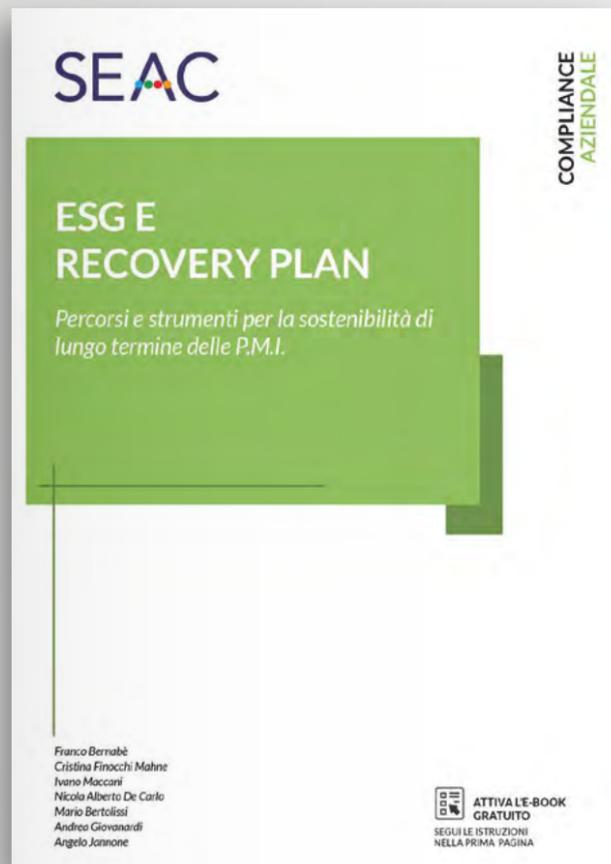


COMPLIANCE



*Passione per
semplificare le cose*

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

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

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



Direttore responsabile: Giovanni Bort
 Product Manager: Giuliano Testi e Tullio Zanin
 Comitato di redazione: Ivano Maccani, Anna Maria Carbone, Luigi Fruscione, Maurizio Block, Mario Bertolissi, Denise Boriero
 Coordinatrici di redazione: Maria Chiara Volpi e Elisabetta Arcuri
 Indirizzo della Redazione:
 Via dei Solteri, 74 – 38121 Trento
 Telefono 0461/805326 – email: compliance@seac.it
 Editore: SEAC S.p.A. – Via dei Solteri, 74 – 38121 Trento
 Telefono 0461/805111 – Fax 0461/805161 – email: seacspa@sicurezza postale.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

00

Editoriale

IL PNRR:

un'opportunità preziosa, con le dovute attenzioni

Pag. 07

01

Pnrr

PNRR e opportunità per le imprese: piccolo vademecum operativo

Pag. 08

02

Pnrr

PNRR e sistemi di controllo

Pag. 16

06

Import-Export

Lo sportello unico doganale: il DPR 29 dicembre 2021 n.235

Pag. 47

08

Antiriciclaggio

I nuovi adempimenti antiriciclaggio per il comparto assicurativo

Pag. 60

03

Sicurezza&Performance

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

Pag. 25

04

Privacy

L'attività di verifica applicata all'ambito *data protection*

Pag. 31

07

Anticorruzione

***Compliance:* il modello organizzativo 231 e la gestione del rischio. Prima parte**

Pag. 54

09

Agroalimentare e Green Economy

All'agricoltura oltre 2 miliardi di euro dalla manovra finanziaria 2022 per incentivare gli investimenti, la spesa sociale, il lavoro giovanile e la parità di genere

Pag. 67

05

Anticorruzione

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

Pag. 38

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

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

Eleonora Fasoli: Avvocato del Foro di Verona, DPO/RPD in carica. Progetta soluzioni e consulenza sulle tematiche di protezione dei dati personali con sentita attenzione alla formazione, alla vigilanza e all'assistenza professionale vicina alle persone.

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

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

Edoardo Franquillo: Avvocato, già collaboratore di cattedra di diritto processuale penale presso l'Università degli Studi di Perugia. Ha maturato esperienza all'interno di studi legali specializzati nel diritto penale dell'economia e, in particolare, nella costruzione di modelli di organizzazione, gestione e controllo ex d.lgs. 231/2001. Attualmente, si occupa di Compliance in ambito 231, anticorruzione e antiriciclaggio presso il network Deloitte.

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

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

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

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

IL PNRR: un'opportunità preziosa, con le dovute attenzioni

di Ivano Maccani e Denise Boriero

Il PNRR, piano elaborato dall'Italia nell'alveo degli interventi previsti dall'Unione Europea per risollevarsi dalla crisi acuita dalla pandemia, è partito nell'anno appena conclusosi e ha una durata prevista di cinque anni, fino al 2026. Molti sono stati gli interventi relativi a questo piano, sia sulla Rivista che sulla collana editoriale (si pensi al testo "ESG e Recovery Plan", edito a fine 2021), ma nel presente numero si vuole dare un taglio diverso. Come tutte le opportunità, in *primis* bisogna assicurarsi di coglierle concretamente e occorre inoltre vigilare affinché l'intervento raggiunga i veri destinatari e non venga deviato. Per questo motivo, in questo secondo numero del 2022 si danno dei riferimenti concreti alle medie e piccole imprese per consentire loro di partecipare effettivamente alle possibilità di finanziamento previste, anche ricorrendo all'aiuto di enti appositi. La Camera dei Conti Europea, infatti, ha evidenziato in un suo studio che soltanto il 30,7% dei fondi a disposizione dell'Italia nel quadriennio 2014-2020 sono stati effettivamente erogati, poiché il nostro Paese si posiziona al penultimo posto per capacità di assorbimento dei fondi stanziati. Non si deve quindi correre il rischio di perdere l'enorme opportunità fornita dal Piano Nazionale di Ripresa e Resilienza. Allo stesso tempo, come riconosciuto dalle più consolidate teorie criminologiche, "l'opportunità fa l'uomo ladro" e la criminalità, che è razionale, è già pronta ad inserirsi in questo fruttuoso spazio. Sono e saranno dunque necessari dei rigidi controlli per consentire che i benefici raggiungano davvero i destinatari previsti. A questo è dedicato l'ar-

ticolo dal titolo "*PNRR e sistemi di controllo*". Una delle Missioni principali del PNRR è la digitalizzazione: questo obiettivo, ormai imprescindibile, è stato portato alla luce ancora più dalla crisi, che ha trovato un sistema impreparato a gestire la produzione a distanza, ma che, allo stesso tempo, ha visto un suo fortissimo acceleramento. La digitalizzazione, che non può che comportare una svolta, ha ovviamente dei rischi intrinseci. Per questo, anche in questo numero, si parla di prevenzione agli attacchi dei dati sanitari, di "*Attività di verifica applicata all'ambito di data protection*" e si conclude la disamina delle linee guida della Guardia di Finanza in materia di prova digitale, a dimostrazione che il digitale è davvero il futuro. Non mancano inoltre altri contributi di rilievo sullo Sportello unico doganale alla luce del recente Dpr n. 235 del 2021, sui modelli di prevenzione dei rischi ai sensi del decreto legislativo n. 231/2001, sui nuovi adempimenti antiriciclaggio per il comparto assicurativo e sui contributi dedicati all'agricoltura, che nella manovra finanziaria 2022 superano i due miliardi e possono costituire dunque un'importante svolta per il settore.



PNRR e opportunità per le imprese: piccolo vademecum operativo

di Denise Boriero

Il PNRR: i numeri

L'Unione Europea ha risposto alla crisi mondiale acuita dalla pandemia in corso con il programma *Next Generation EU*, il quale prevede investimenti e riforme finalizzati all'eliminazione delle discriminazioni e alla transazione ecologica e digitale.

Tra i principali strumenti del *Next Generation EU* si ha il RRF, ossia il Dispositivo per la Ripresa e la Resilienza, il quale richiede ai singoli Stati membri la presentazione di un pacchetto di riforme e programmi da realizzare a fronte delle risorse messe a disposizione dallo stesso RRF.

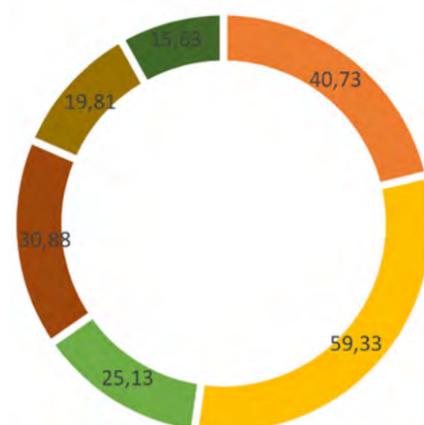
L'Italia, principale beneficiaria di questo strumento, ha presentato il Piano Nazionale di Resistenza e Resilienza (PNRR). Il Piano si articola in sei Missioni, perfettamente in linea con le indicazioni dell'Unione Europea e i temi del NGEU. Le risorse totali sono pari ad euro 191,5 milioni da impie-

gare nel periodo 2021-2026, dei quali 68,9 miliardi sono sovvenzioni a fondo perduto e 122,6 miliardi di prestiti finanziati attraverso il RRF, ai quali si aggiungono poi 30,6 miliardi di risorse nazionali del Fondo complementare e ulteriori 13 miliardi di euro del *React EU*.

Il PNRR si articola in 16 componenti, raggruppate appunto in singole Missioni così suddivise:

- digitalizzazione, innovazione, competitività, cultura (40,73 milioni di euro);
- rivoluzione verde e transizione ecologica (59,33 milioni di euro);
- infrastrutture per una mobilità sostenibile (25,13 milioni di euro);
- istruzione e ricerca (30,88 milioni di euro);
- inclusione e coesione (19,81 milioni di euro);
- salute (15,63 milioni di euro).

Le sei Missioni



- digitalizzazione, innovazione, competitività, cultura
- rivoluzione verde e transizione ecologica
- infrastrutture per una mobilità sostenibile
- istruzione e ricerca
- inclusione e coesione
- salute

Dal grafico è ancora più facilmente visibile la gerarchia interna delle diverse Missioni alla luce della suddivisione delle risorse: in *primis*, l'attenzione per l'ambiente, che non può che passare attraverso la transizione ecologica. Il clima, infatti, è da anni al centro delle politiche europee, si pensi al Trattato di Lisbona che all'articolo 191 indica la politica ambientale comune europea, tradotta in azioni concrete suddivise in *step* progressivi. Ci si riferisce, ad esempio, al "Pacchetto per il clima e l'energia 2020" che l'Unione Europea aveva elaborato e che può dirsi raggiunto (la c.d. politica del 20%, ossia una riduzione del 20% del consumo energetico e delle emissioni di gas serra rispetto agli anni '90, nonché la produzione di un 20% in più di energie rinnovabili). Gli obiettivi stabiliti dall'UE per il 2030 sono ancora più ambiziosi: dimezzamento delle emissioni di gas serra (-40% rispetto al 1990), produzione del 32% di energia da fonti rinnovabili ed efficientamento energetico, quindi una riduzione dei consumi pari almeno al 32,5%. È ovvio che per raggiungere questi obiettivi serve una vera e propria rivoluzione in tutti i singoli Stati Membri, e questo è il fine del NGEU e di tutti i finanziamenti concessi dall'Unione Europea in questo ambito. La sostenibilità è un criterio essenziale per le imprese, non solo alla luce di una scelta propria di coscienza e di risparmio delle risorse, ma anche per i nuovi parametri di valutazione delle aziende e delle società e per le scelte degli investitori. Vale la pena di evidenziare che ben 600 milioni di euro sono stati stanziati per il piano "Progetto faro di economia circolare" della componente 1 della Missione 2 (Rivoluzione verde e transizione ecologica), in ripresa anche dei cardini di riferimento del Piano d'azione Europeo sull'Economia Circolare fulcro del c.d. *Green Deal* europeo.

Segue l'obiettivo della digitalizzazione da intendersi come innovazione e rilancio della competitività, dell'istruzione e della ricerca, che in ogni caso sono anche presupposti per la digitalizzazione e l'innovazione, a loro volta necessari al fine di

arrivare ad una rivoluzione ecologica. Gli interventi risultano così tutti concatenati e correlati.

Il Governo italiano, dopo diverse bozze, ha trasmesso il PNRR alla Commissione europea il 30 aprile 2021, la quale l'ha approvato definitivamente il 13 luglio 2021, erogando in agosto un prefinanziamento di circa 25 miliardi di euro all'Italia (il 13% del totale previsto).

In base all'articolo 24 del Regolamento UE 2021/241, poi, ciascun Stato membro presenterà ogni 6 mesi una richiesta debitamente motivata alla Commissione relativa ai contributi, che saranno rimborsati solo e soltanto previa valutazione del raggiungimento "in misura soddisfacente" degli obiettivi e dei traguardi previsti.

Queste opportunità non potranno che incidere significativamente sull'economia del nostro Paese e l'effetto si sta già dimostrando: secondo Confartigianato, il PNRR ha permesso già nel 2021 un aumento di +0,5 punti sul PIL dell'Italia. Si stima che questo possa arrivare a +3,6 punti alla conclusione del programma, tra quattro anni¹. La positività dell'impatto è potenzialmente più alta, tutto dipende da come e quanto le realtà italiane riusciranno ad usufruire di questa possibilità.

Infatti, una volta chiarita la disponibilità di risorse bisogna assicurarsi che le stesse siano effettivamente distribuite tra gli *stakeholders*, senza venire perse in lungaggini burocratiche o difficoltà procedurali.

Questo pericolo, purtroppo, è molto forte e non riguarda soltanto i fondi messi a disposizione dal PNRR. Secondo uno studio della Camera dei Conti Europea relativo al bilancio 2014-2020, l'Italia è il penultimo stato dell'Unione per capacità di assorbimento dei fondi europei. Soltanto il 30,7% dei contributi esistenti sono stati effettivamente erogati alle imprese italiane in quel quadriennio. Le cause di questo divario tra opportunità fornite e quelle colte sono di certo molteplici e possono essere individuate nella mancanza di conoscenza di tutte le agevolazioni disponibili, circostanza che tuttavia difficilmente si dovrebbe

¹ L'articolo completo, dd. 03.05.2021, è reperibile all'indirizzo web: <https://www.confartigianato.it/2021/05/studi-pnrr-e-crescita156-punti-pil-in-sei-anni-effetti-piu-accentuati-sul-sistema-casa/>.

presentare in relazione ai fondi di cui in oggetto, visto il rilievo che è stato loro riconosciuto, nonché nella difficoltà della presentazione della domanda alla luce di procedure farraginose e complicate. Questo secondo aspetto, purtroppo, potrebbe realizzarsi anche in questo caso. Allo stesso modo, spesso accade che, pur avendo correttamente richiesto il bonus nelle tempistiche previste, le imprese non ottengano effettivamente il finanziamento, o soltanto con grandi ritardi, andando così a vanificare i benefici inizialmente previsti. Nelle ipotesi peggiori, inoltre, non vengono rimborsati i costi già sostenuti alla luce dei contributi attesi poiché ci sono difficoltà ed errori nella rendicontazione delle spese.

Proprio per ovviare a tutti questi problemi, è utile che le imprese sappiano che esistono enti creati appositamente con lo scopo di aiutare le aziende a partecipare ai bandi di gara per l'assegnazione di fondi, a richiedere i contributi pubblici e a rendicontare tutte le spese. Molte sono le associazioni create proprio in vista del PNRR, anche in rappresentanza delle piccole e medie imprese. Ad oggi, il numero maggiore di queste si trova in Lombardia e in generale nel nord Italia. Questo dato è facilmente spiegabile dai numeri: nel Nord

ci sono molte più imprese e opportunità di lavoro del Sud e questa forbice purtroppo si è allargata ancora di più a seguito delle crisi degli ultimi anni. Proprio per questi motivi, la "questione del Mezzogiorno" è uno dei nodi dello stesso Piano Nazionale di Resistenza e Resilienza. Per favorire il superamento del divario lungo la linea Nord/Sud del Paese è stato previsto il vincolo di destinare il 40% delle risorse del PNRR al Mezzogiorno.

Ad ogni modo, anche al Centro e al Sud esistono dei progetti a sostegno delle realtà produttive, in particolare medio-piccole, ad esempio con l'emissione di voucher digitali per agevolare l'innovazione e con l'utilizzo di piattaforme che forniscono *utilities*, supporti e formazione per la digitalizzazione.

Proprio la digitalizzazione, come sopra detto, rappresenta uno degli obiettivi chiave del PNRR. La pandemia di questi anni, infatti, ha dimostrato ancora più chiaramente il ritardo - soprattutto italiano - nella gestione innovativa dei processi produttivi. Allo stesso tempo va riconosciuto che proprio la pandemia ha consentito uno sviluppo notevole della digitalizzazione come risposta necessaria allo stallo che si era creato.



Le opportunità per le imprese

Le imprese che vogliono usufruire dei benefici previsti dal PNRR devono dunque partire dai pilastri già più volte ripetuti. L'investimento non deve essere tuttavia unico o considerato come mero insieme di interventi singoli, ma occorre arrivare ad una vera ri-organizzazione della realtà produttiva. Installare una fonte di energia rinnovabile, ad esempio posizionando sul tetto del proprio capannone dei pannelli fotovoltaici, potrà anche consentire l'accesso al bonus, ma non comporterà un aumento della produttività, della qualità o della competitività. Sarà opportuno, invece, elaborare delle strategie più strutturate, investendo in modalità di gestione automatizzate e innovative, con un'attenzione non solo alla sostenibilità ma anche all'ambiente di lavoro e alle persone, a partire dalla loro sicurezza fisica e mentale fino alla loro formazione e al giusto equilibrio tra vita e lavoro.

Andando ora nello specifico ad alcuni dei finanziamenti di interesse per le aziende, non si può non partire dall'investimento numero uno relativo alla Missione "Digitalizzazione, innovazione e competitività nel sistema produttivo", ovvero il Piano di Transizione 4.0, che prevede il riconoscimento di tre tipologie di credito di imposta:

1. credito di imposta per
 - a. beni strumentali materiali 4.0 (tecnologicamente avanzati);
 - b. beni strumentali immateriali;
 - c. beni strumentali immateriali standard (software relativo alla gestione aziendale);
2. credito di imposta per attività di ricerca, sviluppo e innovazione;
3. credito di imposta con attività di formazione alla digitalizzazione e di sviluppo delle relative competenze.

Tale credito di imposta è pari al 50% dei costi ed è recuperabile in sede di dichiarazione dei redditi per i beni materiali e immateriali ordinari che siano nuovi - quindi acquistati direttamente dal produttore o in qualsiasi caso mai stati utilizzati dall'eventuale terzo cedente - strumentali all'attività esercitata e destinati a strutture situate

sul territorio italiano. Per quanto riguarda i beni "industria 4.0", essendoci un'attribuzione maggiorata del beneficio, oltre a quelli appena elencati è richiesto un altro requisito ossia "l'interconnessione", la quale deve essere attestata da una perizia tecnica asseverata in caso di beni dal valore superiore ad euro 300.000. I beni "industria 4.0" sono riportati nell'Allegato A e nell'Allegato B della Circolare dell'Agenzia delle Entrate n. 4/E del 30 marzo 2017, e possono essere suddivisi in tre macrocategorie:

- beni strumentali controllati da sistemi computerizzati o gestiti tramite opportuni sensori;
- sistemi finalizzati all'assicurazione della qualità;
- dispositivi per l'interazione uomo-macchina nonché l'aumento della sicurezza sul lavoro.

Il credito di imposta per i beni "industria 4.0" è utilizzabile soltanto in compensazione, in tre quote annuali di pari importo a partire dall'anno di avvenuta interconnessione del bene. Al fine di mantenere il credito, nessun requisito può venire meno, in particolare l'interconnessione, la quale deve rimanere almeno per i tre periodi di imposta in cui si usufruirà del beneficio stesso².

Relativamente invece alla formazione, che ovviamente deve essere sulle tecnologie, l'innovazione e l'automazione industriale, il credito di imposta è utilizzabile in compensazione tramite modello F24 a decorrere dal periodo di imposta successivo e anche in questo caso, come detto, parte dal 50% dei costi, ma presenta diversi limiti e tetti massimi annuali in base alla dimensione dell'azienda. L'incentivo è rivolto principalmente alle piccole e medie imprese, infatti nel loro caso è più alto: il 50% con limite massimo di euro 300.000 annui per le micro e piccole imprese, il 40% con il limite di euro 250.000 per le medie imprese e il 30% sul medesimo tetto per le aziende di grandi dimensioni. Indipendentemente dalla dimensione della realtà produttiva, tuttavia, si riconosce un aumento del bonus al 60% se la formazione è rivolta a

² O almeno per tutta la durata del periodo di accertamento della dichiarazione in cui si è iscritto il credito.

dipendenti svantaggiati o molto svantaggiati³. L'attività formativa fornita va rendicontata in modo dettagliato e deve risultare da un'apposita certificazione rilasciata da un revisore legale dei conti anche nel caso di aziende non soggette alla revisione contabile (salva la possibilità di rimborso delle spese in quest'ultimo caso).

Lo sviluppo di questi canali, così come la creazione di nuove e più efficienti piattaforme di *e-commerce*, consentirà alle nostre aziende nazionali di essere più competitive. Proprio il carattere della competitività è un aspetto chiave delle *policies* che si andranno ad attuare e una delle Missioni del Piano Nazionale di Ripresa e Resilienza. Si consideri che, secondo l'OCSE e il suo indice di regolamentazione del Mercato dei Prodotti (PMR), l'Italia risulta molto meno competitiva rispetto ad altri paesi europei in termini di prezzi e qualità dei beni e ciò sarebbe dovuto alla mancanza dello sviluppo delle reti digitali ma anche di quelle dei trasporti, nonché all'esistenza di barriere all'entrata dei mercati⁴. Altro strumento per aumentare la competitività sarà quello dell'internazionalizzazione delle piccole e medie imprese e ciò sarà reso possibile da contributi e prestiti agevolati a realtà italiane che operano in mercati stranieri. Il decreto direttoriale del 26 ottobre 2021 aveva infatti previsto la possibilità di richiedere agevolazioni per la promozione all'estero di marchi collettivi o di certificazione dal 22 novembre 2021 al 22 dicembre 2021. Purtroppo, le domande tardive sono considerate inammissibili, ma essendo questo uno dei punti alla base del PNRR saranno probabilmente aperte nuove modalità di finanziamento per l'internazionalizzazione.

La tutela dell'"italianità" all'interno e all'esterno dei confini nazionali è messa in atto anche tramite l'IP⁵. È infatti prevista una

riforma in materia di proprietà industriale per adeguarla alle sfide del mercato, tutelando così le innovazioni, incoraggiando la diffusione della proprietà industriale in particolare nelle piccole e medie imprese, rafforzando inoltre il ruolo dell'Italia nelle sedi europee e internazionali, consolidando i tratti caratteristici del "*Made in Italy*" che all'estero tanto ci invidiano.

Inoltre, un ruolo sempre più preponderante è riconosciuto al CNALCIS (Consiglio Nazionale per la Lotta alla Contraffazione e all'*Italian Sounding*) istituito nel 2010, proprio in materia di *Made in Italy*, anticontraffazione e proprietà industriale.

Sempre lo strumento del credito fiscale è destinato pure alle imprese che operano nel settore del turismo, altro pilastro del PNRR: 530 milioni di euro sono destinati proprio ad aumentare la qualità dell'ospitalità turistica con investimenti volti alla riqualificazione e alla sostenibilità ambientale. L'accesso al credito è facilitato sia per gli imprenditori che gestiscono attività turistiche esistenti sia ai giovani che vogliono entrare nel settore tramite un rafforzamento del Fondo Centrale di Garanzia. Sempre al fine di aumentare l'attrattività turistica e dunque la "competitività" del nostro Paese anche da questo punto di vista – che dovrebbe essere gioco facile dato il patrimonio culturale di cui disponiamo – gli interventi saranno rivolti alla modernizzazione delle infrastrutture materiali e non, all'aumento dell'accessibilità anche attraverso investimenti digitali nonché alla valorizzazione dei borghi lontani dai grandi centri urbani, ricchi di storia, tradizioni e arte.

Si ricorda inoltre che anche il Fondo Nazionale per l'innovazione vede un'integrazione pari a 0,30 miliardi di euro finalizzati a sostenere nuove *start up*.

L'inclusione, altro tema caldo nel NGEU

³ Per lavoratori dipendenti svantaggiati e molto svantaggiati si intendono non solo i soggetti privi di retribuzione ma anche i non diplomati o le persone che, per condizioni personali quale quella dell'età, non sono particolarmente ricercati dal mercato del lavoro.

⁴ Dato riportato anche nelle schede "L'Italia riparte – il PNRR – Piano Nazionale di Ripresa e Resilienza" elaborate dal Ministero per la Pubblica Amministrazione.

⁵ L'acronimo IP sta per Industrial Property, ossia "Proprietà Industriale", la cui definizione è contenuta nell'articolo 1 del Codice della Proprietà industriale: "Ai fini del presente codice, l'espressione proprietà industriale comprende marchi ed altri segni distintivi, indicazioni geografiche, denominazioni di origine, disegni e modelli, invenzioni, modelli di utilità, topografie dei prodotti a semiconduttori, segreti commerciali e nuove varietà vegetali".



riportato nel PNRR, vuole anche innalzare i livelli di partecipazione delle donne nel mercato del lavoro. Secondo uno studio del 2020 di Unioncamere⁶, le donne che fanno impresa rappresentano soltanto il 22% del totale dell'imprenditoria. Merita evidenziare che, al contrario del *trend* generale, statisticamente le donne imprenditrici sono principalmente giovani e sono situate nel Mezzogiorno.

Gli interventi in questo ambito sono principalmente volti ad una modifica culturale che superi le distinzioni di genere, valorizzando l'imprenditoria femminile anche nelle scuole e cercando di garantire strumenti che favoriscano la conciliazione vita-lavoro nonché le necessità specifiche legate alla genitorialità. Sarà messo a regime un "Fondo Impresa Donna" che supporti *start up* e imprese femminili.

Le imprese saranno poi agevolate anche dalla semplificazione in materia di appalti e contratti pubblici, che quindi permetterà alle aziende private di fornire più facilmente prestazioni agli enti pubblici, semplificando e riordinando le norme avvicinando quanto più possibile alle poche regole fornite dall'UE. In particolare, saranno semplificate le procedure di verifica antimafia e protocolli di legalità (è richiesto all'Auto-

rità Nazionale Anticorruzione di realizzare una piattaforma unica per la trasparenza), saranno ridotte le tempistiche della Conferenza di Servizi, dell'aggiudicazione e dell'esecuzione dei contratti, nonché sarà limitata la responsabilità erariale ai casi in cui il danno sia realizzato con dolo, ad esclusione dei danni cagionati da colpa. Infine, sarà previsto un Collegio Consultivo Tecnico (CTT) per fornire assistenza e risolvere le controversie in sede stragiudiziale. Accanto alla riforma abilitante sulla concorrenza, alla luce degli obiettivi già sopra descritti, sono previste delle riforme collegate in materia di giustizia tributaria (con un intervento del CNEL), processuale civile (ad esempio potenziando le *Alternative Dispute Resolution*), penale e del sistema sanzionatorio penale (volto sempre ad accelerare i tempi della giustizia e a ricomprendere dei provvedimenti di "deindicizzazione" a tutela del diritto all'oblio), già a partire dall'anno appena concluso. Si prevede una riforma fiscale volta a raccogliere e razionalizzare tutta la legislazione fiscale in un Testo Unico integrato dalle disposizioni speciali, da far a sua volta confluire in un unico Codice tributario. In questa direzione si pone anche la riforma della riscossione, la quale nasce anche dall'esigenza

⁶ Unioncamere, Rapporto imprenditoria femminile, 2020.



di tener conto della pronuncia della Corte Costituzionale n. 120/2021, che, tra i vari rilievi mossi all'attuale sistema, evidenzia anche il grandissimo numero di esecuzioni infruttuose. Attesa anche una riforma dell'IRPEF, volta a rispettare il principio di progressività e ad introdurre un reddito minimo esente da dichiarazione che dovrebbe essere più alto per i giovani lavoratori con meno di 35 anni.

In aggiunta, si è prevista una vera e propria riforma del mercato del lavoro, in primis con una forte spinta alle politiche attive e alla formazione, intesa qui in senso più ampio di quella sopra descritta in materia di innovazione, e che sarà rivolta non solo agli inoccupati ma anche ai lavoratori per acquisire nuove competenze e sarà garantita anche in orari diurni grazie alla rimodulazione dell'attività produttiva raggiunta grazie all'intervento dei rappresentanti di categoria. Altro obiettivo è quello dell'eliminazione del lavoro sommerso, del caporalato e di tutte le altre forme di sfruttamento, a partire dal dicembre 2022 con la piena implementazione del "Piano nazionale per la lotta al lavoro sommerso" entro marzo 2024. Sono previsti poi sgravi

fiscali per i datori di lavoro e una platea più ampia di soggetti che potrà usufruire di ammortizzatori sociali in caso di difficoltà delle aziende e delle imprese, con un occhio di riguardo anche ai lavoratori autonomi.

Gli imprenditori, dunque, anche aiutati dagli enti preposti e ricorrendo alla creazione di partenariati, dovranno essere pronti a cogliere tutte le opportunità riportate, che costituiscono solo parte delle possibilità fornite dal PNRR e gli investimenti nazionali, per far sì che gli aiuti forniti possano davvero essere sfruttati arrivando a destinazione e non rimanendo meri benefici teorici.



SEAC SERVIZI ASSICURATIVI

Polizze di responsabilità civile per i professionisti

Fai la cosa giusta,
scegli **un partner affidabile!**

PNRR e sistemi di controllo

di Ivano Maccani e Denise Boriero

Premessa

Purtroppo, la storia ci insegna come gli scenari di difficoltà socio-economica siano sempre stati molto allettanti per la criminalità di ogni genere, rappresentando essi, con tutto il loro carico di dolore, debolezza e insicurezza, anche una deprecabile ma enorme opportunità di arricchimento illecito. Questo vale per ogni forma di criminalità, ma in particolare per quella organizzata, sempre pronta a sfruttare la situazione a suo favore, avendo dalla sua parte tutti gli strumenti per poterlo fare. Non è una novità il fatto che le organizzazioni criminali, disponendo di enormi quantità di denaro contante da riciclare, si infiltrino nel mondo economico e si muovano dove ci sono grandi crisi, cogliendone tutte le possibilità.

L'indubbia rilevanza delle ingenti risorse messe in campo nell'ambito del PNRR, pari a 205 miliardi di euro, cui si aggiungono altri 30 miliardi tratti dal bilancio nazionale con il fondo complementare, implica, pertanto, la necessità che i previsti interventi possano dispiegarsi in maniera efficace e all'interno di una cornice di piena legalità. Inevitabilmente, infatti, le attenzioni di organizzazioni criminali dedite alla corruzione, al riciclaggio, alle frodi e ai reati finanziari, si indirizzeranno anche ai fondi previsti dal PNRR, cercando di sfruttare le

semplificazioni giustamente adottate per la gestione degli stessi.

Ciò a maggior ragione nella contingenza attuale, in cui le frodi e le condotte illecite potranno essere incentivate anche da una quantità di risorse mai così copiosa, considerando anche i fondi dei quadri finanziari pluriennali 2014-2020 e 2021-2027, con le relative quote di cofinanziamento nazionale. In effetti, proprio nell'ambito dell'attuale quadro finanziario pluriennale 2021-2027, l'Italia risulta destinataria di quasi 100 miliardi di risorse europee, alle quali vanno ad aggiungersi impegni di spesa residui (7,5 miliardi di euro) e pagamenti non ancora ammessi per trasferimento (pari a circa 23,5 miliardi) relativi alla precedente programmazione 2014-2020.

Tutto questo significa che improvvisamente il nostro Paese si troverà a dover gestire risorse fino a cinque volte maggiori di quelle generalmente amministrate in precedenza. Trattasi di una sfida delicata, strategica ed importantissima, che mette a dura prova la capacità di gestione e controllo di Pubbliche Amministrazioni ed Enti Pubblici.

Partendo da tali premesse, si è provveduto a rafforzare la politica di coesione anche tramite il "reclutamento" di alcune migliaia di nuovi tecnici in grado di supportare sul territorio le amministrazioni interessate. Per incrementare ulteriormente la capacità



amministrativa dei soggetti attuatori, sarà anche importante rilanciare i c.d. piani di rafforzamento amministrativo (PRA), che comportano per ogni Regione e Ministero competente, in relazione ad un programma della politica di coesione, la necessità di evidenziare i problemi riscontrati nel precedente ciclo di programmazione, prospettando al contempo le possibili soluzioni da applicare entro un arco temporale predefinito.

Un ruolo importante e delicato lo rivestono anche i professionisti che dovranno prestare grande attenzione a investimenti e progettualità in accordo con un motto che si può sintetizzare in "conosci il tuo cliente". Tale auspicabile prospettiva di collaborazione anche con imprese ed associazioni di categoria assume un rilievo particolarmente significativo perché spinge sulla necessità di stabilire relazioni e creare sinergie, nella consapevolezza che gli obiettivi più ambiziosi possono essere raggiunti solo facendo squadra.

Il sistema di gestione e controllo

L'attuazione del PNRR è stata affidata alla

responsabilità di Amministrazioni Centrali e Locali, chiamate ad uno straordinario impegno per la gestione delle relative risorse, peraltro nell'ambito di un generale processo di semplificazione del quadro normativo e procedurale che comporta necessariamente una maggior esposizione al rischio frode.

In tale ottica, il nostro Paese, come tutti gli altri Paesi beneficiari degli interventi europei volti alla ripresa, è tenuto a garantire un sistema di controlli interni efficace ed efficiente, finalizzato a prevenire, individuare e rettificare le frodi, i casi di corruzione e i conflitti di interesse nonché a recuperare le somme erroneamente versate o utilizzate in modo non corretto.

Secondo le linee guida CE, gli Stati membri dovrebbero combinare procedure amministrative di controllo già esistenti con altre, che possiamo definire aggiuntive, ispirate a quelle previste per i fondi strutturali. Ciascun soggetto attuatore (Pubbliche Amministrazioni, Regioni, Province autonome ed Enti locali) responsabile della realizzazione operativa degli interventi previsti dal PNRR è tenuto ad attuare i piani stabiliti in linea



con le modalità previste dalla normativa nazionale ed europea vigente. Il sistema dei controlli deve includere i c.d. controlli interni di regolarità amministrativa e contabile, l'analisi e la valutazione della spesa ed i c.d. controlli di gestione.

Deve inoltre essere assicurata la completa tracciabilità delle operazioni e la tenuta di un'apposita codificazione contabile per l'utilizzo delle risorse del PNRR. Ciascuna Amministrazione interessata deve pertanto conservare tutti gli atti e la relativa documentazione giustificativa su supporti informatici adeguati, da rendere disponibili per le attività di controllo e audit.

Le stesse Amministrazioni centrali titolari di interventi del PNRR, a seguito della ricezione delle informazioni inerenti l'avanzamento dei progetti da parte dei soggetti attuatori ed ai fini della rendicontazione al Servizio centrale per il PNRR, svolgono ulteriori attività di controllo, in particolare:

- verifiche formali e controlli sulla regolarità delle spese e delle relative procedure rendicontate dai soggetti attuatori, a campione e selezionate sulla base dell'analisi dei rischi; tali verifiche consistono in controlli amministrativo-contabili, accompa-

gnati da eventuali approfondimenti in loco finalizzati ad attestare la correttezza e la conformità alla normativa delle procedure di gara e di affidamento nonché l'effettività, la legittimità, l'ammissibilità e l'assenza di doppio finanziamento delle spese sostenute e rendicontate dai soggetti attuatori;

- verifiche finalizzate ad attestare l'effettivo conseguimento di target e milestone attraverso l'esame della documentazione trasmessa dai soggetti attuatori nonché la relativa riferibilità, congruità e coerenza rispetto ai cronoprogrammi attuativi degli interventi;

- verifiche volte ad accertare il rispetto dei principi DNSH, Tagging clima e digitale, nonché delle specifiche prescrizioni e priorità trasversali (parità di genere, giovani, superamento dei divari territoriali).

Ruolo fondamentale nell'ambito dei controlli per il PNRR assume inoltre, l'Unità di audit, che, in qualità di organismo indipendente di audit, ha il primario compito di garantire l'efficacia del sistema di gestione e controllo del PNRR attraverso lo svolgimento di verifiche di sistema e verifiche delle operazioni. Lo scopo è essenzialmente quello di valutare la veridicità e l'affi-

dabilità dei dati di performance con riferimento ai target e traguardi stabiliti al fine di fornire alla Commissione Europea adeguate garanzie sulla corretta realizzazione dei progetti del PNRR nonché sulla regolarità delle spese al momento della presentazione delle richieste di pagamento.

Misure volte a prevenire, ricercare e contrastare gli illeciti

Per quanto riguarda la prevenzione, l'individuazione e la rettifica delle frodi, dei casi di corruzione e dei conflitti di interesse è stato siglato uno specifico protocollo tra la Ragioneria Generale dello Stato e la Guardia di Finanza. Tale protocollo assume un rilievo particolarmente significativo perché spinge sulla necessità di stabilire relazioni e creare sinergie, nella consapevolezza che gli obiettivi più ambiziosi possono essere raggiunti solo facendo squadra.

In effetti, lo stesso rappresenta la naturale cornice di riferimento per le forme di cooperazione interistituzionale allo scopo di rafforzare le azioni a tutela della legalità delle attività amministrative finalizzate alla destinazione e all'impiego delle risorse finanziarie del PNRR.

Si tiene ad evidenziare che la Guardia di Finanza, nel corso delle ordinarie attività di servizio, può avvalersi di ampie potestà istruttorie, di natura amministrativa, ribadite dal D.lgs. n. 68 del 19 marzo 2001, che ha espressamente esteso le prerogative di intervento fissate dalla normativa fiscale anche al settore della tutela dei bilanci pubblici. L'attività investigativa può inoltre svilupparsi tramite l'utilizzo delle penetranti facoltà previste dalla disciplina anticiclaggio.

A ciò si aggiungono i poteri propri della polizia giudiziaria nel contesto delle indagini svolte con le Procure della Repubblica, le Procure Distrettuali Antimafia e la Procura Europea.

Con riferimento a quest'ultima, si segnala che la stessa rappresenta l'unico organismo nell'ambito del diritto penale europeo deputato a proteggere gli interessi finanziari dell'Unione, e, rivestendo tale veste, è destinata ad essere il principale baluardo nella tutela penale delle risorse rientranti nel PNRR.

Nell'evidenziare l'importanza che necessariamente deve essere riservata al controllo degli appalti pubblici, destinati a rappresentare una parte rilevante degli interventi del PNRR, va osservato che dietro le patologie del sistema appalti che emergono dalle indagini, spesso affiorano i lineamenti di condotte, attive e omissive, generatrici di responsabilità amministrative per danno erariale con conseguente attivazione delle Procure Regionali Contabili.

A tal proposito si evidenzia che la Corte dei Conti, peraltro, esercita il controllo sulla gestione attraverso valutazioni di economicità, efficienza ed efficacia circa l'acquisizione e l'impiego delle risorse finanziarie provenienti dai fondi PNRR. Su tale delicato fronte, ossia quello delle gare per l'affidamento di lavori, servizi e forniture, occorrerà attuare una particolare vigilanza per evitare la commissione di reati, o assicurare la tempestiva repressione di quelli eventualmente già consumati come, purtroppo, già accaduto ed emerso grazie a recenti attività, da parte di funzionari pubblici infedeli inseriti nei meccanismi di gestione delle provvidenze pubbliche.

Un particolare impulso, sin da subito, deve, inoltre, essere riservato all'esecuzione di controlli di natura amministrativa e di indagini di polizia giudiziaria, ricorrendo a moduli operativi flessibili. In effetti, le modalità di attuazione dei progetti e di accesso ai finanziamenti del PNRR da parte dei soggetti attuatori e dei destinatari finali, prevedono un numero significativo di differenti procedure e strumenti, quali, a titolo esemplificativo, la partecipazione a bandi e avvisi pubblici, la presentazione di domande/progetti in risposta ad avvisi pubblici, la presentazione di singole istanze/ricieste.

Un aspetto peculiare, ai fini della prevenzione e la repressione degli illeciti, si sostanzia nella costituzione di una rete di referenti antifrode del PNRR, con la funzione di sviluppare analisi, valutazioni, monitoraggio e gestione del rischio frode del Piano nazionale di Ripresa e Resilienza. Tale gruppo di lavoro ha lo scopo di promuovere momenti di scambio finalizzati a individuare i settori maggiormente esposti ai profili di rischio e concordare modalità di

attuazione del dispositivo antifrode e delle relative attività di controllo, nell'ottica di poter intercettare tempestivamente eventuali sistemi di commissione di illeciti nonché orientare i soggetti attuatori affinché, ricorrendone i presupposti, introducano correttivi nella formazione dei bandi e/o degli avvisi pubblici.

Uno dei principali obiettivi cui tende il sistema di Governance risiede, infatti, nell'effettiva capacità di implementare il sistema di prevenzione con degli alert acquisibili in tale fase di confronto.

Sempre in tema di pubblici appalti, assume rilevanza il ruolo dei Gruppi Interforze Antimafia, pool provinciali coordinati dalle Prefetture e composti da rappresentanti territoriali delle Forze di Polizia e dei Centri Operativi della DIA, nel cui ambito viene promosso il controllo di appalti e sub-appalti allo scopo di escludere in partenza quelli potenzialmente interessati dalle infiltrazioni della criminalità. Per dare una dimensione del fenomeno, le interdittive antimafia emesse in tale contesto nel solo 2020 sono state circa un migliaio, in netto aumento rispetto al passato, il doppio

di quelle di quattro anni fa. Tali dati esprimono, purtroppo, la misura di quanto sia necessario non sottovalutare il tema delle infiltrazioni criminali anche nelle procedure pubbliche.

I controlli devono inoltre essere calibrati avendo riguardo anche alle peculiarità tipiche delle varie realtà territoriali, alle fenomenologie di frodi e alla tipologia dei progetti di spesa. Particolare attenzione deve essere riservata alle posizioni degli operatori economici appaltatori e subappaltatori, realizzatori ed esecutori, di recente costituzione e/o privi di solidità finanziaria o connotati da strutture organizzativo-aziendali inadeguate. L'approccio investigativo deve essere tendenzialmente selettivo, orientato da specifiche analisi preventive. Vale la pena di ricordare, pur non essendo questa la sede per una trattazione articolata, che proprio una delle riforme previste nell'ambito del PNRR come obiettivo collegato ad altri, è quello della semplificazione della normativa della contrattazione pubblica, velocizzando e riducendo inoltre i tempi previsti. Questo, che costituisce sicuramente un vantaggio per tutti gli ope-



ratori legali coinvolti, non può che esserlo anche per quelli illegali e malintenzionati e dunque il controllo deve essere ancora più accurato.

Analisi e selezione degli obiettivi da controllare

Nell'ambito dell'ampio e articolato sistema di prevenzione, individuazione e contrasto delle irregolarità va sottolineata la rilevanza, quale fattore trasversale, dell'utilizzo di strumenti informatici integrati e cooperativi in grado di combinare dati eterogenei provenienti da diversi sistemi informativi come il *data warehouse* e il *datamart* attivati all'interno del sistema unitario "Regis" della Ragioneria Generale dello Stato. Lo stesso, consente la consultazione degli interventi realizzati e in corso di realizzazione con le risorse europee e nazionali e, con riferimento al doppio finanziamento, permette una visione a 360 gradi della distribuzione dei fondi nei territori e delle relative fonti di finanziamento; il sistema informativo comunitario *Arachne IT System* consente l'interrogazione di specifici indicatori e classifiche di rischio connessi al conflitto di interessi, finalizzati a verificare la frequenza di interrelazione tra codici fiscali e partite iva; la piattaforma Integrata Anti-frode *PIAF -IT* aggrega dati provenienti a fonte eterogenee nazionali ed europee, con l'obiettivo di avere a disposizione uno strumento tecnologico in grado di intensificare lo scambio informativo e, quindi, potenziare la delicata fase della prevenzione antifrode; la Dorsale Informatica della Guardia di Finanza consente l'interazione delle numerose banche dati nella disponibilità del Corpo, ben ventotto delle quali attinenti al solo comparto delle uscite, imprescindibili serbatoi di informazioni capaci di generare output sistemici e relazionali; la banca dati *Mocop* - monitoraggio contratti pubblici - che rende fruibili per la consultazione elementi puntuali ed aggregati concernenti gli appalti aggiudicati dalle diverse stazioni appaltanti pubbliche, sviluppando, altresì analisi di rischio e di contesto automatizzate; la banca dati unica degli appalti e il fascicolo virtuale dell'operatore economico di Anac sono in grado di digitalizzare l'intera catena degli

appalti pubblici consentendo l'interoperabilità dei dati delle Pubbliche Amministrazioni; la piattaforma Inps *MoCOA* è in grado di effettuare monitoraggi sulla congruità occupazionale degli appalti.

La possibilità di accesso a dati tra di loro relazionati permette, peraltro, di incrementare le funzioni di georeferenziazione dei fenomeni, consentendo di conoscere puntualmente l'andamento sul territorio delle fenomenologie illecite. Trattasi, di fatto, di un vantaggio competitivo nel contesto della lotta alla criminalità economico-finanziaria.

In conclusione, possiamo affermare che la delicatezza degli interessi in gioco e la complessità dei fenomeni da aggredire sono tali che l'impegno di tutte le Istituzioni deve essere necessariamente coordinato, muovendosi in un sistema omogeneo e strutturato.

L'importante opportunità fornita al nostro Paese dal PNRR, dunque, deve essere monitorata e gestita in modo da essere colta dai destinatari "legittimi" e non dalla criminalità, mettendo in campo tutte le risorse disponibili attraverso una rete strutturata.

Da sempre a fianco dei professionisti



SOFTWARE



EDITORIA



FORMAZIONE



ASSICURAZIONI



CONSULENZA
STRATEGICA



GESTIONE
CREDITI IMPOSTA



SICUREZZA
INFORMATICA

seac.it

Dati sanitari sotto attacco: come prevenire!

di Giovanni Finetto e Paola Finetto

Il *Global Risks Report 2022* pubblicato il 19 gennaio 2021 dal World Economic Forum ¹, nel quale sono presentati i risultati dell'ultimo e più recente sondaggio sulla percezione dei rischi globali, evidenzia come le cyber minacce, per quanto non più percepite come alto rischio, siano tuttora presenti e consistenti. In particolare, emerge la percezione di un fallimento della cybersecurity, dovuto per lo più alla maggiore dipendenza digitale, a fronte di una parimenti maggiore disinformazione tecnologica e di un proliferare, spesso non organizzato, di norme e regolamenti nell'ambito IT e *data protection*. Nel rapporto si legge che, nel 2021 e rispetto al 2020, gli attacchi malware sono cresciuti del 358% e gli attacchi *ransomware* addirittura del 435%. Il pagamento di riscatti a fronte di questi ultimi è del pari aumentato in maniera impressionante: da 0.51 milioni US\$ nel 2013, a 92.94 milioni US\$ nel 2019, a 406.34 milioni US\$ nel 2020. Si sono moltiplicate e diversificate anche le truffe nei pagamenti online, a fronte di un aumento, soprattutto durante la pandemia, degli acquisti online: nel Regno Unito, ad esempio, nel 2021 queste truffe sono aumentate del 117% in volume e del 43% in valore. Al contempo, il sondaggio e la

ricerca, i cui risultati sono ben esposti nel *Global Risks Report 2022*, rimarkano come gli incidenti di sicurezza e le violazioni dei sistemi e delle reti siano ancora per lo più dovuti a errori umani: il 43% dei *data breach* è riconducibile a minacce interne, dunque a eventi, per lo più accidentali, riferibili a persone e dovuti, normalmente, a carenza di formazione e informazione.

In questo contesto, soprattutto negli ultimi mesi, sono aumentati in tutto il mondo gli attacchi informatici ai danni delle strutture sanitarie, massivamente colpite da *ransomware*: i dati sanitari sono merce rara e preziosissima e i criminali informatici sanno ben sfruttare le vulnerabilità dei sistemi. Come si legge nel *Global Risks Report 2022*, c'è addirittura un mercato in forte espansione per la prestazione di servizi diretti a manipolare l'opinione pubblica e indirizzarne le preferenze di acquisto, così come a danneggiare o indebolire aziende competitor. In particolare, i dati sanitari potrebbero permettere alle multinazionali farmaceutiche di orientare le proprie scelte di mercato, oppure alle compagnie assicuratrici di elaborare e offrire nuovi prodotti targettizzati. Già nel giugno 2013 il Financial Times pubblicava un articolo

¹ <https://www.weforum.org/reports/the-global-risks-report-2021>

dal titolo "How much is your personal data worth?"², che permetteva di calcolare il valore economico dei propri dati personali; con riferimento ai dati sanitari, si evidenziava come i dati di una donna incinta del primo figlio avessero un valore stimato di circa 0.102 US\$, mentre i dati di un diabetico potessero valere fino a 0.267 US\$. In un comunicato stampa di Kaspersky del 20 dicembre 2021³ si legge che "il 50% dei fornitori di servizi sanitari italiani intervistati ha dichiarato che, per le sessioni a distanza, alcuni dei loro medici utilizzano app non specificamente progettate per la telemedicina, come FaceTime, Facebook Messenger, WhatsApp, Zoom, etc. Inoltre, sempre il 50% dei medici non conoscerebbe i metodi con cui vengono protetti i dati dei loro pazienti", il che espone i dati anche sensibili trattati a rischi da non sottovalutare. Sempre Kaspersky, in altro comunicato stampa del 2 dicembre 2021⁴, evidenzia come "i cybercriminali hanno cercato di trarre profitto dal

vaccino e gli ospedali sono stati attaccati da ransomware, mettendo in serio pericolo la vita dei pazienti. Il prossimo anno, il vettore di attacco per il settore sanitario continuerà ad espandersi, poiché una quantità sempre maggiore di dati dei pazienti si sta spostando online e gli operatori sanitari continuano ad adottare servizi sanitari digitali come la telemedicina. Nel 2021 le violazioni dei dati sanitari sono già aumentate di una volta e mezza rispetto al 2019".

Le minacce cyber alle strutture sanitarie, anche italiane, non si sono fatte attendere: è del 12 settembre 2021 l'attacco informatico all'Ospedale San Giovanni di Roma⁵; è di inizio dicembre 2021 l'attacco informatico all'ULSS 6 Euganea⁶, seguito, a partire dal 15 gennaio 2022, dalla pubblicazione dei dati sanitari nel dark web dapprima, in chiaro in alcuni siti esteri poi⁷. Il 7 gennaio 2021 un altro attacco cyber ha colpito l'ASL Napoli 3, con compromissione di circa

2 <https://ig.ft.com/how-much-is-your-personal-data-worth/>

3 https://www.kaspersky.it/about/press-releases/2021_indagine-kaspersky-il-50-degli-operatori-sanitari-italiani-non-usa-app-progettate-per-la-telemedicina-con-conseguenze-per-la-sicurezza-dei-dati-dei-pazienti

4 https://www.kaspersky.it/about/press-releases/2021_kaspersky-previsioni-minacce-informatiche-e-2022-machine-learning-attacchi-ics-difficili-da-rilevare-e-vulnerabilita-nel-settore-sanitario

5 https://roma.corriere.it/notizie/cronaca/21_settembre_13/roma-attacco-hacker-all-ospedale-san-giovanni-gravi-danni-attivita-6641a5fc-14a9-11ec-ba57-c9ba96e5a256.shtml

6 <https://www.padovaoggi.it/cronaca/attacco-hacker-ulss-6-euganea-padova-11-dicembre-2021.html>

7 https://www.ilgazzettino.it/nordest/padova/attacco_hacker_ulss_euganea_pubblicati_file_rubati_ultime_notizie_oggi_16_gennaio_2022-6442853.html



il 90% dei dati presenti nel server dell'azienda sanitaria⁸. Già nell'aprile 2020, tuttavia, il Nucleo di Sicurezza Cibernetica, organo presieduto dal Prof. Roberto Baldoni, vicedirettore generale con delega cyber del Dipartimento delle Informazioni per la Sicurezza (e attuale direttore generale dell'Agenzia per la Cybersicurezza Nazionale), diffondeva l'allerta massima a fronte dei primi impattanti attacchi hacker agli ospedali italiani⁹. Del resto, le criticità delle reti e dei sistemi IT delle strutture sanitarie italiane sono un dato – ahimè – difficilmente contestabile: "Secondo gli analisti di Swascan, Cyber Security Company, che hanno condotto uno studio sulle criticità del settore sanitario, il 60% delle aziende del campione sotto esame rischiano il furto di dati sensibili ... Dallo studio è emerso che il numero totale misurato in potenziali vulnerabilità riscontrate per il settore è 942, così distribuite: 4 aziende (20% del campione) non sono vulnerabili, 4 aziende (20% del campione) hanno tra 1 e 25 potenziali vulnerabilità, 7 aziende (35% del campione) tra 26 e 50 e 5 aziende (25% del campione) con più di 50 e fino a oltre cento potenziali vulnerabilità"¹⁰. I dati personali sottratti a ospedali e strutture sanitarie sono di grande interesse per il commercio criminale nel dark web; si tratta, oltre che di dati identificativi (nome, cognome, data e luogo di nascita, indirizzo di posta elettronica, recapito telefonico, numero di tessera sanitaria, codice fiscale), anche di altri dati, tra cui pure dati sensibili: informazioni relative a patologie presenti o pregresse o a trattamenti terapeutici in corso, dati assicurativi, dati relativi all'impiego, attestati, certificazioni o altri documenti. Dati che possono essere comprati nel mercato nero del web per essere poi utilizzati per perpetrare di-

verse tipologie di frodi: dalle false fatture finalizzate alla richiesta di rimborsi o indennizzi alle compagnie assicuratrici, alla prescrizione di esami diagnostici o di farmaci (in quest'ultimo caso, normalmente introvabili o molto costosi), senza contare il loro indubbio interesse – come si è già sopra scritto – per imprese che vogliano orientare scelte commerciali o di consumo o che siano interessate a ideare nuove strategie di marketing.

Lo strumento utilizzato per penetrare i sistemi delle strutture sanitarie ed esfiltrarne i dati è, ancora una volta, il ransomware.

I ransomware sono virus malevoli che consentono ai criminali informatici di appropriarsi della rete di un'azienda o di un ente, di criptarne i dati e poi di chiedere alla vittima una somma in denaro (normalmente in cryptovaluta) per restituire i file. Secondo il Clusit¹¹, l'Associazione Italiana per la Sicurezza Informatica, i ransomware sono stati usati nel 42% degli attacchi mondiali gravi, in quasi un terzo di questi c'è stata la richiesta di denaro. Secondo una ricerca di Kaspersky condotta su 15.000 persone in tutto il mondo, il 33% degli italiani che ha subito un attacco ransomware ha dichiarato di aver perso quasi tutti i suoi dati. Indipendentemente dal fatto che abbia pagato o meno, solo l'11% delle vittime è stato in grado di ripristinare tutti i file criptati o bloccati dopo l'attacco. Il 17%, invece, ne ha persi solo alcuni mentre il 22% non è riuscito a recuperarne una quantità significativa¹². Il ransomware si palesa e si riconosce con facilità, in quanto la schermata del computer risulta occupata da un avviso: l'utente viene informato che i suoi dati sono inutilizzabili e che potranno essere

8 https://www.ansa.it/campania/notizie/2022/01/21/hackers-chiedono-due-riscatti-ad-asl-na-3-sud_cdf5bfae-06bc-4712-aa4b-62787d307467.html

9 <https://www.corrierecomunicazioni.it/cyber-security/lallarme-dellintelligence-attacchi-hacker-alla-sanita-coinvolto-lo-spallanzani/>

10 https://www.ansa.it/canale_saluteebenessere/notizie/sanita/2021/09/22/cybersecurity60-aziende-sanita-italiane-rischia-furto-dati_9061c5f9-e1db-4d73-be05-289632497cbd.html

11 Rapporto Clusit 2021 sulla sicurezza ICT in Italia <https://clusit.it/rapporto-clusit/>

12 1° aprile 2021 ANSA -https://www.ansa.it/sito/notizie/tecnologia/software_app/2021/03/31/world-backup-day4-italiani-su-10-pagano-riscatti-ransomware_98332894-dbb5-4553-8a7f-ef5fd03f5a98.html#:~:text=il%2031%20marzo%20giornata%20sensibilizzazione%20sulla%20sicurezza%20dei%20dati&text=Quattro%20italiani%20su%20dieci%20hanno,grado%20di%20recuperare%20i%20documenti.

recuperati soltanto dopo il pagamento di un riscatto, che, solitamente, viene richiesto in criptovaluta (*Bitcoin*). Essenzialmente, esistono due operatività maligne:

- alcune forme di *ransomware* bloccano il sistema e intimano all'utente di pagare un riscatto per sbloccare il sistema stesso;
- altre invece cifrano i file dell'utente, chiedendo di pagare un riscatto per riportare i file cifrati in chiaro.

Questa nuova forma di estorsione si era inizialmente diffusa in Russia. Ora, gli attacchi *ransomware* sono perpetrati in tutto il mondo e sono diventati il nuovo strumento della criminalità organizzata per "raccolgere il pizzo", ovvero effettuare vere e proprie estorsioni su scala globale con il minimo rischio di esposizione umana, nonché per riciclare denaro su scala internazionale. In quest'ultimo caso vengono sfruttate, come copertura, aziende o enti che, paradossalmente, si occupano proprio di cyber security e che, di fatto, offrono servizi di decriptazione dei file ma che, in realtà, mascherano le trattative con gli hacker dirette a favorire il pagamento dei riscatti in criptovaluta, per poi fatturare al cliente, come servizio, anche l'avvenuto pagamento del riscatto.

Le modalità con cui viene sferrato un attacco *ransomware* sono sostanzialmente le medesime usate per gli altri tipi di attacchi informatici:

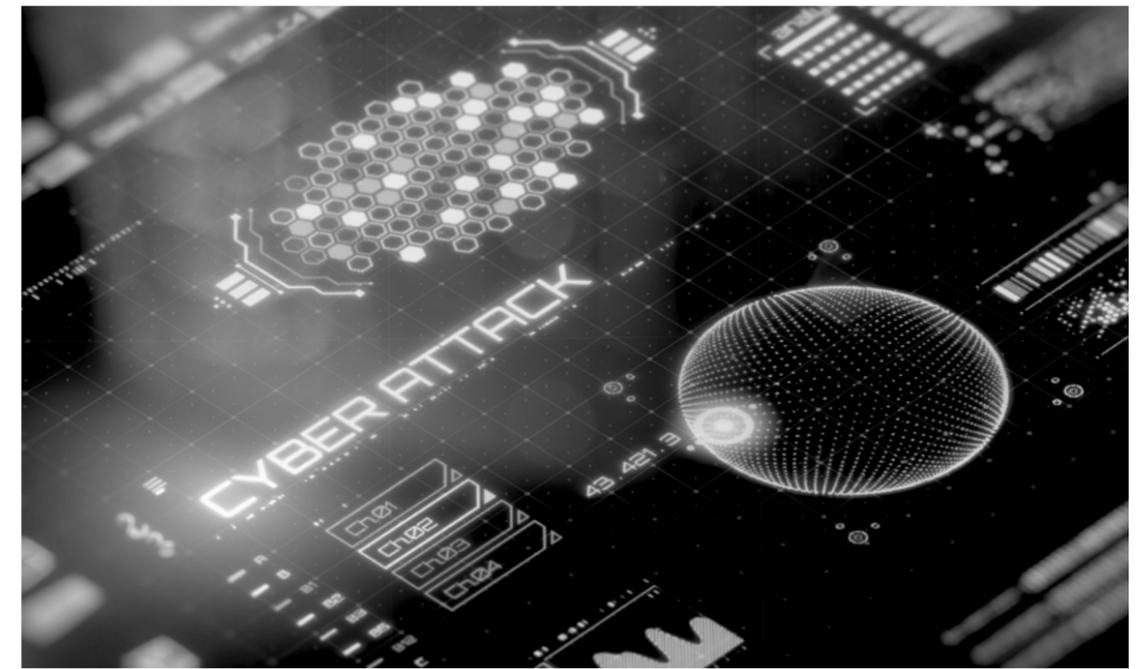
- l'invio di e-mail di *phishing* è ancora diffuso; attraverso questa tecnica, con la quale vengono veicolati oltre il 75% dei *ransomware*, l'utente, se non adeguatamente informato e formato sui rischi *cyber*, viene indotto a cliccare su un link o ad aprire un allegato, i quali fanno penetrare il virus nel sistema informatico;
- purtroppo, non sono rari neppure i casi di *ransomware* veicolati usando un supporto rimovibile, per esempio una chiavetta USB oppure un cavo contenenti il software malevolo; questa tecnica fa leva sul fattore umano, oltre che sulla carenza di informazione e formazione sui rischi *cyber*; le persone sono naturalmente curiose e non è insolito che raccolgano chiavette USB o colleghino il computer o lo smartphone ad un cavo di ricarica lasciati incustodi-

ti in spazi comuni (ingresso dell'azienda, mensa, parcheggio, aeroporti, stazioni ferroviarie ecc.); in questo caso, il *malware* si attiverà appena la chiavetta USB sarà inserita nel computer, oppure appena il cavo di ricarica sarà collegato al computer o al telefono;

- il *ransomware* può essere veicolato anche attraverso altri software, che vengono scaricati dal web e che sono, per lo più, gratuiti e, come tali, possono nascondere più di qualche insidia;
- vi sono, infine, tecniche di attacco che sfruttano le vulnerabilità di una rete o di un sistema informatico; si pensi all'attacco del marzo 2021 che ha utilizzato vulnerabilità di Microsoft Exchange Server (software che aziende e organizzazioni in tutto il mondo utilizzano per gestire e-mail e calendari) per distribuire *ransomware* dopo la compromissione dei server.

La kill-chain tramite la quale un attacco *ransomware* coglie nel segno la vittima, è normalmente costituita dalle seguenti fasi:

- Accesso alla rete aziendale: avviene tipicamente attraverso una campagna di e-mail di *phishing* attraverso la quale si installa il software malevolo (*malware*) sul pc della vittima.
- Infezione: l'esecuzione di questo *malware* permette all'attaccante di carpire le credenziali e diffondere l'infezione all'interno dell'organizzazione.
- Acquisizione di privilegi elevati: il *malware*, aggirando facilmente i meccanismi di difesa presenti sul dispositivo colpito, riesce ad impersonare utenti con maggiori privilegi di accesso ai sistemi (e.g. Amministratori di sistema, IT Manager).
- Movimento laterale: gli attaccanti, in modo silente, si muovono liberamente all'interno dell'infrastruttura aziendale. In questo caso è necessario analizzare l'intera infrastruttura telematica, assumendo che proprio l'intera infrastruttura informatica (pc client, server, apparati di rete e dispositivi connessi) sia stata compromessa.
- Cifratura dei dati: a questo punto viene scaricato il *ransomware* che si occupa della codifica di tutti i file aziendali, del blocco dei sistemi e della richiesta di riscatto. I gruppi hacker che utilizzano il *ransomwa-*



re pubblicano i dati trafugati su Internet finché il riscatto non viene pagato. Oltre al danno di immagine che ne consegue, se i dati pubblicati sono dati personali, si rende necessaria la notifica all'Autorità Garante della Privacy.

I *ransomware* hanno lo stesso meccanismo di diffusione di qualsiasi altro virus. Gli antivirus stanno introducendo strumenti sempre più sofisticati per cercare di arginare questi attacchi ma i risultati, almeno per ora, tardano a vedersi. Una possibile soluzione potrebbe arrivare da un approccio alternativo al problema, un "vaccino" per i *ransomware*: studiando i dati raccolti, si è compreso che i *ransomware* lasciano una sorta di marcatore sui computer che infettano. In altre parole, il *ransomware*, quando si installa su un computer, lo "marchia" in modo che venga riconosciuto. Il "vaccino" per i *ransomware* inserisce un marcatore che inganna il *malware*, facendogli credere che il computer sia già stato infettato: in questo modo il computer viene ignorato dal *malware*. I marcatori vengono aggiornati periodicamente via Internet per adattarsi agli eventuali cambiamenti introdotti dai *cyber-criminali*. Oltre a ciò, comunque, per garantire la piena sicurezza dei dati trattati, l'azienda sanitaria o la struttura ospedaliera dovrà applicare tutte le consuete misure

di sicurezza tecnico-organizzative conformi all'art. 32 GDPR:

- Monitoraggio e aggiornamento continuo della protezione dei sistemi dalle vulnerabilità, comprendendo qui la conoscenza completa e aggiornata dei sistemi hardware e software in essere e il relativo controllo costante.
- Procedure di backup e, soprattutto, di *restore* che siano testate e affidabili, il che include la piena conoscenza dei processi e dei dati gestiti (molto difficile da ottenere e mantenere al crescere delle dimensioni dell'organizzazione); in particolare, è vitale il backup dei dati, cioè copie funzionanti e recenti (non è così scontato, purtroppo) dei propri file. Il backup dei dati dev'essere un'attività pianificata secondo la *security by design* e non può essere affidata alla "buona volontà" di un operatore. Dovrà prevedere sempre la "ridondanza": non una sola copia di backup, ma almeno tre copie secondo la basilare regola 3-2-1. In pratica: tre copie di ogni dato che si vuole conservare, di cui due copie "on-site" ma su storage differenti (HD, NAS, Cloud ecc.) e una copia "off-site" (in sito remoto, ad esempio su Cloud, nastri ecc.). In questo modo, se il *ransomware* dovesse infettare il sistema, una copia dei dati rimarrebbe pro-

tetta, dando all'organizzazione l'opportunità di ripristinarli. Altrettanto importante è la protezione del backup, che deve essere isolato e non accessibile da un qualsiasi utente collegato in rete.

- Formazione e informazione agli utenti, affinché non cadano nelle trappole del *phishing*, il vettore più usato per questo tipo di minaccia; in realtà, la consapevolezza costantemente aggiornata degli utenti potrebbe essere lo strumento migliore per affrontare minacce di questo tipo: negli ambiti tecnologici, il fattore umano è spesso sottovalutato, nel bene e nel male.

Ciò significa che anche le strutture ospedaliere e sanitarie devono dotarsi di una *Privacy Policy* realmente efficace, nel contesto della quale il Titolare del trattamento definisca:

- i dati personali trattati (precisamente, da suoi dipendenti, collaboratori, consulenti) e le relative modalità di trattamento;
- le responsabilità e le modalità con cui gestire la protezione dei dati personali secondo i principi della *data protection by design and by default* (art. 25 Regolamento UE 2016/679 - GDPR), della responsabilizzazione (art. 5 co. 2 Regolamento UE 2016/679 - GDPR), oltre che sulla base dei principi di liceità correttezza e trasparenza (art. 5 co. 1.a Regolamento UE 2016/679 - GDPR), limitazione della finalità (art. 5 co. 1.b Regolamento UE 2016/679 - GDPR), minimizzazione dei dati (art. 5 co. 1.c Regolamento UE 2016/679 - GDPR), esattezza (art. 5 co. 1.d Regolamento UE 2016/679 - GDPR), limitazione della conservazione (art. 5 co. 1.e Regolamento UE 2016/679 - GDPR), integrità e riservatezza (art. 5 co. 1.f Regolamento UE 2016/679 - GDPR);
- le procedure tecnico-organizzative e relative modalità di gestione, al fine di garantire un livello di sicurezza per i dati personali trattati in formato elettronico e cartaceo o con altri mezzi di trattamento, che sia adeguato ai rischi in conformità all'art. 32 del Regolamento UE 2016/679 - GDPR;
- le attività dirette a consentire e rendere effettivo l'esercizio dei diritti attribuiti agli interessati dal Regolamento UE 2016/679 - GDPR e, occorrendo, dal D.Lgs. 196/2003

e, dunque, a titolo meramente esemplificativo, il diritto di informazione e accesso ai propri dati personali, il diritto alla rettifica ed alla cancellazione ("diritto all'oblio"), il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati e, ove previsto, il diritto all'opposizione al trattamento;

- ogni iniziativa assunta per fornire informazione ed erogare formazione sulle disposizioni normative in materia di protezione dei dati personali e sui contenuti, concreti ed operativi, della *Privacy Policy* adottata.

Il Titolare del trattamento deve, dunque, prefiggersi di operare nel pieno rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, con specifico riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati, comunque assicurando l'applicazione dei principi sopra enunciati sulla base di un'attenta valutazione sostanziale – e non formalistica – delle garanzie previste, nonché di un'analisi della quantità e qualità delle informazioni utilizzate e dei possibili rischi connessi al relativo trattamento, al fine di prevenire ed evitare qualsivoglia violazione dei dati personali, tanto più se si tratta di dati sensibili (quali, certamente, sono i dati sanitari). In questo contesto, il Titolare del trattamento deve provvedere a definire una gerarchia di responsabilità e competenze in relazione alla protezione dei dati personali, individuando tra i propri dipendenti o collaboratori o consulenti soggetti che siano capaci ed affidabili, a cui delegare, in tutto o in parte, la gestione (applicazione, verifica, implementazione) delle procedure di protezione dei dati.

Si ricorda che, allorché si parla di dati personali con riferimento alle strutture sanitarie, ci si riferisce pur sempre a dati forniti da utenti e pazienti, fornitori di beni e di servizi, nonché da dipendenti e collaboratori, ai fini della erogazione dei servizi richiesti e dell'adempimento degli obblighi di legge. Si tratta di dati identificativi ma pure di dati sensibili (tra i quali, appunto, i dati personali idonei a rivelare lo stato di salute e la vita sessuale e quelli attinenti alla salute fisica o mentale di una persona

fisica), che il Titolare del trattamento tratta in occasione o nell'ambito delle attività svolte. Sono dati trattati utilizzando supporti non elettronici (= cartacei), nel qual caso i dati devono essere conservati in archivi chiusi a chiave o in apposite stanze dotate di serratura oltre che in apposite casseforti, così come supporti elettronici, precisamente personal computer o server con accesso tramite dispositivo elettronico di sicurezza e dotati di programmi antintrusione e antivirus, oltre che configurati cosicché l'accesso contemporaneo con una stessa User-ID non sia consentito e i supporti non utilizzati vengano cancellati. Va da sé che, per regolare questi specifici e concreti trattamenti dei dati, il Titolare del trattamento dovrà predisporre – e periodicamente aggiornare – un regolamento interno per la *Data Protection* e l'utilizzo dei sistemi di *Information Communication Technology*. La bontà delle misure adottate dovrà peraltro essere periodicamente verificata a cura del Titolare del trattamento, il quale, a tal fine, dovrà auspicabilmente avvalersi di consulenti e tecnici esterni, esenti da conflitti d'interesse.

Obiettivo primario delle misure tecnico-organizzative adottate dal Titolare del trattamento e sopra sintetizzate è assicurare che anche gli eventuali soggetti nominati quali Incaricati del trattamento o Responsabili del trattamento si impegnino a garantire che i dati personali degli interessati siano:

- trattati in modo lecito, corretto e trasparente;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (c.d. minimizzazione dei dati);
- esatti e, se necessario, aggiornati, peraltro impegnandosi il Titolare del trattamento ad assicurare che siano adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- 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;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principi della integrità e riservatezza).

Naturalmente, nel caso in cui, nonostante le misure di sicurezza adottate, si verifici una violazione di dati personali nell'ambito delle operazioni di trattamento effettuate dal Titolare del trattamento (*data breach*), il Regolamento UE 2016/679 - GDPR prevede che il Titolare debba notificare la violazione all'autorità di controllo compe-



tente entro 72 ore da quando ne è venuta a conoscenza e, quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, anche all'interessato senza ingiustificato ritardo. Tra i possibili incidenti, che possono causare violazioni dei dati personali, si ricordano a titolo esemplificativo:

- perdita o furto di strumenti IT (pc, smartphone, chiavette USB, hardware);
- rivelazione di informazioni a soggetti non autorizzati;
- accesso non autorizzato ai dati personali;
- violazione delle misure di sicurezza fisiche dei locali dove i dati personali sono archiviati;
- caricamento/divulgazione per errore di dati personali in rete;
- errore umano (per esempio: perdita di dati personali archiviati presso luoghi non sicuri);
- mancata previsione di eventi di rischio per la sicurezza dei dati quali allagamenti o incendi;
- attacco esterno ai sistemi IT aziendali;
- reati informatici.

Ebbene, per il caso in cui si verifichi una tale violazione, il Titolare del trattamento dovrà approntare una specifica procedura, al fine di assicurare una gestione controllata, strutturata ed efficace degli incidenti e prevenire il verificarsi di altre violazioni.

Si consideri che, a seconda della tipologia

di vittima dell'attacco informatico (organizzazione pubblica o privata, utente privato), il danno derivante dalla indisponibilità, temporanea o permanente, dei dati compromessi può avere conseguenze e costi più o meno rilevanti, a seconda della importanza "strategica" dei dati stessi. Un'azienda pubblica o un'azienda sanitaria, che erogano servizi ai cittadini, si troveranno praticamente bloccate nella operatività quotidiana e, se poi gestiscono servizi urbani, l'intero territorio di riferimento si troverà a scontare le conseguenze dell'attacco informatico. Se ad essere colpita fosse una infrastruttura critica, che fornisce beni e/o servizi essenziali per il Paese (si pensi ai settori dell'energia, dei trasporti, della sanità), in cui i sistemi e le reti sono preposti alla gestione e al controllo di apparecchiature fisiche (macchinari sanitari, pompe e sistemi di chiuse di dighe ed acquedotti, semafori e torri di controllo, ecc.), le conseguenze di un attacco informatico potrebbero essere drammatiche, se non tragiche. Non è un caso che siano proprio le aziende sanitarie ad essere state bersagliate, negli ultimi mesi, dagli attacchi *ransomware*: lo scopo dei criminali è danneggiare quanto più possibile, per indurre le vittime a pagare il riscatto. In questo contesto, la migliore protezione è la prevenzione, come sopra proposta.



L'attività di verifica applicata all'ambito *data protection*

di Eleonora Fasoli

Che cos'è un audit

L'audit è uno strumento volto a verificare, in diversi ambiti, l'adeguata definizione e il rispetto di regole, procedure e norme da parte del soggetto sottoposto a vigilanza. L'audit è un processo di valutazione indipendente, sia che si svolga a livello interno sia esterno alla realtà aziendale, da svolgere periodicamente sulla base di un perimetro ben definito, finalizzato a raccogliere evidenze, relativamente ad un determinato contesto di analisi. Grazie all'attività di verifica, l'Azienda è in grado di classificare con obiettività l'adeguatezza del sistema vigilato e la conformità allo schema d'audit, ossia il raggiungimento dei criteri stabiliti e richiesti dalla normativa.

L'audit è lo strumento più importante per valutare se i requisiti siano applicati in modo coerente nell'ambito dei processi aziendali e se il sistema (di gestione, di adeguamento,...) produca i risultati prestabiliti. I sistemi di gestione, in concreto, nascono per limitare il rischio che l'organizzazione non raggiunga i propri obiettivi, attraverso un efficace governo dei propri processi e delle attività.

Una tipologia di rischio aziendale, ora, è quella che deriva dalla mancata conformità, intesa come mancata osservanza delle leg-

gi, delle linee guida e delle norme tecniche vincolanti per mancata conoscenza o consapevole o involontaria omissione. All'inservanza, anche involontaria (che equivale a mancata padronanza del processo), possono conseguire sanzioni, perdite finanziarie e danni da reputazione.

Anche la normativa GDPR, nella sua articolata definizione, impone l'esigenza di valutare periodicamente il rispetto del processo di adeguamento: l'articolo 39 del GDPR lo pone fra i compiti del DPO (Responsabile della Protezione dei Dati). Nel caso di non conformità alla normativa, posta a tutela della protezione dei dati personali, il rischio sarà quello di subire una sanzione, un reclamo, una segnalazione, una richiesta di risoluzione contrattuale per inadempimento, un esborso economico per fronteggiare le richieste del Garante a seguito di ispezione.

Perché svolgere un audit

Il principio di "*accountability*" (responsabilizzazione) richiede che il titolare del trattamento sia "da un lato" responsabile del rispetto della normativa, applicabile in materia di protezione dei dati personali, e, dall'altro, in grado di dimostrare (all'autorità, agli organi di vigilanza e controllo, ai clienti, ai partner commerciali, ai dipendenti ...),

concretamente, la conformità del proprio contesto. Il nuovo concetto di "accountability" fa leva proprio sulla "capacità di dimostrare" e sulla verificabilità dell'azione. La responsabilità assunta dal Titolare e il dovere di dimostrare sono elementi essenziali di una buona governance (WP Art. 29 parere n. 03/2010) e, pertanto, l'esecuzione periodica di attività di vigilanza, supportata da documentazione di evidenze, agevola nella dimostrazione all'autorità e ad eventuali terzi di essere in linea con i precetti normativi.

Prerogativa del titolare è l'obbligo di saper dimostrare di aver messo in atto tutte le misure necessarie a garantire la conformità al GDPR (art. 25). Tale obbligo si declina in molteplici profili: solo a titolo esemplificativo, nella redazione e mantenimento di un registro dei trattamenti (art. 30 GDPR), nella gestione consapevole dei consensi, ricevuti dagli interessati per fondare, in casi specifici, il trattamento dei loro dati (art. 7 GDPR) e nella tenuta di un registro *data breach*, a dimostrazione di saper riconosce-

re, mappare e attuare tutti i rimedi a tutela degli interessati, impattati dall'incidente di sicurezza.

Al fine di dare attuazione al principio di *accountability*, il titolare dovrebbe adottare anche un proprio modello di gestione, organizzazione e, non meno importante, controllo privacy. Circa quest'ultimo, il titolare sarà in grado di avere il controllo del rischio, insito nei trattamenti svolti o demandati a soggetti esterni, dell'adeguatezza alle richieste normative nazionali ed europee e dell'idoneità delle misure tecnico-organizzative applicate, le quali, si ricorda, non costituiscono un adempimento fisso e statico, ma garantiscono un livello di sicurezza adeguato al rischio, per cui necessitano di continue verifiche. La mancanza di evidenze implica, di per sé, una non conformità e violazione al principio di *accountability* e, quindi, rappresenta un primo spunto di rilievo in sede di verifica ispettiva.

Una disciplinata programmazione di controlli di conformità rappresenta, quindi:

1. uno strumento di tutela del titolare del



trattamento, rispetto a richieste di evidenze specifiche, dalle quali possono scaturire sanzioni o richieste di risarcimenti di danni da parte di terzi. Attraverso l'audit, e cioè verificando il livello di conformità al sistema di gestione e alla normativa *data protection*, è possibile individuare tempestivamente e correggere eventuali vulnerabilità e criticità nella propria attività aziendale;

2. uno strumento di *accountability* a disposizione e supporto del titolare del trattamento. La verifica, infatti, contribuisce a documentare la progettazione (*by design*) e il percorso di adeguamento, nonché a creare nuovi stimoli di conoscenza, acquisendo preventivamente le informazioni e i fattori di rischio;

3. uno strumento di attuazione degli obblighi di sorveglianza e controllo in capo al DPO.

Con quale scopo condurre un audit

Così come accade per gli altri ambiti di *compliance*, per la tutela della sicurezza nei luoghi di lavoro, per l'ambiente, per la qualità, l'auditor deve definire, a priori, gli obiettivi in forma chiara e condivisa con il management aziendale di riferimento.

Nell'ambito della protezione dei dati, lo scopo di un audit si può rinvenire nelle esigenze di:

- verificare il livello di conformità alla normativa vigente;
- verificare la conformità dei processi alle *policy data protection*, alle procedure e ai regolamenti (es. audit su uno specifico dipartimento);
- accertare il livello di conformità al GDPR di un fornitore di servizi, che tratti dati per conto del titolare (es. un *customer care* in *outsourcing*, il consulente del lavoro che elabora le buste paga, ...), al fine di valutare il mantenimento nel tempo e il rispetto di quanto dichiarato nell'atto di designazione a responsabile, nonché l'adeguatezza ai requisiti richiesti dal sistema di gestione privacy, in uso all'azienda (es. audit periodico sui fornitori);
- accertare l'efficacia di azioni correttive, intraprese a seguito di rilevate "non conformità", scaturite da un precedente audit di verifica o a seguito di incidenti di sicurezza.

Chi è l'auditor e chi conduce la verifica

L'auditor è la persona che possiede caratteristiche tecniche e specialistiche; dovrà, quindi, per l'ambito *data protection*, essere un esperto sia a livello giuridico che informatico (motivo per cui si favorisce una trasversalità di competenze, articolate anche fra diversi professionisti).

In quanto vigilante e giudicante, l'auditor possiede le medesime caratteristiche spettanti ai professionisti del giudizio (magistrati), deve essere oggettivo, imparziale e, soprattutto, non deve avere conflitti di interesse e ruolo con l'oggetto dell'audit. In pratica, non deve avere responsabilità dirette con l'organizzazione o con il reparto, interessato dall'attività di valutazione, per la regola generale che chi controlla non può identificarsi nel controllato.

Passando ad abilità attitudinali, l'auditor deve possedere capacità comunicative, di gestione delle risorse, abilità di indagine e tecniche persuasive, per garantire l'acquisizione di informazioni complete e di conoscenza non soltanto degli ambiti proceduralizzati, ma, nell'interesse dell'azienda, di prassi e consuetudini operative, talvolta non ufficiali.

Fondamentale è lo spirito di osservazione e la capacità di giungere tempestivamente a conclusioni basate sull'analisi e su ragionamenti logici. Un aspetto sempre apprezzato, in questo genere di attività, attiene alla ponderazione nell'emettere giudizi, condanne e primeggiando proposte innovative, soluzioni attuabili e cambi di prospettiva di sguardo.

La verifica può essere svolta, ad esempio, da un *privacy officer* interno, o dalla funzione di internal audit, riservando, nei casi in cui sia nominato, al DPO, il compito di contribuire alla definizione del piano di verifiche e delle misure da adottare all'esito del rapporto, oppure, chi non disponesse di tale funzione di controllo interno, può attribuire tale compito direttamente al DPO o ad un consulente esterno.

Sicuramente, la scelta più efficace è quella di individuare un gruppo multidisciplinare con professionisti, che garantiscano competenze di *advisory* nonché *legal* e *security*, ognuno dei quali possa contribuire in

modo specifico, a seconda dell'ambito di analisi.

Gli altri attori fondamentali per l'audit

La Direzione: ha un ruolo fondante sia come fattore promuovente, sia come primo destinatario dell'audit. Solo a titolo esemplificativo, la Direzione approva la pianificazione delle attività e il piano d'audit, stabilisce il budget per l'esecuzione, rende disponibili le risorse da impiegare e formare, acquisisce e trasforma in azioni eventuali rilievi e non conformità.

Il Responsabile del programma di audit: è la figura di riferimento per coordinare le attività inerenti alla pianificazione e gestione delle interviste, della raccolta documentale e organizzazione dei sopralluoghi.

Quale metodologia seguire per condurre un audit

Il titolare, il DPO o l'auditor possono decidere liberamente quale metodologia utilizzare per svolgere l'attività di verifica. Non a caso, parte della dottrina, per tale genere di attività, preferisce parlare di attività di controllo, in quanto non tutte le attività protese all'ispezione e alla verifica rientrano in uno schema d'audit (certificato).

Naturalmente, esistono metodologie di verifica "ufficiali"; le norme tecniche e gli standard di certificazione in tali casi sono emessi da enti di riferimento nel panorama internazionale, europeo o nazionale:

- ISO – International Standards Organization;
- IEC –International Electrotechnical Commission;
- CEN – Comitato europeo di normazione;
- UNI – Ente nazionale di unificazione.

In tal senso, la norma UNI EN ISO 19011-Linee Guida per la conduzione di Audit di Sistema di gestione, fornisce, ad esempio, una guida per condurre e verificare l'implementazione e l'efficacia di un sistema di gestione.

Tale schema è applicabile a qualsiasi organizzazione, che voglia o abbia l'esigenza di pianificare e condurre audit interni o esterni su sistemi di gestione, quale guida nell'impostazione dei programmi di audit, nella conduzione, nella valutazione delle competenze delle persone coinvolte nel

processo e nella definizione dei rilievi conclusivi.

La conduzione di un audit

La corretta gestione di un'attività di verifica prevede la formalizzazione anticipata di un piano di audit, dove definire:

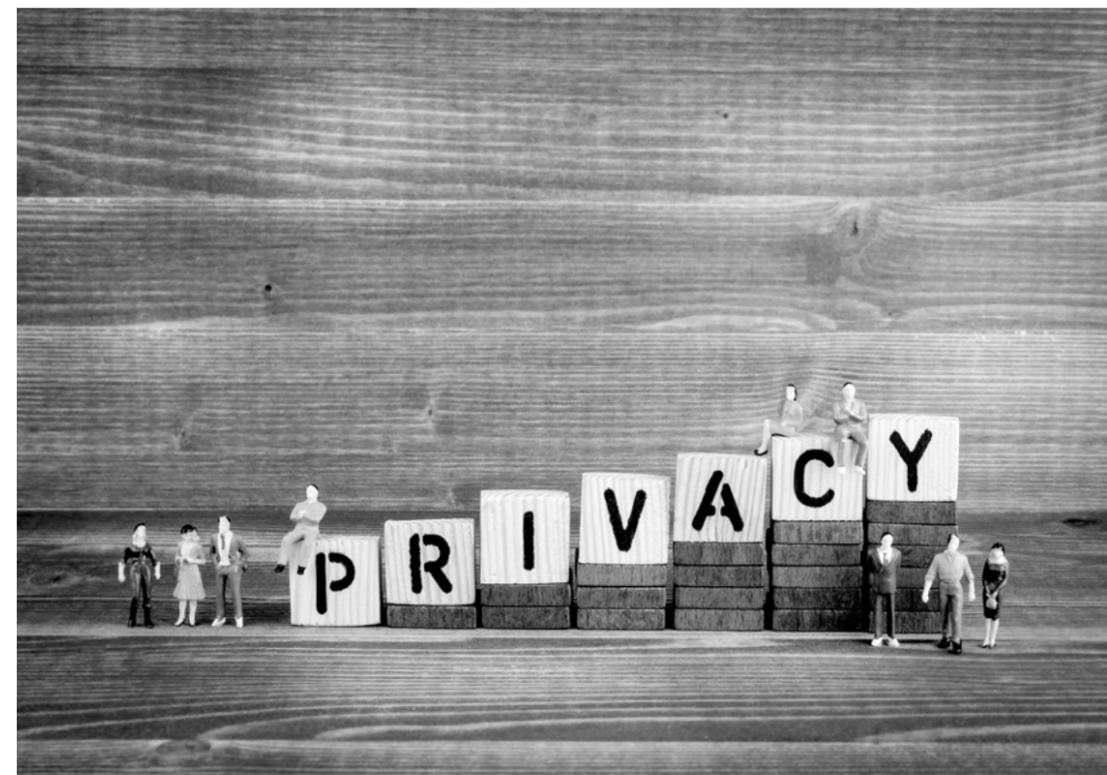
- gli obiettivi;
- i criteri che verranno adottati;
- i parametri di riferimento per raggiungere gli obiettivi (ad. esempio policy, regolamenti interni, procedure operative, ecc.);
- il perimetro e le risorse/uffici coinvolti;
- l'agenda;
- il tempo stimato per le specifiche verifiche: ciò consente di allocare correttamente le risorse interne che dovranno essere coinvolte nell'attività di verifica;
- la check list di domande da compilare privatamente nel corso della verifica: tale strumento fondamentale per l'auditor costituisce un supporto operativo, utile a raggiungere il giusto livello di approfondimento e di indagine.

Tale piano viene condiviso, durante una riunione di apertura con i referenti del progetto, prima di iniziare l'attività di audit, per consentire la comprensione delle attività che si andranno a svolgere e l'organizzazione pratica.

La conduzione della verifica prevede la raccolta e la verifica delle informazioni attraverso attività di osservazione diretta del processo, ausiliata dall'esame documentale (policy, regolamenti, procedure interne, documentazione di programmazione, contratti, ...) e da interviste ai referenti del processo o ai responsabili delegati all'attività. Per tutti gli ambiti verificati, l'azienda deve essere in grado di fornire evidenze (quindi, produrre un campione verificabile).

Nel corso di un audit in ambito privacy è indispensabile verificare la presenza di:

- analisi dei rischi e misure di mitigazione;
- valutazione di impatto;
- registro dei trattamenti;
- informative e consensi;
- atti di designazione, ex art. 28 GDPR (responsabili e sub-responsabili del trattamento);
- nomine a soggetti interni;
- formazione;
- procedure (*data breach*, esercizio dei di-



ritti degli interessati, trasferte, lavoro da remoto, Covid-19).

Le verifiche in ambito privacy sono, quindi, caratterizzate dal dovere di controllare elementi formalizzati, vale a dire per i quali la normativa indica nel dettaglio sia i requisiti attesi (informative sulle modalità di trattamento, registri ex art. 30 GDPR, atti di designazione a responsabile del trattamento), sia i non formalizzati (misure di sicurezza, misure organizzative, analisi dei rischi e valutazioni di impatto, ...), cioè ove la responsabilità della concreta articolazione è in carico allo stesso titolare e varia a seconda del contesto, della tipologia di business, delle risorse economiche e del capitale umano a disposizione.

Gli audit possono riguardare, inoltre, temi specifici introdotti da provvedimenti o linee guida, che integrano la normativa primaria (ad esempio, amministratori di sistema, videosorveglianza, firma grafometrica, cookie), nonché aspetti tecnico-organizzativi del trattamento (profilazione, tempi di conservazione, modalità di esercizio dei diritti, qualità dei dati, *data breach*).

Al titolare del trattamento compete anche un'attività di verifica verso i soggetti di cui si avvale, ossia i soggetti che trattano dati personali per suo conto, ai sensi dell'arti-

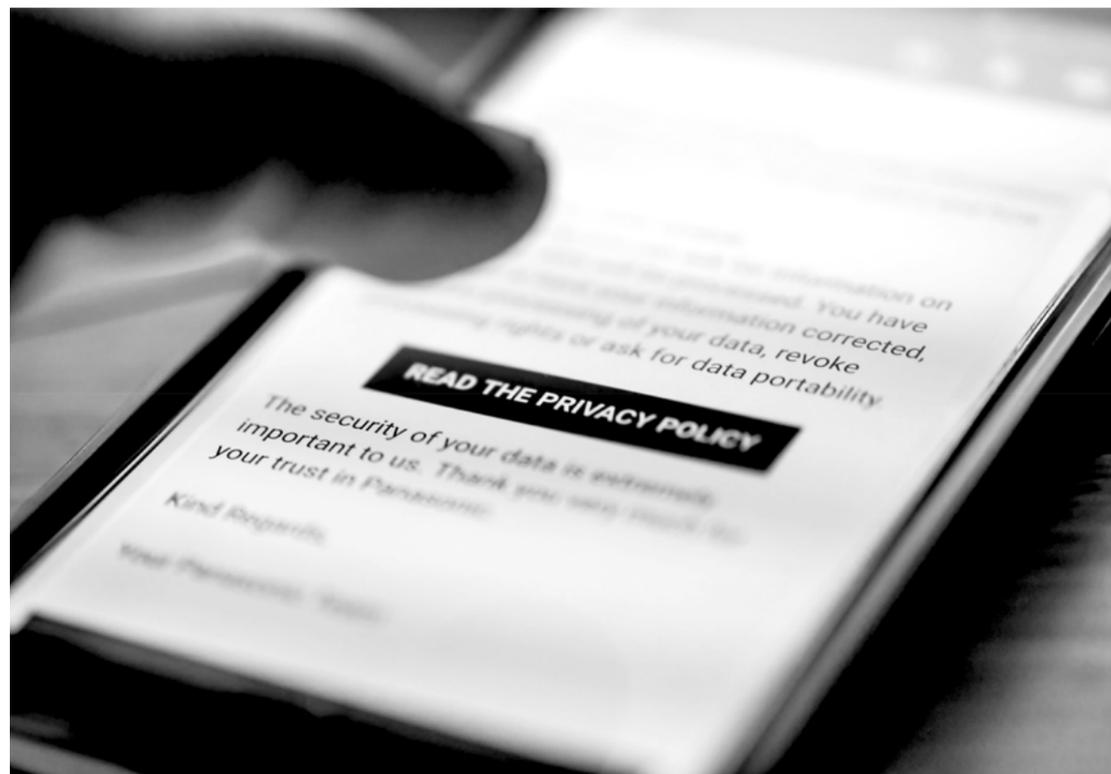
colo 28 GDPR: i responsabili e gli "altri responsabili" (sub responsabili). L'audit sui fornitori è una verifica doverosa e periodica: l'articolo 28 GDPR fornisce un elenco di specifiche, relativamente al responsabile del trattamento, per cui è implicito ci debba essere una verifica da parte del titolare sulla sussistenza e sul mantenimento di tali requisiti prima di avvalersi di un fornitore e in pendenza del rapporto contrattuale di durata.

All'esito della verifica dell'intero perimetro d'audit (conclusione check list), i risultati specifici e l'esito complessivo vengono documentati in un report, presentato al management dell'azienda in una riunione conclusiva. Nella produzione finale è possibile leggere i risultati, ottenuti dalla verifica, tramite una valutazione che traduce la distanza tra il profilo attuale e il profilo "modello".

Le risultanze dell'audit sono generalmente classificate in:

- non conformità (maggiori o minori);
- osservazioni/opportunità di miglioramento;
- commenti/raccomandazioni e suggerimenti.

L'attività d'audit, quindi, non si conclude né con una numerica né con un risultato di



idoneità; la conclusione dettagliata e precisa (rapporto d'audit) costituisce, però, un valido supporto per correggere o colmare le carenze rilevate.

Conclusioni

In conclusione, una corretta verifica o audit si basa su:

- professionalità;
- riservatezza;
- indipendenza;
- approccio basato sull'evidenza;
- comunicazione e rispetto di entrambe le parti.

Condurre un audit interno o sottoporsi ad un audit esterno può essere un compito complesso e stressante, indipendentemente dalle dimensioni della realtà aziendale. L'ampiezza del programma di audit, in termini di attività da svolgere, evidenze da raccogliere e risorse da ascoltare, dipende, invece, dalla complessità dell'azienda, dall'ampiezza del perimetro della verifica e dalla rilevanza dei trattamenti, connessi alla natura del business. Ciò nonostante, adottare un piano di verifiche documentate e preventive del proprio sistema di *data protection* ha un'importanza strategica in termini di *accountability* del Titolare e di

preparazione e difesa in caso di ispezioni dell'autorità di controllo.

Dal lato esterno, avere padronanza e verificare periodicamente i processi, dai quali origina il sistema di gestione privacy, ha un forte impatto sul mercato, garantendo la rispettiva competitività, attraverso un adeguato e sempre aggiornato livello di conformità al GDPR.

Infine, la fiducia nel processo di audit e la capacità di raggiungere gli obiettivi a posteriori dipende dalle competenze, professionalità e sensibilità delle risorse, coinvolte nella verifica. Le attività d'audit devono essere funzionali al raggiungimento degli obiettivi prefissati e, quindi, l'esecuzione di queste attività non dovrà essere un mero adempimento formale, una produzione di evidenze o la corsa alla scrittura della procedura, fine a sé stessa: un simile approccio non porta ai risultati e agli obiettivi prefissati. Al contrario, abituare l'azienda a trovare soluzioni che adeguano i processi alla normativa GDPR è stimolo, fattore di crescita e prova di capacità di analisi.



SEAC CONSULTING SRL

SERVIZI PER LA CRESCITA A 360°

Consulenza gestionale, compliance, evoluzione digitale

SEAC Consulting accompagna le piccole e medie imprese nella **crescita**, sviluppando i **nuovi processi aziendali** di budgeting e controllo di gestione, di accesso ai finanziamenti bancari ed agevolati, quelli di compliance e rispetto delle normative, integrando in essi anche l'adozione di soluzioni tecnologiche fornite da SEAC, per sfruttare al meglio la preziosa miniera di informazioni che SEAC possiede e che mette a disposizione, in modo sicuro e rispettoso, ai propri clienti.

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

di Pier Luca Toselli

Facendo seguito a quanto già evidenziato nella prima parte, riprendo il tema "La ricerca di documenti informatici", alla luce delle linee guida dettate dalla Circolare 1/2018 della Guardia di Finanza.

Relativamente alle "ricerche", a parere dello scrivente, oggi più che un tempo, divengono di grande rilievo, le cd. "attività propedeutiche al controllo", ormai sempre più strategiche ed indispensabili, nel tentativo, da un lato, di prevedere l'emersione nel corso del controllo di profili "penali", e dall'altro, di individuare quei "target" da sottoporre a particolare attenzione. Attesa l'elevata informatizzazione dei processi, impone di concentrare l'attenzione su specifici obiettivi, essendo di fatto ormai utopico, se non materialmente "impossibile" (in tempi ragionevoli), sottoporre a specifici accertamenti la complessiva mole di dispositivi e dati informatici presenti presso le aziende¹.

È necessario, pertanto, all'atto della ricerca, adottare ogni necessaria cautela ed attenzione per:

- assicurare un effettivo collegamento tra il dato e la sua utilità ai fini del controllo,

così da evitare acquisizioni indiscriminate di dati che potrebbero risultare, se non inutili, "ridondanti" rispetto la loro efficacia per gli esiti della verifica e anche lesive, o determinare limitazioni dei diritti di parti terze (consociati, affiliati etc.) estranei alle finalità del controllo;

- evitare che i verificatori, come purtroppo spesso accade, si ritrovino dinanzi ad imponenti quantità di dati che potrebbero, da un lato, evidenziare la loro inutilità o irrilevanza, ma anche non poter essere adeguatamente ed efficacemente esaminati nei tempi ordinari della verifica, oggi fissati generalmente a 30 giorni lavorativi, con conseguenze spesso lesive degli esiti del controllo, soprattutto sul piano del contenzioso che ne deriva (si pensi all'eventualità di dati non acquisiti e non esaminati che, in sede di contenzioso, potrebbero scriminare la condotta del contribuente sottoposto a controllo).

In via del tutto indicativa, non essendovi una regola e dipendendo fortemente non solo dalle caratteristiche dell'azienda ma anche dalla finalità del controllo e dall'esperienza accumulata dagli investigatori,

¹ La stessa circolare ha abbandonato il concetto di "verifica generale" che un tempo accompagnava quelle massive acquisizioni di dati che poi permettevano un analitico e generale controllo da parte degli investigatori circa il rispetto della normativa fiscale nella sua globalità. Attualmente, salvo rari casi, il controllo attiene ad uno specifico settore impositivo, se non un singolo o pochi fatti di gestione economica, ragion per cui se da un lato non ha più senso procedere ad acquisizioni "massive", dall'altro assume maggior rilevanza ed importanza strategica l'ispezione o la ricerca, che deve essere così efficace ed efficiente da riuscire ad individuare, nelle "mole" complessive di dati, quali possono risultare "utili" per le sorti e le finalità del controllo in corso, riuscendo contemporaneamente ad espungere dallo stesso i dati irrilevanti;



il "dove" effettuare le ricerche può essere costituito da: supporti informatici fisici (cd, dvd, *hard-disk* esterni, chiavi usb, ecc.); dati presenti negli *hard-disk* degli elaboratori, ricomprendendo in tale tipologia anche i *server* e *NAS* comunque raggiungibili attraverso la rete aziendale; *smartphone* ed altri dispositivi "mobile" aziendali; macchine virtuali e spazi *cloud* comunque utilizzati a livello aziendale. Si rileva *prima facie* come non esista un "numero chiuso" di dispositivi e luoghi ove concentrare le ricerche; talvolta, anche un semplice lettore musicale di mp3, può rilevarsi un contenitore di dati che potrebbero rilevarsi "strategici" per gli esiti del controllo.

Per quanto attiene i fenomeni *cloud* e "virtualizzazione", in continuo e veloce sviluppo, viene posto l'accento sulla necessità di estendere le ricerche a tutti i sistemi di gestione remota o virtualizzazione dei dati, in quanto, sovente, l'esperienza ha evidenziato come le cd. "contabilità parallele"/"contabilità in nero" etc. trovino gestione e conservazione su sistemi di tale tipologia, nell'intento, da parte del contribuente, di

occultarle alle ricerche degli investigatori, ma anche di poterle più facilmente gestire in termini di modifica e distruzione in caso di controlli². Particolare attenzione va, quindi, riposta alla presenza di macchine virtuali (ormai sempre più diffuse ed utilizzate) ed anche a quei *software* utilizzati per le cd. "connessioni remote" (*VNC*, *TeamViewer*, *Supremo*, *LogMeIn*, *Parallels Acces*, *AnyDesk* etc.). Medesime considerazioni possono poi estendersi a quei sistemi di *cloud storage* che, proprio perché "esterni" all'azienda, ben si prestano alla gestione e conservazione di contabilità parallele occulte. L'uso di tali sistemi, oltre che da più o meno evidenti "icone", può essere rilevata anche attraverso l'identificazione di specifici *artifacts* contenuti all'interno della postazione utilizzata e dalla rilevazione di pagine *web* aperte sui predetti portali (si pensi a *GDRIVE*, *DROPBOX*, etc.), che potrebbero essere anche utilizzati in assenza delle apposite applicazioni *Desktop*, attraverso collegamenti diretti via *Web* al servizio. Riguardo tali situazioni occorre sempre porre particolare attenzione sulla tipologia

² Il riferimento è alla possibilità, certamente più semplice e facile, di procedere alla cancellazione, modifica etc. di dati che si trovino in sistemi *Cloud*, per loro natura più facilmente raggiungibili da remoto, rispetto a dati custoditi su supporti "fisici" presenti presso l'azienda ispezionata e di più facile apprensione ed isolamento da modifiche da parte degli investigatori;



di *account* utilizzato. Accade sovente³, infatti, che l'*account* non risulti direttamente riconducibile all'azienda, ma sia di fatto un archivio utilizzato in modo "promiscuo" su di un *account* privato; in siffatti casi, occorre considerare che l'estrazione "coatta" delle necessarie credenziali all'accesso, qualora non fornite spontaneamente dalla parte, è subordinata al rilascio di un'autorizzazione della Autorità Giudiziaria ex art. 52, comma 3, del D.P.R. n. 633/1972, quant'anche fosse possibile rinvenire dette credenziali senza la collaborazione della parte, codificate su appunti, agende, in appositi password manager conservati su *smartphone*, *tablet* o altri dispositivi in uso al verificato. Diverso è il caso di archivi *cloud* rinvenuti "aperti/collegati/loggati" all'atto dell'intervento o il cui accesso avvenga in modo automatico; qui non è richiesta, di fatto, nessuna "collaborazione" del soggetto e la possibilità di gestire dati aziendali da pc aziendali autorizzerebbe l'ispezione di quello "spazio" ai sensi del comma 4 dell'art. testé richiamato che recita testualmente: "L'ispezione

documentale si estende a tutti i libri, registri, documenti e scritture, compresi quelli la cui tenuta e conservazione non sono obbligatorie, che si trovano nei locali in cui l'accesso viene eseguito, o che sono comunque accessibili tramite apparecchiature informatiche installate in detti locali". Chi scrive ritiene, tuttavia, più prudente, in ogni caso, in assenza di un'autorizzazione espressa del titolare dell'*account*, quando questo sia privato o promiscuo, richiedere apposita autorizzazione, onde non vedersi inficiate le attività di acquisizione, controllo ed esito conseguenti.

Circa cosa cercare nel corso delle ricerche o ispezione, questo è strettamente correlato alle finalità ed oggetto del controllo. Tutto, infatti, può fornire spunti, indicazioni, notizie ed altri elementi utili a definire l'effettività, genuinità e dimensione di un fatto/fenomeno economico. La pratica operativa ha permesso di affinare diverse tecniche, quale quella di porre particolare attenzione ad alcuni elementi nell'immediatezza dell'accesso. Tra questi elementi,

³ Invero, la situazione è alquanto comune anche in aziende di rilevanti dimensioni, laddove si tenta di occultare la documentazione "compromettente" nel *cloud* attraverso *account* privati e non riconducibili all'azienda;

il "cestino", i *file* in uso e quelli aperti di recente vengono quasi sempre a fornire importanti elementi di interesse. La circolare chiede poi di porre particolare attenzione alle eventuali copie di *backup* rinvenute; ciò che non è possibile recuperare da un dispositivo, è invece recuperabile rintracciandone le copie di sicurezza eseguite dal proprietario. Queste sono archiviate ovviamente per fini diversi, ma possono risultare una preziosa fonte d'informazione storica e di riscontro, anche al fine di individuare ove possibile:

- i *files* eventualmente cancellati dal sistema al momento dell'accesso;
- eventuali modifiche apportare anche in precedenza allo stesso, che comunque possono rilevare in modo sostanziale ai fini della determinazione del reddito e della conseguente tassazione in capo al soggetto ispezionato.

Inoltre, l'acquisizione delle copie di *backup* ha anche lo scopo di fungere da deterrente nei confronti del contribuente, laddove avesse intenzione di apportare modifiche, successivamente all'accesso dei militari e durante il controllo. Di fatto, si ottiene mediante l'acquisizione delle copie di *backup* un "congelamento" dei dati riferibili ad un dato momento, che, nella maggior parte dei casi, risulta ampiamente sufficiente ed adeguato all'esecuzione dei controlli, che, qui si rammenta, si riferiscono quasi sempre a fatti e fenomeni economici avvenuti diverso tempo prima del controllo (solitamente vengono prese a riferimento, oltre all'annualità in corso, le due precedenti).

Ad ogni buon conto, non esiste una procedura standardizzata o un diagramma di flusso da seguire, su cosa cercare. Abbiamo visto che la prima attività consisterà in una ricerca ed individuazione di tutti i supporti digitali che potenzialmente possono costituire un contenitore di dati informatici; gli stessi, qualora oggetto di successive ricerche "informatiche", andranno debitamente identificati, al fine di poter poi, nelle fasi successive, specificare in ogni contesto

l'origine dei dati acquisiti. A tal proposito, soprattutto nell'ambito delle aziende e quando si ha a che fare con molti personal computer (quasi sempre della stessa marca e tipo), andranno evitate descrizioni sommarie che possono ingenerare confusione, preferendo una più accurata identificazione basata sul numero di serie del personal computer o altri elementi distintivi. Esistono anche soluzioni "software" che permettono un'identificazione particolareggiata del PC, per esempio *WinAudit*⁴, programma, questo, che non necessita di installazione sulla macchina target e permette di ottenere in breve tempo un "audit" particolareggiato del pc in esame. Anche soluzioni da CMD "prompt dei comandi", come quella attraverso il comando "*systeminfo*" o per il mondo *Mac* "*system profiler*", permettono di ottenere un set di informazioni sul target in esame ed evitano commistioni tra PC di marca e tipo simili.

Per quanto attiene l'eventuale ricerca su *server*, *NAS*, altri PC della rete effettuata da un *client* collegato, si avrà cura di indicare il preciso percorso di rete ed ogni altro elemento utile ad una identificazione del *client* utilizzato e del percorso esaminato; in questi casi, la collaborazione del personale IT dell'azienda è fondamentale e necessaria per una corretta identificazione dei percorsi e dei "nomi"/IP attribuiti.

Come già anticipato ciò che eleva ed esalta l'importanza della ricerca dei documenti informatici è in realtà la capacità di saper individuare solo quegli elementi utili e necessari alle sorti del controllo, espungendo dalla enorme massa dei dati informatici rinvenuti quelli irrilevanti o inutili.

Detta operazione è tutt'altro che semplice e, come vedremo, non scevra di insidie e richiede per un risultato ottimale la sinergia tra elementi di indagine "tradizionale" e "digitale". Detta sinergia risulta sempre più necessaria in ragione di due aspetti:

- il primo consiste nell'evidenza che oggi l'indagine "tradizionale" segna il passo dinanzi ad una quantità di elementi e documenti che ormai richiedono, per una loro

⁴ *WinAudit* crea un rapporto completo sulla configurazione hardware e software di un computer Windows; è una utility gratuita e open source <http://www.parmavex.co.uk/winaudit.html>;



selezione ed esame, il ricorso obbligato a specifici *software* di indicizzazione⁵ e ricerca, che possano aiutare l'investigatore in questo non facile compito. Al contempo, va riconosciuto che solo attraverso un'indagine tradizionale si può giungere oggi all'individuazione dei soggetti coinvolti in un determinato settore o atto economico dell'azienda, concentrando così le ricerche (anche informatiche) solo nei confronti di questi e sugli apparecchi informatici in uso/possesso agli stessi. Appare evidente come, in realtà aziendali gestite da centinaia di persone (si pensi ad una multinazionale), risulti improbo se non impossibile

procedere ad una ricerca ed ispezione su un numero così elevato di persone e dispositivi, senza rischiare di cadere nelle criticità già sopra evidenziate. Tale considerazione va poi allargata alla complessità di atti economici posti in essere dall'azienda in un determinato periodo, ossia le migliaia di migliaia di atti economici che, nella loro totalità, non possono essere adeguatamente esaminati e controllati. Infine, ma non ultimo, il fattore tempo⁶;

• il secondo consiste nell'evidenza che le cd. "ricerche informatiche" avvengono attraverso *software* che poste determinate "parole chiave"⁷ (che andranno sempre

5 L'indicizzazione è il processo di esaminare file, messaggi e-mail e altri contenuti e di catalogarne le informazioni, ad esempio le parole e i metadati che contengono. Quando la si esegue la prima volta, il completamento dell'operazione può richiedere anche diverse ore a seconda della quantità di dati da "indicizzare" e, solo in seguito, verrà eseguita in background nel PC in esame durante l'uso e viene eseguita nuovamente solo per i dati aggiornati con una notevole riduzione di tempo. Per esempio, su Windows 10, per impostazione predefinita, tutte le proprietà dei file vengono indicizzate, inclusi i nomi di file e percorsi completi dei file stessi. Per i file con testo, il contenuto viene indicizzato per consentire di eseguire la ricerca di parole all'interno dei file;

6 La circolare prevede che: "Nei casi in cui sussista l'inderogabile necessità di procedere ad operazioni informatiche che non possono essere completate durante il primo giorno delle operazioni (ad es.: l'esame dettagliato dei contenuti di tutte le strumentazioni e di tutti i supporti informatici presenti presso i locali ove viene effettuato l'accesso; l'effettuazione di copie di supporti di grandezza rilevante; etc.), può essere valutata l'opportunità, ove tecnicamente praticabile, di continuare l'attività successivamente, mediante idonee cautele dei luoghi e dei mezzi ovvero procedere ai necessari adempimenti, dando atto di ciò nel processo verbale di verifica";

7 Si tratta in questi casi di "parole" e "date". Le prime sono costituite da parole relative a nomi di soggetti, società, ma anche altro, riconducibili a vario titolo ai fatti economici oggetto del controllo. Le seconde sono riconducibili al periodo preso a riferimento per il controllo;

specificate a tutela di chi effettua tale operazione di ricerca) vanno a ricercare detta parola "chiave" su interi volumi, partizioni, all'interno di *file* di testo, immagini etc. Tali parole chiave hanno la natura più disparata e sono frutto di appositi *briefing* nel corso dei quali il direttore della verifica fornisce agli operanti una lista di parole chiave su cui concentrare le ricerche informatiche e non, ed anche una lista di "soggetti" da attenzionare. Nulla, però, impedisce agli investigatori sul posto, accertati nuovi elementi, di modificare anche radicalmente la lista di tali parole chiave o orientare le ricerche anche verso altri soggetti fino a quel momento non adeguatamente considerati. Resta il fatto che ricerche di questo tipo, se da un lato agevolano grandemente le operazioni in termini di velocità ed efficienza, dall'altro presentano a loro volta elementi di fallibilità talvolta insuperabili. Pensando per un attimo ad una email, che oggi rappresenta uno degli strumenti maggiormente utilizzati tra aziende e nelle aziende per comunicare⁸, l'oggetto del controllo cui siamo demandati è una verifica della corretta applicazione della normativa "transfer pricing"⁹. Le decisioni in merito a questa materia tra i gruppi delle società multinazionali, quasi sempre dislocate in "altra" parte del mondo, avvengono per ovvie ragioni via email e dirette a particolari soggetti aziendali generalmente responsabili delle aree fiscalità e finanza. Riflettiamo su questi aspetti:

• l'email che dà disposizioni di dettaglio su questi temi non è stata inviata a quei soggetti appartenenti alle cd. aree di interesse (magari individuati al *briefing*), ma ad altro soggetto fiduciario, non appartenente alle aree di riferimento, che poi avrà il compito di diffonderla ai diretti interessati, magari attraverso comunicazioni interne, apposite riunioni in presenza, altri mezzi ... una telefonata;

8 Non a caso è uno dei mezzi preferiti dagli *attacher* per la perpetrazione di frodi e truffe nei confronti delle aziende ... ma questa è una tesi ed un'altra storia;

9 Indica il meccanismo attraverso il quale i prezzi di vendita non corrispondono all'esatto valore delle merci o dei beni trasferiti, ma sono determinati, nell'ambito di gruppi di società multinazionali, per trasferire utili da paesi a elevata fiscalità in paesi a bassa fiscalità (paradisi fiscali);

10 Optical Character Recognition - OCR è detto anche riconoscimento del testo ed è una tecnologia che permette di convertire tipi diversi di documenti, ad esempio documenti scannerizzati, file PDF o foto digitali, in dati modificabili e ricercabili;

• l'email è stata inviata qualche mese prima della fine dell'anno in un periodo che non viene considerato quale annualità di controllo. Tuttavia, il contenuto della email interessa appieno le annualità in esame (solitamente direttive di tal specie vengono anticipate di molti mesi se non di anni ... l'anno di interesse sottoposto a controllo);

• l'oggetto della email è "Auguri di fine anno xxxx" ma nel corpo del messaggio è riportato "ai fini del TP (*transfer pricing*) per il prossimo anno ricordiamo di modificare ...". O ancora ... meglio ... il testo è all'interno di un'immagine JPEG che non verrà individuata in quanto la maggior parte dei *software* che vedremo per l'effettuazione delle ricerche "sul posto" non effettuano di default l'OCR¹⁰.

Esempi banali, ma che fanno già emergere le difficoltà e le fallibilità insite in una ricerca per parole chiave o per data, all'interno di grandi quantità di *files*.

Non a caso ho voluto prendere ad esempio una comunicazione email, in quanto nella pratica operativa rappresentano il primo *target* di attenzione. Si può affermare che la posta elettronica rappresenti nell'ambito dei controlli qui in esame un vero e proprio "obiettivo strategico" quasi sempre, imprescindibile, del resto le esperienze operative confermano che, proprio attraverso questo mezzo, spesso anche inconsapevolmente, si effettuano comunicazioni alquanto rilevanti per l'esito del controllo. Le email rappresentano tuttavia più di una particolarità meritevole di essere qui approfondite, quanto alla loro ricerca, acquisizione ed estrazione.

Preliminarmente, occorre tenere presente le particolari disposizioni previste per l'acquisizione e l'esame di documentazione contenuta in plichi sigillati, o per la quale è opposto il segreto professionale, adattate alle prescrizioni dettate in tema di fatturazione e conservazione dei docu-

menti in forma elettronica; per effetto delle richiamate previsioni, le comunicazioni via e-mail già "aperte" e visionate dal destinatario sono direttamente acquisibili dai verificatori, mentre quelle non ancora lette o per le quali è eccepito il segreto professionale possono essere acquisite sulla base di un provvedimento di autorizzazione dell'Autorità Giudiziaria, ex art. 52, comma 3, del D.P.R. n. 633/1972. Nel condividere quanto dettato dalla circolare in termini di "garanzie Costituzionali" riconosciute alla parte e ai militari che operano l'intervento, va evidenziato come, nella pratica, emergano tuttavia alcune criticità /difficoltà meritevoli di essere considerate.

La prima attiene al mancato consenso da parte dell'interessato alla cosiddetta operazione "one click", ovvero filtra le email non lette e le segna come lette, onde aggirare la problematica. Talvolta, soprattutto quando si ha a che fare con archivi di posta datati e risalenti nel tempo, la controparte non sempre acconsente a fare le cose "in fretta" e preferisce un'analisi "one by one". Ora, è logico ritenere che, se detta operazione può essere effettuata su piccoli archivi o su un numero limitato di email, le cose si complicano non poco quando trattasi di migliaia di mail, spesso non riconducibili ad un unico soggetto, che, per non farci mancare nulla, magari è anche fisicamente assente dal luogo delle operazioni.

La seconda, è che, spesso per ragioni non solo di tempo ma anche di praticità e operative (dettate dallo specifico caso), si rende necessario procedere all'acquisizione di interi archivi di posta:

- esportati di *default* periodicamente dal sistema;
- realizzati dall'utente per diversi scopi (storici, statistici, amministrativi etc.);
- realizzati all'atto dell'accesso su richiesta da parte della Guardia di Finanza.

Quanto ai primi due, si tratta solitamente degli archivi più interessanti, atteso che le email periodicamente conservate "on line" dal sistema, soprattutto in ambito aziendale, sono relative a periodi recenti e limitati per ovvie ragioni di risparmio dello spazio dedicato sul *server* a ciascun dipendente/

dirigente e risultano anche essere le meno "determinanti" nell'ambito di controlli fiscali, che, come già anticipato, si riferiscono a periodi precedenti.

Quanto a quelle realizzate su richiesta della Guardia di Finanza, è invece innegabile come spesso la parte acconsenta, nell'ottica di ricevere il minor disagio possibile dalle operazioni di accesso e controllo in corso, ad esportare, per esempio, nel caso di utilizzo di "Outlook", un *file .pst*, contenente l'intero archivio di posta. O, ancora, si potrebbe decidere, per motivi di opportunità, di procedere all'acquisizione di tutti i *file .pst* presenti in locale su specifici personal computer o sul *server* dell'azienda.

In tutti questi casi, è facile comprendere, soprattutto quando la mole di dati è rilevante, quali siano le difficoltà di procedere, preliminarmente all'acquisizione, ad un'analisi dettagliata dei singoli archivi alla ricerca di eventuali email "chiuse" o di solo quelle di interesse che andrebbero aperte a cura dell'intestatario della casella email corrispondente.

Una soluzione potrebbe consistere in un "congelamento" del dato attraverso la copia dei *file*, nel caso di esempio *.pst* su idonei supporti con le modalità che vedremo meglio dopo. Tale congelamento permetterebbe agli investigatori, da un lato, di conservare lo stato delle cose e, dall'altro, di riservare in un secondo momento e con tempi congrui l'analisi di detti *file* alla ricerca ed individuazione delle sole email d'interesse, previa apertura/visione di quelle non ancora lette.

In subordine, la parte potrebbe rilasciare apposita delega/autorizzazione scritta ad effettuare, anche in sua assenza, l'esame delle email e a procedere alla lettura, anche di quelle non ancora lette, su suo espresso consenso scritto.

Questa potrebbe essere una soluzione capace di temperare le contrapposte esigenze degli attori coinvolti, nell'evidenza che ciò che, a volte, può apparire di facile soluzione con pochi *click*, nella realtà operativa, non lo è affatto!

Concludo con un'ulteriore considerazione relativa al fatto che leggere e poi spuntare come non letta la stessa email equivalga

ad una volontà espressa del destinatario a far risultare quella email come non letta e come tale questa dovrà essere considerata, da chi vorrà acquisirla.

Ulteriore nota concerne le email è insita nelle difficoltà tecnico pratiche legate a questo strumento di comunicazione; cito, a mero titolo di esempio e lungi dall'essere esaustivo:

- l'acquisizione delle *webmail*, allorché si lanciano *software* di acquisizione delle email, quali *MailStore* o *Google Takeout*, che al di là degli innumerevoli pregi di semplicità ed affidabilità hanno il difetto di non fornire una stima del tempo necessario all'effettuazione delle operazioni (cosa non di poco conto per chi effettua operazioni di polizia spesso a carattere coercitivo);
- le problematiche di "sincronizzazione" delle email che spesso si risolvono nel ricaricare all'infinito e più volte un medesimo archivio di una su *Outlook* (mi perdonino gli utilizzatori di "Office"), con il risultato che accade sovente che mail già scaricate e lette vengano ricaricate "come NON lette";
- le ulteriori difficoltà "tecniche" legate

all'utilizzo di alcuni *client* di posta, o meglio a suite complete quali *Lotus Notes*, che complicano ulteriormente quelle elementari operazioni di esportazione delle email in formati poi leggibili, anche attraverso altri *client*.

Va, poi, qui evidenziato come i sistemi di ricerca della maggior parte dei *client* email affidano i loro riferimenti ad elementi quali il mittente, destinatario, oggetto, data ma quasi mai l'indicizzazione comprende il testo della email o il contenuto degli allegati. La possibilità di procedere all'acquisizione dell'intero archivio di posta, come già anticipato, o ancora meglio la possibilità di procedere ad una copia bit to bit del dispositivo, qualora la posta venga scaricata come definito in gergo "in locale" (si pensi all'utilizzo di *client* quali *Outlook*, *Thunderbird* etc.) permette non solo di effettuare le ricerche con molta più calma e parsimonia, ma permette altresì di effettuarle attraverso programmi ad alto livello di indicizzazione, capaci anche di effettuare l'OCR e di ricomprendere nell'indicizzazione testo ed allegati, oltre a molto altro. Il riferimento è alla possibilità tutt'altro che irrilevante di procedere ad un recupero (*carved*) delle



email cancellate in locale e degli eventuali *download* degli allegati quant'anche cancellati. Ad ogni buon conto, sarà sempre necessario acquisire i messaggi di posta elettronica in formato digitale, poiché viene preservata, in tal modo, la componente non visibile del messaggio (cd. *header*) necessario ad individuare l'effettiva provenienza del messaggio.

Infine, anche per la posta elettronica, ove possibile, la ricerca e successiva acquisizione sarà circoscritta agli *account* di posta elettronica di specifici dipendenti della società verificata, nominativamente individuati in ragione dei ruoli e delle responsabilità che essi rivestono in seno all'organizzazione.

Ancora una volta emerge, soprattutto per quanto concerne la ricerca, l'evidente valore aggiunto apportato dalla sinergia di cui sopra, capace, se non di azzerare tali criticità, di mitigarle grandemente. Si rifletta anche sull'utilità strategica delle indagini OSINT (*Open Source Intelligence*) che, se opportunamente ed efficacemente effettuate prima dell'intervento (accesso), possono aiutare in maniera determinata nell'individuazione dei soggetti e degli atti economici "chiave" da sottoporre a controllo¹¹. Peraltro, la stessa circolare contempla la possibilità di cercare elementi utili non risultanti dalle banche dati in uso al Corpo, con particolare attenzione alla consultazione delle "fonti aperte" (articoli stampa, siti internet, *social network*), al fine di acquisire ogni utile elemento di conoscenza sul contribuente da sottoporre a controllo e sull'attività da questi esercitata¹². Il tema

11 *Ogniqualevolta un utente si relaziona con il Web, anche inavvertitamente ed inconsapevolmente, lascia indelebilmente nello stesso molte informazioni. Si rifletta, per esempio, con riferimento al mondo dei social network, chat e blog. In tali contesti, spesso l'utente si lascia andare a comportamenti e rilascia informazioni che possono risultare strategiche, se sapientemente lette ed utilizzate;*

12 *In sintesi viene confermato il contenuto, per quanto qui di interesse, della circolare n. 16/E del 28 aprile 2016 dell'Agenzia delle Entrate, in cui si elencano gli indirizzi operativi per la prevenzione e il contrasto all'evasione fiscale, laddove si dispone che alle notizie che si possono ottenere dalle banche dati si aggiungono quelle che pervengono da altre fonti, ivi incluse fonti aperte. Sono in continuo aumento esempi di accertamenti basati proprio sulla raccolta di elementi da "fonti aperte". A titolo di esempio e per ogni migliore considerazione da parte del lettore, diversi sono ad oggi accertamenti che si sono basati su immagini tratte da social network per la determinazione della realtà capacità contributiva del soggetto (foto delle vacanze, acquisti su piattaforme di e-commerce, viaggi, ricerche effettuate sul web ed incrociate con specifiche movimentazioni bancarie, ma anche notizie giornalistiche e di blog che hanno permesso, talvolta, di svelare rapporti di conoscenza ed economico-commerciali tra soggetti che, viceversa, non sarebbero emersi sulla scorta delle "ordinarie" ricerche effettuate sulle banche dati in uso agli organi di constatazione ed accertamento). <https://www.liberoquotidiano.it/news/economia/30032684/fisco-fotografia-puo-rovinare-evasori-fiscali-agenzia-entrate-social-network.html>.*

OSINT è ormai fondamentale ed indispensabile in ogni attività di ricerca ed indagine, essendo ormai ampiamente documentato e noto come proprio su fonti aperte (si pensi alle potenzialità dei cd. *social network*) si possono rilevare ed acquisire informazioni non altrimenti rilevabili altrove. Tuttavia, il tema OSINT è così complesso ed articolato, da richiedere appositi "approfondimenti" che in futuro sarò ben lieto di affrontare su queste pagine.

In conclusione alle ricerche, occorre precisare che la documentazione delle operazioni svolte è uno degli elementi "imprescindibili". Orbene, la sola verbalizzazione, intesa come descrizione per iscritto di un'azione, segna il passo dinanzi a strumenti e tecnologie che meglio si adattano ad essere descritte con altri mezzi. Anche per le ricerche, l'esperienza operativa ha fatto sì che oggi una *best-practice* sia costituita dalla realizzazione di *screen* video o fotografie atti a compendiare le operazioni svolte. Pertanto, laddove possibile (oggi sempre), sarà bene corredare i verbali di supporti video o fotografici, capaci non solo di descrivere i luoghi e le situazioni affrontate, ma anche (al di là dei Report prodotti dai vari programmi) di mostrare concretamente le operazioni svolte. Qualora si ricorra a tali strumenti, sarà sempre bene ricordare che gli stessi, rientrando a pieno titolo nella verbalizzazione ed operazioni svolte, andranno adeguatamente richiamati nei verbali al pari di un qualsiasi *file* corredato del corrispondente *hash*, come prossimamente meglio specificato.

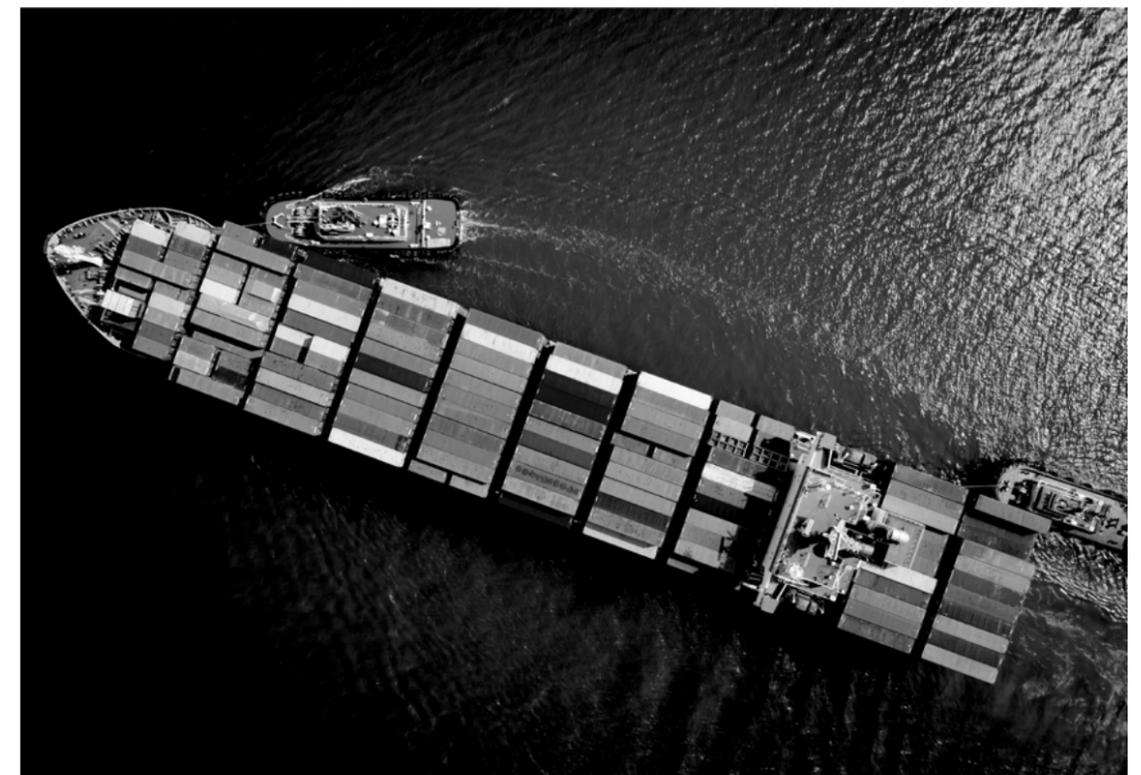
Lo sportello unico doganale: il DPR 29 dicembre 2021 n.235

di Luigi Fruscione

Come evidenziato dall'Agenzia delle dogane sul proprio sito internet "per effettuare un'operazione di import/export, gli operatori debbono presentare, oltre alla dichiarazione doganale, fino a 68 istanze ad altre 18 amministrazioni, trasmettendo ad ognuna informazioni e dati spesso identici o simili nella sostanza per ottenere le autorizzazioni, i permessi, le licenze ed i nulla osta necessari, nella grande maggioranza dei casi rilasciati su carta": questa situazione ha rappresen-

tato l'incipit che ha portato il legislatore a ravvisare la necessità dell'istituzione di un unico punto in cui accentrare le predette molteplici attività.

Con la finanziaria 2004, addirittura prima che l'Unione europea si adoperasse su un progetto simile, il Parlamento italiano formalizzò una norma con cui si individuava l'Agenzia delle dogane quale punto di coordinamento e di controllo del complesso delle informazioni necessarie allo sdoga-



namento.

L'attualità del progetto emerge anche nell'ambito del D.P.R. del 29 dicembre 2021 in cui è rilevata una connessione tra Sportello Unico Doganale e Piano Nazionale di Ripresa e Resilienza (PNRR), nel quale si richiama *"la missione 3 (Infrastrutture per una mobilità sostenibile) ... relativa all'interoperabilità e logistica integrata nell'ambito della quale è previsto, tra l'altro, al punto 2.1 la semplificazione delle transazioni di importazione/esportazione attraverso l'effettiva implementazione dello Sportello Unico Doganale e dei Controlli, finalizzato all'interoperabilità dei sistemi informativi delle diverse amministrazioni interessate e al coordinamento delle attività di controllo da parte degli uffici doganali"*.

Non a caso l'art. 1 del provvedimento *"disciplina lo Sportello unico doganale e dei controlli, al fine di attuare il coordinamento in via telematica di tutti i procedimenti e controlli connessi all'entrata e all'uscita delle merci nel o dal territorio nazionale e di assicurare il conseguimento dell'obiettivo di cui alla Missione 3, riforma 2.1., «Semplificazione delle transazioni di importazione/esportazione attraverso l'effettiva implementazione dello Sportello Unico dei Controlli» del Piano Nazionale di Ripresa e Resilienza"*.

A tale panorama si aggiunga la situazione esistente in Europa su un progetto così importante come quello della semplifi-

cazione dei controlli tra amministrazioni; la Commissione europea ha proposto da poco, il 28 ottobre 2020, in sede di Piano d'Azione dell'unione doganale 2020-2027, l'introduzione negli Stati membri del cosiddetto *"sistema dello sportello unico doganale dell'UE"*, che avrà la funzione di rendere più agevole, per le Autorità coinvolte nell'attività di sdoganamento delle merci, lo scambio telematico delle informazioni trasmesse dagli operatori.

In tal modo si potranno presentare una sola volta le informazioni richieste per l'importazione o l'esportazione delle merci.

La 1ª relazione al Parlamento Europeo, dell'11 ottobre 2021, sulla proposta di Regolamento del Parlamento europeo e del Consiglio che istituisce l'ambiente dello sportello unico dell'Unione europea per le dogane e che modifica il Regolamento (UE) n. 952/2013 (istitutivo del Codice Doganale dell'Unione), evidenzia aspetti di interesse.

Punto di partenza della predetta relazione è rappresentato dalla struttura del Codice Doganale dell'Unione, che rappresenta la base giuridica *"per un ambiente doganale moderno ed elettronico, che mira a un'unione doganale priva di supporti cartacei e completamente automatizzata"*.

L'evoluzione sempre maggiore dei rapporti commerciali tra l'Unione ed i Paesi terzi determina, con sempre maggiore forza, l'insorgenza di due necessità contrapposte:



che le merci che entrano nel territorio doganale siano sicure e soddisfino i requisiti interni e, dall'altro, che le procedure di importazione siano *"quanto più efficienti"* per gli operatori economici, andando ad incidere il meno possibile sulle imprese in fase di sdoganamento.

In sede europea, la proposta di regolamento della Commissione sullo sportello unico dell'Unione europea per le dogane è vista con favore, ritenendo che si tratti del *"primo passo verso la creazione di un quadro digitale per una cooperazione rafforzata fra tutte le autorità di frontiera attraverso uno sportello unico. Per le imprese e i commercianti è fondamentale poter fornire dati ed espletare le formalità alla frontiera mediante un unico portale in un determinato Stato membro, riducendo così la duplicazione degli sforzi, i tempi e i costi. Le autorità doganali e le altre autorità dovrebbero poter utilizzare congiuntamente tali dati e verificare automaticamente che le merci in questione siano conformi ai requisiti dell'Unione e che le formalità necessarie siano state espletate, garantendo così un approccio pienamente coordinato allo sdoganamento delle merci e una visione d'insieme più chiara a livello dell'UE delle merci in entrata nell'Unione o in uscita dalla stessa"*.

Ciò posto, per ritornare al tema dello Sportello Unico Doganale nazionale, esso è stato istituito con l'art. 4, comma 57, della legge n. 350/2003 (legge finanziaria 2004), prevedendosi che *"presso gli uffici dell'Agenzia delle dogane, è istituito lo «sportello unico doganale», per semplificare le operazioni di importazione ed esportazione e per concentrare i termini delle attività istruttorie, anche di competenza di amministrazioni diverse, connesse alle predette operazioni"*.

L'attivazione è avvenuta nel luglio del 2011, con il DPCM 242/2010, il cui articolo 1 chiariva la portata dello strumento: *"lo sportello unico doganale, istituito ai sensi dell'articolo 4, comma 57, della legge 24 dicembre 2003, n. 350, presso gli uffici dell'Agenzia delle dogane, perseguendo lo sviluppo dell'interoperabilità dei sistemi informativi delle diverse amministrazioni interessate, coordina per via telematica i procedimenti coinvolgenti le amministrazioni che intervengono in operazioni doganali, non-*

ché le attività connesse con le predette operazioni e disciplinate dal presente decreto". Ferme le competenze di legge, lo Sportello concentra tutte le istanze inviate, anche in via telematica, dagli operatori interessati, procedendo alla successiva trasmissione alle amministrazioni interessate ed assicurando comunque *"livelli di sicurezza dei controlli dell'Agenzia, specialmente con riferimento alle merci in ingresso, non inferiori, anche sotto i profili sanitari e ambientali, a quelli attualmente garantiti"* (premessa al Regolamento n.235/2021).

Il governo dello Sportello è assegnato ad una struttura istituita presso l'Agenzia delle dogane e dei monopoli, denominata Comitato di coordinamento e monitoraggio permanente dello Sportello unico doganale e dei controlli, che ha il compito di coordinare e armonizzare le scelte strategiche che attengono allo sviluppo dell'interoperabilità dei sistemi informativi che cooperano nell'ambito dello strumento in esame. Il Comitato ha i seguenti compiti: stabilisce le azioni, nonché le tempistiche, per lo sviluppo dello Sportello unico doganale e dei controlli, e ne monitora l'andamento; nel caso in cui emergano criticità in relazione alle attività di competenza, il Comitato adotta ogni misura idonea ad assicurarne il regolare funzionamento.

A presiedere la struttura organizzativa vi è il direttore dell'Agenzia delle dogane e dei monopoli *pro tempore* o un dirigente di vertice suo delegato.

Il Comitato è composto da una pluralità di rappresentanti di diverse Amministrazioni: a) il comandante generale del Corpo delle capitanerie di porto; b) il presidente dell'Ente nazionale per l'aviazione civile (ENAC); c) i presidenti delle Autorità di Sistema portuale; d) un dirigente generale di ogni amministrazione titolare dei procedimenti e dei controlli nonché il direttore dell'Autorità nazionale-UAMA (Unità per le autorizzazioni dei materiali di armamento) per il Ministero degli affari esteri e della cooperazione internazionale e il direttore della Direzione generale della pesca marittima e dell'acquacoltura per il Ministero delle politiche agricole, alimentari, forestali; e) i dirigenti di vertice responsabili dei sistemi informativi, dei controlli e del-

le procedure dell'Agenzia delle dogane e dei monopoli; f) i presidenti delle Società di gestione aeroportuali; g) tre rappresentanti delle Regioni, designati dalla Conferenza delle Regioni e Province Autonome; h) il comandante generale del Corpo della Guardia di finanza; i) un dirigente generale dell'Agenzia delle entrate.

Qualora i designati non possano partecipare agli incontri, è prevista la possibilità di nominare in sostituzione un delegato che abbia poteri decisionali.

Le attività di segreteria del Comitato è previsto che siano svolte dall'Agenzia delle dogane.

In ordine alle materie di volta in volta all'ordine del giorno, si potrà decidere di invitare rappresentanti delle associazioni di categoria più rappresentative sul piano nazionale individuate secondo la specifica competenza.

Si precisa che il Regolamento stabilisce che ai componenti del Comitato e agli osservatori che partecipano alle riunioni non spettano gettoni di presenza, compensi, rimborsi spese, indennità o altri emolumenti comunque denominati.

Nel corso del tempo, le competenze originariamente attribuite allo Sportello con il provvedimento originario sono state oggetto di modifica con l'art. 20, comma 1, del D.Lgs. n. 169/2016, con il quale si sono attribuiti gli ulteriori compiti relativi a competenza e controlli attinenti a tutti gli adempimenti connessi all'entrata e uscita delle merci nel o dal territorio nazionale: oltre ai già previsti procedimenti concernenti l'applicazione delle norme interne dell'Unione, si sono aggiunti quelli disposti da altre Amministrazioni o organi dello Stato.

I controlli, che si eseguono contemporaneamente, sono coordinati dall'Agenzia delle Dogane - ad eccezione di quelli disposti dall'Autorità giudiziaria, dalle forze di polizia e di quelli per la sicurezza dello Stato. L'art. 20 fissava anche le tempistiche entro cui i controlli dovevano essere svolti, prevedendo che le amministrazioni che, a qualsiasi titolo, li effettuavano, dovessero concludere i rispettivi procedimenti di competenza entro il termine di un'ora, per il controllo documentale, e di cinque ore,

per il controllo fisico delle merci, decorrendo dal momento in cui le amministrazioni avessero avuto la disponibilità di tutti gli elementi informativi e fossero state soddisfatte le condizioni previste dalla normativa vigente per l'effettuazione di detti controlli; qualora questi avessero dovuto richiedere accertamenti di natura tecnica o di prelevamento di campioni, i termini di esecuzione sarebbero quelli stabiliti dalla normativa dell'Unione europea o dai protocolli di settore.

L'art. 3 del citato DPCM n.242/2010, attualmente vigente relativamente agli allegati A e B in quanto richiamati dall'art. 4 del Regolamento n.235/2021, stabilisce che "i procedimenti istruttori prodromici alle operazioni di importazione ed esportazione prevedendo che "l'ufficio doganale provvede al controllo e all'eventuale scarico delle certificazioni, delle autorizzazioni, delle licenze e dei nulla-osta, prodromici alle operazioni di importazione ed esportazione ed elencati nella Tabella A, rilasciati dalle amministrazioni di competenza nei tempi previsti in detta Tabella" che è suddivisa con le seguenti voci: Ministero o ente interessato, atto emesso e, infine, tempi di rilascio in giorni. I procedimenti amministrativi e relativi provvedimenti prodromici all'attività di importazione ed esportazione sono per l'appunto indicati nella tabella A che è strutturata su tre colonne: la prima prevede il Ministero o ente interessato, l'atto emesso, i tempi di rilascio espressi in giorni.

Nella prima colonna rientrano, allo stato, il Ministero degli esteri; Ministero dello sviluppo economico; Ministero della salute; Ministero delle politiche agricole, alimentari e forestali; Ministero delle infrastrutture e dei Trasporti; Ministero dell'interno; Ministero dell'ambiente e della tutela del territorio e del mare; Corpo Forestale dello Stato; Agecontrol S.p.a.; Servizi Fitosanitari Regionali; Regioni e Province autonome; C.C.I.A.A.; Cc.naz.prod.canapa; Istituto nazionale per le conserve alimentari; Ente nazionale risi; Ind. Ess. Reggio-Calabria; Cent. Sperim.Palermo; Consorzio Ispettorato per la qualità.

Ad esempio, il Ministero dello Sviluppo economico emetterà la licenza CITES import/export nel termine di 30 giorni dalla

presentazione delle domande complete; però tali termini si interrompono fino alla acquisizione del parere della Commissione scientifica nazionale e alla conclusione di eventuali consultazioni di Autorità CITES estere.

Altro esempio è costituito dal Ministero dell'interno, che ha 90 giorni per concedere l'autorizzazione per l'esportazione di armi comuni e/o munizioni verso Paesi Extra U.E.

L'allegato B del già citato DPCM n.242/2010 prende in esame i procedimenti contestuali alla presentazione della merce ai fini dell'espletamento delle formalità doganali. La suddivisione dell'allegato è basata su quattro colonne relative ai seguenti campi: Ministero o Ente interessato, atto emesso, tempo limite espresso in ore per il controllo documentale e tempo limite visita merci espresso in ore.

Nella prima colonna rientrano l'Agenzia delle dogane, il Ministero della Sanità nelle articolazioni degli Uffici di Sanità marittima e del Posto d'ispezione Frontaliero; l'Azienda Sanitaria Locale; il Ministero delle politiche agricole, alimentari e forestali; il Corpo Forestale dello Stato Nucleo CITES

(adesso passato all'interno dell'Arma dei Carabinieri); l'Agecontrol SpA; il Servizio Fitosanitario Regionale; l'Istituto Commercio Estero; le Camere di Commercio ed, infine, i Comuni.

Anche in tal caso un esempio è costituito dall'Agenzia delle dogane che deve emettere l'atto di svincolo dopo il controllo documentale; il tempo limite in ore per la visita merci è cinque ore.

Si precisa che qualora il controllo richieda accertamenti di natura tecnica sono fatti salvi i tempi necessari per conoscere i relativi esiti.

L'articolo 5 del D.P.R. stabilisce che i procedimenti ed i controlli connessi all'entrata e uscita delle merci, nel o dal territorio nazionale e finalizzati all'assolvimento delle formalità doganali, sono elencati all'interno delle tabelle A e B, allegato al decreto del Presidente del Consiglio dei ministri 4 novembre 2010, n. 242, e pubblicati sul Portale SUDOCO.

Al fine di garantire l'efficace sviluppo dell'interoperabilità e il perseguimento dei principi generali di pubblicità e trasparenza dell'azione amministrativa, le amministrazioni e gli organi dello Stato competenti



sono tenuti a comunicare tempestivamente al Comitato di coordinamento e monitoraggio permanente per la successiva pubblicazione sul Portale SUDOCO:

a) le modifiche, intervenute ai sensi dell'articolo 2 della legge 7 agosto 1990, n. 241, dei termini di conclusione dei procedimenti;

b) le modifiche normative e regolamentari con riferimento ai procedimenti e ai controlli connessi all'entrata e uscita delle merci nel o dal territorio nazionale.

All'atto della presentazione della dichiarazione doganale, l'ufficio doganale provvede ad inviare in via telematica alle amministrazioni competenti i dati raccolti, necessari all'avvio dei procedimenti in parola.

Le amministrazioni comunicano per via telematica gli esiti dei procedimenti di rispettiva competenza all'ufficio doganale, che provvede a definire il procedimento doganale.

L'art.2 del provvedimento stabilisce che "presso l'Agenzia delle dogane e dei monopoli è istituito il Portale dello sportello unico doganale e dei controlli («Portale SUDOCO»)", che rappresenta da interfaccia unica per l'attivazione, per la tracciabilità dello stato, per la conclusione e per la consultazione dei procedimenti e dei controlli.

Stabilisce l'art. 8 del Regolamento che le amministrazioni e gli organi dello Stato, che effettuano controlli ulteriori rispetto a quelli elencati nelle tabelle A e B di cui al DPCM n. 242/2010, ma che comunque concorrono all'assolvimento delle operazioni doganali di importazione ed esportazione, utilizzano il Portale SUDOCO per darne comunicazione all'Agenzia delle dogane.

Così come era già previsto in precedenza, i controlli disposti dall'Autorità giudiziaria e quelli svolti dagli organi competenti per la sicurezza dello Stato e dalle Forze di polizia sono esclusi dalla già menzionata comunicazione.

L'attività di prevenzione e contrasto dell'evasione dell'imposta sul valore aggiunto, nell'ambito delle operazioni doganali, è svolta attraverso l'Agenzia delle dogane che è chiamata ad attuare "ogni necessaria forma di coordinamento con l'Agenzia del-

le entrate e con la Guardia di finanza".

Per quanto riguarda i controlli contestuali alla presentazione della merce ai fini dell'espletamento delle formalità doganali, gli operatori forniscono, attraverso il Portale SUDOCO, le informazioni necessarie, per avvalersi dell'esecuzione contemporanea e nello stesso luogo degli eventuali controlli contestuali alla presentazione della merce. All'atto della presentazione delle merci in dogana o della dichiarazione doganale di cui al CDU, il sistema informativo dell'Agenzia delle dogane e dei monopoli attiva i processi di interoperabilità necessari all'avvio dei controlli, avvalendosi delle informazioni raccolte attraverso il Portale SUDOCO; i sistemi informativi delle amministrazioni e organi dello Stato competenti attivano i processi di interoperabilità necessari al coordinamento dei procedimenti e dei controlli e alla conclusione degli stessi.

Il supporto di natura logistica alle attività svolte attraverso lo Sportello è assicurato: 1) dall'Autorità portuale che fornisce, in caso di necessità e a titolo gratuito, le infrastrutture adeguate a supportare lo svolgimento dei compiti istituzionali dello Sportello unico doganale e dei controlli, e coadiuva, nell'ambito delle proprie risorse umane e strumentali, lo Sportello unico doganale e dei controlli, al fine dell'esecuzione efficiente dei controlli; 2) dalle società di gestione aeroportuale e dai gestori delle strutture logistiche per lo svolgimento dei compiti istituzionali dello Sportello unico doganale e dei controlli e per l'esecuzione efficiente dei controlli.

Stabiliscono le norme transitorie che la richiesta di esecuzione dei controlli, per i quali non è ancora attiva l'interoperabilità, va comunicata attraverso il Portale SUDOCO, affinché il controllo sia eseguito, di norma, contemporaneamente e nello stesso luogo.



**Il tuo consulente
per la gestione
del credito fiscale. **Al 110%****

info@globalbonus.it – globalbonus.it

Compliance: il modello organizzativo 231 e la gestione del rischio. Prima parte

di Matteo Montagner

L'aspetto generale

Il complesso quadro normativo a livello nazionale e internazionale, che si è stratificato nel corso del tempo, ha determinato un notevole aumento delle responsabilità per le Aziende, gli amministratori e i vertici aziendali, con la conseguenza di poter incorrere in pesanti sanzioni sia penali che amministrative, perdite finanziarie e danni reputazionali.

Un'Impresa, per essere concorrenziale e sostenere le sfide dei mercati nazionali ed internazionali, deve strutturarsi in modo tale da mettere al riparo, per quanto è possibile, da tali problemi che possono mettere a rischio l'attività lavorativa.

Tuttavia, l'evoluzione sempre più accelerata del mercato e degli adeguamenti normativi rende più difficile identificare e controllare i comportamenti, che possono essere a rischio di commissione di illeciti o non conformità rispetto a tematiche, quali la sicurezza negli ambienti di lavoro, la tutela ambientale, la tutela della privacy e la sicurezza informatica, oltre ai principi etici di *business ethics* e alla responsabilità sociale connessa all'attività di Impresa.

La normativa che disciplina la materia prevede che la funzione *Compliance* effettui i controlli sulla conformità alle disposizioni di legge, in modo tale da valutare quali siano in ambito aziendale i rischi di non conformità alle norme, nell'ottica di evitare,

per quanto è possibile, attraverso la messa in atto delle opportune azioni correttive, di incorrere in sanzioni a livello penale o amministrativo, nonché in perdite economiche e danni di immagine.

La funzione Compliance

Con il termine *Compliance* in ambito aziendale s'intende la conformità alle leggi, agli standard, alle migliori pratiche (*best practice*) o l'allineamento alle politiche imprenditoriali, ed è individuato con il sistema di controllo interno e di gestione dei rischi.

Tale sistema può essere definito come l'insieme delle attività e dei processi che vengono messi in atto in via preventiva per garantire il rispetto delle norme di settore e per l'identificazione dei rischi di non conformità nell'ambito dell'attività imprenditoriale, proponendo, quando necessario, le opportune azioni correttive.

La *Compliance* si pone anche come un'attività a salvaguardia dell'Impresa e del patrimonio sociale e come garanzia dell'affidabilità dell'Azienda anche rispetto al mercato e agli investitori.

Attraverso la *Compliance*, l'Azienda mette in atto la capacità di adeguarsi agli obblighi normativi di settore e di garantirne il rispetto nell'ambito della propria attività. L'Impresa non deve limitarsi al pedissequo rispetto minimale della normativa, ma, per garantire la conformità alle norme, deve



anche intervenire sull'innovazione costante della sicurezza sul lavoro, delle tecnologie adottate e degli assetti organizzativi.

Al riguardo è da considerare che l'attività di *Compliance* aziendale non è riferita solo agli Enti e alle Imprese che svolgono la propria attività principale o hanno valenze in ambito bancario e finanziario o della Pubblica Amministrazione, ma anche indifferentemente a tutte le Imprese, indipendentemente dalla consistenza dimensionale, e agli Enti sia pubblici che privati. Infatti, la *Compliance* può essere adottata da tutte le Aziende che devono gestire la propria conformità normativa, ad esempio per la prevenzione degli incidenti e Sicurezza sul posto di lavoro, la lotta alla corruzione, la normativa antiriciclaggio, la tutela del consumatore, la normativa ambientale, le certificazioni di qualità e le normative ISO, la sicurezza informatica e i *data protection*, la *privacy* e il trattamento dei dati personali.

In ogni caso, per tutti gli ambiti previsti, le attività di *Compliance* hanno lo scopo di ottimizzare la riorganizzazione dell'assetto aziendale intervenendo, a scopo preventivo, sul rischio di incorrere in non conformità normative dotando l'organizzazione interna degli strumenti necessari, così da evitare il rischio di subire sanzioni. In tal modo, si mettono preventivamente in atto

tutte quelle misure atte ad evitare di dover rispondere in termini civili, penali ed amministrativi delle azioni. Da non sottovalutare, peraltro, è il danno reputazionale che incide fortemente in termini di competitività sul mercato.

Per contro, le attività di *Compliance* valorizzano l'immagine e la reputazione dell'Impresa, in modo tale che ne risulta rafforzata la fiducia dei propri clienti, stakeholder e partner.

Pertanto, un corretto utilizzo della *Compliance* in ambito aziendale non persegue solo la tutela dell'"Ente" da possibili danni patrimoniali e d'immagine, ma contribuisce anche a tutelare gli amministratori da possibili responsabilità e ad armonizzare i comportamenti della dirigenza e del personale in generale.

Per ottenere questi risultati, le Aziende devono dotarsi di puntuali sistemi di controllo ed attuare degli efficaci programmi di *Compliance* che consentano di evitare di incorrere in sanzioni o comunque di ottenere una riduzione delle stesse, nonché di rispondere ad eventuali richieste di clienti e partner di obblighi di conformità reciproci che possono essere formalizzate in vincoli contrattuali a reciproca tutela.

Pertanto le imprese, anche piccole e medie, che intendono garantirsi di non incorrere in problemi, che possano compromettere

la competitività sul mercato o la loro internalizzazione, devono affrontare in modo strutturato e coordinato le tematiche di *Compliance*, al fine di assicurare la conformità dei processi e dei comportamenti ai requisiti previsti dalla normativa di settore mediante procedure e indirizzi standardizzati e condivisi.

Il rischio di non conformità si abbassa monitorando le conseguenze derivanti (penali, economiche e di reputazione) dai disallineamenti alle norme e definendo le opportune azioni preventive e correttive. Le aree aziendali a maggior rischio di non conformità alle norme risiedono, in generale, in corrispondenza di quelle attività che sono soggette in modo puntuale a numerose disposizioni regolamentari come ad esempio l'intermediazione, i rapporti con la clientela e la gestione del contenzioso. Infatti, le specifiche norme di settore incidono maggiormente sui processi aziendali connessi alla gestione delle attività tipiche dell'Impresa, quali il settore degli approvvigionamenti, le linee di produzione o di erogazione di un servizio, la gestione delle attività in rapporto alla clientela e il settore vendite.

Non a caso le norme maggiormente impattanti sotto questo profilo sono quelle più direttamente correlate con le attività d'impresa, quali la normativa in materia di Salu-

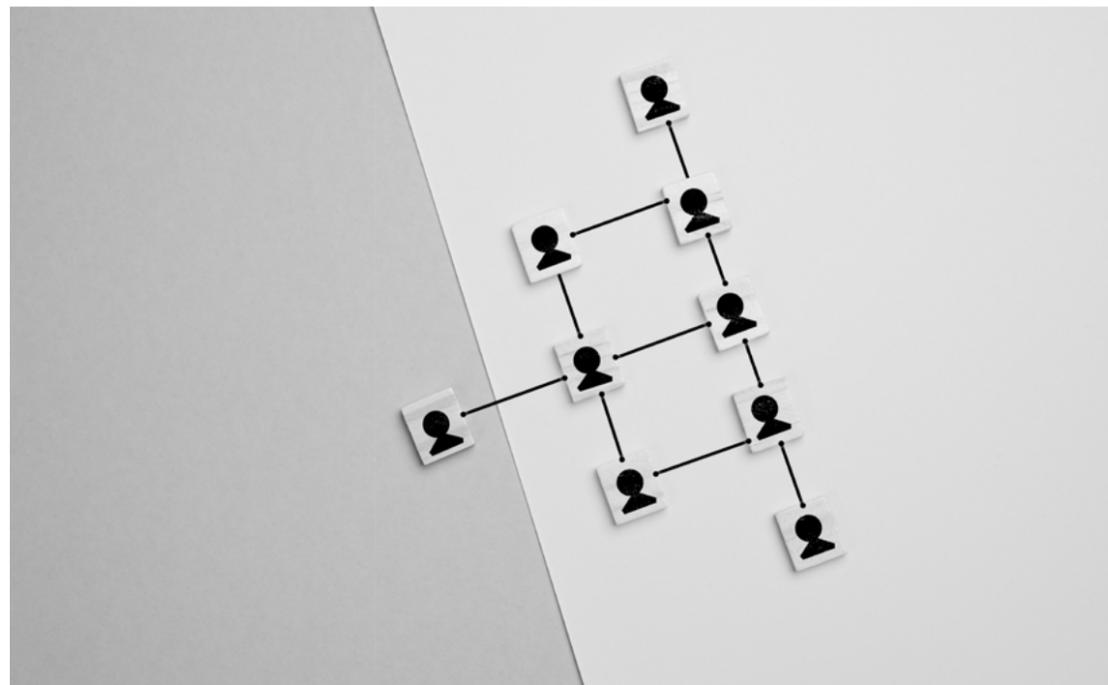
te e sicurezza dei luoghi di lavoro (D.Lgs. n. 81/08), seguita da quella sulla Tutela Ambientale (D.Lgs. n. 152/2006) e dalla relativa specifica regolamentazione normativa di settore.

Per altre norme, invece, la sensibilità è ancora ridotta, nonostante si tratti di tematiche attuali e di forte impatto emergente, quali la legge antiriciclaggio, la tutela della privacy e la sicurezza informatica.

In questa situazione, le Aziende, a prescindere dalle caratteristiche dimensionali, per garantirsi il più possibile dai possibili rischi, devono esaminare la propria struttura organizzativa e individuare le realtà operative aziendali che possono presentare delle criticità. Si deve, quindi, procedere attraverso due fasi:

- la valutazione del rischio (*risk assessment*): il D.Lgs. n. 231/2001 prevede un'analisi delle attività svolte nella società, al fine di individuare quelle che possono ritenersi a rischio di illeciti. Quindi ogni Impresa presenta aree a rischio, la cui individuazione prevede un'analisi della struttura aziendale e delle singole attività svolte;

- la "gap analysis", che consiste nel verificare lo scostamento di un'organizzazione rispetto ad un dettame normativo (es. D.Lgs. n. 231/2001, D.Lgs. n. 196/2003, D.Lgs. n. 81/2008, D.Lgs. n. 152/2006, ecc.) e/o ai requisiti di uno standard internazionale.



Lo scostamento fra le procedure predisposte nella fase di accertamento e le situazioni effettive di rischio che si possono concretizzare possono essere ricondotte sostanzialmente a due principali cause:

- omesso o erroneo recepimento delle direttive predisposte;
- accettazione di una rischiosità residuale da considerarsi ineliminabile.

Le tematiche di *Compliance* si caratterizzano per la loro trasversalità rispetto all'organizzazione e ai suoi processi. In particolare, la loro gestione si deve condurre in modo integrato puntando in modo primario su:

- l'efficacia del sistema di Policy e Procedure;
- il coordinamento fra Funzioni/Direzioni;
- la gestione efficace ed efficiente delle diverse tematiche con la presenza di personale dotato di specifiche competenze.

Tuttavia, in tema *Compliance*, in particolare le piccole e medie Imprese, non affrontano in modo strutturato il problema, ma tendono spesso ad avere un approccio sostanzialmente di tipo reattivo, ossia si attivano sulla base di una necessità o di una sollecitazione, ad esempio a seguito di indagini da parte delle Autorità competenti, anomalie e/o non conformità riscontrate con conseguenze più o meno gravi.

In molti casi le situazioni sono spesso rese problematiche anche dall'assenza di adeguate competenze interne alle Aziende e dalla presenza di sistemi di *governance* non sempre lineari.

Il rischio, infatti, è che, in alcune realtà aziendali, l'Imprenditore sottovaluti le attività di *Compliance*, considerandole dispersive ed estranee all'attività imprenditoriale vera e propria o, purtroppo, valutandole come un dispendio economico inutile senza ritorni positivi.

In questo agire, l'Imprenditore, in quanto le condizioni per restare sul mercato e gli assetti normativi di settore prevedono obblighi e adempimenti sempre più stringenti e complessi, si assume rischi elevati di incorrere in sanzioni molto consistenti per la violazione delle norme, che possono essere fatali per il buon andamento dell'attività aziendale.

Per contro, l'Imprenditore può dotarsi di un'ottimale gestione del rischio aziendale

attraverso l'adozione di un'ideale e costante attività di *Compliance* che, tra l'altro, può permettergli di dedicarsi in modo primario alla gestione manageriale dell'Impresa e alla cura e sviluppo della propria attività imprenditoriale.

La via maestra per affrontare efficacemente il tema consiste nel fatto che le Imprese devono dotarsi in modo strutturale di programmi di gestione della *Compliance* per valutare e gestire, in via preventiva, le tematiche normative che impattano sull'attività aziendale anche attraverso l'attivazione di programmi di formazione e l'effettuazione di attività di verifica (audit).

E' quindi necessario un nuovo approccio alla gestione della *Compliance*, che deve essere considerato importante e prioritario, e tendere a modelli di business sempre più consapevoli, aperti alla realtà sociale e in linea con le normative di settore.

In quest'ottica, l'attività d'Impresa deve essere sempre caratterizzata dal rispetto della legalità, dalla correttezza negli affari e fondata sulla fiducia in dipendenti e collaboratori attraverso la *Compliance* con l'adozione, implementazione e monitoraggio di un approccio integrato ai problemi legati al business uniformando l'insieme dei processi, regole, strumenti e sistemi aziendali. La funzione *Compliance* è in stretto rapporto con la responsabilità amministrativa degli enti delineata dal D.Lgs. n. 231/2001. Pertanto, la funzione *Compliance*, con riferimento al Modello Organizzativo 231 di cui al D.Lgs. n. 231/2001 adottato, ha tra i suoi compiti sia quello di valutare la corretta conformità dell'Impresa ai dettami normativi di settore sia quello di salvaguardare la società con riferimento ai conseguenti danni reputazionali.

Il Modello Organizzativo 231 di cui al D.Lgs. n. 231/2001

In tema di *Compliance* Aziendale è pertanto di fondamentale importanza l'adozione da parte dell'Impresa del Modello Organizzativo 231 previsto dal D.Lgs. n. 231/2001. Infatti, le Imprese, mediante l'adozione di un Modello di organizzazione, gestione e controllo di cui al D.Lgs. n. 231/2001 dei propri processi a rischio, vale a dire di quei processi che, nello svolgersi delle fasi ope-

rative, sono soggetti alla possibilità di incorrere nella commissione di illeciti, possono essere poste in tutto o in parte al riparo dalle relative responsabilità.

Con l'adozione di tale modello, in particolare, è possibile, per l'Azienda:

- non incorrere nei rischi dei potenziali gravissimi danni patrimoniali e d'immagine conseguenti all'irrogazione di sanzioni pecuniarie o interdittive;
- evitare l'instaurarsi di rischi per la salute, la sicurezza dei lavoratori e ambientali, pratiche corruttive, nonché di commettere altri reati definiti "presupposto" della responsabilità degli enti;
- assicurare la buona reputazione aziendale e la fiducia dei clienti, dei partner e degli stakeholders;
- ottenere vantaggi competitivi nel mercato che è sempre più orientato verso comportamenti etici.

Per la predisposizione, realizzazione e conduzione di tutte le attività preliminari e attuative per l'adozione di un Modello Organizzativo 231 efficace ed efficiente, in particolare quelle di *Compliance* del "risk assessment" e "gap analysis", finalizzate, come illustrato in precedenza, ad individuare le aree maggiormente a rischio di condotte illecite nella struttura organizzativa, è necessaria la massima professionalità anche per garantirne la validità sia in termini di attuazione che di validità nel tempo.

Un Modello Organizzativo e di Gestione ai sensi del D.Lgs. n. 231/2001 è un insieme di regole e procedure (protocolli) che disciplinano e definiscono la struttura aziendale e la gestione dei suoi processi, soggetti al possibile rischio di commissione di violazioni delle norme previste dal succitato D.Lgs. o del Codice Etico adottato dall'Azienda, e che, se correttamente applicate, riducono e circoscrivono il rischio e contrastano la possibilità di commissione di illeciti.

I protocolli essenziali di un Modello Organizzativo 231 sono i seguenti:

- 1) il Codice Etico;
- 2) il Sistema Disciplinare dell'Ente;
- 3) l'Organismo di Vigilanza a tutela della Società dall'ipotesi di responsabilità amministrativa;

4) le procedure e i presidi organizzativi specifici per i processi e le attività sensibili individuate a rischio.

Conclusioni

Per le Imprese in tema di *Compliance* è di primaria importanza l'adozione del Modello Organizzativo 231 di gestione e controllo aziendale previsto dal D.Lgs. n. 231/2001. Il Modello Organizzativo 231 è un modello di organizzazione e gestione previsto dal D.Lgs. n. 231/2001 che, pur essendo non obbligatorio, può essere predisposto da tutte le Imprese senza limiti dimensionali e quindi sia che si tratti di grandi, piccole o medie realtà imprenditoriali.

L'adozione di un Modello Organizzativo 231 correttamente predisposto e aggiornato, unitamente ad un'adeguata informazione e formazione del personale sono attività in grado di assicurare il riconoscimento della sua validità sia a livello giurisprudenziale, che in termini di agevolazioni previste dal Codice degli Appalti Pubblici.

Il D.Lgs. n. 231/2001 individua nel Modello Organizzativo 231 e di Gestione, correttamente elaborato, adottato ed aggiornato, lo strumento che permette alle Imprese di minimizzare il rischio che siano commessi illeciti nell'ambito dell'attività aziendale e di essere esonerate, o comunque ottenere una riduzione della propria responsabilità, per i reati imputati ai singoli dipendenti o amministratori in violazione delle norme previste dal D.Lgs. n. 231/2001.

In ogni caso, il Modello Organizzativo 231 non costituisce uno strumento aziendale a sé stante, ma deve risultare integrato ed interagente con gli altri sistemi e procedure aziendali e, in generale, con i sistemi di certificazioni presenti e adottati dall'Impresa, nel campo della Gestione della Qualità, in ambito Ambientale, di Responsabilità Sociale, di Controllo e Gestione della Sicurezza sul Lavoro, di Privacy, di Anticorruzione e di Tutela dei Consumatori.

Bisogna, in definitiva, riferirsi al Modello Organizzativo 231 e di Gestione non come ad un protocollo statico e immutabile, ma come ad uno strumento che deve essere costantemente monitorato, adattato e aggiornato.



Proteggiamo la tua attività e la sicurezza del tuo sistema informatico



Verifica la sicurezza della tua attività con **Seac Security Service**.

I nostri Senior Security Manager sono a tua disposizione per offrirti i migliori strumenti di protezione dagli attacchi informatici.

+39 0461 805490
info@seacsecurity.it

seacsecurity.it

I nuovi adempimenti antiriciclaggio per il comparto assicurativo

di Edoardo Franquillo

Considerazioni introduttive

Il Regolamento n. 44 adottato dall'Istituto per la Vigilanza sulle Assicurazioni (di seguito IVASS) ha riorganizzato in un unico testo le disposizioni dei previgenti Regolamenti n. 41/2012 e n. 5/2014 adeguandoli alla IV Direttiva UE Antiriciclaggio e dettando disposizioni, per la prima volta in ambito assicurativo, in materia di organizzazione, procedure, controlli interni e di adeguata verifica della clientela.

Un ulteriore passo in questa direzione è rappresentato dal recente Provvedimento n. 111 emanato in data 13 luglio 2021, con cui è stata data attuazione agli articoli 15 e 16 del Decreto Legislativo 231/2007, i quali hanno ad oggetto, rispettivamente, la valutazione del rischio da parte dei soggetti obbligati e le procedure di mitigazione del rischio.

Le predette disposizioni delegano, infatti, all'IVASS il compito di definire, per i diversi operatori del mercato assicurativo, i criteri e le metodologie per analizzare e valutare il rischio di riciclaggio cui gli stessi operatori sono esposti, commisurandoli alla specifica attività svolta e alle dimensioni di tali soggetti, i requisiti dimensionali e organizzativi in base ai quali le sedi secondarie di

assicurazioni in Italia e gli intermediari assicurativi sono tenuti ad istituire una funzione antiriciclaggio che verifichi le politiche, le procedure e i controlli, indicandone il titolare responsabile, nonché, infine, indicare un responsabile per le segnalazioni di operazioni sospette alla UIF.

L'Istituto si propone di indicare, dunque, con tale ultimo Provvedimento, i criteri e le metodologie a cui i soggetti obbligati devono conformarsi nell'analisi e nella valutazione dei rischi di riciclaggio e di finanziamento del terrorismo.

A ben vedere, il carattere precettivo delle disposizioni contenute nel Provvedimento, e gli obblighi ivi contenuti, vanno rinvenuti, come detto, nella normativa primaria, cui l'IVASS ha provveduto a dare attuazione.

A questo riguardo, la volontà espressa dal legislatore di delegare alla normativa secondaria le indicazioni di dettaglio su una corretta formalizzazione di procedure, protocolli specifici e presidi da mettere in campo risponde all'esigenza, come emerge nitidamente dalla Relazione illustrativa al Provvedimento, di garantire che sia rispettata la *ratio* fondante che permea tutta la disciplina antiriciclaggio, cioè l'imposizione di una metodologia basata sul rischio

(c.d. approccio *risk-based*)¹.

Non si può sottacere, tuttavia, che l'IVASS, nell'adozione del Provvedimento, ha goduto di margini, seppure ristretti, di discrezionalità, frutto anche della istruttoria normativa e del processo di analisi dell'impatto della regolazione, il c.d. processo AIR.

Le soluzioni che si illustreranno, pertanto, sono il risultato del coinvolgimento di attori del mercato di riferimento esterni all'Istituto, quali, in particolare, le associazioni di categoria del settore assicurativo.

Addentriamoci ora nei meandri tecnici della disciplina.

Il perimetro applicativo della disciplina: i "soggetti obbligati"

In via preliminare, l'art. 3 del Provvedimento stabilisce che l'ambito di operatività nel quale devono operare i soggetti obbligati è il c.d. ramo vita, per come inteso e disciplinato dall'art. 2 comma 1 del Codice delle

Assicurazioni Private (di seguito "CAP" o anche "Codice")².

Nell'alveo di tale classificazione, gli operatori designati dal Provvedimento ad assolvere gli obblighi ivi previsti sono: a) le sedi secondarie di imprese di assicurazione con sede legale in un altro Stato membro dell'Unione europea o in un Paese aderente allo Spazio Economico Europeo (SEE); b) le imprese stabilite senza succursale; c) gli intermediari assicurativi; d) gli intermediari assicurativi stabiliti senza succursale.

Con particolare riferimento alle imprese ed intermediari con sede legale in un altro Stato membro dell'Unione europea o in un Paese aderente allo Spazio Economico Europeo, il Provvedimento precisa, all'art. 4, che dalle suddette devono ritenersi escluse quelle imprese/intermediari considerate stabilite ai sensi dell'articolo 23, comma 1-bis, del CAP³, mentre vanno ricomprese le imprese o intermediari che presentino,

¹ La Direttiva 2009/138/UE Solvency II, in attuazione della quale sono stati emanati due Regolamenti delegati nn. 35/2015 e 467/2016, ha rivisitato profondamente la vigilanza prudenziale del settore assicurativo, uniformandola a quella del settore bancario/finanziario;

² Nel ramo vita sono ricomprese: I) le assicurazioni sulla durata della vita umana; II) le assicurazioni di natalità e nuzialità; III) le assicurazioni, di cui ai rami I e II, le cui prestazioni principali sono direttamente collegate al valore di quote di organismi di investimento collettivo del risparmio o di fondi interni ovvero a indici o ad altri valori di riferimento; IV) l'assicurazione malattia e l'assicurazione contro il rischio di non autosufficienza che siano garantite mediante contratti di lunga durata, non rescindibili, per il rischio di invalidità grave dovuta a malattia o a infortunio o a longevità; V) le operazioni di capitalizzazione; VI) le operazioni di gestione di fondi collettivi costituiti per l'erogazione di prestazioni in caso di morte, in caso di vita o in caso di cessazione o riduzione dell'attività lavorativa;

³ L'art. 23 comma 1-bis del Codice prevede che: "È considerato esercizio dell'attività assicurativa in regime di stabilimento ai sensi del comma 1, anche in assenza di succursali, agenzie o sedi secondarie, qualsiasi presenza permanente nel territorio della Repubblica, inclusa l'organizzazione di un semplice ufficio gestito da personale dipendente dell'impresa ovvero da una persona indipendente ma incaricata di agire in modo permanente per conto dell'impresa stessa". Comma inserito dall'articolo 1, comma 17, lettera a), Decreto legislativo 12 maggio 2015, n. 74;



cumulativamente, i seguenti tre requisiti: i) attività esercitata in regime di libera prestazione di servizi nei rami vita; ii) la distribuzione di prodotti assicurativi attraverso una rete di intermediari iscritti in determinate sezioni del Registro; iii) la concessione di premi lordi contabilizzati, che siano stati comunicati all'IVASS dalla sede centrale dell'impresa stessa, superiori ad € 5 milioni. Al comma 2 della medesima disposizione viene precisato, inoltre, che il disposto normativo si applica anche agli intermediari che effettuino la distribuzione di prodotti assicurativi nei rami vita, in regime di libera prestazione di servizi tramite soggetti intermediari quali dipendenti, collaboratori, produttori e altri incaricati per l'attività di intermediazione svolta al di fuori dei locali in cui opera l'intermediario.

Avuto riguardo alle sedi secondarie di imprese con sede legale in uno Stato membro, vale la pena ricordare, inoltre, che l'Autorità di Vigilanza dello "Stato membro ospitante", intendendosi con tale espressione, come chiarito dalla Relazione illustrativa al Provvedimento, sia gli Stati membri UE che quelli appartenenti SEE, è competente in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela relativi alla prevenzione del riciclaggio e il contrasto al finanziamento del terrorismo ai sensi dell'articolo 3, comma 2, lettera t), del decreto antiriciclaggio n. 231/2007.

Le soluzioni individuate dal Provvedimento

Il Provvedimento IVASS è il risultato di un'attività che l'Istituto ha condotto anche con attori esterni, in particolare nella fase di valutazione prognostica dell'impatto della normativa regolamentare sul mercato di riferimento.

Se si legge con attenzione la Relazione illustrativa al Provvedimento si può verificare che, pur essendo stata esclusa in radice l'opzione zero, ossia l'integrale mantenimento dello *status quo*, in quanto l'IVASS era tenuto inderogabilmente a dare attuazione alla normativa di rango primario, sono stati tenuti in estrema considerazione sia l'obiettivo di conseguire un approccio armonizzato minimo a livello europeo sia l'esigenza di uniformare la disciplina in ambito assicurativo a quella già in vigore nel settore bancario/finanziario.

Nondimeno, per stessa ammissione della Relazione al Provvedimento, le scelte regolamentari, all'interno di più opzioni potenzialmente applicabili, sono state adottate tenendo conto dei principi di proporzionalità, di contenimento dei costi evitabili e di efficacia dei presidi dei rischi di riciclaggio e di finanziamento del terrorismo, nonché dell'efficacia dell'azione di vigilanza.

L'azione regolatrice è stata indirizzata sulle seguenti cinque tematiche: 1) valutazione e gestione dei rischi di riciclaggio e di finanziamento del terrorismo, nonché am-



bito di applicazione dell'attività annuale di autovalutazione per le imprese, per le imprese stabilite senza succursale e per gli intermediari assicurativi; 2) individuazione degli obblighi a carico delle imprese stabilite senza succursale; 3) istituzione della Funzione antiriciclaggio e nomina del titolare della funzione: semplificazioni per le sedi secondarie e individuazione di criteri dimensionali e organizzativi per gli intermediari assicurativi; 4) previsione di una Funzione di Revisione indipendente incaricata di verificare il rispetto di politiche, procedure e controlli interni in materia di antiriciclaggio per le sedi secondarie e gli intermediari assicurativi; 5) definizione dell'intervallo temporale necessario a individuare il superamento delle soglie dimensionali e organizzative rilevanti per l'individuazione dei soggetti tenuti all'adempimento degli obblighi derivanti dal provvedimento.

Con riferimento al primo tema, la soluzione optata dall'Istituto è rinvenibile nell'art. 13 del Provvedimento, in particolare nell'art. 28-sexies della nuova Sezione VI «Valutazione dei rischi di riciclaggio e di finanziamento del terrorismo» che ha modificato, o meglio integrato, il già richiamato Regolamento IVASS n. 44. Al comma 1 viene stabilito che sussistono obblighi informativi, con cadenza annuale, nei confronti dell'IVASS, da espletare mediante la redazione di un documento finale suddiviso in sei sezioni: organizzazione, premi lordi contabilizzati, prestazioni liquidate, gestione e controllo, intermediari ed esito autovalutazione.

Segnatamente, è stato previsto, in primo luogo, che nei confronti delle imprese che commercializzano esclusivamente prodotti standardizzati a basso rischio, sussiste l'obbligo di comunicare soltanto i dati relativi alla sezione II, cioè il numero dei clienti e gli importi dei "Premi" in seno al predetto documento da inviare all'Autorità di Vigilanza.

In secondo luogo, è stato previsto che le imprese stabilite senza succursale sono destinatarie di obblighi di comunicazio-

ne esclusivamente con riferimento alle informazioni dei dati di cui alla sezione V "Intermediari", relative cioè all'importo complessivo della produzione per ogni intermediario assicurativo di cui dette imprese si avvalgono.

Infine, è stato previsto che gli intermediari sono esonerati dallo svolgimento periodico dell'esercizio di autovalutazione, in quanto le singole imprese, oltre a valutare l'attività di commercializzazione, sono tenute a prendere in considerazione, tra i vari fattori di rischio, le caratteristiche della propria rete distributiva.

A ben vedere, viene posta in tal senso, fra gli intermediari, un'ulteriore diversificazione, dal momento che l'Autorità, isolando gli intermediari ex articolo 109 comma 2 lett. d) del Codice, ovverosia le banche e gli intermediari finanziari autorizzati ai sensi dell'art. 14 del TUB, ha stabilito, riguardo ad essi, che le informazioni sui rischi connessi alla distribuzione di prodotti assicurativi vanno comunicati in apposita sezione aggiuntiva al documento di autovalutazione già richiesto dalla normativa bancaria, evitando così una duplicazione di attività in ambito AML.

Passando al secondo tema affrontato dal Provvedimento, riguardante l'individuazione degli obblighi per le imprese stabilite senza succursale, l'Autorità ha individuato un insieme di imprese che sono tenute obbligatoriamente a nominare un responsabile per le operazioni sospette alla UIF⁴. I requisiti indicati dall'art. 4 del Provvedimento includono quelle imprese che operano in regime di libera prestazione di servizi nella distribuzione di prodotti assicurativi sul suolo italiano, avvalendosi di una rete di intermediari assicurativi di cui agli articoli 109, comma 2, lett. a), b) e d), 116-*quater* e 116-*quinquies* del Codice, e che conseguono premi lordi contabilizzati superiori a 5 milioni di euro.

Tali imprese, a mente dell'art. 7 del Provvedimento, possono designare, quale responsabile delle operazioni sospette, il responsabile già nominato per: a) la sede

⁴ Nella Relazione illustrativa al Provvedimento, l'Autorità, con l'intenzione di dimostrare la legittimità della scelta operata, riprende un precedente della Corte di Giustizia UE (sentenza 25 aprile 2013 – causa c-212/11), nel quale era stato dichiarato pienamente conforme al diritto unionale un analogo obbligo della normativa spagnola imposto a tutte le imprese operanti in regime di libera prestazione di servizi, sin dal recepimento della Direttiva I antiriciclaggio;

secondaria dell'impresa, sempreché sia stata istituita per l'esercizio dell'attività anche in regime di stabilimento, l'ultima società controllante italiana o con sede in uno Stato membro UE o in un paese aderente al SEE, una qualunque altra impresa, con sede in uno Stato membro dell'UE o in un paese aderente al SEE, facente parte di un gruppo italiano, a condizione che i predetti soggetti siano tenuti ad istituire la funzione antiriciclaggio; b) la sede centrale della stessa impresa, a condizione che la persona designata, se dipendente della sede centrale, venga distaccata anche a tempo parziale in un ufficio in Italia, anche di terzi, ma comunque nella disponibilità dell'impresa ovvero che, qualora non sia un dipendente della sede centrale, sia comunque domiciliata per la carica in Italia; c) di un intermediario assicurativo di cui all'articolo 109, comma 2, lettera D), che distribuisca in Italia i prodotti del comparto vita dell'impresa; d) di un altro intermediario assicurativo, obbligato ad istituire la funzione antiriciclaggio e a nominare il relativo titolare, che, al momento della designazione, distribuisca in Italia i prodotti del comparto vita dell'impresa da almeno due anni.

Quanto al terzo macro-tema affrontato dal Provvedimento e avente ad oggetto l'istituzione di una funzione antiriciclaggio, i riferimenti normativi da prendere in considerazione sono gli artt. 5 e 6.

L'art. 5, nell'individuare i soggetti obbligati ad istituire tale funzione, cioè le sedi secondarie in Italia di imprese di assicurazione con sede legale in uno stato SEE e gli intermediari assicurativi, stabilisce da un lato la facoltà, per le sedi secondarie che distribuiscono prodotti standardizzati a basso rischio, di non istituire la funzione antiriciclaggio in Italia e di delegarne i relativi a compiti all'omologa funzione della sede centrale, a condizione che uno degli addetti dipendenti della suddetta sede venga distaccato a tempo parziale in Italia ovvero, se non dipendente della società, che sia domiciliato per la carica in Italia o, ancora, ad uno dei Rappresentanti generali che

non sia munito di deleghe che ne pregiudichino l'autonomia; dall'altro lato, individua le caratteristiche quali-quantitative (forma giuridica, profili organizzativi e volume di affari) degli intermediari assicurativi tenuti ad assolvere tale obbligo, ovverosia la distribuzione di premi lordi contabilizzati annuali e comunicati all'IVASS superiori a 15 milioni di euro e un numero di dipendenti e collaboratori iscritti nella sezione E del RUI pari o superiore a 30 unità.

L'art. 6, invece, si occupa, ricalcando le soluzioni tratteggiate dal precedente articolo, di stabilire quali sono i soggetti che possono ricoprire il ruolo di titolare della funzione antiriciclaggio, in particolare prevedendo che: a) le predette sedi secondarie possono individuarlo nel titolare dell'omologa funzione istituita presso la sede centrale dell'impresa, a condizione che, se dipendente, venga distaccato a tempo parziale in Italia ovvero che, se non dipendente, sia comunque domiciliato nel nostro Paese per la carica; b) gli intermediari possono fare a meno di nominare un titolare, potendo essere gli stessi agenti/broker a rivestire tale carica.

Il Provvedimento, come anticipato nei "considerando introduttivi", reca disposizioni, inoltre, sulla necessità di istituire una funzione di revisione interna indipendente su politiche, procedure, controlli interni in ambito AML.

A questo proposito, leggendo l'art. 8 si può agevolmente verificare che le soluzioni elaborate non sono dissimili da quelle già individuate per l'istituzione della funzione antiriciclaggio, seppure con qualche variazione dimensionale. Le sedi secondarie, infatti, possono prevedere che i compiti siano svolti dalla funzione di revisione interna già istituita presso: a) l'ultima società controllante italiana o con sede in uno Stato membro UE o SEE; b) una qualunque altra impresa, con sede in uno Stato membro UE o SEE, facente parte di un gruppo italiano ex art. 2, comma 1, lettera j), del Reg. IVASS n. 44/2019 ovvero di un gruppo estero di cui all'articolo 3, paragrafo 15 della Direttiva (UE) 2015/849⁵; c) la sede centrale

⁵ Intendendosi con l'espressione «gruppo estero» un gruppo di imprese composto da un'impresa madre, dalle sue imprese figlie e dalle entità in cui l'impresa madre o le imprese figlie detengono una partecipazione, nonché le imprese legate tra loro da una relazione ai sensi dell'articolo 22 della Direttiva 34/2013 UE.



dell'impresa. Gli intermediari, al contrario, hanno l'obbligo di istituire la funzione di revisione interna solo ove il numero dei dipendenti e dei collaboratori iscritti nella sezione E del RUI sia pari o superiore a 100 unità e il volume dei premi lordi contabilizzati sia superiore a 20 milioni di euro.

In ultima istanza, l'Autorità di Vigilanza si preoccupa di stabilire, ai fini del possesso dei requisiti e, dunque, dell'applicabilità della disciplina descritta ai soggetti obbligati, l'intervallo temporale necessario a determinare il superamento delle soglie dimensionali.

A tal riguardo, nell'art. 10 è sancito che i requisiti previsti devono essere posseduti nel biennio precedente e, a questo fine, i soggetti obbligati sono tenuti a verificare il possesso dei medesimi per ciascun anno del biennio precedente all'emanazione del Provvedimento.

Valutazione del rischio e adeguata verifica della clientela: le "pietre miliari" della disciplina antiriciclaggio declinate al comparto assicurativo

Il sistema delle verifiche in tema antiriciclaggio ruota tutt'intorno a due componenti fondamentali che s'intersecano fra loro: da un lato, il già richiamato *risk-based approach*, ossia l'approccio metodologico che banche, istituzioni finanziarie e assicurazioni *tout court* devono seguire nella valutazione del rischio riciclaggio e terrorismo; dall'altra, il principio del KYC «*Know your customer*», che richiede un'adeguata verifica della clientela con cui costantemente si

interfacciano gli enti del mondo bancario/finanziario/assicurativo.

Con riguardo al secondo dei due capitali, occorre rammentare che il Reg. IVASS n. 44/2019 ha già provveduto a delinearne le peculiarità in ambito assicurativo, ponendo l'attenzione sull'ampliamento della platea dei soggetti destinatari di tale verifica, che determina un aumento esponenziale degli adempimenti di adeguata verifica.

In questo senso, le specificità del comparto assicurativo, dettate dalla presenza di parti contrattuali tipiche dei contratti assicurativi, emergono dalla classificazione, e definizione, dei vari soggetti coinvolti, prevista nell'art. 2 del Reg. n. 44/2019. A titolo esemplificativo, al comma 1 lett. x) è definita la figura del "beneficiario", inteso quale persona fisica che usufruisce, su designazione effettuata dal contraente o dall'assicurato della prestazione assicurativa, della prestazione erogata dall'impresa di assicurazione, che va distinta da quella del c.d. "titolare effettivo sub 3" di cui alla lett. vv) del medesimo comma e articolo, il quale coincide, al contrario, con quel soggetto in favore del quale viene effettuato il pagamento su disposizione del "beneficiario designato".

Ciò impone, come sancito dall'art. 2 comma 1 lett. aa), che l'indagine antiriciclaggio si diriga su tutti i soggetti coinvolti, essendo previsto, per l'ente assicurativo, l'obbligo di richiedere la trasmissione dei dati identificativi del beneficiario, del relativo titolare effettivo e dell'esecutore.

Orbene, con l'emanazione del recente



Provvedimento n. 111 si è provveduto ad integrare il Reg. 44/2019 sotto l'ulteriore profilo della mitigazione del rischio, nel pieno rispetto dell'approccio metodologico fondante la disciplina antiriciclaggio. Gli sforzi di questo intervento sono stati convogliati in una nuova sezione (la n. VI), nella quale sono previste le attività che le imprese saranno tenute a svolgere e i criteri da seguire.

In particolare, all'art. 28-bis si fa menzione dell'attività di autovalutazione dei rischi di riciclaggio e di finanziamento del terrorismo, attraverso una metodologia di *risk assessment* che deve essere strutturata in due distinte macro-attività: a) valutazione del rischio intrinseco e delle vulnerabilità; b) determinazione del livello di rischio residuo e delle relative attività mitigatrici. Conseguentemente, agli artt. 28-ter e 28-quater l'Autorità si preoccupa di indicare i fattori da prendere in considerazione nella valutazione del rischio intrinseco e nell'analisi delle vulnerabilità, indicando per il primo, a titolo esemplificativo e non esaustivo, l'ammontare dei premi lordi contabilizzati, delle prestazioni liquidate, il corrispondente numero di polizze e di clienti, nonché i mercati geografici di riferimento, la presenza di succursali in paesi terzi ad alto rischio ed altri ulteriori elementi.

Quanto alle vulnerabilità, in esito all'adozione ed attuazione di politiche e procedure idonee a mitigare il rischio intrinseco e tenuto conto dei dati quali-quantitativi emersi in sede di *risk assessment*, l'art. 28-quater suddivide le vulnerabilità in quattro categorie: 1) non significativa; 2) poco significativa; 3) abbastanza signifi-

cata; 4) molto significativa.

Dalla combinazione di queste due macro-attività, le imprese possono determinare, come stabilito dall'art. 28-quinquies e in base all'allegato 1- Tabella C, l'appartenenza ad una data fascia di rischio, grazie alla quale rilevare i gap da colmare e le iniziative correttive da intraprendere.

Brevissime considerazioni finali

La disciplina organica che scaturisce dall'emanazione del Provvedimento in commento, da leggersi in combinato disposto con il Reg. 44/2019, pone l'Italia in prima linea, con gli altri Paesi europei, nella lotta al riciclaggio e al terrorismo anche nel settore assicurativo.

Con essa si configura, dunque, in capo alle imprese di assicurazione a vario titolo richiamate dal Provvedimento, un obbligo di conformità alla disciplina e alle previsioni ivi contenute.

Dette imprese, infatti, nel dare attuazione alle disposizioni, dovranno procedere tempestivamente ad una riorganizzazione della funzione di *compliance*, ricomprendendo nei c.d. controlli di secondo livello pure quelli afferenti alla normativa antiriciclaggio.

In questa prospettiva, le imprese saranno chiamate a costruire e a far adeguatamente funzionare un solido processo strutturato per raccogliere in modo uniforme dalla rete di intermediari assicurativi di cui si avvalgono tutte le informazioni necessarie per elaborare un profilo di rischio, nonché tutte le informazioni necessarie allo svolgimento di una robusta verifica della clientela.

All'agricoltura oltre 2 miliardi di euro dalla manovra finanziaria 2022 per incentivare gli investimenti, la spesa sociale, il lavoro giovanile e la parità di genere

di Olga Bussinello

Agroalimentare e Green Economy

La legge n. 234 del 30 dicembre 2021, pubblicata nella G.U. n. 310 del 31 dicembre 2021 ed in vigore dal 1° gennaio scorso, aggiunge nuove risorse a quelle già previste dal PNRR, circa 4,9 miliardi di euro, e dalla Pac, circa 50 miliardi di euro, per stimolare una crescita del comparto agroalimentare che, attualmente, rappresenta il 17% del prodotto interno lordo. Una strategia complessiva che vede nella sostenibilità ambientale, nell'inclusività e nell'equità sociale i suoi cardini.

Sgravi fiscali e prestiti agevolati per i coltivatori diretti, soprattutto se under 40 e del gentil sesso, fondi per ossigenare le filiere minori, ma anche finanziamenti per la promozione dei prodotti tipici e artigianali e per l'impulso all'internazionalizzazione delle PMI che investono nell'innovazione green e digitale. Sono queste le principali aree di intervento degli importi stanziati dalla Legge Finanziaria 2022 per il Made in Italy agricolo. Alcune di esse rientrano, in realtà, nella programmazione pluriennale dello Stato, come gli sgravi Irpef sui redditi dominicali e sui terreni agricoli e il finanziamento del fondo per sostenere alcune filiere minori come l'apicoltura, la brassicoltura e la canapa. Altre già viste,

come le risorse erogate tramite ISMEA, per la concessione di finanziamenti, operazioni di finanza strutturata o concessione di garanzie a fronte di prestiti agli imprenditori agricoli e della pesca. Ma anche le misure per l'imprenditoria femminile e giovanile e la concessione di contributi a favore dei produttori di vino DOP, IGP e biologico che investano in più moderni sistemi digitali. Nuova, invece, l'istituzione di alcuni Fondi, come quello per la valorizzazione dei prodotti agroalimentari tradizionali e certificati e quello per l'enogastronomia e pasticceria italiana o i budget previsti per dare attuazione alla Strategia forestale nazionale, per lo sviluppo delle montagne italiane, per misure di tutela del territorio e per la prevenzione delle infestazioni fitosanitarie da *Ips typographus*.

Incentivi all'agricoltura e tutela del patrimonio naturale

Fondo mutualistico nazionale

Per fare fronte alle richieste economiche del settore vessato dalle catastrofi meteorologiche, viene istituito un Fondo mutualistico nazionale di 50 milioni di euro per il 2022. Il nuovo Fondo che dovrebbe rispondere più rapidamente e soddisfacen-

temente del Fondo di solidarietà nazionale dedicato agli interventi indennizzatori, dimostratosi spesso inadatto perché privo di sufficiente capienza economica nell'immediatezza dell'evento e per questo non compensativo dei danni subiti. Con decreto del Ministro delle politiche agricole alimentari e forestali sono definite le disposizioni per il riconoscimento, la costituzione, il finanziamento e la gestione del fondo. Oltre a questo stanziamento sarà comunque possibile accedere al succitato Fondo di solidarietà nazionale, che conta una disposizione a tal fine di 161 milioni di euro, e ad un fondo mutualistico su scala nazionale di nuova costituzione che consenta a tutti gli agricoltori di dotarsi di strumenti per la gestione del rischio. Quest'ultimo, previsto fra gli obiettivi del PNRR, prevede l'obbligo dell'accantonamento annuo del 3% delle risorse del primo pilastro. Operativamente, il fondo verrà gestito da Ismea tramite una società di capitali dedicata: Sistema Informativo Nazionale per lo sviluppo dell'Agricoltura S.p.a. (SIN spa). Il Sian, invece, verrà utilizzato per gestire i servizi informatici. Ismea opera da garante o co-garante con altri soggetti accreditati, verso banche Istituti di credito agrario e intermediari finanziari per prestiti o finanziamenti alle imprese agricole, agroalimentari e della pesca. Le garanzie possono essere prestate anche per titoli di debito in possesso di Organismi di investimento collettivo del risparmio (OICR), le cui quote o azioni siano collocate esclusivamente presso investitori qualificati. La SIN spa avrà a disposizione un conto corrente di tesoreria centrale, sul quale confluiranno le somme destinate al finanziamento del Fondo. Il trasferimento verrà fatto dal Ministero delle politiche agricole alimentari e forestali, assegnatario delle somme. Nelle more dell'emanazione del Decreto Ministeriale che definirà l'operatività del Fondo, si applica il decreto del Ministero delle politiche agricole alimentari e forestali 5 maggio 2016, n. 10158. Infine, per garantire la copertura del maggiore fabbisogno finanziario dovuto al presente fondo mutualistico e alle misure dedicate alle assicurazioni agricole nel PSR Nazionale, verranno aggiunti oltre 178 milioni di euro ogni anno dal 2023 al 2027 sul Fondo

di Rotazione.

Decontribuzione per i coltivatori diretti e imprenditori agricoli under 40

I nuovi iscritti alla previdenza agricola che presenteranno la domanda entro il 31 dicembre 2022 potranno avvantaggiarsi dell'esonero al 100% del versamento contributivo presso l'Assicurazione Generale Obbligatoria per l'invalidità, la vecchiaia ed i superstiti. Non è possibile cumulare l'esonero in questione con altri o con riduzioni di aliquote di finanziamento previste dalla Legge, incaricando l'Inps di effettuare le relative verifiche da inviare mensilmente ai Ministeri interessati. Al fine di rispettare i limiti posti dai Regolamenti Europei in materia di aiuti "de minimis", l'Inps ha fornito tutte le indicazioni per accedere all'esonero e ha istituito un conto (GAW37469) per rilevare gli sgravi di oneri contributivi a favore dei beneficiari. Per quanto riguarda la misura della contribuzione dovuta dagli agricoltori under 40, l'aliquota vigente dal 2018 è pari al 24% del reddito determinato per la singola azienda, a cui va aggiunto un contributo addizionale giornaliero. La misura interessa circa 10.000 nuovi iscritti per il 2022, di cui 7800 nella categoria coltivatori diretti e 2200 come imprenditori agricoli professionali.

Incentivi all'imprenditoria agricola femminile e potenziamento della competitività delle imprese agricole e agroalimentari

Sono previsti 50 milioni di euro di finanziamenti per il 2022 che l'ISMEA riconoscerà alle società, economicamente e finanziariamente sane, che operano nella produzione, trasformazione e commercializzazione dei prodotti agricoli, della pesca e dell'acquacoltura e ai beni prodotti nell'ambito delle relative attività agricole connesse. Requisito essenziale è la qualifica agricola della società, comunque costituita. Le formule di finanziamento passano dal ruolo di socio di minoranza, sottoscrivendo aumenti di capitale ovvero prestiti obbligazionari o strumenti finanziari partecipativi, alle operazioni di acquisizione di partecipazioni dove l'ISMEA stipula accordi con gli altri soci, o eventualmente terzi, che si impegnano a riscattare al valore di mercato, le partecipazioni acquisite. Nel caso di inter-

venti a condizioni agevolate, l'ISMEA può erogare mutui di durata massima di 15 anni. Per l'imprenditoria femminile in agricoltura, sono previste agevolazioni analoghe a quelle previste per il ricambio generazionale e per l'imprenditoria giovanile. Cambiano, quindi, le regole per l'accesso, che in passato prevedevano sia la presenza rosa che la giovane età del o dei titolari, sia nella fase di start up, che nel subentro aziendale. Viene, in particolare, eliminato il riferimento alla "metà numerica dei soci" per quanto riguarda il requisito di composizione delle società subentranti, quale condizione determinante perché le stesse possano essere ammesse a beneficiare delle agevolazioni previste. Inoltre, viene incrementato per il 2022 di 5 milioni di euro il Fondo rotativo per favorire lo sviluppo dell'imprenditoria femminile in agricoltura (istituito dalla legge di bilancio per il 2020), destinando tali risorse sia alle agevolazioni legate alla crescita dell'imprenditorialità rosa, che al ricambio generazionale in favore delle sole imprese agricole a prevalente o totale partecipazione femminile. Il Fondo prevede, tra l'altro, la possibilità di ottenere mutui a tasso zero in favore di iniziative finalizzate allo sviluppo o al consolidamento di aziende agricole condotte da imprenditrici

attraverso investimenti nel settore agricolo e in quello della trasformazione e commercializzazione di prodotti agricoli. Tali mutui sono concessi nel limite di 300.000 euro, con una durata massima di 15 anni, comprensiva del periodo di preammortamento. Infine, viene istituito un Fondo per la rilevazione dei prezzi in agricoltura, con una dotazione di 500.000 euro per il 2022, di cui 50.000 euro riservati alle attività di rilevazione nel settore dell'olio. L'obiettivo è quello di coadiuvare le filiere attraverso una corretta programmazione della politica agricola comune, disponendo ed utilizzando dati, studi e valutazioni specifiche, necessari a definire le strategie settoriali. Sempre per sostenere la competitività delle aziende e delle filiere vengono riconfermate le agevolazioni già previste per la cessione di animali vivi della specie bovina e suina e per le carni. Nel primo caso viene riconfermata per il 2022 la compensazione dell'iva al 9,5%, originariamente prevista in via eccezionale per il 2021. Si ricorda che, ante covid 19, la detrazione forfettaria era prevista solo per imprese con minimi volumi d'affari (7000 euro annui) e con un tetto massimo di minori entrate per lo Stato di 20 milioni di euro annui. Entrambe le condizioni sono state eliminate anche per





il 2022. Nel secondo caso, 30 milioni di euro dei fondi destinati nel 2022 a sostegno delle filiere agricole e agroalimentari, pari ad 80 milioni di euro, dovranno essere accantonati per il comparto delle carni bianche, domestiche e selvatiche per alimentazione umana, e uova in genere.

Strategia forestale Nazionale

Per assicurare l'attuazione della tutela e della valorizzazione delle colture forestali e della loro utilizzazione socioeconomica, vengono attribuiti al suddetto Fondo 30 milioni per gli anni 2022 e 2023, e 40 milioni per ciascun anno dal 2024 al 2032. Il Fondo è nelle disposizioni del MIPAAF, che dovrà adottare entro marzo 2022, di concerto con il Ministro dell'economia e delle finanze, previa intesa in sede di Conferenza Stato-regioni, i criteri e le modalità di utilizzo delle risorse destinate al patrimonio forestale italiano. La Strategia forestale nazionale ha una validità di venti anni ed è soggetta a revisione e aggiornamento quinquennale.

Misure di sostegno alle PMI

Proroga del credito d'imposta per le spese di consulenza relative alla quotazione delle PMI

La misura non è nuova, in quanto già prevista dalla Legge di bilancio del 2018. Nuove sono le condizioni che estendono il credito di imposta per tutto il 2022, abbassando il tetto massimo di credito da 500 mila euro a 200 mila euro. Destinatari sono tutte le PMI che si avvalgano di consulenze per l'ammissione alla negoziazione su mercati regolamentati o sistemi multilaterali di negoziazione (Multilateral Trading Facility - MTF) europei, ottenendo la compensazione del 50% delle spese sostenute. L'incentivo vuole creare canali di finanziamento alternativi rispetto al credito bancario, che vanno dall'emissione di specifici strumenti di debito (cd. mini-bond), alla raccolta tramite portali on-line (cd. crowdfunding), ad altre forme di incentivazione fiscale a favore di chi decida di investire in azioni o altro, emessi da PMI. Operativamente, esso va indicato nella dichiarazione dei redditi relativa al periodo d'imposta in cui è maturato e nelle dichiarazioni dei redditi relative ai periodi d'imposta successivi, fino a completamento dell'importo massimo consentito. Inoltre: non concorre alla formazione della base imponibile IRPEF, IRES e IRAP; non rileva ai fini della determinazione della percentuale di deducibilità degli interessi passivi di cui all'articolo 61 del D.P.R. n.

917 del 1986 (Testo Unico delle Imposte sui Redditi - TUIR); non rileva rispetto ai criteri di inerenza per la deducibilità delle spese, di cui all'articolo 109, comma 5, del TUIR e si applicano inoltre il limite annuale di utilizzazione di 250.000 euro, previsti dall'articolo 1, comma 53 della legge n. 244 del 2007.

Rifinanziamento della misura "Nuova Sabatini"

Per le piccole e microimprese viene rifinanziata la Nuova Sabatini in tre differenti

step. Vengono attribuiti: 240 milioni di euro per ciascuno degli anni 2022 e 2023, 120 milioni per ciascuno degli anni dal 2024 al 2026 e 60 milioni per l'anno 2027. E', inoltre, previsto che il contributo possa essere erogato in più quote per finanziamenti superiori a 200.000 euro, ovvero in una sola soluzione fino a tale importo. L'obiettivo è quello di garantire continuità ai finanziamenti iniziati ante Covid 19 delle piccole e microimprese italiane per supportarne la competitività.

PMI (art. 2 dell'allegato alla Raccomandazione della C. E. n. 361 del 6 maggio 2003)	
PMI	Meno di 250 persone e fatturato entro 50 milioni di euro o bilancio entro 43 milioni di euro
Piccole imprese	Meno di 50 dipendenti e fatturato o bilancio annuo entro i 10 milioni di euro
Microimprese	Meno di 10 dipendenti e fatturato annuo o bilancio entro i 2 milioni di euro

Potenziamento dell'internazionalizzazione delle imprese

Vengono rimpinguati i finanziamenti destinati a supportare la crescita del Made in Italy all'estero destinando 1,5 miliardi per ciascuno degli anni dal 2022 al 2026 al Fondo rotativo a favore delle imprese italiane che operano sui mercati esteri (Fondo 394/1981), mentre vanno 150 milioni di euro annui per ciascuno degli anni dal 2022 al 2026 al Fondo per la promozione integrata (art. 72 del D.L. 17 marzo 2020,

n. 18). Le risorse devono, pertanto, considerarsi aggiuntive a quelle già previste nel PNRR, che prevede un finanziamento pari a 1,2 miliardi al Fondo Rotativo 394/1981 gestito da Simest, attribuendo 800 milioni alla Sezione Prestiti (finanziamenti a tasso agevolato ai sensi del D.L. n. 112/2008) e 400 milioni alla Sezione Contributi (cofinanziamenti a fondo perduto fino al 50% di quanto concesso a tasso di favore dalla sezione prestiti).

PNRR – obiettivo 5: Politiche industriali di filiera e internazionalizzazione
<p>Sono destinati 1,2 miliardi di euro al Fondo Rotativo 394/1981 per potenziare la competitività delle PMI a seguito della pandemia. Per concedere contributi e prestiti il CDA del Fondo deve stabilire i criteri che dovranno rispettare alcune condizioni:</p> <ul style="list-style-type: none"> • il progetto da finanziare deve rientrare per natura e portata fra le attività che, sotto il profilo della sostenibilità, "non arrecano danno significativo" all'ambiente; • gli interventi che si sosterranno; • i beneficiari che devono essere PMI e i criteri di ammissibilità; • possibilità di reinvestire in progetti analoghi quanto residua, perché inutilizzato, anche oltre il 2026, se non deve coprire rimborsi e/o interessi;

Per quanto riguarda il Fondo Rotativo 394/1981, dall'ottobre 2021 sino a maggio 2022, sarà possibile presentare domande di contributo sino ad esaurimento risorse,

seguendo i criteri della Delibera quadro del comitato agevolazioni del 30 settembre 2021. Sono ammesse diverse tipologie di interventi.

Interventi ammessi FR 394/1981	
Transizione digitale ed ecologica delle PMI spa con vocazione internazionale	10% di export per ultimo anno o 20% nel biennio e 50% del finanziamento destinato a spese per transizione digitale e il resto per sostenibilità e internalizzazione
Sviluppo del commercio elettronico delle PMI spa in Paesi esteri	Piattaforma propria di e-commerce o di terzi con importi da 10 a 300 mila euro per la strutturazione in proprio e 200 mila euro per supportare il market place
Partecipazione delle PMI a fiere e mostre internazionali e missioni di sistema	150 mila euro anche per un solo evento, anche virtuale, con un 30% della spesa per il digitale o a carattere ecologico

NB: I tre diversi interventi prevedono criteri differenziati di incentivo a seconda della sede operativa dell'azienda. Per le PMI con sede operativa in una Regione del Mezzogiorno, il cofinanziamento a fondo perduto arriva al 40%, mentre per tutte le altre al

25%. Circa 480 milioni del FR sono riservati al Mezzogiorno. Restano ferme sia il preventivo assenso della Commissione europea sull'erogazione e sulla verifica del rispetto del Regolamento EU sugli aiuti di stato.

Fondo per la promozione integrata	
Finalità	Supportare in sinergia con il FR394/1981 gli investimenti esteri delle PMI
Dotazione finanziaria	Dai 150 milioni iniziali nel 2020 è stato più volte rifinanziato per un incremento totale di 613 milioni di euro. Nel 2021 è stato rifinanziato per 610 milioni di euro e di 60 milioni di euro per ciascun anno del 2022 e 2023
Attività ammesse	<ul style="list-style-type: none"> campagna straordinaria di comunicazione per sostenere le esportazioni e il sistema economico nazionale nei settori colpiti dal Covid 19, anche avvalendosi di ICE; attività di promozione in collaborazione con ICE e MAECI; cofinanziamento attività all'estero di altre PA; concessione di cofinanziamenti a fondo perduto fino al 50% dei finanziamenti concessi sul Fondo Legge n. 394/1981

Incentivi alle filiere, all'economia circolare e ai prodotti artigianali e certificati

Fondo valorizzazione prodotti agroalimentari tradizionali e certificati

Viene destinato 1 milione di euro per l'anno 2022 per favorire la transizione ecologica della Ristorazione, che dovrà utilizzare prevalentemente prodotti della propria regione o di zone limitrofe ad essa. Il Fondo, istituito presso il MIPAAF, diverrà operativo

con decreto dello stesso dicastero, che definirà natura e requisiti degli incentivi e delle agevolazioni legati all'utilizzo dei prodotti tradizionali, così come definiti dall'art. 8 del DM n. 350 del 1999 e previsti nell'apposito elenco presso lo stesso MIPAAF.

Incentivi all'installazione di impianti di compostaggio presso i centri agroalimentari
È previsto 1 milione di euro da riconoscere



ai centri agroalimentari del Mezzogiorno che si dotino di un impianto di compostaggio per i rifiuti organici. Il beneficio verrà riconosciuto sotto forma di credito d'imposta al 70% sulle dichiarazioni relative alle spese sostenute nel 2022, purché l'impianto sia in grado di smaltire almeno il 70% dei rifiuti organici prodotti dallo stesso centro. Criteri e modalità per accedere al beneficio saranno definiti con provvedimento dell'Agenzia delle Entrate. Non è previsto né il tetto massimo annuo dei 250.000 euro, né quello per la compensabilità previsto dalla Legge n.388/2000. Resta, invece, l'obbligo del rispetto del "de Minimis".

Lotta all'insetto Bostrico nelle zone Alpine

Viene istituito presso il MIPAAF un fondo di 6 milioni per gli anni 2022 e 2023 per combattere le infestazioni boschive dell'insetto Bostrico. A seguito della Tempesta Vaia nel 2018 e della proliferazione fra gli alberi abbattuti della popolazione dell'insetto *Ips typographus*, nel corso di tre anni, si è assistito ad una vera emergenza fitosanitaria ai danni del patrimonio Silvo-forestale italiano. Dovendo procedere ad una bonifica delle zone interessate dalla presenza dell'insetto ovvero di rimozione e distruzione del materiale ligneo abbandonato sul terreno e fonte di nutrimento del parassita, è necessario sviluppare un'azione gestionale integrata, volta alla prevenzione e basata sul mantenimento di buone con-

dizioni del rimboschimento, che coinvolga anche i soggetti privati proprietari di aree Silvo-colturali all'interno o confinanti con i boschi demaniali. A tal fine Le Regioni e Province Autonome:

- autorizzano i privati proprietari o detentori a qualsiasi titolo di boschi minacciati dal parassita al taglio delle piante e al riconoscimento legale dei tronchi con la massima urgenza;
- in caso di inerzia dei privati o di impossibilità di determinare un titolare (terreni silenti) procedono autonomamente alla bonifica dell'area.

I proprietari dei terreni possono dimostrare il titolo anche mediante autocertificazione nella fase di urgenza, salvo poi essere oggetto di verifica da parte della stessa PA. Per 7 anni gli stessi proprietari possono procedere, con comunicazione alla PA competente, alle operazioni urgenti di prevenzione più adeguate, inclusi gli abbattimenti con rilascio in loco delle piante o allontanamento delle stesse previa scortecciatura. Per gli interventi pubblici è previsto il ricorso al sistema ad evidenza pubblica nella fase di programmazione e alla procedura negoziata nei casi di urgenza.

Valorizzazione internazionale dei patrimoni culturali immateriali agro-alimentari e agro-Silvo-pastorali (UNESCO)

Istituito il Fondo Unesco per i patrimoni immateriali italiani con una dotazione di 2



milioni di euro per l'anno 2022, di cui 500 mila riservati alle nuove iscrizioni alla Lista tenuta presso il Mipaaf, che detiene anche il Fondo. Patrimonio culturale immateriale, secondo l'art. 2 della Convenzione di Parigi del 17 ottobre 2003, sono "le prassi, le rappresentazioni, le espressioni, le conoscenze, il know-how che le comunità (o i gruppi) riconoscono in quanto parte del proprio patrimonio culturale. Tale patrimonio culturale immateriale, ai sensi della stessa disposizione, è costantemente ricreato dalle comunità in risposta al proprio ambiente, alla propria storia dando, alle stesse comunità, un senso d'identità e di continuità."

Incentivi alle filiere apistica, della frutta a guscio e delle filiere minori, alle erbe officinali e al sughero nazionale

La dotazione del fondo per la tutela e il rilancio delle filiere apistica, brassicola della canapa e della frutta a guscio, viene rimpinguata di 12,75 milioni di euro per il 2022 e di 5 milioni di euro per ciascuno degli anni 2023 e 2024. Vengono altresì stanziati 7,75 milioni per il 2022, a favore delle organizzazioni di produttori apistici a livello nazionale e per la stipula di accordi professionali. Per la coltivazione della nocciola sono previsti 300 mila euro per ciascuno degli anni dal 2022 al 2024. Criteri e

modalità saranno previsti in un successivo Decreto del MIPAAF. Istituito anche il Fondo per lo sviluppo delle colture di piante aromatiche e officinali biologiche, presso il Ministero delle politiche agricole alimentari e forestali, con una dotazione di 500.000 euro per ciascuno degli anni 2022, 2023 e 2024. Infine, per promuovere la qualità del sughero nazionale, ci saranno 150 mila euro per il 2022 per finanziare il monitoraggio, a cura dell'Università di Sassari, della diffusione di un insetto nocivo, il *Coraeus undatus*.

Fondo per il sostegno dell'enogastronomia italiana

Viene istituito (anche per la pasticceria), con una dotazione di 20 milioni di euro per ciascuno degli anni 2022 e 2023. L'obiettivo è quello di promuovere e sostenere le eccellenze della ristorazione e della pasticceria italiana valorizzando il patrimonio agroalimentare ed enogastronomico italiano, incentivando le assunzioni di giovani diplomati nei servizi dell'enogastronomia e dell'ospitalità alberghiera da parte dei datori di lavoro privati. Criteri e modalità di uso del Fondo saranno definiti con Decreto del Ministro delle politiche agricole alimentari e forestali di intesa con il Ministro del lavoro e delle politiche sociali.

CeFor
● SEAC

**Il tuo Centro
di Formazione**

vai al nuovo sito
di Seac Cefor



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.