ISSN 2784-8213

COMPLIANCE

Luglio 2021 - n. 2 - mensile - copia omaggio

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

SEAC

SEAC

Passione
per semplificare le cose

- Obiettivi essenziali: performance, autonomia, conciliazione vita-lavoro
- Disciplina del lavoro agile prima e durante il lock-down
- Profili giuridici nella PA: risposte emergenziali e obiettivi di efficienza
- Misure organizzative di sicurezza e responsabilità penale di società e datori di lavoro
- Strumenti e sicurezza informatica per il lavoro via web
- Tutela della riservatezza per la persona e per le informazioni
- Ascolto, recovery, formazione: psicologia online e realtà virtuale

La pubblicazione, dedicata allo smart working, rappresenta una guida pratica per fornire a imprese, pubbliche amministrazioni, datori di lavoro, manager, professionisti e lavoratori consigli pratici su un fenomeno che sta modificando la fisionomia di aziende e pubbliche amministrazioni nonché usi, costumi e configurazione urbanistica del territorio.

Il testo offre un'analisi della disciplina del lavoro agile sotto molteplici punti di vista: dalla sicurezza sul lavoro alle responsabilità penali di datore di lavoro e società, dalla tutela della privacy alla sicurezza informatica, dalla conciliazione vita-lavoro al controllo delle performance.

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

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

00
Editoriale
Professionisti e consulenti di governance
Pag. 07

01
Sicurezza&Performance
PMI e governance. Un caso di innovazione organizzativa in contesto di passaggio generazionale
Pag. 9

02
Import-Export
L'accordo UE e UK in seguito alla Brexit: i profili doganali da tenere presente per i consulenti e le imprese
Pag. 16

03
Rapporti tra imprese e P.A.
Aggiornamenti in tema di organismo di Diritto pubblico
Pag. 24

04
Rapporti tra imprese e P.A.
La conoscibilità degli atti amministrativi: strumenti, diritti e poteri nei rapporti con la Pubblica Amministrazione
Pag. 31

05
Anticorruzione
Transizione del Modello 231 da un approccio per famiglie di reato a un approccio per processi: i vantaggi in un'ottica di controllo e verifiche.
Pag. 40

06
Antiriciclaggio
Il trattamento dei dati personali nelle operazioni societarie straordinarie
Pag. 47

07
Sicurezza Informatica
Incident response. come gestire un attacco informatico
Pag. 53

08
Sicurezza&Performance
Strumenti innovativi di valorizzazione dell'impresa: il ruolo del professionista e dell'influencer
Pag. 65

09
Privacy
Dalla sentenza Schrems II al Provvedimento BayLDA su Mailchimp: il problema aperto del trasferimento dei dati personali verso gli USA
Pag. 73

10
Privacy
Data breach: le Linee guida dell'EDPB e le "istruzioni" del Garante privacy
Pag. 83

11
Agroalimentare e Green Economy
I crimini legati al ciclo dei rifiuti: modi operandi, attori e modalità di contrasto
Pag. 92

Hanno contribuito alla realizzazione di questo numero

Daniela Andreatta: Security Analyst presso Intellegit e collaboratrice di supporto alla didattica per l'Università di Trento. Le sue aree di ricerca riguardano soprattutto i crimini ambientali, la sicurezza urbana e l'analisi di dati sulla criminalità.

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

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

Anna Capoluongo: Avvocato | DPO | Membro Gruppo di Lavoro sull'Intelligenza Artificiale di ANORC | Docente a c. | Vice presidente I.R.L.E.S.S.| Iscritta all'albo dei Maestri della Protezione dei Dati (IIP)

Anna Maria Carbone: Avvocato nel Foro di Matera, RPD/DPO certificata UNI 11697:2017; compliance aziendale D.Lgs.231/01 – Organismo di Vigilanza, prevenzione della corruzione, expert e lead auditor UNI ISO 37001:2016.

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

Giovanni Comazzetto: Avvocato del Foro di Padova e dottore di ricerca in Diritto costituzionale (Università di Padova). Si occupa prevalentemente di diritto amministrativo e civile; ha scritto diversi articoli sui profili costituzionalistici dell'integrazione europea, e partecipato a numerosi convegni sia in Italia che all'estero.

Clarissa Conte: Avvocato, funzionario amministrativo incardinato presso il Servizio Politiche Sociali della Provincia di Trento.

Nicola Alberto De Carlo: Direttore di TPM, rivista internazionale per l'analisi del comportamento individuale e collettivo. Docente universitario, svolge attività professionale su temi di compliance, miglioramento organizzativo, prevenzione stress lavoro-correlato e performance nel lavoro.

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

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

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

Alberto Giustini: Laureato in economia e management presso l'università Tor Vergata di Roma con esperienza lavorativa in ambito risk management e 231/01. Attualmente Compliance Officer di numerose società di diritto estero. Certificato CEPAS Membro OdV / Esperto D.Lgs 231/2001

Roberto Giordani: Ha esperienza manageriale trentennale per aziende appartenenti a gruppi internazionali, coprendo cariche sociali. Dal 2009 è libero professionista, con focus su consulenza direzionale, sviluppo organizzativo e compliance, controllo strategico e modelli di governance. Copre incarichi di revisione, collegi sindacali e Organismi di Vigilanza ex d.lgs. 231/2001.

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.

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

Editoriale

Professionisti e consulenti di governance

di Nicola Alberto De Carlo

Le PMI sono più impegnate nella navigazione a vista e nella salvaguardia della propria efficienza giorno per giorno che nella progettazione, anche strategica, delle *opportunità* e dello *sviluppo*. Il che è comprensibile ma può costituire motivo di preoccupazione per il futuro, date le trasformazioni spesso repentine e non facilmente governabili nei *contesti sociali*, nel *mercato* e negli *ambiti giuridico/economici* di riferimento. Occorre dunque rafforzare in ogni modo l'interazione costante e costruttiva fra i *professionisti,* che operano per contribuire al miglioramento degli obiettivi e dei contenuti delle azioni aziendali, ed imprenditori e manager, che di esse hanno la diretta responsabilità. Ciò in una prospettiva – strutturale – di *stimolo reciproco*, di lungimiranza, di comune attenzione alle sfide presenti e future, così come agli assetti e alle dotazioni che meglio potranno dare le risposte sperate. In tal senso vanno gli obiettivi e le procedure descritti nell'articolo "*Innovazione organizzativa in un contesto di passaggio generazionale*" riportato nelle pagine della nostra rivista. Oltre che essere un sintetico vademecum operativo, esso costituisce un efficace esempio di stimolo reciproco e di costruttiva collaborazione realizzata fra l'imprenditore e il *professionista-consulente di governance*. Ancora in tema di *consulenza alla governance*, si segnalano i lavori tecnico-scientifici e applicativi più avanti riportati. Essi vanno dalla necessità di dare risposta alle *conseguenze doganali* connesse alla *Brexit* – tema di rilevante attualità economica – ai rapporti fra imprese e pubbliche amministrazioni, in riferimento all'istituto dell'*organismo di diritto pubblico* e alla *conoscibilità degli atti amministrativi* in base ai diritti e doveri fra le parti. Adeguati spazi vengono dati alle possibili applicazioni in tema di *modello 231* – da un approccio per famiglie di reato a un approccio per processi – al trattamento dei dati e alla privacy, anche in relazione a operazioni societarie straordinarie, alla *salvaguardia dei dati informatici* in risposta a possibili attacchi, al trasferimento dei dati personali verso gli USA, ai crimini legati al ciclo dei rifiuti e alle modalità di contrasto.

SEAC **SERVIZI ASSICURATIVI**

Polizze di responsabilità civile per i professionisti

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

Seac Servizi Assicurativi S.r.l.
Broker di assicurazioni

T. 0461.805.418
assicurazioni@seac.it
assicurazioni.seac.it

PMI e governance. Un caso di innovazione organizzativa in contesto di passaggio generazionale

di Roberto Giordani

Lo scenario in cui agisce la PMI sta mutando con crescente accelerazione. Tutti i fattori che incidono sulla gestione della PMI continuano a combinarsi in modalità instabile e imprevedibile ed alcuni fattori prendono casualmente il sopravvento su altri. Solo per citare qualche esempio, i sistemi di gestione e di controllo dei processi, le strategie e le politiche aziendali, le infrastrutture e le tecnologie si scontrano spesso con condizioni di mercato, rischi politici e abitudini del consumatore, regolamenti nazionali e sovranazionali. Da ultimo, la pandemia da Covid-19 sta influendo da oltre un anno in modo devastante sulla gestione della PMI; tantoché gli elementi di criticità fisiologicamente influenti sulla gestione hanno lasciato spazio a ben più gravi contingenze e problematiche, in un groviglio di complessità inimmaginabile.
In tale contesto emerge con chiara evidenza l'importanza della *governance* aziendale e del sistema di controllo interno, a cui molte PMI non hanno mai attribuito sufficiente attenzione.
Di conseguenza molte PMI si dimostrano impreparate ad affrontare le conseguenze di eventi imprevisti di notevole portata come la pandemia, subendo di riflesso i gravi effetti della perdita di quote di mercato, come crescente difficoltà di incasso dei crediti e di ottenimento di credito dal sistema, degenerando in situazioni di crisi anche irreversibile da squilibrio economico e/o finanziario.
Altre PMI, la minoranza, più accorte alla gestione dei rischi e dotate di adeguati sistemi di *governance* e di controllo interno, subiscono in minor misura gli effetti della pandemia o addirittura presentano risorse capaci di reagire, realizzando vantaggi competitivi.
Nel seguito si riporta il caso di una PMI che ha felicemente adottato un progetto di innovazione organizzativa, quale presidio a garanzia dello sviluppo e della continuità, in un connubio di esigenze familiari e aziendali. Il progetto è arrivato ad un punto di realizzazione avanzata e può costituire modello di riferimento per le numerose PMI la cui conduzione è unicamente nelle mani del fondatore.

Introduzione
È testimoniato sempre più diffusamente che adeguati sistemi di *governance* e di controllo interno favoriscono la conduzione dell'impresa.
Il sistema di *governance* non si riduce alla scelta della forma societaria, tra società di persone o società di capitale; e neppure è limitato alla scelta della struttura dell'organo societario, tra organo uninominale o organo collegiale. Il sistema di *governance* dell'impresa deve semmai concretizzarsi in un appropriato modello aziendale, dinamicamente adeguato alle mutevoli situazioni del contingente: ogni impresa deve adottare quello più appropriato alle dimensioni ed al proprio contesto di mercato e di interlocutori, nonché funzionale al processo di sviluppo e delle relative situazioni di rischio. Il sistema di *governance* consiste quindi in un complesso di dotazioni, meccanismi e modalità consone alle specifiche esigenze di gestione e finalizzato

all'accrescimento del valore aziendale.
Il controllo interno assicura che standard, regole e procedure siano correttamente applicate e favorisce l'aggiornamento di queste ultime in relazione al mutare dell'organizzazione e delle norme o regole di mercato.
Le imprese a dimensione internazionale, strutturate in forma di gruppo oppure quotate, hanno introdotto già da tempo appropriati sistemi di *governance*, consoni a prevenire situazioni di crisi.
Le PMI, invece, sono in generale tuttora carenti di un appropriato sistema di *governance* aziendale e del relativo sistema di controllo.
L'assenza del solo controllo contabile e la noncuranza nell'identificazione, classificazione e valutazione in modo adeguato di fattori chiave come i ricavi, margini, oneri finanziari, indebitamento, inventari, eccetera può determinare scelte non condivise ed affrettate e quindi inappropriate o addirittura pericolose: decisioni individuali dell'imprenditore-padrone, non supportate da rendiconti finanziari strutturati e ricorrenti, si possono rivelare catastrofiche e irreversibili.
Il processo di cambiamento, per quanto lento, sembra tuttavia avviato. È altrettanto innegabile che le PMI che investono su una *governance* efficace ed integrata con idonei sistemi di *audit* raggiungono prima e meglio il successo, godendo, tra l'altro, di molteplici benefici quale ad esempio facilità di accesso al credito.

Una realtà del territorio: passaggio generazionale e *governance*

Si riporta il caso di una PMI del territorio di cui si mantiene l'anonimato, denominata per praticità "Alfa S.p.a." o più semplicemente "Alfa".
La società Alfa S.p.a. è impresa che opera da alcuni decenni nel settore della produzione e commercializzazione di prodotti destinati al canale B2B. È giuridicamente organizzata nella forma di società di capitali. L'area geografica di influenza è il territorio dell'Italia settentrionale e centrale e conta su circa 200 addetti.
Alfa è nata come impresa a connotazione tipicamente familiare. L'Imprenditore e Presidente è abile, accorto e consapevole dei propri limiti. L'organo amministrativo è da sempre rappresentato da un consiglio di amministrazione composto dai due componenti di prima generazione della famiglia; di cui uno è assiduamente presente in azienda, l'Imprenditore, mentre l'altro limita la presenza e l'operatività ad occasioni più diradate.
L'Imprenditore ha sempre condotto l'impresa con la determinazione di farla crescere con gradualità ed equilibrio, adottando tra l'altro un efficace sistema di controllo diretto cosiddetto "a vista", con impiego di inusuale intuito.
L'Imprenditore ne ha sempre assunto il ruolo di presidente e direttore generale, con connotazioni di eccezionale capacità nel marketing e altrettanto considerevoli capacità negli acquisti e nei progetti di rinnovamento tecnologico.
La gestione aziendale è stata da sempre imperniata su rapporti fiduciari, inizialmente con l'adozione di poche regole scritte: i processi erano basati su prassi ricavate dalla pratica quotidiana trasmessa per affiancamento ed ottimizzata con addizione allargata di buon senso, coinvolgimento e passione.
L'Imprenditore ha regolarmente investito in automatizzazione dei processi dal ciclo passivo al ciclo attivo, inclusi trasformazione, deposito e movimentazione, oltre a presenza sul web e nei social network. Inoltre, ha sempre cercato di coinvolgere le risorse umane, dando preferenza a quelle orientate alla fidelizzazione e disponibili a condividere ed approvare le scelte superiori. L'Imprenditore ha sempre gestito in modo familiare ed aperto, favorendo scambio di idee e informazioni con riunioni prevalentemente spontanee, informali ed estemporanee.
Negli ultimi dieci anni l'Imprenditore ha iniziato ad introdurre i figli in azienda. I figli erano scolarizzati ma carenti di esperienza aziendale. Pertanto, il compito loro assegnato è stato inizialmente legato a funzioni di natura operativa con assoggettamento alla supervisione dei vari responsabili, alla cui area erano stati assegnati. Era previsto che solo dopo un adeguato periodo di accrescimento di conoscenze tecnico-professionali, i figli avrebbero potuto ambire alla copertura di ruoli di crescente responsabilità ed autonomia.
Contemporaneamente, l'Imprenditore aveva avvertito la necessità di implementare un sistema di controllo costruito su un cosiddetto "pannello di controllo di gestione", da cui ricavare giornalmente informazioni sui risultati di gestione in tempo reale.
Più avanti nel tempo, l'Imprenditore aveva iniziato ad avvertire la necessità di adottare strumenti più evoluti. La sua presenza assidua e continuativa e le sue riconosciute capacità di gestione apparivano oramai non più sufficienti a costituire adeguato presidio di governo dell'impresa, anche in vista dell'ulteriore sviluppo che stava prefigurando nel suo pensiero.
Era iniziato un periodo di profonde riflessioni. L'Imprenditore si dibatteva tra l'obiettivo di dare continuità ad Alfa e di preparare la seconda generazione a condurne lo sviluppo, in sintonia con le risorse non appartenenti alla famiglia e di tutti gli altri fattori organizzativi e, altresì, in relazione alle dinamiche dei concorrenti di mercato.
Si susseguirono pertanto numerosi incontri ed approfondimenti con professionisti. L'Imprenditore è sempre stato aperto a dare ascolto a tutti gli interlocutori potenzialmente capaci di fornirgli adeguati suggerimenti; inoltre, è sempre stato orientato a riflettere accuratamente prima di prendere decisioni importanti; infine ha mantenuto nel tempo la caratteristica di prendersi tutti gli onori ed anche gli oneri di qualsiasi decisione importante. Che tuttavia è sempre stato avvezzo a prendere in prima persona, quale sintesi personale di ampie riflessioni.
Maturava quindi la progressiva necessità di configurare nuovi assetti, definire responsabilità, stabilire regole semplici, chiare e formali e di organizzare un efficace sistema della formazione delle decisioni più importanti (cosiddetto *decision making process*).
Appariva tuttavia difficoltoso e soprattutto inopportuno adottare una soluzione che istantaneamente potesse dare garanzia di preservare nel tempo i valori, quali le conoscenze, le buone relazioni e le competenze, senza creare dannose frustrazioni o rivalità.
Inoltre, il pensiero principe dell'Imprenditore era guidato dall'obiettivo di favorire i meritevoli tenendo conto del connubio azienda-famiglia.

Il progetto di innovazione organizzativa

Era quindi progressivamente maturata una soluzione organizzativa che l'Imprenditore ha sposato e posto in essere. Tale soluzione è imperniata su tre fasi temporali:
• una prima fase prevedeva la costituzione di un comitato tecnico di consuntivazione;
• una seconda fase prevedeva la trasformazione di detto organismo in un comitato direttivo;
• una terza fase prevedeva l'allargamento del consiglio di amministrazione sia a membri di famiglia di seconda generazione, sia ad altri componenti; mantenendo il Comitato direttivo in affiancamento e supporto di tale organo sociale.

L'imprenditore aveva maturato la convinzione che il progetto, per conseguire risultati ottimali, avrebbe comportato uno sviluppo di tempo abbastanza lungo, con durata di almeno dodici mesi relativamente a ciascuna delle due prime fasi.
L'Imprenditore aveva altresì ritenuto necessario illustrare al suo staff i principi di fondo del progetto e i suoi obiettivi.
Innanzitutto, merito, trasparenza e correttezza costituivano presupposti essenziali per far parte delle citate entità. Inoltre, i principi aziendali riguardanti la politica della sicurezza e qualità dei prodotti, dell'ambiente e della sicurezza sul luogo di lavoro e del rispetto della privacy, avrebbero dovuto costituire guida di riferimento del lavoro collegiale. Infine, l'approccio sistemico alla gestione del rischio avrebbe dovuto diventare nuovo *driver* di sviluppo consapevole.
Durante le varie fasi, gli interessati avrebbero dovuto gradualmente accrescere abilità, conoscenze e competenze trasversali, condividendo e scambiando informazioni fino ad assumere ruoli a contenuto propositivo.
Gli obiettivi erano basati sullo sviluppo manageriale delle risorse, in una prospettiva di copertura di ruoli con responsabilità ed autonomie crescenti.
Non da ultimo, l'azienda avrebbe dovuto poter contare su un "governo a responsabilità allargata", a garanzia della continuità e dello sviluppo.

Il comitato tecnico di consuntivazione

Nella prima fase si è deciso di strutturare il comitato tecnico di consuntivazione in staff alla direzione generale. Il comitato era costituito da alcuni responsabili di funzione, tra cui uno dei figli dell'Imprenditore con la funzione di coordinamento del gruppo. I responsabili avevano il compito di raccogliere dati relativi alla propria funzione, predisporre appositi report e riunirsi periodicamente per la consultazione e lo scambio delle informazioni. I dati dovevano essere raccolti a cura del coordinatore del comitato, per la successiva archiviazione. L'Imprenditore partecipava alle riunioni prevalentemente con funzione di *coacher*.
La funzione di presidente della riunione del comitato veniva svolta a turno dai vari responsabili di funzione.
È maturata passo dopo passo la cultura dello scambio e della condivisione delle informazioni, della partecipazione e del contributo alle dinamiche di gestione.
Tale fase è durata circa quindici mesi. Al termine del periodo i figli dell'Imprenditore hanno cominciato a partecipare inizialmente con il ruolo di ospite e successivamente di attore, sempre e comunque in funzione dell'apporto di concrete ed utili informazioni, strutturate per costituire spunto di iniziative.
Grazie al contributo del comitato tecnico di consuntivazione, l'imprenditore ha iniziato a focalizzare aree di miglioramento per affrontare temi di controllo direzionale, miglioramento del clima aziendale, pianificazione di attività, adozione di procedure, eccetera.
Infine, si è diffusa la cultura e l'importanza della riunione formale, programmata ed organizzata nei contenuti, che ciascun partecipante alla riunione era tenuto a preparare ed esporre agli altri partecipanti.

Il comitato direttivo

Nella seconda fase si è deciso che il comitato tecnico di consuntivazione dovesse assumere una configurazione progredita. La denominazione di tale "gruppo di lavoro" venne trasformata in comitato direttivo. I componenti rimanevano gli stessi; la periodicità delle riunioni veniva rigorosamente fissata su base mensile, con possibilità di incontri anche più ravvicinati nel caso di situazioni di criticità o di particolari opportunità. La funzione di presidente del comitato direttivo veniva normalmente coperta da uno dei responsabili con maggior anzianità aziendale.
Il compito del comitato, in aggiunta a quello già assegnato al comitato tecnico di consuntivazione, era quello di preordinare e scambiare informazioni che avrebbero dovuto assumere il profilo di proposta di decisioni di natura operativa, progettuale o strategica. Pertanto, le proposte dovevano essere corredate da apposite analisi, simulazioni e valutazioni quali-quantitative. Le proposte dovevano successivamente essere archiviate, trasmesse alla direzione nella persona del presidente per le valutazioni di propria competenza, ovvero, per valutazioni o decisioni nell'ambito del consiglio di amministrazione, la cui composizione era rimasta immutata rispetto alle origini.
I lavori del comitato direttivo dovevano essere sempre verbalizzati dal coordinatore.
Grazie al lavoro del comitato direttivo, nell'ambito delle risorse si è gradualmente diffusa la cultura della governance, con coinvolgimento più completo dei collaboratori ed ulteriore accrescimento di consapevolezza di ruolo, motivazione e spirito di squadra. Ogni componente del comitato aveva superato i limiti dell'operatività individuale, circonstanziata all'area di propria responsabilità. Aveva incominciato a sentirsi parte di una squadra nel cui ambito le responsabilità erano condivise in modo solidale. Fondamentale è diventata inoltre la predisposizione individuale a contribuire nella formulazione di proposte organiche, finalizzate a fornire orientamento e supporto alla formazione delle più importanti decisioni superiori di gestione.
Tale fase è tuttora in corso di attuazione ed è preparatoria di quella successiva, di avvio oramai imminente, in cui è previsto che il consiglio di amministrazione sia integrato con soggetti interni all'organizzazione, che abbiano maturato competenze e caratteristiche funzionali a tale ruolo.

Il consiglio di amministrazione allargato con affiancamento del comitato direttivo

Come appena illustrato, sono oramai mature le condizioni per l'allargamento del consiglio di amministrazione che nella sua nuova struttura andrà ad operare con il supporto del comitato direttivo.
L'Imprenditore, seguendo il suggerimento dei professionisti che lo stanno affiancando, ha utilmente previsto la dotazione di linee guida per la nomina dei componenti del consiglio di amministrazione.
Tale strumento organizzativo stabilisce i requisiti personali dei componenti del consiglio di amministrazione ed il profilo tecnico-professionale di ciascuno, il numero complessivo dei suoi componenti ed inoltre le varietà di competenze necessarie a formare una composizione articolata e complementare di capacità.
Ne consegue che la nomina alla carica di componente del consiglio di amministrazione presuppone metodologia e obiettività di scelta. È garantita la possibilità di nomina estesa sia ai componenti della famiglia, che a soggetti non appartenenti alla famiglia; o meglio, i componenti della famiglia godono di diritto di nomina al pari degli altri soggetti candidabili alla carica. Indistintamente, la condizione necessaria affinché un soggetto possa far parte del consiglio di amministrazione è il bagaglio personale di competenze, esperienze e capacità di coprire ruoli in organismi collegiali.

I risultati del processo di innovazione organizzativa

Quali sono gli aspetti positivi che si possono catalogare quale ricaduta delle esperienze descritte?
Innanzitutto, i responsabili partecipanti al comitato tecnico di consuntivazione prima e successivamente al comitato direttivo hanno avuto la possibilità di acquisire conoscenza orizzontale dei processi, in un quadro di comprensione complessiva del sistema azienda, utile ad accrescere il coinvolgimento personale su un contesto generale delle dinamiche di gestione. Da ciò sono maturate occasioni di formulare proposte di innovazione organizzativa di natura tecnologia, informatica, di prodotto-processo, di marketing, di comunicazione, di logistica, di riduzione di costi ed efficientamento, eccetera.
Inoltre, i responsabili hanno acquisito consapevolezza dei fattori limitanti lo sviluppo, costituito da componenti interne e componenti esterne. Nella prima categoria si annoverano le risorse finanziarie, dimensionali, tecniche, la formazione e le conoscenze, la propensione al cambiamento, le priorità, le regole interne e tutti i relativi rischi endogeni. Nella seconda, si annoverano le norme ed i regolamenti, il mercato e la competizione, i gusti e le esigenze del cliente, le infrastrutture ed i sistemi socio-economici e politici, nazionali e sovranazionali, oltre ai relativi rischi esogeni.
Ancora, i responsabili hanno compreso l'importanza del lavoro di squadra, il valore dell'autostima e quello della responsabilità d'impresa sia come entità in sé ricca di valori, sia come elemento facente parte dell'intero sistema socio-economico.
Infine, l'Imprenditore ha sperimentato sul campo l'importanza di contare su un gruppo di collaboratori fedeli, originariamente meno propensi al lavoro di squadra, mettendoli in gioco in una dimensione più regolata e formale; gradualmente tali collaboratori hanno valorizzato il confronto programmato ed ordinato nel tempo, i flussi informativi, la predisposizione di documentazione concisa ed efficace, con impulso a pragmatismo e uniformità di vedute ed intenti.

Il Covid-19

La pandemia da Covid-19 non era certo evento programmato dalla maggior parte delle PMI. Tantomeno erano stati preventivamente valutati ed eventualmente quantificati i rischi di tale impatto in termini di effetto economico-finanziario.
Neppure Alfa aveva previsto che la pandemia da Covid-19 avrebbe potuto impattare tanto gravemente sui suoi risultati di gestione.

Tuttavia, Alfa aveva anticipatamente predisposto delle risorse organizzative adeguate ad affrontare attivamente la situazione emergenziale causata dal Covid-19. Grazie al progresso nella cultura organizzativa ed alla dotazione del comitato direttivo, Alfa ha potuto affrontare l'emergenza con immediatezza, consapevolezza ed efficace coordinamento.
Tale emergenza ha certamente determinato conseguenze concrete sulla gestione dei processi operativi, sull'assetto organizzativo e sugli equilibri economico-finanziari. Tuttavia, l'impatto è stato relativamente mitigato: grazie al supporto del comitato direttivo, Alfa ha adottato linee di azione tendenti all'ottimizzazione delle risorse, all'ulteriore miglioramento dell'efficienza organizzativa e alla individuazione di nuove opportunità. Alfa ha certamente tratto esperienza dalla pandemia: tali esperienze di gestione sono funzionali al suo consolidamento competitivo in proiezione di una crescita sostenibile.

Il cambiamento culturale

Un breve cenno è opportuno relativamente al tema del cambiamento culturale ed al collegamento di tale aspetto all'evoluzione della tecnologia.
Il progetto di riorganizzazione che l'Imprenditore ha deciso di adottare si fonda sulla sua "visione" di futuro riflessa sulle risorse umane di cui si avvale.
L'imprenditore, che ha sempre adottato un comportamento rispettoso dei vari collaboratori, grazie anche alla tecnologia di cui è affascinato, ha maturato il progressivo convincimento che alle risorse va dato spazio e fiducia ed anche chiarezza di obiettivi e coinvolgimento di metodo.
L'Imprenditore ha infatti positivamente intuito che il crescente cambiamento tecnologico consente ad Alfa di agire con prontezza e quindi di acquisire vantaggi competitivi nella conquista di quote di mercato. È tuttavia inevitabile che la tecnologia comporti competenze e contributi diversificati di una pluralità di risorse il cui impegno deve essere opportunamente coordinato ed integrato. Quindi, l'efficacia delle applicazioni tecnologiche implica cambiamento operativo che faccia leva su adattamento, flessibilità, sostenibilità e gioco di squadra.
Ne discende che l'Imprenditore, con la sua continua azione quotidiana, svolge un paziente lavoro di persuasione, affinché ciascun collaboratore abbia ad agire occupandosi del futuro in un disegno di cambiamento di cui l'evoluzione tecnologica è complice.
Ne consegue una positiva contaminazione: l'impegno quotidiano di ciascuno è profuso prioritariamente a favore dell'interesse aziendale declinandosi in ricaduta nell'interesse per ciascuno.

Il modello proposto

Il caso descritto si colloca in una più ampia casistica di PMI nel pieno dei dilemmi e delle scelte in tema di governo dell'impresa e di passaggio generazionale. Molti imprenditori affrontano il tema semplicemente ignorandolo, oppure facendo scelte impulsive e non sufficientemente meditate. Eppure, è cruciale salvaguardare i valori aziendali, l'integrità patrimoniale ed anche il valore delle relazioni familiari. È pertanto fondamentale gestire il passaggio generazionale in termini di progetto e non in termini di semplice successione.
Il caso di Alfa presenta caratteristiche singolari in quanto il tema del governo dell'impresa e del passaggio generazionale è stato affrontato con rigore, metodo e tempi adeguati. La prudenza e la lungimiranza hanno svolto un ruolo determinante ed i risultati del progetto si possono sintetizzare nei termini che seguono:
• il lavoro di squadra consente scambio di abilità e di punti di vista e quindi accrescimento complessivo delle competenze;
• le tempistiche del processo di formazione delle decisioni sono più ridotte;
• le decisioni prese con metodologia danno impulso al contributo di ciascuno nel raggiungimento degli obiettivi;
• ciascun componente della squadra rafforza le proprie personali predisposizioni ed il senso di fiducia verso i colleghi;
• le decisioni che passano attraverso un appropriato sistema di formazione inevitabilmente presuppongono individuazione e quantificazione dei rischi, diventano rassicuranti e maggiormente produttive.

L'accordo tra UE e UK in seguito alla Brexit: i profili doganali da tenere presente per i consulenti e le imprese

di Luigi Fruscione

Un percorso comune che si interrompe

Dopo 47 anni il Regno Unito è uscito ufficialmente dall'Unione Europea.

Infatti, a far data dallo scorso 1° gennaio 2021, essendo terminato il periodo transitorio stabilito nell'Accordo di recesso ed iniziato il 1° febbraio 2020, Scozia, Galles, Inghilterra ed Irlanda del Nord non fanno più parte dell'Unione; ciò determina la cessazione della libera circolazione di persone, merci, servizi e capitali tra il Regno Unito e l'Unione europea.

In riferimento all'Irlanda del Nord la Direttiva UE 2020/1756 del Consiglio del 20 novembre 2020 modifica la Direttiva 2006/112/CE, relativa al sistema comune d'imposta sul valore aggiunto, per quanto riguarda l'identificazione dei soggetti passivi in Irlanda del Nord; si è voluto evitare, infatti, che a partire dal 1° gennaio 2021 ci fosse una frontiera fisica tra l'Irlanda e l'Irlanda del Nord.

La Brexit ha un'importanza primaria nella storia recente dei rapporti tra gli Stati europei che fin dal 1957 si erano impegnati per dare vita ad un progetto di aggregazione dei popoli.

18 aprile 1951 è datato il Trattato che istituiva la Comunità europea del Carbone e dell'Acciaio (CECA) attraverso cui, per la prima volta nella storia del vecchio continente, sei Stati abbracciavano un percorso comune di integrazione: Belgio, Francia, Repubblica Federale di Germania, Italia, Lussemburgo e Paesi Bassi.

In Italia venne stipulato il Trattato di Roma nel 1957 con cui veniva istituita la Comunità economica europea (CEE), il cui spirito era delineato dall'art.2 in cui si sanciva la via intrapresa dagli Stati partecipanti: *"la Comunità ha il compito di promuovere, mediante l'instaurazione di un mercato comune e il graduale ravvicinamento delle politiche economiche degli Stati membri, uno sviluppo armonioso delle attività economiche nell'insieme della Comunità, un'espansione continua ed equilibrata, una stabilità accresciuta, un miglioramento sempre più rapido del tenore di vita e più strette relazioni fra gli Stati che ad essa partecipano".*

Sotto il profilo più strettamente doganale, il Trattato di Roma aprì all'unione doganale essendo previsto all'art.3 che *"l'azione della Comunità importa, alle condizioni e secondo il ritmo previsto dal presente Trattato:*
a) l'abolizione fra gli Stati membri dei dazi doganali e delle restrizioni quantitative all'entrata e all'uscita delle merci, come pure di tutte le altre misure di effetto equivalente
b) l'istituzione di una tariffa doganale comune e di una politica commerciale comune nei confronti degli Stati terzi
c) l'eliminazione fra gli Stati membri degli ostacoli alla libera circolazione delle persone, dei servizi e dei capitali".

Tale fondamentale passaggio verso la creazione di un'area commerciale unica, nella quale ogni tipologia di merce potesse circolare liberamente, veniva celebrata e raffigurata con una storica animazione voluta dalla Commissione Europea nel 1968; *"dessin anime sur la suppression des droits douane le 1/7/68"* era il titolo iniziale mentre, quello di chiusura, era *"telemessage n.1 de la communaute europeenne"*[1].

Il 1° gennaio 1973 la Gran Bretagna entrava a far parte della Comunità Economica Europea, insieme a Danimarca ed Irlanda, facendo passare da sei a nove i Paesi membri.

Nel 1992 la CEE, con la firma del Trattato di Maastricht, si trasforma nell'attuale Unione Europea; un anno dopo, il 1° gennaio del 1993, segna una tappa fondamentale del nuovo assetto di rapporti tra gli Stati europei con l'entrata in vigore del mercato unico che comporta la libera circolazione di persone, beni, servizi e capitali.

L'importanza del passaggio dalla CEE all'Unione Europea emerge chiaramente dalle primissime statuizioni contenute nel Trattato secondo cui: *"con il presente trattato, le Alte Parti Contraenti istituiscono tra loro un'Unione europea, in appresso denominata "Unione". Il presente trattato segna una nuova tappa nel processo di creazione di un'unione sempre più stretta tra i popoli dell'Europa, in cui le decisioni siano prese il più vicino possibile ai cittadini. L'Unione nel contempo è fondata sulle Comunità europee, integrate dalle politiche e forme di cooperazione instaurate dal presente trattato. Essa ha il compito di organizzare in modo coerente e solidale le relazioni tra gli Stati membri e tra i loro popoli".* Accanto a queste date assumono pari rilevanza storica quella del 23 luglio 2016 - in cui i "leave" si impongono sul "remainer" con 17,410,742 voti pari al 52% dei votanti, sancendo la volontà del popolo britannico - e quella del 29 marzo 2017, quando pervenne al Presidente del Consiglio Europeo, Donald Tusk, la lettera della premier britannica Theresa May con cui si dava inizio alla brexit con l'attivazione dell'articolo 50 del Trattato di Lisbona il quale prevede che *"ogni Stato membro può decidere, conformemente alle proprie norme costituzionali, di recedere dall'Unione".*

L'Accordo di recesso, che è stato approvato il 17 ottobre 2019, è entrato in vigore il 1° febbraio 2020.

Questo percorso, iniziato con il referendum del 2016, ha portato all'uscita della Gran Bretagna dall'Unione Europea a far data dalle 23.00 ora di Londra del 31 gennaio 2020.

In data 24 dicembre 2020, ad un passo dal cosiddetto e tanto temuto "no deal", l'Unione Europea e la Gran Bretagna hanno raggiunto un accordo sugli scambi commerciali e la cooperazione, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea

1 *Il video è reperibile sul sito internet della Commissione Europea all'indirizzo https://audiovisual.ec.europa.eu/en/video/I-001988*

del 31 dicembre 2020; infatti, il 29 dicembre 2020 il Consiglio dell'UE ha proceduto all'approvazione dell'Accordo mentre, il giorno successivo, giungeva la ratifica del Regno Unito da parte della House of Commons e della House of Lord.
In concomitanza con l'approvazione del Regno Unito procedeva alla firma per l'Unione Europea il Presidente del Consiglio Europeo Charles Michel e per la Commissione Europea Ursula von der Leyen.

L'Accordo

Preliminarmente, occorre evidenziare come l'Accordo raggiunto non rispecchi esattamente i punti del mandato individuati dal Consiglio europeo per la Commissione su temi rilevanti quali la mancanza di allineamento automatico del Regno Unito alla normativa europea, in particolare sugli aiuti di Stato o la mancata previsione di un ruolo per la Corte di Giustizia dell'Unione.
Ulteriore tema è rappresentato dalla mancata disciplina degli scambi di merci tra l'UE e l'Irlanda del Nord, rispetto ai quali trova applicazione il protocollo sull'Irlanda e l'Irlanda del Nord che è allegato all'Accordo di recesso.
Altre tematiche, rinviate a successivi incontri di approfondimento sono, ad esempio, la cooperazione in materia di politica estera e di sicurezza comune o il reciproco riconoscimento delle qualifiche professionali.

L'Accordo sottoscritto affronta i temi riconducibili ai quattro pilastri su cui era stata fondata la Comunità Economica Europea: libera circolazione delle persone, dei servizi, delle merci e dei capitali.
Il documento può essere sintetizzato in tre grandi direttrici che sono: 1) un accordo di libero scambio tra le parti, con particolare attenzione a garantire una reciproca collaborazione su temi rilevanti quali quelli economici, sociali, ambientali e relativi alla pesca; 2) una stretta collaborazione per la sicurezza dei cittadini e, da ultimo, 3) un assetto generale di governance.
Così come ben evidenziato dal sito internet della Commissione europea (https://ec.europa.eu/), *"l'accordo non riguarda soltanto gli scambi di merci e servizi, ma anche un'ampia gamma di altri settori d'interesse per l'Unione, come gli investimenti, la concorrenza, gli aiuti di Stato, la trasparenza fiscale, i trasporti aerei e stradali, l'energia e la sostenibilità, la pesca, la protezione dei dati e il coordinamento dei regimi di sicurezza sociale"*.
Questa è la portata del nuovo rapporto tra le parti che, per altro, consente al Regno Unito di continuare a partecipare a diversi programmi bandiera dell'Unione europea, come Orizzonte Europa (programma di ricerca e innovazione), nel periodo 2021-2027, a condizione di versare un contributo finanziario al bilancio dell'UE.

Nello specifico, l'Accordo affronta e disciplina, nella seconda parte, le tematiche del commercio, dei trasporti, della pesca; la terza parte riguarda, invece, la cooperazione delle autorità di contrasto e giudiziarie in materia penale (con l'esame, tra gli altri, di temi quali lo scambio di dati su DNA, impronte digitali e immatricolazione dei veicoli, assistenza giudiziaria, cooperazione con Europol ed Eurojust, antiriciclaggio e lotta al finanziamento del terrorismo).
La parte quarta dell'Accordo, definita cooperazione tematica, affronta la sicurezza sanitaria e la cibersicurezza. La quinta tratta, invece, della partecipazione ai programmi dell'Unione, sana gestione finanziaria e disposizioni finanziarie. La parte sesta è relativa alla risoluzione delle controversie e disposizioni orizzontali.
Oltre alle diverse sezioni di cui si compone l'Accordo sono previsti molteplici allegati attraverso i quali vengono stabilite disposizioni rilevanti per gli operatori economici quali, ad esempio, proprio quelle attinenti all'operatività doganale; in particolare, si fa riferimento agli allegati orig-1: note introduttive alle regole di origine specifiche per prodotto; orig-2: regole di origine specifiche per prodotto; orig-2 a: contingenti di origine e alternative alle regole di origine specifiche per prodotto di cui all'allegato orig-2 [regole di origine specifiche per prodotto]; orig-2 b: regole transitorie specifiche per prodotto per gli accumulatori elettrici e i veicoli elettrici; orig-3: dichiarazione del fornitore; orig-4: testo dell'attestazione di origine; orig-5: dichiarazione comune riguardante il principato di Andorra; orig-6: dichiarazione comune riguardante la Repubblica di San Marino; allegato customs-1 - operatori economici autorizzati o quelle relative allo scambio di vino (allegato TBT-5) oppure quelle relative al trasporto di merci su strada (allegato road-1).

Il passaggio della nuova linea di confine tra UE ed UK: ritorna la dogana

Dal 1° gennaio 2021, essendo la Gran Bretagna diventata Paese extra Ue, rilevanti sono le modifiche sotto il profilo doganale, in quanto non solo si sono dovute stabilire nuove regole relativamente al flusso delle merci ma si è dovuto intervenire anche, da parte delle Amministrazioni nazionali, sulla riorganizzazione delle infrastrutture e dell'IT ai fini dell'espletamento dei controlli e del trattamento della documentazione doganale; ciò ha comportato e comporta un notevole lavoro per tutti gli attori in gioco.
Occorre rilevare come mentre tante aziende non hanno avuto grandi criticità nella nuova gestione con fornitori e clienti presenti in Gran Bretagna (a parte il non aver potuto pianificare la gestione dei rapporti commerciali con adeguato anticipo), in quanto già abituate a gestire le procedure doganali negli scambi con Paesi extra UE, ve ne sono altre che si stanno confrontando in questo periodo con la nuova dinamica, (si pensi al caso di una piccola impresa che effettuava import o export solo verso Paesi europei oltre che, per l'appunto, con l'Inghilterra).
L'operatività con Paesi UE comporta, ovviamente, una mancanza di familiarità con il momento doganale e con tutte le regole particolarmente tecniche che in esso si ritrovano.
Il tema doganale nell'ambito dell'Accordo è trattato innanzitutto dalla parte seconda che è relativa al commercio, ai trasporti, alla pesca.
L'obiettivo di UE ed UK è espresso chiaramente nell'articolo GOODS.1, attraverso il quale si evidenzia come occorra *"agevolare gli scambi di merci tra le parti e mantenere la liberalizzazione degli scambi di merci"* delle parti contraenti.

L'origine preferenziale

Quest'ultima precisazione è di notevole importanza in quanto, in base all'articolo GOODS.5, salvo altrimenti disposto nell'Accordo, sono vietati i dazi doganali esclusivamente su tutte le merci originarie dell'altra parte.
Ai fini dell'operatività doganale, oltre al tema dell'origine della merce, assume importanza l'individuazione dello strumento per la classificazione delle merci oggetto di scambi tra le parti che è individuato nella nomenclatura tariffaria di ciascuna parte, conformemente al sistema armonizzato.
Per classificazione doganale di una merce si intende la classificazione di un prodotto o di un materiale in un determinato capi-

tolo o in una determinata voce o sottovoce del sistema armonizzato.
Ogni merce ha una propria voce doganale; ad esempio, il capitolo 1 tratta degli animali vivi; il 2 delle carni e delle frattaglie commestibili; il 3 dei pesci e dei crostacei, dei molluschi e degli altri invertebrati acquatici; il 4 del latte e dei derivati del latte; uova di volatili; miele naturale; prodotti commestibili di origine animale, non nominati ne' compresi altrove; il 5 di altri prodotti di origine animale, non nominati né compresi altrove; il 6 delle piante vive e prodotti della floricoltura; il 7 di ortaggi o legumi, piante, radici e tuberi mangerecci; l'8 della frutta commestibile; scorze di agrumi o di meloni; il 9 del caffè, the, mate e spezie; il 10 dei cereali; l'11 dei prodotti della macinazione; malto; amidi e fecole; inulina; glutine di frumento; il 12 di semi e frutti oleosi; semi, sementi e frutti diversi; piante industriali o medicinali; paglie e foraggi; il 13 di gomme, resine ed altri succhi ed estratti vegetali; il 14 di materie da intreccio ed altri prodotti di origine vegetale, non nominati né compresi altrove, etc. fino al capitolo 97 relativo agli oggetti d'arte, da collezione o di antichità.
Ogni capitolo che compone il Sistema Armonizzato ha un'ulteriore suddivisione interna; ad esempio, il capitolo 42 è relativo a lavori di cuoio o di pelli; oggetti di selleria e finimenti; oggetti da viaggio, borse, borsette e simili contenitori; lavori di budella.
La voce 4202 prende in esame "bauli, valigie e valigette, compresi i bauletti per oggetti di toletta e le valigette portadocumenti, borse portacarte, cartelle, astucci o custodie per occhiali, binocoli, apparecchi fotografici, cineprese, strumenti musicali o armi e simili contenitori; sacche da viaggio, borse isolanti per prodotti alimentari e bevande, borse per oggetti di toletta, sacchi a spalla, borsette, sacche per provviste, portafogli, portamonete, portacarte, portasigarette, borse da tabacco, borse per utensili, sacche per articoli sportivi, astucci per boccette o gioielli, scatole per cipria, astucci o scrigni per oggetti di oreficeria e contenitori simili, di cuoio o di pelli naturali o ricostituiti, di materie plastiche in fogli, di materie tessili, di fibra vulcanizzata o di cartone, oppure ricoperti totalmente o prevalentemente di dette materie o di carta".
La voce 42 02, a sua volta, si scompone nelle sotto voci:
- Bauli, valigie e valigette, compresi i bauletti per oggetti di toletta e le valigette portadocumenti, borse portacarte, cartelle e contenitori simili:
4202.11 -- con superficie esterna di cuoio o di pelli, naturali, ricostituiti o verniciati:
4202.11-10 --- Valigette portadocumenti, borse portacarte, cartelle e contenitori simili
4202.11-90 --- altri
4202.12 -- con superficie esterna di materie plastiche o di materie tessili:
--- di fogli di materie plastiche:
4202.12-11 ---- Valigette portadocumenti, borse portacarte, cartelle e contenitori simili
4202.12-19 ---- altri
4202.12-50 --- di materie plastiche stampate
--- di altre materie, compresa la fibra vulcanizzata:
4202.12-91 ---- Valigette portadocumenti, borse portacarte, cartelle e contenitori simili
4202.12-99 ---- altri
4202.19 -- altri:
4202.19-10 --- di alluminio
4202.19-90 --- di altre materie

Oltre alla classificazione, uno degli elementi fondamentali per la movimentazione delle merci è rappresentato dal criterio dell'origine, aspetto che assume una grande importanza economica nei casi in cui vi sia, come nel caso dell'Accordo in commento, la definizione di un'origine preferenziale che comporti l'azzeramento o la diminuzione dei dazi.
Nell'Accordo UE-Gran Bretagna tali regole sono previste all'allegato orig-2 che detta, per l'appunto, la disciplina per l'attribuzione dell'origine per singolo prodotto.
Le regole trovano applicazione *"a opera di una parte a una merce originaria dell'altra parte"*.
Sono considerati originari dell'altra parte i seguenti prodotti:
(a) i prodotti interamente ottenuti in tale parte; (b) i prodotti fabbricati in tale parte esclusivamente a partire da materiali originari di tale parte; e (c) i prodotti fabbricati in tale parte incorporando materiali non originari, purché soddisfino le prescrizioni di cui all'allegato ORIG-2 (Regole di origine specifiche per prodotto).
Dall'esame di tale elencazione emerge che per beneficiare della preferenza tariffaria sarà necessario che la merce ricada in una delle tre ipotesi indicate e cioè che il prodotto sia interamente ottenuto all'interno dei territori accordisti oppure che acquisisca l'origine alle condizioni indicate negli Annex Origin da 1 a 6.
La prima casistica, quella indicata alla lettera a), si realizza per i seguenti prodotti:
(a) i prodotti minerari estratti o prelevati dal suo suolo o dal suo fondo marino; (b) le piante e i prodotti del regno vegetale ivi coltivati o raccolti; (c) gli animali vivi ivi nati e allevati; (d) i prodotti ottenuti da animali vivi ivi allevati; (e) i prodotti ottenuti da animali macellati ivi nati e allevati; (f) i prodotti della caccia o della pesca ivi praticate; (g) i prodotti ivi ottenuti dall'acquacoltura, se gli organismi acquatici, compresi pesci, molluschi, crostacei, altri invertebrati acquatici e piante acquatiche, sono nati o allevati da materiale da riproduzione quali uova, avannotti, novellame, larve, parr, smolt o altri pesci immaturi in fase postlarvale con regolari interventi nei processi di allevamento o crescita diretti a migliorare la produzione, quali ripopolamento, nutrimento o protezione dai predatori; (h) i prodotti della pesca marittima e altri prodotti estratti dal mare al di fuori delle acque territoriali con una nave di una parte; (i) i prodotti fabbricati a bordo di una nave officina di una parte, esclusivamente a partire dai prodotti di cui alla lettera h); (j) i prodotti estratti dal suolo o dal sottosuolo marino al di fuori delle acque territoriali, purché essa abbia diritti per lo sfruttamento di detto suolo o sottosuolo; (k) i rifiuti e gli avanzi di operazioni di produzione ivi effettuate; (l) i rifiuti e gli avanzi derivati da prodotti usati ivi raccolti, purché tali prodotti siano idonei soltanto al recupero delle materie prime; (m) i prodotti ivi fabbricati esclusivamente a partire dai prodotti di cui alle lettere da a) a l).
Le casistiche rimanenti, invece, fanno capo alle regole di origine contenute negli appositi allegati all'Accordo; in tal caso si farà riferimento non al concetto di interamente ottenuto ma a quello di lavorazione sufficiente.
Proprio in considerazione della necessità che una lavorazione raggiunga tale minima soglia, ai fini della spendita della preferenza, l'articolo ORIG.7 prende in esame il caso della produzione insufficiente che si verifica nel caso in cui la lavorazione consista solo in una o più delle seguenti operazioni effettuate su materiali non originari: (a) operazioni di conservazione quali

l'essiccazione, la congelazione, la conservazione in salamoia e altre operazioni analoghe il cui unico scopo è assicurare che i prodotti rimangano in buone condizioni durante il trasporto e il magazzinaggio; (b) la scomposizione o la composizione di confezioni; (c) il lavaggio, la pulitura, la rimozione di polvere, ossido, olio, pittura o altri rivestimenti; (d) la stiratura o la pressatura di materie tessili e loro manufatti; (e) le semplici operazioni di pittura e lucidatura; (f) la mondatura e la molitura parziale o totale del riso; la lucidatura e la brillatura dei cereali e del riso; la sbiancatura del riso; (g) le operazioni destinate a colorare o aromatizzare lo zucchero o a formare zollette di zucchero; la molitura parziale o totale dello zucchero allo stato solido; (h) la sbucciatura, la snocciolatura e la sgusciatura di frutta, frutta a guscio, ortaggi e legumi; (i) l'affilatura, la semplice molitura o il semplice taglio; (j) il vaglio, la cernita, la selezione, la classificazione, la gradazione o l'assortimento, ivi compresa la costituzione di assortimenti di articoli; (k) le semplici operazioni di inserimento in bottiglie, lattine, boccette, borse, casse o scatole, o di fissaggio a supporti di cartone o tavolette e ogni altra semplice operazione di imballaggio; (l) l'apposizione o la stampa di marchi, etichette, loghi o altri segni distintivi analoghi sui prodotti o sui loro imballaggi; (m) la semplice miscela di prodotti, anche di specie diverse; la miscela dello zucchero con qualsiasi altra sostanza; (n) la semplice aggiunta di acqua o la diluizione con acqua o con altra sostanza che non alteri di fatto le caratteristiche del prodotto, o la disidratazione o la denaturazione dei prodotti; (o) il semplice assemblaggio di parti di articoli allo scopo di formare un articolo completo o lo smontaggio di prodotti in parti; (p) la macellazione di animali.
In base alla Nota 1 dell'allegato orig-1, le note introduttive indicano quali sono le regole da seguire per l'attribuzione dell'origine preferenziale, la modifica della classificazione tariffaria, un processo di produzione, un valore o peso netto massimo dei materiali non originari o qualsiasi altra prescrizione specificata nel presente allegato e nell'allegato ORIG-2 (Regole di origine specifiche per prodotto).

Riprendendo l'esempio utilizzato per il concetto di classificazione delle merci, la regola di origine prevede per le voci da 42.01 a 42.06 CTH oppure MaxNOM 50 % (EXW).
In sostanza, per CTH, *change of tariff heading*, si intende la sussistenza di un cambio di sottovoce di classificazione tra i semilavorati/materie prime non originarie utilizzate nel processo di fabbricazione ed il prodotto finito; tale "salto" di voce deve intervenire ad un livello di 4 cifre del Sistema Armonizzato.
Per MaxNOM XX% si intende il valore massimo dei materiali non originari.
Per quel che riguarda l'attestazione dell'origine, l'Accordo consente l'autodichiarazione tramite il sistema attraverso il quale si certifica l'origine delle merci nell'ambito del Sistema delle Preferenze Generalizzate (SPG) e nel quadro di alcuni Accordi commerciali preferenziali tra cui proprio quello tra UE e Gran Bretagna.
Per poter accedere al sistema REX occorre che gli operatori economici nazionali, che intendono certificare l'origine preferenziale con un'attestazione su fattura o su altro documento commerciale, presentino un'apposita domanda all'ufficio territorialmente competente dell'Agenzia delle Dogane, compilando l'allegato 22-06 al Regolamento 2447/2015.
Gli uffici delle dogane procedono alla registrazione degli esportatori nella banca dati REX.
Al richiedente viene, in tal modo, attribuito lo status di esportatore registrato.

GRUPPO SEAC

Da sempre a fianco dei professionisti

SOFTWARE
EDITORIA
FORMAZIONE
ASSICURAZIONI

CONSULENZA STRATEGICA
GESTIONE CREDITI IMPOSTA
SICUREZZA INFORMATICA

seac.it

Aggiornamenti in tema di organismo di Diritto pubblico

di Giovanni Comazzetto

Premessa. Le origini dell'istituto

L'organismo di diritto pubblico è, come è noto, figura di matrice squisitamente giurisprudenziale. Una prima definizione di essa risale alla sentenza della Corte di giustizia (quarta sezione) del 20 settembre 1988, causa 31/87 (*Gebroeders Beentjes BV e Stato dei Paesi Bassi*). La domanda pregiudiziale posta al giudice eurounitario concerneva l'interpretazione della direttiva 71/305/CEE del Consiglio, del 26 luglio 1971, relativa al coordinamento delle procedure di aggiudicazione degli appalti di lavori pubblici, in particolare il profilo della sua applicabilità ad enti non facenti parte, formalmente, dell'amministrazione statale – nel caso di specie, la commissione locale olandese per la ricomposizione fondiaria. Trattavasi di organismo privo di personalità giuridica propria, i cui membri erano nominati dallo Stato, e le cui funzioni erano altrettanto integralmente garantite, anche finanziariamente, dalla parte pubblica. Di qui l'accenno, enucleato ancora in forma molto sintetica, ad una nozione "sostanzialistica" di pubblica amministrazione: "*alla nozione di Stato*", diceva la Corte, "*si deve dare un'interpretazione funzionale*"; infatti, "*la finalità della direttiva [...] sarebbe compromessa se l'applicazione del regime della direttiva dovesse essere esclusa per il solo fatto che un appalto di lavori pubblici è stato aggiudicato da un ente che, pur essendo stato creato per svolgere funzioni attribuitegli dalla legge, non rientra formalmente nell'amministrazione statale*". Di conseguenza, "*si deve ritenere che un organismo le cui funzioni e la cui composizione sono, come nella fattispecie, contemplate dalla legge e che dipende dalla pubblica amministrazione per quanto riguarda la nomina dei suoi membri, la garanzia degli obblighi derivanti dai suoi atti e il finanziamento degli appalti ch'esso ha il compito di aggiudicare rientri nella nozione di Stato ai sensi della summenzionata disposizione, anche se formalmente non fa parte dello Stato*".

Questa decisione sopperiva, in particolare, ad una fondamentale lacuna della normativa comunitaria in materia di appalti, ossia alla tassatività del novero dei soggetti destinatari della direttiva. Pur conforme al principio della certezza del diritto, la tassatività dell'elenco finiva infatti per escludere dall'ambito di applicazione delle norme europee a tutela della concorrenza quell'ampio e variegato insieme di enti che, pur non facendo formalmente parte della compagine amministrativa statale, agivano come enti pubblicistici, al di fuori delle logiche di mercato. Nella successiva sentenza del 15 gennaio 1998, causa C-44/96 (*Mannesmann Anlagenbau Austria AG e altri e Strohal Rotationsdruck GesmbH*), basandosi sull'art. 1, lett b), secondo comma, della direttiva 93/37, la Corte definiva l'organismo di diritto pubblico come "*un organismo istituito per soddisfare specificatamente bisogni di interesse generale aventi carattere non industriale o commerciale, dotato di personalità giuridica e dipendente strettamente dallo Stato, da enti pubblici territoriali o da altri organismi di diritto pubblico*". Tali condizioni, puntualizzavano i giudici di Lussemburgo, "*hanno carattere cumulativo*". Già in questa seminale sentenza ad occupare maggior spazio nell'indagine della Corte di giustizia era l'accertamento della sussistenza del primo requisito citato, ossia della specifica destinazione dell'ente al perseguimento di bisogni di interesse generale aventi carattere non industriale o commerciale. Si poneva infatti il problema di stabilire se un ente che esercita tanto attività dirette a soddisfare bisogni di interesse generale aventi carattere non industriale o commerciale quanto attività di natura commerciale, come nella fattispecie portata all'attenzione della Corte, debba o meno essere qualificato come organismo di diritto pubblico; e se abbia un qualche rilievo il rapporto "quantitativo" tra le attività commerciali e quelle non commerciali. La risposta della Corte era positiva quanto al primo quesito, e negativa quanto al secondo: posto che l'ente in questione – "Österreichische Staatsdruckerei", nel prosieguo "ÖS" – era stato istituito allo scopo specifico di soddisfare bisogni di interesse generale – con tutto ciò che ne consegue: dover provvedere in esclusiva alle esigenze fissate, recepire i prezzi stabiliti dallo Stato, ecc. – era per la Corte irrilevante che esso fosse libero di svolgere altre attività. "*Il fatto*" dice la Corte "*che la soddisfazione dei bisogni di interesse generale costituisce solo una parte relativamente poco rilevante delle attività effettivamente svolte dall'ÖS è, esso pure, irrilevante, dato che un tale ente continua a provvedere ai bisogni che è specificamente tenuto a soddisfare*". D'altro canto, aggiungevano i giudici di Lussemburgo, "*lo stesso testo dell'art. 1, lett. b), secondo comma, della direttiva 93/37 non esclude che un'amministrazione aggiudicatrice, oltre al suo compito di soddisfare specificamente bisogni di interesse generale aventi carattere non industriale o commerciale, possa esercitare altre attività*".

L'attuale quadro normativo italiano. Il c.d. "requisito teleologico"

Da quanto fin qui riportato, può agevolmente riconoscersi la *ratio* alla base dell'istituto dell'organismo di diritto pubblico: si tratta di "*classificare quei soggetti che, pur essendo formalmente privati, sono caratterizzati da una forte ingerenza del potere pubblico, tanto da farli entrare nel novero delle amministrazioni aggiudicatrici tenute all'applicazione della normativa sull'evidenza pubblica*"[1]. Si vuole perciò "*evitare che il regime concorrenziale sia falsato per l'attività di soggetti, che pur appartenendo formalmente a categorie di diritto privato, non seguano gli schemi tipici imprenditoriali*"[2].

Nel nostro ordinamento la figura dell'organismo di diritto pubblico è stata introdotta con l'art. 3, comma 26, del d.lgs. 12 aprile 2006, n. 163 (che recepiva le direttive 2004/17/CE e 2004/18/CE); ed è oggi disciplinata dall'art. 3, comma 1, lett. d), del d.lgs. 18 aprile 2016, n. 50 (c.d. "Codice dei contratti pubblici", che ha recepito le direttive 2014/23/UE, 2014/24/UE e 2014/25/UE). Il secondo recita, in particolare, che per

1 *E. SANGINARIO, Organismi di diritto pubblico: la problematica interpretazione del nesso teleologico, in Amministrazione e Contabilità dello Stato e degli Enti pubblici (reperibile in www.contabilita-pubblica.it), 2020, 2.*

2 *Ibidem.*

organismo di diritto pubblico si intende qualsiasi organismo "*1) istituito per soddisfare specificatamente esigenze di interesse generale, aventi carattere non industriale o commerciale; 2) dotato di personalità giuridica; 3) la cui attività sia finanziata in modo maggioritario dallo Stato, dagli enti pubblici territoriali o da altri organismi di diritto pubblico oppure la cui gestione sia soggetta al controllo di questi ultimi oppure il cui organo d'amministrazione, di direzione o di vigilanza sia costituito da membri dei quali più della metà è designata dallo Stato, dagli enti pubblici territoriali o da altri organismi di diritto pubblico*". È allora fondamentale individuare il discrimine tra questa figura e quella dell'impresa pubblica – sono imprese pubbliche, ai sensi della medesima legge, le imprese "*sulle quali le amministrazioni aggiudicatrici possono esercitare, direttamente o indirettamente, un'influenza dominante o perché ne sono proprietarie, o perché vi hanno una partecipazione finanziaria, o in virtù delle norme che disciplinano dette imprese*". Trattasi, riguardo a quest'ultima figura, di ente che, a differenza dell'organismo di diritto pubblico, opera sul mercato essendo esposto alla concorrenza, persegue fini di lucro e sopporta in proprio le eventuali perdite derivanti dall'attività svolta. È chiaro allora che è di fondamentale importanza accertare con particolare rigore la sussistenza dei requisiti che determinano l'ascrizione di un ente all'una o all'altra figura. Da una parte, un'indebita estensione della figura dell'organismo di diritto pubblico rischierebbe di gravare, con eccessivi vincoli pubblicistici, sull'attività di chi opera concorrenzialmente sul mercato, rendendone peraltro note in anticipo – con lo svantaggio che ne deriva – le strategie aziendali; dall'altra parte, una altrettanto eccessiva compressione del novero dei soggetti qualificabili come organismi di diritto pubblico finirebbe per consolidare posizioni di privilegio in capo ad enti favoriti dalla prossimità con la compagine pubblica.

Dei tre requisiti citati, ai fini della qualificazione di un ente come organismo di diritto pubblico, quello che ha provocato un significativo dibattito dottrinale e le maggiori controversie giurisprudenziali è stato certamente il primo, il requisito teleologico. Occorre infatti stabilire che cosa significhi che un ente è stato preposto al perseguimento di esigenze di interesse generale, aventi carattere non industriale o commerciale. Se la questione della eventuale ridondanza del riferimento al "carattere non industriale o commerciale" delle esigenze di interesse generale sembra essere superata, essendosi consolidata piuttosto la convinzione che l'accertamento della "generalità" dell'interesse perseguito non esaurisca l'indagine sul requisito teleologico, dovendosi infatti altresì accertare che tale interesse generale abbia anche carattere non industriale o commerciale[3], non altrettanto condivisa è l'interpretazione di entrambi i segmenti che compongono la definizione del requisito. Con riferimento al primo, e alle difficoltà definitorie che riguardano più in generale cosa sia – e chi faccia parte della – pubblica amministrazione, è sufficiente in questa sede richiamare le acute osservazioni che Massimo Severo Giannini offriva in relazione alla teoria del fine pubblico: "*quella di fine pubblico appartiene alle nozioni falsamente chiare. Che cosa è infatti il fine pubblico? La dottrina prevalente propendeva infatti ad identificarlo con un fine dello Stato; ma anche a delimitarlo così, non diveniva affatto più chiaro [...], e ben presto cominciarono a rilevarsi dei paradossi*"[4]. Le complicazioni insorte indussero infatti la giurisprudenza ad introdurre il criterio degli "indici di riconoscibilità": ma la figura dell'ente pubblico fu via via scomposta, al punto da rendere inservibili gli stessi indici di riconoscibilità[5] (ad es. l'avere "poteri d'impero", l'esser stato istituito dallo Stato o da altro ente pubblico, l'esser sottoposto a controlli dello Stato, il fruire di agevolazioni e di privilegi come le amministrazioni statali). Questo punto non può essere ulteriormente sviluppato in questa sede. È tuttavia utile ricordare, a proposito dell'accertamento del carattere di generalità dell'interesse, che secondo la Corte di giustizia dell'Unione occorre tenere conto "*di tutti gli elementi di diritto e di fatto pertinenti, quali i fatti che hanno presieduto alla creazione dell'organismo interessato e le condizioni in cui quest'ultimo esercita la sua attività*"[6]. Trattasi pertanto di un accertamento *in concreto*, che non può limitarsi, ad esempio, alla considerazione formalistica di quanto previsto dallo statuto organizzativo dell'ente in questione.

A proposito del secondo segmento del requisito, ossia il carattere non industriale o commerciale dell'interesse perseguito, soccorre di nuovo la giurisprudenza sovranazionale. È stata infatti la Corte di giustizia a stabilire alcune coordinate essenziali all'interno delle quali i giudici nazionali esercitano la loro autonomia interpretativa in relazione alla normativa comunitaria in tema di appalti. Risulta preziosa, in particolare, l'indicazione per cui il fatto che un ente eserciti la sua attività in regime di concorrenza costituisce sì un forte indizio a sostegno del fatto che un bisogno di interesse generale ha carattere industriale o commerciale, ma solo in presenza di ulteriori requisiti. Ha osservato infatti la Corte di giustizia che se l'organismo non solo opera in normali condizioni di mercato, ma persegue lo scopo di lucro e subisce le perdite connesse all'esercizio della sua attività, "*è poco probabile che i bisogni che mira a soddisfare abbiano carattere non industriale o commerciale*"[7]. Sono dunque, per contro, criteri quali "*l'assenza dello scopo principalmente lucrativo, la mancata assunzione dei rischi connessi a tale attività, nonché l'eventuale finanziamento pubblico dell'attività*" a dover orientare i giudici di merito verso la qualificazione di un ente come organismo di diritto pubblico, soggetto ai vincoli pubblicistici nella scelta del contraente. Si può quindi affermare, sulla base della giurisprudenza sovranazionale sin qui sinteticamente esaminata, che ciò che conta, ai fini dell'accertamento del carattere "industriale o commerciale" dell'attività svolta, più che l'agire in regime di concorrenza è l'accettazione del rischio d'impresa e ciò che consegue necessariamente da questa scelta – in particolare, il rifiuto di pubbliche sovvenzioni dirette a coprire le eventuali perdite connesse all'esercizio dell'attività.

3 *Sul punto vedi Corte giust., sent. 10 novembre 1998, causa C-360/96, Gemeente Arnhem e Gemeente Rheden contro BFI Holding BV, e Corte giust., sent. 10 maggio 2001, Cause riunite C-223/99 e C-260/99, Agorà Srl e Excelsior Snc di Pedrotti Bruna & C. contro Ente Autonomo Fiera Internazionale di Milano e Ciftat Soc. coop. arl.*

4 *M.S. GIANNINI, Diritto amministrativo, I, Giuffrè, Milano, 1988, 182.*

5 *Ivi, 186.*

6 *Corte giust., sent. 27 febbraio 2003, causa C-373/00, Adolf Truley GmbH e Bestattung Wien GmbH.*

7 *Corte giust., sent. 22 maggio 2003, causa C-18/01, Arkkitehtuuritoimisto Riitta Korhonen Oy, Arkkitehtitoimisto Pentti Toivanen Oy, Rakennuttajatoimisto Vilho Tervomaa, e Varkauden Taitotalo Oy (nota come "sentenza Taitotalo").*

La più recente giurisprudenza italiana in tema di organismo di diritto pubblico

Può ora essere utile, sulla base del quadro testé definito, analizzare alcune recenti pronunce in tema di organismo di diritto pubblico, con particolare attenzione all'accertamento del requisito teleologico. Nella prima decisione esaminata – Cons. Stato Sez. V, sent. 7 febbraio 2020, n. 964 – si afferma, dopo una sintetica ricostruzione della giurisprudenza nazionale e sovranazionale, che "*la tendenza della giurisprudenza a identificare il requisito teleologico attraverso indici presuntivi [...] porta di volta in volta a semplificare l'attività interpretativa. Nondimeno comporta il rischio ultimo della progressiva creazione giurisprudenziale di una figura che in realtà finisce per risultare diversa da quella direttamente emergente dal dato normativo. Occorre, dunque, non discostarsi dal dato normativo*". È proprio con riferimento a quest'ultimo – l'art. 3, comma 1, lett. d), del d.lgs. 18 aprile 2016, n. 50 – che si afferma che "*con l'evidenziare il dato dell'istituzione unitariamente alle finalità, la disposizione pone anzitutto l'accento sulle ragioni istitutive del soggetto. Ricorre, dunque, il requisito teleologico se l'organismo è stato costituito da un soggetto pubblico appartenente al perimetro allargato della pubblica amministrazione, per dare esecuzione ad un servizio che è necessario perché è strettamente connesso alla finalità pubblica di quest'ultimo [...]. In questa prospettiva, la caratterizzazione segnata dai compiti assegnati all'organismo, che sono a base della sua istituzione, risulta per volontà della norma preminente sulle modalità con le quali poi l'attività viene svolta*", trattandosi peraltro, si dice di queste ultime, di un indicatore "*in realtà instabile perché soggetto a contingenti circostanze esterne, dunque non preciso e dirimente*". È proprio la valorizzazione del fine pubblico perseguito dall'ente considerato nella fattispecie – C.I.S. S.p.a., a sua volta istituito da C.D. S.p.a., organismo di diritto pubblico –, ossia la gestione collettiva del risparmio – definita come un compito di cui "*resta innegabile e pregnante il carattere pubblicistico*" – ad indurre il giudice amministrativo a qualificarlo come organismo di diritto pubblico, non rilevando la veste privatistica dello stesso se non come mera "modalità organizzativa" prescelta dall'organismo che l'ha istituito per l'espletamento dei suoi compiti pubblicistici istituzionali. La considerazione della finalità pubblicistica dell'ente che ha istituito, nella fattispecie, la società, e del processo della sua istituzione sembrano qui esaurire il lavoro del giudice: il concreto operare sul mercato dell'ente ha una rilevanza secondaria e certamente soccombente dinanzi alla preponderante attenzione riservata alla scaturigine dello stesso da altro organismo di diritto pubblico.

Altra pronuncia rilevante è T.A.R. Lazio, Sez. I, sent. 20 maggio 2020, n. 5336. Anche in questo caso, alla valutazione specifica della fattispecie è premessa una sintetica ricostruzione del quadro normativo e dei principali nodi interpretativi attinenti alla figura dell'organismo di diritto pubblico. Si ricostruisce infatti la *ratio* della normativa, che consiste nell'imporre alle amministrazioni aggiudicatrici ed agli enti aggiudicatori "*di seguire una logica economica e dunque criteri oggettivi e non discriminatori nell'aggiudicazione dei contratti di lavori, servizi e forniture. In altri termini, come sostenuto in dottrina, l'imposizione delle regole comunitarie è diretta ad ottenere il risultato della imparzialità mediante vincoli giuridici che dovrebbero tenere il posto dei vincoli economici non operanti. A ciò rileva appunto il rischio di impresa: un ente che sopporta tale rischio, e che quindi opera con lo scopo di coprire i costi con i ricavi della propria attività, subendo il rischio delle perdite dovute alle proprie scelte economiche, sarà molto probabilmente immune da pressioni esterne che impongano una logica antieconomica nella stipulazione contrattuale*". Ciò implica che "*la sopportazione per un ente del rischio economico guida le scelte relative ai contratti di acquisto di beni o servizi, sotto l'ispirazione di logiche commerciali, al punto tale che, come affermato da attenta e condivisibile dottrina, l'applicazione delle norme sui contratti pubblici sarebbe non giustificata o addirittura dannosa, costituendo un onere indebito per la stazione appaltante. In altri termini, per un'impresa effettivamente sottoposta alla pressione concorrenziale, la stessa sottoposizione al regime dell'evidenza pubblica sarebbe un handicap insopportabile, poiché essa sarebbe costretta a comunicare al pubblico, anticipatamente e dettagliatamente, i propri programmi di approvvigionamento di beni o servizi e non avrebbe la possibilità di ricercare liberamente sul mercato le occasioni negoziali più convenienti o innovative*". Sul punto si tornerà nelle conclusioni. Per ora è sufficiente richiamare l'attenzione sul diverso approccio qui seguito rispetto alla pronuncia esaminata in precedenza: è infatti evidenziato che non sono decisivi "*né lo status giuridico di un soggetto [...] né lo scopo di lucro (inteso come intento soggettivo), né il tipo di attività svolta o la strumentalità rispetto a interessi generali, per cui può sostenersi che il profilo determinante per stabilire il carattere economico di un'attività sia rappresentato dal modo in cui essa è svolta e, segnatamente, dall'assunzione di un metodo economico e del rischio (economico) connesso all'attività medesima*". È allora la considerazione sia dello Statuto dell'Istituto per il Credito Sportivo – l'ente di cui, nella fattispecie, era posta in dubbio l'appartenenza alla categoria fin qui esaminata – sia del concreto operare dell'ente a far ritenere al giudice che "*la banca assuma i rischi collegati a tale attività*"; né la sua attività "*risulta diversa da quella, tipicamente imprenditoriale, svolta dagli altri istituti di credito, indipendentemente dalla proprietà pubblica o privata del capitale*". Di fronte all'obiezione della ricorrente, per cui "*ri-entrando la gestione del risparmio tra le attività 'di interesse generale', anche l'attività bancaria svolta da I.C.S., essendo volta alla promozione delle attività sportive e culturali, avrebbe rilievo costituzionale e sarebbe riconducibile a funzioni d'interesse generale*", ed essendo inoltre I.C.S. direttamente controllato da organismi di diritto pubblico (il MEF, il Coni e C.D.P.) "*le funzioni da esso svolte sarebbero strettamente connesse a quelle svolte dai soggetti pubblici controllanti*", il giudice amministrativo, su questo punto in contrapposizione critica rispetto alla sentenza sopra esaminata, replica che l'organismo di diritto pubblico "*si distingue da qualsiasi altro soggetto operante nella contrattualistica pubblica non tanto in ragione delle finalità che persegue, che possono essere di interesse generale anche indipendentemente dalla configurabilità dell'organismo di diritto pubblico, quanto per il perseguimento di tali finalità operando con metodo non economico, essendo esente dal rischio di impresa*". Ciò che conta, l'elemento davvero dirimente, è quindi l'accettazione del rischio d'impresa e con esso la rinuncia ai privilegi pubblicistici. Sulla stessa linea di pensiero sembra assestarsi il giudice di legittimità: si vedano, sul punto, le pronunce Cass. civ. Sez. Unite, ord. 28 giugno 2019, n. 17567 e Cass. civ. Sez. Unite, ord. 27 marzo 2020, n. 7562. Nella prima, in particolare, sulla scorta della precedente pronuncia Cass. Sez. Unite,

28 marzo 2019, n. 8673, si offre un riepilogo – tanto sintetico quanto efficace – delle principali coordinate da tenere presente nell'indagine sulla sussistenza del requisito teleologico: per definire la natura di organismo di diritto pubblico di un soggetto, alla luce dei criteri enucleati nel d.lgs. n. 50 del 2016, "*occorrerà avere riguardo: in primo luogo, al tipo di attività svolta dalla società e all'accertamento che tale attività sia rivolta alla realizzazione di un interesse generale, ovvero che sia necessaria affinché la pubblica amministrazione possa soddisfare le esigenze di interesse generale alle quali è chiamata e, in secondo luogo, che tale società si lasci guidare da considerazioni diverse da quelle economiche [...]. In particolare, in merito a quest'ultimo profilo, è necessario, in primo luogo, che la società non fondi la propria attività principale su criteri di rendimento, efficacia e redditività e che non assuma su di sé i rischi collegati allo svolgimento di tale attività i quali devono ricadere sull'amministrazione controllante (Cass. 8225/2010). In secondo luogo, il servizio d'interesse generale che ne costituisce l'oggetto non può essere rifiutato per ragioni di convenienza economica. In conclusione ai fini della qualificazione di una società come organismo di diritto pubblico, per stabilire se essa agisca per un fine di interesse generale, occorrerà procedere ad una valutazione in concreto degli elementi di fatto e di diritto che connotano l'agire della stessa*".

Conclusioni

Un rapido confronto tra le pronunce citate nel paragrafo precedente può condurre alle conclusioni che di seguito, sinteticamente, si offrono. La giurisprudenza sovranazionale, pur non senza oscillazioni, sembra privilegiare – con particolare riferimento all'accertamento del requisito teleologico – un approccio "sostanzialistico" che, più che le ragioni istitutive di un ente, si appunta sulle modalità con cui esso opera sul mercato. A tale approccio sembra essersi conformato – anche qui, non senza eccezioni – il giudice di legittimità; né mancano pronunce affini da parte del giudice amministrativo. Si deve tuttavia dare conto della persistenza di un filone connotato da un approccio maggiormente "formalistico", evidente nella decisione sopra esaminata del Consiglio di Stato, che insiste più sulla finalità pubblicistica dell'ente che sul punto dell'accettazione – o dell'esclusione – del rischio d'impresa, che a parere di chi scrive resta invece il criterio più appropriato ai fini della valutazione dell'appartenenza di un ente alla tipologia dell'organismo di diritto pubblico.

La conoscibilità degli atti amministrativi: strumenti, diritti e poteri nei rapporti con la Pubblica Amministrazione

di Clarissa Conte & Denise Boriero

1. Il principio di trasparenza dell'azione amministrativa

Considerato, a ragione, uno dei principi cardine dell'agire della Pubblica Amministrazione, il principio di trasparenza rappresenta un criterio conformativo dell'azione amministrativa in tutte le sue esplicazioni, pur senza aver assunto, almeno fino ad un recente passato, dei contorni definitori nitidi.

Tale principio rappresenta una declinazione del buon andamento e dell'imparzialità di cui la Costituzione vuole sia caratterizzata l'attività dell'Amministrazione Pubblica.

Esso attiene prima di tutto al piano del linguaggio; costante è, in questo senso, l'attenzione ad una sempre maggiore semplificazione e comprensibilità del linguaggio usato dalla Pubblica Amministrazione, che deve rendere conto, nella maniera più limpida e chiara possibile, del suo operato nei confronti della parte privata.

L'esigenza di trasparenza, poi, rileva anche nella prospettiva della tutela del legittimo affidamento che l'attività pubblicistica ingenera nel soggetto privato, inteso quale convincimento circa la sussistenza di una determinata situazione vantaggiosa legittimamente meritevole di tutela.

Da ultimo, la questione maggiormente lambita dal principio in questione è quella che attiene alla conoscibilità dell'operato della Pubblica Amministrazione, inteso, in senso lato, come quel complesso di attività, comportamenti e provvedimenti che concorrono al perseguimento dell'interesse pubblico e che, proprio per tale ragione, non possono prescindere da un coinvolgimento del soggetto privato.

La conoscenza dell'attività pubblica viene garantita dalla pubblicità che della stessa la P.A. è tenuta a dare, portando così a conoscenza della collettività il suo operato; tale istituto, lungi dall'identificarsi con il principio di trasparenza, ne costituisce, invece, una sua espressione e una delle principali forme di attuazione dello stesso.

Il principio di trasparenza è stato positivizzato per la prima volta nel nostro ordinamento, con l'entrata in vigore del d.lgs. n. 150/2009. All'art. 11, infatti, esso definisce la trasparenza come "a*ccessibilità totale, anche attraverso lo strumento della pubblicazione sui siti istituzionali delle Amministrazioni Pubbliche, delle informazioni concernenti ogni aspetto dell'organizzazione, degli indicatori relativi agli andamenti gestionali e all'utilizzo delle risorse per il perseguimento delle funzioni istituzionali, dei risultati dell'attività di misurazione e valutazione svolta dagli organi competenti, allo scopo di favorire forme diffuse di controllo del rispetto dei principi di buon andamento e imparzialità*".

A ben guardare, già qualche anno prima il legislatore era intervenuto per dare al principio di trasparenza una maggiore concretezza, andando ad apportare, con la legge n. 15/2005, dei significativi interventi in tal senso alla legge sul procedimento amministrativo n. 241/1990 (si possono citare, tra tutti, l'introduzione, tra i principi di cui all'art. 1 anche l'indicazione del principio di trasparenza, ovvero la ridefinizione della disciplina sull'accesso documentale di cui agli artt. 22 e ss.), senza, tuttavia, fornire alcuna definizione del principio ispiratore di detta riforma.

La definizione introdotta con la riforma del 2009 è stata ripresa dal legislatore nel 2012, che ha posto la trasparenza alla base della prevenzione e della repressione della corruzione nella Pubblica Amministrazione, ritenendola assicurata e garantita proprio mediante "*la pubblicazione, nei siti web istituzionali delle pubbliche amministrazioni, delle informazioni relative ai procedimenti amministrativi, secondo criteri di facile accessibilità, completezza e semplicità di consultazione*" (art. 1 comma 15 della legge n. 190/2012).
L'obbligo di trasparenza cui è tenuta la Pubblica Amministrazione è stata, infine, oggetto di un ulteriore intervento legislativo nel 2013, che riprendendo tale principio nella sua accezione di conoscibilità dell'azione amministrativa, lo declina in termini di "*accessibilità totale dei dati e documenti detenuti dalle Pubbliche Amministrazioni allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*"(art. 1 comma 1 del d.lgs. n. 33/2013).

2. Le diverse tipologie di diritto di accesso

L'accesso rappresenta uno dei principali strumenti volti a perseguire finalità di trasparenza, tutelando così i diritti dei cittadini. Proprio alla luce della sua importanza, la legge riserva al singolo plurime possibilità di accesso.

Accesso documentale: la prima (ed unica, fino ad un recente passato) forma di accesso che il nostro ordinamento ha compiutamente disciplinato è l'accesso documentale, di cui agli artt. 22 e ss. della legge n. 241/1990.
Esso è così chiamato perché ha ad oggetto, appunto, i documenti amministrativi, ovvero "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica, o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una Pubblica Amministrazione e concernenti attività di pubblico interesse*" (art. 22, comma 1, lett. d).
Nonostante il legislatore abbia qualificato l'accesso come "diritto" (art. 22, comma 1, lett. a), più precisamente come "*il diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi*", tale natura giuridica non ha avuto un pacifico riconoscimento in sede giurisprudenziale.
Numerose sono state, infatti, le pronunce del giudice amministrativo sul punto, che hanno oscillato tra la qualificazione dell'accesso come interesse legittimo e l'attribuzione, allo stesso, della natura di vero e proprio diritto soggettivo, fino ad approdare, in tempi più recenti, a definirlo come posizione giuridica strumentale al conseguimento di un autonomo bene della vita. Com'è noto, la diversa qualificazione giuridica, tra le numerose ricadute che può avere, incide prima di tutto sulla situazione giuridica del titolare, essendo, l'interesse legittimo, contrariamente al diritto soggettivo, una posizione non autonoma, poiché necessita dell'intermediazione provvedimentale della Pubblica Amministrazione.
L'accesso documentale, in qualsiasi modo lo si voglia qualificare, di fatto permette al soggetto privato di controllare l'operato pubblico, controllo che, però, deve essere comunque funzionale alla tutela di una specifica situazione giuridica collegata al provvedimento e vantata dall'interessato, che deve, pertanto, essere titolare di un interesse diretto, concreto e attuale, non potendosi ammettere, ai sensi del comma 3 dell'art. 24, un'istanza di accesso documentale preordinata ad un controllo generalizzato sull'attività amministrativa. Al fine di dimostrare la sussistenza delle tre caratteristiche riportate, il richiedente deve provare che il suo interesse appartiene immediatamente e direttamente alla sua sfera (diretto), che non è astratto, in quanto deve emergere il collegamento sussistente tra l'interessato e l'utilità da conseguire (concreto) e deve infine essere attuale, non può quindi riguardare circostanze passate ormai non più modificabili o relative ad un futuro incerto, ma deve essere riferito alla situazione dell'interessato al momento della richiesta.
Gli aspetti più propriamente operativi circa le modalità di esercizio del diritto di accesso documentale sono disciplinati dal D.P.R. n. 184/2006.
La richiesta deve essere inoltrata dal singolo privato o dal legale rappresentante della persona giuridica alla Pubblica Amministrazione che ha formato il documento o che stabilmente lo detiene, la quale è tenuta, ai sensi dell'art. 2 della legge n. 241/1990, a provvedere entro il termine di 30 giorni, nel senso dell'accoglimento ovvero del rigetto dell'istanza.
L'istanza può essere formale o informale. In quest'ultimo caso, essa è ritenuta ammissibile pur senza formalità solo qualora non sorgano dubbi circa l'esistenza di controinteressati, la legittimazione del richiedente e il suo interesse qualificato alla stessa, ovvero l'accessibilità del documento (art. 6 del D.P.R. n. 184/2006).
Se, diversamente, sussistano dubbi su una o più delle condizioni sopra citate, l'istante è invitato a presentare richiesta di accesso formale, necessariamente in forma scritta, a fronte della quale verrà rilasciata la relativa ricevuta.
A fronte di un'istanza di accesso, una volta che la Pubblica Amministrazione abbia valutato l'insussistenza di cause di esclusione dell'accesso (cause che verranno in seguito brevemente descritte), nonché la sussistenza dell'interesse diretto, concreto e attuale allo stesso, il richiedente ha il diritto, a seconda dell'oggetto della sua richiesta, di esaminare gratuitamente ovvero estrarre copia dietro rimborso del costo di riproduzione del documento di cui si chiede l'ostensione (art. 25 della legge n. 241/1990).
Risulta evidente come l'interesse qualificato richiesto dalla legge n. 241/1990, qualora l'istanza sia presentata da una società per mezzo del suo legale rappresentante, sia da riferire alla società stessa, in virtù del rapporto di immedesimazione organica sussistente tra quest'ultima e il rappresentante legale.
Il rigetto può essere motivato ed espresso in caso di inammissibilità dell'accesso. Potrebbe, invero, configurarsi anche un diniego "tacito" dell'istanza, nel caso in cui, cioè, decorsi 30 giorni dalla presentazione della domanda, l'amministrazione non si pronunci con un provvedimento espresso.
Il mancato pronunciamento della Pubblica Amministrazione, in questo caso, rappresenta uno degli oramai pochi casi di "silenzio c.d. diniego", quale forma di silenzio significativa di una manifestazione di volontà negativa della Pubblica Amministrazione, equiparabile ad un provvedimento di rigetto.
A fronte del diniego di accesso da parte della Pubblica Amministrazione o del suo differimento ai sensi dell'art. 24 comma 4, il richiedente può adire il Tribunale Amministrativo Regionale dinanzi al quale si instaurerà il rito processuale speciale e semplificato previsto in materia di accesso dall'art. 116 c.p.a., ovvero, relativamente agli atti delle Amministrazioni comunali, provinciali e regionali, il difensore civico competente; nei confronti degli atti delle Amministrazioni centrali e periferiche dello Stato, l'istante può, invece, ricorrere alla Commissione per l'accesso o all'Amministrazione resistente (art. 25 comma 4).

Accesso civico: accanto all'istituto dell'accesso documentale, il sopra citato d.lgs. n.

33/2013 ha introdotto il c.d. "accesso civico", non prima di aver dedicato un'apposita disposizione normativa al "diritto alla conoscibilità" (art. 3), ritenuto soddisfatto con la pubblicazione di tutti i documenti, le informazioni e i dati oggetto di accesso civico, compresi quelli per cui la legge dispone la pubblicazione obbligatoria.
L'accesso civico si sostanzia, infatti, nell'esercizio del diritto di richiedere i documenti, le informazioni e i dati per i quali è stato violato dalla Pubblica Amministrazione l'obbligo di pubblicazione.
Con la positivizzazione di tale diritto si assiste, dunque, ad un cambio di prospettiva: l'accessibilità all'attività amministrativa passa dall'essere un'eccezione a rappresentare la regola, centrata su una situazione giuridica soggettiva meritevole di tutela, ovvero il diritto alla conoscibilità, che scaturisce dal principio di trasparenza, di cui l'accesso, in tutte le sue forme, rappresenta la modalità tipica di esercizio, e specularmente al quale si pone l'obbligo di pubblicazione di taluni documenti ad opera della Pubblica Amministrazione.

Accesso civico generalizzato: da ultimo, la disciplina contenuta nel sopra citato d.lgs. n. 33/2013 è stata oggetto di riforma nel 2016.
Più in particolare, il d.lgs. n. 97/2016 ha novellato, tra l'altro, l'art. 5 del d.lgs. n. 33/2013, introducendo, al comma 2, il c.d. "accesso civico generalizzato", espressione della normativa sul *Freedom of information act* (F.O.I.A.), già diffusa in molti altri Paesi.
Questa nuova forma di accesso prevede un ulteriore allargamento delle maglie dei poteri del cittadino, strumentali ad una tutela sempre più piena del diritto alla conoscibilità, in quanto prescinde dai documenti per cui vige, *ex lege*, un obbligo di pubblicazione per la Pubblica Amministrazione ed estende l'accessibilità, senza obbligo di motivazione, a tutti i documenti e i dati detenuti dalle Pubbliche Amministrazioni.
L'introduzione dell'accesso civico generalizzato ha rappresentato, così, il passaggio da un concetto di trasparenza di tipo proattivo, strettamente connesso all'obbligo di pubblicazione, ad una nuova forma di trasparenza reattiva, sollecitata, cioè, dalle istanze dei privati cittadini.
Circa le modalità operative di esercizio del diritto di accesso civico e generalizzato, occorre in primo luogo evidenziare che se il primo ha ad oggetto dati, documenti e informazioni alla cui pubblicazione l'Amministrazione Pubblica è tenuta in virtù di un obbligo previsto dalla legge (art. 5, comma 1), l'accesso civico generalizzato attiene, invece ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli per i quali vige un obbligo di motivazione (art. 5, comma 2); entrambe le forme di accesso, tuttavia, si caratterizzano per la non necessarietà di una motivazione, ovvero di un particolare interesse qualificato in capo all'istante (art. 5, comma 3).
A fronte dell'istanza di accesso civico semplice e generalizzato, che deve essere inoltrata agli uffici indicati al terzo comma dell'art. 5 (ovvero l'ufficio che detiene i dati, le informazioni o i documenti, l'ufficio relazioni con il pubblico o altro ufficio indicato dall'Amministrazione nella sezione "Amministrazione trasparente" del sito istituzionale), nonché al Responsabile della prevenzione della corruzione (nella sola ipotesi di accesso civico semplice), l'art. 5 comma 6 del d.lgs. n. 33/2013, prevede che il relativo procedimento debba concludersi con provvedimento espresso e motivato nel termine di trenta giorni dalla presentazione dell'istanza.
L'accoglimento dell'istanza di accesso civico comporta la trasmissione tempestiva al richiedente dei dati o dei documenti richiesti, e, nell'ipotesi dell'accesso civico semplice, la pubblicazione sul sito degli stessi, nonché la sua comunicazione all'istante.
Nei casi di diniego totale o parziale dell'accesso o di mancato pronunciamento entro il suddetto termine, il d.lgs. n. 33/2013 prevede che il richiedente possa presentare richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza, che si pronuncia entro il termine di venti giorni, sentito il Garante per la protezione dei dati personali, nell'ipotesi in cui il diniego o il differimento dell'accesso attengano a motivi legati alla tutela dei dati personali di cui all'art. 5 *bis*, comma 2, lett. a (art. 5 comma 7); l'istante dispone, inoltre, anche in questo caso, dei rimedi giurisdizionali del ricorso al T.A.R., ovvero al Difensore civico competente, anche quest'ultimo tenuto a provvedere previo parere del Garante in caso di dati personali di terzi.
A differenza di quanto accade per l'accesso documentale, per quanto concerne l'accesso civico nelle sue due forme, il legislatore, pur disciplinando tempi e modalità per il pronunciamento della Pubblica Amministrazione, non ha, tuttavia, qualificato la mancata pronuncia come silenzio significativo di segno negativo.
Una tale scelta va nella direzione di attribuire all'eventuale contegno omissivo del soggetto pubblico una valenza di silenzio inadempimento, che si configura come inerzia dello stesso a fronte di un obbligo giuridico a provvedere (la giurisprudenza non è tuttavia univoca sul punto).
A fronte del silenzio inadempimento, il richiedente può, quindi, avvalersi anche del ricorso al titolare del potere sostitutivo che, ai sensi dell'art. 2, comma 9 *bis* della legge n. 241/1990, è chiamato ad intervenire proprio nei casi di inerzia dell'Amministrazione adita, oltre che dei rimedi giustiziali (ricorso al Difensore civico e alla Commissione per l'accesso) e giurisdizionali (ricorso al T.A.R.) sopra indicati.

Accesso in materia di contratti pubblici: anche il d.lgs. n. 50/2016 (Codice dei contratti pubblici) contempla la possibilità di accedere agli atti delle procedure di affidamento e di esecuzione dei contratti pubblici, mediante un rimando alla disciplina dell'accesso documentale di cui agli artt. 22 ss. della legge n. 241/1990, limitandosi, l'art. 53 del d.lgs. n. 50/2016, ad individuare le ipotesi di differimento e di esclusione dello stesso. Sul punto, si è discusso circa l'applicabilità della disciplina dell'accesso civico generalizzato anche alla materia dei contratti pubblici, pur in assenza di un rimando *ad hoc* del legislatore. L'Adunanza Plenaria del Consiglio di Stato ha di recente avallato l'orientamento favorevole a tale apertura, ritenendo l'esigenza di trasparenza connaturata al settore dell'attività contrattuale pubblica e fondativa della disciplina delle procedure ad evidenza pubblica, ferme restando le preclusioni di cui all'art. 5 *bis* del d.lgs. n. 33/2013 (v. Adunanza Plenaria n. 10/2020).

Tra le nuove forme di accesso disciplinate dal d.lgs. n. 33/2013 e l'accesso documentale previsto dalla legge n. 241/1990 sussistono, indubbiamente, come già emerso dalla rapida disamina fatta sopra, analogie e differenze, che incidono sulla scelta dello strumento di cui avvalersi per tutelare il proprio diritto alla conoscibilità dell'azione amministrativa. Capire le particolarità di ognuna, dunque, consente al singolo di scegliere come sia più opportuno procedere in ciascun caso specifico.
Tra le prime sono sicuramente da annoverare le ipotesi di esclusione dell'accesso: l'art. 24 della legge n. 241/1990 contempla, infatti, una serie di ipotesi in cui l'accessibilità ai documenti amministrativi è preclusa; si tratta, in particolare, di documenti coperti da segreto di Stato, a contenuto generale, di programmazione e pianificazione, ovvero di atti connessi a procedure selettive e a procedimenti tributari, nonché di documenti sottratti all'accesso con apposito regolamento governativo. Analogamente, l'art. 5 *bis* del d.lgs. n. 33/2013, oltre a rimandare al sopra citato art. 24 della legge n. 241/1990 (comma 3), individua un'ulteriore preclusione all'accesso, qualora lo stesso comporti un potenziale pregiudizio concreto alla tutela degli interessi pubblici inerenti alla sicurezza pubblica e all'ordine pubblico, alla sicurezza nazionale, alla difesa e alle questioni militari, alle relazioni internazionali, alla politica e alla stabilità

finanziaria ed economica dello Stato, alla conduzione di indagini sui reati e al loro perseguimento, al regolare svolgimento di attività ispettive (comma 1).
Anche la tutela dei potenziali controinteressati a fronte dei diversi tipi di accesso è molto simile.
Per quanto riguarda l'accesso documentale, infatti, della relativa istanza la Pubblica Amministrazione cui la stessa è presentata deve dare notizia, ai sensi dell'art. 7 della legge n. 241/1990, agli eventuali controinteressati, ovvero "*tutti i soggetti individuati o facilmente individuabili, in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza*" (art. 22, comma 1, lett. c).
Essi, infatti, al fine di tutelare il proprio diritto, possono agire tanto in via procedimentale, presentando motivata opposizione alla richiesta di accesso entro il termine di dieci giorni dalla comunicazione della stessa, quanto in via processuale, avverso il provvedimento di accoglimento dell'istanza di accesso, secondo il rito abbreviato di cui all'art. 116 c.p.a.
La notifica al controinteressato deve avvenire anche in presenza di un'istanza di accesso civico; anche in questo caso, lo stesso può presentare motivata opposizione nel termine di dieci giorni. Tuttavia, solo per l'accesso civico la legge dispone espressamente la sospensione, nelle more del suddetto termine, del termine di conclusione del procedimento di accesso; è fuori di dubbio che, nonostante il silenzio normativo nella disciplina dell'accesso documentale, il termine di conclusione del procedimento di accesso di cui agli artt. 22 e ss. della legge n. 241/1990 debba considerarsi comunque sospeso, pena l'inutilità dell'opposizione del controinteressato.
Con riguardo tanto ai casi di esclusione dell'accesso, quanto alla tutela dei controinteressati, il d.lgs. n. 33/2013 li disciplina solo relativamente all'accesso civico generalizzato (art. 5, comma 5 e art. 5 *bis*, comma 1); una tale scelta del legislatore risulta coerente con la natura propria dell'accesso civico semplice, che costituisce un mero rimedio alla mancata osservanza degli obblighi di pubblicazione imposti dalla legge.
Le grandi differenze, invece, che emergono subito nel raffronto tra la disciplina dell'accesso documentale e quella dell'accesso civico in entrambe le sue forme attengono sicuramente alla legittimazione attiva ad esperire l'istanza, all'oggetto della stessa, nonché all'aspetto motivazionale.
Come sopra evidenziato, solo per l'accesso documentale è richiesta la sussistenza di un interesse diretto, concreto e attuale all'accesso; nulla viene indicato, a riguardo, dal d.lgs. n. 33/2013; così come, analogamente, è solo per l'accesso documentale che è previsto l'obbligo di motivare la richiesta.
Anche con riguardo all'oggetto della stessa, si può notare una maggiore elasticità nelle forme più recenti di accesso, per le quali si assiste ad un ampliamento delle informazioni accessibili.
Tutto questo porta, inevitabilmente, sussistendone i presupposti di fatto e di diritto, a preferire lo strumento dell'accesso civico generalizzato che poche limitazioni impone al suo esercizio, all'accesso documentale, rimasto, invece, fortemente ancorato a rigide condizioni soggettive e oggettive che male si prestano ad una tutela piena ed effettiva del diritto alla conoscibilità dell'azione amministrativa.

Richiesta documenti alla P.A. nell'ambito delle investigazioni difensive: la legge n. 397 del 7 dicembre 2000 ha introdotto, al Libro V del Codice di Procedura Penale, il Titolo VI *bis*, che indica le modalità attraverso le quali il difensore può ricercare e individuare "*gli elementi di prova a favore del proprio assistito*". La novella mira a rendere più paritaria la posizione di accusa e difesa, consentendo anche a quest'ultima di condurre delle investigazioni finalizzate a trovare elementi favorevoli, sia nell'ambito di un procedimento avviato e dunque durante le indagini preliminari, sia in via preventiva, ovvero soltanto alla luce di un eventuale procedimento.
Gli articoli inseriti nel nuovo Titolo vanno dal numero 391 *bis* al 391 *decies*. Mentre i primi disciplinano le c.d. "indagini difensive personali", la seconda parte è dedicata alle "indagini reali", tra le quali spicca la richiesta di documentazione alla Pubblica Amministrazione, contenuta nell'articolo 391 *quater*.
Il corpo dell'articolo indica che "*il difensore può chiedere i documenti in possesso della Pubblica Amministrazione e di estrarne copia a sue spese*" (comma 1). "*L'istanza deve essere rivolta all'Amministrazione che ha formato il documento o lo detiene stabilmente*" (comma 2) e che "*in caso di rifiuto da parte della Pubblica Amministrazione si applicano le disposizioni degli articoli 367 e 368*" (comma 3).
Come immediatamente emerge da quanto sopra riportato, oltre che dal tenore letterale dell'articolo, questa nuova possibilità è estremamente diversa dai diritti di accesso di cui sopra, sia negli aspetti formali che sostanziali.
In primis, il legittimato è il difensore e soltanto questo: non è una richiesta che può derivare quindi dal cittadino o dalla persona giuridica direttamente interessata, ma deve esserci un difensore nominato o di fiducia o d'ufficio nel caso ci si trovi nell'ambito di un procedimento penale già avviato, o un difensore nominato con apposita procura per lo svolgimento delle investigazioni preventive.
Anche il contesto nel quale si esercita il diritto è diverso: la richiesta di documentazione alla P.A. effettuata ex art. 391 *quater* c.p.p. è finalizzata a trovare i mezzi di prova per un procedimento penale pendente o eventuale, situazione che non si realizza negli altri casi.
Da ciò deriva anche una divergenza degli scopi tra i diritti di accesso: mentre in questo caso il fine primario è la difesa del soggetto nell'interesse del quale si richiede la documentazione, negli altri, che si attivano al di fuori di procedimenti penali, è l'attuazione della trasparenza e la verifica dell'imparzialità dell'operato della Pubblica Amministrazione. Ne consegue dunque che la tutela degli interessi giuridici del richiedente è soltanto indiretta e secondaria.
Dunque, nel momento in cui l'interessato sceglie quale tipologia di diritto di accesso esercitare, deve avere molto chiara la situazione nella quale si ascrive questa richiesta – soprattutto quando non si è già nelle more di un procedimento attivato ma si tratta di indagini difensive preventive – e la scelta deve tenere in considerazione tutte le peculiarità di ciascuna modalità.
Si pensi ad esempio al dovere di collaborazione che scaturisce per la Pubblica Amministrazione negli "accessi amministrativi" che non è presente nell'"accesso penalistico". In quei casi, la P.A. è tenuta a rispondere o comunque a motivare l'eventuale diniego, incorrendo -in caso di inadempienze- anche in profili penalistici. Tale motivazione non è prevista per la P.A. per le istanze ex art. 391 *quater* c.p.p. Al difensore, dunque, in questi casi non resta che ricorrere a quanto previsto dal terzo comma dell'articolo in questione.
Proprio i rimedi sono un'ulteriore grande differenza tra gli accessi fino ad ora descritti e questo. Qualora la P.A. non rispondesse al difensore o lo facesse in termini negativi, la sola possibilità sarebbe quella di chiedere al Pubblico Ministero il sequestro della documentazione ai sensi degli artt. 367 e 368 c.p.p. Granitiche sia la dottrina che la giurisprudenza nel ritenere che la giurisdizione non è dunque in capo al Tribunale Amministrativo ma a quello ordinario. Ci si rivolge infatti al P.M. che può provvedere al sequestro o trasmettere al Giudice per le

Indagini Preliminari la richiesta con il proprio parere. La facoltà di richiedere al P.M. il sequestro della documentazione, che può in prima battuta apparire più veloce di un ricorso amministrativo e meno dispendioso, ha tuttavia una serie di conseguenze negative sulla difesa. Per procedere alla richiesta, infatti, il difensore deve motivare l'esigenza di prendere visione della documentazione detenuta dalla P.A. e nel farlo sarà costretto a svelare parte della propria strategia difensiva. Inoltre, la documentazione diverrebbe a quel punto parte del procedimento e sarebbe a disposizione anche dell'accusa, a differenza di ciò che avviene per le altre prove raccolte tramite indagini difensive: infatti il difensore non è obbligato a presentare tutto quanto emerge dal proprio lavoro, mentre in questo caso non potrebbe impedire che il materiale venisse utilizzato per sostenere il capo di imputazione.
In alcune occasioni per ovviare a questo problema, si era tentata una strada alternativa: il difensore richiedeva un accesso ai luoghi ai sensi dell'art. 391 *septies* e in quel contesto avanzava anche l'istanza di copia dei documenti in possesso alla P.A. Tale via è stata però negata in quanto, secondo la Suprema Corte, contraria ai principi alla base del sequestro penale (v. Cass. n. 42588/2005).
Da un punto di vista di strategia difensiva, un'alternativa potrebbe essere quella di far richiedere direttamente dall'assistito i documenti ricorrendo alla via dell'accesso civico.
Infine, si rammenta che anche nell'accesso richiesto a fini di indagini difensive restano salve le norme che tutelano il segreto di Stato o quelle che prevedono il segreto o divieto di divulgazione.

3. Il diritto di accesso e la tutela della privacy

Il diritto di accesso, pur rivestendo sempre più un maggior rilievo, deve necessariamente essere contemperato al diritto degli interessati di non veder compromessa la tutela dei propri dati personali.
Proprio tale esigenza di tutela, infatti, costituisce un'ipotesi di diniego all'accesso. Stante l'importanza di trovare il giusto bilanciamento tra gli interessi in gioco, in taluni casi è espressamente previsto l'intervento del Garante (si rimanda ad es., nel caso dell'accesso documentale, all'art. 25, comma 4, della legge n. 241/1990).
La necessità di trovare un bilanciamento tra il principio di trasparenza e quello di riservatezza è risalente, ma si è acuita con lo sviluppo della dimensione digitale che ha visto il traslarsi della quasi totalità degli aspetti del quotidiano *online*: proprio alla luce di queste nuove contingenze il Garante per la protezione dei dati personali ha emanato nel 2014 le "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati".
Anche l'ANAC è intervenuta a tutela della privacy prevedendo delle Linee guida per i casi di esclusione nell'accesso civico, ipotesi già elencate sopra.
Il principio da adottare è quello di minimizzazione dei dati, così come previsto dal *GDPR* e più volte richiamato dal Garante, ovvero i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario alle finalità di trattamento.
In caso di pubblicazione online, la P.A. deve *in primis* individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale, verificare poi, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni, nonché sottrarre all'indicizzazione i dati appartenenti a categorie particolari così come definiti dal *GDPR* - Regolamento (UE) 2016/679, ossia i dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, i dati relativi alla salute, all'orientamento sessuale, i dati biometrici e genetici e infine i dati giudiziari.
Quando i dati trattati rientrano in queste categorie, indipendentemente dal tipo di accesso esercitato e dal contesto della loro pubblicazione, la loro comunicazione è consentita solo qualora il diritto da difendere tramite l'acquisizione di queste informazioni personali sia di grado almeno pari al diritto dell'interessato o si sostanzi in un diritto alla personalità o altro diritto o libertà fondamentale. Va da sé che nel caso di accesso ex art. 391 *quater*, trattandosi di procedimenti penali, il diritto alla difesa è considerato pari o superiore alla privacy, ma il bilanciamento va sempre effettuato di volta in volta dalla P.A. in base a criteri di proporzionalità e ragionevolezza, peraltro individuati anche dalla Suprema Corte. Anche qualora uno dei due diritti in gioco soccombesse, ne va comunque assicurata la tutela almeno nel suo nucleo essenziale, nel rispetto di quanto statuito dalle Sezioni Unite della Cassazione con la pronuncia n. 3034 del 2011.
Inoltre, nel caso di richiesta dei documenti a fini di investigazioni difensive, nell'istanza va presentata la procura del difensore con tutti i requisiti affinché sia immediatamente evidente la sua legittimazione, il contesto nel quale si incardina o si incardinerà il procedimento penale e anche l'indirizzo dello Studio professionale dove saranno conservati gli atti e i documenti, nel pieno rispetto di quanto previsto dalla normativa sul trattamento e la protezione dei dati personali.
Il trattamento dei dati è soggetto a dei limiti temporali legati alle finalità individuate e nel caso di pubblicazione *online* non può superare i 5 anni, tranne che per specifiche eccezioni indicate dal Garante.

4. Conclusioni

Negli ultimi trent'anni si è assistito ad un progressivo accorciamento delle distanze tra il soggetto pubblico e quello privato, che è stato progressivamente legittimato ad una sempre maggiore esposizione nei confronti della Pubblica Amministrazione.
La necessità di un cambio di centratura, dalla Pubblica Amministrazione alle esigenze di tutela del privato, inevitabilmente ha portato anche il legislatore ad adeguarsi a tale nuova prospettiva.
La proliferazione delle forme di accesso, che si inserisce in questo solco, sta proprio a significare la grande attenzione che l'ordinamento giuridico riserva alla posizione del privato quale parte debole nel rapporto con la Pubblica Amministrazione, con il duplice fine di garantire allo stesso di esercitare il proprio diritto alla conoscibilità dell'operato dell'Amministrazione, nonché alla propria difesa nel contesto del procedimento penale.
Essendo le varie forme di accesso strumenti preordinati alla soddisfazione di esigenze diverse, non si configurano come alternative l'una con l'altra, ma inerenti ad ambiti eterogenei: occorrerà dunque valutare caso per caso quale di esse risulti maggiormente rispondente alla tutela da apprestare al soggetto anche sotto il profilo dell'opportunità e della convenienza alla luce delle specificità di ciascuna.

Transizione del Modello 231 da un approccio per famiglie di reato a un approccio per processi: i vantaggi in un'ottica di controllo e verifiche

di Alberto Giustini

1. Le fattispecie di reato in ambito D. lgs n.231/01

Il Decreto Legislativo 231 dell'8 giugno 2001, in attuazione della Legge 29 settembre 2000 n. 300, ha introdotto nell'ordinamento italiano la responsabilità "amministrativa" degli enti dipendente da reato, quale conseguenza di determinate tipologie di reati, attuate nell'interesse o a vantaggio dell'ente medesimo da parte di suoi dipendenti, apicali o sottoposti.

I reati richiamati, cd. reati presupposto, sono stati integrati nel corso degli anni; alle fattispecie contro la Pubblica Amministrazione di giugno 2001 se ne sono aggiunte, nel corso degli anni, ulteriori che hanno definito il vigente elenco dei reati sanzionabili.

Come appena evidenziato, i primi reati a comportare per i soggetti collettivi una responsabilità 231/2001 sono stati quelli contro la Pubblica Amministrazione a cui è seguita l'aggiunta, nel settembre del 2001, dei casi di "Falsità in monete, in carte di pubblico credito e in valori di bollo". L'anno successivo, precisamente nell'aprile del 2002, è stato il turno dei reati Societari, seguiti nel 2003 dai "Delitti con finalità di terrorismo o di eversione dell'ordine democratico", nel mese di gennaio, e dai "Delitti contro la personalità individuale", nel mese di agosto.

Le successive modifiche sono intervenute nell'aprile del 2005 con l'introduzione dell'"Abuso di mercato".

Il 2006 ha visto aumentare l'elenco dei reati presupposto con l'inserimento delle "Pratiche di mutilazione degli organi genitali femminili" e dei "Reati transnazionali", rispettivamente a gennaio e a marzo, mentre l'anno seguente come atteso, data l'importanza e la rilevanza che rivestono nel panorama degli Enti italiani, è stata la volta dei Reati di "Omicidio colposo o lesioni gravi o gravissime" (agosto 2007) che ad oggi risultano essere, purtroppo, i principali reati alla base dell'avvio di un procedimento in ambito 231 del 2001.

Sempre nel 2007, anno particolarmente rilevante per via delle modifiche al D. lgs. 231/01, le famiglie dei reati presupposto aumentano includendo i reati di "Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita" (novembre 2007).

A marzo 2008, invece, il legislatore ha apportato come novità al D. lgs. 231/01 l'introduzione dei "Delitti informatici e trattamento illecito di dati".

Ma è stato il 2009 l'anno con maggiori novità in materia di incremento di famiglie di reato nell'ambito del decreto legislativo in parola in quanto il legislatore ha introdotto, tra luglio ed agosto, i "Delitti di criminalità organizzata", i reati di "Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni", i reati di "Introduzione nello stato e commercio di prodotti con segni falsi", i "Delitti contro l'industria e il commercio", i "Delitti in materia di violazione del diritto d'autore" e l'"Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria".

Dopo un periodo di relativa calma si sono succedute ulteriori modifiche con novità importanti che hanno visto in particolare, ad agosto 2011, l'inserimento nel catalogo dei "Reati ambientali", anch'essi come i reati di "Omicidio colposo o lesioni gravi o gravissime" molto rilevanti nello scenario italiano, e successivamente nel 2012 l'"Impiego di cittadini di paesi terzi il cui soggiorno è irregolare" (agosto) e la "Corruzione tra privati" con l'"Induzione a dare o a promettere utilità" (novembre).

Il 2014 è stato l'anno dei reati di "Adescamento di minorenni" e "Scambio elettorale politico-mafioso", entrambi vigenti nel mese di marzo. L'anno seguente il legislatore ha allungato la lista dei reati presupposto 231 del 2001 con l'"Autoriciclaggio", a gennaio, gli "Ecoreati" e il "Falso in bilancio", a maggio. A ottobre 2016 è il turno dell'"Intermediazione illecita e sfruttamento del lavoro" mentre nel 2017 vengono introdotti i reati di "Istigazione alla corruzione tra privati" (aprile) e di "Razzismo e xenofobia" (novembre).

Infine, le modifiche apportate nell'ultimo biennio al D. lgs. 231 del 2001 hanno visto l'introduzione del "Traffico di influenze illecite", a gennaio 2019, delle "Frodi sportive e gioco d'azzardo", a maggio 2019, dei "Reati tributari", a ottobre 2019 e del "Contrabbando", a luglio 2020.

L'ampliamento del perimetro dei reati presupposto ha comportato l'adozione di un proprio Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. n. 231/2001 (di seguito Modello 231) da una sempre maggiore platea di Enti.

2. La responsabilità dell'Ente

Tale normativa, nel caso in cui uno dei reati presupposto venga commesso nell'interesse o a vantaggio dell'Ente da persone che rivestono il ruolo di soggetti in posizione apicale ovvero da soggetti subalterni ai primi, prevede delle sanzioni amministrative, sempre applicabili, e delle sanzioni interdittive, applicabili se previste. Quest'ultime si distinguono in: interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni; divieto di contrattare con la pubblica amministrazione; esclusione da agevolazioni, finanziamenti, contributi o sussidi.

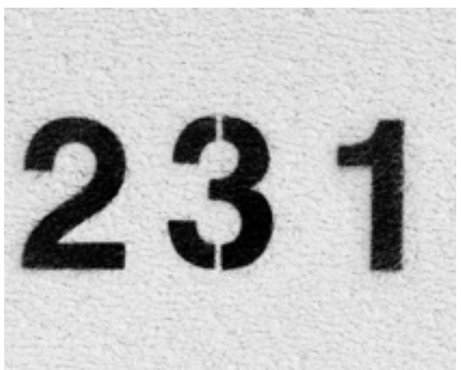
Pertanto, la principale motivazione dell'adozione di un Modello 231 da parte di un Ente e relativa attuazione al fine di prevenire la commissione dei reati presupposto, è l'efficacia esimente del Modello 231 stesso. Secondo il D. lgs. 231/01 non è sufficiente l'adozione ed efficace attuazione di un proprio Modello di Organizzazione e Gestione ma è necessario che l'Ente abbia affidato ad un Organismo (di seguito anche OdV), dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e sull'osservanza dei modelli, curandone il loro aggiornamento. Infine, è necessario che l'eventuale reato presupposto sia stato commesso eludendo fraudolentemente i modelli di organizzazione, gestione e controllo ai sensi del D. Lgs. n. 231/2001, e che non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo incaricato.

In sintesi, secondo l'art. 6 del D. Lgs. n. 231/2001 l'Ente può essere esonerato dalla responsabilità conseguente alla commissione dei reati presupposto se prova:

1. di aver adottato un Modello 231, calato sulla realtà aziendale, e relativa attuazione;
2. di aver affidato il compito di vigilare sul funzionamento, l'efficacia e l'osservanza dei modelli nonché di curare il loro aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo;
3. che le persone fisiche hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
4. che non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Generalmente un Ente, nel momento in cui decide di adottare un proprio Modello 231, si rifà alle Linee Guida di categoria che vengono periodicamente aggiornate con le novità legislative, giurisprudenziali e con la prassi applicativa, distinguendo una Parte Generale e una Parte Speciale.

Tale impostazione, normalmente, prevede nella Parte Generale una descrizione della normativa di riferimento (il D. Lgs. 231/2001



appunto), gli obiettivi del Modello 231, il funzionamento all'interno dell'Ente o Gruppo, i compiti dell'Organismo di Vigilanza, le misure formative e informative, il sistema sanzionatorio e l'elenco dei reati presupposto applicabili rispetto al business perseguito. Inoltre, le Parti Speciali hanno da sempre previsto una suddivisione rispetto alle cd. "Famiglie di Reato" richiamate dal Decreto Legislativo 231/2001. Ad esempio, possiamo individuare una Parte Speciale relativa ai Reati contro la Pubblica Amministrazione, una dedicata ai Reati Societari, una ai Reati Ambientali e così via.

3. L'attività di mappatura delle fattispecie incriminatrici

Sin dal principio dell'adozione del Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. n. 231/2001 si è sempre parlato delle mappature delle aree/attività a rischio strettamente connesse ai reati presupposto indicati nella normativa.

Successivamente, l'evoluzione in un'ottica sempre più aziendale, ha portato gli Enti ad associare alle aree/attività a rischio censite una valutazione del grado di rischio potenziale e residuale.

In effetti, è ormai sempre più diffuso nei programmi di compliance l'approccio "*risk based*" vale a dire basato sul rischio e quindi pesato in maniera continuativa rispetto a vari fattori esogeni ed endogeni. I primi risultano essere principalmente le modifiche normative, eventuali procedimenti in capo all'Ente, la giurisprudenza e l'evoluzione del business e del mercato in cui si opera. I fattori endogeni riguardano principalmente modifiche organizzative, nuove linee di business, operazioni straordinarie (ad esempio attività di *merger & acquisition*), le relazioni delle strutture di controllo come l'Internal Audit e la Compliance con evidenze di carenze e/o malfunzionamento del sistema di controllo interno, le relazioni dell'Organismo di Vigilanza con evidenze di carenze e/o malfunzionamento del sistema di controllo interno.

Questa prima evoluzione degli strumenti di lavoro per tutti i programmi di compliance, e quindi non solo per la 231, in un'ottica *risk based* ha comportato notevoli benefici per il *CRO - Chief Risk Officer*, ove nominato, e comunque per le strutture di controllo dedicate all'attività di *risk management*, al fine di poter monitorare l'andamento del rischio aziendale e quindi del cd. *ERM – Enterprise Risk Management*. Sinteticamente, l'*ERM* è lo strumento a supporto dei manager per valutare e monitorare la gestione del rischio aziendale in un'ottica complessiva mediante un modello integrato relativo a tutti i rischi aziendali. È intuibile che se tutti i programmi di compliance adottati da un Ente vengono basati sugli stessi principi, il compito del monitoraggio dell'andamento dei rischi globale a livello aziendale risulta più efficiente rispetto a molteplici programmi con impostazioni diverse che difficilmente riescono a dialogare tra di loro.

Nel corso degli ultimi anni, un *benchmark* delle principali realtà aziendali del panorama italiano ha evidenziato un'ulteriore evoluzione rispetto all'approccio della struttura dei Modelli 231 basato non più direttamente sui reati presupposto, bensì sui processi aziendali a cui, successivamente, si collegano le diverse fattispecie incriminatrici.

Il motivo principale risiede nel fatto che i Modelli 231 sono ormai presenti in alcune aziende da quasi un ventennio e nel tempo sono diventati "pane quotidiano", in particolare, delle strutture di controllo come la Compliance e l'Audit.

Solitamente tali strutture aziendali svolgono periodiche verifiche in ambito 231 autonomamente o a supporto dell'OdV dell'Ente. In effetti, almeno con cadenza annuale, l'Organismo di Vigilanza definisce un piano verifiche, svolto in autonomia o per il tramite delle strutture di controllo dell'Ente, al fine di valutare l'efficacia di attuazione del Modello 231 adottato.

La principale differenza tra le verifiche svolte dall'ODV e le verifiche svolte dalle strutture di controllo di secondo e terzo livello di un Ente riguarda l'approccio adottato; infatti, generalmente l'Organismo di Vigilanza adotta un approccio focalizzato ai singoli reati presupposto o alle famiglie di reato richiamate dal D. lgs. 231/2001, mentre le strutture aziendali prediligono un ragionamento per processi aziendali.

Il motivo risiede nel fatto che l'Ente da sempre ragiona per processi aziendali al contrario degli Organismi di Vigilanza; questi ultimi, almeno in principio, erano per lo più composti da avvocati penalisti e comunque da liberi professionisti che non operavano secondo tale approccio. Nel primo caso basti pensare che le norme riconosciute a livello internazionale per la creazione, implementazione e gestione di un Sistema di Gestione, ad esempio la ISO 9001 relativa alla Qualità, operano per processi.

Va sottolineato che entrambi gli approcci risultano corretti così come risulta corretto adottare un modello per famiglie di reato, purché basato su un'analisi del rischio che fotografi la realtà aziendale, piuttosto che un modello per processi aziendali.

In termini di efficienza, però, non si può confermare la medesima affermazione in quanto un approccio basato per processi consente alla struttura di controllo che svolge la verifica di ottimizzare i risultati in termini di tempo e risorse.

Prima di analizzare nella pratica le due metodologie applicate e le risultanze in termini di vantaggio per l'Ente, è opportuno ripercorrere il ruolo dell'Organismo di Vigilanza e le verifiche svolte in un'ottica 231/01.

Come già indicato, il compito principale che il D. Lgs. 231/2001 affida all'Organismo di Vigilanza è di vigilare sul funzionamento e sull'osservanza dei Modelli di organizzazione, gestione e controllo.

Tale compito viene espletato mediante la definizione di un piano verifiche che generalmente consiste nell'individuazione di aree/attività a rischio, contemplate dal Modello 231, che saranno oggetto di verifica nel corso di un periodo temporale, usualmente un anno, di interesse.

DI norma gli input di un piano di verifiche dell'OdV possono essere: le aree o le attività a rischio/sensibili mappate con una valutazione del rischio considerevole; le aree o le attività a rischio/sensibili che hanno subito variazioni per via di modifiche organizzative; le aree o le attività a rischio/sensibili introdotte a seguito di nuovi business/mercati; le criticità emerse da attività di verifica dell'OdV; l'introduzione di un nuovo reato presupposto nel catalogo reati del D. Lgs. 231/01; le novità nel business e/o mercato in cui si opera; le modifiche di normative strettamente correlate al D. Lgs. 231/01 (ad esempio il D. Lgs. 81/08); la recente giurisprudenza in ambito 231; gli eventuali procedimenti 231 in capo all'Ente; le modifiche al sistema di deleghe e procure dell'Ente; le modifiche all'organigramma societario (anche con riferimento al D. lgs. 81/08); la reportistica interna in materia di infortuni e *near miss*; la reportistica interna che evidenzia il *gap* da sanare, e quindi l'*action plan* definito, a cura delle strutture di controllo (ad esempio Internal Audit e Compliance); il piano di formazione e informazione; i flussi informativi verso l'OdV con notizie rilevanti ai fini dell'attività di vigilanza.

L'OdV nel definire il piano verifiche periodico si focalizzerà in prima battuta sul grado di rischio potenziale definito in fase di *risk assessment* e successivamente sull'eventuale analisi dei presidi di controllo interno atti a regolare le attività/aree a rischio individuate e quindi mitigare il rischio potenziale in ambito 231.

A valle della verifica svolta, in maniera autonoma o avvalendosi di professionisti e/o strutture di controllo dell'Ente, se vengono evidenziate delle carenze, l'Organismo di Vigilanza individuerà dei punti di miglioramento o proporrà dei protocolli di controllo interni da implementare.

Una volta individuate le aree/attività a rischio da monitorare si definiscono le modalità del controllo che l'OdV intende adottare nel corso delle verifiche.

Nel piano verifiche approvato dall'Organismo di Vigilanza, oltre a individuare le aree/

attività a rischio da verificare durante il lasso di tempo stabilito (di norma un anno), si specificano le modalità con cui l'OdV intende effettuare tali verifiche.
Le attività di verifica possono essere espletate in diverse modalità:
a) si può procedere con una audizione dei responsabili di processo aziendale affiancata dall'analisi delle *policies* interne richiamate nel sistema di controllo interno relative all'area/attività da verificare;
b) un'altra modalità di verifica può essere svolta mediante l'acquisizione documentale relativa a una determinata attività o processo e dal controllo del rispetto di quanto riportato nelle policies interne richiamate dal sistema di controllo interno da parte del personale aziendale;
c) l'Organismo di Vigilanza, in determinati casi specifici, può demandare alcune attività di verifica all'Internal Audit o a quelle strutture aziendali di controllo dedicate al monitoraggio di particolari aree/attività a rischio con ampia rilevanza 231 come la Struttura *HSE - Health, Safety & Environment* in relazione ai temi di Salute e Sicurezza sui luoghi di Lavoro e Ambiente, la Struttura Compliance, il Risk Management e via dicendo;
d) laddove siano necessarie particolari competenze professionali, l'Organismo di Vigilanza può ricorrere all'utilizzo del budget dedicato all'OdV incaricando professionisti esterni all'Ente.
Almeno con cadenza annuale l'Organismo di Vigilanza dovrebbe verificare l'aggiornamento del Modello 231 sia rispetto ai fattori esogeni che endogeni, come sopra definiti, e quindi effettuare una verifica del Modello a livello normativo e organizzativo, l'adeguamento della mappatura delle aree/attività a rischio della Società e infine, ma non meno importante, la rivalutazione eventuale del grado di rischio associato alle attività mappate. Così facendo il piano di verifiche del periodo temporale successivo verrà autoalimentato, almeno per quota parte, dalle risultanze del periodo precedente.
Solitamente nel piano delle verifiche 231 dell'Organismo di Vigilanza vanno ricompresi gli incontri periodici finalizzati allo scambio di informative con il Collegio Sindacale/Sindaco Unico, Società di Revisione, *DPO – Data Protection Officer, CRO – Chief Risk Officer* e, in caso di Gruppo di Società, con gli altri OdV.
Come già anticipato, l'esito delle verifiche dell'Organismo di Vigilanza può comportare una o più conseguenze tradotte in azioni, o meglio reazioni, da parte dell'ente.
L'introduzione di un nuovo reato presupposto nel catalogo dei reati 231 probabilmente comporterà la necessità di adeguare il Modello 231 a livello normativo, a meno che il *risk assessment* effettuato a monte escluda tale reato dal perimetro dei reati presupposto applicabili alla Società, ad esempio per il tipo di business che viene svolto.
Vediamo nella pratica, a seconda delle due metodologie applicate, che risultati si raggiungono in un'ottica prettamente aziendale.
L'analisi del processo di approvvigionamento secondo l'attuale impostazione richiede l'analisi di più parti speciali del Modello con una ridondanza di aree o attività a rischio (ad esempio affidamento di incarichi e consulenze), principi procedurali e procedure, seppur collegati a reati presupposto distinti.
Nel caso di Modello 231 secondo l'impostazione "classica", e cioè tarato su un approccio per famiglie di reato, una verifica su di un'area a rischio come, ad esempio, l'assegnazione di un contratto di consulenza, richiede l'analisi di più Parti Speciali contenenti in maniera ridondante tale area a rischio e, di conseguenza, la verifica dei principi procedurali e procedure richiamate dal Modello 231 in funzione, però, di reati presupposto distinti. Basti pensare che tale area a rischio risulta essere strumentale, a titolo esemplificativo e non esaustivo, per i reati presupposto strettamente connessi alla famiglia di reato "Reati contro la Pubblica Amministrazione", "Reati Societari, "Riciclaggio e Autoriciclaggio". In conclusione, il processo di approvvigionamento collegato all'attività a rischio analizzata risulta essere "frammentato" nelle varie Parti Speciali del Modello vigente con il potenziale rischio di non svolgere una verifica efficace o efficiente del processo in questione.
Nel caso di un Modello 231 basato su di un approccio per processi la verifica verrà svolta con maggiore linearità tenendo conto che i principi e le procedure da controllare risiedono in una Parte Speciale senza correre il rischio di omettere principi considerati in più Parti Speciali. Nel caso esemplificativo dell'affidamento di un contratto di consulenza basterà analizzare la Parte Speciale relativa al processo di *Procurement*, a seconda della definizione dei processi aziendali, per svolgere una verifica a 360°.
Un altro esempio potrebbe riguardare le verifiche svolte in un cantiere che prevedono, secondo l'approccio per famiglie di reato, l'analisi dei principi procedurali contenuti in molteplici Parti Speciali come, a titolo esemplificato e non esaustivo, la parte speciale relativa ai reati di "Omicidio colposo o lesioni gravi o gravissime" e la parte speciale dei "Reati Ambientali". In tale circostanza la struttura che dovrà svolgere la verifica di secondo o terzo livello potrebbe incorrere nel rischio di non svolgere un'analisi completa oppure con un minor grado di efficienza in termini di tempo e risorse impiegate. Risultanze diverse si potrebbero ottenere nel caso di un Modello 231 impostato per processi in quanto la medesima verifica potrebbe focalizzarsi su di un'unica Parte Speciale denominata "*Health, Safety and Environment*". In tal caso si potrebbe raggiungere un grado di efficienza maggiore in termini di verifica da parte delle strutture dedite all'analisi del rispetto dei principi procedurali, richiamati nel documento analizzato, da parte del personale operante in cantiere.
Inoltre, va sottolineato il fatto che secondo questo approccio la struttura dedita al controllo dei principi procedurali e rispetto delle procedure potrà, ampliando la normativa di riferimento, svolgere con una verifica un controllo con molteplici finalità. In effetti, nel secondo caso indicato la verifica svolta potrebbe essere sfruttata anche in ambito 81/08.
Di fatto, se tutti i programmi di compliance (Modello 231, Antitrust, Anticorruzione, Privacy, etc.) adottati da un Ente venissero impostati sui processi aziendali e successivamente ancorati alla normativa specifica, si potrebbe svolgere un'analisi di un determinato processo in base a molteplici normative e con un livello di garanzia maggiore delle risultanze ottenute.
Infine, un'impostazione così delineata potrebbe tornare utile anche nel mondo delle certificazioni dei sistemi di gestione, sia ove non presenti, e quindi a supporto di una prima certificazione, e sia ove presenti, e di conseguenza a supporto delle verifiche periodiche per il mantenimento delle stesse. In effetti un Modello 231 strutturato per processi si integra facilmente con i sistemi di gestione. Inoltre, l'Ente se ne potrebbe servire come documento a supporto di una eventuale prima certificazione o successivo rinnovo per la ISO 9001:2015 (Sistemi di gestione per la qualità), UNI EN ISO 14001:2015 (Sistemi di gestione ambientale), UNI EN ISO 45001:2018 (Sistema di gestione della sicurezza e della salute dei lavoratori), ISO 37001:2016 (Sistemi di gestione per la prevenzione della corruzione), ISO IEC 27001:2013 (Sistema di gestione della sicurezza delle informazioni).

4. Conclusioni – sintesi benefici Modello 231 per processi

Riepilogando, in estrema sintesi, i principali vantaggi di un Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. n. 231/2001 per processi potrebbero consistere in una maggiore efficienza delle verifiche, e relativa *assurance*, da parte delle Strutture di controllo dell'Ente e dell'Organismo di Vigilanza in ambito 231, o più in generale in relazione ai programmi di compliance adottati dall'Ente. Oppure potrebbe risultare un valido supporto, nel caso di adozione di un sistema *ERM – Enterprise Risk Management*, per il *CRO – Chief Risk Officer* al fine di analizzare e monitorare i rischi a 360° con un grado di *assurance* più elevato. Infine, potrebbe tornare utile all'Ente al fine di ottenere o manutenere le certificazioni dei sistemi di gestione.

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.

consulting.seac.it

+ 39 0461 805134
info.consulting@seac.it

Il trattamento dei dati personali nelle operazioni societarie straordinarie

di Anna Capoluongo

Dati ed informazioni permeano l'intero substrato delle quotidiane attività odierne, tanto nell'ambito privato, quanto in quello lavorativo.
Se, però, da un lato tutto ciò che rientra nella sfera prettamente personale e domestica – come noto – viene escluso dall'applicazione della normativa in tema di trattamento e protezione dei dati personali delle persone fisiche[1], lo stesso non può essere detto per quel che concerne la realtà professionale, economico-commerciale e aziendale.
In siffatto panorama è opportuno evidenziare come il dato personale sia da intendersi come vero e proprio *bene*, dotato di un *valore* intrinseco, con tutto ciò che ne consegue in ottica di valutazione dell'*asset*, di creazione di valore aziendale e anche di *compliance* nel *data processing*.
Che i dati siano considerati come il nuovo petrolio – per usare una locuzione ad oggi persino abusata – risulta evidente dall'analisi del "peso" del *cybercrime* sull'economia mondiale, stimabile – dagli ultimi report in tema – intorno a 1.5 trilioni di dollari all'anno. Un fatturato che, per dare un ordine di grandezza, ha ormai abbondantemente superato quello del traffico di droga.

A ciò si aggiunga un profilo ulteriore e differente, sdoganato di recente anche dalla Cassazione sezione Penale, con sentenza n. 11959/2020[2], la quale si è spinta a riconoscere il dato quale "bene immateriale" (suscettibile di divenire oggetto materiale di condotte penalmente rilevanti), statuendo che "*i dati informatici, contenenti files[3], sono qualificabili come cose mobili ai sensi della legge penale e, pertanto, costituisce condotta di appropriazione indebita la sottrazione da un personal computer aziendale, affidato per motivi di lavoro, dei dati informatici ivi collocati, provvedendo successivamente alla cancellazione dei medesimi dati ed alla restituzione del computer formattato*".
Si sta, in buona sostanza, riconoscendo valore patrimoniale al file/dato (anche personale), permettendo di equipararlo a una cosa mobile, pur non essendo pienamente integrato il requisito della fisicità. E così, "*In conclusione, pur se difetta il requisito della apprensione materialmente percepibile del file [...] di certo il file rappresenta una cosa mobile, definibile quanto alla sua struttura, alla possibilità di misurarne l'estensione e [al]la capacità di contenere dati, suscettibile di essere trasferito da un luogo ad un altro, anche senza l'intervento*

1 *Si veda la cd. household exemption, di cui all'art. 2 c. 2 l. c) del Regolamento europeo n. 679/2016 (GDPR).*

2 *Cass., Sez. II, 7 novembre 2019 (dep. 10 aprile 2020), n. 11959, Pres. Cammino, rel. Di Paola, ric. Carluccini, raggiungibile al link: https://www.sistemapenale.it/pdf_contenuti/1614713787_cassazione-11959-2020-appropriazione-indebita-file-dati-informatici-cosa-mobile.pdf.*

3 *La Corte definisce file un supporto sul quale vengono immagazzinati i dati, che occupa uno spazio misurabile in bit e che può essere trasferito da un dispositivo a un altro, anche utilizzando la rete internet; si tratterebbe, quindi, di un'entità fisica, ancorché non percepibile attraverso i sensi.*

di strutture fisiche direttamente apprensibili dall'uomo"[4].
Non bastasse, sempre con riferimento alla corretta valutazione di questo specifico *asset*, è giusto il caso di citare – ove del caso – lo IAS 38, denominato "Attività immateriali", che trova applicazione in tema di immobilizzazioni immateriali considerate non monetarie e prive di consistenza fisica, possedute per essere utilizzate nella produzione o nella fornitura di beni o servizi, per essere affittate a terzi o per fini amministrativi, al fine ultimo di determinarne il *valore contabile*[5]. In alcuni casi è possibile che tali attività siano anche contenute in oggetti di consistenza fisica come un compact disc (nel caso di un software per computer) o della documentazione legale (nel caso di una licenza o di un brevetto).
In tal senso, ciò che si è scritto è ancora più vero con riferimento alle operazioni societarie complesse, cioè a dire quelle che comportano per loro natura gestioni straordinarie, quali M&A (*Mergers and Acquisitions* - fusioni e acquisizioni) e cessioni di azienda o di rami della stessa.
Nell'ambito di tali operazioni, difatti, ad essere ceduti, traferiti o acquisti non sono solamente *asset* aziendali, ma anche posizioni giuridiche e, ovviamente, dati.
Ecco che, pertanto, la corretta applicazione della regolamentazione in punto privacy assume rilievi di una certa importanza. Per lungo tempo questi sono stati abbondantemente sottostimati o, addirittura, ignorati, mentre ad oggi si sta – fortunatamente – assistendo ad un cambio di rotta figlio del "nuovo modo di percepire la privacy", in termini di "*visione (innovativa), approccio (sistematico) e consapevolezza*"[6]. Sul quale incidono, senz'ombra di dubbio, il disposto dell'articolo 2-decies del novellato Codice Privacy, ai sensi del quale "*i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*", e l'impianto sanzionatorio e di responsabilità penale.
Se è vero che il trattamento di dati personali si sostanzia in qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, è pacifico riconoscere come la comunicazione di dati, così come il passaggio di interi *database*, vi rientrino a pieno titolo.
In tal senso, è bene ricordare che nei dati personali non confluiscono solamente il nome, il cognome o un numero di identificazione, bensì qualsiasi informazione riguardante una persona fisica identificata o identificabile e persino i dati di contatto aziendale (fatte salve e-mail generiche)

4 § 1.7, Sentenza cit.

5 Ossia "l'ammontare al quale un'attività è rilevata nel prospetto della situazione patrimoniale-finanziaria dopo aver dedotto l'ammortamento accumulato e le connesse perdite per riduzione di valore accumulate".

6 A. Capoluongo, Videosorveglianza: The Game Changer, Roma, 2021, cap. 4.

vanno qualificati come rientranti nell'alveo di applicazione del Regolamento europeo 679/2016 (GDPR) e del Codice privacy italiano (D.lgs. 196/2003 come novellato dal D.lgs. 101/2018).
Per non parlare, ovviamente, dei dati personali dei dipendenti, dei fornitori e dei clienti.
Oltre a quelli relativi al *deal* stesso, specie nel caso di *due diligence*.
Nello specifico, essendo questa un processo di indagine ed accertamento dei contenuti delle attività di impresa finalizzato alla loro valutazione – e più in generale relativo alla corretta gestione dei *target* – può riguardare tanto aspetti legali, quanto regolatori (*compliance*), contrattuali, commerciali, fiscali, contabili, finanziari, etc.
E così, è certo che in tali frangenti la capacità di dimostrare di aver ben adempiuto agli obblighi imposti dalla normativa di settore (anche privacy), potrà essere usata a maggior supporto della valorizzazione – anche monetaria – del *target* (e dei suoi asset), evitando spiacevoli ripercussioni quali la sospensione o il non perfezionamento dell'accordo/vendita o – peggio ancora – richieste risarcitorie di danni conseguenti all'illiceità del trattamento o danni all'immagine (*brand reputation*). Il caso di una nota catena alberghiera[7] e quello di un fornitore internazionale di telecomunicazioni[8] si può dire pacificamente che abbiano fatto scuola in tal senso.
Doverosamente premesso che la conformità alle norme privacy va intesa come sostanziale (ossia, di fatto e non meramente formale) e specifica per la singola impresa/realtà di riferimento, i profili che richiederanno una necessaria verifica sono gli stessi che potrebbero esporre l'azienda ai rischi di accesso non autorizzato o utilizzo improprio delle informazioni (anche riservate) della società, così come di terzi soggetti connessi al *target*, siano essi interni (dipendenti) o esterni (collaboratori, controparti...) all'entità.
Con specifico riferimento alla protezione dei dati personali, inoltre, andranno analizzati gli attori operanti, da un punto di vista di ruolo ricoperto (titolare, rappresentante, dpo, co-titolari, responsabili, sub-responsabili, autorizzati), la *compliance*, le basi giuridiche a fondamento delle finalità prefissate, la liceità dei trattamenti, la rispondenza ai requisiti previsti per l'*accountability*.
Di norma, gli esecutori della *due diligence* andranno nominati "Autorizzati al trattamento" (e muniti delle opportune istruzioni), oppure individuati quali "Responsabili", mediante un *data protection agreement* (o DPA) ai sensi dell'articolo 28 del GDPR.
Non va dimenticato, inoltre, che la "stanza" fisica in cui si svolgono le analisi sulla documentazione (di norma detta *on site*, se presso la sede legale del *target*, o *data room*, se situata presso una sede esterna), con l'avvento della *digital transformation* ha lasciato il passo alla cd. *data room virtuale*, con tutto ciò che ne consegue sotto il profilo della messa in sicurezza delle informazioni da un punto di vista più prettamente logico. In questo caso, ad esempio, dovranno essere rilasciate delle credenziali ai soggetti autorizzati a seconda dei permessi di accesso e del profilo di autorizzazione spettante, e dovranno essere previste misure di sicurezza adeguate al rischio informatico-digitale, non solo per far fronte alle esposizioni inconsce, ma anche in ragione del dilagare del *cybercrime* e dei casi di infedeltà fraudolenta (es. dei dipendenti). Sul punto, è giusto ricordare che assume particolare rilevanza la cosiddetta *digital awareness*, ossia la presa di coscienza circa la potenziale ricaduta nella dimensione reale di comportamenti tenuti nella sfera del digitale, o comunque in quella reale mediata da strumenti tecnologici[9].

7 Per approfondimenti si rimanda al link: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/.

8 Ci si riferisce allo sconto sul prezzo di acquisto di Yahoo richiesto da Verizon Communications Inc proprio a seguito delle risultanze in punto privacy e cybersecurity emerse dalla due diligence condotta per l'operazione.

9 Sul punto, M. d'Agostino Panebianco, Vivere nella dimensione digitale. Dai diritti del cittadino alla responsabilità dei data processors, Roma, 2019; M. d'Agostino Panebianco, Digital identity: between human rights and cybercrimes, in Ambiente e Diritto, Patti, 2021; A. Capoluongo, Internet of Bodies, neuroscienze e programmazione: dall'Habeas Corpus all'Habeas Mentem, articolo in fase di pubblicazione.

Con specifico riferimento a strumenti di videoconferenza – sempre più utilizzati nello svolgimento dell'attività professionale – a fronte delle vulnerabilità e della mancata sicurezza mostrate[10] da tali piattaforme durante l'attuale periodo pandemico, è indicativo come le Autorità per la protezione dei dati di Australia, Canada, Gibilterra, Svizzera, Regno Unito e Hong Kong, abbiano ritenuto necessaria l'integrazione da parte dei *vendor* di alcune misure di garanzia "minime", sintetizzabili in: sicurezza (crittografia end-to-end, autenticazione a due fattori, password solide), privacy by design e by default, conoscenza della propria audience di riferimento, trasparenza, equità e possibilità di controllo da parte dell'utente finale.

A protezione dei dati personali potranno, inoltre, essere utilizzate le soluzioni previste espressamente dal GDPR, ossia la pseudonimizzazione e la cifratura (cons. 26 e 28, artt. 4, 6 e 32), ad esempio approntando sistemi di schermatura – anche automatizzati – dei dati e delle informazioni riservate/sensibili o l'uso di codici di criptazione in sostituzione delle informazioni personali degli interessati.

Quanto, invece, al citato requisito della base giuridica, di norma sarà necessario invocare la "giusta causa" in relazione all'operazione e, quindi, le condizioni di liceità previste dall'articolo 6 (ad es. consenso, esecuzione di un contratto, obblighi di legge, interesse legittimo) o dall'articolo 9 del GDPR, in caso di trattamento di dati particolari.

Ad ogni buon conto, si tenga presente che è prassi comune nelle operazioni di *due diligence* la "schermatura" del trattamento di dati personali dietro il perimetro della *data room* ed entro i confini degli accordi a base dell'operazione posta in essere.

Tutto ciò premesso, e tornando all'ambito delle operazioni straordinarie, è giusto il caso di evidenziare quelli che risultano essere, concretamente, i rilievi privacy cui dedicare maggiore attenzione.

Certamente la modifica del *Controller*, mediante il trasferimento (e quindi il trattamento) di dati o di interi *database*, comporta – *in primis* – un cambio di titolarità, facendo sorgere l'esigenza di informativa nei confronti degli interessati, sicuramente circa l'identità e i dati di contatto del nuovo soggetto che determinerà mezzi e finalità del trattamento, ma eventualmente anche di altre specifiche, qualora vengano a modificarsi – in via esemplificativa – le finalità, la *data retention*, gli strumenti e le modalità di trattamento o le misure di sicurezza adottate.

Sotto questo profilo, laddove l'attività rimanga identica – pur nel passaggio di consegne – evidentemente non sarà necessario ottenere un consenso (o nuovo consenso) al trattamento dei dati dei soggetti interessati, potendosi imperniare lo stesso sulle medesime basi giuridiche per le quali i dati si erano ottenuti in origine. Diversamente, al cambiare di alcuni fattori – ad esempio per finalità ulteriori di newsletter, marketing o profilazione – il "neo Titolare" dovrà obbligatoriamente preoccuparsi di individuare le corrette basi giuridiche a supporto che, qualora presupponessero il rilascio di un consenso, dovranno rispettare i requisiti ex GDPR. Con espresso riferimento alle basi giuridiche utilizzabili, si richiama quanto accennato in tema di *due diligence*, ossia l'applicabilità delle condizioni di liceità previste dall'articolo 6 (ad es. consenso, esecuzione di un contratto, obblighi di legge, interesse legittimo) o dall'articolo 9 del GDPR, in caso di trattamento di dati particolari.

A ciò si aggiunga che, qualora tali operazioni comportino un trasferimento di dati in Paesi Extra-UE, l'attenzione andrà posta a tutti quei requisiti individuati dalla Corte europea[11], e chiariti dall'EDPB (European Data Protection Board)[12], circa la capacità di assicurare che il livello di protezione dei dati nel Paese Terzo sia equivalente o comunque ritenuto adeguato ai sensi della normativa privacy europea. E così, si renderà necessaria l'esecuzione di un *mapping* strutturato in più fasi, a partire dall'identificazione dei dati e degli strumenti su cui basare il trasferimento, per arrivare alla valutazione dell'efficacia dello stesso alla luce di un'analisi del quadro normativo di riferimento e all'eventuale implementazione di misure aggiuntive di salvaguardia dei dati.

Va rilevato che, di norma, tali operazioni straordinarie investono un numero elevato di soggetti interessati.

In particolare, un profilo che non va sottovalutato è quello della corretta modalità da scegliersi per fornire le informazioni *ex* GDPR. Si ricorda che andrà fatto riferimento all'articolo 14 qualora i dati vengano raccolti non presso l'interessato, ma – ad esempio - per effetto del subentro nei rapporti giuridici pre-esistenti in capo al "primo" Titolare. L'articolo 13, invece, troverà applicazione nei casi di ottenimento dei dati direttamente dall'interessato.

È proprio il primo dei due articoli citati che provvede, inoltre, a dare istruzioni pratiche circa le tempistiche concesse per l'obbligo di informativa, e così:

"*Il titolare del trattamento fornisce le informazioni (...):*

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali".

Nell'impianto normativo del GDPR viene contemplata anche la possibilità di trattare i dati per finalità ulteriori e differenti, ma se all'articolo 6 c. 4 questa è inquadrata in una fase quasi "embrionale", nell'articolo 14 c. 4 viene calata nello specifico contesto informativo, prevedendo che qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, ogni informazione pertinente andrà fornita all'interessato prima di tale ulteriore trattamento.

Ciò premesso, e proprio in virtù della vasta platea di interessati toccati da queste operazioni, un ulteriore aspetto da non sottovalutare è quello relativo alla concreta modalità di comunicazione delle informazioni. Se è vero che le norme in materia di privacy spingono per la corretta informazione di ciascun interessato, è altrettanto vero

10 Quali gli innumerevoli accessi non autorizzati ad account, dati, file, documenti e videochiamate.

11 Si fa riferimento alla cd. Sentenza Schrems II, raggiungibile al link: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091it.pdf.

12 Raggiungibili al link: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en.

che dinnanzi a certi numeri raggiungere l'obiettivo potrebbe diventare difficile, se non addirittura impossibile.
Sul tema – ben prima dell'entrata in vigore del GDPR – l'Autorità Garante italiana aveva preso posizione, stabilendo la possibilità di "*prescindere (...) dal rendere l'informativa individuale agli interessati*", laddove venisse fornita "*agli interessati la prevista informativa:*
a. mediante la pubblicazione di un annuncio recante i contenuti dell'informativa sul proprio sito web;
b. tramite annunci pubblicati su almeno due quotidiani a diffusione nazionale;
c. mediante la comunicazione agli interessati in occasione della prima circostanza utile di contatto"[13].
Chiarito doverosamente che i provvedimenti antecedenti l'entrata in vigore del GDPR e del Codice Privacy come novellato continuano ad avere efficacia nei limiti della loro compatibilità con tali norme, rimanendo formidabili indicatori di metodi di *compliance* e di rispetto dei principi di riferimento, l'indicazione del Garante di cui al citato documento pare potersi rinvenire anche nel panorama attuale all'articolo 14 c. 5 l. b) GDPR. In tal senso, infatti, con riferimento all'informativa da fornire per i dati non ottenuti presso l'interessato, il Regolamento prevede la non applicazione delle disposizioni contenute nell'articolo qualora "*comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato (...). In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni*".
Infine, per assicurare la completezza della valutazione e dell'*assessment*, non andranno dimenticati gli ulteriori adempimenti, sempre richiesti in materia di privacy, e così i controlli – e le eventuali implementazioni o correzioni – circa il registro dei trattamenti, le necessarie valutazioni d'impatto (DPIA), le adeguate misure di sicurezza, le (nuove) nomine o i contratti con i responsabili del trattamento o la necessità di un *Data Protection Officer*.

13 Cfr. Garante per la protezione dei dati personali, provvedimento del 19 febbraio 2015, doc. web n. 3864423.

Incident response: come gestire un attacco informatico

di Giovanni Finetto & Paola Finetto

"*Quattro italiani su dieci hanno pagato il riscatto per ripristinare l'accesso ai propri dati dopo essere stati vittima di un ransomware, solo uno su dieci è stato in grado di recuperare i documenti. Una minaccia informatica che è cresciuta sempre di più, soprattutto nell'anno della pandemia e dello smart working, e fa riflettere sull'importanza della protezione e della sicurezza dei dati*"[1].

Il servizio di Incident Response è volto alla gestione degli incidenti informatici, i quali possono comportare anche violazioni di dati personali – o *data breach* – rilevanti ai sensi degli artt. 33 e 34 del GDPR.

Prima di affrontare la questione che maggiormente qui interessa, qual è la gestione di un *data breach,* può essere utile approfondire alcuni aspetti terminologici. Talora, infatti, si adoperano indifferentemente i termini violazione dei dati, incidente informatico e incidente di sicurezza come fossero sinonimi. In realtà, questi vocaboli fanno riferimento a situazioni che tra loro differiscono, per svariati aspetti.

Un **incidente informatico** è, in generale, un evento che comporta malfunzionamenti degli apparati hardware e software e, dunque, può compromettere la funzionalità di una struttura ICT.

Un **incidente di sicurezza delle informazioni** è, più precisamente, un incidente informatico che determina una compromissione effettiva o una minaccia imminente dei sistemi informatici e telematici di una organizzazione.

A titolo meramente esemplificativo, un incidente di sicurezza può aversi nei seguenti casi:
• criptazione delle informazioni contenute nella struttura ICT o parte di essa;
• accesso non autorizzato alla struttura ICT;
• esfiltrazione e diffusione non autorizzata di dati presenti nella struttura ICT;
• compromissione delle credenziali personali di autenticazione;
• perdita o modifica delle configurazioni di sistema;
• interruzione di servizi ICT;
• furto o perdita dei dispositivi;
• impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
• perdita o distruzione di dati a causa di incidenti, eventi avversi, incendi o altre calamità.

Questi eventi, idonei a compromettere la sicurezza sia delle informazioni custodite nella struttura ICT, che della struttura ICT stessa, possono dipendere da azioni intenzionali o da fattori accidentali. A loro volta, le azioni e/o i fattori, che generano l'incidente di sicurezza, possono provenire dall'interno dell'organizzazione, piuttosto che dall'esterno di essa.

Un'azione intenzionale interna presuppone un evidente intento malevolo: è il caso del c.d. collaboratore infedele, che accede al sistema informatico al fine di sottrarre dati e informazioni, per portarli all'esterno dell'organizzazione e farne un uso contrario agli obblighi di riservatezza. Un **fattore accidentale proveniente pur sempre**

1 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.

dall'interno dell'organizzazione, idoneo a generare un incidente di sicurezza, è solitamente riconducibile a una negligenza, talora ad una mera svista di un operatore: si pensi al caso dell'utente, che apre un file inviato tramite posta elettronica o posta elettronica certificata, proveniente da un account sconosciuto, che in realtà contiene un codice malevolo; si pensi ancora all'ipotesi del collaboratore che utilizza nel computer aziendale una pen-drive personale, che è stata in precedenza inconsapevolmente infettata.

Un'**azione intenzionale proveniente dall'esterno dell'organizzazione** coinvolge terzi soggetti, il cui obiettivo è unicamente quello di danneggiare una struttura ICT, al fine di penetrarla e/o di carpire le informazioni e i dati in essa contenuti. In questi casi, molto spesso, la rete dell'organizzazione viene attaccata per finalità ulteriori. È il caso tipico della rete "*zombie*": infettata per essere in futuro "risvegliata" e usata dai criminali nell'ambito di una *botnet*, per sferrare attacchi ulteriori. Peraltro, i dati carpiti dai criminali informatici possono essere a loro volta sfruttati: immessi nel *dark web*, per farne un commercio illegale. Molto più raro, invece, è il caso dell'incidente informatico causato da un **fattore accidentale esterno**.

Ebbene, un incidente di sicurezza, quale che ne sia la causa scatenante, ha sempre un impatto negativo nella struttura dell'organizzazione: il suo verificarsi evidenzia la vulnerabilità di determinati sistemi o apparati, così come dei protocolli interni di sicurezza, e può avere anche un impatto negativo sul business dell'organizzazione. Non è raro che incidenti di sicurezza comportino l'esfiltrazione e la pubblicazione nel *dark web* di dati riservati (know-how dell'organizzazione o di soggetti terzi con i quali la prima collabora), piuttosto che di dati c.d. particolari (o sensibili) relativi a dipendenti, collaboratori, clienti dell'organizzazione stessa. Simili accadimenti compromettono inevitabilmente l'immagine e la reputazione dell'organizzazione e ne minano seriamente il business.

Gli incidenti di sicurezza sono solitamente distinti in tre categorie, tenendo conto sia degli eventi che li hanno determinati, che delle conseguenze che hanno comportato:

- **eventi a basso impatto** (detti anche non significativi): si tratta di eventi gestiti dal sistema di sicurezza dell'organizzazione in maniera silente, tali da non richiedere ulteriori interventi di ripristino specifici; è il caso, ad esempio, del virus intercettato da un sistema di monitoraggio della rete e messo in quarantena, così da non inficiare la funzionalità del device attaccato;
- **eventi significativi**: tali sono gli allarmi di sicurezza e, comunque, gli eventi rilevati nell'ambito dei sistemi e delle infrastrutture ICT, che devono essere presi in carico e analizzati dal personale incaricato delle attività di monitoraggio (quali ad esempio, il rilevamento in tempo reale delle segnalazioni provenienti dai dispositivi di sicurezza, l'analisi dei *log* prodotti da tali dispositivi, la raccolta e la valutazione di comunicazioni su comportamenti anomali o eventi sospetti);
- **eventi critici**: sono sussumili in questa categoria tutti gli eventi significativi che, a seguito delle analisi effettuate, sono ritenuti idonei a comportare, direttamente o indirettamente, una compromissione della struttura ICT dell'organizzazione e, comunque, una violazione delle politiche di sicurezza della medesima.

Il ***data breach*** (o violazione di dati) è, a sua volta, una particolare tipologia di incidente di sicurezza delle informazioni, che coinvolge i dati personali. Una tale violazione può essere determinata da un fattore accidentale oppure da un'azione intenzionale, al pari di ogni altro incidente di sicurezza. A questo riguardo giova ricordare che l'art. 4, comma 1 n. 12, del GDPR definisce la violazione dei dati personali come la "*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*". Il Considerando 85 del GDPR precisa, peraltro, che "*Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata*". Si comprende, dunque, come sia necessario non solo non sottovalutare una violazione di dati personali ma, ancor più, gestirla correttamente.

Un *data breach* può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali coinvolti.

La **riservatezza** dei dati, riconducibile al diritto alla segretezza e alla non divulgazione dei dati medesimi, può essere compromessa nel caso di furto di informazioni. Così, ad esempio, nella ipotesi di perdita o furto di uno smartphone o di un computer portatile, ma si pensi anche al caso, tutt'altro che raro, di utilizzo di device aziendali per fini privati (navigazione in siti pericolosi, uso di chiavetta USB non aziendale e infetta). Anche l'installazione di programmi gratuiti scaricati dal web potrebbe compromettere la riservatezza dei dati e avere ripercussioni sulla sicurezza della struttura informatica dell'organizzazione.

L'**integrità** dei dati, per tale intendendosi la legittima aspettativa che le informazioni non vengano modificate, cancellate o distrutte in modo non autorizzato o improprio, può parimenti essere compromessa da un incidente informatico che riguarda i dati stessi (gli esempi possono essere i medesimi già richiamati per il caso di incidenti afferenti alla riservatezza dei dati), ma pure il sistema informatico (del quale non sia più possibile garantire il funzionamento; tipico è il caso dell'attacco *phishing* sferrato con successo, con l'invio di virus malevoli contenuti in allegato ad un messaggio di posta elettronica, aperto dall'utente, con conseguente criptazione dei dati e blocco del sistema).

La **disponibilità** dei dati, la quale si riferisce al diritto degli utenti autorizzati di poter disporre sempre di determinate risorse, può essere compromessa da incidenti di sicurezza che impattano su informazioni, applicazioni, servizi, sistemi, reti. Tipico esempio di evento che pregiudica la disponibilità delle risorse sono gli attacchi DoS (*Denial of Service*) e DDoS (*Distributed Denial of Service*).

Ebbene, in caso di *data breach* sono compromesse proprio la riservatezza, la integrità e la disponibilità dei dati, naturalmente con intensità e modalità differenti,

che variano nei singoli casi. Ogni incidente di sicurezza che pregiudica in qualche modo i dati personali dev'essere valutato con attenzione, con riferimento anche agli obblighi di comunicazione specificamente previsti dal GDPR. L'articolo 33 del GDPR stabilisce l'obbligo di comunicare, all'autorità di controllo competente, l'avvenuta violazione di dati personali entro un termine di 72 ore dalla sua scoperta, qualora si sia concretizzato un danno o una minaccia alle libertà o ai diritti delle persone titolari dei dati. L'articolo 34 stabilisce, inoltre, l'obbligo di comunicazione agli interessati, dando notizia del *data breach* che si è concretizzato, solamente nel caso in cui esista un rischio elevato per i diritti e le libertà degli interessati.

L'incremento dei crimini informatici, la (ahimè) notevole fantasia dei criminali informatici, che sviluppano minacce sempre nuove e diverse, la consapevolezza che nessuna struttura ICT può mai considerarsi assolutamente resistente ai rischi *cyber*, deve indurre le organizzazioni ad affrontare con professionalità e competenza adeguate gli incidenti informatici, tanto più se essi comportano una violazione di dati personali. Ciò rende necessario saper gestire ogni incidente di sicurezza correttamente e con efficacia.

L'*Incident Management* e l'*Incident Response* sono i servizi – e relative competenze e attività – a disposizione delle organizzazioni che subiscano un incidente di sicurezza o un *data breach*.

L'***Incident Management*** identifica la capacità di gestire l'evento in modo efficace, così da minimizzarne le conseguenze avverse, assicurare la *business continuity* e, al contempo, gestire i rapporti con terze autorità di Pubblica Sicurezza e con le autorità di controllo. Un servizio concretamente efficace di *Incident Management* deve poter offrire all'organizzazione tutte le risorse – umane e materiali – necessarie, per garantire una gestione lineare dell'incidente di sicurezza, dunque senza stravolgimenti nella operatività quotidiana dell'organizzazione, i quali, altrimenti, appesantirebbero le già presenti – e non indifferenti – conseguenze dell'evento occorso. Obiettivo primario dell'*Incident Management* è quello di definire una corretta strategia di gestione dell'incidente verificatosi, tenendo conto anche delle procedure di sicurezza e dei protocolli di gestione del rischio adottati dall'organizzazione. Quest'ultima può essere realmente e concretamente supportata, laddove il servizio di *Incident Management* sia idoneo a:

• definire e, ove necessario, attuare le misure necessarie per ridurre l'impatto dell'incidente di sicurezza sulla operatività quotidiana;

• identificare le ulteriori iniziative da assumere, in un arco temporale ben definito, al fine di ripristinare e garantire la *business continuity*;
• segnalare ai responsabili dell'organizzazione la necessità od opportunità di denunziare l'occorso alle autorità di Pubblica Sicurezza o di portarlo a conoscenza di una autorità di controllo e, eventualmente, di darne notizia ai terzi i cui dati siano stati compromessi;
• definire e, ove richiesto, mettere in atto misure tecnico-organizzative ulteriori, rispetto a quelle di cui l'organizzazione già dispone, per assicurare o implementare una migliore e più efficace difesa contro gli attacchi;
• effettuare, ove necessario od ove richiesto, un'attività specifica di analisi e investigazione, per ricostruire l'occorso e individuare le vulnerabilità dei sistemi e le ulteriori misure di mitigazione del rischio;
• analizzare, ove necessario o su sollecitazione dell'organizzazione, i protocolli interni di gestione del rischio, per eventualmente individuare misure e protocolli da aggiornare o da introdurre *ex novo*.

L'*Incident Management* riguarda, conclusivamente, tutte le azioni intraprese prima, durante e dopo il verificarsi di un incidente di sicurezza delle informazioni.

Una parte importante, anzi determinante, di questo processo è l'*Incident Response*.

L'***Incident Response*** è, dunque, una fase o, meglio, una componente del più ampio e articolato processo di *Incident Management* e identifica le attività e le risorse necessarie per ripristinare la continuità operativa dell'organizzazione il più velocemente possibile, minimizzando gli impatti negativi dell'incidente di sicurezza e, al contempo, identificando le ulteriori iniziative da adottare a fronte dell'evento occorso.

Se virtuosa, l'organizzazione potrebbe avere già adottato una propria procedura di gestione dell'*Incident Response*, la quale dovrebbe includere:
• la costruzione di un protocollo interno *Incident Response*, che definisca *step by step* le azioni da intraprendere nel caso in cui si verifichi un incidente di sicurezza;
• lo sviluppo di procedure interne per garantire il tracciamento di ogni incidente di sicurezza e un adeguato flusso di informazioni da e verso gli organi amministrativi e di controllo dell'organizzazione;
• l'approntamento di linee guida per definire le comunicazioni dirette ad enti o autorità esterne all'organizzazione, relative sempre ad un incidente di sicurezza (ad esempio, polizia postale o Garante per la protezione dei dati personali);
• la creazione di un team interno, con competenze sia tecnico-informatiche che giuridiche, in grado di gestire un incidente di sicurezza (*Incident Response Team*), con previsione di sessioni formative ricorrenti e specifiche per coloro che ne fanno parte.

In molti casi, tuttavia, l'organizzazione sceglie di affidarsi ad un *Incident Response Team* esterno.

Invero, un gestore esterno dispone solitamente di maggiori competenze e risorse, umane e strumentali, ed è pertanto in grado di offrire un servizio eccellente e completo di gestione dell'incidente di sicurezza. Per molti motivi, non da ultimo per ragioni di maggiore economicità, le organizzazioni colpite da un incidente informatico richiedono il "pronto intervento" di un *Incident Response Team* esterno. Gli attacchi informatici compromettono sempre più frequentemente i dati personali e il business: ciò rende ormai imprescindibile saper rispondere velocemente ed efficacemente agli incidenti di sicurezza e, ancor più, a quelli che comportano un *data breach*. La capacità di gestire l'attività di *Incident Response* è diventata un fattore critico: le organizzazioni hanno bisogno del supporto di un team che sia in grado di:
• affrontare gli incidenti di sicurezza con sistematicità ed efficacia;
• supportare l'organizzazione nel prendere tempestivamente le decisioni appropriate al caso concreto;
• ripristinare e garantire la continuità operativa;
• fornire ogni suggerimento utile per permettere all'organizzazione di migliorarsi e

di trarre, anche da un evento dannoso, qual è un incidente di sicurezza, utili spunti per implementare la resilienza della sua struttura di fronte ad attacchi informatici sempre nuovi e diversificati.
Un *Incident Response Team* effettivamente efficace dovrà, quindi, saper offrire all'organizzazione un insieme di procedure, sistemi e risorse (non solo informatiche ma anche legali), necessari e utili per reagire all'incidente informatico.

Nonostante il GDPR non prescriva espressamente di creare un CSIRT (*Computer Security Incident Response Team*), è evidente che, per garantire la conformità all'articolo 33 del GDPR, una organizzazione non può farne a meno: ogni ente, secondo quanto previsto dal GDPR, deve dotarsi di un piano di gestione degli incidenti informatici, che permetta di attivare, automaticamente, alcuni meccanismi tecnologici e precise procedure tecnico-legali finalizzate alla minimizzazione del danno e alla continuità operativa. Questa gestione si articola essenzialmente nelle seguenti fasi:
• risposta iniziale all'incidente;
• investigazione;
• ripristino dei sistemi compromessi, laddove possibile, e comunque ripristino della continuità operativa;
• supporto all'organizzazione per le comunicazioni da effettuare nei confronti di autorità di Pubblica Sicurezza o di controllo.

Nella prima fase di **risposta iniziale**, il team che interviene determina il tipo di incidente e il suo potenziale impatto, interloquendo con chi ha rilevato l'incidente, revisionando i relativi *log* di rete o di sistema, mantenendo copia documentale di tutte le informazioni raccolte. È, questa, una fase delicata: si approccia, infatti, un'organizzazione che ha subito un incidente informatico e i cui dati sono stati in qualche modo violati, compromessi. Il titolare dell'organizzazione ha, in questo momento, una duplice esigenza: da un lato promuovere ogni iniziativa utile e necessaria per verificare l'occorso; dall'altro ripristinare quanto prima la *business continuity*.

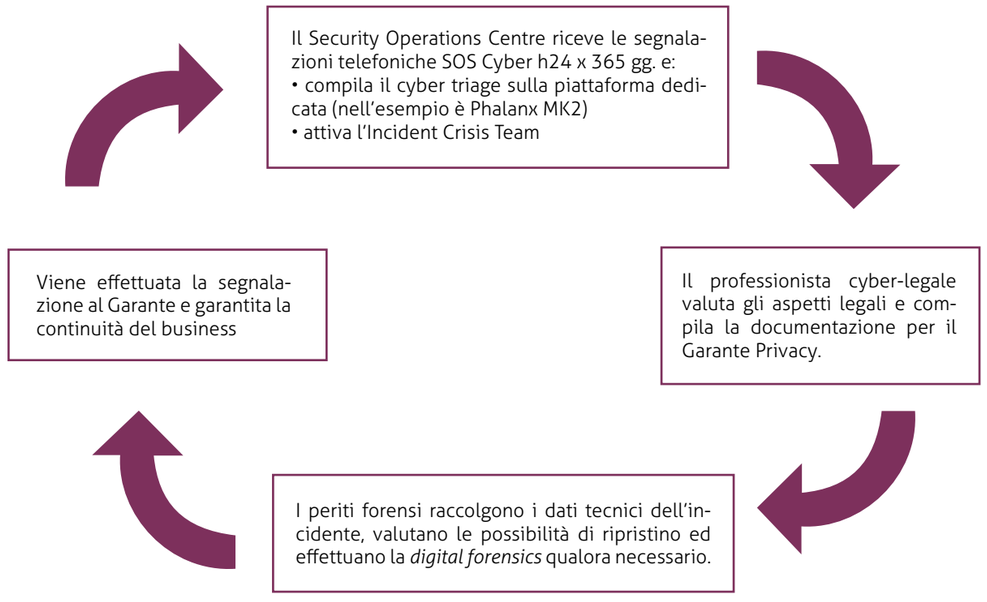
Nella fase successiva, quella **investigativa**, una volta cristallizzata la "scena del crimine informatico" si accerta quanto presente nei sistemi e nelle reti, al fine di ricostruire le cause e la dinamica dell'incidente occorso. In questa fase si applicano le metodologie che fanno capo alla *digital forensics*, l'analisi forense dei campioni rappresentativi rispetto all'incidente informatico verificatosi con una metodologia ben nota, denominata "copia bit a bit". In questa fase è molto importante – anzi, determinante – procedere con attenzione e competenza in ogni singolo step dell'iter di verifica e accertamento, in quanto gli esiti di queste indagini potrebbero essere utili per il titolare del trattamento per individuare responsabilità (o, come più frequentemente accade, corresponsabilità) nella generazione dell'incidente occorso.

La terza fase è diretta al **ripristino della operatività**: essa si concentra sul ripristino dei dati e della rete, possibilmente riportandoli al momento precedente all'attacco informatico, solo dopo avere "bonificato" e "disinfettato" i *device* da ogni codice malevolo presente all'interno.

Da ultimo, l'*Incident Response Team* dovrà fornire all'organizzazione ogni utile supporto per la gestione della **comunicazione verso l'esterno**. Si tratta, in questo caso, di affiancare l'ente nella valutazione, prima, e nella esecuzione, poi, di una eventuale denunzia alle autorità di polizia, piuttosto che di una comunicazione al Garante per la protezione dei dati personali (inevitabile nel caso previsto dall'art. 33 GDPR) o, ancora, di una comunicazione dell'evento occorso nei confronti di terzi soggetti, i cui dati siano stati violati con un conseguente grave rischio per i loro diritti o le loro libertà (è, questo, il caso cui si riferisce l'art. 34 GDPR).

Come si è già evidenziato, l'approccio del team di *Incident Response* sarà necessariamente multidisciplinare e organico: le competenze che il team deve possedere sono, infatti, sia tecniche, che giuridiche, dovendosi verificare, tra l'altro, se l'organizzazione abbia approntato ed efficacemente attuato procedure interne per la corretta gestione della protezione dei dati personali, e dovendo il team altresì interloquire anche il Responsabile della Protezione dei Dati (RPD - DPO), se nominato ai sensi dell'art 37 e seguenti del GDPR. Il team per lo svolgimento delle attività di *Incident Response* è normalmente composto, in relazione alle necessità e in considerazione della concreta organizzazione e operatività della struttura attaccata, anche da una o più figure di *Senior Security Consultant*. In ogni caso, tutte le risorse dell'*Incident Response Team* devono possedere le necessarie competenze per definire con i vertici dell'ente l'approccio metodologico più efficace e adeguato ad affrontare e risolvere le problematiche emerse.

ESEMPIO DI FUNZIONAMENTO DI UN SOC



***

Tutto quanto sopra esposto contiene un inquadramento generale e, per così dire, dottrinale dell'argomento.

Ora intendiamo raccontarvi un'esperienza reale, una storia di sopravvivenza aziendale vissuta da una classica PMI del Nord Italia che ha dovuto affrontare e combattere il "mostro" sopra citato, il *ransomware*.

I ***ransomware*** sono virus malevoli che consentono ai criminali informatici di appropriarsi della rete di un'azienda, di criptarne i dati e poi di chiedere alla vittima una somma in denaro (normalmente in cryptovaluta) per restituire i file. Secondo il Clusit[2], 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 significativa.

La vicenda che di seguito raccontiamo, seguendo la cronologia degli eventi ma rendendo opportunamente non riconoscibile la realtà di cui parleremo, ha rappresentato per il nostro *Incident Response Team*, un modello di gestione, virtuosa, di un incidente informatico, applicando tutte le discipline necessarie alla sua gestione: da quelle tecniche a quelle legali, alla comunicazione interna ed esterna.

Agli inizi di settembre 2020 un dirigente dell'ente, vittima dell'attacco informatico, si accorgeva, mentre si trovava sul posto di lavoro, che i files salvati sul server usuale risultavano non leggibili. Allertava dunque il responsabile dei sistemi informatici, che confermava trattarsi di files infetti da un crypto-locker. Lo stesso informava il dirigente di avere anche ricevuto un messaggio, tramite una chat online (le cui indicazioni aveva trovato in un file non criptato) da parte di sconosciuti, che presumibilmente erano i protagonisti dell'attacco informatico. Il riscatto richiesto era di circa 700.000,00 euro, pena la pubblicazione online della totalità dei dati carpiti.

In realtà, gli aggressori avevano già pubblicato su un sito del deep web, il 5% dei dati carpiti in modo tale da dimostrare l'efficacia delle loro azioni.

A quel punto, il responsabile IT dell'ente, sentendo su di sé il peso di una soluzione e, in parte, la responsabilità dell'accaduto, cominciava a cercare affannosamente in rete una possibile soluzione alla situazione critica che si stava delineando e le cui conseguenze non poteva nemmeno immaginare. Cominciava dunque a contattare online diverse aziende, che propongono la decrittazione dei file cifrati da *ransomware*.

Attenzione, questa attività per una vittima di attacco *ransomware* può essere sia un'opportunità che un ulteriore problema:
• per alcune famiglie di *ransomware*, soprattutto dei più datati, è possibile effettivamente procedere ad una decrittazione, poiché esistono online delle organizzazioni che hanno creato un database di chiavi di decrittazione, oppure perché anche istituzioni pubbliche (FBI, etc.) mettono a disposizione le informazioni a seguito di arresti perpetrati nei confronti dei criminali con conseguente sequestro dei server e dei pc utilizzati per l'attacco;
• alcune aziende invece, con altri intenti, di certo non benevoli e legali, semplicemente si propongono come intermediari tra le vittime e gli attaccanti e trattano il riscatto al posto delle vittime (consapevolmente o inconsapevolmente).

In sintesi, per i nuovi *ransomware* è molto difficile, se non impossibile, poter decifrare i dati. Tuttavia, conviene sempre tenere una copia dei dati cifrati in modo tale da poterli decifrare in un secondo momento in caso di arresto dei malfattori.
Ad ogni buon conto, il responsabile IT dell'ente vittima dell'attacco informatico, contattava anche, tra le altre, l'organizzazione, con la quale gli scriventi operano o comunque collaborano. Immediatamente allertato, tale Incident Response Team esterno, composto da un esperto legale, un esperto tecnico ed un incident commander, prendeva contatti con l'ente vittima e, contestualizzato l'evento in un primo veloce briefing, esponeva i passi necessari per gestire la situazione emergenziale e migliorare la resilienza aziendale:
• effettuazione della copia dell'ultimo back-up in un altro storage anche locale;
• effettuazione della copia dei server criptati per eventuali possibilità di decrittazione future in un altro storage anche locale;
• bonifica della copia dell'ultimo back-up per verificare la presenza di file infetti all'interno;
• effettuazione dell'analisi tecnica dell'incidente (*digital forensic*) prima di ripristinare il back-up;
• bonifica delle macchine/server infetti;
• ripristino del back-up;
• effettuazione della dichiarazione di violazione al Garante della Privacy entro 72 ore (eventualmente posticipando l'invio della *digital forensic* e/o vari approfondimenti);
• comunicazione a clienti e fornitori del *data breach* e delle misure attuate (sito web, social, comunicato stampa/brand reputation);
• riprogettazione ed implementazione di un nuovo sistema di back-up con controlli di efficacia e prove di ripristino;
• effettuazione di *vulnerability assessment* della rete al fine di verificare ulteriori vulnerabilità;
• implementazione delle misure di sicurezza *cyber* al fine di monitorare la rete in tempo reale per prevenire ulteriori minacce;
• valutazione di un'assicurazione *cyber risk* e di un servizio in abbonamento di *SOS cyber/Incident Response*.

Nel caso di specie, dall'analisi della richiesta pervenuta dalla vittima, contenente alcuni dettagli dell'incidente, e dal know how in possesso della organizzazione capofila dell'Incident Response Team esterno sulle moderne tecniche di attacco hacker, si è riusciti a identificare i seguenti, quali principali e più probabili vettori sfruttati per sferrare l'attacco tramite *ransomware*:
• e-mail di phishing;
• vulnerabilità dei sistemi esposti su Internet;

2 Rapporto Clusit 2021 sulla sicurezza ICT in Italia https://clusit.it/rapporto-clusit/
3 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.

• errate configurazioni degli apparati di rete.

Infatti, tra i *ransomware* recenti e in quel periodo (fine 2020) più diffusi, i più noti e temuti erano Ryuk, Ekans e **Maze**. Pur essendo tra loro diversi, questi *ransomware* erano accomunati dalla metodologia (*kill-chain*) con cui attaccavano un'organizzazione o impresa.
La ***kill-chain*** è normalmente costituita dalle seguenti fasi:

1. 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.

2. Infezione: l'esecuzione di questo malware permette all'attaccante di carpire le credenziali e diffondere l'infezione all'interno dell'organizzazione.

3. 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).

4. 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, apparti di rete e dispositivi connessi) sia stata compromessa.

5. 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 *ransomware* Maze 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 dei dati personali, si rende necessaria la notifica all'Autorità Garante della Privacy.**

Tornando dunque al caso in esame, una volta reso edotto il Board di quanto sopra, e a seguito di una prima riunione del *Crisis Action Team* aziendale, nel contesto della quale emergeva che la consistenza numerica dei server in servizio e potenzialmente infettati era di almeno n. 30 con ulteriori 200 macchine, l'Incident Response Team esterno veniva investito della gestione dell'**attività di Incident Response, affiancando con pieni poteri di coordinamento le società e i professionisti informatici (amministratori di rete/sistema – responsabili esterni del trattamento dei dati)**, ai quali l'ente vittima si era fino a quel momento affidato, **e procedendo ad elaborare un piano di gestione comprendente quanto di seguito riportato.**

1) Mappatura fisica dell'infrastruttura tecnologica
• definizione del perimetro di analisi
• mappatura degli spazi fisici
• verifica degli aspetti di continuità elettrica
• verifica degli aspetti di collegamento ad internet
• raccolta delle credenziali di accesso

2) Analisi della rete interna
• rilevazione delle configurazioni di rete
• creazione anagrafica dei dispositivi collegati con catalogazione della tipologia, porte aperte, servizi attivi, condivisioni di rete ed eventuali vulnerabilità
• rilevazione dei punti di accesso fisico alla rete LAN
• rilevazione delle reti wifi e delle politiche di accesso

3) Analisi della rete esterna
• rilevazione degli indirizzi IP pubblici
• creazione anagrafica punti di accesso ed eventuali vulnerabilità tecnologiche

4) Analisi PC CLIENT e SERVER
• rilevazione dei software installati
• catalogazione degli account utente
• raccolta delle configurazioni di rete
• raccolta delle policy di configurazione del sistema
• verifica delle configurazioni di backup
• verifica delle connessioni attive
• verifica dello stato del firewall di sistema
• verifica della risoluzione forzata dei nomi a dominio
• raccolta delle informazioni sui processi attivi
• verifica delle impostazioni e dello stato dei servizi
• verifica dello stato aggiornamento del sistema operativo
• catalogazione contenuto della cartella dei programmi
•mappatura delle unità di rete connesse
• raccolta dell'elenco dei file recenti
• raccolta dell'elenco file modificati di recente
• mappatura delle credenziali di accesso memorizzate
• rilevazione delle politiche di gestione delle periferiche USB

5) Analisi APPARATI DI RETE (switch, router, firewall, access point)
• rilevazione della tipologia di dispositivo
• verifica delle credenziali di accesso
• analisi della configurazione
• raccolta dei file di *log*

6) Analisi DEVICE GENERICI (telecamere, stampanti multifunzione, tecnologie proprietarie)
• rilevazione della tipologia di dispositivo
• verifica delle credenziali di accesso
• analisi della configurazione
• raccolta dei file di *log*

7) Analisi forense dell'attacco informatico
• rilevazione dei punti di accesso
• verifica del vettore di attacco
• identificazione, se possibile, del virus e delle tecniche utilizzate
• replica del funzionamento in ambiente protetto al fine di raccogliere ulteriori informazioni
• definizione del perimetro di accessibilità dell'attaccante
• verifica della possibilità di movimento laterale nella rete
• rilevazione delle modalità di accesso ai dati
• verifica dell'attuazione di tecniche di persistenza dell'attaccante

8) Configurazione del monitoraggio continuativo del traffico di rete su base temporale
• salvataggio degli eventi di rete con analisi del traffico
• ricerca di eventuali comportamenti sospetti
• rilevazione dei dispositivi a rischio
• elaborazione della mitigazione del rischio attraverso procedure e configurazioni software

9) Elaborazione dei dati raccolti
• acquisizione dei dati di input
• normalizzazione dei file strutturati
• archiviazione e armonizzazione degli indicatori di rischio
• valutazione coordinata del team di Cyber Analysis con attribuzione degli indicatori di impatto in base alle linee guida

• elaborazione delle eventuali misure correttive

10) Documentazione e proposta di mitigazione del rischio
• evidenziazione delle criticità fisiche
• rappresentazione grafica della topologia di rete
• elaborazione dei fattori di rischio informatico e tecnologico
• proposta di soluzioni per il miglioramento del livello di rischio
• redazione del report per la notifica al Garante della Privacy in caso di *data breach*

Al termine della fase di analisi si constatava che:
• la violazione era databile almeno al novembre dell'anno precedente al conclamarsi dell'attacco informatico;
• la tipologia di attacco era di tipo *Advanced Persistent Threat*, ovvero si trattava di attacco sferrato mediante l'utilizzo di più tecniche di attacco combinate con esfiltrazione di circa n. 86 GB di dati;
• la causa della violazione era riconducibile ad una combinazione dello sfruttamento di diverse vulnerabilità da parte delle Botnet attive; in sintesi, gli hacker avrebbero potuto sfruttare diversi canali di ingresso vulnerabili;
• era stato compromesso circa il 65% della rete.

Contestualmente, l'esperto legale facente parte dell'Incident Response Team esterno provvedeva ad affiancare il Board aziendale e il RPD/DPO per la Comunicazione del *data breach* al Garante della Privacy, suggerendo di predisporre e tempestivamente inviare una prima notifica c.d. preliminare e, a distanza di qualche settimana, la notifica c.d. integrativa, ove rendere conto dell'occorso nel dettaglio e sulla base delle informazioni raccolte medio tempore dal Team, altresì interloquendo con il Garante per dirimere ogni dubbio circa la correttezza della condotta aziendale.

Nel febbraio di quest'anno giungeva la notizia, diffusa dalla stampa internazionale, dell'arresto in Ucraina di affiliati e operatori del *ransomware* Egregor, individuati – sembra – seguendo il denaro, dunque rintracciando i pagamenti dei riscatti.

***

Conclusivamente, si comprende quanto sia cruciale disporre delle risorse, interne o esterne all'organizzazione, per saper gestire bene l'attività di *Incident Response*. Non ci si improvvisa esperti nella gestione degli incidenti di sicurezza: al contrario, si tratta di un servizio che richiede competenze qualificate e trasversali, capaci di dialogare tra loro al solo fine di affrontare, con immediatezza ed efficacia, una situazione critica e, così, saper restituire all'ente vittima di un attacco informatico la serenità e la forza necessarie per garantire la continuità operativa.

Strumenti innovativi di valorizzazione dell'impresa: il ruolo del professionista e dell'influencer

di Nicola A. De Carlo & Ivano Maccani

Strategie sostenibili nelle PMI

Parlare di sostenibilità non significa mettere in discussione che la priorità di un'azienda sia garantire la redditività del business. Anzi, la sostenibilità è uno strumento chiave per sostenere la competitività di un'impresa e quindi garantire la sua redditività. Rappresenta qualcosa che si aggiunge alle attività ordinarie e ne diventa parte integrante.
Nel nostro Paese operano aziende virtuose rispetto allo sviluppo sostenibile ma questo non vale ancora per il sistema produttivo nella sua interezza, anche per l'assenza di politiche adeguate. Varie, però, sono le iniziative che possono essere messe in atto, grazie anche al ruolo dei professionisti esterni che hanno il delicato e fondamentale compito di condurre l'impresa verso gli standard di sostenibilità.
Una di queste è il *Co Branding*, ovvero la collaborazione tra due marchi, l'unione di due brand che siano compatibili tra loro al fine di apportare valore all'esperienza dei clienti e garantire una partnership vincente che può portare vantaggi ad entrambe le parti (impresa e cliente). Esistono centinaia di esempi di *Co Marketing* per i grandi brand e le grandi realtà, pochi invece sono gli esempi con le PMI e le micro imprese, spesso perchè queste realtànon hanno la documentazione prodotta dalle *public relations* dei brand più strutturati. Ma quali sono i vantaggi che una politica come questa potrebbe portare alle PMI? Perché il *Co Branding* funziona? Sostanzialmente perché si lavora sulla fiducia del cliente, potenziandola a livello emozionale, ma anche perchè si crea movimento e interazione attorno ai due brand e, sfruttando questa opportunità, entrambi possono acquisire nuovi clienti e aumentare il profitto. Fare *Co Branding* creando nuove alleanze e partnership permette di creare molteplici possibilità di business per la propria azienda, riposizionarsi sul mercato e ridurre i costi di pubblicizzazione.
Il "matrimonio" non *è* sempre felice e privo di rischi, naturalmente. Esistono problematiche di cui è necessario tener conto, come riuscire a trovare un brand compatibile che condivida valori e obiettivi comuni della nostra impresa; motivo per cui deve essere eseguita un'analisi oculata da un esperto professionista che ne deve valutare vantaggi e criticità per poter condurre l'impresa verso la scelta più adatta.
Il ruolo del professionista esterno sarà di tipo tecnico nel trovare il giusto partner ma consisterà anche nel saper far riflettere l'impresa su ciò che vuol dire fare buona impresa favorendo il lavoro.
Un altro esempio di sostenibilità può essere rappresentato dall'approccio del *cause-related marketing* (CRM) che rappresenta un altro modo di fare partnership e consiste nell'associare il marchio di un'impresa ad un altro, come organizzazioni no profit e ONG (ad esempio le imprese che sostengono associazioni come Emergency, il WWF o Greenpeace). Per le imprese questo rappresenta un efficace modo di comunicare al proprio cliente il proprio impegno sul tema attraverso azioni concrete.
Tra le nuove sfide del marketing spicca sicuramente anche il ruolo degli influencer. Uno studio del 2020 mette in evidenza

come il 75% delle aziende siano impegnate nell'*influencer marketing*[1]. Che cos'è? Si tratta di una forma di marketing che si basa sull'influenza e sul coinvolgimento che alcuni soggetti – influencer – esercitano sul potere d'acquisto di altri. Sono persone che hanno acquisito notorietà sul web. I social network, canali attraverso i quali l'utente conosce l'influencer, fanno si che i due possano interagire facilmente facendo sentire l'utente parte integrante di quell'ispirazione e influenza. Le aziende si sono accorte del potenziale di queste nuove celebrità e sono disposte a pagare cifre da capogiro per coinvolgerle nelle loro campagne.
Se fino a qualche anno fa i mezzi di comunicazione erano la televisione, la radio, i cartelloni pubblicitari, oggi l'esperienza del consumatore è completamente cambiata, ponendo al centro delle dinamiche del marketing la figura dell'influencer che ha la capacità di potenziare la visibilità del prodotto e del brand e soddisfare appieno le richieste della clientela. Grazie al ruolo dell'influencer il cliente si sente infatti parte di una *community*, sviluppa un senso di appartenenza e un riconoscimento di passioni e valori, e al tempo stesso l'azienda ottiene la fidelizzazione del cliente.
La principale differenza rispetto al modello televisivo risiede nel fatto che attraverso i social network il pubblico non vive passivamente la fruizione di un prodotto ma ha la possibilità di interagire costantemente con il creatore di un contenuto (influencer), il quale viene gratificato quanto più riesce a sviluppare *engagement* attraverso interazioni, commenti e condivisioni.
Quando parliamo di piccole e medie imprese come cambia l'approccio alla Responsabilità Sociale d'Impresa? La figura del professionista esterno risulta dunque fondamentale per far si che siano adottate determinate misure e poste in essere attività utili per il corretto funzionamento dell'impresa. La consulenza aziendale è un servizio poliedrico offerto ad enti *for profit* e mira ad affinare l'efficacia delle tecniche di gestione organizzativa e dei processi operativi. Si può definire come un processo di trasferimento di competenze, conoscenze e abilità da una parte (il consulente) a un'altra (il cliente) con l'obiettivo di fornire aiuto o aiutare a risolvere problemi esistenti[2]. Il ruolo del consulente consiste nel mettere in luce il punto di vista tecnico e metodologico per portare l'azienda a comprendere lo scenario esterno, mitigando i rischi e cogliendo le possibili opportunità legate all'evoluzione dei temi sociali e ambientali. L'imprenditore ha il ruolo di tradurre questi input in vantaggio competitivo per il suo business. È colui che fa dei dati una visione manageriale. È importante che azienda e consulente lavorino insieme.

La Responsabilità Sociale d'Impresa
Il concetto di Responsabilità Sociale di Impresa – RSI (*Corporate Social Responsibility* – CSR) nasce e si diffonde negli Stati Uniti negli anni '50 con l'avanzare della consapevolezza da parte delle aziende di non dare rilievo solo ai risultati economici ma anche alle conseguenze sul piano sociale. In linea con le esigenze del mondo contemporaneo, gli imprenditori, i dirigenti e i professionisti che operano in azienda devono saper coniugare le capacità organizzative, etiche e tecniche, con l'obiettivo di migliorare le condizioni delle persone e dei luoghi in cui l'azienda opera. In questo periodo emerge la concezione secondo cui l'impresa deve impegnarsi in azioni valide che soddisfino anche bisogni e aspettative più ampie della società: le scelte aziendali devono quindi essere valutate anche in riferimento a obiettivi e valori validi anche sul piano sociale.
Negli anni '60 e '70 si apre un dibattito più ampio - pur se continua ad avere notevole peso una visione più conservatrice, anch'essa originaria del mondo dell'impresa americana - secondo cui l'unico dovere di un'azienda è quello di aumentare il profitto, e si afferma una concezione più *liberal* in cui la responsabilità sociale inizia esattamente dove termina l'aspetto normativo. Va affermandosi sempre più un ruolo sociale delle imprese, che va oltre la sfera legale ed economica. Questo significa che un'organizzazione non può essere considerata "socialmente responsabile" se si limita ad attenersi solo a ciò che è previsto dalle norme (che però naturalmente devono essere scrupolosamente rispettate).
In tale nuovo scenario emergono obblighi e responsabilità non più solo in ambito economico di produzione della ricchezza e del profitto, ma agendo sempre secondo valori etici e morali. L'impresa deve quindi essere una "buona impresa" sia facendo profitto, sia contribuendo allo sviluppo della comunità di cui fa parte e al benessere degli operatori afferenti ad essa.
Negli anni '80 si critica sempre con maggior decisione l'idea che l'impresa abbia esclusivamente l'obiettivo di essere redditizia, e in tale periodo si colloca la *Stakeholder Theory* che accentua i valori etici e sociali mettendo in evidenza i ruoli di tutti gli individui coinvolti nel processo organizzativo ovvero gli azionisti/dirigenti ma anche i dipendenti, i clienti, i fornitori, i finanziatori, gli enti pubblici, i media. Si instaura in questo modo un'alchimia di mutuo scambio di crescere e svilupparsi in modo tale che il valore creato dall'impresa stessa viene affiancato anche quello che gli altri creano per essa[3].
Potremmo affermare che le scelte e le azioni delle imprese tendono a collocarsi al di là di essa, tenendo conto delle esigenze dei vari *stakeholder*. Assumono valore i concetti di responsabilità, integrità e sussidiarietà.
Recentemente le Nazioni Unite hanno dato vita all'Agenda 2030 per lo Sviluppo Sostenibile. Si tratta di un programma d'azione molto vasto all'interno del quale sono racchiusi 17 obiettivi da raggiungere in ambito ambientale, economico, sociale e istituzionale entro il 2030. Gli obiettivi hanno una validità globale, e coinvolgono tutti i Paesi e le componenti della società, dalle imprese private al settore pubblico, dalla società civile agli operatori dell'informazione e cultura.
I 17 obiettivi nascono da un insieme di questioni importanti per lo sviluppo, prendendo in considerazione le tre principali dimensioni dello sviluppo sostenibile - economica, sociale ed ecologica - al fine di combattere la povertà, contrastare l'ineguaglianza, affrontare i cambiamenti climatici,

costruire società pacifiche che rispettino i diritti umani.
Come va raggiunto dunque il profitto? Dando voce a fattori sociali quali affidabilità, responsabilità, etica e ambiente e aumentando la propria competitività.
Si può dunque affermare che l'imprenditoria socialmente responsabile significhi anche soddisfare le esigenze del cliente e saper dare un contributo positivo allo sviluppo dell'azienda, gestendo il suo impatto con l'ambiente economico e istituzionale in cui opera.

Fare bene impresa
Cosa intendiamo ai giorni nostri quando parliamo di fare impresa? È, in effetti, un concetto complesso, che in parte si discosta dallo svolgere attività economica in sé e che certamente riguarda il prodotto e il servizio, il come lo si realizza e come lo si raggiunge. L'etica, intesa come valore intrinseco, ovvero come il bene a cui l'impresa tende, si inserisce perfettamente in questo scenario in quanto il fine dell'impresa è ciò che definisce il suo valore.
Intraprendere un'attività produttiva prevede alcuni aspetti sostanziali e concreti: il prodotto/servizio e il profitto da un lato, e un aspetto più "avverbiale" rappresentato dalla modalità, ovvero dal "come" si arriva allo scopo e dallo stile che qualifica l'identità di un'impresa, dall'altro.
Come si può facilmente intuire, un prodotto/servizio è qualunque cosa abbia possibilità di avere un mercato e che soddisfi i bisogni dell'utente target, ecco perché compito essenziale dell'impresa è quello di

1 *Taylor, 2020.*
2 *Jacobson et al. 2005.*
3 *De Carlo et al., 2017.*

individuare i bisogni e i desideri, di crearli laddove non siano presenti o, ancora, modellare e conformare quelli già esistenti per far si che siano coerenti all'offerta. In questa dinamica complessa, l'imprenditore non può essere il solo artefice poiché contesto sociale e culturale dettano i suddetti bisogni e desideri, rendendo complessa la sua azione di modifica o modellamento degli stessi. Anzi, spesso l'imprenditore si trova in balia dei desideri e dei bisogni vigenti ed ecco che per definire un prodotto/servizio di successo diventa prioritario captare quali siano i bisogni reali e conoscere il più possibile i contenuti della cultura a cui ci si rivolge. Esistono livelli minimi di funzionalità, senza i quali non sarebbe possibile parlare di un determinato oggetto. Basti pensare a un utensile domestico che non è in grado di svolgere la funzione per il quale è nato: come un'aspirapolvere che non aspira o un ombrello che non ripara dall'acqua. L'altro lato della medaglia è ciò su cui si fonda il mercato e scatena la competizione, ovvero il poter offrire un prodotto/servizio sempre migliore e all'avanguardia.
Il profitto rappresenta un aspetto dello scopo che non può esistere senza il prodotto/servizio offerto: se quest'ultimo non è adeguato non durerà a lungo o non giungerà neppure nel mercato. Ecco, dunque, che il consolidarsi di una struttura etica d'impresa favorisce un'immagine credibile e affidabile. L'utilizzo di tale struttura oltre che contribuire al diffondersi di principi e valori etici, si riflette sui comportamenti verso l'esterno attraverso i quali l'impresa realizza la propria strategia. È naturale che vi sia una sana proporzione fra ciò che viene investito e ciò che ritorna in termini di guadagni e ricavi e fra profitto e responsabilità sociale ed economica dell'imprenditore[4].
Il terzo e ultimo punto, ma non per importanza, è il concetto di identità di impresa che comprende quell'insieme di pratiche, stili manageriali, responsabilità verso i lavoratori, gli *stakeholder*, il territorio e lo Stato. Gli elementi dell'identità aziendale (ad esempio valori e scopi) giocano un ruolo cruciale all'interno delle organizzazioni e gli sviluppi tecnologici hanno permesso alle organizzazioni di esprimersi in molti nuovi modi. L'identità nel contesto di un'organizzazione ha quindi un potenziale strategico significativo[5]. Ciò è dovuto al fatto che l'identità aziendale è in grado di creare una "reputazione aziendale favorevole", lealtà da parte dei clienti, impegno dei dipendenti, eccetera. Melewar, Karaosmanoglu e Paterson (2005) hanno scoperto che l'identità di impresa è in grado di aumentare la motivazione dei dipendenti favorendo il reclutamento e la fidelizzazione del personale, fornire una solida base per la cultura organizzativa, aumentare la trasparenza e, infine, apportare un vantaggio competitivo e sviluppare migliori relazioni.
La personalità e le peculiarità del prodotto o servizio offerto sono fondamentali per assicurare lunga vita nel mercato ed ecco che ritorna il concetto del "come" vengono eseguite le azioni e dell'etica, perché è proprio qua che si nasconde l'anima e la virtù che distingue l'eccellenza dalla mera esecuzione. L'etica d'impresa è infatti non solo etica del prodotto e del profitto ma anche e soprattutto un'etica del modo.
Posto che non esiste impresa priva di una cultura d'impresa, scopo della stessa dovrebbe essere quello di comprendere la sua natura, verificare che non ci si trovi dinnanzi a una cultura trascurata o contraddittoria per poter raggiungere un buon livello economico, produttivo e culturale.

4 *Menegoni et al., 2017.*
5 *Devereux et al., 2020.*

Il buon lavoro: benessere del personale e performance dell'impresa
Fra i bisogni di base della persona l'*International Labour Organization* colloca il lavoro come attività necessaria per il perseguimento dell'autonomia personale e delle relazioni sociali, in termini di identità e riconoscimento. Nel lavoro, infatti, si realizzano le possibilità di soddisfare bisogni sociali, fra cui la possibilità di ricevere una retribuzione che consenta un'esistenza conforme alla dignità umana e ai bisogni materiali della persona e della famiglia anche in relazione alla scuola e al mantenimento e all'educazione dei figli, al sostegno degli anziani e in generale delle persone care. Ma c'è di più perché sul lavoro le persone trascorrono gran parte della loro vita anche in termini temporali: alle otto ore canoniche va aggiunto il tempo e la fatica per il raggiungimento delle proprie postazioni, anche se lo smart working emergenziale cui la pandemia ha costretto gran parte delle persone potrà, se adeguatamente realizzato in futuro, dare rimedio[6].
Ma ciò che conta è la qualità delle ore passate sul lavoro, durante le quali le persone esprimono le competenze acquisite in anni di studio e di varie applicazioni intellettuali e manuali e le loro capacità relazionali, di confronto e collaborazione con colleghi, superiori e utenti. In sintesi, nel luogo di lavoro si manifesta un'ampia e variegata dimensione dell'umano di cui non potremmo fare a meno se non a prezzo di rinunce ad aspetti fondamentali di noi stessi. Il riconoscimento del ruolo dell'attività lavorativa nel soddisfacimento di differenti bisogni, anche profondi, della persona è evidente negli studi relativi alla motivazione che si sono sviluppati in ambito organizzativo/psicologico a partire dalla seconda metà del ventesimo secolo.
Una delle principali teorie della motivazione è la teoria dei bisogni di Maslow, secondo cui il comportamento della persona, anche sul lavoro, tende alla soddisfazione di bisogni ordinati gerarchicamente, che Maslow stesso ha indicato all'interno di una piramide. Alla base della piramide si collocano i bisogni primari ed essenziali alla sopravvivenza (bisogni fisiologici e di sicurezza fisica ed emotiva); salendo si incontrano i bisogni immateriali e di ordine superiore quali i bisogni sociali e quelli del sé (appartenenza e affiliazione sociale, stima e autostima, autorealizzazione); solo dopo aver soddisfatto i bisogni primari, emergeranno i bisogni gerarchicamente superiori. Si possono declinare i bisogni individuali descritti da Maslow ad elementi/fattori dell'organizzazione così da delineare specifiche ed efficaci politiche di gestione delle risorse umane. Così, per soddisfare i bisogni fisiologici e di sicurezza l'organizzazione può agire a livello di retribuzione, sicurezza sul lavoro, condizioni contrattuali; per soddisfare i bisogni di appartenenza e di stima può favorire la qualità delle relazioni interpersonali sul posto di lavoro, la leadership, le ricompense sociali e la crescita professionale, fino al più alto bisogno di autorealizzazione offrendo possibilità di successo e realizzazione professionale e personale.
Dagli studi condotti da Herzberg e colleghi (1959), volti ad indagare il modo in cui si sviluppano i bisogni di stima e di autorealizzazione, si evidenzia anche che vi sono delle tipologie di fattori che incidono rispettivamente sulla soddisfazione e sull'insoddisfazione lavorativa. Alcuni di essi – retribuzione, condizioni di lavoro, relazioni interpersonali, ambiente di lavoro, eccetera – non hanno diretta funzione motivante ma se restano insoddisfatti possono indurre facilmente demotivazione e malcontento. All'interno di questi rientrano la supervisione da parte dei superiori, le politiche aziendali, le condizioni dei lavoratori, le relazioni con i colleghi e i superiori, lo status e la conciliazione vita privata-lavoro. Altri fattori motivanti rappresentano

6 *De Carlo & Maccani, 2021.*

invece quelli sui quali è importante agire al fine di ottenere una motivazione persistente: opportunità di carriera, riconoscimento, conseguimento di obiettivi e risultati, responsabilità, crescita professionale.
Ne consegue quale sfida per le organizzazioni quella di saper creare condizioni organizzative in grado di favorire nei collaboratori obiettivi di tipo "motivante" quali l'aggiornamento e la formazione continua, la spinta all'innovazione e alla creatività, l'ampliamento dell'area di responsabilità individuale e, in generale, la creazione di un clima e di una mission organizzativi coerenti con tali principi/valori. Dunque, nel lavoro perseguiamo fini individuali e collettivi di grande, insostituibile rilievo. Ma ci chiediamo, anche, se *lavorare stanca* e la risposta non può che essere complessa e articolata. Il lavoro, qualsiasi tipo di lavoro, logora in qualche misura, anche cospicua, le nostre energie intellettuali e fisiche, ma in realtà accresce la nostra *vitalità,* il nostro senso di realizzazione, le relazioni positive e costruttive con gli altri.
Come ben evidenziato nel modello richieste-risorse lavorative (*Job Demands-Resources Model*) di Demerouti e colleghi (2001) nel lavoro sono presenti sia aspetti "negativi" (richieste) quali ad esempio il sovraccarico di lavoro o i conflitti che richiedono uno sforzo fisico e mentale, sia aspetti "positivi" (risorse) come il supporto sociale e le ricompense sociali che possono ridurre i costi fisici/psicologici associati alle richieste lavorative e favorire la crescita personale. Secondo il modello, richieste e risorse lavorative possono attivare due processi ben distinti:
• un processo di indebolimento della salute (*health impairment*) laddove le richieste lavorative eccedano e consumino le risorse a disposizione, non permettendo al lavoratore di recuperare ed esponendolo al rischio di sviluppare sintomi e danni psicofisici;
• un processo di motivazione in cui la presenza di risorse sul lavoro attenua l'effetto delle richieste lavorative sostenendo, al contempo, l'impegno, il coinvolgimento e la motivazione della persona (*engagement*) e, di conseguenza, la salute psicofisica e la performance lavorativa.

In una successiva evoluzione del modello[7] si sono introdotte accanto alle risorse lavorative anche le risorse personali o individuali che impattano la percezione positiva della persona delle proprie capacità di poter agire con successo sull'ambiente circostante: l'ottimismo, l'autoefficacia, la resilienza, la speranza.
Oltre agli interventi per sostenere la motivazione e l'impegno della persona, le organizzazioni dovranno sempre più essere orientate anche ad accrescere le risorse personali dei propri collaboratori attivando training specifici per un miglior utilizzo delle proprie risorse personali, per il recupero della fatica, per la conciliazione vita-lavoro.
Il *lavoro, dunque, ci consuma* in termini di fatica e biologici, ed in ciò è parte della nostra vita, che fatalmente ci conduce verso l'esaurimento e l'ineluttabile fine. Al contempo, il *buon lavoro aggiunge qualità ai giorni della vita. Il buon lavoro, si badi*, cioè quello in cui si realizzano progetti personali e collettivi, valori e obiettivi.
Purtroppo non è di tutti il buon lavoro.
Molte persone sono alle prese quotidianamente con contenuti e finalità lavorativi di modesta qualità e soddisfazione. Giova ricordare che la nostra Costituzione recita testualmente che *"l'Italia è una Repubblica democratica fondata sul lavoro... È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese. La Repubblica riconosce a tutti i cittadini il diritto al lavoro e promuove le condizioni che rendano effettivo questo diritto"*. Dunque, emerge dai princìpi fondamentali che regolano la

nostra convivenza un'importante e centrale responsabilità delle organizzazioni nel promuovere obiettivi e condizioni di lavoro consone alla dignità delle persone, tali che donne e uomini possano trarre da esso contributi per il proprio sviluppo individuale e sociale. E trovino nel loro lavoro attenzione, rispetto, cura e benevolenza.
Responsabilità grande, questa, cui non si può sottrarre una classe imprenditoriale degna di questo nome.
Ma perché questi obiettivi vengano pienamente perseguiti occorre anche un atteggiamento attivo di ciascuno di noi.
Ogni persona, infatti, è chiamata a promuovere in sé e negli altri, colleghi, superiori e utenti, il senso dell'autostima, della efficacia del proprio lavoro, del riconoscimento dell'impegno e dei risultati da conseguire.
L'ambiente di lavoro, ricordiamolo, è una sorta di palestra della moralità e dell'etica.
Sta in noi perseguire la verità, il senso della giustizia e quello del buono e del bello, con colleghi, superiori e utenti. E grava un'ampia e rilevante responsabilità su coloro che hanno funzioni di coordinamento e di supervisione sugli altri. Negli ambienti di lavoro devono essere diffusi obiettivi e comportamenti improntati ad equità e giustizia, alla valorizzazione del merito in termini di risultati di ciascuno ma anche di impegno, di buona volontà, di desiderio di migliorarsi, di inclusione. Altrimenti, l'ambiente di lavoro si intossica, diviene il luogo del sospetto, del timore e dell'ingiustizia. Non si possono negare i diritti degli altri, magari anche solo facendo finta di non vedere, e non si possono disattendere le loro necessità. Le azioni devono essere, al contrario, dirette a realizzare obiettivi belli e utili. Ce lo dobbiamo. È proprio in questo modo che possiamo, tutti, concorrere allo sviluppo di noi stessi e degli altri nel lavoro.

7 *Bakker & Demerouti, 2014.*

Bibliografia

Bakker, A. B., & Demerouti, E. (2014). Job demands-resources theory. In P. Y. Chen & C. L. Cooper (Eds.), *Work and well-being: Wellbeing: A complete reference guide* (Vol. III, pp. 37-64). New Jersey: Wiley-Blackwell.

Demerouti, E., Bakker, A. B., Nachreiner, F., & Schaufeli, W. B. (2001). The job demands-resources model of burnout. *Journal of Applied Psychology, 86*, 499-512.

Devereux, L., Melewar, T. C., Dinnie, K., & Lange, T. (2020). Corporate identity orientation and disorientation: A complexity theory perspective. *Journal of Business Research, 109*, 413-424.

De Carlo, N. A., Dal Corso, L., Falco, A., Girardi, D., & Piccirelli, A. (2017). Il mondo del lavoro fra valori e normative. Risultati di un'indagine empirica sulla relazione tra Employee Assistance Programs – EAPs e benessere organizzativo. In F. Menegoni, N. A. De Carlo, & L. Dal Corso, *Etica e mondo del lavoro. Organizzazioni positive, azione, responsabilità* (pp. 119-133). Milano: FrancoAngeli.

De Carlo, N. A., & Maccani, I. (2021). *Codice smart working.* Trento: SEAC.

Herzberg, F., Mausner, B., & Snyderman, B. (1959). The motivation to work. New Jersey: Wiley

Jacobson, N., Butterill, D., & Goering, P. (2005). Consulting as a strategy for knowledge transfer. *The Milbank Quarterly, 83*(2), 299 – 321.

Maslow, A. H. (2010). *Motivazione e personalità.* Roma: Armando Editore.

Melewar, T. C., Karaosmanoglu, E., & Paterson, D. (2005). Corporate identity: concept, components and contribution. *Journal of General Management, 31*(1), 59-81.

Menegoni, F., & De Carlo, N. A. (2016). *Etica e mondo del lavoro. Razionalità, modelli, buone prassi.* Milano: FrancoAngeli.

Menegoni, F., Dal Corso, L., & De Carlo, N. (2017). *Etica e mondo del lavoro: organizzazioni positive, azione, responsabilità.* Milano: FrancoAngeli

Taylor, C. R. (2020). The urgent need for more research on influencer marketing.

SEAC
SECURITY
SERVICE

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

Dalla sentenza Schrems II al Provvedimento BayLDA su Mailchimp: il problema aperto del trasferimento dei dati personali verso gli USA

di Giulia Bontempini & Stefano-Francesco Zuliani

L'attuale normativa in materia di trasferimenti di dati personali all'estero pare, nel suo dettato, chiara e lineare, garantendo la sicurezza dei dati e del business aziendale. La recente sentenza "Schrems II" ha però fatto "saltare" (per la seconda volta) la copertura normativa al trasferimento dei dati negli USA; nel suo recente provvedimento il Garante Privacy bavarese (BayLDA) ha dunque esclamato con voce autorevole che ora "*il re è nudo*"!

In Europa: la direttiva madre del '95

L'Unione Europea negli ultimi decenni ha adottato numerose normative atte a tutelare i diritti e le libertà fondamentali dei cittadini, anche sotto il profilo della protezione dei dati personali verso paesi terzi. Tale tema è stato introdotto nella c.d. "Direttiva Madre" del '95[1] che recitava: "*Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali (...) può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato*" (art. 25). All'epoca si era ancora agli albori della "privacy europea" ma già allora furono previste misure di salvaguardia atte a limitare l'export indiscriminato dei dati e la conseguente perdita di controllo sui trattamenti effettuati con quegli stessi dati considerati come un potenziale pericolo per il rispetto dei diritti e delle libertà dei cittadini europei. Le aziende americane, pertanto, nella ricezione dei dati europei, dovevano attenersi ai principi individuati nella Direttiva Madre, quali quello di *notifica*, *scelta*, *trasferimento*, *sicurezza*, *integrità dei dati*, *accesso* e *adeguatezza*. Anche per tale ragione la Commissione Europea emanò il *Safe Harbor*[2], uno strumento regolato dai privati, sotto la gestione della Federal Trade Commission (a sua volta monitorata dal Dipartimento del commercio degli Stati Uniti d'America), attraverso il quale le compagnie statunitensi avrebbero potuto certificare il rispetto di detti criteri.

Negli USA: il caso Snowden

Nel 2013 Edward Snowden rese pubblici i programmi di sorveglianza "PRISM" e "Upstream" utilizzati dalla National Security Agency (NSA), l'agenzia di sicurezza nazionale degli USA. Nello specifico:
• *Upstream*, consente di ottenere intercettazioni e dati da tutti gli operatori di Telecom sottostanti all'autorità statunitense, anche senza che si configuri un'ipotesi di reato, attraverso la copia dell'interezza dei dati circolanti nelle dorsali a fibra ottica su cui viaggia il traffico Internet mondiale;
• *PRISM*: le agenzie di intelligence statunitensi possono richiedere ai "big" della net economy (es: Google, Facebook, Microsoft, etc.) di consegnare le comunicazioni (chat,

1 Direttiva 95/46/ CE https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/432175

2 Garante: Autorizzazione al trasferimento verso gli Stati Uniti d´America ('Safe Harbor´) https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/30939

email, dati su cloud, etc.) dei selettori identificati. Alle società è vietato comunicare ai propri utenti che i loro dati sono stati consegnati al governo.
Detti programmi contenevano anche dati relativi a persone estranee alle indagini in corso, definiti dagli stessi analisti della NSA come "irrilevanti" (quali fotografie, e-mail, conversazioni private, etc.). Il Washington Post[3] in un articolo di luglio 2014 citava tra i documenti resi pubblici "*cartelle cliniche inviate da un membro della famiglia a un altro, curriculum di persone in cerca di lavoro e trascrizioni accademiche di studiosi. In una foto, una ragazza in abiti religiosi guarda una telecamera fuori da una moschea.*"
Sotto il profilo giuridico statunitense queste intercettazioni sono perfettamente legali e l'NSA reputa lecita la conservazione dei dati intercettati accidentalmente concernenti persone estranee alle indagini. Gli analisti sono infatti autorizzati ad attuare le procedure di intercettazione dei cittadini stranieri situati all'estero previa semplice loro autodichiarazione fondata sulla ragionevole convinzione che l'obiettivo abbia informazioni di valore su un governo straniero, un'organizzazione terroristica o la diffusione di armi non convenzionali. Per quanto riguarda invece le intercettazioni su cittadini americani e stranieri residenti sul territorio degli Stati Uniti è necessario che la NSA ottenga dal Tribunale speciale di sorveglianza un mandato fondato su una causa "probabile".
Nel dettaglio, le basi giuridiche statunitensi che consentono dette intercettazioni sono principalmente le seguenti:
• "*Executive Order 12333*[4] *- United States intelligence activities*" adottato nel 1981 dal Presidente degli Stati Uniti Ronald Reagan: consente alle agenzie di intelligence statunitensi di poter intercettare, con ampia libertà e discrezionalità, contenuti e trasmissioni di dati, anche al di fuori dei confini nazionali (es: cavi sottomarini).
• *FISA Foreign Intelligence Surveillance Act*[5]: detta le procedure per la sorveglianza fisica ed elettronica, nonché per la raccolta delle informazioni di intelligence straniera (*foreign intelligence information*) messe in atto da potenze straniere (*foreign powers*) negli USA. La modifica dell'art. 702 ha permesso alla NSA di fare un uso più libero di metodi che per trent'anni avevano richiesto la sussistenza di una causa perlomeno "probabile" e il mandato di un giudice.
In estrema sintesi, vale a dire che le agenzie statunitensi possono verificare tutto ciò che viene compiuto in rete, quindi avere accesso anche ai segreti più intimi degli internauti.
In questo senso, nell'articolo del WP citato in precedenza, i programmi PRISM e Upstream avevano "*oltrepassato il limite della proporzionalità*"; Snowden scrive "*la loro continua memorizzazione nei database governativi è sia preoccupante che pericolosa. Chissà come verranno utilizzate queste informazioni in futuro?*"

La sentenza Schrems I

Sulla base delle rivelazioni di Snowden l'allora studente di legge austriaco, Maximilian Schrems, si chiese quali dati Facebook possedesse su di lui e, conseguentemente, a quali informazioni sue personali avesse accesso il governo statunitense. Compì dunque un'analisi sul trattamento dei dati attuato da Facebook Ireland (la filiale europea del social network) e, in particolare, sul loro trasferimento verso i server centrali appartenenti a Facebook Inc. (casa madre) situati nel territorio degli USA, luogo ove risiedono le banche dati del social network.
In esito a detta analisi Schrems presentò nel 2013 al Garante irlandese, competente per il caso, una denuncia finalizzata a vietare i trasferimenti internazionali dei dati asserendo che il diritto e le prassi degli USA non fossero in grado di assicurare una protezione sufficiente contro l'accesso da parte delle pubbliche autorità ai dati trasferiti verso gli Stati Uniti. Tale denuncia venne respinta sostenendo che nel redigere il "*Safe Harbour*" la Commissione aveva constatato che gli USA garantiscono un livello adeguato di protezione.
Schrems ricorse quindi alla Hight Court irlandese che, a sua volta, sollevò il quesito alla Corte di Giustizia EU in quanto questione pregiudiziale, chiedendo se il "*Safe Harbour*" (emanato dalla Commissione Europea) producesse l'effetto giuridico di impedire ad un'autorità nazionale di controllo di effettuare indagini a seguito di una denuncia di inadeguatezza del livello di protezione dei dati personali adottato da un paese terzo e, se necessario, di sospendere il trasferimento di dati contestato.
Con sentenza del 2015 (c.d. «sentenza Schrems I»[6] [7]) la Corte di Giustizia UE stabilì in primis che una decisione della Commissione Europea sull'adeguatezza del livello di protezione dei dati personali adottato da uno stato estero non può sopprimere e neppure ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza della Carta dei Diritti Fondamentali dell'Unione Europea e della "Direttiva Madre". Dichiarò inoltre invalido il Privacy Shield accettando la tesi secondo la quale i controlli svolti da parte degli Stati Uniti in ambito di sicurezza pubblica e nazionale non sono in alcun modo disciplinati nel "*Safe Harbour*" e violano i principi europei di necessità e proporzionalità. La medesima sentenza ritenne inoltre leso il diritto di difesa dei cittadini europei in quanto, nella legislazione americana, la FISC (*Foreign Intelligence Surveillance Court*) non offre ai cittadini dell'Unione, i cui dati personali sono stati trasferiti negli Stati Uniti, la possibilità di promuovere un ricorso giurisdizionale a tutela: le misure atte a salvaguardare il rispetto dei diritti dei cittadini in merito alla attività di sorveglianza posta in essere dai servizi governativi si applicano infatti unicamente ai cittadini americani, nonché ai cittadini stranieri che risiedono legalmente e stabilmente negli Stati Uniti.

L'arrivo del GDPR

Negli anni a seguire la normativa si è evoluta con l'avvento del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. GDPR[8]), che, abrogando la direttiva 95/46/CE, ha subordinato la possibilità

3 *"In NSA-intercepted data, those not targeted far outnumber the foreigners who are" di Barton Gellman, Julie Tate e Ashkan Soltani 05/07/2014 https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html*

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

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

6 *Sentenza della Corte del 06/10/2015, Schrems, C-362/14 https://curia.europa.eu/juris/liste.jsf?td=ALL&language=it&jur=C,T,F&num=C-362/14*

7 *Comunicato stampa n. 117/15 https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117it.pdf*

8 *Regolamento Ue 2016/679 https://www.garanteprivacy.it/il-testo-del-regolamento*

di trasferire i dati all'estero al rispetto di un elenco di condizioni finalizzate a consentire la libera circolazione dei dati quale strumento essenziale per lo sviluppo dell'economia e, in particolare, della società digitale. Parafrasando l'articolo 25 del GDPR, sta bene la "*privacy by default*" ma evitando il "*default by privacy*".
Le condizioni da rispettare per poter esportare i dati all'estero sono indicate prevalentemente all'interno del Capo V del GDPR, ove si compiono richiami anche all'art. 15 in merito ai "Diritto di accesso dell'interessato", all'art. 30.1.d sul censimento dei trasferimenti nel registro dei trattamenti, nonché in numerosi "considerando" tra i quali i c. 101 e c. 102.
Preme osservare preliminarmente che il GDPR all'art. 44 parla di "*trasferimento verso un paese terzo o un'organizzazione internazionale*" intendendo con "paese terzo" la fuoriuscita dei dati dai confini europei ma non dai confini dei singoli stati che compongono l'Unione Europea (in attesa di reciproche decisioni di adeguatezza, sulla base dell'accordo UE-UK[9] quest'ultimo non è considerato paese terzo fino al 30/06/2021). Con "fuoriuscita" si intende l'uscita fisica del dato dal Paese, ad esempio spostando i dati su un server virtuale americano, utilizzando un servizio cloud neozelandese, appoggiandosi ad un servizio di posta elettronica canadese o stipulando un contratto per attività di backoffice amministrativo con una società albanese. Non è poi necessario che i dati vengano "salvati" su un HD fisico estero ma è sufficiente che vengano consultati da "occhi" fisicamente locati all'estero, ad esempio attraverso l'utilizzo di un applicativo web o tramite un accesso di tipo "desktop remoto"[10], seppur adottando tutte le misure di sicurezza del caso. È comune la battuta fra gli addetti ai lavori secondo cui non esiste il "cloud" ma solo i computer di qualcun altro.
Si aggiunga inoltre che anche il trasferimento verso "organizzazioni internazionali" operanti all'interno dei confini EU (quale un'agenzia ONU con una sede fisica a Roma) equivale ad una esportazione dei dati.
Proseguendo nel dettaglio normativo, il trasferimento dei dati all'estero può principalmente avvenire in forza:
• dell'adozione di una decisione di adeguatezza, ovvero "*se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato*" (art. 45 GDPR)[11];
• dell'inserimento di clausole contrattuali tipo (SCC - *Standard Contractual Clauses*) (art. 46, par.2, lett. c e lett. d): la Commissione Europea, o l'autorità di controllo competente previa approvazione della Commissione, può stabilire che determinati strumenti contrattuali consentono di trasferire dati personali verso paesi terzi o organizzazioni internazionali. In pratica, incorporando il testo delle clausole contrattuali in questione in un contratto utilizzato per il trasferimento, l'esportatore dei dati garantisce che questi ultimi saranno trattati conformemente ai principi stabiliti nel Regolamento anche nel Paese terzo o all'interno dell'organizzazione di destinazione. Le clausole tipo di protezione dati non ammettono emendamenti e devono essere sottoscritte dalle parti. Tuttavia, esse possono essere incorporate in un contratto più generale e vi si possono aggiungere clausole ulteriori purché non in conflitto, direttamente o indirettamente, con le clausole tipo così adottate. [12] [13] [14] [15]
Vi sono poi altri casi particolari, di più difficile applicazione e sfruttati nella pratica solo da grosse realtà multinazionali, che si citano per completezza[16]:
• norme vincolanti d'impresa (BCR - *Binding Corporate Rules*) in genere adottate dalle multinazionali. Si tratta di "regolamenti interni" che impongono alle controllate estere di usare i dati secondo la normativa europea. Per poter essere adottate necessitano dell'approvazione del garante dello stato dove ha sede il gruppo. È ottenuto da poche realtà[17] (art. 46, par. 2, lett. b);
• strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a);
• certificazioni (art. 46, par. 2, lett. f) e codici di condotta (art. 46, par. 2, lett. e): purtroppo non esistono ancora le norme di attuazione per poterle sfruttare. Quando esisteranno saranno una vera semplificazione: ad esempio un cloud provider estero potrebbe, se certificato, trattare dati europei senza altra autorizzazione;
• previa autorizzazione del Garante, le clausole contrattuali ad hoc (art. 46, par. 3, lett. a);
• previa autorizzazione del Garante, gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b);
• altri casi, in genere meno diffusi e che per essere "utilizzati" necessitano sicuramente di una solida consulenza legale (es: art. 49 GDPR finalità difensive, eseguire il contratto con il quale l'interessato è parte o il contratto è a favore, interesse pubblico, occasionale per interessi legittimi e cogenti[18]).
Due mesi dopo l'entrata in vigore del GDPR e quale conseguenza della sentenza Schrems I, la Commissione Europea in forza dell'art. 45 del GDPR ha cristallizzato un accordo con gli USA per permettere il libero scambio dei dati, il c.d. *Privacy Shield*[19].
Detto accordo, seppur per alcuni aspetti molto simile al *Safe Harbour*, conteneva strumenti aggiuntivi atti a garantire i diritti

9 The EU-UK Trade and Cooperation Agreement https://ec.europa.eu/info/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en

10 Si segnala giusto come notitia criminis il caso di due persone arrestate nei Paesi Bassi in quanto hanno venduto dati dai sistemi del Ministero della salute: li raccoglievano scattando foto al proprio schermo. https://www.schneier.com/blog/archives/2021/01/dutch-insider-attack-on-covid-19-data.html

11 L'elenco dei paesi per i quali esiste una decisione di adeguatezza è reperibile sul sito del Garante https://www.garanteprivacy.it/temi/trasferimento-dati-estero

12 Trasferimenti da titolare a responsabile - decisione della Commissione UE n. 2010/87/CE del 05/02/2010 https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32010D0087 e relativi provvedimenti del Garante in caso di importatore stabilito in Paese Terzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1728496 e in caso di importatore stabilito in UE https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2191156

13 Trasferimenti da titolare a titolare - decisione della Commissione UE n. 2001/497/CE (I insieme), del 05/06/2021 https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32004D0915 e relativo provvedimento del Garante https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/42156

14 Trasferimenti da titolare a titolare - decisione della Commissione UE n. 2004/915/CE (II insieme), del 27 dicembre 2004 https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32004D0915 e relativo provvedimento del Garante https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1151949

15 Le decisioni nn. 2001/497/CE e 2010/87/UE sono state modificate dalla Commissione con la Decisione di esecuzione (UE) 2016/2297, del 16/12/2016. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016D2297

16 Per dettagli ed approfondimenti si veda il sito del Garante https://www.garanteprivacy.it/temi/trasferimento-dati-estero

17 Al seguente link sono reperibili le autorizzazioni concesse dal garante italiano https://www.garanteprivacy.it/home/ricerca/-/search/tipologia/Bcr

18 In merito si vedano le "Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679" dell'EDPB del 25/05/2018 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf

19 Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016D1250

degli interessati, tra cui si rileva l'introduzione della figura del "*Privacy Shield Ombudsperson*[20]", un "mediatore" o "difensore civico" dedicato a facilitare il trattamento delle richieste da parte di cittadini dell'UE e svizzeri relative alla sicurezza nazionale di accesso ai dati trasmessi dall'Unione Europea o dalla Svizzera agli USA.

Schrems II

Successivamente alla sentenza "Schrems I", Schrems si rivolse nuovamente al Garante irlandese insistendo nella propria richiesta di vietare i trasferimenti effettuati da Facebook verso gli USA sulla base delle SCC e del Privacy Shield, nel frattempo introdotto, adducendo la violazione dell'art. 47 della Carta dei Diritti Fondamentali dell'Unione Europea[21] laddove non prevedono il ricorso al giudice ordinario. Il garante irlandese deferì il caso alla High Court irlandese e la High Court, a sua volta, lo deferì alla Corte di Giustizia UE nel 2018 per una pronuncia pregiudiziale. Con sentenza del luglio del 2020 (c.d. sentenza "Schrems II"[22] [23]), la Corte dichiarò invalido *il Privacy Shield*. Secondo la Corte, infatti, le limitazioni della protezione dei dati personali che risultano dalla normativa interna degli USA in materia di accesso e di utilizzo, da parte delle autorità statunitensi, dei dati personali trasferiti dall'Unione verso gli USA non sono inquadrate in modo da rispondere a requisiti sostanzialmente equivalenti a quelli richiesti, nel diritto dell'Unione, dal principio di proporzionalità, giacché i programmi di sorveglianza fondati sulla suddetta normativa non si limitano a quanto strettamente necessario.
Quanto al meccanismo di mediazione, venne valutato non in grado di fornire garanzie sostanzialmente equivalenti a quelle richieste nel diritto dell'Unione, tali da assicurare tanto l'indipendenza del Mediatore quanto l'esistenza di norme che gli consentano di adottare decisioni vincolanti nei confronti dei servizi di intelligence statunitensi.
Nella stessa sentenza venne confermata invece la validità delle SCC prendendo atto che esse, per il loro carattere contrattuale, non vincolano le autorità del Paese terzo e stabilendo così un obbligo per l'esportatore dei dati e il destinatario del trasferimento di verificare, preliminarmente, che tale livello di protezione venga rispettato nel Paese terzo considerato. Paradossalmente, in tal modo, per l'esportazione verso gli USA vengono richieste salvaguardie superiori a quelle presenti all'interno dei confini europei, ad esempio quando l'attività di sorveglianza ricade nelle competenze extra trattati UE di uno stato membro dell'UE (es: intercettazione e controlli preventivi ex art. 226 disp.att.c.p.p.).
Per la Corte UE pertanto l'esportatore deve valutare se il paese terzo è un luogo adeguato ove trasferire i dati o se le SCC devono essere integrate con clausole in grado di annullare il rischio specifico del paese. Qualche giorno dopo la sentenza il Comitato Europeo per la protezione dei dati (EDPB - *European Data Protection Board*) ha pubblicato delle sue FAQ[24] sulla sentenza Schrems II, chiarendo che non è previsto un periodo di tolleranza e che "*la possibilità di trasferire dati personali sulla base delle clausole contrattuali tipo dipenderà dall'esito della valutazione condotta, tenendo conto delle circostanze dei trasferimenti e delle misure supplementari eventualmente attuabili. Le misure supplementari unitamente alle clausole contrattuali tipo, previa analisi caso per caso delle circostanze del trasferimento, dovrebbero assicurare che la normativa statunitense non interferisca con il livello di protezione adeguato dalle stesse garantito. Qualora si giunga alla conclusione che, tenuto conto delle circostanze del trasferimento e delle possibili misure supplementari, non sarebbero assicurate garanzie adeguate, vi è l'obbligo di sospendere o cessare il trasferimento dei dati personali.*"
Come anche confermato dalle succitate FAQ potrebbero essere utilizzati in casi specifici le altre deroghe ex art. 49 GDPR (ad esempio: esecuzione di un contratto), ma si vedono di difficile attuazione in caso di rapporti B2B dove i dati oggetto di esportazione sono in genere dati di interessati non parte del contratto specifico.
Nel novembre del 2020 l'EDPB ha emanato delle sue raccomandazioni 01/2020[25] relative alle misure supplementari adottabili, ma a parte la non-soluzione della cifratura e pseudonimizzazione dei dati nella pratica non si vedono strumenti utili per garantire l'esportazione sicura dei dati verso gli USA.
In pari data, con le Raccomandazioni 02/2020 [26] l'EDPB ha inoltre fornito gli elementi utili a valutare se le misure di sorveglianza che consentono l'accesso ai dati personali da parte delle autorità pubbliche di un paese terzo, possano configurare un'ingerenza giustificabile o meno. Va da sé che se un titolare del trattamento prima di esportare i dati deve effettuare un Audit sul livello di intelligence di un paese, preferirà senz'altro un altro fornitore.
Infine, il 15/01/2021 il Comitato Europeo per la protezione dei dati e il Garante Europeo per la protezione dei dati (GEPD) hanno adottato pareri congiunti su nuove clausole contrattuali tipo. Si tratta di un parere sulle clausole contrattuali tipo per i contratti tra titolari e responsabili del trattamento e di un parere sulle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi.
Al momento i documenti sono soggetti ai necessari controlli giuridici, linguistici e di formattazione e saranno resi disponibili sul sito web del EDPB una volta completati tali controlli. [27]

Le conseguenze

Come diretta conseguenza della sentenza Schrems II, la Commissione irlandese per la protezione della privacy ha avviato un'indagine specifica e inviato a Facebook, che a Dublino ha il suo quartier generale europeo, un ordine preliminare per sospendere i trasferimenti di dati negli USA.

20 Privacy Shield Ombudsperson https://www.state.gov/privacy-shield-ombudsperson/

21 https://fra.europa.eu/it/eu-charter/article/47-diritto-un-ricorso-effettivo-e-un-giudice-imparziale

22 Comunicato Stampa della Corte di Giustizia relativo alla sentenza Schrems II https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091it.pdf

23 Sentenza Schrems II https://curia.europa.eu/juris/documents.jsf?num=C-311/18

24 Domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems del 23/10/2020 https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_it.pdf

25 EDPB: "Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE" del10/11/2020 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_it.pdf

26 Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza Adottate il 10 novembre 2020 https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_it.pdf

27 Comunicato stampa EDPB https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_it

L'importanza di questa azione è data dal fatto che per ragioni fiscali molti dei "colossi del web" statunitensi hanno sede proprio in Irlanda. Secondo il Wall Street Journal[28], che per primo ha dato la notizia, per rispettare l'ordine Facebook dovrebbe rivedere pesantemente l'architettura IT dei suoi servizi, con ovviamente pesanti costi di migrazione. Nel suo ricorso Facebook ha chiesto all'UE di adottare sulla questione un *"approccio pragmatico e proporzionato fin quando non sarà raggiunta una soluzione di lungo termine"*, cioè fino a quando non sarà adottato un nuovo "*Privacy Shield*". Al momento la soluzione a questo problema pare ancora lontana, tanto che la Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento Europeo (Libe) ha presentato una mozione contro l'autorità irlandese esprimendo "*preoccupazione*" per i ritardi e chiedendo alla Commissione Europea di avviare una procedura di infrazione contro l'Irlanda per *"non aver applicato correttamente il Gdpr"*[29]. Ad un osservatore esterno l'unico aspetto chiaro, in questo momento, è che vi siano enormi interessi economici in gioco. Un recente ma esplosivo fattore di complicazione è arrivato poi nel marzo del 2021. L'Autorità per la Protezione dei Dati bavarese (BayLDA - *Bayerisches Landesamt für Datenschutzaufsicht*) con suo provvedimento[30] ha ritenuto inammissibile l'uso dello strumento di newsletter *Mailchimp*, uno dei principali player di mercato, diffusissimo anche in Italia, da parte di una società tedesca ai sensi della legge sulla protezione dei dati perché oltre alle SCC (correttamente adottate), non erano state adottate anche le "misure aggiuntive" ai sensi della sentenza "Schrems II". Nel suo provvedimento BayLDA le ha definite necessarie in quanto *Mailchimp*, "fornitore di servizi di comunicazione elettronica", è soggetto alla legge di sorveglianza degli USA. Nessuna sanzione ma un punto fermo, che farà forse da precedente per altre autorità europee: l'utilizzo di uno strumento come *Mailchimp* potrebbe essere consentito solo e soltanto adottando misure aggiuntive in grado di prevenire azioni di sorveglianza da parte del governo statunitense. Forse sulla scia della decisione del BayLDA, l'autorità portoghese per la protezione dei dati (CNPD) con sua decisione del 27/04/2021[31] ha ordinato all'INE (il locale Istituto nazionale di statistica) di sospendere l'invio di dati personali relativi al censimento 2021 verso gli Stati Uniti. INE ha esternalizzato a Cloudflare, Inc. con sede in California lo sviluppo del questionario di censimento, attraverso un accordo sul trattamento dei dati che prevede il trasferimento di dati personali negli Stati Uniti, paese reputato non sicuro per le sue politiche di sorveglianza. Il CNPD ha ritenuto che il trasferimento dei dati agli Stati Uniti o a qualsiasi altro terzo paese senza protezione adeguata debba essere sospeso.

Un possibile ausilio: la "Convenzione 108+"

La "*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*"[32] conclusa a Strasburgo il 28 gennaio del 1981 nell'ambito del Consiglio d'Europa, detta anche "Convenzione 108", rappresenta il primo strumento giuridico a livello europeo sulla protezione dei dati personali, nonché l'unico trattato internazionale in questa materia a essere giuridicamente vincolante. Di notevole rilevanza è il fatto che

28 Ireland to Order Facebook to Stop Sending User Data to U.S. di Sam Schechner and Emily Glazer, 09/11/2020 https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980?mod=tech_lead_pos2

29 Irish data regulator sparks row with EU colleagues on Facebook oversight di Derek Scally, 17/03/2021 https://www.irishtimes.com/business/economy/irish-data-regulator-sparks-row-with-eu-colleagues-on-facebook-oversight-1.4513065

30 BayLDA - LDA-1085.1-12159/20-IDV https://gdprhub.eu/index.php?title=BayLDA_-_LDA-1085.1-12159/20-IDV

31 Deliberação 533/2021 Comissão Nacional de Proteção de Dados Ordem de suspensão de transferências internacionais dos dados pessoais do Censos 2021 https://www.cnpd.pt/decisoes/deliberacoes/

32 Testo originale della Convenzione 108 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078c45

la Convenzione 108 sia aperta a stati europei ed a stati non membri del Consiglio D'Europa, consentendo quindi la creazione di un framework normativo sulla protezione dei dati personali diffuso. Sono firmatari della Convenzione 108 infatti paesi come il Messico, l'Urugay e la Tunisia. [33]
Il 18 maggio del 2018 il Consiglio d'Europa ha adottato un protocollo di modifica[34] del testo della Convenzione 108 (c.d. Convenzione 108+[35]), al fine di rafforzare l'attuazione della Convenzione 108 modernizzandola .. Mutuandoli dal GDPR, il protocollo introduce nella Convenzione concetti quali la liceità del trattamento, il data breach, la minimizzazione dei dati, i principi di trasparenza e privacy by design, maggiori tutele in merito all'accesso ai dati e alla protezione delle categorie speciali di dati (i c.d. "dati sensibili"). Come per il GDPR non riguarda i trattamenti operati da persone fisiche all'interno della sfera domestica ma tutti gli altri tipi di trattamenti di dati personali, compresi quelli inerenti alla difesa e la sicurezza nazionale. Per tale ragione la sua adozione da parte di un Paese extra UE può essere considerato un elemento a favore nella valutazione dell'adeguatezza del regime di protezione dei dati[36]. Come espresso dallo stesso Garante per la Protezione dei Dati Personali: *"La Convenzione 108 svolge un ruolo fondamentale nel diffondere il 'modello europeo di protezione dei dati' a livello mondiale, essendo spesso utilizzata come fonte di ispirazione dai Paesi che intendono adottare nuove normative in materia di rispetto della vita privata o armonizzare quelle già esistenti con gli standard internazionali"* .
Il Protocollo di emendamento è stato firmato dall'Italia nel 2019[37] ed è stato ratificato nel maggio del 2021[38].

33 Elenco dei paesi che hanno ratificato la Convenzione 108 https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/108/signatures

34 Council of Europe Modernisation of Convention 108 https://www.coe.int/en/web/data-protection/convention108/modernised

35 Testo della Convenzione 108+ https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

36 Elenco dei paesi che hanno ratificato la Convenzione 108+ https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

37 Council of Europe, 05/03/2019, Italy is the 26th State to sign Convention 108 + https://www.coe.int/en/web/data-protection/-/italy-is-the-26th-state-to-sign-convention-108-

38 L. n. 60 del 22/04/2021 "Ratifica ed esecuzione del Protocollo di modifica alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, fatto a Strasburgo il 10 ottobre 2018" https://www.gazzettaufficiale.it/eli/id/2021/05/10/21G00068/sg

Ca va sans dire gli Stati Uniti non sono tra i firmatari della Convenzione 108.

Conclusioni

In questa fase storica purtroppo l'utilizzo di fornitori che trasferiscono i dati all'estero e, in particolare, negli USA presenta le criticità evidenziate in precedenza nell'analisi del caso "Mailchimp". L'impegno e le risorse che occorrerebbe mettere in campo per gestire in modo corretto l'esportazione dei dati sono complessi e molto probabilmente si rileverebbero strumenti non completamente risolutivi. Viene da chiedersi infatti come un accordo tra privati che, in quanto tale, non ha il potere di modificare la normativa in materia di sicurezza nazionale di uno Stato sovrano, potrebbe superare il giudizio lapidario espresso dalla Corte UE sulla inadeguatezza degli USA nel garantire ai cittadini europei l'effettiva protezione dei loro dati personali.
Probabilmente andrebbe concordato tra l'Unione Europea e gli USA un nuovo "*Privacy Shield*", previo cambiamento delle leggi statunitensi in materia di sicurezza o, in alternativa, della normativa europea. Non si vedono al momento soluzioni adottabili per aziende che non siano dotate di un elevato "budget per le sanzioni". L'impatto integralista della sentenza Shrems II, se applicata alla lettera, potrebbe essere quello di uno "spegnimento" dei servizi cloud offerti dalle aziende statunitensi sul mercato europeo, con conseguente danno economico su entrambi i fronti. Salvo importanti realtà aziendali, ci si chiede come una comune azienda europea potrebbe mai riuscire ad adottare misure tecnologiche sufficienti a contrastare le attività di intelligence di uno strato sovrano, o come dovrebbe comportarsi un DPO o un Consulente Privacy di fronte alle naturali perplessità di un cliente che sta adottando Mailchimp o un qualunque altro fornitore cloud statunitense. Ma, citando Michael Ende, "*questa è un'altra storia*".

Data breach: le Linee guida dell'EDPB e le "istruzioni" del Garante privacy

di Elisa Chizzola e Anna Maria Carbone

L'*European data protection board* il 14 gennaio 2021 ha adottato nuove Linee Guida in tema di *data breach*, che sono state oggetto di consultazione pubblica fino al 2 marzo scorso.
Il nuovo documento integra le Linee guida dell'ottobre 2017 (WP 250) attraverso una casistica dettagliata di specifici *data breaches* segnalati dagli Stati membri dell'Ue nei primi due anni e mezzo di applicazione del GDPR.
Le indicazioni del *Board* supportano i *controller* nella gestione delle violazioni dei dati, attraverso un *focus* sui profili di analisi, gestione e valutazione del rischio, aspetto fondamentale nell'ambito di una *governance compliance privacy* delle organizzazioni.
Le casistiche sono divise in sei macro-categorie: attacchi informatici *ransomware*, attacchi di esfiltrazione di dati, fonti di rischio umano interno, dispositivi smarriti o rubati e documenti su carta, errori nell'invio della posta e casi di *social engineering* (come il furto d'identità).
Il taglio del nuovo documento emesso dall'EDPB è molto interessante ed operativo: per ogni singolo caso, prevede misure preventive e valutazione del rischio, nonché misure di mitigazione, sottolineando di volta in volta gli obblighi in capo al titolare.
Nei ragionamenti del *Board* è sempre sotteso un concetto chiave. Le violazioni dei dati sono criticità in sé e per sé per l'organizzazione, ma sono anche sintomo di un regime di sicurezza dei dati vulnerabile e spesso obsoleto, rivelando punti deboli del sistema che il titolare del trattamento deve affrontare, gestire e risolvere. In generale, anche in una logica di *privacy by design and by default*, è sempre meglio prevenire le violazioni dei dati preparandosi in anticipo con misure e sistemi di sicurezza adeguati ed appropriati, poiché alcune conseguenze dannose sono per natura irreversibili.
Sul versante interno nazionale, il Garante per la protezione dei dati italiano ha agevolato l'applicazione della normativa sul *data breach*, fornendo ai titolari un modello per la notifica ex art. 33 GDPR e un utile strumento di autovalutazione (*self-assessment*) che guida l'operatore nella "qualificazione" della violazione. In applicazione del Provvedimento del 27 maggio 2021 del Garante per la protezione dei dati personali, dal 1° luglio 2021 per la notifica dei *data breach* è obbligatorio utilizzare l'apposita procedura telematica resa disponibile nel portale dei servizi online dell'Autorità.
Inoltre è interessante evidenziare che è stato appena pubblicato in Gazzetta Ufficiale (n. 138 dell'11 giugno 2021) il D.P.C.M. 14 aprile 2021, n. 81, recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza".
Tale decreto prevede norme specifiche in materia di notifica degli incidenti aventi

impatto su beni ICT (*information and communication technology*): in particolare, dal 1° gennaio 2022, i soggetti inclusi nel perimetro cd. "cibernetico", al verificarsi di uno degli incidenti avente impatto su un bene ICT (*Computer security incident response team* istituito presso il DIS - Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio dei ministri) di rispettiva pertinenza individuati nelle tabelle di cui all'allegato A del decreto, procedono alla notifica al CSIRT (*Computer security incident response team* istituito presso il DIS) italiano secondo le specifiche modalità espressamente previste dal Regolamento stesso.

***Personal data breach*: premessa**

La violazione dei dati personali (*personal data breach* o, più comunemente detto, *data breach*) rappresenta un particolare tipo di incidente di sicurezza che, causando perdita di riservatezza, integrità o disponibilità dei dati personali, implica che il titolare del trattamento non sia più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali.
La disciplina normativa contenente norme sostanziali, obblighi e adempimenti, sussistenti in capo ai titolari del trattamento, nel caso in cui si verifichi una violazione di dati personali la ritroviamo nel Regolamento europeo sul trattamento e sulla protezione dei dati n. 2016/679 (*General Data Protection Regulation* – nel proseguo "GDPR"): in particolare nell'art. 4, punto 12 (che fornisce la definizione di "*Violazione dei dati personali*"), nell'art. 33 ("*Notifica di una violazione dei dati personali all'autorità di controllo*") e nell'art. 34 ("*Comunicazione di una violazione dei dati personali all'interessato*").
Il GDPR introduce l'obbligo di notificare una violazione dei dati personali all'autorità di controllo nazionale competente (in Italia, al Garante per la protezione dei dati personali) oppure, in caso di violazione transfrontaliera, all'autorità capofila, se si verifica la condizione specifica prevista dall'art. 33 sopra citato, vale a dire se è il titolare del trattamento ritiene "non improbabile" (quindi, probabile) che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Pertanto, il ragionamento che il titolare deve seguire per decidere se la violazione che, di volta in volta si verifica, richieda o meno l'obbligatorietà della notifica al Garante privacy poggia sull'analisi e la valutazione del rischio collegato alla compressione dei diritti e delle libertà dei soggetti interessati, i cui dati sono oggetto della violazione. Se tale rischio si qualifica come "elevato" vanno anche avvisati gli interessati ex art. 34 GDPR.
In generale, l'operazione di "valutazione/analisi del rischio" rappresenta un concetto chiave nella nuova impostazione del GDPR presente sostanzialmente in tutte le fasi in cui si esplica la gestione dei dati personali. La valutazione del rischio, inoltre, costituisce uno dei pilastri fondamentali del principio di privacy by design e by default e del processo di *accountability* in capo al titolare.
Se la valutazione del rischio, concetto di estrazione organizzativo-aziendale, caratterizza tutta la gestione dei dati personali

fin dall'inizio della progettazione del trattamento comprendendo anche l'eventuale fase del *data breach*, allo stesso modo occorre sottolineare come tale operazione costituisca una *practise* complessa, che coinvolge ambiti "trasversali" (*in primis*, conoscenze giuridico-legali, aziendalistiche e sempre più spesso legate all'*Information technology*) e strettamente legata alla fattispecie concreta.

Linee Guida EDPB e provvedimenti dell'Autorità Garante per la Protezione dei dati personali

Per orientare titolari e responsabili del trattamento, già nell'ottobre 2017, il Gruppo di lavoro Articolo 29 per la protezione dei dati emanava le "*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (EU) 2016/679*" (WP 250rev.01 – nel proseguo anche "WP 250"), interessanti criteri e canoni interpretativi delle norme in tema di *data breach*.
Tali Linee guida si sono concentrate in particolare a chiarire gli aspetti generali in materia di *breach*, partendo dalla definizione di violazione dei dati personali (ex art. 4, punto 12, GDPR), anche attraverso la classificazione delle fattispecie in base ai tre principi della sicurezza delle informazioni (violazione della riservatezza/violazione dell'integrità/violazione della disponibilità), per poi passare al commento specifico degli artt. 33 e 34, GDPR. Con riferimento alla nozione di "rischio" molto interessante è la parte riguardante la valutazione dell'esistenza di un rischio o di un rischio elevato (Parte IV).
Occorre tenere presente che tali Linee guida sono state emanate qualche mese prima dell'applicazione del GDPR agli Stati membri dell'Ue, pertanto "fisiologicamente" non potevano poggiare su concrete ipotesi di notifica di *data breach* secondo la nuova impostazione privacy europea.
Pertanto, il Comitato europeo per la protezione dei dati (EDPB) recentemente, il 14 gennaio scorso, ha adottato nuove Linee guida in tema (n. 1/2021), vertenti su esempi riguardanti la notifica di violazione dei dati, che sono state oggetto di consultazione pubblica fino al 2 marzo scorso. Il *Board* ha sostanzialmente ritenuto opportuno emanare tali nuove indicazioni per "calare" la disciplina normativa del *data breach* nell'esperienza maturata nei primi due anni e mezzo di applicazione del GDPR.
Nell'introduzione alle Linee guida l'*European Data Protection Board* lo dice espressamente: il WP 250 non ha potuto, dato il loro taglio teorico-normativo e data la tempistica di emanazione, affrontare tutte le questioni pratiche in modo sufficientemente dettagliato. Di conseguenza, è sorta la necessità di realizzare una sorta di "guida pratica", basata sulle reali esperienze acquisite dalle Autorità di controllo europee.
Il nuovo documento, quindi, integra le Linee guida WP 250 supportando i titolari e i responsabili del trattamento nelle decisioni necessarie al fine di gestire le violazioni dei dati, con particolare riferimento ai fattori da considerare nell'ambito della valutazione del rischio. Si evidenzia, a quest'ultimo proposito, il focus sui profili di analisi, gestione e valutazione del rischio, aspetto fondamentale di cui si è accennato in premessa, nell'ambito di una *governance compliance privacy* delle organizzazioni.
Dal punto di vista del nostro ordinamento interno, il Garante per la protezione dei dati nel proprio sito istituzionale dedica appositamente una sezione al *data breach* dove è presente ad un'interessante pagina informativa di sintesi dell'istituto.
Come innanzi rilevato, con il Provvedimento del 27 maggio 2021 n. 209, il Garante ha adottato un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità pubblicato all'indirizzo https://servizi.gpdp.it/, attraverso la quale, i titolari del trattamento forniscono le informazioni richieste dall'art. 33 citato, a decorrere dal 1° luglio 2021. Da tale data la nuova procedura costituisce l'unica modalità disponibile per la trasmissione della notifica del *data breach* (anche per eventuali notifiche di *data breach* integrative di notifiche preliminari effettuate con le previgenti modalità).
L'Autorità di controllo, inoltre, aveva già messo a disposizione uno strumento di autovalutazione (*self-assessment*) che guida

l'operatore alla "qualificazione" della violazione. Con tale sistema di *self-assessment*, attraverso alcuni semplici quesiti, il titolare del trattamento viene "guidato" nell'assolvimento degli obblighi in materia di notifica ex art. 33, GDPR e di eventuale comunicazione agli interessati ex art. 34, GDPR. Oppure, in alcuni casi, se la violazione non implica l'obbligatorietà della notifica, al titolare del trattamento viene ricordato di documentare la violazione, registrazione comunque obbligatoria ai sensi dell'art. 33, par. 5, GDPR (usualmente nel cd. registro dei *data breach*).
Come è evidente, pertanto, sul versante interno nazionale, anche il Garante italiano ha cercato di fornire agli operatori strumenti utili e pratici per agevolare l'applicazione della normativa sul *data breach*.
Per completezza occorre dire che nella stessa sezione dedicata alla violazione dei dati presente nel sito del Garante privacy italiano, è presente un link che permette di conoscere i contenuti di singoli provvedimenti con cui l'Autorità di controllo ha gestito i vari *data breaches* segnalati, oltre a interventi e interviste in tema.

Definizione ex GDPR di *data breach* e classificazione delle violazioni dei dati personali

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla, pertanto appare cruciale ricordare la nozione di *data breach* fornita direttamente dal GDPR. L'art. 4, punto 12, GDPR definisce la "violazione dei dati personali" come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".
Così intesa, una violazione è un tipo di incidente di sicurezza che verte su dati personali.
Le violazioni possono essere classificate in base ai seguenti tre principi della sicurezza delle informazioni:
• "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
• "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
• "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.
Tale classificazione era già stata prevista nel Parere n. 3/2014 del 25 marzo 2014 (WP 213) del Gruppo di lavoro Articolo 29 sulla notifica delle violazioni dei dati personali, e poi è stata ripresa sia dalle Linee guida di lavoro Articolo 29 dell'ottobre 2017 (WP 250) sia dalle ultime *Guidelines* EDPB di inizio 2021.

Valutazione dell'esistenza di un rischio o di un rischio elevato

Come noto, tutti i titolari di trattamento a partire dal 25 maggio 2018 sono tenuti a notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "*senza ingiustificato ritardo*", se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (art. 33, GDPR). Se il rischio è elevato occorre comunicare il *breach* anche agli interessati coinvolti.
In sintesi si può dire che l'esistenza del rischio per i diritti e le libertà degli interessati è il fattore che fa scattare l'obbligo di notifica.
Come evidenziato in premessa, il ragionamento giuridico in capo al titolare del trattamento - che di fronte ad una violazione si trova a dover decidere se effettuare o meno la notifica all'Autorità di controllo - verte principalmente sulla valutazione del rischio per i diritti e le libertà degli interessati coinvolti nel *breach*.
Le Linee guida dell'ottobre 2017 (WP 250) forniscono delle interessanti considerazioni vertenti appunto sulla valutazione dell'esistenza di un rischio o di un rischio elevato, sottolineando che, non appena il titolare del trattamento viene a conoscenza di una violazione, è fondamentale che non si limiti a contenere l'incidente, ma valuti anche il rischio che potrebbe derivarne.
Questo per due motivi: innanzitutto conoscere la probabilità e la potenziale gravità dell'impatto sulle persone fisiche aiuterà il titolare del trattamento ad adottare misure efficaci per contenere e risolvere la violazione. In secondo luogo, ciò lo aiuterà a stabilire se è necessaria la notifica all'Autorità di controllo e, se necessario, alle persone fisiche interessate.
Con riferimento al "rischio", aiutano a delineare i contorni di tale concetto il Considerando n. 75, 76 e 85, GDPR. In particolare, il rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati. Esempi di tali danni sono "*la discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata*" (Considerando n. 85).
I Considerando nn. 75 e 76 del GDPR suggeriscono che, di norma, nella valutazione del rischio (che dovrebbe essere di natura oggettiva) si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati.
Il WP 250 sottolinea che la valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati (art. 35, GDPR).
La D.P.I.A., infatti, considera tanto i rischi del trattamento dei dati svolto come pianificato, quanto quelli in caso di violazione. Nel considerare una potenziale violazione, la D.P.I.A. esamina in termini generali la probabilità che la violazione stessa si verifichi e il danno all'interessato che potrebbe derivarne, in quanto si tratta di una valutazione di un evento ipotetico. Invece, nel caso di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione si concentra esclusivamente sul rischio risultante dall'impatto di tale violazione sulle persone fisiche.
Nel valutare il rischio per le persone fisiche derivante da una violazione, il titolare del trattamento dovrebbe considerare le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi. Chiaramente, se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore è anche il rischio.
In caso di dubbio, il titolare del trattamento dovrebbe agire in via prudenziale effettuando la notifica.
Si ricorda che l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha elaborato raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione, che possono essere utili per i titolari del trattamento e i responsabili del trattamento nella progettazione del loro piano di risposta per la gestione delle violazioni ("*Recommendations for a methodology of the assessment of severity of*

personal data breaches").
Il WP 250 specifica che la valutazione del rischio deve essere effettuata esaminando le caratteristiche specifiche del caso concreto e tenendo in considerazione i seguenti fattori:
• tipo di violazione;
• natura, carattere sensibile e volume dei dati personali;
• facilità di identificazione delle persone fisiche;
• gravità delle conseguenze per le persone fisiche;
• caratteristiche particolari dell'interessato;
• caratteristiche particolari del titolare del trattamento di dati;
• numero di persone interessate;
• aspetti generali.

Casistica ed esemplificazioni efficaci di *data breaches*

In relazione a fattispecie concrete ed esemplificazioni dei *breaches*, già l'allegato B al WP 250 ha fornito alcuni esempi utili dei diversi tipi di violazioni che comportano rischi o rischi elevati per le persone fisiche.
Ma, come anticipato in premessa, sono le nuove Linee guida dell'EDPB adottate il 14 gennaio scorso che si dedicano specificatamente e quasi esclusivamente ad analizzare la casistica relativa ai *data breaches* che, in questi due anni e mezzo dall'applicazione del GDPR agli Stati membri, si è presentata alle diverse Autorità di controllo europee.
Paradigmatico è proprio il titolo delle nuove indicazioni che fa riferimento espressamente agli "*esempi riguardanti la notifica di violazione dei dati*".
Prima di analizzare i vari casi concreti, tuttavia, il *Board* compie non solo una breve sintesi dei concetti basilari di applicazione della normativa in tema di violazione dei dati, ma esprime un concetto importante.
Sottolinea che le violazioni dei dati sono criticità in sé e per sé, ma sono anche sintomo di un regime di sicurezza dei dati vulnerabile e spesso obsoleto. In altre parole, le violazioni indicano punti deboli del sistema che il titolare del trattamento deve affrontare, gestire e risolvere in una logica di *compliance*.
In generale, è sempre meglio prevenire, anche nella logica del principio di *privacy by default e by design*, le violazioni dei dati preparandosi in anticipo, poiché alcune conseguenze sono per natura irreversibili.
L'EDPB raccomanda al *controller*, prima di valutare definitivamente il rischio derivante da una violazione causata da qualche forma di attacco, di identificare la causa principale del problema, al fine di identificare se eventuali vulnerabilità che hanno dato origine all'incidente sono ancora presenti e sono ancora potenzialmente pericolosi.
Passando alla casistica, il *Board* evidenzia che i casi presentati nel nuovo documento sono mere esemplificazioni, che fanno riferimento ad ipotesi "fittizie". Tale casistica è, tuttavia, particolarmente significativa in quanto si basa su casi tipici derivanti dall'esperienza collettiva delle varie Autorità di controllo europee nascenti da reali notifiche di violazione dei dati effettuate dagli Stati membri.

Le casistiche sono divise in 6 macro-categorie che potremmo definire "tematiche", le quali poi si strutturano in diverse tipologie di eventi.
Le macro-categorie fanno riferimento ai seguenti ambiti:
• Attacchi informatici *ransomware*;
• Attacchi di esfiltrazione di dati;
• Fonti di rischio umano interno;
• Dispositivi smarriti o rubati e documenti su carta;
• Errori nell'invio della posta;
• Altri casi (ingegneria sociale).
Queste 6 macro-aree sono, a loro volta, strutturate in singoli casi specifici (in totale i casi sono 18).
L'EDPB per ogni singolo caso concreto, prevede le misure preventive e di valutazione del rischio, nonché suggerisce le misure di mitigazione e gli obblighi in capo al titolare.
Mentre, per ogni macro-area indica specifiche misure organizzative e tecniche per prevenire / mitigare il relativo rischio.

1. Attacchi informatici *ransomware*
L'*European data protection baord* osserva che si sono rivelati molto frequenti gli attacchi informatici *ransomware* subìti dai titolari del trattamento.
L'infezione da *ransomware* si verifica quando un *software* dannoso cifra i dati personali del titolare del trattamento e successivamente l'aggressore chiede al *controller* un riscatto in cambio del codice di decrittazione.
Questo tipo di attacco può essere generalmente classificato come una violazione della disponibilità, ma spesso potrebbe verificarsi anche una violazione della riservatezza.
Il *Board* ne tipizza 4 casi:
Caso 1: *Ransomware* con backup corretto e senza esfiltrazione
Caso 2: *Ransomware* senza backup adeguato
Caso 3: *Ransomware* con backup e senza esfiltrazione in un ospedale
Caso 4: *Ransomware* senza backup e con esfiltrazione
Usualmente, il verificarsi di un attacco *ransomware* è sintomo di una o più vulnerabilità nel sistema del *controller*, anche nei casi di *ransomware* in cui i dati personali sono stati crittografati, ma non sono stati esfiltrati.
A prescindere dall'esito e dalle conseguenze dell'attacco, appare importante effettuare una valutazione complessiva del sistema di sicurezza dei dati, con particolare riferimento alla sicurezza informatica.
Le debolezze e le falle del sistema devono essere documentate e affrontate nel più breve tempo possibile.

2. Attacchi di esfiltrazione di dati

Anche gli attacchi informatici finalizzati al furto di dati attraverso Internet sulla base dell'esperienza raccolta dalle Autorità di controllo europee sono fenomeni diffusi.
Tali attacchi hanno in comune con il *ransomware* il fatto che il rischio deriva dall'azione di una terza parte non autorizzata che sfrutta le vulnerabilità nei servizi offerti dal titolare del trattamento su Internet, ma si distinguono per la finalità in quanto mirano a sottrarre informazioni e/o copiare dati per fini dannosi (per esempio, utilizzo di carte di credito altrui).
Tali attacchi si sostanziano principalmente in violazioni della riservatezza, ma possono anche riguardare l'integrità dei dati.
Vengono esaminati 3 casi riguardanti tale argomento:
Caso 5: Esfiltrazione di dati sulla domanda di lavoro da un sito web
Caso 6: Esfiltrazione di password con *hash* da un sito web
Caso 7: Attacco di *credential stuffing* a un sito web bancario

3. Fonte di rischio umano interno

L'errore umano, che può essere volontario od involontario, è un rischio di fonte interna e fisiologico nelle organizzazioni.
Per i titolari del trattamento risulta difficile identificare le vulnerabilità e adottare misure per evitarle completamente.

Il *Board* analizza 2 casi comuni di errori umani e comportamenti commessi da dipendenti infedeli:
Caso 8: Esfiltrazione di dati aziendali da parte di un ex dipendente
Caso 9: Trasmissione accidentale di dati a una terza parte fidata

4. Dispositivi smarriti o rubati e documenti su carta

Lo smarrimento o il furto di dispositivi portatili rappresenta un'altra macro-area di rischio analizzata dall'EDPB.
In queste ipotesi, il titolare del trattamento deve prendere in considerazione le circostanze dell'operazione di trattamento, come la tipologia di dati memorizzati sul dispositivo, le risorse di supporto e le misure adottate prima della violazione per garantire un livello appropriato ed adeguato di sicurezza.
Tutti questi elementi influenzano i potenziali impatti della violazione dei dati.
In questi casi, purtroppo, la valutazione del rischio potrebbe presentare criticità, in quanto il dispositivo che è stato smarrito o rubato non è più a disposizione.
In questo ambito vengono prese in considerazione 3 ipotesi specifiche (le prime due ipotesi si riferiscono a dispositivi elettronici/informatici, mentre l'ultimo caso riguarda la perdita di un supporto cartaceo):
Caso 10: Materiale rubato che memorizza dati personali crittografati
Caso 11: Materiale rubato contenente dati personali non crittografati
Caso 12: File cartacei rubati con dati sensibili

5. Errori nell'invio della posta

I casi appartenenti alla macro-categoria degli "errori nell'invio di posta" fanno riferimento ad una fonte di rischio interna in quanto nascono da un errore umano.
Queste tipologie di violazioni si distinguono dall'ipotesi descritte al punto 3 (Fonte di rischio umano interno) poiché non si caratterizzano da un'azione dolosa, ma frutto della disattenzione.
In queste ipotesi il titolare ha pochi strumenti per risolvere la violazione, quindi in tale contesto la prevenzione è ancora più importante rispetto ad altri tipi di violazione esaminati.
In merito a questa tematica, vengono tipizzati 4 casi concreti:
Caso 13: Errore di posta ordinaria
Caso 14: Dati personali sensibili inviati per posta per errore
Caso 15: Dati personali inviati per posta per errore
Caso 16: Errore di posta ordinaria

6. Altri casi (ingegneria sociale)

Infine, il *Board* esamina altre due tipologie di violazioni che rientrano nelle ipotesi di *social engineering*, tecnica che ha ad oggetto lo studio del comportamento individuale, nel campo della sicurezza informatica, di una persona al fine di carpire informazioni utili.
Anche le violazioni appartenenti a tale area sono sempre più diffuse e subdole.
Con riferimento alle ipotesi di ingegneria sociale, il *Board* esamina 2 casi specifici:
Caso 17: Furto d'identità
Caso 18: Esfiltrazione di e-mail

Si ricorda che la casistica relativa ai *data breaches* analizzata nel paragrafo fa riferimento alle esemplificazioni presenti nelle nuove Linee guida dell'EDPB adottate il 14 gennaio 2021 in tema di *data breach*, che sono state oggetto di consultazione pubblica fino al 2 marzo scorso.

I crimini legati al ciclo dei rifiuti: *modi operandi*, attori e modalità di contrasto

di Daniela Andreatta

Contesto e numeri dei crimini sui rifiuti
La protezione dell'ambiente è diventata una priorità fondamentale nelle agende dei governi di tutto il mondo. Cresce la consapevolezza dell'esistenza di diversi comportamenti dannosi per territorio, aria, acqua, ecosistema che, se fino a poco tempo fa rimanevano poco o non puniti, oggi hanno guadagnato l'attenzione delle autorità competenti e degli interventi di contrasto e prevenzione. L'Unione Europea ha posto l'accento sul ruolo prioritario dei reati ambientali già nel 2017 per la lotta al crimine organizzato nel quadriennio 2018-2021[1] e ne ha confermato l'importanza anche quest'anno per il periodo 2021-2025[2].
I crimini ambientali sono spesso riconosciuti come il quarto mercato illegale più consistente a livello internazionale, dopo quello della droga, della contraffazione e del traffico di esseri umani[3]. Le stime parlano di un business che cresce velocemente di anno in anno, alimentato da un forte sbilanciamento tra alti profitti e bassi rischi. Per quel che riguarda i profitti, ad esempio, Legambiente parla di un giro d'affari in Italia che ha raggiunto complessivamente 419,2 miliardi dal 1995, con un valore di 19,9 miliardi solo nel 2019[4]. Sul lato dei bassi rischi, invece, essi sono dovuti sia alla scarsa probabilità, per chi commette il reato, di essere identificato o catturato, sia a un quadro normativo che prevede pene spesso inadeguate per i rei[5]. Tra le varie condotte etichettate come crimini ambientali, particolarmente sensibile è il tema dei rifiuti e della loro gestione illegale. Da un'analisi dei dati disponibili sulle illegalità connesse al ciclo dei rifiuti in Italia (figura 1) emerge un fenomeno in aumento negli ultimi anni per quel che riguarda il numero di infrazioni accertate, così come quello delle denunce e dei sequestri. Tuttavia, tale aumento può anche essere letto positivamente, come il sintomo di uno sforzo maggiore messo in atto delle forze dell'ordine nell'identificare e contrastare questi tipi di reati. Infatti, anche il numero degli arresti è in crescita, passando dai 78 del 2014 ai 198 del 2019[6], seppur con una numerosità molto inferiore rispetto alle altre categorie dovuta al fatto che una parte consistente di denunce rimane a carico di ignoti[7].

1 *Draft Council conclusions on setting the EU's priorities for the fight against organised and serious international crime between 2018 and 2021 (2017).*

2 *European Commission (2021), Communication from the commission to the European Parliament, the Council, the European economic and social Committee and the committee of the regions On the EU strategy to tackle organised crime 2021-2025.*

3 *UNEP-Interpol (2016), The Rise of Environmental Crime.*

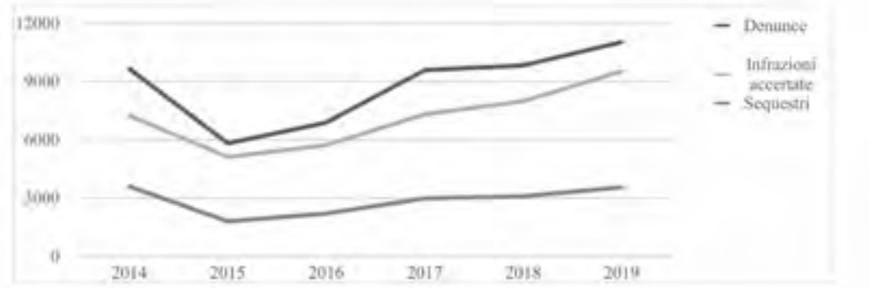
4 *Legambiente (2020), Rapporto Ecomafia.*

5 *ERA, Waste-related crime offences, https://www.era-comm.eu/combatting_waste_crime/module_3/module_3_1.html.*

6 *Dati Legambiente, www.noecomafia.it.*

7 *Istat (2020), Delitti, imputati e vittime dei reati. La criminalità in Italia, attraverso una lettura integrata delle fonti sulla giustizia.*

Figura 1. I numeri del ciclo illegale dei rifiuti in Italia. Anni 2014-2019. Valori assoluti



Fonte: elaborazione di dati Legambiente, www.noecomafia.it.

I dati sulle illegalità connesse ai rifiuti sono comunque caratterizzati da un alto numero oscuro, con molti reati che rimangono sommersi e non scoperti. Questo perché, come vedremo più avanti, tra tutti gli attori che partecipano illecitamente al ciclo di gestione dei rifiuti, c'è un alto livello di connivenza e quindi pochi *whistleblower* (informatori o dipendenti pubblici che segnalano gli illeciti). Inoltre, mancano vittime dirette che possano denunciarli.
Infatti, come molti altri crimini ambientali, anche quelli connessi ai rifiuti sono apparentemente privi di vittime dirette. In realtà, essi provocano gravi conseguenze non solo per l'ambiente, ma anche per la salute pubblica e la collettività, nonché per l'economia.
Dal punto di vista sociale, i territori inquinati sono caratterizzati da una bassa qualità della vita e da degrado ambientale. Risalgono a febbraio di quest'anno le conclusioni di un dossier dell'Istituto Superiore di Sanità che confermano, in alcune zone d'Italia, l'esistenza di una relazione causale o di una concausa tra la presenza di siti di rifiuti incontrollati e l'insorgenza di alcune patologie[8]. Inoltre, l'inquinamento del territorio ha delle conseguenze negative per l'ambiente e l'ecosistema, e mette a rischio l'agricoltura e la catena alimentare a causa della contaminazione del suolo e, conseguentemente, dei prodotti ortofrutticoli.
Dal punto di vista economico, le attività illegali legate alla gestione dei rifiuti minacciano lo sviluppo del mercato legale, in quanto impongono prezzi più bassi e rappresentano una concorrenza sleale, permettendo un vantaggio competitivo illecito e scoraggiando gli imprenditori onesti ad entrare o continuare ad operare nel settore. Queste attività comportano un danno importante anche alle casse pubbliche, non solo perché sottraggono

8 *ANSA (2021), Terra dei fuochi: Procura, insorgenza tumori legata ai rifiuti. https://www.ansa.it/sito/notizie/topnews/2021/02/10/terra-dei-fuochi-procura-insorgenza-tumori-legata-ai-rifiuti_8045978b-56fc-4ad7-b78d-dd408c761842.html.*

al fisco il pagamento di tasse e tributi (ad esempio l'ecotassa per il deposito in discarica dei rifiuti solidi), ma anche perché sono le autorità locali a dover intervenire per bonificare e pulire l'ambiente una volta contaminato.

***Modi operandi* e attori del ciclo dei rifiuti**

I crimini legati ai rifiuti sono molteplici e possono riguardare diverse condotte. In generale, si parla di attività illegali legate allo svolgimento del ciclo di gestione dei rifiuti o al traffico. Tutte le condotte illecite inerenti ai rifiuti possono essere messe in atto all'interno dei confini nazionali oppure coinvolgere due o più paesi ed avere un carattere transnazionale.
Per delle definizioni più precise di questi diversi crimini legati ai rifiuti possiamo rifarci al nostro contesto normativo.
L'articolo 256 del D. Lgs.152/2006 (anche indicato come "Codice dell'Ambiente") definisce la generica attività di gestione di rifiuti non autorizzata, che si concretizza quando "*chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216*". L'articolo ribadisce che le illegalità possono verificarsi in qualsiasi momento del ciclo di gestione e dettaglia quali sono queste fasi. Tuttavia, parlando espressamente di mancata autorizzazione, iscrizione e comunicazione, può rischiare di non coprire attività dolose più strutturate. Ad esempio, l'articolo 259 dello stesso decreto specifica la condotta di traffico illecito di rifiuti, riferendosi a sua volta alle attività di spedizione illegale di rifiuti come definite dall'articolo 26 del regolamento (CEE) 1° febbraio 1993, n. 259. Quest'ultimo definisce il traffico illecito come "*qualsiasi spedizione di rifiuti: a) effettuata senza che la notifica sia stata inviata a tutte le autorità competenti interessate conformemente al presente regolamento, o b) effettuata senza il consenso delle autorità competenti interessate, ai sensi del presente regolamento, o c) effettuata con il consenso delle autorità competenti interessate ottenuto mediante falsificazioni, false dichiarazioni o frode, o d) non concretamente specificata nel documento di accompagnamento, o e) che comporti uno smaltimento o un ricupero in violazione delle norme comunitarie o internazionali, o f) contraria alle disposizioni degli articoli 14, 16, 19 e 2*".
Il punto di forza del nostro ordinamento è la particolarità che viene riconosciuta all'attività organizzata per il traffico illecito di rifiuti secondo l'articolo 452 *quaterdecies*, introdotto nel 2018 nel Codice Penale[9]. L'articolo sancisce: "*chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti è punito con la reclusione da uno a sei anni*". In primo luogo, quindi, esiste la consapevolezza della possibilità per chiunque di poter commettere un illecito nell'ambito del ciclo dei rifiuti e di istituire con altre persone comuni una rete organizzata sulla quale poter fare affidamento per la realizzazione di (ripetute) attività illecite. A tal proposito, la giurisprudenza sottolinea che il requisito dell'ingiusto profitto non è legato all'esercizio abusivo dell'attività di gestione dei rifiuti, bensì dalla condotta continuativa ed organizzata finalizzata a conseguire risparmi di spesa e maggiori margini di guadagno[10]. In secondo luogo, le attività illecite che vengono descritte nell'articolo non sono da intendersi solamente come attività di movimento transfrontaliero di rifiuti, ma considerano praticamente tutti i momenti del ciclo che possono avvenire anche a livello nazionale, allargando quindi la definizione stessa di traffico alle attività di gestione, realizzate però in modo continuativo e organizzato.
Altro aspetto importante da tenere in considerazione quando si parla di crimini sui rifiuti è che essi solitamente si intrecciano con altre condotte illecite.
Fin dalla prima fase del ciclo di gestione, per esempio, i produttori che hanno la necessità di smaltire i loro rifiuti possono falsificare le documentazioni che li accompagnano, ovvero formulari e certificati. Questa falsificazione può avere un duplice scopo: da una parte, declassificare la vera natura dei rifiuti, dall'altra celare una parte o la totalità dei rifiuti prodotti. In entrambi casi, lo scopo è quello di risparmiare eludendo i trattamenti necessari per smaltire determinate tipologie di rifiuti, riducendone la quantità, oppure smaltendo illegalmente la totalità del quantitativo.
La falsificazione dei documenti è una strategia che si trascina anche nella fase del trasporto e che rende possibile lo spostamento dei rifiuti tra tutte le diverse fasi del ciclo, manipolando di volta in volta le informazioni sulla natura, la reale quantità e la destinazione di ciò che viene trasportato, fin a far perdere le tracce del carico. Sempre tramite falsificazione di documenti si camuffano le attività della fase di stoccaggio, durante la quale i rifiuti dovrebbero essere mantenuti rispettando determinate regole e precauzioni, ma che nel ciclo illegale funge solitamente da ulteriore declassamento dei materiali o dei quantitativi. In tutti questi casi, la declassificazione può essere certificata da professionisti che partecipano a vario titolo al ciclo dei rifiuti, come ad esempio gli analisti chimici o gli autotrasportatori, spalleggiati da altre figure compiacenti, come i consulenti ambientali, gli intermediari, i broker e altri responsabili tecnici[11].
Per quel che riguarda il trattamento o lo smaltimento dei rifiuti, abbiamo visto poc'anzi che queste fasi non avvengono nella maniera appropriata o vengono direttamente omesse, al fine di risparmiare notevolmente sui costi di gestione. Oltre al risparmio ottenuto grazie all'omissione di parte o di tutto il trattamento, c'è anche un guadagno diretto per la gestione illecita dei rifiuti. Le aziende illegali, infatti, ottengono un guadagno altrimenti non dovuto, offrendo i loro servizi al 50-60% in meno rispetto agli operatori che agiscono sul mercato lecito[12]. Secondo alcune stime, il business dei rifiuti in Italia vale 20 miliardi l'anno[13] e rappresenta un mercato invitante per le imprese criminali. Il vantaggio illecito permette quindi alle aziende colluse di disporre di capitali da destinare ad altre attività illecite o da riciclare per farne perdere le tracce.
Una pratica che si sta diffondendo sempre più è la combustione illecita di rifiuti, precisamente volta ad evitare le ultime fasi del ciclo (trattamento e smaltimento) e/o a nascondere produzioni improprie di rifiuti. L'articolo 256 bis del D. Lgs.152/2006[14] identifica il reato di combustione illecita di rifiuti quando "*chiunque appicca il fuoco a rifiuti abbandonati ovvero depositati in maniera incontrollata in aree non autorizzate*". Gli ultimi dati ISTAT disponibili in materia (figura 2) mostrano un interessante andamento antitetico tra i procedimenti per incenerimento e quelli per attività

9 *Inserito dall'art. 3 del D. Lgs. 01/03/2018, n. 21, che ha spostato nel Codice Penale, senza modifiche, l'ex art 260 del D. Lgs, 152/2006.*

10 *Ambiente Diritto, CORTE DI CASSAZIONE PENALE, Sez.3^ 07/12/2018, Sentenza n.54703 https://www.ambientediritto.it/giurisprudenza/corte-di-cassazione-penale-sez-3-07-12-2018-sentenza-n-54703/#:~:text=comma%201%2C%20d.-,lgs.,3%2C%20n.*

11 *Direzione Investigativa Antimafia - DIA (2019), Relazione I semestre; Andreatta, Favarin (2020) Features of transnational illicit waste trafficking and crime prevention strategies to tackle it.*

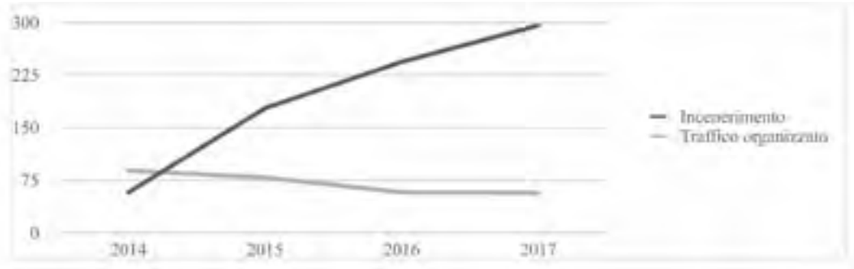
12 *Andreatta, Favarin (2020) Features of transnational illicit waste trafficking and crime prevention strategies to tackle it.*

13 *Il Sole 24 Ore (2020), Traffico illecito di rifiuti: in Italia affare da 20 miliardi, https://www.ilsole24ore.com/art/traffico-illecito-rifiuti-italia-affare-20-miliardi-ADpLqZV.*

14 *Introdotto dall'art.3 comma 1 DL 10 dicembre 2013, n.136.*

organizzata per il traffico di rifiuti (traffico organizzato): dal 2014 al 2017, mentre i primi quadruplicano (da 58 a 296 casi), i secondi sono diminuiti progressivamente (da 89 a 57 casi). Questa comparazione suggerisce che la soluzione dell'incenerimento illecito è vista come una valida alternativa non solo allo smaltimento legale, ma anche al più oneroso traffico organizzato di rifiuti, e merita una specifica attenzione di prevenzione e contrasto.

Figura 2. Procedimenti per cui è iniziata l'azione penale nelle Procure della Repubblica, per incenerimento di rifiuti e traffico organizzato di rifiuti. Anni 2013-2017. Valori assoluti.



Fonte: elaborazione di dati Istat (2020), *Delitti, imputati e vittime dei reati. La criminalità in Italia, attraverso una lettura integrata delle fonti sulla giustizia.*

Sia in merito all'incenerimento di rifiuti sia alle attività organizzate di traffico, si pensa spesso agli interventi di associazioni di tipo mafioso. Le relazioni della Direzione Investigativa Antimafia[15] riportano a tal proposito l'adozione di diversi provvedimenti interdittivi antimafia nei confronti di ditte operanti nel ciclo dei rifiuti. Tuttavia, è bene sottolineare che non si può parlare solo di associazioni di tipo mafioso, perché diversi network e gruppi criminali hanno affinato la tecnica e sono passati dalla "semplice" gestione di attività di scarico illegali a più complessi modelli imprenditoriali di gestione dell'intero ciclo dei rifiuti, anche infiltrando le aziende legali[16]. Oltretutto, si è visto che diversi singoli attori partecipano al processo e possono ricoprire svariati ruoli, attuando tutti dei comportamenti collusivi.
Anche l'attore pubblico può giocare una parte importante, in quanto produttore, gestore e supervisore nel ciclo dei rifiuti. Comportamenti omissivi o violazioni di legge sono spesso giustificati dalla necessità e l'urgenza di trovare soluzioni rapide alla questione rifiuti, *"sia per risolvere conflitti sociali sia per ovviare a esposizioni di responsabilità politica o amministrativa"*[17]. Oltretutto, spesso si parla della relazione tra crimini ambientali e corruzione. Condotte di natura corruttiva possono essere messe in atto per evitare controlli approfonditi, negli stabilimenti o ai passaggi doganali, ma anche per oliare i meccanismi degli appalti per la gestione dei rifiuti in ambito urbano.

Tecniche di investigazione e contrasto

Il ruolo primario delle organizzazioni criminali nella gestione illecita e la natura transfrontaliera dei crimini legati al ciclo dei rifiuti hanno indirizzato l'attenzione delle autorità e delle forze dell'ordine verso la necessità di cooperare, scambiandosi informazioni, risorse e personale anche a livello internazionale[18].
In Europa, la consapevolezza del fenomeno è alta e sono diversi gli sforzi che vengono messi in campo per attuare operazioni congiunte tra diversi paesi[19].
Per istituire una cooperazione efficiente, le tecniche di investigazione e contrasto suggerite[20] sono simili a quelle applicate per la criminalità organizzata: gli Stati possono assicurare assistenza legale reciproca, emettere provvedimenti di estradizione e istituire team di investigazione combinata. Di particolare importanza sono le operazioni sotto copertura, le intercettazioni ambientali, le investigazioni economico-finanziarie (sia per provare l'evento criminale sia per valutare o identificare i ricavi di un crimine), le ricostruzioni dei collaboratori di giustizia e i provvedimenti di sequestri e confisca. Tutti questi elementi concorrono a costituire evidenze importanti, le quali devono poi poter essere utilizzate come prove al momento del processo[21].
L'importanza degli strumenti investigativi sopracitati è ampiamente riconosciuta anche a livello nazionale, come testimoniano le numerose operazioni di contrasto sul ciclo illecito dei rifiuti messe in atto dalle forze di polizia[22]. Abbiamo visto che l'ordinamento italiano già riconosce alcune specificità dei crimini legati al ciclo dei rifiuti e fornisce gli strumenti legislativi adeguati per intervenire. Il D. Lgs. 152/2006 prevede la possibilità di applicare diversi tipi di sanzioni amministrative, patrimoniali e anche detentive. Le sanzioni patrimoniali potrebbero avere un peso particolarmente importante nel ciclo dei rifiuti: esse, infatti, vanno a colpire proprio l'aspetto economico che fa parte della natura di questo tipo di reati ambientali, il cui obiettivo è propriamente il risparmio o il guadagno. Tuttavia, la cornice edittale delle sanzioni imponibili per i diversi tipi di illeciti rimane probabilmente ancora troppo bassa per esercitare una fondamentale strategia deterrente rispetto ai possibili guadagni e deve essere affiancata da previsioni più severe.
A tal proposito, la direttiva europea 99/2008/CE ha imposto agli Stati membri di istituire una tutela penale dell'ambiente. Questa sottolinea la necessità di proteggerlo attraverso i mezzi della legge penale, in modo da prevedere sanzioni più severe e commisurate al danno ambientale e che esercitino un effetto deterrente, omogeneo a livello europeo. In Italia,

15 DIA, l'ultima è la Relazione del I semestre 2020.

16 *Europol, Environmental Crime, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/environmental- crime).*

17 *DIA (2019), Relazione I semestre, p. 584.*

18 *ERA, Waste-related crime offences, https://www.era-comm.eu/combatting_waste_crime/module_3/module_3_1.html.*

19 *DIA (2019), Relazione I semestre.*

20 *United Nations Convention against Transnational Organized Crime, 2003.*

21 *WasteForce Project (2020), Waste Crime Prosecution Guidance.*

22 *Si vedano per esempio i Comunicati Stampa dei Carabinieri (https://www.carabinieri.it/cittadino/informazioni/comunicati-stampa) e le relazioni della DIA (https://direzioneinvestigativaantimafia.interno.gov.it/page/relazioni_semestrali.html).*

la direttiva è stata recepita con legge 68/2015 ed è stata salutata con entusiasmo da chi si occupa di tutela ambientale. Tale provvedimento ha introdotto i cosiddetti ecoreati nel Codice Penale, ovvero: inquinamento ambientale, disastro ambientale, traffico ed abbandono di materiale radioattivo, impedimento di controllo, omessa bonifica. La legge 68/2015 ha permesso di identificare come reati un maggior numero di condotte lesive per l'ambiente e intervenire con una risposta sanzionatoria più rigorosa.
Come detto, i crimini legati ai rifiuti sono caratterizzati da un alto rischio di rimanere sommersi, soprattutto a causa dell'assenza di vittime dirette che possano denunciare il danno e dello stretto legame di connivenza tra i partecipanti all'attività. Per questo motivo, i momenti di controllo e supervisione sul corretto svolgimento del ciclo dei rifiuti devono essere frequenti. Stato, Regioni, ed enti locali concorrono a queste funzioni con differenti poteri e competenze[23] e collaborano con le forze dell'ordine per le attività di controllo. Gli ambiti di intervento devono essere ben definiti, ma allo stesso tempo ci deve essere coordinamento nella supervisione, in modo da non tralasciare nessuna fase del ciclo e ottenere una visione d'insieme sulla corretta gestione dei rifiuti.
Tuttavia, un ruolo fondamentale deve essere giocato da imprenditori e professionisti. Gli attori che partecipano al ciclo dei rifiuti possono sviluppare una maggiore o minore consapevolezza del rischio di incorrere in attività illegali, ma è importante che tutti mantengano alta l'attenzione. A tal proposito, gli articoli 178 e 188 del D. Lgs. 152/2006 parlano di principi di cooperazione e responsabilità della gestione che dovrebbero ispirare, assieme ad altri, il ciclo dei rifiuti. Si tende a riconoscere, quindi, l'esistenza di una forma di responsabilità condivisa, tale per cui il detentore di rifiuti in ogni fase dovrebbe sincerarsi di consegnarli ad altri soggetti che siano conformi ai requisiti normativi per le fasi successive. Il rispetto di questo principio costituisce un importante punto di partenza per l'istituzione di un'efficace rete di controllo e concretizza una modalità di sorveglianza naturale, tra pari, che è spesso citata come efficiente misura di prevenzione situazionale[24].

23 Si vedano per esempio gli articoli 196, 197 e 198 de D. Lgs. 152/2006.

24 Per approfondimenti: Clarke (1997), Situational Crime Prevention: Successful Case Studies.

Investi nella tua formazione Scopri i nostri corsi in Compliance & Risk Management

Aggiorna le tue skill e migliora le tue competenze specialistiche con i nostri corsi di alta formazione studiati appositamente per operare con successo nel mondo corporate e business.

SEAC cefor

Privacy e GDPR

Recovery Fund

Riciclaggio

Passaggio generazionale

Welfare aziendale

Contattaci:
SEAC CEFOR SRL
Via Solteri, 74, 38121 TRENTO
info.cefor@seac.it
0461.805192
Ci trovi anche su:

SEAC

Passione per semplificare le cose

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

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

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

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