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

CORPORATE COMPLIANCE ROUND TABLES 2017

Atti del convegno con sette tavole rotonde con la partecipazione di dodici 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 MANUELA BIANCHI E IRENE PICCIANO
CON TESTI DI ANDREA MANTOVANI, EVA REGGIANI, FRANCESCO DE BIASI, MARCO SORRENTINO, ADRIANO D'OTTAVIO, DEBORAH BOLCO, MARIANGELA PAPADIA, STEFANO CANCARINI, IRENE PICCIANO, EVA CRUELLAS SADA, EUGENIA GAMBARARA, MANUELA BIANCHI, MICAELA BARBOTTI, ROBERTO TIRONE, JOSEPHINE ROMANO, PIETRO ORZALESI, ANTONIO BANA, FRANCESCA CHIARA BEVILACQUA, GIAN LUIGI GATTA.

CORPORATE COMPLIANCE ROUND TABLES 2017

Atti del convegno con sette tavole rotonde con la partecipazione di dodici 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, Eva Reggiani e Francesco De Biasi

Novità interpretative in materia di protezione dei dati personali

Novità interpretative in materia di protezione dei dati personali nel contesto dei controlli datoriali sui dipendenti

sommario: 1. La formulazione dell'art. 4, l. n. 300 del 21 maggio 1970 (lo "Statuto dei Lavoratori") all'esito del "Jobs Act" – 2. L'installazione di strumenti per sorvegliare a distanza l'attività dei lavoratori – 3. L'individuazione dell'ambito dell'esenzione degli strumenti di cui al comma 2 – 3a. Gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" – 3b. Gli "strumenti di registrazione degli accessi e delle presenze" – 4. L'utilizzabilità "a tutti i fini" delle informazioni raccolte. Questioni in materia di data protection – 5. La verifica della condotta di dipendenti sospettati di comportamenti contrari ai propri doveri: la sorte dei c.d. "controlli difensivi"

1. La formulazione dell'art. 4, l. n. 300 del 21 maggio 1970 (lo "Statuto dei Lavoratori") all'esito del "Jobs Act"

La consapevolezza della necessità di rivedere la disciplina sui controlli a distanza dei lavoratori "*tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore*"[1] ha portato all'approvazione del decreto legislativo n. 151 del 14 settembre 2015 (il "Jobs Act") il cui art. 23 ha riscritto l'art. 4 dello Statuto dei Lavoratori. Il Jobs Act ha altresì modificato l'art. 171 del decreto legislativo n. 196 del 30 giugno 2002 (il "Codice Privacy"), prevedendo che la violazione delle disposizioni di cui al comma 1 dell'art. 4 dello Statuto dei Lavoratori è punita con le sanzioni di cui all'art. 38 del medesimo Statuto dei Lavoratori[2].

1 Cfr. art. 7(f) della legge delega n. 183 del 10 dicembre 2014.

2 L'art. 38 citato prevede, salvo che il fatto non costituisca più grave reato, la sanzione dell'ammenda da € 154 a € 1.549 o l'arresto da 15 giorni a un anno (comma 1) e, nei casi più gravi, le pene dell'arresto e dell'ammenda sono applicate congiuntamente (comma 2 e, in questi, l'autorità giudiziaria ordina la pubblicazione della sentenza penale ai sensi dell'art. 36 c.p.). Il comma 3 prevede che qualora, alla luce delle condizioni economiche del reo, l'ammenda stabilita nel comma 1 si presuma essere inefficace anche se applicata nel massimo, il giudice ha la facoltà di aumentarla sino al quintuplo. Per completezza, si segnala che l'art. 171 del Codice Privacy è stato da ultimo modificato dall'art. 15 del decreto legislativo n. 101 del 10 agosto 2018 recante "disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali

L'attuale formulazione del comma 1 dell'art. 4 non riporta più l'espresso divieto di controlli a distanza sui lavoratori[3] e prevede che "*gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale*". Tali impianti possono essere installati previo accordo sindacale[4] oppure, in mancanza di tale accordo, previa autorizzazione della direzione territoriale del lavoro (ora ispettorato territoriale del lavoro)[5].

Il comma 2 esclude dall'ambito di applicazione del comma 1 (e, dunque, dei vincoli di finalità e del regime autorizzativo ivi previsti) gli strumenti "*utilizzati dal lavoratore per rendere la prestazione lavorativa*" nonché gli strumenti "*di registrazione degli accessi e delle presenze*".

Infine, il comma 3 prevede che le informazioni raccolte in base ai commi 1 e 2 siano utilizzabili "*a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196*".

È evidente come, condizionando l'utilizzabilità dei dati raccolti al "*rispetto*" di quanto previsto dalla normativa in materia di protezione dei dati personali, la novella abbia imposto un'effettiva integrazione tra la disciplina laburistica e quella concernente la *data protection*[6]. Ciò significa, ad avviso di chi scrive, che le disposizioni in materia di protezione dei dati personali debbano considerarsi un quadro normativo generale che delimita i contorni di ciò che è lecito e ciò che non lo è nel contesto delle attività dei controlli sui dipendenti, dovendo fungere da guida nella comprensione dell'effettiva portata applicativa della norma laburistica[7].

Ne consegue, in particolare, che l'uso delle informazioni raccolte, anche se possibile in relazione qualsiasi fine connesso al rapporto di lavoro, è in concreto confinato nell'ambito del rispetto delle norme in materia di protezione dei dati personali che impongono al datore di lavoro di comunicare preventivamente al lavoratore una serie di informazioni concernenti il trattamento dei dati, come anche, ad esempio, dai principi di pertinenza e minimizzazione del trattamento[8].

---

dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

3 Il comma 1 dell'art. 4 dello Statuto dei Lavoratori ante Jobs Act prevedeva quanto segue: "*è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori*".

4 Tale accordo è stipulato "*dalla rappresentanza sindacale unitaria oppure dalla rappresentanza sindacale aziendale. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale*" (art. 4, comma 1, Statuto dei Lavoratori).

5 Nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più direzioni territoriali del lavoro (ora ispettorati territoriali del lavoro), tale autorizzazione viene rilasciata dalla sede centrale dell'Ispettorato Nazionale del Lavoro.

6 Cfr. anche G. Proia, *Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza, in Riv. It. Dir. Lav.*, fasc.4, 2016, p. 547 ss.

7 Fermo restando che, nella prospettiva del legislatore, la norma laburistica è costruita come norma speciale rispetto a quella generale sulla *privacy*. Conseguentemente, in linea generale, dovrebbe ritenersi che le disposizioni in tema di *data protection* non siano applicabili ove esse risultino derogate o specificate dalla norma laburistica, che è destinata a prevalere in caso di contrasto (cfr. G. Proia, *op. loc. cit.*).

8 Cfr. anche G. Proia, *op. loc. cit.*

2. L'installazione di strumenti per sorvegliare a distanza l'attività dei lavoratori

La modifica del primo comma dell'art. 4 dello Statuto dei Lavoratori non implica, ad avviso di chi scrive, che sia lecito installare impianti o utilizzare dispositivi la cui unica finalità sia la sorveglianza a distanza dell'attività dei lavoratori[9].

Infatti, come precisato dal Garante per la protezione dei dati personali (il "Garante") nel provvedimento n. 547 del 22 dicembre 2016[10], la disciplina in materia di controlli a distanza, anche a seguito delle modifiche apportate dal Jobs Act, "*non consente l'effettuazione di attività idonee a realizzare (anche indirettamente) il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore*". Sul tema, si veda anche la raccomandazione del Consiglio d'Europa del 1° aprile 2015, CM/Rec(2015)5[11], il cui punto 15 prevede che "*non dovrebbe essere consentito introdurre e utilizzare sistemi informativi e tecnologie aventi per scopo diretto e primario la sorveglianza dell'attività e del comportamento dei dipendenti*".

3. L'individuazione dell'ambito dell'esenzione degli strumenti di cui al comma 2: gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" e gli "strumenti di registrazione degli accessi e delle presenze"

Il legislatore non ha ritenuto di definire gli "*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa*" e gli "*strumenti di registrazione degli accessi e delle presenze*" che ha esentato dall'applicazione dei vincoli di finalità e del regime autorizzativo di cui al comma 1. Di seguito, si fornisce una panoramica dei principali orientamenti interpretativi sul punto.

a. Gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"

I primi chiarimenti su cosa possa ritenersi ricompreso nel novero degli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa sono stati forniti dal Ministero del Lavoro e delle Politiche Sociali, con una nota del

9 Cfr. M.T. Salimbeni, *La riforma dell'articolo 4 dello Statuto dei Lavoratori: l'ambigua risolutezza del legislatore, in Rivista Italiana di Diritto del Lavoro, 4, 2015, p. 602, dove si sostiene che "si può con sicurezza affermare che la novella ha mantenuto in vita il divieto di uso di apparecchiature che abbiano quale esclusiva finalità il controllo a distanza dei lavoratori*". Cfr. anche M. Silvestri, *Controlli difensivi del datore di lavoro: limiti della loro utilizzabilità - il commento, in Lav. Giur., 2017, p. 863: "[c]on la riforma dell'art. 23 del D.Lgs. n. 151/2015, il comma 1 nella sua precedente formulazione è stato cancellato, ma appare evidente anche dalla lettura della nuova versione dell'art. 4 che il generale divieto del controllo a distanza delle attività lavorative esiste ancora: se il datore di lavoro potesse liberamente adottare dispositivi volti alla vigilanza dei lavoratori (es. la telecamera che inquadra la postazione di lavoro o l'applicazione installata sullo smartphone che registra gli spostamenti del lavoratore) non avrebbero senso gli specifici limiti introdotti dal comma 1*".

10 Consultabile al seguente *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5958296.

11 Consultabile al seguente *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4224268.

18 giugno 2015[12] (e, dunque, quando il Jobs Act non era ancora stato approvato), che precisava che tali strumenti sono quelli che "servono" al lavoratore "*per adempiere la prestazione*" e che costituiscono l'equivalente moderno degli "attrezzi da lavoro". Pertanto, "*nel momento in cui tale strumento viene modificato (ad esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione: in tal caso, infatti, da strumento che 'serve' al lavoratore per rendere la prestazione il pc, il tablet o il cellulare divengono strumenti che servono al datore per controllarne la prestazione. Con la conseguenza che queste 'modifiche' possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione*".

Successivamente all'entrata in vigore del Jobs Act, l'Ispettorato Nazionale del Lavoro, con circolare n. 2 del 7 novembre 2016 recante le indicazioni operative circa l'utilizzazione di impianti GPS[13], ha ulteriormente chiarito che: (i) il dato letterale della norma "*porta a considerare quali strumenti di lavoro quegli apparecchi, dispositivi, apparati e congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto e che per tale finalità sia[no] stati posti in uso e messi a sua disposizione*"; (ii) con specifico riferimento agli impianti GPS, "*in linea di massima, e in termini generali, si può ritenere che i sistemi […] di geolocalizzazione rappresentino un elemento 'aggiunto' agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa ma per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro*" e, pertanto "*solo in casi del tutto particolari […]*[14] *si può ritenere che gli stessi finiscano per 'trasformarsi' in veri e propri strumenti di lavoro*", come tali non soggetti a previo accordo sindacale o autorizzazione.

Anche il Garante pare attualmente orientato a ritenere che rientrino nell'esenzione del comma 2 soltanto gli strumenti "indispensabili" per rendere la prestazione lavorativa. In proposito, nel provvedimento n. 479 del 16 novembre 2017[15], il Garante ha ritenuto che "i*l sistema di gestione delle attese allo sportello, non ponendosi come indispensabile per rendere la prestazione lavorativa […], rientra in quegli strumenti anche organizzativi, dai quali può indirettamente derivare il controllo a distanza dell'attività dei lavoratori, con conseguente necessità di attivare le procedure […] previste*" dalla normativa in commento. Analogamente, nel provvedimento n. 139 del 8 marzo 2018[16], il Garante ha ritenuto, in un caso nel quale "*le accertate*

12 Consultabile al seguente *link*: http://www.lavoro.gov.it/stampa-e-media/Comunicati/Pagine/20150618-Controlli-a-distanza.aspx.

13 Tale circolare, vincolante per gli Ispettorati Territoriali del Lavoro, ha superato l'orientamento adottato dalla Direzione interregionale del Lavoro di Milano la quale, con nota del 10 maggio 2016, aveva ritenuto che "*l'automezzo ed il GPS servono entrambi, inscindibilmente ed unitariamente, al lavoratore per rendere la sua prestazione lavorativa*" e, dunque, che "*l'auto fornita in uso ai dipendenti per eseguire la propria prestazione lavorativa è sicuramente strumento di lavoro e lo è nella sua unicità: quindi il sistema GPS (pur se montato successivamente alla originaria consegna del veicolo) non è da considerare separatamente dall'auto cui accede e per la sua installazione non è necessario il preventivo accordo sindacale o la preventiva autorizzazione ministeriale*".

14 L' Ispettorato Nazionale del Lavoro si riferisce ai casi in cui, ad esempio, la prestazione lavorativa non possa essere resa senza ricorrere all'uso di tali strumenti oppure l'installazione sia imposta da obblighi di legge o regolamentari.

15 Consultabile al seguente *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7355533.

16 Consultabile al seguente *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8163433.

caratteristiche del sistema e il novero delle operazioni di trattamento da queste rese possibili non risultano in via esclusiva funzionali alla mera gestione del contatto con il cliente e, dunque, al mero svolgimento della prestazione lavorativa […] il sistema così configurato non può essere considerato 'strument[o] utilizzat[o] dal lavoratore per rendere la prestazione lavorativa'".

Con riferimento agli strumenti informatici in dotazione al lavoratore (quali, ad esempio, *computer, tablet e cellulari*), il Tribunale di Roma ha recentemente precisato[17] che debbono considerarsi strumenti di lavoro quegli strumenti in relazione ai quali il lavoratore svolge un "*ruolo attivo nel* [loro] *utilizzo*" perché *"concretamente impiegat*[i] *dal dipendente nello svolgimento delle mansioni*", a differenza di quanto accade con riferimento agli impianti e strumenti di controllo di cui al comma 1, art. 4 Statuto dei Lavoratori, in relazione ai quali il lavoratore è sempre "*soggetto passivo*"[18].

In realtà, come segnalato in dottrina, il Tribunale di Roma si è limitato a presumere che tutti gli applicativi e *software* incorporati nei dispositivi in uso alla ricorrente fossero da considerare funzionali all'esecuzione della prestazione lavorativa, senza porsi la questione se tali dispositivi ricomprendessero anche applicativi o *software* non necessari per rendere la prestazione lavorativa[19].

A tal fine, è utile il provvedimento n. 303 del 13 luglio 2016[20], nel quale il Garante ha precisato che possono rientrare nella nozione di strumenti funzionali all'esecuzione della prestazione lavorativa di cui al comma 2 dell'art. 4 dello Statuto dei Lavoratori "*solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza", dei quali costituiscono parte integrante anche "i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cosiddetta 'envelope' del messaggio, per una breve durata non superiore comunque ai sette giorni; sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso)*"[21].

17 Cfr. Tribunale di Roma, sentenza del 24 marzo 2017.

18 Pertanto, sulla falsariga della citata nota del 18 giugno 2015 del Ministero del Lavoro e delle Politiche Sociali, il Tribunale di Roma ha ritenuto che "*l'uso degli strumenti informatici deve essere assimilato ad un mero strumento di lavoro messo a disposizione del lavoratore per rendere la prestazione; quindi i computer, i tablet ed i cellulari devono essere considerati come i moderni attrezzi di lavoro utilizzabili senza autorizzazione nel caso in cui vengano attribuiti al lavoratore per rendere la prestazione lavorativa oggetto del contratto di lavoro*". Nel caso di specie, la ricorrente ricopriva il ruolo di impiegata amministrativa e, dunque, il Tribunale di Roma ha ritenuto che il *computer* e la casella di posta elettronica non potessero che essere considerati quali strumenti di lavoro necessari allo svolgimento della prestazione lavorativa e, come tali, non soggetti al regime di cui al comma 1, art. 4 Statuto dei Lavoratori.

19 Cfr. E. Gramano, *La rinnovata (ed ingiustificata) vitalità della giurisprudenza in materia di controlli difensivi,* in *Diritto delle Relazioni Industriali*, I, 2018, p. 265 e ss. e la dottrina ivi richiamata.

20 Consultabile al seguente *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5408460.

21 Cfr. par. 4.3 del provvedimento citato, dove il Garante ha altresì precisato che apparati e *sistemi software che "consentono, con modalità non percepibili dall'utente (c.d. in background) e in modo del tutto indipendente rispetto alla normale attività dell'utilizzatore (cioè senza alcun impatto o interferenza sul lavoro del dipendente),*

Da ultimo, si segnala che l'Ispettorato Nazionale del Lavoro, con circolare n. 5 del 19 febbraio 2018 recante le "*indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e altri strumenti di controllo*", richiamando il provvedimento del Garante n. 513 del 12 novembre 2014[22], ha ritenuto che "*il riconoscimento biometrico, installato sulle macchine con lo scopo di impedire l'utilizzo della macchina a soggetti non autorizzati, necessario per avviare il funzionamento della stessa, può essere considerato uno strumento indispensabile a "…rendere la prestazione lavorativa…*" e pertanto si possa prescindere [...] sia dall'accordo con le rappresentanze sindacali sia dal procedimento amministrativo di carattere autorizzativo previsto dalla legge".

b. Gli "strumenti di registrazione degli accessi e delle presenze"

Si tratta di quegli strumenti il cui scopo consiste essenzialmente nella registrazione dell'entrata e dell'uscita dal lavoro e che, quindi, "*non implica*[no] *un controllo sull'attività dei lavoratori consistendo in una mera verifica del rispetto dell'orario di lavoro*"[23]. Tuttavia, la giurisprudenza (seppure relativamente alla vecchia formulazione dell'art. 4 dello Statuto dei Lavoratori) ha precisato che, qualora lo strumento di registrazione degli accessi non operi quale mero rilevatore di presenza, ma raccolga altresì informazioni circa le sospensioni, i permessi e le pause, è necessario l'accordo sindacale o l'autorizzazione dell'ispettorato del lavoro, atteso che tali strumenti consentirebbero di realizzare "*in concreto, un controllo costante e a distanza circa l'osservanza da parte degli stessi (dipendenti) del loro obbligo di diligenza, sotto il profilo del rispetto dell'orario di lavoro*"[24].

Più problematico è il tema del tracciamento della mobilità dei dipendenti all'interno dell'azienda. Si è sostenuto, in dottrina, che la formulazione letterale del comma 2 dell'art. 4 dello Statuto dei lavoratori supporterebbe una lettura ampia della norma che, dunque, ricomprenderebbe non solo gli strumenti che registrano entrata e uscita dall'azienda ma anche quelli che registrano la presenza dei dipendenti e/o il loro transito dai vari dipartimenti o uffici[25]. Vero è che strumenti di questo tipo potrebbero comportare "*un'estesa potenzialità di controllo sull'attività dei lavoratori, che va intesa come ogni comportamento lavorativo o no che si tenga in azienda*"[26] e che, quindi, un'interpretazione della disposizione maggiormente in linea con la *ratio* ad essa sottesa, farebbe propendere

operazioni di 'monitoraggio', 'filtraggio', 'controllo' e 'tracciatura' costanti e indiscriminati degli accessi a internet o al servizio di posta elettronica" non rientrerebbero in tale nozione.

22 Consultabile al seguente *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992&zx=oc16qotsbp0s.

23 Cfr. M. T. Salimbeni, op. loc. cit. Cfr. anche I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour & Law Issues*, 1, 2016.

24 Cfr. Cass. Civ. n. 9904 del 13 maggio 2016 e Cass. Civ. n. 17531 del 14 luglio 2017.

25 Cfr. I. Alvino, *op. cit.*, p. 22: "*la congiunzione 'e' collocata fra i termini 'accessi' e 'presenze' assume un valore disgiuntivo destinato ad esprimere che il concetto di 'accesso' ha un suo autonomo significato da considerare indipendentemente da quello di 'presenza'. Lo strumento al quale la disposizione fa riferimento non è dunque solo quello che consente di rilevare gli accessi del lavoratore sul luogo di lavoro, ai soli fini della rilevazione della presenza e dunque del rispetto dell'orario di lavoro, ma qualunque strumento idoneo a registrare l'accesso e/o la presenza in determinati locali aziendali*".

26 Cfr. M. T. Salimbeni, *op. cit.*, p. 604.

per una disapplicazione soltanto "parziale" del comma 1 a tali strumenti, nel senso che tali strumenti dovrebbero poter essere utilizzati soltanto in presenza di una delle condizioni dettate dal comma 1 (*i.e.*, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale). Diversamente opinando, si consentirebbe l'installazione e l'utilizzo di impianti preordinati unicamente al controllo dello spostamento dei lavoratori all'interno dell'azienda, ledendo la dignità e la riservatezza dei lavoratori[27].

4. L'utilizzabilità "a tutti i fini" delle informazioni raccolte. Questioni in materia di data protection

Il comma 3 dell'art. 4 dello Statuto dei Lavoratori consente l'utilizzabilità "*a tutti i fini connessi al rapporto di lavoro*" delle informazioni e dei dati raccolti sia mediante gli impianti e altri strumenti di cui al comma 1 sia mediante gli strumenti utilizzati per rendere la prestazione lavorativa oppure per la registrazione di accessi e presenze di cui al comma 2.

L'espressione "a tutti i fini" ricomprende, come precisato da una recente ordinanza del Tribunale di Roma[28], "*anche il controllo sull'osservanza degli obblighi discendenti dal rapporto di lavoro*" e i conseguenti fini disciplinari[29].

Tuttavia, affinché tali informazioni e dati siano utilizzabili, è necessario che (i) il lavoratore sia stato adeguatamente informato circa le modalità d'uso degli strumenti e di effettuazione dei controlli; e (ii) in ogni caso, venga rispettata la normativa in materia di protezione dei dati personali.

Come precisato dal Garante, l'obbligo di fornire ai lavoratori una preventiva informativa sussiste comunque ed è "*indipendente rispetto all'eventuale determinazione assunta* [dal datore di lavoro] *circa la possibilità di utilizzare le informazioni raccolte 'a tutti i fini connessi al rapporto di lavoro*'"[30].

Relativamente al contenuto che deve avere l'informativa data al lavoratore per poter essere ritenuta "adeguata", un punto di riferimento tutt'oggi essenziale è costituito dalle linee guida del Garante per posta elettronica e internet del 1° marzo 2007 (le "Linee Guida")[31]. Le Linee Guida, escludendo l'ammissibilità di controlli prolungati, costanti o indiscriminati sull'attività dei dipendenti, individuano, fra l'altro, l'opportunità che i datori di lavoro adottino un

27 Cfr. M. T. Salimbeni, *op. cit.*, p. 605. La disapplicazione del comma 1 sarebbe soltanto parziale poiché l'Autrice ritiene che l'accordo sindacale o l'autorizzazione dell'ispettorato del lavoro non sarebbero necessarie.

28 Cfr. Tribunale di Roma, ordinanza n. 57668 del 13 giugno 2018.

29 Ovviamente, l'uso consentito è solo quello che abbia ad oggetto fini legittimi. Valga, al riguardo, considerare l'art. 8 dello Statuto dei Lavoratori, che vieta indagini su fatti "*sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore*" (cfr. G. Proia, *op. loc. cit.*).

30 Cfr. provvedimento n. 479 del 16 novembre 2017 citato *supra*. Nel caso di specie, la società aveva sostenuto di non aver fornito alcuna specifica informativa al personale dipendente relativamente al trattamento dei dati personali di questi ultimi raccolti mediante il sistema di gestione delle attese allo sportello poiché non intendeva utilizzare i dati personali del personale dipendente raccolti da tale sistema per le finalità connesse allo svolgimento del rapporto di lavoro..

31 Consultabili al seguente *link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522&zx=vqpl74vzk4za.

disciplinare interno che precisi se, e in quale misura, il datore di lavoro si riserva di effettuare controlli, anche saltuari o occasionali, indicando le ragioni specifiche per cui verrebbero effettuati e le relative modalità[32]. Sul tema, va menzionata anche la sentenza resa dalla Grande Camera della Corte Europea dei Diritti dell'Uomo (la "Corte EDU") del 5 settembre 2017 nel caso *Bărbulescu* c. *Romania*[33], nella quale la Corte EDU, nel ritenere sussistente la violazione dell'art. 8 della Convenzione Europea dei Diritti dell'Uomo[34], ha rilevato, fra l'altro, che il lavoratore, sebbene informato del divieto di utilizzare per fini personali i dispositivi aziendali, non era stato previamente informato: (i) della possibilità che le comunicazioni potessero essere monitorate; (ii) dell'ambito e la natura delle attività di monitoraggio effettuate dal proprio datore di lavoro; (iii) della possibilità che questi potesse avere accesso anche al contenuto dei messaggi inviati.

L'entrata in vigore del Regolamento (UE) n. 2016/679 (il "GDPR") ha ampliato gli obblighi informativi in capo ai titolari del trattamento (e, dunque, in capo ai datori di lavoro in quanto titolari del trattamento dei dati personali dei propri dipendenti). L'art. 13 del GDPR estende il novero delle informazioni minime da fornire all'interessato[35].

Peraltro, la positivizzazione, ad opera dell'art. 5(1)(a) del GDPR, della trasparenza, quale principio fondamentale cui i titolari del trattamento devono attenersi[36], comporta che "*il titolare del trattamento dovrebbe fornire all'interessato*

32 Sul punto, il Tribunale di Roma, nell'ordinanza n. 57668 del 13 giugno 2018, ha ritenuto che, nel caso di specie, il datore non avesse dato al lavoratore adeguata informazione delle modalità di effettuazione dei controlli atteso che: "[…] *avrebbe dovuto previamente avvisare il lavoratore: a) che la sua attività avrebbe potuto essere controllata mediante tali strumenti; b) su come sarebbe stato esperito il controllo. La prodotta 'policy'* […] *non appare soddisfare tali condizioni, posto che non contiene alcun riferimento al possibile svolgimento di attività di controllo e tantomeno sulle modalità dello stesso* […] *essa si limitava a disciplinare l'uso della posta elettronica e a mettere in evidenza che la violazione di tali regole poteva dar luogo a problemi di sicurezza informativa e di indebita diffusione di dati riservati*".

33 Consultabile al seguente *link*: https://hudoc.echr.coe.int/ eng# {"language isocode":["ENG"],"appno": ["61496/08"],"document collectionid2": ["GRANDCHAMBER"],"itemid": ["001-177082"]}.

34 "*Articolo 8 – Diritto al rispetto della vita privata e familiare. 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*".

35 L'art. 13 del GDPR richiede, infatti, di informare l'interessato, fra l'altro, circa: (i) la base giuridica sottostante al trattamento dei propri dati personali (e, nel caso in cui la base giuridica consista nel legittimo interesse del titolare o di un terzo, l'indicazione di quale sia il legittimo interesse perseguito); (ii) l'intenzione, ove applicabile, di trasferire i dati personali a un paese terzo o a un'organizzazione internazionale e la base giuridica in forza della quale viene effettuato il trasferimento (*e.g.*, decisione di adeguatezza della Commissione Europea, norme vincolanti di impresa o clausole contrattuali standard); (iii) il periodo di conservazione dei dati personali oppure, se ciò non è possibile, i criteri utilizzati per determinare tale periodo; (iv) il diritto di proporre reclamo a un'autorità di controllo; (v) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

36 In realtà, la trasparenza non è una novità del GDPR. Invero, il WP29 nel citato *Parere n. 8/2001 sul trattamento dei dati nel contesto lavorativo* già ricavava tale principio dalla direttiva n. 95/46/CE ("[Transparency] [...] *should govern everything. Many processing operations in the employment context in the Member States may be in breach of data protection rules not because such processing is per se unlawful, but because workers have not been properly informed about them. As a very minimum, workers need to know which data is the employer collecting about them (directly or from other sources), which are the purposes of processing operations envisaged or carried out with these data presently or in the future*"). *Da ultimo, il WP29, nelle Guidelines on transparency under Regulation 2016/679, ha chiarito che si tratta di una caratteristica della normativa europea*

eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e [il] *contesto specifici in cui i dati personali sono trattati*"[37].

Tra l'altro, come osservato dal Gruppo di Lavoro Articolo (il "WP29") nel *Parere 2/2017*[38], la trasparenza richiede che "*si dovrebbero informare efficacemente i dipendenti su qualsiasi monitoraggio che venga attuato, sulle sue finalità e sulle circostanze nelle quali viene svolte, nonché sulle possibilità di cui dispongono i dipendenti per impedire che i propri dati vengano acquisiti mediante tecnologie di monitoraggio. Le politiche e le norme riguardanti il monitoraggio legittimo devono essere chiare e facilmente accessibili*".

Altra questione rilevante in tema di protezione dei dati personali riguarda la corretta individuazione della base giuridica del trattamento, atteso che raramente, nel contesto lavorativo, potrà essere invocato, allo scopo, il consenso dei dipendenti. Ciò in ragione dell'intrinseco squilibrio contrattuale che caratterizza la relazione dipendente-datore di lavoro, che rischia di rendere il consenso prestato dal dipendente invalido perché non libero[39]. In proposito, a seconda del caso, si potrà valutare di basare l'attività di trattamento sul legittimo interesse del titolare del trattamento o di un terzo, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali (art. 6(1)(f) del GDPR). In questo caso, come precisato dal WP29 nelle *Guidelines on transparency under Regulation 2016/679*[40], l'informativa dovrà indicare specificamente l'interesse legittimo perseguito e, quale buona prassi, il titolare del trattamento potrà anche fornire indicazioni all'interessato relativamente al bilanciamento operato tra il perseguimento del legittimo interesse (proprio o di terzi) perseguito e gli interessi o i diritti e le libertà fondamentali dell'interessato. In ogni caso, il WP29 ritiene che il titolare del trattamento debba informare chiaramente l'interessato della possibilità di ottenere informazioni circa tale bilanciamento, atteso che tali informazioni sono essenziali, nell'ottica di un'effettiva trasparenza, per il caso in cui gli interessati nutrano dubbi circa la corretta effettuazione, da parte del titolare, del bilanciamento di interessi, oppure intendano presentare un reclamo all'autorità garante competente.

Relativamente al rispetto di altre disposizioni del Codice Privacy[41], meritano particolare attenzione quelle di cui agli artt. 3 e 11, dalle quali si desume il principio di minimizzazione (in virtù del quale il trattamento dei dati personali non deve essere eccedente rispetto alle finalità perseguite). Tale principio,

consolidata da tempo ("Transparency is a long established feature of the law of the EU").

37 Cfr. il considerando n. 60 del GDPR.

38 *Parere 2/2017 sul trattamento dei dati sul posto di lavoro* (adottato l'8 giugno 2017 e consultabile al seguente *link* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169).

39 Cfr., da ultimo, il citato *Parere 2/2017 sul trattamento dei dati sul posto di lavoro* del WP29 che richiama, altresì, il precedente *Parere n. 8/2001 sul trattamento dei dati nel contesto lavorativo* (adottato il 13 settembre 2001 e consultabile al seguente *link* http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf).

40 Tali *guidelines* sono state adottate l'11 aprile 2018 e sono consultabili al seguente *link*: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

41 Da intendersi nella sua interezza, stante l'ampiezza del rinvio al Codice Privacy effettuata dal comma 3 dell'art. 4 dello Statuto dei Lavoratori.

attualmente codificato dall'art. 5(1)(c) del GDPR[42], viene ulteriormente rafforzato nel GDPR poiché la minimizzazione costituisce il presupposto logico dei principi di *data protection by design* e *by default* di cui all'art. 25 del GDPR[43]. In forza di tali principi, il titolare deve predisporre misure tecniche (come ad esempio la pseudonimizzazione) e organizzative adeguate che: (i) consentano di attuare efficacemente i principi generali in materia di trattamento di dati personali "*sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento*"; e (ii) garantiscano che siano trattati, sulla base di impostazioni predefinite, soltanto i dati necessari per le specifiche finalità di volta in volta rilevanti.

Ne discendono, come è evidente, una serie di vincoli concernenti, fra l'altro, la quantità e tipologia di dati personali raccolti e successivamente trattati, i tempi di conservazione, la possibilità di trasferire tali dati personali a soggetti terzi e anche la limitazione dell'accesso ai dati personali nell'ambito del contesto aziendale nonché le finalità per le quali tali dati personali, una volta raccolti, vengono trattati.

5. La verifica della condotta di dipendenti sospettati di comportamenti contrari ai propri doveri: la sorte dei c.d. "controlli difensivi"

All'indomani dell'entrata in vigore del Jobs Act, si discuteva, in dottrina e in giurisprudenza, circa la sorte della categoria dei c.d. controlli difensivi (ossia i controlli volti non a verificare l'attività lavorativa ma a reagire alla commissione di illeciti da parte dei dipendenti) elaborata, non senza oscillazioni, dalla copiosa giurisprudenza formatasi nella vigenza del vecchio art. 4 dello Statuto dei Lavoratori.

Tale categoria di controlli esulava dall'applicazione dell'art. 4 dello Statuto dei Lavoratori, con particolare riguardo al requisito della previa autorizzazione sindacale o amministrativa. In proposito, la giurisprudenza tendeva a valorizzare la necessità che si trattasse di verifica *ex post* del comportamento del dipendente, ossia svolta in ragione dell'esistenza di sospetti. In questa prospettiva, meccanismi di controllo "a distanza", installati per contrastare *ex ante* la commissione di illeciti, avrebbero richiesto il rispetto delle procedure di cui all'art. 4 dello Statuto dei Lavoratori ove permettessero anche la mera possibilità di controllo dell'attività lavorativa.

Con l'introduzione della finalità di tutela del patrimonio aziendale fra quelle per le quali il novellato comma 1, art. 4 dello Statuto dei Lavoratori consente l'impiego di strumenti che consentono il controllo a distanza dell'attività dei lavoratori, si è posto il dubbio se i controlli difensivi siano ormai ricompresi nella previsione normativa (e dunque sempre e comunque assoggettati alla relativa disciplina) oppure se si possa ancora distinguere tra controlli difensivi in senso ampio (ossia, quei controlli volti genericamente a tutelare il patrimonio

42 Tale articolo prevede che "*i dati personali sono* […] *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ('minimizzazione dei dati')*".

43 Cfr. L. Bolognini, E. Pelino, C. Bistolfi, *Il regolamento privacy europeo – commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 108.

aziendale, soggetti ai vincoli di cui all'art. 4 in commento), da un lato, e controlli difensivi in senso stretto (ossia, quei controlli volti ad accertare la commissione di illeciti da parte dei dipendenti, possibili mediante strumenti installati anche in assenza di accordo sindacale o autorizzazione, atteso che "*non è detto che la condotta illecita colpisca solo il patrimonio aziendale*"[44]), dall'altro lato.

In una recente pronuncia sull'attuale formulazione dell'art. 4 dello Statuto dei Lavoratori (e nel contesto di controlli che rientrano nella categoria dei controlli difensivi), il Tribunale di Roma[45] ha ritenuto che "*sul 'come si fa il controllo', la novella ha posto limiti chiari e rigorosi", per cui l' "installazione dell'impianto, anche se finalizzata a ragioni di tutela del patrimonio aziendale, per il mero fatto di consentire il controllo sull' 'attività dei lavoratori' (e non dell' 'attività lavorativa') va previamente autorizzata* […] [e] *dell'installazione dell'impianto e delle sue modalità d'uso il lavoratore va reso previamente edotto*".

Tale prospettiva appare criticabile ad avviso di chi scrive perché ne discende che, quando il datore di lavoro non abbia preventivamente ottenuto l'autorizzazione all'installazione degli strumenti di controllo (e salvo che essi rientrino fra quelli utilizzati dal lavoratore per rendere la prestazione lavorativa) potrebbe essere per questi impossibile accertare e sanzionare illeciti, anche gravi.

Condivisibile appare, invece, la posizione interpretativa di chi ha osservato che le due fattispecie (quella dei controlli predisposti ex ante per monitorare l'attività dei lavoratori e quella delle indagini effettuate ex post per reprimere specifici illeciti già verificatisi o per prevenire ulteriori illeciti) sono diverse sia per natura sia per funzione e che "[l]'*indagine, resa necessaria da seri sospetti o da violazioni già verificatesi, appare, anche logicamente, incompatibile con la procedura richiesta dall'art. 4 per l'installazione dell'impianto di controllo, e ciò sia ove si tenga conto dei tempi necessari per il normale svolgimento di tale procedura, sia ove si consideri che l'avvio del confronto sindacale priverebbe l'indagine della segretezza che è normalmente necessaria perché essa possa dare risultati*"[46].

44 Cfr. A. Maresca, *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore*, in *Ipsoa Quotidiano*, 22 febbraio 2016.

45 Cfr. Tribunale di Roma, ordinanza n. 57668 del 13 giugno 2018.

46 Cfr. G. Proia, op. loc. cit., il quale osserva anche che, se si opinasse diversamente, il datore di lavoro sarebbe posto di fronte ad un'alternativa poco ragionevole: "*o richiedere preventivamente l'autorizzazione alla installazione di impianti che abbiano una maggiore capacità e un maggior raggio di controllo, al fine di precostituire lo strumento necessario per prevenire e reprimere il maggior numero possibile di ipotesi di illeciti da parte dei propri dipendenti, ovvero trovarsi nella impossibilità di accertare e sanzionare quei gravi illeciti che non possono essere scoperti se non con l'ausilio di strumenti tecnologici. La prima alternativa, ammesso e non concesso che ottenga l'autorizzazione sindacale o amministrativa, avrebbe l'effetto paradossale di estendere, anziché contenere, l'uso di strumenti per finalità di controlli a distanza; la seconda sarebbe semplicemente ingiusta*".

CAPITOLO 2 di Deborah Bolco, Mariangela Papadia e Stefano Cancarini

Attività di verifica delle Autorità e sanzioni

SOMMARIO: 1. L'attività di (auto)verifica svolta dal Titolare e dal Responsabile del trattamento ai fini dell'attuazione del processo di accountability previsto dal nuovo Regolamento europeo – 2. Cenni sulle attività di (auto)verifica da svolgere *ante*, durante e *post* trattamento – 3 L'attività di verifica e ispettiva svolta dall'Autorità di controllo nazionale: intervento principalmente *ex post*, ovvero successivamente le valutazioni e le verifiche interne poste in essere dal Titolare del trattamento – 4 Il nuovo sistema sanzionatorio – 5 I.Le sanzioni amministrative pecuniarie – 6 II.Le altre misure sanzionatorie

1. L'attività di (auto)verifica svolta dal Titolare e dal Responsabile del trattamento ai fini dell'attuazione del processo di accountability previsto dal nuovo Regolamento europeo

L'espressione '*attività di verifica*' fa inevitabilmente pensare a quella attività svolta da soggetti terzi (ovvero, nel caso del regolamento, Autorità di controllo nazionali o capofila) nei confronti del soggetto interessato. In realtà, ciò che con il nuovo contesto dettato dal Regolamento privacy (GDPR) rileva è l'attività di (auto)verifica e (auto)controllo cui il Titolare e il Responsabile sono tenuti ai fini dell'attuazione del c.d. processo di *accountability*: come ormai noto, il cambio di prospettiva del GDPR rispetto al Codice privacy è distillato proprio in tale principio che porta in nuce tutta la pregnanza della nuova disciplina e che non a caso è stato definito 'il principio dei principi'. Si tratta dell'*accountability* del titolare rispetto all'effettività della protezione dei dati, un principio a doppio binario, di responsabilizzazione e rendicontazione così come si evince all'art. 5 del Regolamento: il titolare del trattamento è competente per il rispetto dei principi in materia di protezione dei dati (liceità correttezza, trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza) e deve essere in grado di comprovarlo.

Il Codice della privacy non prevedeva in modo diretto il principio di *accountability*, ma fissava una serie di adempimenti formali (rispetto ai quali vi era un controllo dell'autorità garante: informativa, consenso, notificazione al Garante, misure minime e idonee) e un sistema di responsabilità civili, penali e amministrative.

Quello contenuto nel Regolamento rappresenta, pertanto, un forte riconoscimento a livello normativo di un principio riconosciuto già nel 2010 (parere 3/2010, emesso in vista di una revisione della direttiva privacy) dal Gruppo

Art.29, il Gruppo istituito dall'art. 29 della direttiva 95/46 ('WP29'), oggi sostituito dal Comitato Europeo per la protezione dei dati.

Il WP 29 sottolineava che "*La protezione dei dati deve passare 'dalla teoria alla pratica*'", ovvero sanciva la necessità del passaggio da una *protezione reale* a una *protezione formale* dei dati. E l'architettura 'giuridica' per realizzare un sistema basato sulla responsabilità è imperniata **non** sulla declinazione di principi sostanziali di protezione dei dati – questi rimangono pressoché inalterati – bensì sulla definizione di misure e procedure interne, sul modello di quelli utilizzati nell'applicazione del D.lgs 231/01 in materia di responsabilità amministrative delle società: il titolare del trattamento dei dati deve essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi. In altri termini, il titolare deve dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati sono adeguati e conformi al Regolamento europeo in materia di privacy.

2. Cenni sulle attività di (auto)verifica da svolgere *ante*, durante e *post* trattamento

È proprio il richiamato principio di accountability che impone al Titolare o al Responsabile del trattamento di svolgere una pregnante attività di autoverifica costante nel tempo e, di conseguenza, non solo ante trattamento, ma anche durante e post trattamento. Infatti, solo una attenta auto-verifica e valutazione consente al Titolare o Responsabile del trattamento:

- di adottare le soluzioni e gli strumenti pensati in ottica **privacy by design** e **by default**[47] e cioè mettere in atto misure tecniche e organizzative adeguate (quali ad esempio la pseudonimizzazione), volte ad attuare in modo efficace i principi posti a tutela della protezione dei dati (quali ad esempio la minimizzazione all'uso dei dati e le informazioni di carattere personale), e a integrare nel trattamento le necessarie garanzie al fine di tutelare i diritti degli interessati (cfr. Articolo 25 del Regolamento privacy - *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*).
- di definire e procedere con la gestione del **Data breach**[48] e quindi l'adozione di tutti gli strumenti e delle procedure atte a rilevare e affron-

47 Per '*Data protection by default*' si intende l'adozione di quelle misure tecniche e organizzative funzionali a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari alle finalità perseguite; per '*Data protection by design*' si intende la creazione di prodotti e servizi che devono tenere conto, sin dalla loro progettazione, delle regole e dei principi della protezione dei dati in modo da minimizzare a priori non solo la raccolta dei dati ma anche i trattamenti successivi effettuati.

48 Il WP29, con le sue Linee Guida del 3 ottobre 2017, fornisce una definizione di 'data breach' identificandola come una violazione dei dati personali trattati, la quale potrebbe tradursi in una perdita di:
- confidenzialità, ad esempio nel caso di accesso o diffusione non autorizzati dei dati personali;
- disponibilità, come nel caso di perdita o distruzione dei dati personali;
- integrità, nel caso di alterazione dei dati personali, avvenuta in modo accidentale o senza autorizzazione.

tare tempestivamente le violazioni nel trattamento dei dati personali notificando entro 72 ore l'accaduto al Garante e in taluni casi anche agli interessati. Con riguardo alla notifica nei confronti dell'Autorità competente, il GDPR (art. 33) dispone che il Titolare non è obbligato a notificare la violazione se dimostra che tale violazione non comporta alcun rischio per i diritti e le libertà dell'interessato. In altri termini, qualora la confidenzialità, l'integrità e la disponibilità dei dati non siano intaccate in nessun modo dal breach e ciò è dimostrato, la notifica all'Autorità competente non è necessaria: tale passaggio, quindi, risulta ancora una volta subordinato ad una (auto)valutazione da parte del Titolare del rischio per gli interessati.

- quando richiesto (a seconda della tipologia dei dati e dei relativi trattamenti: trattamenti su larga scala di dati sensibili, attività di profilazione, sistematica sorveglianza su larga scala di zona accessibile al pubblico, altri trattamenti previsti dalle autorità di controllo), di procedere con la **PIA**, ovvero l'autonoma valutazione dei rischi per comprendere gli impatti privacy e chiedere, nel caso di impatti elevati, la Prior Consultation del Garante. Per ogni fenomeno il Titolare sarà tenuto a verificare rischiosità complessiva, azioni intraprese e rischiosità residua in modo da realizzare il primo documento che fotografa la situazione corrente. La DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*) in quanto aiuta il Titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni. Come esposto nelle linee guida del WP29, i Titolari devono (auto)valutare in modo continuativo i rischi creati dai propri trattamenti così da individuare quelle situazioni in cui una determinata tipologia di trattamenti "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

La figura che dovrà assistere il Titolare in questa auto-valutazione è il Responsabile della Protezione dei Dati, o Data Protection Officer ('DPO' – art. 39 del Regolamento). Si tratta quindi di un supervisore che, dotato spiccate conoscenze della normativa e della prassi in materia di privacy e di ampia autonomia, avrà il compito di monitorare e assistere il Responsabile e il Titolare nel trattamento e nella gestione dei dati.

In conclusione, il delicato compito di verifica sul rispetto del nuovo assetto normativo non spetterà più unicamente al Garante, ma direttamente al Titolare che dovrà svolgere questa attività ispirandosi al principio di *accountability* e quindi, in modo "responsabilizzante".

3. L'attività di verifica e ispettiva svolta dall'Autorità di controllo nazionale: intervento principalmente ex post, ovvero successivamente le valutazioni e le verifiche interne poste in essere dal Titolare del trattamento

Da quanto sopra si evince come, con il nuovo Regolamento europeo, l'Autorità di controllo svolga principalmente il suo intervento *ex post*, cioè la sua valutazione si colloca successivamente alle valutazioni e alle verifiche interne svolte dal Titolare del trattamento. Per tale ragione non hanno più ragion d'essere i vecchi istituti quali la notifica preventiva dei trattamenti e il *prior checking* (salvo eccezioni), che sono sostituiti da obblighi di tenuta di un registro dei trattamenti e da valutazioni di impatto autonome.

Le attività di indagine e verifica svolte dalle Autorità nazionali sono finalizzate, da un lato, alla tutela dell'interessato (esame dei reclami e relative indagini, attività informativa su richiesta); dall'altro, a verificare la corretta applicazione del Regolamento, investigando sulle possibili violazioni (è il caso, ad esempio, delle richieste di informazioni al titolare o al responsabile, del riesame della validità delle certificazioni). Quindi eventuali indagini non si attivano solo sulla base di un ricorso da parte dell'interessato, ma possono avere origine anche dall'autonoma iniziativa del Garante nonché delle altre autorità nazionali e, con il nuovo Regolamento, dell'autorità capofila nel caso di trattamenti transfrontalieri. Infatti, nell'ipotesi in cui un Titolare o un Responsabile abbia stabilimenti in vari Stati membri o qualora esista la probabilità che l'attività di trattamento abbia un impatto negativo su un numero significativo di interessati collocati in più di uno Stato membro, al fine di assicurare la più ampia coerenza nell'applicazione della disciplina a tutela dei dati personali e certezza del diritto, il legislatore europeo ha introdotto un principio di collaborazione ad ampio raggio sia tra le varie Autorità nazionali coinvolte ('DPA') sia tra Autorità nazionali e Autorità capofila. Tale collaborazione si estende su tutto il territorio europeo e si manifesta per il tramite di due meccanismi: **a**) quello del c.d. sportello unico; **b**) quello dell'assistenza reciproca e delle operazioni congiunte (mutua assistenza e azioni comuni), che possono venire in considerazione sia nell'ambito della procedura dello sportello unico, quanto nell'ipotesi in cui la competenza a decidere la questione venga rimessa alle singole Autorità di controllo interessate.

Tali meccanismi assicurano la coerenza nell'applicazione del Regolamento, la certezza del diritto e l'omogeneità nella sua attuazione anche laddove siano coinvolti più Stati membri.

Alla luce di quanto detto, il quesito che inevitabilmente ci si pone in questo contesto è: in assenza di qualsivoglia indicazione da parte del Regolamento UE su quali siano le "specifiche misure tecnologiche" adeguate per la tutela dei dati personali che Titolare e Responsabile del trattamento sono tenuti ad adottare, cosa occorre fare per evitare l'applicazione di pesanti sanzioni? I soggetti interessati dovranno dimostrare:

- il rispetto degli obblighi di informativa e consenso informato;

- la liceità e correttezza del trattamento dei dati personali con riferimento alla pertinenza e non eccedenza del trattamento e al rispetto del principio di necessità del trattamento (il quale impone di stabilire la durata del trattamento in funzione della sua finalità);
- l'adozione di processi, procedure e relative applicazioni informatiche che garantiscano la protezione dei dati sensibili e giudiziari: ad esempio la gestione degli accessi logici (autenticazione) e fisici; l'adozione di sistemi di controllo interni quali la *segregation of duties*; il rispetto dei principi del *Need to know*, del *Least privilege*.

4. Il nuovo sistema sanzionatorio

I. Le sanzioni amministrative pecuniarie

Le sanzioni di cui all'articolo 83 del Regolamento riguardano violazioni della quasi totalità degli articoli del regolamento stesso; in altri termini, la quasi totalità delle disposizioni del Regolamento è assistita da sanzioni pecuniarie:

- sanzioni pecuniarie fino a € 10 milioni o al 2% del fatturato mondiale (se superiore) nel caso ad esempio di violazione obblighi in materia di consenso dei minori, misure di sicurezza; violazione obblighi impartiti dal titolare; violazione obblighi di comunicazione per *data breach*;
- sanzioni pecuniarie fino a € 20 milioni o al 4% del fatturato mondiale (se superiore) nel caso ad esempio di violazioni concernenti i diritti degli interessati, i principi cardine del trattamento (consenso) i trasferimenti ecc...; violazioni di ordini o misure imposte dall'autorità.

Uno dei punti più spinosi del GDPR è la questione delle sanzioni sotto il profilo della discrezionalità della loro applicazione da parte degli organi competenti. Il Regolamento UE, infatti, prevede, da un lato, sanzioni pecuniarie '*armonizzate*' in termini di criteri per l'imposizione (si veda l'articolo 83, paragrafo 2, del Regolamento) e l'ammontare massimo imponibile; dall'altro, una discrezionalità in capo all'autorità nazione nello stabilire se e quanto sanzionare 'in aggiunta o in sostituzione' alle altre misure correttive di cui dispongono in base al GDPR (che comprendono, ai sensi dell'articolo 58, provvedimenti come l'ammonimento o misure più consistenti che giungono al divieto di trattare dati personali o all'ingiunzione di dare corso a specifiche prescrizioni).

Tuttavia, il superamento di tale impasse potrebbe stare in un'ulteriore previsione del Regolamento che contempla quale compito specifico del Comitato europeo per la protezione dei dati (WP29) una definizione di **criteri europei più precisi** per l'imposizione della sanzione pecuniaria e il calcolo dell'ammontare di questa sanzione.

In questo contesto si inseriscono le linee guida emesse dal WP29 nell'ottobre 2017 con le quali si è proposto di fornire alle Autorità competenti una Guida pratica, anche se non esaustiva, circa gli step da seguire per l'applicazione

di sanzioni che siano "*equivalenti, in tutti gli Stati Membri, al fine di assicurare all'interno dell'Unione Europea un livello equivalente di protezione dei dati personali*".

Si parte dal concetto, appunto, di "*equivalenza*": nonostante, infatti, le Autorità competenti svolgano le relative funzioni in modo assolutamente indipendente, nel rispetto delle leggi nazionali, è richiesto loro di cooperare per assicurare la compattezza nell'applicazione ed effettività del Regolamento europeo, evitando, quindi, di scegliere ad esempio differenti misure correttive, ma anche sanzionatorie, in casi similari. siano essi nazionali o transfrontalieri.

Su tali premesse, le Linee Guida aprono un'analisi circa la valutazione della violazione "caso per caso" che l'Autorità Competente deve realizzare, alla luce dei criteri forniti dal GDPR all'art. 83.

Alcuni di questi riguardano:

A. "*Natura, gravità e durata della violazione*": anche se il GDPR prevede un ammontare massimo delle sanzioni (10-20 milioni di euro) in relazione a specifiche violazioni, che già sono considerate più serie di altre, le Autorità competenti potrebbero rilevare nel caso di specie un bisogno maggiore o minore di reagire attraverso l'adozione di misure nella forma della sanzione amministrativa. In particolare le Linee Guida fanno riferimento alla nozione di "violazioni meno rilevanti", per le quali le Autorità competenti potrebbero predisporre un'ammonizione al posto della sanzione, quando queste non espongono i soggetti interessati a un rischio per i loro diritti.

Quanto alla gravità, alcuni degli elementi che l'Autorità dovrà considerare per la sua valutazione riguardano, ad esempio, il numero di soggetti interessati dalla violazione (al fine di comprendere se si tratta di un evento isolato o, al contrario, di più violazioni sistematiche); il danno sofferto, ovvero se sussistono rischi per i diritti e le libertà dell'individuo.

Anche la durata della violazione può offrire elementi circa la portata della violazione perché può essere rappresentativa di un comportamento doloso del titolare del trattamento nonchè dell'inadeguatezza delle misure preventive adottate.

B. "*Il carattere intenzionale o negligente della violazione*": è generalmente ammesso che le violazioni intenzionali siano trattate con maggiore severità rispetto a quelle non intenzionali.

C. "*Le azioni intraprese da Titolare e Responsabile, per mitigare il danno sofferto dagli interessati*": l'avere un comportamento reattivo di Titolare e Responsabile al verificarsi di una violazione può comportare una mitigazione della sanzione. Tale comportamento responsabile (ad esempio, contattare gli altri titolari/responsabili che potrebbero essere coinvolti nel trattamento), o la sua mancanza, potrebbero essere presi in considerazione dall'Autorità competente nello scegliere la misura correttiva da applicare, ma anche per calcolare la sanzione da imporre nel caso di specie.

D. "*Il grado di responsabilità in capo al Titolare o al Responsabile, tenendo in considerazione le misure tecniche e organizzative da essi implementate*": l'Autorità, nel fare le proprie valutazioni, deve tenere in considerazione anche se siano state intraprese procedure di "*best practice*", normative di settore o codici di condotta nell'ambito del corrispondente settore di business.

E. "*L'esistenza di precedenti violazioni in capo al Titolare o Responsabile*", tale criterio ha lo scopo di valutare il "*track-record*" dell'entità che ha commesso la violazione, per scoprire se ha già commesso in passato la stessa violazione e se ciò è avvenuto nella stessa maniera.

F. "*Il grado di cooperazione con l'Autorità competente, in modo da porre rimedio e mitigare gli effetti sorti a causa della violazione*": tale criterio avvantaggia il Titolare/Responsabile che ha commesso la violazione, quando è indicativo della buona volontà e dell'impegno ad affrontare correttamente gli effetti o i danni da questa provocati.

G. "*Le categorie di dati personali coinvolti nella violazione*", qualora questa riguardi, ad esempio, categorie particolari di dati personali (stato di salute, condanne penali), l'entità della sanzione da applicare sarà inevitabilmente più severa.

H. "*Il modo in cui l'Autorità viene a conoscenza della violazione, in particolare se il Titolare ha notificato il data breach*": non è sufficiente adempiere all'obbligo di notifica per ottenere una mitigazione della pena: come rilevato dal WP29, il titolare che non notifica tutti i dettagli della violazione o che non valuta adeguatamente la portata del *data breach* potrebbe essere valutato dall'Autorità come meritevole di una sanzione più severa.

I. "*Se l'Autorità ha già imposto in capo al Titolare/Responsabile delle misure correttive (previste dal GDPR) in merito allo stesso tipo di violazione, e se esse sono state osservate*": il non aver rispettato le misure correttive precedentemente imposte potrebbe essere valutato negativamente dall'Autorità.

J. "*L'adesione ad approvati Codici di Condotta*": nel caso di una violazione delle previsioni del Regolamento, l'adesione a un codice di condotta approvato, potrebbe aiutare l'Autorità a intervenire in modo *efficace, proporzionato e deterrente*, eventualmente imponendo delle sanzioni amministrative oppure ritenendosi soddisfatta delle azioni poste in essere da parte dell'organo a presidio del rispetto del codice di condotta.

K. "*Ogni altro fattore aggravante o di favore, applicabile in base alle circostanze del caso, come benefici finanziari ottenuti, o perdite evitate direttamente o indirettamente derivanti dalla violazione*": possiamo supporre che ulteriori fattori di mitigazione dell'entità della sanzione da applicare possano riguardare l'eventuale pregiudizio, subito dallo stesso Titolare o Responsabile che ha commesso la violazione, a causa della stessa (ad es. l'aver subito discredito nel mercato, o perdite economiche).

II. Le altre misure sanzionatorie

Il Regolamento prevede che saranno gli Stati membri a stabilire le norme relative alle altre sanzioni assicurandone la proporzionalità e l'efficacia dissuasiva.

Con riferimento all'Italia, nell'ambito della attuazione della Legge 25 ottobre 2017, n. 163 (Legge di delegazione europea 2016-2017) – che richiedeva di "*adeguare … il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse*" – il D.lgs. 101/2018, recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679, ha modificato la disciplina penale prevista dal D.lgs. 196/2003 (Codice Privacy).

I reati oggi previsti dal Codice Privacy, come novellato dal D.lgs. 101/2018 – in numero maggiore rispetto al passato – sono i seguenti:

- trattamento illecito di dati – art. 167 del Codice Privacy;
- comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala – art. 167-bis Codice Privacy;
- acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala – art. 167-ter Codice Privacy;
- falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante – art. 168 Codice Privacy;
- inosservanza di provvedimenti del Garante – art. 170 Codice Privacy;
- violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori – art. 171 Codice Privacy.

Rileva notare, inoltre, che per i reati previsti dagli articoli 167, 167-bis e 167-ter, in caso di precedente applicazione (e riscossione) di una sanzione amministrativa, "*la pena è diminuita*" (art. 167, comma 6, Codice Privacy).

Infine, occorre ricordare che, in generale, la mancata protezione adeguata dei dati personali dei propri clienti o dipendenti può comportare non solo sanzioni civili (e in alcuni casi anche penali) in caso di ispezione da parte del nucleo Privacy della Guardia di Finanza, ma anche, in caso di richiesta di risarcimento danni, ingenti perdite economiche. E non solo, esistono svariati rischi per una organizzazione che gestisce in modo inconsapevole la sicurezza dei dati: si pensi, ad esempio, ai danni reputazionali o ancora, nell'ipotesi di perdita di dati, l'indisponibilità di risorse per garantire la continuità del servizio al cliente e le conseguenti perdite economiche più o meno rilevanti in funzione della gravità dell'evento.

CAPITOLO 3 di Irene Picciano, Eva Cruellas Sada, Eugenia Gambarara

La compliance antitrust: l'agenda delle priorità

La compliance antitrust: l'agenda delle priorità e l'aggiornamento dei programmi alle nuove sfide del mercato

SOMMARIO: 1. Programma di compliance e sanzioni antitrust – a. Le linee guida sanzionatorie dell'AGCM – b. Casistica dell'AGCM – c. Programma di compliance e sanzioni antitrust: prospettiva comparatistica nell'UE – 2. Anonymous Whistleblowing Tool della Commissione europea – 3. Accordi Verticali e vendite online – 4. Rilevanza della scontistica come pratica abusiva – 5. Big Data – a. Introduzione – b. Necessità di riadattare i modelli di compliance al fine di salvaguardare le istanze di privacy – c. Big Data come fonte di potere di mercato e come oggetto della tutela antitrust – d. I Big Data assumono oggi una rilevanza autonoma sotto il profilo economico: impatto nelle operazioni di concentrazione (posizione di mercato delle imprese coinvolte) – e. I Big Data assumono un peso anche nell'attività di audit

1. Programma di compliance e sanzioni antitrust

a. Le Linee Guida Sanzionatorie dell'AGCM

Nel campo della compliance antitrust ricoprono un ruolo centrale le indicazioni fornite dall'Autorità Garante della Concorrenza e del Mercato ("Autorità") attraverso le *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* (le "Linee Guida")[49] pubblicate nel 2014. Tra le attenuanti che permettono di diminuire (fino al 15%) l'importo base di una sanzione decisa dall'AGCM, compare infatti la circostanza di aver adottato, implementato e rispettato uno specifico programma di *compliance*, adeguato e in linea con le *best practice* europee e nazionali[50].

49 Adottate dall'Autorità con delibera n. 25152 del 22 ottobre 2014 (in Boll. n. 42/2014) e disponibili al seguente link: http://www.agcm.it/component/joomdoc/normativa/concorrenza/Linee_guida_criteri_quantificazione_sanzioni.pdf/download.html.

50 Cfr. punto 23 delle Linee Guida: "*Le circostanze attenuanti includono, a titolo esemplificativo: […] l'adozione e il rispetto di uno specifico programma di compliance, adeguato e in linea con le best practice europee e nazionali. La mera esistenza di un programma di compliance non sarà considerata di per sé una circostanza attenuante, in assenza della dimostrazione di un effettivo e concreto impegno al rispetto di quanto previsto nello stesso programma (attraverso, ad esempio, un pieno coinvolgimento del management, l'identificazione del personale responsabile del programma, l'identificazione e valutazione dei rischi sulla base del settore di attività e del contesto operativo,*

b. Casistica dell'AGCM

La recente casistica delle fattispecie esaminate dall'Autorità costituisce un importante punto di rife-rimento per l'individuazione delle componenti che un valido ed efficace programma di compliance deve avere per poter beneficiare dell'attenuante prevista dalle Linee Guida.

Nell'anno 2017 [51], l'Autorità ha adottato sei decisioni nelle quali ha valutato programmi di compliance antitrust al fine di concedere o meno l'attenuante prevista dalle Linee Guida.

Nel caso I742 - *Tondini per cemento armato* [52], l'Autorità aveva inflitto alle imprese coinvolte sanzioni per un totale di circa 143 milioni di euro. Nella quantificazione delle sanzioni alcune parti del procedimento hanno chiesto di tener conto dei propri programmi di compliance. Tuttavia, l'Autorità ha ritenuto che non vi erano i presupposti per accordare l'attenuante nei confronti di nessuna delle parti richiedenti. L'Autorità ha ritenuto che tutti i programmi di compliance erano stati adottati **tardivamente** rispetto all'avvio del procedimento e successivamente o a ridosso della trasmissione della Comunicazione delle Risultanze Istruttorie ("CRI") e, quindi, la documentazione depositata non consentiva un'adeguata valutazione da parte dell'Autorità, in particolare, 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. Inoltre, l'Autorità ha rilevato che alcune imprese erano già state sanzionate dalla Commissione europea e avrebbero, quindi, 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 a livello comunitario.

Nel caso I793 - *Aumento prezzi del cemento* [53], in cui sono state inflitte alle imprese coinvolte sanzioni per un totale di circa 184 milioni di euro, l'Autorità ha accertato l'efficacia del programma di compliance antitrust adottato da alcune imprese e ha riconosciuto a tali imprese una circostanza attenuante riducendo la sanzione nella misura del 10%. In particolare, l'Autorità ha rilevato che (i) i programma di compliance erano stati adottati (in alcuni casi anche implementati) e comunicati prima dell'invio della CRI; e (ii) i programma di compliance prevedevano il coinvolgimento del management, l'identificazione di responsabili del programma, l'organizzazione di attività di training, nonché la previsione di incentivi/disincentivi, sistemi di monitoraggio e di audit. Nella medesima decisione, l'Autorità non ha invece riconosciuto l'attenuante a un'al-

l'organizzazione di attività di training adeguate alle dimensioni economiche dell'impresa, la previsione di incentivi per il rispetto del programma nonché di disincentivi per il mancato rispetto dello stesso, l'implementazione di sistemi di monitoraggio e auditing)."

51 Per la casistica precedente si veda la pubblicazione relativa alle Corporate Compliance Round Tables del 10 Maggio 2016 (http://www.aslaitalia.it/files/pubblicazioni/ASLA_CC2016_Final.pdf).

52 AGCM, provvedimento n. 26686 del 19 luglio 2017, caso I742 – *Tondini per cemento armato*, in Boll. n. 30/2017. Si segnala che il Provvedimento è stato recentemente annullato del Tar Lazio con Sentenza pubblicata il 12 giugno 2018.

53 AGCM, provvedimento n. 26705 del 25 luglio 2017, caso I793 - *Aumento prezzi cemento*, in Boll. n. 31/2017.

tra impresa, in quanto il suo programma di compliance antitrust si sostanziava nella mera adozione di un codice di condotta che ripercorreva genericamente i princìpi a tutela della concorrenza e i comportamenti da assumere in casi di ispezioni, non prevedendo invece tutti gli elementi elencati al punto (ii) supra e, in ogni caso, l'adozione di tale codice di condotta era stata documentata tardivamente, solo in sede di presentazione della memoria finale di riposta alla CRI.

Nel caso I796 - *Servizi di supporto e assistenza tecnica alla PA nei programmi cofinanziati dalla UE* [54], in cui sono state inflitte alle imprese coinvolte sanzioni per un totale di circa 23 milioni di euro, l'Autorità ha valutato in maniera differente programmi di *compliance* antitrust che, pur essendo nella sostanza molto simili (pieno coinvolgimento del *management*, nomina di un responsabile *antitrust*, adozione di codici di condotta etc.), erano stati adottati e comunicati all'Autorità in momenti differenti e per alcuni di loro non era quindi stato possibile valutarne appieno l'attuazione. Da un lato, l'Autorità ha riconosciuto un'attenuante del 5% alle imprese che ben prima dell'invio della CRI (i) avevano adottato un programma di *compliance* antitrust ovvero aggiornato un programma di *compliance* antitrust già esistente e (ii) avevano fornito all'Autorità tutti gli elementi necessari per la valutazione del programma di *compliance*. Diversamente, l'Autorità non ha concesso alcun attenuante ad un'impresa che aveva adottato il programma di *compliance* antitrust **dopo** l'invio della CRI, comunicandolo all'Autorità solo in sede di memoria finale di risposta alla CRI. L'Autorità ha ritenuto che tale circostanza non consentiva all'Autorità un'adeguata valutazione dell'efficacia dell'attuazione del programma di *compliance* antitrust.

Nel caso A484 - *Unilever/Distribuzione Gelati* [55], in cui è stata imposta una sanzione di circa 60 milioni di euro, l'Autorità ha riconosciuto, a titolo di circostanza attenuante, una riduzione dell'importo base della sanzione pari al 10-15%, pari a 5-10 milioni di euro, in ragione del fatto che la Società aveva rafforzato un programma di *compliance* antitrust prima dell'avvio del procedimento e successivamente, nel corso del 2016, ossia prima della notifica della CRI, lo aveva integrato al fine di adeguarlo alle *best practice* nazionali ed europee. Infatti, l'Autorità ha rilevato che tale programma prevedeva: il coinvolgimento del *management*; l'identificazione del personale responsabile del programma; l'organizzazione di attività di *training*; la predisposizione di un manuale e di un vademecum volti ad illustrare al personale i principi e le procedure nonché ad impartire istruzioni operative relative alle specifiche condotte oggetto del presente procedimento; la previsione di disincentivi (sanzioni disci-plinari) per il mancato rispetto del programma; sistemi di monitoraggio e di *audit*; e un meccanismo di periodica revisione del programma stesso.

Più recentemente, nel caso A500A - *Vodafone-SMS informativi aziendali* [56], in cui è stata imposta una sanzione di circa 5,8 milioni di euro, l'Autorità ha

54 AGCM, provvedimento n. 26815 del 18 ottobre 2017, caso I796 - *Servizi di supporto e assistenza tecnica alla PA nei programmi cofinanziati dalla UE*, in Boll. n. 43/2017.

55 AGCM, provvedimento n. 26822 del 31 ottobre 2017, caso A484 - *Unilever/Distribuzione Gelati*, in Boll. n. 47/2017.

56 AGCM, provvedimento n. 26901 del 13 dicembre 2017, caso A500A - *Vodafone-SMS informativi aziendali*, in Boll. n. 50/2017.

negato l'attenuante ritenendo che la circostanza che fosse stato adottato (precedentemente all'avvio del procedimento) e aggiornato (successivamente) un programma di *compliance* antitrust non potesse essere valutata positivamente in quanto (i) l'adozione di un piano di *compliance*, avvenuta prima dell'avvio del procedimento, non ha di fatto impedito la condotta oggetto di contestazione. Sul punto, l'Autorità ha osservato che il programma di *compliance* precedente alle modifiche suindicate poneva un accento maggiore sulla fattispecie di intesa restrittiva della concorrenza rispetto a quella di abuso di posizione dominante, la quale rivestiva nel programma una posizione marginale. Ad avviso dell'Autorità, la laconica trattazione delle condotte di abuso di posizione dominante, l'assenza di indicazioni pratiche e di un sistema sanzionatorio, hanno comportato l'inefficacia del programma di *compliance* ai fini del contrasto delle condotte sanzionate. Inoltre, l'Autorità ha ritenuto che una parte del materiale del programma di *compliance* antitrust in oggetto forniva ad alcuni dipendenti indicazioni che si ponevano in contrapposizione con l'obbligo di collaborazione in capo all'impresa, in quanto potenzialmente idonee a favorire il rifiuto, l'omissione o il ritardo, senza giustificato motivo, di fornire all'Autorità informazioni ed esibire documenti richiesti nel corso dell'ispezione.

Infine, nel caso A493 - *Poste Italiane/prezzi recapito* [57], in cui è stata imposta una sanzione di circa 23 milioni di euro, l'Autorità ha ritenuto che non vi erano i presupposti per accordare l'attenuante in considerazione del fatto che il programma di *compliance*, adottato alla fine del 2015, è rimasto invariato nel corso dell'istruttoria, non avendo l'impresa apportato alcun elemento che abbia inciso sulla sua efficacia e utilità ai fini antitrust.

Alla luce delle decisioni più recenti dell'Autorità in tema di valutazione dei programma di *compliance* antitrust al fine della concessione dell'attenuante, appare evidente che elemento essenziale per poter usufruire dell'attenuante è la **tempestività**, sia nell'adozione e implementazione del programma sia nella fornitura all'Autorità di tutti gli elementi necessari a consentire un'adeguata valutazione del programma di *compliance* antitrust da parte dell'Autorità.

Inoltre, l'Autorità ha sempre di più analizzato nel dettaglio il contenuto dei programmi di *compliance* presentati dalle imprese per valutare la loro adeguatezza, escludendo l'applicazione dell'attenuante in relazione a programmi di *compliance* antitrust manifestamente inadeguati, per esempio, per l'insufficienza (o addirittura inadeguatezza) del contenuto (come nel caso A500A).

Alla luce di quanto sopra, risulta fondamentale che le imprese adottino, implementino e comunichino all'Autorità il programma di *compliance* antitrust in maniera tempestiva al fine di consentire all'Autorità un'adeguata valutazione dello stesso. Inoltre, è fondamentale che il contenuto del programma sia adeguato, anche in relazione alle specifiche circostanze dell'impresa. È imprescindibile, quindi, mantenere un monitoraggio ed un aggiornamento costante di tutte le fasi del processo di *compliance* antitrust per garantire che l'adeguatezza del programma di *compliance* antitrust si mantenga nel tempo, non solo in conside-

57 AGCM, provvedimento n. 26900 del 13 dicembre 2017, caso *Poste Italiane/prezzi recapito*, in Boll. n. 1/2018.

razione dell'evoluzione della casistica antitrust, ma anche alla luce dei possibili mutamenti nell'organizzazione e nelle attività dell'impresa e, quindi, dei rischi antitrust dell'impresa.

Infine, rileva segnalare che l'Autorità ha avviato nel mese di maggio 2018 una consultazione pubblica su uno schema di linee guida sulla *compliance* antitrust, le quali si propongono di descrivere cosa si intende e quali misure debbano essere adottate per una effettiva *compliance* antitrust e disci-plinare i benefici - in termini di attenuante - che ne possono derivare in caso di coinvolgimento dell'impresa in un procedimento antitrust. Conclusa la fase di consultazione, l'Autorità dovrebbe adottare a breve la versione definitiva di tali Linee Guida.

c. Programma di compliance e sanzioni antitrust: prospettiva comparatistica nell'UE

Meritano di essere tenute in considerazione anche alcune novità in relazione all'approccio adottato da altre Autorità antitrust in merito ai programmi di *compliance* antitrust.

Nel Regno Unito, a partire dal documento "*Drivers of Compliance and Non-compliance with Compe-tition Law*" [58] redatto nel 2010 dall'*Office of Fair Trading* (OFT), è prevista una possibile diminuzione della sanzione nel caso in cui l'impresa interessata abbia adottato, prima o dopo l'illecito, un programma di *compliance* conforme alle linee guida [59].

Anche l'*Autorité de la Concurrence* francese ha sottolineato, nel 2012, l'importanza dei programmi aziendali di compliance antitrust, pubblicando un apposito documento [60] nel quale i programmi di compliance già esistenti vengono presi in considerazione solo ai fini della *leniency*/immunità parziale o come attenuante negli illeciti in cui la *leniency* non è prevista, a patto che l'impresa dimostri di aver posto termine all'illecito prima dell'apertura del procedimento. Tuttavia, sembra essere attualmente in corso un ridimensionamento dell'importanza attribuita all'impegno di implementare programmi di *compliance* ai fini della riduzione della sanzione nell'ambito delle procedure di *settlement*, nella prassi dell'*Autorité*. In seguito a una decisione e ad un comunicato dell'autunno 2017, sembra infatti che l'autorità cominci a considerare la presenza di programmi di compliance come *standard practice*/prerequisito, specialmente per le imprese di grandi dimensioni, e non sia disposta a riconoscere l'attenuante in caso di promessa di implementazione degli stessi di per sé.

In Romania, i programmi di *compliance* antitrust sono riconosciuti dal 2011 quale circostanza attenuante (per una riduzione fino al 10% della sanzione).

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

59 Nello stesso senso si vedano le *Guidelines* pubblicate dalla *Competition and Markets Authority* nel 2011 (disponibili al seguente link: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284402/oft1341.pdf).

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

Nel giugno 2017 l'autorità di concorrenza rumena ha avviato una consultazione pubblica sulle sue nuove linee guida su come strutturare programmi di *compliance* efficaci e "su misura", pubblicandone una nuova versione, rivolta a società di tutte le dimensioni, alla fine dello stesso anno.

Il *Bundeskartellamt* tedesco, pur ammettendo l'importanza delle attività di *compliance* antitrust (considerate un obbligo legale), nelle proprie linee guida per il calcolo delle sanzioni antitrust adottate nel 2013 non riconosce alcun rilievo come circostanza attenuante all'adozione di un programma di *compliance* antitrust [61]. Tuttavia, il 9 maggio 2017, la *German Federal Court of Justice* (BGH) ha stabilito che i *compliance management systems* debbano essere presi in considerazione ai fini del calcolo delle sanzioni. La Corte si è pronunciata in un caso relativo ad iniziative di *antibribery compliance*, ma il riferimento normativo sul quale è intervenuta sono, più in generale, le regole applicabili ai sensi dell'*Administrative Offences Act* (che rileva anche in materia antitrust).

In Austria, l'autorità di concorrenza ha dichiarato nel mese di settembre 2017 di stare valutando la possibilità di riconoscere i programmi di *compliance* quale circostanza attenuante.

Altre Autorità, invece, pur riconoscendo l'importanza dell'adozione da parte delle aziende di programmi di *compliance* efficaci, mantengono la loro posizione di non ritenere che la mera esistenza di un programma di *compliance* antitrust possa essere considerata una circostanza attenuante o dare luogo a una diminuzione della sanzione.

A livello comunitario, con il documento "*Compliance matters. What companies can do better to re-spect EU competition rules*"[62], la Commissione europea aveva 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. La Commissione, tuttavia, continua a mantenere un'impostazione restrittiva e non prevede alcuna riduzione di pena in caso di adozione o efficace implementazione di un programma di *compliance*[63].

2 *Anonymous Whistleblowing Tool* della Commissione europea

Il 16 marzo 2017 la Commissione europea ha varato un nuovo strumento mediante il quale un priva-to cittadino può segnalarle l'esistenza di cartelli segreti e di altre violazioni delle norme antitrust, mantenendo l'anonimato.

61 Questa posizione è stata successivamente reiterata anche dal Presidente del *Bundeskartellamt* Andreas Mundt, cfr. Compliance Praxis, Service Guide 2014.

62 Disponibile al seguente link: http://bookshop.europa.eu/is-bin/INTERSHOP.enfinity/WFS/EU-Bookshop-Site/en_GB/-/EUR/ViewPublication-Start?PublicationKey=KD3211985.

63 Nello stesso senso si noti l'approccio adottato negli Stati Uniti dal *Department of Justice, Antitrust Division*, secondo cui, la mera esistenza di un programma di compliance non è sufficiente ad evitare un'indagine antitrust o a ridurre la sua sanzione in caso di un procedimento da parte del Dipartimento di Giustizia. La ragione di ciò, secondo la Divisione Antitrust, sta nel fatto che se un programma di conformità ha fallito nel prevenire o fermare la condotta illecita ad uno stadio preliminare, allora l'azienda in questione non merita credito per il programma che ha adottato.

Tale strumento offre un mezzo ulteriore ai singoli cittadini che sono a conoscenza dell'esistenza o del funzionamento di un cartello o di altri tipi di violazioni delle norme antitrust per contribuire a porre fine a tali pratiche.

Prima della sua introduzione, infatti, i cittadini potevano contattare la Direzione della Commissione che si occupa di concorrenza tramite un numero di telefono e un indirizzo di posta elettronica ad hoc, rinunciando all'anonimato.

Il nuovo strumento protegge l'anonimato degli informatori tramite un sistema di messaggistica criptata specificamente concepito, gestito da un fornitore di servizi esterno specializzato che, agendo da intermediario, si limita a inoltrare il contenuto dei messaggi ricevuti senza trasmettere i metadati, che potrebbero essere utilizzati per identificare l'informatore. Tale sistema consente comunicazioni bidirezionali: oltre a permettere agli individui di fornire informazioni, consente quindi alla Commissione di chiedere chiarimenti e dettagli, aumentando così la probabilità che le informazioni ricevute siano sufficientemente precise e affidabili per consentire l'avvio di un'indagine. Più in particolare, il nuovo strumento:

- permette ai singoli cittadini di fornire informazioni, dando loro anche la possibilità di chiedere alla Commissione una risposta ai messaggi inviati;
- consente alla Commissione di chiedere chiarimenti e dettagli;
- tutela l'anonimato dei singoli cittadini tramite comunicazioni criptate e il ricorso a un fornitore di servizi esterno;
- intende aumentare la probabilità che le informazioni ricevute siano sufficientemente precise e attendibili, consentendo in tal modo alla Commissione di darvi seguito aprendo un'indagine.

La Commissaria europea per la concorrenza Margrethe Vestager ha commentato l'importanza di tale strumento evidenziando che grazie allo stesso "*chiunque sia preoccupato riguardo ad una pra-tica commerciale a suo parere scorretta può contribuire a porvi rimedio"* e che *"le informazioni basate su una conoscenza diretta possono essere uno strumento efficace per aiutare la Commissione a smascherare i cartelli e le altre pratiche anticoncorrenziali. (…) Tali informazioni possono contribuire rapidamente e più efficacemente alla conclusione delle nostre indagini, a vantaggio sia dei consumatori che dell'economia europea nel suo insieme*".

Nelle intenzioni della Commissione il nuovo sistema dovrebbe aumentare la probabilità di smascherare e perseguire le imprese responsabili e, pertanto, costituirebbe per esse un ulteriore deterrente all'ingresso o alla permanenza in cartelli o all'adozione di altri tipi di comportamenti anticoncorrenziali illegali.

Per le imprese coinvolte in cartelli ciò non significa solo che aumenta la probabilità di essere sottoposti a indagini da parte della Commissione, ma anche che in tali casi diminuisce la possibilità di ottenere l'immunità dalle ammende nel quadro dei programmi di *leniency*. Infatti, qualora la Commissione abbia già ottenuto le informazioni rilevanti da un singolo, le imprese che collaborano

con la Commissione possono beneficiare al massimo di una riduzione dell'ammenda per la loro cooperazione e non della totale immunità.

Alla luce del nuovo strumento di segnalazione della Commissione, è pertanto opportuno che le aziende adottino adeguati strumenti interni di segnalazione (ad es. *internal whistleblower hotline, ombudsman system*, *compliance declaration processes*) e di incentivazione alla segnalazione, per conoscere tempestivamente le potenziali violazioni antitrust.

A riprova della convinzione della Commissione circa l'efficacia degli strumenti di *whistleblowing* e degli sforzi tesi a incentivarne l'utilizzo, nell'aprile 2018 la Commissione ha adottato una serie di iniziative per rafforzare la protezione dei *whistleblowers*[64], tra cui una proposta di direttiva per la protezione di coloro che denunciano **violazioni del diritto UE** (i cosiddetti "*whistleblowers*"), al fine di offrire una protezione più efficace e omogenea dei denuncianti nell'UE. L'art. 1 della proposta di direttiva contiene l'elenco delle materie di diritto UE cui lo standard minino comune di tutela dei *whistleblowers* dovrebbe applicarsi, tra cui il diritto della concorrenza[65]. L'art. 4 prevede l'obbligo di predisporre un meccanismo di segnalazione degli illeciti e di riscontro delle denunce sia nel privato, per tutte le imprese con più di 50 dipendenti o con un fatturato annuo superiore ai 10 milioni di euro, sia nel pubblico, per tutte le amministrazioni statali e regionali e tutti i comuni con più di 10.000 abitanti. La proposta, che dovrà ora passare al vaglio del Parlamento europeo e del Consiglio UE, mira da un lato a garantire la riservatezza del denunciante e a prevenire forme di ritorsione nei suoi confronti, dall'altro a favorire un'adeguata divulgazione al pubblico qualora la questione si riveli di particolare importanza per l'interesse pubblico.

3 Accordi Verticali e vendite online

Gli accordi verticali e le restrizioni alle vendite *online* sono state oggetto negli ultimi anni di crescente attenzione, sia da parte delle Autorità nazionali della concorrenza e della Commissione europea, sia da parte della Corte di giustizia dell'Unione europea. Con riferimento agli accordi istitutivi di un sistema di distribuzione selettiva [66], nella sentenza *Pierre Fabre* [67], la Corte di giusti-

64 Cfr. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=620400

65 Tra cui, appalti pubblici, servizi finanziari, riciclaggio di denaro e finanziamento del terrorismo, sicurezza dei prodotti, sicurezza dei trasporti, tutela ambientale, sicurezza nucleare, sicurezza degli alimenti e dei mangimi e salute e benessere degli animali, salute pubblica, protezione dei consumatori, tutela della vita privata, protezione dei dati e sicurezza delle reti e dei sistemi informativi, violazioni delle norme UE sulla concorrenza e violazioni e abusi concernenti le norme in materia di imposta sulle società e i danni causati agli interessi finanziari dell'UE.

66 Ai sensi dell'articolo 1, lettera e), del regolamento (UE) n. 330/2010 relativo all'applicazione dell'articolo 101, paragrafo 3, del trattato sul funzionamento dell'Unione europea a categorie di accordi verticali e pratiche concordate (GUUE L 102 del 23.04.2010), "*…per «sistema di distribuzione selettiva» si intende un sistema di distribuzione nel quale il fornitore si impegna a vendere i beni o servizi oggetto del contratto, direttamente o indirettamente, solo a distributori selezionati sulla base di criteri specificati e nel quale questi distributori si impegnano a non vendere tali beni o servizi a rivenditori non autorizzati nel territorio che il fornitore ha riservato a tale sistema…*".

67 CGUE 13.10.2011, causa C-439/09, *Pierre Fabre*. La controversia oggetto di tale causa era sorta a seguito del divieto imposto dall'impresa *Pierre Fabre Dermo Cosmétique* ai suoi distributori autorizzati

zia ha affermato che, se da un lato, in assenza di una giustificazione oggettiva, tali accordi devono essere considerati come restrizioni della concorrenza per oggetto, dall'altro lato, esistono esigenze legittime, come la salvaguardia di un commercio specializzato, in grado di fornire prestazioni specifiche per prodotti di alto livello qualitativo e tecnologico, che giustificano la limitazione della concorrenza sui prezzi a vantaggio della concorrenza riguardante fattori diversi dai prezzi. Pertanto, nel rispetto di determinate condizioni la scelta di una simile rete non ricade nel divieto di cui all'art. 101, n. 1, del Trattato sul funzionamento dell'Unione europea (TFUE)[68]. La Corte ha osservato che la clausola controversa che vieta, di fatto, la commercializzazione via internet dei prodotti oggetto del contratto costituisce una restrizione per oggetto ai sensi dell'articolo 101, paragrafo 1, TFUE, se risulta non essere giustificata a seguito di un esame individuale e concreto del tenore e dell'obiettivo della stessa nonché del contesto giuridico ed economico in cui si colloca.

Nella successiva sentenza relativa alla causa *Coty Germany* [69], la Corte ha ripreso i suddetti criteri e ha osservato che la clausola che vieta ai rivenditori autorizzati dell'impresa *Coty Germany* di vendere *online* i prodotti contrattuali tramite piattaforme terze riconoscibili inserita nell'accordo di distribuzione selettiva in esame[70], persegue in effetti l'obiettivo di salvaguardare l'immagine di lusso e prestigio dei prodotti interessati, ha natura oggettiva e uniforme e si applica indiscriminatamente nei confronti di tutti i distributori autorizzati[71]. La Corte ha inoltre sottolineato che, differentemente dal caso *Pierre Fabre*, nel caso *Coty Germany* non si vieta in assoluto ai distributori autorizzati di vendere su internet i prodotti contrattuali, ma è vietata soltanto la vendita *online* tramite piattaforme terze. Pertanto, i distributori autorizzati possono vendere *online* i prodotti oggetto del contratto sia mediante i propri siti internet, qualora dispongano di una vetrina elettronica del negozio autorizzato e il carattere lussuoso dei prodotti sia salvaguardato, sia tramite piattaforme terze non autorizzate se l'intervento di queste ultime non è visibile[72]. Secondo la Corte, a queste condizioni, il divieto in esame non si spinge oltre quanto necessario per salvaguardare l'immagine di lusso dei prodotti della *Coty Germany*[73].

di vendere su internet i suoi prodotti cosmetici e di igiene personale. Per l'autorità della concorrenza francese, un tale divieto violava il Codice del commercio francese, nonché l'allora articolo 81 CE (ora articolo 101 TFUE).

68 CGUE 13.10.2011, causa C-439/09, *Pierre Fabre*, punti 39-41. Si vedano inoltre i punti 54 e 56 degli Orientamenti sulle restrizioni verticali (GUUE C 130 del 19.05.2010).

69 CGUE 06.12.2017, causa C-230/16, *Coty Germany*.

70 Ai rivenditori autorizzati era tuttavia consentito di vendere i prodotti contrattuali su internet, a condizione che utilizzassero la propria vetrina elettronica, oppure piattaforme terze ma senza che l'intervento di esse fosse riconoscibile dal consumatore.

71 CGUE 06.12.2017, causa C-230/16, *Coty Germany*, punti da 30 a 35.

72 CGUE 06.12.2017, causa C-230/16, *Coty Germany*, punto 54.

73 La sentenza *Coty Germany* ha avuto un impatto sulla giurisprudenza delle Corti degli Stati membri. Nei Paesi Bassi, il Tribunale di Amsterdam, con decisione dell'ottobre 2017, sulla base delle conclusioni dell'Avvocato Generale *Wahl* rese nel caso *Coty Germany*, ha stabilito che l'impresa *Nike* non aveva violato il diritto della concorrenza nell'imporre al suo rivenditore *Action Sport* di commercializzare i prodotti *Nike* sul *marketplace* di *Amazon* [Decisione del Tribunale di Amsterdam del 04.10.2017, C/13/615474 / HA ZA 16-959, Nike]. La sentenza della Corte nel caso *Coty Germany* è inoltre in linea con la precedente decisione della Corte di appello di Francoforte nel caso *Deuter* [Decisione della Corte di appello di Francoforte del 22.12.2015, 11 U (Kart) 84/14, Deuter], in cui detta Corte ha stabilito che il produttore tedesco di zaini *Deuter Sport GmbH* ("Deuter") ha agito legalmente nel vietare

La particolare attenzione rivolta alla compatibilità dei sistemi di distribuzione selettiva per le vendite *online* con le norme europee sulla concorrenza è dovuta all'aumento del ricorso a tali sistemi da parte dei produttori. Nella Relazione finale sull'indagine settoriale sul commercio elettronico del 10 maggio 2017[74], la Commissione ha osservato come l'aumento del commercio elettronico abbia avuto un impatto significativo sulle strategie di distribuzione delle imprese e sul comportamento dei consumatori, che ha comportato un maggior ricorso a sistemi di distribuzione selettiva. L'indagine ha anche evidenziato un più ampio ricorso alle restrizioni di tipo verticale che consentono un maggior controllo sulla distribuzione dei prodotti. A seconda del modello aziendale e della sua strategia, le restrizioni alle vendite *online* possono assumere varie forme, come restrizioni riguardanti i prezzi o gli strumenti di confronto dei prezzi *online*, il divieto di vendere su *marketplace* e/o l'esclusione di operatori presenti esclusivamente *online* dalla rete di distribuzione.

Poco dopo la pubblicazione della Relazione finale, la Commissione europea ha aperto, nel giugno 2017, un'indagine formale sulle pratiche di distribuzione dell'impresa di abbigliamento *Guess* per determinare se gli accordi di distribuzione di *Guess* possano limitare i rivenditori autorizzati a vendere *online* ai consumatori o ai rivenditori di altri Stati membri, o ai grossisti di rifornire i rivenditori di Stati membri differenti. Nello stesso mese, la Commissione ha altresì avviato tre indagini separate per valutare se alcune pratiche di licenza e distribuzione messe in atto da *Nike*, *Sanrio* e *Universal Studios* restringano, in violazione delle norme antitrust, la vendita transfrontaliera e *online* dei prodotti per il *merchandise* concessi in licenza all'interno del mercato unico europeo. Tali indagini si legano a precedenti indagini avviate dalla Commissione nel febbraio 2017, relative ai settori delle prenotazioni alberghiere, dei videogiochi e dei prodotti elettronici di consumo.

Alla luce di quanto sopra, risulta fondamentale che le imprese includano i propri contratti di distribuzione e di vendita *online* nell'ambito delle loro attività di *compliance*, e che questi siano eventualmente oggetto di revisione per allinearsi alla normativa europea sulla concorrenza.

ai rivenditori autorizzati di vendere prodotti *Deuter* su mercati online come il *marketplace* di *Amazon*, ritenendo tuttavia che il divieto di utilizzare i siti web di comparazione dei prezzi fosse illegale. In alcuni casi precedenti alla causa *Coty Germany,* tuttavia, alcuni Stati membri hanno ritenuto che le restrizioni alle vendite online attraverso piattaforme fossero in contrasto con il diritto della concorrenza. A tal proposito, nel caso *Adidas,* l'Autorità della concorrenza tedesca aveva aperto un'indagine nei confronti dell'impresa *Adidas* a causa di alcune clausole contrattuali che vietavano ai rivenditori di vendere i prodotti contrattuali attraverso piattaforme quali *eBay* e *Amazon*. Il procedimento è stato chiuso dopo che l'impresa ha modificato le condizioni previste nei suoi contratti di distribuzione relative alla vendita online in modo da non restringere la concorrenza [*Bundeskartellamt,* B3-137/12, 27.06.2014. Inoltre, in data 18.11.2015, l'Autorità per la concorrenza francese ha chiuso un'indagine nei confronti di *Adidas*, a seguito dell'impegno di questa di eliminare dai propri contratti di distribuzione qualsiasi clausola che vieta ai suoi distributori di utilizzare i marketplace]. Infine, nel caso *Caudalie/eNova*, la Corte di Appello di Parigi aveva stabilito che il divieto imposto ai rivenditori *Caudalie* di vendere i suoi prodotti attraverso piattaforme online poteva costituire una restrizione alla concorrenza [Tuttavia, la Corte di Cassazione francese ha ribaltato tale decisione ritenendo che la Corte d'Appello non avesse sufficientemente motivato la sua conclusione secondo cui un obbligo nel sistema di distribuzione selettiva di *Caudalie* costituiva una probabile restrizione della concorrenza per oggetto. *Cour de Cassation, Chambre commerciale*, 13.09.2017, 16-15067, *Caudalie/eNova*].

74 COM(2017) 229 final.

4. Rilevanza della scontistica come pratica abusiva

Tra i comportamenti che possono comportare un abuso di posizione dominante a causa della loro capacità di compromettere una concorrenza effettiva sul mercato rientra la prassi di conferire sconti ai propri clienti. Nei suoi Orientamenti[75] del 2008 la Commissione definisce gli sconti condizionati come "... *sconti concessi ai clienti per ricompensarli di un particolare tipo di comportamento di acquisto… lo sconto viene concesso su tutti gli acquisti (sconti retroattivi) o soltanto su quelli che superano la soglia richiesta (sconti incrementali)*...". Nella sua analisi dei casi riguardanti sconti effettuati da imprese in posizione dominante, la Corte di giustizia ha storicamente individuato tre categorie differenti di sconti:

- gli sconti quantitativi, o di quantità, connessi esclusivamente al volume degli acquisti effettuati presso un'impresa in posizione dominante;
- gli sconti di esclusiva la cui concessione è subordinata alla condizione che il cliente si rifornisca, per la totalità o per una parte considerevole del suo fabbisogno, presso l'impresa in posizione dominante; e,
- gli sconti facenti parte della terza categoria, o sconti di fedeltà, nei quali la concessione di un incentivo finanziario non è direttamente connessa alla condizione di un approvvigionamento esclusivo o quasi esclusivo presso l'impresa in posizione dominante, ma nei quali il meccanismo della concessione dello sconto può anche rivestire un effetto fidelizzante.

Mentre gli sconti puramente quantitativi non comportano particolari effetti negativi dal punto di vista della concorrenza, la situazione è differente per quanto riguarda le altre due categorie di sconti. Nella sentenza *Hoffmann-La Roche* del 1979, la Corte di giustizia ha affermato che "... [p]*er un'impresa che si trova in posizione dominante su un mercato, il fatto di vincolare — sia pure a loro richiesta — gli acquirenti con l'obbligo o la promessa di rifornirsi per tutto o gran parte del loro fabbisogno esclusivamente presso l'impresa in questione, costituisce sfruttamento abusivo di posizione dominante ai sensi dell'art. 86 del Trattato, tanto se l'obbligo in questione è imposto sic et simpliciter, quanto se ha come contropartita la concessione di sconti…*"[76]. Mentre nella sentenza *Michelin I* la Corte ha sostenuto che "...*a differenza degli sconti quantitativi, che dipendono solo dal volume degli acquisti effettuati presso il produttore, il premio di fedeltà, mirante ad impedire, mediante la concessione di vantaggi finanziari, che i clienti si riforniscano presso produttori concorrenti, costituisce un abuso ai sensi dell'art. 86 del Trattato… Per altro, l'art. 86 non prescrive che venga dimostrato che il comportamento abusivo abbia, in effetti, pregiudicato in misura rilevante gli scambi fra stati membri, ma richiede che sia provato che tale comportamento è atto a produrre quest'effetto…*"[77].

75 Orientamenti sulle priorità della Commissione nell'applicazione dell'articolo 82 del trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti, COM/2008/0832 def.

76 CGUE 13.02.1979, causa 85/76, *Hoffmann-La Roche*/Commissione, punto 89.

77 CGUE 09.11.1983, causa 322/81, *Nederlandsche Banden Industrie Michelin* (Michelin I)/ Commissione, punti 13, 15.

Negli Orientamenti del 2008, la Commissione ha affermato che "… [s]*petta all'impresa dominante fornire tutte le prove necessarie a dimostrare che il comportamento in questione è obiettivamente giustificato…*" (paragrafo 30). Nonostante gli Orientamenti, nella sentenza del Tribunale del 2014 relativa al caso *Intel*, i giudici ribadiscono che, con riferimento agli sconti di esclusiva, "*…non è necessario verificare se la Commissione abbia effettuato il test AEC secondo le regole applicabili e che non è neanche necessario esaminare la questione se i calcoli alternativi proposti dalla ricorrente siano stati effettuati correttamente. Infatti, neanche un risultato positivo di un test AEC sarebbe idoneo ad escludere l'effetto preclusivo potenziale…*"[78]. *Intel* ha impugnato la sentenza del Tribunale innanzi alla Corte di giustizia; quest'ultima ha annullato la sentenza del Tribunale e, assumendo un nuovo orientamento, ha affermato che "*…nel caso in cui l'impresa considerata sostenga nel corso del procedimento amministrativo, sulla base di elementi di prova, che il suo comportamento non ha avuto la capacità di restringere la concorrenza e, in particolare, di produrre gli effetti di esclusione dal mercato addebitati … la Commissione è tenuta, non solo ad analizzare, da un lato, l'ampiezza della posizione dominante dell'impresa sul mercato pertinente e, dall'altro, il tasso di copertura del mercato ad opera della pratica concordata, nonché le condizioni e le modalità di concessione degli sconti di cui trattasi, la loro durata e il loro importo, ma deve anche valutare l'eventuale esistenza di una strategia diretta ad escludere dal mercato i concorrenti quantomeno altrettanto efficaci…*"[79]. La Corte ha inoltre aggiunto che "*…l'analisi della capacità di escludere dal mercato è del pari pertinente ai fini della valutazione della questione se un sistema di sconti rientrante in linea di principio nell'ambito del divieto di cui all'articolo 102 TFUE possa essere oggettivamente giustificato…*"[80] e che il Tribunale, di conseguenza, è tenuto a valutare "*…tutti gli argomenti della parte ricorrente diretti a rimettere in discussione la fondatezza delle constatazioni raggiunte dalla Commissione quanto alla capacità di preclusione dal mercato del sistema di sconti considerato…*"[81] incluso, qualora la Commissione lo abbia svolto, il test AEC (*As Efficient Competitor Test*), al fine di constatare un abuso di posizione dominante. La sentenza della Corte nel caso *Intel*, quindi, sembrerebbe costituire un punto di svolta sottolineato anche dall'Avvocato generale *Wahl* nelle conclusioni relative alla causa MEO, nelle quali afferma che "…[s]*i è progressivamente imposto, tanto nella prassi decisionale delle autorità preposte alla concorrenza quanto nella giurisprudenza più recente della Corte, il principio secondo cui, quando si tratta di esaminare un comportamento imprenditoriale sotto il profilo dell'articolo 102 TFUE, la presenza di una restrizione della concorrenza non può essere presunta. Per concludere nel senso dell'esistenza di una tale restrizione, occorre, in ogni caso, procedere a un esame degli effetti reali o potenziali della misura incriminata alla luce di tutte le circostanze della fattispecie…*"[82]. Un'analisi delle condotte anticompetitive eseguita sulla base dei loro effetti, anziché per oggetto, rende possibile una migliore difesa per le imprese accusate di violazioni della normativa antitrust. Se questo orientamento venisse confermato, cesserebbero di esistere categorie di sconti abusive

78 CGUE 12.06.2014, causa T-286/09, *Intel Corp.*/ Commissione europea, punto 151.

79 CGUE 06.09.2017, causa C-413/14 P, *Intel Corporation Inc.*/Commissione europea, punti 138, 139.

80 CGUE 06.09.2017, causa C-413/14 P, *Intel Corporation Inc.*/Commissione europea, punto 140.

81 CGUE 06.09.2017, causa C-413/14 P, *Intel Corporation Inc.*/Commissione europea, punto 141.

82 Conclusioni dell'Avvocato Generale Wahl del 20.12.2017, causa C-525/16, *Meo – Serviços de Comunicações e Multimédi*a, punto 70

a priori e ogni caso andrebbe analizzato nel dettaglio. Ciò permetterebbe alle imprese dotate di uno schema di sconti accuratamente formulato nel rispetto della disciplina antitrust, di sviluppare un'opportuna difesa in caso di indagini o di sanzioni per la violazione di tale normativa. A tal fine, le imprese dovrebbero valutare l'adozione di schemi in cui i periodi di riferimento per il calcolo degli sconti siano di breve durata, convertire gli sconti retroattivi in sconti incrementali e ridurre la distanza tra i differenti livelli negli schemi incrementali; insieme all'adozione di ulteriori misure quali, ad esempio, legare la concessione di sconti a riduzioni di costi documentabili o effettuare gli sconti solo su prodotti in riferimento ai quali l'impresa non riveste una posizione dominante sul mercato.

5. Big Data

d. Introduzione

Nel contesto della sua Indagine di settore sul commercio digitale, la Commissione ha precisato come l'emersione di Internet e la creazione di un mercato unico digitale costituiscano una grande opportunità di crescita per l'economia europea, sottolineando per l'appunto che "*Digital technologies have already made a major contribution to economic growth. Between 2001 and 2011, digitalisation accounted for 30% of GDP growth in the EU*"[83].

A tal proposito, (un) ruolo centrale – anche in ambito antitrust - è indubbiamente assunto dal fenomeno dei Big Data ovvero l'ingente ammontare di informazioni, generalmente di carattere personale, che può essere raccolto, immagazzinato, analizzato (*data analytics*) e in ultima analisi sfruttato dalle piattaforme quale possibile vantaggio competitivo. Le caratteristiche salienti dei Big Data sono solitamente individuate in quattro "v": *volume, velocità, varietà e valore*[84]. In particolare, tali dati hanno acquisito un valore enorme per l'economia digitale tale da meritare la definizione di *new currency* del nuovo millennio[85].

Se da un lato, dunque, l'avvento di tale fenomeno accresce il livello innovativo e apporta notevoli guadagni in termini di efficienza, a livello applicativo comporta anche che i modelli di *compliance* aziendale si aggiornino sotto un triplice profilo: al fine di salvaguardare le crescenti istanze di *privacy*, di riconoscere la rilevanza che tale tipologia di dati assume nelle fattispecie antitrust (in particolare nelle operazioni di concentrazione) e nell'ottica di regolare le sempre più "invasive" attività di *audit*.

83 COMMISSION STAFF WORKING DOCUMENT A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015SC0100#footnote5) .

84 Gartner, 2014.

85 Giannaccari, 2017.

e. Necessità di riadattare i modelli di compliance al fine di salvaguardare le istanze di privacy

La prima considerazione da svolgere riguarda la specifica circostanza che i Big Data sono anche, in larga parte, *personal data* dei consumatori che li forniscono. Il discorso del rapporto tra dati e concorrenza è perciò intersecato da tutte le valutazioni ed istanze che riguardano le nuove frontiere della protezione della privacy, della tutela del consumatore e dei diritti di proprietà sui dati del consumatore e di proprietà intellettuale sul processo di elaborazione dei dati in capo all'impresa.

Si osserva a riguardo, come esempio di interazione tra la disciplina della concorrenza e quella posta a tutela della privacy, che l'Autorità garante della concorrenza tedesca ha avviato un'indagine nei confronti di Facebook volta ad accertare se quest'ultima, ritenuta dominante nel mercato dei social network in Germania, possa aver abusato del proprio potere di mercato ottenendo l'accesso a dati di terze parti, attraverso WhatsApp e Instagram, nonché con il monitoraggio dei siti ai quali gli utenti accedono. Nel mirino dell'antitrust tedesco è pertanto finita la raccolta di dati da parte del social network di Palo Alto al di fuori dello stesso e la loro inclusione nell'account di Facebook. In particolare, l'autorità sottolinea come "*Data protection, consumer protection and the protection of competition interlink where data, as in Facebook's case, are a crucial factor for the economic dominance of a company*"[86].

In quest'ottica, i modelli di *compliance* devono essere adattati alla struttura societaria e alla *governance* interna della singola società coinvolta, conformandosi alle disposizioni attualmente vigenti in materia di privacy e protezione dei dati, così come definite nel Regolamento Privacy[87].

f. Big Data come fonte di potere di mercato e come oggetto della tutela antitrust

Dalla recente casistica della Commissione europea si evince una particolare attenzione al fenomeno dei Big Data nell'ambito dello scrutinio delle fattispecie antitrust.

In particolari si noti che i Big Data sono considerati un potente strumento per accrescere il potere di mercato degli operatori, permettendo l'innalzamento di barriere all'ingresso.

L'utilizzo di tali dati può, infatti, sfociare in condotte abusive unilaterali, consistenti

i. nello sfruttamento di tali dati da parte delle imprese

ii. nel *lock-in* degli utenti, ovvero nel contribuire a rendere la domanda meno mobile in quanto la perdita di dati nel passaggio da una piattaforma all'altra rappresenta uno *switching cost* per gli utenti

86 Bundeskartellamt, risultati preliminari indagine: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html).

87 Regolamento (UE) n. 2016/679.

iii. nella violazione della *privacy*, e infine

iv. nel rifiuto di concedere l'accesso ai dati da parte di concorrenti qualora questi possano qualificarsi come una *essential facility*.

Meritevole di considerazione è anche la circostanza secondo la quale l'avanzare della nuova frontiera degli algoritmi e dell'intelligenza artificiale agevola la collusione tra più imprese.

Contrariamente, è stato argomentato che i Big Data non possano per loro natura rappresentare un vantaggio competitivo per le imprese che ne hanno il controllo, poiché una delle loro caratteristiche consiste proprio nell'agile reperibilità degli stessi: i costi di raccolta non sono necessariamente elevati e tali dati sono sostanzialmente dappertutto, si possono comprare/barattare con un servizio, o acquisire da *brokers*.

In aggiunta, il valore dei dati per un'impresa è il risultato della relazione tra il loro volume e varietà, e dipende in larga misura dalla qualità dell'app/algoritmo che li sviluppa. Il trattamento di tali dati, inoltre, è generalmente finalizzato all'identificazione e valutazione delle caratteristiche, preferenze e abitudini del consumatore (c.d. attività di profilazione), allo scopo di rendere maggiormente personalizzato il servizio offerto. In particolare, nel mercato della pubblicità *online*, le imprese competono principalmente sul piano tecnologico e degli algoritmi per aumentare l'efficacia dei messaggi.

La volontà di indagare a fondo il fenomeno ha aperto la strada in data 30 maggio 2017 ad un'indagine conoscitiva congiunta sui Big Data da parte dell'Autorità Garante della Concorrenza e del Mercato ("AGCM"), insieme con l'Autorità per le Garanzie nelle Comunicazioni ("AGCOM") e il Garante Privacy[88] volta, per l'appunto, ad approfondire i cambiamenti derivanti dai Big Data sugli utenti che forniscono i dati, sulle imprese che li utilizzano e sui mercati.

g. I Big Data assumono oggi una rilevanza autonoma sotto il profilo economico: impatto nelle operazioni di concentrazione (posizione di mercato delle imprese coinvolte)

Al momento la casistica antitrust che vede interessati i Big Data è circoscritta prevalentemente a fattispecie concentrative. Le operazioni di concentrazione connesse ai Big Data sono aumentate globalmente tra il 2008 e il 2013 da 55 a 134, un esempio è costituito dall'acquisizione da parte di Google dell'applicazione di navigazione GPS israeliana *Waze*[89], avvenuta nel 2013. In tale contesto, lo scrutinio dell'autorità antitrust competente si focalizza sulla possibilità che si realizzi attraverso l'operazione di concentrazione, una *foreclosure* del mercato, frutto del maggiore e migliore accesso alle informazioni, non replicabile dai concorrenti. Un caso emblematico è rappresentato dall'acquisi-

88 IC53 Big data (http://www.agcm.it/indagini-conoscitive-db/open/C12564CE0049D16/59255F62EC162CC1C1258137003BB842.html).

89 Waze Ltd. / Alphabet Inc. L'operazione è stata approvata dalla *Federal Trade Commission* (U.S.) e dall'*Office Fair Trading* (UK).

zione da parte di Facebook di Whatsapp[90] avvenuta nel 2014 e approvata dalla Commissione europea in quanto non precludeva la reperibilità dei dati da parte dei concorrenti. Come ricordato, infatti, l'impatto dei Big Data sulla capacità delle imprese di concorrere dipende dal volume e dalla varietà di informazioni, nonché dalla capacità dell'impresa di raccogliere e analizzare velocemente tali informazioni.

Si osserva come tali operazioni contribuiscano a generare importanti efficienze nel mercato di riferimento (caso emblematico la concentrazione *TomTom/Tele Atlas* [91]) e/o a contrastare altre imprese in posizione monopolistica come, a titolo di esempio, Google. L'approvazione della *joint venture* Microsoft/Yahoo![92] si sarebbe basata proprio sulla circostanza, tra altre, per cui quest'ultima avrebbe potuto accedere ad una mole di dati talmente ampia da poter aumentare la concorrenza nei confronti di Google, spingendola a mantenere se non ad accelerare gli sforzi innovativi sul mercato.

Attualmente, tuttavia, si rileva come sfuggano dal controllo, quelle concentrazioni che vedono interessate imprese, le cui quote di mercato non superano le soglie necessarie, ma che detengono nondimeno un ingente ammontare di dati, tale per cui l'operazione potrebbe far sorgere effetti pregiudizievoli sul piano concorrenziale. Avanza perciò la necessità di esaminare le operazioni conglomerali con lenti nuove, non essendo le soglie di fatturato in grado di rappresentare efficacemente la nuova economia digitale.

h. I Big Data assumono un peso anche nell'attività di audit

In conclusione, l'utilizzo dei Big Data nell'ambito delle operazioni di *audit* ha modificato la modalità di reperimento delle informazioni. L'integrazione dei Big Data con i dati tradizionali ha, inoltre, comportato un'estensione delle informazioni reperibili. Mentre i dati contabili tradizionali sono prevalentemente quantitativi e strutturati, i Big Data includono anche dati non strutturati e semi-strutturati che offrono più prove e informazioni dettagliate.

Parallelamente all'aumento quantitativo e qualitativo dei dati seguono crescenti esigenze di *privacy*. Per tale motivo, ai fini delle attività di *audit* sarà necessario indicare come e da chi verranno svolte le indagini informatiche e come verrà tutelata la *privacy*.

90 Commissione europea, 3 ottobre 2014, M.7217, *Facebook/Whatsapp*.
91 Commissione europea, 14 maggio 2008, M.4854, *Tomtom/Tele Atlas*.
92 Commissione europea, 18 febbraio 2010, M.5727, *Microsoft/Yahoo! search business*.

CAPITOLO 4 di Manuela Bianchi, Micaela Barbotti e Roberto Tirone

I flussi informativi da e verso l'Organismo di Vigilanza

sommario: 1. Il ruolo centrale dei flussi informativi nel sistema di controllo interno previsto ex D. Lgs. 231/2001 – 2. Le indicazioni dottrinali, giurisprudenziali e le Linee Guida in tema di Modello Organizzativo e flussi informativi – 3. I modi e i tempi dei flussi informativi – 4. Rapporti dell'OdV con altri organi di controllo nell'ottica di un sistema integrato – 5. La realizzazione dei documento contenente i flussi informativi verso l'OdV – 6. Coordinamento degli obblighi in materia di flussi informativi con il sistema sanzionatorio

1. Il ruolo centrale dei flussi informativi nel sistema di controllo interno previsto *ex* D. Lgs. 231/2001

1.1

Come noto, il D.lgs. 231/2001, se da un lato ha introdotto nell'ordinamento giuridico italiano la responsabilità c.d. (penal)amministrativa degli enti in caso di commissione, da parte di un soggetto apicale o sottoposto di uno dei reati presupposto contemplati dalla stessa legge, dall'altro ha riconosciuto, al verificarsi del fatto penale, la possibilità per gli enti medesimi di sottrarsi alle conseguenze sanzionatorie previste a loro carico, attraverso l'adozione e l'effettiva applicazione del c.d. Modello Organizzativo.

Tuttavia, la funzione schermante del Modello Organizzativo a favore dell'ente risulta efficace, ai sensi del disposto di cui alla lettera b) del primo comma dell'art. 6, D.lgs. 231/2001, solamente se "*il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo*", l'Organismo di Vigilanza (di seguito, anche "OdV").

Tralasciando in questa sede le problematiche inerenti alla posizione nell'organigramma aziendale dell'OdV e all'identità dei soggetti che lo compongono, risulta importante sottolineare come quest'attività di monitoraggio e di aggiornamento è e deve essere resa possibile attraverso un continuo flusso di informazioni da e verso l'OdV. Tale necessità viene riconosciuta anche dal Legislatore, ove prevede che il Modello Organizzativo abbia al proprio interno "*uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite,*

rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione" (art. 6, comma 2-bis lett. a), D. Lgs. 231/2001).

Tale flusso informativo risulta essere essenziale in quanto permette all'Organismo di Vigilanza, pur mantenendo il suo ruolo autonomo, di monitorare l'effettiva applicazione del Modello Organizzativo e di segnalare tempestivamente profili di rischio della sua violazione o lacune.

1.2

Tuttavia, le informazioni in ingresso non costituiscono l'unico flusso che interessa l'OdV.

Ricorrendo alla metafora offertaci da Carlo Piergallini, professore ordinario di diritto penale presso l'Università di Macerata, il flusso di informazioni che riguarda l'Organismo di Vigilanza ben può essere descritto come "*una stella con tante punte, che si muovono, continuativamente, a doppio senso: per un verso, si proiettano verso i soggetti che presidiano il processo a rischio-reato, per ottenere i flussi informativi previsti dal modello; per altro e collegato verso, possono insinuarsi nel processo, come controllori di secondo grado, esercitando poteri ispettivi e di vigilanza. Destinatario dell'attività dell'OdV è, essenzialmente, il vertice della società, al quale compete la decisione finale sulle segnalazioni che gli vengono trasmesse. Va, infatti, sottolineato subito un aspetto fondamentale dell'Organismo di Vigilanza, desumibile dal dettato normativo: esso vanta esclusivamente poteri di sorveglianza e di controllo, sì che gli è preclusa qualsiasi attività di gestione, sia essa attiva che impeditiva: tale divieto è funzionale alla salvaguardia e all'implementazione della imparzialità dell'organo, argine indispensabile per evitare insanabili conflitti di interesse*" (C. Piergallini, "*Paradigmatica dell'autocontrollo penale (dalla funzione alla struttura del "modello organizzativo" ex d.lg. n. 231/2001*", in Cass. pen., fasc.1, 2013, pag. 0376B).

Al fine di descrivere compitamente le informazioni che l'Organismo di Vigilanza è chiamato a gestire, è necessario superare l'efficace descrizione metaforica di cui sopra. Infatti, il flusso informativo promanante dall'OdV non risulta essere indirizzato solo al vertice della società, ma ha come destinatari (seppur i contenuti possano essere differentemente rilevanti a seconda del destinatario) tutti coloro che svolgono funzioni di direzione, gestione, amministrazione e controllo dell'ente, nonché tutti i dirigenti e i dipendenti. La finalità di tale flusso informativo in uscita è quella di assicurare la massima diffusione del Modello Organizzativo, per renderne effettiva l'applicazione ad ogni livello aziendale.

L'Organismo di Vigilanza si trova dunque a dover gestire un flusso che risulta essere complesso e multidirezionale.

Riassumendo, l'OdV, dopo aver posto in essere un'adeguata formazione nei confronti dei soggetti operanti all'interno dell'ente, dapprima riceve le informazioni riguardanti l'effettiva applicazione del Modello Organizzativo e le eventuali lacune che possano comportare violazioni rilevanti ai sensi del D.lgs. 231/2001. Qualora risultassero lacune, l'OdV le comunicherà agli organismi di vertice dell'ente suggerendo il da farsi, affinché questi, avvalendosi delle proprie facoltà decisorie – di cui l'OdV è necessariamente sprovvisto - adeguino il Modello Organizzativo e/o le procedure rilevanti nel caso concreto. Infine, l'Organismo di Vigilanza curerà che, tramite adeguata informazione e formazione, le modifiche del Modello Organizzativo siano rese note ai componenti della struttura aziendale dell'ente.

2. Le indicazioni dottrinali, giurisprudenziali e le Linee Guida in tema di Modello Organizzativo e flussi informativi

2.1

Partendo dalle indicazioni generali del Legislatore, l'interpretazione giurisprudenziale divenuta oramai maggioritaria afferma che l'organizzazione aziendale dell'ente deve riconoscere all'Organismo di Vigilanza autonomi poteri di controllo e di iniziativa, affinché possa svolgere la propria attività adeguatamente (Corte d'Assise d'Appello Torino, 27/05/2013). Partendo da tale presupposto, è stato affermato che "*l'iniziativa e, principalmente, il controllo*, [da parte dell'Organismo di Vigilanza] *possono essere ritenuti effettivi e non meramente "cartolari", soltanto ove risulti la non subordinazione del controllante al controllato: non a caso, l'art. 6, comma 2, lett. d), prevede una serie di obblighi di informazione nei confronti dell'organo di vigilanza, al fine evidente di consentire l'esercizio "autonomo" del potere (di vigilanza, appunto)*" (Cassazione penale, sez. II, 27/09/2016, n. 52316).

Non è sufficiente la mera e generica previsione di flussi informativi in ingresso nei confronti dell'Organismo di Vigilanza, dovendo essere anche prevista "*l'introduzione nel modello organizzativo di specifiche norme che stabilivano flussi informativi verso l'organismo*" (GUP Milano, 17/11/2009, in Foro padano 2010, 2, I, 360).

Non basta, quindi, la mera e generica previsione di canali dei flussi informativi, ma, sempre sulla scorta del principio di effettività che deve interessare in ogni ambito l'applicazione del Modello Organizzativo, quest'ultimo deve precisare le modalità di comunicazione ed invio dei flussi e disporre che a tali modalità i dipendenti, i direttori e gli amministratori si conformino nell'adempiere ai propri obblighi informativi verso l'OdV (Tribunale di Milano, Ordinanza del 9 novembre 2004).

Tale interpretazione giurisprudenziale trova eco all'interno della dottrina, la quale afferma che "*l'effettività dei flussi informativi dipende dalla chiara individuazione del canale di comunicazione, cioè dall'esistenza di un responsabile del processo a rischio-reato, che funga da interfaccia informativo dell'OdV*" (C. Piergallini, "*Paradig-*

matica dell'autocontrollo penale - dalla funzione alla struttura del "modello organizzativo" ex d.lg. n. 231/2001", in Cass. pen., fasc.1, 2013, pag. 0376B).

2.2

Come abbiamo visto, l'interpretazione giurisprudenziale si limita a richiedere e a constatare che i flussi informativi, così come il Modello Organizzativo, siano attuati, efficaci e delineati con precisione, lasciando tuttavia all'interprete l'onere di individuare le modalità più efficaci per l'attuazione del Modello avendo a riferimento l'attività imprenditoriale svolta dall'ente e i caratteri principali dell'ente stesso.

Sotto tale profilo, risultano essere d'aiuto le linee guida per l'organizzazione del modello pubblicate dalle varie associazioni di categoria, tra le quali ricordiamo quelle di Confindustria.

Le linee guida di Confindustria, oggetto di periodico aggiornamento, innanzitutto sottolineano l'importanza della previsione da parte del Modello Organizzativo di adeguati flussi informativi, necessari al funzionamento dell'Organismo di Vigilanza. Sotto tale profilo, viene suggerito che l'organizzazione e la gestione dei canali attraverso i quali l'Organismo di Vigilanza riceve informazioni sia lasciata all'OdV stesso, andando così a rafforzare l'autonomia di tale organo.

Inoltre, le Linee Guida di Confindustria, in ossequio a quanto sostenuto dalla giurisprudenza, sottolineano altresì che il modo corretto della gestione delle informazioni che riguardano l'applicazione del Modello Organizzativo avvenga in modo bidirezionale, e, cioè, sia in entrata che in uscita.

Dal lato delle informazioni in entrata, le Linee Guida, partendo dalla lettera della norma, richiamano l'importanza della previsione di un obbligo, in capo a ciascuno dei responsabili delle varie funzioni, di veicolare all'OdV gli eventuali scostamenti comportamentali che dovessero verificarsi attraverso i canali informativi previsti (es. report periodici e report *ad hoc*). Inoltre, viene chiarito che "*le informazioni fornite all'Organismo di Vigilanza mirano a consentirgli di migliorare le proprie attività di pianificazione dei controlli e non, invece, ad imporgli attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati. In altre parole, all'OdV non incombe un obbligo di agire ogni qualvolta vi sia una segnalazione, essendo rimesso alla sua discrezionalità (e responsabilità) di stabilire in quali casi attivarsi*".

Partendo da tale presupposto, le Linee Guida di Confindustria introducono una distinzione di target per quanto riguarda le informazioni promananti dall'Organismo di Vigilanza.

Da un lato, è compito dell'Organismo di Vigilanza comunicare ai soggetti che operano all'interno dell'organizzazione aziendale sicuramente "*il codice etico, ma anche gli altri strumenti attraverso i quali il Modello Organizzato trova la propria applicazione, quali i poteri autorizzativi, le linee di dipendenza gerarchica, le procedure, i flussi di informazione e tutto quanto contribuisca a dare trasparenza nell'operare quotidiano. In tale ambito, la comunicazione deve essere: capillare, efficace, autorevole (cioè*

emessa da un livello adeguato), chiara e dettagliata, periodicamente ripetuta. Inoltre, risulterà utile consentire l'accesso e la consultazione della documentazione costituente il Modello anche attraverso l'intranet aziendale".

Dall'altro, anche le Linee Guida sottolineano l'importanza centrale dei flussi informativi che dall'OdV si dipanano verso "*l'organo dirigente, ai fini degli opportuni provvedimenti, di quelle violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo all'ente*".

3. I modi e i tempi dei flussi informativi

Per le motivazioni di cui sopra, le prescrizioni del Modello Organizzativo in tema di flussi informativi devono essere puntali e, di conseguenza, devono senza dubbio fornire dettagli per quanto riguarda le modalità, le tempistiche e i mezzi con cui i soggetti deputati devono porre in essere le comunicazioni nei confronti dell'OdV.

Nell'individuazione di ciò, da un lato vi è la necessità di rendere possibile per l'OdV capire la provenienza delle informazioni inerenti al Modello Organizzativo, al fine di constatarne la veridicità, l'attendibilità e, se ne fosse il caso, per integrarne i contenuti. In questo caso, dunque, risulta evidente come i flussi informativi debbano seguire modalità completamente tracciabili.

Dall'altro lato, invece, vi è la necessità di tutelare i soggetti che, magari senza rivestire posizioni di controllo sulla gestione del rischio, individuano delle violazioni del Codice Etico o delle disposizioni del Modello Organizzativo e decidono di intervenire denunciandole. Si tratta dei casi dei cc.dd. *whistleblower*.

Il Legislatore, rendendosi conto dell'importanza di tali segnalazioni, con la L. 179/2017, ha introdotto delle tutele, obbligando gli enti di dotarsi di canali informatici alternativi a quelli principali per gestire i flussi informativi dei *whistleblower*, in grado di garantire "*la riservatezza dell'identità del segnalante*" e che prevedano il divieto di ogni misura ritorsiva e/o discriminatoria nei confronti dei *whistleblower* e la conseguente nullità di tali atti. Sotto questo profilo, una recente sentenza del giudice di legittimità, avente ad oggetto il *whistleblowing* effettuato da parte di dipendente pubblico, afferma che l'anonimato del quale il *whistleblower* può avvantaggiarsi si traduce nel riserbo sulle generalità del soggetto che pone in essere la segnalazione. Tale riserbo opera unicamente in ambito disciplinare, essendo peraltro subordinato al fatto che la contestazione sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione. Di conseguenza, ove la contestazione si basi, in tutto o in parte, sulla segnalazione stessa, l'identità può essere rivelata ove la sua conoscenza sia assolutamente indispensabile per la difesa dell'incolpato. Allo stesso modo, qualora l'illecito segnalato diventi oggetto di giudizio penale, in questa sede la riservatezza sull'identità del *whistleblower* non può in nessun caso risultare d'ostacolo al diritto di difesa dell'imputato, il quale deve essere messo nella posizione di difendersi

rispetto a tutte le prove usate nel giudizio a suo carico (Cassazione penale, sez. VI, 31/01/2018, n. 9041).

Il Modello Organizzativo dovrà tenere conto di tali indicazioni e uniformarsi ad esse, cercando soluzioni operative in grado sia di mantenere traccia dei flussi informativi, sia, in determinati casi, in grado di preservare la provenienza di queste informazioni, senza tuttavia arrivare a giustificare l'utilizzo di segnalazioni anonime.

3.1

Per quanto riguarda le tempistiche con cui le informazioni devono essere veicolate nei confronti dell'OdV, le *best practices*, tra cui le Linee Guida di Confindustria, distinguono tra flussi informativi periodici e flussi informativi relativi a fattispecie peculiari, indicative di specifici rischi in essere.

I primi dipendono dalle dimensioni dell'ente e dal settore in cui esso opera. Tuttavia, risulta agevole individuare la natura e la provenienza di tali flussi nelle informazioni che dovranno essere condivise verso l'Organismo di Vigilanza dalle funzioni che operano in aree a rischio reato (ad esempio: responsabile HR, CFO, responsabile IT). Tali flussi informativi periodici dovranno avere ad oggetto l'attività a rischio di commissione reato e i relativi presidi posti in essere, oltre agli eventuali indici di discostamento dalle previsioni del Modello Organizzativo e del Codice Etico.

Anche i flussi che devono essere posti in essere *ad hoc* al verificarsi di determinati requisiti non possono essere identificati in via astratta, dipendendo la loro qualificazione da molti fattori, tra cui l'attività aziendale svolta dall'ente e la relativa organizzazione aziendale.

A livello meramente indicativo, tali flussi possono essere riassunti in:

1. notizie provenienti dalla struttura riguardo eventuali procedimenti posti in essere dalla Magistratura in relazione a reati previsti dal Decreto e risultanze di indagini interne dalle quali sono emerse infrazioni del Modello;
2. procedimenti disciplinari a carico di dipendenti per infrazioni del Modello o del Codice Etico e in informazioni di ogni provenienza, concernenti possibili commissioni di reati o comunque violazioni del Modello.

Appartengono all'ultima fattispecie i flussi informativi che possono pervenire all'Organismo di Vigilanza tramite i canali informativi deputati al *whisl-teblowing*, a cui abbiamo accennato supra.

A mero fine esplicativo di quanto sopra, si andranno ad elencare nella sottostante tabella esempi di flussi informativi specifici, periodici e *ad hoc*, di alcune delle deleghe presenti nella maggior parte dei casi all'interno dell'organizzazione aziendale degli enti.

SOGGETTO PROMANANTE IL FLUSSO INFORMATIVO	FLUSSI INFORMATIVI PERIODICI	FLUSSI INFORMATIVI AD HOC
Responsabili della sicurezza sui luoghi di lavoro	piano di formazione, modifiche ed aggiornamento del DVR, budget degli investimenti in materia di sicurezza sul lavoro	infortuni occorsi; esiti di ispezioni e/o visite ispettive
Responsabile della gestione ambientale	report sugli adempimenti di monitoraggio e di controllo ambientale	violazioni delle procedure in uso; risultanze di visite ispettive
Responsabile IT	Report sull'applicazione, e eventuali variazioni, dei sistemi finalizzati ad evitare il compimento di illeciti informatici (utilizzo di credenziali di registrazione, software utilizzati)	Violazione delle procedure in uso
Responsabile HR	Report sulla formazione del personale dell'ente in materia di Modello Organizzativo e Codice Etico; report sullle sanzioni applicate in tema di Modello Organizzativo	Violazione delle procedure in uso

3.2

Alla raccolta di informazioni posta in essere da parte dell'OdV fa seguito un'attività di elaborazione di un'informativa destinata al management deputato a prendere le conseguenti decisioni operative e ai soggetti deputati a controllo di secondo grado sull'attività dell'ente. Anche tali flussi, a livello generale, possono essere divisi tra periodici e *ad hoc*.

Per quanto riguarda quelli periodici, l'*exposure draft* 2 del 25 novembre 2008 elaborato da AIIA in tema di "*Approccio integrato al sistema di controllo interno ai fini di un efficace ed efficiente governo d'impresa*" suggerisce che un flusso informativo dovrebbe essere messo in atto con periodicità almeno semestrale dal Comitato di Controllo Interno e dal Collegio Sindacale nei confronti dell'Organismo di Vigilanza su fatti di interesse di quest'ultimo, e dunque utili per valutare l'efficacia del Modello e, a sua volta, l'OdV dovrebbe informare periodicamente gli stessi Organi (nonché il Consiglio di Amministrazione nel suo complesso) con riferimento al funzionamento complessivo del Modello, all'aggiornamento delle aree di rischio, ai fatti di rilievo emersi dall'attività di controllo.

Con riguardo all'accadimento di specifici casi di violazioni, "*il flusso informativo proveniente dall'Organismo di Vigilanza può dover essere diversificato a seconda del soggetto che ha commesso la violazione; un'analisi compiuta da chi scrive sulle società dello S&P MIB ha evidenziato che, con riferimento alle violazioni commesse dai soggetti*

in posizione apicale, a carico dell'Organismo è spesso previsto un obbligo di comunicazione al Consiglio di Amministrazione e al Collegio Sindacale, ovvero al Comitato per il Controllo Interno; per le violazioni commesse dai membri del Consiglio di Amministrazione devono essere informati nella maggioranza dei casi il Consiglio stesso e il Collegio Sindacale, oppure il Comitato per il Controllo Interno; infine, per violazioni che coinvolgono il Collegio Sindacale, l'Organismo provvede in genere ad una vasta informativa, coinvolgendo tutti gli organi sociali" (G. Gargnani, "*La rilevanza dei flussi informativi nei modelli organizzativi ai sensi del d.lgs. n. 231/2001*" Riv. dottori comm., fasc.2, 2009, pag. 319).

4. Rapporti con altri organi di controllo nell'ottica di un sistema integrato

4.1

Nell'ambito di un ente, l'attività di controllo dell'OdV ha come oggetto soltanto l'applicazione del Modello Organizzativo, mentre altri organismi avranno la responsabilità di altre tipologie di controllo, ad esempio dell'attività gestionale o della correttezza della contabilità dell'ente.

Di conseguenza, risulta necessario che il Modello Organizzativo regoli con specifica cura i flussi di informazioni che partono da tali altri organi controllori nei confronti dell'OdV, andando così di fatto ad aumentare la capacità di controllo di tale organo. Anche il Regolamento ISVAP sulla gestione dei controlli interni delle imprese di assicurazione (Regolamento n. 20 del 26 marzo 2008) sottolinea l'importanza della condivisone delle informazioni tra gli organi di controllo, affermando che "*l'organo di controllo, la società di revisione, la funzione di revisione interna, di risk management e di compliance, l'organismo di vigilanza di cui al decreto legislativo 8 giugno 2001, n. 231, l'attuario incaricato e ogni altro organo o funzione cui è attribuita una specifica funzione di controllo collaborano tra di loro, scambiandosi ogni informazione utile per l'espletamento dei rispettivi compiti*".

4.2

I principali organi con funzione di controllo, che solitamente operano all'interno dell'organigramma di ogni ente, sono:

1. *Collegio Sindacale*. L'attività del Collegio Sindacale risulta essere ormai sempre meno imperniata sulle verifiche contabili e sempre più focalizzata su quelle inerenti la legittimità e la correttezza dell'operato degli amministratori. L'art. 2403 c.c., 1° comma, c.c. recita: "*il collegio sindacale vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento*". Partendo da tale presupposto, risulterà quindi essenziale la condivisione delle informazioni raccolte dal Collegio Sindacale con l'Organismo di Vigilanza. Ugualmente importante per il corretto esple-

tamento delle attività di controllo sarà prevedere che l'OdV comunichi, in una relazione periodica, le attività di verifica che ha effettuato nel periodo di riferimento, al fine di mettere il Collegio Sindacale nella condizione di porre in essere la propria attività di controllo.

2. *Revisore legale (o società di revisione).* Ai sensi dell'art. 2409-bis c.c., "*la revisione legale dei conti sulla società è esercitata da un revisore legale dei conti o da una società di revisione legale iscritti nell'apposito registro*". Stante la richiesta di legge sull'autonomia e indipendenza del revisore legale, risulta essere opportuno introdurre controlli ad hoc sull'operato del revisore, soprattutto in termini di mantenimento di quell'indipendenza senza la quale la certificazione rischia di risultare un mero timbro formale sui documenti predisposti dall'ente. Sotto tale profilo, i protocolli aziendali dovrebbero prevedere almeno una riunione tra la società di revisione e l'Organismo di Vigilanza – e quella degli altri organi di controllo come il collegio sindacale e il comitato per il controllo interno, prima della seduta del consiglio di amministrazione indetta per l'approvazione del bilancio.

3. *Comitato Audit*. È una struttura esterna che coadiuva il CdA nel definire il sistema di controllo interno e i protocolli aziendali, identificando e quantificando i rischi d'impresa, al fine di evitare che influenzino negativamente la corretta gestione aziendale.

4. *Comitato per il controllo interno*. Tale organo definisce le linee di indirizzo del sistema di controllo interno, in modo che i principali rischi afferenti all'emittente e alle sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati. È compito del Comitato di controllo interno individuare i criteri di compatibilità tra tali rischi e una corretta gestione d'impresa.

Sarà sempre compito dell'interprete, a seguito di una adeguata mappatura della struttura imprenditoriale dell'ente e dei rischi esistenti, prevedere all'interno del Modello Organizzativo i giusti adempimenti informativi sui giusti soggetti, raggiungendo la migliore circolazione possibile di informazioni, al fine di ottimizzarla al meglio.

5. La realizzazione del documento contenente i flussi informativi verso l'OdV

Considerata la difficoltà che spesso l'Organismo di Vigilanza incontra nell'ottenere le adeguate informazioni sull'applicazione delle disposizioni contenute nel Modello Organizzativo, è giusto che esso si interroghi per capire quali siano le modalità migliori per mezzo delle quali la veicolazione dei flussi informativi possa risultare adeguata.

Le due principali e possibili modalità attraverso le quali le informazioni possono essere veicolate all'OdV sono:

i) tramite l'invio di documentazione scritta secondo i canali individuati dal Modello Organizzativo, o

ii) oralmente, durante riunioni *ad hoc* con i componenti dell'Organismo di Vigilanza. In questo caso è bene verbalizzare attentamente le informazioni assunte al fine di tenerne traccia precisa.

Al contrario, risulta essere più complessa e difficoltosa la comunicazione dei flussi informativi tramite l'utilizzo di documentazione scritta, in quanto l'assenza di un confronto diretto col soggetto da cui proviene il flusso informativo potrebbe facilmente comportare l'invio di informazioni non attinenti o non sufficienti a determinare la situazione di applicazione del Modello Organizzativo da parte dell'ente o, ancora peggio, al mancato invio delle informazioni in questione.

Per limitare i problemi, l'Organismo di Vigilanza può ricorrere alla stesura di *format* prestampati per sollecitare i soggetti tenuti a fornire le comunicazioni a dare le informazioni in maniera precisa, completa e attinente. Potrebbe essere persino proposto il ricorso a modelli che abbiano al proprio interno un doppio contenuto. Da un lato, una serie di informazioni di tipo generale inerenti l'applicazione del Modello Organizzativo, le quali risultano essere applicabili per tutte le figure preposte alle diverse aree di criticità (ad es: provvedimenti e/o notizie riguardanti l'avvio di procedimenti nei confronti dell'ente da parte di organi di polizia giudiziaria o di qualsiasi altra autorità; cambiamenti e/o modifiche dell'assetto organizzativo, compreso il sistema di deleghe; *report* sulla gestione dei rapporti con la pubblica amministrazione, etc.). Dall'altro, la richiesta di informazioni specifiche per ogni diversa figura preposta al controllo di un'area critica dell'organizzazione imprenditoriale dell'ente. Ad esempio, ai Responsabili della sicurezza sui luoghi di lavoro dovrà essere richiesto un *report* contente il piano di formazione, le modifiche e l'aggiornamento del DVR, il *budget* degli investimenti in materia di sicurezza sul lavoro, etc.

Le modalità di veicolazione delle informazioni verso l'OdV dovranno essere combinate in modo da massimizzarne l'effettività. Per esempio, l'Organismo di Vigilanza, potrà fissare incontri *vis-a-vis* con le figure preposte al controllo dopo aver ricevuto i documenti con le informazioni richieste al fine di integrarle o di approfondirne alcuni aspetti.

6. Coordinamento degli obblighi in materia di flussi informativi con il sistema sanzionatorio

In generale, l'art. 6, comma 2, lett. e) D.lgs. 231/2001 richiede l'introduzione di un sistema disciplinare volto a sanzionare la violazione delle procedure, delle regole e dei protocolli previsti dal Modello Organizzativo, le quali devono essere considerate, a tutti gli effetti, disposizioni impartite dal datore di lavoro ai sensi dell'art. 2104 c.c.

Partendo da tale presupposto, deve altresì considerarsi violazione rilevante sul piano disciplinare anche l'inottemperanza agli obblighi informativi verso l'Organismo di Vigilanza secondo i tempi e le modalità stabilite, nonché l'omessa trasmissione o invio di documentazione, dati o informazioni non veritiere.

L'invio dei flussi periodici da parte delle funzioni interessate rappresenta un preciso dovere, rilevante ai fini del corretto funzionamento del Modello, in quanto anche l'obbligo di informare il datore di lavoro di eventuali comportamenti contrari al Modello organizzativo rientra nel più ampio dovere di diligenza e obbligo di fedeltà del prestatore di lavoro di cui agli articoli 2104 e 2105 c.c

Considerando che l'obbligo di informazione assolve anche alla funzione di conferire maggiore autorevolezza alle richieste di documentazione che si rendono necessarie all'Organismo di vigilanza nel corso delle sue verifiche, la previsione nell'ambito del Modello Organizzativo di sanzioni, nel caso di inottemperanze ripetute a tale incombenza, non appare, dunque, affatto inopportuna.

CAPITOLO 5 di Josephine Romano e Pietro Orzalesi

Multinazionali italiane: 231 e sistemi di compliance

Multinazionali italiane: 231 e sistemi di compliance – Implementazione di modelli organizzativi e/o di compliance nelle controllate italiane ed estere di gruppi multinazionali

sommario: 1. Premessa – 2. Fonti e interpretazioni – 3. Elementi di riflessione – 4. Benchmark

1. Premessa

È necessario/opportuno che i Gruppi multinazionali italiani che operano anche all'estero e ivi hanno società controllate dotino queste ultime di Modelli di Organizzazione, Gestione e Controllo e procedano alla nomina di Organismi di Vigilanza ai sensi del Decreto Legislativo n. 231/2001?

2. Fonti e interpretazioni

Decreto Legislativo 231/2001

- art. 4: responsabilità dell'ente per i reati commessi all'estero;
- artt. 6 e 7: adozione Modello organizzativo e nomina Organismo di Vigilanza.

Best practice - Linee Guida di Confindustria

Ciascuna società del Gruppo, in quanto entità singolarmente destinataria delle previsioni contenute nel D.Lgs. 231/2001, deve:

- adottare un proprio modello organizzativo;
- nominare un proprio Organismo di Vigilanza;
- prevedere che gli Organismi di Vigilanza delle varie società del Gruppo sviluppino adeguati flussi informativi fra di loro.

Per quanto riguarda la responsabilità 231 nei Gruppi trasnazionali (cap. V, par. 4), la presenza di profili di rischio elevati e il diverso contesto normativo suggeriscono di adeguare il Codice di Comportamento, la formazione e i pro-

tocolli operativi, anche attraverso l'adozione di compliance programs fondati su principi di controllo minimi.

Giurisprudenza (Cassazione Penale, Sez. IV, 18 gennaio 2011, n. 24583)

Risalita della responsabilità verso la capogruppo quando ricorrono congiuntamente le seguenti condizioni:

- commesso un reato presupposto richiamato dal D.Lgs. 231/2001;
- reato posto in essere da una persona fisica che abbia con la capogruppo rapporti di tipo organizzativo/funzionale;
- reato commesso nell'interesse o vantaggio della holding.

3. Elementi di riflessione

Econimicità

Costi/benefici per l'implementazione e il costante aggiornamento/manutenzione del Modello organizzativo e per il compenso dell'Organismo di Vigilanza

Rischio di «auto-soggezione» al D.Lgs. 231/2001

Autodichiarazione di soggezione all'apparato sanzionatorio dettato dal D.Lgs. 231/2001

Diversi contesti normativi

Differenti discipline normative nei diversi Paesi esteri:

- necessità/opportunità di recepire anche le specificità locali
- validità quale esimente

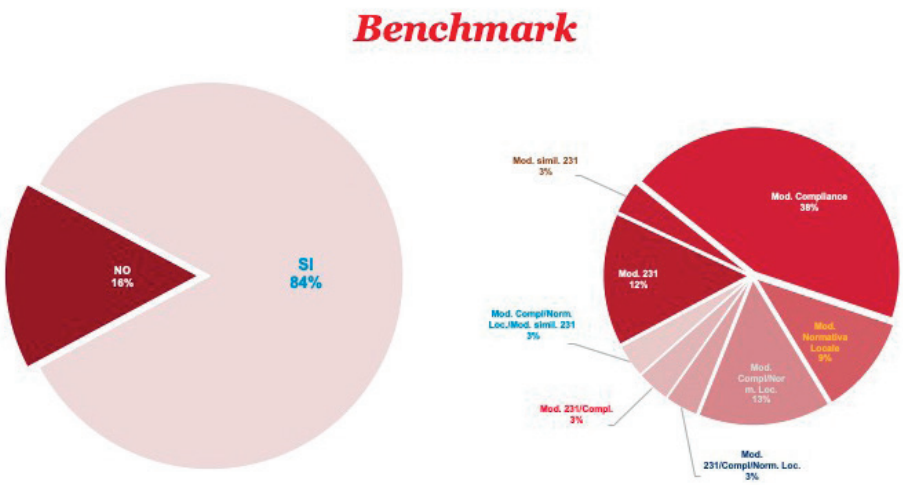
Flussi

Canali informativi tra i diversi Organismi di Vigilanza delle società del Gruppo, anche in funzione di prevenzione della risalita della responsabilità verso la capogruppo

4. Benchmark

Il grafico seguente riporta le scelte effettuate da un campione di 32 gruppi societari multinazionali con holding/sub-holding italiana rappresentativi di differenti settori di business in relazione alla gestione dei modelli di compliance delle società operanti all'estero:

- **Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01** (12%);
- **Modello di Organizzazione, Gestione e Controllo ispirato a quanto previsto dal D.Lgs. 231/2001**, in termini di ambiti/aree a rischio, principi di controllo a presidio (3%);
- **Modello di Compliance**, da intendersi come l'insieme di policy, procedure ed altri strumenti normativi definiti a livello di Gruppo a regolamentazione di determinati ambiti (ad esempio, anticorruzione, SSL, antitrust, privacy) (38%);
- **Modello ispirato a specifiche normative locali**, in tema di responsabilità amministrativa degli enti, vigenti all'interno del Paese in cui la Società opera (9%).



CAPITOLO 6 di Antonio Bana, Francesca Chiara Bevilacqua e Gian Luigi Gatta

Verso un sistema di monitoraggio nella sinergia dei presidi antocorruttivi

Verso un sistema di monitoraggio nella sinergia dei presidi anticorruttivi del D. Lgs. 231/01 e l'avvento dell'ISO 37001

sommario: 1. Premessa – 2. La definizione giurisprudenziale di certificazione di qualità nell'ordinamento italiano e gli effetti della sua adozione – 3. Linee guida e best pratice internazionali sui compliance program anticorruzione – 4. L'importanza delle diverse fasi di audit – 5. Conclusioni: i vantaggi potenziali ed effettivi derivanti dalla certificazione

1. Premessa

È corretto dotare la nostra impresa di un'organizzazione certificata per la prevenzione del rischio di corruzione?

Questo quesito è stato posto inizialmente durante il secondo Corporate Compliance Round Tables 2017 organizzato da ASLA e in particolare nel tavolo di lavoro coordinato sul tema specifico dei presidi corruttivi e dell'avvento dell'ISO 37001.

Dal punto di vista aziendale, infatti, la problematica sottesa alla corruzione rientra a pieno titolo nel tema di governance.

Risulta quanto mai opportuno definire i diversi ruoli di responsabilità di regole e dei differenti sistemi di controllo finalizzati a ridurre il rischio correlato ad eventuali fatti corruttivi.

I reati corruttivi possono determinare enormi danni sotto differenti profili, come l'esclusione di diritto e di fatto per una società dai mercati o dalla possibilità di contrarre con la Pubblica Amministrazione.

Un aspetto non trascurabile è il danno reputazionale che ha senza dubbio una notevole incidenza.

La Compliance Policy aziendale dovrà essere supportata in questo modo nel suo percorso di attuazione da idonee strutture di consulenza in grado di sostenere un lavoro effettivo per l'Ente.

Sarà necessario focalizzare una serie di attività e tra queste alcune sono di vitale importanza come:

- Contrastare la corruzione in tutte le sue forme, rendendo consapevoli e mobilitando tutte le forze vive della società.

- Analizzare e studiare i fenomeni di corruzione, le loro cause e i loro effetti, al fine di elaborare risoluzioni e strumenti che ne possano eliminare o ridurre l'incidenza. –

- Sensibilizzare l'opinione pubblica sul tema della lotta alla corruzione per mezzo di incontri, riflessioni, dibattiti e di ogni altra forma di comunicazione e di espressione consentita dalla legge.

- Promuovere nelle scuole e negli istituti universitari la sensibilizzazione alle tematiche legate alla corruzione, mediante anche la formazione e l'aggiornamento del personale scolastico, al fine di rendere ciascuno, e i giovani in particolare, consapevole dei valori fondamentali del vivere civile.

- Promuovere l'approvazione a livello nazionale di quegli strumenti giuridici ed economici che siano internazionalmente riconosciuti come efficaci nel contrasto alla corruzione.

- Incoraggiare gli operatori economici pubblici e privati a formulare e ad applicare principi etici condivisi.

2. La definizione giurisprudenziale di certificazione di qualità nell'ordinamento italiano e gli effetti della sua adozione

La certificazione di qualità è una procedura con la quale un soggetto verificatore esterno all'impresa, terzo e indipendente, che sia a ciò autorizzato (cosiddetto organismo di certificazione), fornisce attestazione scritta che un prodotto, processo produttivo o servizio, a seguito di valutazione, sia conforme ai requisiti specificati da norme tecniche, garantendone la validità nel tempo attraverso un'adeguata attività di sorveglianza (cosiddetta *auditing* di impresa). Per i sistemi di gestione, fino al dicembre 2003, la normativa europea di riferimento (cosiddetta UNI EN ISO 9001) si deve applicare ad ogni modello di assicurazione della qualità nella progettazione, sviluppo, fabbricazione, installazione e assistenza.

La garanzia della validità nel tempo della qualità certificata dipende ovviamente dalla validità della certificazione, a sua volta subordinata alla vigenza temporale di essa. La scadenza della certificazione, infatti, indica che l'organismo di certificazione non può garantire oltre un certo limite temporale la conformità ai requisiti qualitativi di un certo prodotto, processo o servizio, senza sottoporlo a nuova verificazione. Per tale ragione un certificato di qualità scaduto è da considerarsi *tamquam non esset*, atteso che esso non può assolvere alla funzione

di garanzia, per la quale è previsto, oltre il termine di validità indicato nell'attestazione scritta.

L'approccio operativo, la flessibilità di utenza, la compatibilità del Modello, la sua applicabilità multigiurisdizionale ne fanno uno strumento agile ed al contempo potenzialmente efficace che presenta risonanze importanti con modelli esistenti.

Così come con gli altri *standard* emessi dall'ISO, la 37001 include una disposizione che consente la certificazione da parte di una terza parte indipendente, che indica che il programma di lotta alla corruzione attuato dall'azienda è conforme allo *standard*. Poiché fornisce un approccio globalmente accettato per la conformità anti-corruzione, ISO37001 è stato annunciato come un passo significativo nella continua globalizzazione del rispetto contro la corruzione, in particolare nei paesi in cui la corruzione potrebbe essere considerata parte della cultura. Le aziende possono ora utilizzare uno strumento che alza sia «l'asticella» per le attività di conformità che la consapevolezza del rischio di corruzione.

Naturalmente, il fatto che il programma di lotta alla corruzione di una società abbia ricevuto una certificazione ISO non sarà sufficiente, da solo, a costituire un'adeguata difesa nei procedimenti giudiziari. Ma i pubblici ministeri, di solito, tengono in considerazione lo stato di attuazione e l'efficacia dei programmi di conformità di un'azienda, per determinare se la società debba essere anch'essa perseguita per crimini commessi da coloro che agiscono per suo conto.

Mentre i pubblici ministeri, ovviamente, resteranno liberi di procedere a discrezione nelle loro indagini, una società potrà comunque puntare a una certificazione ISO 37001 come prova che abbia fatto ogni sforzo per attuare un programma anticorruzione efficace.

3. Linee guida e best pratice internazionali sui compliance program anticorruzione

Vengono qui di seguito suggeriti alcuni possibili criteri generali per un efficace compliance program anticorruzione.

- ***Impegno dei vertici societari contro la corruzione, cd "Top-level commitment"***: i vertici della società devono esprimere in modo inequivocabile sia il ripudio di qualsiasi pratica corruttiva sia l'obbligo per tutti i dirigenti e dipendenti della società di rispettare i principi etici, i controlli e le misure di prevenzione previsti dal "compliance program".
- ***Principi etici, procedure e controlli che proibiscano la corruzione***: devono essere previsti principi etici, procedure e controlli specificatamente congegnati per prevenire pratiche corruttive. Queste procedure e controlli devono essere effettivamente attuati e applicati e il loro rispetto deve essere obbligatorio per tutti i livelli aziendali.

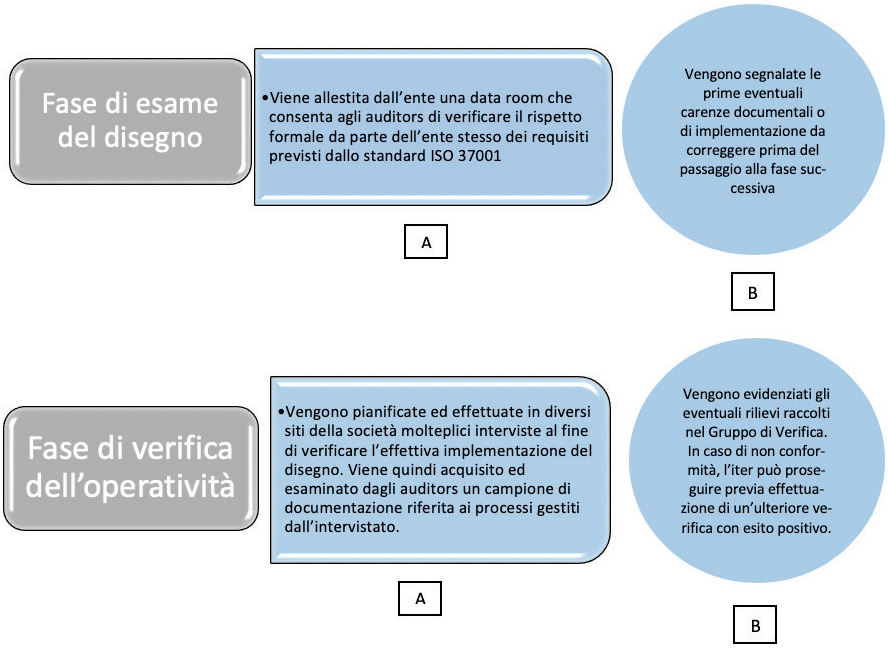
- *Attività di risk assessment anti-corruzione*: una specifica attività di analisi che individui le aree di attività esposte al rischio di pratiche corruttive. Tale attività deve essere periodicamente ripetuta e il compliance program anti-corruzione deve essere aggiornato di conseguenza, tenendo conto, fra l'altro, anche della scoperta di eventuali violazioni e condotte illecite.
- *Affidamento a "Senior Officer" della responsabilità del compliance program anti-corruzione*: il controllo dell'applicazione e dell'osservanza del compliance program anti-corruzione deve essere affidato a dirigenti di alto livello del management della società che devono poter riportare direttamente ai vertici e agli organi di controllo e avere adeguata autorità, autonomia e disponibilità di risorse.

Questo in via semplificativa sono gli aspetti più importanti che sono emersi durante i lavori svolti in un confronto collaborativo.

4. L'importanza delle diverse fasi di audit

Riassumendo l'analisi delle fasi di lavoro si potrebbero evidenziare due differenti stage di lavoro:

- Fase di esame del disegno (A e B)
- Fase di verifica dell'operatività (A e B)

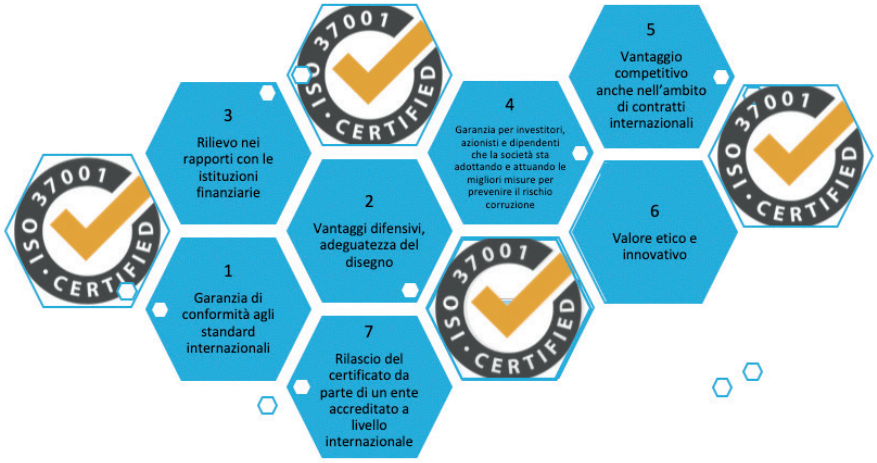


5. Conclusioni: i vantaggi potenziali ed effettivi derivanti dalla certificazione.

Il rilascio della certificazione ISO 37001 porterebbe ad ottenere degli indubbi vantaggi

Standard ISO 37100/2016 "Antibribery Management System"

I possibili vantaggi derivanti dalla certificazione



APPENDICE DI di Pietro Orzalesi

Analisi di benchmark

Analisi connessa all'adozione di «Modelli di Compliance» nei gruppi multinazionali – Presentazione dei risultati

sommario: 1. Premessa – 2. Metodologia di conduzione dell'analisi – 3. Il campione di riferimento – 4. Presentazione dei risultati – a. Adozione di «Modelli» – b. Ambito di riferimento dei «Modelli» – c. Valutazione di conformità dei «Modelli» rispetto alle normative locali vigenti – d. Monitoraggio dei «Modelli»

1 Premessa

L'obiettivo del presente documento è quello di illustrare una sintesi delle risultanze emerse a seguito delle attività di benchmark in merito all'adozione di "Modelli" in conformità a disposizione normative in materia di responsabilità amministrativa d'impresa (di seguito, in breve, il "Modello") da parte di Società operanti all'estero e appartenenti a gruppi multinazionali, la cui capogruppo ha sede legale in Italia (di seguito, in breve, Società controllate estere).

2 Metodologia di conduzione dell'analisi

Le analisi di benchmark sono state effettuate attraverso la raccolta di specifiche informazioni, reperite da:

- fonti non pubbliche mediante la somministrazione di un apposito questionario alle Società in ambito;
- fonti pubbliche (siti web e documenti istituzionali delle Società oggetto del campione, ad es. Relazione sul Governo societario e gli assetti proprietari, Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01).

I principali ambiti di informazione oggetto del benchmark hanno riguardato i seguenti aspetti:

- ***Adozione di «Modelli»***
- ***Ambito di riferimento dei «Modelli»***
- ***Valutazione di conformità dei «Modelli» rispetto alle normative locali vigenti***
- ***Monitoraggio dei «Modelli»***

3 Il campione di riferimento

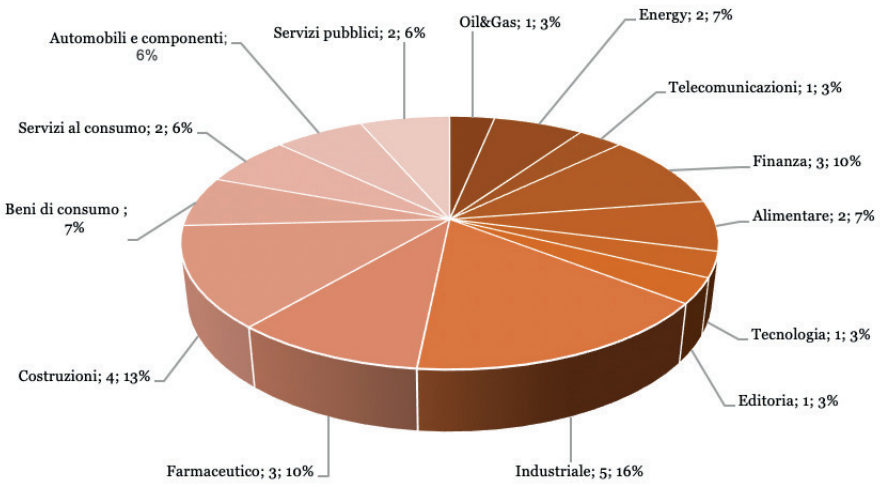
Le attività di benchmark sono state condotte su un universo di analisi composta da **45 Società** appartenenti a **gruppi societari multinazionali** con **holding/sub-holding italiana**.

Rispetto a tale universo di analisi e tenuto conto della disponibilità di informazioni acquisite attraverso fonti pubbliche e non, le analisi sono state effettuate su un campione finale costituito da **32 Società**.

Tale campione, inoltre, è caratterizzato da una selezione di:

- emittenti di titoli quotati su mercati regolamentati gestiti da Borsa Italiana, appartenenti all'indice FTSE-MIB;
- Società non quotate, ritenute rilevanti sia per dimensioni, sia per struttura organizzativa.

Settore di appartenenza (*) delle Società oggetto di analisi



(*) Il settore di appartenenza delle Società oggetto di analisi fa riferimento a quanto indicato sul sito di Borsa Italiana S.p.A.

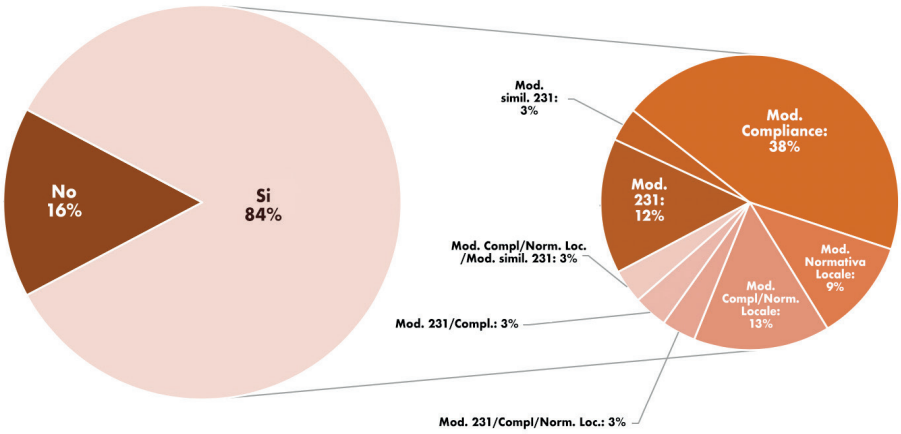
Nelle pagine seguenti si riportano le risultanze delle analisi condotte sul campione di riferimento.

4 Presentazione dei risultati

a. Adozione dei «Modelli»

Si riportano graficamente, i risultati delle scelte effettuate dalle Società controllate estere in merito all'adozione di differenti tipologie di "Modelli", nonché delle possibili combinazioni:

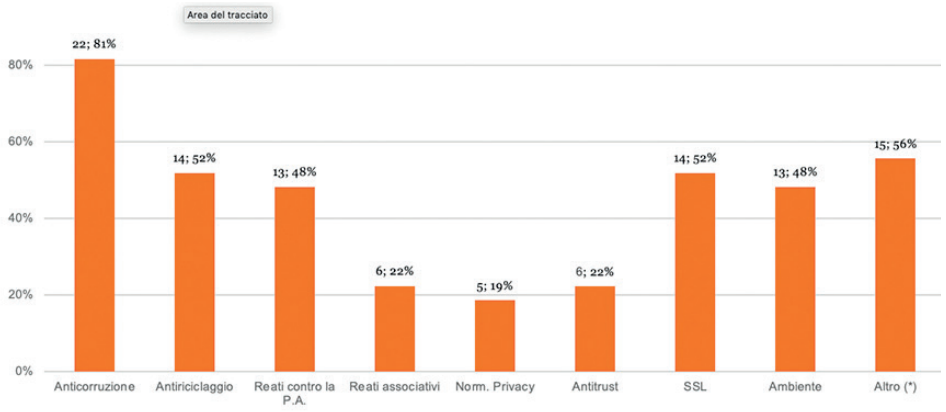
- **Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01** (di seguito, in breve, **Modello 231**);
- **Modello di Organizzazione, Gestione e Controllo ispirato a quanto previsto dal D.Lgs. 231** (di seguito, in breve, **Modello similare alla 231**), in termini di ambiti/aree a rischio, principi di controllo a presidio:
- **Modello di Compliance,** da intendersi come l'insieme di policy, procedure ed altri strumenti normativi definiti a livello di gruppo a regolamentazione di determinati ambiti (ad esempio, anticorruzione, SSL, antitrust, privacy);
- **Modello ispirato a specifiche normative locali,** in tema di responsabilità amministrativa degli Enti, (di seguito, in breve, **Modello Normativa Locale**) vigenti all'interno del Paese in cui la Società opera.



SI – Modello: n°27 (Astaldi, Atlanti/Autostrade, Barilla, Brembo, Chiesi Farmaceutici, CNH Industrial, Enel, ERG, Esprinet, FCA, Fendi srl, Finmeccanica, Generali, Italcementi, Mediaset, Moncler, Parmalat, RCS, Recordati, Saipem, Salini Impregilo, Unicredit, Telecom Italia, Unipol/Unipol Sai, Snam, Saras, Yoox Net-a-porter Group). NO - Modello: n°5 (Autogrill, Buzzi Unicem, Diasorin, Hitachi, Prysmian). ****** SI – Mod. 231: n°4 (Salini Impregilo, Unicredit, Generali, Saipem). SI – Mod. similare alla 231: n° 1 (Parmalat). SI – Mod. Compliance: n°12 (Barilla, CNH Industrial, Fendi, Finmeccanica, Italcementi, Moncler, Snam, Telecom Italia, Yoox, Astaldi, ERG, Unipol/Unipol Sai). SI – Mod. Normativa locale: n°3 (Esprinet, FCA, RCS). SI – Mod. Coml./Norm. Loc.: n° 4 (Atlantia/Autostrade, Chiesi farmaceutici, Recordati, Brembo). SI – Mod. 231 / Compl / Norm. Loc.: n°1 (Mediaset). SI – Mod. 231/ Compl. : n°1 (Saras). SI- Mod. Compl./Norm. Loc./simil. 231: n°1 (Enel).

b. Ambito di riferimento dei «Modelli»

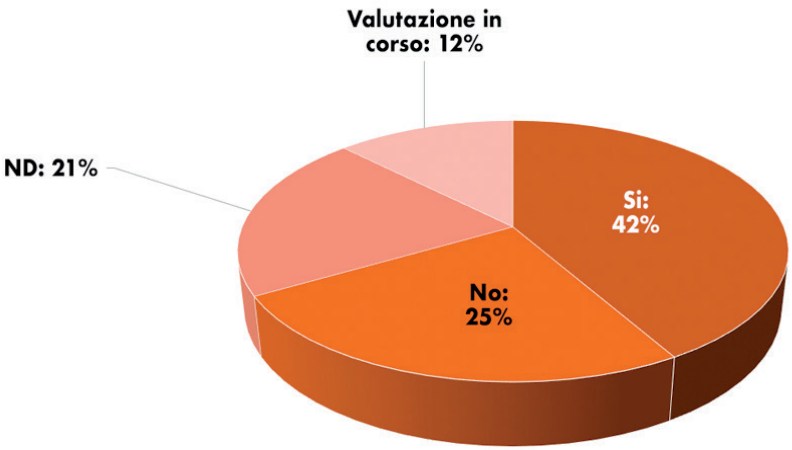
Si riportano graficamente i risultati emersi in merito agli ambiti di riferimento dei "Modelli" adottati dalle Società controllate estere.



(*) Comprende i reati societari, market abuse, reati di frode, traffico di organi, ecc.

c. Valutazione di conformità dei «Modelli» rispetto alle normative locali vigenti

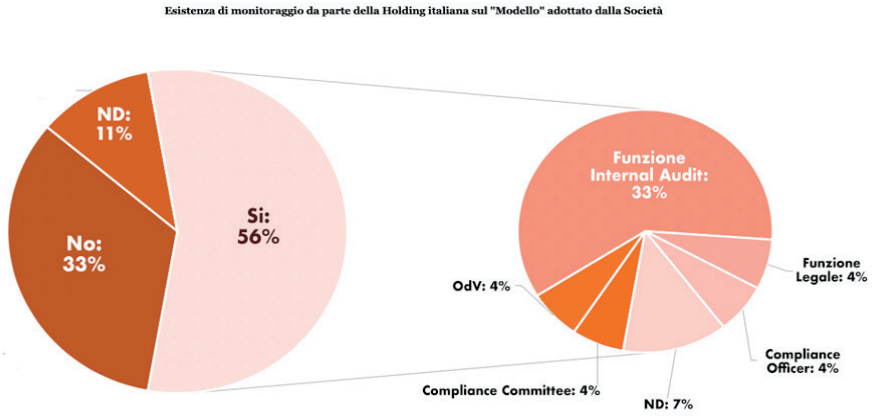
Si riporta graficamente una rappresentazione delle Società controllate estere che, avendo adottato Modelli 231 e/o Modelli similari alla 231 e/o Modelli di Compliance (24 Società), ne hanno valutato la conformità dei rispettivi principi rispetto a quanto previsto dalle normative locali nel Paese in cui operano.



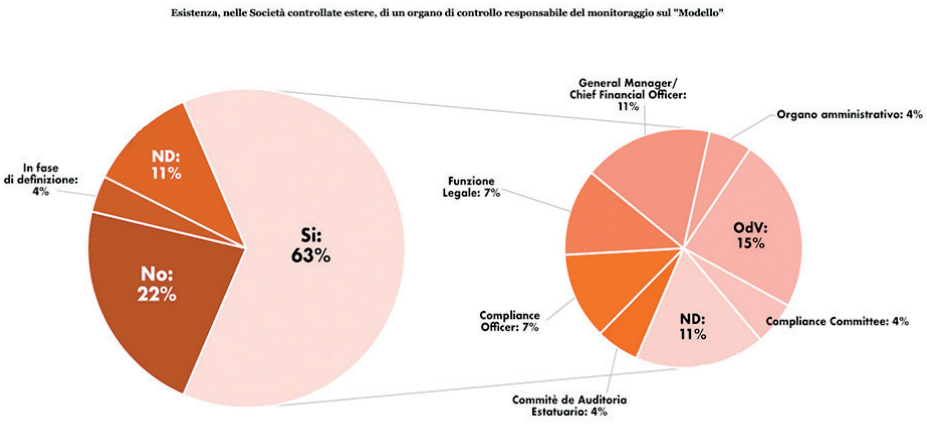
d. Monitoraggio dei «Modelli»

Si riportano, di seguito, le risultanze emerse in tema di monitoraggio sui "Modelli", a seconda che l'organo di controllo deputato faccia parte:

- della Holding



- della Società controllata estera.



SI – Monitoraggio holding: n° 15 (Atlantia/Autostrade, Barilla, Chiesi Farmaceutici, Enel, Esprinet, Italcementi, mediaset, RCS, Recordati, Saras, Snam, Telecom Italia, Brembo, Unicredit, Unipol/Unipol Sai). Compliance Committee: Chiesi OdV: Recordati Compliance Officer: Unipol/Unipol Sai Funzione Legale: Italcementi IA: (Atlantia, Barilla, Enel, Esprinet, Mediaset, Saras, Telecom, Unicredit, Brembo) ND, ovvero in fase di definizione: (RCS, Snam)

SI – Monitoraggio controllata: n° 17 (Brembo, Salini Impregilo, Unicredit, Unipol/Unipol Sai, Chiesi farmaceutici, CNH Industrial, Enel, Generali, Italcementi, Mediaset, RCS, Recordati, Saipem, Saras, ERG, Snam, Telecom Italia). Comitè de Auditoria Estatutario: (CAE-Tim Brasil) (Telecom) ND: (Mediaset, RCS, Snam) Compliance Committe: (Saipem) OdV: (Generali, Saras, Salini Impregilo, Unicredit) Organo amministrativo: (ERG) Compliance Officer: (Enel) GM/CFO: (Recordati, Chiesi, Brembo) Funzione Legale: (Itlacementi, CNH Industrial)

-

NOTE

NOTE

NOTE

NOTE

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

In particolare, hanno contribuito a questo Quaderno:

L'Avv. **Irene Picciano**, curatrice e co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato De Berti Jacchia (www.dejalex.it)

L'Avv. **Manuela Bianchi**, curatrice e co-autrice del Capitolo 4 di questo Quaderno, dello Studio Legale Associato CastaldiPartners (www.castaldimourre.com/it)

L'Avv. **Stefano Cancarini**, co-autore del Capitolo 2 di questo Quaderno, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

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

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

L'Avv. **Micaela Barbotti**, co-autrice del Capitolo 4 di questo Quaderno, dello Studio Legale Associato Albe e Associati (www.albeeassociati.it)

L'Avv. **Josephine Romano**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Deloitte Legal (www.deloitte.com/it)

L'Avv. **Pietro Orzalesi**, co-autore del Capitolo 5 e dell'Appendice di questo Quaderno, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

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

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

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

Il Prof. **Avv. Gian Luigi Gatta**, co-autore del Capitolo 6 di questo Quaderno, Ordinario di Diritto penale nell'Universita degli Studi di Milano (www.unimi.it)

L'Avv. **Eva Cruellas**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)

L'Avv. **Eugenia Gambarara**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)

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

L'Avv. **Deborah Bolco**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.paviaeansaldo.it)

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

Pubblicazione giuridica n° 13 di ASLA

A cura del Gruppo di lavoro sulla Corporate Compliance
Curatrici: Manuela Bianchi e Irene Picciano
Editor: Ezio Rotamartir

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

www.aslaitalia.it

In particolare, hanno contribuito a questo Quaderno:

L'Avv. **Irene Picciano**, curatrice e co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato De Berti Jacchia Franchini Forlani (www.dejalex.it)

L'Avv. **Manuela Bianchi**, curatrice e co-autrice del Capitolo 4 di questo Quaderno, dello Studio Legale Associato Castaldi & Partners (www.castaldimourre.com/it)

L'Avv. **Stefano Cancarini**, co-autore del Capitolo 2 di questo Quaderno, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

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

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

L'Avv. **Micaela Barbotti**, co-autrice del Capitolo 4 di questo Quaderno, dello Studio Legale Associato Albe e Associati (www.albeeassociati.it)

L'Avv. **Josephine Romano**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Deloitte Legal (www.deloitte.com/it)

L'Avv. **Pietro Orzalesi**, co-autore del Capitolo 5 e dell'Appendice di questo Quaderno, dello Studio Legale Associato PricewaterhouseCoopers Tax and Legal (www.pwc.com)

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

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

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

Il Prof. **Avv. Gian Luigi Gatta**, co-autore del Capitolo 6 di questo Quaderno, Ordinario di Diritto penale nell'Universita degli Studi di Milano (www.unimi.it)

L'Avv. **Eva Cruellas**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato Gianni, Origoni, Grippo, Cappelli & Partners (www.gop.it)

L'Avv. **Eugenia Gambarara**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato Hogan Lovells (www.hoganlovells.com)

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

L'Avv. **Deborah Bolco**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.paviaeansaldo.it)

L'Avv. **Mariangela Papadia**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.paviaeansaldo.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 le curatrici e i co-autori del Quaderno stesso, sopra specificati), ove è stata constituita nel 2003 come organizzazione apolitica senza scopo di lucro, operando in particolare nel settore del diritto d'impresa e con il fine di promuovere e diffondere la cultura e le modalità più attuali dell'esercizio della professione legale in forma associata, organizzata e certificabile.

ASLA
Associazione Studi Legali Associati