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

CORPORATE COMPLIANCE ROUND TABLES 2019

Atti del convegno con sette tavole rotonde con la partecipazione di ventitre 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 ALESSANDRA ANSELMI, ANTONIO BANA, MICAELA BARBOTTI, FRANCESCA CHIARA BEVILACQUA, PIETRO BOCCACCINI, DEBORAH BOLCO, TIZIANA BONESCHI, EVA CRUELLAS SADA, SIMONA CUSTER, PAOLA DE PASCALIS, FEDERICA DENDENA, EUGENIA GAMBARARA, GIACOMO GORI, PIERO MAGRI, ANDREA MANTOVANI, MARTA MARGIOCCO, GIULIO NOVELLINI, PIETRO ORZALESI, MARIANGELA PAPADIA, IRENE PICCIANO, EVA REGGIANI, JOSEPHINE ROMANO, ROBERTO TIRONE

CORPORATE COMPLIANCE ROUND TABLES 2019

Atti del convegno con sette tavole rotonde con la partecipazione di ventitre 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 Andrea Mantovani, Giulio Novellini e Eva Reggiani

L'attività ispettiva e sanzionatoria del Garante Privacy: spunti operativi per prepararsi al meglio

SOMMARIO: 1. *Enforcement* del GDPR: stato dell'arte e principali orientamenti a livello nazionale ed europeo – 2. L'attività ispettiva del Garante Privacy – 2.1 La pianificazione dell'attività ispettiva – 2.2 I poteri ispettivi del Garante Privacy – 2.3 La rilevanza dell'*accountability* in sede di ispezione – 3. Il procedimento innanzi al Garante Privacy: il Regolamento n. 1/2019 – 4. L'attività sanzionatoria del Garante Privacy – 4.1 I poteri correttivi del Garante Privacy: elementi di continuità con il Codice Privacy e principali novità introdotte dal GDPR – 4.2 Le sanzioni per le violazioni della normativa in materia di protezione dei dati personali nel GDPR e nel Codice Privacy

1. *Enforcement* del GDPR: stato dell'arte e principali orientamenti a livello nazionale ed europeo

Con l'entrata in vigore del Regolamento Generale sulla Protezione dei Dati n. 2016/679 ("GDPR"), datata 25 maggio 2018, la realtà normativa in tema di protezione dei dati personali è radicalmente mutata. Da una parte, gli Stati membri dell'Unione europea hanno dovuto implementare la propria legislazione *privacy* di riferimento, ove già esistente, o redigerla *ex novo*, se mancante; dall'altra, le imprese hanno cominciato a rimodellare, talvolta sopportando notevoli costi, la propria strategia gestionale circa il trattamento e la conservazione dei dati personali, per essere *compliant* con il nuovo dettato normativo di matrice europea. Ciò ha altresì determinato una revisione in merito alle modalità di *business* delle imprese, fino a quel momento utilizzate.

Tra le più rilevanti novità introdotte dal GDPR si evidenziano: (*i*) la redazione di un dettagliato Registro dei trattamenti che racchiude la c.d. mappatura di tutti i processi di trattamento eseguiti dall'impresa; (*ii*) l'effettuazione di una valutazione d'impatto sulla protezione dei dati (o *Data Protection Impact Assessment*; "DPIA") ogniqualvolta il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche interessate; (*iii*) la designazione di un DPO nei casi richiesti dal GDPR, ed ancora (*iv*) l'imposizione di un'etica

generalizzata verso il trattamento dei dati personali, riassumibile nel concetto di *accountability* [1].

Sebbene il GDPR, quale strumento legislativo, possa definirsi direttamente applicabile agli Stati membri, i tempi e le modalità di attuazione dello stesso non sono stati omogenei a livello europeo. Ad esempio, come poc'anzi ricordato, alcuni Stati membri hanno implementato la preesistente normativa *privacy* alla luce delle nuove regole poste dal GDPR. È il caso dell'Italia, che ha visto l'introduzione del d.lgs. 101/2018 volto a modificare il Codice Privacy (d.lgs. 196/2003), e ancora, dell'Austria, Bulgaria, Francia, Germania e Ungheria. Altri Stati membri hanno invece colto l'opportunità per introdurre nuovi testi legislativi in materia di protezione dei dati personali (Danimarca, Polonia, Estonia e Svezia).

Ancora differenti sono stati gli approcci dei singoli legislatori nazionali su specifici temi *privacy* disciplinati (e non) dal GDPR. Tale normativa, invero, fornisce una soglia di tutela minima che dev'essere uniformemente garantita in ogni nazione, ma nulla vieta al singolo Stato membro di emanare regole più garantiste e stringenti secondo propria discrezionalità. A titolo esemplificativo il GDPR si applica alle sole persone vive, tuttavia Bulgaria, Repubblica Ceca, Estonia, Danimarca, Francia ed Italia (nello specifico attraverso l'articolo 2-*terdecies* del d.lgs. 101/2018) hanno esteso la tutela alle persone defunte, garantendo che l'esercizio dei diritti di cui agli articoli 15-22 GDPR possa essere effettuato anche da altri soggetti di volta in volta identificati nei vari atti legislativi.

Trattando del consenso prestato da soggetti minorenni si verificano molteplici differenze tra gli Stati membri: per Belgio, Danimarca, Estonia, Finlandia, Portogallo e Svezia, l'età minima per poter prestare il proprio consenso al trattamento dei dati è 13 anni; in Austria, Bulgaria, Italia, Lituania e Spagna 14 anni; in Polonia, Croazia, Germania, Ungheria e Slovacchia l'età minima si eleva ad anni 16.

Anche per ciò che attiene alla già citata DPIA (o valutazione d'impatto) si registrano forti divergenze tra gli Stati membri. Alcuni Stati hanno introdotto disposizioni di rango nazionale volte ad incrementare la lista di ipotesi che richiedono la necessità di una DPIA (per citarne solo alcuni: Austria, Danimarca, Francia, Grecia, Irlanda e Norvegia), mentre altri hanno mantenuto intatto il tessuto normativo predisposto sul tema dal legislatore europeo all'articolo 35 del GDPR.

Inoltre, a livello sanzionatorio, a distanza di due anni dall'entrata in vigore del GDPR è possibile affermare che le Autorità di controllo si sono distinte fortemente per il numero di procedimenti aperti o l'ammontare delle sanzioni irrogate. Se in Italia e Spagna si è registrato nel corso del 2019 il maggior numero di casi che hanno poi condotto all'emanazione di un provvedimento sanzionatorio ad opera dei rispettivi Garanti (30 per l'Italia e 28 per la Spagna),

1 Ovvero la responsabilità di rendicontare il trattamento dei dati personali sia sul piano della regolarità e conformità a quanto previsto dalla normativa *privacy*, sia su quello dell'efficacia della loro gestione.

è pur vero che l'importo medio per sanzione risulta ben inferiore rispetto a quello di Paesi quali Germania e Francia.

La disomogeneità che caratterizza le modalità attuative del GDPR, nonché il rispettivo frequente rimando ad implementazioni da emanarsi con legge nazionale, ha imposto alle varie Autorità di controllo nazionali e ad organismi europei, quali il Gruppo di lavoro Articolo 29 ("WP29") e il Comitato Europeo per la Protezione dei Dati (o *European Data Protection Board*; "EDPB"), la necessità di predisporre alcune misure finalizzate ad accrescere la comprensione, interpretazione e gestione di tutti gli adempimenti derivanti dalla normativa regolamentare.

Anche nei confronti delle persone fisiche, interessate al trattamento dei rispettivi dati personali, è essenziale garantire chiarezza e semplicità nelle dichiarazioni. A tal riguardo, di significativa importanza è l'articolo 12 del GDPR, dove viene chiarito che il titolare del trattamento è tenuto a predisporre un'informativa in forma concisa, trasparente ed intelligibile, specie quando quest'ultima sia diretta a soggetti minori. Ed invero, sempre allo scopo di agevolare la comprensione della normativa europea da parte dei soggetti coinvolti nel trattamento, si sono mosse le Autorità nazionali, predisponendo sui propri siti istituzionali strumenti dedicati agli utenti: infografiche semplificate su temi specifici, aree dedicate alle FAQ, e infine, come di recente si è avuto modo di riscontrare in occasione dell'emergenza Covid-19, singole sezioni *web* dedicate a macro argomenti, volte sia a riassumere in un unico contesto le novità legislative sull'argomento, sia a fornire suggerimenti pratici.

Peraltro, poiché l'effettività delle tutele approntate dal GDPR postula, fra l'altro, un *enforcement* coerente nei diversi Stati membri anche sotto il profilo sanzionatorio, l'art. 70(1)(k) del GDPR attribuisce specificamente all'EDPB il compito di "*elaborare per le autorità di controllo linee guida riguardanti l'applicazione delle misure di cui all'articolo 58, (1)-(3), e la previsione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 83*" che ad oggi non sono ancora state predisposte, sebbene alcune autorità di controllo nazionali[2] abbiano adottato proprie linee guida in materia e nonostante l'istituzione, in seno all'EDPB della c.d. *Taskforce fining* alla quale partecipa anche il Garante per la protezione dei dati personali italiano[3].

2 Si fa riferimento alle linee guida pubblicate nell'ottobre 2019 dalle autorità garanti tedesche (https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf) nonché a quelle pubblicate dall'autorità garante belga nel marzo 2019 (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586.pdf).

3 In proposito, la Relazione Annuale 2019 del Garante Privacy presentata al Parlamento il 23 giugno 2020, p. 172 (consultabile al seguente link: https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2019.pdf/4fcc5ca8-5ca7-432f-c3f8-4e9e69181a23?version=1.1).

2. L'attività ispettiva del Garante Privacy

2.1 La pianificazione dell'attività ispettiva

Parte dell'attività ispettiva del Garante per la protezione dei dati personali ("Garante Privacy" o "Autorità") viene programmata sulla base di un piano ispettivo semestrale che questi pubblica periodicamente sul proprio sito *web* istituzionale. Ad esempio, nel piano ispettivo relativo al primo semestre del 2020 approvato con deliberazione del 6 febbraio 2020[4], l'Autorità ha pianificato lo svolgimento di 80 accertamenti ispettivi di iniziativa concentrandoli su attività di trattamento di dati personali effettuate in determinati ambiti, quali, ad esempio, i trattamenti effettuati (*i*) da società multinazionali operanti nel settore farmaceutico e sanitario, con riguardo a dati personali relativi alla salute; (*ii*) nel quadro dei servizi bancari *on line*; (*iii*) mediante applicativi per la gestione delle segnalazioni di condotte illecite (c.d. *whistleblowing*); (*iv*) per la gestione e la registrazione delle telefonate nell'ambito del servizio di *call center*; (*v*) per attività di *marketing*; (*vi*) relativamente all'attività di profilazione degli interessati che aderiscono a carte di fidelizzazione; nonché prevedendo "*controlli nei confronti di soggetti, pubblici e privati, appartenenti a categorie omogenee sui presupposti di liceità del trattamento e alle condizioni per il consenso, qualora il trattamento sia basato su tale presupposto, sul rispetto dell'obbligo dell'informativa nonché sulla durata della conservazione dei dati*".

Inoltre, una parte molto importante dell'attività ispettiva dell'Autorità trova la propria radice nei reclami presentati dagli interessati ai sensi dell'art. 77 del GDPR nonché nelle segnalazioni presentate dagli interessati oppure dalla Guardia di Finanza[5] così come nelle notifiche di violazioni di dati personali (*data breach*)[6] oppure in notizie pubblicate sulla stampa[7].

Per comprendere l'effettivo perimetro di qualunque accertamento ispettivo del Garante Privacy è fondamentale esaminare attentamente l'ordine di servizio ex art. 22, comma 5, del regolamento n. 1/2019 ("Regolamento n. 1/2019")[8], che deve essere consegnato al destinatario del controllo e nel quale sono indicati, oltre all'ambito del controllo, informazioni chiave quali, ad esempio, i poteri di

4 Consultabile al seguente link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9269607. Alla data di redazione del presente lavoro, non è ancora disponibile il piano ispettivo del Garante Privacy per il secondo semestre 2020.

5 https://bit.ly/2Cz5Cya sul quale si rimanda al paragrafo 2.2 che segue.

6 Cfr. il considerando n. 87 del GDPR il quale prevede, fra l'altro, che la notifica all'autorità di controllo, di una violazione di dati personali "*può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal [GDPR]*".

7 Cfr. il provvedimento del 28 febbraio 2019 relativo a un dispositivo che una società che si occupa della raccolta dei rifiuti intendeva far indossare agli operatori ecologici (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9094427), ma anche, fra i casi più recenti, l'istruttoria avviata a seguito dell'attacco informativo ai danni della piattaforma Rousseau annunciato tramite Twitter (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7400401).

8 Regolamento n. 1/2019 "*concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali*".

indagine utilizzati, il luogo in cui si svolgerà l'accertamento nonché le sanzioni previste dall'art. 83(5)(e) del GDPR e dagli artt. 166 e 168 del Codice Privacy.

2.2 I poteri ispettivi del Garante Privacy

Uno degli aspetti maggiormente innovativi del GDPR, che mira a garantire coerenza applicativa delle sue disposizioni, consiste nel "*radicamento regolamentare dei poteri riconosciuti alle autorità di controllo*"[9], ossia nell'aver individuato in modo più puntuale e dettagliato rispetto a quanto non prevedesse la direttiva n. 95/46/EC i compiti e i poteri attribuiti alle autorità di controllo nazionali.

Con specifico riferimento ai poteri di indagine (e pur facendo salva la possibilità, per gli Stati membri, di ampliarne il novero[10]), l'art. 58(1) del GDPR prevede che ciascuna autorità di controllo abbia, fra l'altro, il potere di (*i*) ingiungere al titolare e al responsabile del trattamento (nonché, ove applicabile, al rappresentante del titolare o del responsabile del trattamento) di fornirle ogni informazione necessaria per l'esecuzione dei propri compiti; (*ii*) condurre indagini sotto forma di attività di revisione sulla protezione dei dati personali; (*iii*) effettuare un riesame delle certificazioni rilasciate; nonché (*iv*) ottenere dal titolare o dal responsabile del trattamento accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei propri compiti, così come a tutti i locali del titolare o del responsabile del trattamento, ivi inclusi gli strumenti e i mezzi utilizzati per il trattamento dei dati personali, nel rispetto della legislazione europea o del diritto processuale nazionale.

In Italia, nel regime precedente al GDPR, il Garante Privacy già godeva di poteri ispettivi piuttosto ampi. In particolare, oltre alla possibilità di richiedere informazioni nonché l'esibizione di documenti al titolare, al responsabile del trattamento, all'interessato ma anche a terzi[11], già si prevedeva che l'Autorità avesse il potere di "*disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali*", non solo presso la sede del titolare o del responsabile del trattamento, ma anche presso l'"*abitazione o in un altro luogo di privata dimora o nelle relative appartenenze*"[12], in quest'ultimo caso essendo necessario l'assenso informato del titolare o del responsabile del trattamento o la "*previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento*"[13].

9 Cfr. G. M. Riccio, G. Scorza, E. Belisario (a cura di), GDPR e normativa privacy, 2018, Milano, p. 486 e ss.

10 Cfr. art. 58(6) del GDPR il quale prevede che "[o]*gni Stato membro può prevedere per legge che la sua autorità di controllo abbia ulteriori poteri rispetto a quelli di cui ai paragrafi 1, 2 e 3*". In proposito, cfr. l'art. 154-bis del Codice Privacy.

11 Cfr. l'art. 157 del Codice Privacy che, nella propria formulazione precedente al d.lgs. n. 101/2018, prevedeva che "[p]*er l'espletamento dei propri compiti il Garante può richiedere al titolare, al responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti*".

12 Cfr. art. 158, comma 3, del Codice Privacy nella propria formulazione precedente al d.lgs. n. 101/2018 e confermata anche nell'attuale formulazione dell'art. 158, comma 4 del Codice Privacy.

13 Cfr. art. 158, comma 3 nella propria formulazione precedente al d.lgs. n. 101/2018. Si precisa che copia di tale autorizzazione deve essere consegnata "*ai soggetti presso i quali sono eseguiti gli accertamenti*" (cfr. art. 159, comma 2 nella propria formulazione precedente al d.lgs. n. 101/2018).

Il d.lgs. n. 101 del 10 agosto 2018, nel novellare Codice Privacy, ha ampliato poteri ispettivi attribuiti al Garante Privacy. È stato chiarito che il potere dell'Autorità *ex* art. 157 del Codice Privacy di richiedere, prima di eventualmente procedere all'accertamento ispettivo *in loco*, informazioni e l'esibizione di documenti, oltre ad essere esercitabile anche nei confronti del rappresentante del titolare o del responsabile del trattamento (se presente), è applicabile anche "*anche con riferimento al contenuto di banche dati*"[14]. Inoltre, il potere di accesso dell'Autorità *ex* art. 158 del Codice Privacy è esercitabile, con le stesse garanzie previste per gli accertamenti svolti presso l'abitazione o altri luoghi di privata dimora (*i.e.*, consenso informato del destinatario dell'accertamento oppure autorizzazione del presidente del tribunale competente per territorio) anche con riferimento a "*reti di comunicazione accessibili al pubblico, potendosi procedere all'acquisizione di dati e informazioni on-line*"[15].

Inoltre, è stata introdotta una tipologia di controllo, denominata "attività di revisione" (o "*data protection audit*" nella versione in inglese del GDPR) prevista dall'art. 52(1)(b) del GDPR. Come precisato dall'art. 22, comma 4 del Regolamento n. 1/2019, tale attività può essere avviata presso la sede del titolare del trattamento o del responsabile oppure presso la sede dell'Autorità (in questo caso, previa convocazione del titolare del trattamento o del responsabile del trattamento da parte dell'Autorità stessa) senza essere necessariamente preceduta da una richiesta di informazioni *ex* art. 157 del Codice Privacy. Al momento, considerata la recente introduzione, non è possibile prevedere come il Garante Privacy intenderà utilizzare questa tipologia di controllo[16]; in ogni caso, non pare trattarsi di un'attività ispettiva in senso stretto e, quindi, il Garante Privacy potrebbe utilizzarla anche per analizzare attività di trattamento nuove o comunque meritevoli di attenzione; in ogni caso, ove l'attività di revisione riveli "*elementi di criticità nel trattamento dei dati personali" potranno "essere avviate attività ispettive al fine di rilevare eventuali violazioni della normativa sulla protezione dei dati personali*"[17].

Inoltre, il GDPR rafforza notevolmente la collaborazione e cooperazione fra le autorità di controllo dei vari Stati membri non limitandole al meccanismo del c.d. *one stop shop*[18], ma attribuendo loro portata più generale, con l'obiet-

14 Cfr. art. 157 del Codice Privacy attualmente vigente.

15 Cfr. art. 158, comma 5 del Codice Privacy attualmente vigente, in cui si precisa altresì che "*a tal fine, viene redatto apposito verbale in contraddittorio con le parti ove l'accertamento venga effettuato presso il titolare del trattamento*".

16 In proposito, la Relazione Annuale 2019 del Garante Privacy (cit.), p. 163, riferisce semplicemente che in capo al Dipartimento attività ispettive del Garante Privacy "*sono […] poste le attività di revisione sulla protezione dei dati personali che potranno essere avviate ai sensi dell'art. 58, par. 1, lett. b) del [GDPR], presso il titolare o il responsabile del trattamento ovvero presso la sede dell'Autorità*".

17 Cfr. art. 22, comma 4 del Regolamento 1/2019.

18 In forza di tale meccanismo, nel caso di trattamenti di dati personali transfrontalieri, viene individuata un'autorità di controllo "capofila" ossia "*l'autorità cui spetta in prima battuta la gestione di un trattamento transfrontaliero – per esempio, in caso di reclami presentati da un interessato rispetto al trattamento dei suoi dati personali*" e che "*dovrà coordinare ogni attività di accertamento attraverso il coinvolgimento di altre autorità di controllo 'interessate'" (cfr. Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento del* WP29 del 5 aprile 2017, p. 4 (consultabili al seguente link https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235)).

tivo di garantire un'applicazione e attuazione coerente del GDPR all'interno dell'Unione[19].

In primo luogo, Il GDPR introduce stringenti obblighi di assistenza reciproca che comprendono "*le richieste di informazioni e le misure di controllo, quali le richieste di autorizzazioni e consultazioni preventive e le richieste di effettuare ispezioni e indagini*"[20]. A tali richieste l'autorità di controllo destinataria non può sottrarsi, a meno che non eccepisca (*i*) la propria incompetenza con riferimento all'oggetto della richiesta oppure (*ii*) la circostanza che soddisfarla costituirebbe una violazione delle disposizioni del GDPR o delle normative nazionali o dell'Unione cui l'autorità di controllo destinataria della richiesta è soggetta[21].

In secondo luogo, il GDPR permette di svolgere vere e proprie "*operazioni congiunte, incluse indagini congiunte e misure di contrasto congiunte, cui partecipano membri o personale di autorità di controllo di altri Stati membri*"[22]. In tale contesto, il Garante Privacy ben può effettuare i controlli di cui all'art. 158 del Codice Privacy anche "*con la partecipazione, se del caso, di componenti o personale di autorità di controllo di altri Stati membri dell'Unione europea*"[23].

Nello svolgimento degli accertamenti ispettivi, il Garante Privacy si avvale della Guardia di Finanza in forza di uno specifico protocollo di intesa stipulato il 10 marzo 2016 e attualmente in corso di revisione ("Protocollo d'Intesa")[24]. Il Protocollo d'Intesa prevede che la Guardia di Finanza collabori alle attività ispettive del Garante Privacy mediante, fra l'altro, (*i*) il reperimento di dati e informazioni sui soggetti da sottoporre a ispezione; (*ii*) la partecipazione di proprio personale agli accessi alle banche dati e alle rilevazioni nei luoghi in cui svolgono le attività di trattamento; e (*iii*) l'esecuzione, su richiesta del Garante Privacy, "*di verifiche* on-line, *codificate sulla base di uno o più provvedimenti del Garante [Privacy], volte a rilevare, dall'esame dei siti web e degli altri strumenti telematici utilizzati, il rispetto della disciplina di protezione dei dati personali da parte dei titolari, pubblici e privati, che effettuano trattamenti di dati personali per mezzo di reti telematiche*"[25].

2.3 La rilevanza dell'*accountability* in sede di ispezione

Il principio di *accountability* richiede che il titolare del trattamento sia in grado non soltanto di assicurare il rispetto della normativa in materia di pro-

19 In proposito, l'art. 57 del GDPR prevede che ciascuna autorità di controllo "*collabor[i], anche tramite scambi di informazioni, con le altre autorità di controllo e prest[i] assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del [GDPR]" e che "svolg[a] indagini sull'applicazione del [GDPR], anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica*".

20 Cfr. art. 61(1) del GDPR.

21 Cfr. art. 61(4) del GDPR.

22 Cfr. art. 62 del GDPR.

23 Cfr. art. 158, comma 2 del Codice Privacy.

24 Cfr. Relazione Annuale 2019 del Garante Privacy (cit.), p. 163. Cfr. altresì la Relazione Annuale 2018 del Garante Privacy presentata al Parlamento il 7 maggio 2018, p. 172 e ss. (consultabile al seguente link https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2018.pdf/e5bc382b-c5e9-b41b-b0d8-882f0904e546?version=1.0).

25 Cfr. art. 1 del Protocollo d'Intesa.

tezione dei dati personali, ma anche di dimostrarlo[26]. In proposito, il considerando n. 74 del GDPR precisa che "*il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure*".

Dimostrare di essere *compliant* con il GDPR è certamente un'esigenza che assume fondamentale rilievo nel contesto di un'ispezione del Garante Privacy. È pertanto opportuna la predisposizione di procedure interne che, fra l'altro, contengano adeguate istruzioni al personale su come comportarsi in caso di ispezione e individuino i soggetti, interni (quali, ad esempio, legali interni e personale IT) e/o esterni (quale, ad esempio, il consulente legale oppure il *data protection officer*, se esterno) da coinvolgere durante l'ispezione in quanto in grado di reperire i documenti eventualmente richiesti dal Garante Privacy e di fornire le spiegazioni che l'Autorità dovesse chiedere.

Peraltro, quanto più il destinatario dell'ispezione sarà in grado di collaborare con l'Autorità e documentare le scelte effettuate (ad esempio, in materia di nomina del *data protection officer*, di notifica di un *data breach* o di valutazioni di impatto *ex* art. 35 del GDPR), tanto più l'Autorità potrà tenerne conto (favorevolmente) nella determinazione della sanzione amministrativa pecuniaria *ex* art. 83 del GDPR eventualmente da infliggere, in aggiunta alle (o in luogo delle) misure correttive.

3. Il procedimento innanzi al Garante Privacy: il Regolamento n. 1/2019

Il Garante Privacy, con delibera del 4 aprile 2019 ha emanato il Regolamento n. 1/2019 che dettaglia le procedure interne, aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati a tale Autorità[27]. Più specificamente, il Regolamento n. 1/2019 disciplina le modalità di trattazione di reclami e segnalazioni, l'attività istruttoria, i procedimenti d'ufficio e le attività ispettive.

Il reclamo e la segnalazione al Garante sono due strumenti messi a disposizione per permettere ai soggetti che ritengano infrante le disposizioni in materia *privacy* di contestare tali violazioni. Il reclamo generalmente è proposto direttamente dall'interessato che lamenta la violazione dei propri diritti e richiede l'intervento del Garante Privacy, a differenza della segnalazione, la quale proviene da un qualunque soggetto, purché identificato, ed è volta a sollecitare un controllo da parte del Garante Privacy sulla disciplina rilevante in materia di

26 Cfr. art. 5(2) del GDPR, il quale prevede che "*il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")*". Cfr. altresì l'art. 24 del GDPR, il quale prevede che "[t]*enuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*".

27 In particolare, tali poteri riguardano l'adozione dei provvedimenti correttivi di cui all'art. 58(2) del GDPR, e delle sanzioni di cui agli articoli 83 del GDPR e 166, commi 1 e 2, del Codice Privacy (così come emendato dal d.lgs. n. 101/2018).

trattamento dei dati personali. Il carattere della personalità nella lesione, elemento caratterizzante il reclamo rispetto alla segnalazione, comporta che solo in sede di reclamo il reclamante debba essere informato dall'Autorità – al più tardi entro tre mesi – dello stato o dell'esito del reclamo, mentre al segnalante può (ma non necessariamente deve) essere dato riscontro.

Entrambi gli strumenti appena descritti non sempre comportano l'apertura di un procedimento amministrativo per l'adozione di provvedimenti correttivi e sanzionatori da parte dell'Autorità. Invero, le previsioni di cui agli artt. 11 e 19, comma 5 del Regolamento n. 1/2019 prevedono che in taluni casi[28] il reclamo e la segnalazione, al termine dell'istruttoria preliminare, possano essere archiviati.

Diversamente, qualora il Garante Privacy decidesse di procedere con l'apertura del procedimento amministrativo per l'adozione di provvedimenti correttivi e sanzionatori, si osserveranno le disposizioni di cui agli artt. da 9 a 18 del Regolamento n. 1/2019. Successivamente, il dipartimento o altra unità del Garante Privacy incaricata, avvierà, con propria comunicazione al titolare e, se del caso, al responsabile del trattamento, il procedimento per l'adozione dei provvedimenti di cui agli artt. 58(2) e 83 del GDPR. La comunicazione dovrà contenere: (*i*) una succinta descrizione dei fatti contestati e delle presunte violazioni; (*ii*) l'indicazione dell'Autorità presso la quale sarà possibile estrarre copia degli atti istruttori, e ancora, (*iii*) l'avvertimento che entro trenta giorni sarà possibile esercitare il proprio diritto di difesa (ad esempio, tramite scritti difensivi, richieste d'audizione, presentazione di documenti utili ad evitare le sanzioni).

Come poc'anzi ricordato, il Regolamento n. 1/2019 prevede la possibilità per il Garante Privacy di aprire un'istruttoria preliminare pur in assenza di reclamo, segnalazione o notificazione di violazione dei dati personali. Anche nel corso dell'istruttoria aperta a seguito di procedimento d'ufficio troverà applicazione la disciplina valevole in tema di reclamo e segnalazione.

Sotto il profilo istruttorio, per raccogliere materiale utile all'analisi documentale e al fine di eventualmente contestare il trattamento dei dati personali da parte del titolare e/o del responsabile del trattamento destinatario dell'accertamento ispettivo, l'Autorità esercita i propri poteri istruttori ai sensi degli articoli 157 e 158 del Codice Privacy[29].

Infine, il Regolamento n. 1/2019 prevede che, ove risultino accertati i fatti e le violazioni sospette, il dipartimento o unità del Garante Privacy che abbia seguito la fase istruttoria curi la redazione dello schema di provvedimento da sottoporre al Collegio, il quale provvederà a deliberare i provvedimenti corret-

28 Al termine dell'istruttoria preliminare, l'unità o il dipartimento competente possono decidere di concludere l'esame del reclamo disponendo l'archiviazione. L'art. 11 del Regolamento n. 1/2019 specifica i casi nei quali l'archiviazione può essere disposta. A solo titolo esemplificativo ciò potrà avvenire quando: (*i*) la questione prospettata con il reclamo non sia riconducibile alla protezione dei dati personali o ai compiti demandati al Garante Privacy; (*ii*) quando non siano integrati a seguito dell'istruttoria gli estremi di una violazione della disciplina *privacy*, ovvero (*iii*) la richiesta appaia pretestuosa o sia già stata affrontata dal Garante in altri provvedimenti.

29 Cfr. il paragrafo 2 che precede.

tivi e sanzionatori ritenuti opportuni. Il provvedimento sarà dunque notificato alle parti.

Entro trenta giorni decorrenti momento dal ricevimento della comunicazione del provvedimento i soggetti notificati avranno diritto a proporre ricorso avverso la decisione del Garante in sede giurisdizionale, per contestarne il contenuto nonché eventuali aspetti meramente formali e/o procedurali (ad esempio, violazioni compiute dagli operatori in sede ispettiva). Il ricorso si propone al giudice ordinario ed il rito attinge la propria disciplina dal rito del lavoro, così come enucleata dal codice di procedura civile. Infine, al giudice sono attribuiti i più ampi poteri circa la rimodulazione del contenuto del provvedimento, potendo questi intervenire nella rideterminazione di sanzioni pecuniarie ovvero sindacare l'opportunità del provvedimento adottato.

4. L'attività sanzionatoria del Garante Privacy

4.1 I poteri correttivi del Garante Privacy: elementi di continuità con il Codice Privacy e principali novità introdotte dal GDPR

Analogamente all'approccio adottato con riferimento ai poteri ispettivi, il GDPR individua in modo più puntuale rispetto alla direttiva 95/46/EC e al Codice Privacy i poteri correttivi attribuiti alle autorità di controllo nazionali[30]. In particolare, l'art. 58(2) del GDPR prevede che ciascuna autorità di controllo abbia, *inter alia*, il potere di (*i*) rivolgere avvertimenti al titolare o al responsabile del trattamento in relazione al fatto che le attività di trattamento "*possono verosimilmente violare*" le disposizioni del GDPR; (*ii*) rivolgere ammonimenti al titolare o al responsabile del trattamento nel caso in cui le attività di trattamento effettuate abbiano violato le disposizioni del GDPR; (*iii*) ingiungere al titolare o al responsabile del trattamento di soddisfare le richieste degli interessati di esercizio dei diritti loro garantiti dal GDPR; (*iv*) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; (*v*) revocare una certificazione oppure ingiungere all'organismo di certificazione di ritirare quella già rilasciata (oppure di non rilasciarla); (*vi*) infliggere una sanzione amministrativa pecuniaria *ex* art. 83 del GDPR, in aggiunta alle (o in luogo delle) misure correttive previste dall'art. 58(2) del GDPR, a seconda delle cir-

30 L'art. 154 del Codice Privacy, nella formulazione precedente all'intervento del d.lgs. n. 101/2018, fra i compiti dell'Autorità indicava, *inter alia*, quelli di "p*rescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti ai sensi dell'articolo 143*" nonché di "*vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali*". Per completezza, si precisa che l'art. 143 del Codice Privacy, nella formulazione precedente all'intervento del d.lgs. n. 101/2018 e limitatamente a quanto qui di interesse, prevedeva che "*Il Garante [Privacy], anche prima della definizione del procedimento: […] b) prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti; c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o comunque delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati; (d) può vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti o a categorie di soggetti che si pone in contrasto con rilevanti interessi della collettività*".

costanze del caso concreto; nonché (*vii*) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Da un punto di vista generale, una delle principali novità del GDPR risiede nel fatto che, a differenza del regime previgente e coerentemente con l'esistenza di ben precisi obblighi imposti dal GDPR direttamente al responsabile del trattamento[31], i poteri correttivi sono esercitabili non soltanto nei confronti del titolare del trattamento, ma anche direttamente nei confronti del responsabile del trattamento.

In relazione ai singoli poteri correttivi, è utile richiamare l'attenzione in particolare su due poteri introdotti dal GDPR, ossia l'avvertimento e l'ammonimento.

L'avvertimento tecnicamente non pare essere una vera e propria misura correttiva, poiché il presupposto affinché l'Autorità possa rivolgere un avvertimento a un titolare o a un responsabile del trattamento risiede nel fatto che una violazione del GDPR si possa "*verosimilmente*" verificare e, dunque, non si sia ancora verificata. In proposito, si è osservato che rivolgere un avvertimento al titolare o al responsabile del trattamento impedirebbe l'applicazione di una sanzione amministrativa pecuniaria *ex* art. 83 del GDPR in quanto l'irrogazione di tale sanzione "*è ammessa solo in presenza di un'avvenuta violazione delle disposizioni regolamentari*"[32]. Ovviamente, nel caso in cui il titolare o il responsabile del trattamento non dessero seguito all'avvertimento ricevuto dall'Autorità rendendo, quindi, la violazione delle disposizioni del GDPR non più solo verosimile, ma effettiva, ciò aprirebbe la strada per l'adozione, da parte dell'Autorità, di ulteriori misure, ivi compresa l'irrogazione di una sanzione amministrativa pecuniaria *ex* art 83 del GDPR, ove ne ricorrano i presupposti.

Per quanto riguarda l'ammonimento, il considerando n. 148 del GDPR prevede che "[i]*n caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria*". In assenza di una definizione di cosa costituisca una "violazione minore", il WP29[33] ha precisato che la qualificazione in tal senso della violazione di una o più disposizioni del GDPR elencate dall'art. 83(4) o (5) del GDPR dipende dalla valutazione delle circostanze del caso concreto, perché l'applicazione dei criteri di valutazione di cui all'art. 83(2) del GDPR[34] può portare l'autorità di controllo "*a ritenere che nelle circostanze concrete del caso la violazione, ad esempio, non crei un rischio significativo per i diritti degli interessati in questione e non incida sull'essenza dell'obbligo in questione*". In caso di violazione minore, dunque, l'autorità di controllo

31 Quali, ad esempio, l'obbligo della tenuta del registro delle attività di trattamento ex art. 30 del GDPR, l'adozione di misure tecniche e organizzative adeguate *ex* art. 32 del GDPR nonché la nomina del *data protection officer*, qualora ricorrano i presupposti di cui all'art. 37 del GDPR oppure ciò sia imposto dal diritto nazionale.

32 Cfr. G. M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy*, 2018, Milano, p. 491 e ss.

33 Cfr. le *Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE)* n. 2016/679 del 3 ottobre 2017, p. 9 (consultabili al seguente link https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237).

34 Sui quali, cfr. il paragrafo 4.2 *infra*.

avrà la possibilità (e non l'obbligo) di sostituire la sanzione pecuniaria con un ammonimento[35].

4.2 Le sanzioni per le violazioni della normativa in materia di protezione dei dati personali nel GDPR e nel Codice Privacy

Come precisato dal Garante Privacy nella Relazione Annuale 2018[36], "*le sanzioni amministrative pecuniarie rappresentano un elemento centrale nel nuovo regime introdotto dal* [GDPR] *e un potente strumento con il quale le autorità di controllo possono attuare la normativa unitamente alle altre misure correttive*".

Da un punto di vista generale, è necessario che "*le sanzioni amministrative pecuniarie […] siano in ogni singolo caso effettive, proporzionate e dissuasive*"[37]. In realtà, tale principio ha portata generale e trova applicazione per tutte le misure correttive poiché, come chiarito dal WP29, "[l]*a valutazione di quanto sia effettivo, proporzionato e dissuasivo in ciascun caso dovrà anche riflettere l'obiettivo perseguito dalla misura correttiva prescelta, che è quello di ripristinare la conformità alle norme oppure di punire un comportamento illecito (o entrambi)*"[38].

In proposito, l'art. 83(2) del GDPR individua una serie di criteri che l'autorità di controllo deve tenere in considerazione "*in ogni singolo caso*"[39] al fine di "*valutare sia l'opportunità di irrogare una sanzione amministrativa*" sia "*l'importo della sanzione*"[40] quali, ad esempio, (*i*) la natura, la gravità e la durata della violazione; (*ii*) il suo carattere doloso o colposo; (*iii*) le misure adottate dal titolare o dal responsabile del trattamento per attenuare il danno subito dagli interessati; (*iv*) le categorie dei dati personali interessate dalla violazione; (*v*) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione; nonché (*vi*) la maniera in cui l'autorità di controllo è venuta a conoscenza della violazione, in particolare se e in che misura il titolare o il responsabile del trattamento abbia notificato la violazione.

Per quanto riguarda le sanzioni amministrative pecuniarie, oltre alle condotte sanzionate ai sensi dell'art. 83(4)-(6) del GDPR, l'art. 166 del Codice Privacy così come novellato dal d.lgs. n. 101/2018 individua ulteriori illeciti

35 Cfr. le *Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE)* n. 2016/679 del 3 ottobre 2017, (cit.), p. 9.

36 Cfr. Relazione Annuale 2018 del Garante Privacy, p. 182.

37 Cfr. art. 83(1) del GDPR.

38 Cfr. le *Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE)* n. 2016/679 del 3 ottobre 2017, (cit.), p. 5.

39 Cfr. l'art. 83(2) del GDPR il quale prevede che "[l]*e sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 28, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure*".

40 Cfr. le *Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE)* n. 2016/679 del 3 ottobre 2017, (cit.), p. 9. Cfr. altresì p. 7 dove il WP 29 chiarisce che "[l]*e sanzioni pecuniarie rappresentano un importante strumento che le autorità di controllo dovrebbero utilizzare nelle opportune circostanze. Le autorità di controllo sono incoraggiate a ricorrere alle misure correttive con un approccio ponderato ed equilibrato, al fine di reagire in maniera effettiva, dissuasiva e proporzionata alla violazione. Il punto non è qualificare le sanzioni pecuniarie come misure di ultima istanza, né evitare di irrogarle, bensì utilizzarle in un modo che non ne riduca l'efficacia come strumento*".

amministrativi in corrispondenza della violazione delle disposizioni contenute nel Codice Privacy[41], prevedendo l'applicabilità:

- della sanzione amministrativa fino a € 10 milioni oppure, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente (se maggiore)[42] per la violazione, ad esempio: (*i*) dell'obbligo, in capo al titolare del trattamento *ex* art. 2-*quinquies* del Codice Privacy, di redigere "*con un linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile al minore*" le informazioni e comunicazioni relative alle attività di trattamento che lo riguardino; (*ii*) degli obblighi informativi *ex* art. 123, comma 4, del Codice Privacy posti in capo al fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico con riguardo al trattamento dei dati relativi al traffico riguardanti contraenti e utenti; e (*iii*) degli obblighi di sicurezza imposti a tali fornitori *ex* art. 132-*ter* del Codice Privacy;
- della sanzione amministrativa fino a € 20 milioni oppure, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente (se maggiore)[43] per la violazione, ad esempio: (*i*) delle disposizioni in materia di trattamento dei dati relativi a condanne penali e reati *ex* art. 2-*octies* del Codice Privacy; (*ii*) delle disposizioni in materia di trattamento di dati sanitari *ex* artt. 75 e ss. del Codice Privacy; e (*iii*) delle disposizioni in materia di comunicazioni indesiderate *ex* art. 130 del Codice Privacy.

Per quanto riguarda le sanzioni penali, il d.lgs. n. 101/2018 ha profondamente rimodulato il catalogo degli illeciti, depenalizzando la maggior parte dei reati presenti nel Codice Privacy, poiché "*quasi tutte le vigenti disposizioni penali (gli art. 167 ss del codice privacy) reprimono comportamenti che, in attuazione dell'art. 83 del Regolamento, dovranno essere puniti con sanzioni amministrative*" e, dunque, il d.lgs. n. 101/2018 ha operato una "*mirata e limitata depenalizzazione, in modo da scongiurare i rischi di violazione del principio del* ne bis in idem *tra sanzioni penali e sanzioni amministrative affermato nella giurisprudenza delle Corti europee*"[44].

Oltre a una significativa revisione del reato di trattamento illecito di dati personali *ex* art. 167 del Codice Privacy (che, nell'ipotesi ordinaria di cui al comma 1, non richiama più la violazione delle disposizioni in materia di consenso), vengono introdotte alcune nuove fattispecie, quali, ad esempio il reato di comunicazione e diffusione illecita di dati personali oggetto di trattamento su

41 Cfr. l'art. 84(1) del GDPR il quale prevede che "[g]*li Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive*".

42 Cfr. art. 83(4) del GDPR.

43 Cfr. art. 83(5) del GDPR.

44 Cfr. la relazione illustrativa al d.lgs. n. 101/2018, p. 32 (consultabile al seguente link http://documenti.camera.it/apps/nuovosito/attigoverno/Schedalavori/getTesto.ashx?file=0022_F001.pdf&leg=XVIII).

larga scala[45] e l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala[46].

Inoltre, al reato di falsità nelle dichiarazioni al Garante Privacy (già presente in precedenza nel Codice Privacy), si aggiunge l'illecito che sanziona penalmente la condotta di chi "*cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante* [Privacy] *o degli accertamenti dallo stesso svolti*" (art. 168, comma 2, Codice Privacy).

45 Cfr. l'art. 167-*bis* del Codice Privacy il quale sanziona penalmente la condotta di "c*hiunque comunica o diffonde al fine di trarne profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contente dati personali oggetto di trattamento su larga scala in violazione degli articoli 2-ter, 2-sexies e 2-octies" oppure "comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contente dati personali oggetto di trattamento su larga scala* […] *ove il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione*".

46 Cfr. l'art. 167-*ter* del Codice Privacy il quale sanziona penalmente la condotta di "*chiunque, al fine di trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala*".

CAPITOLO 2 di Tiziana Boneschi, Giacomo Gori, Marta Margiocco e Alessia Placchi

Trasferimento di dati personali verso Paesi Terzi: come scegliere lo strumento più adeguato

sommario: 1. Il trasferimento di dati personali verso Paesi terzi – 1.1 Decisioni di adeguatezza – 1.2 Clausole contrattuali standard – 2. Norme vincolanti d'impresa, codici di condotta e certificazioni – 2.1 Scopo – 2.2 Requisiti – 2.3 Procedure per l'approvazione – 3. Codici di condotta e certificazioni – 4. Deroghe al diverso di trasferimento extra-UE ex articolo 49 – 4.1 Deroghe ex art. 49 – 4.2 Consenso – 4.3 Esecuzione contrattuale e contratto concluso a favore dell'interessato – 4.4 Interesse pubblico rilevante – 4.5 Tutela giudiziaria – 4.6 Interesse vitale dell'interessato – 4.7 Registro pubblico – 4.8 Interesse legittimo cogente

1. Il trasferimento di dati personali verso Paesi terzi

I flussi di dati personali verso e da Paesi al di fuori dell'Unione Europea, aumentati in modo esponenziale per consistenza e rapidità negli ultimi decenni e riconosciuti come necessari per l'espansione del commercio internazionale e della cooperazione internazionale, hanno posto nuove sfide riguardanti la protezione dei dati personali.

Se infatti la circolazione dei dati personali all'interno dell'Unione Europea è libera e anzi enunciata dallo stesso Regolamento (UE) 2016/679 ("Regolamento"), che ha garantito una tutela uniforme del diritto alla protezione dei dati personali in tutto il territorio europeo, il trasferimento di dati personali verso Paesi al di fuori dell'Unione Europea e verso organizzazioni internazionali è soggetto a limiti molto stringenti.

Al trasferimento dei dati personali verso Paesi extra UE è dedicato il capo V del Regolamento, e pertanto gli articoli da 44 a 50.

L'obiettivo della disciplina, enunciato all'articolo 44, è quello di garantire che il livello di protezione delle persone fisiche garantito dal Regolamento non sia pregiudicato per effetto del trasferimento dei dati in un Paese terzo, e quindi quello di evitare che i titolari del trattamento soggetti al Regolamento ne aggirino gli obblighi trasferendo i dati in territorio extra UE.

Gli articoli 45 e seguenti descrivono i casi nei quali è ammesso il trasferimento verso un Paese terzo, compresi i trasferimenti successivi di dati personali da un paese terzo verso un altro paese terzo, in modo cioè che i dati che escono dall'Unione Europea siano tutelati in caso di successivo e ulteriore trasferimento.

Il trasferimento di dati personali è in primo luogo consentito qualora la Commissione europea abbia stabilito, mediante una c.d. decisione di adeguatezza, che il paese terzo a cui sono destinati i dati garantisce un livello di protezione adeguato.

In mancanza di una decisione di adeguatezza il titolare e il responsabile del regolamento possono adottare le c.d. "garanzie adeguate" di cui all'articolo 46 del Regolamento, che consentono il trasferimento verso Paesi terzi che non siano stati sottoposti a decisione di adeguatezza, senza che il trasferimento necessiti di autorizzazione specifica da parte di un'autorità di controllo. Si tratta di strumenti tipici che assicurano all'interessato diritti effettivi e azionabili in relazione al trattamento dei suoi dati personali, garantendone un'adeguata protezione.

In assenza di decisione di adeguatezza e di garanzie adeguate è ammesso il trasferimento solo al verificarsi di determinate condizioni, descritte all'articolo 49, che derogano agli articoli 45 e 46 del Regolamento.

L'articolo 13 del Regolamento ha introdotto nel contenuto dell'informativa uno specifico riferimento al trasferimento in Paesi terzi. Qualora intenda trasferire i dati personali, il titolare del trattamento deve cioè, prima del trasferimento, informarne l'interessato,

precisando su quale strumento tale trasferimento si baserà. Il trasferimento rileva anche con riferimento al principio di "responsabilizzazione": tra le informazioni che titolare e responsabile devono inserire nel registro delle attività di trattamento condotte sotto la loro responsabilità ai sensi dell'articolo 30 del Regolamento rientra anche l'eventuale trasferimento in Paesi terzi.

1.1 Decisioni di adeguatezza

Attraverso la c.d. decisione di adeguatezza la Commissione europea valuta che un Paese terzo garantisce un livello di protezione adeguato e che è pertanto ammesso il trasferimento di dati in tale Paese, senza ulteriori autorizzazioni.

L'adeguatezza del livello di protezione assicurato è valutato sulla base di una serie di elementi, descritti all'articolo 45, non solo di natura giuridica ma anche relativi alla sfera politica del Paese, la cui presenza è ritenuta indice di un adeguato livello di protezione.

A rilevare non è ovviamente l'identità delle norme adottate dal Paese terzo a quelle europee ma piuttosto la sostanziale equivalenza delle stesse: la Commissione valuta cioè sostanzialmente se le misure adottate nel Paese terzo sono

basate sui medesimi principi UE di protezione dei dati e se dimostrano un'efficacia verificabile.

La decisione di adeguatezza è soggetta a un riesame periodico basato sugli sviluppi rilevanti nel Paese terzo che potrebbero avere conseguenze dirette sul livello di protezione dei dati personali e che può concludersi con una modifica ma anche con la sospensione o la revoca della decisione.

Le decisioni di adeguatezza ad oggi vigenti, adottate principalmente ai sensi della Direttiva 95/46/CE, riguardano un numero limitato di Paesi. Tra queste rientra la decisione con la quale è stato approvato il *Privacy Shields*, che regolamenta il trasferimento di dati tra UE e USA.

1.2 Clausole contrattuali standard

Le clausole contrattuali standard adottate dalla Commissione Europea, previste all'articolo 46, paragrafo 2, lettera c), del Regolamento, costituiscono uno degli strumenti più usati per il trasferimento di dati personali.

Si tratta di clausole destinate ad essere incorporate, nella loro formulazione letterale, nei contratti che regolano il trasferimento di dati e quindi a essere sottoscritte dalle parti, individuate come "esportatore" e "importatore" di dati.

Una volta che tali clausole siano integrate nel contratto tra le parti è ammesso il trasferimento di dati personali verso soggetti (titolari o responsabili) collocati in Paesi terzi che non hanno ottenuto la decisione di adeguatezza della Commissione e che quindi non assicurerebbero un adeguato livello di tutela.

Pur non essendo consentita la modifica di tali clausole, si ritiene possibile che le parti aggiungano alle clausole standard clausole e garanzie ulteriori a condizione che queste ultime non siano in contrasto diretto o indiretto con le clausole standard.

Con riferimento ai trasferimenti da titolare stabilito nell'Unione Europea a responsabile stabilito in Paese terzo si applicano le clausole contrattuali standard di cui alla decisione n. 2010/87/CE, oggetto di autorizzazione del Garante con provvedimento del 27 maggio 2010 (doc. web 1728496).

Con provvedimento del 15 novembre 2012 (doc. web 2191156), il Garante ha previsto la possibilità che il titolare del trattamento stabilito in Italia ("esportatore"), che abbia designato un responsabile con sede nell'Unione Europea che intenda affidare, a sua volta, il trattamento dei dati ad un altro responsabile stabilito in un Paese terzo che non assicuri un livello di protezione adeguato ("importatore"), conferisca un apposito mandato, ai sensi dell'art. 1704 c.c., al responsabile del trattamento stabilito nell'Unione Europea, per la sottoscrizione delle clausole contrattuali tipo di cui alla decisione della Commissione 2010/87/CE.

Pertanto, nel caso in cui il trasferimento sia dovuto all'affidamento del trattamento dei dati, da parte di un responsabile designato dal titolare e stabilito nell'Unione europea, ad un sub responsabile avente sede in un Paese terzo che

non assicuri un livello di protezione adeguato, il responsabile stabilito nell'Unione europea potrà, sulla base dell'esplicito mandato ricevuto dal titolare, sottoscrivere le clausole contrattuali tipo con il sub responsabile.

Con riferimento invece ai trasferimenti da titolare a titolare si applicano le clausole contrattuali di cui alla decisione della Commissione n. 2001/497/CE, emendate con decisione n. 2004/915/CE, oggetto di autorizzazione del Garante rispettivamente con provvedimento del 16 novembre 2001 (doc. web 42156) e con provvedimento del 9 giugno 2005 (doc. web. 1151949).

Le clausole contrattuali standard mirano ovviamente alla massima tutela dell'interessato e impongono una serie di obblighi all'esportatore e soprattutto all'importatore di dati, che deve sostanzialmente garantire il rispetto dei principi di cui alla normativa europea in materia di protezione dei dati personali. I dettagli relativi allo specifico trattamento di dati vengono rinviati all'appendice, nella quale le parti di volta in volta specificano le informazioni richieste.

Quelle adottate dalla Commissione Europea non sono le uniche clausole contrattuali tipo previste dal Regolamento. Secondo l'articolo 46, paragrafo 2, lettera d), anche le singole autorità di controllo possono adottare clausole tipo di protezione dei dati, che devono essere sottoposte all'approvazione della Commissione Europea e al parere del Comitato europeo per la protezione dei dati.

Importatore ed esportatore di dati possono infine elaborare proprie clausole contrattuali relative al trasferimento di dati. In questo caso però, secondo quanto previsto all'articolo 46, paragrafo 3, lettera a) del Regolamento, prima di procedere al trasferimento è necessaria l'autorizzazione della competente autorità di controllo nazionale, preceduta dal parere del Comitato europeo per la protezione dei dati.

2. Norme vincolanti d'impresa, codici di condotta e certificazioni

2.1 Scopo

L'art 46 del Regolamento prevede che, in mancanza di una decisione di adeguatezza adottata ai sensi dell'art. 45, il titolare del trattamento oppure il responsabile del trattamento siano legittimati a trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Tra le garanzie adeguate che non necessitano di autorizzazioni specifiche, in quanto soggette ad una approvazione preventiva, rientrano le norme vincolati di impresa (c.d. "*Binding Corporate Rules*" o "BCR"), disciplinate dall'art. 47 del Regolamento.

Si tratta di uno strumento particolarmente utile in caso di trasferimento di dati personali dal territorio dello Stato verso paesi terzi (extra-UE) tra società

facenti parti dello stesso gruppo d'impresa. Grazie infatti alla preventiva autorizzazione delle clausole (*rules*) che fissano i principi vincolanti (*binding*) tutte le società appartenenti a uno stesso gruppo (*corporate*) possono trasferire i dati nei diversi Paesi ove hanno sede le varie filiali senza ulteriori adempimenti (come le clausole contrattuali tipo, il rilascio di specifiche autorizzazioni, ecc.).

Si tratta, in sostanza, di regole di comportamento alle quali le società di un gruppo si obbligano ad attenersi. Tra l'altro, alla luce del *considerando* n. 110 del Regolamento, lo strumento è adottabile sia da imprese multinazionali "verticali", quindi con un'impresa che svolge la funzione di capogruppo, che "orizzontali", senza una capogruppo. In questo secondo caso, le clausole si avvicinano ai codici di condotta ma si differenziano da questi ultimi in quanto per poter usufruire delle BCR ci deve essere un'attività economica comune e non soltanto la semplice appartenenza allo stesso settore.

Inoltre, a differenza delle clausole tipo, non è necessario sottoscriverle per ogni trasferimento, e consentono il trasferimento anche nei paesi terzi che non hanno ottenuto una decisione di adeguatezza.

Ai sensi dell'art. 47, l'autorità di controllo competente (in Italia è il Garante per la protezione dei dati personali) approva le norme vincolanti di impresa in conformità al meccanismo di coerenza previsto dall'art. 63: è quindi previsto l'intervento, in ogni caso, del Comitato europeo per la protezione dei dati.

2.2 Requisiti

Affinché le norme siano approvate è necessario che consentano un livello di protezione adeguata nei flussi di dati infragruppo. A tal fine le norme devo essere "*giuridicamente vincolanti*", attraverso l'imposizione ai membri del gruppo di sanzioni in caso di infrazione, e "*si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti*". È inoltre fondamentale che siano previsti, a favore dei soggetti interessati, tutti i diritti azionabili in relazione al trattamento dei loro dati personali.

Per quanto concerne il contenuto delle norme, il n. 2 dell'art. 47 offre un dettaglio analitico delle disposizioni minime che dovranno prevedere:

- la struttura e le coordinate di contatto del gruppo imprenditoriale e di ciascuno dei suoi membri;
- i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;
- la natura giuridicamente vincolante, a livello sia interno che esterno;
- l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla

protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa;

- i diritti dell'interessato in relazione al trattamento ed i mezzi per esercitarli;
- l'assunzione di responsabilità da parte del titolare o del responsabile del trattamento per qualunque violazione delle norme vincolanti d'impresa commessa da un membro interessato non stabilito nell'Unione eurpea, con l'espressa previsione che il titolare o il responsabile del trattamento possono essere esonerati in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;
- le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa;
- i compiti di qualunque *Data Protection Officer* o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale, del controllo della formazione e della gestione dei reclami;
- le procedure di reclamo;
- i meccanismi volti a garantire la verifica della conformità alle norme vincolanti d'impresa, compresi la protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti degli interessati;
- i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo;
- il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità delle norme e la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure adottate;
- i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa;
- l'appropriata formazione in materia di protezione dei dati al personale che ha accesso ai dati personali.

2.3 Procedure per l'approvazione

La procedura di approvazione prevede che le norme vincolanti di impresa siano autorizzate dall'autorità di controllo competente, ai sensi dell'art. 58.3, lett. j, del Regolamento oppure dall'autorità capofila, ai sensi dell'art. 57.1, lett. s.

In base al parere WP 263 dell'EDPB (*European Data Protection Board* che ha sostuito l'*Article 29 Data Protection Working Party*) il gruppo di imprese interessato all'approvazione propone la bozza di BCR all'autorità che ritiene competente sulla base dei seguenti criteri:

- l'ubicazione della sede europea del gruppo;
- l'ubicazione dell'azienda all'interno del gruppo con responsabilità delegate sulla protezione dei dati;
- l'ubicazione della società che si trova nella posizione migliore (in termini di funzione di gestione, oneri amministrativi, ecc.) per gestire l'applicazione e far rispettare le norme aziendali vincolanti nel gruppo;
- il luogo in cui vengono prese la maggior parte delle decisioni in termini di finalità e mezzi del trattamento (ovvero trasferimento);
- lo stato membro all'interno dell'UE da cui avverranno la maggior parte o tutti i trasferimenti al di fuori del SEE.

Il richiedente è inoltre tenuto a fornire tutte le informazioni rilevanti a giustificare la scelta tra cui la natura e la struttura generale delle attività di trattamento nell'UE, con particolare attenzione al luogo o ai luoghi in cui vengono prese le decisioni, all'ubicazione e alla natura delle affiliate nell'UE, al numero di dipendenti o persone interessate, ai mezzi e alle finalità del trattamento, ai luoghi da cui avvengono i trasferimenti verso paesi terzi luogo e paesi terzi in cui tali dati sono trasferiti.

L'autorità prescelta invierà l'istanza ricevuta alle altre autorità astrattamene competenti affinché queste possano esprimere il proprio parere e si giunga all'individuazione della Lead Authority che poi agirà in rappresentanza di tutte le autorità di controllo coinvolte.

L'attività delle autorità di controllo proseguirà sino alla formulazione della c.d. "bozza consolidata" che verrà trasmessa all'istante affinché siano apportate eventuali modifiche. All'esito delle stesse si giungerà alla c.d. "bozza finale" che sarà sottoposta al parere dell'EDPB.

Durante la procedura è previsto anche l'intervento della Commissione, *ex* art. 47.3 del Regolamento, la quale può indicare "*il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa*."

Al termine del procedimento, la cui durata è di circa 18 mesi, l'autorità di controllo capofila comunica l'approvazione delle norme.

3. Codici di condotta e certificazioni

Introdotte con il Regolamento, i codici di condotta (art. 40 del Regolamento) e le certificazioni (art. 42 del Regolamento) rappresentano un modo alternativo per effettuare il legittimo trasferimento dei dati all'estero e sono

espressione dell'approccio basato sul rischio come corollario del principio di responsabilizzazione del titolare (o del responsabile).

In sostanza, anche senza un'autorizzazione da parte dell'autorità di controllo nazionale, il trasferimento sarà possibile grazie agli impegni sottoscritti attraverso l'adesione a un codice di condotta o ad un meccanismo di certificazione (ove questi, naturalmente, disciplinino il trasferimento). Tra l'altro, ai sensi dell'art. 83.2 del Regolamento, l'adesione a codici di condotta o certificazioni costituisce un parametro che l'autorità di controllo valuta nell'applicazione delle sanzioni.

Detti strumenti costituiranno adeguate garanzie per il trasferimento a patto che siano accompagnati da un impegno "vincolante ed esecutivo", da intendersi come vincolo giuridico, da parte del titolare o del responsabile stabiliti nel paese terzo, ad applicare le necessarie garanzie al fine di ottemperare ai principi di protezione dei dati ed ai diritti degli interessati.

Il vincolo richiamato deve essere duplice, prevedendo sia delle sanzioni, in caso infrazioni, che meccanismi volti a garantire il pieno esercizio dei diritti da parte degli interessati.

Ai sensi dell'art. 40.3 del Regolamento, ai codici di condotta potranno aderire anche i titolari o i responsabili per i quali non sarebbe applicabile la normativa europea, sempre che sottoscrivano un impegno che li rendano giuridicamente vincolati al rispetto del GDPR.

4. Deroghe al diverso di trasferimento extra-UE ex articolo 49

4.1 Deroghe ex art. 49

Come visto nei paragrafi precedenti, se i flussi di dati all'interno dell'Unione Europea sono **sostanzialmente liberi**, quelli verso Paesi terzi sono **generalmente vietati** salvo che non intervengano particolari garanzie.

L'evoluzione dei mercati in forme sempre più "4.0" e lo sviluppo delle interconnessioni digitali a livello globale ha reso il fenomeno del *data transfer* una realtà concreta e spesso inevitabile, facendo emergere la necessità di garantire **adeguata protezione ai dati personali** trasferiti al di fuori all'Unione Europea verso Paesi terzi. Qualora non vi siano decisioni di adeguatezza e/o garanzie adeguate offerte dal Paese destinatario, trasferire i dati personali extra-UE è possibile in via assolutamente residuale (c.d. *layered approach* adottato sia dall'EDPB[47], che dal WP29[48]) e solo a determinate condizioni nell'ambito delle c.d. "deroghe" di cui all'art. 49 del GDPR.

47 Il Comitato europeo per la Protezione dei Dati (*European Data Protection Board*) è un organismo europeo indipendente il cui scopo è garantire un'applicazione coerente del Regolamento generale sulla Protezione dei Dati. Il 25 maggio 2018, l'EDPB ha elaborato le *Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del Regolamento 2016/679* (v. *infra*)

48 Article 29 Working Party, Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, November 25,2005 (WP114).

Prima di passare all'analisi di tali specifiche condizioni, è opportuno osservare come il termine "deroga" includa di per sé una connotazione di eccezionalità rispetto al principio dell'adeguatezza e alle altre garanzie e che, pertanto, come confermato dallo stesso Garante[49], l'ambito di operatività delle suddette deroghe debba essere soggetto ad un'interpretazione restrittiva.

E proprio ai fini di una corretta interpretazione, l'EDPB (*European Data Protection Board*) ha provveduto a elaborare delle linee guida (*Linee guida 2/2018 sulle deroghe di cui all'articolo 49 del Regolamento 2016/679* del 25 maggio 2018) il cui tema è quello dei presupposti legali per effettuare un trasferimento legittimo, occasionale e necessario di dati al di fuori del territorio dell'Unione Europea. Le Linee Guida dell'EDPB e muovono dalla necessaria premessa che il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, oltre che rientrare in una delle condizioni di adeguatezza o di deroga previste dal GDPR, debba anche essere conforme alle disposizioni generali in materia di protezione dei dati e, in particolare, deve avvenire in modo tale da assicurare il rispetto dei diritti fondamentali delle persone fisiche[50].

Venendo ora all'analisi letterale del testo dell'art. 49 GDPR, tali deroghe possono brevemente essere elencate nelle seguenti voci: (*a*) Consenso; (*b*) Esecuzione contrattuale; (*c*) Contratto a favore dell'interessato; (*d*) Interesse pubblico; (*e*) Tutela giudiziaria; (*f*) Interesse vitale dell'interessato; (*g*) Registro pubblico; e (*h*) Interesse legittimo cogente del titolare del trattamento.

4.2 Consenso

Affinché il consenso sia considerato una valida base giuridica, esso deve presentarsi come una manifestazione libera, specifica, informata e inequivocabile della volontà dell'interessato[51].

Rispetto ai requisiti generali sopra menzionati, l'articolo 49 richiede poi che il consenso sia **esplicito** e **granulare** con riferimento a ipotesi in cui il trasferimento dei dati verso Paesi terzi possa determinare particolari rischi per la protezione dell'individuo e sia, quindi, necessario un elevato livello di controllo individuale sulle operazioni di trattamento. Non sempre, tuttavia, è possibile ottenere il previo consenso dell'interessato per un futuro trasferimento non – o non ancora – previsto al momento della raccolta dei dati. In questo caso, l'impatto sull'interessato non può essere preventivamente valutato e perché il trasferimento sia valido sulla base di tale deroga il titolare (e *data exporter*) dovrà assicurarsi di ottenere un consenso specifico prima di procedere al trasferimento e nel momento in cui questo è previsto, anche se successivo alla raccolta dei dati.

49 Provvedimento n. 2036021 "Trasferimento di Dati all'estero".

50 Article 29 Working Party, WP 114, p.9, and Article 29 Working Party Working Document on surveillance of electronic communications for intelligence and national security purposes (WP228), p.39.

51 La base giuridica del consenso valida per i trasferimenti extra-UE deve essere interpretata anche alla luce degli articoli 4 e 7 GDPR, i *considerando* 32, 33, 42 e 43 e alla luce delle linee guida del WP29 sul consenso (*Article 29 Working Party Guidelines on Consent under Regulation 2016/679*).

Il consenso deve, altresì, essere **informato** nella specifica accezione che gli interessati devono essere resi edotti anche dei **rischi specifici**[52] derivanti dal fatto che i loro dati saranno trasferiti in un Paese che non fornisce una protezione adeguata e che non vengono attuate adeguate garanzie volte a garantire la protezione dei dati.

La fornitura di queste informazioni è essenziale per consentire all'interessato di dare il proprio consenso con piena conoscenza. Ma occorre anche considerare che se il consenso può sempre essere revocato in qualsiasi momento, questa base giuridica non sempre potrebbe rappresentare la soluzione più idonea a lungo termine per i trasferimenti verso Paesi terzi. Altrettanto problematica è la validità del consenso fornito dai dipendenti nell'ambito di rapporti di lavoro, poiché - come affermato anche dal WP29[53] - in considerazione del peculiare **rapporto di squilibrio tra il datore di lavoro e i dipendenti**, i lavoratori non sono quasi mai nella posizione di poter manifestare (rifiutare o revocare) liberamente la loro volontà con la conseguenza che difficilmente il consenso del dipendente può essere considerato una **libera** – e dunque valida – **scelta**.

4.3 Esecuzione contrattuale e contratto concluso a favore dell'interessato

Il Regolamento consente il trasferimento di dati verso Paesi terzi nei casi in cui tra titolare e interessato sia in essere uno specifico contratto o ne sia contemplata la conclusione (implementazione di misure precontrattuali). In questo caso, e in assenza di decisioni di adeguatezza e di adeguate garanzie, il trasferimento è possibile solo qualora sia "**occasionale** e **necessario** all'esecuzione di un contratto".

Il "*test di necessità*"[54] limita il numero di casi in cui è possibile ricorrere all'articolo 49, paragrafo 1, lettera b) in quanto è necessaria una stretta e sostanziale connessione tra il trasferimento dei dati e le finalità del contratto. Inoltre, se il trasferimento è necessario dipenderà anche dalla natura dei beni o dei servizi forniti in base al contratto piuttosto che in base alle modalità in cui sono state organizzate le operazioni di fornitura da parte del titolare. E, dunque, il trasferimento non potrà dirsi necessario qualora un gruppo aziendale abbia deciso di centralizzare, a fini commerciali, tutte le sue funzioni di pagamento e di gestione delle risorse umane in un paese terzo, poiché non esiste un legame diretto e oggettivo tra l'esecuzione del contratto e il trasferimento. È invece necessario nel caso in cui un'agenzia di viaggio dovrà trasferire i dati personali dei clienti alle strutture alberghiere o ai propri partner siti nel Paese terzo al fine di consentire l'esecuzione del contratto di viaggio.

52 Ad esempio, l'elenco delle categorie di destinatari dei dati, tutti i paesi verso i quali i dati personali vengono trasferiti e il fatto che il paese terzo di destinazione non prevede un livello adeguato di protezione dei dati o che manchi un'autorità di controllo.

53 WP29 Opinion 2/2017, WP249.

54 V. anche il concetto di "necessità contrattuale" in *Linee guida 2/2019 sul trattamento dei dati personali ai sensi dell'Articolo 6, paragrafo 1, lettera b), GDPR nell'ambito della fornitura di servizi online servizi agli interessati* del 9 aprile 2019.

Al requisito della necessità, si aggiunge quello dell'**occasionalità** del trasferimento (Considerando 111 GDPR). Secondo l'EDPB, il termine "occasionale" indica che tali trasferimenti possono avvenire più di una volta, ma non regolarmente o in maniera sistematica, così come non nell'ambito di una relazione stabile tra interessato e titolare (*data exporter*) bensì in circostanze casuali ed entro intervalli di tempo limitati. Ad esempio, non potrà dirsi occasionale il trattamento svolto dal soggetto situato nel Paese terzo a cui viene concesso l'accesso diretto a una banca dati su base generale.

4.4 Interesse pubblico rilevante

Tale deroga prevede che il trasferimento abbia luogo solo se necessario o richiesto per motivi di interesse pubblico rilevante con ciò intendendosi[55] solo gli **interessi pubblici riconosciuti** dal diritto dell'Unione o dal diritto dello Stato membro al quale il titolare del trattamento è soggetto. Per l'applicazione di questa deroga, non è sufficiente che il trasferimento dei dati sia richiesto da una pubblica autorità di un paese terzo, quanto piuttosto[56] si dovrà poter dedurre dal diritto dell'UE o dal diritto dello Stato membro al quale il titolare è soggetto che tale trasferimento sia giustificato da importanti finalità di interesse pubblico, in uno spirito di reciproca cooperazione internazionale.

Dalla lettura dei *considerando* 111 e 112, si deduce inoltre che questa deroga non sia limita ai trasferimenti di dati "*occasionali*". Ciò non significa tuttavia che i trasferimenti possano avvenire su vasta scala e in modo sistematico, bensì devono sempre essere limitati a situazioni specifiche.

4.5 Tutela giudiziaria

La tutela in sede giudiziaria di cui all'articolo 49, paragrafo 1, lettera e), ammette il trasferimento occasionale di dati in Paesi extra-UE se tale trasferimento sia "*necessario per l'accertamento, l'esercizio o la difesa di diritti legali*" e "*indipendentemente dal fatto che si tratti di un procedimento giudiziario o di un procedimento amministrativo o extragiudiziale, comprese le procedure dinanzi agli organismi di regolamentazione*" (Considerando 111). Questa definizione, piuttosto ampia, può dunque trovare applicazione, ad esempio, nel caso di un'indagine penale o amministrativa in un Paese terzo, di avvio di contenziosi o di procedure formali di accertamento preprocessuale, ma anche nel caso di approvazione di una fusione all'estero.

Anche questa deroga impone il rispetto dei requisiti di **necessità**, intesa come una stretta e sostanziale connessione tra i dati trattati e la specifica azione giudiziaria o amministrativa da intraprendere e di **occasionalità** (non ripetitività e non sistematicità) del trasferimento.

55 Ai sensi dell'articolo 49, paragrafo 4, GDPR.

56 Article 29 Working Party Opinion 10/2006 on the processing

4.6 Interesse vitale dell'interessato

La deroga di cui all'articolo 49, paragrafo 1, lettera f), si applica ovviamente quando i dati sono trasferiti in caso di emergenza medica e quando si ritiene che tale trasferimento sia direttamente necessario per fornire cure mediche necessarie all'interessato. Tale deroga trova applicazione esclusivamente nelle ipotesi in cui l'interessato non abbia la possibilità di prendere una decisione valida in merito alla propria salute, vale a dire quando l'interessato sia incapace – fisicamente, mentalmente o legalmente (ad esempio nell'ipotesi di minorenne) - di fornire il proprio consenso al trasferimento dei suoi dati personali.

4.7 Registro pubblico

Il registro in questione deve, secondo il diritto dell'Unione o degli Stati membri, essere destinato a fornire informazioni al pubblico e, pertanto, deve essere **liberamente consultabile**, alternativamente, (*i*) dal pubblico in generale; (*ii*) dai destinatari del trasferimento; o (*iii*) su richiesta di qualsiasi persona che abbia un interesse legittimo alla consultazione.

4.8 Interesse legittimo cogente

L'articolo 49, paragrafo 1, comma 2 introduce un'ulteriore deroga applicabile in *extrema ratio*, solo quando "*un trasferimento non può essere basato su una disposizione dell'articolo 45 o 46, comprese le disposizioni sulle norme vincolanti d'impresa, e non è applicabile nessuna delle deroghe per una situazione specifica*".

Tale strumento può essere utilizzato solo in casi residui[57] e dipende da un numero significativo di condizioni espressamente previste dalla legge:

a. in linea con il principio di responsabilità sancito dal GDPR[58], il titolare del trattamento e *data exporter* deve essere in grado di dimostrare che **non** è stato possibile **applicare** gli altri strumenti previsti dal GDPR per legittimare il trasferimento;

b. il trasferimento deve essere necessario per il perseguimento di **interessi legittimi** e **preminenti** del titolare ed essenziali per proteggere la sua organizzazione imprenditoriale da gravi danni e pregiudizi,

c. gli interessi legittimi cogenti del titolare non devono prevalere sugli interessi, i diritti e le libertà dell'interessato con questi intendendosi qualsiasi possibile danno, fisico e materiale, ma anche immateriale, ad esempio in relazione a una perdita di reputazione[59] (**bilanciamento di interessi**[60]);

57 V. Considerando 113.

58 Articolo 5 (2) e Articolo 24 (1).

59 V. Considerando 75: "*The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage.*"

60 Valutazione del titolare del trattamento di tutte le circostanze del trasferimento (*i.a.* della natura dei dati, della finalità e della durata del trattamento, nonché della situazione nel paese d'origine e nel paese di

d. il trasferimento dei dati deve essere **occasionale**, non sistematico e deve riguardare un **numero limitato di interessati**;

e. il titolare ha l'obbligo di **informare l'Autorità di controllo** competente; nonché

f. l'obbligo di **informare l'interessato** del trasferimento e dei legittimi interessi legittimi cogenti perseguiti ai sensi degli artt. 13 e 14 del GDPR.

Qualora nessuna delle deroghe di cui all'articolo 49 primo e secondo paragrafo sia applicabile al caso concreto, il trasferimento nel Paese terzo sarà illecito e pertanto andrà evitato.

destinazione finale del trasferimento) e sull'impegno, quale *data exporter*, a fornire "adeguate garanzie" idonee a ridurre l'impatto indebito del trasferimento dei dati sulle persone interessate (*i.a.* misure volte a garantire la cancellazione dei dati dopo il trasferimento o a limitare le finalità; pseudonimizzazione o criptazione, ecc.).

CAPITOLO 3 di Pietro Boccaccini, Simona Custer, Federica Dendena e Mariangela Papadia

Marketing e Privacy: la sfida continua

SOMMARIO: 1. Le basi di legittimità a cui è possibile fare ricorso per attività di marketing – 2. L'approccio del Garante Privacy: alcuni aspetti a cui prestare attenzione – 2.1 Spam: i contenuti dell'informativa, opt-in, opt-out e social spam – 2.2 Tempo di conservazione dei dati – 2.3 Telemarketing: legittimità del trattamento e diritto di opposizione – 2.4 Utilizzo di banche dati per finalità promozionali: qualificazione dei rapporti privacy e obblighi dei soggetti coinvolti – 2.5 PEC e indirizzi reperiti sui sociali network – 2.6 Utilizzo di pop-up con consenso obbligato – 2.7 Giurisprudenza vs Garante Privacy

1. Le basi di legittimità a cui è possibile fare ricorso per attività di marketing

L'operatore economico che effettui attività di marketing per promuovere prodotti e servizi deve trattare i dati personali dei destinatari delle comunicazioni promozionali in conformità alla normativa applicabile in materia di protezione dei dati personali – che in Italia è costituita dal Regolamento UE n. 2016/679 ("**GDPR**") e dal D. Lgs. n. 196/2003 ("**Codice Privacy**"), così come modificato dal D. Lgs. n. 101/2018 – oltre che nel rispetto di tutti i provvedimenti del Garante per la protezione dei dati personali ("**Garante**").

Affinché il trattamento dei dati personali avvenga in modo lecito, occorre innanzitutto che questo sia basato su un adeguato presupposto. In proposito, alla luce del GDPR, è in principio possibile fondare un trattamento di dati per finalità di *marketing* sia sul consenso dell'interessato, che sul legittimo interesse.

In ogni caso, l'operatore soggetto alla normativa italiana non può prescindere dal rispetto delle disposizioni previste dall'art. 130 del Codice Privacy, ai sensi del quale per l'invio di comunicazioni di marketing effettuate tramite strumenti automatizzati di contatto (come chiamate senza operatore, email, sms, mms, ecc.) è necessario il consenso dell'utente o del contraente.

Per le comunicazioni di *marketing* effettuate tramite l'uso del telefono o della posta cartacea, invece, non occorre il consenso preventivo, ma resta fermo il diritto di opposizione dell'interessato. A tal fine, è stato istituito dal D.P.R. n. 178/2010 il Registro Pubblico delle Opposizioni, di cui si parlerà diffusamente al successivo paragrafo 2.3).

Il medesimo articolo 130 del Codice Privacy prevede, al comma 4, che per le comunicazioni di *marketing* effettuate tramite *email* non sia necessario il con-

senso – in deroga, quindi, a quanto previsto dal comma 2 dello stesso articolo – ma ciò a condizione: (*i*) che venga utilizzato esclusivamente l'indirizzo email fornito dall'interessato nel contesto della vendita del prodotto/servizio; (*ii*) che i servizi promossi siano analoghi a quelli oggetto della vendita; e (*iii*) che l'interessato, adeguatamente informato, non si opponga esercitando il cosiddetto *opt-out*, inizialmente o in occasione di successive comunicazioni. Il titolare deve inoltre informare l'interessato, sia al momento della raccolta dell'email che in occasione dell'invio di ogni comunicazione promozionale, della possibilità di opporsi in ogni momento al trattamento. La suddetta eccezione alla regola del consenso preventivo per le comunicazioni di marketing effettuate tramite email è il cosiddetto "*soft spam*".

Per ciò che riguarda il consenso, ai sensi del GDPR e sulla base anche delle indicazioni dello *European Data Protection Board* (cfr. *Guidelines on consent under Regulation 2016/679* adottate il 4 maggio 2020), per essere validamente prestato, deve essere:

- **libero**: occorre, ad esempio, che l'accesso a un servizio non sia subordinato al conferimento del consenso per finalità di *marketing* o che la casella per la raccolta del consenso online non sia già spuntata. Non è libero il consenso se non è possibile esprimerne uno separato in relazione a distinti trattamenti (i.e. principio della "granularità del consenso") o se l'interessato subirebbe conseguenze negative in caso di rifiuto di fornirlo o di revoca dello stesso;
- **specifico**: occorre acquisirne uno ad hoc per ciascuna distinta finalità perseguita; è altresì necessario acquisire uno specifico consenso anche per cedere i dati personali a terzi affinché questi svolgano proprie attività di marketing;
- **informato**: occorre fornire un'informativa adeguata all'interessato (la trasparenza è uno dei principi fondamentali del GDPR) affinché comprenda chiaramente a che trattamento sta acconsentendo. Non è peraltro consentito chiedere all'interessato il consenso al trattamento dati per finalità di *marketing* con un messaggio che ha già un contenuto promozionale e che presupporrebbe a sua volta un consenso; perché il consenso sia acquisito legittimamente occorre quindi utilizzare modalità che non lo presuppongono (es. un'*e-mail* mirata alla sola acquisizione del consenso o una telefonata con operatore);
- **inequivocabile**: occorre una manifestazione di volontà chiara (scritta o verbale) dell'interessato, che non possa prestarsi a letture ambigue; una raccolta del consenso basata sul silenzio o sull'inattività dell'interessato non sarebbe ritenuta valida, ad esempio.

Il titolare deve inoltre essere in grado di dimostrare che l'interessato ha fornito il proprio consenso, adottando quindi dei sistemi di raccolta e di memorizzazione idonei a tale fine (e.g. dei registri che tengano traccia di come e quando sono stati ottenuti i consensi).

Il consenso deve infine poter essere revocato dall'interessato con la stessa facilità con la quale è stato fornito, ad esempio tramite un semplice clic, in un contesto digitale.

Come anticipato, il titolare del trattamento – ai sensi dell'art. 6, comma 1, lett. f) del GDPR e alla luce del considerando 47 del GDPR – potrebbe basare il trattamento avente finalità di *marketing* anche sul legittimo interesse, a condizione però che abbia esito positivo il cosiddetto "*balancing test*" o "*legitimate interest assessment*", ossia la valutazione svolta dal titolare volta a verificare che gli interessi o i diritti e le libertà fondamentali dell'interessato – che, nel caso del marketing, sono ravvisabili soprattutto nel diritto alla protezione dei dati e alla non eccessiva ingerenza di terzi nella sfera individuale – non prevalgano sul legittimo interesse del titolare.

Inoltre, prima di procedere a qualsiasi trattamento per finalità di *marketing* basato sul legittimo interesse, occorre tenere conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento: potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare.

Ai sensi dell'art. 21, comma 2, del GDPR, l'interessato ha poi il diritto di opporsi in qualsiasi momento al trattamento dei dati che lo riguardano effettuato per finalità di *marketing*.

Il ricorso al legittimo interesse per i trattamenti aventi finalità di *marketing*, in ogni caso, è limitato non solo dalle sopra richiamate norme del Codice Privacy che richiedono il consenso per le comunicazioni promozionali effettuate con strumenti automatizzati, ma anche dall'attuale orientamento del Garante il quale, sotto questo profilo, si è fino ad oggi rivelato poco propenso ad aperture significative.

Infatti il Garante, con il provvedimento correttivo e sanzionatorio nei confronti di TIM S.p.A. del 15 gennaio 2020, ha in proposito precisato, tra l'altro, che:

- il legittimo interesse non può surrogare in via generale il consenso dell'interessato quale base giuridica del *marketing*;
- occorre tenere in debito conto le ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento;
- è necessaria un'attenta valutazione in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un simile trattamento;
- l'applicazione della base giuridica del legittimo interesse presuppone la prevalenza in concreto (in base a un bilanciamento rimesso al titolare, ma sempre valutabile dall'Autorità di controllo) di quest'ultimo su diritti, libertà e meri interessi dei destinatari delle comunicazioni promozionali;

- è necessaria la concreta attuazione di misure adeguate a garantire i diritti degli interessati ed in particolare del diritto di opposizione.

Il Garante ha altresì precisato che il titolare del trattamento non può ricorrere retroattivamente alla base dell'interesse legittimo in caso riscontri problemi di validità del consenso (come peraltro evidenziato anche dall'EDPB nelle citate linee guida sul consenso). Infatti, il titolare ha l'obbligo di comunicare nell'informativa rilasciata all'interessato *ex*. art. 13 del GDPR la base di legittimità alla quale intende fare ricorso al momento della raccolta dei dati personali e pertanto tale base deve essere decisa (adottando tutte le misure collegate) prima della raccolta dei dati.

La conclusione che è quindi possibile trarre dal quadro normativo citato e dall'orientamento attuale del Garante è che, laddove non ricorrano i presupposti per il legittimo interesse sopra richiamati e ad eccezione delle ipotesi del "*soft spam*" nonché del sistema di "*opt-out*" previsto per i dati presenti negli elenchi pubblici, la regola generale da seguire per i trattamenti effettuati per finalità di *marketing* è quella del previo consenso libero, specifico, informato e inequivocabile degli interessati.

2. L'approccio del Garante Privacy: alcuni aspetti a cui prestare attenzione

2.1 Spam: i contenuti dell'informativa, opt-in, opt-out e social spam

L'invio di comunicazioni con materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale effettuate senza il preventivo consenso del soggetto (persona fisica) destinatario, ai sensi dell'artt. 7 e 13 del GDPR con sistemi automatizzati di chiamata senza operatore (c.d. telefonate preregistrate) oppure via *e-mail, fax, sms, mms* è definito come "*spam*" ed è vietato ai sensi dell'art. 130 del Codice Privacy[61].

La persona fisica ha la possibilità di opporsi a tale trattamento illecito tramite segnalazione al Garante, invece le persone giuridiche si possono rivolgere alle autorità giudiziarie, infatti a quest'ultime non si applicano le tutele previste dal GDPR (cfr. Considerando 14 del GDPR). Si segnala, tuttavia, che possono nascere dubbi in merito alla tutela che una persona fisica possa avere nel caso di trattamento illecito dell'indirizzo di posta elettronica usato nell'ambito del proprio rapporto lavorativo (es. nome.cognome@azienda.it). In questo caso, rimane valido il criterio affermato dal Gruppo Articolo 29 (ora *European Data Protection Board*), con i pareri nn. 4/1997 e 5/2004, ovvero è necessario analizzare il "contenuto", le "finalità" o il "risultato" delle comunicazioni inviate al predetto indirizzo *e-mail* per poter stabilire che alcune informazioni sulle persone giuridiche siano "concernenti" persone fisiche e applicare le relative tutele.

61 Linee guida del Garante in materia di attività promozionale e contrasto allo spam del 4 luglio 2013(https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2542348)

Alla luce di quanto sopra, pertanto, 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 alla persona fisica 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 (c.d. "*opt-in*").

Nonostante quanto sopra, si segnala l'eccezione del "*soft spam*" (art. 130, comma 4, Codice Privacy) riferita, come già su anticipato, ai messaggi promozionali per la sola posta elettronica, in base alla quale, se il titolare del trattamento utilizza, 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 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 c.d. "*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* 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 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 a 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.

2.2 Tempo di conservazione dei dati

2.2.1 Principio di limitazione della conservazione

Nel rispetto del principio di limitazione della conservazione sancito all'art. 5, comma 1, lettera e) del GDPR, i dati oggetto del trattamento devono essere conservati per il periodo di tempo strettamente necessario a consentire al titolare il conseguimento della finalità per le quali sono stati raccolti.

Trascorso detto periodo, infatti, i dati non avranno più alcuna utilità per il titolare del trattamento, che dovrà, quindi, provvedere alla loro cancellazione o anonimizzazione, mediante l'utilizzo di sistemi e tecniche efficaci che consentano ai dati di non essere più riconducibili all'interessato a cui appartenevano.

Tuttavia non è sempre così semplice individuare con precisione il periodo di conservazione dei dati. Ove ciò risulti particolarmente difficile, l'art. 13 del GDPR consente però al titolare del trattamento di indicare all'interessato – al

momento della raccolta dei dati - il criterio utilizzato per determinare tale periodo[62].

Qual è, quindi, il periodo di conservazione dei dati per le attività di *marketing*?

2.2.2 Le indicazioni del Garante

Nell'ambito dell'attività di marketing il periodo di conservazione dei dati è cristallizzato ormai da parecchi anni. Ciò, in quanto con provvedimento a carattere generale del 24 febbraio 2005 il Garante ha espressamente previsto che "*[…] i dati relativi al dettaglio degli acquisti con riferimento a clienti individuabili possono essere conservati per finalità di profilazione o di marketing per un periodo non superiore, rispettivamente, a* ***dodici*** *e a* ***ventiquattro*** *mesi dalla loro registrazione*"[63].

Il titolare del trattamento è, quindi, autorizzato a conservare i dati per finalità di *marketing* e profilazione rispettivamente non oltre i ventiquattro e i dodici mesi dalla data della loro raccolta, salvo il caso in cui non sia stato espressamente autorizzato dal Garante a seguito dell'accoglimento dell'istanza di verifica preliminare presentata ai sensi dell'art. 17 del Codice Privacy[64].

In considerazione della predetta possibilità e nel vigore del Codice Privacy (precedentemente alle modifiche apportate dal D. Lgs. n. 101/2018), infatti, sono state molte le istanze di verifica preliminare presentate al Garante (soprattutto da società appartenenti al settore del lusso e della moda), le quali hanno fondato la loro esigenza ad ottenere un allungamento del periodo di conservazione nella necessità di poter effettuare in modo più diretto e mirato l'attività di *marketing* nei confronti della propria clientela.

Attività che in soli ventiquattro mesi non è certamente possibile, soprattutto se si pensa che la frequenza media di acquisto dei beni classificati come di lusso e/o di fascia medio alta da parte di ciascun cliente è stata quantificata in due volte l'anno, in concomitanza con i periodi di *release* delle collezioni primavera-estate e autunno-inverno[65].

Queste, quindi, le motivazioni che hanno portato il Garante ad accogliere una buona parte delle predette istanze e ad autorizzare la conservazione dei dati oltre i ventiquattro mesi, arrivando addirittura a stabilire periodi di sette/dieci anni, in determinati casi e in presenza di idonee misure di sicurezza in grado di garantire il rispetto della c.d. *data retention*.

62 Cfr. articolo 13, comma 2, del Reg. (UE) n. 2016/679: "[…] *il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;* […]".

63 Cfr. articolo 8 del Provvedimento a carattere generale "*Fidelity card e garanzie dei consumatori. Le regole del Garante per i programmi di fidelizzazione*", Garante, 24 febbraio 2005, doc. web n. 1103045.

64 Articolo abrogato dal D. Lgs. n. 101/2018.

65 Cfr. Garante, verifica preliminare - conservazione di dati personali riferiti alla clientela per finalità di profilazione e di marketing diretto, 22 maggio 2018, doc. web n. 9018628; cfr. Garante, verifica preliminare presentata da Bulgari S.p.A. - trattamento e conservazione di dati personali della clientela per finalità di profilazione, 24 aprile 2013, doc. web. n. 2499354; cfr. Garante, verifica preliminare presentata da Salvatore Ferragamo - trattamento dei dati personali della clientela per finalità di profilazione e marketing, 30 maggio 2013 doc. web. n. 2547834.

Con l'avvento del GDPR il predetto panorama ha, però, subito un enorme cambiamento, essendo stato eliminato lo strumento della verifica preliminare per consentire al titolare del trattamento di richiedere, tra l'altro, l'allungamento dei tempi di conservazione dei dati.

Ciò, però non vuol dire che al titolare sia stata inibita la possibilità di conservare i dati per finalità di marketing per un periodo di tempo superiore rispetto a quanto stabilito dal Garante. Per fare ciò, il titolare dovrà compiere un'approfondita **valutazione circa la conformità del trattamento** che intende realizzare ai principi *privacy*, con analisi di tutti gli elementi che lo caratterizzano compresi gli eventuali rischi per i diritti e le libertà degli interessati.

Qualora, poi, dalla predetta valutazione dovesse emergere che il trattamento presenti un *rischio elevato per i diritti e le libertà degli interessati*, il titolare dovrà procedere con l'esecuzione della valutazione di impatto ai sensi dell'art. 35 del GDPR[66]. Se anche all'esito della valutazione di impatto dovesse residuare un rischio elevato, prima di procedere con il trattamento il titolare dovrà consultare il Garante[67], così come previsto dall'art. 36 del GDPR[68].

2.3 *Telemarketing*: legittimità del trattamento e diritto di opposizione

2.3.1 Cosa si intende per *telemarketing* e quali i ruoli *privacy*

Il *telemarketing* è una tipologia di *marketing* realizzata tramite l'utilizzo del telefono e impiegata da numerose società al fine di promuovere e/o commercializzare i propri prodotti o servizi a possibili clienti (interessati).

Nello specifico, tale attività potrà essere svolta - in nome e per conto delle società, che ai fini *privacy* rivestono il ruolo di titolari del trattamento dei dati - da operatori telefonici:

- interni alle organizzazioni dei titolari ed espressamente autorizzati al trattamento dei dati, ai sensi dell'art. 29 del GDPR[69] e dell'art. 2-*quaterdecies* del Codice Privacy[70];

66 Cfr. articolo 35, comma 1, Reg. (UE) n. 2016/679 "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*".

67 Cfr. Garante, verifica preliminare - prolungamento dei tempi di conservazione dei dati personali riferiti alla clientela per il loro utilizzo a fini di profilazione e di promozione commerciale profilata, 09 maggio 2018, doc. web n. 8998319.

68 Cfr. articolo 36, comma 1, Reg. (UE) n. 2016/679: "*Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottare dal titolare del trattamento per attuare il rischio*"..

69 Cfr. articolo 29, Reg. (UE) n. 2016/679, rubricato "*Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento", secondo cui "Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*".

70 Cfr. articolo 2-quaterdecies, D. Lgs. n. 196/2003, rubricato "*Attribuzione di funzioni e compiti a soggetti designati*" ove è previsto che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria*

- esterni (c.d. *call center*) alle organizzazioni dei titolari e nominati responsabili del trattamento, ai sensi dell'art. 28 del GDPR.

A seconda del caso, il titolare dovrà quindi disciplinare i rapporti con i predetti soggetti. Nel primo caso, il titolare dovrà predisporre specifiche lettere di designazione in cui verranno individuate precise indicazioni circa il trattamento dei dati; nel secondo, invece, le parti andranno a concludere un vero e proprio contratto con previsione di tutta una serie di elementi e obblighi, così come richiesto dall'art. 28 del GDPR.

Ciò, al fine di garantire che anche i trattamenti dei dati realizzati nell'ambito dello svolgimento di attività di *telemarketing* vengano effettuati da soggetti autorizzati e conformemente alle disposizioni normative contenute nel GDPR, nel Codice Privacy e nei numerosi provvedimenti emanati dal Garante.

2.3.2 Il consenso quale condizione di liceità del trattamento

Per potersi considerare legittimo, il trattamento dei dati deve trovare fondamento in una delle basi giuridiche specificamente elencate all'art. 6 del GDPR[71] Tale principio, ovviamente, vale per tutte le operazioni di trattamento effettuate dal titolare, tra cui rientrano anche quelle realizzate nell'ambito dello svolgimento di attività di telemarketing, per le quali, però, non possono sorgere dubbi circa la base giuridica che ne legittima il trattamento.

Infatti, l'art. 129, comma 2, del Codice Privacy prevede espressamente che "*il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi […]*", individuando nel consenso la condizione di liceità dei predetti trattamenti.

Tuttavia, affinché il consenso espresso dall'interessato possa considerarsi valido ed efficace, è opportuno che lo stesso soddisfi le caratteristiche[72], già elencate al precedente paragrafo 1, ovvero deve essere: libero, specifico, inequivocabile e informato.

Prima di procedere con il trattamento dei dati, è quindi fondamentale che il titolare - a prescindere dal fatto che i dati siano stati raccolti da lui direttamente, piuttosto che acquistati da terzi soggetti - verifichi la sussistenza di un valido

responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità".

71 Cfr. articolo 6, Reg. (UE) n. 2016/679, rubricato "*Liceità del trattamento", che stabilisce "Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è 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; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. […]*".

72 Secondo quanto previsto dall'articolo 4, paragrafo 1, numero 11) GDPR, il consenso deve essere una "*manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato". Cfr. considerando (42) e (43)*, GDPR.

ed efficace consenso da parte dell'interessato. In entrambi i casi resta, infatti, in capo al titolare l'onere di dimostrare[73] che il trattamento realizzato è legittimo e rispettoso delle disposizioni normative in materia di *privacy*.

Tale concetto, peraltro, è stato ripreso e ribadito dallo stesso Garante in diversi provvedimenti. Il Garante si è, infatti, trovato più volte costretto a sanzionare società - quali titolari del trattamento - per aver realizzato operazioni di trattamento per finalità di *telemarketing* in assenza del rilascio di un valido consenso da parte degli interessati o per non aver compiuto i necessari controlli[74].

È, quindi, evidente che al fine di andare esente da eventuali sanzioni il titolare debba fare tutto quanto necessario per appurare che i dati degli interessati in suo possesso siano stati acquisiti nel rispetto della normativa *privacy*; ma in che modo? Richiedendo, ad esempio, alla società che gli ha venduto i dati il rilascio di una dichiarazione, ove venga affermato che gli stessi sono stati raccolti nel rispetto del GDPR e/o di visionare sia l'informativa sul trattamento dei dati, sia il modulo per l'espressione del consenso.

2.3.3 L'eccezione alla "regola" del consenso

Non tutti i trattamenti effettuati nell'ambito del *telemarketing* necessitano, però, del consenso degli interessati per essere considerati legittimi.

Esiste, infatti, un'eccezione alla predetta "regola".

Ai sensi dell'art. 130, comma 3 bis, del Codice Privacy[75] gli interessati - i cui dati e contatti sono stati reperiti dal titolare del trattamento da elenchi o pubblici registri - possono essere contattati telefonicamente senza consenso, a condizione che:

- il contatto avvenga per il tramite di un operatore e non mediante sistemi automatizzati;
- i numeri telefonici e/o gli altri dati personali degli interessati non risultino iscritti nel registro delle pubbliche opposizioni, di cui si dirà meglio al seguente paragrafo.

In questo caso, è comunque consentito agli interessati di esercitare il c.d. "*opt-out*" prima del termine della chiamata. Nello specifico, dopo aver ricevuto tutte le informazioni circa le finalità e le modalità del trattamento dei dati, gli interessati contattati saranno liberi di manifestare la propria volontà di non essere più ricontattati.

73 Ciò, anche al fine del rispetto del principio di accountability di cui all'articolo 24 del GDPR.

74 Cfr. Garante, ordinanza ingiunzione, 11 aprile 2019, caso Vincall s.r.l.s., doc. web n. 9116053.; cfr. Garante, ordinanza ingiunzione, 26 luglio 2018, caso Fastweb S.p.A., doc. web n. 9040267.

75 Cfr. articolo 130, comma 3 bis, D. Lgs. n. 196/2003, che prevede "*In deroga a quanto previsto dall'art. 129, il trattamento dei dati di cui al comma 1 del predetto articolo, mediante l'impiego del telefono e della posta cartacea per le finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito nei confronti di chi non abbia esercitato il diritto di opposizione, con modalità semplificate e anche in via telematica, mediante l'iscrizione della numerazione della quale è intestatario e degli altri dati personali di cui all'articolo 129, comma 1, in un registro pubblico delle opposizioni*".

2.3.4 Il registro pubblico delle opposizioni

Con il D.P.R. n. 178/2010 "*Regolamento recante istituzione e gestione del registro pubblico dei contraenti che si oppongono all'utilizzo dei propri dati personali e del proprio numero telefonico per vendite o promozioni commerciali*" è stato ufficialmente istituito il registro pubblico delle opposizioni ("**RPO**"), che nell'ambito dello svolgimento delle attività di *telemarketing* ha una doppia valenza: da un lato, è certamente lo strumento di maggior tutela a disposizione degli interessati e, dall'altro, rappresenta un possibile ostacolo per l'attività di *telemarketing* del titolare del trattamento.

Infatti, prima di procedere con la predetta attività, il titolare si ritrova ancora una volta nella posizione di dover effettuare verifiche circa i dati dei potenziali interessati da contattare. Nello specifico, il titolare dovrà controllare che detti dati (quali recapiti telefonici e/o altro)[76] non risultino iscritti nel registro pubblico delle opposizioni.

Ove così fosse, il trattamento dei dati da parte del titolare per finalità di telemarketing non troverebbe alcun impedimento alla sua realizzazione; in caso contrario, invece, il titolare 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.

È bene, però, ricordare che tale verifica deve essere compiuta non solo da parte del titolare del trattamento, bensì anche dai call center eventualmente incaricati per l'esecuzione del trattamento, che - in qualità di responsabili - agiscono in nome e per conto dei rispettivi titolari. Prima di procedere con l'attività di *telemarketing* e ogniqualvolta ricevano liste contenenti le numerazioni telefoniche estratte da pubblici elenchi, i call center avranno quindi l'onere e il dovere di analizzare tali liste, caricandole sul sito dedicato al registro delle opposizioni[77] al fine di ottenerne la c.d. "pulitura", ovvero l'eliminazione da tutti quei dati di coloro che hanno manifestato il diritto di opposizione al trattamento.

Inutile dire che anche sui predetti aspetti l'attenzione del Garante è da sempre molto elevata. Infatti, ogniqualvolta siano state rilevate violazioni di questo tipo, i trasgressori sono stati sanzionati con importi davvero "salati", a nulla rilevando eventuali giustificazioni addotte[78].

76 Nel registro delle pubbliche opposizioni possono essere iscritti i recapiti di telefonia fissa e di telefonia mobile - a seguito dell'ampliamento dell'ambito di applicazione operato dalla Legge n. 5/2018 "*Nuove disposizioni in materia di iscrizione e funzionamento del registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato*" -, nonché gli indirizzi per la ricezione della posta cartacea - a seguito dell'entrata in vigore del D.P.R. n. 149/2018 "Regolamento recante modifiche al decreto del Presidente della Repubblica 7 settembre 2010, n. 178, in materia di registro pubblico delle opposizioni, con riguardo all'impiego della posta cartacea".

77 Cfr. http://www.registrodelleopposizioni.it.

78 Cfr. Garante, ordinanza di ingiunzione, 29 novembre 2018, caso Wind Tre S.p.A., doc. web n. 9079005; cfr. Garante per la protezione dei dati personali, ordinanza di ingiunzione, 05 luglio 2018, caso Vodafone Italia S.p.A., doc. web n. 9025351.

Tra le tante pronunce del Garante, è utile ricordare quella comminata lo scorso 11 dicembre a Eni Gas e Luce S.p.A. per l'importo di 8,5 milioni di euro[79]. La società è stata sanzionata per la commissione di una serie di violazioni, tra cui: (*i*) la **realizzazione di telefonate pubblicitarie in assenza di consenso** delle persone contattate o nonostante il loro diniego a ricevere chiamate promozionali, (*ii*) **l'assenza di specifiche procedure di verifica del registro pubblico delle opposizioni**, (*iii*) l'assenza di misure tecniche e organizzative in grado di recepire le manifestazioni di volontà degli utenti, (*iv*) tempi di conservazioni dei dati superiori a quelli consentiti e (*v*) l'acquisizione dei dati dei potenziali clienti da soggetti (*list provider*) che non avevano acquisito il consenso per la comunicazione di tali dati.

2.3.5 Gli obblighi in capo ai call center e le telefonate mute

Come anticipato al precedente paragrafo 2.3.1, l'attività di *telemarketing* può essere affidata e svolta da soggetti esterni all'organizzazione del titolare del trattamento. Ai fini privacy, quindi, tali soggetti (*call center*) ricopriranno il ruolo di responsabili del trattamento ai sensi dell'art. 28 del GDPR[80], con assunzione di tutta una serie di obblighi nei confronti dei rispettivi titolari.

Ma non solo. Con l'accettazione della predetta nomina, i *call center* sono altresì chiamati a rispondere in solido con i rispettivi titolari per la commissione di eventuali trattamenti di dati illeciti.

È, quindi, molto importante che prima di procedere con il trattamento dei dati per lo svolgimento di attività di *telemarketing*, i *call center* pongano in essere tutte le verifiche necessarie ad accertare la legittimità dei dati ricevuti e la loro conformità alle disposizioni normative in tema di *privacy*. Ciò, soprattutto al fine di andare esenti da eventuali responsabilità.

Un obbligo analogo viene, altresì, sancito dalla Legge n. 5/2018, ove è espressamente previsto che gli operatori dei call center devono "*consultare mensilmente, e comunque precedentemente all'inizio di ogni campagna promozionale, il registro pubblico delle opposizioni e di provvedere all'aggiornamento delle proprie liste*"[81].

Ma non solo. Nell'esercizio dell'attività di *telemarketing* gli operatori dei *call center* sono altresì chiamati a rispettare ulteriori accorgimenti, prescritti non solo dal nostro legislatore con la predetta Legge, ma anche dal Garante con il

79 Cfr. Garante, provvedimento correttivo e sanzionatorio, 11 dicembre 2019, caso Eni Gas e Luce S.p.A., doc. web n. 9244365.

80 Occorre individuare ove è situato il *call center*, al fine di verificare la configurazione o meno di un trasferimento di dati extra UE. Infatti, qualora il *call center* sia ubicato in un paese extra UE il titolare del trattamento dovrà anzitutto verificare se il paese rientra tra quelli per ritenuti adeguati dalla Commissione Europea; diversamente dovranno essere utilizzate le clausole contrattuali tipo al fine di disciplinare il trasferimento.

81 Art. 1, comma 11, Legge n. 5/2018: "*Gli operatori che utilizzano i sistemi di pubblicità telefonica e di vendita telefonica o che compiono ricerche di mercato o comunicazioni commerciali telefoniche hanno l'obbligo di consultare mensilmente, e comunque precedentemente all'inizio di ogni campagna promozionale, il registro pubblico delle opposizioni e di provvedere all'aggiornamento delle proprie liste*".

provvedimento generale a carattere prescrittivo sulle c.d. telefonate mute[82] del 20.02.2014.

Nello specifico, gli operatori dei *call center*:

- non potranno effettuare chiamate con numero riservato;
- dovranno utilizzare specifici prefissi;
- dovranno indicare agli interessati che i loro dati sono stati estratti da elenchi di abbonati, fornendo loro indicazioni utili circa l'eventuale iscrizione al registro pubblico delle opposizioni;
- dovranno fornire agli interessati l'informativa sul trattamento dei dati personali;
- dovranno evitare le c.d. **telefonate mute**.

Con riferimento a questo ultimo aspetto, il Garante è stato chiaro nell'introdurre apposite tutele a favore degli interessati, volte a ridurre l'utilizzo delle c.d. telefonate mute, che in molti casi hanno generato stati di ansia, allarme e preoccupazione nei confronti di chi le riceveva[83]. Il Garante ha, infatti, stabilito che:

- non possono essere effettuate più di tre telefonate "mute" ogni cento andate a "buon fine";
- la telefonata "muta" deve interrompersi trascorsi tre secondi dalla risposta dell'interessato;
- a seguito di una telefonata "muta" deve essere preclusa la possibilità di richiamare lo stesso interessato per almeno cinque giorni;
- il riutilizzo del numero dell'interessato deve avvenire in modo da assicurare la presenza di un operatore;

sostenendo che l'insieme dei predetti accorgimenti riesca così a rendere residuale la possibilità di ricevere una telefonata "muta". È stato, poi, altresì vietato agli operatori di porre in attesa silenziosa gli interessati, prescrivendo che il sistema da loro utilizzato generi una sorta di rumore ambientale (c.d. *comfort noise*, quali voci di sottofondo, brusio e squilli di telefono) al fine di rassicurare la persona chiamata.

82 Cfr. Garante, provvedimento generale a carattere prescrittivo sulle c.d. telefonate "mute" del 20.02.2014, doc. web n. 3017499, ove per telefonate "mute" si intendono quelle chiamate "*[…] nelle quali la persona contattata, dopo aver sollevato il ricevitore non viene messa in comunicazione con alcun interlocutore*".

83 Le persone chiamate, infatti, sono naturalmente portate ad associare tale evento a comportamenti illeciti (controlli indebiti, molestie, *stalking*, verifiche di malintenzionati volte alla commissione di eventuali reati, quali furti o aggressioni).

2.4 Utilizzo di banche dati per finalità promozionali: qualificazione dei rapporti privacy e obblighi dei soggetti coinvolti

Il Garante ha adottato importanti provvedimenti anche per quanto concerne il trattamento dei dati per finalità di marketing tramite l'acquisizione di banche dati create da terzi soggetti.

Non è rara l'ipotesi in cui, infatti, in occasione della pianificazione di una campagna di *marketing*, si procede all'acquisizione di banche dati per ampliare il numero di destinatari cui poter inviare le comunicazioni commerciali. In questi casi, quindi, i dati di contatto degli interessati non vengono acquisiti direttamente dalla società interessata a svolgere l'attività di *marketing* ma da un soggetto terzo che crea apposite liste di contatti.

In tali casi, è fondamentale che i soggetti coinvolti nell'operazione di trasferimento/cessione dei *database*, per un verso, garantiscano l'adozione e il rispetto di tutte le misure tecniche organizzative poste a tutela dei dati personali (definizione dei ruoli e responsabilità, sicurezza, raccolta dati in conformità alla normativa di settore); per altro verso, coinvolgano l'interessato in tale processo rendendolo consapevole e consentendogli di esprimere un valido e compiuto consenso al trasferimento dei propri dati.

Partendo da questo ultimo profilo, il Garante ha avuto modo di affrontare il tema in occasione delle "*Linee Guida in materia di attività promozionale e contrasto allo spam*" del 4 luglio 2013[84]: in termini generali è necessario che il soggetto che acquisisce i dati di contatto dell'interessato raccolga il consenso dell'interessato alla comunicazione dei dati a società esterne (con l'indicazione chiara della società destinataria dei dati o delle categorie economiche o merceologiche - es. finanza, editoria – cui appartiene) per loro finalità di marketing; mentre, in capo a chi acquista la banca dati rimane solo l'obbligo di fornire l'informativa privacy al momento della registrazione dei dati o della prima eventuale comunicazione, senza tuttavia acquisire un nuovo consenso per la finalità promozionale. Tale ultima informativa dovrà anche contenere un riferimento sull'origine dei dati, affinché gli interessati possano rivolgersi anche alla società cedente per esercitare i loro diritti.

Secondo il Garante, tuttavia, se l'informativa resa dalla società cedente individua in maniera specifica i soggetti destinatari dei dati e specifica i dettagli dell'attività di trattamento che questi ultimi effettueranno sui dati acquisiti, non è necessario che il predetto soggetto, a seguito della cessione, debba rilasciare un'ulteriore informativa, potendo utilizzare i dati senza problemi (ma sarà tenuto a fornire un idoneo recapito per l'esercizio dei diritti dell'interessato).

In tutti gli altri casi (si pensi alle ipotesi in cui una società vende dati ad altra, oppure una società ne acquisisce un'altra o le succede), la società che subentra dovrà rilasciare l'apposita informativa e ottenere uno specifico e libero consenso per l'uso dei dati, in assenza del quale il trattamento deve ritenersi illecito.

84 Le Linee guida sono consultabili al seguente link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2542348

Quanto, poi, alla gestione dei rapporti interni tra le società interessate dal trasferimento dei dati e delle diverse responsabilità in gioco, spesso il Garante ha affrontato casi in cui società specializzate nella realizzazione e vendita di banche dati abbiano del tutto trascurato i profili *privacy*, procedendo comunque alla cessione dei dati personali raccolti. È il caso, ad esempio, delle tre pronunce emesse tra il 2012 e il 2013[85] nei confronti di due società specializzate nel settore delle banche dati e di un operatore di telecomunicazioni che hanno ricevuto sanzioni elevatissime pari a Euro 700.000,00.

In particolare, le due imprese specializzate nella creazione di banche dati, avevano realizzato e venduto archivi di dati di milioni di persone, recuperando le informazioni contenute, ad esempio, negli elenchi telefonici e nelle liste elettorali. Questi dati erano stati raccolti in assenza di qualsivoglia adempimento *privacy* previsto dal previgente Codice Privacy e in particolare senza fornire agli interessati idonea informativa né tanto meno raccogliere uno specifico consenso al trasferimento di dati a terzi per finalità di *marketing*. Con riferimento, invece, alla società operante nel settore delle telecomunicazioni, il Garante ha accertato che quest'ultima, nonostante fosse a conoscenza dell'origine irregolare dei dati, li aveva non soltanto acquistati, ma utilizzati per proprie finalità promozionali.

I tre provvedimenti di ingiunzione contengono alcuni spunti particolarmente interessanti sulla vendita e l'acquisto di banche dati per effettuare attività promozionali e sui ruoli dei soggetti coinvolti in tali operazioni.

In primo luogo viene ribadito il principio che la individuazione dei ruoli *privacy* e l'attribuzione dei relativi poteri, doveri e responsabilità devono basarsi su elementi sostanziali, mentre sono del tutto irrilevanti le qualificazioni formali. Ciò vuol dire che l'eventuale nomina a responsabile del trattamento "fittizia" volte ad aggirare eventuali criticità non è da ritenersi valida.

In secondo luogo viene confermato che, nel caso in cui la comunicazione di dati da un titolare ad un altro sia stata preceduta dal rilascio di un'idonea informativa che prevedeva espressamente "*la comunicazione dei dati a terzi per finalità di marketing*", il titolare destinatario di tali dati è tenuto a rendere comunque la propria informativa alla prima occasione utile. Secondo il Garante, infatti, tale onere consente agli interessati cui i dati riferiscono "*di mantenere un effettivo controllo sui propri dati personali e di poter esercitare i diritti previsti dall'art. 7 del Codice direttamente presso ciascun titolare, senza intermediazioni non previste dalla normativa*".

Pertanto, chi intenda avvalersi di dati acquisiti da soggetti terzi per svolgere attività di *marketing* non può esimersi dal verificare se gli interessati abbiano rilasciato un valido consenso a tale tipo di trattamento: infatti, secondo quanto stabilito dal Garante, il titolare destinatario dei dati può essere ritenuto responsabile anche dell'illecito trattamento dei dati svolto da chi gli ha venduto il *database*.

85 Cfr. Ordinanza di ingiunzione del 10 gennaio 2013: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2438949; Ordinanza ingiunzione del 18 ottobre 2012: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2368171; Ordinanza ingiunzione del 7 febbraio 2013: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2428316

Il principio è stato più volte enunciato dal Garante: si veda ad esempio, il provvedimento n. 49 dell'11 febbraio 2016[86] con il quale il Garante ha ritenuto illecito l'invio di comunicazioni *marketing* trasmesse da una società a un indirizzo *e-mail* presente nelle liste acquistate da un terzo, in quanto non risultava, tra l'altro, che l'interessato avesse manifestato il proprio specifico consenso per l'invio delle menzionate comunicazioni commerciali, come richiesto dall'art. 130, commi 1 e 2, del Codice Privacy. Il Garante ha vietato alla società l'utilizzo di tali dati ai fini *marketing*.

E ancora, con il provvedimento del 22.05.2018[87], il Garante, nell'ambito di un'indagine condotta per verificare la liceità di un trattamento operato da una società proprietaria di un sito *web* su dati acquisiti, tra le altre cose, da società terze, ha riscontrato che, anche in detta occasione, queste ultime non avevano correttamente ottenuto il consenso da parte degli interessati al trattamento dei dati personali per finalità di *marketing* e di comunicazione ai terzi per analoghe finalità. Tuttavia, la società acquirente, affidandosi al fatto che la società cedente avesse correttamente ottenuto il consenso, aveva utilizzato i dati per scopi commerciali. Il Garante, dopo aver richiamato i propri precedenti provvedimenti, ha ribadito il principio in base al quale la società acquirente di dati personali è tenuta a verificare che ciascun interessato abbia validamente prestato il proprio consenso all'utilizzo dei dati per finalità promozionali; verifica che, nella specie, non era avvenuta. Per tale ragione, anche in questo caso, il Garante ha disposto che i dati così raccolti non potessero essere ulteriormente trattati.

Alla luce di quanto detto e tenuto conto dei profili di responsabilità connessi a tale tipi di trattamenti e delle ingenti sanzioni in cui oggi, sotto la vigenza del GDPR, si incorrerebbe nell'ipotesi di trattamento illecito di dati per mancanza di idonea informativa o valido consenso (cfr. art. 83, paragrafo 5, lett. a) e b)), è necessario prestare particolare attenzione agli aspetti *privacy* quando si decide di acquisire un *database* ai fini *marketing*, affrontando tale profilo anche a livello contrattuale. In questo senso, si potrebbe valutare l'inserimento di un'apposita clausola con cui la società che cede il data base dichiari che le informazioni raccolte si riferiscono a soggetti che abbiano rilasciato valido consenso alla trasmissione a terzi per fini *marketing* e concordare opportune verifiche, eventualmente con controlli a campione.

2.5 PEC e indirizzi reperiti sui sociali network

Numerosi gli interventi del Garante sul tema del *social spam* e sull'utilizzo a fini promozionali degli indirizzi pec recuperati dai registri pubblici: anche in questi casi, in base alle indicazioni del Garante, l'invio di comunicazioni a scopo promozionale deve necessariamente avvenire con il preventivo consenso informato degli utenti cui le comunicazioni sono trasmesse.

86 Cfr. Provvedimento n. 49 dell'11 febbraio 2016: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4885578

87 Cfr. Provvedimento n.363 del 22 maggio 2018: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8995274

Con particolare riferimento al cd '*social spam*' - ovvero la pratica di inviare messaggi pubblicitari (non richiesti) ad un numero elevato di utenti tramite posta elettronica - il Garante, negli anni, ha assunto una posizione molto chiara e precisa: la presenza di un indirizzo *e-mail* su un *social network* non significa che possa essere utilizzato liberamente per qualsiasi scopo, tanto meno per finalità di *marketing*. In tali casi è sempre necessario raccogliere il consenso dei destinatari.

Tali principi sono stati più volte enunciati dal Garante per il tramite di provvedimenti generali[88], Linee guida[89], o, più semplicemente, *newsletter* a scopo informativo e/o divulgativo[90].

Più di recente[91], il Garante è tornato sul tema prendendo l'avvio dalla segnalazione di una società di consulenza finanziaria che lamentava l'invio di numerose email promozionali indirizzate alle caselle di posta elettronica di alcuni suoi promotori senza che questi ne avessero autorizzato la ricezione. Dagli accertamenti è emerso che la raccolta degli indirizzi di posta elettronica avveniva, oltre che in occasione della partecipazione degli interessati ad incontri di natura professionale (quali, ad esempio, fiere e seminari), anche attraverso l'instaurazione di rapporti su *LinkedIn* e *Facebook* o recuperando contatti sui social. Con il provvedimento n. 378 del 21 settembre 2017, il Garante, richiamando i propri precedenti in tema di "*social spam*", ha dichiarato illecita la condotta della società di consulenza che trattava per fini promozionali indirizzi di posta elettronica reperiti on line in quanto tali i dati non possono essere utilizzati liberamente. Il Garante, infatti, ha ritenuto infondata la tesi della società, secondo cui l'iscrizione a un *social network* implicherebbe, automaticamente, il consenso all'utilizzo dei dati personali per l'attività di *marketing*: secondo quanto affermato dal Garante, tale finalità non è compatibile con le funzioni dei *social network* che sono preordinate alla condivisione di informazioni e allo sviluppo di contatti professionali, e non alla commercializzazione e promozione di prodotti e servizi. Opinione, questa, in linea con i principi espressi sul tema anche dal Gruppo europeo delle Autorità garanti per la protezione dei dati[92] il quale ha espressamente escluso che l'iscrizione ad un servizio presente sul *web* com-

88 Sul tema si vedano il provvedimento di carattere generale del 29 maggio 2003 "*Spamming. Regole per un corretto invio delle e-mail pubblicitarie*" con il quale, partendo dal presupposto che gli indirizzi di posta elettronica costituiscono dati di carattere personale, si affermava che la loro utilizzazione per fini commerciali fosse consentita unicamente nell'ipotesi in cui l'utente avesse manifestato in precedenza un consenso libero, specifico e informato (cfr. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/29840).

89 Si tratta delle "*Linee guida in materia di attività promozionale e contrasto allo spam*" del 4 luglio 2014 con le quali il Garante, dopo aver evidenziato l'emergere di nuove forme di spam, tra le quali il c.d. "*social spam*", affermava che, senza il consenso preventivo era da escludersi la possibilità di inviare comunicazioni promozionali neanche nel caso in cui i dati personali fossero tratti da registri pubblici, elenchi, siti web atti o documenti conosciuti o conoscibili da chiunque.

90 Si vedano, a titolo di esempio, il comunicato stampa del 23 luglio 2013 "*No allo spam, sì a offerte commerciali "amiche" dei consumatori*" (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2549317); la Newsletter n. 435 del 29 novembre 2017 (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/7221009).

91 Cfr. Provvedimento n.378 del 21 settembre 2017: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7221917

92 Si tratta del Il Gruppo di lavoro "Articolo 29" (Art. 29 WP), sostituito, a partire dal 25 maggio 2018, dal Comitato europeo per la protezione dei dati (EDPB).

porti la legittimità del trattamento dei dati personali da parte di altri partecipanti alla medesima piattaforma ai fini dell'invio di informazioni commerciali[93].

Del pari, anche le *pec* dei professionisti non possono essere utilizzate ai fini *marketing* senza il relativo consenso.

Con provvedimento del 1° febbraio 2018[94], il Garante si è trovato costretto a intimare ad una società italiana di cessare l'invio massivo di *e-mail* commerciali agli indirizzi *pec* di avvocati, notai e commercialisti reperiti *online* grazie alla semplice consultazione degli elenchi pubblici di cui al sito *internet* INI-PEC. Anche in questo caso, a nulla sono valse le tesi fatte valere dalla società per sostenere la legittimità del proprio comportamento con le quali evidenziava, da un lato, la possibilità per l'utenza contattata di cancellarsi dalla *mailing list* utilizzando il *link* incluso nelle comunicazioni promozionali inviate; dall'altro, il carattere 'istituzionale' e non promozionale delle comunicazioni trasmesse. Con riferimento a tale ultimo profilo, secondo il Garante non vi era alcun dubbio che le *e-mail* avessero una natura promozionale in quanto favorivano le attività dell'associazione connesse alla figura di "consulente reputazionale" e dunque dovevano essere inviate nel rispetto delle regole previste dalla normativa privacy e dalle Linee guida del Garante in materia di attività promozionale e contrasto allo spam. Quanto, poi, alla possibilità di richiedere la rimozione dei propri dati, l'Autorità ha precisato ancora una volta che l'inserimento nelle *e-mail* indesiderate di un *link* per la cancellazione dalla *mailing list* non è sufficiente per fa venir meno l'illiceità del trattamento poiché il consenso richiesto deve essere legittimamente acquisito anteriormente all'invio delle comunicazioni promozionali.

Di conseguenza, il Garante ha vietato alla società l'ulteriore illecito trattamento dei dati dei professionisti e ne ha prescritto la cancellazione, riservandosi di valutare eventuali profili sanzionatori.

In conclusione, tre gli aspetti da tenere in considerazione per quanto concerne l'attività di *marketing* utilizzando dati reperibili su *social spam* o *pec* contenuti in registri pubblici:

- la presenza di dati in elenchi pubblici o reperibili su piattaforme *social* non autorizza in alcun modo il trattamento dei relativi dati per scopi differenti da quelli previsti dalla pubblicazione;
- per poter inviare materiale promozionale (dove promozionale ha una accezione estremamente allargata) è necessario aver acquisito preventivamente il consenso dell'interessato
- il consenso dell'interessato deve essere stato rilasciato in maniera libera, specifica ed informata: non può, ad esempio, ritenersi idoneo un unico consenso prestato per finalità di natura differente.

93 Cfr. Parere 15/2011 del 13 luglio 2011: https://www.garanteprivacy.it/documents/10160/2052659/1895739.pdf/8fde4893-ed9a-4217-a669-7925aa05a0d6?version=1.0.

94 Cfr. Provvedimento n. 52 del 1° febbraio 2018: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/dweb/7810723.

2.6 Utilizzo di pop-up con consenso obbligato

Il Garante ha vietato a una società che offre servizi di comparazione sul proprio sito *web* (mutui, assicurazioni, luce, gas, telefonia) il trattamento, per finalità di *marketing* e di vendita ad altre aziende, dei dati raccolti attraverso un *pop-up* (finestra che si apre sopra la schermata attiva durante la navigazione in siti *web*, usata soprattutto per annunci pubblicitari) senza il necessario consenso degli utenti[95].

Il *pop-u*p in tal caso non permetteva l'accesso ai servizi offerti se l'utente non accettava, con un consenso unico e obbligato, il trattamento dei dati per diverse finalità (fra le quali il *marketing* o la comunicazione dei dati a terzi). In caso di compilazione delle caselle di testo, ma di mancata spunta del consenso, infatti, il sito non acquisiva i dati inseriti e non consentiva di procedere con la richiesta. Pertanto, ancorché l'informativa facesse riferimento alle diverse finalità di trattamento di dati, non si consentiva agli utenti di effettuare una scelta specifica e differenziata per ciascuna diversa finalità di trattamento come ribadito dalla *Linee guida in materia di attività promozionale e contrasto allo spam* del 4 luglio 2013.

2.7 Giurisprudenza vs Garante Privacy

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[96] ha stabilito che il consenso è validamente prestato solo se sia espresso liberamente e in modo specifico con riferimento ad 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 e

95 Relazione annuale dell'Autorità della Protezione dai Dati 2018, pag. 112 https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2018.pdf/e5bc382b-c5e9-b41b-b0d8-882f0904e546?version=1.0

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

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[97].

In particolare, il Tribunale ha accolto il ricorso presentato dall'operatore telefonico avverso il provvedimento emesso dal Garante[98], con cui veniva indicata come non conforme alla normativa l'attività dell'operatore telefonico, che aveva estratto dal proprio CMR i numeri di telefono dei propri clienti (vecchi e nuovi) per l'invio di campagne pubblicitarie via *sms* finalizzate alla raccolta del consenso 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.

97 Tribunale di Roma, sentenza 10789 del 1° agosto 2019

98 Provvedimento n. 437 del 27 ottobre 2016 del Garante

CAPITOLO 4 di Micaela Barbotti, Josephine Romano e Roberto Tirone

Modalità pratiche per l'adozione di un Modello Organizzativo e per le attività dell'OdV

SOMMARIO: 1. Adozione iniziale e aggiornamento del Modello – 2. Modalità di diffusione e comunicazione del Modello – 3. Individuazione dell'Odv – 4. Insediamento dell'OdV – modalità di azione e operative – 5. La gestione delle segnalazioni – 5.1 I canali di segnalazione – 5.2 Coordinamento con i canali di Gruppo – 5.3 Riservatezza, anonimato e privacy – 5.4 Sanzioni – 6. Rapporto dell'Organismo di Vigilanza con gli organi di controllo

1. Adozione iniziale e aggiornamento del Modello

Secondo il Dlgs. 231/2001, l'adozione e la corretta applicazione del Modello può rappresentare un esimente della responsabilità dell'ente in caso di commissione di reato da parte di soggetti apicali o subordinati.

Il D.Lgs. 231/2001 non disciplina approfonditamente le caratteristiche del modello di organizzazione, ma si limita a dettare alcuni principi di ordine generale. Spesso vengono in aiuto le linee guida di Confindustria e/o di altri enti di rilievo ma certamente i modelli non possono essere redatti in maniera semplificata o meramente acquisendo un format predisposto da terzi. I redattori dei modelli, dunque, devono necessariamente effettuare una previa analisi dell'organizzazione dello specifico ente al quale il modello si riferisce, individuando i processi sensibili sotto il profilo del rischio di commissione di reati rilevanti.

In primis, dunque, i redattori dei modelli prendono in considerazione le procedure, i presidi e le sanzioni già esistenti all'interno dell'ente, finalizzati alla prevenzione dei reati di cui al DLGS 231/2001.

Ad esito di tale analisi, si potranno, poi, individuare gli ulteriori presidi o le modifiche alle procedure esistenti che permettano una migliore prevenzione dei reati.

Il Modello viene redatto, ormai per dottrina e prassi consolidata, dividendolo in due parti: parte generale e parte speciale.

La parte generale descrive le finalità del Modello secondo il D.Lgs. 231/2001 e l'organizzazione dell'ente, con particolare attenzione alla struttura dell'ente e le aree di attività.

La parte speciale descrive nello specifico i meccanismi di prevenzione e reazione dell'ente ai rischi di commissione di reati rilevanti ai fini del D.Lgs. 231/2001.

Una volta redatto il Modello, esso deve essere approvato ed adottato da parte dell'Ente. L'organo preposto a ciò è il Consiglio di Amministrazione, attraverso una propria delibera.

È di centrale importanza che all'approvazione e adozione del modello abbia data certa, affinché vi sia sicurezza sul contenuto e sulla data di adozione. A tal fine, si può ricorrere all'intervento di un Notaio, ovvero procedere con uno scambio via *pec* del Modello tra due indirizzi di posta elettronica certificata.

Contestualmente all'adozione del modello, normalmente viene anche istituito l'Organismo di Vigilanza, con l'indicazione dei membri, durata dell'incarico, compenso e, se del caso, l'individuazione del Presidente.

2. Modalità di diffusione e comunicazione del Modello

Affinché possa dirsi efficacemente adottato, il Modello deve essere oggetto di comunicazione tempestiva, accurata, continua e accessibile. A tal fine, può risultare utile pubblicare il Modello nel sistema *intranet* dell'ente, ovvero inviato per *e-mail*. Potrebbe essere opportuno anche esporre copie cartacee del Modello negli spazi comuni.

Oltre che internamente, il Modello deve essere posto a conoscenza anche ai soggetti esterni all'ente, in quanto quest'ultimo potrebbe essere ritenuti responsabile anche per azioni di tali soggetti. Di conseguenza, deve essere previsto che i contratti tra l'ente e soggetti terzi, quali ad esempio appaltatori o fornitori, prevedevano clausole standard, in forza delle quali il soggetto terzo è messo a conoscenza dell'esistenza del Modello ed è obbligato ad uniformarsi ad esso, pena la risoluzione del contratto stesso.

Oltre ad attività di informazione, l'ente deve porre in essere anche la formazione dei propri dipendenti. Per essere efficace, questa deve riguardare il Modello, il D.lgs. 231/2001 e il Codice etico. Inoltre, tale attività deve tenere conto delle specifiche mansioni dei soggetti, al fine di avere a oggetto i rischi ad essere di solito relati. Infine, la partecipazione alla formazione deve essere documentata attraverso l'apposizione della firma di presenza e l'inserimento in una banca dati dei nominativi dei presenti. In caso di assenze ingiustificate, il Modello deve provvedere l'applicazione di sanzioni disciplinari.

3. Individuazione dell'Odv

Il D. Lgs. n. 231/2001 non fornisce indicazioni in merito alla composizione dell'OdV. Utili spunti sono stati forniti dalla giurisprudenza e dalle principali associazioni di categoria, in particolare dalle Linee Guida predisposte da Confindustria.

L'ente potrà optare per una composizione monocratica o collegiale (con componenti interni ed esterni all'ente). La scelta è opportuno che venga effettuata sulla base delle dimensioni dell'ente, della sua struttura organizzativa, delle caratteristiche aziendali e del settore di appartenenza. In linea di massima, la composizione collegiale sarà da preferire per le imprese medio-grandi; negli altri casi, sarà invece possibile optare per un organismo monocratico.

Le imprese di piccole dimensioni hanno facoltà di affidare in compiti di OdV all'organo dirigente (art. 6, comma 4 D. Lgs. 231/2001). Con l'espressione "organo dirigente", la dottrina ritiene debba intendersi l'organo amministrativo; quanto invece alla qualifica di impresa di "piccole dimensioni", in mancanza di specificazioni al riguardo, vengono utilizzati diversi riferimenti (ad esempio i parametri comunitari, l'art. 30, comma VI, del Testo Unico Sicurezza, l'ammontare del capitale sociale); certo è che le Linee Guida di Confindustria raccomandano, in queste ipotesi, che l'organo dirigente si avvalga, per l'espletamento dei compiti di OdV, di professionisti esterni cui affidare l'incarico di effettuare verifiche periodiche sull'efficacia e sul rispetto del Modello.

Le altre imprese possono avvalersi, per l'espletamento delle funzioni tipiche di OdV, degli organi di controllo interni e, in particolare, se esistenti, del Comitato Controllo e Rischi e della funzione di *Internal Auditing*.

Il comma 4 bis dell'art. 6 del D. Lgs. 231/2001 consente poi di attribuire le funzioni di OdV al Collegio Sindacale. In questo caso, le Linee Guida di Confindustria suggeriscono di verificare attentamente l'effettiva sussistenza, in capo ai componenti del Collegio Sindacale, dei requisiti di professionalità richiesti per l'espletamento delle funzioni di OdV e di valutare attentamente che la duplice funzione svolta dal Collegio Sindacale non possa comportare possibili conflitti di interesse o, addirittura, carenze nei sistemi di controllo. Sempre le Linee Guida raccomandano, inoltre, che il Collegio si riunisca con frequenza maggiore rispetto ai 90 giorni previsti dall'art. 2404 c.c. e ciò al fine di garantire la continuità di azione.

Qualunque sia la scelta dell'ente, certamente dovrà garantirsi la sussistenza in capo all'OdV dei requisiti specifici richiesti dal D Lgs. 231/2001: autonomia e indipendenza, professionalità, continuità.

Il primo dei tre requisiti è fondamentale per guidare la scelta dell'eventuale componente interno dell'OdV. Argomentando proprio da questo, si ritengono incompatibili il Responsabile Servizio Prevenzione e Protezione (RSPP) il delegato ambientale, il *Data Protection Officer* (DPO), ma anche soggetti apicali interni con autonomia decisionale nell'ambito dei processi sensibili.

Per quanto concerne le modalità di nomina, la durata, le ipotesi di cessazione della carica è opportuno che siano disciplinate nel Modello Organizzativo. Particolarmente delicata la questione dell'applicabilità all'OdV dell'istituto della prorogatio prevista per il Collegio sindacale dall'art. 2400

c.c. Trattandosi di una norma dettata specificamente per il Collegio Sindacale non sembra validamente sostenibile la sua applicabilità in via analogica anche all'OdV. La possibilità, quindi, per l'OdV di proseguire nell'incarico anche successivamente alla scadenza dell'incarico, dovrà essere espressamente prevista nel Modello Organizzativo o nell'atto di nomina; in difetto, l'OdV cesserà dall'incarico, con tutte le conseguenze che potrebbero derivare ai danni dell'ente qualora non si procedesse tempestivamente alla nuova nomina.

4. Insediamento dell'OdV – modalità di azione e operative

La definizione e individuazione degli aspetti attinenti al funzionamento dell'OdV è utile ed opportuno che siano rimesse ad un Regolamento di funzionamento interno da adottarsi esclusivamente da parte dell'OdV, affinché sia garantita l'assoluta indipendenza dello stesso. Nel Regolamento dovranno, inoltre, essere disciplinate le modalità di conservazione ed archiviazione di ogni informazione (e segnalazione) ricevuta e dei verbali delle riunioni.

L'OdV svolge le proprie verifiche circa il rispetto del Modello Organizzativo in base a una pianificazione, solitamente annuale, dei controlli da effettuare (piano di *audit*), anche se possono risultare efficaci verifiche non preannunciate o programmate.

Per poter espletare adeguatamente ed efficacemente l'attività di vigilanza, l'OdV: ha libero accesso a tutte le aree aziendali, può avvalersi non solo dell'ausilio di tutte le strutture dell'ente ma altresì di consulenti esterni, ha a disposizione una adeguata dotazione di risorse finanziarie (*budget*) della quale potrà disporre per ogni esigenza necessaria al corretto svolgimento dei suoi compiti.

Per consentire all'OdV di svolgere le proprie funzioni, fondamentale è garantire un sistema di flussi informativi efficaci. È opportuno che il Modello disciplini il meccanismo dei flussi informativi verso l'OdV, distinguendo tra flussi informativi da effettuarsi al verificarsi di particolari eventi e flussi informativi periodici. È utile, inoltre, che anche l'OdV dia indicazioni precise dei flussi di cui chiede di essere destinatario (a titolo esemplificativo i report redatti dai responsabili delle diverse funzioni aziendali nell'ambito della loro attività, ogni operazione particolarmente significativa da svolgersi nell'ambito dei "processi sensibili", modifiche dell'assetto organizzativo).

Analogamente l'OdV deve garantire un adeguato sistema di *reporting* verso i vertici aziendali, su base continuativa, così da mantenere uno stretto contatto con i vertici dell'ente, ma anche su base periodica; sotto questo ultimo aspetto, fondamentale sarà la relazione annuale dell'OdV avente a oggetto i risultati della propria attività con l'indicazione, tra l'altro dei controlli effettuati e l'esito degli stessi, delle verifiche specifiche e l'esito delle stesse, dell'eventuale neces-

sità o opportunità di aggiornamento della mappatura dei processi sensibili e del Modello e delle eventuali criticità riscontrate con suggerimenti e spunti per il miglioramento.

5. La gestione delle segnalazioni

5.1 I canali di segnalazione

Prassi ormai consolidata vede l'Organismo di Vigilanza quale naturale destinatario delle segnalazioni di mancato rispetto del Modello Organizzativo o di condotte che possano integrare fattispecie di reato rilevanti ai fini del D.Lgs. 231/2001. I Modelli di organizzazione, gestione e controllo sono infatti soliti prevedere specifici canali dedicati alle segnalazioni dirette all'Organismo di Vigilanza: **casella di posta elettronica** dedicata e cassetta per le **segnalazioni cartacee**, generalmente utilizzata nelle realtà produttive.

Tuttavia, il comma 2-bis dell'art. 6 D.Lgs. 231/2001, introdotto dalla tanto citata L. 30 novembre 2017, n. 179 sul sistema del cd. *whistleblowing*, non prevede che il destinatario delle segnalazioni debba essere necessariamente l'Organismo di Vigilanza, lasciando pertanto le organizzazioni libere di adottare soluzioni differenti, quali l'utilizzo di **piattaforme** informatiche gestite da ***provider* esterni**; tramite tali piattaforme le segnalazioni vengono generalmente indirizzate a consulenti o a specifiche funzioni aziendali o di gruppo, anche dislocate al di fuori del territorio italiano. Lo strumento, se da un lato parrebbe garantire maggiore riservatezza dell'identità del segnalante, così come richiesto dalla L. 179/2017, dall'altro potrebbe rendere difficile l'immediata conoscenza dell'Organismo di Vigilanza di **tutte** le segnalazioni di propria competenza: le società dovranno pertanto mettere l'Organismo nelle condizioni di poter espletare efficacemente i propri compiti di vigilanza sul rispetto del Modello Organizzativo, predisponendo tempestivi ed efficaci meccanismi di **reportistica** tra il destinatario delle segnalazioni veicolate tramite la piattaforma e lo stesso OdV.

5.2 Coordinamento con i canali di Gruppo

Alla luce di quanto sopra, il processo di gestione della segnalazione richiede senz'altro un'adeguata regolamentazione, ancor più necessaria nell'ambito di grandi gruppi societari, anche multinazionali, generalmente caratterizzati da una stratificata struttura societaria e da un'articolata rete di canali di comunicazione/segnalazione, che potrebbero nascere anche dall'esigenza di adeguarsi a ulteriori specifiche normative di settore, nazionali e internazionali.

In tali contesti, sarà quindi necessario che il sistema di *whistleblowing* sia armonicamente inserito tra i preesistenti canali di comunicazione attraverso lo sviluppo di **soluzioni costruite "su misura"**, in base alla realtà della singola azienda e del singolo gruppo.

5.3 Riservatezza, anonimato e privacy

Come già anticipato, le modalità di trasmissione delle segnalazioni devono garantire la massima **riservatezza dell'identità** dei segnalanti.

Inoltre, al fine di poter diffondere una positiva cultura del *whistleblowing* e incoraggiare le segnalazioni, si ritiene opportuno che le relative procedure prevedano anche la possibilità di effettuare segnalazioni **anonime**. Tale possibilità è importante per due ragioni: la prima è che nel contesto culturale odierno gli individui sono restii ad effettuare segnalazioni; la seconda riguarda la funzione della segnalazione che è di allerta e non di denuncia, il che implica che l'organizzazione sia tenuta ad approfondire, accertare e verificare i fatti, a prescindere dalla conoscenza dell'identità del segnalante.

Infine, i **dati personali**, ivi inclusi quelli sensibili, dei soggetti segnalanti, nonché di altri individui eventualmente coinvolti, devono essere correttamente gestiti, in conformità con la normativa applicabile. In particolare, è opportuno che le operazioni di trattamento siano affidate a soggetti specificamente formati sulle procedure aziendali di *whistleblowing* e sulle modalità di tutela della riservatezza dei soggetti coinvolti e delle informazioni contenute nelle segnalazioni.

5.4 Sanzioni

Per costruire un sistema di *whistleblowing* efficace è opportuno che le relative procedure prevedano **specifiche sanzioni disciplinari** non solo per il soggetto segnalato, nell'ipotesi in cui i fatti siano confermati, ma anche per tutti coloro che agiscano in violazione delle medesime procedure.

A tale riguardo, le Linee Guida di *Transparency International* del 2016 precisano le necessaria previsione di sanzioni (*i*) nel caso in cui il segnalato sia ritenuto responsabile a seguito dell'attività di indagine svolta dall'organo destinatario della segnalazione, (*ii*) in caso di abusi da parte del segnalante, (*iii*) in ipotesi di comportamenti ritorsivi o discriminatori nei confronti del segnalante, (*iv*) nel caso in cui l'organismo preposto a ricevere la segnalazione non verifichi quanto segnalato e, infine, (*v*) in caso di violazione degli obblighi di riservatezza.

Tali sanzioni, da applicarsi a dirigenti e dipendenti in conformità allo Statuto dei lavoratori (Legge n. 300/1970) e al CCNL concretamente applicabile, dovrebbero essere dirette anche ai terzi, vale a dire a tutti quei soggetti che operano all'interno o per conto dell'organizzazione (come ad esempio collaboratori, consulenti, lavoratori somministrati, *partner* commerciali e i fornitori), laddove gli stessi abbiamo la possibilità di accedere al sistema di *whistleblowing* aziendale; per tale motivo le procedure di *whistleblowing* dovrebbero prevedere l'inserimento di specifiche clausole contrattuali che sanzionino (con diffida, applicazione di penali, risoluzione del contratto) il mancato rispetto delle procedure stesse da parte di soggetti terzi.

6. Rapporto dell'Organismo di Vigilanza con gli organi di controllo

Nello svolgimento delle proprie attività di monitoraggio, l'Organismo è chiamato a relazionarsi periodicamente con gli organi societari di controllo (primi fra tutti, Collegio Sindacale e Revisori), nei cui confronti è opportuno instaurare un efficace ed effettivo rapporto di **collaborazione e cooperazione**. Ciò al fine di condividere gli esiti delle verifiche di rispettiva competenza in ottica di sinergia ed efficacia del sistema aziendale dei controlli, tramite **incontri** dedicati periodici e la partecipazione dell'Organismo, ove quest'ultimo lo ritenga necessario e ne faccia richiesta, alle riunioni degli organi di controllo in cui sia all'ordine del giorno la discussione di argomenti di interesse.

È importante che di tali incontri venga tenuta traccia mediante puntuale **verbalizzazione**.

Si auspica inoltre che l'Organismo di Vigilanza sia destinatario (e mittente) di **flussi informativi** sia periodici, riguardanti gli esiti delle verifiche svolte soprattutto a ridosso dell'approvazione del bilancio d'esercizio, sia **occasionali**, aventi a oggetto anomalie o atipicità riscontrate nell'espletamento delle attività di competenza. È opportuno che il Modello Organizzativo preveda espressamente tali flussi informativi, nonché il necessario coinvolgimento degli organi di controllo (in particolare, del Collegio Sindacale) in caso di presunte violazione del Modello o della commissione di illeciti da parte dell'organo amministrativo.

CAPITOLO 5 di Deborah Bolco e Pietro Orzalesi

Operazioni di acquisizione. Tematiche di compliance nel processo e nella contrattualistica

SOMMARIO: 1. Incidenza della *privacy* nella gestione del processo: la fase preparatoria – 2. Aspetti di rilievo dalla attività di *due diligence* alla negoziazione dell'accordo – 2.1 L'attività di due diligence: *buy side* o *sell side*, una questione di prospettiva – 2.2 La trasmissione delle *liabilities* – 2.3 Temi oggetto di analisi: *privacy*, *anticorruption* e *compliance* 231 – 3. La negoziazione dello SPA – 4. Adempimenti dell'acquirente post acquisizione e possibili temi di attenzione

1. Incidenza della privacy nella gestione del processo: la fase preparatoria

La *due diligence*, come noto, è finalizzata ad ottenere una "fotografia" della *target* che si intende acquisire (sia essa una società o un'azienda), per quanto concerne, *inter alia*, gli aspetti regolamentari, legali, fiscali e finanziari, contrattuali e di *compliance*, al fine di consentire al *buyer* di avere una visione globale della *target* e del suo *business*, dei vari *assets* e delle *liabilities*. Più nel dettaglio, dopo aver esaminato le suddette informazioni, il *buyer* otterrà un quadro conoscitivo che gli consentirà di prendere **una decisione "informata" in merito all'effettiva convenienza strategica dell'operazione**: sostanzialmente, dovrà decidere se portare a termine il *deal*, quanto valutare la *target*, il prezzo di acquisizione e le protezioni contrattuali (condizioni sospensive, manleve, etc.) da ottenere dal venditore. Insomma, lo scopo della *due diligence* è di ridurre l'asimmetria informativa tra chi vende e chi compra, tenendo conto che, da un lato, chi vende conosce il proprio *business*, e sarà ovviamente intenzionato a mettere in risalto i propri punti di forza; dall'altro lato, chi si appresta ad assumere il controllo di una nuova realtà deve essere sicuro di avere fatto una scelta corretta.

Alla luce di quanto sopra, normalmente accade che le parti si accordino affinché il venditore metta a disposizione una serie di documenti, tutti preventivamente concordati ed elencati in una *check list* (variabile a seconda del settore commerciale in cui si opera), dai quali emergeranno, *inter alia*, informazioni:

- sulla struttura di *governance* della *target*;
- sulla sussistenza di eventuali contenziosi;

- sui rapporti contrattuali;
- sugli aspetti finanziari e contabili;
- sulla compliance della target alle varie legislazioni di settore (i.e. *privacy*, *antitrust*, 231/01, ecc.).

Dal punto di vista della *data protection* i temi in gioco in relazione alla fase preparatoria sono molteplici. Nel dettaglio:

› **La comunicazione di dati** è un trattamento (art. 4 Regolamento UE 2016/679 "GDPR"). Qual è la base giuridica di tale trattamento? Pare possibile giustificare il trasferimento ai sensi dell'art. 6.1 (f) del GDPR sulla base del legittimo interesse, tanto della società *target* che del potenziale acquirente. È, in particolare, evidente l'interesse di entrambi a, rispettivamente, dare e avere accesso a dati personali, quali in particolare quelli dei dipendenti, nella misura in cui questi siano necessari a consentire alle parti di comprendere rischi e opportunità dell'operazione. Si pensi ad esempio al caso di controversie giuslavoristiche in atto o minacciate, che possono comportare il rischio dell'insorgenza di passività anche ingenti a carico della *target* (e quindi dell'acquirente nel caso di perfezionamento dell'operazione).

  D'altro canto, qualunque operazione di trattamento, anche se in ipotesi lecita ai sensi dell'art. 6 GDPR, deve comunque essere rispettosa dei principi generali di cui all'art. 5, tra cui di particolare rilievo è il (troppo spesso trascurato) principio di minimizzazione del trattamento di cui alla lettera c del richiamato articolo. Questo principio pretende che il trattamento sia pertinente e limitato a quanto strettamente necessario rispetto alle finalità perseguite. A mente dunque di questo principio, tornando all'esempio del trasferimento di dati personali nel contesto di un'operazione di acquisizione, se l'acquirente potenziale chieda di avere accesso a informazioni relative agli stipendi dei dipendenti, tale richiesta si può ritenere giustificata in base al legittimo interesse; allo stesso tempo, però, il principio di minimizzazione verosimilmente richiederà che tali informazioni siano fornite in forma anonimizzata, con la sola eccezione tutt'al più di quei *key employees* per cui, oltre al dato di stipendio, anche l'individuazione specifica del soggetto interessato può essere rilevante e può dunque trovare giustificazione nel legittimo interesse delle parti dell'operazione.

  Il *due diligence report* e l'*executive summary* dovranno, naturalmente, essere ripuliti dai dati personali.

› **Nomine**. Nella fase di *due diligence*, è inoltre bene che le parti coinvolte nella transazione e, in particolare, i venditori, siano consapevoli che eventuali rischi di *data breach* possono sussistere, tenendo conto dell'elevato quantitativo di dati (i.e. dati degli impiegati, clienti, contraenti, fornitori, partner commerciali della *target*, ecc.) che sono oggetto di *disclosure* all'acquirente e suscettibili di essere condivisi con avvocati, consulenti, banche, assicurazioni per portare a termine

l'acquisizione: conseguentemente, opportune cautele dovranno essere adottate.

In particolare, è opportuno che le parti inseriscano nell'ambito del *non disclosure agreement* o accordo di riservatezza che solitamente viene sottoscritto prima della successiva fase di *due diligence*, una clausola *ad hoc* attraverso la quale, in aggiunta al riserbo sul contenuto e sull'esistenza delle trattative o su qualunque informazione riservata scambiata, il *buyer* sia nominato responsabile del trattamento e si impegni a tutti gli obblighi già previsti dal GDPR e, in particolare, a non divulgare i dati per scopi estranei allo svolgimento e conclusione delle trattative e a distruggerli in caso di mancata conclusione del *deal*. Tale impegno dovrebbe estendersi anche con riguardo alle attività dei consulenti coinvolti nell'attività di *due diligence* (avvocati, fiscalisti etc).

› VDR vs servizi di *cloud storage* (eg: *drop box*). Che la condivisione dei documenti sia la base di ogni *due diligence* è oltremodo noto. Diventa, tuttavia, assolutamente necessario controllare in modo dettagliato quali informazioni vengono condivise e con chi e a questo riguardo assume una importanza fondamentale lo strumento utilizzato allo scopo, che deve poter garantire una sicurezza senza falle.

La *Data Room* non richiede l'installazione di alcun *software*. Non è dunque legata a una specifica postazione di lavoro e offre, al contrario, il vantaggio della mobilità. È possibile monitorare l'attività di scambio di documenti della *due diligence* anche in movimento su *smartphone* o *tablet*, con lo stesso livello di sicurezza.

Di contro, sistemi di *cloud storage* come *Dropbox* hanno spesso dimostrato i loro limiti. Nel 2016, ad esempio, gli *hacker* sono stati in grado di ottenere decine di milioni di ID di accesso a *Dropbox* grazie ad una falla di sicurezza conosciuta dal 2012.

2. Aspetti di rilievo dalla attività di *due diligence* alla negoziazione dell'accordo

2.1 L'attività di due diligence: buy side o sell side, una questione di prospettiva

Entrando nel merito dell'operazione (ed una volta sottoscritti gli accordi preliminari quali LoI o MoU) un passaggio quasi obbligato è quello dello svolgimento della *due diligence*.

Al riguardo, le prospettive di acquirente e venditore sono necessariamente contrapposte: da un lato, il venditore avrà interesse a presentare il *target* con un sostanziale allineamento alle tematiche di *compliance* per evitare che una difformità possa incrementare le garanzie richieste (e di cui si dirà infra) o, perfino, costituire un *deal breaker*. Dall'altro lato, l'acquirente avrà la necessità di acquisire in poco tempo una visione della situazione di *compliance* normativa per potere

capire i rischi sottesi al *deal*, valutare le opportune garanzie e – ove implementabili – i costi di eventuale *remediation*. Per l'acquirente, inoltre, potrebbe essere opportuno capire lo stato di adozione di misure in tali ambiti per valutare gli eventuali costi di allineamento post deal ai propri modelli e sistemi gestionali e di controllo.

Va altresì tenuto presente che, soprattutto per i soggetti acquirenti facenti parte di gruppi multinazionali, la sensibilità verso questi temi è diventata materiale e l'emersione di alcune criticità (soprattutto nelle aree *anticorruption* e/o *antibribery*) sono dei veri e propri *deal breaker*, in grado di far cessare le trattative.

2.2 La trasmissione delle liabilities

Le ragioni di una simile sensibilità devono essere rintracciate, oltre che nel rischio di immagine per l'acquirente ed il suo gruppo, anche per i meccanismi giuridici di successione nelle responsabilità economiche e patrimoniali degli illeciti di compliance.

A questo proposito, occorre distinguere tra c.d. *share deal* e *asset deal*. Nel primo caso, ferma la natura personale della responsabilità penale dell'individuo autore materiale del reato / illecito, occorre tenere conto delle conseguenze sanzionatorie (anche sotto forma di misure interdittive) che possono colpire l'ente e che avrebbero quindi un impatto diretto sul patrimonio della società che l'acquirente avrebbe appena acquistato. Parimenti, anche nel caso di transazioni che avvengono sotto forma di cessione o conferimento di azienda, o anche nel caso di scissioni o fusioni, le discipline specifiche (per citare un riferimento, gli articoli 29-33 del D.Lgs. n. 231/2001) prevedono una trasmissione delle responsabilità patrimoniali anche in capo al beneficiario/cessionario.

È quindi evidente che tali temi rivestono una importanza notevole per l'acquirente; sensibilità che deve essere valutata sia in termini di rischi (noti o latenti) che di costi di adeguamento normativo *post deal*.

2.3 Temi oggetto di analisi: privacy, anticorruption e compliance 231

Venendo alle materie che sono più di frequente oggetto di analisi, esse sono trasversalmente tutte quelle oggetto di trattazione ai Tavoli delle *Corporate Compliance Round Tables*; si tratta, infatti, di:

- trattamento dei dati personali e *privacy*, anche alla luce del GDPR;
- *Anticorruption* e *Antibribery*, che nel nostro ordinamento trovano una disciplina nell'ambito dei Modelli organizzativi adottati ai sensi del D.Lgs. n. 231/2001, anche se non esclusivamente per tale fine;
- rispetto delle disposizioni in materia della tutela della concorrenza e del mercato;
- eventuali normative settoriali di carattere regolamentare specifiche al *business* della *target*.

Il tutto ovviamente al netto delle verifiche che saranno condotte sugli aspetti HR, HSE o più in generale societari legati al caso di specie e che non tocca il tema della corporate compliance invece di carattere trasversale e generico.

Uno degli aspetti più delicati in merito alle verifiche che saranno condotte dall'acquirente e dai suoi consulenti riguarda senza dubbio il livello di approfondimento delle verifiche. È, infatti, evidente che in alcuni ambiti – *in primis* il Modello organizzativo adottato ai sensi del D. Lgs. 231/2001 – non sarà possibile procedere a una ri-valutazione dell'intero processo di *risk assessment* svolto. Sarà però senza dubbio possibile (e consigliabile) verificare con quale metodologia e livello di dettaglio questo sia stato fatto, quale sia l'aggiornamento normativo ed organizzativo del documento e indubbiamente da consigliare una lettura dei verbali delle riunioni dell'Organismo di Vigilanza al fine di verificare la presenza di rilievi e avere un'idea della qualità dell'operato dei suoi membri.

3. La negoziazione dello SPA

Una volta ultimata la fase di analisi e approfondimento, le parti potranno concordare un'apposita disciplina delle materie di *corporate compliance* nell'ambito dei contratti che regoleranno la transazione (*Investment Agreement*, SPA, *Asset Purchase Agreement*).

A questo proposito, le risultanze delle precedenti fasi di analisi potranno servire a:

- determinare delle attività o adempimenti che dovranno essere posti in atto e/o verificarsi prima del *Closing* (c.d. *condition precedent*): queste potranno consistere per esempio nella adozione di programmi di *corporate compliance*, nella revisione di documenti e/o processi;
- definire l'ambito delle dichiarazioni e garanzie che saranno rese dal venditore all'acquirente (c.d. *representations & warranties*). Al riguardo, queste potranno eventualmente essere qualificate da limitazioni di conoscenza del venditore e/o del management della target (c.d. *Seller's best knowledge qualifier*), soprattutto per quanto concerne l'eventuale (avvenuto) verificarsi di fatti o circostanze dai quali possa discendere una responsabilità della *target* e che non siano invece noti ai venditori;
- offrire indicazioni in relazione all'ammontare di eventuali garanzie collegate agli obblighi di indennizzo (sotto forma di fideiussioni, *escrow* o *hold back*), così come identificare il limite massimo di responsabilità (cap) ed eventuali franchigie, nonché la durata dei correlati obblighi di indennizzo (normalmente fino a prescrizione e non soggetti a limitazioni almeno per quanto riguarda l'anticorruzione).

4. Adempimenti dell'acquirente post acquisizione e possibili temi di attenzione

Anche a questo riguardo vi sono diversi temi da considerare. Nel dettaglio:

› Innanzitutto si segnala un provvedimento del Garante abbastanza datato – *ante* GDPR – ma attuale nei contenuti *mutatis mutandis*: si tratta delle "Prescrizioni in materia di operazioni di fusione e scissione fra società" - 8 aprile 2009: doc. *web* n. 1609999: il Garante prescrive quale misura opportuna alle società coinvolte in operazioni di scissione e fusione di fornire agli interessati i necessari aggiornamenti rispetto all´informativa resa dalla società scissa e dalle società partecipanti alla fusione e, tra essi, in particolare, la nuova denominazione del titolare del trattamento e gli estremi identificativi dell´eventuale nuovo responsabile presso il quale esercitare il diritto di accesso ai dati personali, secondo le seguenti modalità:

   a. attraverso il sito *web* delle società interessate dalle operazioni di scissione e fusione, in corrispondenza del loro verificarsi;

   b. con comunicazione individualizzata agli interessati in occasione della prima circostanza utile di contatto, anche per altre finalità.

› Ad acquisizione avvenuta occorrerà, inoltre, procedere a una attività di *gap analysis* del sistema di gestione *privacy* della *target* allo scopo di identificare con immediatezza situazioni inadeguate e *gap* organizzativi, individuare delle aree di rischio e poter pianificare un piano di intervento. Da tenere sotto la massima attenzione:

- il registro dei trattamenti, documento fondamentale per la conformità alla normativa GDPR, vero punto di partenza dell'analisi e della revisione dei processi di trattamento posti in essere da titolari e responsabili, che non a caso è anche il primo documento che viene sicuramente richiesto in caso di attività ispettiva da parte del Garante tramite nucleo speciale *privacy* della Guardia di Finanza.

Preliminare alla valutazione dei rischi, alla loro analisi, alla scelta delle misure di sicurezza, alle loro revisioni, il registro è un documento indispensabile che viene redatto, con precisione ed attenzione, come documento di analisi iniziale dei processi interni. Sempre obbligatorio per le PA e per le aziende con oltre 250 dipendenti, il registro è sempre consigliato anche per chiunque effettui trattamento di dati personali di persone fisiche per scopi non privati. Il registro dei trattamenti sarà, dunque, molto utile per compiere una ricognizione preliminare delle attività di trattamento svolte dalla *target*; ove non fosse presente occorrerà provvedere alla sua redazione, aiutandosi magari, per una prima mappatura, con documenti eventualmente già presenti in azienda come il Documento Programmatico per la Sicurezza ("DPS"), obbligatorio fino al 2012;

- quei trattamenti, eventualmente condotti dalla *target*, che potrebbero richiedere un *Data Protection Impact Assessment* ("DPIA") a norma dell'art. 35 GDPR.

Prima del GDPR non c'era un'assunzione di responsabilità in prima persona del titolare del trattamento circa la possibilità di intraprendere trattamenti di dati personali potenzialmente rischiosi, dal momento che la relativa valutazione era rimessa al Garante *privacy.* Con il GDPR, invece, il titolare del trattamento deve in prima persona compiere una serie di riflessioni e approfondimenti che dovranno fondare la sua decisione finale circa la fattibilità o meno di determinati trattamenti di dati; e dal momento che di tali scelte il titolare, cioè l'azienda *target*, risponderà in prima persona, ad acquisizione avvenuta sarà consigliabile effettuare un'ulteriore delibazione per assicurarsi che il processo valutativo sia stato compiuto in modo corretto o se, invece, non siano richiesti dei correttivi.

CAPITOLO 5 di Alessandra Anselmi, Antonio Bana, Francesca Chiara Bevilacqua, Paola De Pascalis e Piero Magri

Le attività "cross-border" nella 231: come aiutare le aziende multinazionali a fronteggiare i rischi compliance

SOMMARIO: 1. L'organizzazione e l'esercizio "multinazionale" dell'attività di impresa e i riflessi sulla "*compliance* 231" – 2. Un antidoto alla "globalizzazione dei rischi di *compliance*": il modello "*cross-border*" come modello "integrato" – 3. Il dato normativo e giurisprudenziale – 3.1 (segue) applicabilità del D. Lgs. 231/01 al fenomeno del Gruppo – 3.2 (segue) normativa 231 e dimensione multinazionale del reato o dell'ente – 4. L'adozione di un modello organizzativo c.d. *cross-border* nell'elaborazione dottrinale e giurisprudenziale – 5. Caratteristiche del modello *cross-border* e suo *iter* di realizzazione – 6. L'Organismo di Vigilanza nell'ambito del gruppo multinazionale: quali soluzioni? – 7. Conclusioni

1. L'organizzazione e l'esercizio "multinazionale" dell'attività di impresa e i riflessi sulla "compliance 231"

Il processo di globalizzazione e la tendenza crescente delle imprese a sviluppare il proprio *business* in mercati geograficamente "lontani" – da tanti punti di vista - comportano – anche quanto ai profili di responsabilità penale/amministrativa ai sensi del D. Lgs. 231/01 e alla sua dimensione territoriale - la necessità di rispettare contestualmente regole proprie di ordinamenti diversi e, conseguentemente, di individuare strumenti di "*compliance* trasversale" per farvi fronte.

Le imprese, infatti, si ritrovano sovente a dover fronteggiare "rischi di *compliance*" ubiquitari, tipici dei Paesi in cui hanno la sede ma anche di quelli in cui, nello stesso tempo e con diverso impegno, si trovano ad operare e in cui hanno avuto occasione e opportunità di espansione.

La sfida non appare banale, laddove si tengano in debita considerazione le peculiarità legislative e regolamentari di ciascun ordinamento, dalle quali discende la necessità di rispettare principi e regole talvolta tanto distanti quanto lo è il contesto culturale e sociale.

Si pensi al fenomeno corruttivo, severamente represso in alcuni Paesi, ma ancora endemico, sicuramente tollerato e, in alcuni casi, "riconosciuto" in altri contesti geografici e socio culturali, ove le grandi organizzazioni multinazionali si trovano pure a coltivare interessi e a operare. La proliferazione di leggi e regolamenti a livello nazionale e internazionale, unito all'intensificarsi dei controlli da parte di autorità nazionali e sovranazionali e all'inasprimento delle sanzioni comminabili a fronte di situazioni di "non conformità", hanno determinato un aumento notevole della complessità del quadro normativo in cui le società operano, introducendo nuovi vincoli e responsabilità in capo alle stesse.

Non solo: le attività imprenditoriali multinazionali sperimentano sempre più spesso forme nuove anche in termini di organizzazione, con strutture e linee di riporto all'interno della singola società o del singolo gruppo molto articolate, oppure con una interazione – anche soltanto momentanea – di più società o gruppi. Si pensi ad esempio alle associazioni temporanee di imprese o ai consorzi, macro-aggregazioni che di frequente gestiscono importanti progetti in aree geografiche complesse.

Tutto ciò contribuisce a rendere ulteriormente impegnativa quanto indefettibile una declinazione della *compliance* che sappia oltrepassare le frontiere e le dinamiche organizzative, conservando la propria efficacia.

Ovviamente, la prospettiva che qui interessa è quella relativa alla responsabilità da reato ai sensi del D. Lgs. 231/01 e al modello organizzativo quale strumento di esclusione della stessa; in tal senso, ovviamente, nell'impossibilità di affrontare tutte le casistiche possibili, saranno prese in considerazione alcune precise ipotesi: (*i*) la **società italiana che operi anche all'estero**, (*ii*) l'**ente estero che operi in Italia**, in via diretta, tramite enti controllati oppure mere *branch*.

2. Un antidoto alla "globalizzazione dei rischi di compliance": il modello "cross-border" come modello "integrato"

È dunque da tale condizione di difficoltà per l'impresa "multinazionale" che nasce l'esigenza di individuare strumenti di *compliance* 231 che tengano conto, non solo dei rischi "domestici", ma anche di quelli internazionali e transnazionali, siano essi legati alla globalizzazione, o comunque derivanti dalla frammentazione dell'attività di impresa in più unità organizzative o giuridiche in sé distinte e anche diversamente localizzate dal punto di vista geografico. D'altronde, l'esigenza dei gruppi multinazionali di affrontare in modo integrato e coordinato i temi di *compliance*, al fine di assicurare la conformità normativa dei processi e dei comportamenti attraverso indirizzi e *standard* procedurali condivisi a livello di gruppo, va spesso conciliata con la specificità delle regole prescritte dalle singole legislazioni nazionali.

Ovviamente, lo strumento di gestione della *compliance* 231 per definizione - il modello di organizzazione, gestione e controllo – diviene lo strumento primario di *reductio ad unum* della complessità del quadro sopra rappresentato, in vista di una radicale esclusione di responsabilità: laddove il contesto di ope-

ratività dell'impresa si allarghi, ed assuma una dimensione multinazionale, con aumento e diversificazione dei rischi anche penali, anche il modello dovrà "allargare" la sua portata e le sue caratteristiche.

Molteplici sono le ragioni che impongono l'adozione di un modello di questo tipo, tra queste ricordiamo:

- il profilo reputazionale;
- l'approccio coerente alla realtà 231/01 "domestica";
- l'onere della prova ed una completa difesa processuale;
- la riduzione dei costi del contenzioso.

Ciò premesso, diviene indispensabile chiarire la cornice giuridica – normativa, giurisprudenziale e dottrinale – entro la quale si colloca la c.d. *compliance* 231 del gruppo multinazionale.

3. Il dato normativo e giurisprudenziale

La laconicità del D. Lgs. 231/2001 – o addirittura i silenzi – rispetto a molti profili che avrebbero certamente dovuto essere regolati – perché di portata evidente e rilevante in concreto - hanno costretto giurisprudenza e dottrina – nonché gli stessi esponenti d'impresa e le loro associazioni - a un importante esercizio interpretativo, ineludibile per gestire la congerie di problematiche afferenti alla realtà aziendale contemporanea, articolata e ormai sempre più spesso "*cross-border*".

Tra le questioni che hanno variamente impegnato giudici e interpreti a fronte delle lacune normative, una menzione particolare va al tema del "gruppo di Società": fenomeno frequentissimo nella realtà imprenditoriale, risulta infatti ignorato da un sistema di responsabilità da reato calibrato esclusivamente su un modello di società-isola non esaustivo rispetto al panorama societario attuale.

3.1 (segue) applicabilità del D. Lgs. 231/01 al fenomeno del Gruppo

Poiché, come detto, il *corpus* normativo di cui al decreto ha ignorato la prospettiva – tanto giuridicamente imprecisa quanto concreta nell'applicazione – dei gruppi di società, diverse incertezze ermeneutiche hanno consentito soluzioni anche tra loro contrastanti, oscillanti tra lo "scarico verso il basso"della responsabilità sanzionatoria della controllante sulla controllata e la risalita dalla controllata alla controllante. Parallelamente, si è posta anche la questione relativa alla "unicità" o meno dei modelli Organizzativi di cui agli artt. 6 e 7 del D. Lgs. 231/01 nei gruppi di imprese: sarebbe possibile, in estrema sostanza, predisporre un modello di organizzazione e di gestione da parte della capogruppo e applicarlo identicamente a tutte le società controllate? Devono invece essere adottati tanti modelli quante sono le società? Tale modello soddisferebbe quanto richiesto dalla normativa per consentire l'esenzione da responsabilità?

In dottrina, si è giunti a negare – in generale – l'identificazione del gruppo quale soggetto giuridico autonomo e sovraordinato, ben distinto dalle società in esso ricomprese, destinatario in via diretta delle disposizioni di cui al D. Lgs. 231/01: in ragione, sostanzialmente, del principio di piena autonomia di personalità giuridica dei singoli enti che lo costituiscono (d'altronde: quale obbligo di impedimento *ex* art. 40 co. 2° cp. sussisterebbe per la capogruppo? Molti sarebbero gli interrogativi, che naturalmente non è possibile affrontare in questa sede).

A ciò è conseguita la conclusione circa l'impossibilità di un unico modello valido per ogni componente del gruppo, anche in ragione del sempre più frequente richiamo della giurisprudenza al requisito di specificità del modello organizzativo.

La giurisprudenza si è invero progressivamente spesa sul tema dei gruppi societari, precisando via via le sue conclusioni.

Inizialmente, la tendenza interpretativa – della giurisprudenza di merito in particolare – era nel senso dell'estensione della responsabilità anche a livello "aggregato" in ragione della nozione di "interesse di gruppo", inteso – soprattutto – quale "distribuzione di utili". In definitiva, in caso di reato commesso dalla controllata, vi sarebbe anche per la controllante, e le altre società facenti parte del gruppo, un indiretto ma oggettivo vantaggio in termini di utilità economico - patrimoniale: ciò sarebbe di per sé sufficiente a soddisfare il criterio di imputazione dell'interesse/vantaggio di cui all'art. 5 D. Lgs. 231/01. Chiaro che, in quest'ottica, si finisce per eliminare in radice la possibilità di considerare una singola unità del gruppo quale soggetto terzo, nel cui interesse esclusivo abbia agito il singolo, presupposto su cui avrebbe potuto fondarsi l'esonero da responsabilità.

Negli anni successivi, la giurisprudenza ha ulteriormente e variamente motivato in merito alla possibile condivisione della responsabilità da reato all'interno dei gruppi, con particolare riferimento alle implicazioni di addebito "automatico" per la capogruppo. Ad esempio, secondo alcune interpretazioni, la *holding* non sarebbe solo una mera cassaforte di partecipazioni, ma finirebbe per esercitare – in via mediata - la stessa attività[99] della propria controllata. Oppure, si è data rilevanza anche al rapporto "qualificato" tra le società[100] tipico dei contesti societari "aggregati", non solo sul piano strettamente giuridico (formalizzato) ma anche per mero collegamento sostanziale, materiale e di fatto rinvenibile nell'operatività concreta degli enti[101].

La Corte di Cassazione è intervenuta comunque nel 2011[102], riportando la prospettiva della responsabilità sul singolo ente parte del Gruppo e precisando i presupposti indefettibili per i quali anche la capogruppo potrebbe dover rispondere per il reato commesso nell'ambito di una controllata. Ciò può avvenire se, e soltanto se:

99 G.i.p. Tribunale di Milano, 20 settembre 2004.
100 G.i.p. Tribunale di Milano, 14 dicembre 2004.
101 Tribunale Milano, 14 maggio 2007.
102 Cass. Pen., Sez. V, 20 giugno 2011, n. 24583. Parzialmente difforme Cass. Pen., Sez. V, 8 novembre 2012.

- vi è concorso del soggetto esponente della *holding* – che ne trascina la responsabilità – con il responsabile del reato presso la controllata;
- vi è un interesse e vantaggio concreto della controllante (o di altra società facente parte del gruppo) nel reato verificatosi.

Non è sufficiente dunque il riferimento ad un generico interesse di gruppo per affermare l'estensione di responsabilità: per ciascuna società occorre verificare un interesse immediato, diretto, concreto e attuale rispetto alla singola vicenda sottoposta all'autorità giudiziaria; non può desumersi, in via automatica, dalla mera appartenenza delle società ad un contesto aggregato e dalla sussistenza di rapporti di direzione e controllo.

Tale orientamento è stato poi confermato da una pronuncia di legittimità del 2016[103].

Tanto precisato, in termini generali, sul fenomeno dei gruppi, deve allora essere affrontata la prospettiva multinazionale in cui possono operare: può darsi l'ipotesi di una presenza sul territorio italiano della sola capogruppo, di una sola o più controllate e di entrambe. Ovviamente, temi e soluzioni si riveleranno essere molto diverse per ciascuno di questi casi.

3.2 (segue) normativa 231 e dimensione multinazionale del reato o dell'ente

Il D. Lgs. 231/01 ha lasciato scoperto un altro punto critico del funzionamento della responsabilità da reato, vale a dire quello della possibile responsabilità degli enti privati con sede principale all'estero per reati commessi in Italia.

Già prima della recente pronuncia della Corte di Cassazione – che parrebbe quindi aver cristallizzato la soluzione interpretativa - la giurisprudenza di merito aveva generalmente riconosciuto – Tribunale di Milano in testa[104] – la sussistenza di un dovere di osservanza e rispetto della legge italiana, tanto per le persone fisiche che per le persone giuridiche, laddove operino in Italia, indipendentemente dall'esistenza o meno nel paese di appartenenza di norme regolanti in modo analogo la responsabilità penale dell'ente e di assimilabili istituti: uno su tutti, il modello di organizzazione, gestione o controllo.

Questo orientamento trovava accoglimento anche nella sentenza del Tribunale di Lucca del 2017 a conclusione del procedimento di primo grado relativo al terribile incidente ferroviario alla stazione di Viareggio: in questo caso, fu affermata la responsabilità anche di due società straniere, prive sia di una sede sia di uno stabilimento, ma che avevano fornito in locazione i carri cisterna poi deragliati e che ne curavano la manutenzione. Il Tribunale riconobbe come l'obbligo di rispettare la legge italiana discenda dall'operatività su territorio italiano – quindi dallo svolgimento di una condotta – a prescindere da qualsiasi nesso materiale o spaziale dato da una sede secondaria o da uno stabilimento.

103 Cass. Pen., Sez. II, 27 settembre 2016, n. 52316.

104 G.i.p. Milano, 27 aprile 2004, FI 2004, II, 435 seguita da G.u.p. Milano, ord. 13 giugno 2007.

D'altronde, la stessa dottrina maggioritaria conviene sul punto, seppur sulla base di diverse argomentazioni.

Un appiglio normativo in questa direzione è ravvisabile peraltro nell'art. 97 *bis* co. 5° del T.U.L.B.C., laddove si rende applicabile il D. Lgs. 231/01 alle banche comunitarie ed extracomunitarie con succursali in Italia.

Ciò premesso, l'operatività oltre i confini nazionali delle società straniere pone una domanda pratico-operativa: **se le società straniere facenti parte del gruppo debbano adottare un vero e proprio modello 231 volto a coprire l'operatività in Italia o se possa essere sufficiente una sostanziale equivalenza del modello di *compliance* straniero**.

L'osservazione della realtà concreta indica che oggi molte società straniere fanno ancora affidamento sulla sostanziale equipollenza dei sistemi di compliance e ritardano l'adozione di un modello 231 *cross-border*. Va però detto che tale scelta potrebbe non rivelarsi premiale in caso di necessità di difesa dell'ente in giudizio, a fronte dell'elevato tasso di specificità dei requisiti di idoneità del modello 231, che non sempre potranno essere facilmente rispecchiati in un diverso sistema di *compliance* (basti pensare alla peculiarità del sistema italiano in termini di Organismo di Vigilanza) e stante la ormai pacifica assoggettabilità della società straniera operante in Italia alla legge italiana.

Né si ritiene che una valida via di uscita possa essere rappresentata dalla costituzione di una *branch* o altra unità priva di autonomia giuridica (e dunque come tale esonerata dall'onere di adozione di un proprio modello 231) in luogo di una vera e propria *subsidiary* estera, in quanto questo potrebbe comportare, in caso di commissione di un reato-presupposto, una più immediata risalita di responsabilità in capo alla società controllante, come si dirà anche più sotto rispetto al caso del reato commesso interamente all'estero.

Diverso invece il caso in cui **la società estera, sia essa la capogruppo o una controllata, non operi direttamente e autonomamente sul territorio italiano ma soltanto in coordinamento, strategico od orizzontale, con società italiane del gruppo, senza però esercitare una vera e propria attività sul territorio a livello gestorio ovvero operativo**: in tal caso sembrerebbe eccessivo concludere per la necessità di adozione di un modello 231 "*cross-border*" da parte di detta società.

Una seconda domanda è invece se il **modello 231 della società italiana operante all'estero** debba contemplare, a fini di prevenzione, anche la possibilità di commissione di reati al di fuori del territorio nazionale, in ossequio al disposto di cui all'art. 4 del D. lgs. 231/2001[105].

È utile premettere che, in pratica, tale evenienza sarà nella maggior parte dei casi già coperta dalla "parte italiana" del modello 231, nella misura in cui

105 Di seguito per comodità di lettura se ne riporta il testo: "*Art. 4. Reati commessi all'estero. 1. Nei casi e alle condizioni previsti dagli articoli 7, 8, 9 e 10 del codice penale, gli enti aventi nel territorio dello Stato la sede principale rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui e' stato commesso il fatto. 2. Nei casi in cui la legge prevede che il colpevole sia punito a richiesta del Ministro della giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti di quest'ultimo*".

difficilmente un reato sarà commesso interamente all'estero ma più facilmente una parte della sua condotta avverrà in Italia. Si pensi, ad esempio, al caso di corruzione di un funzionario estero: ben di frequente l'ideazione del piano corruttivo o l'utilità conseguita potranno essere ricondotte alla sede (principale) italiana. L'eventualità non è tuttavia ipotesi soltanto astratta (si pensi, ad esempio, all'iniziativa corruttiva del tutto autonoma di un mandatario estero oppure ancora all'infortunio sul lavoro occorso in uno stabilimento estero) e la risposta è affermativa: il modello 231 dovrà coprire e adeguatamente presidiare anche l'operatività della società che può avvenire interamente all'estero. E questo non soltanto per fornire un'adeguata protezione alla società in caso di commissione di reati-presupposto, ma anche in una prospettiva più ampia, per l'essere elemento indicativo di un modello 231 realmente "vivente", che rispecchi effettivamente ed integralmente le attività della società.

Chiaramente il tema si pone soltanto per la società italiana che operi all'estero attraverso propri dipendenti, rappresentanti o unità prive di autonomia giuridica. Qualora, al contrario, la società italiana operi all'estero attraverso una distinta società locale, allora varranno le regole sopra descritte e la società estera adotterà un modello 231 "*cross-border*", a seconda che la sua operatività si estenda all'Italia o meno.

Si noti come, anche in questo, come sopra accennato, la separazione giuridica delle entità potrebbe circoscrivere il rischio di risalite di responsabilità verso la società italiana.

4. L'adozione di un modello organizzativo c.d. cross-border nell'elaborazione dottrinale e giurisprudenziale

La dottrina prevalente, come sopra ricordato, ha ritenuto insufficiente la soluzione di un unico modello adottato formalmente dalla capogruppo ed applicato – in via generale – a tutte le controllate, sia in ragione della presunta conseguente a – specificità dello stesso, in quanto non calibrato sulla realtà della singola società, sia in ragione del consueto (e ovvio) principio di autonomia giuridica dei singoli enti, i cui organi sarebbero tenuti ad una propria adozione del modello (anzi secondo le regole di cui all'art. 2497 – *ter* c.c.)

Se l'adozione deve quindi essere "autonoma" da parte delle società del gruppo, è invece ben considerato che la capogruppo svolga un ruolo di indirizzo anche in tal senso fornendo indicazioni di coordinamento in modo che i diversi modelli approvati nell'ambito del gruppo siano tra loro coerenti e congruenti, efficaci nel loro insieme a presidiare anche i gangli funzionali tra società.

Anzi, nella dottrina gius - commercialistica si discute anche di un vero e proprio obbligo della capogruppo di coordinare gli adeguati assetti organizzativi del gruppo e quindi i modelli 231: ciò in relazione all'innegabile ruolo che la controllante comunque esercita (anche al di fuori della stretta applicabilità di direzione e controllo).

Ogni singolo modello deve dunque dare conto della collocazione del rispettivo singolo ente nel contesto del gruppo, e quello della controllante deve dare a sua volta conto della direzione e coordinamento esercitati (se del caso) nel perimetro del gruppo.

5. Caratteristiche del modello cross-border e suo iter di realizzazione

Occorre dunque stabilire quali siano in definitiva i tratti distintivi che deve avere un modello "*cross-border*".

Come visto, all'art. 6 D. Lgs. 231/01 il nostro legislatore si è limitato a indicare – senza declinarli – gli elementi indefettibili per l'adeguatezza del modello organizzativo; altre caratteristiche sono ricavabili dalle diverse linee guida via via emanate da associazioni di categoria (CONFINDUSTRIA, ABI, FARMINDUSTRIA, ecc.), dalle discipline regolatorie dei vari settori e dalle prescrizioni di varie autorità, dalle soluzioni proposte dagli interpreti.

Con riferimento alla redazione dei modelli organizzativi, la dottrina concorda nel ritenere che una delle caratteristiche degli stessi sia la **specificità**. Ciò comporta che il punto di partenza per ogni redazione sia proprio l'analisi e la valutazione della realtà interna aziendale – delle sue caratteristiche e dei suoi bisogni – dei processi e della finalizzata attività di *business*, con particolare riferimento alle aree più sensibili al rischio di commissione di reati: ovviamente però, ciascuno di questi aspetti troverà una particolare connotazione in ragione delle dinamiche di gruppo e, segnatamente, di un gruppo multinazionale che opera in diversi contesti e a geometrie organizzative variabili. Ovvero, diversa organizzazione, nei diversi luoghi, a seconda delle normative.

La piena consapevolezza di queste ultime, in particolare, pare significativa da diversi punti di vista.

Intanto, è innanzitutto necessario individuare i soggetti da coinvolgere nelle attività tenendo presente che, non di rado, il centro decisionale è da collocarsi "extra Paese", ovvero al di fuori del Paese di operatività dell'ente.

Si pensi, ad esempio, alle grandi multinazionali ove ai riporti gerarchici locali si sovrappongono quelli funzionali di gruppo, con conseguente possibile risalita delle responsabilità dalla *legal entity* locale a quella che esercita effettivamente il potere decisionale, che si ritrova a sua volta ad operare in un Paese soggetto a normativa differente.

Nondimeno occorre evidenziare che, in strutture particolarmente complesse, anche l'impianto procedurale è caratterizzato da altrettanta complessità: alle procedure locali si sovrappongono le *policies* di gruppo e la *segregation of duties* nei processi aziendali impone più livelli approvativi che possono coinvolgere anche funzioni di gruppo e non solo locali.

Nel predisporre le attività in vista del *risk assessment* andrà quindi posta particolare attenzione, alla comprensione dei processi aziendali avendo cura di

approfondire quando il processo si esaurisce a livello locale e quando invece prevede necessariamente il coinvolgimento di funzioni trasversali o di gruppo.

Sarà quindi prioritario acquisire conoscenza del sistema di deleghe e procure in essere, degli eventuali *service* infragruppo e del sistema dei flussi informativi tra casa madre e controllate o tra casa madre e *branch*.

Nel passare alla fase di individuazione dei referenti del *committment*, è indispensabile tenere presente le eventuali situazioni di conflitto di interesse esistenti anche se a causa dello sbilanciamento tra il soggetto economico, i *manager* e gli *stakeholder*, il modello di *governance* non potrà contenere – perché imprevedibile – tutte le molteplici variabili del comportamento umano.

La consapevolezza di questo particolare rischio non deve però rallentare la costruzione verso un corretto equilibrio nell'adozione del modello "*cross-border*" e i diversi benefici che da questo ne possono scaturire.

È evidente che in base alla predisposizione assunta dal gruppo, si dovrà prendere coscienza delle aree di potenziale conflitto e negoziare il *top level committment* al fine di poter iniziare l'implementazione del modello "*cross-border*" con la consapevolezza che non si tratta di una soluzione definitiva, ma solo di un punto di partenza da verificare e tenere aggiornato costantemente.

Qualsiasi elaborazione del modello non potrà non tener conto – ovviamente - della configurazione delle Direttive di gruppo - e per tale termine si intendono sia le procedure (*policies*) che il sistema di poteri e le responsabilità operative e gestionali assegnate in ottica funzionale - fatta propria dalla *Legal entity* della società attraverso il controllo della specifica normativa nazionale nonché attraverso l'applicazione di adeguati presidi di controllo interno dello stesso ente coinvolto.

Altrettanto, in termini generali, occorrerà tenere conto dei programmi di compliance locali, evidenziando e valorizzando le possibili sinergie e i punti di connessione con quanto prescritto dal D. Lgs. 231/2001.

Ad esempio, se la società italiana ha una controllata o è controllata da una società inglese, non potrà non farsi riferimento allo UK BRIBERY ACT, così come al FCPA in caso di connessioni con società del gruppo americana.

Ciò in quanto da un lato il *compliance program*, qualunque esso sia e in qualunque modo sia chiamato, dovrebbe recepire le peculiarità della singola società e del Paese in cui si trova ad operare e, dall'altro, in quanto il modello, dopo l'approvazione da parte del Board, dovrebbe essere effettivamente conosciuto e implementabile a livello locale.

Preferibile sarebbe dunque la scelta di adottare un modello *ex* D. Lgs. 231/2001 che tenga conto delle peculiarità dei processi e dei rischi *cross-border*, nell'ambito della *legal entity* italiana e predisporre successivamente degli strumenti semplificati (Codice Etico, *policies*, protocolli, procedure) da declinare nelle società estere che siano sprovviste di strumenti di *compliance* compatibili con il D. Lgs. 231/2001 e dunque accettabili.

Chiaramente questa opportunità sarà più facilmente realizzabile nell'ipotesi in cui la *legal entity* italiana sia la casa madre e le società estere delle mere controllate e dunque nell'ipotesi in cui la società italiana abbia maggior potere decisionale.

Nell'ipotesi contraria, invece, ovvero di casa madre straniera e *branch* italiana, potrebbe presentarsi qualche difficoltà in più nell'imporre alla controllante straniera delle *policies* o procedure nate nell'ambito della *branch* italiana.

Si tratta però di un problema facilmente superabile se si considera che, innanzitutto, l'adozione di un siffatto strumento tutela non solo la società italiana, ma anche la società controllante estera dai rischi di risalita di responsabilità; in secondo luogo spesso la normativa locale come il D. Lgs. 231/2001 rappresenta la declinazione di una normativa sovranazionale recepita in Paesi diversi; infine spesso, in materia di *compliance*, trovano applicazione standard a valenza internazionale (es. standard ISO 37001 in materia di corruzione) e dunque facilmente esportabili e applicabili trasversalmente.

Individuati i soggetti coinvolti nel progetto di costruzione, il passo successivo è quello di individuare e valutare i rischi di compliance cui l'organizzazione è effettivamente esposta.

Da un punto di vista metodologico in tema di individuazione, ponderazione e gestione dei rischi, l'analisi deve essere tale da assicurare la copertura rispetto alle previsioni normative del paese in cui si svolge l'*assessment*, quindi estesa alle altre *countries* al fine di individuare sia le plurime sinergie che le strutturali differenziazioni.

Esempio utile potrebbe essere quello di rappresentare, da un punto di vista della *legal entity* italiana, la necessità di mappare tutti i rischi rilevanti ai sensi del D. Lgs.231/01 per poi procedere all'integrazione con la specifica procedura internazionale a ponderare e bilanciare il modello *cross-border* sulla base della normativa più ristretta nel differente ambito applicativo.

In questa prospettiva non può trascurarsi ancora una volta l'analisi del *corpus* procedurale esistente a livello locale e di gruppo, nonché le relazioni esistenti tra i due sistemi per valutare l'idoneità del sistema nel suo insieme a prevenire reati e, in particolare, reati presupposto *ex* D. Lgs. 231/2001.

L'approccio più agevole dovrebbe quindi partire dall'analisi dei processi aziendali per passare poi alla valutazione della loro adeguatezza rispetto alla capacità di prevenzione dei reati, e non viceversa, avendo cura di suggerire l'integrazione dei processi aziendali secondo i principi di ispirazione del D. Lgs.231/2001 e tarando conseguentemente il modello *cross-border* sulla base dapprima della normativa di cui al D. Lgs. 231/2001 e successivamente secondo la normativa di Paese se più stringente.

Non si potranno certamente trascurare i processi relativi ai rapporti con la Pubblica Amministrazione, i rapporti con la clientela internazionale, la gestione del processo di acquisto e di produzione di beni, la gestione di marchi e brevetti, i rapporti con i *partner* commerciali e gli agenti esteri, nonché la gestione

dei flussi finanziari e della fatturazione gestiti spesso a livello di gruppo tramite "*shared services centers*".

Anche se i casi più noti di condanne di multinazionali (es. SIEMENS, ENI) riguardano fenomeni corruttivi, i rischi da prevenire riguarderanno in particolare anche i reati transnazionali, o di riciclaggio, o di criminalità organizzata oppure ancora di finanziamento al terrorismo e tributari.

Giova ricordare che nella non facile fase di *assessment*, una volta focalizzato il rischio dal punto di vista nazionale e/o internazionale, è necessario comprendere come, nella specifica organizzazione, il rischio potrebbe effettivamente realizzarsi ed i presidi esistenti. Nel mitigare i rischi da evitare nell'adozione di un modello *cross-border* si ritiene utile procedere per processi piuttosto che per reati.

Risulta importante non solo evidenziare la fattispecie penale configurabile, quanto piuttosto implementare un processo che renda difficile la commissione di un reato nell'ambito dell'ente, a prescindere dal destinatario designato.

Per brevità si evidenziano i processi maggiormente esposti attraverso una elencazione non esaustiva, ma con mera finalità espositiva:

- selezione delle terze parti coinvolte;
- processo di assunzione;
- sistema di incentivazione;
- donazioni e altre forme liberali;
- omaggi.

Non di poco conto, infine, sono gli aspetti relativi alla **lingua di redazione** del modello *cross-border*: dovrebbe seguire – con necessità di relativa traduzione – quella del Paese ove si vuole che venga applicato e ove opera il personale chiamato ad applicarlo o, quanto meno, in inglese.

6. L'Organismo di Vigilanza nell'ambito del gruppo multinazionale: quali soluzioni?

Da ultimo, merita breve cenno il tema della **costituzione dell'Organismo di Vigilanza all'interno dei gruppi multinazionali**.

La dottrina maggioritaria tende a escludere, sempre in ragione della distinta soggettività giuridica, l'adeguatezza di una soluzione che individui in un unico Organismo, costituito presso la controllante, l'organo di vigilanza per tutte le società del gruppo[106]; alcuni interpreti, ancor più rigorosi, non ritengono auspicabile neppure la coincidenza di componenti tra un organismo e l'altro delle diverse società del gruppo. Nel 2003, il Tribunale di Roma ha peraltro ammesso la configurazione dell'Organismo della capogruppo quale risorsa esterna a disposizione – in termini di risorse e competenze – di quelli delle controllate.

106 Maggiori aperture per soluzioni alternative si rinvengono con riferimento ai c.d. enti di piccole dimensioni.

Pare invero preferibile che laddove ciascuna società del gruppo si doti di un proprio modello 231, del pari istituisca un proprio autonomo Organismo. Al contrario, l'istituzione di un unico Organismo di gruppo non solo potrebbe pregiudicare la valutazione complessiva dell'idoneità del modello (per i motivi sopracitati), ma potrebbe agevolare allargamenti e risalite di responsabilità, in quanto possibile spia di rapporti di direzione e controllo.

Ciò, ovviamente, non esclude la possibilità di un coordinamento e raccordo fra i vari Organismi, da attuarsi innanzitutto attraverso un periodico scambio di informazioni, che, anzi, va incoraggiato quale indice di un effettivo e integrato sistema di prevenzione di gruppo.

In particolare tale coordinamento deve consistere in un'attività di vigilanza sui processi *cross-border*, anche attraverso *audit* presso le società straniere e il coordinamento con le funzioni di *Internal Audit*, o equipollenti, locali.

7. Conclusioni

Ripercorrendo quanto detto sopra, se si guarda alla *compliance* del gruppo multinazionale nella prospettiva del sistema giuridico italiano, il tema va inquadrato nella cornice normativa del D. lgs. 231/2001 che, da un lato (*i*) non contempla (e non considera idoneo) un modello di *compliance* di gruppo, dall'altro (*ii*) ha una portata non solo nazionale ma extraterritoriale, nella misura in cui, da un lato, impone il suo rispetto a tutte le società, anche straniere, comunque operanti sul territorio italiano e, dall'altro, estende la sua applicabilità anche all'operatività estera delle società italiane[107].

Pare possibile affermare che la *holding* italiana debba adeguarsi al D. Lgs. 231/01 anche con riferimento all'operatività del gruppo all'estero, e coordinare le controllate estere nello sforzo di *compliance*; simmetricamente, pare invece opportuno che la controllata italiana si adegui al D. Lgs. 231/01, serbando però attenzione per le *policies* di casa madre e sensibilizzando altresì le varie società appartenenti allo stesso gruppo circa il rischio di commissione di illeciti in Italia.

Il gruppo multinazionale, se vorrà essere esonerato da responsabilità *ex* D. lgs. 231/2001 in caso di commissione di reati-presupposto, dovrà adoperarsi nel senso dell'adozione – da parte di ciascuna società, italiana o straniera, operante in Italia - di un modello 231, specificamente elaborato e specificamente approvato tenendo conto delle peculiarità del contesto geografico originario; dall'altro, nel senso di assicurare che il modello 231 di ciascuna società italiana copra l'eventuale operatività estera della stessa.

Comunque, se il modello 231 adottato dalla capogruppo non esime ciascuna società controllata dall'onere di una distinta elaborazione ed adozione di

107 Fra gli altri, si veda CERQUA, *L'applicabilità del d.lgs. 231/2001 alle società estere operanti in Italia: il caso degli istituti di credito e degli intermediari finanziari*, in Rivista 231, n. 2/2009; PISTORELLI, *Profili problematici della «responsabilità internazionale» degli enti per i reati commessi nel loro interesse o vantaggio*, in Rivista 231, n. 1/2011; RUTA, *La responsabilità amministrativa degli enti stranieri e i limiti del principio di territorialità*, in Rivista 231, n. 4/2018.

un modello plasmato sulla singola e specifica attività, rimane tuttavia auspicabile un coordinamento tra le varie iniziative assunte dalle società del gruppo[108].

Tale coordinamento si rende decisivo proprio con riferimento all'operatività *cross-border* che si sostanzi in attività sensibili ai sensi del D. Lgs. 231/2001 (vale a dire le attività a carattere transnazionale e a elevato rischio - reato: ad esempio, tutti i processi di natura finanziaria ed economica ed i relativi riflessi in termini di reati societari, di riciclaggio e tributari) attraverso l'adozione di principi di condotta (ad esempio, a livello di Codice Etico) e di *policies* che istituiscano indicazioni di comportamento e presidi di controllo comuni.

108 Così, anche CONFINDUSTRIA, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231*, approvate il 7 marzo 2002 (aggiornate al marzo 2014).

CAPITOLO 7 di Eva Cruellas Sada, Eugenia Gambarara e Irene Picciano

Profili di compliance antitrust nelle operazioni di M&A e recente prassi applicativa

Profili di compliance antitrust nelle operazioni di M&A e recente prassi applicativa AGCM sulla valutazione dei programmi di compliance a fini sanzionatori

SOMMARIO: 1. Compliance antitrust nelle operazioni di M&A – 1.1 Fase preliminare – 1.2 Fase intermedia – 1.3. Fase finale – 2. Le nuove linee guida sulla Compliance Antitrust e prassi applicativa dell'AGCM

1. Compliance antitrust nelle operazioni di M&A

Le operazioni di *Merger & Acquistion* ("M&A") rappresentano un fenomeno economico di notevoli dimensioni, orientato principalmente all'accrescimento del potere di mercato di un'impresa. La complessità di tali operazioni, nonché il loro carattere sempre più transfrontaliero, richiede un'analisi puntuale delle potenziali criticità antitrust che possono presentarsi nel corso dell'operazione, e che devono essere valutate e risolte tempestivamente. La compliance antitrust rappresenta quindi un aspetto di fondamentale importanza, che va tenuto in considerazione durante tutto l'iter dell'operazione, dalla fase preliminare fino al *closing* e al *post-closing*.

Le operazioni di M&A sono caratterizzate da un'esigenza legittima di accesso ad informazioni dettagliate sul *business* della controparte, anche qualora le due imprese siano concorrenti attuali ovvero quantomeno concorrenti potenziali, e richiedono quindi fisiologicamente la condivisione di informazioni tra l'impresa *target* e l'acquirente. I principali rischi connessi a tale attività sono legati alla possibile violazione del divieto di scambio di informazioni commercialmente sensibili tra concorrenti e del divieto di *gun-jumping*[109], che

109 Il c.d. "*gun jumping*" può verificarsi in due casi distinti. Il primo è quello in cui l'acquisizione viene perfezionata senza aver effettuate le prescritte notifiche alle competenti autorità antitrust, o, peggio ancora, prima di aver effettuato tali notifiche e aver quindi ottenuto le prescritte autorizzazioni ("clearance"). Si veda la decisione Marine Harvest/ Morpol (Caso No COMP/M.7184). Il secondo caso di "*gun-jumping*" riguarda la concentrazione tra due concorrenti e si riferisce all'eventualità che nel periodo intercorrente tra la firma del *Sale and Purchase Agreement* e l'ottenimento della clearance da parte delle autorità antitrust competenti (il c.d. "*Interim Period*"), le due società coinvolte, l'acquirente e la target, coordinino la loro attività commerciale e operativa, con la società acquirente che nella pratica si comporta come se fosse già l'azionista di controllo della società che dovrebbe essere acquisita. Si veda la decisione Altice/PT Portugal (Caso No COMP/ M.7993).

consiste nell'attuazione (anche parziale) di una concentrazione[110] prima della sua approvazione da parte dell'autorità *antitrust* competente.

In particolare, il rischio di *gun-jumping* è comune a varie giurisdizioni[111], oltre a essere previsto espressamente dal Regolamento comunitario sulle concentrazioni[112], a causa della presenza dell'obbligo di *standstill*.

Il secondo aspetto problematico (che prescinde da qualsiasi obbligo di notifica/controllo delle concentrazioni) attiene invece agli scambi di informazioni sensibili tra imprese concorrenti, ovvero lo scambio di dati strategici la cui condivisione può determinare effetti restrittivi sulla concorrenza, in quanto riduce l'indipendenza decisionale delle parti nell'operare sul mercato[113]. È bene infatti ricordare che le parti dell'operazione dovrebbero restare concorrenti fino al *closing* della stessa.

La violazione di questi principi costituisce un illecito antitrust e potrebbe portare all'irrogazione di una sanzione, o comunque all'apertura di indagini da parte delle autorità competenti che potrebbero ritardare o comunque ostacolare la chiusura dell'operazione.

Proprio per evitare che la società sia esposta a rischi di natura legale e commerciale, è opportuno adottare un processo interno di compliance che disciplini i comportamenti e le cautele da adottare in ogni fase dell'operazione e ne monitori in modo continuativo il rispetto.

Di seguito si illustreranno più nel dettaglio, i rischi e le criticità antitrust peculiari di ogni fase dell'operazione (preliminare, intermedia e finale) e le condotte che è bene adottare per evitare di incorrere in illeciti.

1.1 Fase preliminare

1.1.1 Accesso alle informazioni, discussioni preliminari e Due Diligence

Come già osservato, le varie fasi del processo di M&A richiedono la condivisione di numerose informazioni anche di natura confidenziale tra acquirente

110 Nell'ambito del diritto antitrust, si ha una concentrazione quando si produce una modifica duratura del controllo dell'impresa.

111 Legge 289/1990, art. 17: "L'Autorità, nel far luogo all'istruttoria di cui all'articolo 16, può ordinare alle imprese interessate di sospendere la realizzazione della concentrazione fino alla conclusione dell'istruttoria La disposizione del comma 1 non impedisce la realizzazione di un'offerta pubblica di acquisto che sia stata comunicata all'Autorità ai sensi dell'articolo 16, comma 5, sempre che l'acquirente non eserciti i diritti di voto inerenti ai titoli in questione."

112 Regolamento (CE) n. 139/2004 del Consiglio, del 20 gennaio 2004, relativo al controllo delle concentrazioni tra imprese ("Regolamento comunitario sulle concentrazioni" o in inglese "*Merger Regulation*"): "art.7.1. "*Sospensione della concentrazione 1. Una concentrazione di dimensione comunitaria, quale è definita all'articolo 1, o che è destinata ad essere esaminata dalla Commissione a norma dell'articolo 4, paragrafo 5, non può essere realizzata prima di essere notificata, né prima di essere stata dichiarata compatibile con il mercato comune da una decisione adottata a norma dell'articolo 6, paragrafo 1, lettera b), o dell'articolo 8, paragrafo 1 o paragrafo 2, ovvero sulla base della presunzione di cui all'articolo 10, paragrafo 6.*"

113 Si veda art. 54 e seguenti della Comunicazione della Commissione — Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale.

e venditore al fine di *inter alia* verificare la fattibilità della potenziale operazione, stimare il valore della *target* o dell'operazione e negoziare i termini contrattuali.

Anzitutto, l'accesso ad informazioni è necessario nell'ambito delle discussioni preliminari tra le parti e nell'attività di *due diligence*, che rappresentano passaggi fondamentali in ogni operazione M&A, in quanto permettono all'acquirente di avere accesso alle informazioni necessarie per poter valutare la società *target* nel suo complesso e decidere consapevolmente sull'operazione.

Inoltre, l'accesso alle informazioni sulla *target* può servire a individuare possibili condotte anticoncorrenziali della *target* e permettere quindi all'acquirente di adottare misure finalizzate ad evitare che le stesse si protraggano anche dopo l'operazione e/o ad essere manlevato dal venditore dalle eventuali conseguenze negative di tali possibili condotte[114].

Infine, l'accesso alle informazioni sulla *target* (e in certe circostanze anche del gruppo venditore) sarà necessario anche per identificare eventuali obblighi di notifica *antitrust* e le Autorità Antitrust competenti.

Il perimetro delle informazioni necessarie ai fini dei suddetti obiettivi può variare a seconda del tipo di operazione. In particolare, operazioni di natura complessa, con alti livelli di rischio o che prevedano il finanziamento da parte di terzi possono richiedere una quantità e una specificità maggiore di condivisione di informazioni commerciali, mentre nel caso di operazioni tra società quotate, sottoposte a stringenti obblighi di trasparenza, molte informazioni potrebbero risultare già pubbliche o di dominio pubblico.

Nonostante l'indiscussa necessità di acquisire informazioni nell'ambito delle operazioni di M&A, vi sono validi motivi per essere prudenti nel rivelare informazioni commerciali riservate, in particolare quando l'acquirente e la *target* sono in un rapporto di concorrenza attuale o potenziale.

Infatti, lo scambio di informazioni commercialmente sensibili tra imprese indipendenti (specie se concorrenti) è suscettibile di ricadere nel divieto di intese restrittive della concorrenza (art. 2 L. 287/90 e art. 101(1) del Trattato sul Funzionamento dell'Unione Europea, "**TFUE**").

La possibilità che uno scambio di informazioni generi effetti anticoncorrenziali sul mercato dipende da una pluralità di fattori, che includono le caratteristiche del mercato ove le parti operano (con particolare riguardo al livello di concentrazione e alle quote di mercato delle parti coinvolte) nonché la tipologia delle informazioni scambiate. Nello specifico, informazioni non disponibili al pubblico, in forma individualizzata e disaggregata ovvero relative a prezzi o altri fattori rilevanti dal punto di vista concorrenziale possono spingere il mercato verso un esito collusivo, facilitando il coordinamento tra concorrenti[115].

Tale divieto si applica anche ai contatti e agli scambi di informazioni precedenti alle operazioni M&A e alla fase di *due diligence*: non è necessario per

114 Cfr. Guida pratica ICC alla compliance antitrust, 2013, p. 62 e ss.

115 Comunicazione della Commissione Europea, Linee direttrici sull'applicabilità dell'articolo 101 TFUE agli accordi di cooperazione orizzontale (2011/C 11/01), §§54 e seguenti.

incorrere in una pratica censurabile che lo scambio di informazioni avvenga con l'intento di restringere la concorrenza né che esso sia parte di una fattispecie più ampia.

Per evitare il rischio di una violazione del divieto di scambio di informazioni commercialmente sensibili, è essenziale che le parti adottino tempestivamente opportune misure di tutela[116], già a partire dai primi contatti preliminari relativi alla potenziale operazione e, in ogni caso, prima di qualsiasi scambio di informazioni.

L'adozione di tali misure serve a tutelare sia il venditore sia il compratore. Pertanto, gli interessi delle due parti dovrebbero risultare sostanzialmente coincidenti.

Per quanto riguarda le possibili misure per garantire la *compliance antitrust* nel contesto dell'accesso agli informazioni nella fase preliminare delle operazioni M&A, gli accordi di riservatezza o di non divulgazione (c.d. "*Non-Disclosure Agreements*" o "NDA") costituiscono un primo strumento utile per regolare le modalità di accesso, scambio ed uso delle informazioni da parte delle imprese coinvolte.

Inoltre, le parti adottano frequentemente anche degli specifici protocolli con l'obiettivo di disciplinare puntualmente quali informazioni potranno essere fornite/scambiate, chi può avere accesso a quali informazioni e con quali modalità si svolgerà tale accesso, al fine di garantire che tutto il processo informativo avvenga in maniera pienamente conforme con la normativa *antirtust*.

È essenziale che i suddetti protocolli antitrust e accordi di riservatezza siano concordati tra le parti ed entrino in vigore molto presto, già nelle fasi iniziali dell'operazione, prima che possa avvenire qualsiasi scambio di informazioni.

Quanto al loro contenuto, i protocolli antitrust/gli NDAs prevedono generalmente le seguenti clausole:

- una chiara definizione delle informazioni che saranno oggetto di scambio, che in ogni caso dovrebbero essere limitate a quanto strettamente necessario ai fini della *due diligence* e della valutazione dell'operazione (c.d. *need to know basis*), di norma associata a una ripartizione delle stesse in varie classi, coincidenti con livelli crescenti di sensibilità e, quindi, di riservatezza delle informazioni[117];
- il divieto che le informazioni che saranno oggetto di scambio siano utilizzate per fini ulteriori o diversi rispetto a quello della valutazione e dell'attuazione dell'operazione, in particolare per fini commerciali;

116 Nota della Federal Trade Commission: "Avoiding antitrust pitfalls during pre-merger negotiations and due diligence", 20 marzo 2018.

117 Solitamente si distingue tra: informazioni commerciali non sensibili (dati generali, storici, pubblici o aggregati); informazioni commerciali sensibili (dati recenti, disaggregati o comunque precisi al punto da poter avere effetti sulla concorrenza sul mercato); e informazioni altamente sensibili che, se diffuse, potrebbero causare gravi distorsioni della concorrenza (si pensi ai dati sui prezzi futuri di una delle parti).

- la definizione del perimetro di persone abilitato ad avere accesso a ciascuna classe di informazione, che in ogni caso dovrà includere solo coloro il cui coinvolgimento sia strettamente necessario ai fini della valutazione dell'operazione (c.d. *need to know basis*);
- l'obbligo, per i soggetti di cui sopra, di non fornire a terzi le informazioni di cui si viene a conoscenza, oltre all'obbligo di non condividere all'interno dell'impresa le informazioni di una certa classe con persone che non sono abilitate ad accedere a tale classe di informazione;
- l'obbligo di restituire o distruggere le informazioni nel caso in cui l'operazione non sia portata a termine, le modalità tramite le quali tale restituzione o distruzione dovrà essere attuata e le eventuali sanzioni nel caso di mancata distruzione;
- spesso gli accordi di non divulgazione contengono anche previsioni sull'obbligo di non fare menzione del fatto che l'operazione stia avendo luogo o, se i titoli di una o di entrambe le parti sono negoziati pubblicamente, clausole di c.d. *stand-still* che vietano alla parte acquirente di acquisire le azioni della *target* o lanciare offerte pubbliche di acquisto per un determinato periodo di tempo.

In relazione alle informazioni classificate come commercialmente sensibili, il processo di *disclosure* può essere implementato anche in più fasi, adottando il modello della c.d. *timing cascade*, secondo il quale le informazioni sensibili non vengono condivise subito bensì in una fase molto avanzata dell'operazione in prossimità/contestualmente al *closing*, mentre le informazioni che non danno adito a preoccupazioni dal punto di vista concorrenziale possono essere condivise anche durante le discussioni preliminari e nella fase di *due diligence* senza limitazioni sui destinatari.

In alternativa, laddove l'accesso a informazioni commercialmente sensibili sia necessario ai fini dell'operazione già dalle prime fasi, sarà necessario prevedere che l'accesso a questa tipologia di informazioni sia riservato ad un numero ristretto di persone (c.d. *Clean Team*). Il *Clean Team* potrà essere formato da consulenti esterni – che, in quanto tali, sono soggetti terzi e imparziali rispetto alle imprese coinvolte – ma anche, a certe condizioni, da *manager*, dipendenti o esponenti dell'impresa acquirente a patto che essi non siano coinvolti nelle decisioni commerciali della stessa.

L'accesso alle informazioni commercialmente sensibili sarà quindi strettamente riservato ai membri del *Clean Team*, ai quali verranno imposti obblighi molto stringenti di riservatezza e di non divulgazione delle informazioni riservate al *Clean Team* a persone esterne ad esso. In particolare, i membri del *Clean Team*, dopo avere esaminato le informazioni commercialmente sensibili accessibili solo a loro, non potranno condividere tali informazioni con altre persone ma potranno elaborare e condividere con esponenti dell'impresa esterni al *Clean Team* unicamente resoconti che facciano riferimento alle informazioni commercialmente sensibili, ma solo se rielaborate con modalità che garanti-

scano la neutralità e la non sensibilità delle stesse (p.es. in forma aggregata, anonimizzata, ecc.).

Nella prassi, le operazioni di *due diligence* prevedono solitamente l'accesso, da parte dei membri del *Clean Team*, a una c.d. *data room* separata (diversa della *data room* generale accessibile anche alle persone che non sono membri del *Clean Team*) allestita dal venditore, il cui accesso è condizionato ad una verifica sulle persone nominate come membri del Clean Team e alla sottoscrizione di stringenti obblighi di riservatezza e non divulgazione.

Le specifiche regole di sicurezza della *data room* possono rafforzare ulteriormente la tutela delle informazioni sensibili, prevedendo compartimentazioni e differenziazioni nell'accesso, oltre a misure precauzionali come i *log-off* automatici e l'interdizione di operazioni che potrebbero compromettere i livelli di sicurezza della *data room*, come il download, la condivisione tramite *e-mail* o la stampa di documenti.

In relazione alle informazioni che vengono fornite esclusivamente in relazione ai profili antitrust dell'operazione (i.e. al fine dell'esame di notificabilità e per la compilazione dei formulari di notifica), le quali non rientrerebbero nel processo *standard* di *due diligence*, si può prevedere che esse siano rese disponibili esclusivamente ai consulenti antitrust esterni (su base *counsel-to-counsel*).

È poi consigliabile tracciare tutti i contatti tra le parti, che devono rimanere in un rapporto di concorrenza effettiva fino al *closing*. Il tracciamento dovrebbe avvenire in maniera specifica, segnalando tutte le categorie di informazioni che sono state oggetto di scambio e gli individui coinvolti nello scambio. In quest'ottica, eventuali incontri tra le parti dell'operazione dovrebbero essere puntualmente verbalizzati e condotti sulla base di agende predisposte sotto la supervisione dai legali competenti. Una simile rendicontazione delle operazioni di *due diligence* potrebbe rivelarsi utile anche nel caso in cui, a seguito della scoperta di eventuali violazioni della normativa antitrust, una delle parti decidesse di ricorrere a programmi di clemenza[118].

1.1.2 Identificazione degli obblighi di notifica e analisi sostanziale dell'operazione

Un'altra tematica che è bene affrontare molto presto nell'ambito di un'operazione M&A in un'ottica di *compliance* è quella relativa all'individuazione di obblighi di notifica preventiva *antiturst* dell'operazione e delle Autorità Antitrust competenti nonché dei potenziali rischi *antitrust*.

Questo consentirà di prevedere con una certa precisione la tempistica per l'ottenimento delle autorizzazioni *antitrust* necessarie al *closing* e decidere le strategie in caso di riscontro preliminarmente negativo delle autorità competenti (i.e. considerare tempestivamente lo strumento degli impegni).

118 Cfr. Guida pratica ICC alla compliance antitrust, 2013, p. 65.

Possono sorgere seri problemi *antitrust* soprattutto nel caso di operazioni M&A che coinvolgono concorrenti (attuali o potenziali), specie se di grandi dimensioni, con quote di mercato elevate o attive in mercati con pochi operatori o con alte barriere all'ingresso.

In tali casi, è bene iniziare l'analisi dei profili sostanziali antitrust già nella fase preliminare dell'operazione M&A. Infatti, l'individuazione delle problematiche *antitrust* già in una fase preliminare consente di affrontare e risolvere tali questioni prima che vengano concordati gli aspetti fondamentali della struttura dell'operazione (in particolare il prezzo), anche al fine di una migliore negoziazione degli obblighi di cooperazione nella (eventuale) fase di notifica *antitrust* dell'operazione e dell'allocazione dei rischi *antitrust* tra le parti.

1.2 Fase intermedia

È di preliminare importanza sottolineare come vi sia una crescente attenzione da parte delle autorità *antitrust* verso i comportamenti delle imprese nelle attività propedeutiche alla chiusura delle operazioni di M&A[119]. Tra il *signing* e il *closing* dell'operazione, infatti, le parti hanno forti interessi a scambiare informazioni, ad esempio a fini di *due diligence*, per identificare possibili sinergie o per iniziare ad adottare iniziative idonee a garantire che il processo di transizione si svolga nel modo più fluido possibile. Quindi, potrebbero risultare necessari ulteriori scambi di informazioni ai fini della pianificazione dell'integrazione. Tuttavia, anche in questa fase, in linea di principio i concorrenti non devono avere accesso a informazioni sensibili dal punto di vista della concorrenza (come ad esempio prezzi, costi, progetti di R&S o altri piani strategici) né possono comportarsi in maniera coordinata sul mercato prima del *closing*.

L'impresa acquirente può ricevere e valutare informazioni relative al *business* della *target* ed iniziare a preparare il *closing*, a condizione che le informazioni richieste siano ragionevolmente necessarie per pianificare l'integrazione e per la continuità operativa, e che non siano informazioni commercialmente sensibili. In ogni caso è buona prassi consultare sempre un consulente legale esterno al fine di valutare la natura sensibile delle informazioni in questione.

In base al Regolamento 139/2004[120], ci sono due criteri di controllo delle concentrazioni: quelle aventi una dimensione comunitaria sono sottoposte alla giurisdizione della Commissione e quelle che ne sono prive restano soggette al controllo da parte delle autorità nazionali (c.d. *one stop shop*). A seconda del superamento o meno delle soglie di fatturato previste a livello europeo e a livello nazionale, le concentrazioni devono essere notificate alle autorità competenti che devono vagliarne la compatibilità o meno con il mercato interno e quindi autorizzarle o vietarle.

119 Si veda, ad esempio, la nota "Avoiding antitrust pitfalls during pre-merger negotiations and due diligence" pubblicata dalla Federal Trade Commission (Bureau of Competition), disponible al seguente link: https://www.ftc.gov/news-events/blogs/competition-matters/2018/03/avoiding-antitrust-pitfalls-during-pre-merger.

120 Art. 7 del Regolamento (CE)n. 139/2004 del Consiglio, del 20 gennaio 2004, relativo al controllo delle concentrazioni tra imprese ("Regolamento comunitario sulle concentrazioni").

Come si è anticipato in precedenza, uno dei rischi principali sotto il profilo *antitrust*, anche in virtù della posizione sempre più rigida assunta dalla Commissione europea in materia, è quello del *gun jumping*, ovvero di un eventuale coordinamento delle attività commerciali e operative tra la società acquirente e la *target*, durante il c.d. *interim period* (cioè prima dell'ottenimento dell'approvazione della concentrazione da parte dell'autorità *antitrust* competente), con la conseguenza che la società acquirente si comporti come se avesse già acquistato il controllo della *target*[121].

È quindi opportuno al fine di scongiurare il verificarsi di simili situazioni, che tale fase venga espressamente disciplinata, prevedendo che fino al *closing* dell'operazione la società *target* continui a svolgere il suo *business as usual*, evitando quindi di mutare il perimetro della sua attività e impegnandosi ad astenersi da azioni al di fuori dell'ordinaria amministrazione. Dall'altro lato l'acquirente non può cercare di influenzare l'attuale *business* della *target*, né tantomeno di gestirla prima dell'ottenimento dell'autorizzazione da parte dell'autorità *antitrust*. L'ottenimento della clearance costituisce infatti una condizione sospensiva dei contratti di acquisizione societaria, ciò significa che la loro efficacia è subordinata al rilascio di tale autorizzazione.

Fare altrimenti, quindi come ribadito dalla Commissaria Margrethe Vestager, significherebbe "*…jump the gun by implementing mergers prior to notification or clearance, (so undermining) the effective functioning of the EU merger control system*"[122].

121 A tal proposito si veda Corte giust. UE, 31 maggio 2018, C-633/16 ECLI:EU:C:2018:371, Ernst & Young P/S contro Konkurrenceådet. Si tratta di una domanda di pronuncia pregiudiziale presentata nell'ambito di un ricorso di annullamento proposto da Enrnst & Young avverso una decisione del Consiglio per la concorrenza danese. L'autorità danese ha contestato alle società EY e KPMG di aver violato l'obbligo di sospensione di attuare una concentrazione prima della sua approvazione da parte del Consiglio per la concorrenza. Il 18 novembre 2013 le società KPMG DK e EY hanno concluso un accordo di cooperazione che conteneva alcune clausole riguardanti la ripartizione dei client, l'obbligo di prestare servizi ai clienti in altri stati e un compenso annuale per poter far parte della rete e prevedeva che le società partecipanti non potessero concludere tra loro contratti commerciali. Tale accordo costituiva una cooperazione volontaria tra le due società, sebbene ognuna di essa rimanesse autonoma dal punto di vista della concorrenza. Dopo aver firmato l'accordo di concentrazione (che non raggiungeva le soglie comunitarie e doveva essere pertanto analizzato dalle autorità danesi), le società KPMG DK recedevano dall'accordo di cooperazione, che non era di per sé oggetto di approvazione da parte dell'autorità della concorrenza. Il Consiglio danese per la concorrenza dichiarava che le società KPMG DK, recedendo dall'accordo di cooperazione prima dell'approvazione della concentrazione avessero violato l'obbligo di standstill. Si riteneva infatti che il recesso dall'accorso di cooperazione, essendo legato alla concentrazione, sarebbe stato idoneo a produrre effetti irreversibili sul mercato nel periodo compreso tra il recesso e l'approvazione della concentrazione. La EY ha impugnato la decisione, richiedendone l'annullamento e la questione è stata rinviata al giudice europeo. La Corte di Giustizia ha chiarito la portata dell'obbligo di sospensione previsto dall'art. 7 del Regolamento, prevendo che quest'ultimo debba essere interpretato nel senso che una concentrazione è realizzata unicamente mediante un'operazione che, in tutto o in parte, in fatto o in diritto, contribuisca al cambiamento di controllo dell'impresa target. Nel caso di specie non si può considerare che il recesso da un accordo di cooperazione comporti la realizzazione di una concentrazione. Tale interpretazione è stata seguita anche dalla più recente sentenza della Corte di Giustizia nella Causa C-10/18 P, *Mowi ASA c. Commissione europea*, sull'impugnazione con cui la *Mowi ASA*, già Marine Harvest ASA, 4 marzo 2020.

122 Press release del 24 aprile 2018 caso Altice, disponibile al seguente link: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3522.

1.3. Fase finale

Nell'ambito di un'operazione di M&A, le parti possono concordare delle restrizioni accessorie (*ancillary restrainits*), che sebbene non costituiscano l'oggetto principale dell'operazione, sono considerate dalle parti indispensabili alla realizzazione della stessa. Tali clausole, sebbene configurino delle intese restrittive della concorrenza (e come tali andrebbero valutate ai sensi dell'art. 101 del Trattato sul Funzionamento dell'Unione europea, o delle corrispondenti disposizioni nazionali), vengono attratte nell'ambito di applicazione del regolamento comunitario sul controllo delle concentrazioni, con la conseguenza che un eventuale giudizio favorevole relativo all'operazione notificata, si estenderà automaticamente anche a tali clausole, qualora (*i*) siano direttamente collegate all'operazione di concentrazione e (*ii*) necessarie per la sua implementazione[123].

Tra le restrizioni accessorie più frequenti vi rientrano:

- le clausole di non concorrenza, che sono soggette a dei limiti oggettivi, temporali (durata massima di 2 o 3 anni in caso di acquisizione, o per l'intera durata della *joint venture*), e territoriali.
- Gli obblighi di acquisto/fornitura volti a garantire la continuità di approvvigionamento dell'una o dell'altra delle parti dell'operazione per i prodotti necessari allo svolgimento delle attività mantenute dal venditore o rilevate dall'acquirente. La loro durata va limitata ad un periodo sufficiente a consentire la sostituzione dei rapporti di dipendenza con una posizione di autonomia sul mercato. Gli obblighi di acquisto o di fornitura intesi a garantire i quantitativi precedentemente consegnati (senza imporre obblighi di esclusiva) possono quindi essere giustificati per un periodo massimo di cinque anni.
- Gli accordi di licenza (con o senza esclusiva) relativi allo sfruttamento di privative industriali o di *know-how*.

È bene altresì ricordare che laddove le clausole accessorie esulino dal perimetro delle clausole standard sopra descritte e diano luogo a questioni nuove, tali clausole non saranno considerate automaticamente illecite sotto il profilo antitrust ma richiederanno un'analisi antitrust *ad hoc* e le parti dell'operazione potranno chiedere che la decisione della Commissione o dell'Autorità si pronunci espressamente anche sulla liceità di tali clausole.

2. Le nuove linee guida sulla Compliance Antitrust e prassi applicativa dell'AGCM

Nel corso degli ultimi anni, la *compliance antitrust* è divenuto un tema di primaria importanza per le aziende al fine di prevenire o mitigare i rischi connessi alla violazione delle norme europee e nazionali poste a tutela della piena concorrenza dei mercati.

123 Comunicazione della Commissione sulle restrizioni direttamente connesse e necessarie alle concentrazioni (2005/C 56/03).

Il percorso normativo che ha condotto a tale consapevolezza è relativamente recente, essendo partito con l'elaborazione da parte della Commissione Europea della guida "*Compliance matters. What companies can do better to respect EU competition rules*", nella quale, la Commissione Europea ha sottolineato l'importanza dell'adozione, da parte delle aziende, di programmi di compliance efficaci al fine di prevenire la violazione della normativa in materia di concorrenza dando così il successivo impulso a una serie di iniziative da parte della autorità di concorrenza nazionali in tale ambito.

Fino a quel momento, il rispetto della normativa *antitrust* era sostanzialmente basato quasi esclusivamente sull'effetto deterrente derivante dall'applicazione di elevate sanzioni *antitrust*, al fine di scoraggiare le imprese dal violare la normativa in considerazione delle pesanti ripercussioni economiche connesse.

Con l'accrescersi delle esigenza di garantire strumenti *corporate governance* efficaci connessi all'affermarsi di codici di condotta aziendali volti a delineare i principi etici e di conformità nella conduzione del business e la prevenzione degli illeciti, la necessità di adottare una prevenzione generale *ex-ante*, rispetto agli illeciti *antitrust*, si è resa sempre più necessaria.

In tale contesto, le aziende più virtuose, sempre più coscienti dei potenziali danni non solo economici ma altresì reputazionali derivanti da tali violazioni, avevano intrapreso, già prima degli sviluppi normativi che avremo modo di analizzare nel prosieguo, un percorso teso allo sviluppo di *best practices*. miranti ad assicurare il rispetto delle normative antitrust applicabili e la prevenzione di illeciti attraverso policies e strategie interne atte a rendere consapevole il personale aziendale, ad ogni livello, dell'importanza del rispetto della normativa antitrust e dei rischi derivanti da una sua eventuale violazione.

Con le nuove Linee Guida adottate dall'AGCM nel settembre 2018 i programmi di *compliance antitrust* hanno trovato definitivo riconoscimento nel nostro sistema di *public enforcement* e sono sviluppati dalle imprese con lo scopo di assicurare il rispetto della normativa in materia di concorrenza al fine di prevenire eventuali illeciti, informando e rendendo consapevole il personale delle conseguenze derivanti dalle violazioni di tale normativa. Oltre all'Italia, anche le Autorità nazionali garanti della concorrenza di numerosi altri Stati Membri hanno fornito indicazioni in materia di compliance antitrust. Nel 2010 l'allora *Office of Fair Trading* (OFT) del Regno Unito, oggi divenuto *Competition and Markets Authority*, aveva redatto il documento "*Drivers of Compliance and Non-compliance with Competition Law*"[124], che già prevedeva che le imprese potessero godere di una riduzione della sanzione in presenza di un programma di compliance conforme alle linee guida. Nel 2012 l'*Autorité de la Concurrance* francese aveva pubblicato un documento-quadro[125] indicante le condizioni alle quali l'adozione di un programma di *compliance antitrust* poteva essere considerato ai fini della *leniency*/immunità parziale o come attenuante negli illeciti in

124 Disponibile al seguente link: https://www.gov.uk/government/publications/business-drivers-of-compliance-and-non-compliance-with-competition-law.

125 Document-cadre du 10 février 2012 sur les programmes de conformité aux règles de concurrence, disponibile al seguente link: http://www.autoritedelaconcurrence.fr/doc/document_cadre_conformite_10_fevrier_2012.pdf.

cui la *leniency* non trovava applicazione[126]. A livello europeo, invece, la Commissione non prevede alcuna riduzione di sanzione in caso di adozione e finanche implementazione di un programma di *compliance*[127].

Le Linee Guida evidenziano il contenuto tipico di un programma di *compliance antitrust*, necessario a renderlo idoneo a svolgere la sua funzione di prevenzione degli illeciti consentendo quindi l'applicazione di una riduzione della sanzione comminata all'impresa in caso di violazione che ricordiamo, potrà arrivare fino a un massimo del 15%, nel caso in cui il programma abbia funzionato efficacemente, consentendo di individuare e interrompere tempestivamente l'infrazione prima dell'avvio del procedimento o consentendo di presentare una richiesta di *leniency*.

Ai sensi delle Linee Guida, ai fini del riconoscimento di un programma di compliance per ottenere la riduzione della sanzione, è centrale la sua idoneità a svolgere una funzione di prevenzione degli illeciti. Pertanto, il programma dovrà tenere in considerazione le caratteristiche dell'impresa, ossia la sua natura, la sua dimensione e la sua posizione di mercato, e il contesto di mercato in cui essa opera[128]. Tra gli elementi tipici qualificanti di un programma di *compliance* vi sono:

- il riconoscimento del valore della concorrenza (ad esempio, in un codice etico o di condotta aziendale) come parte integrante della cultura e della politica allocando a tale scopo sufficienti risorse aziendali e individuando un *Antitrust Compliance Officer* a tale scopo con l'attribuzione delle necessarie risorse;
- l'identificazione e la valutazione del rischio antitrust specifico dell'impresa, ossia la concreta analisi del rischio di porre in essere condotte anticompetitive che l'impresa si trova a fronteggiare. Una tale analisi permette infatti la corretta individuazione delle priorità di intervento, identificando le attività di prevenzione più adeguate e massimizzando in tal modo l'impiego delle risorse utilizzate per la realizzazione del programma;

126 I programmi di *leniency* (clemenza) hanno la finalità di indurre le imprese partecipanti a un cartello a collaborare in maniera attiva e determinante all'individuazione delle condotte illecite, in cambio della non applicazione, o sostanziale riduzione, delle sanzioni. Tali programmi sono qualificabili come sistemi premiali che mirano a destabilizzare i cartelli minando la fiducia reciproca tra coloro che vi partecipano. Trattandosi di un sistema premiale, l'efficacia dei programmi di clemenza è legata alla deterrenza delle sanzioni e alla effettività della loro applicazione, che il *leniency applicant* sarà propenso a evitare o attenuare attraverso una concreta attività di collaborazione.

127 Si veda, *ex multis*, CGUE 18.07.2013, causa C-501/11P, *Schindler Holding Ltd e altri contro Commissione europea, punti 113-114 e 140-144*. Si veda altresì la sentenza del TAR Lazio, causa n. 9048, pubblicata il 28.07.2017: "… *il riconoscimento delle circostanze attenuanti, sia nell'an che nel quantum, è il risultato dell'esercizio di un'ampia discrezionalità da parte di AGCM (ex multis, Cons. Stato, Sez. VI, 3 giugno 2014, n. 2838; id., 9 febbraio 2011, n. 896) la quale, peraltro, segue un orientamento più indulgente di quello della Commissione europea, secondo cui l'esistenza di un programma di compliance non funge da esimente, posto che, laddove vi sia stata una violazione della normativa antitrust, questa è la prova stessa dell'inefficacia di un siffatto programma*…".

128 L'AGCM ha già tenuto conto di tali criteri nella sua prassi: cfr. caso I789 - agenzia di modelli, sconto del 5% concesso "*tenendo conto anche delle piccole dimensioni economiche delle imprese*".

- attività di formazione e *know-how* interno, al fine di diffondere la conoscenza delle tematiche antitrust tra i dipendenti e i funzionari, rendendoli consapevoli dei rischi antitrust legati alla loro attività;
- la definizione di processi gestionali idonei a ridurre il rischio che vengano poste in essere condotte in violazione della normativa a tutela della concorrenza come, ad esempio, modelli di *reporting* interno che consentano al personale di segnalare rapidamente problematiche *antitrust* e ottenere chiarimenti su specifiche questioni, fino a consentire la denuncia, anche in forma anonima, di possibili violazioni;
- un sistema di misure disciplinari nel caso di violazione delle norme in materia di concorrenza da parte dei dipendenti e funzionari e un sistema di incentivi al rispetto delle procedure e dei processi di gestione del rischio *antitrust* come individuati dal programma;
- un monitoraggio periodico del programma e il suo eventuale aggiornamento, che tenga conto delle evoluzioni dell'attività dell'impresa e del contesto di mercato in cui essa opera, nonché dello stato dell'arte giurisprudenziale in materia.

Nella valutazione dei programmi di compliance l'AGCM ha piena discrezionalità nella considerazione degli stessi in termini di circostanza attenuante[129]. Il riconoscimento del beneficio all'impresa coinvolta in un procedimento è sottoposto alla presentazione di un'apposita richiesta all'AGCM, accompagnata da una relazione illustrativa che spieghi le ragioni per cui il programma possa ritenersi adeguato, nonché l'effettiva ed efficace applicazione/implementazione del programma. La valutazione del programma di compliance potrà essere condotta *ex ante* per quanto riguarda l'idoneità del programma a prevenire violazioni anticoncorrenziali o ex post per verificare se il programma abbia permesso la rapida individuazione e l'interruzione dell'infrazione. In tale contesto è bene ricordare che "*l'adozione di un programma di compliance adeguato ed efficace prima dell'apertura del procedimento …. è, in linea di principio, il caso più meritevole di considerazione in termini di benefici*"[130].

Sotto il profilo temporale, sono valutabili, ai fini dell'eventuale attribuzione dell'attenuante, solo i programmi di compliance adottati, attuati e trasmessi dalle parti del procedimento o prima dell'apertura dell'istruttoria o entro sei mesi dalla notifica dell'inizio del procedimento. In ogni caso, i programmi devono essere accompagnati da una relazione illustrativa e da documentazione che dimostri la concreta applicazione del programma.

Il trattamento premiale dei programmi di *compliance* potrà quindi variare in base al momento in cui viene adottato il programma stesso. Se questo viene adottato dopo l'avvio del procedimento istruttorio, è prevista la possibilità di una riduzione dell'importo base della sanzione fino al 5%. Per ottenere l'attenuante, è in ogni caso necessario che il programma venga attuato in tempo

129 Tar Lazio, n. 6080/2018.

130 Cfr. Punto 30 delle Linee Guida.

utile per essere valutato dall'AGCM nel corso del procedimento[131]. Per i programmi di *compliance* adottati prima dell'avvio del procedimento istruttorio, invece, l'ammontare della riduzione dipende dalla loro adeguatezza ed efficacia. In particolare, come già evidenziato la riduzione della sanzione potrà arrivare fino al 15% nel caso in cui i programmi di compliance adeguati e che hanno funzionato in maniera efficace, consentendo la tempestiva scoperta e interruzione dell'illecito prima della notifica dell'avvio del procedimento istruttorio. Nel caso in cui sia applicabile l'istituto della clemenza, l'attenuante del 15% può essere riconosciuta solo laddove l'impresa presenti la domanda di clemenza prima che l'AGCM abbia condotto ispezioni riguardanti la medesima ipotesi collusiva. Diversamente, i programmi di *compliance* che non hanno funzionato in maniera del tutto efficace, non consentendo la tempestiva scoperta e interruzione dell'illecito prima dell'avvio del procedimento dell'AGCM, ma che, tuttavia, non sono manifestamente inadeguati, possono permettere all'impresa di beneficiare di un trattamento premiale fino al 10% della sanzione, a condizione che essa integri adeguatamente il programma e inizi a darvi attuazione entro sei mesi dalla notifica dell'apertura dell'istruttoria[132]. L'ammontare dell'attenuante sarà valutato tenendo in considerazione la completezza del programma esistente al momento dell'avvio del procedimento istruttorio e delle modifiche attuate dall'impresa. Infine, i programmi di *compliance* manifestamente inadeguati[133] non permettono di beneficiare di trattamenti premiali. Tuttavia, è previsto che, nel caso in cui l'impresa presenti modifiche sostanziali al programma entro sei mesi dalla notifica dell'apertura dell'istruttoria, essa possa beneficiare di una potenziale riduzione della sanzione fino al 5%.

Nessuna attenuante potrà essere concessa a un'impresa recidiva che abbia già beneficiato di una riduzione della sanzione antitrust ad esito di una precedente istruttoria per aver adottato un programma di compliance. "*Ciò anche nel caso di modifiche del programma apportate dopo l'avvio del procedimento*"[134].

In generale, l'AGCM non considererà l'esistenza di un programma di *compliance* quale circostanza aggravante, salvo ipotesi eccezionali. Ad esempio, potrà

131 Paragrafo 29 delle Linee Guida: "… *La quantificazione dell'attenuante è commisurata alla completezza e alla qualità del programma presentato (adeguatezza), ma anche alla maggiore o minore possibilità da parte dell'Autorità di verificare la fattiva, concreta e continuativa implementazione e attuazione del programma*…".

132 Paragrafo 37 delle Linee Guida: "… *È onere dell'impresa dimostrare che: i) il programma da essa adottato era ben calibrato nella prevenzione dei rischi di commissione di attività anti-competitive e che l'attuazione del programma è stata curata con serietà e costanza per tutta la sua durata, benché non abbia in concreto impedito il verificarsi di una condotta illecita e la sua cessazione/denuncia tempestiva; ii) le modifiche al programma proposte dall'impresa sono idonee a colmare le lacune che avevano impedito l'efficace funzionamento del programma di compliance originario*…".

133 La manifesta inadeguatezza di un programma di *compliance* può risultare da gravi carenze dei contenuti, dall'assenza di elementi probatori circa l'effettiva attuazione, o il coinvolgimento dei vertici del management aziendale nella condotta illecita. Inoltre, un programma è sempre considerato manifestatamente inadeguato se, nei casi in cui sia applicabile l'istituto della clemenza, l'impresa o l'associazione di imprese non abbia posto fine all'illecito e non abbia presentato domanda di clemenza ai sensi dell'articolo 15, comma 2-bis della Legge n. 287/1990.

134 Paragrafi 40 e 41 delle Linee Guida. Al contrario, ciò potrebbe costituire una circostanza aggravante; si veda il paragrafo 46 delle Linee Guida.

sussistere un'aggravante qualora il programma sia stato strumentale all'occultamento dell'infrazione o abbia ostacolato l'attività istruttoria dell'AGCM[135].

Per una rassegna dei principali provvedimenti adottati dall'AGCM sino al giugno 2020 si rimanda all'Appendice del presente Capitolo.

135 Tali ipotesi potrebbero costituire un'aggravante secondo quanto previsto dal paragrafo 21 delle Linee Guida sulla modalità di applicazione dei criteri di quantificazione delle sanzioni amministrative pecuniarie irrogate dall'Autorità in applicazione dell'articolo 15, comma 1, della Legge n. 287/90.

APPENDICE 1

Appendice Capitolo 2

TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI: COME SCEGLIERE LO STRUMENTO PIÙ ADEGUATO?

Gli strumenti previsti dal GDPR

- Decisioni di adeguatezza (*Privacy Shield*)
- Garanzie adeguate (norme vincolanti d'impresa, clausole contrattuali standard, codici di condotta e certificazioni)
- Deroghe (consenso, esecuzione di un contratto, interesse legittimo)

Casi di trasferimento

- Il trasferimento di dati nell'ambito del gruppo imprenditoriale
- Il trasferimento di dati a clienti e fornitori
- Il trasferimento nell'ambito dei servizi di *cloud computing*

Gli ulteriori adempimenti

- Informativa
- Registro dei trattamenti
- DPIA

APPENDICE 2

Appendice Capitolo 4

MODALITÀ PRATICHE PER L'ADOZIONE DI UN MODELLO ORGANIZZATIVO E PER LE ATTIVITÀ DELL'ODV

Adozione iniziale e aggiornamento del Modello

- Ruolo "multifunzionale" del Modello
- Analisi dell'organizzazione e individuazione dei processi sensibili
- Valutazione, costruzione e adeguamento delle procedure e, in generale, del sistema di controllo preventivo
- Struttura del Modello
- Approvazione
- Data certa?
- Modifiche e aggiornamenti

Individuazione dell'OdV

- Composizione: Monocratico o collegiale?
- Componente interno? Situazioni di incompatibilità
- Modalità di nomina, contratto e compenso
- Durata in carica e possibilità di rielezione
- Revoca
- Prorogatio?

Modalità di diffusione e comunicazione del Modello

- Comunicazione iniziale: come e quali canali
- Clausole di rispetto
- Formazione: quando è davvero efficace?

Insediamento dell'OdV e individuazione delle modalità di azione e operative

- Regolamento di funzionamento
- *Budget* e modalità di spesa
- Piano di *audit* – *check list*
- Flussi informativi
- Reporting su base continuativa e su base periodica
- Tracciabilità e conservazione dei verbali e dei documenti

Gestione segnalazioni

- *E-mail* dedicata – piattaforma *whistleblowing*
- Coordinamento con i canali di Gruppo
- Riservatezza e *privacy*
- Sanzioni

Rapporti con gli altri organi di controllo e con il Revisore

- Riunioni periodiche e flussi informativi

APPENDICE 3

Appendice Capitolo 5

OPERAZIONI DI ACQUISIZIONE – TEMATICHE DI COMPLIANCE NEL PROCESSO E NELLA CONTRATTUALISTICA

Incidenza della privacy nella gestione del processo: la fase preparatoria

- La messa a disposizione dei dati della *target*: condizioni di legittimità (tema base giuridica e nomina responsabile esterno del possibile futuro acquirente);
- *Virtual data room* o servizi di *cloud storage* (tema della riservatezza delle informazioni scambiate e valutazione dei sistemi normalmente utilizzati, vdr o *dropbox*, con analisi dei pro e contro)

Aspetti di rilievo dalla attività di due diligence alla negoziazione dell'accordo

- L'attività di *due diligence*: *buy side* o *sell side*, una questione di prospettiva (se devo vendere devo sistemare la compliance per non perdere in appetibilità; se devo comprare c'è una serie di aspetti dei quali devo tenere conto e dai quali non posso prescindere)
- La trasmissione delle *liabilities* (es. Responsabilità 231: *asset deal/share deal*)
- Temi oggetto di analisi: *privacy, anticorruption* e *compliance 231* (quali aree e con quale profondità per un corretto rapporto costi benefici)

La negoziazione dello SPA

- Le dichiarazioni e garanzie. Estensione e operatività degli obblighi di indennizzo (materie da coprire, formulazione delle garanzie in materia di *compliance* 231, diversi approcci culturali e sensibilità)

Adempimenti dell'acquirente post acquisizione e possibili temi di attenzione

- Adempimenti *privacy* (adempimenti di informativa, registro trattamenti, eventuali *gap analysis* da fare, ecc.)
- Aggiornamento del modello 231 e figure (nuovi processi, nuova *governance* e possibile integrazione in un sistema preesitente di prevenzione del rischio).

APPENDICE 4

Appendice Capitolo 7

PROFILI DI COMPLIANCE ANTITRUST NELLE OPERAZIONI DI M&A E RECENTE PRASSI APPLICATIVA AGCM SULLA VALUTAZIONE DEI PROGRAMMI DI COMPLIANCE A FINI SANZIONATORI

Caso	Data	Attenuante (si/no)	Elementi valorizzati
I772 - Mercato del calcestruzzo Friuli Venezia Giulia	25 marzo 2015	No	(i) programma di compliance post-CRI non permette valutazione dell'efficacia della sua attuazione, e (ii) assenza di evidenza sulla attuazione e sull'impegno del management
I761 - Servizi Tecnici Accessori	16 dicembre 2015	No	Informazioni generiche, assenza di elementi di valutazione sull'efficacia dell'attuazione e sull'impegno del management.
I780 - Mercato del calcestruzzo in Veneto	22 dicembre 2015	Si (5%)	(i) programma di compliance implementato pre-CRI; (ii) evidenze sufficienti di attuazione (es. training).
		No	(i) programma di compliance implementato pre-CRI; MA (ii) mancanza di evidenze di concreta implementazione (solo delibera del CdA).
I777 - Tassi sui mutui nelle province di Bolzano e Trento	24 febbraio 2016	Si (10%)	(i) programma di compliance implementato (in parte) pre-CRI; **(ii) documentata adozione di un codice di condotta e svolgimento di attività seminariale rivolta ai dipendenti.**

Caso	Data	Attenuante (si/no)	Elementi valorizzati
I783 – Accordo tra operatori nel settore del Vending	8 giugno 2016	Si (10%)	(i) programma di compliance adottato pre-CRI; (ii) prevedevano il coinvolgimento del management, l'identificazione del personale responsabile del programma, l'organizzazione di attività di training, nonché la previsione di incentivi/disincentivi, sistemi di monitoraggio e di audit.
		No	(i) programma di compliance adottato post-CRI, non consente un'adeguata valutazione dell'efficacia di attuazione; (ii) non sufficienti le evidenze dell'attuazione del programma (es. produzione del solo manuale di Antitrust Compliance; oppure erano state riferite all'AGCM solo iniziative future).
4480 - Incremento prezzo farmaci Aspen	29 settembre 2016	Si ([5-10]%)	(i) adozione di un programma di antitrust compliance prima dell'avvio dell'istruttoria; (ii) aggiornamento e ampliamento del programma nel corso dell'istruttoria; (iii) peculiarità dell'abuso di sfruttamento oggetto del caso.
I789 – Agenzie di modelle	26 ottobre 2016	Si (5%)	(i) programma di compliance implementato pre-CRI; (ii) per l'associazione di categoria: modifica di alcuni meccanismi statutari da parte dell'associazione di categoria tra cui ammissibilità/permanenza nell'associazione solo in presenza di misure di antitrust compliance (adozione Codice di condotta + formazione antitrust per responsabili commerciali); (iii) per le imprese: adozione di misure di compliance predisposte/raccomandate dall'associazione di categoria.

Caso	Data	Attenuante (si/no)	Elementi valorizzati
I792 - Gare di ossigenoterapia e ventiloterapia	21 dicembre 2016	Si (5%)	(i) programmi di compliance posti in essere già in periodi antecedenti all'avvio del procedimento; (ii) aggiornamento dei programmi esistenti antecedentemente alla CRI.
		No	(i) programmi di compliance adottati pre-CRI; MA (ii) non implementati e/o aggiornati dopo l'avvio dell'istruttoria.
I742 - Tondini per cemento armato	19 luglio 2017	No	(i) programmi di compliance adottati tardivamente rispetto all'avvio del procedimento e successivamente o a ridosso della trasmissione della CRI; (ii) la documentazione depositata non consente un'adeguata valutazione dell'efficacia dell'attuazione del programma della quale non vi sono evidenze, anche con riferimento alla dimostrazione di un effettivo e concreto impegno al rispetto di quanto previsto nello stesso; (iii) alcune imprese già sanzionate dalla Commissione europea (caso non definitivo) avrebbero dovuto di per sé adottare idonei programmi di antitrust compliance proprio per evitare di incorrere nuovamente in violazioni della concorrenza analoghe a quelle già sanzionate.
I793 - Aumento prezzi del cemento	25 luglio 2017	Si (10%)	(i) programma di compliance adottati (in alcuni casi implementati) e comunicati pre-CRI; (ii) revisione di misure di antitrust compliance già esistenti.
		No	(i) mera adozione di un codice di condotta (pre-CRI); (ii) circostanza documentata solo in sede di presentazione della memoria finale.

Caso	Data	Attenuante (si/no)	Elementi valorizzati
I796 - Servizi di supporto e assistenza tecnica alla pa nei programmi cofinanziati dall'UE	18 ottobre 2017	Si (5%)	(i) programma di compliance adottati ben prima dell'invio della CRI oppure già esistenti prima dell'avvio del procedimento e aggiornati nel corso dell'istruttoria; (ii) comunicazione del programma di compliance all'AGCM prima della CRI.
		No	(i) adozione del programma di compliance ben oltre l'invio delle CRI; (ii) comunicazione del programma di compliance all'AGCM in sede di memorie finali. Tale circostanza non consente un'adeguata valutazione da parte dell'Autorità, in particolare, dell'efficacia della sua attuazione.
A484 - Unilever/ Distribuzione gelati	31 ottobre 2017	Si ([5-10%])	(i) programma di compliance rafforzato prima dell'avvio del procedimento; (ii) programma di compliance integrato, adeguandolo alle best practice nazionali ed europee, prima della notifica della CRI.
A493 - Poste Italiane/Prezzi recapito	13 dicembre 2017	No	(i) programma di compliance rimasto invariato nel corso dell'istruttoria; (ii) PI non ha apportato alcun elemento che abbia inciso sull'efficacia ed utilità del programma di compliance ai fini antitrust.
A500A - VODAFONE-SMS informativi aziendali	13 dicembre 2017	No	(i) l'adozione del programma di compliance, avvenuta prima dell'avvio dell'istruttoria, non ha di fatto impedito la condotta oggetto di contestazione; (ii) il programma di compliance ha fornito istruzioni ai dipendenti potenzialmente idonee a determinare l'ostacolo delle attività di acquisizione dei documenti da parte dell'Autorità.

Caso	Data	Attenuante (si/no)	Elementi valorizzati
I811- Finanziamenti auto	20 dicembre 2018	Si (10%)	(i) adozione del programma di compliance prima dell'avvio dell'istruttoria; (ii) programma di compliance ulteriormente integrato a seguito dell'avvio del procedimento e prima dell'invio della CRI; (iii) in caso di violazione delle indicazioni prescritte dai programmi, gli stessi prevedono un impianto sanzionatorio che appare possedere una valenza dissuasiva.
A511-Enel/ condotte anti-concorrenziali nel mercato della vendita di energia elettrica	20 dicembre 2018	Si (10%)	(i) programma di compliance consistente in modifiche e miglioramenti di un programma preesistente, su cui il gruppo era più volte intervenuto per tenere conto delle best practices europee e internazionali, è stato sottoposto prima dell'invio della CRI; (ii) prevede il coinvolgimento del management, l'identificazione del personale responsabile del programma, l'organizzazione di attività di training , nonché la previsione di incentivi/ disincentivi, sistemi di monitoraggio e di audit.
I806 - Affidamento appalti per attività antincendio boschivo	13 febbraio 2019	Sì (5%)	(i) programma di compliance, adottato dal 2015, non risulta essere efficace in quanto la società non ha scoperto e interrotto autonomamente la condotta illecita contestata prima delle ispezioni dell'Autorità; (ii) la società ha integrato e apportato modifiche anche significative al programma a seguito dell'avvio del procedimento e prima della CRI.
		Sì (10%)	(i) la società risulta avere ricevuto il programma di compliance dal consulente esterno incaricato della sua redazione in una data sostanzialmente contestuale con quella di ultimo accertamento della condotta.

Caso	Data	Attenuante (si/no)	Elementi valorizzati
I808- Gara Consip FM4- accordi tra i principali operatori del facility management	17 aprile 2019	Si (10%)	(i) adozione del programma di compliance antecedente all'avvio del Procedimento; (ii) il CNS ha adottato significative misure al fine di diffondere la cultura della concorrenza nel settore, quali in particolare l'adozione e l'aggiornamento di un programma di compliance antitrust , deliberato dal nuovo management nell'aprile del 2016 (nell'ambito di un processo di self cleaning intrapreso da CNS a partire dalla metà del 2015); (iii) il programma di compliance del CNS risulta dunque adeguato allo scopo ma non pienamente efficace, atteso che la Parte ha presentato istanza di leniency solo successivamente all'avvio del Procedimento e a distanza di oltre un anno rispetto alla sua adozione.
I814 - Diritti Internazionali	24 aprile 2019	Sì (5%)	(i) il programma di compliance risulta adottato e pienamente implementato solo successivamente all'apertura del procedimento; (ii) considerazione del tipo di illecito accertato.
I805 - Prezzi del cartone ondulato	**17 luglio 2019**	Sì (5%)	(i) introduzione tempestiva di un programma di compliance antitrust in linea con le best practices europee e internazionali.
		Sì (15%)	(i) per aver rafforzato un programma preesistente all'avvio dell'istruttoria, che aveva comunque consentito all'Autorità di intervenire nei confronti del cartello in seguito alla adesione del gruppo al programma di clemenza.
		No	(i) manifestamente inadeguato nella misura in cui, a fronte di una fattispecie in cui è applicabile l'istituto della clemenza, tale programma non ha indotto la parte a porre termine all'infrazione e a presentare domanda di clemenza; (ii) la parte non ha aggiornato il proprio programma di compliance.

Caso	Data	Attenuante (si/no)	Elementi valorizzati
I822- Consip/ Gara sicurezza e salute 4	18 settembre 2019	Si (5%)	(i) adozione del programma di compliance dopo l'avvio del procedimento; (ii) le società hanno fornito evidenza di aver posto in essere programmi di compliance che prevedono il pieno coinvolgimento del management e che si sono declinati nell'elaborazione di manuali antitrust, in seminari a cui ha partecipato la dirigenza delle società e il personale che opera nelle aree sensibili sotto il profilo antitrust, nonché nella nomina di responsabili antitrust con il compito di monitorarne la puntuale e concreta attuazione.
I820 - Fatturazione mensile con rimodulazione tariffaria	28 gennaio 2020	Sì (5%)	(i) adozione di un programma di compliance aziendale prima dell'avvio del procedimento; (ii) l'Autorità ha ritenuto che tale programma di compliance, così come strutturato prima dell'avvio del procedimento, non abbia svolto efficacemente la propria funzione di prevenzione degli illeciti antitrust all'interno dell'azienda (a mero titolo esemplificativo, il Top Management delle aziende era coinvolto direttamente nella realizzazione degli illeciti); (iii) ciononostante, l'Autorità ha valutato positivamente il le modifiche apportate al programma di compliance aziendale apportate dopo l'avvio del procedimento.

Caso	Data	Attenuante (si/no)	Elementi valorizzati
A514 - Condotte fibra Telecom Italia	25 febbraio 2020	Sì (5%)	(i) adozione di un programma di compliance aziendale prima dell'avvio del procedimento; (ii) l'Autorità ha ritenuto che tale programma di compliance, così come strutturato prima dell'avvio del procedimento, non abbia svolto efficacemente la propria funzione di prevenzione degli illeciti antitrust all'interno dell'azienda (a mero titolo esemplificativo, il Top Management delle aziende era coinvolto direttamente nella realizzazione degli illeciti); (iii) ciononostante, l'Autorità ha valutato positivamente il le modifiche apportate al programma di compliance aziendale apportate dopo l'avvio del procedimento.

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 i curatori e i co-autori del Quaderno stesso, sotto specificati), ove è stata costituita 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.

Hanno contribuito a questo Quaderno:

L'Avv. **Irene Picciano**, curatrice e co-autrice del Capitolo 7 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)

L'Avv. **Antonio Bana**, curatore e co-autore del Capitolo 6 di questo Quaderno, dello Studio Legale Bana di Milano (www.studiobana.it)

L'Avv. **Alessandra Anselmi**, co-autrice del Capitolo 6 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)

L'Avv. **Micaela Barbotti**, co-autrice del Capitolo 4 di questo Quaderno, di A&A Studio Legale (www.albeeassociati.it)

L'Avv. **Francesca Chiara Bevilacqua**, co-autrice del Capitolo 6 di questo Quaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)

L'Avv. **Pietro Boccaccini**, co-autore del Capitolo 3 di questo Quaderno, dello Studio Legale Associato King & Wood Mallesons (www.kwm.com/.it)

L'Avv. **Deborah Bolco**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.pavia-ansaldo.it)

L'Avv. **Tiziana Boneschi**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Associato LCA (www.lcalex.it)

L'Avv. **Eva Cruellas Sada**, co-autrice del Capitolo 7 di questo Quaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)

L'Avv. **Simona Custer**, co-autrice del Capitolo 36 di questo Quaderno, di A&A Studio Legale (www.albeeassociati.it)

L'Avv. **Paola De Pascalis**, co-autrice del Capitolo 6 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, di SILS Studio Italiano Legale Societario (www.silsitalia.it)

L'Avv. **Eugenia Gambarara**, co-autrice del Capitolo 7 di questo Quaderno, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)

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

L'Avv. **Pietro Magri**, co-autore del Capitolo 6 di questo Quaderno, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)

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

L'Avv. **Marta Margiocco**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Cocuzza e Associati (www.cocuzzaeassociati.it)

L'Avv. **Guido 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 5 di questo Quaderno, dello Studio Legale Associato CastaldiPartners (www.castaldimourre.com/it)

L'Avv. **Mariangela Papadia**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.pavia-ansaldo.it)

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

L'Avv. **Josephine Romano**, co-autrice del Capitolo 4 di questo Quaderno, dello Studio Legale Associato Deloitte Legal (www.deloitte.com/it)

L'Avv. **Roberto Tirone**, co-autore del Capitolo 4 di questo Quaderno, dello Studio Legale Cocuzza e Associati (www.cocuzzaeassociati.it)

Pubblicazione giuridica n° 18 di ASLA

A cura del Gruppo di lavoro sulla Corporate Compliance
Curatori: Antonio Bana e Irene Picciano
Editor: Ezio Rotamartir

I materiali raccolti nella presente pubblicazione hanno valore soltanto esemplificativo e non vanno intesi come specifiche raccomandazioni di ASLA.

Impaginazione ed elaborazioni grafiche: Ezio Rotamartir
Progetto grafico originale: Edoardo Steiner

www.aslaitalia.it

Hanno contribuito a questo Quaderno:

L'Avv. **Irene Picciano**, curatrice e co-autrice del Capitolo 7 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)
L'Avv. **Antonio Bana**, curatore e co-autore del Capitolo 6 di questo Quaderno, dello Studio Legale Bana di Milano (www.studiobana.it)

L'Avv. **Alessandra Anselmi**, co-autrice del Capitolo 6 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)
L'Avv. **Micaela Barbotti**, co-autrice del Capitolo 4 di questo Quaderno, di A&A Studio Legale (www.albeeassociati.it)
L'Avv. **Francesca Chiara Bevilacqua**, co-autrice del Capitolo 6 di questo Quaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)
L'Avv. **Pietro Boccaccini**, co-autore del Capitolo 3 di questo Quaderno, dello Studio Legale Associato King & Wood Mallesons (www.kwm.com/.it)
L'Avv. **Deborah Bolco**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.pavia-ansaldo.it)
L'Avv. **Tiziana Boneschi**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Associato LCA (www.lcalex.it)
L'Avv. **Eva Cruellas Sada**, co-autrice del Capitolo 7 di questo Quaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)
L'Avv. **Simona Custer**, co-autrice del Capitolo 36 di questo Quaderno, di A&A Studio Legale (www.albeeassociati.it)
L'Avv. **Paola De Pascalis**, co-autrice del Capitolo 6 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, di SILS Studio Italiano Legale Societario (www.silsitalia.it)
L'Avv. **Eugenia Gambarara**, co-autrice del Capitolo 7 di questo Quaderno, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)
L'Avv. **Giacomo Gori**, co-autore del Capitolo 2 di questo Quaderno, dello Studio Legale Cocuzza e Associati (www.cocuzzaeassociati.it)

www.aslaitalia.it

L'Avv. **Pietro Magri**, co-autore del Capitolo 6 di questo Quaderno, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)
L'Avv. **Andrea Mantovani**, co-autore del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)
L'Avv. **Marta Margiocco**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Cocuzza e Associati (www.cocuzzaeassociati.it)
L'Avv. **Guido 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 5 di questo Quaderno, dello Studio Legale Associato CastaldiPartners (www.castaldimourre.com/it)
L'Avv. **Mariangela Papadia**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.pavia-ansaldo.it)
L'Avv. **Eva Reggiani**, co-autrice del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)
L'Avv. **Josephine Romano**, co-autrice del Capitolo 4 di questo Quaderno, dello Studio Legale Associato Deloitte Legal (www.deloitte.com/it)
L'Avv. **Roberto Tirone**, co-autore del Capitolo 4 di questo Quaderno, dello Studio Legale Cocuzza e Associati (www.cocuzzaeassociati.it)

ASLA, **Associazione Studi Legali Associati**, *www.aslaItalia.it*, editrice di questo Quaderno, comprende circa cento fra i principali Studi nazionali e di affiliazione estera operanti in Italia (fra cui quelli a cui appartengono i curatori e i co-autori del Quaderno stesso, sopra specificati), ove è stata costituita 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