strategica dell'Amministrazione, in tale scenario, parrebbe ricollegarsi non tanto alla necessità di ottenere proroghe nella realizzazione degli interventi, ma di modificare o addirittura cancellare, anche valorizzando le indicazioni ottenute in sede di controllo concomitante, in un quadro di flessibilità, i programmi che si manifestino incoerenti o scarsamente realizzabili con le modalità previste.

La responsabilità dell'ente da reato tributario: considerazioni metodologiche su valutazione del rischio e predisposizione del modello organizzativo

di Ivano Maccani e Diego Tatulli

Come è noto, laddove venga commesso uno dei reati annoverati nel D. Lgs. 231/2001, nell'interesse dell'ente e da un soggetto qualificato, è possibile schivare le conseguenze sanzionatorie previste dalla normativa di settore ove si dia dimostrazione di avere precedentemente costituito un idoneo ed efficace modello organizzativo.

Tale esimente può essere invocata dall'ente sotto accusa solamente nel caso, al di là degli sforzi formali profusi nella predisposizione di un assetto regolamentare interno astrattamente capace di conformare i processi di controllo interni alle cautele imposte dall'ordinamento, siano provati il previo svolgimento di un'attività ricognitiva sui rischi cui è esposto il *business* aziendale (*risk assessment*) ed il coerente approntamento di presidi gestionali coerenti con i rischi identificati (*risk management*).

Ne deriva che ogni ente dovrà dotarsi di meccanismi di controllo attagliati alle proprie esigenze, se vuole che il proprio modello organizzativo venga preso in considerazione in termini esimenti.

A mero titolo esemplificativo, un ente che coltivi strutturali rapporti con la pubblica amministrazione, perché concessionario di un servizio pubblico ovvero fornitore di beni e/o servizi per numerose società pubbliche, dovrà tarare i percorsi formativi sull'esigenza che le condotte dei propri dirigenti – nelle fasi di aggiudicazione e di esecuzione del contratto – non si traducano in delitti contro la pubblica amministrazione.

Una società che, invece, sia impegnata in generiche attività edili, fortemente foraggiate dai numerosi *bonus* fiscali introdotti per stimolare la ripresa economica del Paese - talvolta illecitamente strumentalizzati negli ultimi tempi - dovrà, tra l'altro, istruire meticolosamente i propri dirigenti affinché non si cada risucchiati in una di quelle frodi multimilionarie troppe volte svelate dagli organi investigativi.

In questo scenario si coglie agevolmente la reale importanza di conoscere quali sono i metodi ricognitivi dei rischi[1] giudicati positivamente dalla giurisprudenza e le caratteristiche dei modelli organizzativi prese in considerazione dagli inquirenti, nella prospettiva di verificare se i presidi apprestati abbiano avuto un ruolo meramente formale, inidoneo a proteggere l'ente coinvolto dalla scure sanzionatoria, ovvero esprimano un ragionato e virtuoso tentativo di tutelare la legalità, sebbene l'arguzia del dirigente infedele abbia avuto la meglio.

Il *risk assessment* quale punto di partenza

Prima di procedere ad una più dettagliata esposizione delle regole da seguire, è opportuno sottolineare che il metodo di analisi qui condiviso ben si presta ad essere calato nel contesto delle società di capitali, per le quali già il Codice Civile fissa alcuni obblighi assolutamente complementari alle finalità che ogni modello organizzativo è incaricato di perseguire.

Nelle società di capitali, ad esempio, uno stimolo importante ad intervenire efficacemente sul modello, è atteso dai sindaci, non tanto per le generali responsabilità codicistiche assegnate all'Organo di Controllo, non sempre colte nella loro reale dimensione, quanto per le competenze specifiche possedute dai componenti.

E' stato, infatti, evidenziato in più occasioni che il rischio di commissione dei reati fiscali e, oggi, delle collegate conseguenze 231, sia più consistente nelle imprese con amministratori unici e senza organi di controllo rispetto a quanto non lo sia nelle società assoggettate ad un'amministrazione collegiale ed alla vigilanza di Sindaci e Revisori.

L'esperienza investigativa e giudiziaria, tuttavia, ha fatto emergere che nelle interazioni tra società strutturate e piccole/medie imprese, il rischio di coinvolgimento in attività fiscalmente criminali – cui è più esposto il soggetto di minori dimensioni - può infettare anche la controparte meglio strutturata, soprattutto laddove le attività di *due diligence* e di vigilanza nella esecuzione dei contratti siano prese alla leggera.

Un esempio concreto può ben spiegare questa dinamica: se un dirigente di una complessa società di capitali intende ridurre fraudolentemente la base imponibile della propria impresa, potrà richiedere alla piccola controparte di sovraffatturare le operazioni esternalizzate (circostanza che non sarà facilmente intercettata in seno ad una piccola realtà, magari a conduzione famigliare, priva di adeguati presidi di

1 *Al riguardo, si segnala la pubblicazione "Reati tributari: la responsabilità degli enti ex D. Lgs. n. 231", di Ivano Maccani, Luigi Fruscione, Angelo Jannone e Denise Boriero - Ed. Seac – 2021. L'opera contiene una dettagliata analisi di tutte le sfaccettature della normativa de qua, mettendo in relazione i distinti e numerosi profili giuridici che l'istituto in commento coinvolge sul piano tributario, societario e penale.*

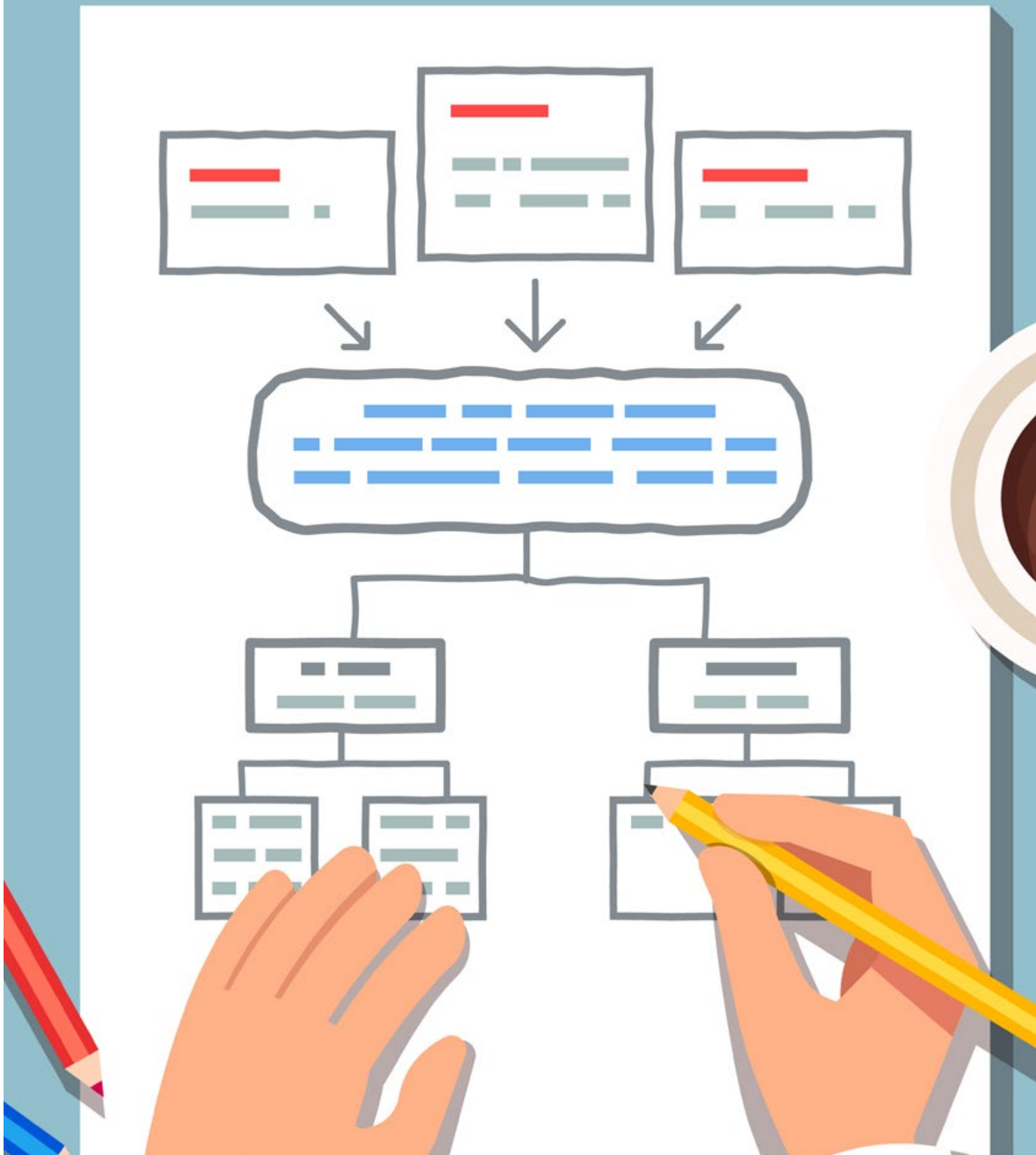
controllo), giovandosi, sul piano criminale, della debolezza organizzativa della controparte.
I reati tributari coinvolgono sia i flussi finanziari sia le sottostanti operazioni economiche, così come definite dai contratti stipulati, mettendo fisiologicamente in relazione più soggetti economici, ragion per cui sono richieste tante più attenzioni quanto meno strutturata e l'altra parte negoziale.
Su tali premesse poggia l'obbligo gravante sugli Enti di eseguire un adeguato *risk assessment*, individuando precisamente le aree di rischio, presupposto metodologico cogente ai sensi dell'art.6 del D.Lgs. n. 231/01, capace di fare la differenza nell'eventualità che il modello organizzativo venga esaminato in una prospettiva esimente.

Dalla teoria alla pratica: iniziative concrete per ridurre il rischio che nell'ente si consumino attività illecite

In principio, è opportuno porsi la seguente domanda: quali sono le azioni che in concreto vanno valutate ai fini di tale *assessment*?
Prima di ogni altra considerazione, vanno enucleate tutte quelle attività che intervengono fisiologicamente nella definizione delle obbligazioni tributarie, qualunque sia l'indicatore di capacità contributiva imputabile all'ente, potenzialmente rilevanti ai fini della commissione dei reati tributari.
Oltre a queste, debbono essere prese in considerazione quelle ulteriori attività e processi, esterni all'area "*tax*", strumentali rispetto alla commissione dei reati in questione: è il caso di quelle funzioni complementari che si occupano (1) della registrazione contabile delle operazioni quotidiane, (2) della tenuta dei libri contabili e della documentazione commerciale in generale, ovvero (3) dei processi rilevanti ai fini della corretta esecuzione degli adempimenti fiscali, come l'aggiornamento delle variazioni del magazzino.
Tra le fasi del ciclo imprenditoriale più esposte al rischio di essere illecitamente strumentalizzate, e che, pertanto, dovranno essere prioritariamente e più attentamente monitorate e presidiate, in quanto più sensibili alle frodi concepite dagli artt. 2 e seguenti del D.Lgs. n. 74/2000, rientrano a pieno titolo quella dell'approvvigionamento di beni e servizi, inquadrabile nell'area "amministrazione e finanza" e quella servente alla predisposizione del bilancio e delle dichiarazioni fiscali.
A tal proposito, si segnala che i protocolli di prevenzione dovranno prevedere, per ogni operazione di acquisto e/o vendita:
- un'adeguata tracciabilità, tramite una curata raccolta di ordini e contratti scritti, in cui dovranno essere chiaramente indicati prezzi o corrispettivi, al fine di consentire una verifica di congruità;
- appropriati e preventivi approfondimenti sui fornitori (visura camerale per valutare l'esistenza e la rispondenza tra la prestazione indicata in fattura e l'oggetto dell'attività dichiarata; autocertificazioni circa precedenti condanne e carichi pendenti degli esponenti e documenti DURC fiscali e contributivi) per valutarne l'affidabilità;
una verifica di congruità tra chi materialmente cede i beni o presta servizi ed il soggetto che emette fattura;
- una verifica sull'intestazione del conto utilizzato per i pagamenti;
- l'effettivo luogo di giacenza delle merci acquistate.
Alle fasi operative critiche sopra enumerate vanno aggiunte quelle amministrative, legate alla corretta esecuzione delle operazioni di rendicontazione civilistica e fiscale, la cui taratura, per essere ritenuta soddisfacente, deve tener conto di quanto verrà di seguito esposto.
Il sistema di controllo interno non può considerarsi statico, in quanto le varie fasi della vita dell'ente, i cambiamenti del mercato e le novità legislative periodicamente introdotte ne richiedono un costante aggiornamento.
In tal senso, ogni revisione del Modello Organizzativo deve partire da un riscontro sulla efficacia dei controlli introdotti nelle aree di rischio censite, attraverso un processo di *gap analysis*, vale a dire di misurazione della distanza (se esistente) tra i risultati teoricamente attesi e quelli realmente conseguiti. Tale attività ricognitiva vale anche per i reati tributari, per i quali lo schema di analisi deve prevedere i seguenti *step*:

<u>Analisi di contesto ed anamnesi storica</u>

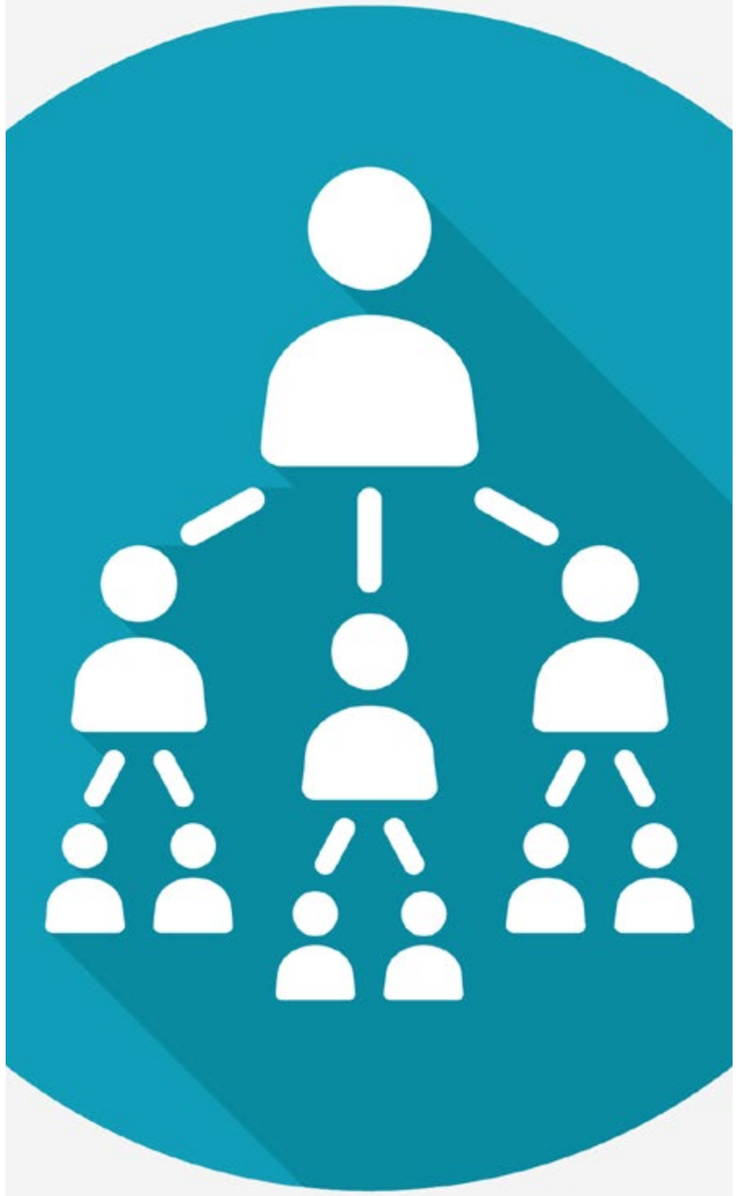
In questa prospettiva, è necessario comprendere, attraverso l'esame della giurisprudenza, delle linee guida, della dottrina e delle circolari, come si può manifestare in concreto la singola fattispecie di reato, per poi analizzare la storia fiscale della società al fine di comprenderne i punti di debolezza, ponendovi rimedio. In particolare:
- l'evoluzione giurisprudenziale sulle fattispecie di reato rilevanti e le pronunce delle Corti, anche di merito, possono fornire indicazioni utili sulle concrete modalità esecutive dei reati, contribuendo ad identificare i rischi in concreto;
- l'analisi della storia fiscale della società (c.d. anamnesi fiscale), ossia l'insieme delle passate vi-



cende fiscali, quali, ad esempio, i contenziosi avuti con le Autorità Fiscali, ma anche le frodi interne gestite in passato, potenzialmente capaci di produrre un illecito impatto fiscale, consentono certamente di comprendere meglio la propensione al rischio dell'ente scrutinando.

Identificazione e valutazione del rischio teorico
In questa fase è necessario:
- passare al setaccio i processi aziendali finali e di supporto che incidono sul rischio fiscale;
- monitorare i comportamenti concretamente adottati rispetto ai processi ed alle attività sensibili, focalizzando l'attenzione sugli snodi decisionali. Debbono essere definite precise regole di condotta concretamente attuabili, perché coloro che sono coinvolti nei processi e nelle attività aziendali sopra identificate siano precisamente guidati;
- pesatura del rischio potenziale, secondo logiche quali/quantitative.

Valutazione dei controlli preesistenti e del rischio residuo
In questa ultima fase si procede alla ricognizione dei preesistenti moduli di controllo - di natura procedurale, organizzativa e di sistema - inseriti per prevenire altri reati (es. corruzione). Si tratta, in altri termini, di comprendere se le attività più delicate siano già eseguite ed organizzate secondo efficaci *standard* e regole di controllo. In tal senso, è opportuno verificare l'esistenza di disposizioni sottese alla:
- formalizzazione delle regole secondo procedure;
-segregazione di ruoli, onde evitare che ci sia sovrapposizione tra controllato e controllore;
- tracciabilità delle attività, ovvero documentazione dettagliata delle azioni per ricostruire quanto fatto ed eseguito;
- chiara attribuzione delle deleghe interne, a cui devono corrispondere poteri coerenti;
- riduzione dei controlli manuali ed introduzione di sistemi informativi aziendali (gestionali e contabili), impostati coerentemente con i poteri attribuiti.
Qualunque deroga alle regole su cui si fonda il modello, così come sopra richiamate, dovrebbe prevedere obbligatoriamente la comunicazione all'Organismo di Vigilanza, che, se effettivamente indipendente ed autonomo, ha l'onere di vagliare l'appropriatezza della proposta, anche secondo una logica di campionamento, in modo da poter ragionevolmente escludere abusi di qualunque natura.
È facilmente intuibile che un sistema di controlli così congegnato, nato per rendere meno agevole,



ad esempio, la costituzione di provviste destinate ad attività corruttive, riduce drasticamente il rischio di fatturazioni false, usualmente valorizzate nella costituzione dei c.d. fondi neri.
Sul punto è bene rimarcare che il dolo specifico di evadere le imposte rileva solo nella configurabilità della ipotesi di reato, non anche nell'accertamento della responsabilità dell'ente, ragion per cui si potrebbe andare esenti da responsabilità realizzando un modello organizzativo che, in termini oggettivi, fornisca regole precise e tari correttamente i controlli di coerenza interna.
Aldilà del semplice esempio sopra riportato, le condotte astrattamente idonee a perfezionare i reati tributari rilevano concretamente ai fini "231", proprio perché possono attraversare plurime aree aziendali e, soprattutto, possono propiziare la commissione di ulteriori e ben più gravi reati (dal riciclaggio alla bancarotta fraudolenta), a seconda della finalità perseguita dal soggetto attivo.
Sicuramente, nella definizione dei presidi da approntare, giocano un ruolo fondamentale le numerose variabili - interne ed esterne - che normalmente caratterizzano la vita dell'impresa: le dimensioni, la possibilità di collocare sui mercati regolamentati i propri strumenti finanziari, la natura del mercato in cui operano - regolamentati e non, *retail* o B2B - infatti, incideranno necessariamente sulla conformazione delle cautele da predisporre, laddove si voglia costruire un modello organizzativo idoneo a ridurre il rischio da reato.

Ulteriori classificazioni utili alla costruzione del modello organizzativo
Una distinzione utile di ordine generale potrebbe essere quella tra le tipologie di processo che attraversano il ciclo dell'impresa: operativo, contabile e fiscale.
Si tratta di blocchi di attività in cui si producono i dati che potrebbero "comporre" una fattura falsa o concorrere alla presentazione di una dichiarazione dei redditi infedele.
Come sappiamo, ogni realtà produttiva si basa su due cicli di processi fondamentali: il ciclo attivo ed il ciclo passivo.
Ognuno di questi cicli parte da fenomeni operativi (es. processo di gestione delle consulenze-formazione, dell'albo fornitori, del processo di vendita), che innescano una o più operazioni contabili (es. registrazione fatture, accertamento dei costi, accertamento dei ricavi, adempimenti connessi al servizio di tesoreria e pagamenti) per poi restituire precisi *output* fiscali (es. calcolo dell'obbligazione tributaria e versamento imposte, es. IVA).
Esempio di processo operativo: *iscrizione albo fornitori e gestione del fornitore*, a cui corrisponderà, ad esempio, il processo contabile sensibile del *Servizio di tesoreria*. Concluderà il ciclo il processo fiscale sensibile del Calcolo dell'IVA e di eventuali crediti.
Un altro esempio di ciclo sensibile, caratterizzato da fasi operative, contabili e fiscali può essere ricondotto alla sequela:
- gestione delle vendite (processo operativo);
- accertamento dei ricavi (processo contabile) e i correlati costi ricorrenti;
- identificazione ed applicazione del regime di competenza degli oneri fiscali appropriato (processo fiscale).
Un'ulteriore possibile distinzione può riguardare:
- processi e rischi diretti, ovvero quei processi in cui, avendo luogo attività di natura fiscale, come la predisposizione e la presentazione delle dichiarazioni fiscali, la liquidazione e il versamento dei tributi e la tenuta e la custodia della documentazione obbligatoria, possono comportare la diretta commissione dei nuovi reati tributari inseriti nel Decreto 231;
- rischi e processi indiretti, in quanto non prevedono attività di natura fiscale, ma solo condotte c.d. propedeutiche alla commissione degli stessi. Consistono in attività di natura operativa, non direttamente connessi ai processi fiscali, ma che possono generare conseguenze sulla correttezza fiscale e potenzialmente rilevanti per la commissione dei reati tributari.
Sono esempi di processi indiretti la gestione dell'anagrafica fornitori, soprattutto per alcuni dati che dovrebbero essere difficilmente modificabili, come l'IBAN, se non attraverso un processo autorizzativo; la gestione della rete di vendita per il rischio di contratti fasulli per finalità di frode; gli acquisti di beni e servizi, un processo che, se fuori controllo, può essere generatore di fatture passive non rispendenti al vero con conseguenti impatti sul corretto calcolo delle imposte (ma prima ancora sulla trasparenza del bilancio). Anche la gestione del personale, in teoria, almeno per le aziende più strutturate, può generare una serie significativa di costi sulla cui deducibilità è opportuno fare delle riflessioni (si pensi, in tal senso, alle risorse stanziate per rimborsare le trasferte ed altre attività onerose demandate ai dipendenti).
Tra i processi direttamente esposti al pericolo di strumentalizzazione illecita, è possibile censire quello di gestione della determinazione delle imposte, riferita al calcolo degli importi dovuti, quello di gestione degli adempimenti fiscali, inteso come identificazione di ruoli e responsabilità, scadenze temporali, rap-

porti con le autorità fiscali, quello di gestione della contabilità fornitori, riconducibile alla registrazione delle fatture passive, per i rischi connessi all'art.8, che punisce l'emissione di fatture o altri documenti per operazioni inesistenti, quello inerente alla fatturazione attiva, per il rischio di emissione di fatture false, soprattutto nei rapporti tra società riconducibili ad una medesima *holding*, nonché quello di definizione delle compensazioni debiti/crediti. Ricordiamo che nel concetto di altri documenti secondo recente giurisprudenza rientrano anche i documenti doganali.

Ma quali sono invece i punti chiave di controllo (*c.d. critical control point)*?

Anche per i reati tributari, i controlli chiave di natura preventiva derivano dai principi generali del sistema di controllo interno, da un lato, e dall'esperienza investigativa dall'altro. Ricordiamo al riguardo che, come qualunque ulteriore area di rischio reato, i controlli chiave sono quelli che consentono, in una logica di *accountability*, di provare che l'Ente ha fatto di tutto per restringere le maglie, nei limiti delle proprie possibilità, per impedire condotte illecite (idoneità del modello), a condizione che tali controlli siano concretamente attuati (efficace attuazione).

I principi di controllo interno suggeriscono come sempre:

- la formalizzazione delle regole, soprattutto di natura amministrativo-contabile (es. *revenue recognition* o accertamento dei ricavi), in modo da assicurare la corretta applicazione dei principi di competenza;
- l'accertamento dei costi, mediante un processo tracciato con una chiara identificazione delle responsabilità e di ruoli, tra chi attesta l'effettiva prestazione o la fornitura, in coerenza con quanto contrattualmente previsto (entrata merci), e chi registra il costo;
- la formalizzazione delle procedure di rettifica (risconti attivi e passivi), ossia di quelle operazioni necessarie a riportare nella corretta competenza di esercizio alcune variazioni economiche, in tutto o in parte, che possono impattare sui risultati di esercizio e, quindi, sul reato di dichiarazione fraudolenta;
- la procedura di acquisto di beni e servizi, che comprende l'attività di gestione di albo e anagrafica fornitori. È fondamentale prevedere *escalation* autorizzative per alcuni dei dati essenziali, tra cui l'IBAN del fornitore. Va considerato infatti che, il reato di cui all'art. 8 riguarda, come si è detto, anche la falsità soggettiva della fatturazione, che è legata al raffronto tra il documento contabili è l'effettività dei soggetti intervenuti nelle operazioni negoziali. Se il pagamento, attraverso una successiva modifica dell'IBAN, avviene verso un soggetto giuridico diverso dalla controparte contrattuale risultante in fattura (spesso per finalità di elusione fiscale, favorendo il fornitore o, peggio, per determinare la costituzione di fondi neri all'estero), si configura il reato.

La tracciabilità è meglio assicurata dai sistemi contabili, mediante controlli c.d. bloccanti. Ma in altri casi è necessario che le procedure siano accompagnate da modulistiche che consentano di ricostruire le ragioni delle scelte.

Il terreno della *compliance* organizzativa, insomma, è molto scivoloso, poiché richiede il possesso di competenze e conoscenze appartenenti a differenti branche della gestione aziendale e del diritto. Ogni ente che voglia svolgere serenamente la propria attività dal punto di vista legale ha la necessità di attrezzarsi in maniera diligente, sul piano organizzativo, delle cautele qui brevemente condivise, pur nella consapevolezza che l'eliminazione del rischio non è nelle facoltà umane ma una sua intelligente e corretta minimizzazione sì, e può fare davvero la differenza nella malaugurata ipotesi che la commissione di un reato trascini in Tribunale un ente illecitamente strumentalizzato.

Perquisizioni digitali e ausiliario di p.g.: criticità e possibili soluzioni

di Pier Luca Toselli

In un mondo iper-connesso e digitale non esiste ormai contesto nel quale un dispositivo informatico direttamente o indirettamente non sia coinvolto nella nostra quotidianità, l'assunto è ben noto a qualsiasi operatore del diritto tant'è che oggi qualsiasi decreto di perquisizione prevede sempre la cosiddetta perquisizione informatica nell'evidente considerazione che ormai il luogo in cui gestiamo e conserviamo i nostri "dati" è quasi sempre "digitale". Di qui la necessità di perquisire dispositivi digitali oggi sempre più protetti da uno o più livelli di sicurezza fisici e/o informatici. Si pensi non solo alle password che possono proteggere l'accesso ai vari dispositivi ma anche quelle cautele "fisiche" spesso obbligatorie e presenti nella maggior parte delle aziende (accessi blindati alle sale server, rack server chiusi a chiave etc.).

Sorge quindi sempre più spesso, la necessità di rimuovere quelli che nel linguaggio giuridico vengono definiti "ostacoli fissi". Tale termine si adatta perfettamente a ricomprendere nel novero non solo gli ostacoli di natura "fisica" (porte blindate, rack chiusi a chiave etc.) ma anche tutti gli ostacoli "informatici" che tutelano, proteggono, impediscono l'accesso indiscriminato ai nostri dati (password a tutela degli account, del bios, di volumi crittografati etc.). È a tutti noto come nella nostra quotidianità lavorativa e privata ci troviamo continuamente a dover "superare" quegli "ostacoli fissi" che abbiamo frapposto a tutti coloro che a vario titolo non sono autorizzati ad accedere ai nostri dati indiscriminatamente.

La polizia giudiziaria nel nostro ordinamento, in virtù di un apposito decreto dell'Autorità Giudiziaria che l'autorizzi, gode della possibilità di poter "rimuovere gli ostacoli fissi" che si interpongono a quelle attività di perquisizione e ricerca cui viene delegata. Ora se gli ostacoli fissi tradizionali (serramenti ed altre serrature) possono essere superate con l'aiuto di qualche "tecnico" della materia (fabbri e vigili del fuoco) , il tema si complica non poco quando si ha a che fare con password, codici ed altre tecniche informatiche, che se all'apparenza di facile superamento (basta inserire una password) possono di fatto costituire un baluardo talvolta impossibile da superare.

Se fino a poco tempo fa questa "rimozione ostacoli fissi" veniva ricondotta alla capacità della polizia giudiziaria di poter "bypassare", per esempio, d'imperio, la password di Windows, magari attraverso l'utilizzo di una distro linux[1]. Oggi tutto questo risulta molto più difficile e complicato, tanto da poter affermare che in taluni casi senza il ricorso a particolari tecniche e risorse non sempre disponibili, risulta pressocché alquanto complicato e laborioso, superare uno di questi ostacoli, mi si perdoni il termine, ma rende bene l'idea, "informatici".

Di qui il sempre più "necessario" ricorso all'ausiliario di P.G. sul quale vorrei proporre una serie di riflessioni e considerazioni. Forse qualcuno di voi ha già avuto occasione di sentir parlare di questa particolare figura ed in questo mio articolo, vorrei esaltare una serie di criticità legate a questa figura che se da un lato risulta ormai quasi sempre "indispensabile" dall'altro presenta sempre più spesso diverse difficoltà di individuazione, non sempre facilmente superabili.

1 *Questa fatela leggera ai vostri "administrator" di rete che la comprenderanno e ci rideranno su.*

Attorno all'ausiliario di polizia giudiziaria si tende spesso a far non poca confusione, il legislatore, in termine all'art. 348 del codice di procedura penale, al comma 4, specifica: *"La polizia giudiziaria, quando, di propria iniziativa o a seguito di delega del pubblico ministero, compie atti od operazioni che richiedono specifiche competenze tecniche, può avvalersi di persone idonee le quali non possono rifiutare la propria opera."*.

Qui i più esperti potranno già rilevare ai fini di quanto approfondirò nel seguito un primo elemento rappresentato dalla collocazione dell'articolo che pur essendo inserito nella parte dedicata all'attività di iniziativa della polizia giudiziaria, contempla il ricorso all'ausiliario di P.G. anche nelle attività delegate dal pubblico ministero, quasi a voler attribuire particolare importanza a questa figura, per l'effettuazione di alcune operazioni. La genericità della formula utilizzata dal legislatore in quel "quando compie atti od operazioni che richiedono specifiche competenze tecniche" di fatto allarga gli spazi di coinvolgimento dell'ausiliario di P.G. ad una miriade di situazioni nelle quali la polizia giudiziaria può venire a trovarsi.

In rete si trovano attraverso una semplice ricerca, diverse pagine dedicate all'ausiliario di P.G. che riepilogano nei tratti essenziali quali possano essere le persone "idonee" e quali siano le potestà e responsabilità a quest'ultime attribuite.

Molte di queste pagine a fattore comune riportano che:

- come sancito dalla Corte di Cassazione, "Qualsiasi atto compiuto dall'Ausiliario di P.G. nelle sue funzioni, è da considerarsi un atto stesso della Polizia Giudiziaria", esso assume la qualifica di Pubblico Ufficiale ed opera sotto la direzione ed il controllo della P.G.;
- i requisiti per svolgere tale Pubblica Funzione sono: Speciali competenze tecniche; Assenza di condanne; Maggiore età; Nessuna interdizione; Nessuna misura di sicurezza e prevenzione; Nessun interesse nel procedimento; Non essere stato cancellato da Albo Professionale (se inscritto);
- l'ausiliario di polizia giudiziaria non può rifiutare la propria opera;

Nel prosieguo cercherò attraverso alcuni brevi approfondimenti, di evidenziare alcune criticità legate a quanto testé elencato, basandomi su alcune esperienze operative maturate nello specifico nell'ambito della digital forensics, ove il ricorso all'ausiliario di P.G. è oggi sempre più frequente alla luce di quanto sopra già anticipato[2].

La polizia giudiziaria nel corso delle ordinarie attività d'istituto può avere la necessità di procedere ad una perquisizione anche informatica. A questo punto

2 *Basta pensare alla necessità di ottenere la password di amministratore di un sistema, ovvero quella di accesso ad un sistema protetto da bitlocker "et simila" o ancora la necessità per la polizia giudiziaria di conoscere nel dettaglio le funzioni (backup, memorizzazione, esportazione dei dati) di uno specifico sistema informatico. Ma anche le password e credenziali necessarie ad accedere al data center dell'azienda piuttosto che indicazioni specifiche circa le "politiche" di sicurezza e backup adottate a livello aziendale.*

si possono aprire sinteticamente due scenari:
a) l'organo di polizia è dotato tra il proprio personale di figure esperte, in possesso delle necessarie competenze tecniche e comunque capaci di effettuare la perquisizione informatica sul "target", in sintesi è capace in autonomia di superare "gli ostacoli fissi";
b) l'organo di polizia che interviene è privo di personale qualificato, specializzato o comunque pur essendone provvisto e recandolo al seguito, nel particolare contesto operativo in cui si trova, ad operare, non è in grado, per svariate ragioni, (essenzialmente e per dirla meglio ... per mancanza delle necessarie competenze tecniche), di procedere alla perquisizione dello specifico target;
Pur apparendo più facile ed idillica la situazione a), va precisato che oggi risulta sempre più raro non ricorrere all'ausiliario di P.G. si pensi a tutti i casi in cui il "target" è rappresentato da un server, protetto dalle necessarie misure di sicurezza; o ancora la necessità di effettuare una perquisizione informatica in presenza di software gestionali particolarmente complessi e spesso sconosciuti ai più; o ancora particolari tipologie di target (scatole nere, altre apparecchiature informatiche di uso non comune e diffuso) che richiedono specifiche competenze anche solo per apprenderne le modalità di elaborazione, trasmissione e conservazione dei dati.
Va anche considerato che l'ormai inarrestabile evoluzione tecnologica, sforna quotidianamente nuovi dispositivi digitali, accompagnati da sempre più sofisticati sistemi di gestione e protezione dei dati, che quando "superati" e noti al personale appartenente alle Forze di Polizia, vengono di fatto soppiantati da altri più recenti e complessi il cui superamento risulta sempre più complesso ed articolato.[3] Di qui la necessità di un continuo aggiornamento ma anche il ricorso nelle situazioni di urgenza e più complesse: al progettista, all'installatore, al gestore ed all'utilizzatore di quello specifico dispositivo.
È evidente quindi come in tutti questi casi, risulti necessario, anche in presenza di personale "altamente qualificato e specializzato" ricorrere quasi sempre laddove possibile alla nomina di un ausiliario di P.G. ex art. 348 comma 4 c.p.p.
Circa quando debba avvenire la nomina, dell'ausiliario di P.G., va precisato che salvo che si abbia un quadro ben chiaro e preciso di ciò che si troverà sulla "scena operativa", risulta spesso complicato e difficile se non proprio impossibile, prevedere ed individuare l'ausiliario di P.G. più adatto allo scopo! Sempre più spesso la nomina avviene "on site" e solo quando la polizia giudiziaria ha preso piena e completa cognizione di una effettiva carenza di competenze tecniche che le impediscono di procedere oltre nei compiti demandatele.
Non si può escludere infatti che anche la nomina preliminare all'effettuazione dell'operazione, di personale esperto, eviti il ricorso ad un "altro" ausiliario di P.G. "on site" riconosciuto nel particolare contesto operativo l'unica persona idonea in quanto in possesso delle necessarie competenze a risolvere un particolare atto od operazione necessaria alla P.G., che ovviamente, l'ausiliario precedentemente nominato, non è in grado di assolvere autonomamente.[4]
Nella quotidianità operativa non è difficile imbattersi in situazioni, nelle quali anche il più grande degli esperti deve arrendersi dinanzi ad ostacoli che solo l'ausiliario di P.G. (se correttamente individuato) può superare (per semplicità: le password di amministrazione del sistema piuttosto che le necessarie "credenziali" ormai biometriche necessarie ad accedere a talune sale server).
Non a caso è consigliabile premunirsi dotarsi di una rubrica aggiornata degli indirizzi di produttori, centri di assistenza, installatori etc. etc. Ciò oltre che utile per l'individuazione di un ausiliario adatto si rivela strategico per la conoscenza di funzionalità spesso non note all'utilizzatore finale ma che potrebbero rivelarsi strategiche per la polizia giudiziaria (a mero titolo di esempio alcuni sistemi realizzano anche a insaputa dell'utente file di Log. completi e dettagliati che talvolta possono risolvere le "istanze" della polizia giudiziaria attraverso l'esportazione di un semplice file di testo.
In ogni caso, è impossibile creare una casistica o un numero chiuso di casi nei quali si debba procedere alla nomina di un ausiliario di P.G., le casistiche sono pressoché infinite dipendendo da variabili quali il "target" da perquisire e la presenza o meno di personale capace ad approcciarvisi e molto ... molto altro.
Il "quando" riveste ulteriore caratteristica ed importanza. La caratteristica attiene per esempio al pagamento della prestazione resa dall'ausiliario. Invero alcune Procure della Repubblica per redimere eventuali controversie, su chi debba pagare l'intervento dell'ausiliario, sostengono che il pagamento deve avvenire a cura della P.G. ogni qual volta la stessa stia operando d'iniziativa, sostenendo invece che il pagamento dell'ausiliario avverrà a carico della A.G. requirente solo allorquando il Pubblico Ministero abbia assunto la direzione delle indagini e ne abbia delegato la nomina alla P.G. Così da specificare che la polizia giudiziaria dovrà essere in possesso di apposita delega che l'autorizza alla nomina di ausiliari di P.G. poiché solo in questo caso il compenso eventualmente riconosciuto all'ausiliario verrà corrisposto dalla Procura.
Quanto invece a chi possa essere nominato ausiliario di P.G., anche qui le variabili e le casistiche aumentano in maniera esponenziale la platea dei potenziali candidati. L'utente finale, il progettista, l'installatore, l'IT manager, l'IT security e volendone comunque definire una platea o un numero chiuso di candidati, chiunque è coinvolto a vario titolo nella **"vita"** di quel particolare sistema o dispositivo ed è in possesso di quelle specifiche competenze tecniche necessarie a compiere quegli atti ed operazioni richieste dalla polizia giudiziaria. Invero talvolta il loro intervento è legato ad azioni di natura strettamente individuale e personale (l'inserimento di una password, l'effettuazione di una procedura, la ricerca di documenti all'interno di un server, lo scarico di profili di posta, lo smontaggio di un dispositivo etc.) che non richiedono particolari abilità o competenze tecniche, ma oltre alle necessarie autorizzazioni; la conoscenza di un particolare dato, azione, tecnica, pratica ed esperienza.
Di qui due difficoltà una conseguente all'altra:
– la prima è quella di delineare correttamente l'effettività del problema (verificare quindi se il ricorso all'ausiliario è necessario e non può essere delegato ad altri); la polizia giudiziaria dovrà essere in grado di delineare il problema che si frappone alle proprie attività e richiedere quindi l'intervento di un ausiliario, solo nel caso in cui lo specifico problema non possa essere risolto altrimenti. Cosa non sempre facile se non si ha un minimo di conoscenza dei sistemi informatici, se non si è assistiti da personale esperto ma soprattutto se non si è in grado di comprendere e discernere le effettive difficoltà tecniche da quelle

3 *Si pensi alla doppia autenticazione 2FA – la gestione dei dispositivi MDM o ancora l'introduzione della biometria quale fattore 2FA.*

4 *Talvolta in sede di predisposizione dell'intervento si ricorre ad una "nomina" preliminare dell'ausiliario di P.G. tra personale tecnico particolarmente preparato sullo specifico tema (per esempio sapendo di perquisire l'azienda dotata di uno specifico gestionale si fa ricorso a personale tecnico della ditta/società produttrice del software), tuttavia anche tale attività preventiva non sempre è capace di escludere ed impedire la nomina di altro ausiliario, qualora poi sul posto vengano rilevati altri ostacoli (per esempio l'utilizzatore del gestionale è l'unico a conoscenza di dove e come vengano svolti i backup è a conoscenza delle password "private" di accesso al gestionale o è stato delegato dal produttore a detenere le password di admin del software, cosa che accade sovente per ovvie ragioni di riservatezza).*

che potrebbero essere solo scuse o supposte difficoltà di comodo, spesso avanzate se non per ostacolare l'attività della P.G., per timore, confusione, inesperienza conseguente all'intervento etc. O ancora, potrebbe trattarsi di difficoltà che possono essere "bypassate" attraverso altre soluzioni.[5]

– la seconda, individuata l'effettività del problema, occorre "ricercare" la persona giusta, opera rimessa al vaglio della P.G. che dovrà essere capace ... dato il problema ... di individuare tra una rosa di potenziali "ausiliari" quello più adatto, alla risoluzione dello stesso ed anche qui occorreranno non comuni doti ed una adeguata preparazione *tecnico-giuridico-informatica* in capo all'operatore di polizia giudiziaria. Vanno evitate infatti nomine di ausiliari che ricoprono posizioni di vertice, magari all'interno della struttura IT ma che non hanno una conoscenza così approfondita del problema da risolvere. Invero accade sovente che la nomina venga effettuata in capo ad un responsabile IT il quale poi si avvale giocoforza, non avendone le specifiche capacità di altro suo personale subordinato all'effettuazione dell'operazione (si dà erroneamente per scontato che il responsabile IT sappia fare tutto nell'ambito della rete aziendale, tuttavia soprattutto in realtà complesse vi è una necessaria frammentazione dei compiti e delle responsabilità tanto da porre il responsabile IT in una posizione sì di vertice ma che però tuttavia non si accompagna sempre ad un *"posso fare tutto io"*).

Saranno quindi le specifiche "necessità" della polizia giudiziaria a fare da sfondo all'individuazione della persona idonea ad assolvere la richiesta. Sul punto, relativamente alla necessità di una nomina scritta che individui, identifichi il soggetto interessato e contenga in sintesi l'incarico affidatogli, rappresento che la Cassazione[6] nega tale necessità, tuttavia pur nel conforto degli "Ermellini", consiglio di provvedervi, risultando l'incombente una garanzia sia per la polizia giudiziaria che per l'ausiliario. Infatti, una specifica richiesta scritta contenente, in sintesi, i motivi di ricorso all'ausiliario (ovvero quali siano le specifiche competenze tecniche riconosciute allo stesso e quali siano sempre in sintesi le incombenze a questi richieste) può a mio avviso risolvere *"ab origine"* problematiche che potrebbero sorgere in sede dibattimentale circa la necessità, competenze, ed opportunità di tale intervento; ma anche in punto di idoneità o meno di quell'ausiliario ad assolvere l'incombente. Inoltre, la forma scritta e sottoscritta anche dall'ausiliario di P.G. permette da un lato di documentare l'oggetto della richiesta dall'altro di evitare equivoci e fraintendimenti che potrebbero riverberare responsabilità penali a carico di quest'ultimo, sia in caso di rifiuto di prestare la propria opera, sia nel caso in cui quanto richiestogli non venga adempiuto correttamente o ancora peggio in modo volutamente parziale o omissivo. Un incarico dato "verbalmente" infatti potrebbe non dimostrare che l'ausiliario è stato informato dei suoi diritti e doveri ma ancora peggio non terrebbe traccia di cosa gli è stato effettivamente richiesto e se ciò poteva nello stato dei luoghi e delle condizioni presenti essere assolto. Ecco che allora la forma scritta e sottoscritta dall'ausiliario assume a parere di chi scrive elemento necessario a tutela delle parti ... ed anche. ma non ultimo all'eventuale pagamento delle prestazioni dell'ausiliario!

Relativamente al chi sia mi siano permessi alcuni specifici ed ulteriori approfondimenti.

Il primo si riferisce ai requisiti, che l'ausiliario deve possedere. L'elencazione fatta dalla maggior parte dei siti che hanno trattato detto tema si rifanno ai requisiti previsti per la figura del Consulente Tecnico del Giudice, e che si evincono dagli articoli da 69 a 73 delle Norme di Attuazione del C.P.P.

Non è mia intenzione proporre nel seguito una digressione sulle profonde differenze, che contraddistinguono la figura in trattazione da quella del consulente tecnico, mi limito qui solo a dire che le due figure sono profondamente diverse nelle loro potestà, compiti e responsabilità, tanto da non poter essere confuse.

Orbene il consulente tecnico nel caso di specie C.T.U. consulente tecnico d'ufficio è nominato, anche dopo rigorosi accertamenti, dal pubblico ministero; mentre l'ausiliario della P.G. a ragione del proprio nome è nominato da quest'ultima e solitamente in situazioni di urgenza. Come è facile rilevare alcuni dei requisiti presuppongono una serie di accertamenti e verifiche che se ben posso essere realizzate rispetto ad una "rosa" di candidati sono giocoforza rimesse ad una mera dichiarazione dell'interessato nelle situazioni d'urgenza, soprattutto quando la persona

5 Esempio classico e già sopra anticipato (agli admin) è quello relativo al superamento delle password utente di windows in assenza della persona interessata, se da un lato è vero che attraverso una password di admin è possibile accedere al pc e profilo è altrettanto vero che attraverso alcune distribuzioni linux è ancora oggi possibile accedere in modalità forense al dispositivo bypassando la necessità di password. Resterà poi da risolvere l'eventuale presenza di dischi crittografati, ma questo è un altro problema. Faccio qui l'esempio della cassaforte nella stanza con porta chiusa a chiave. Per superare la porta basta un passpartout (distro linux) ma poi mi ritroverò nella necessità di un fabbro (password admin per le password di Bitlocker) per aprire la cassaforte. Ancora, si pensi alla diffusione di sistemi complessi della gestione della rete aziendale, talvolta gestiti da società esterne ed estere, che richiedono per l'accesso e gestione dei dati ivi contenuti una "collaborazione" tra polizia giudiziaria, titolare dei dati e per l'appunto gestore esterno.

6 Sez.III, sent.n. 17177 del 18-02-2010 (ud. Del 18-02-2010), (rv. 246978)

sia peraltro "l'unica idonea" sul posto ad assolvere lo specifico compito.
Ovvero laddove non vi è scelta ... di necessità virtù!
Alcuni esempi:
– accertare l'assenza di condanne, interdizioni, misure di sicurezza e prevenzione, non è certo compito agevole per l'ufficiale di P.G. impegnato nella perquisizione di un server aziendale che ha necessità di nominare un ausiliario, non un soggetto dalla "fedina penale" pulita, ma uno capace di risolvere urgentemente i problemi tecnici che si oppongono all'attività di polizia. Ci si domanda quindi se all'atto della nomina sia necessario richiedere al potenziale "ausiliario" un'autocertificazione circa il suo stato e di qui mi si permetta, di avvalorare allora, la necessità della forma scritta nella nomina dello stesso, dove può trovare accoglimento una formula che informi la persona dei requisiti necessari e che ove non presenti dovranno orientare (ove possibile) la polizia giudiziaria verso una diversa scelta della persona da nominare;
– nessun interesse nel procedimento...qui la cosa si fa ancora più complessa. Nella nomina di un Consulente Tecnico requisito essenziale è l'estraneità dello stesso ad eventuali interessi nel procedimento; pena, l'attendibilità delle proprie conclusioni che potrebbero essere viste quantomeno, come "di parte".
Per quanto concerne l'ausiliario di P.G. e chi ne ha esperienza non può che confermarlo, questi è spesso, nell'urgenza e nell'immediatezza, tratto da personale appartenente talvolta alla stessa azienda perquisita (es. classico l'amministratore di rete dell'azienda, l'IT Manager o suo delegato o specifico dipendente addetto ad una determinata mansione). La scelta per quanto possa apparire inopportuna è spesso (forse troppo) l'unica percorribile e non sembra dare spazio a soluzioni alternative.[7]
Sovente l'ausiliario di P.G., per i motivi già anticipati, viene ad essere molto spesso (troppo spesso) persona "dipendente" dell'azienda perquisita. La norma invero di per sé non lo vieta espressamente rifugiandosi in quell'"idonea", tuttavia è altrettanto vero ed innegabile, che molto spesso, solo un dipendente dell'azienda oggetto della perquisizione informatica, incarna quelle competenze tecniche ed è in possesso del necessario patrimonio "informativo" di cui la P.G. è sprovvista (chi ha esperienze di perquisizioni informatiche ... lo sa!), si pensi a particolari "linee" CNC produttive ove spesso solo alcuni addetti altamente specializzati sono a conoscenza del loro specifico funzionamento e sono in grado di attingere specifici dati.

Al di là di simpatici aneddoti è evidente come la nomina di un ausiliario di P.G. "insider" alla stessa compagine aziendale possa costituire quantomeno elemento di imbarazzo sia per l'azienda che per la P.G., tanto più qualora poi lo stesso si rilevi concorrente e non estraneo ai fatti in procedimento o al fine di salvaguardare la propria posizione nei confronti del datore di lavoro venga meno all'incarico demandatogli dalla P.G.
La polizia giudiziaria deve porre quindi particolare attenzione alla "posizione" del soggetto scelto, ovvero che lo stesso per qualsivoglia motivo (e si badi accade più spesso di quanto si creda), non venga poi a ricoprire anche lui la posizione di persona sottoposta alle indagini per reati a lui ascrivibili o in concorso con altri, simili o anche diversi da quelli per cui si procede. In sintesi, andrà evitata la nomina (ove possibile) in capo a coloro che ricoprono posizioni di alta responsabilità spesso *"oggettiva"* prediligendo nella scelta persone della compagine aziendale in possesso delle specifiche competenze richieste ed in posizioni escluse dalle cosiddette *"responsabilità oggettive"* legate alla carica.
Un breve accenno, infine, all'aspetto concernente l'eventuale rifiuto a prestare la propria opera da parte dell'ausiliario individuato, che molti sintetizzano in: l'ausiliario di P.G. non può rifiutare la propria opera poiché in virtù della qualifica rivestita incorrerebbe nella violazione dell'art. 328 C.P. (Rifiuto di atti d'ufficio – Omissione). Il reato in trattazione prevede una sanzione da 6 mesi a due anni, volendo qui significare che non ha certo un effetto deterrente circa eventuali condotte "omissive" di altro genere che l'ausiliario di P.G. potrebbe commettere nell'assolvimento dell'opera (ausiliario di P.G. che non rifiuta l'incarico ma assolve infedelmente lo stesso), va comunque considerato che eventuali altre omissioni potrebbero poi configurare altri reati ben più gravi e puniti in maniera più pesante (favoreggiamento personale ex art. 378 C.P. o casi di concorso nel reato ex art. 110 C.P.). Ma di ciò spesso non si informa adeguatamente l'ausiliario di P.G. ed ecco che ancora una volta ... prediligo la forma scritta, che indichi specificatamente che il "prescelto" è stato (e lo deve essere) adeguatamente informato delle "responsabilità" conseguenti a tale nomina.
In conclusione, se dal 1989 l'attuale codice di procedura penale con l'art. 348 comma 4 è risultato al passo coi tempi in tutte quelle situazioni che venivano a richiedere la nomina di un ausiliario di P.G., oggi in un rinnovato ed evoluto mondo digitale (diretto

7 *Fatico a pensare che le password di amministrazione e gestione della rete aziendale siano indiscriminatamente patrimonio di più soggetti aziendali.*

anche verso una imponente e giusta protezione dei dati), questa figura ha anche bisogno a parere dello scrivente di una nuova regolamentazione, al passo coi tempi e con le evidenti difficoltà e cambi di paradigma con i quali siamo chiamati a confrontarci.
Abbiamo visto come diverse siano le criticità che orbitano attorno a questa figura. Da un lato spero di aver aiutato i tanti imprenditori che ci leggono ad avere una più attenta ed accurata sensibilità verso quei loro dipendenti che potrebbero "giocoforza" ritrovarsi nominati quali ausiliari per un qualche motivo.[8] Dall'altro spero anche di aver sensibilizzato i dipendenti che devono essere ben consapevoli al di là di mere formule di stile ed atti, di quali siano gli effettivi doveri, diritti e responsabilità che su di loro incombono a seguito della nomina da parte della polizia giudiziaria.
Ho riflettuto sempre molto su questa figura e non è la prima volta che affronto queste tematiche, mi permetto quindi, ferme le criticità già evidenziate, di proporre in via del tutto ipotetica una proposta che a parere del sottoscritto potrebbe mitigare in parte, alcune delle difficoltà sopra evidenziate.
A seguito del GDPR (General Data Protection Regulation) sono sorte nuove figure nelle aziende maggiormente organizzate e strutturate, quale quella del DPO (Data Protection Officer) che potrebbe rappresentare quel soggetto capace di interfacciarsi in modo nuovo e moderno con la polizia giudiziaria.
Il DPO è infatti, una sorta di ibrido fra il ruolo di vigilanza dei processi interni alla struttura ed il ruolo di consulenza, nonché "ponte di contatto" e super partes con l'Autorità Garante nazionale. Di qui un ruolo certamente "privilegiato" nella gestione dei dati aziendali, tanto da vederlo in futuro, ove presente, il "referente diretto", un "ausiliario di P.G. qualificato" un "intermediario" capace insieme alla polizia giudiziaria di individuare il soggetto più adatto ad "ausiliare" la polizia giudiziaria nei compiti demandategli nello specifico contesto[9]. Elemento di preferenza nella sua individuazione e scelta da parte della P.G. sarà proprio questa sua posizione di terzietà che potrà risolvere molte delle problematiche che in questo articolo molto modestamente e senza pretesa di esaustività ho voluto evidenziare e che spero, quale operatore del diritto vengano mitigate a sicuro vantaggio delle "parti" oggi chiamate a confrontarsi in nuovo, e sempre in evoluzione, "mondo digitale".

8 *Ricordo che l'ausiliario può essere nominato anche nelle operazioni cosiddette d'iniziativa della polizia giudiziaria e non solo in quelle delegate, nulla vieta quindi che la polizia giudiziaria in via del tutto "prudenziale" allorquando debba ritenere di trovarsi dinanzi ad "indizi" di reato, proceda alla nomina di questa figura. Invero capita sovente, anche nel corso di attività amministrative del Corpo che a seguito dell'emergere di "indizi di reato" la Guardia di Finanza proceda per il prosieguo dell'attività a nomina di un ausiliario di P.G.*

9 *In taluni casi potrebbe essere lo stesso DPO la persona più adatta ad assolvere lo specifico incombente, ma in ogni caso questa sua terzietà e particolare posizione potrebbero scemare parte delle criticità qui evidenziate anche nella individuazione nell'ambito dell'azienda da questi meglio conosciuta (quanto meno sul piano della gestione e tutela dei dati) della persona più idonea a soddisfare le richieste della polizia giudiziaria.*

PNRR e Sicurezza Informatica, per le PMI un'occasione da cogliere...ancora

di Ernesto Cotugno

PNRR e Sicurezza Informatica

Il titolo dell'articolo finisce con un ...ancora, che vuole significare che se relativamente al PNRR ancora non sono state utilizzate appieno le sue numerose possibilità, c'è ancora sia tempo che modo di accedere a svariati nuovi finanziamenti; questi ultimi sono a disposizione per ridefinire e consolidare, in generale molti aspetti dell'attività aziendale, e nello specifico per rinnovare, implementare ed in alcuni casi creare quel "perimetro" di sicurezza informatica che, in qualsiasi punto del web ci troviamo (o crediamo di essere...), interessa o dovrebbe interessare tutti noi.

Perché quindi leggere questo articolo e perché vale la pena chiedersi cosa centra il PNRR con la sicurezza informatica aziendale? Come può il Piano aiutare una PMI a implementare il proprio perimetro di sicurezza sempre se ci siamo mai chiesti "*...sono veramente in pericolo anch'io...?*" Ritengo che le risposte siano un insieme di diversi fattori, e volendo già preliminarmente accennarli, sono da ricercarsi, nella intrinseca "missione" innovativa tecnologico-digitale del Piano stesso[1], nel fatto che la ricerca dei finanziamenti non deve essere sempre vista come un peso e/o come un costo ma come un investimento soprattutto a lungo termine, e poi per uno dei fattori che rappresenta un caposaldo all'interno delle PMI, il "fattore umano" che può fare la differenza anche nel campo della sicurezza informatica, campo in cui spesso però si è mostrato anello debole.

Cercherò quindi di seguito di ripercorrere questi interrogativi, illustrando brevemente perché credo che la sicurezza informatica ci debba interessare, quali dovrebbero essere gli accorgimenti aziendali di base da porre in essere (considerando le cyber-minacce più comuni) e come le opportunità date dal PNRR (o ad esso direttamente collegate), possono aiutare una PMI innanzitutto nella definizione di quel già citato perimetro di cyber-sicurezza ma soprattutto nello sviluppo della cultura dello human-firewall[2] che ritengo essenziale per affiancare, "accompagnare" e gestire software e device "fisici" di protezione.

Siamo in pericolo?

Una piccola premessa per comprendere che la sicurezza informatica riguarda tutti noi indistintamente e questo perché siamo inseriti in un "cyber-sistema" che ci circonda e di cui a volte, nostro malgrado, facciamo attivamente parte. La nostra vita personale digitale è diventata sempre più "intimamente" collegata a quella "analogica", e la nostra "internettità" è collegata molto più di quanto immaginiamo anche al nostro lavoro. Utilizziamo molto spesso in maniera "promiscua" per lavoro e per fini personali, smartphone, PC, mail, social ecc.; ad esempio per scambiarci documenti aziendali ma anche per acquisti on-line, per meeting, call di programmazione di bilancio, ma anche solo per incontrare ed accordarci con qualcuno su dove fare l'aperitivo. Tutto questo per dire che la cosiddetta "trasformazione digitale" ha praticamente annullato il confine tra mondo fisico e virtuale, aumentando la "superficie digitale utile" appetibile per la cyber-criminalità che deve portare ad un cambio di paradigma definitivo nella percezione dei rischi sottesi al digitale.

Negli ultimi anni infatti le PMI europee e italiane hanno subito molteplici attacchi informatici principalmente causati da una scarsa attenzione a quelle minime precauzioni considerate "igiene di base" dagli esperti; il famoso e più volte richiamato in svariati articoli Report Clusit[3] 2022 ha evidenziato un notevole numero di attacchi informatici[4] anche verso l'Italia[5] e senza tediarci qui con percentuali e statistiche, è stato rilevato che questa tendenza è in aumento[6].

A questo punto mi chiedo e vi chiedo, lasceremmo mai il nostro diario personale su una panchina in un

1 *Digitalizzazione, innovazione e competitività delle PMI è uno degli obiettivi del Piano Nazionale Ripresa e Resilienza (PNRR), che mira a sostenere ed implementare la competitività del sistema produttivo nazionale anche attraverso il rafforzamento e consolidamento del livello di digitalizzazione, innovazione tecnologica e internazionalizzazione. La proposta ed opportunità del Piano è indirizzata a passare da un approccio di tipo emergenziale (rappresentato dall'esperienza e dalle nuove "necessità" date dalla pandemia) a uno strategico di lungo periodo, nell'ottica di una ripartenza economica del Paese attraverso un'innovazione sostenibile e reale. Suddiviso in 6 missioni, il Piano ha destinato più di 49 miliardi di euro alla prima missione, "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo", di cui circa 31 miliardi (oltre il 60%) dedicati all'innovazione e digitalizzazione delle imprese; in questo contesto si inserisce il Nuovo Piano Nazionale Transizione 4.0 (evoluzione del precedente programma Industria 4.0), di cui al DL "Sostegni-bis" 73/2021".*

2 *La definizione maggiormente utilizzata da tutti i siti web e riviste specializzate per definire lo "human firewall" è "...un dipendente opportunamente educato, istruito e formato per riconoscere gli attacchi che sfruttano le persone e le loro lacune in ambito cyber security prima ancora che le falle tecnologiche dei sistemi informatici..."*

3 *I dati sono rilevati dal report 2022 del Clusit, la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.*

4 *L'attacco informatico più sfruttato per colpire le aziende è stato il Malware, uno speciale tipo di software in grado di infilarsi a nostra insaputa nei computer, telefonini e nelle reti aziendali per sottrarre informazioni sensibili (dati personali, informazioni riservate, etc.), ma anche il Phishing, il furto d'identità e di account e attacchi DDos hanno registrato un notevole incremento rispetto al passato.*

5 *Si rappresenta che durante la redazione dell'articolo sono stati rilevati attacchi hacker su vasta scala tra cui a decine di siti istituzionali, da quelli del Governo del Ministero della Difesa e del Viminale passando per le piattaforme di banche, carabinieri, Tim e tanti altri ancora (nella giornata di mercoledì 22 febbraio 2023). L'attacco è stato rivendicato dal collettivo di hacker filorussi "NoName057" https://notizie.virgilio.it/attacco-hacker-ai-siti-di-governo-carabinieri-e-tim-piattaforme-down-rivendicato-dal-collettivo-filorusso-1558802.*

6 *Lo scenario si è rivelato talmente serio da spingere il Governo italiano ad annunciare una strategia specifica in tema Cybersecurity, con il Decreto Legge del 14 giugno 2021 dove è stata istituita l'Agenzia per la Cyber-sicurezza Nazionale (ACN) a tutela degli interessi nazionali nel cyber-spazio. Un altro esempio per comprendere l'evoluzione più che iperbolica del fenomeno della criminalità informatica a livello globale, è dato dal fatto che nel 2011 nell'ambito del "Global Risk Report del World Economic Forum", i rischi "cyber" non erano nemmeno considerati (...sono stati introdotti solo nel 2015) ma già dal 2019 erano assunti al primo posto per impatto e probabilità di accadimento, insieme ai disastri naturali ed agli effetti globali del climate change (report World Economic Forum, 2021).*

parco? Pubblicheremmo mai i nostri sentimenti intimi sulla prima pagina di un giornale? E se siamo titolari di una attività con un marchio registrato, con un progetto innovativo, con una idea sensazionale o anche semplicemente in qualità di custodi di "segreti" di nostri clienti, andremmo a spargere ai quattro venti, senza arte né parte tutto questo? Penso proprio di no!
Anzi credo che i dati e le informazioni, che rappresentano gli asset aziendali, siano "cose" da proteggere e di cui prendersi molta cura.
Oggi prendersi cura a livello aziendale dei propri dati e delle proprie informazioni digitali, per quanto abbiamo detto prima, passa indubbiamente dall'attenzione che poniamo alla sicurezza informatica a tutti i livelli ed in tutti i settori dell'attività, per la creazione di quel "perimetro" in cui la cultura della sicurezza informatica, non deve essere uno spauracchio da temere ma funzionale consapevolezza. Questo per dire che sicuramente sono fondamentali software performanti, nuovi device e ove possibile una "sezione" informatica/IT con personale dedicato e specializzato, ecc, ma altrettanto indubbia è la necessità che come detto prima, all'interno di un'azienda il "fattore umano" sia adeguatamente consapevole che col proprio agire può determinare la sicurezza o l'insicurezza aziendale.

Sicurezza informatica aziendale: accorgimenti di base e PNRR

Lungi dal voler rappresentare "La" guida, data la vastità e complessità dell'argomento, questo articolo vuole però essere una "finestra" su quelle minime regole di base (per lo meno da conoscere per poi trovare il modo di metterle in pratica) per non essere preda del primo cyberhacker della domenica!
Alcune nozioni, magari già pensate e messe in pratica da qualcuno di voi, potranno sembrare scontate, ma i vari report sugli attacchi informatici sparsi nei numerosi articoli sia su carta che nel web, dimostrano come il cyber-malintenzionato è attento alle più piccole dimenticanze/distrazioni/lacune.
Quanto segue quindi per permettere di iniziare a configurare o consolidare buone pratiche di sicurezza informatica aziendali che, suddivise sinteticamente in relazione a criticità/azioni "fisiche"/accorgimenti "immateriali, verranno parallelamente messe in corrispondenza con i vari fondi a disposizione del PNRR così da poter programmare eventuali investimenti (naturalmente per quanto detto prima questi non possono/devono essere considerati meri costi) a medio e lungo termine.

a. Definizione degli asset digitali aziendali da proteggere: indubbiamente la prima attività afferente alla sicurezza informatica è riconoscere/stabilire a livello aziendale quali siano i dati e le informazioni digitali che meritano protezione; per spiegarci meglio, mi riferisco alle "cose" digitali cui dedicare una attenzione particolare in tema di preservazione e prevenzione. Questo molte volte può risultare difficoltoso, anche dal punto di vista concettuale/tecnico, ma è essenziale per la definizione degli asset digitali aziendali; investire anche magari in una attività di consulenza specialistica, al fine di delineare le "priorità", può sicuramente essere utile per quanto ai punti successivi.
PNRR. Le spese in oggetto sono previste nell'ambito del programma del PNRR Transizione 4.0[7] in particolare Credito d'imposta ricerca e sviluppo, innovazione tecnologica, design e ideazione estetica[8] relativo a Attività di innovazione tecnologica (comma 201 della legge di bilancio n. 160 del 27 dicembre 2019): lett. C spese per servizi di consulenza e servizi equivalenti inerenti alle attività di innovazione tecnologica ammissibili al credito d'imposta.

b. Database, dati sensibili, profilazione/condivisione accessi: non tutti all'interno dell'azienda dovrebbero avere accesso a tutti i dati; questo non per mancanza di fiducia e/o rispetto nei confronti di tutti i dipendenti, ma perché stabilire chi deve avere la possibilità di accedere anche ad informazioni sensibili e riservate deve essere premurosamente profilata ed autorizzata rispetto alle mansioni e responsabilità dei dipendenti stessi.
PNRR. Le spese relative alla profilazione delle utenze aziendali, può essere ricompresa nelle spese di cui alla lettera precedente, ove non vi sia personale aziendale specializzato/servizio IT in seno all'azienda per la richiesta di definizione e impostazione dei vari livelli di profilo, che possono essere ad esempio effettuate tranquillamente anche sulle macchine e software già in uso all'interno dell'azienda.

c. Firewall, antivirus, programmi licenziati, e aggiornamento costante (app, software,_pach ecc.): i programmi software sui dispositivi aziendali (siano essi PC o smartphone) devono essere naturalmente licenziati (certo è indubbio che non ci possiamo lamentare di eventuali problemi di sicurezza informatica se "scarichiamo" i programmi utilizzati in azienda da qualche non meglio identificato sito e/o servizio streaming comunque esso denominato, ma questa ritengo sia la base!!) e dovrebbero essere aggiornati regolarmente, al pari dei sistemi operativi; i regolari aggiornamenti permettono non solo l'accesso a nuove funzionalità e peculiarità dei diversi software, ma anche di installare patch per risolvere eventuali vulnerabilità di sicurezza. Se non vi è un servizio o una sezione dedicata, è necessario che tutto il personale sia sensibilizzato e responsabilizzato per l'installazione/aggiornamento dei programmi di utilizzo aziendale.
PNRR. a) Le spese in oggetto, sempre relative alle spese previste nella sezione Transizione 4.0, prevedono una serie di agevolazioni, sotto forma di crediti di imposta, Credito d'imposta per investimenti in beni strumentali - *Incentivi per la trasformazione tecnologica e digitale delle imprese*[9] relativamente a beni strumentali immateriali tecnologicamente avanzati funzionali ai processi di trasformazione 4.0 (allegato B, Legge 11 dicembre 2016, n. 232, come integrato dall'articolo 1, comma 32, della Legge 27 dicembre 2017, n. 205). Si considerano agevolabili anche le spese per servizi sostenute mediante soluzioni di cloud com-

7 *https://www.mise.gov.it/index.php/it/incentivi/nuovo-piano-nazionale-transizione-4-0*

8 *https://www.mise.gov.it/it/incentivi/credito-d-imposta-r-s*

9 *https://www.mise.gov.it/it/incentivi/credito-dimposta-per-investimenti-in-beni-strumentali*

puting per la quota imputabile per competenza nel 2023: 20% del costo nel limite massimo dei costi ammissibili pari a 1 milione di euro. Beni immateriali (software, sistemi e system integration, piattaforme e applicazioni) connessi a investimenti in beni materiali «Industria 4.0».

b) Un'altra opzione per l'effettuazione di un cambio/miglioramento dei software aziendali, è rappresentata dal Credito d'imposta ricerca e sviluppo, innovazione tecnologica, design e ideazione estetica, *Incentivi per spesa privata in R&S*[10] *e innovazione in particolare.* b3) Per le attività di innovazione tecnologica 4.0 e green, finalizzate alla realizzazione di prodotti o processi di produzione nuovi o sostanzialmente migliorati per il raggiungimento di un obiettivo di transizione ecologica o di innovazione digitale 4.0, nel 2023 il credito d'imposta è riconosciuto in misura pari al 10%.

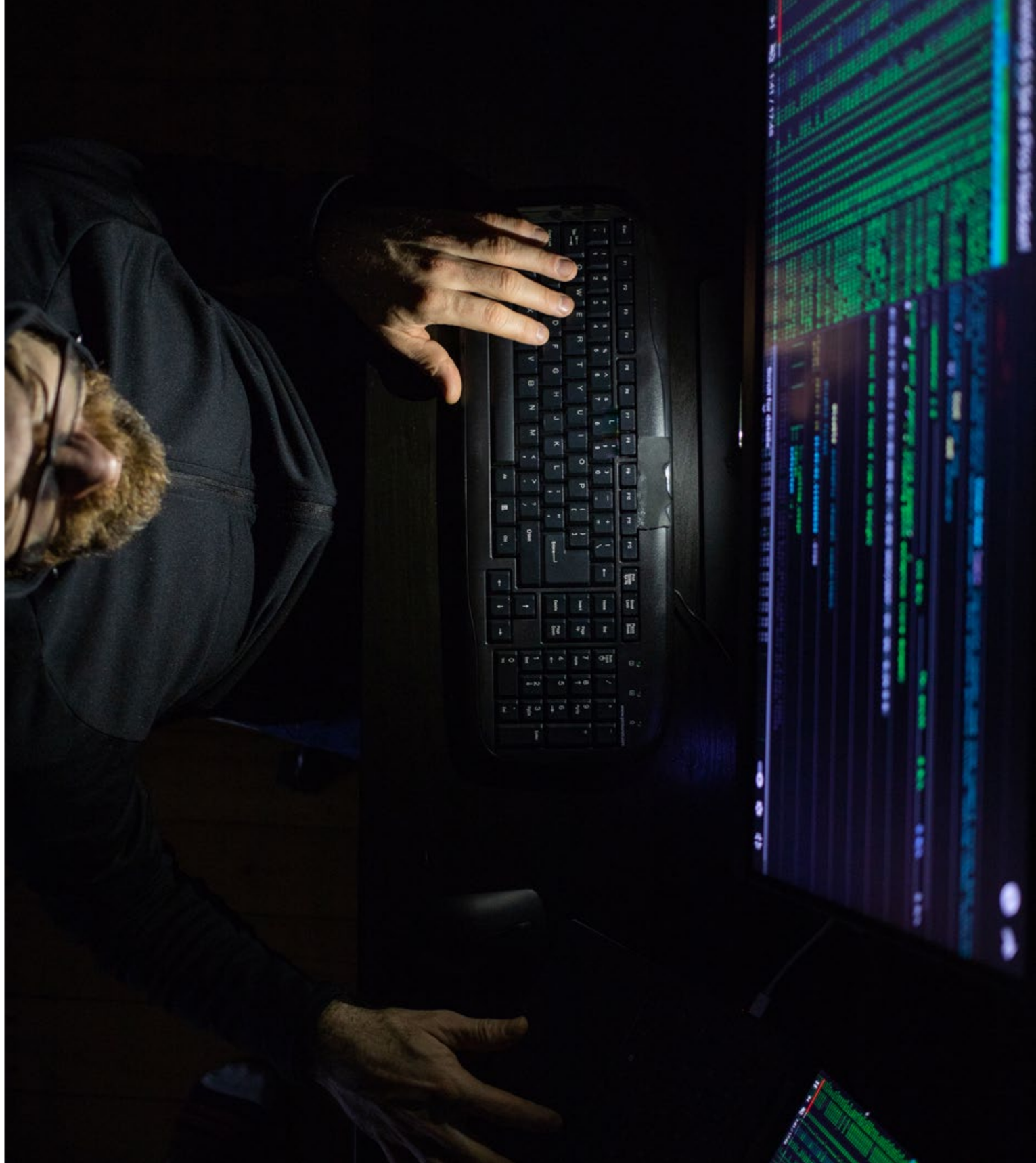
c) Ai crediti di imposta si affiancano le agevolazioni (sotto forma di contributi in conto interessi) previste dalla "Nuova Sabatini"; l'agevolazione[11], che si rivolge proprio alla le micro, piccole e medie imprese, messa a disposizione dal Ministero delle Imprese e del Made in Italy, sostiene gli investimenti per acquistare o acquisire in leasing macchinari, attrezzature, impianti, beni strumentali ad uso produttivo e hardware, nonché software e tecnologie digitali. Le agevolazioni consistono nella concessione di finanziamenti nonché di un contributo da parte del Ministero rapportato agli interessi sui predetti finanziamenti.

d. Backup dei dati aziendali (cloud?!?). Questo importante accorgimento/operazione deriva direttamente dalle predette "preliminari" operazioni di definizione degli asset tecnologici aziendali; purtroppo non sempre sarà possibile proteggersi da intrusioni/attacchi informatici, Ma possedere una copia di backup "dell'azienda" può risultare fondamentale per svariati motivi che vanno dal poter proseguire la propria attività senza lunghi stop forzati, alla possibilità di gestione/negoziazione dell'attacco stesso.

PNRR. Oltre a quanto accennato sopra, altri finanziamenti per l'acquisto/rinnovo/miglioramento dei "parco" software aziendale, affiancati alle possibilità date dal PNRR, possono rinvenirsi nel Bando MISE "Digital Transformation"[12], per sostenere la trasformazione tecnologica e digitale dei processi produttivi delle PMI attraverso la realizzazione di progetti diretti all'implementazione delle tecnologie abilitanti individuate nel Piano Nazionale Impresa 4.0 nonché di altre tecnologie relative a soluzioni tecnologiche digitali di filiera. Le agevolazioni sono concesse sulla base di una percentuale delle spese ammissibili pari al 50% (10% sotto forma di contributo, 40% come finanziamento agevolato) e finanzia tecnologie abilitanti individuate dal Piano nazionale Impresa 4.0 (tra le quali cloud, cybersecurity, big data e analytics) e **t**ecnologie relative a soluzioni tecnologiche digitali di filiera anche relativamente ai software.

e. VPN - protezione della rete aziendale. L'acronimo VPN (Virtual Private Network) si traduce in *Rete Privata Virtuale*, sta a significare una rete privata che sfrutta una Rete pubblica – ovvero Internet – per permettere ai computer connessi di comunicare tra loro come se fossero tutti fisicamente collegati. Con una VPN per uso aziendale, i dipendenti in Smart Working, possono utilizzare in modo sicuro reti Wi-Fi/internet senza compromettere i dati sensibili dell'azienda[13], quando lavorano da casa.

PNRR. Anche l'acquisto di programmi/



10 *https://www.mise.gov.it/it/incentivi/credito-d-imposta-r-s*

11 *https://www.mise.gov.it/index.php/it/incentivi/agevolazioni-per-gli-investimenti-delle-pmi-in-beni-strumentali-nuova-sabatini*

12 *https://www.mise.gov.it/it/incentivi/digital-transformation*

13 *Ulteriore protezione ad esempio, nell'ottica della creazione di un perimetro informatico aziendale, potrebbe essere l'utilizzo dell'accorgimento di utilizzare device dedicati per le operazioni Internet banking, solo per le operazioni bancarie no interazioni con altre informazioni, mail, altre comunicazioni, niente altro.*

software per lo sviluppo/implementazione di una rete VPN con la quale gestire le connessioni da remoto dei propri dipendenti rientra negli incentivi previsti per sostenere la trasformazione digitale delle imprese; il credito d'imposta da richiedere nelle dichiarazioni dei redditi tra il 1° gennaio 2021 e il 31 dicembre 2023. Comprende anche la definizione di codici di credito d'imposta per consentire ai beneficiari di utilizzarli con il modello F24 per beni immateriali di investimento standard e quindi software relativi alla gestione aziendale.

f. Pishing, password deboli, autenticazione a più fattori, criptazione dei device

Ho inserito queste problematiche/criticità all'interno dello stesso paragrafo, in quanto le ritengo di competenza (come anche in parte qualche altra sopra già descritta) dei dipendenti di un'azienda, senza troppe distinzioni ed afferenti a quel fattore umano di cui parlavamo prima, importante tassello nella cybersecurity aziendale nell'ottica della creazione di una cultura funzionale dello human-firewall.

Lo sviluppo di competenze funzionali in riferimento alla cybersecurity aziendale, necessita di adeguata informazione rispetto ai basilari obiettivi relativi alla sicurezza delle informazioni; questo al fine di creare quella consapevolezza nell'attenzione continua nello svolgimento di attività lavorative che va ad integrare e valorizzare le diverse soluzioni tecnologiche materiali di protezione. Spesso le intromissioni malevole sfruttano comportamenti errati che potranno sicuramente essere "minimizzati" investendo in opera di informazione (linee guida, "percorsi" organizzativi, policy definite e mirate ecc.) e formazione.

- Pishing. È un tentativo di attacco di solito posto in essere tramite mail, che sfruttando comunicazioni "simili" agli originali, con l'inganno portano l'utente distratto a cliccare sui link inviati attivando la trappola informatica;
- Password deboli. Andrebbero evitate password direttamente riferibili alla propria persona (date di nascita, nomi di figli, coniugi ecc.), sarebbe buona norma non "riportare" le password per comodità su biglietti, post-it o simili direttamente sugli schermi dei PC cui si riferiscono o altri luoghi direttamente collegabili; andrebbero inoltre integrati numeri, lettere, simboli e soprattutto, utile policy aziendale, dovrebbero essere modificate con una certa regolarità;
- Autenticazione a più fattori. La tipologia di autenticazione a doppio fattore, utilizzata quasi universalmente nelle operazioni di internet banking, dovrebbe/potrebbe essere utilizzata per l'accesso ai device aziendali, così da integrare una doppia sicurezza, con la quale solo il dipendente che ha la possibilità di mettere in correlazione le informazioni di accesso (es. password e codice/msg sul telefono...) può accedere ai dati aziendali;
- Criptazione dei device. I PC ed i device mobili, utilizzati in maniera promiscua casa-lavoro, dovrebbero essere criptati per policy aziendale; la criptazione dei device avviene attraverso un algoritmo che data una chiave di criptazione restituisce dei dati completamente differenti; è possibile ritornare ai dati originali solamente attraverso un altro algoritmo complementare che usa a sua volta una chiave di criptazione. In parole povere in caso di furto/smarrimento, i dati contenuti nel device sono praticamente inutilizzabili

Le attività di formazione sono previste dalla misura Credito d'imposta formazione 4.0[14], volta a sostenere le imprese nel processo di consolidamento delle competenze nelle tecnologie abilitanti necessarie a realizzare il paradigma 4.0.

Il credito d'imposta è riconosciuto in misura del 70% delle spese ammissibili nel limite massimo annuale di 300 mila euro per le piccole imprese e 50% delle spese ammissibili nel limite massimo annuale di 250 mila euro per le medie imprese, a condizione che le attività formative siano erogate dai soggetti individuati con decreto del Ministro dello sviluppo economico di prossima emanazione e che i risultati relativi all'acquisizione o al consolidamento delle suddette competenze siano certificati secondo le modalità stabilite con il medesimo decreto ministeriale.

Sono ammissibili al credito d'imposta le seguenti spese: - spese di personale relative ai formatori per le ore di partecipazione alla formazione; - costi di esercizio relativi a formatori e partecipanti alla formazione direttamente connessi al progetto di formazione, quali le spese di viaggio, i materiali e le forniture con attinenza diretta al progetto, l'ammortamento degli strumenti e delle attrezzature per la quota da riferire al loro uso esclusivo per il progetto di formazione; - costi dei servizi di consulenza connessi al progetto di formazione; - spese di personale relative ai partecipanti alla formazione e le spese generali indirette (spese amministrative, locazione, spese generali) per le ore durante le quali i partecipanti hanno seguito la formazione.

Spero che quanto sopra possa aiutare a comprendere il motivo e l'importanza di prendersi cura dei dati e delle informazioni digitali aziendali e delle opportunità di investimento date dai finanziamenti, anche correlati, del PNRR; questo nell'ottica di implementare il proprio perimetro di sicurezza informatica dal punto di vista tecnico/strutturale ma anche con una particolare attenzione allo sviluppo di quella cultura della sicurezza cui il "fattore umano" aziendale, soprattutto nelle PMI, è il protagonista principale.

14 *https://www.mise.gov.it/it/incentivi/credito-d-imposta-formazione-4-0*

La nuova normativa sul whistleblowing: il D.Lgs. n. 24 del 2023

di Luigi Fruscione

Premessa

Il Consiglio dei Ministri del 10 marzo 2023 ha approvato, in via definitiva, il testo del decreto legislativo relativo all'attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio risalente all'ottobre del 2019.

Il provvedimento europeo fa riferimento sia alla protezione delle persone che segnalano violazioni del diritto dell'Unione che alla protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

Il Dlgs n.24/2023 pubblicato sulla Gazzetta Ufficiale del 15 marzo 2023, è suddiviso in IV capi (I° - ambito di applicazione e definizioni; II° - segnalazioni interne, segnalazioni esterne, obbligo di riservatezza e divulgazioni pubbliche; III° - misure di protezione; IV° - disposizioni finali) per un articolato complessivo di 25 articoli.

Ambito di applicazione

L'ambito di applicazione del provvedimento è circoscritto alla conoscenza, in un contesto lavorativo[1], di violazioni di disposizioni normative, siano esse nazionali o europee, attraverso le quali si leda l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato.

Il disposto dell'articolo 1 deve essere necessariamente letto in stretta connessione con il significato attribuito, nell'ambito del decreto legislativo, ad alcuni termini ivi citati ed in particolare rispetto a cosa si debba intendere per "violazione", quali sono i "soggetti del settore pubblico" ed i "soggetti del settore privato" interessati dall'applicazione del provvedimento. A) La "*violazione*" si concretizza in quei "comportamenti, atti od omissioni che consistono in: 1) illeciti amministrativi, contabili, civili o penali che non rientrano nei [successivi] numeri 3), 4), 5) e 6); 2) condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001 n. 231[2], o violazioni dei modelli di organizzazione e gestione ivi previsti, che non rientrano nei [successivi] numeri 3), 4), 5) e 6); 3), illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati [in un allegato al decreto legislativo] ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato al presente decreto, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi; 4) atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea[3] specificati nel diritto derivato pertinente dell'Unione europea; 5) atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea[4], comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società; 6) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei [precedenti] numeri 3), 4) e 5)".

B) Per "*soggetti del settore pubblico*" devono intendersi "le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165[5] , le autorità amministrative indipendenti di garanzia, vigilanza o regolazione, gli enti pubblici economici, gli organismi di diritto pubblico di cui all'articolo 3,comma 1, lettera d), del decreto legislativo 18 aprile 2016, n. 50[6], i concessionari di pubblico servizio, le società a controllo pubblico e le società in house, così come definite, rispettivamente, dall'articolo 2, comma 1, lettere m) e o), del decreto legislativo 19 agosto 2016, n. 175[7], anche se quotate.

C) Il perimetro delineato dalla normativa per i "*soggetti del settore privato*" include i soggetti "diversi da quelli rientranti nella definizione di soggetti del settore pubblico, i quali: 1) hanno impiegato, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato; 2) rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti

1 *Per "contesto lavorativo" in base all'art. 2, comma 1, lett. i) si intendono "le attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di cui all'articolo 3, commi 3 o 4, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile".*

2 *Il D.Lgs. n.231/01 è relativo alla responsabilità amministrativa dei soggetti collettivi in sede penale.*

3 *L'articolo 325 del TFUE stabilisce che l'Unione e gli Stati membri combattono contro la frode e le altre attività illegali che ledono gli interessi finanziari dell'Unione stessa mediante misure adottate sulla base di tale disposizione.*

4 *L'articolo 26, par.2, del TFUE è relativo al mercato interno aspetto che comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali secondo le disposizioni dei Trattati.*

5 *Il D.Lgs. n.165/2001 detta norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.*

6 *Il D.Lgs. n.50/2016 è il Codice dei contratti pubblici.*

7 *Il D.Lgs. 175/2016 è il Testo unico in materia di società a partecipazione pubblica.*

I.B e II dell'allegato [alla normativa in commento], anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al numero 1); 3) sono diversi dai soggetti di cui al numero 2), rientrano nell'ambito di applicazione del decreto legislativo 8 giugno 2001, n. 231, e adottano modelli di organizzazione e gestione ivi previsti, anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al [precedente] numero 1)".

La normativa di cui al D.Lgs. n. 24/2023 non trova applicazione nei seguenti casi[8]: "a) contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate; b) segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali indicati nella parte II dell'allegato al decreto legislativo in commento, ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell' allegato alla Direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al provvedimento qui in commento; c) segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea".

L'ambito di applicazione soggettivo

La normativa suddivide l'ambito di applicazione soggettiva in base al se il segnalante sia un soggetto appartenente al settore pubblico o privato: nel primo caso vi rientrano le persone indicate al comma 3 dell'art. 3 che procedono ad effettuare "segnalazioni" interne o esterne, divulgazioni pubbliche o denunce all'autorità giudiziaria o contabile.

In tale categoria vi rientrano non solo i dipendenti delle amministrazioni pubbliche come definiti nel testo o i dipendenti degli enti pubblici economici, degli enti di diritto privato sottoposti a controllo pubblico ai sensi dell'articolo 2359 del codice civile[9], delle società in house, degli organismi di diritto pubblico o dei concessionari di pubblico servizio ma anche, in alcuni casi, i lavoratori subordinati di soggetti del settore privato; i lavoratori autonomi nonché i titolari di un rapporto di collaborazione che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato.

A questi si aggiungono anche i lavoratori o i collaboratori, che svolgono la propria attività lavorativa presso soggetti del settore pubblico o del settore privato che forniscono beni o servizi o che realizzano opere in favore di terzi; i liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato; i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso soggetti del settore pubblico o del settore privato; gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico o del settore privato[10].

La tutela delle persone segnalanti di cui all'art.3, comma 3, trova applicazione anche nel caso in cui la segnalazione, la denuncia all'autorità giudiziaria o contabile o la divulgazione pubblica di informazioni avvenga: a) quando il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali; b) durante il periodo di prova; c) successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso.

Per quanto attiene, invece, i soggetti del settore privato il decreto legislativo prevede la sua applicazione: a) per i soggetti che hanno impiegato, nell'ultimo anno, la media di almeno 50 lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato; b) che rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti I.B e II dell'allegato al provvedimento in commento, anche se nell'ultimo anno non hanno raggiunto la media di 50 lavoratori subordinati; c) alle persone di cui ai commi 3 o 4 dell'articolo 3, che effettuano segnala-

8 Come testualmente disposto dall'art. 1, comma 2, del D.Lgs. n. 24/2023.

9 L'art. 2359 del codice civile detta disposizioni sulle società controllate e società collegate.

10 Per le specifiche normative dei soggetti rientranti nell'ambito del settore pubblico si veda l'art. 3, comma 3 del D.Lgs. n. 24/2023 ed in particolare il comma 3 lett. a, b, c, d.

zioni interne o esterne, divulgazioni pubbliche o denunce all'autorità giudiziaria o contabile delle informazioni sulle violazioni di cui all'articolo 2, comma 1,lettera a), numeri 3), 4), 5) e 6); d) per i soggetti di cui all'articolo 2, comma 1, lettera q), numero 3), alle persone di cui ai commi 3 o 4 dell'art. 3 che effettuano segnalazioni interne delle informazioni sulle violazioni di cui all'articolo 2, comma 1, lettera a), numero 2, ovvero, se nell'ultimo anno hanno raggiunto la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato, segnalazioni interne o esterne o divulgazioni pubbliche o denunce all'autorità giudiziaria o contabile anche delle informazioni delle violazioni di cui all'articolo 2, comma 1, lettera a), numeri 3), 4), 5) e 6).
Le misure di protezione predisposte dalla normativa si applicano anche ad una serie di ulteriori figure tra le quali: i facilitatori; le persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado; i colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente; gli enti di proprietà della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

Il canale di segnalazione interna: obblighi e modalità di gestione

L'articolo 4 della normativa in esame stabilisce alcuni aspetti rilevanti sotto il profilo operativo ovverosia: la tutela della riservatezza di quei soggetti che rientreranno nell'ambito della segnalazione, chi deve gestire il canale di segnalazione e le relative modalità di effettuazione, le attività da effettuarsi nel caso di segnalazione interna presentata a soggetto diverso da quello legittimato a riceverla.
Sia i soggetti pubblici che quelli privati sono chiamati a predisporre dei canali di segnalazione che devono garantire la riservatezza – anche mediante l'utilizzo di strumenti di crittografia - dell'identità dei soggetti che sono parte del flusso informativo (segnalante, persona coinvolta e persona comunque menzionata nella segnalazione) nonché del contenuto della segnalazione e della relativa documentazione.
Per quel che riguarda i soggetti collettivi che hanno adottato un modello organizzativo previsto dal D.Lgs. n. 231/01, l'art. 4 comma 1 del D.Lgs. n. 24/2023 stabilisce che anche tali soggetti devono predisporre canali di segnalazione interna come delineati nella nuova normativa.
Le disposizioni transitorie, in tema di responsabilità amministrativa, prevedono che le nuove disposizioni avranno effetto a decorrere dal 15 luglio 2023.
Alle segnalazioni effettuate precedentemente alla data di entrata in vigore del dlgs n.24/2023, nonché a quelle effettuate fino al 14 luglio 2023, continueranno ad applicarsi le disposizioni di cui all'articolo 6, commi 2-bis, 2-ter e 2-quater, del decreto legislativo n. 231 del 2001.
Per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, fino a duecentoquarantanove, l'obbligo di istituzione del canale di segnalazione interna ai sensi del presente decreto ha effetto a decorrere dal 17 dicembre 2023 e, fino ad allora, continuerà ad applicarsi l'articolo 6, comma 2-bis, lettere a) e b), del decreto legislativo n.231 del 2001, nella formulazione vigente fino alla data di entrata in vigore del Dlgs n.24/2023

Per quel che riguarda la gestione operativa del canale di segnalazione questa deve essere attribuita a una persona, ad un ufficio interno o, anche, ad un soggetto esterno autonomo e con personale specificamente formato.
Le segnalazioni possono essere realizzate sia in forma orale che scritta: nel primo caso queste andranno effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole.
La segnalazione interna presentata ad un soggetto diverso da quello legittimato a riceverla deve essere trasmessa, entro sette giorni dal suo ricevimento, al soggetto competente, dando contestuale notizia della trasmissione alla persona segnalante.
L'art. 5 sviluppa il tema operativo della gestione vera e propria del canale di segnalazione interna prevedendo le seguenti regole che devono essere rispettate dal soggetto che gestisce il canale, il quale:
a) rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
b) mantiene le interlocuzioni con la persona segnalante e può richiedere a quest'ultima, se necessario, integrazioni;
c) dà diligente seguito alle segnalazioni ricevute;
d) fornisce riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione;
e) mette a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne.
Tali informazioni devono essere esposte e rese facilmente visibili nei luoghi di lavoro, nonché accessibili alle persone che pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico in una delle forme di cui all'articolo 3, commi 3 o 4 (ambito di applicazione soggettivo).
Se dotati di un proprio sito internet, i soggetti del settore pubblico e del settore privato sono tenuti a pubblicare le predette informazioni anche in una sezione dedicata del portale.

Il canale di segnalazione esterna: casi e modalità di gestione

La persona segnalante invece di effettuare una segnalazione interna può effettuarne una esterna[11] qualora ricorra una delle seguenti ipotesi: a) non è prevista, nell'ambito del contesto lavorativo in cui

11 Per "segnalazione esterna" si intende in base alla definizione di cui all'art. 2, comma 1 lett. e) del D.Lgs. n. 24/2023 la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione esterna di cui all'articolo 7.

opera, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dall'articolo 4 (canali di segnalazione interna); b) la persona segnalante ha già effettuato una segnalazione interna ai sensi dell'articolo 4 e la stessa non ha avuto seguito; c) la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito, ovvero che la stessa segnalazione possa determinare il rischio di ritorsione; d) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

L'obbligo di riservatezza e conservazione della documentazione relativa alla segnalazione

Di particolare importanza è la gestione dell'obbligo di riservatezza imposto dalla normativa essendo previsto che le segnalazioni "non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse".

L'identità della persona segnalante - e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità - non possono essere rivelate, senza il suo consenso espresso a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

Tale disposizione va letta in connessione con gli obblighi di conservazione della documentazione inerente la segnalazione – sia essa interna o esterna – che rappresenta il successivo passaggio del processo di gestione della segnalazione; in particolare si prevede che le predette segnalazioni e la relativa documentazione debbano essere conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza stabiliti all'articolo 12 del D.Lgs. n.23/2024 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679[12] e 3,comma 1, lettera e), del decreto legislativo n. 51 del 2018[13].

Qualora per la segnalazione sia utilizzata una linea telefonica registrata o un altro sistema di messaggistica vocale registrato essa, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione ed all'ascolto oppure mediante trascrizione integrale (in tale ultimo caso il segnalante potrà verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione).

Qualora invece, per la segnalazione sia utilizzata una linea telefonica non registrata o altro sistema di messaggistica vocale sempre non registrato, la segnalazione dovrà essere documentata per iscritto mediante resoconto dettagliato della conversazione da effettuarsi a cura del personale addetto alla gestione del canale; anche in tal caso la persona segnalante potrà verificare, rettificare e confermare il contenuto della trascrizione mediante sottoscrizione.

Ultimo caso preso in esame è quello in cui, su richiesta della persona segnalante, la segnalazione è effettuata per via orale nel corso di un incontro con il personale addetto alla gestione del canale: in tal caso, previo consenso della persona segnalante, la segnalazione è documentata a cura del predetto personale mediante registrazione su un dispositivo idoneo alla conservazione ed all'ascolto, oppure mediante la predisposizione di un apposito verbale che potrà essere verificato, rettificato e confermato mediante la propria sottoscrizione.

La tutela del segnalante

La normativa affronta in maniera ampia la tematica della tutela del segnalante che è suddivisa in diversi articoli: l'art. 16 attiene alle condizioni per la protezione della persona segnalante, l'art. 17 il divieto di ritorsione, l'art. 18 le misure di sostegno, l'art. 19 la protezione dalle ritorsioni e, infine, l'art. 21 che detta le sanzioni suddivise per il settore pubblico (applicate dall'ANAC) e privato (sistema disciplinare adottato ai sensi del D.Lgs. n. 231/01).

12 L'art. 5, paragrafo 1, lettera e), del Regolamento (UE) 2016/679 stabilisce che "i dati personali sono: ... e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)".

13 Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Vincere le competizioni del nuovo millennio: Olacrazia e organizzazione Bossless

di Matteo Montagner

I modelli tradizionali di organizzazione con la relativa creazione di livelli gerarchici hanno raggiunto nelle loro applicazioni il loro limite strutturale e quindi le aziende innovative cercano di applicare nuovi modelli di organizzazione che consentano loro di strutturare le imprese evitando di moltiplicare i livelli manageriali – gerarchici e così ridurre i costi migliorando l'efficienza e l'efficacia della governance.
Olacrazia rappresenta uno dei modi alternativi per creare una nuova struttura organizzativa che aiuti le aziende a gestire la propria attività in modo più efficace ed efficiente. In questo articolo pertanto si illustra questo sistema alternativo di gestione aziendale, il suo sviluppo e i vantaggi e gli svantaggi che un tale modello comporta.
In tale sistema organizzativo innovativo di governance l'autorità e le decisioni non sono stabiliti sulla base di una gerarchia di tipo manageriale strutturata dall'alto verso il basso, ma distribuiti nell'ambito di una olarchia di team autonomi per quanto riguarda gli aspetti formali organizzativi e gestionali.
Ma perché si dovrebbe cambiare l'attuale struttura organizzativa aziendale?
Le aziende devono costantemente affrontare nuove sfide dettate dai sempre più rapidi e repentini cambiamenti delle condizioni in cui operano. Le situazioni economiche e sociali degli ultimi anni sono caratterizzate da una rapida evoluzione che a volte è completamente caotica e imprevedibile.
Tuttavia, anche in queste condizioni di mutevolezza delle condizioni del mercato e del contesto generale della società, molte aziende sono ancora in grado di funzionare in modo adeguato secondo il modello tradizionale della cosiddetta gerarchia dall'alto verso il basso. Questa forma di organizzazione non può dirsi a priori superata, ma eventualmente è da valutare se risulta ancora in grado di rispondere alle nuove condizioni "ambientali", intese come economiche e sociali, che hanno caratteristiche di grande complessità e variabilità.
Infatti secondo gli esperti di management e strategia aziendale l'ambiente in cui operano le aziende sta diventando estremamente turbolento e supera la capacità delle organizzazioni di adattarsi e rispondere puntualmente e velocemente alle condizioni mutevoli e impreviste della società e del mercato. Le strutture delle organizzazioni tradizionali non sono state concepite per affrontare questo tipo di cambiamenti.
Scenari internazionali problematici e pericoli di pandemie si sommano a grandi ristrutturazioni, crisi aziendali, difficoltà a reperire collaboratori qualificati e a trattenere ed attrarre talenti, e questi sono ormai problemi diffusi.
Come sempre ogni organizzazione può decidere di anticipare il problema innovando per tempo, acquisendo un vantaggio competitivo, o provare a cambiare quando ormai adeguarsi diventa inevitabile.
I cambiamenti sono all'attenzione di tutti come fenomeni che esigono di prendere in considerazione un nuovo modo di organizzare le imprese. Le imprese infatti si devono confrontare con:
- la rivoluzione digitale;
- la proliferazione dell'intelligenza artificiale;
- la pervasività della tecnologia ad ogni livello in particolare di quella informatica;
- la diffusione delle telecomunicazioni;
- l'iperconnettività e l'iperconnessione.

Viviamo immersi in flussi di comunicazione costante con una accelerazione esponenziale del tempo di feedback. La comunicazione tra zone diverse, anche continentali, può avvenire in tempo reale. Pertanto al giorno d'oggi un team può essere distribuito potenzialmente in tutto il mondo anche con fusi orari differenti che comunicano istantaneamente.
In questo contesto la gerarchia può soffocare l'innovazione. La gerarchia implica tempi di risposta lenti, iter decisionali e passaggi burocratici.
Oggi invece il mercato impone velocità come fattore chiave di competitività e pertanto le aziende innovative e moderne iniziano ad improntare la loro organizzazione seguendo un nuovo modello che abbia la capacità di evolvere e garantire la capacità decisionale in tempo reale.
Viviamo nel mondo della sincronicità, un mondo che decreta costantemente che le risposte per funzionare devono essere sempre più rapide.
Sappiamo che la natura umana è estremamente sensibile alle problematiche relative al cambiamento in generale. I cambiamenti quando si verificano possono indurre nelle persone inquietudine e nervosismo, ma anche stimolare l'intuizione e la creatività. L'importante è indirizzare la tensione a produrre il massimo sforzo per risolvere i problemi nel migliore dei modi.
In queste situazioni molti manager gestiscono i processi aziendali secondo schemi obsoleti lavorando per logiche di ottemperanza e non di servizio. Le organizzazioni gerarchiche sono apparati principalmente burocratici dove i processi lavorativi e lo scambio di informazioni sono dominati da dinamiche di controllo e non solo di tensione al raggiungimento di un obiettivo.
La burocrazia nasce da una esigenza umana di isolare le problematiche e disegnare sistemi ideali funzionali al governo dell'esistente. Pertanto il pericolo è di stabilire procedure che una volta adottate e standardizzate siano già superate perché i mercati evolvono in modo celere.
La contemporaneità impone un ritmo completamente diverso: la progettazione organizzativa deve essere cambiata costantemente sulla base delle tensioni e

problematiche reali acquisite tramite dati rispetto all'evoluzione dell'ambiente economico in cui si opera.
Il cambiamento non può essere evitato creando una struttura organizzativa "ideale" che sia per sempre in grado di rispondere alle esigenze del mercato. Una tale organizzazione valida a prescindere in realtà non esiste, invece è necessario pensare a una struttura aziendale flessibile e facilmente adattabile.
In tale ottica si inquadra l'introduzione di un nuovo modello organizzativo come l'olacrazia che si configura come una risposta volta alla sostituzione del sistema di gestione dall'alto verso il basso con un innovativo sistema che mantenga un più adeguato equilibrio tra responsabilità e collaborazione.
L'olacrazia è un modo di organizzare l'impresa che supera le norme convenzionali. Alcune delle caratteristiche principali che la rendono unica sono una struttura estremamente flessibile, un alto livello di adattabilità, un contatto costante con tutti i soggetti aziendali coinvolti nell'attività e nello scambio di informazioni, la buona "tolleranza" dell'incertezza, l'approccio sistematico al business, l'alto coinvolgimento dei dipendenti in tutti gli aspetti della vita aziendale.
La declinazione concreta implica una dimensione "Bossless" (senza capi) dove al centro sono posti i dipendenti e i collaboratori, le loro personali motivazioni con una forma aziendale che si adatta a loro perché è espressione dei loro comuni intenti, delle loro passioni, dei loro talenti e attitudini all'interno di una dimensione lavorativa che guarda alla persona nel suo complesso.
Inoltre l'olacrazia è un primo vero tentativo nel senso della completa democratizzazione della gestione delle imprese. In proposito alcune riviste economiche internazionali come The Economist affermano che essa ha "scosso" la pratica organizzativa aziendale più di ogni altro approccio fino ad ora.
Rispetto ad altri sistemi di gestione, permette infatti alle organizzazioni, ad un livello molto più alto, di creare una struttura poco profonda ed estremamente adattabile, tenendo riunioni di lavoro efficaci, autorità chiaramente distribuita e lavoro completamente orientato al compito da eseguire.
La struttura organizzativa olacratica è costituita da team auto-organizzati che in questo sistema sono chiamati cerchi o holon, come si può vedere dal modello della struttura a cerchi in figura 1.

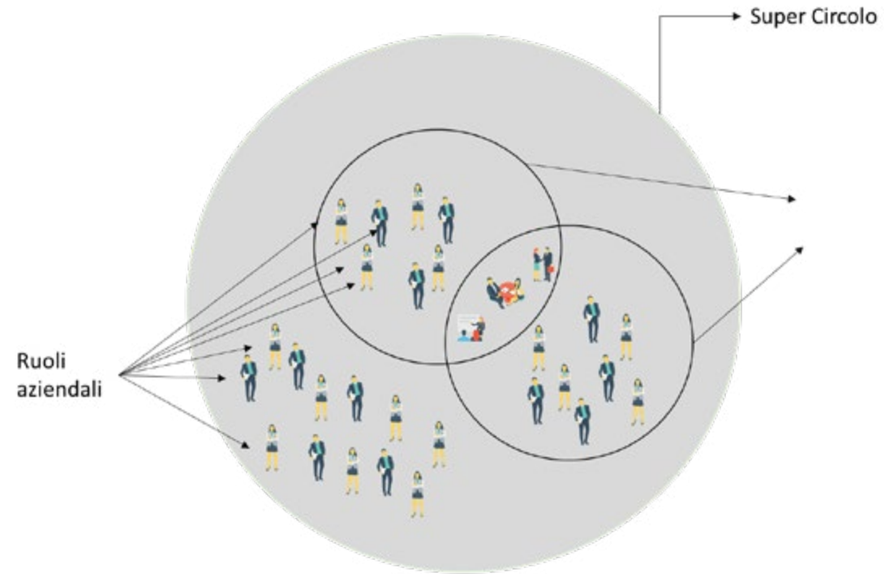


Fig. 1 – Struttura organizzativa olacratica

L'*holon* (il circolo) è un'entità separata, ma allo stesso tempo fa parte di un'entità più grande. Il termine deriva dalla parola greca " ", che può essere tradotto come "tutto quanto, intero".
Un filosofo contemporaneo Ken Wilber[1] definisce l'*holon* come un'identità in fase di costante sviluppo ed espansione.
Nel contesto organizzativo, i team di progetto sono nidificati in modo da far parte di aree funzionali, settori/dipartimenti che a loro volta sono parte di un'azienda nel suo complesso.
I circoli/holon si formano quando se ne presenta la necessità, a seconda del compito che l'organizzazione sta svolgendo in quel momento. In questo modo si crea una gerarchia naturale e realmente necessaria e funzionale al compito che si deve svolgere, che si rivolge al lavoro stesso e ai processi, non ai singoli individui.
Ogni circolo ha una serie di ruoli raggruppati intorno a una funzione specifica. Alcuni di essi possiedono dei sotto-circoli e tutti insieme si trovano all'interno di un grande cerchio organizzativo, di solito conosciuto come Circolo Aziendale Generale. Inoltre, i circoli hanno le loro prerogative e godono di autonomia, ma devono essere costantemente in coordinamento reciproco e sono vincolati al reciproco flusso di informazioni.
Una delle maggiori differenze tra l'olacrazia e le strutture tradizionali è rappresentata dal sistema di assegnazione dei titoli all'interno dell'organizzazione. Questi non esistono nell'olacrazia.
I titoli sono sostituiti dai ruoli dei dipendenti che sono chiaramente definiti, in base al compito che svolgono e al modo in cui possono contribuire al lavoro del proprio circolo e all'organizzazione in generale. Non appena il ruolo ricoperto da un dipendente diventa non più importante per un obiettivo che è stato definito, viene semplicemente richiamato o cancellato. In questo sistema, tutti i leader sono responsabili del loro lavoro e del ruolo che ricoprono in un determinato momento. È molto importante sottolineare che non ci sono regole preimpostate nell'olacrazia: esse vengono stabilite e applicate contemporaneamente allo svolgimento del lavoro.
In questo modo, tutti i membri dell'organizzazione capiscono chiaramente che cosa ci si aspetta da loro, quali sono le loro responsabilità e doveri. Il funzionamento dell'olacrazia infatti può essere meglio descritto come l'organizzazione dell'azienda focalizzata sul lavoro da svolgere e non sulle persone che lo svolgono.
Durante il processo di svolgimento del lavoro un individuo può avere più compiti e quindi opererà parallelamente in più circoli. Ogni ruolo porta con sé un

1 *K.E. Wilber Jr, Breve storia del tutto, Spazio Interiore, 2016. E' un saggista e filosofo statunitense che si è dedicato alla ricerca di una "teoria integrale" in grado di spiegare l'evoluzione e la coscienza.*

certo livello di responsabilità e autorità e ogni dipendente capisce chiaramente cosa ci si aspetta da lui.
In una situazione in cui le responsabilità connesse a un certo ruolo superano le capacità di un individuo, il ruolo stesso può essere suddiviso in diversi ruoli più piccoli. In questo modo si crea un sottocircolo che fa parte del circolo iniziale.
A differenza delle strutture tradizionali in cui la gestione avviene secondo lo schema alto-basso, nell'olacrazia esiste a ogni livello dell'organizzazione. Ciò significa che la classica posizione di CEO diventa superflua. Al contrario, c'è una cooperazione "peer-to-peer" (tra pari) dove tutti hanno il diritto di partecipare.
Sebbene l'olacrazia sia un nuovo modello, molti autori affermano che in realtà rappresenta l'integrazione di diversi modelli già esistenti. Così alcuni autori sottolineano che l'odierna olacrazia è in realtà una sorta di sociocrazia perfezionata. Il modello sociocratico, utilizzando i principi della cibernetica, ottenne un discreto successo inizialmente nei Paesi Bassi e successivamente si è diffuso in tutto il mondo.
Uno dei maggiori vantaggi dell'olacrazia è che consente alle aziende di adattarsi alle possibilità e alle minacce dell'ambiente, secondo il sistema JIT[2] (Just In Time - appena in tempo) caratterizzato da un basso livello di progettazione preliminare, prototipazione veloce e produzione sulla base delle esigenze del mercato.
Inoltre la struttura organizzativa è soggetta a rapidi adattamenti ogni volta che è necessario, a differenza dell'organizzazione tradizionale in cui le decisioni sono assunte solo dal top management, nelle olacrazie le decisioni sono collegialmente assunte dai colleghi che sono ugualmente coinvolti nel progetto (il cosiddetto peer-to-peer).
Come indicato anche in precedenza molte idee sull'olacrazia e sull'importanza di un processo decisionale integrato sono state teorizzate in numerose opere di filosofi e psicologi contemporanei.
Tuttavia, l'olacrazia al di là degli aspetti teorici è innanzitutto una pratica la cui applicazione si realizza attraverso la costante implementazione che comunque è soggetta a tutti i possibili errori che accompagnano l'introduzione di un tipo di innovazione così rivoluzionaria.
Le innovazioni devono pertanto essere introdotte gradualmente, poiché i valori che caratterizzano l'olacrazia devono diventare il fondamento della futura "nuova" organizzazione.
Pertanto, se si pianifica un cambiamento questo non dovrebbe essere introdotto bruscamente, l'attenzione dovrebbe infatti essere focalizzata sull'aggiornamento graduale e sul miglioramento progressivo del modo in cui funziona l'organizzazione esistente.
Probabilmente la rivoluzione più grande di questo approccio implica una revisione delle modalità con cui concepiamo oggi le organizzazioni, cambia radicalmente l'approccio alla gestione delle persone dell'organizzazione. La retribuzione e i benefit vengono distribuiti nel modo più uniforme possibile tra tutto il personale individuando 2 o 3 fasce di retribuzione.
Le persone che operano in una organizzazione olacratica lo fanno poiché hanno una sintonia con i valori dell'azienda, condividono la sua visione e missione, apprezzano i prodotti e servizi che discendono da quella cultura aziendale, questo rappresenta pertanto il concetto centrale della motivazione.
Non c'è il capo che assegna compiti, ma sono i lavoratori stessi che negoziano insieme assegnandosi compiti basati sulla considerazione di chi sia più adatto a realizzarli. In questo modo le persone mettono a valore e massimizzano i loro punti di forza, capacità e competenze, e i propri interessi.
In una Olacrazia ogni proposta di cambiamento di un ruolo avviene tramite una negoziazione tra tutti i membri della comunità e deve essere oggetto di adeguate argomentazioni e motivazioni razionali. I membri del circolo possono opporsi alle proposte qualora la modifica di assetto possa risultare dannosa per l'equilibrio e l'efficacia del circolo stesso.
I ruoli sono formalizzati e diventano parte di una knowledge base (una base di conoscenza) condivisa all'interno dell'organizzazione. L'accordo e l'adesione collettiva agiscono in modo positivo sulla soddisfazione del dipendente stesso. Sono le persone che guidano i processi produttivi in modo proattivo per raggiungere traguardi di gruppo e individuali.
Tuttavia in merito alla olacrazia, anche a distanza di anni dalla sua positiva applicazione in molte realtà, resta da parte di molti leader e manager una certa diffidenza sul fatto che un'organizzazione possa essere effettivamente gestita unicamente secondo il principio del consenso, in quanto ritengono che tale forma organizzativa sia troppo piatta e suscettibile di cadere nel caos organizzativo.
In ogni caso, in una realtà in rapida trasformazione caratterizzata da un'estrema imprevedibilità, olacrazia e cultura bossless possono effettivamente diventare condizioni determinanti per anticipare i cambiamenti, incrementare la propria competitività e innovare le regole gestionali con i vantaggi sopra illustrati prima che siano le condizioni del mercato a costringere a cambiare quando può essere ormai troppo tardi.

2 JIT (appena in tempo): sistema produttivo che consiste nella gestione delle scorte e dell'inventario finalizzata a minimizzare gli sprechi di risorse e per rinnovare gli articoli in funzione della domanda.

Le fonti di stress negli ambienti di lavoro

di Ilaria De Vito

Premessa

Il termine stress, ampiamente diffuso in ambito clinico e nel mondo del lavoro, risale alla metà degli anni '50 quando il medico austriaco Hans Selye ne introdusse il concetto descrivendolo inizialmente come *"uno stato di tensione aspecifica della materia vivente, che si manifesta mediante modificazioni morfologiche tangibili in vari organi, e particolarmente nelle ghiandole endocrine"* e successivamente come *"risposta aspecifica dell'organismo per ogni richiesta effettuata su di esso dall'ambiente esterno"* (Selye 1936). Selye è stato tra i primi ricercatori ad aver introdotto in medicina tale termine, definendo poi "Sindrome Generale di Adattamento" (GAS - General Adaptation Syndrome) *"la somma di tutte le reazioni che si manifestano in seguito ad una esposizione prolungata ad uno stress"*. Tale sindrome genera, dunque, una risposta di adattamento da parte dell'organismo la cui funzione è quella di prepararlo ad una reazione adattiva ad agenti stressanti esterni. Il concetto di stress è stato successivamente calato anche nel contesto lavorativo, tanto che oggi lo stress collegato al lavoro è diventata una delle maggiori preoccupazioni per le aziende che devono far fronte agli effetti dello stress collegato al lavoro sia in termini di costi, sia di prevenzione. Secondo gli studi effettuati dalla Fondazione Europea, tra il 1996 ed il 2000 circa il 28% dei lavoratori ha manifestato sintomi collegati allo stress, con un 50-60% di assenze sul posto di lavoro collegate allo stress da lavoro definito come un *"insieme di reazioni emotive, cognitive, comportamentali e fisiologiche collegate ad aspetti negativi e nocivi del contenuto, della organizzazione e del luogo di lavoro"*. Un'altra definizione di stress sul lavoro è quella del NIOSH (1999) che definisce il fenomeno come *"insieme di reazioni fisiche ed emotive dannose che si manifesta quando le richieste poste dal lavoro non sono commisurate alle capacità, risorse ed esigenze del lavoratore. Lo stress connesso al lavoro può influire negativamente sulle condizioni di salute e provocare infortuni"*. Lo stress nei luoghi di lavoro è stato, pertanto, oggetto di ampio studio, tanto che diverse ricerche hanno analizzato quantitativamente e qualitativamente le principali fonti di stress in ambito lavorativo e le risorse individuali ed organizzative che i lavoratori sentono di possedere per fronteggiarlo. L'importanza della materia ha, inoltre, condotto all'emanazione di un Accordo Internazionale, seguito in Italia dalla firma di un Accordo Interconfederale sullo stress mentre, a livello legislativo, la normativa di riferimento in materia di sicurezza nei luoghi di lavoro è il decreto legislativo n. 81 del 2008 (che ha abrogato la precedente legge n. 626/1994 e che attua l'articolo 1 della legge n. 123/2007 in materia di tutela della salute e della sicurezza nei luoghi di lavoro), il cui scopo è proprio quello di includere nella valutazione dei rischi da lavoro in azienda tutte quelle condizioni che possono determinare situazioni collegate allo stress.

Stress e fattori di rischio psicosociali sui luoghi di lavoro

Negli ultimi anni gli studi sullo stress associati agli ambienti di lavoro hanno evidenziato quanto le nuove modalità di lavoro, caratterizzate dall'utilizzo di tecnologie sempre più avanzate, dai tempi di trasferimento da e per le sedi di lavoro, dagli impegni familiari e sociali, possano determinare, in molti casi, un sovraccarico di richieste tali da generare quei fenomeni ormai ampiamente conosciuti con il termine "stress" e che hanno sempre più rilevanza nella valutazione del benessere organizzativo delle aziende. Lo stress da lavoro si manifesta quando le persone, nell'esercizio delle proprie mansioni, percepiscono uno squilibrio tra le richieste avanzate nei loro confronti e le risorse che hanno a disposizione per far fronte a tali richieste. Lo stress ha sostanzialmente una natura "specifica" che lo rende diverso dagli altri fattori di rischio occupazionali, essendo collegato al "fattore umano", in quanto la percezione dello stress è un qualcosa di estremamente soggettivo. Infatti, alcuni fattori che vengono riconosciuti universalmente come altamente stressogeni possono poi nel concreto essere percepiti in maniera differente dai diversi soggetti e, quindi, in alcuni provocare malessere e disagio mentre in altri essere stimolanti. Ciò significa che le persone sviluppano stress solo se le richieste ambientali sono al di sopra delle loro capacità di risposta. Alla variabile soggettiva si aggiunge la valutazione dei fattori oggettivi di stress, che si fonda sul principio che esistono variabili organizzative che rendono possibile l'insorgere di condizioni di stress nei lavoratori. Pertanto, per poter individuare i fattori di rischio stress all'interno delle aziende è indispensabile considerare la variabile "soggettiva" ed effettuare un confronto tra procedure, processi e prassi aziendali esistenti che possano generare stress (fattori oggettivi) ed il vissuto personale dei lavoratori rispetto a tali procedure, processi, prassi (fattori soggettivi). Date le premesse, valutare i rischi correlati allo stress da lavoro è un compito tutt'altro che facile, poiché i fattori da considerare sono molteplici. Innanzitutto occorre fare chiarezza sul termine stress, che non è la causa bensì il processo, vale a dire ciò che sta nel mezzo tra lo *stressor* (la causa dello stress, ovvero la situazione che crea disagio) e lo *strain* (l'effetto dello stress, ovvero lo stato di esaurimento). L'evento patologico (lo stress o lo stato di "esaurimento" dell'individuo) potrà verificarsi solo quando lo *stressor* supera le capacità di resilienza dell'individuo (capacità di opporsi

all'agente di rischio con nel mentre fattori modulanti che intervengono nell'aumentare o diminuirne gli effetti).
Gli studi sullo stress occupazionale negli anni hanno portato ad indentificare una serie di condizioni capaci di interferire con il benessere psicofisico dei lavoratori. Il lavoro da sempre è considerato una delle fonti primarie di realizzazione personale e relazionale dell'individuo ma, se svolto in determinate condizioni critiche, può diventare per molti fonte di stress e causare sofferenza, frustrazione, scarsa produttività, assenteismo, con perdita di giornate di lavoro e, quindi, di produttività per l'azienda. Le cause dello stress nei luoghi di lavoro possono essere molteplici e riguardare problemi di inadeguatezza premiale (*benefits*, servizi, salari, contratti precari, pensioni etc.) strutturale (agenti nocivi, ambienti inidonei, macchine obsolete), relazionale (rapporti mal gestiti in senso verticale o orizzontale) o organizzativa (*overload*, turni, ritmi, pause, precarietà etc.). Ad esempio, un ambiente di lavoro particolarmente rumoroso può essere fonte di stress, perché ciò per i lavoratori comporta una difficoltà di concentrazione e di comunicazione con i colleghi mentre un lavoro di responsabilità nei confronti di terze persone, come per i piloti, il personale sanitario, le forze dell'ordine, i conduttori degli autobus, etc. può generare elevati livelli di stress per la delicata missione che gli operatori sono chiamati ogni giorno a compiere. Fonte di stress possono essere anche quegli ambienti di lavoro i cui rapporti con superiori o colleghi sono caratterizzati da competitività, scarsa considerazione o incomprensione o quando il lavoro non offre adeguate garanzie di stabilità (es. lavori "atipici") o sicurezza o quando non ci sono possibilità di avanzamento professionali per i dipendenti o ancora quando i dipendenti sono demotivati e insoddisfatti per una mancanza di realizzazione personale, nonostante una discreta remunerazione. Sono stati elaborati da alcuni ricercatori dei modelli finalizzati alla prevenzione di quei comportamenti e di quelle condizioni di lavoro potenzialmente dannosi per i dipendenti in termini di stress.
Un primo modello è quello di Karasek e Theorell secondo cui la condizione di rischio per l'equilibrio psicofisico del lavoratore è il risultato di una "domanda", vale a dire un carico di lavoro eccessivo rispetto al "controllo", ovvero la capacità del soggetto di svolgere quel compito. Ciò significa che quando le risorse fisiche e psicologiche richieste al soggetto nel proprio ambiente lavorativo superano le sue reali capacità di fronteggiamento si genera una di quelle condizioni rischiose per la salute del soggetto stesso. Questo primo modello rileva un ambiente di lavoro che gli autori definiscono di tensione (*strain*), in cui la domanda supera il controllo e, quindi, i lavoratori saranno più inclini allo sviluppo di malattie, con conseguenze ovviamente negative anche in termini di produttività aziendale.
Un secondo modello è quello transazionale elaborato da Cox e Mackay secondo i quali lo sbilanciamento che si genera tra le richieste del contesto e le capacità dei lavoratori non è da individuare nelle reali potenzialità degli stessi quanto nelle percezioni individuali. Essi sostengono, quindi, che esiste la variabile individuale tanto nell'esperienza dello stress quanto nella risposta allo stress e che il contesto sociale ha una grande rilevanza nella valutazione dell'esperienza che ne fa il soggetto (Cox, 1978 citato in Favretto, 1994).
Un terzo modello è quello "Persona/Ambiente" elaborato da Van Harrison e Caplan secondo cui lo stress occupazionale è il risultato di una discrepanza (disadattamento) tra ciò che la persona è, le abilità che possiede e le caratteristiche oggettive del lavoro, vale a dire ciò che l'ambiente lavorativo fornisce in termini di spazi e di opportunità (discrepanza oggettiva), oppure tra le percezioni del soggetto su di sé e sul proprio ambiente lavorativo (discrepanza soggettiva). In questo modello fondamentali sono le strategie di *coping* (strategie per la risoluzione dei problemi), che devono essere impiegate dall'ambiente nei confronti delle capacità della persona (es. cambiamenti a livello organizzativo) e dalla persona nei confronti dell'ambiente, attraverso la realizzazione di un percorso formativo che consentirebbe al soggetto di poter meglio operare all'interno dell'organizzazione.
Cooper (1986), invece, propone un modello in cui individua quattro elementi che sintetizzano la dinamica dello stress nei luoghi di lavoro. Il primo elemento è dato dalle fonti di stress (fattori fisici e ambientali, ruolo organizzativo, rapporti sul lavoro, evoluzione della carriera, interfaccia casa-lavoro, caratteristiche di personalità, clima e struttura organizzativa); il secondo elemento dalle caratteristiche dell'individuo (livello di ansia, *locus of control*, tolleranza per l'ambiguità, etc.); il terzo elemento è rappresentato dai sintomi dello stress, che si distinguono in sintomi individuali (fisico, comportamentale e psicologico) e in sintomi organizzativi (scarso livello di *performance* lavorativa, assenteismo, *turn over*, etc.) e, infine, ultimo elemento è rappresentato dalle malattie somatiche e organizzative, che rappresentano l'effetto patologico di una cronicizzazione dei sintomi.
Nel 1991 Kasal propone un modello diverso dai precedenti, in cui l'attenzione si sposta sugli aspetti del lavoro collegati più alla pianificazione e organizzazione dello stesso (come lavoro articolato su turni, specialmente quelli a rotazione, ore di lavoro eccessive rispetto alla retribuzione, mancanza di sostegno dei colleghi, mancanza di partecipazione ai processi decisionali, etc.), rispetto ai fattori di rischio per la salute del lavoratore (come polveri, fumo, sostanze nocive per l'organismo, etc.). Secondo l'autore queste condizioni, ravvisabili nel contenuto dell'attività lavorativa, nei rapporti interpersonali nel gruppo di lavoro, nei rapporti interpersonali con i superiori e nelle condizioni dell'organizzazione, possono incidere sul benessere del lavoratore se lo stesso non ha la percezione dell'importanza del suo ruolo all'interno dell'organizzazione.
Infine, il modello delle relazioni tra stress lavorativo e salute di Hurrel (1987) sottolinea l'importanza della relazione tra i fattori stressogeni e le reazioni psicologiche, fisiologiche o comportamentali del soggetto, che a sua volta dipendono dai tratti di personalità, dal contesto familiare, economico e sociale della persona.

Interventi migliorativi a fronte del rischio stress lavoro correlato

Il concetto di rischio stress lavoro correlato compare per la prima volta in Italia con l'accordo interconfederale del 9 giugno 2008[1] ma solo con il D.Lgs. n. 81/2008 (art. 28, comma 1 "*la valutazione* (...) *deve riguardare tutti i rischi per la sicurezza e la salute dei lavoratori* (...), *tra cui anche quelli collegati allo stress lavoro-correlato, secondo i contenuti dell'accordo europeo dell'8 ottobre 2004*") entra a far parte della nostra legislazione, permettendo, in tal modo, di considerare come fattori di rischio per la salute e sicurezza dei lavoratori anche i rischi di natura psicosociale *"derivanti dall'interazione tra gestione, organizzazione,*

1 A seguito dell'accordo interconfederale sottoscritto dalle maggiori associazioni datoriali nazionali (con l'esclusione di banche ed assicurazioni) e da Cgil, Cisl e Uil, viene recepito dal nostro Paese l'accordo quadro europeo, stipulato a Bruxelles dal sindacato europeo (Ces) e dalle tre organizzazioni datoriali europee (Unice, Ueapme, Ceep) e realizzato su base volontaria, con l'obiettivo di aumentare la consapevolezza e la comprensione dello stress lavoro-correlato da parte dei datori di lavoro, dei lavoratori e dei loro rappresentanti e offrire loro un modello per individuare, prevenire e gestire i problemi ad esso associati.

contenuto del lavoro, condizioni ambientali da un lato e competenze ed esigenze dei lavoratori dall'altro". Il testo unico sulla salute e sicurezza sul lavoro ha avuto, tra le altre, il merito di aver attribuito nuovi compiti al medico del lavoro, che nello specifico riguardano *"le aree della valutazione, della prevenzione dei rischi, della sorveglianza sanitaria, dell'informazione e formazione, dei programmi volontari di promozione della salute*" (art. 25 del D.Lgs. n. 81/2008). Il medico competente è, dunque, una figura di supporto al datore di lavoro che deve aiutarlo a predisporre delle misure per la tutela della salute e integrità psico-fisica dei lavoratori. Le aziende hanno, pertanto, l'obbligo di attuare degli interventi di valutazione dei rischi sullo stress lavoro correlato che devono prevedere un percorso di gestione orientato alla prevenzione, ovvero degli interventi e procedure migliorative che riducano tali rischi. Per poter introdurre delle strategie di valutazione e prevenzione dei rischi che siano realmente orientate al benessere organizzativo è fondamentale analizzare le aziende a livello sistemico. Non basta, quindi, intervenire sui fattori di rischio ma è necessario avere una visione più ampia che permetta di capire in che modo determinati interventi possano impattare sull'intero sistema aziendale. In questo modo sarà possibile individuare sia i vincoli organizzativi su cui intervenire, individuando i punti di maggiore debolezza dell'azienda, sia l'elemento di resilienza organizzativa, individuando le aree di forza da poter usare come fulcro per migliorare la situazione. Tale visione permetterà di analizzare da un lato l'insieme di fattori che determinano o contribuiscono a determinare il benessere dei lavoratori (fattori oggettivi), dall'altro lo stato soggettivo di coloro che lavorano in uno specifico contesto organizzativo (percezione soggettiva), per arrivare ad effettuare una diagnosi che permetta, successivamente, di individuare i fattori organizzativi stressogeni (processi, contesto, ambiente, etc.) e di valutare le criticità percepite dai lavoratori (sotto forma di dati aggregati). Dall'intersezione dei fattori oggettivi esistenti e della percezione soggettiva condivisa è possibile risalire a quali sono i fattori oggettivi di stress che causano disagio o malessere, quali sono i fattori oggettivi di stress che non causano situazioni di effettivi disagio, quali sono le situazioni effettive di disagio che non sono causate da fattori oggettivi di stress e quali sono i punti di forza organizzativi su cui far leva (fattori oggettivi a rischio basso e percezione soggettiva positiva). Inoltre, qualora sia possibile intervenire sui fattori di stress, nelle aziende dovranno essere strutturati specifici interventi sull'organizzazione; possono essere interventi sui processi (es. consulenza strategica, sistemi di gestione, organizzazione e revisione processi, politiche di sviluppo sostenibile, interventi di programmi di promozione del benessere, *people care solutions*, etc.) o di supporto direzionale (es. mappatura di competenze, formazione sul benessere, processi di *engagement*, creazione di strumenti di valutazione delle performance, sistemi incentivanti, piani di sviluppo e retributivi, outplacement, etc.). Qualora non fosse possibile intervenire sull'organizzazione, gli interventi andranno fatti sulle risorse, vale a dire sulle persone a livello di gruppo (es. azioni e progetti sui temi del *team working*, *team building*, etc., collaborazione, comunicazione/diffusione valori aziendali, coaching di gruppo, interventi sullo sviluppo delle capacità di leadership, interventi di integrazione culturale, etc.) o individualmente (es. preparazione mentale al controllo dello stress, consulenza al ruolo, counseling individuale, coaching individuale, bilancio di competenze, empowerment, protocolli di diagnosi e cura di patologie lavoro-correlate). L'obiettivo finale è quello di ridurre i vincoli organizzativi presenti nelle aziende, che non necessariamente significa eliminarli (se ad esempio la percezione soggettiva da parte dei lavoratori rispetto ad un determinato fattore oggettivo di stress è bassa non sarà necessario eliminarlo) e aumentare la resilienza organizzativa. In tal modo, facendo un'analisi del benessere organizzativo è possibile prevedere quale tipo di intervento è più efficace. Questa logica "sistemica" di definizione degli interventi migliorativi ha dei vantaggi sia diretti, come l'ottimizzazione di processi e procedure, ottimizzazione dei sistemi di gestione, aumento della produttività, riduzione del turnover, riduzione delle prestazioni sanitarie, riduzione degli infortuni, riduzione dell'assenteismo, riduzione generale dei costi diretti, sia indiretti come una migliore gestione delle risorse umane, migliore soddisfazione delle risorse, maggiore *committent* delle risorse, valutazione positiva dei cambiamenti attuati, miglioramento del clima aziendale, riduzione delle prestazioni sanitarie, miglioramento dei rapporti interpersonali.

Conclusioni

La riflessione sugli obblighi di valutazione e di prevenzione dello stress lavoro-correlato, così come degli altri rischi di carattere psico-sociale, vale a dire la misurazione della probabilità che esistano rischi per la salute e la sicurezza dei lavoratori, ha evidenziato quanto sia fondamentale analizzare i fattori oggettivi e soggettivi di stress all'interno delle aziende. Sarebbe fortemente limitativo ragionare in un'ottica meramente meccanicistica di causa-effetto. È, invece, auspicabile ragionare secondo una visione sistemica, ove tutti gli elementi coinvolti nella valutazione del rischio sono interdipendenti tra di loro. Il modello bio-psico-sociale (art. 2, comma I, lettera o, D.Lgs. n. 81/2008) parte dal presupposto che il benessere reale non è un passaggio lento da invalidità malattia mancanza di malattia, bensì un qualcosa di molto più complesso che va dalla mancanza di malattia alla ricerca del benessere, inteso come stato di completo benessere fisico, mentale e sociale che permette una conservazione attiva della salute a tutti gli effetti. Questo modello, che nasce in ambito di psicologia della salute, può essere totalmente applicato alla valutazione del rischio stress lavoro-correlato, il cui obiettivo finale è quello di prevedere un modello sistemico complessivo dove inevitabilmente in azienda l'ambiente di lavoro è solo un elemento che coinvolge sia l'individuo, sia il rapporto lavoro/famiglia in una relazione di scambio reciproco. Solo considerando tutti e tre gli elementi è possibile fare una reale prevenzione primaria, sul piano organizzativo e sociale.

Bibliografia

Argentero P. & Maisetti M. (2014). *Valutazione degli Aspetti soggettivi dello stress Lavoro-Correlato: Quando e come farla*, in *Dossier Ambiente 106 – Stress Lavoro Correlato e Benessere Organizzativo*.

Buselli R. & Cristaudo A. (2009). *Il medico competente e il rischio stress lavoro correlato: dalla collaborazione alla valutazione del rischio alla sorveglianza sanitaria*, in *Giornale Italiano di Medicina del Lavoro ed Ergonomia*, 31(3), 261-264.

De Falco G., Messineo A. & Vescuso S. (2008). *Stress da lavoro e mobbing*, Roma.

Magnavita N. (2008). *Strumenti per la valutazione dei rischi psicosociali sul lavoro*, in *G Ital Med Lav Erg*, 30(1), A87-A97.

Nunin R. (2013). *Prevenzione dello stress lavoro-correlato e responsabilità datoriali: nuove prospettive per la tutela della salute e della sicurezza nei luoghi di lavoro*. La prevenzione dei rischi da stress lavoro-correlato, 9.

Pasquarella V. (2012). *La disciplina dello stress lavoro-correlato tra fonti europee e nazionali: limiti e criticità*, in *I Working papers di Olympus*, (6).

https://www.psicologiadellavoro.org/articolo-4-lo-stress-lavoro-correlato-prospettive-di-intervento-principali-teorie/.

Rischio Stress lavoro correlato. Metodologia, interventi di miglioramento e formazione specifica - Ordine degli Psicologi dell'Emilia-Romagna (ordinepsicologier.it).

Chiarimenti in materia di individuazione del «Titolare Effettivo» alla luce delle posizioni dell'UIF e del Notariato

di Manlio d'Agostino Panebianco

Introduzione

Gli obblighi di *Adeguata Verifica della Clientela* assolvono una funzione fondamentale, tanto per i destinatari delle disposizioni antiriciclaggio (al fine di conoscere la propria controparte, ed adeguare il relativo *approccio basato sul rischio*); quanto, in un contesto più ampio, al fine di garantire una efficacia e completezza informativa, in sede di scambio comunicativo con le diverse Autorità competenti (in specie nell'eventuale effettuazione di segnalazioni di operazioni sospette all'Unità di Informazione Finanziaria per l'Italia)[1].

Infatti, «attraverso lo strumento dell'adeguata verifica, in particolare, i soggetti obbligati possono intercettare e valutare il rischio di riciclaggio che essi assumono nell'instaurare rapporti con la clientela: la valutazione del rischio connesso con il cliente è infatti richiesto prima e in funzione dell'avvio dell'operatività e costituisce un'attività costante nel corso dell'intero rapporto»[2].

Nei primi mesi del 2023, questo argomento è stato oggetto di due interessanti pubblicazioni (dell'UIF e del Consiglio Nazionale del Notariato) che, *inter alia*, riguardano direttamente il mondo professionale, facendo riferimento a due specifici ambiti di ampia applicazione e portata, fornendo così alcuni interessanti ed importanti chiarimenti, in particolar modo circa l'individuazione del *titolare effettivo*.

Prima di descrivere le novità, sembra opportuno e propedeutico effettuare un breve *recap*, sia con la funzione di promemoria, che di contestualizzazione per la migliore comprensione delle stesse.

La definizione di "titolare effettivo"

Nello specifico, il presupposto della individuazione del "*titolare effettivo*"[3] (in inglese, *beneficial owner*[4]) è funzionale a garantire la riconducibilità di una o più operazioni ad una (o più) persona fisica che ne tra beneficio e/o vantaggio, ovvero per conto e/o interesse la stessa viene posta in essere: ciò con la finalità ultima - in specie in strutture giuridiche particolarmente complesse[5] - di evitare di poter celare l'identità di un terzo, che potrebbe beneficiarne attraverso un uso strumentale non lecito delle stesso (cosiddetta "*schermatura*"), ovvero ponendo in essere condotte riconducibili ad uno (o più) reati della famiglia del

1 *L'Autorità istituita presso la Banca d'Italia dal Decreto Legislativo n. 231/2007, in conformità di regole e criteri internazionali che prevedono la presenza in ciascuno Stato di una Financial Intelligence Unit (FIU), dotata di piena autonomia operativa e gestionale, con funzioni di contrasto del riciclaggio e del finanziamento del terrorismo.*

2 *G. Castaldi, C. Clemente (a cura di), La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli, Banca d'Italia, 2023, pag.112*

3 *Il "titolare effettivo è 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".*

4 *Che intende individuare, in una logica più ampia, la persona che, nonostante l'apparente e formale intestazione, ha l'effettivo controllo ovvero gode de facto dei vantaggi della proprietà di un determinato bene, materiale e/o immateriale.*

5 *In generale si fa riferimento, a società e altri enti, trust e istituti giuridici affini, e nel seguito, verrà chiarito in dettaglio tale concetto e contesto.*

riciclaggio e del finanziamento del terrorismo, ovvero ad uno (o più) dei loro reati presupposto.
In tale contesto, per esemplificare, una delle ragioni per cui nasce tale obbligo di individuazione è, dunque, la possibile presenza di un prestanome e contestualmente "alla figura dell'imprenditore occulto", ovvero di interposizione fiduciaria "irregolare", per celare e non rivelare (cosiddetta, *disclosure*) la presenza di un terzo estraneo al negozio giuridico oggetto della prestazione e/o dell'operazione.
In ultimo, per completare il quadro, sembra opportuno e necessario evidenziare come «la locuzione "titolare effettivo", peraltro, era già nota nel nostro ordinamento e precisamente in ambito fiscale, pur con accezione diversa: infatti l'art. 37 D.P.R. n. 600/1973 disponeva l'imputazione al contribuente dei redditi di cui appaiono titolari altri soggetti quando sia dimostrato che egli ne è l'effettivo possessore per interposta persona»[6].

I criteri di individuazione del titolare effettivo

Al fine di individuare il titolare effettivo, il Legislatore ha declinato dei criteri diversificati per tipologia di clientela, sebbene nella comunità scientifica esista la perplessità circa la non completezza delle casistiche descritte, che richiamano la necessità di dover intervenire con interpretazioni di buon senso, nella maggior parte dei casi "prudenziali". In tal senso, intervengono le due pubblicazioni dell'UIF e del Notariato (di seguito, richiamate e descritte).
In generale, l'elencazione degli stessi guida anche l'ordine di adozione ed applicazione: ossia all'impossibilità di poter applicare il primo, si procede con il secondo, ed in caso con il terzo, con l'obiettivo di individuare almeno un "titolare effettivo". È, infatti, impossibile che l'entità giuridica non ne abbia almeno uno.
Il primo criterio riguarda la "*proprietà*" (cosiddetto, *threshold approach*), applicabile alle società di capitali (partecipazione superiore al 25%) in modo diretto[7] o indiretto[8].
Il secondo riguarda il "*controllo*", che quindi può essere applicato solo in modo "subordinato", nel caso in cui sia infruttuoso l'esito del primo, in applicazione

6 *G. Arcella, S. Carioni, M. Nastri, L. Piffaretti, La ricerca del titolare effettivo, STUDIO 1/2023 B, Commissione Antiriciclaggio del Consiglio Nazionale del Notariato, 2023, pag.6*

7 *detenuta da una persona fisica.*

8 *posseduto per il tramite di società controllate, società fiduciarie o per interposta persona.*

nominale e l'esercizio del diritto di voto) [...]»[9]. D'altro canto, per i soggetti giuridici diversi da società, il legislatore ha espressamente previsto le casistiche puntuali. Nel caso di persone giuridiche private (ossia fondazioni), individuando: a) i fondatori, ove in vita; b) i beneficiari, quando individuati o facilmente individuabili; c) i titolari di funzioni di direzione e amministrazione. Allo stesso modo, per i Trust e le Fiduciarie, le informazioni sulla titolarità effettiva del trust, sono relative all'identità del fondatore, del fiduciario o dei fiduciari, del guardiano ovvero di altra persona per conto del fiduciario, ove esistenti, dei beneficiari o classe di beneficiari e delle altre persone fisiche che esercitano il controllo sul trust e di qualunque altra persona fisica che esercita, in ultima istanza, il controllo sui beni conferiti nel trust attraverso la proprietà diretta o indiretta o attraverso altri mezzi.

Il terzo criterio viene anche definito caso "*residuale*" proprio per la logica di subordinazione - prima descritta - chiarendo esplicitamente che non è possibile adottarlo se prima non si sono quantomeno esplorate le due precedenti modalità.
In tale casistica, «il titolare effettivo coinciderà con la persona fisica o le persone fisiche titolari di poteri di amministrazione o direzione della società». Una "interpretazione autentica" che aiuta a declinare quali figure possano rientrare nella citata definizione, viene dalla relazione illustrativa al Decreto Legislativo 4 ottobre 2019, n. 125 che recepisce la V Direttiva Antiriciclaggio, la quale *expressis verbis*, descrive come: «il titolare effettivo possa essere individuato nella figura di soggetti titolari di poteri di rappresentanza legale, amministrazione o direzione quali, esemplificativamente, il rappresentante legate, gli amministratori esecutivi ovvero i direttori generali della società o del cliente comunque diverso dalla persona fisica, non cumulativamente ma in relazione alle specifiche organizzative di ciascun ente e conformemente all'organizzazione societaria e a disposizioni statutarie».
Seguendo tale logica, il Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (CNDCEC) nelle Linee Guida del 22 maggio 2019, evidenziava come sia necessario individuare il titolare effettivo in relazione ai poteri ed alle deleghe rilasciate dalla società stessa a ciascun amministratore.

Le modalità di individuazione del titolare effettivo

Dal punto di vista metodologico, è opportuno soffermarsi su due ulteriori aspetti: per quanto attiene le società, è possibile attribuire «*la qualifica di titolare effettivo a una o più persone che esercitano il controllo, seguendo una o più delle seguenti logiche: individuare chi detiene (de facto) il controllo della maggioranza o di sufficienti voti per esercitare un'influenza dominante in assemblea ordinaria (ad esempio, secondo quanto previsto dall'art. 2352 del codice civile, soggetti che possono prevedere nel caso di pegno, usufrutto e sequestro, una separazione tra la "proprietà"* di quanto statuito dall'art. 20 co. 3 del Decreto ossia "n*elle ipotesi in cui l'esame dell'assetto proprietario non consenta di individuare in maniera univoca la persona fisica o le persone fisiche cui è attribuibile la proprietà diretta o indiretta dell'ente, il titolare effettivo coincide con la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile il controllo del medesimo in forza:*
a) *del controllo della maggioranza dei voti esercitabili in assemblea ordinaria;*
b) *del controllo di voti sufficienti per esercitare un'influenza dominante in assemblea ordinaria;*
c) *dell'esistenza di particolari vincoli contrattuali che consentano di esercitare un'influenza dominante*".
Prima di richiamare il terzo ed ultimo criterio - facendo riferimento ancora ai due precedentemente descritti - è opportuno soffermarsi su due ulteriori aspetti: per quanto attiene le società, è possibile attribuire «*la qualifica di titolare effettivo a una o più persone che esercitano il controllo, seguendo una o più delle seguenti logiche: individuare chi detiene (de facto) il controllo della maggioranza o di sufficienti voti per esercitare un'influenza dominante in assemblea ordinaria (ad esempio, secondo quanto previsto dall'art. 2352 del codice civile, soggetti che possono prevedere nel caso di pegno, usufrutto e sequestro, una separazione tra la "proprietà"*

9 *M. d'Agostino Panebianco, Antiriciclaggio – Vademecum per l'Operatore, Bancaria Editrice, 2022, pagg145-146.*

fermarsi su alcuni aspetti essenziali, utili ed indispensabili perché guidano il corretto assolvimento di questo obbligo, pur consapevoli che è *in itinere* la messa in funzione del *registro nazionale dei titolari effettivi*, di cui si è già affrontato in precedenza[10].
In primo luogo, il processo di "*identificazione del titolare effettivo*" va inteso *lato sensu*, poiché Provvedimento della Banca d'Italia sull'Adeguata Verifica della Clientela, Parte II, Sezione IV, *expressis verbis* richiama la modalità secondo cui "i destinatari identificano il titolare effettivo, senza che sia necessaria la sua presenza fisica, contestualmente all'identificazione del cliente e sulla base dei dati identificativi da questo forniti": in tal senso, proprio per la non necessaria presenza della persona fisica, sarebbe più opportuno definirla "*individuazione*", piuttosto che una *identificazione, stricto sensu*[11].
In secondo luogo, ai sensi dell'art. 22 (Obblighi del cliente) del Decreto Legislativo 21 novembre 2007, n. 231[12], sono i clienti del destinatario che "*forniscono per iscritto, sotto la propria responsabilità, tutte le informazioni necessarie e aggiornate per consentire ai soggetti obbligati di adempiere agli obblighi di adeguata verifica*", ed in particolare quelle relative alla titolarità effettiva delle imprese dotate di personalità giuridica e delle persone giuridiche private. In tale contesto il Legislatore ha espressamente previsto che non solo è obbligatorio fornire queste informazioni (veritiere ed aggiornate) ma sottolinea come non sia possibile effettuare alcuna eccezione di merito, poiché prevede che esiste una specifica responsabilità in capo ai legali rappresentanti di raccogliere gli elementi informativi necessari, superando così ogni eventuale e possibile ostacolo insorgente.
Infatti, il medesimo articolo recita, *expressis verbis*, che "*qualora permangano dubbi in ordine alla titolarità effettiva, le informazioni sono acquisite, a cura degli amministratori, a seguito di espressa richiesta rivolta ai soci rispetto a cui si renda necessario approfondire l'entità dell'interesse nell'ente*". È opportuno sottolineare come ogni comportamento contrario a tale disposizione siano sanzionabile: infatti "*l'inerzia o il rifiuto ingiustificati del socio nel fornire agli amministratori le informazioni da questi ritenute necessarie per l'individuazione del titolare effettivo ovvero l'indicazione di informazioni palesemente fraudolente rendono inesercitabile il relativo diritto di voto e comportano l'impugnabilità, a norma dell'articolo 2377 del codice civile, delle deliberazioni eventualmente assunte con il suo voto determinante*".
Dal punto di vista operativo, pertanto, «sembra opportuno e importante sottolineare come il Legislatore richieda:
- di conservare traccia delle verifiche effettuate ai fini dell'individuazione del titolare effettivo, soprattutto alla luce delle sanzioni previste in caso di violazione delle specifiche indicazioni;
- di ottenere dai clienti le informazioni inerenti alla titolarità effettiva degli ultimi 5 anni;
- ai clienti diversi da persona fisica, di adottare una metodologia univoca per determinare la titolarità effettiva, evitando così la (spesso) "inconsapevole" violazione delle disposizioni in materia di trattamento dei dati personali»[13].

In tale contesto, è necessario evidenziare come «la normativa domestica accoglie nel nostro ordinamento i criteri per l'individuazione del titolare effettivo già recepiti, a livello internazionale, dalle Raccomandazioni GAFI e quindi, principalmente, il criterio della proprietà (*ownership*) ed il criterio del controllo (*control*), eventualmente anche indiretti, cui si è aggiunto un terzo criterio (*residuale*) in caso di inoperatività dei primi due con una modalità applicativa "a scalare", posto che per la disciplina vigente, negli enti di qualunque tipo il titolare effettivo deve sempre essere individuato e potrà essere non solo una singola persona fisica, ma anche più persone fisiche, eventualmente tra loro legate da rapporti e relazioni tali da essere idonee a realizzare il possesso o il controllo della società (patti parasociali, vincoli contrattuali, contitolarità di partecipazione, e così via)»[14].

La posizione dell'Unità di Informazione Finanziaria[15] per la "revisione legale e contabile"

Tra i vari destinatari delle disposizioni antiriciclaggio, nella macrocategoria dei professionisti, sono elencati[16] anche i revisori legali e le società di revisione legale. Per completezza è opportuno però richiamare che ai sensi del Decreto Legislativo n.39/2010, il Decreto all'art. 1, comma 2, lett. a) e c) distingue due diversi profili di incarichi di revisione: un primo, in cui i Revisori hanno incarichi di revisione legale su enti di interesse pubblico o su enti sottoposti a regime intermedio (di seguito "Revisori EIP"), assoggettati alla su-

10 *Per i dettagli di merito, si rinvia M. d'Agostino Panebianco, Antiriciclaggio: pubblicato il Regolamento per il Registro italiano dei "titolari effettivi", in Rivista Compliance, n.7/2022, pagg.52-58.*

11 *Si veda M. d'Agostino Panebianco, Antiriciclaggio – Vademecum per l'Operatore, Bancaria Editrice, 2022, pag.110*

12 *aggiornato a seguito delle modifiche introdotte dal Decreto Legislativo 25 maggio 2017, n.90.*

13 *M. d'Agostino Panebianco, Antiriciclaggio – Vademecum per l'Operatore, Bancaria Editrice, 2022, pag.141*

14 *G. Arcella, S. Carioni, M. Nastri, L. Piffaretti, La ricerca del titolare effettivo, STUDIO 1/2023 B, Commissione Antiriciclaggio del Consiglio Nazionale del Notariato, 2023, pag.20*

15 *Si richiama in specie, il Quaderno Antiriciclaggio n.20/2023 da pag.276 a pag.280*

16 *Ai sensi dell'art. 3, comma 4, lett. d) ed e), del D.lgs. 231/2007.*

pervisione ai fini antiriciclaggio della Consob; ed un secondo, che riguarda i revisori privi di tali incarichi, invece, assoggettati alla supervisione del Ministero dell'Economia e delle Finanze.
Tale previsione deriva dalla potenziale esposizione al rischio che il professionista o la società incaricata possa sottovalutare e/o non valorizzare adeguatamente quegli elementi di potenziale anomalia o sospetto rilevanti ai fini della disciplina di settore, nel contesto del considerevole patrimonio informativo acquisito nello svolgimento degli incarichi professionali.

In tal senso, l'Unità di Informazione Finanziaria oltre a passare in rassegna i vari aspetti peculiari dell'attività di "*Adeguata Verifica della Clientela*" e del relativo "*approccio basato sul rischio*", individua nell'obbligo del "*controllo costante*" una componente essenziale al contributo al sistema antiriciclaggio.
Infatti, proprio in ragione del fatto che gli incarichi di revisione contabile hanno per oggetto lo «svolgimento delle verifiche e dei controlli previsti dai Principi di revisione e nell'esame dei dati e delle informazioni (contabili ed extracontabili) acquisiti nell'esecuzione della prestazione professionale, che devono essere analizzati anche nell'ottica di individuare elementi di anomalia o di sospetto di riciclaggio o di finanziamento del terrorismo. Il livello di pervasività dell'attività di controllo costante deve essere modulato, come per gli altri soggetti obbligati, sulla base del livello di rischio attribuito al cliente e in tale contesto il regolamento Consob richiede ai Revisori EIP di prendere in considerazione anche gli elementi riscontrabili nello svolgimento dell'attività professionale, quali eventuali incompletezze, irregolarità o manipolazioni della documentazione contabile, ovvero il rifiuto o la riluttanza a concedere accesso alle registrazioni contabili»[17].
In tale contesto si inquadra la raccomandazione di dover prontamente individuare, *inter alia*, la necessità di dover aggiornare, e dunque ripetere, l'identificazione e la verifica dell'identità del titolare effettivo, in specie se acquisite prima del conferimento dell'incarico, quando all'avvio delle attività professionali risultino differenti e/o divergenti.
Pertanto, emerge chiaramente la natura *dinamica* dell'applicazione combinata degli obblighi di "*Adeguata Verifica della Clientela*" e di "*approccio basato sul rischio*", in cui - proprio in sede di *controllo costante* - all'emergere di elementi "*discordanti*" e/o potenzialmente illeciti, sia necessario adottare la modalità "*rafforzata*" nei confronti dei clienti (oggetto di revisione) che risultino essere a maggiore (ossia, elevato) rischio di riciclaggio e di finanziamento del terrorismo, richiamando le vigenti disposizioni di attuazione[18]. Per completezza, ed in modo alquanto pragmatico, si ricorda che in questa casistica, le verifiche in modalità *rafforzata*, si sostanziano - in particolar modo - nell'esecuzione di analisi e verifiche contabili più approfondite, estese e/o frequenti nel corso dello svolgimento della prestazione (sia essa erogata dal singolo professionista, che da una società), coerenti con i fattori di rischio del cliente e, che in ultima istanza, sono volte a rilevare quegli eventuali elementi di anomalia[19], utili ad avviare il processo di valutazione del sospetto e del comportamento anomalo, potenzialmente riconducibili ad uno dei reati della famiglia del riciclaggio e/o del finanziamento del terrorismo (ovvero di uno o più reato presupposto), nel contesto dell'obbligo di *Segnalazione di Operazione Sospetta* (SOS).

Risulta evidente come chi riceve un incarico di revisione debba adottare delle specifiche procedure di *screening* ai fini della *detection* di operazioni anomale, che - a differenza di altri destinatari[20] - non possono avere una natura di automazione e standardizzazione, poiché il processo di rilevazione è piuttosto collegato - di norma - «all'analisi di un complesso di informazioni acquisite progressivamente nel corso della prestazione professionale e sulle quali il team di lavoro conduce articolati approfondimenti in relazioni ai Principi di revisione»[21].

La posizione del Notariato per i clienti "*Pubblica Amministrazione*"

Nella evoluzione della normativa antiriciclaggio, il trattamento dei clienti classificati come "*pubblica amministrazione*"[22] vi è una linea di demarcazione con l'emanazione del Decreto Legislativo 25 maggio

17 *G. Castaldi, C. Clemente (a cura di), La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli, Banca d'Italia, 2023, pag.278*

18 *Ad esempio, il regolamento della Consob per i Revisori EIP.*

19 *Che possono essere connessi a rilievi di carattere contabile o anche a fatti e/o operazioni che non danno luogo a rilievi sotto il profilo contabile (ad es. operazioni straordinarie, cambi di management, rapporti di finanziamento infragruppo)*

20 *A mero titolo esemplificativo e non esaustivo, gli intermediari bancari, finanziari ed assicurativi.*

21 *G. Castaldi, C. Clemente (a cura di), La normativa in tema di prevenzione del riciclaggio: autorità, regole e controlli, Banca d'Italia, 2023, pag.279*

22 *In dettaglio, pubbliche amministrazioni ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea.*

2017, n.90, quando questa categoria è stata interamente parificata alle altre e, *de facto*, individuando l'applicazione dell'Adeguata Verifica della Clientela in associazione con un indice di basso rischio riciclaggio, con la possibilità di eseguirla in modalità "*semplificata*".
Questa deve essere oggigiorno interpretata come una forma ridotta sotto il profilo dell'estensione e della frequenza degli adempimenti prescritti, poiché è venuta meno ogni precedente sorta di esimente nell'individuazione (e quindi, dichiarazione da parte del cliente stesso) del titolare effettivo.
Pertanto, al fine di dare indicazioni ai signori Notai, il Consiglio Nazionale del Notariato[23] ha provveduto ad emanare delle "*Regole Tecniche*" per individuare concretamente in cosa consista tale modalità.
Nello specifico, risulta interessante disaminare quanto contenuto nello "*Studio 1/2023-B*"[24] della Commissione Antiriciclaggio, proprio in materia di individuazione del titolare effettivo, quando il cliente è una "*pubblica amministrazione*", per tentare di colmare una lacuna lasciata dal Legislatore: in tal senso, questa interpretazione è applicabile in specie ai notai, pur divenendo un importante *best practice*, anche per gli altri destinatari (si vedano conclusioni, *infra* riportate).

Infatti, nella elencazione dei criteri per l'individuazione di tale figura, quantomeno nelle prime due macrocategorie, non si scorgono elementi attinenti alla Pubblica Amministrazione[25].
Pertanto il Consiglio Nazionale del Notariato (CNN) evidenzia come «bisognerebbe argomentare che, nella PA - nelle sue diverse articolazioni centrali e territoriali - non vi sia un titolare effettivo che possa essere individuato con i criteri della "*proprietà*" e del "*controllo*" di cui ai paragrafi precedenti, essendo essa stessa attributaria di pubbliche funzioni esercitate nell'interesse di tutti i cittadini o di determinati gruppi di cittadini. Ciò porterebbe alla conseguenza che per individuare il titolare effettivo - come per le società a capitale diffuso, o le associazioni o le cooperative - si tornerebbe al criterio residuale dell'art. 20 comma 5 in base al quale esso coinciderebbe con il soggetto dotato di poteri di rappresentanza o di amministrazione dell'ente pubblico».
Quindi, la Commissione Antiriciclaggio del CNN, avendo la necessità di fornire adeguate indicazioni circa l'individuazione di "almeno" un titolare effettivo, a ragion veduta, adotta la posizione di procedere con il cosiddetto "*caso residuale*" (ossia la terza categoria, precedentemente descritta), in cui il titolare effettivo è quella figura apicale e dirigenziale che ha in capo la responsabilità decisionale. Tale posizione viene motivata richiamando tanto gli orientamenti 4.23[26] *dell'European Banking Authority* (EBA)[27], quanto la metodologia di classificazione delle Persone Esposte Politicamente (PEP) in seno alla Pubblica Amministrazione[28].

In conclusione, è opportuno sottolineare che con la pubblicazione del citato "*Studio 1/2023-B*" del Consiglio Nazionale del Notariato, si pone un pilastro interpretativo importante anche per orientare un approccio omogeneo[29] (fino ad ora non sempre raggiunto) quando il cliente è una *società* oggetto di un *procedimento giurisdizionale di natura penale*, in cui il giudice affida "l'amministrazione" ad un tecnico/professionista ("*delegato*"), con la contestuale "*estromissione*" dei soci da ogni potere decisionale, in un contesto in cui il medesimo procedimento viene posto in essere in favore della collettività e/o dei creditori.
È da notare come, ad esempio, un "*incaricato del tribunale*" (ossia, l'esecutore) - che svolge un incarico in forza di specifiche leggi e norme, in nome e per conto del Tribunale[30] - nella maggior parte dei casi in ambito penale, è impossibilitato, *ex legem*, ad entrare in contatto diretto con il cliente: da cui deriva la oggettiva difficoltà a reperire le copie dei documenti di identità e/o informazioni diverse da quelle contenute negli atti/documentazione ufficiale, rendendo impossibile l'adempimento dichiarativo, ex art. 22 del Decreto 231 Antiriciclaggio.
Quantomeno - al di là della condivisibilità sulla efficacia della dichiarazione[31] - è possibile rintracciare una linea guida di condotta professionale, oggettivamente riconosciuta da un organismo di autoregolamentazione previsto per legge.

23 in qualità di organismo di autoregolamentazione, come previsto per legge.

24 Si veda G. Arcella, S. Carioni, M. Nastri, L. Piffaretti, La ricerca del titolare effettivo, STUDIO 1/2023 B, Commissione Antiriciclaggio del Consiglio Nazionale del Notariato, 2023, pag.40 e ss.

25 in virtù di una assenza del capitale sociale (tipico delle società) o di controllo, stricto sensu.

26 G. Arcella, S. Carioni, M. Nastri, L. Piffaretti, La ricerca del titolare effettivo, STUDIO 1/2023 B, Commissione Antiriciclaggio del Consiglio Nazionale del Notariato, 2023, pagg.41-42: «Se il cliente è un'amministrazione pubblica o un'impresa statale, per identificare il dirigente di alto livello le imprese dovrebbero seguire le indicazioni degli orientamenti 4.21 e 4.22"; a loro volta gli orientamenti richiamati 4.21 e 4.22 indicano che nel decidere quale/i dirigente/i di alto livello debba essere identificato come titolare effettivo, bisognerebbe considerare chi "ha la responsabilità ultima e generale del cliente e prende decisioni vincolanti per suo conto"; inoltre in questi casi, il soggetto obbligato dovrebbe documentare chiaramente le motivazioni per identificare il dirigente di alto livello, anziché il titolare effettivo del cliente, e registrare le proprie azioni", conservando pertanto la prova che si tratti di una PA e, nel caso delle società partecipate pubbliche, che non vi siano altri soggetti privati che abbiano il controllo, diretto o indiretto, sulla società predetta».

27 L'Autorità Bancaria Europea (ABE) è un'autorità indipendente dell'Unione europea (UE), che opera per assicurare un livello di regolamentazione e di vigilanza prudenziale efficace e uniforme nel settore bancario europeo.

28 G. Arcella, S. Carioni, M. Nastri, L. Piffaretti, La ricerca del titolare effettivo, STUDIO 1/2023 B, Commissione Antiriciclaggio del Consiglio Nazionale del Notariato, 2023, pag.42: «a conferma che questa potrebbe essere l'interpretazione preferibile per l'individuazione del titolare effettivo nella Pubblica amministrazione, è possibile richiamare la norma che non considera Persone Politicamente Esposte i soggetti dotati di poteri di direzione e coordinamento della PA, quando agiscono dell'esercizio delle loro funzioni (v. art. 24, comma 5, lett. c) del Decreto AR)».

29 Tra banche e professionisti economico-legali.

30 ossia una Pubblica Amministrazione.

31 Esistono, invero, posizioni critiche circa la mera formalità e poca sostanzialità stessa.

La Compliance al diritto dell'Unione Europea

Ne parliamo con Daniel Calleja, Direttore Generale del Servizio giuridico della Commissione Europea

di Alessandro Butticé

Daniel Calleja è, senza ombra di dubbio, uno dei più brillanti dirigenti delle Istituzioni dell'Unione Europea. Non è quindi un caso che la Presidente della Commissione Europea, Ursula von der Leyen, nel 2020, lo abbia nominato Direttore Generale del Servizio Giuridico della Commissione. Unico funzionario, assieme al Segretario Generale, che siede di diritto, accanto alla Presidente, alle riunioni settimanali del Collegio dei commissari europei, come primo consigliere giuridico dell'esecutivo comunitario.
Chi scrive ha avuto l'onore ed il piacere di collaborare con Daniel Calleja, quale responsabile della sicurezza, poi della comunicazione, ed infine delle risorse umane, quando era Direttore generale della Direzione Generale del Mercato Interno, dell'Industria e dell'Impresa (DG GROW) della Commissione Europea. Un'esperienza straordinaria. Grazie anche alla guida politica dell'allora Vicepresidente della Commissione Europea, oggi Vicepresidente del Consiglio dei ministri e Ministro degli Affari Esteri e della Cooperazione Internazionale, Antonio Tajani. Sono stato testimone della perfetta sinergia che si era creata tra due personaggi di grandissimo livello e valore. Uno politico, l'altro *grand commis* della funzione pubblica europea. Entrambi profondamente rispettosi del ruolo dell'altro, perché entrambi uomini delle Istituzioni, ed autentici patrioti europei oltre che, rispettivamente, italiano e spagnolo.

Dal 2015 al 2020, prima di essere nominato alla testa del Servizio Giuridico, Daniel Calleja è stato il Direttore Generale dell'Ambiente della Commissione Europea (DG ENV). Ha ricoperto quel ruolo dopo essere stato nominato, da Antonio Tajani, Direttore Generale per l'Industria, l'Impresa e poi anche del Mercato Interno (DG ENTR e DG GROW) dal 2011 al 2015. Prima, sempre sotto la responsabilità politica di Tajani, era stato direttore del trasporto aereo alla Direzione Generale dei Trasporti. Dimostrandosi in modo particolare un leader europeo e mondiale nel settore Ambiente, che ben conosce anche quello dell'industria. Grazie a questa grande esperienza anche nell'industria, e nella politica dell'industria spaziale, ha potuto essere protagonista di alcune tra le riforme più ambiziose nel panorama europeo, quale la direttiva quadro sull'acqua nell'Ue e la stesura della proposta del Green Deal europeo. Esperienze delle quali l'Unione Europea continua a beneficiare avendolo oggi al vertice del Servizio Giuridico della Commissione Europea, quale guardiano dei Trattati e dello stesso stato di diritto Ue.

Proseguendo nella serie di interviste a responsabili di importanti società agenti sul piano europeo, e a dirigenti di Istituzioni Ue e internazionali, ho voluto parlare con Daniel Calleja di una compliance che riguarda tutti i cittadini e le imprese europee. Quella della legislazione Ue. La quale, senza accorgersi, gestisce da settant'anni, grande parte della loro vita.

Daniel, cosa significano settant'anni di legislazione europea per i cittadini?
Che sono trascorsi 70 anni dalla firma del trattato che istituisce la Comunità europea del carbone e dell'acciaio (CECA). Il preambolo stesso del trattato CECA individuava già gli elementi essenziali del progetto europeo: la pace, un'Europa organizzata e vivace, misure concrete per realizzare una vera solidarietà, la sostituzione di antiche rivalità con interessi essenziali condivisi e le basi di un originale schema istituzionale per guidare le nazioni verso un destino comune.
I tristi eventi verificatisi nel 2022 ci dimostrano che, proprio come 70 anni fa, preservare la pace, sostenere lo stato di diritto e affrontare le sfide legate all'energia continuano a essere al centro del progetto dell'UE.

Cos'ha rappresentato il diritto europeo per la vita dei cittadini?
Che negli ultimi 70 anni, il diritto è stato il motore della crescente integrazione dell'Europa. Tutti i principali passi avanti nel processo di integrazione si riflettono in atti legislativi dell'UE. Di conseguenza, il diritto è probabilmente la rappresentazione più accurata della trasformazione dell'UE. Da unione economica a unione per i suoi cittadini. Il diritto europeo ha avvicinato l'Europa ai suoi cittadini e ci ha permesso di affrontare una crisi dopo l'altra.

Come ha voluto spiegare nel libro "70 anni di diritto dell'UE - Un'Unione per i suoi cittadini", che ha fatto pubblicare dal Servizio Giuridico della Commissione Europea, da lei diretto?
Esatto, è un libro che consiglio a tutti di leggere. Perché è stato scritto da avvocati il cui lavoro quotidiano nel Servizio giuridico garantisce che il diritto dell'UE sia applicato correttamente, e attuato in modo adeguato all'interno dell'Unione. Inoltre mi sarebbe piaciuto invitarvi a partecipare alla Conferenza annuale del Servizio giuridico della Commissione europea, la cui prima edizione si è tenuta il 17 marzo 2023.

Che significato ha la compliance per l'Ue?
La costruzione dell'Ue genera diverse sfide di compliance. Da un lato, le istituzioni dell'UE emanano atti legislativi. Dall'altro, ciascuno dei 27 Stati membri dell'UE è responsabile del rispetto di tali atti legislativi. Sessant'anni fa, nella causa Van Gend (Sentenza

della Corte del 5 febbraio 1963, Van Gend en Loos contro Administratie der Belastingen, n.d.r.), la Corte di giustizia ha stabilito che ogni cittadino ha il diritto di far valere le disposizioni del diritto dell'Ue, che prevedono un diritto chiaro e incondizionato direttamente davanti a un giudice nazionale. Ciò significa che i giudici nazionali sono gli esecutori in prima linea del diritto dell'Ue. Tuttavia, non è raro che gli Stati membri differiscano nell'applicazione del diritto dell'Ue. Le istituzioni dell'Ue sono progettate per affrontare e risolvere rapidamente tali differenze. I cittadini e le imprese dell'Ue devono godere degli stessi diritti, indipendentemente dal loro Stato membro. Un'applicazione uniforme del diritto dell'Ue è un pre-requisito non solo del corretto funzionamento del mercato interno, ma anche della legittimità dell'UE nel suo complesso.

Qual è il ruolo della Commissione europea in materia di compliance?
La Commissione europea ha molti ruoli, ma il più delle volte viene definita "custode dei trattati", ruolo che svolge sotto l'autorità della Corte di giustizia europea. In questa veste, l'articolo 17 del Trattato sull'Unione Europea affida alla Commissione il compito di dovere garantire l'applicazione e il rispetto del diritto dell'UE negli Stati membri. A tal fine, i Trattati mettono a disposizione della Commissione una serie di strumenti, tra cui l'avvio di procedure di infrazione. La Commissione può avviare una procedura di infrazione se ritiene che uno Stato membro non abbia adempiuto a uno degli obblighi previsti dai Trattati, e gode di un ampio margine di discrezionalità, sotto il controllo della Corte di giustizia, nel perseguire tali infrazioni. Tuttavia, la Commissione attribuisce grande importanza anche alla prevenzione. Attraverso vari strumenti, la Commissione assiste gli Stati membri nei loro sforzi per attuare e applicare il diritto dell'UE in modo tempestivo e corretto. Inoltre, la Commissione presenta costantemente le proprie osservazioni nei procedimenti pregiudiziali. La prevenzione e la conformità sono i modi migliori per evitare che le violazioni si verifichino in primo luogo.

E quale ruolo svolge il servizio giuridico in materia di compliance per l'istituzione stessa?
Il servizio giuridico della Commissione europea ha il compito di consigliare e rappresentare l'Istituzione e, nello svolgimento di tali compiti, di garantire il rispetto della legge, contribuendo così a sostenere lo Stato di diritto. In particolare, come servizio unico e orizzontale, sotto l'autorità del Presidente della Commissione europea, il Servizio giuridico svolge tre funzioni principali.

In primo luogo, fornisce una consulenza legale indipendente alla Commissione nel suo complesso, guidando l'Istituzione in merito ai limiti e alle opportunità offerte dalla legge.
In secondo luogo, rappresenta la Commissione dinanzi ai tribunali dell'Ue, nazionali e internazionali, e agli organi arbitrali. In questo modo, persegue l'applicazione del diritto dell'Ue e difende le misure attribuibili alla Commissione e/o all'Unione europea. Inoltre, il Servizio giuridico assiste la Corte di giustizia presentando la posizione della Commissione in tutte le procedure di rinvio pregiudiziale che le vengono notificate, e talvolta informa giudici e arbitri, in qualità di *amicus curiae*, su punti rilevanti del diritto dell'UE e internazionale.
In terzo luogo, fornisce consulenza alla Commissione nei suoi compiti legislativi e normativi, cercando di garantire che tutti i testi giuridici adottati dalla Commissione rispettino pienamente i Trattati, e siano redatti con la necessaria chiarezza giuridica, e nell'interesse dei cittadini dell'UE.

Che significato ha la compliance UE per i cittadini europei?
Il diritto dell'UE non comporta solo obblighi per gli Stati membri, ma anche diritti per i singoli, che possono invocarli direttamente davanti ai tribunali nazionali ed europei, a determinate condizioni. Per i cittadini dell'UE, la conformità all'UE garantisce i diritti e i benefici derivanti dal diritto dell'UE e assicura che siano rispettati senza soluzione di continuità nei 27 Stati membri.

E per le imprese?
Per le imprese dell'UE, la compliance dell'UE garantisce condizioni di parità nel mercato interno. Nella causa Van Gend en Loos, il ricorrente, una società di trasporti olandese che importava prodotti chimici dalla Germania occidentale ai Paesi Bassi, si è rifiutato di pagare le tasse di importazione richieste dalle autorità doganali olandesi, sostenendo che erano contrarie al diritto dell'UE. La compliance all'Ue facilita la possibilità di evitare tali situazioni.

Intelligenza artificiale e conformità UE. Quali rischi vedete per i cittadini e le imprese, e quali rimedi da parte dell'UE?
L'intelligenza artificiale sta dimostrando di avere il potenziale per migliorare la nostra vita e risolvere molte sfide sociali. Tuttavia, allo stesso tempo, alcuni sistemi di intelligenza artificiale presentano già dei rischi che devono essere affrontati per evitare risultati indesiderati. Secondo Mira Murati, Chief Technology Officer di OpenAI (creatore di ChatGPT), l'Intelligenza Artificiale "può essere usata in modo improprio, o può essere usata da cattivi attori". Ecco perché abbiamo bisogno di regole che disciplinino l'Intelligenza Artificiale. Nell'aprile 2021, la Commissione europea ha proposto il Pacchetto Intelligenza Artificiale, che comprende una comunicazione sulla promozione di un approccio europeo all'Intelligenza Artificiale, una revisione del Piano coordinato sull'Intelligenza Artificiale e una proposta di regolamento che stabilisce norme armonizzate sull'intelligenza artificiale.

Come definire la compliance dell'Ue in epoca di intelligenza artificiale?
L'Ue si sta attivando per garantire che i cittadini possano fidarsi di ciò che l'Intelligenza Artificiale ha da offrire. I cittadini dovrebbero essere in grado di scoprire perché un sistema di intelligenza artificiale ha preso una decisione o una previsione, e ha intrapreso una determinata azione. Altrimenti, potrebbe non essere possibile valutare se qualcuno è stato ingiustamente svantaggiato da un sistema di Intelligenza Artificiale. È necessario un quadro normativo per garantire la sicurezza e i diritti fondamentali delle persone e delle imprese. Inoltre, l'Ue intende fornire agli sviluppatori, agli implementatori e agli utenti requisiti e obblighi chiari riguardo agli usi specifici dell'Intelligenza Artificiale, riducendo al contempo gli oneri amministrativi e finanziari per le imprese, in particolare per le piccole e medie imprese (PMI). Infine, questa azione mira anche a rafforzare l'adozione, gli investimenti e l'innovazione nell'Intelligenza Artificiale in tutta l'Ue.

Quali sono le differenze tra le PME e le grandi imprese in materia di compliance europea?
Le PMI sono la spina dorsale dell'economia europea. Le voci delle PMI devono essere ascoltate e i loro interessi devono essere presi in considerazione dai responsabili politici. Allo stesso modo, il contesto imprenditoriale deve favorire lo sviluppo delle PMI. La conformità all'UE garantisce che le PMI possano sfruttare appieno e giustamente l'ambiente imprenditoriale facilitato dal diritto comunitario.
Già nel 2008 la Commissione europea ha adottato la cosiddetta comunicazione "Small Business Act", approvata dal Consiglio, dal Consiglio europeo e dal Parlamento europeo. Questa comunicazione introduce, tra l'altro, il principio "pensare anzitutto in piccolo", secondo il quale le norme che hanno un impatto sulle imprese devono tenere conto della posizione spe-

cifica delle PMI. Inoltre, delinea le migliori pratiche tratte dall'esperienza degli Stati membri, come il test PMI, che fa parte delle valutazioni di impatto normativo di un numero sempre maggiore di Stati membri. Attualmente è in fase di elaborazione un test PMI rafforzato, con l'obiettivo di garantire che le imprese europee traggano vantaggio dal mercato unico senza pagare un prezzo sproporzionato.
Più di recente, nel suo programma di lavoro per il 2023, la Commissione ha ribadito il suo impegno a rimuovere gli ostacoli che ancora frenano le PMI, riconoscendo il loro ruolo di "spina dorsale della lunga storia industriale dell'Europa". A tal fine, la Commissione si è impegnata a presentare un pacchetto di aiuti alle PMI. Si è inoltre impegnata a rivedere la direttiva sui ritardi di pagamento per ridurre gli oneri per le PMI, continuando a seguire l'approccio "uno dentro, uno fuori" nel quadro dell'agenda per una migliore regolamentazione, per ridurre la burocrazia e semplificare la legislazione relativa alle PMI.

L'Italia, comprese le sue imprese, come applica la compliance UE? E Quali sono le principali differenze che nota rispetto agli altri Paesi europei?
La Commissione continua a impegnarsi con tutti gli Stati membri, compresa l'Italia, per sostenerli nella corretta applicazione del diritto dell'UE, per rimediare rapidamente ai problemi che si verificano e per intervenire con decisione sulle violazioni che rischiano di minare i valori e le libertà fondamentali dell'UE, o che possono ostacolare importanti obiettivi politici dell'UE.
L'Italia, da parte sua, deve garantire che i suoi cittadini e le sue imprese possano beneficiare dei diritti e dei vantaggi conferiti dal diritto dell'Ue, sotto il controllo della Commissione.
In generale, l'Italia ha un livello accettabile di conformità alla legislazione europea e al recepimento delle direttive comunitarie. Ciò non impedisce alla Commissione di dover avviare procedure d'infrazione su alcune questioni importanti - in cui sono chiamati in causa anche altri Stati membri -, come la prevenzione della diffusione di specie esotiche invasive, le norme sul distacco dei lavoratori o il funzionamento dei registri centrali della proprietà effettiva.

In qualità di ex direttore generale della DG GROW (Mercato Interno, Industria e Imprese) e della DG ENV (Ambiente), quali consigli darebbe alle PMI sulla conformità all'UE, in particolare per quanto riguarda le politiche ambientali?
Che non c'è contraddizione tra competitività e sviluppo sostenibile. Anzi, vanno di pari passo. La conformità ambientale e la ricerca sono diventate una chiave per la competitività. Incoraggio quindi le PMI a investire nell'economia circolare e nella sostenibilità, perché saranno più efficienti, più sostenibili e più competitive.

Concludendo, la compliance Ue è solo amica o può anche essere un ostacolo per le aziende? Quali opportunità e quali rischi vede per le imprese in materia di conformità alla legislazione europea?
La compliance all'Ue è uno strumento indispensabile al servizio delle imprese. La principale opportunità per le aziende è l'accesso a condizioni di parità nel mercato interno. I rischi principali sono gli oneri burocratici, che l'Ue si sforza di affrontare con l'approccio "one in, one out" e con altri strumenti dell'agenda per una migliore regolamentazione.

E per i liberi professionisti, come gli avvocati, i commercialisti e i medici, quale ruolo svolge la legislazione europea nella loro compliance?
Sono fermamente convinto che la compliance all'UE sia fondamentale per ogni impresa, indipendentemente dalla forma societaria o dall'attività professionale. Il diritto dell'Ue offre grandi vantaggi e opportunità a ogni individuo.

Daniel Calleja si è laureato in Giurisprudenza, con lode, nel 1982, all'Università di Comillas. ICADE. Madrid. Cui è seguito, nel 1983, un Master in Economia e Commercio, ed un Diploma in diritto commerciale europeo (City of London Polytechnic) e, nel 1985, un Diploma in Diritto dell'Unione Europea con lode (Universidad Complutense di Madrid).
Dal 15 luglio 2020 è il Direttore generale del Servizio giuridico (LS) della Commissione Europea, dopo essere stato (dal settembre 2015 al luglio 2020) Direttore generale dell'Ambiente (DG ENV), e (dal febbraio 2012 all'agosto 2015) Direttore generale del Mercato interno, industria, imprenditoria e PMI (DG GROW) e inviato per le PMI.
È stato anche (dal novembre 2004 al gennaio 2011) Direttore per il trasporto aereo della Commissione europea (DG TREN/MOVE), e (dall'ottobre 2000 al novembre 2004) Capo di gabinetto della Vicepresidente della Commissione europea, Loyola de Palacio, responsabile dei trasporti e dell'energia; dopo essere stato (dal novembre 1995 al settembre 1999) il Capo di gabinetto del Commissario Marcelino Oreja, responsabile degli affari istituzionali, della politica audiovisiva e delle relazioni con il Parlamento Europeo. Ha iniziato la sua carriera alla Commissione Europea proprio al Servizio Giuridico (dal 1986 al 1992), che ora dirige. Prima di essere stato (dal 1993 al 1994) membro del gabinetto dei Commissario ai Trasporti e all'Energia, Abel Matutes e Marcelino Oreja e (nel 1995) Membro del gabinetto del Presidente della Commissione europea, Jacques Santer. Prima dell'ingresso in Commissione Europea, dal 1984 al 1986, ha lavorato come consigliere giuridico presso Procter & Gamble (Spagna).
È iscritto all'Ordine degli Avvocati di Madrid dal 1984 ed é stato docente di diritto dell'Ue presso diverse Università quali l'Universidad de Comillas, ICADE, l'Istituto Europeo di Amministrazione Pubblica di Maastricht, l'Università Nazionale Spagnola (UNED), il Real Instituto de Estudios Europeos de Zaragoza e la Fordham University di New York.
Di madre lingua spagnola, parla correntemente inglese, francese, tedesco, italiano e portoghese.

La compliance secondo Barilla

Intervista a Silvia Garsi

di Giuliano Testi

La storia di Barilla inizia a Parma nel lontano 1877, con una piccola bottega di pane e pasta. Oggi, a 145 anni di distanza, i prodotti Barilla sono presenti in oltre cento paesi e sono diventati icone del settore alimentare. Molti saranno sorpresi nel sapere che, nonostante tutto ciò, Barilla rimane un'azienda familiare non quotata in borsa. Anche per il Gruppo Barilla il tema della compliance è divenuto sempre più importante. Ne ho parlato con Silvia Garsi, Head of Legal Compliance & Regulatory

Cosa significa compliance per Barilla?
Fermo restando che il concetto di compliance si riferisce alla conformità delle attività e delle operazioni alle norme, alle leggi, ai regolamenti, al *corpus* normativo di *sotf law* e, infine, alle policy e procedure interne, per Barilla la compliance è stata, sin dalla sua istituzione, uno dei presidi fondamentali per garantire che l'Azienda agisse in modo etico e secondo i più elevati standard di settore.
Barilla, poi, ha inteso conferire alla nozione di compliance un ampio spettro semantico, ricomprendendovi le seguenti materie: diritto alimentare; diritto della comunicazione; anti-riciclaggio; antitrust; anti-corruzione; sanzioni internazionali e, infine, privacy.
Il tutto è stato poi tradotto in una specifica policy a cui l'intero Gruppo è chiamato a conformarsi, oltre ad un Codice Etico che si pone al vertice nelle fonti di governo interno della conformità.

Quante sono le persone che in Barilla si occupano di compliance?
Barilla ha istituito un team denominato *Global Compliance & Regulatory*, di cui sono responsabile, attualmente composto da 5 professionisti.

Come è organizzata la sua funzione?
Il team *Global Compliance & Regulatory* è inserito all'interno della Process Unit *Global Legal Corporate and Compliance* e sostanzialmente consta di tre unità:
- diritto alimentare e diritto della comunicazione;
- privacy;
- anti-riciclaggio; antitrust; anti-corruzione; sanzioni internazionali e gestione del canale whistleblowing.

Quali sono le maggiori difficoltà che ha incontrato nel gestire un tema delicato come quello della compliance?
Introdurre nel tessuto organizzativo la funzione di conformità presenta senz'altro molteplici sfide. In linea generale, nella nostra esperienza, queste possono riassumersi nelle seguenti: definizione di un perimetro netto di normative di settore come riferimento delle attività poste sotto la gestione della compliance; comprensione e adeguamento alle norme e regolamenti in continua evoluzione; integrazione efficace della compliance nella cultura e nella strategia aziendale; assicurare la coerenza delle pratiche aziendali con le norme e i regolamenti; rilevare e prevenire potenziali violazioni della compliance; gestire il rischio reputazionale e legale connesso a eventuali violazioni della compliance.
Una volta ultimata la fase di progettazione del sistema di compliance, poi, abbiamo avuto cura che fosse posta nelle condizioni di svolgere efficacemente il proprio compito. Questo obiettivo è stato raggiuto dotandola delle risorse necessarie a svolgere la propria funzione di garanzia e monitoraggio e ponendola al giusto livello gerarchico in modo da salvaguardarne l'indipendenza di azione e di riporto organizzativo.

Quali sono i principi ispiratori del vostro modello 231?
Barilla si è dotata di un Modello in tre società del gruppo: Barilla G. e R. Fratelli - Società per Azioni, che è la holding operativa del Gruppo; Barilla Iniziative, che svolge prevalentemente attività di gestione delle partecipazioni; e First S.p.A., che è la società commerciale del Gruppo per il territorio italiano.
Il Modello di Barilla G. e R. Fratelli è stato il primo ad essere adottato, nel 2005. Da tale data, si sono succeduti molteplici mutamenti del quadro normativo di riferimento, dell'assetto societario e della struttura organizzativa aziendale in conseguenza dei quali si è resa necessaria un'importante e continua attività di revisione e sviluppo; infatti, i nostri Modelli si ispirano alla particolare realtà imprenditoriale dell'azienda che ha inteso dotarsene.
Nel 2021, in cooperazione con la funzione interna di Group Internal Audit, è stato svolta una considerevole revisione dell'impostazione dei Modelli: si è passati da un approccio basato sull'identificazione del reato ad un approccio basato sull'identificazione del processo. Questo significa che, oggi, le Persone Barilla interessate avranno la possibilità di leggere i Modelli con maggiore facilità di consultazione, ritrovando nei processi di proprio interesse le norme di comportamento che dovranno seguire per prevenire il rischio di commissione del reato.
Attraverso tale revisione si è voluto dare ancor più risalto ad uno dei principi cardine dei nostri Modelli, ovvero la sensibilizzazione ed informazione delle nostre Persone rispetto ai temi della compliance. Solo in questo modo le azioni di ciascuno di noi possono essere caratterizzate da comportamenti corretti e trasparenti, in linea con i valori etico-sociali cui Barilla si ispira nel perseguimento del proprio oggetto sociale e tali da prevenire il rischio di commissione dei reati previsti dal decreto.

Quali devono essere le qualità del moderno manager della compliance?
Il manager della compliance deve essere prima di tutto un business partner e, come tale, deve essere ben integrato nel tessuto organizzativo e di processo dell'azienda. Come competenze fondamentali citerei: la conoscenza dell'organizzazione aziendale e delle leggi e regolamenti disciplinanti le materie nel perimetro; la capacità di guidare e motivare gli stakeholder verso l'adempimento degli obblighi normativi; la capacità di comunicare in modo chiaro e trasparente sia verso l'interno che verso l'esterno; la capacità di identificare e gestire i rischi aziendali e di adottare misure preventive o di mitigazione; il prestare attenzione ai dettagli e prevenire circostanze da cui possano insorgere delle non conformità; il lavorare in stretta e proficua collaborazione con altre figure aziendali per garantire l'efficacia dei sistemi di compliance.

Come diffondete la cultura della compliance all'interno della vostra azienda?
Diffondere la cultura della compliance è un elemento imprescindibile di un programma efficace. Infatti, per quanto possiamo essere addentro ai processi aziendali, il contributo di tutti verso il rispetto delle norme è essenziale nella prevenzione del rischio.

Sono molte le iniziative attraverso le quali cerchiamo di diffondere la cultura della compliance.
Anzitutto, consapevoli dell'importanza del commitment dall'alto, informiamo periodicamente il Consiglio di Amministrazione delle aree e dei processi a maggior rischio e delle cautele adottate. Questo ci permette di alzare il livello di attenzione, così come di avere accesso alle risorse necessarie per garantire la tenuta del sistema.
Inoltre, abbiamo strutturato un programma di training con un approccio *tailored*, che ci permette di formare le varie funzioni aziendali in modo che le Persone Barilla si ispirino nel loro agire a quelli che sono i principi etici e giuridici da cui Barilla non può prescindere, posti dalla legge e recepiti dalle Policy e Procedure aziendali.
Infine, ci facciamo promotori di molteplici campagne di comunicazione attraverso le quali vogliamo sempre tenere alta l'attenzione sulle tematiche di compliance, con l'obbiettivo di informare tutte le Persone Barilla dei risultati raggiunti attraverso le attività promosse dal nostro dipartimento.

Quali sono i più evidenti e principali vantaggi di una buona compliance?
L'adozione ed efficace implementazione di un programma di compliance porta evidenti vantaggi, che possono essere osservati sia nel quotidiano che nelle situazioni di maggior criticità.
Riteniamo che una buona compliance sia idonea prima di tutto a guidare le Persone Barilla verso comportamenti eticamente corretti, oltre che ad evitare l'applicazione di sanzioni che graverebbero sul conto economico dell'Azienda e sulla sua reputazione. Ulteriormente contribuisce a consolidare sempre più la relazione di fiducia con i nostri consumatori, che insieme alle Persone Barilla sono il bene più prezioso per l'Azienda.
Non solo, infatti, i nostri consumatori si aspettano che Barilla continui a realizzare prodotti buoni e di qualità, ma pretendono anche che ciò avvenga attraverso un comportamento ispirato ai valori etici che l'Azienda persegue e rispettoso del quadro normativo di riferimento.

Utilizzate degli indicatori reputazionali o dei rating di legalità?
Agire eticamente e nel rispetto delle leggi significa anche relazionarsi con soggetti che tengano i medesimi standard. Per fare ciò adottiamo delle procedure di valutazione dei clienti e dei fornitori che ci permettono di sapere esattamente chi sono i nostri partner.
Il controllo è duplice, all'ingresso e in costanza del rapporto.
Per poter lavorare con Barilla chiediamo che i nostri partner abbiano adottato delle politiche aziendali improntate all'etica e alla legalità. Chiediamo sempre l'accettazione del nostro Codice Etico, il che significa che i nostri partner devono riconoscersi nei nostri valori.
Inoltre, a seconda del loro ambito professionale, richiediamo ulteriori requisiti specifici. Ad esempio, i fornitori di servizi logistici, manutentivi e di smaltimento rifiuti per poter lavorare con Barilla devono essere iscritti all'interno delle c.d. White List presso le Prefetture; questo requisito, imprescindibile per partecipare alle gare d'appalto pubbliche, non sarebbe necessario nei rapporti fra privati, ma riteniamo che sia un importante presidio nella prevenzione dei rischi legati a potenziali inopportune interferenze ed influenze esterne nella rete di fornitori.
In costanza del rapporto, poi, monitoriamo i nostri partner sottoponendoli a screening periodici automatizzati effettuati attraverso software ad hoc che ci permettono di rilevare prontamente qualsiasi variazione dell'affidabilità del partner. Questo controllo, assieme a specifiche clausole contrattuali che ci consentono di intervenire prontamente con la sospensione o risoluzione dei rapporti in essere, garantiscono che Barilla operi solamente con partner commerciali rispettosi dei principi etici e di legalità propri di Barilla.
Avete un sistema strutturato di audit interno?
La funzione posta sotto la mia responsabilità svolge regolarmente attività di monitoraggio sia interno, per perseguire il miglioramento continuo dei processi che gestiamo, sia verso l'esterno. In questo caso, soprattutto nei confronti di fornitori e clienti del Gruppo da cui ci aspettiamo, come presupposto minimo, l'adozione di standard qualitativi, etici e di sostenibilità adeguati, oltre che naturalmente di conformità alle normative applicabili ai contesti in cui operiamo.
In aggiunta, abbiamo instaurato una proficua collaborazione con il team Group Internal Audit per mantenere un approccio coordinato, sia sul versante della pianificazione che su quello della metodologia per condurre le attività di cui discorriamo.

La compliance è un costo che porta dei benefici o un beneficio che comporta dei costi?
Onestamente faccio molta fatica ad associare la funzione Compliance con l'idea che, direttamente o indirettamente, rappresenti un costo.
La considero semmai un'opportunità, oramai divenuta imprescindibile visto il proliferare di normazione in qualsiasi settore.

Quanto si ritiene soddisfatto del suo lavoro?
Mi ritengo molto soddisfatta, in particolare nel constatare come le attività di compliance che coordino siano apprezzate e divenute parte integrante dei processi aziendali.

È più giusto credere in quello che si fa o fare quello in cui si crede?
Non penso ci sia una risposta giusta ed una sbagliata potendo scegliere solo una delle opzioni.
Credere in quello che si fa significa che si ha fiducia nelle proprie azioni e decisioni, e si ritiene che siano giuste e corrette. Questo può essere utile in situazioni in cui si hanno l'esperienza e la conoscenza del contesto in cui si opera e si hanno le competenze per operare e quindi per concretizzare i propri obiettivi.
D'altra parte, fare quello in cui si crede significa che si agisce in base ai propri valori e a propri principi cercando di condividerli e quindi di fare in modo che essi vengano accettati anche dalle altre persone. Questo può essere importante quando si cerca di perseguire un obiettivo più grande, come una causa sociale.
In generale, entrambi gli approcci possono essere giusti a seconda del contesto. Tuttavia, è importante essere consapevoli delle proprie motivazioni e delle conseguenze delle proprie azioni su se stessi e sugli altri, per assicurarsi che siano in linea con i propri valori.

Dal “Codice Etico” del Gruppo Barilla

Valori

Barilla è un Gruppo alla cui guida è da quattro generazioni la stessa famiglia, per questo ha una forte identità alla cui base è da sempre uno «stile» umano e professionale fatto di correttezza nei comportamenti, di equilibrio tra il rispetto per le persone e l’interesse per l’Azienda.
Cambiano le pratiche e gli scenari, ma la coerenza con questi valori è e resterà il migliore biglietto da visita. Lo «stile» Barilla, inteso come un reciproco arricchimento umano e professionale delle persone che vi lavorano, resterà immutato se tutti coloro che operano nel Gruppo continueranno a rispettare i basilari valori e princìpi di riferimento.
Barilla considera come punti irrinunciabili nella definizione dei propri valori la Dichiarazione Universale dei Diritti Umani dell’ONU, le Convenzioni e le Raccomandazioni Internazionali del Lavoro emanate dall’ILO (International Labour Organization), la Carta della Terra redatta dall’Earth Council e i princìpi enunciati nel Global Compact proposto dall’ONU.

1. Onestà e Trasparenza
L’onestà rappresenta il principio fondamentale per tutte le attività di Barilla, le sue iniziative, i suoi prodotti, i suoi rendiconti e le sue comunicazioni e costituisce elemento essenziale della gestione aziendale. I rapporti con gli stakeholder[1], a tutti i livelli, devono essere improntati a criteri e comportamenti di correttezza, coerenza, lealtà e reciproco rispetto.
Barilla dialoga in modo chiaro, trasparente, accurato e tempestivo, con i suoi stakeholder.

2. Responsabilità sociale
Barilla crede che la propria attività imprenditoriale, per potersi qualificare come eticamente responsabile, debba perseguire modelli di produzione che rispettino e salvaguardino i diritti umani, le capacità rigenerative della Terra e il benessere delle comunità, promuovendo lo sviluppo umano in modo equo e sostenibile, nella consapevolezza che la responsabilità sociale ed etica si estende anche alle comunità, soprattutto nei paesi in via di sviluppo, che producono materie prime utilizzate per alcuni prodotti.

3. Centralità della persona – Diversità e Inclusione (D&I)
In coerenza con la sua visione etica, Barilla intende sviluppare il valore di ogni persona, rispettandone l’integrità fisica, culturale e morale, così come il diritto di interagire ed associarsi con altri. Barilla pone attenzione a tutti gli aspetti inerenti la vita delle persone, poiché è la vita umana ad ispirare tutte le attività della società. Barilla supporta e rispetta i diritti umani nelle sue attività e sfera d’influenza, offre eguali opportunità per lo sviluppo delle sue persone e ne protegge la privacy.
Barilla crede che fare la cosa giusta sia corretto per il business e che rispettare la diversità e promuovere l’inclusione possa essere fonte di vantaggio competitivo, creando una forza lavoro più motivata per l’adozione delle migliori decisioni, basate su una profonda comprensione delle persone che acquistano e consumano i prodotti della società in tutto il mondo. Barilla non tollera alcuna forma di discriminazione o esclusione, fra l’altro per quanto attiene età, cultura, etnìa, nazionalità, credo religioso, razza, opinione politica, stato civile, gravidanza, stato di reduce di guerra, genere e orientamento sessuale, identità e/o espressione di genere, informazione genetica, salute o disabilità.

4. Tutela del lavoro
Barilla garantisce la libertà di associazione dei lavoratori e riconosce il diritto alla contrattazione collettiva. Si impegna a non usufruire, neppure indirettamente, sia del lavoro forzato e obbligatorio, sia del lavoro minorile. Rifiuta ogni discriminazione in base all’età, al sesso, alla sessualità, allo stato di salute, alla razza, alla nazionalità, alle opinioni politiche e alle credenze religiose; ripudia ogni forma di discriminazione nelle politiche di assunzione e nella gestione delle risorse umane. Barilla si impegna a impedire ogni forma di mobbing e di sfruttamento del lavoro, sia diretto che indiretto, e a riconoscere nel merito, nelle prestazioni di lavoro e nelle potenzialità professionali i criteri determinanti per gli sviluppi retributivi e di carriera.

5. Salvaguardia dell’ambiente e benessere degli animali
L’impegno di Barilla nei riguardi della Terra, è volto a salvaguardarne l’abbondanza e la bellezza per le generazioni presenti e future, con l’obiettivo di trasmettere loro i valori e le tradizioni che sostengono lo sviluppo a lungo termine delle comunità umane e ambientali.

Barilla si impegna in ogni fase del suo agire ad applicare criteri di cautela – il «Principio di Precauzione»[2] – e un approccio preventivo nei riguardi dell’ambiente e della sua biodiversità; a promuovere iniziative per una maggiore responsabilità ambientale aziendale; a sviluppare l’impiego di mezzi e di tecnologie che non danneggino l’am- biente.
Sia nella scelta delle materie prime, sia nella distribuzione dei prodotti Barilla si adopera per il rispetto della «Sovranità Alimentare[3], nella consapevolezza che la responsabilità etico-sociale si estende anche alle comunità che producono le materie prime.
L’impegno di Barilla a salvaguardare il pianeta ed il benessere delle generazioni presenti e future include anche il benessere degli animali. Barilla, infatti, non testa i propri prodotti o le proprie materie prime su animali, né finanzia o sostiene, in modo diretto o indiretto, la sperimentazione sugli animali, salvo che ciò sia strettamente necessario per ordine delle autorità competenti o sia imposto da leggi, regolamenti o esigenze di sicurezza.
Barilla dissuade i suoi fornitori dall’uso della sperimentazione animale e sostiene fermamente l’impiego di metodi alternativi alla sperimentazione animale.

6. Rispetto di leggi, codici e regolamenti vigenti
Barilla reputa il rispetto delle normative nazionali e internazionali come condizione vincolante e imprescindibile del proprio agire. Si impegna pertanto, anche con attenta opera di prevenzione sulla consumazione di illeciti, a rispettare tali normative nonché le prassi generalmente riconosciute. Ispira inoltre le proprie decisioni e i propri comportamenti alle possibili evoluzioni del quadro normativo.

Norme e standard di comportamento

1. Rapporti con gli stakeholder
I rapporti con gli stakeholder, a tutti i livelli, devono essere improntati a criteri e comportamenti di assoluta correttezza, collaborazione, lealtà e reciproco rispetto. Barilla considera come propri stakeholder: azionisti e finanziatori, Esponenti Aziendali e collaboratori esterni, clienti, fornitori, concorrenti, pubblica amministrazione, acquirenti di prodotti, collettività, comunità locali, mass-media.

2. Marketing e Comunicazione
Barilla ha il dovere di assicurare le condizioni necessarie affinché i suoi prodotti possano contribuire a una alimentazione nutrizional- mente equilibrata. Tuttavia l’alimentazione, oltre che un fatto biologico, è legata profondamente all’identità culturale dei singoli individui; per questo tutte le attività di marketing devono muoversi nel pieno rispetto delle diverse consuetudini e dei diversi valori, in materia di produzione e consumo del cibo.
È quindi necessario considerare gli acquirenti dei prodotti Barilla come veri e propri interlocutori: delle «persone» che hanno il diritto di ricevere tutte le informazioni necessarie per compiere una scelta consapevole al momento dell’acquisto, e non solamente quali semplici
«consumatori» di prodotto.
Per il raggiungimento degli obiettivi di impresa Barilla ha quindi il dovere di:
- garantire alle persone una relazione basata su fiducia e lealtà;
- prendere in considerazione, oltre ai «bisogni», anche quelle naturali esigenze intellettuali e cognitive che spingono le persone ogni giorno a chiedersi cosa stiano mangiando.
La comunicazione di Barilla:
- sarà sempre rispettosa della centralità della «persona» con tutto il suo articolato sistema di bisogni

1 Sono stakeholder quei soggetti (intesi nel senso di individui, gruppi, organizzazio- ni, istituzioni) i cui interessi sono, a vario titolo, coinvolti nell’attività del Gruppo.

2 «Principio di Precauzione» è principio in base al quale, in caso di dubbio sull’innocuità per l’ambiente o per la salute di un prodotto o di un metodo di produzione, la dimostrazione della non nocività deve essere a carico del produttore.
3 Per «Sovranità Alimentare» intendiamo il diritto dei popoli ad autodeterminare le proprie scelte nei settori della produzione, della distribuzione e del consumo di ali- menti, nel rispetto dei criteri di sostenibilità ambientale, culturale e sociale, allo scopo di garantire il diritto di ogni individuo a un’alimentazione sufficiente e sana. Il diritto all’alimentazione è un diritto umano fondamentale, saldamente fondato sul diritto internazionale. E implicito nella Carta delle Nazioni Unite ed è stato riaffermato e sviluppato in numerose dichiarazioni della comunità internazionale, inclusa la Dichiarazione Universale dei Diritti dell’Uomo (art. 25), e in molti accordi internazionali sia a livello regionale che universale. La «Sovranità Alimentare» procede parallelamente e favorisce la sovranità economica, politica e culturale dei Paesi.

fisici, psicologici, culturali e affettivi: la logica di mercato non dovrà mai ostacolare la piena trasparenza informativa relativamente a contenuto e corretto utilizzo dei prodotti;
- rifiuterà messaggi volgari, contraddittori, incerti o ambigui;
- avrà sempre presente la propria responsabilità nell'influenzare le scelte delle persone, facendosi garante della qualità della relazione fra impresa e persone.

3. Informazione e rendicontazione
Tutte le attività di informazione e di dialogo con gli stakeholder devono avere caratteristiche di chiarezza, trasparenza, tempestività, completezza e coerenza, nel rispetto del diritto all'informazione.
Ciascun dipendente è tenuto a collaborare affinché i fatti di gestione siano rappresentati correttamente e tempestivamente nella contabilità sulla base di informazioni veritiere, accurate, complete e verificabili. Ogni operazione e transazione deve essere correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua. È compito di ogni dipendente far sì che la documentazione di supporto sia facil- mente rintracciabile e ordinata secondo criteri logici.
Nessuna scrittura contabile falsa o artificiosa può essere inserita nei registri contabili dell'Azienda (o del Gruppo) per alcuna ragione. Nessun dipendente può impegnarsi in attività che determinino un tale illecito, anche se su richiesta di un superiore.

4. Controllo interno
Barilla riconosce la massima importanza al controllo interno inteso come un processo, svolto dagli Esponenti Aziendali, finalizzato ad agevolare la realizzazione degli obiettivi aziendali, a salvaguardare le risorse, ad assicurare la conformità alle leggi ed ai regolamenti appli- cabili, a predisporre bilanci e dati economico-finanziari attendibili, veritieri e corretti.
Per questo fine Barilla ha creato e sviluppato nel tempo un insieme di strumenti, procedure e meccanismi idonei a gestire il funzionamento ed il monitoraggio dell'organizzazione.
Ben consapevole che il sistema di controllo interno rappresenta un elemento che caratterizza una buona gestione dell'Azienda, Barilla si impegna ad operare affinché la sensibilità del personale alla necessità del controllo possa essere accresciuta a tutti i livelli organizzativi. Allo stesso tempo, tutti gli Esponenti Aziendali devono sentirsi responsabili dell'aggiornamento e gestione di un efficace sistema di controllo interno. Per questo motivo la dirigenza non deve limitarsi a partecipare al sistema di controllo nell'ambito delle proprie competenze, ma deve impegnarsi a condividerne valori e strumenti con ciascun collaboratore o collega.
Tutti devono sentirsi responsabili della salvaguardia dei beni dell'Azienda (siano essi materiali o immateriali) e del loro corretto utilizzo. È fatto divieto di utilizzare in modo improprio o danneggiare i beni e le risorse dell'Azienda e di consentire ad altri di farlo.

5. Corruzione e concussione
Barilla si impegna a mettere in atto tutte le misure necessarie a prevenire ed evitare fenomeni di corruzione e concussione.
Non è consentito che siano versate somme di denaro, esercitate altre forme di corruzione allo scopo di procurare vantaggi diretti o indiretti all'Azienda stessa. Si fa divieto di accettare doni o favori da parte di terzi che oltrepassino le normali regole di ospitalità e cortesia.
Questo vale sia nel caso in cui un Esponente Aziendale persegua un interesse diverso dalla missione di impresa o si avvantaggi personal- mente di opportunità d'affari.

6. Diligenza e correttezza nella gestione dei contratti
I contratti e gli incarichi di lavoro devono essere eseguiti secondo quanto stabilito consapevolmente dalle parti. Per una corretta gestione dei rapporti contrattuali Barilla si impegna a non sfruttare posizioni di dominio rispetto alle proprie controparti ed a garantire una informativa ampia ed esaustiva verso tutti i dipendenti e collaboratori coinvolti nelle attività previste dai contratti stipulati.

7. Protezione delle informazioni
Barilla riconosce che i beni intangibili digitali hanno col tempo acquisito un'importanza sempre crescente e considera la sicurezza delle informazioni, e l'osservanza dei relativi principi di riservatezza, integrità e disponibilità dei dati, come parte integrante delle sue attività.
Barilla si impegna a proteggere i propri sistemi informativi dall'accesso illegittimo e dalla divulgazione non autorizzata delle informazioni trattate, garantendo al contempo la piena conformità alle applicabili normative in materia di protezione dei dati personali e agli standard di sicurezza delle informazioni.

Uno sguardo sull'UE

di Denise Boriero
Supervisione di Carlo Zadra[1]

Si riportano, di seguito, alcune tra le più importanti novità relative alle istituzioni dell'UE, attinenti ai temi della Compliance:

Atti delle istituzioni UE:

Al via dal 1° giugno 2023 il Brevetto Unitario per l'UE
Dal 1° giugno 2023 prenderà il via il Brevetto Unitario per l'Unione Europea. Attraverso tale sistema sarà consentita una tutela brevettuale uniforme in tutti gli Stati aderenti dell'Unione, attraverso un'unica domanda di brevetto depositata presso l'Ufficio Europeo dei Brevetti (EPO).
Il Governo tedesco ha recentemente depositato lo strumento di ratifica dell'Accordo su un Tribunale unificato dei brevetti (UPCA, Accordo 2013/C 175/01 del Consiglio) presso il Consiglio dell'Unione Europea, completando così le procedure di ratifica necessarie per l'entrata in funzione del sistema.
Il nuovo sistema mira a creare un mercato tecnologico uniforme, facilitando le transazioni in una grande regione economica. Il Brevetto Unitario rappresenta un progresso storico per gli innovatori e la protezione delle invenzioni in Europa. In particolare, esso dovrebbe risultare particolarmente vantaggioso per le piccole realtà, fornendo una tutela più ampia a costi limitati.
Attualmente il sistema unitario riguarda 17 Stati membri ma è prevista la prossima adesione di altri. L'interesse ad oggi dimostrato è infatti molto ampio: dal 1° gennaio 2023, data di avvio delle procedure transitorie di attuazione, nei soli due primi mesi dell'anno sono state presentate oltre 2.200 richieste.

Orientamenti del Consiglio per una nuova *governance* economica dell'UE
Il Consiglio UE ha indicato gli orientamenti per provvedere ad una riforma del quadro di *governance* economica dell'Unione per far fronte alle sfide economiche e sociali di questi ultimi anni. Pur mantenendo il ciclo di sorveglianza annuale nel contesto del semestre europeo, il Consiglio riconosce l'importanza di una programmazione a medio-lungo termine: il passaggio ad una pianificazione di bilancio pluriennale potrebbe infatti comportare diversi vantaggi. Sarà necessario tenere in considerazione la situazione iniziale dell'economia di ciascuno Stato membro e la differenziazione dei singoli percorsi economici. Andrà riconosciuto il processo democratico dei diversi Paesi nella creazione della loro politica economica, pur dovendo ciascuno garantire la conformità al criterio del disavanzo o, almeno, progressi sufficienti e credibili verso la conformità.

Commissione europea: comunicazione interpretativa in merito alla Direttiva sull'orario di lavoro
La Commissione europea ha aggiornato la sua Comunicazione interpretativa relativa alla direttiva sull'orario di lavoro (2003/88/CE) alla luce delle sentenze della Corte di Giustizia UE. La Direttiva in parola stabilisce i requisiti minimi di salute e sicurezza in

1 *Direttore dell'équipe Giustizia Affari Interni – Servizio giuridico del Consiglio dell'Unione Europea.*
Il contributo fornito e le opinioni espresse nel presente ambito non rappresentano e non esprimono in alcun modo la posizione del Consiglio dell'Unione Europea.

materia di orario di lavoro, delineando i diritti individuali di ogni lavoratore dell'Unione: il diritto di tutti a condizioni di lavoro che rispettino la salute, la sicurezza e la dignità, nonché limitazioni all'orario massimo di lavoro, ai periodi di riposo giornaliero e settimanale nonché alle ferie annuali retribuite.
Pur ribadendo che soltanto la Corte di Giustizia è competente a fornire interpretazioni vincolanti della Direttiva, la comunicazione ha lo scopo di orientare ed aiutare le Autorità nazionali, le attività imprenditoriali e i singoli cittadini che devono applicare la normativa in oggetto.

Esenzione del visto per i viaggi in Europa dei titolari di passaporto del Kosovo
Il Consiglio UE ha adottato la sua posizione in prima lettura su una proposta di regolamento che mira ad esentare del visto coloro che hanno un passaporto del Kosovo e vogliono viaggiare in Europa. In base alla procedura legislativa ordinaria, applicabile nel caso di specie, ora spetta al Parlamento prendere posizione sulla proposta al fine di raggiungere un accordo col Consiglio. Tale esenzione una volta adottata, dovrebbe trovare applicazione alla data di entrata in funzione del sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) o dal 1° gennaio 2024, se precedente.

Attività giurisprudenziale:

Per la CEDU, costituisce una violazione al diritto ad un equo processo il rifiuto immotivato di sollevare una questione pregiudiziale innanzi alla Corte di Giustizia UE
La Corte europea dei diritti dell'uomo (CEDU) il 14 marzo c.a. ha stabilito, nell'ambito della causa Georgiou v. Grecia (57378/2018) che il mancato esame, da parte di una giurisdizione di ultima istanza – nel caso di specie la Corte di Cassazione greca –di una richiesta di pronuncia pregiudiziale ai sensi dell'articolo 277 del Trattato sul funzionamento dell'Unione europea (TFUE) da parte del ricorrente, senza alcuna motivazione costituisce una violazione del diritto ad un equo processo previsto dall'articolo 6, primo comma, della Convenzione europea dei diritti dell'uomo.

La comunicazione orale di dati configura un trattamento degli stessi ai sensi del GDPR?
L'*Itä-Suomen hovioikeus* (la Corte d'appell della Finlandia orientale) ha sollevato un rinvio pregiudiziale nella causa (C-740/22) relativamente all'interpretazione delle nozioni di trasferimento e trattamento dei dati ai sensi del Regolamento generale sulla Protezione dei dati (GDPR). In particolare, il giudice del rinvio chiede di valutare se la comunicazione orale

di alcuni dati personali configuri un trattamento dei dati ai sensi dell'articolo 2, paragrafo 1, e dell'articolo 4, punto 2, GDPR.
Inoltre, si chiede se l'accesso del pubblico ai documenti ufficiali possa essere conciliato con il diritto alla protezione dei dati personali ai sensi dell'articolo 86 GDPR, qualora tale accesso consenta di ottenere, senza restrizioni, informazioni sulle condanne penali o sui reati di una persona fisica contenute nel registro delle persone di un tribunale a seguito di una richiesta di trasferimento orale delle informazioni al richiedente.
Infine, il giudice finlandese chiede di chiarire se, in tale ambito, rilevi il fatto che il richiedente sia una società o un privato.

Divieto di prestare assistenza legale a seguito di sanzioni internazionali

Alcuni Ordini degli Avvocati, in particolare quello degli Avvocati fiamminghi in Belgio (*Ordre néerlandais des avocats du Barreau de Bruxelles*, Belgio - Causa T-797/22 - 2023/C 63/79) e quello di Parigi (*Ordre des avocats à la Cour de Paris*, Francia - Causa T-798/22 - 2023/C 63/80), hanno presentato dei ricorsi di annullamento contro le misure restrittive adottate dal Consiglio UE nei confronti della Russia, a seguito dell'aggressione dell'Ucraina in violazione del diritto internazionale. In entrambe le cause, i ricorrenti chiedono al Tribunale di annullare l'articolo 1, paragrafo 12, del regolamento del Consiglio n. 2022/1904 e l'articolo 1, paragrafo 13, del regolamento del Consiglio n. 2022/2474 nella misura in cui tali disposizioni introducono un divieto di prestazione di servizi di consulenza legale.
I motivi dedotti sono plurimi: nella causa T-797/22 i ricorrenti sostengono che le nuove disposizioni in oggetto sarebbero contrarie ai principi fondamentali, riconosciuti anche nella Carta Fondamentale dei diritti dell'UE, alla tutela della vita privata e all'accesso alla giustizia, impedendo di fatto di potersi rivolgere al proprio legale e interferendo sull'indipendenza di quest'ultimo e sul segreto professionale; tali disposizioni costituirebbero altresì una violazione del principio di proporzionalità, in quanto l'introduzione di un divieto generale di prestazione di servizi di consulenza legale non sarebbe idonea a conseguire gli obiettivi legittimi perseguiti dall'Unione europea nel contesto del conflitto tra Russia e Ucraina e andrebbe oltre quanto strettamente necessario per il raggiungimento di tali obiettivi; infine, esse sarebbero state adottate in violazione del diritto alla certezza del diritto, in quanto il divieto generale di prestare di assistenza legale non sarebbe né chiaro né preciso.
Nella causa T-798/22 i ricorrenti ripresentano i primi due motivi di ricorso relativi alla lesione del diritto di avvalersi di un avvocato e a conoscere pienamente le tutele esperibili assieme alla lesione del segreto professionale. Oltre a tali motivi, esse aggiungono il motivo della violazione dell'obbligo di motivazione di cui all'articolo 296 TFUE, in quanto il Consiglio non avrebbe fornito alcuna spiegazione in merito alla ragione del divieto generale di fornire servizi di consulenza legale in materia non contenziosa. Spetta ora al Consiglio presentare il proprio contro ricorso dinanzi al Tribunale in merito alla portata delle norme di cui si chiede l'annullamento.

Corte di Giustizia UE: Statistiche giudiziarie per il 2022

La Corte ha pubblicato la relazione sulle statistiche giudiziarie per il 2022. Tra i principali temi affrontati dalla Corte di Giustizia e dal Tribunale dell'Unione europea vi sono lo Stato di diritto, l'ambiente, la privacy digitale, la lotta alla discriminazione e l'applicazione delle norme sulla concorrenza contro i giganti digitali. Mentre il numero dei procedimenti dinnanzi al Tribunale rimane abbastanza invariato (con una media di 883 cause l'anno), l'attività della Corte è aumentata del 21%. Il precedente anno, il maggior numero di richieste di pronuncia pregiudiziale sono state presentate dai tribunali tedeschi, italiani, bulgari, spagnoli e polacchi.
La durata media dei procedimenti è di circa 16,2 mesi se si considerano sia le cause concluse con sentenza sia quelle con ordinanza, e di 20,4 mesi se si considerano solo le cause concluse con sentenza.

Tribuna UE

di Pierpaolo Rossi

Novità Fiscalità

La relazione annuale 2022 dell'EPPO segnala preponderanza di frodi transfrontaliere in materia di IVA

L'ufficio della Procura europea (EPPO) ha pubblicato la relazione annuale per il 2022. Essa riassume la sua azione a contrasto delle frodi dell'UE che incidono sulle entrate nazionali ed europee, in particolare sulle frodi transfrontaliere in materia di IVA. Il rapporto indica che l'EPPO aveva 1.117 indagini attive alla fine del 2022, relative ad un danno totale stimato di 14,1 miliardi di euro, di cui quasi la metà (47%) derivante da frodi IVA. Secondo la relazione, l'EPPO ha elaborato 3.318 denunce di reato e ha aperto 865 indagini nel 2022. Su segnalazione dell'EPPO, i competenti giudici nazionali hanno sequestrato oltre 359,1 milioni di euro, pari a più di sette volte il budget 2022 dell'EPPO. La relazione rileva tuttavia che l'EPPO necessita ancora di adeguamenti organizzativi e giuridici per migliorarne la capacità di azione nei settori demandatigli. È in particolare necessario ultimare la revisione del regolamento EPPO e l'attribuzione di investigatori specializzati in frodi finanziarie presso tutti i procuratori nazionali delegati in tutti gli Stati membri partecipanti. Il rapporto evidenzia inoltre che l'EPPO ha scoperto che gruppi appartenenti alla criminalità organizzata si sono resi responsabili di 2,2 miliardi di euro di frode IVA e che permangono discrepanze significative nella lotta contro la frode IVA transfrontaliera nei diversi Stati membri. (https://www.eppo.europa.eu/it/node/475)

Il Consiglio aggiunge le Isole Vergini britanniche, il Costa Rica, le Isole Marshall e la Russia all'elenco UE delle giurisdizioni non cooperative

Il Consiglio europeo, nella sua revisione semestrale dell'elenco UE delle giurisdizioni non cooperative a fini fiscali, ha deciso di aggiungere le Isole Vergini britanniche, il Costa Rica, le Isole Marshall e la Russia. Per quanto riguarda le Isole Marshall, la ragione è che la giurisdizione ha un'aliquota dell'imposta sul reddito delle società pari a zero o comunque nominale e quindi può attrarre la localizzazione di redditi senza il corrispondente esercizio di un'attività economica reale. Per quanto riguarda le Isole Vergini britanniche, esse sono state incluse nella lista in quanto ritenute avere una legislazione non sufficientemente conforme alla normativa OCSE sullo scambio di informazioni su richiesta. Per quanto riguarda il Costa Rica, questo è stato incluso perché non ha adempiuto l'impegno ad eliminare gli aspetti di concorrenza fiscale dannosa relativamente al suo regime di esenzione dei redditi di fonte estera. La Russia non ha adempiuto all'impegno preso ad eliminare gli aspetti dannosi del proprio regime speciale per le holding internazionali. L'elenco dell'UE comprende ora 16 giurisdizioni in totale. Il Consiglio ha invitato le giurisdizioni interessate a migliorare il loro quadro giuridico per risolvere le questioni fiscali che ne hanno causato l'inclusione nella lista. Tra le questioni, figurano la trasparenza fiscale e l'equa tassazione, ed il rifiuto di conformarsi agli standard internazionali sulla concorrenza fiscale non dannosa. Il gruppo del Codice di condotta, che prepara gli aggiornamenti dell'elenco, collabora strettamente con organismi internazionali come l'OCSE per promuovere le pratiche di buona governance fiscale nel mondo. Il Consiglio ha inoltre sottolineato che l'Albania, il Belize, Curaçao, Israele e Qatar e Aruba hanno assunto impegni in materia di eliminazione della concorrenza fiscale internazionale dannosa, il cui rispetto sarà verificato. Il Consiglio ha poi rimosso dall'elenco Barbados, Giamaica, Macedonia del Nord e Uruguay dopo aver constato che queste giurisdizioni avevano adempiuto agli impegni presi in tal senso. (https://www.consilium.europa.eu/en/press/press-releases/2023/02/14/taxation-british-virgin-islands-costa-rica-marshall-islands-and-russia-added-to-eu-list-of-non-cooperative-jurisdictions-for-tax-purposes/)

Giurisprudenza Fiscalità

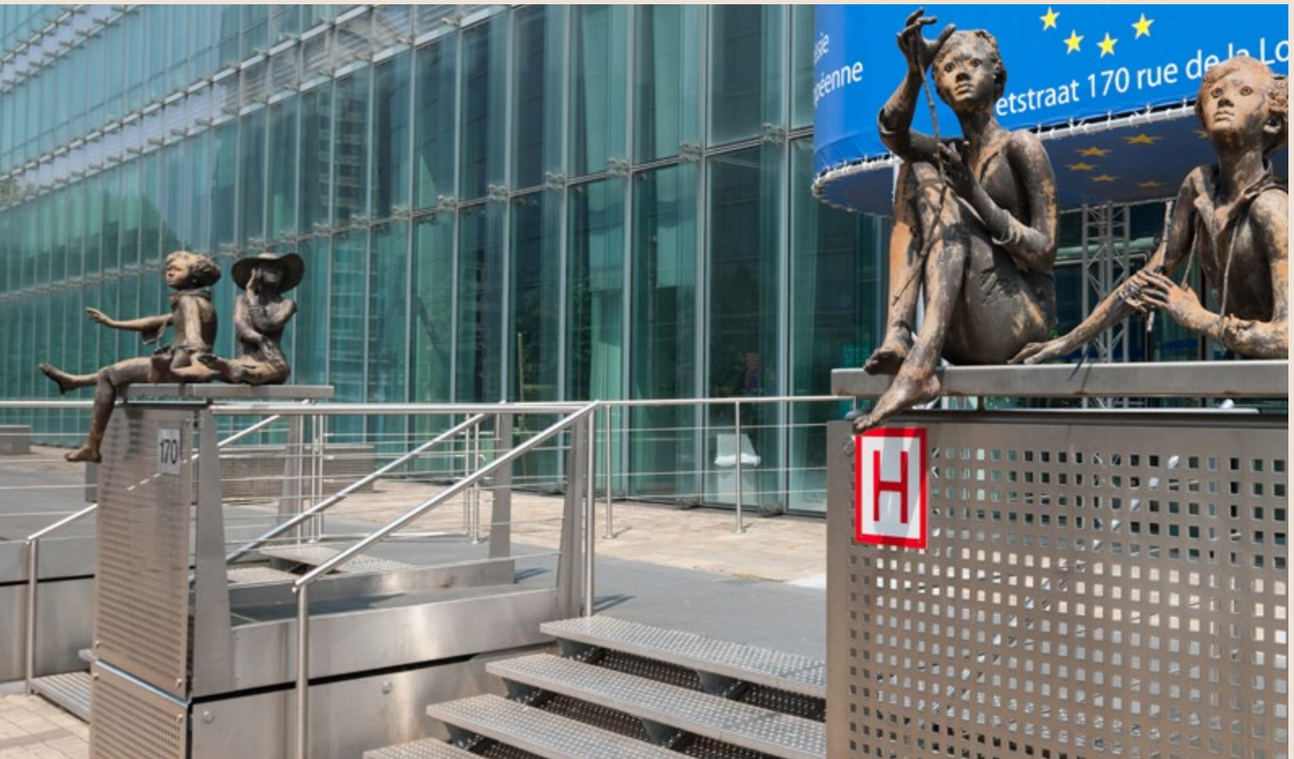
La Corte EDU sancisce che il diritto al rispetto della vita privata e familiare è violato a causa della pubblicazione sistematica dei dati personali dei debitori fiscali che avviene in modo automatico e pertanto ingiustificato

Il 9 marzo 2023, nella causa *L.B. c. Ungheria* (ricorso n. 36345/16), la Corte europea dei diritti dell'uomo (Corte EDU) ha reso un'importante sentenza stabilendo che l'articolo 8 della CEDU (diritto al rispetto della vita privata e familiare e del domicilio) è violato da una disposizione legislativa ungherese che prevede la pubblicazione dei dati personali dei contribuenti indebitati. Il caso riguardava un cittadino ungherese che aveva arretrati fiscali per circa 625.000 euro. A seguito di una verifica fiscale nel 2013, l'Agenzia delle Entrate aveva accertato che il soggetto (ricorrente) non aveva pagato l'imposta sui redditi per circa 2 milioni di euro che questi aveva ricevuto in contanti da una società a responsabilità limitata di cui era stato amministratore delegato fino al 2009. Gli era stata quindi inflitta una multa di 490.000 euro maggiorata di interessi, sanzione passata definitivamente in giudicato. Nel 2014, l'autorità fiscale pubblicava il nome del ricorrente assieme ai suoi dati personali in un elenco dei debitori inadempienti sul suo sito web. I dati pubblicati comprendevano il suo nome, indirizzo di casa, numero di identificazione fiscale e l'importo dell'imposta non pagata dovuta. Ai sensi della legislazione modificata del 2006, nel 2016 il ricorrente è stato poi incluso anche in un elenco di "principali debitori fiscali" del sito web dell'autorità fiscale. Una testata giornalistica online ha poi pubblicato una mappa interattiva dei debitori fiscali, che indicava l'indirizzo di casa del ricorrente, basata sui dati tratti dall'elenco dei principali debitori pubblicato dall'autorità fiscale. I dati personali del ricorrente sono stati infine rimossi dall'elenco dei maggiori debitori fiscali, ma solo quando gli arretrati dovuti sono caduti in prescrizione nel 2019. In tale contesto fattuale, la Corte EDU nella sentenza del 12 gennaio 2021 aveva dichiarato, con 5 voti contro 2, che non vi era stata violazione dell'articolo 8 della CEDU in quanto la pubblicazione dei dati personali in questione era giustificata dalla finalità dissuasiva sottesa al provvedimento. Il 31 maggio 2021 la stessa Corte EDU ha tuttavia accolto la richiesta del ricorrente di deferire il caso alla Grande Sezione. Il 14 marzo, la Grande Sezione della Corte EDU ha ribaltato la sentenza del 12 gennaio 2021 ritenendo invece che vi fosse stata violazione dell'articolo 8 della CEDU. La sentenza prende atto del fatto che i dati pubblicati sul ricorrente riguardavano chiaramente la sua vita privata e che la pubblicazione è avvenuta in modo automatico e senza eccezioni. La disposizione legislazione in esame prevede infatti che nel caso

in cui un debito tributario sia rimasto non eseguito da 180 giorni continuativi, sia obbligatorio e sistematico che il debitore identificato con il proprio nome e domicilio venga incluso nell'elenco pubblicato sul sito web dell'Agenzia delle Entrate. Questo comporta che chiunque con accesso a Internet possa avere accesso illimitato alle informazioni su ciascun debitore d'imposta della lista, con il rischio di ripubblicazione come conseguenza naturale, probabile e prevedibile. Questa limitazione del rispetto della vita privata non è risultata giustificabile, per la maggioranza dei giudici della Corte EDU. (https://hudoc.echr.coe.int/eng#%7B%22itemid%22:[%22001-223675%22]%7D)

La Corte di giustizia chiarisce quando l'elettricità utilizzata per la produzione di altra elettricità sia esente dalla tassazione sui prodotti energetici

Il 9 marzo 2023, la Corte di giustizia ha pronunciato la sua sentenza nella causa pregiudiziale *RWE Power*, C-571/21 in materia di accise sull' energia, stabilendo che solo l'energia elettrica utilizzata in produzioni di energia che sono indispensabili e contribuiscono direttamente al processo tecnologico di generazione di altra elettricità possono essere esentate da tassazione dui prodotti energetici (direttiva 2003/96 del Consiglio). Il rinvio pregiudiziale è stato proposto dal Finanzgericht Düsseldorf (Tribunale tributario di Düsseldorf) nell'ambito di una controversia tra la RWE Power e l'ufficio doganale principale di Duisburg, avente ad oggetto il rifiuto di quest'ultimo di concedere l'esenzione dall'imposta l'elettricità utilizzata da RWE Power nel 2003 e nel 2004 per le sue attività minerarie a cielo aperto e nelle sue centrali elettriche per la generazione di energia. Il giudice del rinvio ha posto alla Corte due questioni. In primo luogo, se l'esenzione fosse applicabile alle miniere a cielo aperto dove veniva praticata l'estrazione di prodotti energetici e nelle centrali termoelettriche per migliorarne l'alimentazione. In secondo luogo, il giudice del rinvio ha chiesto alla Corte di chiarire se anche l'utilizzo dell'energia elettrica per il funzionamento degli impianti di stoccaggio e dei mezzi di trasporto necessari per il funzionamento continuativo delle centrali elettriche possa essere esente da accisa. Nella sua sentenza, la Corte ha dichiarato che l'esenzione prevista dalla direttiva 2003/96 non copre l'elettricità utilizzata per l'estrazione di un prodotto energetico in una miniera, poiché tale energia (nella specie l'elettricità) è utilizzata per la produzione di un prodotto energetico, e non direttamente nel processo di generazione di elettricità. Tuttavia, la Corte ha sottolineato che può essere esentato l'ulteriore utilizzo di questo prodotto energetico nelle centrali elettriche ai fini della produzione di elettricità, purché tale utilizzo sia indispensabile e contribuisca direttamente alla generazione di elettricità. Inoltre, la Corte ha stabilito che l'esenzione può anche riguardare l'energia elettrica utilizzata per il funzionamento degli impianti di stoccaggio di un prodotto energetico e dei mezzi di trasporto per la fornitura del prodotto, qualora tali operazioni avvengano all'interno di centrali di produzione dell'energia elettrica e siano indispensabili e contribuiscano al mantenimento della capacità di produzione di energia elettrica, perché ad esempio necessarie ad evitare interruzioni dell'erogazione di elettricità. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=271071&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=1065997)



Imposta britannica sulle plusvalenze sulle vendite transfrontaliere di attivi infragruppo non contraria al diritto dell'UE. Il 18 febbraio 2023, la Corte di giustizia sta ha reso un'importante sentenza nella causa pregiudiziale *Gallaher Limited contro Her Majesty's Revenue and Customs*, C-707/20 in materia di imposizione di plusvalenze realizzate dalla cessione di beni aziendali. La società Gallaher Limited (GL) effettuava due operazioni riguardanti la cessione di attività a società collegate del gruppo Japan Tobacco. La stessa GL residente ai fini fiscali nel Regno Unito, effettuava nel 2011 una prima transazione riguardante diritti di proprietà intellettuale relativi a marchi per la produzione e commercializzazione di prodotti del tabacco a una consorella in Svizzera e una seconda transazione riguardante la cessione di azioni di una controllata alla sua controllante intermedia società nei Paesi Bassi, nel 2014. Le transazioni non si qualificavano per le norme britanniche sui trasferimenti esenti infragruppo, e per questo GL considerava la differenza di trattamento violasse la libertà di stabilimento (articolo 49 TFUE) e/o della libera circolazione dei capitali (articoli 63 e 64 TFUE). La Corte ha stabilito, in primo luogo, che l'articolo 63 TFUE non si applica alla legislazione che riguarda i gruppi di società. In secondo luogo, la Corte ha detto che l'articolo 49 TFUE non si oppone all'imposizione di una cessione di beni a una società affiliata che è fiscalmente residente in un paese terzo e non ha una stabile organizzazione nello Stato membro in questione in quanto l'imposizione , si giustifica per la necessità di mantenere un'equilibrata ripartizione dei poteri impositivi tra gli Stati membri per affermare che un regime di gruppo come quello in questione costituisce una lecita restrizione al diritto di libertà di stabilimento, e quindi che può fare la differenza tra una situazione nazionale e una situazione transfrontaliera. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=270511&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=2370726)

Il Tribunale respinge il ricorso contro la decisione della Commissione sulla determinazione dell'origine non preferenziale proposta dalla Harley Davidson

L'1 marzo 2023, il Tribunale ha reso un'importante sentenza nella causa *Harley-Davidson Europe e Neovia Logistics Services International/Commissione*, T-324/21, respingendo un ricorso di annullamento avverso una decisione della Commissione europea (2021/563) relativa alla validità di talune decisioni relative alle informazioni doganali sull'origine (IVO). La sentenza ha confermato la validità della decisione della Commissione oggetto di ricorso che aveva stabilito che diverse decisioni IVO riguardanti i ricorrenti contenevano una determinazione dell'origine non preferenziale delle merci incompatibile con l'articolo 60, paragrafo 2, del codice doganale dell'Unione (CDU). Questo in quanto, secondo la Commissione, tali decisioni IVO erano state ottenute abusivamente in quanto incompatibili con le norme sull'acquisizione dell'origine previste da tale disposizione, in quanto le operazioni di trasformazione o lavorazione effettuate nell'ultimo paese di produzione (la Thailandia) non erano economicamente giustificate. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=270786&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2704550)

La Corte di giustizia chiarisce la soggettività IVA delle prestazioni di servizi digitali

Il 28 febbraio 2023, la Corte di Giustizia ha reso un'importante sentenza nella causa pregiudiziale *Fenix International Limited/Commissioners for HMRC*, C-695/20sulla tassazione dei servizi digitali stabilendo che un intermediario di servizi online il quale interfaccia dei prestatori di servizi coi loro clienti è debitore dell'IVA applicabile sull'intero valore delle transazioni offerte dai prestatori e non sulla sola provvigione da lui trattenuta o a lui versata. La Corte, pronunciando la sua sentenza in Grande Sezione, ha confermato la validità di una disposizione del regolamento di esecuzione del Consiglio 282/2011 (il regolamento IVA di esecuzione) che reca disposizioni di attuazione della direttiva 2006/112/CE relativa al sistema comune di imposta sul valore aggiunto (la direttiva IVA), in quanto non confliggente con la Direttiva IVA, e neppure eccede le competenze di esecuzione attribuite dalla stessa direttiva. La Corte ha in sostanza statuito che un soggetto passivo che gestisce una piattaforma di social network, avente il potere di autorizzare e fatturare i servizi, nonché di definire gli elementi essenziali di questi, deve essere considerato il prestatore di tali servizi ai fini

della soggettività IVA. Questo perché, tenuto conto dell'evoluzione del sistema IVA e al fine di garantire un'applicazione uniforme nell'Unione di tale norma, il Consiglio aveva competenza ad indicare, nel regolamento IVA di esecuzione, che il soggetto passivo che interviene in una prestazione di servizi forniti tramite un'interfaccia o un portale quale un mercato delle applicazioni si presume che agisca in nome proprio ma per conto del prestatore di tali servizi. In quel senso, quando si tratta di prestare servizi per via elettronica tramite una rete o una piattaforma di telecomunicazioni, come un mercato di applicazioni, si presume che il soggetto passivo coinvolto nella prestazione agisca per conto del prestatore di servizi ed è pertanto considerato esso stesso come prestatore dei servizi intermediati quando ha il potere di addebitare oneri e imporre condizioni al cliente. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=270747&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=2161002)

L'Avvocato Generale della Corte di giustizia considera l'esenzione concessa alle retribuzioni per i progetti associati agli aiuti allo sviluppo finanziati con risorse nazionali non può essere trattata diversamente da quelli finanziati con risorse del Fondo europeo di sviluppo (FES)

L'8 febbraio 2023, l'Avvocato generale della Corte di giustizia (AG) Medina ha reso le proprie conclusioni nella causa pregiudiziale *Finanzamt G (Projets d'aide au développement)*, C-15/22, concernente la compatibilità con il diritto dell'Unione di una prassi amministrativa nazionale di esenzione del salario corrisposto per un'attività nel campo dell'assistenza allo sviluppo dalla tassazione, a condizione che l'attività sia finanziata con fondi delle autorità tedesche, mentre lo stipendio corrisposto per tale attività finanziata con fondi dell'UE è soggetto a tassazione. Il caso in questione riguarda un individuo che ha lavorato come project manager per un'associazione di assistenza allo sviluppo in Africa dal 2009 al 2012 con un contratto a tempo determinato. La residenza principale e il centro degli interessi del ricorrente era in Germania. Poiché il progetto non è stato finanziato dalla Germania, ma piuttosto dal Fondo europeo di sviluppo, l'ufficio delle imposte convenuto ha addebitato lo stipendio del ricorrente all'imposta sul reddito. Poiché la sua opposizione e il suo ricorso dinanzi al Finanzgericht (Tribunale tributario, Germania) non hanno avuto successo, la ricorrente ha chiesto l'esenzione dall'imposta sul reddito del suo stipendio mediante ricorso in cassazione dinanzi al Bundesfinanzhof (Germania). Il giudice del rinvio aveva chiesto alla Corte di giustizia se l'articolo 4, paragrafo 3, e l'articolo 208 TUE, in combinato disposto con l'articolo 210 TFUE, ostino a una prassi nazionale di non concedere esenzioni fiscali nei casi in cui un progetto di cooperazione allo sviluppo è finanziato dal Fondo europeo di sviluppo, mentre gli stipendi guadagnati dai lavoratori in rapporti di lavoro relativi all'assistenza ufficiale tedesca allo sviluppo che sono finanziati da un ministero federale responsabile per la cooperazione allo sviluppo o da un'associazione privata di assistenza allo sviluppo di proprietà statale per almeno il 75% possono essere esenti da tassazione a determinate condizioni. Ad avviso dell'AG Medina, l'articolo 63 TFUE deve essere interpretato nel senso che osta all'applicazione di una norma tributaria di uno Stato membro che prevede l'esenzione dall'imposta sul reddito per la retribuzione percepita da un dipendente addetto ad attività di aiuto allo sviluppo solo qualora tale attività è finanziato per almeno il 75% dalle risorse del bilancio tedesco, ma che ha l'effetto di privare un dipendente del beneficio di tale esenzione qualora sia assegnato a un'attività di tale natura finanziata nella stessa misura da uno dei Fondi europei di sviluppo. In subordine, l'AG propone che l'articolo 4, paragrafo 4, l'articolo 208, paragrafo 1, e l'articolo 210, paragrafo 1, TFUE, in combinato disposto con il principio di leale cooperazione sancito dall'articolo 4, paragrafo 3, TUE, debbano essere interpretati nel senso che ostano l'applicazione di una norma fiscale di uno Stato membro che priva un dipendente del beneficio di un'esenzione fiscale in quanto tale dipendente è destinato ad attività di aiuto allo sviluppo finanziate dai FES. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=270335&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=664)

L'Avvocato generale presso la Corte di giustizia si pronuncia sulla compatibilità delle diverse forme di calcolo dell'imposta di successione con la libera circolazione dei capitali

Il 9 febbraio 2023, l'Avvocato generale della Corte di giustizia (AG) Collins ha reso le proprie conclusioni nella causa *BA/Finanziamt X*, C-670/21 sulla compatibilità della legislazione nazionale tedesca in materia di riscossione dell'imposta di successione con le disposizioni del TFUE sulla libera circolazione dei capitali. La normativa nazionale in esame prevede che i beni immobili ubicati in un paese terzo facenti parte del patrimonio personale del de cujus e dati in locazione ad uso abitativo debbano essere presi in considerazione per il loro intero valore ai fini del calcolo dell'imposta di successione. Al contrario, lo

stesso tipo di bene immobile se si trova in uno Stato dell'UE o dello Spazio Economico Europeo (SEE) ed è locato a scopo abitativo, deve essere preso in considerazione solo per il 90% del suo valore nel calcolo dell'imposta di successione. Il giudice del rinvio chiedeva specificamente se tale distinzione fosse vietata dagli articoli 63(1), 64 e 65 TFUE. Secondo AG Collins, l'articolo 63(1) TFUE non osta a leggi nazionali che prevedono un trattamento più favorevole per il calcolo dell'imposta di successione sugli immobili locati a scopo residenziale all'interno di uno Stato membro o di uno Stato dello Spazio economico europeo rispetto agli immobili utilizzato per lo stesso scopo in un paese terzo. La ragione della differenza di trattamento è di incoraggiare la disponibilità di alloggi in affitto a prezzi accessibili nell'UE e nello SEE. Secondo l'AG, una tale distinzione è da considerarsi giustificata da ragioni di interesse generale e purché la legislazione in questione sia idonea a raggiungere l'obiettivo prefissato e non esistano metodi alternativi meno restrittivi ma ugualmente efficaci. Separatamente, l'AG Collins ha anche proposto alla Corte di giustizia di dichiarare che l'articolo 63(1) TFUE osta invece ad una normativa nazionale che, ai fini del calcolo dell'imposta di successione, tratti il valore di un immobile locato per uso residenziale in un altro Stato membro o in un Stato dello SEE in modo più favorevole rispetto ai beni situati in un paese terzo destinati allo stesso uso al fine di garantire l'efficacia della vigilanza fiscale, laddove esista un quadro giuridico equivalente ai fini dello scambio di informazioni pertinenti tra le autorità fiscali competenti. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=270334&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=3061870)

Novità Concorrenza e Aiuti di Stato

La Commissione abbandona metà del suo caso App Store

Il 28 febbraio 2023, la Commissione ha inviato ad Apple una nuova comunicazione degli addebiti (CA) chiarendo le sue preoccupazioni sulle regole dell'App Store per i fornitori di streaming musicale. Più che un chiarimento, o un ampliamento della precedente CA, la nuova CA ha eliminato una delle due obiezioni. Per memoria, la Commissione aveva inviato ad Apple una CA nell'aprile 2021, delineando la sua convinzione preliminare secondo la quale Apple aveva abusato della sua posizione dominante nella distribuzione di app, in primo luogo, imponendo il proprio meccanismo di pagamento in-app agli sviluppatori di app di streaming musicale ("obbligo IAP"), e in secondo luogo, limitando la capacità degli sviluppatori di app di informare gli utenti sui metodi di abbonamento alternativi ("obbligo anti-steering"). La Commissione ha ritirato la prima delle due obiezioni originariamente formulate. La Commissione non ha chiarito la ragione ma è possibile ritenere che la Commissione abbia preso atto della difficoltà di provare che l'obbli-

go IAP abbia prodotto sufficienti effetti anticoncorrenziali: le app di streaming musicale hanno margini veramente ristretti dato che devono la maggior parte delle loro entrate (diciamo, il 70%) alle etichette discografiche e quindi potrebbe semplicemente non esserci un margine del 30% per pagare la quota IAP. La conclusione sarebbe che l'incidenza dell'obbligo IAP sarebbe troppo ridotta per produrre effetti significativi. Una tesi alquanto discutibile e forse un'occasione persa da parte dell'esecutivo UE di chiarire il carattere anticoncorrenziale di quella che viene da alcuni percepita come una tassa sugli abbonamenti on line attraverso l'App Store. (https://ec.europa.eu/commission/presscorner/detail/it/ip_23_1217)

Orientamenti sulla modifica dei piani PNRR nel quadro di REPowerEU pubblicate in GU

La Gazzetta Ufficiale UE del 3 marzo reca la pubblicazione della Comunicazione della Commissione che orientamenti sugli adattamenti dei piani nazionali di ripresa e resilienza di cui alla facility creata dal regolamento (UE) 2021/241 (il regolamento RRF) nel quadro di REPowerEU. A seguito della proposta della Commissione volta a rafforzare i piani nazionali per la ripresa e la resilienza (PNRR) in risposta alle sfide create dall'aggressione militare russa all'Ucraina e dalla crisi COVID-19, è stato modificato il regolamento RRF. La modifica, nota come REPowerEU, mira a migliorare la sicurezza energetica, ridurre la dipendenza sui combustibili fossili e rafforzare la competitività dell'industria dell'UE. Secondo gli orientamenti, gli Stati membri sono incoraggiati a modificare i loro PNRR presentando una versione consolidata dei loro piani iniziali per riflettere le modifiche apportate durante la fase di valutazione coerentemente con le rispettive decisioni di approvazione date dal Consiglio. Gli Stati membri dovrebbero presentare piani modificati come addendum ai loro piani consolidati utilizzando un apposito modello dedicato. Eventuali modifiche richiederanno una nuova valutazione da parte della Commissione e sarà richiesta una valutazione positiva del piano. Gli Stati membri sono fortemente incoraggiati a presentare i PNRR modificati entro aprile 2023 per rispettare il termine legale del 31 agosto 2023 per la presentazione delle relative richieste di erogazione dei fondi. Una eventuale presentazione dopo agosto 2023 rischierebbe di far a perdere il 30% dell'assegnazione della sovvenzione e l'accesso ai prestiti dal regolamento RRF. Gli orientamenti sottolineano inoltre che il regolamento REPowerEU introduce una nuova categoria di sostegno finanziario a fondo perduto. Queste risorse possono essere utilizzate solo per finanziare le riforme e gli investimenti

inclusi nel capitolo REPowerEU di cui all'articolo 21 quater, paragrafo 1, del regolamento RRF. Per quanto riguarda gli aiuti di Stato, la Guida afferma che le norme sugli aiuti di Stato si applicano integralmente agli investimenti aggiuntivi o modificati. È responsabilità di ciascuno Stato membro garantire che tali riforme e investimenti rispettino le norme dell'UE in materia di aiuti di Stato, in particolare la proporzionalità, e seguano le procedure applicabili in materia. (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2023:080:FULL&from=EN)

La Commissione pubblica gli Orientamenti che aiutano le piattaforme online e i motori di ricerca a comunicare il numero dei rispettivi utenti quali soggetti obbligati ai sensi del regolamento Digital Services Act (DSA)

Il 1° febbraio 2023, la Commissione ha pubblicato orientamenti non vincolanti per le piattaforme online e i motori di ricerca sull'obbligo di segnalare i numeri degli utenti nell'UE ai sensi del Digital Services Act (DSA). La guida ha lo scopo di aiutare queste società a rispettare l'obbligo di rendicontazione entro il 17 febbraio 2023 e successivamente su base semestrale. Per memoria, ai sensi del regolamento DSA se il numero di utenti pubblicati di una piattaforma o di un motore di ricerca raggiunge oltre il 10% della popolazione dell'UE (45 milioni di utenti), la Commissione può designarli rispettivamente come piattaforme online molto grandi o come motori di ricerca online molto grandi. Ciò farebbe scattare ulteriori obblighi come lo svolgimento di una valutazione del rischio e l'adozione di misure per mitigare tali rischi. Il DSA, entrato in vigore nel novembre 2022, mira a creare un ambiente online più sicuro e responsabile ponendo le piattaforme digitali sotto un nuovo quadro di trasparenza e responsabilità. (https://ec.europa.eu/commission/presscorner/detail/it/mex_23_523)

Giurisprudenza Concorrenza e Aiuti di Stato

L'Avvocato generale Szpunar si pronuncia sulla compatibilità della norma UEFA che richiede un numero minimo di giocatori cresciuti in casa per partecipare alle partite di calcio col mercato unico

Il 9 marzo 2023, l'Avvocato generale (AG) della Corte di Giustizia Szpunar ha reso le sue conclusioni nella causa pregiudiziale *Royal Antwerp Football Club*, C-680/21, relativa alla compatibilità del regolamento UEFA sui giocatori con le regole UE in materia di concorrenza e di libera circolazione dei lavoratori. La UEFA è un'associazione la cui missione è regolamentare e organizzare il calcio in Europa e i cui membri sono varie federazioni calcistiche nazionali europee, tra le quali la belga Union royale belge des sociétés de football association (URBSFA) la parte interessata nella causa nazionale che ha dato luogo al rinvio pregiudiziale. Nel 2005, il Comitato Esecutivo UEFA adottava una regola che impone ai club che partecipano alle competizioni interclub della UEFA di avere un massimo di 25 giocatori per ciascuna lista, che deve includere un numero minimo di giocatori del vivaio ("GDV") locale da ammettere nelle partite. La norma è stata approvata dalle 52 federazioni affiliate alla UEFA. Un calciatore con doppia cittadinanza israeliana e belga aveva adito il tribunale arbitrale dello sport belga sostenendo che la norma GDV violava i diritti alla libera circolazione (articolo 45 TFUE) e il divieto di accordi anticoncorrenziali (articolo 101 TFUE). Il Tribunal de première instance francophone de Bruxelles (Belgio) investito del ricorso contro l'arbitrato, ha chiesto alla Corte di giustizia di pronunciarsi sulla questione se gli art.li 45 e 101 TFUE ostino all'attuazione della norma GDV da parte dell'UEFA o dei suoi membri. Nelle conclusioni in rassegna, l'AG Szpunar ha osservato che le norme GDV possono discriminare indirettamente i cittadini di altri Stati membri dell'UE in quanto, sebbene neutrali nella formulazione, pongono i giocatori locali in vantaggio rispetto ai giocatori di altri paesi. Tuttavia, l'AG ha riconosciuto che una tale discriminazione potenziale è da giustificarsi in relazione all'obiettivo di formare e reclutare giovani calciatori, apprendistato che avviene naturalmente a livello locale. L'AG suggerisce inve-

ce alla Corte di dubitar della coerenza delle disposizioni impugnate e della loro efficacia nel raggiungere l'obiettivo della formazione dei giovani calciatori, che dovrebbe includere anche i giovani giocatori allenati da altri club. L'AG Szpunar sugerisce che il requisito di includere un numero predefinito di giocatori cresciuti in casa in un elenco pertinente è quindi giustificabile, ma l'estensione della definizione di GDV ai giocatori al di fuori del programma di formazione di uno specifico club non è coerente e non idonea a raggiungere l'obiettivo di formare giovani calciatori. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=271085&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=1220845)

La Corte annulla tre decisioni della Commissione che dispongono altrettante ispezioni ad imprese sospettate di partecipazione in cartelli, in quanto viziate dall'inosservanza dell'obbligo di registrazione delle audizioni delle persone interessate

Il 9 marzo 2023, la Corte di giustizia ha reso tre interessanti sentenze nelle cause *Les Mousquetaires e ITM Entreprises/Commissione*, C-682/20 P, *Casino, Guichard-Perrachon e Achats Marchandises Casino/Commissione*, C-690/20 P, e *Intermarché Casino Achats/Commissione*, C-693/20 P, relative a tre ricorsi di annullamento avverso altrettante sentenze del Tribunale che avevano parzialmente respinto i ricorsi delle ricorrenti diretti all'annullamento di tre decisioni della Commissione che ordinavano alle società di sottoporsi a ispezioni in quanto sospettate di partecipazione in intese vietate dall'art. 101 TFEU, ai sensi dell'art. 20(4) del regolamento 1/2003. Avendo ricevuto informazioni relative agli scambi di informazioni tra Casino e altre imprese, tra cui Les Mousquetaires e ITM Entreprises (le imprese ricorrenti), la Commissione aveva adottato tre decisioni che ordinavano alle ricorrenti di sottoporsi a ispezione da parte della Commissione, nei casi AT.40466 e AT.40467, relativamente alla loro possibile partecipazione a intese o pratiche concordate contrarie all'articolo 101 TFUE. Le ricorrenti avevano impugnato le decisioni, ed il Tribunale aveva respinto le loro richieste. Nelle sentenze in rassegna, la Corte ha ribaltato le sentenze di primo grado annullando parzialmente le decisioni controverse in quanto si erano basate su informazioni ottenute dalla Commissione mediante audizioni che avrebbero dovuto essere formalmente verbalizzate attraverso registrazione dal momento che queste, in considerazione del contesto nel quale erano state eseguite, miravano a raccogliere informazioni relative all'oggetto delle indagini in relazione alle quali sarebbero state disposte le ispezioni, conformemente all'art. 19 del regolamento 1/2003. In primo luogo, la Corte ha stabilito che la Commissione è tenuta a registrare qualsiasi intervista condotta allo scopo di raccogliere informazioni relative all'oggetto di un'indagine. Questo requisito si applica indipendentemente dal fatto che un'audizione sia stata condotta prima o dopo l'apertura formale di un'indagine e la Commissione può verbalizzare attraverso registrazione l'audizione in qualsiasi forma, anche orale, per garantire l'efficacia e la rapidità dell'indagine. In secondo luogo, la Corte ha rilevato che il Tribunale aveva commesso un errore di diritto dichiarando che l'obbligo di registrazione non si applicava ai colloqui svolti coi fornitori delle imprese in questione, prima dell'avvio di un'indagine formale. Il Tribunale avrebbe dovuto determinare invece se tali audizioni fossero state volte a raccogliere informazioni relative all'oggetto di un'indagine, in base al loro contenuto e contesto, e concludere che dovevano essere verbalizzate attraverso registrazione. Di conseguenza, la Corte ha annullato in parte le citate sentenze del Tribunale, e con esse le decisioni di ispezione nella misura in cui non erano suffragate da indizi sufficientemente gravi. (https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-03/cp230044it.pdf)

Conclusioni dell'Avvocato Generale della Corte sulla qualificazione di una clausola di non concorrenza come restrizione della concorrenza per oggetto o per effetto e sul concetto di concorrenza potenziale

Il 2 marzo 2023, l'Avvocato Generale (AG) Rantos della Corte di giustizia ha reso le sue conclusioni nella causa pregiudiziale *Autoridade da Concorrência e EDP*, C-331/21, sulla questione se una clausola di non concorrenza in un accordo di partenariato tra imprese operanti in diversi mercati del prodotto possa costituire un accordo con oggetto anticoncorrenziale ai sensi dell'articolo 101 TFUE e a quali condizioni. Nel caso in esame, l'Autoridade da Concorrência (Autorità garante della concorrenza, Portogallo) ha accusato i ricorrenti (un rivenditore di prodotti alimentari e un fornitore di energia elettrica) di aver commesso una violazione del diritto della concorrenza consistente nel reato classificato e punito ai sensi dell'articolo 9, paragrafo 1 c) e 68, n. 1, lett. a), della Lei da Concorrência (legge sulla concorrenza), quest'ultimo articolo essendo basato sull'articolo 101 TFUE e riproducendolo praticamente. Tuttavia, al momento della conclusione dell'accordo, i ricorrenti non erano concorrenti in alcun mercato. L'Autorità Garante della Concorrenza e del Mercato riteneva comunque che, come nell'ambito di un accordo di associazione, le ricorrenti avessero stipulato un patto di non concorrenza costituente un accordo restrittivo della concorrenza per oggetto, in vigore dal 5 gennaio 2012. Il Tribunal da Concorrência, Regulação e Supervisão de Santarém (Portogallo) confermava con sentenza tale addebito. In tale contesto, il giudice del rinvio dubitava che l'accordo di partnership e la clausola di non concorrenza potessero avere un impatto negativo sulla concorrenza nei mercati rilevanti. La Corte di giustizia è stata interrogata su ben undici questioni in materia. Con le conclusioni in rassegna, l'AG ha ritenuto che le questioni pregiudiziali possano essere raggruppate attorno alle seguenti questioni, vale a dire: i) quale sia il concetto di «concorrenza potenziale», e più specificamente se e a quali condizioni le imprese operanti su mercati del prodotto distinti possano essere considerate potenziali concorrenti ai fini dell'articolo 101 TFUE; (ii) quale sia la qualificazione giuridica di un accordo di partenariato tra imprese finalizzato alla promozione incrociata delle rispettive attività; (iii) quali siano le condizioni alle quali una restrizione della concorrenza può essere considerata accessoria ad un accordo il cui obiettivo non è anticoncorrenziale; (iv) e se una tale restrizione possa essere qualificata come restrizione per oggetto ovvero per effetto. In primo luogo, AG Rantos ha consigliato alla Corte di interpretare l'articolo 101, paragrafo 1, TFUE nel senso che un rivenditore al dettaglio vincolato da un accordo di associazione con un fornitore di energia elettrica, il cui scopo è promuovere, mediante un sistema di vendite, le rispettive attività e che includa una clausola di non concorrenza, può essere considerato un potenziale concorrente sul mercato della fornitura di energia elettrica, anche se al momento della conclusione di tale accordo non era attivo su tale mercato se, è dimostrato che a quel momento esistevano possibilità reali e concrete per quel dettagliante di entrare in quel mercato. Al fine di verificare se tale impresa possa essere considerata un potenziale concorrente e quindi rappresentare un vincolo concorrenziale per il fornitore di energia elettrica, possono essere rilevanti elementi relativi, tra l'altro, l'intenzione del rivenditore di entrare il mercato della fornitura di energia elettrica, come prova della sua capacità di entrare in tale mercato e le attività sul mercato a monte della produzione di energia elettrica, nella misura in cui tali attività siano idonee a conferire reali e concreti vantaggi al dettagliante in vista di un'eventuale integrazione nel mercato della fornitura di energia elettrica. In secondo luogo, secondo l'AG, la nozione di accordo verticale ha come oggetto è quello di promuovere, mediante un sistema di vendita abbinata le attività di imprese operanti a differenti livelli della filiera mercato, indipendentemente dal fatto che tali imprese debbano essere considerate concorrenti effettive o potenziali, poiché si presume che tali imprese agiscano, ai fini dell'accordo di cooperazione, allo stesso livello della filiera economica. Tanto premesso, l'AG Rantos ha suggerito che l'articolo 101, paragrafo 1, TFUE possa essere interpretato nel senso che una clausola di non concorrenza concordata tra le parti nell'ambito di un accordo come quello in questione, non si sottrae al divieto di intese, a meno che non sia dimostrato che tale clausola è oggettivamente necessaria per l'attuazione del partenariato e proporzionata agli obiettivi da esso perseguiti. In conclusione,

l'AG ha consigliato alla Corte di dichiarare che una clausola di non concorrenza, come quella contenuta nell'accordo di società di cui trattasi, purché stipulata tra imprese considerate potenziali concorrenti, deve considerarsi un accordo di ripartizione del mercato che costituisce una restrizione della concorrenza per oggetto, senza che sia necessario dimostrare effetti dannosi concreti, a meno che tale clausola non possa essere considerata una restrizione accessoria l'accordo principale o le parti fanno valere effetti favorevoli sulla concorrenza. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=270837&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=371914)

La Corte di giustizia si pronuncia sulla debenza delle spese e la stima dell'ammontare del danno nei casi di risarcimento del danno causato da violazione delle regole di concorrenza

Il 16 febbraio 2023, la Corte di giustizia ha reso un'importante sentenza nella causa pregiudiziale *Tráficos Manuel Ferrer*, C-312/21, chiarendo la ripartizione dei costi nelle azioni civili di risarcimento del danno causato da violazione delle regole di concorrenza e come stimare il danno senza rendere la quantificazione praticamente impossibile o eccessivamente difficile. La domanda di pronuncia pregiudiziale trae origine dall'azione per risarcimento danni antitrust promossa da un acquirente di autocarri nei confronti di Daimler AG. L'azione civile faceva seguito alla decisione della Commissione del 2016 che sanzionava alcuni produttori di autocarri per aver partecipato a un cartello (caso AT.39824). Ai fini della presente causa, il giudice del rinvio ha evidenziato due circostanze: (i) l'attore aveva presentato una perizia di quantificazione del danno, che l'imputato contestava con propria perizia; e (ii) sebbene la ricorrente avesse acquistato autocarri da altri partecipanti al cartello, essa ha intentato l'azione solo contro Daimler AG. In questo contesto, la Corte è stata chiamata a chiarire (i) se fosse ragionevole che un attore che chiede il risarcimento dei danni antitrust sia tenuto a pagare la metà delle spese del procedimento in cui vinca in parte; e (ii) se un giudice nazionale possa stimare l'ammontare del danno causato dal cartello qualora i ricorrenti abbiano avuto accesso ai dati su cui si basava la perizia della parte convenuta relativa al danno e qualora la richiesta di risarcimento riguardi anche beni che la ricorrente non ha acquistato dalla convenuta ma da altri partecipanti al cartello. Quanto alla prima questione, la Corte ha stabilito che una norma di procedura civile nazionale che ripartisca equamente le spese tra le parti, salvo in caso di condotta illecita, non viola il diritto dell'UE (la direttiva 2014/104 copre la responsabilità extracontrattuale derivante da danno da comportamento anticoncorrenziale) in quanto non rende impossibile alla vittima il pieno risarcimento del danno causato da comportamenti anticoncorrenziali. In tal senso, la Corte ha osservato che la direttiva 2014/104 tenta di bilanciare gli interessi delle parti nell'azione per danni, consentendo alla vittima di utilizzare gli strumenti disponibili per correggere eventuali squilibri nei rapporti di forza. Se la vittima del danno è pure parzialmente soccombente, è ragionevole che essa sopporti le proprie spese e parte delle spese comuni, purché l'origine di tali spese sia a lei imputabile. Per quanto riguarda la seconda questione, la Corte ha anche evidenziato che l'onere della stima del danno ai sensi della direttiva 2014/104 è a carico della parte ricorrente che ha in principio una parità di strumenti di prova rispetto alla convenuta nel processo civile, ma non deve risultare in un'impossibilità di quantificarlo. Ciò può verificarsi quando la richiesta di divulgazione delle prove prevista dalla direttiva sia rigettata facendo sorgere difficoltà estreme, anche quando le parti si trovano su un piano di parità per quanto riguarda le informazioni disponibili. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=270505&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=119236)

Il confine tra omissione ed evasione contributiva

di Mauro Petrassi

Studio Legale PROIA & PARTNERS

Il regime sanzionatorio applicabile in caso di violazione della disciplina sul versamento dei contributi e dei premi dovuti alle Gestioni previdenziali ed assistenziali è regolato dall'art. 116, commi 8 e 9, Legge 23 dicembre 2000, n. 388.

La previsione normativa distingue le ipotesi di omissione contributiva da quelle di evasione contributiva, prevedendo sanzioni graduate a seconda che la condotta *contra legem* rientri nell'una o nell'altra categoria. Senonché, sull'esatta portata del perimetro applicativo delle fattispecie dell'omissione e dell'evasione contributiva, si è prodotto nel corso degli anni un copioso contenzioso, attraverso il quale i giudici di merito e di legittimità sono ripetutamente intervenuti, con l'intento di risolvere alcune delle questioni giuridiche emerse a seguito dell'introduzione della disciplina di legge, sulle quali, tra l'altro, si è soffermata, più volte, anche l'INPS.

Il criterio distintivo individuato dalla legge

L'art. 116 Legge n. 388 del 2000 individua il regime sanzionatorio per i soggetti che, entro i termini previsti, non provvedano, anche solo parzialmente, al versamento dei contributi o premi dovuti alle gestioni previdenziali e assistenziali.

In particolare, il comportamento sanzionato concerne le ipotesi di:

- omissione contributiva: qualificata come "*mancato o ritardato pagamento di contributi o premi, il cui ammontare è rilevabile dalle denunce e/o registrazioni obbligatorie*" (art. 116, comma 8, lett. a);
- evasione contributiva: "*registrazioni o denunce obbligatorie omesse o non conformi al vero, cioè nel caso in cui il datore di lavoro, con l'intenzione specifica di non versare i contributi o premi, occulta rapporti di lavoro in essere ovvero le retribuzioni erogate*" (art. 116, comma 8, lett. b).

A seconda della tipologia di violazione posta in essere dal datore di lavoro[1] è prevista una graduazione sanzionatoria differente. Più precisamente:

- in caso di omissione contributiva è imposto il pagamento di una sanzione civile, in ragione d'anno, pari al tasso ufficiale di riferimento maggiorato di 5,5 punti; la sanzione civile non può essere superiore al 40% dell'importo dei contributi o premi non corrisposti entro la scadenza di legge (art. 116, comma 8, lett. a);
- in caso di evasione contributiva consegue il pagamento di una sanzione civile, in ragione d'anno, pari al 30%; la sanzione civile non può essere superiore al 60% dell'importo dei contributi o premi non corrisposti entro la scadenza di legge. Qualora la denuncia della situazione debitoria sia effettuata spontaneamente prima di contestazioni o richieste da parte degli enti impositori e comunque entro dodici mesi dal termine stabilito per il pagamento dei contributi o premi e sempreché il versamento dei contributi o premi sia effettuato entro trenta giorni dalla denuncia stessa (cd. ravvedimento operoso), si è tenuti al pagamento di una sanzione civile, in ragione d'anno, pari al tasso ufficiale di riferimento maggiorato di 5,5 punti; in tal caso la sanzione civile non può essere superiore al 40% dell'importo dei contributi o premi non corrisposti entro la scadenza di legge (art. 116, comma 8, lett. b).

È inoltre previsto che:

- nei casi di mancato o ritardato pagamento di contributi o premi derivanti da oggettive incertezze connesse a contrastanti orientamenti giurisprudenziali o amministrativi sulla ricorrenza dell'obbligo contributivo, successivamente riconosciuto in sede giudiziale o amministrativa, sempreché il versamento dei contributi o premi sia effettuato entro il termine fissato dagli enti impositori, si applica una sanzione civile, in ragione d'anno, pari al tasso ufficiale di riferimento maggiorato

1 *Le ipotesi di cui alle lettere a) e b) trovano applicazione, in via generale, nei confronti sia dei soggetti che rivestono la qualifica di datori di lavoro e/o committenti che dei lavoratori autonomi in relazione alla diversa tipologia degli adempimenti previsti per ciascuna Gestione previdenziale.*

di 5,5 punti; tale sanzione non può essere superiore al 40% dell'importo dei contributi o premi non corrisposti entro la scadenza di legge (art. 116 comma 10);
• fermo restando l'integrale pagamento dei contributi e dei premi dovuti, è possibile la riduzione delle sanzioni civili di cui al comma 8 fino alla misura degli interessi legali, nei casi in cui il mancato o ritardato pagamento sia derivato da oggettive incertezze connesse a contrastanti ovvero sopravvenuti diversi orientamenti giurisprudenziali o determinazioni amministrative sulla ricorrenza dell'obbligo contributivo (art. 116 comma 15).

L'interpretazione dell'INPS

Più volte l'INPS ha espresso le proprie interpretazioni sull'estensione delle fattispecie dell'evasione e dell'omissione contributiva.
Nei primi interventi che sono succeduti alla novella legislativa del 2000, l'INPS aveva ritenuto sussistere l'evasione contributiva anche nelle ipotesi di dissimulazione del rapporto di lavoro subordinato, ossia di rapporti di lavoro regolarmente denunciati e di contributi correttamente pagati dal datore di lavoro, ma in relazione a un contratto diverso da quello subordinato e successivamente qualificato in tal senso, con una conseguente parziale scopertura contributiva (Circolare n. 110 del 2001).
Siffatta interpretazione suscitò dei rilievi critici in dottrina, evidenziandosi la forzatura di far discendere l'intenzionalità del datore di lavoro in tutti i casi in cui venga accertata la natura subordinata di un rapporto giuridico non qualificato dalle parti come tale.
Così con Circolare n. 74 del 10 aprile 2003, l'Istituto previdenziale adottò un atteggiamento più cauto sul tema: tenuto conto che la formulazione del concetto di evasione si basava (e si basa) sull'intenzionalità dell'occultamento del fatto da parte del datore di lavoro, l'INPS rilevò che, nelle ipotesi di rapporto di lavoro riqualificato in sede giudiziale, tale intenzionalità potesse anche non sussistere, facendo così venir meno uno dei requisiti che contraddistinguono fattispecie dell'evasione.
Ed infatti, con Circolare n. 66 del 2008, l'Istituto previdenziale ha specificato che l'evasione contributiva, si configura nei casi in cui vi sia la contemporanea presenza di due requisiti: il volontario occultamento del rapporto di lavoro o delle retribuzioni erogate (profilo oggettivo) e l'intenzionalità del datore di lavoro di non adempiere agli obblighi contributivi ai quali è tenuto (profilo soggettivo); e ciò indipendentemente dalla natura del rapporto (subordinazione o parasubordinazione).
In quella Circolare, l'INPS ha ricondotto nell'alveo dell'omissione alcuni specifici casi, quali le contribuzioni dovute a seguito di reintegrazione nel posto di lavoro disposta dal giudice o di accertamento giudiziale di differenze retributive (sempre che queste ultime non siano riconducibili ad ipotesi di occultamento) e la mancata o tardiva presentazione della denuncia contributiva mensile DM10, recante la dettagliata indicazione dei contributi previdenziali da versare (a condizione che il datore di lavoro abbia adempiuto nei termini di legge alla comunicazione di assunzione e che il lavoratore sia registrato nei libri paga e matricola dell'azienda).
Un decennio più tardi, con Circolare n. 106 del 2017, l'INPS, dopo aver premesso che "*si configura l'ipotesi dell'evasione laddove vi sia occultamento di rapporti di lavoro ovvero di retribuzioni erogate e l'occultamento sia attuato con l'intenzione specifica di non versare i contributi o i premi, ossia con un comportamento volontariamente indirizzato a tale scopo*", ha precisato che l'elemento oggettivo dell'"occultamento" si configura non solo nel caso di assoluta mancanza "*di qualsivoglia elemento documentale che renda possibile l'eventuale accertamento della posizione lavorativa o delle retribuzioni*", ma anche nei casi di denuncia obbligatoria all'Ente previdenziale che risulti non presentata, incompleta o non conforme al vero.
Ed infatti, a dire dell'Istituto, il mancato invio (occultamento) all'Istituto previdenziale delle denunce mensili (adempimento funzionalmente diretto a consentire a quest'ultimo la conoscenza mensile o periodica del proprio credito contributivo) impedendo allo stesso di disporre degli elementi idonei a definire l'obbligo dell'imposizione, integra un comportamento sintomatico della volontà di occultare i rapporti e le retribuzioni nel quale è possibile individuare il profilo soggettivo dell'intenzionalità (necessario a ricondurre la fattispecie nell'alveo dell'evasione). Trattasi di una interpretazione che, come si vedrà, è stata sposata anche dalla giurisprudenza prevalente.
Ma la Circolare n. 106 del 2017 si sofferma anche sull'ipotesi del "ravvedimento operoso", precisando che tale condotta presuppone una denuncia mensile tardiva, la cui mancanza appartiene quindi all'ipotesi di evasione di cui all'art. 116, comma 8, lett. b).
Solo ove il ravvedimento del soggetto obbligato sia attuato spontaneamente e prima di contestazioni o richieste da parte dell'Istituto entro dodici mesi dalla data di scadenza legale dell'adempimento omesso, e sempre che il pagamento della contribuzione denunciata sia effettuato nei successivi trenta giorni dalla presentazione, le sanzioni civili saranno dovute nella misura prevista dall'art. 116, comma 8, lett. a).

L'interpretazione della Cassazione

Come accennato in premessa, sulla distinzione tra l'omissione e la più grave fattispecie dell'evasione si registra un notevole contenzioso.
Punto indiscusso è il fatto che a mente del citato art. 16, comma 8, lett. a) si ha l'ipotesi dell'evasione laddove sussistano due requisiti: occultamento di rapporti di lavoro ovvero di retribuzione erogate; tale occultamento sia stato attuato con l'intenzione specifica di non versare contributi o i premi, ossia con un comportamento volontario finalizzato allo scopo indicato (Cass. 27 settembre 2016, n. 18962).
Sennonché, sull'estensione dei due requisiti è sorto nella giurisprudenza di legittimità un contrasto di opinioni.
Un terreno di scontro è risultato essere l'esatto inquadramento della mancata presentazione da parte del datore di lavoro del modello DM10.
Si sono registrate, infatti, pronunce inclini a ritenere che tale condotta rientri nella fattispecie dell'omissione contributiva "*qualora il credito dell'istituto previdenziale sia comunque evincibile dalla documentazione di provenienza del soggetto obbligato (nella specie libri contabili e denunce riepilogative annuali), dovendo in tal caso escludersi l'occultamento del rapporto di lavoro e delle retribuzioni erogate*" (Cass. 20 gennaio 2011, n. 1230) e pronunce, invece, che hanno escluso che la semplice registrazione dei lavoratori nei libri paga e matricola possa ritenersi sufficiente a configurare la fattispecie dell'omissione, trattandosi di documenti che restano nella disponibilità del datore di lavoro e controllati dall'ente previdenziale soltanto in occasione di eventuali ispezioni, con l'effetto che in tali ipotesi dovrebbe presumersi "*l'esistenza della volontà del datore di occultare i rapporti di lavoro al fine di non versare i contributi*" "*gravando sul medesimo l'onere di provare la sua buona fede*" (Cass. 10 maggio 2010, n. 11261).
Componendo il contrasto interpretativo insorto, la giurisprudenza successiva ha aderito a tale ultimo orientamento.
Lo ha fatto attraverso un'analisi puntuale dei due requisiti sopracitati che compongono l'evasione contributiva.
In relazione al primo, la giurisprudenza ha chiarito che "*il termine occultamento non indica necessariamente l'assoluta mancanza di qualsivoglia elemento documentale che renda possibile l'eventuale accertamento della posizione lavorativa o delle retribuzioni, posto che anche soltanto attraverso la mancata (o incompleta o non conforme al vero) denuncia obbligatoria viene celata all'ente previdenziale (e, quindi, occultata) l'effettiva sussistenza dei presupposti fattuali dell'imposizione e ciò, si badi, proprio attraverso l'adempimento funzionalmente diretto a consentire all'Istituto l'agevole conoscenza, mese per mese, del proprio credito contributivo*" (così Cass. 27 dicembre 2011, n. 28966, poi ripresa da Cass. 16 dicembre 2020, n. 28700; Cass. 23 marzo 2021, n. 8110; Cass. 16 febbraio 2023, n. 5000).
A nulla varrebbe sostenere, continua la Corte, che l'ente impositore potrebbe venire a conoscenza della situazione effettiva, atteso che tale conoscenza resterebbe, in difetto di una denuncia periodica veritiera, collegata ad un eventuale accertamento, e non farebbe quindi venir meno, il requisito dell'occultamento (cfr., ancora, Cass. 27 dicembre 2011, n. 28966).
Quanto al secondo requisito, di carattere soggettivo (l'intenzionalità), si è affermato che l'omissione o l'infedeltà della denuncia mensile è di per sé sintomatica (ove non meramente accidentale, episodica e strettamente marginale) della volontà di occultare i rapporti e le retribuzioni, facendo dunque presumere l'esistenza di una specifica volontà datoriale di sottrarsi al versamento dei contributi dovuti (Cass. 7 ottobre 2022, n. 29272).
Trattasi, tuttavia, di una presunzione relativa che può essere superata mediante l'allegazione e la prova (l'onere delle quali è a carico dal datore di lavoro) di circostanze dimostrative dell'assenza del fine fraudolento (Cass. 11 luglio 2022, n. 21831), come potrebbe essere il caso, ad esempio, delle ipotesi in cui gli inadempimenti siano derivati da mera negligenza o da altre circostanze contingenti (così Cass. 27 settembre 2016, n. 18962).
Anche se, in relazione a tale ultimo aspetto, è stato precisato che lo stato di incertezza sulla sussistenza dell'obbligo contributivo, che consente di attribuire i connotati della buona fede alla posizione del contribuente, non assume rilevanza all'interno della possibile alternativa tra omissione ed evasione contributiva, ma esclusivamente nell'ambito delle specifiche disposizioni di cui all'art. 116, commi 10 e 15, lett. a), della Legge n. 388 del 2000, che, come visto, attenuano grandemente il carico sanzionatorio ma presuppongono l'avvenuto pagamento della contribuzione non versata (Cass. 3 giugno 2022, n. 17970).

Conclusioni

La breve disamina delle interpretazioni che si sono succedute a livello giurisprudenziale e di prassi amministrativa mostra che in sede di qualificazione dell'inadempimento contributivo del datore di lavoro non vigono automatismi di sorta, essendo necessario che si proceda a una accurata verifica delle circostanze del caso concreto, in modo che si possa incanalare la condotta inadempiente nell'ambito del confine tra omissione e evasione contributiva.

Un giro in libreria

a cura di Oumou K. Konate

Crisis of Conscience: Whistleblowing in an Age of Fraud
di Tom Mueller

608 pagine
In questi ultimi decenni i "whistleblower", ovvero gli *insider* che denunciano gli illeciti di organizzazioni pubbliche o private, hanno acquisito una rilevanza legale e sociale senza precedenti. Queste persone infatti fungono da arma per il Governo contro le cattive condotte aziendali e sono una difesa per i cittadini avverso le azioni illecite dell'esecutivo.
I whistleblower ci costringono ad affrontare questioni fondamentali sull'equilibrio tra libertà di parola e segreto di stato, e tra moralità individuale e potere aziendale.
L'autore, Mueller ripercorre l'ascesa delle denunce attraverso una serie di casi avvincenti tratti dal mondo della sanità e di altre imprese, Wall Street e Washington.

Building a Cybersecurity Culture in Organizations
di Isabella Corradini
154 pagine

Questo libro offre una guida pratica su come sviluppare una cultura della sicurezza informatica efficace nelle aziende. Fornisce una prospettiva psicosociale sulle minacce informatiche comuni che colpiscono le organizzazioni e indica soluzioni che sfruttano gli atteggiamenti e i comportamenti dei lavoratori.
Secondo l'autrice la sicurezza informatica inizia infatti con il migliorare il rapporto tra le persone e le tecnologie digitali.
È grazie alla formazione del personale che le aziende possono raggiungere la resilienza informatica.

Speaking Truth to Power - A Theory of Whistleblowing
di Daniele Santoro e Manohar Kumar
204 pagine

Per coloro che non hanno ancora ben capito che cosa sia il whistleblowing, questo libro offre una spiegazione a 360°, definendone il concetto, le origini e la sua posizione all'interno del dibattito etico attuale.
Il libro distingue tra due forme di denuncia, civica e politica, mostrando come si applicano nei contesti di corruzione e segretezza del governo.
L'autore offre un importante contributo sui rischi della segretezza in una democrazia, in particolare, sulle restrizioni che questa impone al diritto epistemico dei cittadini di sapere a quali condizioni i loro diritti sono limitati dalle politiche di sicurezza e dagli interessi aziendali.

Work like a woman: a manifesto for change
di Mary Portas
240 pagine

Non è una novità che le donne oggi lavorano all'interno di una cultura patriarcale dannosa per il loro progresso e per gli affari.
L'autrice, facendo tesoro di quanto imparato nel corso della sua carriera, rende note le trappole comuni che limitano le donne: dalla malsana cultura del "*girl boss*" alle difficoltà nel combinare una carriera con la maternità, nonché il bullismo sul posto di lavoro.
L'autrice si cimenta anche in soluzioni progressiste a questioni pratiche come il lavoro flessibile, il congedo parentale e la parità salariale.
Il libro di Portas è un "manifesto per il cambiamento". Una lettura che consiglio sia alle giovani donne che ai dirigenti esperti.

News

di Ivano Maccani e Denise Boriero

Novità normative
Tra le principali novità legislative, si segnalano:

• Decreto Legislativo n. 24/2023 "Attuazione Direttiva UE 1937/2019 - Whistleblowing"
Il testo normativo, entrato in vigore il 30 marzo 2023, allarga in maniera significativa il perimetro di applicazione della disciplina in materia di *whistleblowing* ed introduce le c.d. "segnalazioni esterne". Ulteriori novità sono rappresentate dalla previsione normativa che annovera, fra i soggetti obbligati ad applicare la disciplina, le imprese private che hanno impiegato, nell'ultimo anno, la media di almeno 50 lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato, oppure che rientrano nell'ambito di applicazione degli atti dell'UE, in materia soprattutto di protezione del risparmio, anche se nell'ultimo anno non hanno raggiunto questa media di lavoratori subordinati oppure che hanno adottato Modelli di organizzazione ai sensi del D.Lgs. n. 231/2001 e che hanno nominato un Organismo di Vigilanza (ODV).
A questi si aggiungono i soggetti del settore pubblico ed altri soggetti previsti all'articolo 1 del D.Lgs. 24/2023.
Tra i principali obblighi previsti dalla normativa si segnalano:
- definizione *ex* ante della *governance* del processo di gestione delle segnalazioni, individuando e valutando idonee soluzioni organizzative;
- affidare la gestione del canale di segnalazione a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero ad un soggetto esterno, purché con le stesse caratteristiche;
- calendarizzare a cadenza periodica la formazione in materia di *whistleblowing*;
- definire le modalità operative in cui si articola il processo di gestione delle segnalazioni;
- implementare un canale interno per la ricezione e la gestione delle segnalazioni e prevedere adeguate modalità di tutela del segnalante;
- predisporre *policy* e procedure specifiche in materia di *whistleblowing*, che consentano di gestire, in modo conforme, anche segnalazioni pervenute mediante canali distinti da quello scritto e informatizzato.
Sono previsti ulteriori obblighi in materia di trasparenza:
- fornire informazioni chiare e facilmente accessibili riguardo al canale, alle procedure e ai presupposti per effettuare le segnalazioni interne e esterne;
- comunicare al segnalante la presa in carico della segnalazione, mediante "avviso di ricevimento" da rilasciare entro sette giorni dalla ricezione;
- fornire riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione;
- assicurarsi che, alle informazioni fornite ai sensi della normativa in materia di *whistleblowing*, si affianchino le informazioni in merito al trattamento dei dati del segnalante e di tutte le altre persone coinvolte nel processo (quali i soggetti segnalati e i c.d. "facilitatori"), ai sensi della normativa in materia di protezione dei dati personali.
Per quanto riguarda l'aspetto sanzionatorio l'ANAC potrà applicare sanzioni amministrative pecuniarie fino a euro 50.000, nei casi in cui accerti che:
- non sono stati istituiti canali di segnalazione;
- non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni;
- l'adozione di tali procedure non è conforme a quelle previste dal decreto;
- non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute;
- sono state commesse ritorsioni;
- la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza.
Le disposizioni del presente decreto avranno effetto a decorrere dal 15 luglio 2023, con eccezione dei soggetti del settore privato che abbiano impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato fino a 249 per i quali l'obbligo di istituzione del canale di segnalazione interna, ai sensi del nuovo decreto, avrà effetto a decorrere dal 17 dicembre 2023.

• Decreto Legge n. 198/2022 cd. "Decreto Milleproroghe"
La legge di conversione del Decreto Milleproroghe contiene rilevanti novità legate al diritto allo "*smart working*" per determinate categorie. In particolare si concederà un'estensione, fino al 30 giugno 2023, del diritto al lavoro agile alle categorie di seguito elencate:
- ai lavoratori dipendenti affetti da patologie individuate dal Decreto del Ministro della Salute del 4 febbraio 2022 (tra cui immunodeficienze, patologie oncologiche trattate con farmaci immunodepressivi, pazienti trapiantati o in attesa di trapianto). Tale estensione dei termini riguarda sia la categoria di lavoratori dipendenti pubblici che privati;
- al datore di lavoro che assicura di lavorare in modalità agile anche con una diversa mansione, compresa nella stessa categoria o area di inquadramento come definite nei contratti di lavoro collettivi senza decurtazione della retribuzione;
- ai dipendenti nel privato che hanno almeno un figlio sotto 14 anni se in famiglia non c'è altro genitore beneficiario di sostegno al reddito per sospensione o cessazione del lavoro o non lavoratore;
- ai lavoratori esposti al rischio di contagio da Covid-19 per età o altre condizioni in base alle valutazioni dei medici competenti (cd. pazienti fragili).

• Disegno di Legge Delega per la riforma fiscale approvato C.d.M. 16 marzo 2023
Le nuove regole, operative entro 24 mesi dall'entrata in vigore della legge delega, ambiscono a semplificare e ridurre la pressione fiscale, a favorire investimenti e assunzioni e ad instaurare un rapporto tra contribuenti e amministrazione finanziaria nella logica di un dialogo mirato tra le parti secondo le esigenze di cittadini e imprese.
Le principali novità della riforma sono:
- la garanzia dell'equità orizzontale, attraverso la riduzione della pressione fiscale, passando a 3 aliquote e con l'obiettivo della *flat tax* per tutti;
- la revisione delle *tax expenditures*, (oggi più di 600 voci), il riordino delle aliquote Iva e l'equiparazione della "*no tax area*" per lavoratori dipendenti;
- la riduzione dell'attuale aliquota IRES per chi investe e\o assume;
- l'azzeramento delle sanzioni per i contribuenti che adotteranno un sistema di rilevazione dei rischi fiscali certificato (TCF);
- il rafforzamento del regime di adempimento collaborativo (*cooperative compliance*);
- le nuove forme di contraddittorio preventivo con l'obbligo di interlocuzione anticipata in caso di parere negativo ad un'istanza del contribuente;
- l'introduzione di procedure semplificate in caso di adesione a indicazione dell'Agenzia da cui scaturisca il ravvedimento operoso. In caso di violazioni non gravi è previsto inoltre che l'eventuale fuoriuscita dal regime sia preceduta da un periodo di "osservazione" al termine del quale valutare l'uscita dal regime di adempimento.
Tali novità porterebbero una maggior attrazione verso il regime di adempimento collaborativo non soltanto per le grandi imprese ma anche per le imprese di medie e piccole dimensioni che avrebbero dei vantaggi concreti in grado di compensare gli investimenti necessari per implementare e rendere funzionale

il sistema di rilevazione e gestione dei rischi fiscali.

• Decreto Legislativo n. 150/2022 cd. "Riforma Cartabia" – Focus in materia penal-tributaria
La presente riforma ha introdotto numerose novità anche nell'ambito penal-tributario. In particolare ha stabilito che si celebra udienza preliminare per i seguenti reati previsti dal D.Lgs. n. 74/2000:
- art. 2 - dichiarazione fraudolenta mediante fatture per operazioni inesistenti;
- art. 3 - dichiarazione fraudolenta mediante altri artifici;
- art. 4 - dichiarazione infedele;
- art. 8 - emissione di fatture per operazioni inesistenti;
- art. 10 - occultamento o distruzione documenti contabili;
- art. 10 quater comma 2 - indebita compensazione di crediti inesistenti;
- art. 11 comma 1, ii° periodo - sottrazione fraudolenta di imposte maggiore a 200.000 euro.

Ha disposto, inoltre, che l'azione penale è esercitata con la citazione diretta a giudizio per i seguenti reati previsti dalla medesima normativa penal-tributaria:
- art. 5 - omessa dichiarazione;
- art. 10 bis - omesso versamento di ritenute certificate;
- art. 10 ter - omesso versamento iva;
- art. 10 quater comma 1, indebita compensazione di crediti non spettanti;
- art. 11 comma 1, I° periodo - sottrazione fraudolenta al pagamento delle imposte;

È prevista un'udienza filtro predibattimentale in camera di consiglio innanzi a un giudice diverso da quello davanti al quale si celebrerà il dibattimento.

Novità dalla Pubblica Amministrazione
Per quanto riguarda invece le novità in materia di circolari amministrative, si segnalano:

• Ministero della Giustizia, Circolare n. 57216/2023
La Circolare chiarisce i requisiti di iscrizione, gli obblighi formativi e i requisiti alternativi ai fini del primo popolamento dell'albo dei gestori della crisi d'impresa, art. 356 del Codice della crisi d'impresa e dell'insolvenza (Ccii).
I chiarimenti sono forniti in materia di:
- enti erogatori della formazione iniziale;
- enti erogatori dell'aggiornamento biennale;
- requisito alternativo alla formazione, ai fini del primo popolamento dell'albo.

Essendo previsto un limite temporale per la validità degli incarichi giudiziali utili ai fini dell'iscrizione all'albo (art. 356, comma 2, Ccii), viene chiarito che lo sono anche quelli conferiti successivamente alla data del 16 marzo 2019, sino all'entrata in vigore del codice della crisi di impresa e dell'insolvenza, e pertanto tutti gli incarichi giudiziali assegnati dal 17 marzo 2015 sino al 15 luglio 2022. Quanto alla formazione iniziale necessaria ai fini dell'iscrizione all'albo, ottenuta tramite la partecipazione a corsi di perfezionamento istituiti a norma dell'art. 16 del D.P.R. 10 marzo 1982 n. 162 di durata non inferiore a duecento ore nell'ambito disciplinare della crisi dell'impresa e di sovra indebitamento, viene specificato che sono legittimati a erogare tale formazione iniziale anche gli ordini professionali dei consulenti del lavoro, qualora risulti un'apposita convenzione con università pubbliche o private e a condizione che i corsi rispettino gli ulteriori requisiti di legge. Infine, vengono debitamente riconsiderati anche gli ordini professionali legittimati a erogare l'aggiornamento biennale, ricomprendendovi anche quello dei consulenti del lavoro, pur in assenza di apposita convenzione con università pubbliche o private, a condizione che i corsi rispettino gli ulteriori requisiti di legge.

• INAIL, Linee di indirizzo per l'applicazione di un sistema di gestione della salute e sicurezza sul lavoro per l'industria chimica 2023
Per favorire la diffusione della cultura, della salute e della sicurezza, in un settore molto variegato e complesso, sono state prodotte dall'INAIL, in collaborazione con Federchimica, le nuove "Linee di indirizzo" che aggiornano un analogo documento prodotto nel 2015 e che intendono costituire un punto di riferimento per la corretta gestione degli aspetti di salute e sicurezza per tutte le imprese chimiche che operano in Italia. Le "Linee di indirizzo" in parole vogliono fornire alle imprese un supporto operativo funzionale all'adozione dei sistemi di gestione, finalizzato ad aumentare il livello di salute e sicurezza sui luoghi di lavoro. Le imprese avranno in tal modo la possibilità di sviluppare un approccio compatibile con il percorso necessario per conseguire la certificazione secondo lo schema previsto dallo standard UNI ISO 45001:2018 e, grazie al contributo presente nell'appendice A, di adottare un modello organizzativo e gestionale relativo alla responsabilità amministrativa degli Enti, di cui al decreto legislativo n. 231 del 2001, che rispetti i requisiti previsti all'art. 30 del D.Lgs. 81/2008. Sarà possibile inoltre estendere agevolmente l'approccio del sistema di gestione della salute e sicurezza a tutte le altre aree della sostenibilità (quale ad esempio ambiente, energia, gestione responsabile del prodotto lungo l'intero ciclo di vita, responsabilità sociale) in linea con quanto previsto per il settore della chimica, dal programma *Responsible Care*. Nel documento sono inoltre presenti sezioni in cui sono state inserite delle "*good pratice*" da poter adottare nei differenti contesti. Tali suggerimenti vogliono essere di ausilio alle imprese che avendo già un sistema di gestione, possono avere indicazioni, spunti e suggerimenti per migliorare ulteriormente le condizioni di salute e sicurezza.

• Ispettorato Nazionale del Lavoro (INL), Documento di programmazione della vigilanza 2023
Nel documento viene rimarcato il ruolo centrale dell'Ispettorato, chiamato ad assicurare gli accertamenti in ambito lavoristico, previdenziale, assicurativo ed in materia di salute e sicurezza del lavoro in adesione all'approccio "*Vision Zero*" delineato nel Quadro Strategico UE 2021-2027 della Commissione UE. Inoltre nell'ambito degli impegni assunti dall'Italia con il PNRR, il Ministero del Lavoro e delle Politiche Sociali ha attribuito all'INL un ruolo centrale nel realizzare azioni specifiche finalizzate a prevenire e contrastare il lavoro sommerso nei diversi settori dell'economia. Nella programmazione dell'attività di vigilanza di iniziativa, l'INL dovrà attuare gli obiettivi definiti dal Piano Nazionale per la lotta al lavoro sommerso (PNS). Le due direttrici principali che pertanto orienteranno la vigilanza saranno:
- l'incremento dell'efficacia dei controlli mediante un rafforzamento dell'attività ispettiva;
- l'adozione di misure di prevenzione volte a promuovere comportamenti virtuosi da parte delle imprese.

Pertanto l'INL prevede di effettuare nell'annualità corrente 75.000 accessi ispettivi, con un incremento di circa il 18% delle ispezioni attivate nel corso del 2022. Oltre al lavoro sommerso proseguiranno i controlli ispettivi sul settore della prevenzione in materia di salute e sicurezza sul lavoro. I settori sui quali si indirizzerà la vigilanza nel corso del 2023 saranno:
- edilizia, agricoltura, logistica, trasporti, esternalizzazioni illecite, caporalato;
- diversa qualificazione del rapporto di lavoro/corretto inquadramento/regime orario;
- nuovi lavori e piattaforme digitali;
- azioni transnazionali in materia di vigilanza sul lavoro;
- vigilanza previdenziale;
- vigilanza assicurativa;
- controlli sul regolare utilizzo delle risorse finanziarie pubbliche dedicate al lavoro e alla sicurezza sociale.

Saranno previste delle "ispezioni lampo" che saranno gestite come "accertamenti a tavolino" sulla parola di lavoratori e sindacati e senza accesso in azienda.
Nel documento viene rinnovato anche l'impegno dell'INL di proseguire nel garantire ai lavoratori che ne hanno la necessità (soprattutto i cosiddetti lavoratori "vulnerabili"), un supporto puntuale ed efficace in ragione della gravità dei fatti riportati.

Novità giurisprudenziali
Qui di seguito alcune tra le più rilevanti pronunce sui temi trattati dalla rivista *Compliance*:

• Corte di Cassazione, VI° Sezione Penale, Sentenza n. 8963/2023
La Suprema Corte accogliendo il ricorso presentato

dal Procuratore europeo delegato della sede di Palermo, al quale era stata rigettata la richiesta di applicazione della misura cautelare reale del sequestro preventivo ai fini di confisca diretta o per equivalente sui beni di pari valore nei confronti dell'imputato, ha annullato l'ordinanza affermando che l'art. 30, par. 1, del Regolamento UE n. 2017/1939, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea, stabilisce che almeno nei casi in cui il reato oggetto dell'indagine è punibile con una pena massima di almeno quattro anni di reclusione, gli Stati membri sono tenuti ad assicurare che i procuratori europei delegati sono autorizzati a disporre o a chiedere le misure investigative tra le quali quella del congelamento degli strumenti o dei proventi di reato, compresi i beni, di cui si prevede la confisca da parte del giudice competente.

• Consiglio di Stato, Sentenze n. 6, 7, 8/2023
Il Consiglio di Stato ha chiarito in adunanza plenaria le competenze del Prefetto e della magistratura penale sui controlli antimafia che possono evitare l'espulsione dell'impresa dal mercato come previsto dal Codice Antimafia. In particolare, il rapporto di vigilanza prefettizia e penale puntano entrambe ad evitare le contaminazioni mafiose dell'impresa, ma la prevenzione collaborativa (prefettizia) e il controllo giudiziario (penale) hanno percorsi autonomi sostenuti da differenti presupposti: mentre il Prefetto valuta la storia dell'impresa, attingendo elementi registrati nella banca dati interforze (indagini, informazioni, parentele, condanne), il giudice penale considera anche le possibilità future di bonifica, se cioè l'impresa può evitare contatti mafiosi. In forza di questa autonomia, i due controlli potranno avere esiti diversi: il tribunale della prevenzione, con l'ausilio dei propri esperti potrà convincersi della trasparenza dell'impresa e della mera occasionalità di eventuali contatti mafiosi; contemporaneamente il Prefetto, consultando la banca dati interforze ed altri elementi d'indagine potrà ritenere consolidata un'infiltrazione mafiosa nella medesima impresa.

• Corte di Cassazione, Sentenza n. 5586/2023
Con l'ordinanza in commento la Suprema Corte ha chiarito che in tema di accertamento, a fronte della presunzione legale di ricavi non contabilizzati, dunque occulti, scaturente da prelevamenti bancari non giustificati, il contribuente può sempre, anche in caso di accertamento analitico-induttivo, opporre la prova presuntiva contraria e in particolare può eccepire l'incidenza percentuale dei costi relativi, che vanno, dunque, detratti dall'ammontare dei prelievi non giustificati. La Suprema Corte, alla luce della pronuncia n. 10/2023 della Corte Costituzionale, ha rivisto il proprio orientamento e riconosciuto che anche nel caso di un accertamento analitico o analitico-presuntivo (come in caso di indagini bancarie) l'Ufficio è tenuto al riconoscimento forfettario di costi deducibili afferenti ai maggiori ricavi o compensi.

• Corte di Cassazione, Sentenza n. 4904/2023
Con la presente sentenza la Suprema Corte ha affermato che non scatta la condanna per l'omesso versamento delle ritenute fiscali atteso che la prova non può essere costituita dal solo contenuto della dichiarazione di cui al modello 770, essendo necessario dimostrare l'avvenuto rilascio ai sostituiti delle certificazioni attestanti le ritenute operate dal datore di lavoro quale sostituto di imposta. Questa è la conclusione della Corte, in base alla disciplina previgente alle modifiche introdotte dal D.Lgs. n. 158/2015, applicabile al caso di specie.

• Corte di Cassazione, Sentenza n. 5984/2023
Il caso in esame ha riguardato un imprenditore che ha subito due procedimenti penali per il reato di dichiarazione infedele (ex art. 4 del D.Lgs. n. 74/2000), che si sono entrambi conclusi con un verdetto a lui favorevole: uno, infatti, è stato definito con un provvedimento di archiviazione del P.M., mentre l'altro si è concluso con una sentenza di assoluzione piena pronunciata dal GUP. I suddetti procedimenti sono stati innescati dalla denuncia, ex art. 331 c.p.p., presentata all'esito dell'ispezione fiscale in azienda da parte di funzionari dell'Amministrazione finanziaria. La Suprema Corte ha accertato la responsabilità colposa dell'Agenzia delle Entrate e dei suoi due dipendenti, per i fatti erroneamente attribuiti all'appellante all'esito dell'ispezione fiscale che diede origine ai due procedimenti penali (infondati), e pronunciato, pertanto, la condanna al risarcimento dei danni non patrimoniali, quantificati in 20.000 euro affermando, così, il principio secondo il quale il contribuente che abbia subito un procedimento penale ingiusto, a causa dell'errore commesso da funzionari della P.A. nell'espletamento del controllo fiscale, ha diritto al risarcimento del danno.

• Corte di Cassazione, Sentenza n. 17689/2022
Il caso è relativo ad un licenziamento comminato ad un Dirigente che durante la riunione del C.d.A., aveva dato lettura di un documento, a propria firma, in cui venivano prospettate delle fattispecie di reato astrattamente imputabili alla Società (datore di lavoro). In particolare, il Dirigente aveva manifestato una serie di perplessità con riferimento al bilancio di esercizio dell'anno 2012, ritenendo potenzialmente configurabili i reati di "falso in bilancio", "ricorso abusivo al credito" e "false comunicazione sociali". Gli Ermellini, conclusa la premessa sul bilanciamento dei contrapposti interessi (dovere di fedeltà e diritto alla critica), si sono addentrati nella disamina del caso di specie oggetto del giudizio, evidenziando che nella fattispecie in esame la condotta del Dirigente non doveva intendersi quale espressione del "diritto di critica" bensì nei termini di un normale "dissenso" rispetto a quanto dichiarato nel documento di bilancio dell'anno 2012. I Giudici hanno poi precisato che la manifestazione del dissenso in sede di C.d.A., rispetto alle previsioni del bilancio di esercizio, era condizione necessaria affinché le responsabilità e le conseguenze pregiudizievoli del relativo bilancio non venissero imputate allo stesso Dirigente nella sua qualifica di Direttore Generale. La Corte ha rilevato come il legame fiduciario e obbligo di fedeltà, che caratterizza il rapporto dirigenziale, non possa determinare alcuna automatica compressione del diritto di critica, di denuncia e di dissenso spettante al lavoratore. Ne consegue che anche nel rapporto di lavoro dirigenziale, e ai fini della verifica della legittimità del licenziamento intimato al Dirigente, dovrà tenersi in debita considerazione il contemperamento tra l'obbligo di fedeltà e i predetti diritti di critica, denuncia e dissenso, escludendo che l'esercizio di questi diritti, nei limiti riconosciuti dalla giurisprudenza sopradetti, possa di per sé giustificare il licenziamento del Dirigente.

• Corte di Cassazione, Sentenza n. 4855/2023
Il caso in esame ha riguardato un uomo, ritenuto responsabile per il reato di acquisto e detenzione illecita di sostanze stupefacenti e di autoriciclaggio, ha fatto ricorso in Cassazione lamentando la violazione di legge in relazione all'art. 648-ter1 c.p., posto che la punibilità andava esclusa in tutti i casi in cui il denaro o le altre utilità, derivanti dal reato presupposto, fossero destinate alla mera utilizzazione personale ovvero la condotta non risultasse concretamente idonea ad ostacolare l'identificazione dell'origine delittuosa. L'esimente di cui all'art. 648-ter1 c.p., esclude l'assoggettamento a pena per coloro che, fuori dei casi di cui ai commi precedenti, destinino il denaro, i beni o le altre utilità, derivanti dal reato presupposto, alla mera utilizzazione o al godimento personale.
La sentenza afferma il principio secondo il quale sussiste l'autoriciclaggio anche per le spese personali di chi ha compiuto il reato presupposto, essendo esclusa l'esimente del godimento di natura personale ex art. 648-ter1 c.p., considerato che la molteplicità delle operazioni effettuate attraverso plurimi conti correnti tutti a servizio dell'attività di ripulitura delle somme provento del traffico illecito di stupefacenti, la pluralità di beni mobili e immobili, acquisiti tramite le stesse, la sistematica attività di pagamento tramite i profitti illeciti di rate di finanziamento o

mutuo immobiliare precedentemente accesi, costituiscono elementi per ritenere sia che l'attività svolta abbia assunto natura finanziaria e speculativa, sia che la stessa essendo priva della finalità dell'utilizzo contingente del profitto illecito, risulti punibile quale complessa attività di autoriciclaggio.

Relazioni e studi

Si riportano di seguito alcune Relazioni e ricerche svolte attinenti ai temi della Rivista:

• Relazione EPPO frodi comunitarie 2022

Le frodi comunitarie colpiscono le entrate pubbliche e nel 2022 sono stati stimati danni complessivi per 14,1 miliardi di euro. Alla fine del 2022, l'EPPO aveva 1.117 indagini attive con danni stimati per 14,1 miliardi di euro, di cui quasi la metà (47%) derivanti da frodi sull'Iva; inoltre, sempre nel medesimo periodo, ha ricevuto e trattato 3.318 segnalazioni di reato e ha aperto 865 indagini in seguito alle quali i giudici hanno concesso il congelamento di 359,1 milioni di euro.

• Polizia Postale, Report Cybersicurezza 2022

Nel 2022 il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic) ha registrato un aumento del 138% degli attacchi rilevati alle infrastrutture critiche rispetto al 2021 (12.947). Per porre rimedio a tali attacchi la Polizia Postale ha elaborato un apposito *Vademecum* destinato al mondo dell'industria allo scopo di prevenire dannose intrusioni informatiche nei sistemi. Ciò non sarà sufficiente ad eliminare del tutto questa tipologia di condotta criminale ma certamente potrà limitarne gli effetti seguendo alcune linee guida di seguito elencate:

- avere sempre una copia dei dati da recuperare in caso di attacchi;
- proteggere la navigazione in rete e l'utilizzo del traffico dati;
- mantenere sistemi e software antivirus costantemente aggiornati;
- introdurre password con autenticazioni a due fattori;
- cautele nell'aprire e-mail e messaggi.

Tra le cause riconducibili alla proliferazione di tali attacchi vi sono sostanzialmente due fattori: l'utilizzo di tecniche più sofisticate e la ridotta consapevolezza del fenomeno *cyber* criminale. I dati contenuti nel *Thread Intelligence Report* dell'osservatorio *cyber security* di Exprivia, evidenziano come il settore *finance* sia il settore più colpito con 939 casi (36% degli attacchi totali nel 2022); mentre sempre lo stesso *report* mostra come la tipologia di danno maggiormente diffusa sia il "furto di dati" (70% della totalità dei fenomeni registrati).

Tali attacchi, sono riconducili sia a critici fattori geopolitici sia, come sostiene il Dottor Manfredini, Presidente Associazione Italiana Professionisti Security Aziendale (AIPSA), ad una rara presenza di figure come i *security manager* nelle aziende; per tali ragioni, è auspicabile che tali figure possano diventare obbligatorie nelle imprese al pari del responsabile della salute e sicurezza nei luoghi di lavoro o del certificatore del bilancio.

• Indagine DLA Piper su sanzioni e data breach in UE - Gennaio 2023

L'indagine, relativa ai 27 Stati membri dell'UE (più Regno Unito, Norvegia, Islanda e Liechtenstein) ha rivelato un altro anno record, con un importo totale delle sanzioni emesse dal 28 gennaio 2022 a gennaio 2023 pari a 1,64 miliardi di euro, con un aumento del 50% rispetto all'anno precedente. Per quanto riguarda l'applicazione della *privacy*, i Paesi dell'UE registrano un andamento assai difforme: ci sono Paesi con un'altissima sensibilità, dove le segnalazioni ufficiali delle violazioni sono elevate (oltre 117 mila in Olanda), e Paesi dove il numero è stato bassissimo (si consideri la Bulgaria con 434 notificazioni di *data breach*); ci sono nazioni con un cospicuo numero di sanzioni irrogate (567 la Spagna) e altre con un numero decisamente basso (per la Francia se ne contano 33). Per quanto riguarda l'Italia si posiziona a metà classifica (11ª) per il numero totale di *data breach*, ma sprofonda se si rapporta il numero delle violazioni alla popolazione (27ª), mentre risale fino al 2° posto per numero di sanzioni irrogate e si adagia al sesto livello per ammontare delle stesse. Nel commentare i risultati, *Dla Piper* ritiene che l'aumento dimostri la volontà dei Garanti della *privacy* europei di imporre multe elevate per violazioni del GDPR, in linea con gli orientamenti del Comitato Europeo per la protezione dei dati, che ha ripetutamente richiesto aumenti significativi delle ammende proposte dai singoli Garanti. Proseguendo con l'analisi, si può affermare che la situazione, presa in tutte le sue sfaccettature, non ha significativi reconditi e dimostra solamente che in ambito comunitario si viaggia in ordine sparso e che non sono stati sufficienti 26 anni di *privacy* europea a fare del Vecchio Continente un'unione normativa sul fronte della tutela della riservatezza.

• Indagine Fondazione studi consulenti del lavoro 2022

L'indagine mostra come nei primi 9 mesi del 2022 siano state assunte oltre 2,5 milioni di donne ma che, nello stesso periodo, oltre 600 mila ha deciso di lasciare il proprio impiego (+21,5% rispetto al 2021). I dati mostrano tra le principali cause che spingono le donne attive nel mondo del lavoro a cambiare professione vi siano le seguenti motivazioni: la ricerca di un miglior salario (50,7%) e di un miglior equilibrio psico-fisico (50,6%).

Più nel dettaglio, ulteriori elementi di insoddisfazione del lavoro per le donne risultano essere:

- *welfare* aziendale/*benefit* (49,4%);
- le prospettive di crescita (43,4%);
- la retribuzione (37,1%).

La mobilità nel mercato femminile del lavoro ha mostrato per il 2022 il seguente quadro:

- il 21,4% è stato assunto mentre il 29,1% ha presentato dimissioni.

Per quanto concerne le donne "occupate" in cerca di un nuovo lavoro l'analisi ha prodotto il seguente quadro:

- 4,5% ha cambiato professione;
- 12,6% si è attivato per cambiare lavoro;
- 38,7% desidera cambiare lavoro;
- 44,3% non è interessato a cambiare lavoro.

Dunque oltre il 55% delle donne sarebbe intenzionata o avrebbe cambiato lavoro secondo le elaborazioni fornite dalla seguente indagine. Le donne sembrano interpretare le trasformazioni in atto nel mondo professionale più dei loro colleghi uomini, con una visione maggiormente dinamica e una cultura più in linea con i cambiamenti epocali che attraversa il mondo del lavoro.

• "Cosa cercano le donne sul lavoro" sondaggio condotto da ManpowerGroup, marzo 2023

Il sondaggio effettuato su un campione di 4 mila lavoratori evidenzia che l'80% delle donne chiede un miglior *work-life balance*, l'equiparazione degli stipendi a

quelli dei colleghi maschili e avere dei capi "empatici" che possano meglio comprendere l'esigenza di chi ha figli. Tali richieste si rifletterebbero positivamente sulla produttività e sulla qualità del lavoro espressa. Considerando il presente, la metà delle lavoratrici abbandonerebbe l'attuale posto di lavoro per uno stipendio più alto ma il 30% cambierebbe azienda solo per un miglior *work-life balance*. Oltre 1 donna su 3 sarebbe disposta a rinunciare al 5% dello stipendio per una settimana lavorativa di quattro giorni, mentre il 16% accetterebbe una riduzione di salario per poter lavorare da remoto.
Per quanto concerne il lavoro in presenza, è stato rilevato dalla presente indagine come le donne sarebbero più motivate nel lavorare in presenza per favorire una miglior collaborazione e per "staccare" in modo netto i tempi del lavoro da quelli familiari. La ricerca infine conferma la voglia di imparare nel mondo femminile: il 31% ha dichiarato di aver ricevuto formazione tecnica, mentre il 67% ha denunciato difficoltà rispetto agli uomini ad accedere al *training* che favorisce la crescita professionale. Solo il 19% delle lavoratrici ha affermato di essere stata inserita in percorsi di avanzamento di carriera, e forse anche per queste circostanze il 40% delle donne sono convinte che i propri manager non abbiano ben compreso le loro reali potenzialità.

• **Ricerca Community Research&Analysis per Federmeccanica**
La ricerca evidenzia come ci sia un progressivo declino del valore dal lavoro manuale. Le cause sono molteplici: da un lato c'è un problema di valorizzazione economica e di trattamenti per una parte di questi lavoratori (occupazioni sottopagate, orari eccedenti); dall'altra parte si pone la questione degli aspetti qualitativi su cui le persone oggi mettono l'accento. Oggi, non è più sufficiente come accadeva in passato, offrire "un posto di lavoro ed un salario" per essere attrattivi; occorrono altri fattori che possano rendere attrattivo quella determinata mansione. Come rimarca la presente ricerca confrontando le due generazioni dei "figli" (fino a 34 anni) e dei "padri" (oltre 65 anni) la classifica delle professioni è simile, tuttavia per i "giovani" praticamente tutte le professioni proposte ottengono punteggi inferiori a quelli attribuiti dai "padri" eccetto le professioni di *influencer e blogger*.

Focus
Il Reporting di sostenibilità
La Direttiva europea approvata il 28 novembre 2022, la n. 2464/2022 intitolata "Corporate Suistainability Reporting" (CSRD) introduce nuove regole di rendicontazione di sostenibilità per le grandi imprese. I nuovi obblighi di trasparenza dovranno essere rispettati a partire da gennaio 2024, andando ad ampliare il numero delle imprese coinvolte nell'obbligo di dichiarazione dell'impatto ambientale e sociale (da 11.700 a 50.000), aumentando al contempo l'analiticità delle informazioni da comunicare annualmente. Il recepimento della direttiva comporterà, necessariamente, l'aggiornamento del modello organizzativo ex D.Lgs. n. 231/2001.
L'ampliamento dei soggetti coinvolti è graduale:
• dal 2024 le imprese costituiscono enti di interesse pubblico già obbligati alla pregressa "dichiarazione non finanziaria";
• dal 2025 l'adempimento riguarderà anche le grandi imprese non già soggette alla "dichiarazione non finanziaria";
• dal 2026 l'obbligo interesserà le piccole e medie imprese con valori mobiliari ammessi alla negoziazione in mercati regolamentati dell'UE;
• dal 2028 l'obbligo riguarderà le imprese dei Paesi terzi che generano ricavi netti dalle vendite e dalle prestazioni superiori a 150 milioni di euro nell'UE e che hanno impresa figlia o succursale nel territorio della stessa.
L'intervento mira a fornire nuovi standard di sostenibilità all'interno dell'UE, essendo al momento lacunosa la legislazione al riguardo. Tale argomento è già stato trattato all'interno della Rivista Compliance[1].
Allo stesso tempo, le nuove misure dovrebbero ridurre il fenomeno dell'ambientalismo di facciata, c.d. "greenwashing" ed a tipizzare le relative figure perseguibili come pratiche commerciali ingannevoli. Altro ambito in cui sta intervenendo l'Unione Europea.

1 *Si veda Rivista Compliance, Luglio 2022 – "L'informativa ESG e il nuovo quadro europeo degli standard per il reporting di sostenibilità" di G. Fraccaro.*
Il tema dei criteri ESG sono stati ampliamente trattati nel manuale "ESG e Recovery Plan – Percorsi e strumenti per la sostenibilità di lungo termine delle P.M.I.", edito da SEAC nell'ambito della Collana Compliance in settembre 2021.

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.