I QUADERNI DEL GRUPPO ASLA DI **CORPORATE COMPLIANCE**

CORPORATE COMPLIANCE ROUND TABLES 2022

Atti del convegno con sei tavole rotonde con la partecipazione di quattordici esperti di diritto societario e relative strutture organizzative ai sensi del Decreto Legislativo n° 231 del 2001, un'occasione unica per diffondere la cultura del diritto d'impresa e la condivisione delle conoscenze più aggiornate in materia da parte dei professionisti dei propri Studi Membri

ASLA
ASSOCIAZIONE STUDI LEGALI ASSOCIATI

I QUADERNI DEL GRUPPO ASLA DI **CORPORATE COMPLIANCE**

A CURA DI IRENE PICCIANO E ANTONIO BANA
CON TESTI DI MICAELA BARBOTTI, ANGELA BERINATI, FRANCESCA BEVILACQUA, PIETRO BOCCACCINI, TIZIANA BONESCHI, EVA CRUELLAS SADA, SIMONA CUSTER, PAOLA DE PASCALIS, FEDERICA DENDENA, EUGENIA GAMBARARA, GIACOMO GORI, PIERO MAGRI, FEDERICA MAMMÌ BORRUTO, ANDREA MANTOVANI, ELENA MANDARÀ, MARTA MARGIOCCO, GIULIO NOVELLINI, PIETRO ORZALESI, MARIANGELA PAPADIA, JOSEPHINE ROMANO, ROBERTO TIRONE

CORPORATE COMPLIANCE ROUND TABLES 2022

Atti del convegno con sei tavole rotonde con la partecipazione di quattordici esperti di diritto societario e relative strutture organizzative ai sensi del Decreto Legislativo n° 231 del 2001, un'occasione unica per diffondere la cultura del diritto d'impresa e la condivisione delle conoscenze più aggiornate in materia da parte dei professionisti dei propri Studi Membri

ASLA
ASSOCIAZIONE STUDI LEGALI ASSOCIATI

Indice

CAPITOLO 1 di Pietro Boccaccini, Federica Mammì Borruto, Elena Mandarà, Andrea Mantovani, Giulio Novellini

Sfide legali collegate all'Intelligenza Artificiale Le azioni da mettere in campo in ottica di prevenzione e gestione del "rischio *privacy*"

SOMMARIO: Case study – 1.Risk based approach, privacy-by-design e by-default – 1.1. GDPR e risk based approach – 1.2. Privacy-by-design e privacy-by-default – 1.3Valutazione d'impatto preventiva (DPIA) – 2. L'individuazione dei ruoli privacy – 3. Gli obblighi di trasparenza verso gli interessati – 4. L'esercizio dei diritti degli interessati – 5. La base giuridica del trattamento – 6. Il divieto di decisioni basate unicamente su un trattamento automatizzato – 7. L'individuazione delle misure di sicurezza – 8 Anonimizzazione e pseudonimizzazione

Case study

La società Alpha Italia S.p.A. ("**Società**") attiva nel settore del *digital advertisement* e controllata dalla casa madre americana Alpha US LLC, ha sviluppato una tecnologia, basata su un sistema di *deep learning*, che, tramite l'uso di algoritmi, consente di profilare in modo estremamente accurato i consumatori per poter poi svolgere iniziative di *marketing* nei loro confronti ("**Tool**").

Le aziende che fanno ricorso al servizio della Società inseriscono nel Tool tutte le informazioni dei clienti o dei *prospect*, raccolte direttamente o mediante l'acquisto di banche dati da terzi (tra cui nome, cognome, età, tipologia di prodotti/servizi acquistati, importo acquisti effettuati, localizzazione dei negozi ove è stato effettuato l'acquisto, ecc.) ricevendo poi come *output*, tra l'altro, un'indicazione dei prodotti/servizi cui i clienti/*prospect* possono essere interessati, del *range* di prezzo che sono disposti a pagare, delle località ove è possibile ingaggiare tali consumatori mediante eventi promozionali, ecc., il tutto grazie alle capacità predittive dell'Intelligenza Artificiale (AI) alla base del Tool.

La Società, per fornire questo servizio, si avvale del supporto tecnico sia della casa madre che di terze parti, stabilite negli Stati Uniti e in India.

1. Risk based approach, privacy-by-design e by-default, DPIA

1.1. GDPR e risk based approach

Nell'ambito del trattamento dei dati personali, il Regolamento (UE) 679/2016 ("**GDPR**" o "**Regolamento**") ha introdotto il principio del *risk based approach*, inteso come l'obbligo, posto in capo al titolare del trattamento e strettamente correlato al principio di *accountability* sancito dall'art. 5 GDPR, di porre in essere una preliminare valutazione dei rischi legati ai trattamenti, in termini di possibili violazioni dei diritti e delle libertà degli interessati, individuando di conseguenza le misure tecniche ed organizzative da adottare, della cui efficacia è direttamente chiamato a rispondere.

Si tratta di un principio generale che permea interamente il testo del Regolamento e si riflette in diverse disposizioni, a partire da quanto previsto dall'art. 32 GDPR in tema di sicurezza del trattamento, ma anche dagli artt. 25 e 35 GDPR, che disciplinano rispettivamente i principi di *privacy-by-design* e *privacy-by-default* e la Valutazione d'impatto preventiva (DPIA), di cui si dirà meglio nel prosieguo.

È chiaro che, nel caso di trattamenti correlati all'utilizzo di sistemi AI, (quali ad esempio il Tool) la preventiva valutazione del livello di rischio possa risultare particolarmente onerosa, tanto in ragione della complessità del funzionamento di tali sistemi, quanto alla luce dei problemi legati all'utilizzo dei cosiddetti *big data*[1].

Eppure, il principio del *risk based approach* è stato richiamato anche nella Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale ("**AI Act**"). L'AI Act, infatti, distingue i diversi sistemi a seconda del livello di rischio a essi correlato, prevedendo regole diverse con un approccio graduale. Lo scopo è infatti quello di costruire un sistema proporzionato, basato appunto sul rischio. Nel caso di sistemi definiti "ad alto rischio" è prevista, ad esempio, la creazione di un sistema di gestione dei rischi costituito da un processo continuo da eseguire nel corso dell'intero ciclo di vita del sistema AI (art. 9). Il medesimo approccio si riflette anche nelle previsioni di cui all'art. 10 dell'AI Act, relative ai dati e alla governance dei dati, ed in particolare con riguardo alle pratiche da porre in essere nel caso di sistemi AI ad alto rischio. Tali pratiche, infatti, presuppongono una preventiva valutazione delle possibili distorsioni, nonché delle eventuali mancanze o lacune dei dati, congiuntamente all'individuazione delle tecniche più appropriate da adottare.

1 Sebbene non esistano definizioni normative precise, con il termine *big data* ci si riferisce comunemente alla raccolta, l'analisi e l'accumulo di grandi quantità di dati, provenienti da fonti diverse e che non possono essere elaborati da strumenti informativi tradizionali.

1.2. Privacy-by-design e privacy-by-default

In ottica di *accountability* e prevenzione del rischio, sia in prospettiva generale che con esplicito riferimento al *case study* di cui sopra, occorre precisare anche la previsione di cui all'art. 25 GDPR, sancente i principi di *privacy-by-design* e *privacy-by-default*.

Come evidenziato dallo European Data Protection Board ("**EDPB**") nelle *Linee-guida 4/2019 sull'art. 25*, in relazione all'utilizzo delle nuove tecnologie, e in particolare di sistemi AI, questi principi assumono grande rilevanza in quanto sanciscono il nesso imprescindibile fra piano normativo e tecnico, svolgendo un ruolo fondamentale nel garantire la protezione dei dati personali già a livello strutturale e promuovendo un atteggiamento proattivo e preventivo piuttosto che reattivo e rimediale.

La centralità della norma si comprende ancor di più tenendo conto del fatto che il rispetto dell'art. 25 GDPR è strettamente funzionale all'attuazione di tutti gli altri principi previsti all'art. 5 GDPR (i.e. trasparenza, liceità, correttezza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione). Ad esempio, le citate Linee-guida fanno riferimento all'art. 25 come strumento per garantire il rispetto del principio di esattezza nel caso di utilizzo di sistemi AI.

In primo luogo, l'articolo pone in capo al titolare del trattamento l'obbligo di predisporre, tenendo conto di tutte le circostanze concrete (i.e. natura, ambito di applicazione, contesto e finalità del trattamento), misure adeguate volte ad attuare nella maniera più efficace i principi di protezione dei dati, sia nella fase di scelta dei mezzi impiegati per il trattamento che in quella di concreta attuazione dello stesso. Nell'individuazione di tali misure, il titolare dovrà inoltre tenere in considerazione i costi di implementazione e lo stato dell'arte.

Con esplicito riferimento al *case study*, ciò presuppone che la Società (titolare del trattamento) sia in grado di individuare, prima che il trattamento abbia inizio, (i) i dati personali oggetto dello stesso, (ii) le specifiche finalità, e (iii) le categorie di soggetti interessati coinvolti.

Tuttavia, uno dei principali problemi legati all'utilizzo di sistemi AI, emerso particolarmente in relazione all'utilizzo di algoritmi *machine learning*[2], è quello concernente l'imprevedibilità dei risultati e/o del concreto utilizzo dei dati personali, da cui consegue inevitabilmente la difficoltà nell'individuare a monte quali misure adottare in concreto.

Un altro elemento importante che la Società deve prendere in considerazione in merito all'implementazione del Tool è il riferimento al cd. "stato dell'arte". All'interno delle Linee-guida dell'EDPB, si sottolinea infatti la necessità che i titolari siano non soltanto a conoscenza dei progressi tecnologici, ma anche dei rischi ad essi correlati e, di conseguenza, delle misure da adottare al fine di assicurare un'attuazione efficace di tali principi. La velocità con cui il contesto tecnologico si evolve, specialmente in settori in fase di piena esplora-

2 Termine con il quale ci riferisce a sistemi in grado di attribuire nuovo significato ai dati raccolti e generare nuovi modelli di analisi, che migliorano grazie all'esperienza, senza necessità di intervento umano.

zione come quello dell'AI, implica in capo al titolare del trattamento un particolare sforzo di valutazione continuativa, funzionale a garantire l'efficacia delle misure adottate. Il fatto che la norma richiami espressamente "lo stato dell'arte" ha quindi come conseguenza che l'assenza di una valutazione costante da parte del titolare, nei termini in cui si è detto, possa tradursi in una violazione dell'art. 25 GDPR.

Il comma 2 dell'art. 25 GDPR obbliga invece il titolare ad adottare misure tali da garantire che siano trattati "*per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento*". Si tratta di un corollario del principio di minimizzazione, che mal si concilia con l'utilizzo dei *big data* e con la natura stessa dei sistemi AI, specie laddove sia previsto l'impiego di algoritmi *machine learning*, il cui buon funzionamento dipende proprio dalla possibilità di utilizzare enormi quantità di dati.

Nonostante le difficoltà di attuazione, il rispetto dei principi di *privacy-by-design* e *privacy-by-default* non viene tuttavia considerato come un elemento in grado compromettere lo sviluppo dei sistemi AI. Al contrario, il rispetto di tali principi è incoraggiato e ritenuto idoneo a garantire uno sviluppo virtuoso di tali sistemi, rispettoso della disciplina sulla protezione dei dati personali. Questo è quanto sottolineato anche nel report "*The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*", pubblicato dallo European Parliamentary Research Service ("**EPRS**") nel 2020.

In relazione all'utilizzo dei sistemi AI, fra le misure idonee da adottare viene spesso citato il ricorso a tecniche di criptazione e pseudonimizzazione, di cui si discuterà più diffusamente al successivo paragrafo "Anonimizzazione e pseudonimizzazione".

1.3 Valutazione d'impatto preventiva (DPIA)

L'art. 35 GDPR prevede che nel caso in cui un trattamento, in particolare qualora comporti l'uso di nuove tecnologie, e tenuto conto della natura, dell'oggetto, del contesto e delle finalità dello stesso, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare ha l'obbligo, prima che il trattamento abbia inizio, a svolgere una valutazione d'impatto preventiva (DPIA).

Lo scopo della DPIA è quello di valutare preventivamente il livello di rischio collegato al trattamento, al fine di individuare le misure più adeguate da adottare per mitigare tale rischio. È evidente, dunque, il nesso con quanto discusso fino a questo momento, sia in relazione al *risk based approach*, di cui l'art. 35 è senz'altro espressione, sia con riferimento ai *principi di privacy-by-design* e *privacy-by-default* che, come si è visto, sono strettamente legati sia alla valutazione del rischio che all'individuazione delle misure da adottare.

Non a caso, lo stesso EDPB, all'interno delle linee-guida sull'art. 25, richiama a sua volta le indicazioni sulla valutazione del rischio previste dalle linee-guida sulla DPIA, affermando che queste possano trovare applicazione anche in attuazione dei *principi by-design* e *by-default*.

È il caso di chiarire che l'art. 35 identifica solo alcuni casi specifici nei quali sussiste senz'altro l'obbligo del titolare di effettuare la DPIA, mentre nelle altre ipotesi quest'ultimo è chiamato a svolgere una valutazione circa la sussistenza o meno delle condizioni che la renderebbero necessaria.

Al fine di tale valutazione, bisogna comunque tenere conto di quanto previsto dal considerando 75 del GDPR, che riconduce al concetto di rischio elevato i trattamenti potenzialmente discriminatori, o che possano determinare un furto d'identità, un danno economico o alla reputazione, la privazione della libertà personale o del controllo sui propri dati personali, la violazione di dati appartenenti a categorie particolari e via discorrendo.

In particolare, l'art. 35 prevede che la valutazione d'impatto debba essere effettuata laddove il trattamento:

a) implichi una valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su un trattamento automatizzato, compresa la profilazione, su cui si fondano decisioni che hanno effetti giuridici o incidono in modo analogo sulle persone fisiche;

b) sia su larga scala ed abbia ad oggetto categorie particolari di dati personali, ai sensi dell'art. 9 GDPR;

c) comporti la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Nel novembre del 2018, il Garante per la protezione dei dati personali ("**Garante**") ha inoltre adottato un provvedimento volto a individuare più nel dettaglio i trattamenti che dovrebbero essere soggetti a valutazione d'impatto, in linea con le considerazioni già svolte dall'Art. 29 Working Party (nelle *Linee guida in materia di valutazioni d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del GDPR*). È significativo evidenziare che fra le ipotesi previste si faccia espressamente riferimento ai trattamenti effettuati attraverso l'uso di tecnologie innovative, includendo fra gli esempi rilevanti in tal senso proprio i sistemi di intelligenza artificiale.

Peraltro, perimenti a quanto detto trattando dell'art. 25 GDPR, in relazione all'utilizzo di sistemi AI, il preventivo svolgimento di una DPIA è considerato un importante strumento idoneo a garantire la *compliance* dei sistemi AI rispetto alla normativa sulla protezione dei dati personali.

Quest'ultima considerazione va ricollegata a una riflessione ulteriore, particolarmente rilevante nel contesto dei sistemi AI, riguardante la distinzione fra dati personali e non personali.

Com'è noto, infatti, le disposizioni del GDPR trovano applicazione solo laddove abbia luogo un trattamento di dati personali, intesi come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*", ai sensi dell'art. 4, no. 1 del Regolamento. Sebbene sul concetto di identificabilità si tornerà più specificatamente nel prosieguo, va evidenziato sin d'ora che il funzionamento e le caratteristiche dei sistemi AI mettono in discussione la netta distinzione fra

dati personali e non personali, dal momento che dal trattamento di dati non personali è comunque possibile ricavarne altri che consentono l'identificazione dell'interessato, rientrando quindi nell'ambito di applicazione del GDPR.

Alla luce di quanto sopra, e nell'ottica di un approccio in linea con il generale principio di *accountability*, nonché con gli obblighi di cui all'art. 25, la Società dovrebbe eseguire una DPIA per scongiurare ogni possibile rischio agli interessati e garantire il pieno rispetto della normativa *privacy* applicabile all'utilizzo del Tool.

2. L'individuazione dei ruoli privacy

L'uso di sistemi di AI comprende normalmente una pluralità di trattamenti diversi e l'intervento di più soggetti. Per mettere a fuoco i possibili ruoli *privacy* occorre quindi muovere dalle regole generali previste dal GDPR.

In linea di principio, è possibile configurare il ruolo di titolare nel caso in cui la società raccolga in prima battuta i dati e prenda le seguenti decisioni:

- che tipo di dati raccogliere e di che interessati;
- perché e come trattare i dati raccolti;
- quanto tempo conservare i dati;
- come gestire i diritti degli interessati.

Il responsabile, invece, agisce in base alle istruzioni del titolare, con un margine di discrezionalità quindi molto inferiore sul trattamento. Il responsabile è comunque legittimato ad assumere alcune decisioni di tipo tecnico, ad esempio:

- i sistemi IT e i metodi per trattare i dati;
- come conservare i dati;
- le misure di sicurezza da adottare;
- come cancellare i dati.

Una società potrebbe essere in grado di assumere decisioni per supportare la fornitura di servizi di AI ma rimanere comunque un responsabile, ad esempio nelle seguenti aree:

- implementazione di algoritmi di *machine learning* generici, come il linguaggio di programmazione;
- come i dati e i modelli sono conservati;
- misure per ottimizzare gli algoritmi di apprendimento;
- dettagli collegati all'uso dei modelli, come la scelta dell'interfaccia di programmazione (API).

Nel *case study* la società Alpha Italia S.p.A., per poter usare il servizio, immette nel sistema "propri" dati, rispetto ai quali riveste il ruolo di titolare. La

società che fornisce il supporto tecnico, così come la casamadre, trattano invece i dati per conto di Alpha, quindi come responsabili del trattamento. In entrambi i casi il rapporto dovrà essere formalizzato tramite una nomina ai sensi dell'art. 28 del GDPR. Mentre però con la controllante il contratto potrà essere anche "*light*", il rapporto con il fornitore esterno dovrà essere disciplinato con particolare attenzione, anche con riferimento alle misure di sicurezza alle quali il responsabile si deve attenere.

In entrambi i casi occorre tenere in considerazione il fatto che le entità sono stabilite in giurisdizioni che non fanno parte dello Spazio Economico Europeo e che non sono considerate adeguate dalla Commissione europea. Sarà pertanto necessario rispettare anche il framework di regole applicabili in materia, che impone lo svolgimento di un assessment in merito al trasferimento, anche al fine di individuare i rischi specifici e le possibili misure da adottare per mitigarli, nell'ottica di rendere il livello di protezione dei dati trasferiti analogo a quello garantito nell'UE. Occorrerà poi sottoscrivere le clausole contrattuali standard approvate dalla Commissione europea (nel caso in esame, il modulo titolare-responsabile), specificando negli allegati gli elementi peculiari del trattamento e le misure di sicurezza da porre in essere, che dovrebbero tenere conto di quanto emerso in sede di assessment e dovrebbero garantire l'adeguatezza della tutela dei dati. Le misure supplementari individuate e formalizzate nelle SCC devono naturalmente essere implementate e la loro efficacia deve essere poi verificata.

Uscendo dal *case study*, nel caso in cui la tecnologia di AI usata da un certo titolare sia sviluppata e messa a disposizione da un'altra società, i dati immessi nel sistema andranno quasi certamente ad alimentare l'algoritmo, allenandolo e consentendo così alla macchina di formulare previsioni sempre più accurate: le finalità del trattamento connesse sono difficilmente riconducibili al titolare, ma piuttosto al fornitore. Questo, quindi, rispetto agli stessi dati di cui è responsabile potrebbe doversi qualificare anche titolare, con tutto ciò che ne consegue in termini di adempimenti obbligatori.

Acquistare un sistema AI da un terzo non esonera in ogni caso la società che si avvale del servizio dal rispetto della normativa sulla protezione dei dati. Nella maggior parte dei casi, infatti, la società che usa il servizio è il titolare del trattamento, in quanto decide come utilizzare il sistema AI, quali sono le caratteristiche del modello e quale sarà l'output (i.e. cosa viene classificato o predetto) e quindi – seguendo le regole del GDPR – è il soggetto che definisce le finalità e i mezzi del trattamento e ha quindi l'onere di dimostrare che il sistema AI sia conforme alla normativa privacy applicabile. Dal punto di vista pratico occorre quindi:

- scegliere un fornitore adeguato, valutando preventivamente la società e il sistema di intelligenza artificiale che offre, anche sotto il profilo della sicurezza;
- ottenere dal fornitore copia della documentazione da cui risulta che è stato adottato un approccio di protezione dei dati *by design* e *by default*;

- con il supporto del fornitore, effettuare una valutazione d'impatto (anche nelle situazioni in cui questa non sarebbe obbligatoria ex art. 35 del GDPR, è senz'altro raccomandabile, considerati anche tutti gli orientamenti in materia delle Autorità di controllo; in caso si valuti di non procedere con l'assessment occorre documentare i motivi della scelta);
- formalizzare i ruoli *privacy* tra la società che usa l'AI e il fornitore (mediante apposite clausole e *data processing agreement*), considerando in anticipo anche aspetti come il riscontro alle richieste di esercizio dei diritti degli interessati o lo svolgimento di *audit* e *test* di sicurezza;
- valutare la questione della conservazione dei dati e di eventuali trasferimenti dei dati in paesi non adeguati, poiché in questo caso si rendono necessari adempimenti piuttosto onerosi (tra cui lo svolgimento di un *transfer impact assessment*, prima della conclusione delle nuove *standard contractual clauses* (SCC) e l'adozione di misure supplementari affinché ai dati sia assicurato un livello di protezione sostanzialmente equivalente a quello garantito nell'UE);
- capire a fondo il funzionamento dell'AI, per poterlo spiegare agli interessati.

L'ipotesi della contitolarità non è da escludere a priori con riferimento alle situazioni in cui è coinvolto un fornitore di modelli di *machine learning*, perché potrebbe essere rilevato che almeno parte delle finalità (e dei mezzi) del trattamento siano congiunte, in particolare ragionando rispetto all'allenamento dell'algoritmo, i cui benefici a ben vedere ricadono sia sulla società che usa il servizio basato su AI (avrà *output* sempre più precisi) che sul fornitore (il proprio "prodotto" evolverà, diventando maggiormente appetibile sul mercato). Laddove questa ipotesi non sia applicabile, è comunque raccomandabile documentare perché sia stata esclusa.

Nel caso del cosiddetto *federated learning* – ossia la tecnica che prevede la condivisione tra differenti entità di singoli modelli di apprendimento per farli confluire in un modello solo, più accurato – secondo alcune Autorità potrebbe essere configurabile una contitolarità, anche nel caso in cui le parti coinvolte non abbiano accesso ai dati degli altri.

Tuttavia, una situazione di contitolarità potrebbe configurarsi più probabilmente in un rapporto *intercompany*, in cui due o più entità fanno ricorso al medesimo sistema di AI per le stesse finalità (es. analizzare dati dei clienti o efficientare le campagne di *marketing* del gruppo), oppure nel caso di una *partnership* tra entità diverse, nell'ambito di un progetto comune di *business* o di ricerca. In simili situazioni occorrerà includere nel contratto che è obbligatorio stipulare ai sensi dell'art. 26 del GDPR anche previsioni specifiche con riferimento allo svolgimento degli *assessment*, all'esercizio dei diritti degli interessati (particolarmente complessi in certi casi, si pensi al diritto di cancellazione dei dati immessi "nella macchina" e usati anche per il suo *training*), alla ripartizione dei compiti e delle responsabilità in caso di situazioni ordinarie (ad esempio, la

gestione dei rapporti con il fornitore del sistema di AI a livello di formalizzazione dei contratti e di verifica del loro rispetto) o di situazioni critiche o di gestione complessa (come eventuali *data breach*, contenziosi, ispezioni da parte di Autorità, ecc.).

3. Gli obblighi di trasparenza verso gli interessati

Quello della trasparenza verso gli interessati è uno dei temi più articolati, perché la complessità dei sistemi di intelligenza artificiale ne implica naturalmente una notevole opacità.

Come è noto, in base al GDPR, gli interessati hanno il diritto di ricevere tutte le informazioni di cui agli artt. 13 e 14, per cui, oltre a dover essere informati circa l'identità e i dati di contatto del titolare del trattamento, le finalità e le relative basi giuridiche, devono ottenere, ad esempio, informazioni sui tempi di conservazione dei dati, sulle terze parti eventualmente destinatarie dei dati e sulla circostanza che i dati sono trasferiti al di fuori dello Spazio economico europeo. Laddove i dati personali siano raccolti presso l'interessato, l'informativa deve essere fornita al momento della raccolta dei dati e, quindi, prima di utilizzarli per allenare l'algoritmo o di applicare il modello algoritmico.

Qualora il trattamento si basi sul legittimo interesse, l'interessato ha il diritto a opporsi al trattamento in qualsiasi momento (art. 21(1) del GDPR). Peraltro, quando, come nel *case study* che stiamo commentando, i dati personali sono trattati per finalità di *marketing*, non occorre che l'interessato motivi l'esercizio del diritto di opposizione (art. 21(2) del GDPR). Sotto il profilo della trasparenza, ai sensi dell'art. 21(4) del GDPR, il titolare del trattamento ha specifici obblighi informativi anche con riguardo al diritto di opposizione degli interessati, perché deve portare alla loro attenzione la sua esistenza, presentandolo chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con gli interessati.

Nella fattispecie descritta nel *case study*, l'informativa dovrà fra l'altro indicare, oltre alle finalità del trattamento: (i) la base giuridica del trattamento (si tratterà più avanti il tema nella relativa selezione); (ii) i diritti degli interessati, fra cui il citato diritto di opposizione o, se la base giuridica fosse ad esempio il consenso, il diritto di revocarlo; (iii) il titolare del trattamento (che immaginiamo essere un'impresa che si avvale dei servizi di Alpha Italia S.p.A., salvi altri titolari coinvolti); (iv) i destinatari dei dati (che potrebbero ricomprendere società del gruppo Alpha che gestiscono il sistema); (v) i tempi di conservazione dei dati.

L'Information Commissioner's Office britannico (nella *Guidance on AI and data protection* del 15 marzo 2023) individua due categorie fondamentali a cui applicare le regole di trasparenza: (i) la trasparenza relativa al processo (che concerne informazioni sulla governance del sistema di intelligenza artificiale); (ii) la trasparenza relativa al risultato (che serve a chiarire cosa è successo nel caso di una particolare decisione).

Peraltro, per espressa previsione normativa (artt. 13(2)(f) e 14(2)(g) del GDPR), l'informativa deve contenere informazioni in merito all'esistenza di processi decisionali automatizzati (inclusa la profilazione) che producano effetti giuridici che riguardano gli interessati o che incidano significativamente su di loro. In questo caso, gli interessati devono ricevere le informazioni significative sulla logica utilizzata e sull'importanza e sulle conseguenze che tale trattamento può avere.

Nel caso dell'intelligenza artificiale, il problema della *compliance* con questo requisito di trasparenza si pone in termini complessi, a causa dell'opacità del funzionamento degli algoritmi. Questo, in particolare, può riguardare i sistemi di *deep learning*, basati su reti neurali e meccanismi di autoapprendimento, che rendono difficile (perfino per i programmatori) predire gli *output* che saranno prodotti. Nel *case study* che stiamo commentando il *tool* che consente di profilare gli interessati è, appunto, basato su un sistema di *deep learning*.

Dunque, che informativa deve essere fornita in proposito agli interessati? È da escludere che sia necessario (o utile) rendere note agli interessati le formule matematiche alla base dell'algoritmo utilizzato, che, del resto, risulterebbero di difficile comprensione per la maggior parte delle persone[3]. In proposito, anche l'Information Commissioner's Office, nella citata *Guidance on AI and data protection* del 15 marzo 2023, precisa che le ragioni in base alle quali un sistema di intelligenza artificiale "prende una decisione" devono essere "*fornite in modo accessibile e non tecnico*".

Inoltre, fornire dati prettamente tecnici potrebbe creare un conflitto con i diritti di proprietà intellettuale dei soggetti coinvolti nella produzione del sistema. In altri termini, fornendo agli interessati informazioni relative al sistema di intelligenza artificiale, potrebbe porsi il rischio di rivelare segreti industriali o aziendali che non c'è ragione di rivelare.

È bene invece fornire, come suggerito anche dal Gruppo di lavoro Articolo 29 (nelle *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*), alcuni elementi che sono quelli più significativi per l'interessato, chiarendo, in particolare:

- quali tipi di dati sono utilizzati dal sistema di intelligenza artificiale per creare il profilo;
- con un linguaggio che sia il più semplice e comprensibile possibile, come (in termini di logica, più che di processo tecnologico) dai dati si arriva alla creazione del profilo dell'interessato utilizzato dal sistema;
- i motivi per i quali tale profilo è pertinente rispetto alle finalità del trattamento;
- le modalità di utilizzo del profilo ai fini di una decisione riguardante l'interessato.

3 Del resto, l'art. 12(1) del GDPR prescrive che l'informativa sia fornita in "*forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro*".

Quindi, in proposito, nel *case study*, l'informativa dovrà chiarire in modo trasparente che il sistema di intelligenza artificiale raccoglie un certo tipo di informazioni (quali nome, cognome, età, tipologia di prodotti/servizi acquistati, importo degli acquisti effettuati, localizzazione dei negozi ove è stato effettuato l'acquisto), che lo fa non soltanto direttamente ma anche tramite terzi, e che i dati raccolti vengono combinati e valutati con metodi predittivi in modo tale che, da tale valutazione, emergano i gusti, la capacità di acquisto, ecc., degli interessati. Nella descrizione della logica sottostante la profilazione è importante che non venga omessa la descrizione di elementi che possano comportare rischi per gli interessati (come la predizione della capacità di acquisto).

Un tema rilevante e caratteristico dei sistemi di intelligenza artificiale, chiaramente connesso a quello dell'informativa, riguarda l'individuazione dei soggetti dei cui dati personali si tratta e a cui, quindi, l'informativa va fornita. I sistemi di intelligenza artificiale che accedono a un servizio trattano normalmente dati personali degli utenti di tale servizio ma possono trattare anche dati di terzi, raccolti da fonti più o meno pubbliche. Ad esempio, dati di non utenti potrebbero essere raccolti da *internet* o dai *social media* affinché un sistema di intelligenza artificiale generativa possa elaborare risposte basandosi su quei dati. Anche questi terzi (non utenti) si qualificano come interessati e, quindi, possono vantare un diritto di essere informati dell'esistenza del trattamento.

In generale, può essere difficile identificare e comunicare con gli interessati non utenti (inclusi gli interessati i cui dati personali sono contenuti nei dati di *training*). Quindi, fornire l'informativa direttamente a tali interessati potrebbe risultare impossibile o comportare uno sforzo sproporzionato. In questi casi, potrebbe risultare possibile ovviare alla difficoltà diffondendo pubblicamente le informazioni necessarie, fra cui quelle che spieghino da dove il sistema di intelligenza artificiale ottiene i dati che utilizza e come gli interessati possono opporsi al trattamento[4].

4. L'esercizio dei diritti degli interessati

Il GDPR riconosce numerosi diritti agli interessati e garantirne l'esercizio nel contesto dei sistemi di intelligenza artificiale - nei vari momenti del ciclo di sviluppo e uso di tali sistemi, inclusa l'attività di *training*[5] - può essere tutt'altro che agevole.

Oltre al diritto di opposizione al trattamento, a cui si è già fatto cenno, ad esempio gli interessati hanno il diritto alla portabilità dei dati *ex* art. 20 del GDPR, quando il trattamento, effettuato con mezzi automatizzati, si basi sul consenso o sull'esecuzione di un contratto. Questo comporta il diritto degli

4 Relativamente al caso di dati che non siano ottenuti presso l'interessato, in base all'art. 14(5)(b) del GDPR, quanto fornire l'informativa risulti impossibile o implichi uno sforzo sproporzionato, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi degli interessati, anche rendendo pubbliche le informazioni.

5 Peraltro, prima di essere utilizzati per l'addestramento di un modello statistico, i dati di training vengono normalmente sottoposti a trattamenti necessari a renderli più adatti agli algoritmi. Questi processi possono rendere molto più difficile collegare i dati a uno specifico individuo, senza che, però, questo escluda la lora natura di dati personali e, quindi, l'applicabilità della relativa normativa.

interessati di ricevere i dati che hanno fornito al titolare in un formato strutturato, di uso comune e leggibile da dispositivo automatico e il diritto a che tali dati siano trasmessi a un altro titolare senza impedimenti.

La trasmissione diretta dei dati da un titolare all'altro è però subordinata alla fattibilità tecnica (art. 20(2) del GDPR) e, nel contesto di sistemi complessi come quelli di intelligenza artificiale, questo potrebbe non essere sempre possibile.

Gli interessati, fra l'altro, hanno anche diritto ad accedere a una serie di informazioni relative al trattamento dei loro dati ai sensi dell'art. 15 del GDPR[6] e a ottenerne la cancellazione "*senza ingiustificato ritardo*" ai sensi dell'art. 17 del GDPR, ad esempio se il consenso al trattamento viene revocato o se viene esercitato il diritto di opposizione al trattamento fondato sul legittimo interesse.

Il diritto di accesso, così come visto per il rispetto del principio di trasparenza, può porre il problema del bilanciamento con i diritti di proprietà industriale e intellettuale.

Lo stesso considerando 63 del GDPR chiarisce, infatti, che tale diritto non dovrebbe ledere "*il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software*".

Tema comune all'esercizio di tutti i diritti degli interessati è poi quello dei dati inferenziali o "derivati". Questi dati, tra i quali rientrano i risultati prodotti da un algoritmo, possono essere dati personali in quanto, in combinazione con altri dati, siano riconducibili all'interessato.

Ad esempio, nel caso tipo che stiamo commentando, gli *output* elaborati dal *tool* di profilazione, tra cui l'indicazione dei prodotti/servizi che i clienti/*prospect* possono essere propensi ad acquistare, il *range* di prezzo che sono disposti a pagare, le località ove è possibile ingaggiare tali consumatori mediante eventi promozionali, salvo che non siano formulati su base anonima e aggregata, sono dati personali.

I dati derivati devono essere comunicati all'interessato in caso di esercizio del diritto di accesso. Il problema, nel caso di sistemi di intelligenza artificiale, può però essere la stessa identificazione, nel corso dell'elaborazione fatta dal sistema, di quali siano tutti i dati che possano definirsi personali, perché fra *input* e *output* c'è un meccanismo complesso, che quindi deve essere tecnicamente

6 In proposito, la Corte di giustizia dell'Unione europea, con sentenza del 4 maggio 2023 (causa C-487/21, Österreichische Datenschutzbehörde v CRIF GmbH) ha precisato che "*il diritto di accesso di cui all'articolo 15 del GDPR deve consentire all'interessato di verificare che i dati personali che lo riguardano siano corretti e trattati in modo lecito*", così da permettergli anche di esercitare gli altri diritti riconosciutigli dal GDPR; conseguentemente, la copia dei dati personali oggetto di trattamento, che il titolare del trattamento è tenuto a fornire ai sensi dell'art. 15(3), prima frase, del GDPR, "*deve presentare tutte le caratteristiche che consentano all'interessato di esercitare effettivamente i suoi diritti a norma* [del GDPR] *e, pertanto, deve riprodurre integralmente e fedelmente tali dati*". Secondo la Corte, dunque, "*il diritto di ottenere dal titolare del trattamento una copia dei dati personali oggetto di trattamento implica che sia consegnata all'interessato una riproduzione fedele e intelligibile dell'insieme di tali dati. Detto diritto presuppone quello di ottenere copia di estratti di documenti o addirittura di documenti interi o, ancora, di estratti di banche dati contenenti, tra l'altro, tali dati, se la fornitura di una siffatta copia è indispensabile per consentire all'interessato di esercitare effettivamente i diritti conferitigli* [dal GDPR]*, fermo restando che occorre tener conto, al riguardo, dei diritti e delle libertà altrui*".

reso il più possibile "manovrabile", per consentire in punto di fatto l'esercizio di questi diritti. Dunque, i sistemi informatici andrebbero impostati, sotto il profilo tecnico, in modo tale da classificare i dati processati dal sistema di intelligenza artificiale, permettendo di distinguerli tra dati personali e non personali.

I dati derivati non rientrano, invece, nell'ambito di applicazione del diritto alla portabilità perché non sono dati "forniti" dall'interessato, ma generati dal titolare del trattamento[7].

Una tematica complessa nel contesto dei sistemi che utilizzano l'intelligenza artificiale è quella dell'accuratezza dei dati personali ("esattezza", in base all'art. 5(1)(d) del GDPR) e del correlato diritto di rettifica dei dati inesatti vantato dagli interessati (art. 16 del GDPR). Per come funziona l'intelligenza artificiale, è difficile che l'accuratezza dei dati sia un punto di partenza. Nei sistemi di intelligenza artificiale, l'accuratezza viene più spesso con il tempo e con l'uso, man mano che i sistemi vengono utilizzati. Allora, è possibile che dati inaccurati siano naturalmente esistenti nei sistemi di intelligenza artificiale e che la loro rettifica non sia possibile. In questi casi, il diritto di ottenere che i dati inesatti siano rettificati, può trasformarsi nel diritto di vederli cancellati.

Sul tema del diritto alla cancellazione si è espresso anche l'Information Commissioner's Office britannico nella citata *Guidance on AI and data protection*, ritenendo difficile che un titolare del trattamento possa giustificare un rifiuto alla richiesta di un interessato di cancellare i propri dati personali trattati per finalità di *training* degli algoritmi. Questo anche perché la cancellazione difficilmente dovrebbe inficiare l'esito del *training*, avendo il titolare del trattamento ancora a disposizione i dati personali di altri individui da utilizzare a tale scopo.

5. La base giuridica del trattamento

Come è noto, il GDPR prevede varie basi giuridiche alternative fra loro. E per ogni trattamento va individuata quella corretta.

Nel caso di impiego di sistemi di intelligenza artificiale, le basi giuridiche astrattamente concepibili sono principalmente le seguenti.

- L'esecuzione di un contratto di cui l'interessato è parte o di misure contrattuali adottate su richiesta dell'interessato ai sensi dell'art. 6(1)(b) del GDPR. Questa base giuridica può essere, però, utilizzata solo in casi limitati. Nello specifico, è necessario che il trattamento sia oggettivamente necessario per una finalità che è parte integrante della prestazione contrattuale all'interessato e che la prestazione contrattuale non sia di fatto suscettibile di essere fornita senza lo specifico trattamento

7 Come notato, i dati immessi nei sistemi di intelligenza artificiale vengono spesso modificati per essere analizzati più efficacemente dagli algoritmi di apprendimento automatico. Se questa trasformazione è significativa, i dati risultanti possono non essere più considerati "forniti" dall'interessato e, quindi, non essere oggetto del diritto alla portabilità, pur qualificandosi ancora come dati personali e, in quanto tali, oggetto di altri diritti (come il diritto di accesso). La forma originale dei dati resta comunque soggetta al diritto alla portabilità, ricorrendone i presupposti (cioè, se il trattamento, effettuato con mezzi automatizzati, si basa sul consenso o sull'esecuzione di un contratto).

dei dati personali in questione. Quindi, ad esempio, questa base giuridica è ipotizzabile quando lo stesso servizio offerto all'utente sia caratterizzato dall'uso dell'intelligenza artificiale, come potrebbe essere un videogioco che funziona con l'intelligenza artificiale e il relativo trattamento dei dati dell'utente.

- Il legittimo interesse del titolare o di un terzo, se nel bilanciamento di interessi non prevalgono interessi, diritti e libertà degli interessati ai sensi dell'art. 6(1)(f) del GDPR. Le valutazioni circa il bilanciamento tra il legittimo interesse del titolare o del terzo e gli interessi, i diritti e le libertà degli interessati sono incluse nel cd. *legitimate interests assessment* (LIA). Tuttavia, a parere del Gruppo di lavoro Articolo 29 (nelle già citate *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*), sarebbe difficile per un titolare del trattamento giustificare il ricorso al legittimo interesse come base giuridica in caso di pratiche intrusive di profilazione e tracciamento per finalità di *marketing*, ad esempio quelle che comportano il tracciamento di persone fisiche su più siti web, ubicazioni, dispositivi, servizi o tramite l'intermediazione di dati. Vi è poi rischio di esercizio del diritto di opposizione da parte degli interessati, che, come si è detto, non deve essere nemmeno giustificato in caso di *marketing* diretto.
- Il consenso dell'interessato ai sensi dell'art. 6(1)(a) del GDPR (da cui, peraltro, non si può prescindere e che deve essere esplicito nel caso in cui vengano trattate categorie particolari di dati personali). Sul punto, l'Information Commissioner's Office, nella citata *Guidance on AI and data protection*, ha indicato che l'utilizzo del consenso come base giuridica può avere come vantaggio quello di infondere maggiore fiducia agli interessati e così avere una maggiore adesione. Il fatto di consentire agli interessati il controllo sui propri dati personali tramite il consenso può anche essere un elemento da valorizzare nella valutazione d'impatto ai sensi dell'art. 35 del GDPR. L'interessato ha però il diritto di revocarlo liberamente e in qualsiasi momento e deve essere informato di tale facoltà. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Il consenso potrebbe comunque essere impossibile da raccogliere (e quindi non essere utilizzabile come base giuridica) in alcuni casi, ad esempio con riguardo a dati raccolti non direttamente dagli interessati e utilizzati per addestrare gli algoritmi.
- Nel caso della Pubblica Amministrazione (ad esempio, nel contesto delle *smart cities*) il trattamento potrebbe essere necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento sulla base del diritto dell'Unione europea o di uno Stato membro ai sensi dell'art. 6(1)(e) del GDPR.

Nel *case study*, non risulta esservi un contratto da eseguire per cui risulti necessario il trattamento dei dati personali. Inoltre, data la quantità e varietà di

dati personali trattati mediante il sistema di intelligenza artificiale e il livello di precisione della profilazione per finalità di *marketing*, il ricorso al legittimo interesse come base giuridica potrebbe non essere corretto ed essere opportuna una richiesta di consenso agli interessati (peraltro, non è escluso che nella fattispecie descritta nel *case study* si trattino dati sensibili, ad esempio connessi alle abitudini di acquisto di medicinali).

L'utilizzo della base giuridica del consenso può comunque risultare problematico anche nel case study. Nel *case study*, gli interessati sono sia clienti del titolare del trattamento sia prospect. Possiamo immaginare che la raccolta del consenso dei clienti avvenga all'atto dell'interazione con il titolare (in particolare, nel momento in cui l'interessato diventa cliente acquistando beni o servizi dal titolare). Per i prospect, possiamo immaginare che questi siano individui i cui dati sono contenuti nelle banche dati che il titolare ha acquistato presso terzi. Allora, saranno quei terzi ad aver dovuto raccogliere il consenso degli interessati. Ma il consenso deve essere informato e può essere ben difficile immaginare che il terzo che ha creato un *database* fosse a conoscenza di come il titolare del trattamento (cessionario) avrebbe trattato i dati per mezzo del sistema di intelligenza artificiale e che, dunque, possa aver fornito un'informativa completa agli interessati.

6. Il divieto di decisioni basate unicamente su un trattamento automatizzato

L'art. 22 del GDPR prevede che l'interessato abbia il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Questa decisione è però consentita se è necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare, è autorizzata dalla legge o se si basa sul consenso esplicito dell'interessato. Il titolare deve poi attuare misure appropriate per tutelare i diritti degli interessati, tra cui almeno consentire agli interessati di ottenere l'intervento umano nel processo trattamento, di esprimere la propria opinione e di contestare la decisione.

Nella fattispecie di cui al *case study*, il divieto di cui all'art. 22 del GDPR potrebbe applicarsi se si conclude che le decisioni del sistema di intelligenza artificiale incidono significativamente sugli interessati.

Invero, a seconda, fra l'altro, dell'invasività della profilazione, delle aspettative degli interessati e dello sfruttamento della conoscenza di vulnerabilità degli interessati, si potrebbe rientrare nell'ambito di applicazione dell'art. 22 del GDPR ove, ad esempio, la decisione automatizzata abbia l'effetto di discriminare alcuni interessati escludendo di fatto il loro accesso a determinate offerte commerciali a cui potrebbero avere interesse.

Sul punto, l'Information Commissioner's Office, nella citata *Guidance on AI and data protection*, ha suggerito di verificare: (i) se il sistema di intelligenza artificiale interagisce con eventuali revisori umani; (ii) le tipologie di decisioni auto-

matizzate che il *design* del sistema di intelligenza artificiale permette o impedisce; (iii) il collegamento tra gli *output* del sistema di intelligenza artificiale e gli effettivi impatti che questi possono avere sugli individui; e (iv) i processi umani che il sistema di intelligenza artificiale mira a sostituire.

Il divieto di cui all'art. 22 del GDPR non si applicherebbe in caso di consenso esplicito degli interessati. Resta comunque il diritto di ottenere l'intervento umano (che potrebbe essere complesso da gestire nel funzionamento del sistema di intelligenza artificiale) e di contestare la decisione.

Affinché gli interessati possano efficacemente contestare la decisione è fondamentale che il titolare del trattamento assicuri la trasparenza e la comprensibilità del funzionamento del sistema di intelligenza artificiale, come è stato ribadito anche dall'Information Commissioner's Office nella citata *Guidance on AI and data protection*.

L'ultimo comma dell'art 22 del GDPR prevede poi il divieto di basare le decisioni automatizzate sul trattamento di categorie particolari di dati personali *ex* art. 9 del GDPR, ad esempio i dati sanitari. Questo salvo il consenso esplicito dell'interessato. Nel *case study* che stiamo commentando non si menziona il trattamento di dati sensibili ma, come si è detto, non può escludersi questa casistica, ad esempio se prodotti acquistati su cui si basa la profilazione siano medicinali o servizi profilati siano prestazioni mediche.

7. L'individuazione delle misure di sicurezza

Seguendo l'approccio alla sicurezza che è stato introdotto dal GDPR, nel caso in cui il sistema di AI preveda anche il trattamento di dati personali (quindi quasi sempre di fatto, considerato che è molto difficile che sia possibile escluderlo), le misure che devono essere implementate – sia dal titolare che dal responsabile – devono essere quelle adeguate rispetto ai possibili rischi, per proteggere in modo effettivo i dati da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Alcuni dei rischi collegati all'AI sono del tutto peculiari, in alcuni casi assimilabili considerando le diverse categorie di dati che tipicamente entrano in gioco in un algoritmo:

- **Dati di input**: se i dati immessi sono incompleti o sbagliati lo sarà anche l'*output* (in gergo informatico si usa l'acronimo GIGO, "*garbabe in, garbage out*");
- **Dati per il training**: se un terzo interroga le macchine predittive di un altro soggetto potrebbe effettuare un'operazione di *reverse engineering* dell'algoritmo o utilizzare i dati di *output* dell'algoritmo come dati di *training* per le sue macchine;
- **Dati di feedback**: malintenzionati possono inserire nell'AI dati che snaturano il processo di apprendimento, insegnando alla macchina a fornire previsioni sbagliate.

Non esiste quindi un approccio *standard* alla sicurezza. Occorre chiedersi, quindi, cosa possa differenziare la AI da tecnologie più tradizionali. Dal punto di vista tecnologico, i sistemi di intelligenza artificiale presentano elementi di complessità che obiettivamente non sono presenti nei sistemi a cui siamo abituati da più tempo. L'utilizzo di sistemi di AI, inoltre, prevede quasi sempre il coinvolgimento di fornitori e la necessità di integrare i sistemi con componenti IT ulteriori: da ciò deriva una maggiore difficoltà nel definire un insieme di misure che, nel complesso, risulti adeguata.

L'impatto dell'AI sulla sicurezza dipende anche:

- dal modo in cui la tecnologia è costruita e usata;
- dalla complessità dell'organizzazione che la usa; e
- dalla natura, dallo scopo, dal contesto del trattamento e dai rischi che, in concreto, possono quindi esistere per gli interessati.

Anche i volumi contano: si pensi al caso ChatGPT, 100 milioni di utenti attivi a soli due mesi dal lancio. Non deve quindi stupire l'attenzione da parte delle Autorità di controllo *privacy*, *in primis* il nostro Garante, anche rispetto ai profili di sicurezza di questi sistemi, vista la loro enorme diffusione.

Considerate queste premesse, sarebbe un'impresa ardua ipotizzare, seppure a livello esemplificativo, un elenco di misure di sicurezza potenzialmente idonee rispetto al contesto in esame. Una ricognizione su questi temi è stata però già effettuata da alcune Autorità di controllo privacy. Recentemente anche l'ENISA – l'Agenzia dell'UE per la cibersicurezza – ha pubblicato un report in materia (*Cybersecurity of AI and standardisation*) nel quale ha osservato che l'AI Act, allo stato, non disciplina adeguatamente gli aspetti di sicurezza informatica.

Si riportano di seguito alcuni spunti dell'ICO e della CNIL ritenuti significativi.

L'Autorità inglese (nel proprio documento intitolato *How to use AI and personal data appropriately and lawfully*) raccomanda, a livello metodologico, di:

- effettuare una valutazione del rischio di sicurezza, che includa un inventario aggiornato dei sistemi di IA per ottenere una visione di base rispetto a "dove" potrebbero verificarsi possibili incidenti;
- far svolgere periodicamente il debug del modello - ossia il processo di individuazione e correzione dei problemi - sia a un dipendente della società che a un consulente esterno;
- monitorare costantemente il sistema di AI così da poter individuare subito eventuali anomalie.

L'omologo francese del Garante, invece, nella propria *checklist* in materia di AI (schede pratiche rivolte a imprese e professionisti) suggerisce di verificare, tra altri, anche i seguenti punti:

- includere nell'analisi dei rischi anche gli specifici attacchi che possono essere rivolti agli algoritmi (tra cui avvelenamento dei dati, attacchi avversari, evasione del modello e inferenza di appartenenza);
- prevedere un sistema di analisi dei log che consenta di identificare possibili attacchi come l'inferenza di appartenenza o l'avvelenamento del modello (soprattutto in caso di apprendimento continuo);
- prevedere un sistema di controllo degli accessi, per limitare le possibili modifiche al sistema di AI;
- adottare soluzioni per garantire *business continuity* e *disaster recovery*;
- svolgere *audit*;
- adottare un sistema per la gestione del rischio.

In aggiunta a queste, considerando le *best practice* in materia per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei trattamenti, è possibile considerare, tra molte altre, anche le seguenti ulteriori misure:

i) organizzative

- definire in modo chiaro i ruoli, i compiti e le responsabilità in materia di protezione dei dati all'interno dell'organizzazione, mediante la definizione di un funzionigramma *privacy* che garantisca una *governance* dei dati efficace;
- predisporre *policy*, procedure e regolamenti relativamente alla protezione dei dati e verificare che questi documenti siano correttamente implementati a livello di processi;
- sottoporre i fornitori a verifiche prima della conclusione del contratto e durante la vigenza del rapporto;
- svolgere periodicamente sessioni di formazione in materia di *privacy*, *data protection* e *cybersecurity* rivolte sia ai dipendenti che ai *manager*;
- mappare i rischi specifici collegati all'AI (come l'inaccuratezza dei dati o i possibili "*bias*"), tenerli monitorati e gestirli, anche mediante lo svolgimento di DPIA;

ii) tecniche

- dare attuazione pratica al principio di *data minimisation*, affinché vengano trattati solo i dati necessari;
- implementare efficaci meccanismi di *opt-out*, affinché sia garantito il diritto di opposizione al trattamento (l'esperienza di ChatGPT insegna);
- laddove possibile anonimizzare i dati, ovvero pseudonimizzarli;
- implementare *Privacy Enhancing Technologies* (PET), come ad esempio l'aggiunta di "rumore" ai dati (mantenendo solo risultati statistici) o la creazione e l'uso nei modelli predittivi di dati cd. sintetici (quindi non personali).

8. Anonimizzazione e pseudonimizzazione

Come si è già detto, l'ambito di applicazione del GDPR è limitato ai trattamenti di dati personali, ossia di "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*", facendo riferimento alla possibilità di identificare il soggetto sia direttamente che indirettamente.

Ne rimangono quindi esclusi i dati cd. anonimi, qualificabili come tali soltanto qualora sia impedita in maniera irreversibile l'identificazione dell'interessato.

Da tenere ben distinto è invece il concetto di pseudonimizzazione, con il quale si fa riferimento al "*trattamento dei dati personali in modo tale che non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive*", posto che tali informazioni siano soggette a specifiche misure di sicurezza (Art. 4, no. 5 GDPR).

In altre parole, la pseudonimizzazione si configura come una misura utile a ridurre i possibili rischi per i diritti e le libertà degli interessati correlati al trattamento dei dati personali, ma non esclude l'applicazione della disciplina del GDPR, dal momento che i dati continuano a poter essere qualificati come dati personali. Il titolare del trattamento sarà dunque soggetto, in ogni caso, agli obblighi previsti dalla normativa.

La distinzione fra anonimizzazione e pseudonimizzazione è dunque di cruciale importanza e verte intorno al concetto di identificabilità del soggetto, inteso come la possibilità di ricondurre il dato ad uno specifico interessato.

Secondo quanto affermato dall'Art. 29 Working Party nel Parere 05/2014 sulle tecniche di anonimizzazione, si ha infatti identificazione del soggetto in tre diverse ipotesi. In particolare, quando:

a) Attraverso i dati è possibile **individuare** un soggetto;

b) È possibile **collegare** fra loro i dati riferiti al medesimo soggetto;

c) Informazioni riguardanti un soggetto possono essere **dedotte** a partire dai dati.

Sul tema dell'identificabilità e, dunque, sulla possibilità di qualificare un dato come dato personale in ragione dell'efficacia delle tecniche di anonimizzazione, si è peraltro espresso di recente il Tribunale dell'Unione Europea nella causa T-557/20, richiamando i principi già affermati dalla Corte di Giustizia dell'Unione Europea ("**CGUE**") nella nota sentenza Breyer (C-582/14).

Nella pronuncia in esame, infatti, il Tribunale ha ribadito la necessità di tenere conto della possibilità di utilizzare in concreto le informazioni aggiuntive in grado di consentire la re-identificazione del soggetto, al fine di valutare se possa parlarsi di anonimizzazione del dato o semplice pseudonimizzazione. Pur dovendo tenere conto delle peculiarità del caso di specie, il principio sancito dal Tribunale assume rilevanza anche nel contesto dei sistemi di intelligenza

artificiale, nei quali la possibilità di re-identificazione in concreto è senz'altro maggiore.

Non a caso, all'interno del già citato parere dell'Art. 29 Working Party, si evidenzia infatti subito la difficoltà di stabilire con certezza e in maniera definitiva quali tecniche garantiscano l'effettiva anonimizzazione del dato, dal momento che l'efficacia delle stesse va in ogni caso correlata al livello di sviluppo tecnologico e al contesto specifico del trattamento. Non rileva, inoltre, quali siano le intenzioni del titolare o del responsabile del trattamento, ma soltanto che, sulla base della tecnologia disponibile, l'identificazione del soggetto sia possibile.

L'applicazione di questi principi nell'ambito dell'utilizzo di sistemi AI - e dunque del Tool - pone tuttavia non pochi problemi, in primo luogo legati al fatto che, come si è già avuto modo di chiarire, questo implichi utilizzo dei cosiddetti *big data*. Da un lato, infatti, è possibile che certi dati, irrilevanti se osservati singolarmente, assumano un significato diverso se correlati ad altri. Dall'altro, è ben possibile che siano gli algoritmi stessi, sulla base dell'esperienza e dell'analisi continua dei dati, ad attribuire a questi ultimi un significato diverso, giungendo a conclusioni inizialmente neanche prevedibili e secondo meccanismi a volte difficili da comprendere per gli stessi sviluppatori.

Queste considerazioni hanno portato alcuni esperti a ritenere addirittura che non sia più possibile distinguere in maniera netta fra dati personali e dati non personali, né che possano ritenersi efficaci le tecniche di anonimizzazione normalmente adottate. Questo approccio, criticato perché condurrebbe ad un'eccessiva estensione dell'ambito di applicazione della disciplina sulla protezione dei dati personali, è comunque utile ad evidenziare la rilevanza dei rischi connessi all'utilizzo dei sistemi AI e la necessità di adottare un approccio precauzionale che, anche alla luce del generale principio di *accountability*, impone il ricorso a strumenti quali ad esempio la DPIA al fine di garantire una corretta valutazione del rischio e l'individuazione di misure di sicurezza idonee.

È comunque il caso di ribadire qui che, come evidenziato anche dallo EPRS, il ricorso a tecniche di anonimizzazione e pseudonimizzazione è comunque considerato un ottimo strumento in grado di assicurare la sicurezza del trattamento, in ossequio ai principi di cui agli artt. 5, 25 e 32 del GDPR.

Alla luce di quanto sopra, anche al fine di promuovere lo sviluppo di sistemi di intelligenza artificiale in grado di ottenere la fiducia dei consumatori e la piena *compliance* con la disciplina, la Società dovrebbe fare ricorso a tali tecniche, selezionando le più adeguate sulla base della preventiva valutazione dei rischi (emersi anche in fase di DPIA), pur tenendo presente che l'utilizzo dell'AI rende difficile, se non addirittura impossibile, poter escludere con assoluta certezza e in maniera irreversibile l'applicazione della disciplina sulla protezione dei dati.

CAPITOLO 2 di Simona Custer, Giacomo Gori
e Mariangela Papadia

Trasferimento dati extra UE, Cookie e Google Analytics: implicazioni e rischi

SOMMARIO: 1. Trasferimento dati extra UE – 1.1 Il concetto di "trasferimento internazionale di dati personali": i criteri che consentono di qualificare un trattamento come "trasferimento" – 1.2 Come trasferire i dati all'estero senza violare il GDPR: le misure che garantiscono la protezione dei dati personali – 1.3 Le deroghe previste dal GDPR nel caso di impossibilità di applicazione degli strumenti per il trasferimento – 2. Cookie: quali sono e come gestirli nel rispetto della normativa vigente – 2.1 La normativa applicabile – 2.2 Che cosa sono e come vengono qualificati – 2.3 Accorgimenti privacy da realizzare per gestire al meglio i cookie – 3. Google Analytics e trasferimenti dati tra UE e USA – 3.1 Il blocco all'utilizzo di Google Analytics e l'indirizzo IP come dato personale – 3.2 Trasferimenti dati tra UE e USA: verso il nuovo Framework

1. Trasferimento dati extra UE

1.1 Il concetto di "trasferimento internazionale di dati personali": i criteri che consentono di qualificare un trattamento come "trasferimento"

Il Regolamento europeo in materia di protezione dei dati personali (il Regolamento UE 2016/679, "**Regolamento**" o "**GDPR**") disciplina il trasferimento di dati personali al di fuori dello Spazio Economico Europeo (il '**SEE**' ovvero l'Unione Europea più Norvegia, Liechtenstein e Islanda). La regolamentazione sui flussi transfrontalieri dei dati personali è collocata al Capo V del GDPR, all'interno del quale, tuttavia, non esiste una definizione di "trasferimento di dati". Ed è in tale contesto che si inseriscono le Linee guida 05/2021 del 14 febbraio 2023[8] adottate dal Comitato Europeo per la Protezione dei Dati (European Data Protection Board, l'"**EDPB**"): l'obiettivo delle citate guidelines è proprio quello di chiarire quali trasferimenti internazionali di dati rientrino nell'ambito di applicazione del Capo V del GDPR.

Il documento ha introdotto tre criteri cumulativi per poter definire un 'trasferimento di dati':

8 Il testo integrale delle Linee guida 5/2021 dell'EDPB del 14 febbraio 2023 è consultabile al seguente link: *https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf*.

1. il titolare o il responsabile del trattamento, in qualità di esportatore di dati, è soggetto al GDPR;
2. l'esportatore di dati trasmette o rende comunque disponibili i dati personali ad altro titolare, contitolare o responsabile del trattamento, in qualità di importatore di dati;
3. l'importatore di dati si trova in un paese terzo o è un'organizzazione internazionale.

In relazione alla condizione di cui al punto **1.**, l'EDPB ricorda che anche titolari e responsabili non stabiliti in Unione Europea possono comunque rientrare nel campo di applicazione del GDPR (cfr. art. 3, par. 2, del Regolamento[9]): in tal caso, tali titolari o responsabili saranno tenuti a soddisfare i requisiti del Capo V quando si accingono a trasferire i dati personali ad un destinatario stabilito in un paese terzo.

Quanto alla condizione di cui al punto **2.**, l'EDPB fa presente che la nozione di "*trasferimento di dati personali presso un paese terzo o un'organizzazione internazionale*" si applica solo alle comunicazioni di dati personali nelle quali sono coinvolti due soggetti separati (siano essi titolari, contitolari o responsabili). Quindi, precisa sempre l'EDPB, nel caso di gruppi di imprese, i flussi di dati diventano "trasferimento" nella misura in cui le operazioni sui i dati siano eseguite tra due organizzazioni distinte (titolari o responsabili). Del pari, non potrà aversi "trasferimento" quando i dati sono comunicati o messi a disposizione dell'impresa stabilita extra UE direttamente da parte di un interessato.

Rispetto alla condizione di cui al punto **3.**, è fondamentale che l'importatore - ovvero il destinatario dei dati - sia collocato al di fuori dell'UE, indipendentemente dal fatto che esso sia o meno soggetto al GDPR.

Nel caso in cui i tre requisiti sopra esposti siano soddisfatti, potrà affermarsi che sussiste un "trasferimento presso un paese terzi o un'organizzazione internazionale". Di conseguenza, il titolare o il responsabile del trattamento dovranno rispettare le condizioni poste dal Capo V del GDPR ed utilizzare gli strumenti ivi previsti, che mirano a tutelare i dati personali a fronte del trasferimento dati extra UE.

1.2 Come trasferire i dati all'estero senza violare il GDPR: le misure che garantiscono la protezione dei dati personali

Come anticipato, il trasferimento dati al di fuori del SEE è consentito solo a determinate condizioni, in assenza delle quali esso è vietato.

9 Recita l'art. 3, par. 2, del Regolamento: "2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

Anzitutto, il trasferimento di dati extra SEE è consentito se il paese terzo garantisce un livello di protezione dei dati adeguato a quello europeo, laddove il livello di protezione è riconosciuto dalla Commissione europea tramite l'emissione di una decisione di "adeguatezza" di cui all'art. 45 del Regolamento.

In assenza di tale decisione, l'art. 46 del Regolamento regola l'ipotesi di trasferimenti verso paesi terzi non adeguati, prescrivendo che "*il titolare o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale se ha fornito garanzie adeguate*" che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati.

A tal riguardo, la norma offre un elenco dettagliato e completo delle 'garanzie adeguate' tra le quali si annoverano:

- le norme vincolanti d'impresa (o *Binding corporate rules*);
- le clausole tipo (o *Standard Contractual Clauses*);
- i codici di condotta;
- i meccanismi di certificazione.

In assenza di una decisione di adeguatezza o di garanzie adeguate, il trasferimento dati personali verso un paese terzo può comunque avere luogo in presenza di una delle deroghe previste dall'art. 49 del Regolamento (ma sul punto si veda *infra*).

Le Decisioni di adeguatezza - art. 45 GDPR

In termini generali, un paese terzo può chiedere alla Commissione europea di esaminare la propria legislazione al fine di ottenere una decisione di adeguatezza. La Commissione, valutati gli elementi indicati nell'art. 45 del Regolamento[10], può stabilire che il paese terzo o l'organizzazione internazionale garantiscono un livello di protezione adeguato, ammettendo così la possibilità di trasferirvi dati personali. Diversi paesi hanno ottenuto il riconoscimento di "adeguatezza" dalla Commissione, per citarne alcuni l'Argentina, il Canada, Israele, la Nuova Zelanda, l'Uruguay e da ultimo il Giappone e la Corea del Sud.

Le decisioni di adeguatezza possono essere modificate, sospese o revocate, laddove emerga che il paese terzo non sia più in grado di soddisfare i criteri necessari e, conseguentemente, di garantire un livello di protezione adeguato[11].

10 Ai sensi dell'art. 45 del GDPR, nel valutare l'adeguatezza, la Commissione è tenuta a prendere in considerazione diversi aspetti: le norme in materia di dati personali, le misure di sicurezza osservate, i diritti azionabili dagli interessati, l'esistenza e l'effettivo funzionamento di autorità di controllo indipendenti che garantiscano il rispetto della normativa sulla protezione dei dati.

11 È quanto avvenuto con riferimento ai trasferimenti dati Europa-USA: la Corte di Giustizia europea, con sentenza del 16 luglio 2020, ha invalidato la decisione di adeguatezza adottata dalla Commissione nell'agosto 2016, il cosiddetto *Privacy Shield*. Di conseguenza, venendo meno il *Privacy Shield,* qualsivoglia trasferimento dati personali negli Usa dovrà basarsi sugli altri strumenti messi a disposizione dalla normativa. Si segnala che il *Privacy Shield* è stato adottato nel 2016 dalla Commissione europea in seguito alla decadenza dell'accordo *Safe Harbor*, anch'esso invalidato dalla Corte di Giustizia europea con sentenza del 6 ottobre 2015.

Le norme vincolanti d'impresa (o *Binding corporate rules*) - art. 47 GDPR

Le norme vincolanti d'impresa (o *Binding corporate rules* - "**BCR**") disciplinate all'art. 47 del Regolamento - sono uno specifico strumento volto a consentire il trasferimento dei dati personali verso paesi terzi tra società facenti parti dello stesso gruppo d'impresa, laddove una di queste si trovi al di fuori dell'Unione Europea. In particolare, le BCR si concretizzano in "*un documento contenente una serie di clausole (rules) che fissano i principi vincolanti (binding) […] al cui rispetto sono tenute tutte le entità (che agiscono in qualità di controller o di processor) appartenenti ad uno stesso gruppo (corporate)*"[12].

Sono disponibili due modelli di riferimento che differiscono in base al ruolo che rivestono le entità - titolare o responsabile - che esportano ed importano i dati all'interno del gruppo: le BCR for Controller e le BCR for Processor[13].

Quanto al contenuto, sarà necessario far riferimento (i) all'applicazione dei principi di protezione dei dati, quali quelli sulla finalità, minimizzazione e proporzionalità dei dati, (ii) ai diritti dell'interessato, ivi incluso il diritto ad ottenere il risarcimento del danno connesso al mancato rispetto delle BCR da parte di una società del gruppo (c.d. clausola del terzo beneficiario), (iii) alle modalità in base alle quali viene rilasciata idonea informativa all'interessato, (iv) alle misure di sicurezza adottate.

Inoltre, sempre a garanzia della legittimità del trasferimento internazionale di dati, è fondamentale che il gruppo multinazionale provveda a (a) predisporre un programma di formazione del personale in materia di protezione dei dati personali; (b) condurre audit periodici al fine di verificare il rispetto delle BCR da parte del gruppo; (c) implementare meccanismi / procedure volte a monitorare il rispetto delle BCR e a gestire le segnalazioni degli interessati.

Clausole tipo o *Standard Contractual Clauses* - art. 46, par. 2, lett. c) e lett. d), GDPR

Le clausole contrattuali tipo (o *Standard Contractual Clauses* - "**SCC**") sono previsioni *standard* adottate dalla Commissione europea, tramite decisione, che trovano applicazione in caso di trasferimento dati da un titolare o responsabile del trattamento stabilito nell'Unione ad un titolare o responsabile del trattamento stabilito in un paese terzo per conformarsi alle prescrizioni del Regolamento. Le SCC, che riguardano esclusivamente la protezione dei dati, potranno essere incluse dalle parti negli accordi contrattuali, garantendo che i dati saranno trattati conformemente alle disposizioni del Regolamento anche nel paese terzo o all'interno dell'organizzazione di destinazione.

12 Cfr. pagina web del sito del Garante per la protezione dei dati personali sul trasferimento dati all'estero: https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero

13 Per maggiori informazioni sui contenuti delle BCR, si rinvia ai seguenti documenti emessi dal Gruppo Art. 29 (o *Article 29 Working Party*, "**WP29**", autorità sostituita dall'EDPB a partire dal 25 maggio 2018 ai sensi del GDPR):
- Wp 256 - Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules - in caso di BCR for controller
- Wp 257 - Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules - in caso di BCR for processor

In termini generali, le clausole tipo elaborate dalla Commissione non possono essere modificate; tuttavia è possibile integrarne il testo con ulteriori previsioni, purché queste non siano in contrasto con quanto previsto dalle stesse SCC.

Il 4 giugno 2021, la Commissione europea, con decisione n. 2021/914/UE[14], ha adottato nuove SCC, abrogando, a far data dal 27 settembre 2021, le precedenti decisioni in materia[15] e prevedendo un periodo di transizione di 18 mesi (fino al **27 dicembre 2022**) per passare dalle vecchie SCC alle nuove.

Le nuove SCC coprono una più ampia gamma di scenari di trasferimento che possono innescarsi tra i diversi attori privacy e impongono alle parti coinvolte una concreta valutazione del trasferimento dei dati personali in termini di valutazione del rischio e dell'impatto del trasferimento (*Transfer Impact Assessment* – "**TIA**") che coinvolga anche l'esame, sotto il profilo privacy, della legislazione e delle prassi del paese terzo di destinazione. In altri termini, ai sensi della clausola 14 delle SCC, le parti devono assicurare "*di non avere motivo di ritenere che la legislazione e le prassi del paese terzo di destinazione applicabili al trattamento dei dati personali da parte dell'importatore, […], impediscono all'importatore di rispettare gli obblighi che gli incombono a norma delle presenti clausole*" al fine di garantire la tutela adeguata dei dati. A tal fine, le circostanze da prendere in considerazione sono:

- gli elementi specifici del trasferimento (che includono la lunghezza della catena di fornitura, il numero di soggetti coinvolti nel trasferimento; eventuali trasferimenti successivi; finalità del trattamento; categorie e formato di dati personali trasferiti; luogo di conservazione dei dati);
- l'esistenza di leggi e prassi del paese terzo (ivi incluse quelle che impongono la comunicazione di dati alle autorità pubbliche o che le autorizzano ad accedere ai dati) "*pertinenti alla luce delle circostanze specifiche del trasferimento, nonché le limitazioni e le garanzie applicabili*";
- garanzie contrattuali, tecniche o organizzative eventualmente messe in atto per integrare le garanzie delle SCC.

Inoltre, ai sensi della clausola 14 lett. d) delle SCC, le parti sono soggette all'obbligo di documentare il processo di valutazione d'impatto del trasferimento e di metterla a disposizione dell'autorità di controllo competente su richiesta.

14 Il testo integrale della Decisione della Commissione europea del 4 giugno 2021 (2021/914/UE) è consultabile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32021D0914.

15 Si trattava delle Decisioni della Commissione europea del 15 giugno 2001 (2001/497/CE) e del 5 febbraio 2010 (2010/87/UE).

Codici di condotta e meccanismi di certificazione - art. 46, lett. e) e lett. d), GDPR

I codici di condotta prevedono la possibilità per associazioni e altri organismi di categoria di titolari o responsabili del trattamento di elaborare "codici di condotta" in materia di privacy, approvati dall'autorità di controllo.

Una volta approvati, i codici di condotta potranno essere utilizzati da titolari e responsabili ubicati al di fuori dell'Unione Europea purché vi sia un «*impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati*» (art. 46, par.2, lett. e) del Regolamento)[16].

Il 4 marzo 2022 l'EDPB ha annunciato di aver adottato le Linee guida 04/2021[17] sui codici di condotta come strumenti per i trasferimenti di dati all'estero ai sensi del Regolamento, a completamento ed integrazione di quanto già prescritto dalle precedenti Linee guida 01/2019[18]. L'obiettivo delle Linee guida del 2021 è quello di "*fornire una guida pratica* [su] *contenuto di tali codici di condotta, il loro processo di adozione e i soggetti coinvolti, nonché* [sui] *requisiti che un codice di condotta per i trasferimenti deve soddisfare e le garanzie che deve fornire*" al fine di poter essere ritenuto valido ai sensi dell'art. 46 del Regolamento (Linee guida 04/2021, p. 5).

L'oggetto principale del codice di condotta finalizzato ai trasferimenti internazionali si identifica con l'insieme delle norme e dei comportamenti cui dovrà conformarsi l'importatore dei dati per garantire un livello adeguato di protezione dei dati personali, una volta trasferiti nel paese terzo. Inoltre, l'EDPB offre un dettagliato elenco degli elementi che un codice di condotta dovrebbe includere per essere utilizzato come strumento per il trasferimento dati extra UE che, in sintesi, hanno ad oggetto:

- principi essenziali, diritti e obblighi per l'importatore dei dati in linea con quanto previsto dal Regolamento; e
- garanzie specifiche rispetto ai trasferimenti (ad esempio in relazione alla "*questione dei trasferimenti successivi o [al]l'esistenza di legislazione confliggente nel paese terzo*" - Linee guida 04/2021, p. 8).

16 Ai sensi dell'art. 40, par. 3, del Regolamento, ai fini dell'adesione ad un codice di condotta da parte di un soggetto extra-UE, deve sussistere, non solo la volontà del *data importer* ad aderire al codice, ma anche un "*impegno vincolante e azionabile*" al rispetto degli obblighi previsti dal codice di condotta, da provarsi attraverso "*strumenti contrattuali o di altro tipo giuridicamente vincolanti*". In base alle Linee guida 4/2021, tali strumenti possono identificarsi anche con soluzioni diverse dal mero contratto, "*purché i titolari/responsabili del trattamento che aderiscono al codice siano in grado di dimostrare il carattere vincolante e azionabile di tali diversi strumenti*" (cfr. Linee guida dell'EDPB 4/2021).

17 Il testo integrale delle Linee guida 4/2021 dell'EDPB del 22 febbraio 2022 è consultabile al seguente link: https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_it.pdf.

18 Il testo integrale delle Linee guida 1/2019 dell'EDPB del 4 giugno 2019 è consultabile al seguente link:https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_it.pdf

Quindi, affinché un codice di condotta venga utilizzato come *transfer tool* è fondamentale che quest'ultimo disciplini in maniera completa ed esaustiva il tema dei trasferimenti di dati personali.

I meccanismi di certificazione di cui all'art. 46, para 2, lett. f), del Regolamento consentono a titolari e responsabili del trattamento di dimostrare l'adozione di garanzie appropriate nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali. Su tale tema, il 14 febbraio 2023 l'EDPB ha emesso le Linee guida 07/2022[19] con le quali vengono forniti chiarimenti in relazione all'utilizzo pratico delle certificazioni come strumento per i trasferimenti all'estero.

Le Linee guida individuano gli elementi che dovrebbero essere inclusi in un meccanismo di certificazione per utilizzarlo come strumento per i trasferimenti verso paesi terzi, elementi che necessitano di essere di essere '*tailorizzati*' rispetto alle attività di trattamento oggetto della certificazione.

Come per i codici di condotta, anche in questo caso il *data importer* è tenuto a manifestare un "*impegno vincolante ed esigibile* [...] *ad applicare le garanzie adeguate*" (cfr. art. 46, par. 2, lett. f), del Regolamento). Sul punto, specifica l'EDPB che "*il contratto o altro strumento deve stabilire che il titolare del trattamento/responsabile del trattamento in possesso di una certificazione che agisce in qualità di importatore si impegna a rispettare le norme specificate nella certificazione destinata ai trasferimenti durante il trattamento dei dati pertinenti ricevuti dal SEE e garantisce di non avere motivo di ritenere che le leggi e le pratiche nel paese terzo applicabili al trattamento siano adottate, compresi eventuali obblighi di divulgazione di dati personali o misure che autorizzano l'accesso da parte delle autorità pubbliche, impedire che essa rispetti gli impegni assunti nell'ambito della certificazione e che informi l'esportatore di eventuali modifiche pertinenti della legislazione o della prassi al riguardo*" (Linee guida 7/2022, p. 17).

1.3 Le deroghe previste dal GDPR nel caso di impossibilità di applicazione degli strumenti per il trasferimento

In mancanza di decisioni di adeguatezza ex art. 45 del Regolamento o di una delle garanzie adeguate ex art. 46 del Regolamento, il trasferimento è possibile sulla base delle deroghe elencate all'art. 49 ovvero, a titolo esemplificativo:

- il consenso dell'interessato, previa adeguata informativa anche sui possibili rischi del trasferimento;
- per dare esecuzione ad un contratto di cui l'interessato è parte;
- per accertare, esercitare o difendere un diritto in sede giudiziaria;
- per il perseguimento di interessi legittimi cogenti dell'esportatore dei dati, purché il trasferimento non sia ripetitivo e riguardi un numero limitato di interessati e a condizione che "*il titolare del trattamento*

19 Il testo integrale delle Linee guida 7/2022 dell'EDPB del 14 febbraio 2023 è consultabile al seguente link: https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf

abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali", informando del trasferimento l'autorità di controllo.

Il ricorso alle deroghe deve avere carattere "eccezionale". Infatti, l'EDPB, in occasione delle Linee guida n. 2/2018 adottate il 25 maggio 2018[20] sulla corretta applicazione delle deroghe di cui all'art. 49 del Regolamento, ha offerto un'interpretazione particolarmente restrittiva della norma: infatti, secondo l'EDPB, gli strumenti previsti dall'art. 49 del Regolamento possono essere utilizzate solo nel caso di trasferimenti necessari, occasionali e non ripetitivi: "*i trasferimenti possono ripetersi ma non con cadenza regolare e devono avvenire in circostanze non ordinarie, ad esempio al manifestarsi di condizioni casuali o ignote e a intervalli di tempo arbitrari*" (Linee guida 2/2022, pp. 4 e 5).

Va da sé che il trasferimento andrà evitato - perché illecito - nell'ipotesi in cui neppure le deroghe trovino applicazione. A tal proposito, va segnalato che la sanzione in caso di illecito trasferimento di dati all'estero va fino a 20 milioni di euro o al 4% del fatturato annuo.

2. *Cookie*: quali sono e come gestirli nel rispetto della normativa vigente

2.1 La normativa applicabile

I *cookie* trovano una loro precisa disciplina all'interno del provvedimento del 10 giugno 2021 n. 231 "*Linee Guida cookie e altri strumenti di tracciamento*" emanato dal Garante per la protezione dei dati personali, che ha sostituito e mandato in pensione il provvedimento del 08 maggio 2014 n. 229 "*Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*", ormai datato e basato su un quadro normativo non più attuale.

Infatti, le novità introdotte dal GDPR e dalle Linee guida dell'EDPB, da un lato, e le prassi rilevate dal Garante nel corso dello svolgimento delle sue attività e le indicazioni emerse in sede di consultazione pubblica, dall'altro, hanno reso più che mai necessaria la pubblicazione del nuovo provvedimento.

Ciò, soprattutto al fine di fornire agli addetti ai lavori uno strumento più contemporaneo, che tenga conto oltre che del nuovo quadro normativo anche dell'evoluzione tecnologica verificatasi negli ultimi anni.

2.2 Cosa sono e come vengono qualificati

Come noto, i *cookie* non sono altro che piccole stringhe di testo che i siti web visitati dall'utente archiviano all'interno del dispositivo terminale[21] uti-

20 Il testo integrale delle Linee guida 2/2018 dell'EDPB del 25 maggio 2018 è consultabile al seguente link:https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf

21 Per terminale si intende, ad esempio, un computer, un tablet, uno smartphone, ovvero ogni altro

lizzato per la navigazione e che possono contenere una serie di informazioni - di natura personale o meno - sull'utente stesso, tra cui l'indirizzo IP, il nome utente, l'identificativo univoco o l'indirizzo e-mail, le preferenze espresse, le impostazioni della lingua o le informazioni sul tipo di dispositivo utilizzato per la navigazione.

Considerata la tipologia e la varietà di informazioni raccolte, è evidente che l'utilizzo dei *cookie* possa consentire lo svolgimento di importati e differenti attività e funzioni. Se da un lato, infatti, possono favorire il caricamento più veloce delle pagine dei siti web e l'indirizzamento delle informazioni su una rete così da garantire l'operatività dei siti web, dall'altro possono addirittura veicolare la pubblicità comportamentale (c.d. *behavioural advertising*) e misurare l'efficacia del messaggio pubblicitario, ovvero adeguare la tipologia e le modalità dei servizi resi ai comportamenti dell'utente oggetto di precedente osservazione.

A seconda, quindi, delle singole caratteristiche è possibile configurare varie tipologie di cookie; i cookie, infatti, possono distinguersi non solo in considerazione delle finalità perseguite, ma anche sulla base della loro durata (di sessione o permanenti) e a seconda che il publisher agisca autonomamente (prima parte) o per conto di altre parti (terze parti).

Nonostante ciò, nelle proprie Linee guida il Garante decide di soffermarsi e di approfondire unicamente la classificazione per finalità, senza nulla prevedere rispetto alla classificazione per durata e per publisher. Nello specifico, il Garante prevede e descrive due macrocategorie:

- i ***cookie tecnici*** utilizzati per "*effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio*[22]". In altre parole, sono quei cookie essenziali e necessari al funzionamento del sito web;
- i ***cookie di profilazione*** utilizzati per "*ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (pattern) al fine del raggruppamento dei diversi profili all'interno di cluster omogenei di diversa ampiezza, in modo che sia possibile al titolare, tra l'altro, anche modulare la fornitura del servizio in modo sempre più personalizzato al di là di quanto strettamente necessario all'erogazione del servizio, nonché inviare messaggi pubblicitari mirati, cioè in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete*[23]". In altre parole, sono quei cookie che permettono il tracciamento del comportamento degli utenti, così da creare dei profili per formulare annunci basati sul marketing comportamentale.

dispositivo in grado di archiviare informazioni. Tra questi occorre già annoverare anche i c.d. dispositivi IoT (*Internet of Things* o Internet delle cose), i quali sono progettati per connettersi alla rete e tra loro per fornire servizi di varia natura, non necessariamente limitati alla mera comunicazione.

22 Cfr. Linee guida *cookie* e altri strumenti di tracciamento del 10 giugno 2021, Garante per la protezione dei dati personali: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876

23 Cfr. Linee guida cookie e altri strumenti di tracciamento del 10 giugno 2021, Garante per la protezione dei dati personali.

Accanto ai predetti cookie non possono, poi, essere trascurati i c.d. ***cookie analitici***, sebbene questi non trovino una precisa menzione all'interno delle Linee guida. Detti *cookie* - già noti in quanto espressamente previsti nel provvedimento del 2014 - vengono infatti utilizzati per misurare l'efficacia di un servizio della società dell'informazione e possono essere assimilati ai *cookie* tecnici nei soli casi in cui:

- vengano impiegati per produrre statistiche aggregate e relative ad un solo sito o una sola applicazione;
- venga mascherata, per quelli di terze parti, almeno la quarta componente dell'indirizzo IP, impedendo così l'identificazione diretta dell'interessato;
- le terze parti si astengano dal combinarli, così minimizzati, con altre elaborazioni o dal trasmetterli ad ulteriori terzi.

In tutti gli altri casi, invece, devono essere considerati alla stregua dei *cookie* diversi da quelli tecnici.

È, quindi, molto importante che i titolari sappiano sempre con esattezza quali *cookie* sono presenti sui propri siti *web*, posto che, a seconda della tipologia di *cookie*, il Garante richiede l'implementazione di diversi accorgimenti al fine di garantire la massima protezione dei dati personali degli utenti.

Ma quali sono gli accorgimenti richiesti? Andiamo a vederli nel paragrafo che segue.

2.3 Accorgimenti privacy da realizzare per gestire al meglio i cookie

Nelle proprie Linee guida il Garante chiede ai titolari di garantire il rispetto dei principi di *privacy by design* e *by default*, di essere maggiormente trasparenti nei confronti degli utenti circa il trattamento dei loro dati personali, nonché di individuare nel consenso la corretta base giuridica per quei trattamenti di dati personali realizzati per fini diversi da quelli tecnici. Ciò, anche in considerazione di quanto espressamente previsto all'art. 122 del D. Lgs. n. 196/2003, come modificato dal D. Lgs. n. 101/2018 (di seguito "**Codice Privacy**"[24]).

I titolari sono, quindi, tenuti a:

24 L'art. 122 del Codice Privacy prevede, infatti, che "*L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente. Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente. Salvo quanto previsto dal comma 1, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente*".

- realizzare trattamenti rispettosi non solo dei principi sanciti all'art. 5 del GDPR, ma anche di quelli previsti all'art. 25 (c.d. ***principi di privacy by design*** e ***by default***), prevedendo l'implementazione di accorgimenti tali da garantire la protezione dei dati personali come impostazione predefinita fin dalla progettazione. Al momento del primo accesso al sito web, infatti, non deve essere utilizzato alcun *cookie* che non abbia natura tecnica così da garantire il trattamento dei soli dati strettamente necessari al funzionamento del sito;
- predisporre ***informative chiare, semplici e multi layer*** (ovvero dislocate su più livelli o rese tramite più canali, come *pop-up* informativi, interazioni vocali, *chatbot*, ecc.), che tengano anche conto delle tipologie dei *cookie* presenti sui rispettivi siti *web*.

Infatti, se i siti *web* installano:

- unicamente **cookie tecnici** - per cui peraltro **non è necessaria l'acquisizione del consenso** da parte degli utenti - la relativa informazione potrà essere collocata nella home page o integrata all'interno dell'informativa generale dei siti (per intenderci la c.d. **Privacy Policy**). Ciò, anche nel caso in cui il sito preveda l'installazione di **cookie analitici** aventi caratteristiche tali da essere equiparati ai tecnici;
- altri **cookie non tecnici** - per cui invece è necessaria la manifestazione di consenso da parte degli utenti - la relativa informazione dovrà essere resa mediante l'implementazione di un ***banner*** a scomparsa immediata e di adeguate dimensioni. È questo il caso in cui sia prevista l'installazione di **cookie di profilazione** o di altri cookie diversi da quelli tecnici.

Ciò chiarito, è evidente che in presenza di **cookie diversi da quelli tecnici** i titolari dovranno, quindi, prevedere all'interno dei propri siti *web* un ***banner*** - posizionato in modo tale da creare una percettibile discontinuità nella fruizione dei siti, ben visibile e con colori a contrasto rispetto a quelli del sito stesso - che contenga i seguenti elementi:

- l'indicazione che il sito web utilizza cookie tecnici e, previo consenso dell'utente, cookie di profilazione con previsione delle relative finalità (c.d. **informativa breve**);
- il link al testo della **Privacy Policy** e alla **Cookie Policy** contenente l'**informativa estesa** in cui dovranno essere espressamente menzionati gli eventuali ed ulteriori soggetti destinatari dei dati, i tempi di conservazione e le modalità di esercizio dei diritti previsti dal GDPR;
- l'avvertenza che la **chiusura del banner** (ad esempio, mediante selezione dell'apposito comando contraddistinto da una X posizionata in alto a destra) comporta il mantenimento delle **sole impostazioni di default** e il proseguimento della navigazione in assenza di *cookie* diversi da quelli tecnici.

Con riferimento, poi, alle modalità di acquisizione del **consenso**, i titolari non devono poi trascurare che - per essere ritenuto valido - il consenso deve essere **libero, specifico, informato, inequivocabile** e **revocabile**. Pertanto, oltre a fare attenzione affinché il consenso soddisfi le predette caratteristiche, i titolari dovranno essere altresì in grado di dimostrare di averlo correttamente acquisito, mediante precisa documentazione che attesti nel dettaglio ogni consenso raccolto o revocato ed anche per che tipologia di cookie è stato reso.

Sul punto, il Garante precisa che non possono ritenersi adatti per il predetto fine i *sistemi di scrolling*, salvo che questi non vengano inseriti in un processo più articolato che consenta la generazione di un evento registrabile, documentabile e qualificabile come azione positiva a manifestare l'inequivoca volontà dell'utente di prestare il consenso al trattamento (ad esempio mediante l'utilizzo di un apposito *cookie* tecnico).

Quanto, invece, ai **cookie wall**, il Garante chiede che non siano strutturati con meccanismi (c.d. **take it or leave it**), che obblighino quindi l'utente a esprimere il proprio consenso all'installazione dei *cookie* senza alcuna ulteriore possibilità di scelta. Così facendo, infatti, il consenso espresso non potrebbe di certo considerarsi lecito.

Il **banner** dovrà, quindi, essere implementato in modo da prevedere:

- un **comando** (ad esempio, una X posizionata in alto a destra) che permetta all'utente di chiudere il banner senza manifestare il proprio consenso all'utilizzo dei cookie. In questo modo, il sito web manterrà le sue **impostazioni di default** nel rispetto dei principi sanciti dal GDPR;
- un **comando** che permetta all'utente di **accettare tutti i cookie**;
- il **link** a una **specifica area** attraverso la quale l'utente potrà scegliere in modo analitico le funzionalità, le terze parti e i *cookie* che vuole installare e **due ulteriori comandi** mediante i quali poter modificare le scelte precedentemente effettuate, ovvero prestando il consenso all'uso di tutti i cookie se non dato in precedenza o revocandolo, anche in unica soluzione, se già espresso. Tale area dovrà, comunque, essere raggiungibile mediante un ulteriore *link*, che potrà, per esempio, essere posizionato nel *footer* di ciascuna pagina del sito *web*.

Il Garante, inoltre, raccomanda che nel rispetto del principio di **privacy by default** tutte le scelte sui *cookie* dovranno essere presentate all'utente in modo da negarne l'utilizzo, lasciando così allo stesso utente l'espressione del proprio consenso mediante azione positiva e inequivocabile.

Ultima indicazione; nel caso in cui l'utente abbia deciso di non prestare il consenso all'installazione dei *cookie* e di mantenere quindi le **impostazioni di default**, potrà essere chiamato ad esprimere nuovamente il consenso solo se sussistono le seguenti casistiche:

- sono notevolmente mutate le condizioni di trattamento;
- non è possibile sapere se il *cookie* sia già stato memorizzato nel dispositivo;

- sono trascorsi almeno **6 (sei) mesi** dalla precedente presentazione del *banner*.

Ciò, al fine di evitare continue reiterazioni di richieste di consenso mediante la comparsa del *banner*, che potrebbe portare l'utente ad accettare trattamenti cui altrimenti non avrebbe acconsentito pur di far scomparire il *banner*, incidendo così sulla sua libertà.

3. Google Analytics e Trasferimenti dati tra UE e USA

3.1 Il blocco all'utilizzo di Google Analytics e l'indirizzo IP come dato personale

Allineandosi alle decisioni assunte dalle autorità di controllo sulla privacy austriaca e francese, il Garante italiano per la protezione dei dati personali, con provvedimenti n. 224 del 9 giugno 2022 e n. 243 del luglio 2022, ha dichiarato che l'utilizzo di Google Analytics può comportare un trasferimento dei dati negli Stati Uniti, in violazione ai principi di cui alla sentenza della Corte di Giustizia C-311/18, c.d. Schrems II.

Come noto, Google Analytics è lo strumento, fornito dal colosso americano, che consente ai gestori di siti *web* di analizzare le statistiche degli utenti anche al fine di ottimizzare i servizi resi, migliorando gli strumenti *marketing* a disposizione dei gestori stessi.

In particolare, attraverso l'utilizzo di *cookies*, i gestori raccolgono informazioni relative alle modalità di interazione degli utenti con il sito *web*; tali dati consistono in identificatori online unici che consentono sia l'identificazione del *browser* o del dispositivo dell'utente che utilizza il sito, che il gestore stesso del sito (grazie all'ID account di Google). Oltre a quanto sopra, i dati riguardano l'indirizzo visitato, il nome del sito, i dati di navigazione e l'indirizzo IP del dispositivo utilizzato dall'utente. Da ultimo, vengono raccolte informazioni relative al browser, al sistema operativo, arrivando addirittura ad individuare la risoluzione dello schermo utilizzata e la lingua selezionata oltre, naturalmente, alla data e all'ora della visita al sito *web*.

Partendo dal presupposto che l'indirizzo IP è un dato personale a tutti gli effetti, posto che consente di identificare un determinato dispositivo e, conseguentemente, il relativo utente, soprattutto ove associato ad altre informazioni come quelle relative al *browser* ed alla data e all'orario - in particolare nel caso in cui l'utente visiti il sito dopo aver effettuato l'accesso al proprio account Google (con conseguente associazione delle relative informazioni tra cui indirizzo email, telefono, data di nascita ed immagine del profilo), il Garante ha sollevato alcune criticità legate all'utilizzo di Google Analytics ed espresso alcune considerazioni anche in merito al c.d. "IP-*Anonymization*".

Partendo da tale ultimo profilo, con la suddetta espressione si fa riferimento all'opzione, offerta da Google Analytics, per i gestori di siti *web* di inoltrare a

Google l'indirizzo privo della sua porzione meno significativa e composta da 8 numeri (c.d. "ottetto"). Ebbene, il Garante ha evidenziato che tale opzione comporta di fatto una pseudonimizzazione del dato relativo all'indirizzo di rete dell'utente, dal momento che l'eliminazione dell'ottetto significativo non impedisce a Google di identificare l'utente stesso, vista la mole di informazioni detenute dal gigante di Mountain View. Quanto sopra senza considerare che, come detto, qualora la visita al sito avvenga dopo aver effettuato l'accesso al proprio account di Google, quest'ultima sarà in grado di integrare l'indirizzo IP con altre informazioni dell'utente, con conseguente re-identificazione dello stesso.

Quanto al primo profilo viene rilevato che, fino al 30 aprile 2021, i gestori dei siti, titolari del trattamento, per poter utilizzare Google Analytics dovevano nominare quale responsabile del trattamento, Google LLC, società con sede in USA, verso la quale venivano trasferiti i dati personali raccolti tramite Google Anlytics. Successivamente, è subentrata nella fornitura dei servizi di analytics Google Ireland Limited, ma la *branch* europea può nominare altri sub-responsabili del trattamento, tra cui, appunto, Google LLC: in entrambi i casi, dunque, i dati possono essere trasferiti negli Stati Uniti.

Tuttavia, come sancito dalla richiamata sentenza Schrems II, il diritto statunitense, nel quadro di determinati programmi di sicurezza nazionale, consente deroghe alla propria normativa interna in tema di protezione dei dati tali per cui le autorità statunitensi possono accedere ai dati degli interessati peraltro senza che, in capo a questi, siano preposti adeguati strumenti di tutela che possano essere azionati in via giudiziale.

I rischi non risultano mitigati neppure dall'adozione da parte del Titolare - come avvenuto nei casi di cui ai richiamati provvedimenti del Garante - delle clausole contrattuali standard, uno degli strumenti a disposizione per poter trasferire dati personali ad un soggetto stabilito in un Paese terzo in mancanza di una decisione di adeguatezza, come appunto gli Stati Uniti. L'esportatore di dati non può infatti limitarsi ad aderire a tali clausole senza aver preventivamente verificato, in ottemperanza al principio di accountability, se la legge e le prassi del Paese terzo in questione incidano sull'efficacia delle garanzie predisposte nelle predette clausole. Richiamando anche la Raccomandazione n. 1/2020 dell'EDPB, il Garante ha evidenziato che la valutazione deve concentrarsi sulla legislazione e sulle prassi applicabili, nel paese terzo, ai dati specificamente trasferiti e comportare la verifica della "*possibilità o meno, per le autorità pubbliche del paese terzo* [...] *di tentare di accedere ai dati" nonché della "capacità o meno, per le autorità pubbliche del paese terzo* [...]*) di accedere ai dati attraverso l'importatore stesso o attraverso i fornitori di telecomunicazioni o i canali di comunicazione*".

Acclarata la possibilità di accesso ai dati (tra cui l'indirizzo IP) da parte delle autorità USA e rilevata l'assenza di adozione di ulteriori misure di sicurezza - peraltro non di facile attuazione - da parte dalle società oggetto dei provvedimenti, le decisioni del Garante hanno di fatto sancito l'illegittimità dell'utilizzo, da parte dei gestori dei siti, di Google Analytics.

3.2 Trasferimenti dati tra UE e USA: verso il nuovo Framework

I provvedimenti relativi a Google Analytics in realtà hanno una portata ancora più ampia poiché evidenziano la sostanziale inadeguatezza degli strumenti a disposizione per il trasferimento di dati verso gli Stati Uniti.

La sentenza Schrems II ha infatti invalidato la decisione di adeguatezza relativa al trasferimento di dati negli Stati Uniti, lasciano pericolosi vuoti normativi che, allo stato, non sono ancora colmati.

Nel marzo del 2022 la Presidente della Commissione europea Ursula von der Leyen ha rilasciato una dichiarazione congiunta con il Presidente degli Stati Uniti Joe Biden in merito al raggiungimento di un accordo relativo al trasferimento dei dati personali dall'UE agli USA volta a colmare tale lacuna, il c.d. "***Trans-Atlantic Data Privacy Framework***".

Successivamente, il Presidente degli Stati Uniti ha firmato l'"*Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*", un ordine esecutivo sul rafforzamento delle salvaguardie per le attività di intelligence degli Stati Uniti, nel solco dell'accordo politico raggiunto nella primavera del 2022 tra Europa e USA.

Tale Ordine Esecutivo, in generale, dispone che l'accesso ai dati da parte delle agenzie di intelligence statunitensi avvenga in modo proporzionato e solo se necessario per proteggere la sicurezza nazionale, solo nel perseguimento di obiettivi di sicurezza nazionale definiti, che tengano conto della *privacy* e delle libertà degli individui; è inoltre previsto l'ampliamento del perimetro delle responsabilità dei funzionari e l'introduzione di compiti di supervisione per individuare situazioni di non conformità. È stato inoltre previsto un meccanismo di ricorsi a due livelli: i cittadini potranno rivolgersi sia al *Civil Liberties Protection Officer che al Data Protection Review Court* (DPRC).

A seguito dell'*Executive Order*, il 13 dicembre 2022 la Commissione europea ha pubblicato il progetto di *Implementing Decision on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, dando inizio alla relativa procedura di adozione.

Tale decisione determina che gli Stati Uniti assicurano un livello di protezione adeguato dei dati trasferiti dall'Unione Europea alle organizzazioni statunitensi incluse in un'apposita lista, amministrata dal Dipartimento del Commercio americano, il cui accesso è condizionato al rispetto di una serie di principi in materia di protezione dei dati. Le aziende saranno certificate ed incluse nella lista su base annuale e la *Federal Trade Commission* ed il Dipartimento dei Trasporti americano godranno di vari poteri investigativi ed esecutivi sulle stesse.

Sulla base del *Data Integrity and Purpose Limitation Principle*, i dati personali oggetto del trasferimento potranno essere raccolti solo per scopi specifici, nella misura e per il tempo necessario al conseguimento delle singole finalità e saranno conservati ed aggiornati in modo appropriato.

È inoltre prevista la possibilità per l'interessato di opporsi al trattamento (c.d. "*opt-out*" in base al *Choice Principle*). Sulla base del *Security Principle* titolari e responsabili dovranno adottare misure tecniche e organizzative appropriate per proteggere i dati da possibili minacce, inclusa l'adozione di misure volte ad evitare trattamenti non autorizzati o illegittimi, la perdita o la distruzione di dati e il danno accidentale.

Il *Notice Principle* presiederà la trasparenza del trattamento e gli obblighi informativi e le aziende sono tenute a rendere pubbliche le proprie *polices*, mentre l'*Access Principle* dovrebbe garantire l'accesso, da parte degli interessati, ai dati personali eventualmente trattati da un'organizzazione e a ogni informazione rilevante sul loro trattamento, e potranno richiederne anche la rettifica e la cancellazione.

L'*Accountability for Onward Transfer Principle*, relativo agli ulteriori trasferimenti dei dati a soggetti terzi è volto a porre limitazioni per specifiche finalità sulla base di un accordo tra l'azienda iscritta nella lista e il terzo ricevente, e il trasferimento sarà consentito soltanto se tale accordo sottopone il terzo allo stesso regime di tutela dei dati garantito dai richiamati Principi.

Il *Recourse, Enforcement and Liability Principle* impone alle aziende certificate di fornire meccanismi effettivi per assicurare l'adeguamento dei trattamenti ai Principi, adottando misure per verificarne la loro conformità su base periodica e per istruire dipendenti e collaboratori.

Le aziende dovranno essere in grado, su richiesta, di giustificare il procedimento di adeguamento adottato, supportando eventuali verifiche a cui saranno sottoposte, da adeguata documentazione.

È inoltre previsto che siano messi a disposizione degli interessati meccanismi di ricorso indipendenti, efficaci e prontamente disponibili, che non comportino costi per gli stessi.

Gli interessati potranno infatti:

- contattare direttamente l'azienda certificata e questa è tenuta a riscontrare la richiesta entro 45 giorni;
- rivolgersi all'organismo indipendente di risoluzione delle controversie designato dall'azienda;
- proporre una segnalazione o un reclamo ad un'autorità di controllo indipendente, all'interno dell'Unione, che collaborerà con il Dipartimento del Commercio americano e la *Federal Trade Commission* che potranno intervenire in caso di violazioni della legge o di inottemperanza a quanto prescritto dalle stesse;
- rivolgersi direttamente al Dipartimento del Commercio americano o alla *Federal Trade Commission*;
- in via residuale, proporre un arbitrato vincolante a opera di un apposito Panel che può imporre provvedimenti equitativi non monetari e specifici per ogni individuo necessari per rimediare a eventuali inottemperanze;

- adire l'autorità giudiziaria statunitense.

L'accesso ai dati da parte delle autorità statunitensi potrà avvenire esclusivamente sulla base dei principi di proporzionalità e adeguatezza.

In caso di trattamento di dati per esigenze di polizia, la legislazione federale impone una serie di limitazioni e dispone meccanismi di controllo e reclamo adeguati ed effettivi, disponendo un livello di protezione uguale a quello garantito ai cittadini americani; dall'altro lato, i procuratori e gli altri soggetti inquirenti federali degli Stati Uniti sono tenuti ad ottenere un'autorizzazione giudiziaria per raccogliere dati personali.

Inoltre, le pubbliche amministrazioni federali sono in generale sottoposte alla supervisione di una serie di organismi in modo da scongiurare abusi di potere.

Non da ultimo, oltre ad alcuni rimedi esperibili di fronte ai tribunali ordinari del circuito federale, i cittadini europei potranno adire un'apposita *Data Protection Review Court* attraverso le autorità di controllo indipendenti negli Stati membri dell'Unione.

Chiaramente la Commissione europea monitorerà ogni cambiamento giuridico e adotterà revisioni periodiche della propria decisione di adeguatezza che potrà anche essere sospesa o revocata.

La bozza di decisone adottata dalla Commissione è stata sottoposta al vaglio dell'EDPB, il quale ha espresso un parere positivo per i miglioramenti sostanziali riscontrati, grazie all'introduzione dei principi di necessità e proporzionalità per la raccolta di dati da parte dell'intelligence statunitense e del nuovo meccanismo di ricorso per gli interessati dell'UE.

Tuttavia, lo stesso Comitato ha espresso anche alcune perplessità e ha chiesto chiarimenti su diversi punti, tra cui determinati diritti degli interessati, i trasferimenti successivi, la portata delle esenzioni e il funzionamento pratico del meccanismo di ricorso.

Nel frattempo, con una risoluzione adottata dal Comitato Libertà Civili, i Membri del Parlamento europeo hanno votato contro la bozza di decisione rilevando che il nuovo *framework*, pur rappresentando un miglioramento, consente ancora la raccolta in blocco di dati personali in alcuni casi senza un'autorizzazione preventiva indipendente e non prevede norme chiare sulla conservazione dei dati. Inoltre, le decisioni della *Data Protection Review Court* sarebbero segrete, violando il diritto dei cittadini di accedere e rettificare i dati che li riguardano.

CAPITOLO 3 di Angela Berinati, Federica Dendena e Marta Margiocco

Marketing e profilazione 2022 - elementi di novità e orientamenti consolidati

SOMMARIO: 1. Trattamento dei dati per finalità di marketing: le basi giuridiche, tra consenso e legittimo interesse; spam e soft spam. – 2. I contenuti dell'informativa, opt-in, opt-out, social spam e marketing virale. – 3. Il Registro pubblico delle opposizioni. – 4. Telemarketing: legittimità del trattamento e diritto di opposizione. – 5. Profilazione con sistemi automatizzati. Cookie di profilazione e modalità di acquisizione del consenso. – 6. Giurisprudenza e Garante: le campagne di "recupero consenso" e invio di offerte promozionali. – 7. I tempi di conservazione dei dati per finalità di marketing e profilazione. – 8. Campagne di marketing: utilizzo di banche dati.

1. Trattamento dei dati per finalità di marketing: le basi giuridiche, tra consenso e legittimo interesse; spam e soft spam.

Il trattamento di dati per finalità di marketing richiede, come per ogni trattamento, un'adeguata base giuridica.

Il dato normativo da cui partire è l'art. 130 del D. Lgs. n. 196/2003 (di seguito "Codice Privacy"), come modificato dal D.Lgs. n. 101/2018, in forza del quale le comunicazioni per l'invio di materiale pubblicitario, di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, se effettuate con l'utilizzo di sistemi automatizzati di chiamata (chiamata senza l'intervento di un operatore) o mediante posta elettronica, telefax, mms, sms, ecc. richiedono il consenso del contraente o utente.

Fuori dai predetti casi – quindi nelle ipotesi di comunicazioni di marketing effettuate con mezzi diversi da quelli sopra indicati – il trattamento non richiede il consenso, ma deve comunque avvenire nel rispetto degli articoli 6 e 7 del Regolamento UE 2016/679 (di seguito "Regolamento" o "GDPR").

Come specificato dal comma 3-*bis* dell'art. 130 del Codice Privacy, le comunicazioni di marketing effettuate tramite l'uso del telefono o della posta cartacea sono consentite nei confronti di chi non abbia esercitato il diritto di opposizione mediante l'iscrizione della numerazione della quale è intestatario nel Registro Pubblico delle Opposizioni. Del Registro si parlerà al successivo paragrafo.

Un'eccezione alla "regola" del consenso preventivo per le comunicazioni di marketing effettuate tramite e-mail la troviamo nel cosiddetto "*soft spam*". Sempre l'art. 140 del Codice Privacy prevede, infatti, la possibilità per il titolare del trattamento di non richiedere il consenso per le comunicazioni ai fini della vendita diretta di propri prodotti o servizi, a condizione che:

(i) vengano utilizzate le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o servizio;

(ii) i prodotti o servizi promossi siano analoghi a quelli oggetto della vendita;

(iii) l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni.

L'interessato, aggiunge il Codice Privacy, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per dette finalità, deve essere informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuita.

Sono, in ogni caso, vietate le comunicazioni di marketing o, comunque, a scopo promozionale, effettuate camuffando o celando l'identità del mittente o in violazione dell'art. 8 D. Lgs. 9 aprile 2003, n. 70[25] o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui agli artt. da 15 a 22 del Regolamento, oppure esortando i destinatari a visitare siti web che violino il predetto articolo 8 del citato Decreto Legislativo.

2 I contenuti dell'informativa, opt-in, opt-out, social spam e marketing virale.

Alla luce di quanto descritto nel paragrafo precedente, il fenomeno dello *spam* è lecito solo con la preventiva acquisizione del consenso dell'interessato/destinatario delle comunicazioni. L'informativa e il modulo di raccolta del consenso da consegnare all'interessato devono avere i contenuti di cui all'art. 13 del GDPR e in particolare, è necessario raccogliere un preciso consenso per ogni specifico trattamento che abbia come finalità il marketing così come anche per la comunicazione dei dati a terzi per effettuare in nome e per conto del titolare attività di marketing (cd. "*opt-in*").

Nonostante quanto sopra, si segnala l'eccezione del "*soft spam*" (art. 130, comma 4, Codice Privacy) riferita, come già descritto, ai messaggi promozionali per la sola posta elettronica, in base alla quale, se il titolare del trattamento utilizzi, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall´interessato nel contesto della vendita di un prodotto o

25 Art. 8 D.Lgs. 9 aprile 2003, n. 70 "*1. In aggiunta agli obblighi informativi previsti per specifici beni e servizi, le comunica-zioni commerciali che costituiscono un servizio della società dell'informazione o ne sono parte integrante, devono conte-nere, sin dal primo invio, in modo chiaro ed inequivocabile, una specifica informativa, diretta ad evidenziare: a) che si tratta di comunicazione commerciale; b) la persona fisica o giuridica per conto della quale è effettuata la comunicazione commerciale; c) che si tratta di un'offerta promozionale come sconti, premi, o omaggi e le relative condizioni di accesso; d) che si tratta di concorsi o giochi promozionali, se consentiti, e le relative condizioni di partecipazione.*"

di un servizio, può non richiedere il consenso dell´interessato, a condizione che si tratti di servizi analoghi a quelli oggetto della vendita e che l´interessato, adeguatamente informato, non rifiuti tale uso.

In tal caso è opportuno utilizzare la formula del cd "*opt-out*" a titolo cautelativo, ovvero l'interessato deve avere la possibilità di esprimere la propria volontà di non ricevere più nemmeno le comunicazioni pubblicitarie, che rientrano nella eccezione del "*soft spam*". Pertanto, è sempre opportuno predisporre in ogni singola e-mail la possibilità di revocare il proprio consenso tramite un apposito *link*.

Segnaliamo, infine, alcune nuove forme di *spam*[26] direttamente connesse alla crescita dell'utilizzo di *internet* e alla nascita dei cd. *social network*. In particolare, si assiste sempre maggiormente al fenomeno denominato "*social spam*", che consiste in un insieme di attività mediante le quali sono veicolati messaggi e *link* attraverso le reti sociali online sfruttando i dati personali degli utenti dei *social network*, che lasciano il proprio profilo "aperto" al pubblico.

Il rischio in tale caso è doppio: (1) per gli utenti dei *social network* è per i propri dati personali che possono essere utilizzati senza il preventivo consenso per attività di profilazione e marketing da parte di società terze, che possono anche non essere partner commerciali delle società che gestiscono i *social network*; (2) per i contatti degli utenti consiste nella possibilità che il messaggio *spam* veicolato al profilo riesca a catturare tutto l´elenco dei contatti dell´utente, aumentando in tal modo la portata virale del messaggio. Il Garante ha chiarito alcuni aspetti con riferimento a determinate situazioni:

1 l'utente riceve, in privato, in bacheca o nel suo indirizzo di posta e-mail collegato al suo profilo social, un determinato messaggio promozionale relativo a uno specifico prodotto o servizio da un'impresa che abbia tratto i dati personali del destinatario dal profilo del *social network* al quale egli è iscritto. In tale caso, il trattamento sarà da considerarsi illecito, a meno che il mittente non dimostri di aver acquisito il consenso dell'interessato ai sensi del GDPR e dell´art. 130, commi 1 e 2, del Codice Privacy;

2 L'utente è diventato "*fan*" della pagina di una determinata impresa o società oppure si sia iscritto a un gruppo di *follower* di un determinato marchio, personaggio, prodotto o servizio (decidendo così di seguirne le relative vicende, novità o commenti) e successivamente riceve messaggi pubblicitari concernenti i suddetti elementi. In tal caso, l´invio di comunicazione promozionale riguardante un determinato marchio, prodotto o servizio, effettuato dall´impresa a cui fa riferimento la relativa pagina, può considerarsi lecito se dal contesto o dalle modalità di funzionamento del *social network*, anche sulla base delle informazioni fornite, può evincersi in modo inequivocabile che l´interessato abbia in tal modo voluto manifestare anche la volontà di fornire il proprio

26 Linee guida in materia di attività promozionale e contrasto allo spam del 4 luglio 2013 emanate dal Garante per la prote-zione dei dati.

consenso alla ricezione di messaggi promozionali da parte di quella determinata impresa. Se, invece, l'interessato si cancella dal gruppo, oppure smette di seguire quel marchio o quel personaggio, o comunque si oppone ad eventuali ulteriori comunicazioni promozionali, il successivo invio di messaggi promozionali sarà illecito, con le relative conseguenze sanzionatorie. Ciò, ferma comunque restando la possibilità degli utenti dei *social network* di bloccare l'invio di messaggi da parte di un determinato contatto o di segnalare quest'ultimo come *spammer*.

Nell'ipotesi dei "contatti" (i c.d. "amici") dell'utente, dei quali spesso nei *social network* o nelle comunità degli iscritti ai servizi di cui sopra, sono visualizzabili numeri di telefono o indirizzi di posta elettronica, l'impresa o società che intenda inviare legittimamente messaggi promozionali dovrà aver previamente acquisito, per ciascun "contatto" o "amico", un consenso specifico per l'attività promozionale.

Infine, il Garante riscontra anche un altro fenomeno in continua evoluzione, il c.d. *marketing virale*[27], che è una modalità di attività promozionale mediante la quale un soggetto promotore sfrutta la capacità comunicativa di pochi soggetti destinatari diretti delle comunicazioni per trasmettere il messaggio ad un numero elevato di utenti finali. È un'evoluzione del "passaparola", ma se ne distingue per il fatto che fin dall'inizio emerge la volontà dei promotori di avviare una campagna promozionale.

In genere, con il *marketing* virale si fa riferimento agli utenti di Internet che suggeriscono o raccomandano ad altri l'utilizzo di un determinato prodotto o servizio. Ultimamente, questa tecnica promozionale si sta diffondendo anche per prodotti non strettamente connessi a Internet: veicolo del messaggio resta comunque la comunità del *web*, che può comunicare in maniera chiara, veloce e gratuita.

Per agevolare la diffusione del messaggio, il soggetto promotore offre un incentivo o un bonus o altro bene economico ai destinatari delle comunicazioni che a loro volta, in cambio, si offrano di inoltrare o comunque far conoscere a terzi (talora con e-mail o sms) la comunicazione promozionale ricevuta.

Tale attività, quando viene svolta con modalità automatizzate e per finalità di marketing, può rientrare nello spam se non rispetta principi e norme già sopra indicati nell'ambito del quadro normativo attualmente in vigore, con particolare riferimento al GDPR.

27 Linee guida in materia di attività promozionale e contrasto allo spam del 4 luglio 2013 emanate dal Garante per la prote-zione dei dati.

3 Il Registro Pubblico delle Opposizioni: effetti dell'iscrizione e obblighi degli operatori.

3.1 Il Registro delle Opposizioni: ambito di applicazione

Come sopra precisato, ai sensi del comma 3-*bis* dell'art. 130 del Codice Privacy, le comunicazioni di marketing effettuate tramite l'uso del telefono o della posta cartacea sono consentite nei confronti di chi non abbia esercitato il diritto di opposizione mediante l'iscrizione della numerazione della quale è intestatario o dell'indirizzo postale nel Registro Pubblico delle Opposizioni.

Con il D.P.R. n. 26/2022 è stato emanato il "Regolamento recante disposizioni in materia di istituzione e funzionamento del registro pubblico dei contraenti che si oppongono all'utilizzo dei propri dati personali e del proprio numero telefonico per vendite o promozioni commerciali, ai sensi dell'articolo 1, comma 15, della legge 11 gennaio 2018, n. 5".

Detto Regolamento disciplina il Registro Pubblico delle Opposizioni di cui all'art. 130, comma 3-*bis* del Codice e si applica ai trattamenti, effettuati mediante comunicazioni telefoniche con qualunque mezzo effettuate (sia tramite operatore, sia mediante sistemi automatizzati di chiamata o chiamate senza l'intervento di un operatore) oppure tramite posta cartacea, per fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, delle numerazioni telefoniche nazionali fisse e mobili, che siano o meno riportate in elenchi di contraenti e degli indirizzi postali riportati nei medesimi elenchi.

Restano esclusi dall'ambito di applicazione del regolamento i trattamenti di dati riferiti alle numerazioni telefoniche nazionali fisse e mobili e agli indirizzi postali inseriti negli elenchi di contraenti, effettuati per finalità statistiche dagli enti e dagli uffici di statistica appartenenti al Sistema statistico nazionale.

Come indicato nel Regolamento stesso, il diritto di opposizione previsto all'art. 21, paragrafo 2 del GDPR può essere esercitato dal contraente iscrivendosi al Registro e ha efficacia con riferimento al trattamento dei dati personali effettuato per le finalità commerciali sopra indicate.

3.2 Iscrizione dei contraenti al Registro e obblighi degli operatori.

Ciascun contraente può chiedere al gestore del Registro che la numerazione della quale è intestatario (riportata o meno negli elenchi di cui all'art. 129 del Codice) o il corrispondente indirizzo postale, riportato nei medesimi elenchi, siano iscritti nel registro per opporsi al trattamento di tali dati per le finalità di marketing sopra indicate.

L'iscrizione al Registro preclude qualsiasi trattamento degli indirizzi postali contenuti negli elenchi di contraenti e delle numerazioni nazionali fisse e mobili da parte degli operatori per le finalità indicate.

Con l'iscrizione si intendono, infatti, revocati tutti i consensi precedentemente espressi, con qualsiasi forma o mezzo, che autorizzano i predetti trattamenti.

I contraenti iscritti al Registro possono:

- rinnovare l'iscrizione in qualsiasi momento. Il rinnovo dell'iscrizione comporta la revoca del consenso al trattamento prestato ai titolari precedentemente alla data di rinnovo dell'iscrizione;
- revocare in qualunque momento la propria opposizione nei confronti di uno o più operatori. La revoca dell'opposizione consente il trattamento da parte dei titolari: (i) della numerazione e dell'indirizzo postale, contenuti negli elenchi di contraenti, dalla data di annotazione della revoca dell'opposizione; (ii) delle numerazioni nazionali, se è stato raccolto apposito consenso successivamente alla data più recente di iscrizione o rinnovo, purché ciò sia avvenuto o avvenga nel rispetto del Regolamento.

L'iscrizione è a tempo indeterminato e cessa solo in caso di revoca da parte del contraente.

Gli operatori che utilizzano sistemi di pubblicità telefonica e di vendita telefonica o che compiono ricerche di mercato o comunicazioni commerciali telefoniche, nonché mediante l'impiego della posta cartacea, per effettuare i predetti trattamenti[28] devono presentare apposita istanza presso il gestore del Registro. Gli stessi, inoltre, hanno l'obbligo di consultare mensilmente – e comunque prima dell'inizio di ogni campagna promozionale – il Registro e di provvedere all'aggiornamento delle proprie liste.

Prima di effettuare il trattamento, dunque, il titolare deve verificare che i dati da trattare non risultino iscritti nel Registro perché, se così fosse, non potrà effettuare il trattamento, avendo di fatto gli interessati esercitato il diritto di opposizione, con conseguente annullamento dei consensi precedentemente espressi per finalità di *marketing*, vendita diretta con modalità telefonica e ricerche di mercato.

La consultazione del Registro da parte di ciascun operatore ha efficacia pari a quindici giorni per i trattamenti di dati per fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, mediante l'impiego del telefono, con o senza operatore, e pari a trenta giorni per i trattamenti di dati per le medesime finalità mediante l'impiego della posta cartacea.

È bene, infine, ricordare che tale verifica deve essere compiuta non solo da parte del titolare del trattamento, ma anche dai call center eventualmente

28 Trattamento delle numerazioni nazionali fisse e mobili, mediante l'impiego del telefono con o senza l'intervento di un operatore umano o degli indirizzi postali riportati in elenchi di contraenti, mediante posta cartacea, per fini di invio di ma-teriale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

incaricati per l'esecuzione del trattamento, che – in qualità di responsabili – agiscono per conto dei rispettivi titolari.

Aspetti, questi, sui quali l'attenzione del Garante è da sempre molto elevata.

4. Telemarketing: legittimità del trattamento e diritto di opposizione.

4.1 Il telemarketing.

Il *telemarketing* è diffusamente impiegato da numerose società al fine di promuovere e/o commercializzare prodotti o servizi a potenziali clienti.

Tale attività può essere svolta dalle società, titolari del trattamento, attraverso operatori telefonici interni all'organizzazione, espressamente autorizzati al trattamento dei dati oppure esterni (c.d. call center), nominati responsabili del trattamento ai sensi dell'art. 28 del GDPR.

A seconda del caso, dunque, il titolare deve attivarsi con i relativi adeguamenti: nel caso di impiego di operatori interni, predisponendo specifiche lettere di designazione in cui individuate precise istruzioni circa il trattamento dei dati; nel caso di *call center*, stipulando il contratto richiesto dall'art. 28 del GDPR, completo di tutti gli elementi richiesti.

Ciò, al fine di garantire che anche i trattamenti dei dati eseguiti nell'ambito dello svolgimento di attività di *telemarketing* vengano effettuati conformemente alla normativa vigente, da soggetti autorizzati.

4.2 Opposizione nel telemarketing: il "no" dell'utente va registrato subito.

In tema di opposizione si è già parlato del Registro Pubblico delle Opposizioni e degli effetti conseguenti all'iscrizione da parte degli utenti, che impedisce agli operatori di prendere contatti per finalità di marketing.

Il Garante per la protezione dei dati personali si è recentemente espresso in merito all'opposizione manifestata dagli utenti nel corso delle telefonate per finalità commerciali.[29]

Il principio puntualizzato dall'Autorità conferma che se l'utente si oppone alla telefonata commerciale indesiderata, la società o il call center che lo ha contattato deve annotare subito la volontà di questo e provvedere alla cancellazione del nominativo dalle liste utilizzate per il *telemarketing*.

Più in dettaglio, come precisa l'Autorità, l'opposizione espressa dall'interessato nel corso della telefonata deve essere sufficiente ai fini della cancellazione dalle liste, senza che debba essere confermata con e-mail o altra modalità; detta

29 Provvedimento inibitorio, prescrittivo e sanzionatorio del 15 dicembre 2022 – Registro dei provvedimenti n. 431 del 15 dicembre 2022, emesso all'esito di un'attività istruttoria condotta a seguito di reclami e segnalazioni da parte di diversi interessati.

opposizione, inoltre, è valida anche per le campagne promozionali future attuate dalle società e non solo per quella in corso.

Con il Provvedimento in commento, il Garante ha sanzionato la Società per alcune condotte illecite[30]. In particolare: (i) la ricezione di telefonate senza consenso; (ii) il mancato riscontro alle richieste di non ricevere più telefonate indesiderate; (iii) l'impossibilità per l'interessato di esprimere consensi liberi e specifici per diverse finalità (promozionali, profilazione, comunicazione di dati a terzi) durante l'accesso e la navigazione sul sito internet o nell'ambito dell'app; (iv) la presenza di informative carenti o inesatte.

Il Garante ha quindi ingiunto alla Società:

(i) di fornire agli utenti un'idonea informativa nella quale sono indicate solo le attività di trattamento effettivamente svolte (artt. 12 e 13 Regolamento).

(ii) di facilitare l'esercizio dei diritti previsti dalla normativa in materia di protezione dei dati e di soddisfare, senza ingiustificato ritardo, le relative istanze, compreso il diritto di opposizione che può essere avanzato dall'interessato in qualsiasi momento; di indicare chiaramente, già nello script di chiamata, il titolare a cui dovrà essere indirizzata la richiesta di cancellazione dei dati personali e che vi provvederà in via definitiva, ai sensi degli artt. 6, 7 e 13 del Regolamento, 130 Codice.

Il Garante ha inoltre vietato:

(i) ogni ulteriore trattamento per finalità promozionali effettuato utilizzando liste di contatti predisposte da soggetti terzi che non abbiano acquisito dagli interessati un consenso libero, specifico, informato alla comunicazione dei dati. A tal fine, l'Autorità ha ingiunto di adottare idonee procedure volte a verificare costantemente, anche mediante adeguati controlli a campione, che i dati personali siano trattati nel pieno rispetto delle disposizioni in materia (acquisizione di un consenso libero, specifico, inequivocabile, documentato, oltre che informato, degli interessati per l'invio di comunicazioni commerciali) ai sensi degli artt. 6, 7 e 13 del Regolamento nonché 130 del Codice;

(ii) il trattamento dei dati personali raccolti senza che sia stato acquisito il necessario preventivo consenso informato, libero e specifico degli interessati in relazione all'attività di marketing e profilazione ex artt. 6, 7 e 12 del Regolamento nonché 130 del Codice.

30 L'Autorità ha ingiunto alla società di pagare, a titolo di sanzione amministrativa, la somma di € 4.900.000,00. Tra le circostanze aggravanti: (i) l'elevato numero di soggetti coinvolti, la gravità delle violazioni rilevate, (iii) il carattere negligente delle condotte, "posto che la presenza della Società nel mercato da molti anni avrebbe dovuto consentire alla medesima di acquisire un bagaglio sufficiente di esperienza e competenza per adottare scelte di fondo maggiormente aderenti al dettato normativo, la complessa valutazione sulla capacità economica della Società. Tra gli elementi attenuanti: (i) l'assenza di precedenti procedimenti a carico della Società, la tempestiva adozione di misure correttive, alcune delle quali avviate subito dopo la conclusione degli accertamenti ispettivi, (iii) l'elevato grado di cooperazione nell'interazione con l'Autorità di controllo".

4.3 Il Codice di condotta per le attività di telemarketing e teleselling.

Il Garante per la protezione dei dati personali ha recentemente approvato il "Codice di condotta per le attività di *telemarketing* e *teleselling*" (di seguito Codice di Condotta) promosso da associazioni di committenti, *call center*, *teleseller*, *list provider* e associazioni di consumatori, per assicurare il rispetto della normativa privacy "dal contatto al contratto" e quindi lungo tutta la "filiera" del *telemarketing*.

Le società che aderiranno al Codice, infatti, si impegneranno a rispettare i principi e le regole ivi previste e ad adottare le specifiche misure indicate, per garantire la correttezza e la legittimità dei trattamenti di dati svolti nell'ambito delle predette attività.

Il Codice di Condotta si applica ad attività di trattamento di dati personali effettuati da soggetti operanti in territorio italiano o estero per promuovere e/o offrire beni o servizi, tramite il canale telefonico, a soggetti ubicati in Italia[31] [32].

Obiettivi del Codice sono, da un lato, la necessità di porre un freno alle condotte in contrasto con la normativa in materia di protezione dei dati personali e lesive del diritto alla tranquillità individuale delle persone; dall'altro, parallelamente, stimolare maggiore fiducia da parte degli interessati rispetto alle attività promozionali veicolate telefonicamente.

Il Codice di Condotta acquisterà efficacia una volta conclusa la fase di accreditamento dell'Organismo di monitoraggio (Odm)[33] e la successiva pubblicazione in Gazzetta Ufficiale.

Entrando, sia pur sommariamente, nel merito delle indicazioni contenute nel Codice di Condotta, le società che vi aderiranno si impegneranno, tra l'altro, a (i) garantire il rispetto di principi di liceità, proporzionalità, minimizzazione dei dati, correttezza e trasparenza nei confronti degli interessati (ii) adottare misure specifiche volte ad assicurare l'idonea informazione dell'utenza, l'adozione della corretta base giuridica e l'esercizio dei diritti, nonché misure tecniche e organizzative volte a garantire elevati standard di protezione dei dati personali.

Anche il Codice di Condotta presta un'attenzione specifica al consenso, che non può essere: generico, unico per finalità diverse (*marketing*, profilazione, ecc.), preselezionato e non adeguatamente documentato o documentabile con

31 Per "*telemarketing*" si intendono le attività di contatto telefonico con operatore effettuate per finalità promozionale attraverso chiamate dirette a numerazioni fisse e mobili nazionali; per "*teleselling*" le attività di contatto telefonico con operatore effettuate per finalità di vendita diretta attraverso chiamate destinate a numerazioni fisse e mobili nazionali

32 Sono escluse dal Codice di Condotta le promozioni in app e il *digital advertising*, nonché i contatti telefonici con finalità esclusivamente limitata alla rilevazione del grado di soddisfazione della clientela, a sondaggi e/o ricerche di mercato senza alcuna finalità commerciale. Si intendono, altresì, escluse dall'ambito di applicazione del Codice di Condotta tutte le modalità di contatto sviluppate tramite canali diversi da quello telefonico quali, ad esempio, il canale SMS, nonché le attività di contatto e le altre attività a ciò connesse dirette verso soggetti diversi da persone fisiche, liberi professionisti e imprese individuali.

33 L'Odm è un organismo indipendente chiamato a verificare l'osservanza del Codice di Condotta da parte degli aderenti e a gestire la risoluzione dei reclami

certezza; si sottolinea, inoltre, la necessità di informare in maniera precisa le persone contattate sulle finalità per le quali vengono usati i loro dati, assicurando il pieno esercizio dei diritti previsti dalla normativa *privacy* (opposizione al trattamento, rettifica o aggiornamento dei dati).

Ai titolari è richiesto, tra le altre condotte, di prestare particolare attenzione nella scelta dei partner commerciali, privilegiando, nel rispetto della normativa sulla concorrenza, i soggetti aderenti al Codice di Condotta. Allo scopo, è richiesta l'adozione di una procedura di prequalifica del fornitore, che assicuri il rispetto degli adeguati standard previsti dal Codice di Condotta e che consenta la raccolta di informazioni e la selezione del partner anche sulla base di modelli di organizzazione, gestione e controllo o, comunque, di *standard* adeguati di *compliance*.

Indispensabili, poi, per titolare e responsabili, in caso di affidamento di trattamenti a questi, l'adozione di specifiche procedure, quali quella per la gestione del *data breach*, che assicuri, tra l'altro, tempi di individuazione della violazione in caso di trattamenti affidati in *outsourcing* e quella per la gestione delle istanze di esercizio dei diritti degli interessati. Quest'ultima, dovrà garantire (i) il presidio di tutti i possibili canali di ricezione di tali istanze da parte di soggetti autorizzati al trattamento, istruiti per riconoscerle ed incardinarle secondo il canale più efficace; (ii) il coordinamento tra il titolare ed eventuali affidatari di servizi, che dovranno informare senza ingiustificato ritardo il titolare nel caso di ricezione di una richiesta, fornire tutte le informazioni necessarie ad evadere la richieste, con la possibilità di mettere in *black list* i dati di contatto nel caso l'istanza abbia ad oggetto l'opposizione ai contatti commerciali.

Viene ribadito l'obbligo, prima di avviare una campagna di *telemarketing* o *teleselling*, di aggiornare le liste tramite il Registro Pubblico delle Opposizioni.

Una specifica sezione del Codice di Condotta è poi dedicata alle misure che gli aderenti e i soggetti operanti per conto di questi sono tenuti ad adottare a garanzia del corretto trattamento nell'intera "filiera" del *telemarketing*.

Il titolare deve, infatti, garantire, anche grazie alla necessaria cooperazione dei propri responsabili, il pieno, puntuale e costante controllo di tutti i soggetti comunque coinvolti in qualunque fase preparatoria o di esecuzione della compagna promozionale. Si va dagli obblighi di verifica circa il possesso dei requisiti dichiarati dall'affidatario del servizio (mediante verifica documentale e/o ispezione interna), al divieto di affidare le attività delegate a *sub-responsabili*, salva espressa autorizzazione del committente/titolare del trattamento che potrà essere concessa solo per soggetti che garantiscano i medesimi *standard* richiesti dal Codice di Condotta.

Il titolare deve garantire e richiedere ai propri responsabili che il trattamento avvenga in conformità al Regolamento, al Codice e al Codice di Condotta a partire dalla fase di raccolta dei dati. A tal fine il titolare adotta misure adeguate per verificare che il responsabile rispetti le istruzioni impartire attraverso audit quali, ad esempio, le "numerazioni civetta" (numerazioni proprie all'interno della lista delle numerazioni contattabili) e controlli a campione sui contratti

stipulati per verificare che i contatti siano effettuati con le modalità corrette e che, in particolare, l'informativa sia stata resa in maniera intelleggibile.

Nei contratti stipulati dai committenti che regolano i rapporti commerciali con i fornitori andranno, inoltre, richiamati gli obblighi di controllo e collaborazione derivanti dal Codice di Condotta e occorrerà prevedere meccanismi di risoluzione e/o altre misure negoziali, come ad esempio l'applicazione di penali, idonee a scoraggiare pratiche contrarie alle regole previste.

Attenzione viene posta anche alla formazione, con l'indicazione di adottare piani di formazione per il personale con cadenza almeno annuale e richiede ai soggetti nominati responsabili di adottare piani di formazione che siano coerenti con i propri.

lI Codice di Condotta disciplina inoltre i rapporti tra committente e *list provider*, ovvero il soggetto che, in qualità di titolare del trattamento e sulla base del consenso ottenuto dagli interessati, fornisce dati personali al committente per finalità di *telemarketing*.

Nella fase di selezione del *list provider* il committente deve valutare con la massima diligenza la presenza di tutti gli elementi di garanzia necessari e, tra l'altro, verificare l'adozione di corrette modalità di acquisizione del consenso su un campione significativamente rappresentativo della banca dati, attraverso l'esame delle informative rilasciate al momento della raccolta dei dati e della modalità adottate per documentare il consenso. Il *list provider* deve in ogni caso fornire al committente una dichiarazione scritta attestante la correttezza, liceità e aggiornamento di tutti i consensi raccolti.

Prima di utilizzare i dati il committente deve inoltre richiedere che le liste siano state verificate dal list provider presso il Registro Pubblico delle Opposizioni e deve a sua volta verificare che nella lista non siano presenti soggetti che si siano opposti al trattamento o abbiano revocato il consenso nei confronti del committente. È previsto inoltre l'obbligo del committente di informare il *list provider*, entro e non oltre 15 giorni, di manifestazioni di volontà negative espresse dagli interessati rispetto alla racconta del consenso da parte del *list provider* stesso.

Sono previsti, inoltre, obblighi specifici per i fornitori che, in qualità di responsabili del trattamento, effettuano materialmente la campagna di promozione prendendo i contatti con gli interessati.

Tra questi:

i l'obbligo di iscrizione al "ROC" (Registro degli operatori di comunicazione) e di comunicare tutte le numerazioni telefoniche messe a disposizione del pubblico ed utilizzate per i servizi[34];

ii l'obbligo di presentazione dell'identificazione della linea chiamante utilizzando l'apposito codice prefisso per identificare le attività di

34 L'obbligo di iscrizione, precisa il Codice di Condotta, sussiste anche a carico dei soggetti terzi affidatari dei servizi di *call center* e deve essere contemplato nel contratto di affidamento del servizio.

pubblicità, vendita e comunicazione commerciale o, in alternativa (e sino a diverse disposizioni che dovessero essere introdotte, precisa il Codice di Condotta) l'utilizzo della propria numerazione priva del codice prefisso purché ricontattabile da parte dell'utente. Dette numerazioni devono essere comunicate al committente prima dell'inizio dell'attività promozionale e devono risultare iscritte al ROC;

iii divieto di contattare gli interessati in alcune fasce orarie o giorni;

iv essere in grado di fornire agli interessati, nel corso della telefonata e senza eccezioni, le previste informazioni sul trattamento dei dati e sulle modalità di esercizio dei diritti, delineando con chiarezza ruoli e incombenze;

v non accettare incarichi da committenti che non prevedano un obbligo espresso di utilizzo, in caso di contatti commerciali *outbond*, unicamente tali numerazioni;

vi fornire ai committenti, entro 15 giorni dalla chiusura delle singole campagne promozionali, un report dettagliato sulle telefonate effettuate, completo di tutte le indicazioni previste dal Codice di Condotta.

Tutti i principi e le prescrizioni contenute nel Codice di Condotta sono quindi finalizzati ad una tutela degli interessati, attraverso la diffusione nel mercato di principi e misure a tutela degli stessi.

Principi e tutele che trovano riscontro nelle già vigenti indicazioni in materia di protezione dei dati personali e che ormai da anni l'Autorità sta veicolando anche attraverso numerose e consolidate pronunce e una costante attività sanzionatoria.

5 Profilazione con sistemi automatizzati; cookie di profilazione e modalità di acquisizione del consenso.

Il titolare del trattamento può svolgere attività di profilazione e processi decisionali automatizzati purché sia in grado di soddisfare tutti i principi e disponga di una base legittima per il trattamento[35]. L'art. 22, paragrafo 1, del GDPR prevede garanzie supplementari e limitazioni nel caso di decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, in particolare "*l'interessato ha il diritto di* ***non essere sottoposto*** *a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*."

L'articolo 22, paragrafo 1, stabilisce un divieto generale nei confronti del processo decisionale basato unicamente sul trattamento automatizzato. Tale divieto si applica indipendentemente dal fatto che l'interessato intraprenda un'azione in merito al trattamento dei propri dati personali. In sintesi, l'articolo 22 stabilisce

35 Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottate il 3 ottobre 2017 ed emendate il 6 febbraio 2018 dallo *European Data Protection Board*.

che esiste un divieto generale all'adozione di decisioni completamente automatizzate relative alle persone fisiche, compresa la profilazione, che hanno un effetto giuridico o che incidono in modo analogo significativamente.

Il trattamento ai sensi dell'articolo 22, paragrafo 1, non è consentito in generale, tuttavia, tale divieto si applica esclusivamente in circostanze specifiche quando una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, ha un effetto giuridico o incide in modo analogo significativamente su una persona. Anche in questi casi esistono precise eccezioni che consentono l'esecuzione di tale trattamento. Le garanzie richieste comprendono il diritto di essere informati (di cui agli articoli 13 e 14 – informazioni specificamente significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste per l'interessato) e garanzie, quali il diritto di ottenere l'intervento umano e il diritto di contestare la decisione (di cui all'articolo 22, paragrafo 3). Qualsiasi trattamento che possa presentare un rischio elevato per gli interessati impone al titolare del trattamento di svolgere una valutazione d'impatto sulla protezione dei dati. Oltre ad affrontare qualsiasi altro rischio connesso al trattamento, una valutazione d'impatto sulla protezione dei dati può essere particolarmente utile per i titolari del trattamento che non sono certi che le attività da loro proposte rientrino nella definizione di cui all'articolo 22, paragrafo 1, e, laddove tali attività siano consentite da un'eccezione individuata, non sappiano quali garanzie debbano essere applicate. L'articolo 22, paragrafo 1, si riferisce a decisioni "basate unicamente" sul trattamento automatizzato. Ciò significa che non vi è alcun coinvolgimento umano nel processo decisionale.

Alla luce di quanto sopra, il Garante si è pronunciato in merito ad un trattamento di profilazione automatizzata effettuato da un social network con riferimento a determinati dati di persone maggiorenni iscritte ***senza*** la raccolta di uno specifico consenso, giustificando tuttavia tale trattamento con la base giuridica del legittimo interesse ai sensi dell'art. 6, paragrafo 1, lettera (f) del Regolamento[36].

Il Garante ha avvertito il *social network* che è illecito utilizzare dati personali archiviati nei dispositivi degli utenti per profilarli e inviare loro pubblicità personalizzata in assenza di un esplicito consenso.

In particolare, ha rilevato che[37]: "*(1) non è stato esplicitato quale sia il legittimo interesse perseguito dal titolare e da terzi (i partner pubblicitari) nonché "dagli stessi utenti"; (2) non è stato precisato se il trattamento riguarda anche i dati di carattere particolare e quale sia, in tal caso, l'eccezione prevista dall'art. 9, par. 2, del Regolamento che potrebbe giustificarlo; (3) il test di bilanciamento è indicato in modo generico e insufficiente a consentire una adeguata valutazione della sua correttezza alla luce dei criteri forniti dalla giurisprudenza della Corte di Giustizia dell'Unione europea. Peraltro "il mero adempimento dei doveri di informazione a norma dell'art. 13 del GDPR - menzionato al primo punto del test di bilanciamento - non costituisce una misura di trasparenza da prendere in considerazione per la ponderazione degli interessi conformemente all'art. 6, paragrafo 1, lett. f) del GDPR"; pertanto l'affermazione secondo cui il test di bilanciamento si ritiene soddisfatto per questo trattamento non pare adeguatamente argomentata; (4) la valutazione di impatto che il social*

36 Provvedimento 248 del 7 luglio 2022 del Garante per la protezione dei dati personali.

37 Provvedimento 248 del 7 luglio 2022 del Garante per la protezione dei dati personali.

network sostiene di aver condotto consultando il proprio DPO non è stata fornita, pur a fronte di una esplicita richiesta da parte dell'Ufficio; (5) le misure di verifica dell'età non sono state rappresentate neppure in linea generale e social network si è limitata a richiamare genericamente la circostanza per cui starebbe collaborando con esperti di settore e con l'autorità irlandese; (6) i risultati sin qui prodotti dai meccanismi posti in essere dal social network per la verifica dell'età dell'utente non paiono in grado di escludere che la pubblicità personalizzata possa essere rivolta a minori di 18 anni, e persino ai minori di 14 anni, che rappresentano un bacino presso cui la piattaforma è assai popolare. Inoltre, dall'informativa risultano i seguenti elementi: (i) vengono con alto grado di probabilità effettuate operazioni a fini di "personalizzazione" della pubblicità che comportano verosimilmente l'uso di cookie o di altre tecniche di tracciamento (anche di terze parti); (ii) vengono con alto grado di probabilità effettuate operazioni di profilazione che comportano anche processi di decisione automatizzata ai sensi dell'art. 22 del Regolamento in assenza delle previste garanzie; (iii) nell'informativa il diritto di opposizione non è posto in adeguata evidenza, è citato in modo generico alla fine del testo senza alcun collegamento diretto con l'attività di pubblicità personalizzata.

Tra gli strumenti utilizzati per la profilazione vi è quello dei *cookie* c.d. "di profilazione", che consentono di analizzare i comportamenti di determinati soggetti, identificati o identificabili, nell'uso delle funzionalità offerte attraverso la navigazione al fine di personalizzare la fornitura di un servizio e di inviare messaggi pubblicitari mirati, in linea con le preferenze manifestate dall'utente.

La base giuridica del trattamento di dati derivante da *cookie* di profilazione è quella del consenso - e quindi di una manifestazione di volontà libera, specifica, informata e inequivocabile.

Le modalità di acquisizione del consenso con riferimento ai *cookie* di profilazione sono state recentemente oggetto di chiarimenti da parte del Garante[38], che ha evidenziato la necessità che il soggetto interessato compia una scelta effettiva, non condizionata da possibili conseguenze negative in assenza del consenso. Nello specifico il Garante ha chiarito che deve considerarsi illecito il c.d. "*cookie wall*", ovvero quel meccanismo che impedisce l'accesso a un sito *internet* all'utente che non abbia espresso il proprio consenso alla profilazione attraverso i *cookie*, perché carente del requisito della libertà del consenso. Unica eccezione è il caso in cui l'utente abbia la possibilità di accedere a un contenuto equivalente senza obbligo di prestare il proprio consenso. Nel medesimo provvedimento il Garante ha inoltre precisato che il consenso non può ritenersi acquisito attraverso il mero "*scroll down*" - e quindi un semplice movimento - del cursore, ma deve consistere in un comportamento che esprima una scelta inequivocabile e consapevole e sia registrabile e documentabile.

38 Garante per la protezione dei dati personali, provvedimento 10 giugno 2021, n. 231, doc *web* n. 9677876.

6 Giurisprudenza e Garante: le campagne di "recupero consenso" e invio di offerte promozionali.

L'argomento del consenso al trattamento dei dati personali per finalità di *marketing* e di profilazione è stato oggetto non solo di provvedimenti del Garante, ma di recente anche della giurisprudenza sia di legittimità che di merito.

In particolare, la Corte di Cassazione nel 2018[39] ha stabilito che il consenso è validamente prestato solo se sia espresso liberamente e in modo specifico con riferimento a un trattamento, che deve essere chiaramente individuato.

Con riferimento al caso di specie, si è reso necessario stabilire se il condizionamento del consenso – non conforme alla normativa – possa essere ravvisato nell'ipotesi in cui l'offerta di un determinato servizio da parte del gestore di un sito *internet* sia condizionata al rilascio del consenso all'uso dei dati personali per un successivo invio da parte di terzi di messaggi pubblicitari. Il sito forniva un servizio di *newsletter* su tematiche legate alla finanza, fisco, diritto e lavoro, ma l'utente – una volta prestato il consenso al trattamento dei propri dati personali per la ricezione di tali *newsletter* tematiche – riceveva anche messaggi pubblicitari da parte di altre società.

La Corte ha, pertanto, ravvisato un condizionamento del consenso in tale caso, in quanto l'invio di messaggi pubblicitari da parte di terze società non è un servizio infungibile, la cui rinuncia comporta all'utente un gravoso sacrificio, stabilendo che l'invio dei predetti messaggi – oltre alle *newsletter* tematiche (attività principale del sito) – è valido solo se il consenso sia singolarmente ed inequivocabilmente prestato in riferimento anche a tale servizio, di cui sia data nell'informativa e nel modulo di consenso almeno una descrizione dei settori merceologici o dei servizi cui i messaggi pubblicitari si riferiscono, in modo da rendere edotto l'utente.

La Corte ha ritenuto che l'attività principale del sito (invio di *newsletter* tematiche) non fosse strettamente connessa con l'invio di messaggi pubblicitari da parte di società terze e pertanto senza uno specifico consenso per tali due trattamenti di dati personali, il gestore può continuare a offrire il proprio servizio di *newsletter* senza cedere i dati personali dei propri utenti a società terze.

Anche la giurisprudenza di merito si è, recentemente, espressa sul consenso, stabilendo la legittimità del comportamento di un operatore telefonico che inviava messaggi sms, in assenza di consenso, diretti ad aggiornare le preferenze dei propri clienti sia nuovi che storici in materia di trattamento dei dati personali[40].

In particolare, il Tribunale ha accolto il ricorso presentato dall'operatore telefonico avverso il prov-vedimento emesso dal Garante[41], con cui veniva indicata come non conforme alla normativa l'attività dell'operatore telefonico, che aveva estratto dal proprio CRM i numeri di telefono dei propri clienti (vecchi

39 Corte di Cassazione Civile, Sezione I, Sentenza n. 17278 del 2018.

40 Tribunale di Roma, sentenza 10789 del 1° agosto 2019.

41 Provvedimento n. 437 del 27 ottobre 2016 del Garante per la protezione dei dati personali.

e nuovi) per l'invio di campagne pubblicitarie via sms finalizzate alla raccolta del con-senso e all'aggiornamento delle preferenze.

Il Tribunale di Roma ha accolto il ricorso stabilendo che non è vietato dall'art. 130 del Codice *Privacy* l'invio di messaggi diretti ad acquisire il consenso per la ricezione di messaggi promozionali o pubblicitari, ciò che la norma vieta è l'invio di messaggi contenenti già promozioni e offerte in assenza del preventivo consenso del destinatario. Inoltre, il Tribunale ha anche asserito che secondo l'art. 13 della Direttiva 2002/58/CE è vietato l'utilizzo di sistemi automatizzati di chiamata "a fini di commercializzazione diretta" in assenza del previo consenso, ma non anche l'utilizzo di detti sistemi per acquisire il consenso al futuro e distinto invio di messaggio con finalità commerciali.

Tuttavia, la prima sezione civile della Corte di Cassazione con Sentenza n. 9920 del 28 marzo 2022 ha accolto il ricorso presentato dal Garante, cassando la menzionata pronunzia del Tribunale di Roma e rinviando allo stesso per la determinazione delle spese, sostenendo che se al momento della sottoscrizione del contratto di utenza non è stato prestato apposito consenso, le comunicazio-ni automatizzate successive (nella specie, via sms) volte all'acquisizione del consenso per l'effettuazione di attività di marketing costituiscono un'interferenza illegittima nella vita privata del destinatario; pertanto la mancanza di consenso all'uso di sistemi automatizzati per campagne di "*marketing*" deve intendersi come espressione di dissenso, con la conseguenza che ogni comunicazione automatizzata volta a farne mutare la volontà costituisce essa stessa una comunicazione commerciale non consentita, in quanto finalizzata a commercializzare il servizio aggiuntivo nonostante la mancanza di una preventiva autorizzazione.

7 I tempi di conservazione dei dati per finalità di marketing e profilazione.

Il periodo di conservazione dei dati personali trattati per finalità di *marketing* e profilazione è individuato dal titolare del trattamento che, in applicazione del principio di responsabilizzazione, deve determinare quale sia il periodo di conservazione proporzionato e congruo rispetto alla realizzazione della specifica finalità e indicarlo nell'informativa fornita ai soggetti interessati.

Non esistono cioè periodi di conservazione prestabiliti ma è il titolare a dover condurre in concreto una valutazione, che deve basarsi sulle peculiarità del contesto di mercato e delle proprie esigenze concrete ed effettive, e che deve essere giustificata e documentata dal titolare stesso.

A ispirare questa valutazione è il principio di limitazione del trattamento, ai sensi del quale è lecito trattare dati personali solo per il periodo necessario al conseguimento della finalità per la quale sono stati raccolti, cui si accompagna il principio di minimizzazione dei dati, che consente di trattare solo quei dati che siano adeguati, pertinenti e limitati a quanto necessario rispetto alla finalità per la quale sono stati trattati. Il trattamento deve essere cioè limitato, sia con riferimento alla sua durata sia con riferimento alla quantità di dati trattati, a

quanto necessario al raggiungimento delle finalità individuate dal titolare del trattamento.

I periodi di conservazione individuati dal Garante con provvedimento del 2005 – 12 mesi per finalità di profilazione e 24 mesi per finalità di *marketing*[42] – e quindi prima dell'entrata in vigore del Regolamento, restano un parametro cui i titolari possono fare riferimento nel processo di valutazione necessario all'individuazione del periodo di conservazione. Un utile riferimento è anche costituito dalle argomentazioni elaborate dal Garante in diversi provvedimenti emessi in risposta a istanze di verifica preliminare presentate da titolari del trattamento ai sensi del previgente Codice della *Privacy* al fine di ottenere l'autorizzazione al prolungamento dei tempi di conservazione dei dati personali riferiti alla propria clientela per il loro utilizzo a fini di profilazione e di *marketing*.

Nello specifico il Garante, anche prima dell'entrata in vigore del Regolamento, aveva più volte ritenuto necessario individuare un arco temporale più esteso rispetto a quello previsto dal provvedimento del 2005, basandosi sulla frequenza media di acquisti da parte per la clientela. Con riferimento cioè a specifici settori merceologici quali quelli dei beni di lusso e di fascia alta, il Garante in numerosi provvedimenti ha ritenuto congruo e proporzionato un periodo di conservazione particolarmente esteso (ad esempio 7 e 10 anni) considerando, in ragione della frequenza media di acquisti, che periodi inferiori avrebbero privato di effettivo valore qualsiasi profilazione della clientela[43].

Analoghe considerazioni possono oggi essere elaborate dal titolare del trattamento nell'individuazione del periodo di conservazione dei dati per finalità di *marketing* e profilazione da riportare nella politica interna di conservazione dei dati. Tali considerazioni circa la conformità del trattamento dovranno essere attentamente documentate, in modo che possa essere giustificata e dimostrata l'adeguatezza del periodo di conservazione individuato.

8 Campagne di marketing: utilizzo di banche dati.

Il Garante è più volte intervenuto sul tema della cessione di banche dati nell'ambito della realizzazione di campagne di *marketing* e cioè dell'ipotesi in cui i dati utilizzati per finalità di *marketing* siano raccolti non direttamente dal soggetto promotore della campagna *marketing* ma da un soggetto diverso, autonomo titolare del trattamento, che proceda poi alla cessione della banca dati.

In linea generale il tema è stato affrontato dal Garante con provvedimento del 2013[44], che ne ha delineato i requisiti di liceità, da applicarsi anche nel caso in cui la cessione di dati avvenga tra società a vario titolo collegate a quella che

42 Garante per la protezione dei dati personali, provvedimento 24 febbraio 2005, doc *web* 1103045.

43 Garante per la protezione dei dati personali, provvedimento 22 maggio 2018, n. 320, doc. web n. 9018628; 9 maggio 2018, n. 274, doc. *web* n. 8998319; 7 novembre 2013, n. 500, doc. *web* n. 2920245; 24 aprile 2013, n. 219, doc. *web* n. 2499354; 30 maggio 2013, n. 263, doc. *web* n. 2547834.

44 Garante per la protezione dei dati personali, Linee guida in materia di attività promozionale e contrasto allo *spam*, 4 luglio 2013, n. 330, doc. *web*. 2542348.

ha raccolto i dati, e prima ancora con provvedimento del 2003[45]. Requisito essenziale è quello della specificità del consenso: la cessione di dati non può cioè basarsi sull'acquisizione di un generico consenso dei soggetti interessati ma è necessario un consenso specifico per la comunicazione o cessione di dati a terzi per fini promozionali, distinto da quello richiesto dal titolare per svolgere attività promozionale. I soggetti terzi devono essere puntualmente individuati nella informativa rilasciata ai soggetti interessati o in alternativa deve essere indicata la categoria economica o merceologica di riferimento. Nel caso in cui l'informativa data dal soggetto cedente non contenga già gli elementi relativi al trattamento che verrà svolto dal soggetto terzo, quest'ultimo, una volta ricevuti i dati, è tenuto a rilasciare la propria informativa, che indichi anche l'origine dei dati comunicati.

I più recenti provvedimenti del Garante sul tema della cessione delle banche dati consolidano i precedenti orientamenti, delineando chiaramente i rigidi obblighi cui il titolare cessionario della banca dati è soggetto.

Chi acquista una banca dati deve cioè verificare il rispetto degli adempimenti vigenti rispetto a tutte le anagrafiche acquisite e quindi, tra l'altro, verificare che ciascun soggetto interessato abbia validamente acconsentito alla comunicazione dei propri dati e al loro successivo utilizzo ai fini di invio di materiale pubblicitario. Come confermato nel marzo 2021 nel provvedimento emesso nei confronti di Mediacom S.r.l.[46], tale verifica deve essere condotta, ove possibile, con riferimenti a tutti i soggetti interessati e "*deve garantire anche l'esattezza, correttezza e aggiornamento dei dati trattati, anche perché ad ognuno dei relativi interessati va riconosciuta, indefettibilmente, la tutela effettiva dei diritti fondamentali alla protezione dei dati personali e alla tranquillità individuale che spesso può venire in rilievo nello svolgimento dell'attività di telemarketing*". Ancora, il Garante precisa che il titolare del trattamento deve inoltre tener traccia delle verifiche effettuate con specifico riferimento "*alla logica e ai parametri utilizzati; ai risultati ottenuti; ai dati in concreto verificati; alle valutazioni effettuate al riguardo, unitamente alle relative argomentazioni*".

Con provvedimento del maggio 2021 emesso nei confronti di Iren Mercato S.p.A.[47], il Garante ha precisato che il consenso degli interessati alla cessione dei propri dati personali per finalità di *marketing* vale per una sola cessione e non anche per le successive. Pertanto, l'acquisizione di liste di dati personali da un autonomo titolare, a sua volta cessionario di dette liste da una società diversa iniziale titolare del trattamento, non può basarsi sul consenso rilasciato dagli interessati a quest'ultima, ma richiede che venga prestato un ulteriore consenso alla successiva comunicazione da parte della società intermediaria.

Il Garante ha poi evidenziato che il legittimo interesse può costituire idonea base giuridica del trattamento per finalità di *marketing* solo in presenza di

45 Garante per la protezione dei dati personali, *Spamming*. Regole per un corretto uso dei sistemi automatizzati e l'invio di comunicazioni elettroniche, 29 maggio 2003, doc. *web* 29840.

46 Garante per la protezione dei dati personali, Ordinanza di ingiunzione nei confronti di Mediacom S.r.l., 11 marzo 2021, n. 99, doc. *web*. n. 9577065

47 Garante per la protezione dei dati personali, Ordinanza di ingiunzione nei confronti di Iren Marcato S.p.A., 13 maggio 2021, n. 192, doc. *web* n. 9670025.

specifici requisiti. Nello specifico, secondo quanto previsto al Considerando 47 GDPR il ricorso al legittimo interesse è lecito solo a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato. È quindi necessario che il titolare proceda a un attento bilanciamento, adeguatamente documentato, tra il proprio interesse e i diritti e le aspettative degli interessati circa il trattamento dei relativi dati personali[48].

Tale bilanciamento deve essere condotto e documentato prima che il trattamento abbia inizio, non essendo quindi possibile ricorrere retroattivamente alla base giuridica dell'interesse legittimo in caso di problemi di validità del consenso.

Nel provvedimento emesso nei confronti di Fastweb nel marzo 2021[49], il Garante ha evidenziato che la necessità di uno specifico consenso alla comunicazione di dati a terzi in caso di cessione non può essere elusa dalla designazione dei partner quali responsabili del trattamento, qualora in concreto tali soggetti non svolgano le funzioni del responsabile. Il Garante, richiamando precedenti provvedimenti, precisa inoltre che obiettivo delle disposizioni di cui agli articoli 6 e 7 del Regolamento e dei considerando 42 e 43 è quello di conferire all'interessato il pieno controllo dei trattamenti di dati personali per i quali egli stesso ha prestato il consenso precisando come tale controllo "…*verrebbe meno in ogni caso in cui il complesso delle disposizioni sopra richiamato potesse essere eluso da arbitrarie scelte in ordine alla veste giuridica che, di volta in volta, i soggetti del trattamento concordassero di assumere al fine di mascherare proprio quegli effetti a catena difficilmente riconducibili all'iniziale manifestazione di volontà dell'interessato*".

48 Viene in particolare richiamato il provvedimento Garante per la protezione dei dati personali 15 gennaio 2020, n. 7, doc. web 9256486 ai sensi del quale "… *il legittimo interesse, di cui all'art. 6, par. 1, lett. f), del Regolamento - già previsto sia dall'abrogata direttiva 95/46/CE, nonché dal Codice previgente alle modifiche apportatevi dal d.lgs. n. 101/2018 (d.lgs. n. 196/2003, art. 24, comma 1, lett. g) - non può surrogare - in via generale - il consenso dell'interessato quale base giuridica del marketing. Invero, il Regolamento stesso – come già la direttiva 95/46/CE all'art. 7, comma 1, lett. f) - lo ammette solo a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventuali-tà che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine*".

49 Garante per la protezione dei dati personali, Ordinanza di ingiunzione nei confronti di Fastweb S.p.A., 25 marzo 2021 doc. *web*. n. 9570997.

CAPITOLO 4 di Antonio Bana, Francesca Bevilacqua,
Paola De Pascalis e Piero Magri

Il sistema di compliance 231 e gli indicatori ESG

Il sistema di compliance 231 e gli indicatori ESG: i futuri pilastri di controllo in ottica sostenibilità e prevenzione del rischio

SOMMARIO: 1. Premessa – 2. La responsabilità sociale di impresa – 3. La sostenibilità – 4. I criteri ESG – 5. Sostenibilità, gestione dei rischi e "compliance integrata" – 6. La gestione dei rischi con adeguati assetti organizzativi, predisposizione di un efficace sistema di controllo interno e principi della sostenibilità: spunti normativi – 7. Sistema di controllo interno e modello organizzativo 231 nell'ottica di una *compliance* integrata – 8. ESG e contenuti del modello 231: punti di convergenza – 9. Conclusioni – 10. Bibliografia

1. Premessa

L'adozione di un Modello 231, quale strumento volto a gestire, ridurre o eliminare una serie di rischi-reato e quale volano culturale nello spingere l'impresa a perseguire obiettivi di non esclusivo profitto ma anche di portata etica e valoriale, può certamente costituire un valore aggiunto anche nell'affrontare la sfida posta dalla "*Responsabilità Sociale d'Impresa*" e dalla "*Sostenibilità"*.

Sono infatti numerose e significative le correlazioni e interazioni tra i Modelli 231 e gli "*Obiettivi di Sviluppo Sostenibile*".

Il Modello 231, oltre ad essere uno degli [adeguati] assetti organizzativi societari nonché parte fondamentale del sistema di controllo interno, può ben essere considerato in coordinamento con i parametri ESG - in particolare quello della *Governance* – e quindi quale strumento di sostenibilità.

Tale approccio, inoltre, risponde pienamente alla sempre crescente – ormai riconosciuta anche a livello normativo - esigenza di una *compliance* integrata.

Fattori ESG, sostenibilità aziendale, *corporate social responsibility* (CSR), dichiarazioni sulle informazioni non finanziarie (DNF) sono nozioni correlate a un *trend* normativo in grande evoluzione (a livello internazionale, comunitario e nazionale) che gradualmente impatterà su tutte le imprese, a partire da quelle di più grandi dimensioni fino alle PMI.

2. La responsabilità sociale di impresa

All'interno del mercato sia globale sia locale, le imprese non vivono un'esistenza a sé stante, ma vivono e agiscono in un tessuto sociale che comprende diversi soggetti, tra cui spicca sicuramente una società civile ormai molto attenta all'operato imprenditoriale.

Nei sistemi di gestione aziendale, l'attenzione ai c.d. *stakeholders* è divenuta di importanza cruciale per le imprese e lo sviluppo nel tempo di relazioni positive con tali soggetti può diventare un elemento di valore aggiunto per l'impresa.

In questo rinnovato contesto culturale si inserisce la c.d. responsabilità sociale d'impresa (*Corporate Social Responsibility*), cornice in cui inquadrare - sostanzialmente - i profili etici e sociali della gestione strategica e dello sviluppo d'impresa.

In sostanza, si chiede all'impresa di adottare anche un comportamento socialmente responsabile, che possa rispondere alle aspettative economiche, ambientali, sociali di tutti i portatori di interesse (*stakeholders*), e che possa – e contestualmente e come conseguenza - raggiungere anche l'obiettivo di un vantaggio competitivo e di massimizzazione degli utili di lungo periodo.

In questa nuova prospettiva anche culturale, si ritiene ormai - e si auspica - che un prodotto non sia apprezzato unicamente per le caratteristiche qualitative esteriori o funzionali e che l'impegno "etico" di un'impresa sia parte fondamentale nella cosiddetta *catena del valore*, nell'ottica di nuovi percorsi e leve competitive coerenti con uno "sviluppo sostenibile" per la collettività.

3. La sostenibilità

Se il concetto di sostenibilità si riferisce alla possibilità di mantenere una realtà, un contesto, un processo in una condizione di equilibrio per un tempo indefinibile, nell'ambito dell'impresa si intende la condizione in cui tutte le componenti di questa - lo sfruttamento delle risorse, il piano degli investimenti, l'orientamento dello sviluppo tecnologico e le modifiche istituzionali – siano tutte in armonia nella direzione di far fronte, anche in prospettiva futura, ai bisogni e alle aspirazioni collettive.

Il principio correlato al concetto di sostenibilità è allora lo sviluppo sostenibile: lo sviluppo volto a soddisfare i bisogni della generazione presente senza compromettere la capacità delle generazioni future di far fronte ai propri.

4. I criteri ESG

Legato all'investimento responsabile, l'acronimo ESG, ossia «*Environmental, Social, Governance*», è utilizzato in ambito economico/finanziario per indicare tutte quelle attività che, all'interno di una impresa, perseguono gli obiettivi

tipici della gestione finanziaria tenendo però in considerazione anche aspetti di natura ambientale, sociale e di *governance*.

La sigla ESG individua quindi un insieme di parametri alla cui stregua valutare il carattere più o meno sostenibile di un'impresa, di un fondo, di un investimento o titolo speculativo. Questi parametri corrispondono a un insieme di *standard* operativi cui devono essere ispirate le *operations* di un'azienda per garantire il raggiungimento di determinati risultati a livello ambientale, sociale e di *governance* dell'impresa.

In estrema sintesi, si tratta di orientare l'attività imprenditoriale secondo taluni principi che esprimono il rispetto dell'ambiente e della relativa normativa vigente ("*Environmental*"), l'osservanza di valori di non discriminazione ed inclusione nei contesti sociale e lavorativo ("*Social*"), l'efficienza e l'adeguatezza dell'assetto organizzativo interno adottato e – infine – l'osservanza da parte della Società, dei propri dipendenti e collaboratori delle leggi e prassi diffuse volte a prevenire i fenomeni corruttivi ("*Governance*").

Si vedrà nel prosieguo come questi elementi di natura valoriale potranno costituire gli elementi di collegamento con il "Sistema 231".

5. Sostenibilità, gestione dei rischi e "compliance integrata"

La Sostenibilità è allora divenuta un elemento imprescindibile di cui tenere conto nella definizione degli obiettivi, delle strategie aziendali nonché nelle scelte di *governance* connesse alla predisposizione degli adeguati assetti organizzativi. La *compliance* - come predisposizione di presidi per gestire e mitigare determinati tipi di rischi e quale criterio di conformità alla legge - non può non rappresentare un elemento fondamentale della Responsabilità sociale di impresa e - di conseguenza – non può ignorare – quali proprie componenti - i parametri ESG.

Allora diventa necessario integrare l'assetto di controlli diretto ad identificare e prevenire i rischi di non conformità normativa, con presidi adeguati a governare quei possibili rischi ESG che possano direttamente o indirettamente causare conseguenze negative per società e *stakeholders*.

La *compliance* normativa, in questa accezione, diventa quindi un formidabile strumento di competitività per l'impresa che l'adotta come filosofia di gestione, integrata con i processi operativi.

Se l'obiettivo è il successo sostenibile, ogni organizzazione deve definire i propri obiettivi strategici anche in una logica ESG, identificando e valutando i fattori che possono influire sul loro raggiungimento, predisponendo piani di azione e mezzi di controllo idonei a mitigare le potenziali vulnerabilità. E d'altronde, questo *modus operandi*, organizzato e strutturato, è caratteristico dei sistemi di controllo interno e gestione del rischio ed è un modello di riferimento ormai assodato per i sistemi di *compliance*.

È ovvio poi che un successo sostenibile non può prescindere da un sistema di gestione dei rischi e quindi dalla creazione di valore di lungo periodo.

I rischi di *compliance* sono molteplici e dinamici in funzione della variazione del contesto di riferimento (ad es. Covid-19).

Ovviamente però, si pone la necessità di affrontare i rischi, dalle diverse citate prospettive – *compliance* e ESG – in una ottica integrata; si rende cioè necessaria un'opera di razionalizzazione e sintesi.

Le ultime linee guida di Confindustria circa la redazione dei Modelli 231/01 si esprimono chiaramente sulla necessità di una *compliance integrata*

3.1 Sistema integrato di gestione dei rischi

È ormai dato acquisito che il rischio di compliance, ossia di non conformità alle norme, comporta per le imprese il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni reputazionali in conseguenza di violazioni di norme imperative[14] ovvero di autoregolamentazione, molte delle quali rientrano nel novero dei reati di cui al D.Lgs. 231/2001.
Ciò posto, la gestione dei numerosi obblighi di *compliance*, secondo un approccio tradizionale, può risultare connotata da una pluralità di processi, informazioni potenzialmente incoerenti, controlli potenzialmente non ottimizzati, con conseguente ridondanza nelle attività.

Il passaggio ad una *compliance* integrata potrebbe permettere invece agli Enti di:

- razionalizzare le attività (in termini di risorse, persone, sistemi, ecc.);
- migliorare l'efficacia ed efficienza delle attività di *compliance*;
- facilitare la condivisione delle informazioni attraverso una visione integrata delle diverse esigenze di *compliance*, anche attraverso l'esecuzione di *risk assessment* congiunti, e la manutenzione periodica dei programmi di compliance (ivi incluse le modalità di gestione delle risorse finanziarie, in quanto rilevanti ed idonee ad impedire la commissione di molti dei reati espressamente previsti come fondanti la responsabilità degli enti).

Tra le novità di maggior rilievo introdotte, si può evidenziare il paragrafo dedicato al "*Sistema integrato di gestione dei rischi"* che muove dal *"dato acquisito che il rischio di compliance, ossia di non conformità alle norme, comporta per le imprese il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni reputazionali in conseguenza di violazioni di norme imperative ovvero di autoregolamentazione, molte delle quali rientrano nel novero dei reati di cui al D.Lgs. 231/2001*".

Spetta quindi a una buona *governance* il compito di decidere da dove iniziare e come raggiungere il proprio obiettivo di sostenibilità, sapendo di poter contare sul supporto di diversi strumenti messi a disposizione dal legislatore e volutamente interconnessi.

Appare chiaro che i fattori ESG e, più in generale, il nuovo paradigma della sostenibilità aziendale, avranno un impatto significativo negli anni a venire anche sulle vicende organizzative e della responsabilità amministrativa delle società ed enti.

6. La gestione dei rischi con adeguati assetti organizzativi, predisposizione di un efficace sistema di controllo interno e principi della sostenibilità: spunti normativi

L'art. 2086 c.c., rubricato "Gestione dell'impresa" recita:

"*L'imprenditore, che operi in forma societaria o collettiva, ha il dovere di istituire un* ***assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa, anche in funzione della rilevazione tempestiva della crisi dell'impresa e della perdita della continuità aziendale****, nonché di attivarsi senza indugio per l'adozione e l'attuazione di uno degli strumenti previsti dall'ordinamento per il superamento della crisi e il recupero della continuità aziendale*".

e, altrettanto, l'art. 2381 c.c., nel disciplinare il ruolo degli organi di gestione, prevede al co. 3° che

"***Il consiglio di amministrazione*** *(…) sulla base delle informazioni ricevute* ***valuta l'adeguatezza dell'assetto organizzativo, amministrativo e contabile della società****; quando elaborati, esamina i piani strategici, industriali e finanziari della società; valuta, sulla base della relazione degli organi delegati, il generale andamento della gestione*".

e al co. 4° che

"***Gli organi delegati curano che l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell'impresa*** *e riferiscono al consiglio di amministrazione e al collegio sindacale, con la periodicità fissata dallo statuto e in ogni caso almeno ogni sei mesi, sul generale andamento della gestione e sulla sua prevedibile evoluzione nonché sulle operazioni di maggior rilievo, per le loro dimensioni o caratteristiche, effettuate dalla società e dalle sue controllate*".

Il nuovo codice di *Corporate Governance*, alle sue Raccomandazioni, dispone che

"***1. L'organo di amministrazione***:

a) *esamina e approva il piano industriale della società e del gruppo ad essa facente capo, anche in base all'analisi dei temi rilevanti per la* ***generazione di valore nel lungo termine*** *effettuata con l'eventuale supporto di un comitato del quale l'organo di amministrazione determina la composizione e le funzioni;*

b) *monitora periodicamente l'attuazione del piano industriale e valuta il generale andamento della gestione, confrontando periodicamente i risultati conseguiti con quelli programmati;*

c) *definisce* ***la natura e il livello di rischio compatibile con gli obiettivi strategici della società****, includendo nelle proprie valutazioni tutti gli elementi che possono assumere rilievo nell'ottica del successo sostenibile della società;*

d) *definisce il sistema di governo societario della società e la struttura del gruppo ad essa facente capo e valuta* ***l'adeguatezza dell'assetto organizzativo, amministrativo e contabile*** *della società e delle controllate aventi rilevanza strategica, con particolare riferimento al sistema di controllo interno e di gestione dei rischi; definisce la natura e il livello di rischio compatibile con gli obiettivi*

strategici della società, includendo nelle proprie valutazioni tutti gli elementi che possono assumere rilievo nell'ottica del successo sostenibile della società (…)".

La Direttiva 254/14/UE, considerando n. 6 circa l'"*informativa non finanziaria*", prevede che:

"*Per migliorare l'uniformità e la comparabilità delle informazioni di carattere non finanziario comunicate nell'Unione, è opportuno che talune imprese di grandi dimensioni siano tenute a elaborare* ***una dichiarazione di carattere non finanziario contenente almeno le informazioni sociali e ambientali, attinenti al personale, al rispetto dei diritti umani e alla lotta contro la corruzione attiva e passiva****. La dichiarazione dovrebbe comprendere la descrizione delle* ***politiche*** *applicate in materia, dei* ***risultati*** *conseguiti e dei* ***rischi*** *connessi e dovrebbe essere inclusa nella relazione sulla gestione dell'impresa interessata. La dichiarazione di carattere non finanziario dovrebbe altresì contenere informazioni sulle* ***procedure*** *in materia di* ***dovuta diligenza*** *applicate dall'impresa,* ***tra l'altro per quanto riguarda le catene di fornitura e subappalto delle imprese****, ove opportuno e proporzionato, onde individuare, prevenire e attenuare le ripercussioni negative esistenti e potenziali (…)*".

Da ultimo, il Decreto legislativo 30/12/2016, n. 254 (attuativo della direttiva 2014/95/UE) rinvia esplicitamente al Sistema 231:

"*1. La dichiarazione individuale di carattere non finanziario, nella misura necessaria ad assicurare la comprensione dell'attività di impresa, del suo andamento, dei suoi risultati e dell'impatto dalla stessa prodotta, copre i temi ambientali, sociali, attinenti al personale, al rispetto dei diritti umani, alla lotta contro la corruzione attiva e passiva, che sono rilevanti tenuto conto delle attività e delle caratteristiche dell'impresa, descrivendo almeno:*

a. ***il modello aziendale di gestione ed organizzazione delle attività dell'impresa, ivi inclusi i modelli di organizzazione e di gestione eventualmente adottati ai sensi dell'articolo 6, comma 1, lettera a), del decreto legislativo 8 giugno 2001, n. 231, anche con riferimento alla gestione dei suddetti temi****;*

b. le ***politiche*** *praticate dall'impresa, comprese quelle di dovuta diligenza, i risultati conseguiti tramite di esse ed i relativi indicatori fondamentali di prestazione di carattere non finanziario;*

c. principali ***rischi****, ivi incluse le modalità di gestione degli stessi generati o subiti, connessi ai suddetti temi e che derivano dalle attività dell'impresa, dai suoi prodotti, servizi o rapporti commerciali, incluse, ove rilevanti, le catene di fornitura e subappalto (…)*".

7. Sistema di controllo interno e Modello organizzativo 231 nell'ottica di una *compliance* integrata

Nell'ambito degli adeguati assetti organizzativi, del sistema di controllo interno a prevenzione e gestione del rischio, ruolo fondamentale è giocato dai Modelli di organizzazione, gestione e controllo ai sensi del d.lgs. 231/2001 (nel prosieguo Modello/i 231). Anche i Modelli, infatti, adottano una logica *risk-ba-*

sed, dove il rischio è rappresentato dalla possibilità di commettere uno (o più) reati indicati nel catalogo.

Il sistema di controllo, quindi, per essere efficace nel mitigare i possibili rischi deve prevedere la definizione e l'implementazione di presidi di controllo, tipicamente di natura preventiva, per indirizzare l'operato di soggetti apicali, dipendenti, collaboratori e *partner* commerciali. L'identificazione e la valutazione di applicabilità del rischio è fatta attraverso un processo ben definito, il *risk assessment*; l'*output* che ne deriva definisce il profilo di rischio specifico per l'organizzazione.

L'adozione del Modello 231 richiede un approccio delle imprese ai propri processi produttivi secondo **la lente del rischio della commissione di reati**. Ciò implica un'attenzione particolare alle specifiche aree **sensibili che** andranno presidiate nell'ottica **di prevenire il verificarsi, nel loro ambito, di condotte di rilevanza penale** che dagli apicali e dai dipendenti si estendano all'ente.

L'Organismo di Vigilanza può - anzi deve - assumere il ruolo di baricentro nell'ambito del sistema di controllo interno da cui riceve e a cui trasmette fondamentali informazioni:

Il Modello vuole valorizzare la cultura aziendale e la filosofia manageriale attraverso la formalizzazione di un codice etico e un *corpus* di regole e di procedure strumentalia al raggiungimento della finalità espressa dalla normativa.

La *compliance* al d.lgs. 231/2001 nasce con un approccio orientato all'ottimizzazione e alla valorizzazione del sistema di controllo interno sviluppato dall'ente in un momento anteriore all'adozione del Modello; per l'identifi-

cazione dei protocolli le Linee guida di Confindustria suggeriscono infatti di considerare quanto già presente nei sistemi aziendali. Il questo modo, il Modello 231 si posiziona, già di per sé, come sistema di *compliance* sostenibile in quanto integrata.

Ecco allora che il sistema di prevenzione dei reati attuato da un'impresa con l'adozione del Modello di organizzazione, gestione e controllo ai sensi del d.lgs. 231/2001si incasella a buon diritto negli **indicatori ESG** (*Environmental Social Governance*), ovvero **quei criteri di misurazione delle attività ambientali, sociali e della governance di un'organizzazione aziendale idonei a definire standard operativi ottimali a cui devono ispirarsi i processi produttivi**.

Sotto tale angolo visuale, dunque, il sistema 231 - incentrato sul *risk approach* - contribuisce alla **crescita di valore dell'azienda** laddove la sua operatività sia effettiva e non solo formale.

La crescente attenzione ai **temi dell'agire sostenibile**, come strumento di raggiungimento di maggiori standard di benessere sociale e di miglioramento della qualità della vita delle generazioni future, impone necessariamente agli operatori economici di orientare anche l'attività di impresa a tali obiettivi.

Individuare i **rischi/opportunità legati alla sostenibilità** diventa, dunque, di per sé un obiettivo strategico, da integrare nei processi aziendali, in una rinnovata concezione della gestione di impresa e dei suoi rischi non più focalizzata solo sul rischio caratteristico, ma attenta alle dinamiche organizzative interne e al contempo al complesso reticolato di relazioni e di interessi esterni all'impresa.

In questo articolato contesto, diventa quindi essenziale, anche al fine di rendere efficienti costi e risorse e **massimizzare i vantaggi competitivi dell'impresa**, da un lato, sintetizzare tutti i momenti del controllo aziendale secondo una visione integrata, dall'altro, perseguire costantemente la diffusione a tutti i livelli aziendali di una cultura della legalità, della responsabilità sociale e dell'etica degli affari.

La naturale vocazione del Modello 231 quale strumento di sensibilizzazione e responsabilizzazione degli *stakeholders*, oltre alla intrinseca trasversalità dei relativi ambiti di intervento, fa dello stesso uno strumento privilegiato per un **approccio integrato alla gestione dei rischi, anche in ottica ESG**.

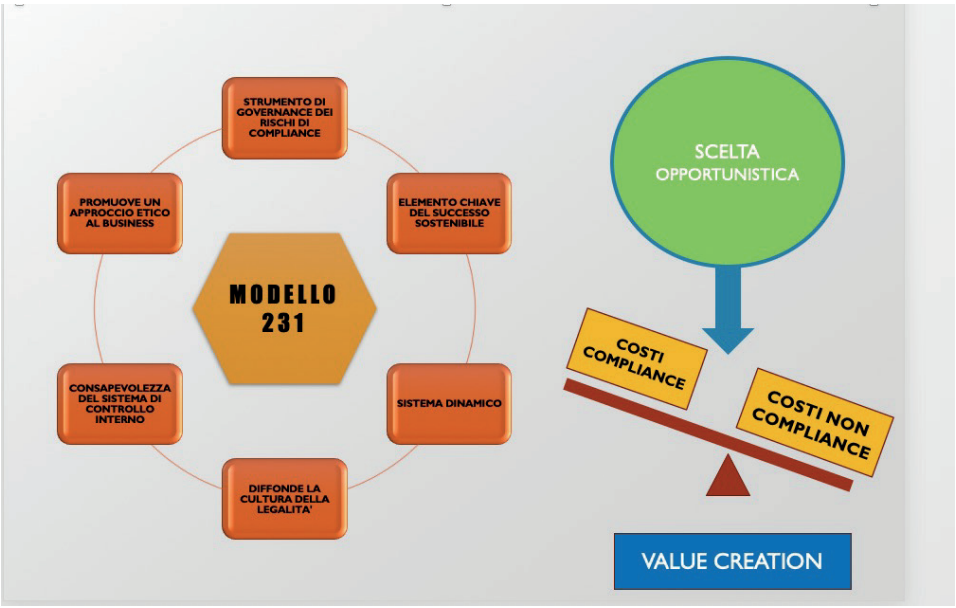
I **modelli di *compliance* integrata** possono e devono essere strumenti di governance funzionali al raggiungimento degli obiettivi strategici dell'impresa per garantire un **successo sostenibile e creare valore**.

A tal fine è necessario avere un **approccio non formalistico/burocratico**, ma imperniato sull'efficacia e l'efficienza del sistema di controllo interno valorizzando le sinergie per mitigare i rischi.

Tale risultato è ottenibile anche grazie a:

- *top level committment*;
- cultura del controllo e dell'etica di impresa;
- coordinamento tra gli attori del sistema di controllo interno.

L'Organismo di Vigilanza può essere il baricentro dei sistemi di compliance integrata, un pilastro del successo sostenibile aziendale e della creazione del valore.



Tra i vantaggi indiretti che ad un'azienda possono derivare dall'adozione del Modello231 vanno certamente annoverati l'**aumento della credibilità** e della reputazione sul mercato - soprattutto per quelle che partecipano a bandi e a procedure di accreditamento pubblico - e il contributo al miglioramento del proprio *business*.

8. ESG e contenuti del Modello 231: punti di convergenza

Alla luce di tutto ciò si vuole qui evidenziare la **stretta correlazione tra queste tematiche e la "*compliance 231*"**. Sottese alle politiche di sostenibilità ed ai principi ESG vi sono, infatti, molti aspetti di connessione con le aree sensibili e i rischi reato previsti dal D.lgs. 231/2001.

Si veda a titolo esemplificativo:

Environment

nel cui ambito sono ricompresi ad esempio i rischi legati al cambiamento climatico, alle non conformità alla normativa ambientale, alla gestione dei rifiuti e delle risorse idriche ecc. – è associabile alla prevenzione dei:

- Reati ambientali;
- Reati contro la P.A. (es. in tema di urbanizzazione e speculazione edilizia)

Social

le politiche di genere, i diritti umani, gli *standard* lavorativi e sindacali nel cui alveo si possono collocare i rischi correlati ai diritti delle persone e/o dei lavoratori (discriminazioni di genere, violazioni dei diritti relativi alla salute di persone e dei dipendenti aziendali, illeciti in materia di dati personali e/o della sicurezza informatica ecc.) – richiama la prevenzione dei:

- Reati contro la Pubblica Amministrazione legati all'erogazione di finanziamenti pubblici (ancor più rilevante a seguito dei contributi e delle facilitazioni connesse all'emergenza Covid) ovvero legati alle diverse forme di corruzione e/o ai rapporti con le Autorità di Vigilanza.
- Reati contro la salute e sicurezza dei lavoratori;
- Reati informatici, con particolare riferimento alla *compliance* in materia di GDPR (Regolamento UE 2016/679);
- Reati contro la personalità individuale, con particolare riguardo alla recente tematica del cd. "*caporalato*" che richiede standard di maggiore attenzione nella scelta dei fornitori di servizi,
- Reati legati ai lavoratori irregolari e alle dichiarazioni all'autorità giudiziaria.

Governance

le pratiche di governo societarie, le politiche di retribuzione dei *manager*, la composizione del consiglio di amministrazione compresa la presenza di consiglieri indipendenti e le politiche di diversità nella composizione del CdA, le procedure di controllo, i comportamenti dei vertici e dell'azienda in termini di rispetto delle leggi e della deontologia possono impattare sui rischi connessi all'assetto societario, alla gestione delle risorse finanziarie e ai rapporti tra la società e le istituzioni pubbliche – quindi possono essere rilevanti rispetto ai:

- Reati contro la pubblica amministrazione;
- *Market abuse*;
- Reati tributari e reati di contrabbando;
- Reati societari, con particolare riguardo alle false comunicazioni sociali;
- Reati di riciclaggio e autoriciclaggio;
- Reati associativi e transnazionali funzionali alla commissione di altri reati 231.

L'implementazione del Modello 231, ad esempio, si pone in linea e contribuisce al perseguimento degli SDGs 16 e 17, definendo i principi, anche etici e comportamentali, che ispirano l'azione aziendale.

Anche in questo caso, la trasversalità nella natura dei reati diventa, per le attività di controllo, una condizione che le abilita a indirizzare, potenzialmente, più di un'area ESG.

Prendiamo, a titolo di esempio, uno dei processi sensibili a diverse aree di reato: il processo di accreditamento del fornitore.

Dal punto di vista della *governance* aziendale, la chiara definizione di criteri di valutazione operativi (ad esempio, requisiti tecnici, tempistiche e modalità di consegna) ed economici (ad esempio, solidità della struttura societaria, applicazione di prezzi di mercato, standardizzazione delle condizioni contrattuali) per decidere se includere un potenziale fornitore nella propria *vendor list* rappresenta ormai un elemento essenziale per indirizzare diversi reati previsti dal catalogo; oggi, in una logica ESG, gli stessi criteri possono aiutare a comprendere l'approccio del fornitore nei confronti dell'ambiente (ad esempio, in relazione all'utilizzo di sostanze nocive o impattanti per il clima, gli ambienti terrestri e quelli marini) e la trasparenza nella gestione delle attività, con l'attenzione rivolta verso gli aspetti più sociali (ad esempio, condizioni di lavoro eque per i collaboratori, produzione responsabile di beni e servizi).

Per esemplificazione grafica:

9. Conclusioni

L'evoluzione normativa nazionale e sovranazionale richiede alle imprese un approccio integrato di *compliance* capace di far dialogare sistemi di controllo diversi. Nel governo dell'impresa risulta infatti fondamentale sviluppare una comune metodologia per una efficiente impostazione delle attività di prevenzione e gestione dei rischi di impresa. Accanto alla funzione sua propria di ridurre le opportunità di commissione di illeciti e fungere da contrappunto alle spinte criminose che possono sprigionarsi nelle organizzazioni, il Modello 231 deve svolgere un ruolo virtuoso nella *governance* aziendale, contribuendo alla

creazione di valore e a garantire la sostenibilità del *business* in una prospettiva di lungo periodo.

Analogamente, l'Organismo di Vigilanza ha il compito di sovrintendere al funzionamento e all'osservanza dei Modelli di organizzazione, gestione e controllo e di curarne il relativo aggiornamento, e, unitamente al *management* aziendale, risponde alla sfida di saper trasformare le indicazioni normative in opportunità di miglioramento dell'efficacia e dell'efficienza della *governance* dell'Ente.

Il programma di sostenibilità insieme ai Modelli 231 ha l'obiettivo di supportare le imprese in una transizione che porti ad allineare gli obiettivi professionali con quelli della società civile, promuovendo una linea di *governance* eticamente sostenibile così da trasformare l'impegno delle imprese verso l'ambiente, la società e l'etica in un vero e proprio *asset* in grado di incidere direttamente sui risultati di *business* delle aziende stesse e di determinarne il valore.

Gli obiettivi da raggiungere e gli spunti di riflessione che sono emersi durante la *Round Table* possono così riassumersi:

- l'interpretazione del quadro normativo in materia di *Compliance* aziendale
- la rappresentazione degli incentivi a investire in *Compliance* e il ruolo dell'OdV nel sistema 231
- lo sviluppo di una *governance* orientata alla legalità e all'etica imprenditoriale
- l'implementazione del dialogo tra le funzioni e gestire il sistema dei controlli
- l'attivazione dei flussi informativi e la gestione dei sistemi di *Whistleblowing*
- la comprensione e la progettazione dei profili di integrazione fra Modello 231, fattori ESG legati al *business*.

L'acronimo ESG indica tre fattori fondamentali per verificare, misurare e sostenere l'impegno in termini di sostenibilità di una impresa o di un'organizzazione.

Nello specifico, gli indicatori ESG rappresentano una serie di criteri di misurazione delle attività ambientali, sociali e della *governance* di un'organizzazione, che si concretizzano in un insieme di *standard* operativi a cui si devono ispirare le operazioni di un'azienda.

Negli ultimi anni le imprese si stanno interrogando su come integrare i processi aziendali che governano la gestione dei rischi d'impresa e le tematiche di sostenibilità.

Gli ordinamenti giuridici e le imprese europee stanno convergendo verso un **modello di impresa per il raggiungimento integrato di obiettivi** di lungo termine *environmental*, sociali e di *governance* (ESG).

1. si afferma un modello di **corporate governance** non più basato sul profitto come unico o primario scopo sociale, ma che **recepisce i valori della responsabilità di impresa** (*corporate social responsibility*) tra i pilastri delle scelte organizzative e strategiche.
2. l'**allargamento del perimetro** dell'interesse sociale oltre la sfera dei soci e dei creditori sociali ed il riconoscimento esplicito dei profili socio-ambientali fra i poteri-doveri degli amministratori nella guida e nella valutazione degli interessi di tutti gli *stakeholder*.
3. i **doveri e le responsabilità degli amministratori** si misurano nel **perseguimento di una pluralità di interessi a beneficio degli azionisti**, ma anche di tutti coloro che entrano in contatto con la società, di tutti gli *stakeholder*.

Le imprese, nel percorso verso la sostenibilità integrata, devono:

- definire una **strategia di sostenibilità** che esce dal proprio perimetro aziendale per nuovi engagement dei clienti e dei fornitori, per la creazione e lo sviluppo di un'economia circolare
- definire un **piano di sostenibilità** integrato e/o presentato nei Piani Industriali
- definire un sistema di governance per la **diffusione all'interno dell'impresa della cultura sulla CSR – corporate sustainability reporting**
- condividere la centralità del bilancio di sostenibilità come strumento di comunicazione delle ***performance* di sostenibilità**

Il bilancio di sostenibilità è la misurazione basata su indicatori KPI specifici, validata da audit esterni con standard di rendicontazione di un percorso passato, in corso e futuro. Il processo è ben più complesso della mera misurazione.

All'interno degli ESG **l'ambiente rappresenta la sfida principale** in termini anche di risorse necessarie, con continui nuovi *committment* e *target* ambientali.

Oggi più che mai le sfide saranno quelle di analizzare, comprendere, indirizzare le imprese verso la **sostenibilità che diventa prassi**.

In questo processo il consulente, il professionista, deve aiutare le imprese a trasformare le sfide in opportunità, secondo diverse possibili aree di intervento:

- Valutazione delle questioni non finanziarie
- Revisione della *compliance* e della materialità
- Revisione del Modello 231
- Valutazione del modello di *governance*
- Valutazione del *reporting* ESG
- Valutazione della percezione interna ESG

- Priorità e raccolta dei dati
- *Reporting* non finanziario per definire i KPI (indicatore chiave prestazione) più appropriati
- Redazione ed approvazione della dichiarazione non finanziaria DNF
- Relazioni con gli investitori
- Piano strategico per sviluppare il profilo ESG, indirizzare i gestori patrimoniali sensibili all'ESG e rafforzare il rapporto con gli azionisti

10. Bibliografia

P. VERNERO – M.F. E B. PARENA, *Environmental Social Governance (ESG): impatto sui Modelli 231,* in *Rivista della responsabilità amministrativa degli enti, f. 2, 2023*

M. PETA, *Il peso dell'informativa non finanziaria (DNF) nella definizione del Modello di organizzazione e gestione e gli adeguati assetti organizzativi,* in *Rivista della responsabilità amministrativa degli enti, f. 2, 2023*

Pubblichiamo le *slides* presentate il 14 dicembre in occasione del Webinar "*Value creation: gli indicatori ESG e il sistema di compliance di cui al D.Lgs. 231/2001. L'integrazione dei presidi di controllo in ottica di sostenibilità e di prevenzione del rischio reato*"

G. PUTZU – A. R. CARNÀ, *Gli indicatori ESG e il d.lgs. 231/2001. L'integrazione dei presidi di controllo a servizio della sostenibilità e della prevenzione del rischio-reato,* in *Rivista della responsabilità amministrativa degli enti, f. 2, 2023*

S. SARNO – R. DI PIETRO, *La relazione tra il Modello di organizzazione e gestione e gli indici ESG,* in *Rivista della responsabilità amministrativa degli enti, f. 2, 2023*

M. CHIODI, *Il D.Lgs. 231/2001 e criteri ESG. Il sistema di compliance 231 quale pilastro dello sviluppo sostenibile,* in *Rivista della responsabilità amministrativa degli enti, f. 2, 2023*

G. VILLA, *Il Modello di Organizzazione, Gestione e Controllo: le sfide della responsabilità di impresa e della sostenibilità,* in *Rivista della responsabilità amministrativa degli enti, f. 2, 2023*

M. MORETTI – P. SILVESTRI, *ESG - tra sistema integrato e autonomia dei suoi componenti,* in *Rivista della responsabilità amministrativa degli enti, f. 2, 2023*

E. BERTOLLI – C. GUIZZETTI, *ESG, sviluppo sostenibile e Modello 231 tra opportunità e integrazione,* in *Rivista della responsabilità amministrativa degli enti, f. 2, 2023*

C. SANTORIELLO, *L'adozione di un idoneo Modello organizzativo 231 quale indispensabile (ed unico) presupposto per la responsabilità sociale dell'impresa, in Rivista della responsabilità amministrativa degli enti, f. 1, 2023*

CAPITOLO 5 di Eva Cruellas Sada, Eugenia Gambarara e Irene Picciano

Il nuovo Regolamento UE di esenzione per categoria sugli accordi verticali

Il nuovo Regolamento UE di esenzione per categoria sugli accordi verticali: (VBER) nuove criticità/opportunità per le imprese

SOMMARIO: A. Introduzione – B. Le principali novità – 1. Mantenimento dell'esenzione con quote di mercato inferiori al 30% – 2. Ampliamento dell'esenzione per alcune restrizioni territoriali e/o di clientela – 3. Accordi di distribuzione tra concorrenti – 4. Gli accordi di agenzia commerciale – 5. La fissazione dei prezzi di rivendita - 6. Gli obblighi di non concorrenza – 7. Obblighi di parità (cd. "clausole della nazione più favorita") – 8. Le vendite online – 9. Piattaforme online – 10. Sostenibilità – 11. Take away

A. Introduzione

Ad esito di un lungo processo di consultazione da parte della Commissione europea con l'obiettivo di adattare la disciplina degli accordi verticali agli sviluppi intervenuti nell'ultimo decennio, con particolare riferimento alla crescita esponenziale del commercio online, il 1 giugno 2022 è entrato in vigore il Regolamento UE n. 720/2022 della Commissione relativo all'applicazione dell'articolo 101 (3) del Trattato sul Funzionamento dell'Unione Europea (TFUE) agli accordi verticali (*Vertical Block Exemption Regulation* - "**VBER**" o "**Regolamento**[50]") . L'adozione del Regolamento è stata accompagnata dalla pubblicazione da parte della Commissione di nuove Linee Guida (Comunicazione 2022/C 248/01, "**Linee guida**" o "**Orientamenti**[51]").

Il nuovo VBER sostituisce il precedente VBER del 2010 (Regolamento UE n. 330/2010)[52] ed è destinato a rimanere in vigore fino al 31 maggio 2034.

Il VBER si è applicato da subito ai contratti stipulati successivamente alla sua entrata in vigore, mentre era previsto un regime transitorio di un anno,

50 Regolamento (UE) n. 2022/720 della Commissione del 10 maggio 2022 relativo all'applicazione dell'articolo 101, paragrafo 3, del trattato sul funzionamento dell'Unione europea a categorie di accordi verticali e pratiche concordate - C/2022/3015.

51 COMUNICAZIONE DELLA COMMISSIONE, Orientamenti sulle restrizioni verticali - 2022/C 248/01.

52 Regolamento (UE) n. 330/2010 della Commissione del 20 aprile 2010 relativo all'applicazione dell'articolo 101, paragrafo 3, del trattato sul funzionamento dell'Unione europea a categorie di accordi verticali e pratiche concordate - L 102, 23 aprile 2010.

fino al 31 maggio 2023, per permettere alle imprese di adeguare alle nuove disposizioni i contratti già in vigore che rispettavano le condizioni di esenzione stabilite dal precedente regolamento VBER del 2010.

Nel contesto della normativa antitrust si definiscono accordi verticali le intese che intervengono tra imprese attive a livelli diversi della catena produttiva e distributiva, come i contratti di distribuzione esclusiva, i contratti di distribuzione selettiva o il *franchising*.

B. Le principali novità

1. Mantenimento dell'esenzione con quote di mercato inferiori al 30%

Il primo aspetto di rilievo della nuova disciplina è il mantenimento, per tutti gli accordi verticali, della medesima zona di sicurezza (cosiddetto *safe-harbour*) prevista dalla precedente disciplina, la quale è delimitata dalla soglia di quota di mercato del 30%[53].

In particolare, laddove le quote di mercato del fornitore e del distributore non superino il 30% nel mercato rilevante in cui essi rispettivamente vendono e acquistano i beni o servizi oggetto del contratto, gli accordi verticali possono beneficiare dell'esenzione automatica garantita dal Regolamento, cioè di una presunzione di liceità, a condizione altresì che essi non contengano restrizioni fondamentali vietate dal Regolamento (cosiddette *hard-core restrictions*), ossia restrizioni ritenute gravemente lesive della concorrenza, tra cui quelle relative alla fissazione del prezzo di rivendita e all'instaurazione di una protezione territoriale assoluta.

2. Ampliamento dell'esenzione per alcune restrizioni territoriali e/o di clientela

Il precedente regolamento VBER del 2010 già prevedeva alcune eccezioni al generale divieto di imposizione di restrizioni territoriali e/o di clientela ai distributori, al fine di tutelare ed incentivare gli investimenti cui questi ultimi incorrono. Tuttavia, tale regime era diventato inadeguato rispetto all'evoluzione dei mercati e, durante la consultazione, è emersa la necessità di garantire più flessibilità ai fornitori nell'organizzazione delle proprie reti distributive e di garantire un migliore coordinamento tra i diversi sistemi di distribuzione utilizzanti dal fornitore in diversi territori.

a) Distribuzione esclusiva

In un sistema di distribuzione esclusiva, la VBER ammette che il fornitore imponga agli altri distributori un **divieto di vendite attive** all'interno del territorio o con riferimento al gruppo di clienti assegnati al distributore esclusivo.

53 Cfr. art. 3 VBER.

Oltre alle possibilità di imporre una restrizione relativa al luogo di stabilimento dell'acquirente e una restrizione delle vendite attive o passive agli utenti finali da parte di un acquirente operante al livello del commercio all'ingrosso, rispetto al regime precedente, il Regolamento introduce le seguenti importanti novità:

i. è stata introdotta la possibilità della c.d. "**esclusività condivisa**", superando l'impostazione del precedente sistema secondo cui la restrizione delle vendite attive era possibile solo con riferimento a territori o gruppi di clienti assegnati in via esclusiva a **un unico distributore**. Ora sarà possibile **assegnare un territorio e/o un gruppo di clienti in via esclusiva fino ad un massimo di 5 distributori**[54];

ii. è stata ampliata la definizione di **vendite attive** al fine di adeguarla al contesto attuale di significativo aumento dell'*e-commerce*, precisando che costituisce vendita attiva *inter alia* (i) la gestione di un sito internet con un dominio di primo livello che corrisponde a determinati territori; (ii) l'offerta su un sito internet di opzioni linguistiche comunemente utilizzate in determinati territori, quando tali lingue siano diverse da quelle comunemente utilizzate nel territorio in cui è stabilito l'acquirente e (iii) l'utilizzo di strumenti di confronto dei prezzi o pubblicità associata a motori di ricerca, che siano destinati a clienti in determinati territori o a gruppi di clienti[55];

iii. è stata introdotta la possibilità per il fornitore di trasferire (c.d. ***pass-on***) la **restrizione di vendite attive**, quindi, di chiedere ai propri distributori di imporre a loro volta, ai loro diretti clienti, un divieto di vendite attive nei territori e/o gruppi di clienti assegnati in esclusiva ad altri distributori[56];

iv. è stata riconosciuta la **possibilità di utilizzare sistemi di distribuzione diversi tra i vari Stati membri** e, in questo caso, di proteggere i distributori esclusivi in uno Stato membro dalle **vendite attive** da parte di distributori selettivi o liberi – e dei loro clienti – nei paesi in cui esiste, rispettivamente, la distribuzione selettiva o la distribuzione libera[57].

b) Distribuzione selettiva

Il Regolamento garantisce una maggiore protezione anche per i sistemi di **distribuzione selettiva** (i.e., quella forma di distribuzione in cui i prodotti o servizi sono commercializzati tramite distributori selezionati sulla base di criteri specificati e nella quale questi distributori si impegnano a non vendere tali beni o servizi a rivenditori non autorizzati nel territorio che il fornitore ha riservato a tale sistema)[58]. In particolare, oltre alle possibilità di imporre una restrizione relativa al luogo di stabilimento dell'acquirente e una restrizione delle vendite

54 Cfr. art. 4(b)(i) VBER e § 219 delle Linee Guida.
55 Cfr. art. 1(1)(l) VBER.
56 Cfr. art. 4(b)(i) VBER.
57 Cfr. artt. 4(c)(i)(1) VBER e 4(d)(i) VBER.
58 Cfr. art. 1(1)(g) VBER.

attive o passive agli utenti finali da parte di un acquirente operante al livello del commercio all'ingrosso, rispetto al regime precedente, il Regolamento introduce le seguenti importanti novità:

i. è stata introdotta, per evitare elusioni del divieto di rivendita fuori rete tipico della distribuzione selettiva, la possibilità per il fornitore di trasferire (c.d. ***pass-on***) la **restrizione di vendite attive e passive a distributori non autorizzati**, quindi, di chiedere ai propri distributori selettivi di imporre a loro volta, ai loro diretti clienti, un divieto di vendite attive e passive a distributori non autorizzati situati all'interno del territorio in cui il fornitore opera il sistema di distribuzione selettiva[59];

ii. è stata riconosciuta, come detto, la **possibilità di utilizzare sistemi di distribuzione diversi tra i vari Stati membri** e, in questo caso, la possibilità di proteggere i distributori selettivi in uno Stato membro dalle **vendite attive e passive** da parte di distributori esclusivi o liberi - e dei loro clienti - a distributori non autorizzati situati nei paesi in cui il fornitore gestisce un sistema di distribuzione selettiva[60];

iii. è stato precisato nelle Linee Guida che la combinazione della distribuzione selettiva con la distribuzione esclusiva nello stesso territorio non può beneficiare dell'esenzione di cui al Regolamento, anche quando il fornitore applica la distribuzione esclusiva all'ingrosso e la distribuzione selettiva al dettaglio[61].

c) Distribuzione libera

Il Regolamento introduce, per la prima volta, una disciplina applicabile ai sistemi di distribuzione che non sono né esclusivi né selettivi (c.d. distribuzione libera), che specifica quali restrizioni possono essere imposte ai distributori liberi senza perdere il beneficio dell'esenzione. In particolare, oltre alle restrizioni di cui ai punti a) iv. e b) ii. *supra* a tutela dei distributori esclusivi e selettivi in altri paesi, è riconosciuta *inter alia* la possibilità di (i) imporre una restrizione relativa al luogo di stabilimento dell'acquirente, (ii) imporre una restrizione delle vendite attive o passive agli utenti finali da parte di un acquirente operante al livello del commercio all'ingrosso[62] e (iii) in certe circostanze, come già riconosciuto per gli accordi di distribuzione selettiva[63], vietare l'utilizzo dei *marketplaces* online, a condizione che tale restrizione non abbia, direttamente o indirettamente, come oggetto di impedire l'uso efficace di internet da parte dell'acquirente o dei suoi clienti per vendere i beni o servizi oggetto del contratto[64].

59 Cfr. artt. 4(c)(i)(2) VBER.
60 Cfr. artt. 4(b)(ii), 4(c)(i) e 4(d)(ii) VBER.
61 Cfr. § 236 delle Linee Guida.
62 Cfr. artt. 4(d)(iii) e (iv) VBER.
63 Cfr. C-230/16 - Coty Germany, § 64-69.
64 Cfr. § 335 delle Linee Guida.

3. Accordi di distribuzione tra concorrenti

Tra le novità più rilevanti introdotte dalla riforma vi è quella relativa alla disciplina della c.d. duplice distribuzione ("**dual distribution**"), ovvero i modelli di distribuzione nei quali il distributore vende i propri beni tanto direttamente ai consumatori finali quanto tramite distributori indipendenti, e che si caratterizza pertanto da uno scenario nel quale il fornitore opera in regime di concorrenza diretta con i propri distributori.

Recependo i commenti provenienti dagli *stakeholders*, il Regolamento non include, come aveva inizialmente proposto la Commissione Europea, una nuova soglia del 10% per l'esenzione degli accordi verticali in caso di *dual distribution*, mantenendo, quindi, anche per questi accordi la zona di sicurezza del 30% di quota di mercato.

Inoltre, il Regolamento ha ampliato l'ambito dell'esenzione, includendo espressamente i vari livelli della catena distributiva. Quindi, l'esenzione si applica agli accordi verticali tra un fornitore che opera, a monte, come produttore, importatore o grossista e, a valle, come importatore, grossista o distributore di beni, e un acquirente che opera a valle come importatore, grossista o distributore e non è un'impresa concorrente a monte[65].

La novità più importante del Regolamento in relazione a questi accordi è l'introduzione di una nuova previsione che esclude dall'esenzione gli scambi di informazioni tra fornitore e distributore che non sono direttamente connessi all'esecuzione dell'accordo verticale o necessari per migliorare la produzione o la distribuzione dei beni o servizi oggetto del contratto[66]. Al riguardo, nelle Linee Guida è stato incluso un elenco (esemplificativo e non esaustivo), che viene sintetizzato nella seguente tabella, delle informazioni il cui scambio è generalmente ritenuto direttamente connesso all'esecuzione del contratto o necessario per migliorare la produzione o distribuzione dei beni o servizi oggetto del contratto, e che pertanto potrebbero, verosimilmente e in base alle circostanze del caso concreto, beneficiare dell'esenzione di cui alla VBER[67], nonché delle informazioni che sono generalmente ritenute non direttamente connesse all'esecuzione del contratto o necessarie per migliorare la produzione o distribuzione dei beni o servizi oggetto del contratto[68]. Questa nuova previsione richiede ovviamente una valutazione molto accurata dei flussi informativi in essere tra fornitore e distributore al fine di evitare rischi antitrust.

Infine, la versione finale del Regolamento ha mantenuto un approccio restrittivo nei confronti delle piattaforme, escludendo dall'esenzione le piattaforme ibride. In particolare, si precisa che l'esenzione per categoria non si applica agli accordi verticali relativi alla fornitura di servizi di intermediazione online in cui il fornitore di tali servizi è un'impresa concorrente sul mercato

65 Cfr. art. 2(4) VBER.
66 Cfr. art. 2(5) VBER.
67 Cfr. § 99 Linee Guida.
68 Cfr. § 100 Linee Guida.

rilevante per la vendita dei beni o servizi oggetto dell'intermediazione[69]. È prevedibile che questa nuova previsione escluda dalla VBER numerosi accordi, i quali resteranno soggetti a una valutazione individuale *ad hoc* con i conseguenti aggravi per le imprese.

INFORMAZIONI AUTORIZZATE	INFORMAZIONI NON AUTORIZZATE
➢ Informazioni tecniche ➢ Informazioni logistiche ➢ Feedback dei clienti (a certe condizioni) ➢ Prezzi di sell-in ➢ Prezzi al dettaglio suggeriti ➢ Informazioni di marketing e promozionali (non prezzi futuri) ➢ Informazioni di mercato	➢ Informazioni sui prezzi futuri ➢ Informazioni su clienti specifici dei distributori ➢ Informazioni relative a beni venduti da un acquirente con il proprio marchio con un produttore di prodotti di marca concorrenti, a meno che il produttore non sia anche il produttore dei prodotti a marchio proprio

4. Gli accordi di agenzia commerciale

La nuova disciplina mantiene l'impostazione precedente, secondo cui la condizione perché un rapporto di agenzia possa essere considerato escluso dall'ambito di applicazione dell'art. 101 TFUE (e quindi dal VBER) consiste nella mancanza di indipendenza economica dell'agente, cioè nell'assenza o non significatività di rischio finanziario o commerciale in relazione ai contratti che l'agente conclude o negozia per conto del preponente (il c.d. "*agency test*").

Le Linee Guida introducono, tuttavia, un'interpretazione più restrittiva dell'*agency test*, facendo riferimento al criterio della significatività del rischio assunto dall'agente, che va valutato rispetto alle entrate generate dalla prestazione di servizi di agenzia da parte dell'agente (tipicamente, le commissioni che questo percepisce dal preponente), anziché con riferimento alle entrate realizzate dalla vendita di beni o servizi oggetto del contratto di agenzia[70]. Tale valutazione può risultare particolarmente complessa nel caso in cui si svolga attività di agenzia e di distribuzione indipendente per lo stesso fornitore (c.d. "*dual role*"), in quanto questo crea difficoltà nel distinguere tra investimenti e costi relativi alla funzione di agenzia, compresi gli investimenti specifici del mercato, e quelli che riguardano esclusivamente l'attività indipendente[71].

Le Linee Guida specificano poi (i) che laddove l'agente faccia capo ad un numero considerevole di preponenti è meno probabile che il rapporto possa essere qualificato come di agenzia[72] e (ii) che gli accordi conclusi da imprese attive nell'economia delle piattaforme online generalmente non soddisfano le condizioni per essere classificati come contratti di agenzia che esulano dall'ambito di applicazione dell'articolo 101 TFEU. Viene inoltre ribadito come l'eventuale qualificazione che le parti diano del contratto come di agenzia (ciò che è frequente con riferimento alle imprese operanti su piattaforme online[73]) sia irrilevante ai fini antitrust, poiché ciò che rileva è che il rapporto soddisfi l'*agency test*.

69 Cfr. art. 2(6) VBER.
70 Cfr. § 32 delle Linee Guida.
71 Cfr. § 37 delle Linee Guida.
72 Cfr. § 30 delle Linee Guida.
73 Cfr. § 63 delle Linee Guida.

5. La fissazione dei prezzi di rivendita

Tra le restrizioni fondamentali di cui all'art. 4 nuovo VBER, continua ad essere ricompresa l'imposizione dei prezzi di vendita (*Resale price maintenance* o RPM), ossia «*gli accordi o pratiche concordate volti a stabilire, direttamente o indirettamente, un prezzo di rivendita fisso o minimo o un livello di prezzo fisso o minimo che deve essere rispettato dall'acquirente*».

Benché la restrizione di cui all'art. 4 lett. a) nuovo VBER sia rimasta invariata nella formulazione, i recenti Orientamenti introducono nuovi spunti interpretativi al fine di comprenderne il perimetro.

In primo luogo, la Commissione individua alcune previsioni contrattuali che equivalgono, di fatto, ad un'imposizione dei prezzi. Tra queste pare opportuno ricordare:

- la fissazione del margine del distributore;
- la fissazione del livello massimo degli sconti che il distributore può praticare a partire da un livello di prezzo descritto;
- la subordinazione di sconti o del rimborso dei costi promozionali da parte del fornitore al rispetto di un dato livello di prezzo;
- il collegamento del prezzo di rivendita imposto ai prezzi di rivendita dei concorrenti.

È altresì considerata un'imposizione indiretta dei prezzi di rivendita l'imposizione di vincoli di prezzo minimo pubblicizzato (*minimum advertised prices* o MAP). Sebbene i MAP lascino al distributore la libertà di vendere ad un prezzo inferiore rispetto a quello pubblicizzato, vincoli di questo tipo sono considerati strumenti indiretti di imposizione di prezzi di rivendita in quanto disincentivano il distributore dal fissare un prezzo di vendita più basso, limitando la sua capacità di informare i clienti sugli sconti disponibili[74]. Proprio quest'ultima valutazione ha chiuso la strada a una possibile apertura che era stata considerata dalla commissione in sede di consultazione.

Non è, invece, considerata un'imposizione dei prezzi (né un indice decisivo in tal senso) l'impiego di strumenti (anche automatizzati) di controllo sui prezzi applicati dai rivenditori. Secondo la Commissione, infatti, il controllo dei prezzi aumenta la trasparenza sul mercato e permette ai produttori di monitorare efficacemente i prezzi di rivendita della propria rete di distribuzione, così da poter intervenire prontamente in caso di riduzione dei prezzi[75].

Inoltre, pare opportuno precisare che secondo i nuovi Orientamenti, la fissazione del prezzo prevista in un accordo verticale tra fornitore e un distributore non è vietata ove tale accordo sia stato concluso per dare esecuzione a un precedente accordo tra il fornitore e un utente finale specifico, a condizione

74 Cfr. § 174 Linee Guida.
75 Cfr. § 177 Linee Guida.

che quest'ultimo abbia rinunciato al proprio diritto di scegliere l'impresa che dovrebbe dare esecuzione all'accordo.[76]

Innovando rispetto al passato le nuove Linee Guida esemplificano una serie di casi in cui le pratiche di RPM possono tuttavia determinare incrementi di efficienza tali da giustificare l'esenzione individuale *ex* art. 101(3) TFUE. Tuttavia, tali casi non potranno comunque beneficiare dell'esenzione automatica garantita dalla VBER. Le imprese dovranno svolgere un'analisi *ad hoc* di tali pratiche per valutare se esse soddisfino i requisiti per poter beneficiare di un'esenzione individuale ai sensi dell'art. 101(3) TFUE. Si tratta nello specifico di:

- lancio di un nuovo prodotto[77];
- campagne di breve termine di prezzi bassi - generalmente, dalle 2 alle 6 settimane[78];
- la fornitura da parte del dettagliante di servizi aggiuntivi prevendita, in particolare in caso di prodotti la cui qualità è di difficile valutazione prima del consumo (c.d. prodotti "d'esperienza") o nel caso di prodotti complessi[79];
- la possibilità per il fornitore di imporre al distributore un prezzo minimo di rivendita nel caso in cui tale distributore rivenda sistematicamente i prodotti del fornitore al di sotto dei prezzi all'ingrosso al fine di attirare nuova clientela (c.d. "prodotto civetta")[80].

6. Gli obblighi di non concorrenza

In continuità con il regime precedente, anche il VBER prevede che gli obblighi di non concorrenza di durata superiore a cinque anni o di durata indeterminata debbano essere esclusi dal beneficio di esenzione (art. 5 (1), lett. a, VBER).

Per «obbligo di non concorrenza» si intende qualsiasi obbligo, diretto o indiretto, che impone all'acquirente di non produrre, acquistare, vendere o rivendere beni o servizi in concorrenza con i beni o servizi oggetto del contratto, ovvero qualsiasi obbligo, diretto o indiretto, che impone all'acquirente di acquistare dal fornitore o da un'altra impresa da questi indicata più dell'80 % degli acquisti annui complessivi dei beni o servizi oggetto del contratto, e dei relativi succedanei, effettuati dall'acquirente stesso sul mercato rilevante, calcolati sulla base del valore o, se tale è la normale prassi del settore, del volume dei suoi acquisti effettuati nell'anno civile precedente[81].

76 Cfr. § 178 Linee Guida.
77 Cfr. § 197 (a) Linee Guida.
78 Cfr. § 197 (b) Linee Guida.
79 Cfr. § 197 (d) Linee Guida.
80 Cfr. § 197 (c) Linee Guida.
81 Cfr. § 1(1)(f) VBER.

Tali clausole potevano beneficiare dell'esenzione per categoria a condizione che fosse rispettata la soglia del 30% di quote di mercato e che la loro durata non fosse superiore a cinque anni. Erano pertanto escluse dal beneficio dell'esenzione le clausole di non concorrenza:

- di durata indefinita,
- di durata determinata superiore ai cinque anni, e
- tacitamente rinnovabili oltre cinque anni.

La nuova disciplina VBER mantiene l'impostazione precedente, lasciando immutato il periodo quinquennale ma **amplia il novero degli obblighi di non concorrenza che possono beneficiare del "*safe harbour*"**. In particolare, oltre agli obblighi di non concorrenza di durata determinata non superiore ai 5 anni, anche le clausole di non concorrenza tacitamente rinnovabili sono ora esentate, a condizione che il distributore possa effettivamente cambiare fornitore dopo 5 anni rinegoziando o risolvendo l'accordo verticale con un ragionevole periodo di preavviso e a un costo ragionevole, così che possa passare a un altro fornitore dopo la scadenza del periodo di cinque anni[82].

La nuova disposizione consente di adottare un approccio sicuramente più flessibile rispetto agli accordi verticali contenenti obblighi di non concorrenza tacitamente rinnovabili al termine del quinquennio. Permane tuttavia un'area grigia relativa alla mancata estensione anche per gli accordi di durata indefinita e a quelli di durata determinata superiore ai cinque anni che possano essere risolti con un ragionevole preavviso e a costi ragionevoli, non essendo chiaro in cosa questi ultimi possano differire dai primi rispetto agli obiettivi perseguiti dalla norma.

7. Obblighi di parità (cd. "clausole della nazione più favorita")

Gli obblighi di parità, anche denominati "clausole della nazione più favorita" (cd. "clausole NPF"), impongono a un venditore di beni o servizi di offrire questi ultimi a un'altra parte a condizioni che non siano meno favorevoli rispetto a quelle offerte ad altre parti o tramite determinati altri canali[83]. Le condizioni possono riguardare prezzi, scorte, disponibilità o altri termini o condizioni di offerta o vendita. L'obbligo di parità può assumere la forma di una clausola contrattuale o può derivare da altre misure dirette o indirette, quali prezzi differenziati o altri incentivi la cui applicazione dipende dalle condizioni alle quali il venditore offre i propri beni o servizi ad altre parti o tramite altri canali.

Gli obblighi di parità nella vendita al dettaglio si riferiscono alle condizioni alle quali i beni o servizi sono offerti agli utenti finali. Tali obblighi sono spesso imposti da fornitori di servizi di intermediazione online (ad esempio, mercati online o servizi di confronto dei prezzi) agli acquirenti dei loro servizi

82 Cfr. § 248 Linee Guida.

83 Si veda al tal proposito, § 6.2.4, 8.2.5 e 8.2.5.1-8.2.5.5 delle Linee Guida.

di intermediazione (ad esempio, imprese che vendono tramite la piattaforma di intermediazione).

Negli ultimi anni, le autorità garanti della concorrenza europee hanno condotto un numero crescente di azioni di *enforcement* contro tali clausole, a fronte del sospetto che il loro utilizzo da parte di piattaforme con grandi basi di utenti abbia limitato in modo esponenziale la concorrenza tra le piattaforme, nonché tra le piattaforme e il canale di vendita diretto degli utenti commerciali.

L'articolo 5, lettera d) del Regolamento 2022/720 si occupa espressamente delle clausole NPF, escludendo dal beneficio dell'esenzione per categoria le NPF concernenti la vendita al dettaglio volte a limitare gli utenti commerciali di una piattaforma dalla vendita di beni o servizi a condizioni più favorevoli attraverso piattaforme di intermediazione concorrenti (cd. NPF "ampie" o "tra piattaforme"). Di conseguenza, questo tipo di restrizione deve sempre essere valutato individualmente ai sensi dell'articolo 101, paragrafo 3 del TFUE, indipendentemente dalle quote di mercato delle imprese coinvolte.

Al contrario, le NPF relative solo ai canali diretti gestiti dagli utenti commerciali (dette "NPF ristrette") continuano a beneficiare dell'esenzione per categoria. Le NPF ristrette, così come gli "obblighi del cliente più favorito" (ossia, gli obblighi di parità possono essere imposti anche da produttori, grossisti o dettaglianti relativamente alle condizioni di acquisto di beni o servizi come fattori produttivi dai fornitori), continuano a beneficiare dell'esenzione per categoria come nel vecchio regolamento (soggetto alla soglia del 30% di quota di mercato). Tuttavia, le Nuove Linee Guida cercano di sensibilizzare le imprese dall'uso delle clausole "NPF ristrette" nei mercati concentrati delle piattaforme. Infatti, se le NPF ristrette vengono applicate cumulativamente da piattaforme che coprono un'ampia quota di potere di mercato e non vi sono prove di effetti favorevoli alla concorrenza, la Commissione o le autorità nazionali garanti della concorrenza potrebbero revocare il beneficio dell'esenzione per categoria.

8. Le vendite online

La nuova VBER introduce importanti novità in tema di vendite online.

Significativamente, le Linee Guida rimuovono l'obbligo di equivalenza previste nel precedente regime[84], con la conseguenza che non è più richiesto che i criteri imposti dai fornitori in relazione alle vendite online siano complessivamente equivalenti ai criteri imposti ai punti vendita fisici, a condizione, tuttavia, che tali diversi criteri non si pongano l'obiettivo di ostacolare le vendite *online*. In particolare, con riferimento ai sistemi di distribuzione selettiva, un fornitore che gestisce un sistema di distribuzione selettiva può selezionare i suoi distributori autorizzati sulla base di criteri qualitativi e/o quantitativi. I criteri qualitativi in genere devono essere stabiliti sia per i canali *online* che per quelli offline. Considerando tuttavia che i canali *online* e *offline* presentano caratteristi-

84 Le Linee Guida 2010 ricomprendevano tra le restrizioni fondamentali anche l'imposizione, da parte del fornitore, di criteri per le vendite *online* che non fossero nel complesso equivalenti a quelli imposti presso un punto vendita "non virtuale" (c.d. "*criterio di equivalenza*").

che diverse, un fornitore che gestisce un sistema di distribuzione selettiva può imporre ai propri distributori autorizzati dei criteri per le vendite *online* diversi da quelli imposti per le vendite nei negozi non virtuali, purché i requisiti imposti per le vendite online non abbiano indirettamente per oggetto di impedire all'acquirente di utilizzare efficacemente internet al fine di vendere i beni o servizi oggetto del contratto in territori o a clienti particolari[85].

Inoltre, recependo le criticità emerse durante il processo di consultazione indetta dalla Commissione Europea e avente ad oggetto la bozza del Regolamento 2022/720[86], l'articolo 1, paragrafo 1, lettera l)[87], in combinato disposto con l'articolo 1, paragrafo 1, lettera m)[88], fornisce una definizione più dettagliata di vendite attive e passive in ambito digitale Inoltre, le Nuove Linee Guida forniscono nuovi esempi e chiarimenti su cosa si intende per "vendita attiva *online*", tra cui vengono annoverate: la pubblicità su motori di ricerca rivolti a territori specifici; l'offerta in un negozio *online* di un'opzione linguistica diversa da quelle comunemente utilizzate nel territorio in cui è stabilito il venditore; o la creazione di un negozio *online* con un dominio di primo livello corrispondente a un territorio diverso da quello in cui è stabilito il venditore.

Al contempo, il Regolamento 2022/720 prevede espressamente che qualsiasi restrizione finalizzata, direttamente o indirettamente, a limitare la capacità del distributore o dei suoi clienti di utilizzare *Internet in modo efficace*, tale restrizione sarà in ogni caso considerata una restrizione fondamentale, il che significa che l'intero accordo non potrà beneficiare dell'esenzione per categoria e sarà improbabile che soddisfi le condizioni per l'esenzione individuale ai sensi dell'articolo 101, paragrafo 3 TFEU.

Al riguardo, le Nuove Linee Guida forniscono indicazioni su come valutare le restrizioni *online* sulla base di quanto stabilito dalla Corte di Giustizia in sentenze successive all'entrata in vigore del vecchio regolamento categorie di

85 Un fornitore, ad esempio, può imporre requisiti per garantire determinati *standard* qualitativi per le vendite *online*, come l'istituzione e la gestione di uno sportello di assistenza *post*-vendita *online*, l'obbligo di sostenere i costi della restituzione dei prodotti acquistati da parte dei clienti o l'uso di sistemi di pagamento sicuri. Analogamente, un fornitore può definire criteri diversi relativi allo sviluppo sostenibile per i canali di vendita *online* e *offline* che richiedano, ad esempio, punti vendita eco-compatibili.

86 La consultazione ha, infatti, evidenziato una mancanza di chiarezza su ciò che può essere considerato vendita attiva o passiva e hanno rivelato che il tipo di distribuzioni esclusive per le quali le restrizioni alle vendite attive sono state esentate non è in linea con i nuovi sistemi di distribuzione e le esigenze commerciali.

87 Tale norma prevede che: "per 'vendite attive' si intende il fatto di contattare in maniera attiva e mirata dei clienti mediante visite, lettere, *e-mail*, telefonate o altri mezzi di comunicazione diretta o attraverso azioni di pubblicità e promozione mirate, *offline* o *online*, ad esempio attraverso: media cartacei o digitali, compresi i media *online*; strumenti di confronto dei prezzi o pubblicità associata a motori di ricerca, che siano destinati a clienti in determinati territori o a gruppi di clienti; la gestione di un sito *internet* con un dominio di primo livello che corrisponde a determinati territori; l'offerta su un sito *internet* di opzioni linguistiche comunemente utilizzate in determinati territori, quando tali lingue siano diverse da quelle comunemente utilizzate nel territorio in cui è stabilito l'acquirente".

88 Tale norma prevede che: "per vendite 'passive' si intendono vendite effettuate in risposta a richieste spontanee di singoli clienti, comprese la consegna di beni o la prestazione di servizi al cliente, senza che la vendita sia stata avviata sollecitando attivamente particolari clienti, gruppi di clienti o territori, incluse le vendite risultanti dalla partecipazione ad appalti pubblici o dalla risposta a bandi di gara privati".

accordi verticali e pratiche concordate, in particolare nei casi "Pierre Fabre"[89] e "Coty"[90]. Da un lato, le Nuove Linee Guida indicano ora in modo più esplicito che alcune restrizioni alle vendite sui mercati online negli accordi verticali (cd. "divieti di mercato") possono beneficiare dell'esenzione per categoria ai sensi del Regolamento 2022/720, a prescindere dal tipo di sistema di distribuzione, purché non abbiano indirettamente per oggetto di impedire all'acquirente di utilizzare efficacemente *Internet* al fine di vendere i beni o servizi oggetto del contratto in territori o a clienti particolari. Tra gli esempi di restrizioni alle vendite *online* che possono beneficiare dell'esenzione di cui all'articolo 2, paragrafo 1 del Regolamento 2022/720 si annoverano le imposizioni di requisiti intesi a garantire la qualità o un particolare aspetto del negozio *online* dell'acquirente; fissazione di criteri concernenti le modalità di esposizione nel negozio online dei beni o servizi oggetto del contratto; e l'obbligo per l'acquirente di gestire uno o più negozi o *showroom* non virtuali.

Dall'altro, le Nuove Linee Guida[91] forniscono un ampio elenco di obblighi che, direttamente o indirettamente, sono concepiti per impedire ai distributori di utilizzare efficacemente Internet per vendere i propri beni o servizi (rappresentando quindi restrizioni fondamentali) ai sensi dell'articolo 4, lettera e), del Regolamento 2022/720. Fra questi, vengono menzionati l'obbligo per l'acquirente di impedire ai clienti situati in un altro territorio di visualizzare il suo sito *web* o negozio *online* o di reindirizzare i clienti al negozio *online* del produttore o di un altro venditore e l'obbligo per l'acquirente di interrompere le transazioni *online* dei consumatori qualora la loro carta di credito riveli un indirizzo che non rientra nel territorio dell'acquirente.

Infine, per quanto riguarda i *price comparison tools*, le Linee Guida stabiliscono che un divieto assoluto di utilizzare servizi di comparazione dei prezzi impedirebbe l'uso di un intero canale pubblicitario e configurerebbe, quindi, una restrizione *hardcore*. Viene tuttavia chiarito che le restrizioni che non impediscono l'utilizzo di tutti i servizi di comparazione dei prezzi, ad esempio l'obbligo che il servizio soddisfi determinati *standard* qualitativi, possono beneficiare dell'esenzione per categoria.

Il Regolamento 2022/720 e le Nuove Linee Guida rivedono anche le regole sulla cd. "doppia tariffazione" (ossia, l'applicazione di prezzi diversi ai distributori per le vendite *online* e *offline*), nonché il principio di "equivalenza", entrambi strettamente legati alle reti parallele di vendita mediante negozi *online* e i punti vendita "non virtuali" (cd. "*brick-and-mortar*"). Ai sensi del precedente regolamento di esenzione per gli accordi verticali, sia la doppia tariffazione che l'applicazione di criteri di selezione sostanzialmente diversi tra negozi *online* e negozi "*brick-and-mortar*" erano considerate restrizioni fondamentali.

Dieci anni dopo, la Commissione Europea ritiene che il mercato del commercio elettronico e le piattaforme digitali non necessitino più di una prote-

89 Causa C-439/09 Pierre Fabre Dermo-Cosmetique SAS contro Président de l'Autorité de la concurrence EU:C:2011:649.

90 Causa C-230/16 Coty Germany GmbH contro Parfümerie Akzente GmbH EU:C:2017:941.

91 In particolare, si veda § 206 delle Linee Guida.

zione così specifica per favorire le vendite *online*. Conseguentemente, l'obbligo per l'acquirente di pagare un prezzo all'ingrosso diverso per i prodotti venduti *online* rispetto ai prodotti venduti offline può beneficiare dell'esenzione di cui all'articolo 2, paragrafo 1 del Regolamento 2022/720, perché può incentivare un livello adeguato di investimenti in canali di vendita *online* od *offline*, a condizione che non abbia per oggetto la limitazione delle vendite in territori o a clienti particolari, come previsto all'articolo 4, lettere b), c) e d) del Regolamento 2022/720.

Tuttavia, anche in questo caso, qualora l'obiettivo di un tale obbligo sia quello di impedire all'acquirente di utilizzare efficacemente Internet ai fini della vendita dei beni o servizi oggetto del contratto in territori o a clienti particolari, la "doppia tariffazione" configura una restrizione fondamentale ai sensi dell'articolo 4, lettera e) del Regolamento 2022/720. Questo vale in particolare laddove la vendita *online* non risulti redditizia o sia finanziariamente insostenibile a causa della differenza di prezzo all'ingrosso, o laddove si applichi la doppia tariffazione per limitare la quantità di prodotti forniti all'acquirente per la vendita *online*.

9. Piattaforme online.

Come specificato dalle Nuove Linee Guida, le piattaforme *online* svolgono un ruolo sempre più importante nella distribuzione di beni e servizi e consentono di attuare nuove modalità di *business*, alcune delle quali non sono agevolmente classificabili utilizzando i concetti applicati agli accordi verticali nell'ambiente non virtuale.

Nelle Nuove Linee Guida, la Commissione Europea chiarisce che le imprese in questione sono spesso qualificate come "agenti" nel diritto contrattuale o commerciale. Tuttavia, tale qualifica è irrilevante per stabilire se gli accordi da esse stipulate rientrano nell'ambito di applicazione dell'articolo 101, paragrafo 1 TFEU in quanto tali imprese operano in genere come operatori economici indipendenti e non come parte delle imprese a cui forniscono servizi. In particolare, le piattaforme online spesso offrono i propri servizi a un numero molto elevato di venditori, il che impedisce loro di diventare effettivamente parte dell'impresa di uno o dell'altro venditore[92].

Chiarito il ruolo strategico delle piattaforme *online* nella distribuzione di beni e servizi, ai fini dell'applicazione del Regolamento 2022/720 a tali imprese l'articolo 1, paragrafo 1, lettera e) del Regolamento 2022/720 definisce i servizi di intermediazione *online* come servizi della società dell'informazione[93] che consentono alle imprese di offrire beni o servizi ad altre imprese o ai consumatori finali, con l'obiettivo di facilitare l'avvio di transazioni dirette tra imprese o tra un'impresa e un consumatore finale, a prescindere da dove sono concluse

92 Cfr. § 46 delle Linee Guida.

93 Si veda l'articolo 1 della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

le transazioni e dal fatto che siano effettivamente concluse o meno[94]. Tra gli esempi di servizi di intermediazione *online* vengono ricompresi i mercati di commercio elettronico, gli *app store*, i servizi di comparazione dei prezzi e i servizi di *social media* utilizzati dalle imprese.

Inoltre, a norma dell'articolo 2, paragrafo 6, del Regolamento 2022/720, le eccezioni relative alla duplice distribuzione di cui all'articolo 2, paragrafo 4, lettere a) e b), del Regolamento non si applicano agli accordi relativi alla fornitura di servizi di intermediazione online se il prestatore dei servizi di intermediazione online svolge una funzione ibrida, ossia è anche un'impresa concorrente sul mercato rilevante per la vendita di beni o servizi oggetto di intermediazione. Gli accordi verticali relativi alla fornitura di servizi di intermediazione online conclusi da fornitori di servizi di intermediazione online che svolgono tale funzione ibrida non soddisfano requisiti per le eccezioni relative alla duplice distribuzione, di cui all'articolo 2, paragrafo 4,lettere a) e b), del Regolamento. Tali fornitori possono avere interesse a favorire le proprie vendite e la capacità di influire sull'esito della concorrenza tra le imprese che si avvalgono dei loro servizi di intermediazione online. Tali accordi verticali possono pertanto suscitare riserve sotto il profilo della concorrenza in generale sui mercati rilevanti perla vendita dei beni o servizi oggetto di intermediazione.

Le Nuove Linee Guida distinguono, inoltre, i mercati *online* dai siti *web* di confronto prezzi puri[95]: generalmente, questi ultimi non offrono funzionalità di vendita e di acquisto, quanto piuttosto reindirizzano i clienti al negozio online del dettagliante, consentendo l'avvio di una transazione diretta tra il cliente e il dettagliante al di fuori del servizio di confronto dei prezzi. I servizi di confronto dei prezzi, quindi, non sono un canale di vendita online distinto, bensì un canale pubblicitario online. Inoltre, le Nuove Linee Guida forniscono indicazioni per valutare le varie restrizioni all'uso di entrambi i tipi di piattaforme che possono essere imposte ai distributori negli scenari in cui non si applica l'esenzione per categoria.

10. Sostenibilità

Una delle principali sfide che il legislatore europeo è chiamato ad affrontare è quella di stabilire norme sulla concorrenza atte al perseguimento del principio fondamentale del TFEU (nonché obiettivo primario delle politiche dell'Unione[96]) dello sviluppo sostenibile. A tal proposito, nel 2022 la Commissione ha avviato una consultazione pubblica sui regolamenti di esenzione orizzontale per categoria in materia di ricerca e sviluppo e sulle relative linee

94 Si vedano i paragrafi 65 e 66 delle Linee Guida.

95 Per "servizi di confronto dei prezzi" si intendono servizi che non prevedono una funzionalità che permette l'acquisto diretto. I servizi che permettono agli utenti di concludere transazioni di acquisto fornendo funzionalità di vendita e di acquisto sono classificati come mercati *online* ai fini delle Nuove Linee Guida. Le restrizioni relative all'uso dei mercati *online* sono trattate nelle sezioni 8.2.3 e 8.2.4 delle Linee Guida.

96 Cfr. articolo 3, paragrafo 3, del trattato sull'Unione europea. Si veda anche la Comunicazione della Commissione del 5 maggio 2021 "Aggiornamento della nuova strategia industriale 2020: costruire un mercato unico più forte per la ripresa dell'Europa".

guida[97]: l'iniziativa si pone l'obiettivo di adattare le norme vigenti in settori specifici che, in base alla valutazione, non risultano pienamente adeguate agli sviluppi economici e sociali degli ultimi dieci anni, fra i quali viene annoverata anche la cd. "transizione verde".

Invero, lo stesso Regolamento 2022/720, nonché le Nuove Linee Guida, affrontano il tema della sostenibilità, chiarendo che questa nozione comprende, tra l'altro, la risposta ai cambiamenti climatici (a mero titolo esemplificativo, attraverso la riduzione delle emissioni di gas a effetto serra), la limitazione dello sfruttamento delle risorse naturali, la riduzione degli sprechi e la promozione del benessere animale[98]. Invero, gli obiettivi di sostenibilità, resilienza e digitalizzazione dell'Unione sono promossi da accordi di fornitura e distribuzione efficienti tra le imprese; in quest'ottica, gli accordi verticali che perseguono obiettivi di sostenibilità o che contribuiscono a un mercato unico digitale e resiliente devono essere valutati applicando i principi indicati nelle Nuove Linee Guida, tenendo conto dell'obiettivo specifico da essi perseguito.

L'esenzione cui all'articolo 2, paragrafo 1, del Regolamento 2022/720 si applica agli accordi verticali che perseguono obiettivi di sostenibilità, resilienza e digitalizzazione, purché soddisfino le condizioni del suddetto Regolamento. La sezione 8 delle Nuove Linee Guida contiene indicazioni sulla valutazione di tali accordi verticali nei casi individuali, ma la Commissione Europea chiarisce che possono essere pertinenti e rilevanti ai fini di tale valutazione anche altri orientamenti della Commissione, fra i quali le linee direttrici sull'applicazione dell'articolo 101, paragrafo 3 TFEU, le linee direttrici relative agli accordi orizzontali[99] ed eventuali indicazioni fornite in versioni future delle stesse.

Invero, il tema della sostenibilità rileva anche sotto il profilo del "monomarchismo"[100]. Come chiarito al punto 300 delle Nuove Linee Guida, gli accordi di monomarchismo possono beneficiare dell'esenzione di cui all'articolo 2, paragrafo 1 del Regolamento 2022/720 se la quota di mercato del fornitore e quella dell'acquirente non superano il 30% e l'obbligo di non concorrenza non

97 Comunicato stampa della Commissione Europea circa l'avvio di una consultazione pubblica su due progetti di revisione dei regolamenti orizzontali di esenzione per categoria relativi agli accordi di ricerca e sviluppo e di specializzazione (congiuntamente denominati regolamenti di esenzione per categoria relativi agli accordi orizzontali (HBER) e al progetto di revisione degli orientamenti orizzontali), nonché circa il conseguente invito rivolto a tutte le parti interessate a formulare osservazioni su tali progetti di legge.

98 La valutazione degli accordi verticali può tenere conto di eventuali definizioni di sostenibilità, digitalizzazione o resilienza contenute nel diritto dell'Unione.

99 A tal proposito, si veda la "Comunicazione della Commissione — Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale".

100 La denominazione "monomarchismo" raggruppa gli accordi la cui principale caratteristica è che l'acquirente è costretto o indotto a concentrare gli ordini di un particolare tipo di prodotto presso un unico fornitore. Possibili rischi per la concorrenza sono la preclusione del mercato nei confronti dei fornitori concorrenti e dei fornitori potenziali, l'indebolimento della concorrenza e l'agevolazione della collusione tra i fornitori in caso di uso cumulativo e, qualora l'acquirente sia un dettagliante, una perdita della concorrenza tra marchi all'interno dei punti vendita. Gli obblighi di monomarchismo possono determinare una preclusione anticoncorrenziale in particolare quando, in mancanza di detti obblighi, sia esercitata una considerevole pressione concorrenziale da parte dei concorrenti che non erano ancora presenti nel mercato al momento della conclusione dei relativi accordi o che non sono in grado di competere per soddisfare interamente il fabbisogno dei clienti. Si veda anche il punto 248 delle Nuove Linee Guida.

supera i cinque anni. A tal proposito, la Commissione afferma che gli obblighi di non concorrenza possono anche essere utilizzati per affrontare un problema di rinuncia all'investimento nel caso di investimenti che perseguono obiettivi di sostenibilità. A titolo esemplificativo, un simile problema può sorgere quando un fornitore di energia che si trova ad affrontare un aumento della domanda di energia rinnovabile[101] desidera investire in una centrale idroelettrica o in un parco eolico. Il fornitore può essere disposto ad assumere il rischio di un simile investimento a lungo termine solo se un numero sufficiente di acquirenti intende impegnarsi ad acquistare energia rinnovabile per un periodo di tempo più lungo. Tali accordi verticali con gli acquirenti possono essere favorevoli alla concorrenza, in quanto l'obbligo di non concorrenza a lungo termine può risultare necessario affinché l'investimento sia effettuato o comunque avvenga secondo quanto previsto in termini di entità o di tempistica.

11. Take away

Il nuovo assetto normativo sulle intese verticali ha riproposto la struttura e, in larga parte, le disposizioni del precedente Regolamento, adeguandole tuttavia agli elementi innovativi del mercato, sempre più orientato alla controparte digitale e conformandole alle esigenze di semplificazione delle aziende. In quest'ottica, a fronte delle sfide poste dal mondo digitale, in continua evoluzione, il VBER mira ad essere un valido strumento a supporto delle imprese per la valutazione della legittimità dei propri accordi verticali.

La Commissione, ha accolto con favore le raccomandazioni delle parti interessate, semplificando le disposizioni vigenti al fine di renderle maggiormente accessibili agli *stakeholders*, con lo scopo di garantire un'applicazione armonizzata nel territorio europeo, integrativa degli orientamenti della Corte di Giustizia in materia, e chiarendo gli aspetti più complessi delle norme in vigore al fine di determinare un concreto beneficio in termini di costi e spese di compliance in capo alle imprese interessate.

101 Si veda l'articolo 2, paragrafo 1, della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili.

CAPITOLO 6 di Micaela Barbotti, Tiziana Boneschi, Pietro Orzalesi, Josephine Romano e Roberto Tirone

I benefici della compliance integrata e le nuove sfide della compliance 231

I benefici della compliance integrata e le nuove sfide della compliance 231 in base alla recente giurisprudenza sui controlli dell'ODV e sulla validità del modello

SOMMARIO: 1. La giurisprudenza sui controlli dell'OdV e sulla validità del MOG – 2. La compliance integrata anche alla luce dei principi giurisprudenziali emersi e dall'esperienza applicativa – 2.1 La compliance integrata: quali ambiti, quali funzioni e come? – 2.2 L'interazione/integrazione dei sistemi di compliance nei gruppi societari. Strumenti e complessità. – 3. 3. L'approccio metodologico integrato tra D. Lgs. 231/2001, Anticorruzione e Trasparenza

1. La giurisprudenza sui controlli dell'OdV e sulla validità del MOG

È noto che il D. Lgs. 231/2001 contiene un testo legislativo piuttosto sintetico, che non si sofferma a specificare i comportamenti richiesti agli enti per prevenire i reati, limitandosi a prescrivere l'adozione di un Modello Organizzativo e Gestionale (MOG) e l'istituzione di un Organismo di Vigilanza (OdV) come elementi fondamentali per la prevenzione dei reati e per la limitazione della responsabilità degli enti.

In parte, a tali lacune hanno sopperito la dottrina e le linee guida delle associazioni di categoria, come ad esempio Confindustria.

Negli ultimi anni, poi, la giurisprudenza si è assunta l'incarico di interpretare la normativa, indicando quali comportamenti in concreto debbano essere posti in essere dalle società al fine di evitare o limitare la propria responsabilità in caso di commissione di un reato da parte di propri apicali o dipendenti.

Di particolare interesse sono alcune sentenze pubblicate tra il 2020 ed il 2022 in tema di elusione fraudolenta del MOG da parte dell'agente che commette il reato, che come noto consente alla società di andare esente da responsabilità, ed in tema di composizione ed attività dell'OdV.

La sentenza di Cassazione del 15.06.2022 n. 23401 ha, così, espressamente affermato che le società sono esenti da responsabilità se dimostrano che il comportamento del colpevole è stato tale da aggirare o violare le regole del MOG

in maniera ingannevole e fraudolenta, non essendo sufficiente una violazione frontale del MOG.

In altre parole, il MOG non può contenere regole e controlli solamente formali ma deve contenere presidi che in concreto siano efficaci, cosicché solamente un ben costruito disegno criminoso possa aver successo, mentre quelli più elementari devono poter essere rilevati dal sistema organizzativo e di controllo.

Sul punto, il Tribunale di Milano, con la sentenza del 7 aprile 2021 ha precisato che la colpa nell'organizzazione consiste anche nell'inerzia dell'OdV, se il reato non si sarebbe verificato se l'OdV si fosse adeguatamente attivato o se l'OdV avesse avuto la possibilità di esprimere una *dissenting opinion* rispetto ad un prospettato comportamento.

Quanto alla composizione dell'Organismo di Vigilanza, proprio ai fini di maggiori e migliori controlli, la giurisprudenza più recente ha affermato che l'Internal Audit non può essere anche membro dell'OdV in quanto la funzione Audit non sarebbe indipendente rispetto all'ente, riferendo funzionalmente al Consiglio di Amministrazione e, quindi, subendo le direttive di tale organo. Allo stesso modo, è opportuno che non siano nominati membri dell'OdV i dipendenti «operativi», che sono per loro natura incompatibili con compiti di vigilanza, così come non sono indipendenti coloro che ottengono dall'ente o da società ad esso collegate o da esso controllate incarichi ulteriori rispetto a quello di membro dell'OdV (cfr. Trib. Vicenza 7.06.2021; Trib. Milano 12 maggio 2020; Trib. Milano 7 aprile 2021).

La medesima giurisprudenza sopra citata pone, poi, ulteriori problemi sui corretti presidi da porre in essere nelle società per evitare la commissione di reati.

Innanzitutto, infatti, viene affermato che il MOG deve essere costantemente aggiornato sia in funzione dell'evoluzione dell'ente sia in funzione dell'evoluzione della società e del progressivo aumento del numero e tipologia dei reati rientranti nel D. Lgs. 231/2001 e sia in base all'esperienza acquisita dall'ente.

La giurisprudenza ha, poi, anche offerto uno spunto di riflessione sul punto: quando l'OdV afferma che il MOG è da aggiornare, si può affermare che da quel momento il MOG è inidoneo in quanto riconosciuto come tale dall'OdV?

L'opinione prevalente è che il MOG non può certamente essere considerato integralmente inidoneo, ma eventualmente solo per la parte interessata dalle future modifiche. Inoltre, anche la parte interessata dalle modifiche ha quasi certamente ancora una sua valenza ed efficacia. Per tale motivo, affermare che la richiesta di aggiornamento del MOG da parte dell'OdV sia un riconoscimento di inefficacia del MOG stesso è eccessivo, ma è un giusto stimolo per l'ente per procedere all'aggiornamento.

Un diverso aspetto esaminato dalla giurisprudenza è quello relativo al numero minimo di incontri dell'OdV, tipologia di valutazioni dell'OdV e loro formalizzazione, e approfondimenti dell'OdV.

La recente giurisprudenza afferma che l'OdV dovrebbe svolgere un numero di riunioni non predeterminato ma pari a quelle di fatto necessarie per un adeguato controllo. Durante le riunioni, l'OdV deve essere posto in grado di esaminare e valutare i documenti rilevanti e deve dare atto a verbale del proprio esame.

In sostanza, in base a tale recente giurisprudenza, l'OdV deve approfondire sempre i temi che siano apparentemente sensibili, richiedendo i documenti necessari, svolgendo interviste ed approfondimenti. Un diverso agire rischia di essere interpretato come una carenza organizzativa di cui all'art. 6 D. Lgs. 231/2001.

La recente giurisprudenza sembra aver, dunque, individuato nell'OdV l'organo perno di tutta la fase di controllo e viene, pertanto, richiesto all'OdV di poter dimostrare l'effettività dei flussi informativi, l'efficacia dei controlli, eventualmente anche svolgendone a sorpresa, differenziandoli per aree di rischio, così supportando l'ente non solo nella prevenzione del reato ma anche nell'impedimento dello stesso.

2. La compliance integrata anche alla luce dei principi giurisprudenziali emersi e dall'esperienza applicativa

2.1 La compliance integrata: quali ambiti, quali funzioni e come?

Al recente incremento della regolamentazione, nazionale e comunitaria, dell'attività di impresa è senz'altro conseguito uno speculare incremento dei rischi cui le società sono esposte. Si pensi, ad esempio, alla disciplina anticorruzione, a quella ambientale, antiriciclaggio, alle tematiche di gestione della salute e sicurezza sul lavoro, ecc.. Tali discipline prevedono un set di sanzioni a carico delle società per la loro inosservanza.

Peraltro, spesso la violazione dei precetti previsti da tali discipline può assumere rilevanza penale. Ai predetti rischi connessi a specifiche fattispecie di reato, a carico degli esponenti delle società, si affianca anche il rischio di responsabilità amministrativa degli enti ai sensi del D. Lgs. 231/2001. Molti dei reati posti a presidio dei vari *framework* regolatori definiti dal legislatore nazionale e da quello comunitario sono, infatti, inclusi nel c.d. "Catalogo dei reati presupposto" di cui al D. Lgs. 231/2001.

Ne consegue che uno dei principali strumenti per gestire e mitigare i vari rischi cui le società sono esposte possa essere proprio il modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001 (o "Modello Organizzativo") come misura di compliance necessaria (ancorché, da sola, non sufficiente) perché l'ente possa beneficiare della condizione esimente della responsabilità amministrativa dipendente da reato.

Nondimeno, come anticipato, nel corso degli ultimi anni il *focus* sulla *compliance* richiesto alle società nei vari contesti normativi in cui operano si sta

dimostrando sempre più stringente e articolato, rendendo complesse e onerose le attività per la gestione dei rischi di conformità perfino per quelle società dotate di un Modello Organizzativo.

Le varie novelle legislative europee tra cui la "Direttiva *Whistleblowing*" richiedono alle aziende interventi di adeguamento spesso non coordinati che comportano spesso un aggravio dei costi di compliance (alla luce della necessità di prevedere nuovi presidi di controllo, adottare procedure e istituire organi di controllo *ad hoc*).

Ne è scaturita l'esigenza, sempre più diffusa, di integrare i sistemi di *compliance* adottati dalle società all'interno di un unico sistema. Le stesse "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231" (le c.d. "Linee Guida di Confindustria"), nell'ultima versione aggiornata a giugno 2021, confermano tale esigenza: "*Ciò posto, la gestione dei numerosi obblighi di compliance, secondo un approccio tradizionale, può risultare connotata da una pluralità di processi, informazioni potenzialmente incoerenti, controlli potenzialmente non ottimizzati, con conseguente ridondanza nelle attività. Il passaggio ad una compliance integrata potrebbe permettere invece agli Enti di: • razionalizzare le attività (in termini di risorse, persone, sistemi, ecc.); • migliorare l'efficacia ed efficienza delle attività di compliance; • facilitare la condivisione delle informazioni attraverso una visione integrata delle diverse esigenze di compliance, anche attraverso l'esecuzione di risk assessment congiunti, e la manutenzione periodica dei programmi di compliance (ivi incluse le modalità di gestione delle risorse finanziarie, in quanto rilevanti ed idonee ad impedire la commissione di molti dei reati espressamente previsti come fondanti la responsabilità degli enti)*.".

Una *compliance* integrata può infatti accompagnare l'attività di impresa lungo un percorso di rispetto e applicazione delle norme cogenti, nonché nelle scelte di conformità volontarie, consentendo una gestione dei processi (e degli annessi rischi) uniforme in tutta la società a prescindere dal mero obiettivo di prevenzione di reati.

Questo percorso verso una compliance integrata è strettamente connesso ad una strutturata **analisi dei rischi** insiti nella complessità dei processi, nell'applicazione delle norme, nella prevenzione e gestione di eventi avversi, nel monitoraggio dell'applicazione delle procedure. Inoltre, questo percorso si basa su una sinergia tra le varie funzioni aziendali deputate alla gestione dei singoli modelli di compliance: detto altrimenti, occorrerà passare dal paradigma secondo cui ogni *process owner* sia anche *risk owner* rispetto al singolo processo (ad esempio, la Funzione Finance con riferimento ai rischi AML) a una gestione integrata, in cui ciascun responsabile di funzione sia consapevole del ruolo che esercita non soltanto nella gestione dei rischi direttamente connessi alla propria area di competenza, ma anche a quelli – direttamente ricollegati a differenti aree aziendali – rispetto ai quali può comunque contribuire.

A riguardo, soccorrono nuovamente le Linee Guida di Confindustria: "*Per dare attuazione a una gestione integrata di questo tipo occorre quindi anche definire specifici e continui meccanismi di coordinamento e collaborazione tra i principali soggetti aziendali interessati tra i quali, a titolo esemplificativo, il Dirigente Preposto, la funzione*

Compliance, l'Internal Audit, il Datore di lavoro, il responsabile AML (per le imprese che ne sono tenute), il Collegio sindacale, il Comitato per il controllo interno e la revisione contabile (ai sensi dell'art. 19, d.lgs. n. 39/2010) e l'OdV (che ha pur sempre il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento). A tal proposito, si evidenzia l'importanza di definire, tra le informazioni da produrre per l'OdV, quelle che consentano di determinare indicatori idonei a fornire tempestive segnalazioni dell'esistenza o dell'insorgenza di situazioni di criticità generale e/o particolare, al fine di permettere all'Organismo stesso ed eventualmente agli altri attori coinvolti, un monitoraggio continuo basato sull'analisi di potenziali red flag".

2.2 L'interazione/integrazione dei sistemi di compliance nei gruppi societari. Strumenti e complessità.

L'importanza della *compliance* integrata è anche (e soprattutto) avvertita all'interno di gruppi societari, in special modo di quelli che operano all'interno di molteplici giurisdizioni.

Sono proprio questi gruppi a implementare dei *compliance program* internazionali volti alla gestione di molteplici rischi in conformità a più legislazioni. Un esempio può essere costituito dai modelli anticorruzione di gruppo che rispondono all'obiettivo di soddisfare i requisiti regolatori di più giurisdizioni (il D. Lgs. 231/2001 in Italia, il FCPA negli U.S.A., lo UK Bribery Act, la Sapin II ecc.).

Con riferimento a detti gruppi, va ricordato che il D. Lgs. 231/2001 non considera il tema della responsabilità dell'ente appartenente ad un gruppo di imprese e non prevede un "Modello Organizzativo del gruppo".

È tuttavia possibile che, nell'adozione di tale strumento di *compliance*, la società tenga conto degli esistenti *compliance program* di gruppo. Potrebbe risultare efficiente, infatti, il richiamo a linee guida implementate dalla *holding* in materia anticorruzione o antiriciclaggio, in tema di gestione dei rischi ambientali o di salute e sicurezza sui luoghi di lavoro, come pure di gestione delle segnalazioni.

In particolare, le *subsidiary* italiane di gruppi multinazionali potranno attingere a *policy* e procedure di gruppo volte a regolare attività che, a valle del *risk assessment*, si siano rivelate "a rischio" rispetto ai reati presupposto. Giova sul punto richiamare, a titolo esemplificativo, quelle *policy* in materia di *Gift & Hospitality*, spesso approvate a livello di gruppo, che possono costituire idoneo presidio nella regolamentazione di pratiche a rischio corruttivo: i principi previsti da simili *policy* potranno essere richiamati all'interno del Modello Organizzativo. Inoltre, un sistema di *compliance* integrata risulta ulteriormente rafforzato grazie alla possibilità di coordinare le attività dei vari *process owner* e *risk owner* delle *subsidiary* e della controllante, evitando duplicazioni dei controlli e ottimizzando, così, il funzionamento del sistema di controllo. Anche le Linee Guida di Confindustria valorizzano il supporto del gruppo nella costruzione di un sistema di *compliance* 231 della *subsidiary*: "*In tale contesto, pertanto, le società controllate potrebbero ragionevolmente richiedere alle competenti funzioni della capogruppo (in*

luogo del ricorso a consulenti esterni) un supporto di natura prettamente consulenziale, dai contenuti maggiormente operativi rispetto al ruolo di indirizzo generale sopra richiamato, volto invece ad agevolare le attività di adozione, aggiornamento, implementazione e monitoraggio del proprio Modello 231 (ad es. supporto al management per la valutazione delle attività o processi astrattamente a rischio; orientamento nella strutturazione dei flussi informativi verso l'Organismo di vigilanza; indicazioni sulle caratteristiche dei possibili presidi da implementare a fronte delle aree di rischio individuate; contributi professionali ai fini dell'aggiornamento dei Modelli per evoluzioni normative con impatto sulle specifiche realtà del gruppo rispetto alle indicazioni generali; attività formative e di sensibilizzazione sulla materia; supporto operativo all'Organismo di vigilanza nell'espletamento delle attività di monitoraggio).".

3. L'approccio metodologico integrato tra D. Lgs. 231/2001, Anticorruzione e Trasparenza

Il tema della integrazione del D. Lgs. 231/2001 con altri sistemi preventivi della corruzione è di particolare interesse per gli enti e le società che soggiacciono all'applicazione della L. 190/2012.

Il comma 2-*bis* dell'art. 1 della L. 190/2012 prevede, infatti, che il Piano nazionale anticorruzione costituisca atto di indirizzo per le pubbliche amministrazioni di cui all'art. 1, comma 2, del D. Lgs. 165/2001, ai fini dell'adozione dei propri Piani Triennali di Prevenzione della Corruzione, e per gli altri soggetti di cui all'art. 2-bis, comma II, del D. Lgs. 33/2013, ai fini dell'adozione di misure di prevenzione della corruzione integrative di quelle adottate ai sensi del D. Lgs. 231/2001.

Il citato comma 2-*bis* dell'art. 1 – come diffusamente evidenziato da ANAC nella delibera 1134/2017 - non ha reso obbligatoria l'adozione del Modello Organizzativo ex D. Lgs. 231/2001, che continua dunque ad essere implementato unicamente su base discrezionale (benché per ANAC sia una scelta fortemente raccomandata), ma ha previsto l'obbligo per le società già dotate di Modello Organizzativo di integrare le misure di prevenzione della corruzione con misure idonee a prevenire anche i fenomeni di corruzione e di illegalità in coerenza con le finalità della L. 190/2012.

Ciò sicuramente nella piena consapevolezza che il passaggio ad una compliance integrata consente di razionalizzare i sistemi implementati ai sensi del D. Lgs. 231/2001 e della L. 190/2012, di migliorare l'efficace e l'efficienza delle attività, di facilitare la condivisione delle informazioni, di ottimizzare i controlli, evitando così inutili e costose sovrapposizioni e pericolose lacune.

Del resto, sebbene la normativa anticorruzione e quella dettata dal D. Lgs. 231/2001 presentino evidenti differenziazioni - prima tra tutte il fatto che il D. Lgs. 231/2001 ha riguardo ai reati commessi nell'interesse o a vantaggio dell'ente, mentre la L. 190/2012 previene reati commessi in danno dell'ente ed episodi di corruzione, intesi in un'accezione ampia facendovi ricomprendere non solo l'intera gamma dei delitti contro la pubblica amministrazione, ma anche tutte le situazioni di cattiva amministrazione che possono dare luogo

a una responsabilità di carattere dirigenziale, disciplinare, erariale e pregiudizi all'immagine dell'ente - entrambi i provvedimenti muovono da una finalità comune, che è quella di creare un sistema organizzativo idoneo a contrastare taluni illeciti, primi fra tutti quelli corruttivi, sia in termini di prevenzione che di repressione.

A seguito della normativa citata e delle indicazioni metodologiche offerte da ANAC nella delibera 1134/2017 gli enti e le società che soggiacciono all'applicazione della L. 190/2012 hanno implementato sistemi integrati adottando Modelli che comprendono sia il Modello Organizzativo *ex* del D. Lgs. 231/2001 che le "misure integrative" per la prevenzione della corruzione e della trasparenza di cui alla L. 190/2012, precedentemente inserite nei Piani Triennali per la Prevenzione della Corruzione e Trasparenza (PTPCT), ora collocate in apposita sezione e dunque chiaramente identificabili.

Lo scopo principale è quello di

i attuare e implementare un sistema strutturato e organico di principi, regole di condotta, regolamenti, procedure e protocolli idonei a

- prevenire e contenere il rischio di commissione dei reati previsti nel D. Lgs. 231/2001;
- prevenire e contenere il rischio di fenomeni di corruzione e di illegalità in coerenza con le finalità della L. 190/2012;
- garantire il raggiungimento degli obbiettivi di trasparenza previsti dalla normativa di riferimento e, in particolare, dal D. Lgs. 33/2013;

ii attuare e implementare un sistema strutturato ed organico di verifiche e controlli (preventivi ed *ex post*) idonei a garantire l'efficacia e l'efficienza, in concreto, del Modello Integrato e di tutte le misure ivi previste.

Le indicazioni per costruire i modelli integrati possono riassumersi come segue:

- analisi approfondita dell'ente, della sua organizzazione e del contesto interno ed esterno;
- individuazione e mappatura dei processi a rischio "231/2001 e 190/2012" e delle aree di attività a supporto;
- valutazione delle misure di prevenzione adottate e del sistema dei controlli preventivi in essere;
- integrazione delle procedure e/o regolamenti esistenti, nonché elaborazione di ulteriori misure di prevenzione e presidi di controllo relativamente ai processi e alle attività a supporto risultate, all'esito dell'analisi dei rischi, maggiormente esposte ai rischi;
- implementazione delle misure integrative in materia di anticorruzione e trasparenza precedentemente racchiuse nei PTPCT;

- verifica e implementazione delle attività di monitoraggio e vigilanza sull'efficacia e l'efficienza del Modello Integrato;
- coordinamento fra il sistema di controllo interno previsto ai sensi del D. Lgs. 231/2001 con quello per la prevenzione di rischi di corruzione di cui alla L. 190/2012, attuando meccanismi di integrazione dei controlli e dei flussi informativi tra l'OdV e il Responsabile della prevenzione della corruzione e della trasparenza (RPCT), al fine di garantire, nell'ambito delle rispettive competenze, un maggior livello di prevenzione dei comportamenti illeciti e assicurare l'efficace attuazione del "sistema integrato 231 –Anticorruzione – Trasparenza";
- integrazione del Codice Etico con quanto previsto in materia di Codice di Comportamento dal D. Lgs. 165/2001;
- implementazione di un sistema sanzionatorio volto a garantire l'efficace attuazione del Modello Integrato, contenente le misure disciplinari applicabili in caso di violazione delle prescrizioni ivi contenute;
- revisione del sistema di *whistleblowing* e coordinamento tra l'OdV e il RPCT nella gestione delle segnalazioni e nel sistema dei flussi informativi.

A questo ultimo proposito, le Linee guida ANAC del 2017 sembrano escludere la partecipazione del RPCT nell'OdV collegiale, in ragione delle diverse funzioni attribuite dalle rispettive normative e dalle loro finalità. Pur tuttavia, è certamente necessario un costante coordinamento tra i due organi e, dunque, prevedere ad esempio la stretta collaborazione nella fase di mappatura rischi quantomeno rispetto agli ambiti che presentano rischi corruttivi, la partecipazione del RPCT alle riunioni dell'OdV, la condivisione dei rispettivi piani di *audit*, l'esecuzione congiunta di alcuni *audit* (si pensi ad esempio agli appalti o al conferimento di incarichi), la programmazione condivisa della formazione, specifici flussi documentali reciproci e apposite *policy* per la gestione delle segnalazioni

NOTE

NOTE

NOTE

NOTE

NOTE

NOTE

ASLA, Associazione Studi Legali Associati, editrice di questo Quaderno (*www.aslaitalia.it*), comprende circa cento fra i principali Studi nazionali e di affiliazione estera operanti in Italia (fra cui quelli a cui appartengono le curatrici e i co-autori del Quaderno stesso, sotto specificati), ove è stata constituita nel 2003 come organizzazione apolitica senza scopo di lucro, operando in particolare nel settore del diritto d'impresa e con il fine di promuovere e diffondere la cultura e le modalità più attuali dell'esercizio della professione legale in forma associata, organizzata e certificabile.

In particolare, hanno contribuito a questo Quaderno:

L'Avv. **Irene Picciano**, curatrice e co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Antonio Bana**, curatore e co-autore del Capitolo 4 di questo Quaderno, dello Studio Legale Bana Avvocati Associati (www.studiobana.it)

L'Avv. **Micaela Barbotti**, co-autrice del Capitolo 6 di questo Quaderno, di A&A Studio Legale Associato (www.albeeassociati.it)

L'Avv. **Angela Berinati**, co-autrice del Capitolo 3 di questo Quaderno, di A&A Studio Legale Associato (www.albeeassociati.it)

L'Avv. **Francesca Bevilacqua**, co-autrice del Capitolo 4 di questoQuaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli& Partners (www.gop.it)

L'Avv. **Pietro Boccaccini**, co-autore del Capitolo 1 di questo Quaderno, di Deloitte Legal Studio Legale (www.deloitte.com/it)

L'Avv. **Tiziana Boneschi**, co-autrice del Capitolo 6 di questo Quaderno, di LCA Studio Legale (www.lcalex.it)

L'Avv. **Eva Cruellas Sada**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)

L'Avv. **Simona Custer**, co-autrice del Capitolo 2 di questo Quaderno, di A&A Studio Legale Associato (www.albeeassociati.it)

L'Avv. **Paola De Pascalis**, co-autrice del Capitolo 4 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.pavia-ansaldo.it)

L'Avv. **Federica Dendena**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato SILS (www.silsitalia.it)

L'Avv. **Eugenia Gambarara**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)

L'Avv. **Giacomo Gori**, co-autore del Capitolo 2 di questo Quaderno, di Cocuzza & Associati Studio Legale (www.cocuzzaeassociati.it)

L'Avv. **Piero Magri**, co-autore del Capitolo 4 di questo Quaderno, dello Studio Legale Associato RP Legal & Tax (www.rplt.it)

L'Avv. **Federica Mammì Borruto**, co-autrice del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)

L'Avv. **Andrea Mantovani**, co-autore del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)

La Dott.ssa **Elena Mandarà**, co-autrice del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Marta Margiocco**, co-autrice del Capitolo 3 di questo Quaderno, di Cocuzza & Associati Studio Legale (www.cocuzzaeassociati.it)

L'Avv. G**iulio Novellini**, co-autore del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Pietro Orzalesi**, co-autore del Capitolo 6 di questo Quaderno, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

L'Avv. **Mariangela Papadia**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.pavia-ansaldo.it)

L'Avv. **Josephine Romano**, co-autrice del Capitolo 6 di questo Quaderno, di Deloitte Legal Studio Legale (www.deloitte.com/it)

L'Avv. **Roberto Tirone**, co-autore del Capitolo 6 di questo Quaderno, di Cocuzza & Associati Studio Legale (www.cocuzzaeassociati.it)

Pubblicazione giuridica n° 24 di ASLA del 25 luglio 2023

A cura del Gruppo di lavoro sulla Corporate Compliance
Curatori: Irene Picciano e Antonio Bana
Editor: Ezio Rotamartir – *rotamartir.it*

Elaborazioni grafiche e impaginazione: Ezio Rotamartir
su progetto grafico originale di Edoardo Steiner

www.aslaitalia.it

In particolare, hanno contribuito a questo Quaderno:
L'Avv. **Irene Picciano**, curatrice e co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Antonio Bana**, curatore e co-autore del Capitolo 4 di questo Quaderno, dello Studio Legale Bana Avvocati Associati (www.studiobana.it)

L'Avv. **Micaela Barbotti**, co-autrice del Capitolo 6 di questo Quaderno, di A&A Studio Legale Associato (www.albeeassociati.it)

L'Avv. **Angela Berinati**, co-autrice del Capitolo 3 di questo Quaderno, di A&A Studio Legale Associato (www.albeeassociati.it)

L'Avv. **Francesca Bevilacqua**, co-autrice del Capitolo 4 di questoQuaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli& Partners (www.gop.it)

L'Avv. **Pietro Boccaccini**, co-autore del Capitolo 1 di questo Quaderno, di Deloitte Legal Studio Legale (www.deloitte.com/it)

L'Avv. **Tiziana Boneschi**, co-autrice del Capitolo 6 di questo Quaderno, di LCA Studio Legale (www.lcalex.it)

L'Avv. **Eva Cruellas Sada**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)

L'Avv. **Simona Custer**, co-autrice del Capitolo 2 di questo Quaderno, di A&A Studio Legale Associato (www.albeeassociati.it)

L'Avv. **Paola De Pascalis**, co-autrice del Capitolo 4 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.pavia-ansaldo.it)

L'Avv. **Federica Dendena**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato SILS (www.silsitalia.it)

L'Avv. **Eugenia Gambarara**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)

www.aslaitalia.it

L'Avv. **Giacomo Gori**, co-autore del Capitolo 2 di questo Quaderno, di Cocuzza & Associati Studio Legale (www.cocuzzaeassociati.it)

L'Avv. **Piero Magri**, co-autore del Capitolo 4 di questo Quaderno, dello Studio Legale Associato RP Legal & Tax (www.rplt.it)

L'Avv. **Federica Mammì Borruto**, co-autrice del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)

L'Avv. **Andrea Mantovani**, co-autore del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)

La Dott.ssa **Elena Mandarà**, co-autrice del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Marta Margiocco**, co-autrice del Capitolo 3 di questo Quaderno, di Cocuzza & Associati Studio Legale (www.cocuzzaeassociati.it)

L'Avv. G**iulio Novellini**, co-autore del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Pietro Orzalesi**, co-autore del Capitolo 6 di questo Quaderno, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

L'Avv. **Mariangela Papadia**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.pavia-ansaldo.it)

L'Avv. **Josephine Romano**, co-autrice del Capitolo 6 di questo Quaderno, di Deloitte Legal Studio Legale (www.deloitte.com/it)

L'Avv. **Roberto Tirone**, co-autore del Capitolo 6 di questo Quaderno, di Cocuzza & Associati Studio Legale (www.cocuzzaeassociati.it)

ASLA, **Associazione Studi Legali Associati**, *www.aslaItalia.it*, editore di questo Quaderno, comprende circa cento fra i principali Studi nazionali e di affiliazione estera operanti in Italia (fra cui quelli a cui appartengono gli autori del Quaderno stesso, sopra specificati), ove è stata constituita nel 2003 come organizzazione apolitica senza scopo di lucro, operando in particolare nel settore del diritto d'impresa e con il fine di promuovere e diffondere la cultura e le modalità più attuali dell'esercizio della professione legale in forma associata, organizzata e certificabile.

ASLA
ASSOCIAZIONE STUDI LEGALI ASSOCIATI