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

CORPORATE COMPLIANCE VIRTUAL ROUND TABLES 2020

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

ASLA
Associazione Studi Legali Associati

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

A CURA DI IRENE PICCIANO E ANTONIO BANA
CON TESTI DI ALESSANDRA ANSELMI, ANTONIO BANA, MICAELA BARBOTTI, FRANCESCA CHIARA BEVILACQUA, PIETRO BOCCACCINI, TIZIANA BONESCHI, EVA CRUELLAS SADA, SIMONA CUSTER, PAOLA DE PASCALIS, FEDERICA DENDENA, EUGENIA GAMBARARA, GIACOMO GORI, PIERO MAGRI, ANDREA MANTOVANI, MARTA MARGIOCCO, GIULIO NOVELLINI, MARIANGELA PAPADIA, IRENE PICCIANO, ALESSIA PLACCHI, EVA REGGIANI, JOSEPHINE ROMANO, ROBERTO TIRONE

CORPORATE COMPLIANCE VIRTUAL ROUND TABLES 2020

Atti delle sei tavole rotonde virtuali e la partecipazione di ventuno 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

Premessa

e-book Virtual Corporate Compliance

Anche quest'anno, nonostante questo periodo così difficile per tutti noi dove la pandemia ha interrotto i nostri rapporti di vicinanza, la nostra attività del Gruppo Corporate Compliance non si è fermata.

Insieme all'amica Irene Picciano, storica coordinatrice del Gruppo, abbiamo pensato di mantenere alto l'entusiasmo del gruppo, con costanti incontri diventati ormai un must e anche un'eccellenza importante per ASLA.

Abbiamo voluto immaginare – anche a distanza – di essere tutti presenti nella grande sala del Four Seasons che da anni ci ha sempre ospitato, creando ancora una volta quella magica atmosfera di convivialità e di scambio di informazioni che da sempre ha caratterizzato il nostro gruppo di lavoro.

Abbiamo creato in questo modo il primo Virtual Round Tables con questo e-book ricco di argomenti e che spero possa suscitare ancora una volta lo stesso interesse che siamo riusciti a trasmettervi nel corso dei precedenti incontri.

Vi aspettiamo in presenza al prossimo incontro che il Gruppo Corporate Compliance organizzerà.

Noi ci saremo!

Buona lettura a tutti.

Irene Picciano e Antonio Bana

Milano, 15 marzo 2021

CAPITOLO 1 di Andrea Mantovani, Giulio Novellini ed Eva Reggiani

Principio di *accountability* e prassi sanzionatoria dei Garanti europei

SOMMARIO: Introduzione – 2. Possibili angolature dell'*accountability* a valle della prassi sanzionatoria dei Garanti europei – 2.1 Il controllo della filiera dei *partner* commerciali – 2.2 La gestione delle richieste degli interessati di esercitare i diritti *ex* artt. 15 – 22 del GDPR – 2.3 La cancellazione dei dati – 2.4 Le misure di sicurezza – 2.5 Le c.d. violazioni minori – 2.6 Il coinvolgimento del DPO

1. Introduzione

La piena applicazione del Regolamento europeo in materia di protezione dei dati personali n. 2016/679 ("**GDPR**" o il "**Regolamento**") ha senza dubbio modificato l'assetto legislativo precedentemente in vigore, imponendo l'onere per ciascun legislatore nazionale di rivedere la disciplina *data protection* vigente nel proprio stato di riferimento. Tuttavia, occorre dare conto di quali reali incidenze abbia avuto (e stia avendo) l'introduzione del GDPR sugli operatori economici che, quotidianamente, si trovano a dover prendere decisioni, le cui conseguenze possono avere rilevanti impatti non solo dal punto di vista economico, ma anche sull'assetto tecnico, organizzativo e gestionale della rispettiva realtà aziendale. Invero, ogni decisione compiuta dalle figure imprenditoriali o dirigenziali deve ad oggi essere bilanciata, ed ancor prima, dovrà tener conto degli effetti che queste potranno avere nei confronti dei vari soggetti coinvolti.

È ormai imprescindibile per la maggior parte delle realtà aziendali interagire con una moltitudine di dati personali (da quelli dei propri dipendenti a quelli del consumatore finale) ragion per cui ogni scelta economica operata necessita di una preventiva analisi in termini di *compliance* alle disposizioni contenute nel GDPR, nonché rispetto alle varie implementazioni predisposte su base nazionale.

Il Regolamento impone l'osservanza di taluni principi da parte di tutti quei soggetti che, alla stregua delle definizioni fornite dallo stesso GDPR, possano considerarsi titolari o responsabili del trattamento dei dati personali. Come noto, uno dei principi cardine del Regolamento è il cosiddetto principio di *accountability*, ovvero il compito demandato a ciascun titolare del trattamento (ma, nei limiti degli obblighi su questi direttamente gravanti, ciò potrebbe valere anche per il responsabile del trattamento, sebbene l'art. 5(2) del GDPR si

riferisca soltanto ai titolari) di risultare "responsabile" nelle scelte compiute con riferimento ai dati personali all'interno della propria attività.

Tale principio si caratterizza per un certo margine di ampiezza circa il significato precipuo da attribuirsi, con ciò comportando talvolta un vero e proprio disagio per coloro che debbono arbitrariamente operare ogni giorno scelte aventi impatti nei confronti dei soggetti interessati al trattamento dei dati personali.

Responsabilizzare l'operatore nel trattamento dei dati porta con sé quale corollario il fatto che quest'ultimo non può più definirsi mero esecutore di un elenco di misure imposte da una norma, ma diviene invero il responsabile delle misure operative e tecniche che riterrà opportune, efficaci e dunque adeguate per salvaguardare i dati che tratta. Un indizio circa la portata del principio di *accountability* può rinvenirsi all'interno della disposizione di cui all'art 32 GDPR, secondo la quale "*il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio*".

Pertanto, l'obiettivo di ogni titolare o responsabile del trattamento dei dati personali sarà dunque quello di essere "*accountable*" con le previsioni del Regolamento. Questo significa sostanzialmente non solo essere responsabile delle scelte di mezzi, operazioni, procedure o finalità in materia di trattamento dei dati, ma anche essere in grado di "dare conto" delle valutazioni svolte alla base delle scelte poi operate. In ogni caso, non appare immediato comprendere quali reali compiti siano demandati al titolare o al responsabile del trattamento per garantire un adeguato livello di sicurezza dei dati personali trattati; piuttosto il Regolamento fornisce alcuni esempi di circostanze che debbono essere tenute in considerazione nella predisposizione ed attuazione di tutti quei mezzi tecnico-organizzativi e gestionali idonei a prevenire o mitigare il rischio di violazione della disciplina normativa contenuta nel GDPR. Sempre l'art. 32 GDPR specifica che ogni scelta dovrà essere effettuata "[…] *tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche* […]", riservando però a ciascun soggetto il pragmatico compito di porre in essere le idonee valutazioni.

Ed ecco dunque che il margine di incertezza circa le decisioni da intraprendere cresce notevolmente per coloro che sono chiamati ad assicurare un trattamento "responsabile" all'interno del proprio contesto aziendale. Valga per tutti, ad esempio, il trattamento effettuato attraverso strumenti elettronici: nella vigenza del precedente decreto legislativo 30 giugno 2003, n. 196 (il "**Codice Privacy**") erano presenti dettagliate disposizioni che chiarivano le modalità con le quali effettuare il trattamento attraverso l'utilizzo di sistemi informatici (si veda il cd. allegato B al Codice Privacy), così risultando agevole anche per lo stesso titolare o responsabile del trattamento verificare *ex* ante la correttezza del proprio operato in termini di *accountability*. Tuttavia, il 19 settembre 2018 è entrato in vigore il decreto legislativo 10 agosto 2018, n. 101, emanato per armonizzare l'esistente normativa del Codice Privacy con il Regolamento, il

quale ha disposto l'abrogazione dello stesso allegato B e così rendendo meno chiari i contorni delle procedure esperibili per risultare *compliant* al nuovo dettato normativo.

Invero l'incertezza per gli odierni titolari e responsabili del trattamento è ben più ampia sotto molteplici aspetti disciplinati dal GDPR. Alcuni esempi permetteranno una migliore comprensione di quanto riferito.

L'art. 35 del GDPR prevede che "[q]*uando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*". Appare evidente che la valutazione circa l'opportunità di una valutazione d'impatto è rimessa alla discrezionalità del titolare del trattamento, e a tal riguardo, preziose indicazioni possono essere rintracciate all'interno delle linee guida del Gruppo di lavoro Articolo 29 ("**WP29**") in materia[1]. Tali linee guida – unitamente alle liste contenenti l'elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto adottate anche dall'Autorità Garante per la protezione dei dati personali ("**Garante**") – specificano alcuni criteri da tenere in considerazione nel momento in cui occorre valutare quali trattamenti siano soggetti ad un elevato rischio per i diritti e le libertà delle persone fisiche. Ad esempio, sarà opportuno domandarsi se il trattamento sia effettuato con processi decisionali automatizzati, se coinvolge monitoraggi sistematici, sia effettuato su larga scala o abbia ad oggetto dati relativi a soggetti vulnerabili.

Anche per quanto riguarda l'opportunità della notifica di una violazione dei dati personali (cd. *data breach*) all'autorità competente, le indicazioni fornite dal Regolamento presentano contorni incerti. Come noto, il titolare del trattamento in caso di violazione dei dati personali è tenuto a notificare la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il medesimo non ritenga improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Ne consegue che al titolare del trattamento sarà imposto il delicato compito di valutare la gravità della stessa violazione a pena di essere giudicato *ex post* non *compliant* al principio di *accountability*.

Ed ancora, come accennato in apertura, al titolare del trattamento sarà demandata la scelta circa le opportune misure di sicurezza da adottare all'interno della propria realtà aziendale per garantire la protezione dei dati trattati. Le valutazioni dovranno tener in considerazione la tipologia di attività effettuata, la quantità e qualità di dati trattati, l'eventuale trasferimento degli stessi presso paesi terzi, le modalità con le quali vengono trattati i dati nonché i sistemi utilizzati a tal fine ed ulteriori elementi che di volta in volta caratterizzino lo specifico modello di *business*, con l'avvertimento che una totale certezza circa

1 Cfr. le *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento 'possa presentare un rischio elevato' ai fini del regolamento (UE) 2016/679* del WP29 adottate il 4 ottobre 2017.

la correttezza del proprio operato non si potrà raggiungere in via definitiva. Questa è una delle ragioni in virtù delle quali, nei casi *borderline*, si suggerisce di ricorrere piuttosto a una consultazione preventiva dell'autorità competente per identificare quali misure implementare al fine di non rischiare di incorrere in futuro in eventuali sanzioni.

Nel prosieguo si vedrà come i Garanti europei hanno, a oggi, interpretato il principio di *accountability* ai fini sanzionatori e quali sono stati i riflessi pratico-operativi sul mercato di riferimento. Ciò con l'intento di fornire all'operatore un ulteriore elemento per meglio interpretare il principio di *accountability* e per programmare e/o strutturare più efficacemente il proprio trattamento di dati personali.

2. Possibili angolature dell'*accountability* a valle della prassi sanzionatoria dei Garanti europei

2.1 Il controllo della filiera dei *partner* commerciali

In termini di rispetto del principio di *accountability*, il Garante si è peraltro espresso con riferimento ai cosiddetti "controlli" imposti al titolare del trattamento nei confronti dei *partner* commerciali coinvolti nelle operazioni economiche riconducibili al titolare stesso. La tematica si riferisce a tutte quelle fattispecie in cui un titolare del trattamento decida di avvalersi di ulteriori soggetti terzi all'interno della propria attività per attuare il proprio *business*. Come noto, il GDPR prevede che, qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo debba ricorrere esclusivamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti imposti dal Regolamento e garantisca la tutela dei diritti dell'interessato. Ma il rispetto del principio di *accountability* non potrà considerarsi del tutto assolto ed essere limitato alla sola fase iniziale di selezione dei *partner* commerciali che verranno coinvolti, risultando necessario anche un più esteso controllo dell'operato di questi ultimi per tutta la durata dei rapporti contrattuali.

Per non rendere eccessivamente astratto l'assunto riportato è opportuno riflettere su alcune recenti decisioni adottate dal Garante.

Con provvedimento dello scorso luglio 2020, il Garante ha sanzionato una compagnia telefonica a seguito di segnalazioni relative alla ricezione di contatti promozionali indesiderati effettuati tramite telefono, *sms*, *e-mail*, *fax* o chiamate automatizzate. Le condotte erano state realizzate da partner commerciali nominati dalla società quali propri responsabili del trattamento. Ciononostante, il Garante ha ritenuto che nel caso di specie "*Le condotte descritte [abbiano dato] atto della mancanza di adeguate misure tecniche e organizzative, in violazione degli artt. 24 e 25 del Regolamento, con particolare riguardo all'incapacità di controllare efficacemente la filiera dei partner che effettuano attività promozionale a vantaggio della Società*".

In un altro caso portato all'attenzione del Garante, il soggetto reclamante lamentava la ricezione al proprio indirizzo di posta elettronica di un messaggio indesiderato a contenuto promozionale. La società reclamata dichiarava di non detenere l'indirizzo di posta elettronica dell'interessato nelle proprie banche dati e di aver affidato l'invio delle *newsletter* (a cui il messaggio indesiderato era riconducibile) a una società esterna. Il Garante, anche in questa circostanza, ha accertato che la società reclamata non avesse posto in essere alcuna preliminare verifica circa il rispetto delle condizioni previste dalla disciplina in materia di protezione dei dati personali circa l'invio delle comunicazioni a contenuto promozionale (ivi comprese le modalità utilizzate dal *partner* contrattuale per acquisire il consenso degli interessati), né avesse in alcun modo disciplinato contrattualmente il ruolo dei *partner* contrattuali chiamati ad effettuare l´invio delle comunicazioni promozionali. Per tali ragioni, la società è stata condannata ad adottare idonee misure volte ad assicurare l'utilizzo, per le proprie campagne di *marketing* effettuate anche per il tramite di soggetti esterni, di dati personali relativi ad interessati che avessero prestato il proprio idoneo consenso.

Sempre in tema di campagne promozionali, il Garante ha confermato, con provvedimento dello scorso gennaio 2020, che è compito del titolare del trattamento rispettare il principio di *accountability* anche dimostrando di aver controllato che le attività compiute dai propri *partner* commerciali siano state eseguite in *compliance* con i dettati normativi tutelanti i dati personali. Invero, nel caso analizzato, la condotta contestata dal Garante al titolare era rappresentata dal fatto che quest'ultimo aveva condiviso con i rispettivi *partner* delle cosiddette "*blacklist*" clienti (ovvero le liste di coloro che avevano già espresso il loro diniego al riguardo) senza che fossero loro impartite specifiche istruzioni circa il trattamento di tali dati o fossero evidenziate le finalità di tale condivisione. A seguito di tale condivisione, i *partner* avevano (illegittimamente) contattato per fini promozionali alcuni clienti del titolare, i cui nominativi erano presenti in tali liste. Da ciò il Garante aveva ravvisato un difetto di *compliance* da parte del titolare del trattamento (con contestuale responsabilità di tutti i soggetti coinvolti nelle attività promozionali) nel trattamento dei dati personali contenuti in tali *blacklist*, con diretta e conseguente violazione del principio di *accountability*.

Considerando quanto sopra, appare dunque evidente che i contorni del principio di *accountability* possano espandersi anche ben oltre la mera propria attività del titolare del trattamento, essendo richiesto a quest'ultimo un controllo non solo limitato a tutto ciò che avviene all'interno della propria organizzazione, bensì anche alle attività di trattamento che siano direttamente e/o indirettamente riconducibili alla sua responsabilità.

2.2 La gestione delle richieste degli interessati di esercitare i diritti *ex* artt. 15 – 22 del GDPR

La gestione delle richieste degli interessati costituisce uno dei banchi di prova dell'*accountability* poiché l'art. 12 del GDPR impone ai titolari del trattamento il rispetto di tempistiche ben precise nonché specifici obblighi informativi in caso di ritardo[2].

In primo luogo, il principio di *accountability* – oltre al principio di trasparenza – presuppone che agli interessati siano fornite informazioni chiare e non contraddittorie circa le modalità mediante le quali questi possono esercitare i propri diritti. Sul punto, nell'ambito di un recente procedimento nei confronti di un operatore telefonico[3], quest'ultimo aveva giustificato il fatto che molte richieste degli interessati non fossero state adeguatamente riscontrate perché inviate a indirizzi *e-mail* ordinari o di posta elettronica certificata "*non presidiati da personale idoneo a gestire istanze relative alla protezione dei dati personali*", ciò a maggior ragione in considerazione del fatto che in una "*struttura complessa*" come è quella dell'operatore telefonico in questione "*non è possibile assicurare la corretta gestione delle richieste se non pervengono ai corretti recapiti, come indicato nelle informative presenti sui siti web dei brand* […]*"*. In proposito, il Garante ha rilevato, fra l'altro, come (*i*) pur comprendendo l'esigenza del titolare del trattamento di *"far confluire verso un unico 'canale' le richieste relative alla protezione dei dati personali, la numerosità delle doglianze pervenute ha reso evidente che i soggetti interessati non sempre sono in grado di ricondurre autonomamente le proprie istanze a problematiche connesse alla disciplina della protezione dei dati personali*", rilevando altresì come fra i segnalanti non vi fossero anche diversi professionisti; (*ii*) le numerose segnalazioni ricevute concernevano quasi sempre gli stessi indirizzi di posta elettronica (e diversi rispetto a quelli indicati nelle varie informative *ex* art. 13 del GDPR), dunque, "[l]*'utilizzo così ricorrente dei medesimi recapiti da parte di numerosi segnalanti, in luogo di quelli riportati nelle informative, può considerarsi indicativo del fatto che, innanzitutto, essi siano stati in qualche modo resi noti ai clienti (verosimilmente nella documentazione contrattuale o, come riferito in alcune segnalazioni, forniti telefonicamente dallo stesso servizio clienti)*".

Analogamente, nell'ambito di un procedimento nei confronti di un altro operatore telefonico in cui quest'ultimo aveva giustificato il non aver dato seguito alla richiesta di esercizio dei diritti ricevuta da un reclamante adducendo che tale richiesta fosse stata inoltrata a un indirizzo di posta elettronica certificata del titolare del trattamento deputato alla gestione dei recessi contrattuali, il Garante ha osservato come "l'*indirizzo PEC* […] *utilizzato per veicolare la richiesta del reclamante corrisponde ad una utenza di posta elettronica certificata della Società (ancorché deputata alla gestione dei recessi contrattuali) e pertanto è stato consi-*

2 Cfr. l'art. 12(2) del GDPR il quale prevede che "[i]*l titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta*. […]".

3 Cfr. il provvedimento n. 143 del 9 luglio 2020 (doc. *web* 9435753).

derato del tutto ingiustificato il mancato riscontro ad una missiva regolarmente pervenuta tramite mail certificata nei sistemi societari"[4].

Peraltro, la necessità di adottare misure tecniche e organizzative idonee a far sì che le richieste degli interessati siano intercettate e correttamente smistate impone, fra l'altro, che: (*i*) con particolare riferimento al servizio clienti o comunque, più in generale, ai soggetti – interni o esterni al titolare del trattamento – preposti a interagire con gli interessati per conto del titolare del trattamento, siano fornite le necessarie istruzioni in merito; (*ii*) non siano adottate procedure che rendano più difficoltoso, per gli interessati, l'esercizio dei diritti *ex* artt. 15-22 del GDPR; (*iii*) le informazioni e i documenti contenenti i dati personali dell'interessato siano cancellati allo spirare dei termini di conservazione indicati nell'informativa *ex* art. 13 del GDPR.

In relazione al punto (*i*), il Garante ha qualificato il servizio clienti come "*interlocutore primario per gli interessati*".

In relazione al punto (*ii*), il Garante[5] ha censurato la prassi di un titolare del trattamento di richiedere agli interessati che intendessero revocare il proprio consenso alla ricezione di comunicazioni commerciali o opporsi al trattamento dei loro dati personali per finalità di *marketing* di fornire un documento di identità in quanto,"*ferma restando la necessità di adottare, all'occorrenza, misure per identificare gli interessati" tale richiesta appare "ultronea nel caso di soggetti che non abbiano in essere un rapporto contrattuale con la Società ma che, contattati per finalità promozionali, vogliano comunque opporre il proprio diniego*".

È interessante notare come il Garante operi un bilanciamento fra la necessità, in generale, di identificare correttamente l'interessato che intende esercitare i propri diritti, da un lato, e dall'altro la ragionevolezza delle misure che il titolare del trattamento deve adottare a seconda del diritto concretamente esercitato: in particolare, il Garante precisa che "*la ragionevolezza delle misure adottate può essere valutata tenendo conto del contesto e dei potenziali rischi ma anche dell'utilità a conseguire lo scopo (di pervenire alla corretta identificazione)*". Più precisamente, il Garante osserva come la revoca del consenso per finalità di *marketing* potrebbe avere "*scarse conseguenze* […] *nella sfera giuridica dell'interessato rispetto a quelle, ben più pregiudizievoli, derivanti dall'esercizio di altri diritti, laddove fosse un terzo malintenzionato a esercitarli*", oltre al fatto che non sarebbe ipotizzabile un interesse di altri soggetti a revocare il consenso od opporsi al trattamento per finalità di *marketing*.

2.3 La cancellazione dei dati

Sempre alla stregua del principio di *accountability* dev'essere considerato anche il tema del periodo di conservazione dei dati (*data retention*) ovvero della loro relativa cancellazione. Il Regolamento non prevede, infatti, il termine ultimo entro cui sia possibile conservare i dati oppure risulti necessario elimi-

4 Cfr. il provvedimento n. 224 del 12 novembre 2020 (doc. *web* 9485681).

5 Cfr. il provvedimento n. 143 del 9 luglio 2020 (doc. *web* 9435753).

narli, ma dispone che il titolare debba informare l'interessato nel momento di raccolta dei dati circa il periodo di conservazione degli stessi, o in subordine, qualora non sia possibile determinarlo *ex ante*, quali siano i criteri alla luce dei quali verrà identificato il periodo di conservazione.

Con riferimento al periodo di conservazione dei dati rilevano alcune discipline legislative particolari che dovranno essere tenute in considerazione dal titolare del trattamento nel momento di predisposizione di un modello di *data retention*. Il tutto per evitare di risultare *compliant* dal punto di vista *data protection*, ma, allo stesso tempo, infrangere differenti disposizioni normative. Sarà dunque opportuno analizzare all'interno di ciascun diverso *business* quali tipologie di obblighi di legge impongano una conservazione specifica dei dati.

Alcuni esempi pratici potranno utilmente ricavarsi a valle delle decisioni sanzionatorie delle competenti autorità europee in materia di protezione di dati. È il caso dell'autorità garante francese – *Commission nationale de l'informatique et des libertés* ("**CNIL**") – che ha irrogato una sanzione a una società operante nel *retail online* per aver conservato per un periodo superiore a cinque anni alcuni dati personali di soggetti interessati – a dire della società, potenziali clienti – per il sol fatto che questi ultimi, nei pregressi cinque anni, avevano consultato le *e-mail* contenenti la *newsletter* a loro inviata dalla società. Secondo il CNIL, le previsioni erano in aperto contrasto con i principi di minimizzazione e violavano sistematicamente anche il principio di *accountability*. Così in Spagna è stato il caso di un istituto di credito, sanzionato per aver conservato alcuni dati personali di soggetti interessati che avevano aperto un conto corrente e non risultavano più clienti della banca da circa 16 anni, e ciò senza fornire alcun elemento utile al fine di illustrare le ragioni e la metodologia utilizzata per determinare tale periodo di conservazione.

Nell'ambito della posta elettronica gestita dai dipendenti, con provvedimento n. 53/2018[6] il Garante ha sanzionato la conservazione *sine die* dei messaggi ad opera di una società. Gli addebiti mossi contro quest'ultima hanno riguardato la conservazione in modo sistematico di dati esterni e del contenuto di tutte le *e-mail* scambiate dai dipendenti per l'intera durata del rapporto di lavoro, nonché dopo la relativa interruzione del rapporto contrattuale. Ancora una volta, la contestazione del Garante si concentra sul riferimento generico e non contestualizzato degli elementi utilizzati dalla società per determinare la conservazione dei dati.

Alla luce di quanto sopra, si evidenzia quindi che le contestazioni mosse dai Garanti non siano tanto concentrate circa il "*quantum*" dei periodi di conservazione identificati, quanto piuttosto sulla mancanza da parte delle società di essere in grado di dar conto degli gli elementi dalle stesse utilizzate al fine di determinare tali periodi di conservazione, sottolineando dunque come tali condotte siano in palese contrasto con l'*accountability* richiesta.

In sintesi: l'*accountability* garantisce una grande flessibilità al titolare del trattamento nel determinare il periodo di conservazione dei dati dal medesimo

6 Cfr. il provvedimento n. 53 del 1° febbraio 2018 (doc. *web* 8159221).

trattati; pertanto, lo stesso potrà decidere come meglio crede, considerando le proprie necessità, finalità perseguite e i sistemi tecnici a sua disposizione. In ogni caso, tale flessibilità non può prescindere dall'obbligo in capo al titolare di fornire evidenza circa i fattori dallo stesso considerati per tale determinazione e dimostrare come gli stessi risultino *compliant* con la normativa *privacy* applicabile.

2.4 Le misure di sicurezza

Riprendendo il disposto dell'art. 32 del GDPR, si era già avuto occasione di menzionare il principio secondo cui il titolare del trattamento è tenuto a dotarsi di efficienti sistemi di sicurezza per garantire un livello di sicurezza adeguato al rischio.

Peraltro, è la stessa disposizione a prevedere una serie di elementi che potrebbero fungere da adeguate misure di sicurezza. A solo titolo esemplificativo, il Regolamento prevede che le citate misure di sicurezza possano ricomprendere, tra le altre, la pseudonimizzazione e la cifratura dei dati personali, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, ed ancora, un'efficace procedura per verificare e testare regolarmente l'efficacia delle misure tecniche e organizzative. La lista non esaurisce né pretende di elencare in via onnicomprensiva le misure idonee a salvaguardare i dati dal rischio di *deficit* nel trattamento, pertanto spetterà al titolare del trattamento comprendere il modello gestionale più opportuno da adottare per ciascun caso specifico.

Il secondo comma dell'art. 32 del GDPR, in particolare, sancisce che "[n]*el valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*". Ne deriva quale corollario che la tematica coinvolgerà necessariamente anche la fase successiva ad una eventuale dispersione dei dati o immissione non autorizzata, sicché sempre all'interno del principio di *accountability* dovrà essere effettuata la valutazione circa le attività compiute dal titolare, ad esempio, nel momento in cui si verifica un episodio di *data breach*. Infatti, il Regolamento (cfr. artt. 33-34) conferisce al titolare del trattamento una certa discrezionalitùà nel decidere anzitutto se comunicare all'autorità competente tale avvenimento e se, in via ulteriore, procedere a tale comunicazione anche nei confronti dei soggetti interessati i cui dati personali siano stati oggetto del *data breach*.

In via prudenziale, la valutazione dovrà tenere conto della tipologia di danni che potrebbero verificarsi a seguito della violazione dei dati. Il Garante ha specificato, all'interno della pagina informativa dedicata sul proprio sito *web* istituzionale, che devono essere notificate le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali. Per effetti avversi significativi nei confronti degli individui si intendono, per esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode,

la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

Il Regolamento, dunque, intende lasciare ampio margine di discrezionalità al titolare del trattamento sotto diversi profili, essendo improntato a una visione "responsabilizzante". Pertanto, al titolare è fortemente suggerito un costante aggiornamento sulle interpretazioni delle più rilevanti tematiche *privacy*, attraverso la consultazione diretta delle fonti più qualificate quali, *inter alia*, oltre alle linee guida e ai provvedimenti sanzionatori del Garante, le linee guida e i provvedimenti sanzionatori degli altri Garanti europei, nonché le linee guida e i pareri dello *European Data Protection Board* ("**EDPB**") e del WP29. Sarà così possibile, da una parte, mitigare il rischio di eventuali violazioni e, dall'altra, colmare quel *gap* spesso intercorrente tra l'astrattezza della disposizione normativa e la realtà concreta nella gestione del proprio *business*.

2.5 Le c.d. violazioni minori

Il considerando n. 148 del GDPR prevede che "[i]*n caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria*". In assenza di una definizione di cosa possa costituire una "violazione minore", il WP29, nelle *Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679* del 3 ottobre 2017, ha precisato che la qualificazione in tal senso della violazione di una o più disposizioni del GDPR elencate dall'art. 83(4) o (5) del GDPR dipende dalla valutazione delle circostanze del caso concreto, perché l'applicazione dei criteri di valutazione di cui all'art. 83(2) del GDPR può portare l'autorità di controllo "*a ritenere che nelle circostanze concrete del caso la violazione, ad esempio, non crei un rischio significativo per i diritti degli interessati in questione e non incida sull'essenza dell'obbligo in questione*". Pertanto, nel caso in cui l'autorità di controllo ritenga che quella specifica violazione è qualificabile come una violazione minore, tale autorità avrà la possibilità (e non l'obbligo) di sostituire la sanzione pecuniaria con un ammonimento.

In proposito, da una disamina dei primi provvedimenti del Garante in materia, emerge come la soglia perché una violazione possa essere qualificata come minore sia piuttosto elevata e come l'*accountability* giochi un ruolo fondamentale, poiché rileva:

- in un'ottica preventiva, in quanto è possibile qualificare una violazione come minore qualora tale violazione possa essere considerata come un caso isolato, una svista, o una mera disattenzione dovuta a errori non intenzionali[7] e giustificabili alla luce delle peculiari circostanze del caso

7 Cfr., fra gli altri, i provvedimenti n.ri 103 del 18 giugno 2020 (doc. *web* 9451705) e 123 del 2 luglio 2020 (doc. *web* 9440096) relativi alla consegna di una cartella clinica a un paziente diverso dal paziente cui quella cartella afferiva nonché il provvedimento n. 141 del 9 luglio 2020 (doc. *web* 9440117) relativo all'erronea identificazione di un paziente al pronto soccorso con conseguente pubblicazione del referto sul fascicolo sanitario elettronico di un altro soggetto.

concreto[8], tenendo conto altresì della circostanza che non risultino precedenti violazioni della normativa in materia di protezione dei dati personali né che il Garante abbia precedentemente adottato misure correttive o sanzionatorie;

- in un'ottica rimediale, con riguardo alla circostanza che il titolare del trattamento sia intervenuto prontamente adottando le misure correttive più adatte, a seconda dei casi, anche rimuovendo gli effetti negativi che tale violazione aveva determinato[9].

2.6 Il coinvolgimento del DPO

Come noto, l'art. 38 del GDPR prevede che il responsabile per la protezione dei dati personali o *data protection officer* ("**DPO**") debba essere "*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*". Coerentemente con tale impostazione, l'art. 39 del GDPR individua in via esemplificativa e non tassativa i compiti dei quali il DPO debba essere incaricato e che possono essere sinteticamente categorizzati come segue: (*i*) attività di consulenza, sia in generale sia in ipotesi più specifiche (*e.g.*, in merito alla valutazione di impatto *ex* art. 35 del GDPR); (*ii*) attività di sorveglianza e monitoraggio circa la *compliance* con la normativa in materia di protezione dei dati personali; (*iii*) attività di raccordo con l'autorità di controllo.

In proposito, il WP29, nelle *Linee guida sui responsabili della protezione dei dati* adottate il 5 aprile 2017, ha precisato, fra l'altro, che è "*essenziale che il* [DPO], *o il suo* team *di collaboratori, sia coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati*" e che occorrerà garantire, ad esempio, che (*i*) il DPO "*sia invitato a partecipare su base regolare alle riunioni del* management *di alto e medio livello*"; (*ii*) che la sua presenza "*ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati*"; e (*iii*) che il suo parere "*riceva sempre la dovuta considerazione*", raccomandando, quale buona prassi, che in caso di disaccordo, vengano documentate "*le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal* [DPO]"[10].

Alla luce di ciò – premesso che la responsabilità ultima per la *compliance* con il GDPR resta in ogni caso in capo al titolare del trattamento (o al responsabile del trattamento, con riferimento agli adempimenti che il GDPR gli impone direttamente) e tralasciando la questione relativa agli eventuali profili di responsabilità professionale del DPO[11] – *quid* nel caso in cui il titolare (o il responsa-

8 Cfr. il provvedimento n. 55 del 12 marzo 2020 (doc. *web* 9365178) in cui il titolare del trattamento aveva riscontrato tardivamente la richiesta di accesso del reclamante ai dati personali delle figlie minori perché il titolare era venuto a conoscenza che le stesse erano state affidate ai servizi sociali e la potestà genitoriale del reclamante era stata sospesa.

9 Cfr., fra gli altri, il provvedimento n. 45 del 5 marzo 2020 (doc. *web* 9365147) relativo a una annotazione nel registro elettronico nonché il provvedimento n. 20 del 12 marzo 2020 (doc. *web* 9365159) relativo alla pubblicazione sul sito *web* di una scuola delle graduatorie relative al personale amministrativo, tecnico e ausiliario.

10 Cfr. le *Linee guida sui responsabili della protezione dei dati* del WP29 adottate il 5 aprile 2017, pp. 17-18.

11 In proposito, cfr., fra gli altri, M. C. Carpenelli in L. Bolognini ed E. Pelino (diretto da) *Codice della Disciplina Privacy*, 2019, Milano, pp. 273 e ss.

bile) del trattamento si conformi a un parere del DPO che successivamente si riveli erroneo?

In proposito, in un recente caso sottoposto all'esame del Garante[12], il titolare del trattamento – un Comune toscano – aveva giustificato la propria condotta adducendo, fra l'altro, di aver sempre agito secondo diligenza e correttezza perché aveva sempre chiesto – conformandovisi prontamente – il parere del DPO, il quale (*i*) in un primo momento aveva ritenuto che pubblicare, sul sito *web* istituzionale, una determinazione del Comune relativa a una vicenda giudiziaria che coinvolgeva il Comune stesso e una sua dipendente indicando soltanto le iniziali della dipendente fosse una misura sufficiente per tutelare la riservatezza di quest'ultima; successivamente (*ii*) aveva cambiato idea, suggerendo di optare, ove tecnicamente possibile, per la rimozione anche delle iniziali della dipendente.

Il Garante, all'esito dell'istruttoria, pur condannando comunque il Comune ritenendo illecita la diffusione dei dati personali della reclamante, fra le circostanze del caso concreto valutate *ex* art. 83 del GDPR aveva valutato favorevolmente la circostanza che il Comune avesse coinvolto il DPO e che si fosse "*conforma*[to] *in buona fede*" al suo parere. Sebbene al momento non sia possibile prevedere se e in quale misura il Garante seguirà in futuro questa linea interpretativa, si tratta comunque di una decisione utile, soprattutto nel caso in cui il parere del DPO riguardi questioni particolarmente sofisticate o dibattute, ad esempio in materia di intelligenza artificiale e tecnologie IoT.

12 Cfr. il provvedimento n. 118 del 2 luglio 2020 (doc. *web* 9440025)

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

Il targeting degli utenti dei social media

sommario: 1. Introduzione – 2. Ruoli e responsabilità dei soggetti coinvolti – 3. I differenti meccanismi di targeting: basi giuridiche, ruoli ed esempi pratici – 3.1 Targeting sulla base di dati forniti dall'utente – 3.2 Targeting sulla base di dati osservati – 3.3 Targeting sulla base di dati dedotto o derivati – 4. Principio di trasparenza e diritto di accesso – 5. La valutazione dell'impatto sulla protezione dei dati (DPIA) – 6. Le categorie particolari di dati – 7. Contitolarità e responsabilità

1. Introduzione

L'European Data Protection Board ("EDPB") è recentemente intervento sul tema del *targenting* degli utenti dei *social media*, ovvero di quella attività che consente di indirizzare messaggi specifici agli utenti dei *social media* per promuovere determinati interessi, commerciali o di altro tipo.

Nello specifico, lo scorso 2 settembre sono state adottate le Linee guida 8/2020 sul *targeting* degli utenti dei *social media* (Guidelines 8/2020 on the targeting of social media users, "Linee Guida"), il cui testo è stato quindi sottoposto a consultazione pubblica finalizzata a raccogliere le opinioni delle parti interessate, che si è conclusa il 19 ottobre 2020.

L'EDPB evidenzia nelle Linee Guida che, alla diffusione dei *social media*, intendendosi per tale qualsiasi piattaforma online che consenta lo sviluppo di reti e comunità di utenti che condividono informazioni e contenuti e non solo quindi i più noti *social network*, si è accompagnata negli ultimi dieci anni un sempre più diffuso utilizzo dello strumento del *targeting* degli utenti degli stessi *social media*, che consente, tra l'altro, di indirizzare messaggi pubblicitari personalizzati, mirati cioè al soggetto che in un dato momento risulta essere interessato a un determinato prodotto o servizio.

Il *targeting* si basa sull'analisi di dati personali, anche aventi natura sensibile, provenienti da fonti diverse e che in alcuni casi, come si vedrà, determina la profilazione degli utenti, definita dal GDPR come quella forma di trattamento automatizzato dei dati personali che valuta aspetti personali di una persona fisica al fine di analizzarne o prevederne quegli elementi riguardanti, ad esempio, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti.

Evidenti sono i rischi per i soggetti interessati sotto il profilo della protezione dei dati personali. Il *targeting* degli utenti dei *social media* può determinare trattamenti di dati personali che vanno oltre le ragionevoli aspettative dei soggetti interessati, perché trattati per finalità e secondo modalità diverse da quelle inizialmente individuate; le attività di profilazione connesse al *targeting* possono portare all'individuazione di interessi o altre caratteristiche che l'individuo non aveva fornito volontariamente, mettendo a rischio il suo esercizio del controllo sui propri dati personali; ancora, la mancanza di trasparenza sul ruolo dei diversi attori coinvolti può pregiudicare l'esercizio dei diritti degli interessati.

In questo scenario, l'obiettivo delle Linee Guida è quello di fornire, nella cornice della disciplina del GDPR, indicazioni pratiche a chiunque svolga attività di *targeting*, e nello specifico di definire ruoli e responsabilità dei soggetti coinvolti (in particolare di fornitori di servizi di *social media* e *targeters*) e di individuare, alla luce dei rischi potenziali per i diritti e le libertà degli individui, gli adempimenti necessari ai sensi della disciplina in materia di protezione dei dati personali.

2. Ruoli e responsabilità dei soggetti coinvolti

Le Linee Guida definiscono i servizi di *targeting* come "*servizi che consentono a persone fisiche o giuridiche (targeters) di comunicare messaggi specifici agli utenti dei social media al fine di promuovere interessi commerciali, politici o di altro tipo*".

I servizi di *targeting* offerti dai *social media providers* ai *targeters* utilizzano algoritmi sviluppati sulla base di un'ampia gamma di criteri che si applicano ai dati personali degli utenti. Si tratta non solo dei dati personali forniti dall'utente nell'utilizzo del *social media*, ma anche di dati personali "osservati" dal *social media provider* nell'utilizzo del *social media* da parte dell'utente o ancora di dati derivati, ovvero creati dal *social media provider* o da soggetti terzi sulla base dei dati forniti o osservati[13].

Nell'ambito di questo processo di trattamento dei dati degli utenti dei *social media* (i soggetti interessati), i ruoli principali sono quelli svolti dai *social media providers* e dai *targeters*, accanto ai quali possono eventualmente inserirsi altri soggetti.

I soggetti interessati sono ovviamente gli utenti dei *social media*. Si tratta normalmente di soggetti titolari di un "*account*" o "*profilo*" personale ma in alcuni casi anche di soggetti non registrati, che pur non avendo accesso a tutti i servizi offerti dal *social media* devono essere qualificati come soggetti interessati laddove siano direttamente identificati o identificabili. Gli utenti dei *social network* non necessariamente rendono noto il proprio nome, potendo il *targeting* basarsi ad esempio su codici identificativi *online*.

I *social media providers*, che offrono i servizi di *targeting*, sono i soggetti che forniscono servizi *online* che consentono lo sviluppo di reti e comunità di utenti. Sono i *social media providers* a determinare le funzionalità del servizio e

13 Si veda § "I differenti meccanismi di *targeting*: basi giuridiche, ruoli ed esempi pratici".

quindi i dati trattati, la finalità e modalità del loro trattamento e ad avere quindi accesso ai comportamenti e alle interazioni degli utenti e quindi a informazioni sugli interessi e preferenze degli stessi. Questo non solo attraverso le attività svolte dagli utenti sulla piattaforma ma anche al di fuori di essa, combinando dati derivanti da fonti diverse.

I *targeters* sono invece soggetti che fanno ricorso ai servizi di *targeting* per indirizzare, sulla base delle caratteristiche, degli interessi e delle preferenze degli utenti, messaggi mirati agli stessi sulla base di specifici criteri. Esempio tipico è quello delle società che utilizzano il *targeting* per pubblicizzare i propri prodotti e quindi per inviare comunicazioni commerciali: questo può avvenire non solo attraverso messaggi contenuti in appositi spazi che compaiono sulle pagine web ma anche in messaggi che appaiono insieme ai contenuti generati dagli utenti.

Infine, nel processo di *targeting* possono essere coinvolti altri soggetti, quali i fornitori di servizi di marketing e di servizi di gestione di dati, che in alcuni casi aggregano i dati derivanti da fonti diverse.

Individuate le attività di *social media providers* e *targeters*, le Linee Guida partono dalla definizione di titolare di trattamento quale soggetto che, singolarmente o insieme ad altri, determina le modalità e le finalità del trattamento di dati personali ed evidenziano come, secondo la giurisprudenza della CGCE, l'esistenza di più titolari del trattamento non implichi necessariamente eguali responsabilità tra i due soggetti, potendo gli stessi essere coinvolti in diversi livelli e a gradi diversi.

Nello specifico le Linee Guida richiamano il caso Wirtschaftsakademie (C-210/16), nel quale la CGCE ha individuato l'amministratore di una "*fan page*" di Facebook come titolare del trattamento, unitamente al *social media provider.* In questa decisione, richiamata anche nei casi Jehovah's Witnesses (C-25/17) e Fashion ID (C-40/17), la Corte insiste sul fatto che il livello di responsabilità degli autonomi titolari del trattamento deve necessariamente essere valutato sulla base delle specifiche circostanze del singolo trattamento e quindi può avere livelli diversi tra i due soggetti che devono essere individuati.

Diverso è il caso dei contitolari del trattamento che, ai sensi dell'articolo 26 GDPR, devono preventivamente individuare in uno specifico accordo le rispettive responsabilità con riferimento agli obblighi di cui al GDPR.

Alla luce di questi presupposti le Linee Guida individuano gli specifici ruoli di *social media providers* e *targeters* sulla base dei diversi meccanismi di *targeting* presi ad esame.

3. I differenti meccanismi di targeting: basi giuridiche, ruoli ed esempi pratici

I meccanismi di *targeting*, analizzati dalle Linee Guida, consistono nelle diverse modalità attraverso cui i dati degli utenti dei *social media* possono essere trattati e appunto targetizzati. I meccanismi di *targeting* vengono classificati dall'EDPB secondo tre tipologie principali individuando, per ciascuna tipologia, i ruoli

privacy dei soggetti coinvolti e le possibili basi giuridiche su cui fondare il trattamento.

Gli utenti dei *social media* possono essere targettizzati sulla base di:

1. dati forniti dagli stessi utenti al social media provider o al targeter;
2. dati osservati dal social media provider o al targeter;
3. dati dedotti o derivati (sempre dal social media provider o al targeter.

3.1 Targeting sulla base di dati forniti dall'utente

Nella prima ipotesi sondata dall'EDPB, le informazioni personali sono fornite attivamente dall'interessato al *social media provider*. Questo avviene, ad esempio, nel caso in cui l'utente indichi nome, cognome e la propria età sul suo profilo *social* oppure anche nel caso in cui il *targeter* usi dati forniti direttamente dall'interessato sulla piattaforma per creare dei *cluster*, delle *audience* di utenti cui inviare i messaggi pubblicitari mirati.

Un esempio concreto del caso 1, si potrebbe avere quando un cliente X interessato a conoscere – ed eventualmente a usufruire di – i servizi mutuo di una banca, contatti l'istituto bancario per avere informazioni e fornisca a quest'ultimo il suo indirizzo *e-mail*. Successivamente la banca, nonostante il cliente X non abbia deciso di sottoscrivere il contratto di mutuo, inserisce l'indirizzo *e-mail* del cliente X nei propri database e nelle proprie liste che successivamente carica sul *social media* Y per incrociarle con le informazioni possedute dallo stesso *social media* e, dunque, targettizzare i propri clienti o *prospect* su tale social in relazione ai servizi finanziari offerti.

Un altro esempio concreto di questo primo caso potrebbe essere quello in cui sia la stessa azienda Y a voler promuovere la vendita di una sua collezione di prodotti tramite un canale social, identificando un *target* di consumatori ben preciso (a puro titolo di esempio, uomini di età compresa tra i 30 e i 45 anni, single). In tal caso, sarà il *social media provider* a individuare i criteri, le modalità e le tempistiche di *targeting* per identificare l'*audience* di riferimento a cui mostrare la pubblicità dell'azienda Y.

In relazione ai ruoli privacy di questi esempi, l'EDPB suggerisce che entrambi i soggetti (il *targeter* e il *social media*), agiscono come titolari del trattamento nella misura in cui il *targeter* – negli esempi citati, la banca o l'azienda Y – determina le finalità e le modalità della raccolta, elaborazione e successiva trasmissione dei dati personali mentre il *social media provider* decide di utilizzare i dati personali acquisiti dall'utente (es. l'indirizzo *e-mail* fornito al momento della creazione del suo account) per consentire al *targeter* di mostrare il messaggio a un'*audience* determinata. Sussiste, dunque, una contitolarità in relazione alle operazioni di trattamento per le quali il provider e il *targeter* determinano congiuntamente gli scopi e i mezzi.

I contitolari dovranno individuare una base giuridica che legittimi il trattamento. L'EDPB ne individua due: il consenso, *ex* art. 6.1 (a) GDPR o il legittimo interesse *ex* art 6.1 (f).

Qualora, si voglia sfruttare l'art. 6.1 (f) GDPR, il legittimo interesse potrebbe ravvisarsi nell'interesse economico del *targeter* a incrementare la pubblicità dei propri beni e servizi attraverso le operazioni di *targeting* sui *social media*. Dal proprio lato, il *social media provider* potrebbe considerare come proprio legittimo interesse far sì che i propri servizi social siano profittevoli attraverso la vendita di spazi pubblicitari. In tal caso, occorrerà un appropriato bilanciamento di interessi tra i diritti e le libertà fondamentali dell'interessato e l'interesse dei contitolari, il cui esito dipenderà dalla presenza di controlli e di forme di protezione a favore dell'interessato quali – suggerisce l'EDPB – la possibilità di esprimere preventivamente l'eventuale opposizione all'utilizzo dei dati personali per finalità di *targeting*.

Non in tutti i casi, il legittimo interesse può essere una base giuridica appropriata. Non lo sarebbe, ad esempio, nel primo esempio sopra citato, in cui il cliente X – i cui dati sono stati raccolti con l'originaria finalità di fornire informazioni su un servizio – non avrebbe alcuna ragionevole aspettativa a vedere i propri dati utilizzati per finalità di targeting. In tal caso, sarà necessario il consenso del cliente X, così come occorrerà fondare il trattamento sul consenso esplicito nei casi di profilazione intrusiva tramite social media o di attività di monitoraggio a fini marketing, come quelle che comportano la tracciabilità degli interessati attraverso i siti web visitati, luoghi, devices, servizi o data *brokering*[14].

In tutti i casi in cui si optasse per – o fosse necessario – il consenso come base giuridica, occorrerà che tutti i requisiti per il consenso[15] siano soddisfatti e che l'attività di *targeting* non sia sproporzionata o iniqua.

3.2 Targeting sulla base di dati osservati

L'osservazione dei comportamenti dell'utente e la raccolta dei relativi dati può anche avvenire attraverso diverse modalità che possono consistere nell'analisi dell'attività che l'utente stesso svolge sulla piattaforma di *social media* (contenuti che l'utente condivide, consulta o mette "*like*") oppure possono derivare dall'analisi di dati raccolti tramite dispositivi su cui viene eseguita una app (coordinate GPS, numero di cellulare) o attraverso siti web di terze parti che hanno incorporato *plugin* o *pixel*.

L'EDPB fornisce nelle Linee Guida due interessanti esempi di questa tipologia di *targeting*, analizzando (*i*) un esempio di targeting fondato su pixel e (*ii*) un esempio di geolocalizzazione operato da un *device*.

Il primo caso si verifica quando il titolare di un sito web decide di integrare un c.d. *tracking pixel* fornito da un *social media* X con lo scopo di monitorare

14 WP29, *Opinion on profiling and authomated decision making.*

15 Linee Guida sul consenso 05/2020 del 4 maggio 2020.

e targetizzare gli utenti del *social media* X che fanno visita al suo sito web. In questo modo, quando l'utente apre il proprio *account* sul social media X inizia a visualizzare la pubblicità dei prodotti venduti tramite il sito precedentemente visitato. Il secondo caso si riferisce, invece, all'ipotesi in cui l'utente Y installi un'applicazione sul proprio *smartphone* accettando i permessi previsti dal *social media provider* della stessa app, con riferimento all'uso della funzionalità GPS. In questo modo, il *social media provider* può raccogliere informazioni sul posizionamento dell'utente Y e segnalare a quest'ultimo la pubblicità delle aziende e/o negozi che usano le funzionalità di *geo-targeting* offerte dal *social media provider* per targettizzare le proprie comunicazioni commerciali.

In entrambi i casi, le finalità della targetizzazione sono piuttosto evidenti: la pubblicità suggerita dal *social media provider* può indurre l'utente a usufruire dei servizi o acquistare i prodotti del *targeter*.

Secondo l'EDPB sussiste una contitolarità del trattamento tra *targeter* e *service provider* in quanto essi determinano congiuntamente le finalità e i mezzi del trattamento: nel primo esempio, il *targeter* decide di installare il *pixel* e il *social media* fornisce il *software* che porta alla raccolta automatica, trasmissione e utilizzo per fini di marketing dei dati personali; nel secondo caso, il *targeter* definisce i parametri della pubblicità targetizzata sulla base delle sue esigenze di *business* e il *social media provider* raccoglie le informazioni al fine di consentire la pubblicità mirata.

Quanto alla base giuridica della casistica analizzata, l'EDPB ritiene che l'interesse legittimo non possa fungere da base giuridica appropriata, in quanto la finalità del trattamento è il monitoraggio del comportamento degli individui attraverso siti web e tecnologie di tracciamento. Pertanto, in tali circostanze, la base giuridica appropriata ai sensi dell'art. 6 GDPR sarà, verosimilmente, il consenso.

Inoltre, gli esempi citati implicano l'utilizzo di *cookie* e, pertanto, trova applicazione l'art. 5.3 della Direttiva ePrivacy[16], oltre che le regole generali sul consenso, secondo cui è necessario fornire agli utenti informazioni chiare e complete sulle finalità del trattamento prima che prestino il consenso precisando che lo scorrere di una pagina web non vale a costituire una chiara e inequivoca azione affermativa di consenso, né sarà possibile pre-selezionare la casella del consenso.

3.3 Targeting sulla base di dati dedotto o derivati

Le Linee Guida dell'EDPB affrontano infine la casistica del *targeting* dei dati dedotti dall'interessato o derivati da quelli osservati dallo stesso titolare de trattamento.

Questi dati, che tipicamente coinvolgono gli interessi o altre caratteristiche personali dell'utente, possono riguardare – sempre a titolo esemplificativo – i

16 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche

"*like*" che l'utente Z rivolge ai post di una determinata azienda od organizzazione dimostrando interesse verso quello specifico prodotto o servizio, cosicché quando la società o l'organizzazione in questione cercheranno potenziali clienti potranno utilizzare i criteri di targeting offerti dal social media provider (*e.g.* interesse per i prodotti α, sesso, età, luogo di residenza) e l'utente Z riceverà sul proprio profilo una pubblicità mirata in tal senso.

In un caso di questo genere, tra *targeter* e *social media provider* sussiste sempre un rapporto di contitolarità poiché sia la raccolta dei dati via '*like*', sia l'analisi svolta dal *social media provider* concorrono al fine di determinare e offrire dei criteri di targettizzazione.

Questo tipo di *targeting* implica in genere una profilazione, ossia, secondo la definizione del Gruppo WP29[17] (ora sostituito dall'EDPB), "*un processo automatizzato di dati che mira alla valutazione di aspetti personali dell'utente*". Per tale ragione, nonché per il fatto che nel caso sopra citato si applica l'articolo 5.3 della Direttiva ePrivacy, la base giuridica appropriata è il consenso dell'utente.

Un altro esempio di profilazione e di *targeting* condotto sulla base di dati dedotti, potrebbe verificarsi nell'ipotesi in cui l'utente W indichi, sul proprio profilo social, di avere un particolare interesse, ad esempio per lo sport, e molti dei suoi abituali comportamenti riguardino appunto questo interesse (quali usare spesso il pc fisso al lavoro per cercare i risultati sportivi su internet o visitare regolarmente dal proprio *smartphone* siti di scommesse *online*). *Il social media provider* traccia l'attività svolta dall'utente W attraverso i diversi dispositivi e sulla base di queste attività e delle informazioni fornite dallo stesso utente W deduce che egli è interessato alle scommesse *online*. In questo modo, il titolare di un sito di scommesse *online* potrà targettizzare gli utenti interessati alle scommesse e che potrebbero scommettere con frequenza e mostrare loro una pubblicità *ad hoc*.

In quest'ultimo esempio, l'EDPB conferma sempre che, in tema di ruoli, sussiste una contitolarità tra il *social media provider* e il *targeter* (il sito di scommesse *online*), mentre si sofferma a svolgere alcune precisazioni in merito alla corretta base giuridica del trattamento.

Infatti, l'EDPB ricorda che nel caso di processo decisionale automatizzato che produca effetti giuridici o incida in modo significativo sulla persona, come stabilito all'articolo 22 GDPR, i titolari possono svolgere attività di profilazione solo in casi eccezionali, ossia quando il trattamento:

- sia necessario per la conclusione o l'esecuzione di un contratto tra interessato e titolare;
- sia autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare;
- si basi sul consenso esplicito dell'interessato.

17 WP29, *Guidelines on Authomated individual decision-making and Profiling for the purpose of Regulation 2016/679*, WP251rev01).

In un caso come quello descritto, la pubblicità mirata relativamente alle scommesse online potrebbe cadere nella sfera dell'art. 22 GDPR poiché, se diretta a persone finanziariamente vulnerabili e interessate alle scommesse *online*, potrebbe produrre effetti significativi sulla loro situazione finanziaria.

Alla luce di queste considerazioni, l'EDPB afferma che sia necessario il consenso preventivo dell'utente (in base al combinato disposto dell'art. 22 GDPR e art. 5.3 Direttiva ePrivacy).

In conclusione, dunque, la regola generale prevista dall'EDPB è quella della contitolarità tra *targeter* e *social media provider*, mentre la base giuridica potrà essere, a seconda dei casi, il legittimo interesse o il consenso. Le Linee Guida ricordano, poi, l'importanza di osservare i principi dettati dall'art. 5 del GDPR, "vale a (*i*) dire valutare..." attentamente la necessità di effettuare una valutazione d'impatto laddove il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone, (*ii*) fornire un'idonea informativa e (*iii*) garantire l'effettivo esercizio dei diritti degli interessati.

4. Principio di trasparenza e diritto di accesso

Come è noto, l'articolo 5 del GDPR prevede che i dati personali devono essere trattati in modo lecito, corretto e trasparente e devono essere raccolti per finalità determinate, esplicite e legittime.

Le informazioni presentate agli interessati riguardo al modo in cui i loro dati personali sono trattati, devono inoltre essere concise, trasparenti, rese in forma intelligibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice. Sul punto l'EDPB ricorda che il semplice uso della parola "pubblicità" non sarebbe sufficiente per informare gli utenti che la loro attività è monitorata ai fini di una pubblicità mirata. È infatti necessario evidenziare agli interessati quali tipi di attività di trattamento vengono svolte e se il loro comportamento sarà oggetto di profilazione.

Ulteriore espressione del principio di trasparenza è l'obbligo di mettere a disposizione dell'interessato i termini essenziali dell'accordo di contitolarità del trattamento (ex art. 26, par. 2, GDPR) posto che i contitolari adottano misure adeguate a garantire che gli interessati siano consapevoli della ripartizione delle responsabilità.

L'interessato ha dunque diritto di ricevere, sin dall'inizio, tutte le informazioni richieste dagli articoli 13 e 14 GDPR, incluse le finalità dei trattamenti condivisi o strettamente collegati, i periodi di conservazione, la trasmissione dei dati a terzi e così via.

Sebbene entrambi i contitolari del trattamento siano soggetti all'obbligo di informativa, possono concordare che uno di loro sia incaricato di fornire le informazioni iniziali agli interessati, soprattutto nei casi in cui solo uno dei titolari del trattamento interagisca con gli utenti.

Nel caso in cui uno dei contitolari non disponga di tutte le informazioni in dettaglio perché, ad esempio, non conosce l'esatta esecuzione tecnica delle attività di trattamento, l'altro contitolare è tenuto a fornirgli tutte le informazioni necessarie per fornire all'interessato una informativa completa.

I titolari del trattamento non sono comunque tenuti a fornire informazioni in merito ad ulteriori operazioni di trattamento che non rientrano nell'ambito della contitolarità. In pratica, il *targeter* non sarà dunque direttamente responsabile in merito alle informazioni relative a qualsiasi successivo trattamento che sarà effettuato dalla piattaforma di *social media*.

Tuttavia, l'EDPB sottolinea che il contitolare del trattamento che intende utilizzare ulteriormente i dati personali, ha specifici obblighi di informazione in relazione al suddetto ulteriore trattamento laddove non vi sia una responsabilità congiunta, ai sensi dell'art.14, par.4, GDPR.

Ad esempio, il *targeter* e il fornitore di *social media* potrebbero concordare che il *targeter* fornirà determinate informazioni per conto del fornitore di *social media*. Quest'ultimo, tuttavia, resta il responsabile ultimo tenuto a garantire che all'interessato siano state fornite le informazioni pertinenti in relazione a tutte le attività di trattamento sotto il suo controllo.

In aggiunta a quanto sopra, i titolari devono naturalmente consentire agli utenti di esercitare facilmente e pienamente i propri diritti attraverso uno strumento facile da usare ed efficiente, in particolare per ciò che concerne i diritti di cancellazione, opposizione e di accesso si dati e preferibilmente da remoto, senza dimenticare che agli utenti dei *social media* dovrebbe essere fornita anche una copia dei dati personali che li riguardano, ove richiesto.

L'interessato ha il diritto di conoscere l'identità del *targeter* ed i titolari devono facilitare l'accesso alle informazioni riguardanti il *targeting*, inclusi i criteri di *targeting* utilizzati, nonché le altre informazioni richieste dall'art. 15 GDPR.

L'utente dovrà inoltre avere accesso anche alle informazioni sui destinatari o categorie di destinatari a cui i dati personali sono stati o saranno divulgati, in particolare destinatari in paesi terzi o organizzazioni internazionali. Peraltro, un targeter non sarà necessariamente un "destinatario" dei dati personali poiché i dati personali potrebbero non essergli stati comunicati, ma riceverà statistiche dei clienti target in forma aggregata o anonima, ad esempio come parte della sua campagna o in una revisione delle prestazioni della stessa. Tuttavia, nella misura in cui il *targeter* agisce come contitolare del trattamento, deve essere identificato come tale per l'utente dei *social media*.

5. La valutazione dell'impatto sulla protezione dei dati (DPIA)

Prima di avviare le operazioni di targeting previste, entrambi i contitolari del trattamento dovrebbero controllare l'elenco delle operazioni di trattamento "che potrebbero comportare un rischio elevato" per determinare se il *targeting*

designato corrisponda a uno qualsiasi dei tipi di operazioni di trattamento soggette all'obbligo di condurre una preventiva DPIA.

In alcuni casi, la natura del prodotto o del servizio pubblicizzato, il contenuto del messaggio o il modo in cui viene fornito potrebbero infatti produrre effetti sugli individui il cui impatto deve essere accuratamente valutato sulla base delle finalità della campagna pubblicitaria e della sua invadenza, in ragione dell'eventuale trattamento di dati personali osservati, dedotti o derivati oppure, ancora, nel caso in cui gli effetti si possano ripercuotere su soggetti vulnerabili.

Quando l'operazione di trattamento coinvolge i contitolari, i rispettivi obblighi devono essere definiti con precisione ed entrambi i contitolari del trattamento devono valutare se sia necessaria la DPIA. Teoricamente entrambi i contitolari devono prendere parte alla realizzazione della DPIA e pertanto disporre di un livello sufficiente di informazioni sul trattamento, circostanza peraltro non sempre agevolmente realizzabile, soprattutto nel caso di contitolarità con un *social network*.

All'atto pratico, i contitolari del trattamento poteranno comunque decidere chi tra loro debba essere incaricato di eseguire la DPIA, indipendentemente dal permanere del riparto delle rispettive responsabilità.

Ogni DPIA dovrà evidentemente includere l'indicazione delle misure previste per affrontare i rischi, le misure di sicurezza ed i meccanismi per garantire la protezione dei dati personali e per dimostrare la conformità con il GDPR, tenendo conto dei diritti e degli interessi legittimi degli interessati. Naturalmente, nel caso in cui, all'esito della valutazione, permangano rischi elevati, ciascun titolare dovrà provvedere ad una consultazione preventiva con le autorità di controllo competenti e, nel caso in cui persista il contrasto con il GDPR, perché i rischi non sono stati sufficientemente identificati o mitigati, le operazioni di *targeting* non dovrebbero aver luogo.

6. Le categorie particolari di dati

Il GDPR fornisce una protezione specifica per particolari categorie di dati personali che includono i dati sulla salute di una persona, l'origine razziale o etnica, la biometria, le convinzioni religiose o filosofiche, le opinioni politiche, l'appartenenza sindacale, la vita sessuale o l'orientamento sessuale.

Nel contesto dei *social media* e del *targeting*, è dunque necessario determinare se il trattamento dei dati personali coinvolge categorie particolari di dati e se tali dati sono elaborati dal fornitore di *social media*, dal *targeter* o da entrambi e determinare se e a quali condizioni gli stessi soggetti possano trattare legalmente tali dati.

Se il fornitore di *social media* tratta categorie particolari di dati per scopi di targeting, è tenuto ad individuare una base giuridica ai sensi dell'art. 6 GDPR o fare affidamento su un'esenzione di cui all'art. 9, par. 2 GDPR, come il consenso esplicito. Nel caso in cui il *targeter* si avvalga della collaborazione di un fornitore di *social media*, richiedendo che questo si rivolga agli utenti trattando

anche categorie particolari di dati, il *targeter* sarà corresponsabile con il fornitore di *social media* per il predetto trattamento.

Accanto alle categorie particolari di dati esplicite, come ad esempio nel caso di una dichiarazione da parte di una persona che fa parte di un determinato partito politico o associazione religiosa, ci sono delle categorie particolari di dati che sono il prodotto di una deduzione o di una combinazione di dati, come nel caso di una persona che potrebbe votare per un determinato partito dopo aver visitato una pagina in cui predica opinioni liberali. Come evidenziato dall'EDPB, la profilazione può determinare il trattamento di categorie particolari di dati tramite inferenza da dati che non appartengono a detta categoria particolare di per sé, ma lo diventano se combinata con altri dati. Ad esempio, potrebbe essere possibile dedurre lo stato di salute di qualcuno dai registri della spesa alimentare combinata con i dati sulla qualità e il contenuto energetico degli alimenti . Oppure, ancora, l'elaborazione di una semplice dichiarazione, o di un singolo dato di posizione può rivelare che un utente ha visitato un luogo tipicamente visitato da persone con determinate credenze religiose benché il dato, di per sé, possa non rientrare nella categoria di dati particolari.

Tuttavia, un dato può essere considerato appartenente a una categoria particolare se questo dato sia combinato con altri dati a causa del contesto in cui i dati vengono elaborati o delle finalità per le quali vengono utilizzati. Se un fornitore di *social media* o un *targeter* utilizza i dati osservati per classificare gli utenti come aventi determinate convinzioni religiose, filosofiche o politiche, indipendentemente dal fatto che la categorizzazione sia corretta o veritiera, questa categorizzazione dell'utente deve essere valutata come elaborazione di una categoria particolare dei dati personali.

Sul punto parte opportuno evidenziare che l'art. 9, par. 2, lett. e), GDPR consente il trattamento di categorie particolari di dati nei casi in cui questi siano stati "manifestamente" resi pubblici dall'interessato. Tale avverbio implica che ci deve essere una soglia elevata per fare affidamento su questa esenzione.

Sarà dunque necessaria una valutazione caso per caso che tenga in debito conto le seguenti circostanze:

1) se l'interessato ha intrapreso un'azione specifica per modificare le impostazioni private predefinite della piattaforma del *social media*;

2) se la piattaforma è intrinsecamente collegata all'idea di connettersi con stretti conoscenti della persona interessata o creare relazioni intime (come le piattaforme di appuntamenti *online*), o se, al contrario, è finalizzata ad instaurare relazioni interpersonali di più ampia portata, come relazioni professionali o *microblogging*, condivisione di media, piattaforme sociali per condividere recensioni *online*, ecc.;

3) se le informazioni sono pubblicamente accessibili o se, ad esempio, è necessaria la creazione di un *account* prima di accedere alle informazioni;

4) se l'interessato viene propriamente informato che le informazioni saranno rese pubbliche;

5) se l'interessato ha pubblicato personalmente categorie particolari di dati o se invece tali dati sono stati pubblicati da una terza parte (ad esempio una foto pubblicata da un amico che rivela categorie particolari di dati).

L'EDPB rileva che la presenza di un singolo elemento potrebbe non essere sempre sufficiente per stabilire che i dati siano stati "manifestamente" resi pubblici dall'interessato e potrebbe essere necessario prendere in considerazione una combinazione di altri elementi affinché i titolari del trattamento dimostrino che l'interessato abbia chiaramente manifestato l'intenzione di rendere pubblici i dati.

7. Contitolarità e responsabilità

Come accennato, l'art. 26, par. 1, GDPR, richiede ai contitolari del trattamento di determinare in un accordo, in modo trasparente, le rispettive responsabilità, in merito al rispetto degli obblighi del GDPR, incluso l'ottemperamento al requisito della trasparenza, in modo da ricomprendervi tutti i trattamenti di cui sono contitolari.

Al tal fine, sia il fornitore di *social media* che il *targeter* devono disporre di informazioni sufficientemente dettagliate sulle specifiche operazioni di trattamento dei dati in atto. L'accordo tra il *targeter* e il fornitore di *social media* dovrà quindi contenere (o fare riferimento a) tutte le informazioni necessarie per consentire a entrambe le parti di adempiere ai loro obblighi ai sensi del GDPR, incluso il dovere di rispettare i principi di cui all'art. 5, par. 1, GDPR e di dimostrarne la loro conformità.

L'EDPB ritiene inoltre che le finalità del trattamento e la corrispondente base giuridica dovrebbero riflettersi anche nell'accordo congiunto tra destinatari e fornitori di *social media* contitolari del trattamento. Sebbene il GDPR non precluda ai contitolari di utilizzare basi legali diverse per le diverse operazioni di trattamento che svolgono, vi è la raccomandazione di utilizzare, quando possibile, la stessa base giuridica per un particolare strumento di *targeting* per la singola finalità. Se infatti ogni fase del trattamento fosse trattata su una base giuridica diversa, l'esercizio dei diritti per l'interessato risulterebbe impraticabile (ad esempio per una fase ci potrebbe essere il diritto alla portabilità dei dati, per un'altra il diritto di obiezione).

Nel caso in cui il *targeter* desideri utilizzare i dati personali forniti dall'interessato per indirizzare gli annunci sui *social media*, dovrà adottare misure appropriate per garantire che i dati forniti non siano ulteriormente utilizzati dal fornitore di *social media* in un modo che sia incompatibile con tali finalità, (salvo che non sia stato ottenuto il valido consenso dell'interessato). Allo stesso modo, il fornitore di *social media* deve garantire che l'uso dei dati per scopi di *targeting* da parte dei destinatari sia conforme ai principi di limitazione delle finalità, trasparenza e liceità.

Può inoltre accadere che i destinatari che desiderano utilizzare strumenti di *targeting* forniti da un fornitore di *social media* possono trovarsi di fronte alla

necessità di aderire ad accordi predefiniti, senza alcuna possibilità di negoziare o apportare modifiche. Secondo l'EDPB, tale situazione non fa venir meno la responsabilità congiunta del fornitore di *social media* e del *targeter* ed entrambi i contitolari sono inoltre tenuti a garantire che l'attribuzione delle responsabilità rifletta debitamente i rispettivi ruoli.

Indipendentemente da quanto pattuito nell'accordo di contitolarità, ciascun titolare rimane, in linea di principio, responsabile della conformità del trattamento. Tuttavia, il grado di responsabilità del *targeter* e del fornitore di *social media* in relazione a obblighi specifici può variare: benché i contitolari del trattamento siano entrambi responsabili del rispetto degli obblighi previsti dal GDPR e l'interessato possa esercitare i propri diritti nei confronti di ciascuno dei titolari, il loro livello di responsabilità deve essere valutato in base al loro ruolo effettivo nel trattamento.

A tal fine, i fattori rilevanti concernono la capacità di influenzare il trattamento a livello pratico, la conoscenza effettiva di ciascuno dei contitolari, la fase del trattamento e in quale misura o in che grado il *targeter* e il fornitore di *social media* sono responsabili del trattamento.

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

I principali ruoli privacy alla luce delle recenti Linee Guida dell'EDPB

SOMMARIO: 1. Titolare del trattamento – 2. Responsabile del trattamento – 3. Rapporto titolare-responsabile: designazione e documentazione contrattuale – 4. Subresponsabile del trattamento e documentazione contrattuale – 5. Contitolare del trattamento – 5.1 Nozione e inquadramento normativo – 5.2 Accordo di contitolarità – 5.3 Casistica – 6. Ruoli privacy interni – 6.1 L'autorizzato – 6.2 Il designato – 6.3 Il delegato

1. Titolare del trattamento

L'EDPB (European Data Protection Board), con le proprie Linee guida n. 7/2020 (*Guidelines on the concepts of controller and processor in the GDPR*, adottate il 2 settembre 2020 e soggette a consultazione pubblica, di seguito "**Linee Guida**")[18], si sofferma dapprima sul concetto di Titolare del trattamento, ponendosi l'obiettivo di dare una certa concretezza alla sua definizione al fine di chiarire possibili dubbi sulla sua qualificazione soggettiva e sulla centralità del suo ruolo sia rispetto alle funzioni che gli spettano sia con riferimento agli obblighi che gli competono, anche in rapporto con il Responsabile del trattamento[19].

Il punto di partenza da cui muove l'EDPB per inquadrare correttamente ciascun soggetto coinvolto nelle operazioni di trattamento è quello di interpretare i diversi ruoli sulla base di due criteri, quello della funzionalità e quello dell'autonomia: in altri termini, l'individuazione di ciascuna figura deve avvenire principalmente alla luce della normativa europea sulla protezione dei dati e

18 Alla data attuale, il testo definitivo delle Linee Guida all'esito della consultazione non è ancora stato reso pubblico dall'EDPB.

19 Come noto, con il nuovo Regolamento UE, il Titolare 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. A tal fine, il GDPR istituisce un nuovo quadro a tutela della privacy: da un lato, rafforzando i vecchi obblighi a carico del Titolare del trattamento; dall'altro, introducendone di nuovi, sopprimendo e ridefinendo talune previsioni alla luce del diverso approccio richiesto ai titolari del trattamento, nel rispetto dei principi di cui all'art. 5 GDPR (in particolare, quelli di *accountability,* minimizzazione, *privacy by default e by design*). In questo modo il Titolare viene dotato di tutti gli strumenti idonei a consentirgli, per un verso, di effettuare le corrette valutazioni e analisi sia sui rischi connessi alle attività di trattamento; per altro verso, di individuare le citate misure tecniche e organizzative idonee a mitigare tali rischi.

basarsi su un approccio fattuale, del tutto svincolato da designazioni formali, che passa quindi dall'esame dei ruoli effettivamente svolti dalle parti[20].

Ciò chiarito e venendo alla definizione di Titolare del trattamento contenuta nel GDPR e richiamata nelle Linee Guida, ai sensi dell'art. 4 (7) del GDPR, il Titolare è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*".

In base quindi alle indicazioni fornite dal GDPR, il Titolare è il soggetto che **decide gli elementi chiave delle attività di trattamento**: le finalità e i mezzi, ovvero il perché e il come del trattamento e li determina entrambi. In particolare, la definizione di Titolare si compone di cinque elementi chiave: (*i*) "*la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo*", (*ii*) "*determina*", (*iii*) "*da sola o congiuntamente ad altri*", (*iv*) "*le finalità e i mezzi*", (*v*) "*del trattamento dei dati personali*".

Quanto al primo profilo, l'EDPB precisa che, in base a quanto previsto dal legislatore europeo, non viene posta alcuna limitazione alla tipologia di entità potenzialmente in grado di ricoprire il ruolo di Titolare. Ciò vuol dire che il Titolare potrà dunque essere indistintamente la singola persona fisica, l'associazione di persone o la persona giuridica o altro organismo, intendendo in tali ultimi casi, l'ente nel suo complesso e non la persona fisica rappresentante dell'ente (es. amministratore delegato o consiglio di amministrazione) a cui eventualmente è possibile effettuare solo una delega di funzioni che dovrebbero essere svolte dal Titolare nel suo complesso. Principi, questi, del tutto in linea con quanto affermato su tale tema anche dal Garante per la protezione dei dati personali ("**Garante**") laddove ha avuto occasione di precisare che "*il riferimento alla "persona fisica" , che compare nella definizione del "titolare" (…), non riguarda coloro che amministrano o rappresentano la persona giuridica, la pubblica amministrazione o l´ente, ma concerne gli individui che effettuano un trattamento di dati a titolo personale (ad esempio, il libero professionista, il piccolo imprenditore), e che assumono individualmente la piena responsabilità di un´attività che va distinta nettamente, anche sul piano giuridico, da quella che singole persone fisiche possono coordinare nell´ambito e nell´interesse di una persona giuridica, di un´impresa o di un ente nel quale ricoprono incarichi di rilievo*"[21]. Peraltro, l'orientamento suesposto è pacifico anche in ambito europeo: a tal riguardo, l'EDPB richiama una vicenda giunta all'e-

20 Le Linee Guida, p. 3, affermano: "*The concepts of controller, joint controller and processor are functional concepts in that they aim to allocate responsibilities according to the actual roles of the parties and autonomous concepts in the sense that they should be interpreted mainly according to EU data protection law*".

21 Precisa ancora il Garante, "*In altre parole, qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il "titolare" è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.) anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante ecc.).", cfr. il provvedimento "Titolare, responsabile e incaricato – individuazione del "titolare del trattamento"" – 9 dicembre 1997* (doc. web n. 39785).

same della Corte di Giustizia dell'Unione Europea, in occasione della quale ha qualificato l'intera comunità religiosa, insieme ai propri fedeli, Titolare[22].

Il secondo elemento chiave del concetto di Titolare, ovvero il verbo "*determina*", si riferisce all'"influenza" del Titolare sull'attività di trattamento, in virtù dell'esercizio di un potere decisionale. Tale elemento è quello che contraddistingue la figura del Titolare da quella del Responsabile. Per verificare la sussistenza di tale influenza/controllo sul trattamento, occorre procedere, come detto, con un'analisi fattuale piuttosto che formale[23]. Ed è in questo contesto che l'EDPB ritiene di dover distinguere tra due tipologie di controllo: (**a**) il controllo derivante da disposizioni di legge; e (**b**) il controllo derivante da una concreta influenza fattuale e cioè dall'attento esame **delle circostanze del caso**.

Secondo quanto chiarito dall'EDPB, sono da considerarsi Titolari sulla base della prima classificazione quelli che vengono esplicitamente designati come tali dall'ordinamento (citando l'esempio riportato nelle Linee Guida, è il caso di un'entità a cui la legge affida determinati compiti pubblici, come, per esempio la sicurezza, che possono essere svolti solo raccogliendo dati personali o utilizzando una banca dati[24]). Nell'ambito, invece, della seconda tipologia di controllo, rientrano sia i Titolari che effettuano determinate attività di trattamento perché strettamente collegate e necessarie all'esercizio delle proprie funzioni/attività, anch'esse attribuite dalla legge (ad esempio, un datore di lavoro per i dipendenti, un editore per gli abbonati)[25]; sia i Titolari che vengono qualificati come tali **sulla base dell'esame delle circostanze concrete**: sul punto le Linee Guida precisano che una valutazione dei termini contrattuali tra le diverse parti interessate **può facilitare** la determinazione di quale parte (o parti) agisce (o agiscono) in qualità di Titolare[26]; tuttavia, in altri casi, occorrerà far riferimento ad altri e ulteriori elementi laddove il dato contrattuale non rifletta la realtà dei fatti ed esuli dall'effettivo ruolo di influenza esercitato dalle parti sul trattamento.

Il terzo elemento fa riferimento all'eventualità di un rapporto di contitolarità nella determinazione di finalità e modalità del trattamento, ritenendo

22 Si tratta della sentenza della Corte di Giustizia UE del 10 luglio 2018 emessa nell'ambito della causa C-25/17, "*Jehovah's witnesses*".

23 Su tale profilo cfr. anche il Parere del 22 gennaio 2019 in occasione del quale il Garante, nel chiarire il ruolo privacy del consulente del lavoro dopo l'applicazione del GDPR, dà atto che "*L'Autorità, vigente la precedente disciplina, si è espressa sulla qualificazione in termini di titolare o responsabile di alcune figure che effettuano trattamenti di dati personali, anche nell'ambito del rapporto di lavoro, all'esito dell'esame – effettuato sul piano sostanziale e non formale – delle attività in concreto svolte" (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9080970).*

24 Cfr. sul punto Le Linee Guida, § 22.

25 L'EDPB fa rientrare in tale ultima ipotesi anche gli studi legali, dovendo necessariamente trattare, con un importante grado di indipendenza, i dati personali del proprio cliente per poter procedere con la propria attività; cfr. Le Linee Guida, p. 12.

26 Il corretto inquadramento del ruolo di Titolare e Responsabile attraverso un'analisi di tipo fattuale e non formale rileva anche sotto un altro profilo ovvero quello della riqualificazione del Responsabile come Titolare laddove il primo abbia effettivamente un potere decisionale a prescindere da quanto previsto, ad esempio, a livello contrattuale: le Linee Guida, infatti, ricordano che, ai sensi dell'art. 28 (10) del GDPR, quando un Responsabile del trattamento elabora i dati al di fuori delle istruzioni del Titolare o viola le disposizioni del Regolamento, ciò equivale a una decisione che determina le finalità e i mezzi del trattamento e sarà di conseguenza considerato un Titolare del trattamento con ogni conseguenza anche da un punto di vista sanzionatorio e risarcitorio (cfr. Le Linee guida n. 7/2020, §§ 79, 114, 146). Cfr. sul punto le Linee Guida, § 22.

in tal caso tutte le entità coinvolte egualmente soggette alle disposizioni della normativa comunitaria (ma sul punto vedi *infra*).

Con riferimento invece al quarto elemento, l'EDPB specifica che la locuzione "*le finalità ed i mezzi*" sta a significare che, per integrare la figura del Titolare è necessario che il potere decisionale esercitato da quest'ultimo riguardi non solo lo scopo del trattamento ma anche le modalità attraverso le quali il trattamento si articola. Sul punto, l'EDPB chiarisce che se da un lato le decisioni sullo scopo del trattamento debbano essere sempre di esclusiva competenza del Titolare, dall'altro la determinazione dei mezzi può essere lasciata al Responsabile del trattamento, prevedendo in questo modo "*un certo margine di manovra in capo al Responsabile del trattamento, il quale può prendere di propria iniziativa alcune limitate decisioni in relazione ai mezzi impiegati per il trattamento*"[27]. A tal fine, l'EDPB distingue tra 'mezzi essenziali' e 'mezzi non essenziali': i primi si identificano con i mezzi strettamente legati allo scopo e alla portata del trattamento, intrinsecamente riservati al Titolare (es. quali dati trattare, la durata del trattamento, categorie di destinatari), mentre i secondi riguardano gli aspetti più tecnici ed esecutivi dell'attività di trattamento, come la scelta di un particolare tipo di hardware o software o le misure di sicurezza da applicare, la cui decisione può anche essere delegata al Responsabile[28].

Infine, quanto all'ultimo requisito chiave relativo al "*trattamento di dati personali*" cui le finalità e i mezzi si riferiscono, l'EDPB, nel partire dalla sua definizione riportata dall'articolo 4 (2) del GDPR[29], chiarisce che il coinvolgimento del Titolare può essere limitato ad una singola operazione di trattamento o riguardare un insieme di operazioni. Inoltre, in perfetta aderenza con il passato, viene altresì specificato che non è necessario che il Titolare, per essere qualificato come tale, tratti effettivamente i dati personali o vi abbia accesso[30].

Alla luce di quanto detto, è evidente che l'EDPB, con le recenti Linee Guida, ha voluto rimarcare, anche in questa sede[31], come il corretto inquadramento dello status giuridico di un soggetto come "*titolare del trattamento*" o "*responsabile del trattamento*" debba avvenire, in linea di principio, sulla base dell'esame del contesto e dell'attività svolta in concreto, piuttosto che sulla qualificazione formale di tali soggetti derivante, ad esempio, da un contratto. In tale prospettiva, i casi proposti dall'EDPB evidenziano proprio l'importanza dell'analisi fattuale e del contesto per l'esatta qualificazione di tali soggetti[32].

27 Cfr. Prof. Avv. Del Ninno, "*Le Linee Guida 7/2020 del Comitato europeo sulla protezione dei dati personali sui concetti di Titolare e Responsabile del trattamento nel RGPD: riflessioni critiche e difficoltà applicative*", in *Diritto e Giustizia*, 23.12.2020, p. 9.

28 In questi stessi termini si era già espresso il WP29 (ovvero il *Working Party* art. 29, l'organismo europeo oggi sostituito dal EDPB) con il Parere 1/2010 (p. 14) sui concetti di "*titolare del trattamento*" e "*responsabile del trattamento*", sostituito dalle Linee Guida.

29 L'art. 4 (2) del GDPR definisce il «trattamento» come "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzat*i e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*"..

30 Cfr. il Parere 1/2010 del WP29, p. 23: "[…] *il fatto d'avere accesso ai dati non è un prerequisito per essere [titolare] del trattamento*".

31 Cfr. il Parere 1/2010 del WP29.

32 Tali profili erano stati affrontanti anche dal Garante, con il parere del 22 Gennaio 2019, che, nel chiarire il ruolo privacy del consulente del lavoro, ha specificato che: "*occorre dunque distinguere*

Si veda, ad esempio, il caso dei servizi forniti da una società di revisione: ove tale soggetto svolga la propria prestazione sulla base di istruzioni molto generali da parte del cliente e goda di ampia autonomia – in conformità con le leggi che regolano questa professione – nel decidere, per svolgere la propria attività, i dati da raccogliere, per quanto tempo gli stessi devono essere conservati e quali misure tecniche e organizzative devono essere adoperate, la società di revisione verrà considerata alla stregua di un Titolare. In caso contrario, nell'ipotesi in cui i revisori dovessero attenersi a istruzioni dettagliate del cliente, svolgendo un'attività più operativa e ausiliaria, in una situazione in cui la legge non stabilisce obblighi specifici, la società andrà considerata come responsabile. E ancora, si pensi alla società incaricata da un cliente di gestire i pagamenti degli stipendi dei propri dipendenti: nel caso in cui il cliente fornisca i dettagli su chi pagare, quali importi erogare e entro quale data, a quale banca riferirsi, è evidente che la società di *payroll* tratterà i dati per i soli scopi individuati dal cliente e non potrà utilizzare i dati per finalità proprie. In altri termini, sarà il cliente a individuare le finalità e i mezzi del trattamento e la società di *payroll* sarà inquadrata nell'ambito della figura del responsabile. Quand'anche la società di *payroll* abbia una certa autonomia in relazione ai mezzi da impiegare per il trattamento, come ad esempio il software da utilizzare, questo non altererà il suo ruolo di responsabile, almeno fino a quando non violi le istruzioni impartite dal cliente[33].

È evidente, quindi, che la qualifica di Titolare o Responsabile possa variare a seconda del contesto. Tuttavia, sebbene in alcuni casi sarà agevole individuare con certezza il Titolare e distinguerlo dalle altre figure privacy facendo ricorso al dettato contrattuale o al concreto svolgimento dei rapporti, in altri casi tale processo potrà risultare particolarmente difficoltoso e potrà, probabilmente, indurre anche a qualificazioni errate, con ogni conseguenza dal punto di vista sanzionatorio a seguito di un'eventuale riqualificazione da Responsabile a Titolare (cd. autonomo[34]) o Contitolare: in tale ultimo contesto, ciascun Titolare fornisce all'interessato una prestazione specifica o un particolare servizio e, insieme, rappresentano per il medesimo interessato un unico beneficio.

Per l'effetto, la comunicazione dei dati tra i diversi Titolari è necessaria per rendere all'interessato il servizio richiesto.

il segmento di attività in cui il consulente del lavoro tratta i dati nella sua qualità di professionista, attività fiscalmente e normativamente regolamentata, dalla diversa attività (tipica di questo ordine professionale) per la quale il medesimo soggetto tratta i dati dei dipendenti del cliente. Nel primo caso il consulente del lavoro agisce in piena autonomia e indipendenza determinando puntualmente le finalità e i mezzi del trattamento dei dati del cliente per il perseguimento di scopi attinenti alla gestione della propria attività. Per tali ragioni, egli ricopre il ruolo di titolare del trattamento in quanto non si limita ad effettuare un'attività meramente esecutiva di trattamento, "per conto" del cliente, bensì esercita un potere decisionale del tutto autonomo sulle finalità e i mezzi del trattamento. Nel secondo caso occorre fare riferimento alla figura del responsabile, che rimane connotata dallo svolgimento di attività delegate dal titolare il quale, all'esito di proprie scelte organizzative, può individuare un soggetto particolarmente qualificato allo svolgimento delle stesse (in termini di conoscenze specialistiche, di affidabilità, di struttura posta a disposizione, etc.), delimitando l'ambito delle rispettive attribuzioni e fornendo specifiche istruzioni sui trattamenti da effettuare" (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9080970).

33 Per un quadro più completo e per un esame dei casi enunciati dall'EDPB, cfr. Linee Guida, p. 14.

34 Nell'ipotesi in cui non sussista alcuna condivisione della finalità e dei mezzi tra i soggetti privacy coinvolti non vi sarà contitolarità ma vi saranno, se del caso, rapporti tra autonomi titolari o tra titolare e responsabile – cfr. Linee Guida, §§ 60 e 66.

2. Responsabile del trattamento

Il Responsabile è definito dall'art. 4 (8) del GDPR come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

Le Linee Guida[35] precisano che non ci sono particolari limiti ai soggetti, che possono assumere tale ruolo: possono essere persone fisiche, giuridiche o altri organismi.

Tuttavia, l'EDPB delinea **due condizioni** necessarie per la qualifica di un soggetto, quale Responsabile del trattamento dei dati: (1) essere un'entità separata rispetto al Titolare e (2) trattare i dati personali sulla base di istruzioni del Titolare.

In particolare, l'EDPB conferma che il Responsabile possa essere solo esterno all'organizzazione del Titolare (eliminando in modo definitivo la possibilità di nominare un responsabile interno all'organizzazione prevista dal precedente Codice Privacy italiano[36]). A questo proposito, l'EDPB stabilisce in modo chiaro che una società appartenente ad un gruppo di imprese possa ricoprire il ruolo di Responsabile di un'altra società appartenente allo stesso gruppo, purché siano entità distinte; tuttavia, uno specifico dipartimento interno appartenente alla società Titolare non può svolgere generalmente il ruolo di Responsabile.

L'EDPB precisa, inoltre, che anche i dipendenti della società Titolare, che trattano dati personali non possano essere qualificati come Responsabili, in quanto il trattamento dei dati è effettuato come parte dell'organizzazione interna del Titolare.

L'EDPB conferma che il **Responsabile debba agire in nome e per conto del Titolare e seguire le specifiche istruzioni dallo stesso impartite** con riferimento al trattamento dei dati personali ed è, pertanto, esclusa la possibilità per il Responsabile di trattare i dati personali per sue specifiche finalità. L'EDPB ha elaborato un esempio pratico relativo all'applicazione di tale concetto: una società di servizi che si occupa della gestione della pubblicità e del marketing diretto per una determinata società (a seguito della conclusione di uno specifico contratto che regola i termini del trattamento dei menzionati dati personali dei clienti della società Titolare), che decide di utilizzare i dati dei clienti del Titolare per sviluppare il proprio business, viene considerata come Titolare per tali determinate attività, che non risultano coperte dalle istruzioni del Titolare. Tale comportamento del Responsabile è considerato come una violazione delle norme del GDPR ed anche del contratto sottoscritto con la società Titolare[37].

L'EDPB precisa, infine, che il ruolo di Responsabile dipende anche delle attività concrete effettuate e dal contesto specifico e non solo dal fatto che sia

35 Cfr. sul punto le Linee Guida, p. 24 e seguenti.

36 Cfr. Prof. Avv. Del Ninno, "*Le Linee Guida 7/2020 del Comitato europeo sulla protezione dei dati personali sui concetti di Titolare e Responsabile del trattamento nel RGPD: riflessioni critiche e difficoltà applicative*", in *Diritto e Giustizia*, 23.12.2020, p. 14.

37 Cfr. sul punto le Linee Guida, p. 25.

un'entità separata rispetto al Titolare. In particolare, se il trattamento dei dati personali non è un elemento chiave del servizio offerto e il soggetto non ha come attività specifica il trattamento degli stessi, potrebbe essere qualificato come Titolare e non Responsabile. Anche in tal caso, l'EDPB elabora un esempio chiaro dell'applicazione di tale principio: una società di trasporti (taxi) offre il servizio di *pick-up* per dipendenti od ospiti da e verso l'aeroporto tramite una piattaforma *on-line*. La prenotazione dei *pick-up* è solitamente effettuata per i dipendenti o gli ospiti dalla società datrice di lavoro o ospitante, che comunica anche il nome della persona fisica che usufruirà del trasporto, in tal modo l'autista può verificare l'identità della persona per cui è stato prenotato il servizio. In questo caso, vengono processati i dati personali da parte della società di trasporti come parte del proprio servizio offerto alla società, anche se non corrisponde al servizio principale offerto, che è quello di trasporto. In questo caso la società di trasporti agisce quale Titolare, anche se tale trattamento è stato generato dalla richiesta di una società cliente; di fatti la società di trasporti ha programmato il servizio di prenotazione in modo autonomo per lo sviluppo del proprio business e pertanto è considerata quale Titolare[38].

L'EDPB sottolinea che il fornitore di servizi può essere considerato come Responsabile anche se non è il principale obiettivo del suo servizio, a condizione che il cliente determini in pratica lo scopo e i mezzi di tale trattamento. L'EDPB elabora diversi esempi rispetto a tale principio[39], in particolare:

(1) una società X esternalizza la propria funzione di supporto clienti alla società Y, che fornisce un servizio di call center per rispondere alle richieste dei clienti della società X. La società Y per poter dare tale supporto può accedere al data base della società X. La società Y è legittimata ad accedere a tale data base solo per eseguire le proprie funzioni di supporto cliente e non per altri scopi. In tale caso, la società Y è considerata quale Responsabile, che comporta la stipula di un apposito contratto tra le due società.

(2) una società usufruisce del servizio di assistenza di un provider informatico, che ha accesso sistematicamente a molti dati personali di cui la società è Titolare. L'accesso ai dati personali non è la principale attività fornita dal provider informatico e pertanto viene considerato un Responsabile, che è obbligato ad accedere ai dati per poter fornire il proprio servizio. In questo caso, è necessario stipulare un apposito contratto tra le due società.

(3) una società assume uno specialista informatico da un'altra società per sistemare un bug nel proprio software. Lo specialista non è stato assunto per trattare dati personali e ogni accesso a tali dati è incidentale e casuale e dunque nella pratica molto limitato. In tal caso lo specialista informatico non può essere considerato come un Responsabile, ma nemmeno un Titolare autonomo e la società dovrà adottare apposite misure tecniche per evitare che lo specialista possa anche solo incidentalmente trattare

38 Cfr. sul punto le Linee Guida, p. 25.

39 Cfr. sul punto le Linee Guida, p. 26.

in modo non autorizzato i dati personali raccolti dalla società Titolare del trattamento.

Infine, l'EDPB afferma che il Titolare deve sempre prendere la decisione finale in merito al trattamento dei dati personali e istruire il Responsabile e/o chiedere le opportune modifiche anche nel caso in cui quest'ultimo proponga un'offerta predefinita e seriale[40].

3. Rapporto titolare-responsabile: designazione e documentazione contrattuale

L'EDPB dedica poi una parte delle Linee Guida al rapporto tra Titolare e Responsabile e alla regolamentazione dello stesso. Come noto, l'art. 28 del GDPR impone al Titolare di ricorrere unicamente a Responsabili che presentino garanzie sufficienti per implementare misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato. Tale indagine, in base a quanto riportato nelle Linee Guida, equivale ad un vero e proprio *risk assessment*, durante la quale il Titolare è tenuto a prendere in considerazione (*i*) le conoscenze specialistiche del Responsabile (ad es. competenza tecnica in materia di misure di sicurezza e violazioni dei dati); (*ii*) la sua affidabilità e (*iii*) le risorse in suo possesso. Anche il profilo reputazionale può essere un aspetto rilevante ai fini della designazione del Responsabile.

Il rapporto tra Titolare e Responsabile deve essere regolato da un contratto o da un atto che abbia potere di vincolare le parti secondo la normativa dello Stato Membro e che deve essere provato per iscritto. A tal fine, i Responsabili possono scegliere di negoziare ogni singola clausola oppure di utilizzare, in tutto o in parte, delle clausole contrattuali standard[41], ciò che rileva è che includano gli elementi richiesti dall'art. 28 del GDPR[42], ma evitando di riportare pedissequamente il dettato normativo, quanto piuttosto includendo informazioni specifiche e concrete su come i requisiti richiesti dall'art. 28 del GDPR sono rispettati, nonché il livello di sicurezza richiesto per lo specifico trattamento di dati personali oggetto del contratto. Peraltro, ai fini della qualificazione dei

40 Cfr. sul punto le Linee Guida, p. 26.

41 Nel novembre 2020 la Commissione europea ha predisposto una bozza di clausole contrattuali standard per regolare, ai sensi dell'articolo 28 del GDPR, il rapporto contrattuale tra Titolare e Responsabile. La versione definitiva sarà adottata dalla Commissione UE nei primi mesi del 2021 (è possibile consultare la bozza al seguente link: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Commission-Implementing-Decision-on-standard-contractual-clauses-between-controllers-and-processors-located-in-the-EU). Si segnala altresì che l'EDPB e l'EDPS (*European Data Protection Supervisor*) hanno espresso parere favorevole sulle clausole contrattuali standard quale strumento per regolare i rapporti tra Titolare e Responsabile e hanno proposto una serie di emendamenti alla bozza volti, tra le altre cose, a rendere il più chiaro possibile i ruoli e le responsabilità di ciascuna delle parti coinvolte in relazione a ciascuna attività di trattamento. Inoltre, l'EDPB e l'EDPS chiariscono che l'applicazione di tali clausole riguarderanno le situazioni che comportano trasferimenti solo all'interno dell'UE.

42 Dal momento che l'accordo Titolare-Responsabile va inevitabilmente replicato tra Responsabile-Subresponsabili è evidente che quanto più risulta personalizzato il primo accordo tanto più difficile sarà conformare i Subresponsabili alle prescrizioni di dettaglio vigenti tra Titolare-Responsabile. Di conseguenza, le clausole standard rappresentano la soluzione migliore per far funzionare i rapporti a cascata e i correlati accordi.

rispettivi ruoli non ha importanza se il testo di accordo è predisposto da una o dall'altra parte: la prassi conferma, infatti, che in molti casi i fornitori di servizi, Responsabili del trattamento, stabiliscono servizi e contratti standard da far firmare ai Titolari. A tale proposito l'EDPB specifica che il fatto che il contratto e le sue condizioni generali siano preparate dal fornitore di servizi invece che dal Titolare, in primo luogo, non basta in sé per far concludere che il fornitore di servizi debba essere considerato come un titolare, e in secondo luogo, comporta che il Titolare, nella misura in cui ha liberamente accettato le clausole contrattuali, ne assuma di conseguenza la piena responsabilità. Analogamente, lo squilibrio fra il potere contrattuale di un piccolo Titolare del trattamento rispetto a un grosso fornitore di servizi non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati.

Le Linee Guida forniscono anche una piccola guida pratica su come redigere il contratto ex art. 28 del GDPR. In particolare, come già accennato, l'EDPB chiarisce che l'atto di designazione a Responsabile dovrebbe contenere, oltre alle prescrizioni previste dalla normativa europea, ulteriori e specifiche previsioni, già in uso nella prassi. Segnatamente, seguendo quanto riportato nelle Linee Guida, andrà specificato quanto segue:

- L'**oggetto del trattamento**, ad esempio, registrazioni di videosorveglianza di persone; entrare e uscire da una struttura ad alta sicurezza.
- La **durata del trattamento** ovvero l'esatto periodo di tempo oppure i criteri utilizzati per **determinarlo**, da parametrarsi, ad esempio, alla durata del contratto sul trattamento dei dati personali, anche se potrebbero esserci obblighi di legge che impongono periodi di conservazione dei dati più lunghi o più brevi del tutto svincolati dal contratto. Infatti, è lo stesso EDPB a chiarire che la durata del trattamento non è necessariamente equivalente alla durata del contratto sul trattamento dei dati[43].
- La **natura del trattamento** ovvero il tipo di operazioni svolte nell'ambito del trattamento (per esempio: "riprese", "registrazione"...) e le **finalità del trattamento**.
- La **tipologia di dati personali**, evitando riferimenti generici alle norme (ad esempio "*dati personali ai sensi dell'articolo 4, paragrafo 1, GDPR"* o *"speciali categorie di dati personali ai sensi dell'articolo 9*") e cercando di essere quanto più specifici e dettagliati possibili.
- Le **categorie di soggetti interessati**.

43 Cfr. sul punto le Linee Guida, p. 33.

- Gli **obblighi e i diritti del Titolare**: quanto ai diritti, si tratta ad esempio del diritto del Titolare di eseguire ispezione e audit presso il Responsabile. Quanto agli obblighi, occorre che il Titolare fornisca al Responsabile (e documenti se del caso per iscritto[44]) le istruzioni relative al trattamento dei dati che quest'ultimo è tenuto ad effettuare.
- Nel caso di **trasferimento di dati personali all'estero**, sarà opportuno che il contratto specifichi sulla base di quali misure e garanzie avviene tale trasferimento, tenendo conto di quanto previsto dal Capo V del GDPR. Quindi, il Responsabile sarà tenuto ad astenersi dal trasferire dati all'estero in assenza di istruzioni specifiche sul punto da parte del Titolare o di una sua autorizzazione.
- Le **misure di sicurezza** adottate dal Responsabile: in termini generali, il Titolare deve fornire al Responsabile del trattamento una descrizione delle attività di trattamento e degli obiettivi di sicurezza, nonché approvare le misure proposte dal responsabile del trattamento.
- La **gestione delle richieste relative all'esercizio dei diritti** da parte degli interessati: sebbene la gestione pratica delle singole richieste possa essere affidato in outsourcing al Responsabile, il Titolare resta il soggetto responsabile nei confronti dell'interessato dell'adempimento di tali richieste. Di conseguenza, è opportuno che il contratto contenga i dettagli riguardanti l'assistenza che deve essere fornita dal Responsabile.
- La gestione del **data breach**: il Responsabile deve assistere il Titolare nell'adempiere all'obbligo di notifica delle violazioni dei dati personali all'autorità di controllo e ai soggetti interessati. L'EDPB, quindi, raccomanda di prevedere nel contratto tempi e modalità della notifica da parte del Responsabile al Titolare ove si verifichi una violazione dei dati presso la struttura del primo, nonché i dettagli di contatto per le eventuali notifiche.

Come già detto, il Responsabile viola il GDPR se va oltre le istruzioni conferite dal Titolare: in questo caso, il Responsabile sarà considerato a propria volta un Titolare e, da un lato, sarà passibile di sanzione amministrativa pecuniaria nella misura prevista dall'art. 83 del GDPR; dall'altro, risponderà per il danno cagionato all'interessato.

4. Subresponsabile del trattamento e documentazione contrattuale

La gestione del trattamento dei dati personali è svolta da molti soggetti, tra cui i Subresponsabili del trattamento. Tale figura è disciplinata dall'art. 28 (2)

44 Poiché anche tali istruzioni devono essere documentate, l'EDPB precisa di includere allegare le istruzioni in un allegato al contratto sul trattamento dei dati o ad altro atto giuridico. In termini generali, le istruzioni possono essere fornite in qualsiasi forma scritta (ad esempio e-mail), purché siano conservate su supporto documentale e, per evitare qualsivoglia difficoltà nel documentare tali istruzioni, l'EDPB raccomanda di conservarle unitamente al contratto o altro atto legale - cfr. le Linee Guida, p. 34.

del GDPR[45]. Anche l'EDPB nelle Linee Guida ha dedicato alcune riflessioni rispetto alla procedura di nomina e alla relativa documentazione contrattuale.

In particolare, è prevista la **preventiva autorizzazione scritta** da parte del Titolare al coinvolgimento di un Subresponsabile da parte del Responsabile. Tale principio è nell'ottica di voler sempre più responsabilizzare il Titolare, che deve essere informato con riferimento ad ogni singola fase del trattamento dei dati personali da parte di altri soggetti.

L'EDPB detta una serie di indicazioni specifiche con riferimento al procedimento di approvazione dei Subresponsabili e, in particolare, stabilisce che anche la nomina del Subresponsabile deve essere regolata da un contratto o almeno essere inserita all'interno del contratto tra Titolare e Responsabile.

L'EDPB considera valida la nomina di un Subresponsabile, ove il Responsabile abbia ottenuto una specifica autorizzazione o una autorizzazione generale scritta da parte del Titolare. È necessario scegliere la modalità di nomina di un Subresponsabile già nel contratto stipulato tra Titolare e Responsabile.

In particolare, se si è scelta l'**autorizzazione specifica**, allora il Responsabile dovrà ricevere dal Titolare un'autorizzazione scritta avente ad oggetto l'approvazione del singolo Subresponsabile, l'elenco dei trattamenti, che può effettuare e la durata. Ogni successivo cambiamento dovrà essere approvato dal Titolare. Nel caso in cui il Titolare non si esprima in merito alla richiesta di autorizzazione specifica nel tempo stabilito, il silenzio dovrà essere considerato come silenzio-rifiuto e, pertanto, il Responsabile non potrà ricorrere all'attività del Subresponsabile, in quanto non autorizzata.

Nell'**autorizzazione generale** a usare dei Subresponsabili, inserita direttamente nel contratto tra Titolare e Responsabile a cui è allegata anche la lista specifica dei Subresponsabili (che contiene oltre alla denominazione anche la sede legale, nonché la descrizione delle attività e le misure di sicurezza implementate), devono essere aggiunti anche i criteri guida per la scelta del Subresponsabile (es. garanzie in termini di misure tecniche ed organizzative di sicurezza, esperienza ricercata, affidabilità e risorse). Nel caso in cui il Titolare non si esprima in merito all'effettiva attivazione della autorizzazione generale concessa nel tempo stabilito, il silenzio dovrà essere considerato come silenzio-assenso e pertanto il responsabile potrà ricorrere all'attività del Subresponsabile, in quanto autorizzata.

In ogni caso, è necessario inserire nel contratto tra Titolare e Responsabile le tempistiche (che devono essere ragionevoli) e le modalità di comunicazione dell'approvazione dei Subresponsabili da parte del Titolare (è utile anche inserire un modello di richiesta e comunicazione).

45 Cfr. Art. 28 (2) del GDPR: "[…] *Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche*".

L'EDPB richiama l'art. 28 (4) del GDPR[46] e ribadisce che il Responsabile risponde nei confronti del Titolare per le obbligazioni del Subresponsabile. Inoltre, il Responsabile che decide di iniziare a lavorare con un Subresponsabile autorizzato deve a sua volta stipulare un contratto, che contenga gli stessi obblighi imposti al Responsabile. Con tale espressione, l'EDPB intende che non è necessario nel contratto includere esattamente le stesse parole utilizzate nel contratto tra Titolare e Responsabile, ma deve essere certo che gli obblighi siano gli stessi anche se espressi con parole diverse. L'EDPB sottolinea anche che il Responsabile, nel caso in cui incarichi un Subresponsabile per determinate attività, a cui non è possibile applicare determinati obblighi gravanti sul responsabile, non è legittimato ad inserire tali obblighi anche nel contratto con il Subresponsabile, altrimenti genererebbero disparità ed incertezza.

Il principio ribadito dall'EDPB è che tutta la catena di attività che implica il trattamento dei dati personali da parte di tutti i soggetti coinvolti debba essere regolata mediante contratti scritti.

5. Contitolare del trattamento

5.1 Nozione e inquadramento normativo

Accanto alla figura del Titolare il GDPR ha introdotto quella dei Contitolari del trattamento ("**Contitolari**")[47]. Tale figura - del tutto nuova rispetto a quelle cui eravamo abituati e previste dal D. Lgs. 196/2003 ("**Codice Privacy**") - trova una sua precisa disciplina all'interno dell'art. 26 del GDPR, in cui viene espressamente sancito che "*allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento […]*".

Affinché, quindi, si possa parlare di contitolarità, è necessario che la determinazione di finalità e mezzi del trattamento venga stabilita congiuntamente [48] da due o più Titolari. Ma cosa si intende esattamente per determinazione congiunta e quando si configura?

46 Cfr. Art. 28 (4) del GDPR: "[…] *Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.*"

47 La prima volta che si è parlato di contitolarità è stato, però, nell'art. 2, par. 1, lett. d) della Direttiva 95/46/CE ove si definiva il titolare del trattamento come la persona "*fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o con altri, determina le finalità e gli strumenti del trattamento dei dati personali*". Tuttavia la direttiva, nonostante abbia previsto la configurabilità di una titolarità congiunta rispetto a un trattamento di dati di natura personale, non è entrata nel merito degli obblighi gravanti su ciascun contitolare, né si è preoccupata di stabilire regole per disciplinare i rapporti che, di volta in volta, si sarebbero instaurati tra i vari titolari.

48 Cfr. punto 48 delle Linee Guida dell'EDPB, in cui è previsto espressamente che "*In broad terms, joint controllership exists with regard to a specific processing activity when different parties determine jointly the purpose*

Al riguardo ci vengono in soccorso le Linee Guida emanate dell'EDPB, ove anzitutto viene chiarito che una determinazione congiunta può sussistere non solo quando due o più Titolari agiscono tra loro in perfetta simmetria dando vita ad una decisione comune, ma anche quando questi agiscono ognuno per conto proprio, sviluppando decisioni distinte, che siano, però, tra loro convergenti. In questa ultima ipotesi, ciascuna decisione deve quindi avere un impatto tangibile sul trattamento, in modo tale che l'una non possa esistere ed esplicare i propri effetti senza l'altra: la partecipazione di entrambe le decisioni è "**inestricabile**" e "**imprescindibile**"[49].

Le Linee Guida proseguono, poi, con un'analisi dettagliata dei concetti di finalità e mezzi del trattamento, rispetto alla loro determinazione congiunta da parte dei Titolari.

Sul primo concetto l'EDPB evidenzia che le finalità del trattamento possono essere perseguite congiuntamente o meno dai Titolari. Tuttavia, in questa seconda ipotesi, è necessario che i singoli scopi siano tra loro "**strettamente collegati o complementari**", in considerazione dei principi esposti in una sentenza della Corte di Giustizia Europea[50].

Sul secondo concetto, invece, l'EDPB ribadisce la distinzione tra mezzi del trattamento:

- essenziali, in cui sono ricompresi le finalità, la tipologia dei dati oggetto del trattamento, i soggetti interessati e i destinatari, la durata del trattamento, i soggetti che hanno accesso ai dati;
- non essenziali, tra cui sono annoverati gli aspetti più pratici del trattamento quali le misure di sicurezza e le infrastrutture coinvolte nel trattamento.

È evidente che solo i primi rilevano ai fini della valutazione circa la configurabilità o meno della contitolarità; ad ogni modo, il consiglio è quello di valutare attentamente caso per caso. Al riguardo, l'EDPB precisa che la condivisione di infrastrutture informatiche non è di per sé sintomo di contitolarità, occorrerà sempre fare attenzione alla separabilità o meno del trattamento. Parimenti, il coinvolgimento di più Titolari in differenti fasi, gradi o misure del trattamento non deve necessariamente essere considerato come elemento qualificante la titolarità autonoma, dovendosi comunque valutare se vi è il perseguimento di una finalità comune.

and means of this processing activity".

49 Cfr. punto 53 delle Linee Guida dell'EDPB, ove è sancito che "*Decisions can be considered as converging on purposes and means if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing. As such, an important criterion to identify converging decisions in this context is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked*".

50 Cfr. Giudizio Fashion ID, C-40/17, ECLI:EU:2018:1039, par. 80.

5.2 Accordo di contitolarità

L'art. 26 del GDPR stabilisce, altresì, che i ruoli e le responsabilità, rispetto agli obblighi sanciti dal GDPR, di ciascun Contitolare debbano essere disciplinati da un accordo interno (c.d. accordo di contitolarità, di seguito "**Accordo**"). Nulla dice il GDPR in merito alla forma di tale Accordo; tuttavia, nelle proprie Linee Guida l'EDPB ha caldamente consigliato la forma scritta, soprattutto nell'ottica di garantire il rispetto del principio di *accountability*.

Quali sono gli elementi che devono essere indicati nell'Accordo? Al riguardo, l'EDPB suggerisce anzitutto di inquadrare il trattamento realizzato dai Contitolari, descrivendone i suoi elementi principali e, nello specifico: (*i*) la tipologia dei dati oggetto del trattamento, (*ii*) la categoria dei soggetti interessati cui appartengono i dati, (*iii*) l'oggetto e (*iv*) la finalità del trattamento.

Una volta individuati i predetti elementi, l'Accordo dovrà necessariamente prevedere l'allocazione delle responsabilità tra i vari Contitolari. Nell'ambito del trattamento occorre, quindi, che ciascun Contitolare si assuma determinati obblighi e responsabilità rispetto:

- all'attuazione dei principi di cui all'art. 5 del GDPR;
- all'individuazione della base di legittimità ai sensi dell'art. 6 del GDPR;
- all'individuazione delle misure di sicurezza e nella definizione di specifiche istruzioni ai fini della gestione di eventuali violazioni di dati (c.d. data breach);
- alla definizione di specifiche indicazioni per l'esercizio dei diritti da parte dei soggetti interessati;
- alla redazione della valutazione di impatto (c.d. DPIA);
- all'individuazione e alla formalizzazione dei rapporti con i responsabili del trattamento ai sensi dell'art. 28 del GDPR;
- alla cura degli aspetti legati al trasferimento dei dati al di fuori dell'UE;
- all'individuazione di un punto di contatto nei confronti dei soggetti interessati e delle competenti Autorità di Controllo.

Ciò posto, il consiglio è quello di strutturare il contenuto dell'Accordo nel modo più preciso e completo possibile, suddividendolo in tre parti: i) l'intestazione, ove andranno indicati i dati di ciascun Contitolare, ii) le premesse, in cui potrà essere descritta l'attività svolta da ciascun Contitolare, la natura del rapporto e le valutazioni svolte in merito alla necessità di determinare congiuntamente finalità e mezzi del trattamento e iii) l'oggetto dell'accordo, nonché gli obblighi e le responsabilità in capo a ciascun Contitolare.

In aggiunta ai predetti elementi si potrà, altresì, valutare l'inserimento di specifiche clausole di riservatezza in merito non solo ai dati, ma anche alle informazioni assunte da ciascun Contitolare nell'ambito dell'esecuzione

dell'Accordo ed eventuali clausole di responsabilità, che dovranno comunque tenere conto di quanto stabilito all'art. 82, comma 4, del GDPR[51].

Una volta definito il contenuto dell'Accordo, le sue parti essenziali dovranno essere rese note agli interessati in modo chiaro, coerente e trasparente. Quali sono, però, le parti essenziali dell'Accordo e quali sono i mezzi da utilizzare per rendere noto agli interessati tali aspetti? Se da un lato il GDPR non fornisce alcuna indicazione al riguardo[52], dall'altro l'EDPB fornisce alcuni suggerimenti. Precisamente, con riferimento al contenuto essenziale dell'Accordo l'EDPB raccomanda che lo stesso debba quantomeno evidenziare qual è il Contitolare responsabile rispetto a ciascun elemento previsto nell'informativa sul trattamento dei dati personali di cui all'art. 13 o 14 del GDPR. Con riferimento, invece, alle modalità, l'EDPB suggerisce che siano i Contitolari a stabilire il modo più efficace per rendere disponibile agli interessati il contenuto essenziale dell'Accordo; a titolo esemplificativo, l'EDPB consiglia di inserire il contenuto essenziale dell'Accordo all'interno del testo dell'informativa, oppure di individuare un punto di contatto che - se interpellato - sia autorizzato a fornire anche questo tipo di informazioni agli interessati oppure di incaricare il DPO - ove nominato - di tale compito.

5.3 Casistica

Sempre all'interno delle Linee Guida, l'EDPB analizza e descrive una serie di casi, la cui comprensione e lettura è certamente utile al fine di capire la ratio sottesa alla configurabilità della contitolarità del trattamento.

Di seguito, quindi, alcuni casi proposti dall'EDPB.

i. Agenzia viaggi

Un'agenzia viaggi trasmette i dati personali dei propri clienti alla compagnia aerea e ad una catena d'alberghi per effettuare la prenotazione di un pacchetto viaggio. Ricevuti i predetti dati, da un lato la compagnia aerea conferma la disponibilità dei posti e dall'altro la catena d'alberghi conferma la disponibilità delle camere richieste. L'agenzia di viaggi provvede, quindi, all'emissione dei biglietti aerei e dei voucher ai suoi clienti. In questo caso, agenzia di viaggi, compagnia aerea e catena d'alberghi sono da considerarsi ai fini privacy tre distinti titolari del trattamento, su cui gravano gli obblighi imposti dal GDPR.

La situazione, però, potrebbe variare nel caso in cui detti soggetti dovessero decidere di creare una piattaforma on-line comune per il perseguimento congiunto delle proprie finalità e, nello specifico, per

51 Cfr. art. 82, comma 4, del GDPR sancisce che "*Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento o il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno al fine di garantire il risarcimento effettivo dell'interessato*".

52 Cfr. art. 26, comma 2, del GDPR, infatti, prevede semplicemente che "*Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato*", senza entrare nel merito del contenuto essenziale e delle modalità che i Contitolari devono utilizzare per rendere noto il contenuto agli interessati.

la gestione dei servizi di prenotazione e l'effettuazione di attività di marketing, condividendo i dati dei propri clienti. Infatti, se per la creazione della piattaforma, tali soggetti ne stabiliscono congiuntamente gli aspetti fondamentali, oltre a determinare gli strumenti da utilizzare, questi agirebbero quali Contitolari relativamente a tutti quei trattamenti realizzati tramite la predetta piattaforma, restando invece Titolari autonomi rispetto ad eventuali attività svolte al di fuori di quest'ultima.

ii. Marketing

Due società decidono di lanciare un prodotto *co-branded* e di organizzare un evento per promuoverlo. A tale proposito e al fine di definire la lista degli invitati all'evento, le società condividono i dati dei rispettivi clienti e prospect, stabilendo insieme le modalità di: (*i*) invio degli inviti; (*ii*) raccolta dei feedback durante l'evento e (*iii*) attuazione delle successive attività di marketing. È evidente che, in questo caso, le due società agiscono quali Contitolari, in quanto oltre a definire congiuntamente le finalità del trattamento, ne stabiliscono anche i mezzi essenziali.

iii. Ricerca scientifica

Un medico (sperimentatore) e un istituto universitario (sponsor) decidono di avviare una sperimentazione clinica avente una finalità comune. Al fine di valutare se si possa configurare una contitolarità tra detti soggetti o meno, occorre anzitutto capire se il protocollo dello studio è stato redatto congiuntamente dallo sperimentatore e dallo sponsor (con definizione di finalità, metodologia, tipologia di dati da raccogliere, database coinvolti, ecc.) o se il protocollo è stato predisposto unicamente dallo sponsor. Infatti, nella prima ipotesi siamo di fronte ad un caso di contitolarità, mentre nel secondo lo sponsor potrà qualificarsi quale Titolare e lo sperimentatore quale responsabile del trattamento. In tutto ciò, resta comunque ferma la titolarità autonoma in capo al medico per il trattamento dei dati dei pazienti ai fini di cura.

iv. Comunicazione dei dati dei dipendenti all'Autorità fiscale

Una società raccoglie e tratta i dati personali dei propri dipendenti per la gestione del rapporto di lavoro. Al fine di adempiere alle prescrizioni di legge in materia di rafforzamento del controllo fiscale, la società è obbligata a trasmettere i dati relativi alle retribuzioni dei dipendenti all'Autorità fiscale. Nonostante la società e l'Autorità si trovino a trattare i medesimi dati personali (retribuzioni dei dipendenti), questi non condividono né finalità, né i mezzi del trattamento. Pertanto, alcuna contitolarità può configurarsi, restando la società e l'Autorità fiscale due titolari autonomi del trattamento.

v. Attività di marketing svolto da un gruppo imprenditoriale con database condiviso

Un gruppo imprenditoriale utilizza lo stesso database per la gestione dei dati di clienti e *prospect*. Ciascuna impresa ha, quindi, accesso alla propria

area del predetto database alimenta al fine di inserire i dati dei propri clienti e prospect. Alcun accesso è, infatti, consentito alle aree delle altre imprese. I livelli di accesso ai dati, i tempi di conservazione, la modifica o la cancellazione sono, peraltro, stabiliti autonomamente da ciascuna impresa, che agisce quale titolare autonoma del trattamento.

Rispetto alla conservazione dei dati, essendo il database ospitato su server dell'impresa controllante, questa ricoprirà il ruolo di responsabile del trattamento rispetto a ciascuna singola impresa.

Dall'analisi della predetta casistica emerge, quindi, che occorre sempre valutare con attenzione caso per caso, senza generalizzare, valutando di volta in volta tutti gli elementi che potrebbero effettivamente far sorgere la configurabilità della contitolarità.

6. Ruoli privacy interni

Il GDPR, sotto il profilo dei ruoli privacy interni alla struttura del Titolare o del Responsabile del trattamento, contiene prescrizioni limitate, lasciando quindi, da questo punto di vista, una discreta libertà organizzativa agli operatori. Come *infra* meglio precisato, l'unica figura interna delineata dal Regolamento europeo è quella dell'autorizzato al trattamento, la prima quindi a essere analizzata qui di seguito (par. 6.1).

Sul tema in oggetto dell'organigramma interno privacy, la riforma del Codice Privacy ad opera del D. Lgs. 101/2018 ha introdotto un elemento di novità, ossia la figura del designato (par. 6.2). La prassi societaria ha poi portato alla configurazione di una ulteriore figura in ambito privacy, quella del delegato, resasi necessaria per l'attribuzione di poteri normalmente in capo all'organo amministrativo a un determinato soggetto individuato dal *management* (par. 6.3).

In questa breve trattazione delle figure privacy "aziendali" non ci soffermerà su quella del *data protection officer* (DPO) poiché si tratta di un ruolo a sé stante e strutturalmente autonomo, anche quando il soggetto chiamato a ricoprire tale incarico è interno all'organizzazione dell'ente.

6.1 L'autorizzato

Tra le definizioni elencate nell'art. 4, il GDPR non include alcuna figura interna. Si noti, tuttavia, che il "terzo" viene definito (art. 4, n. 10) come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo* ***che non sia*** *l'interessato, il titolare del trattamento, il responsabile del trattamento* ***e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.***"

Da tale definizione emerge come gli autorizzati al trattamento siano di fatto ricompresi organicamente nella struttura del titolare o del responsabile del trattamento, non essendo appunto parti "terze".

Le disposizioni del GDPR più rilevanti per inquadrare la figura dell'autorizzato sono l'art. 29 e l'art. 32, comma 4, in base alle quali il Titolare e il Responsabile del trattamento devono fare sì che ***chiunque*** agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare. Si consideri, inoltre, che in base all'art. 24 del GDPR il Titolare deve mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato a norma di legge e la nomina degli autorizzati rientra senza dubbio tra tali misure.

I soggetti interni in questione potrebbero essere eventualmente definiti in certi contesti anche "incaricati" (definizione già presente nel Codice Privacy prima della modifica ad opera del D. Lgs. 101/2018, che ha abrogato l'art. 30 rubricato appunto "incaricati del trattamento") o "addetti" al trattamento ma, dal contenuto della definizione e delle disposizioni del GDPR sopra citate, pare più opportuno fare ricorso al termine "autorizzato".

L'autorizzato è senz'altro:

- una persona fisica (il testo in inglese dell'art. 29 è ancora più esplicito in tal senso "*any person acting under the authority of the controller…*" della versione italiana "*chiunque agisca sotto l'autorità…*");
- un soggetto subordinato all'interno della struttura del Titolare o del Responsabile, agendo sotto l'autorità di questi.

Interessante notare che in nessuna delle disposizioni citate relative alla figura dell'autorizzato si faccia riferimento al DPO, al quale, ove presente, l'autorizzato non è in alcun modo legato da vincoli di sorta, essendo peraltro il DPO – sia interno che esterno – una figura che gode di autonomia nell'organizzazione del Titolare o del Responsabile: nell'esecuzione dei propri compiti, non deve infatti ricevere alcuna istruzione e non può essere rimosso o penalizzato in conseguenza delle proprie attività.

L'unico legame tra il DPO e gli autorizzati è rinvenibile nell'attività di formazione svolta dal primo a favore dei secondi in virtù dell'art. 39, comma 1, lettera a), del GDPR, che prevede che il DPO debba "*informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento* ***nonché ai dipendenti che eseguono il trattamento*** *in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati*".

Per quanto concerne la nomina dell'autorizzato e le istruzioni da fornire allo stesso affinché svolga le attività di trattamento, il GDPR non fornisce indicazioni specifiche. In proposito, è senz'altro preferibile procedere, anche per rispettare il principio di *accountability,* con nomine scritte (come richiedeva il vecchio art. 30 del Codice Privacy relativo agli incaricati, ora abrogato) nelle quali delimitare il perimetro del trattamento consentito al dipendente. Fra le indicazioni fornite all'autorizzato nella nomina potrebbe opportunamente esservi, ad esempio, quella di limitare il trattamento dei dati personali a quanto sia necessario per lo svolgimento delle mansioni proprie del dipendente, nel rispetto non solo della vigente normativa privacy ma anche delle regole e delle

procedure aziendali (come, ad esempio, regolamenti interni per l'uso degli strumenti informatici, policy di riservatezza, ecc.).

La nomina ad autorizzato potrebbe altresì precisare che, in caso di inadempimento del dipendente alle istruzioni previste nell'autorizzazione stessa, si applicherebbero le sanzioni disciplinari applicabili in base al contratto di lavoro vigente.

Gli autorizzati dovranno anche ricevere opportune istruzioni in merito alla riservatezza delle informazioni di cui vengono a conoscenza nell'ambito della propria attività. A tali indicazioni deve evidentemente corrispondere un impegno al rispetto della confidenzialità di tutte o di certe informazioni da parte del dipendente-autorizzato. In proposito, si ricorda che l'art. 28, comma 3, lettera b), del GDPR richiede espressamente che il contratto tra il Titolare e il Responsabile includa anche, tra altre previsioni, che gli autorizzati al trattamento di dati per conto del Titolare abbiano un obbligo di riservatezza contrattuale o legale.

6.2 Il designato

Come anticipato, il GDPR non prevede espressamente la figura del designato. Questa è stata introdotta nel Codice Privacy dal decreto di armonizzazione della disciplina italiana a quella europea, il D. Lgs. 101/2018.

In base al nuovo art. 2-*quaterdecies* del Codice Privacy, il Titolare o il Responsabile possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Sempre a mente del medesimo articolo, il Titolare o il Responsabile devono individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Tale disposizione prevede il potere di titolare e responsabile di delegare compiti e funzioni a persone fisiche che operano sotto la loro autorità e che, a tal fine, devono essere espressamente designati.

Quella del designato è una figura intermedia tra il Titolare, o il Responsabile, e l'autorizzato e, lo si precisa, non è obbligatoria ma si renderà tanto più opportuna nelle strutture di medie e grandi dimensioni nelle quali le attività di trattamento di dati personali possono essere numerose e complesse, richiedendo quindi una strutturazione dell'organigramma privacy su più livelli. Sarebbe possibile ipotizzare di nominare designati i soggetti che ricoprono in azienda funzioni particolarmente rilevanti sotto il profilo dei dati personali, come ad esempio il responsabile delle risorse umane o del marketing. Le specifiche operazioni di trattamento sarebbero comunque svolte dai dipendenti-autorizzati, in base alle istruzioni ricevute e alle proprie specifiche mansioni.

La vecchia figura del "responsabile interno" prevista dall'art. 30, ora abrogato, del Codice Privacy si può considerare in parte coperta dall'art. 2-*quaterdecies* del Codice Privacy; tuttavia, nei casi in cui all'interno di un'organizzazione siano

ancora utilizzati atti di nomina che richiamano la terminologia non più vigente (ciò è, a oggi, ancora piuttosto frequente), è certamente consigliabile prevedere una revisione della documentazione, che potrebbe essere non solo formale ma dare anche spunti per un ripensamento sostanziale dei ruoli e dell'allocazione delle responsabilità e delle funzioni privacy.

6.3 Il delegato

Per quanto attiene alla strutturazione dell'organigramma, l'ente potrebbe altresì considerare l'opportunità di una ulteriore figura di collegamento tra la società e i ruoli operativi dei designati e degli autorizzati, ossia il "delegato".

Anche questa figura, come quella del designato, non è espressamente prevista dal GDPR ma deriva dall'esigenza di natura societaria e di *governance* di attribuire, da parte dell'organo amministrativo della società, specifici poteri a un determinato soggetto – solitamente un amministratore della società ma anche, eventualmente, un dirigente con un profilo ritenuto adeguato dal *management* – perché questo ponga in essere quanto necessario per dare attuazione alla normativa privacy.

Il delegato ha il potere di esercitare le proprie competenze entro il limite della delega ricevuta dal Titolare (tramite l'organo amministrativo) e l'inosservanza del contenuto della stessa può determinare una responsabilità del delegato.

I poteri conferiti al delegato, ove la delega lo preveda, potrebbero essere a loro volta delegati a diversi soggetti, eventualmente uno o più "designati".

Si noti, infine, che la delega è cosa diversa dalla procura: la prima è un atto interno per l'attribuzione di poteri, compiti e funzioni che specifica il contenuto dei compiti assegnati, mentre la seconda è l'atto con cui la società attribuisce a un soggetto poteri di rappresentanza verso terzi. La procura è quindi necessaria per la sottoscrizione dei documenti privacy che hanno una rilevanza esterna, come ad esempio le nomine a responsabile (i cd. *data processing agreement*). La controparte contrattuale del Titolare vorrà quasi certamente sincerarsi che il soggetto che sta firmando il contratto per conto della società, se non è il legale rappresentante, sia dotato dei necessari poteri e la procura darebbe a tal fine pubblicità.

Anche l'attribuzione dei poteri privacy a un delegato – così come la nomina di uno o più designati e la corretta individuazione, istruzione e formazione degli autorizzati – rientra nel generale obbligo dell'ente soggetto all'ambito di applicazione GDPR di mettere in campo misure organizzative adeguate affinché le attività di trattamento siano effettuate in conformità alla normativa privacy (anche in virtù degli artt. 24 e 25 del GDPR).

Evidentemente, ogni valutazione in ordine alla strutturazione di un organigramma privacy (che potrebbe prevedere ruoli, definizioni e funzioni anche diversi da quelli qui citati) deve essere fatta tenendo in considerazione tutti gli elementi a tal fine rilevanti, tra cui anche la dimensione della società, il suo ambito di attività, la propria *governance*, la ripartizione interna delle funzioni e

le specifiche attività di trattamento di dati poste in essere. Risulta in ogni caso fondamentale che i singoli aspetti dell'assetto organizzativo individuato per la propria organizzazione, dal vertice alla base, siano adeguatamente documentati.

CAPITOLO 4 di Micaela Barbotti, Josephine Romano e Roberto Tirone

Il principio di riservatezza nel sistema del D.Lgs. 231/2001

SOMMARIO: 1. La riservatezza nel sistema di *whistleblowing* – 1.1 Il *whistleblowing* nell'impianto del D.Lgs. n. 231/2001 – 1.2. La segnalazione del *whistleblower* tra riservatezza e anonimato– 1.3. Pluralità di canali di *whistleblowing*: strumenti per un approccio integrato alla gestione delle segnalazioni – 2. I verbali dell'Organismo di Vigilanza: tra riservatezza e obbligo di reporting – 3. Riservatezza e responsabilità dell'OdV

1. La riservatezza nel sistema di whistleblowing

1.1 Il whistleblowing nell'impianto del D.Lgs. n. 231/2001

Nell'ambito dell'impianto del D.Lgs. n. 231/2001, il tema della riservatezza ha assunto una sempre maggiore rilevanza in virtù della L. 14 dicembre 2017 n. 179 ("Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"), che ha modificato la normativa in tema di obbligo di segreto d'ufficio, aziendale, professionale, scientifico e industriale, introducendo la disciplina del c.d. *Whistleblowing* anche nei rapporti di lavoro privato.

Come noto, tale novella legislativa è intervenuta sull'articolo 6 del D.Lgs. n. 231/2001 disponendo in primo luogo che i Modelli debbano prevedere uno o più canali, nonché un canale alternativo informatico, che consentano ai soggetti in posizione apicale e ai c.d. subordinati di presentare – a tutela dell'integrità dell'ente – **segnalazioni circostanziate di condotte illecite o di violazioni dello stesso Modello, di cui siano venuti a conoscenza in ragione delle funzioni svolte**. Le condotte illecite oggetto delle segnalazioni devono in ogni caso essere rilevanti ai sensi del D.Lgs. 231/2001 e devono essere fondate su elementi di fatto precisi e concordanti.

Unitamente a tale previsione generale, la L. n. 179/2017 ha richiesto alle Società che adottino il Modello di stabilire **modalità di gestione delle segnalazioni che assicurino la riservatezza dell'identità del *whistleblower***. Costui è poi ulteriormente garantito attraverso il divieto di atti di ritorsione o discriminatori (si pensi a possibili condotte di *mobbing* o *straining*, mutamenti di mansioni o demansionamenti, fino ad arrivare al licenziamento) nei confronti del medesimo *whistleblower*, per motivi collegati, direttamente e non, alla segnalazione effettuata.

Inoltre, per la costruzione di un sistema di *whistleblowing* efficace, viene prescritto che il Modello contempli delle specifiche sanzioni disciplinari a carico non solo del soggetto segnalato, nell'ipotesi in cui i fatti siano confermati, ma anche di tutti coloro che agiscano in violazione della disciplina delle segnalazioni. A tale riguardo, si ricorda che le Linee Guida di *Transparency International* del 2016 hanno evidenziato il forte legame tra la previsione di sanzioni nel sistema di *whistleblowing* e la riservatezza del segnalante. Tali Linee Guida, infatti, indicano tra le condotte necessariamente sanzionabili, tra le altre, la **violazione degli obblighi di riservatezza**.

In particolare, si deve apportare un aggiornamento del Modello, predisponendo un'apposita integrazione del sistema disciplinare (previsto dallo Statuto dei lavoratori e dal CCNL applicabile alla Società e richiamato, secondo una consolidata prassi, all'interno della Parte Generale del Modello), che includa sanzioni nei confronti di chi (dirigente o dipendente) violi le misure a tutela della riservatezza del segnalante, nonché del *whistleblower* stesso che effettui, con dolo o colpa grave, segnalazioni rivelatesi infondate.

All'interno del sistema di *whistleblowing* si potrà altresì valutare la previsione di misure sanzionatorie a tutela della riservatezza anche a carico di soggetti terzi (ad es. collaboratori, consulenti, lavoratori somministrati, partner commerciali e i fornitori), attraverso l'inserimento di specifiche clausole contrattuali che sanzionino (con la diffida o l'applicazione di penali e, nei casi più gravi, la risoluzione del contratto) il mancato rispetto delle procedure previste dallo stesso sistema di *whistleblowing*.

1.2. La segnalazione del whistleblower tra riservatezza e anonimato

Se, nell'ambito del sistema di *compliance* 231, le modalità di trasmissione delle segnalazioni devono garantire la massima riservatezza dell'identità dei segnalanti, la **L. n. 179/2017 nulla prevede circa la possibilità di effettuare segnalazioni anonime**.

Dal mero dato normativo, dunque, non è possibile identificare la riservatezza con l'anonimato, da intendersi come assoluta impossibilità, da parte del segnalato, di venire a conoscenza dell'identità del soggetto segnalante.

Anche la giurisprudenza di legittimità sembra escludere la possibilità di un'assoluta coincidenza tra riservatezza e anonimato. Nella prima sentenza sul whistleblowing emessa, a seguito dell'entrata in vigore della L. n. 179/2017, in un giudizio a carico di un dipendente pubblico, infatti, la Suprema Corte ha stabilito che, nel procedimento penale, l'anonimato non trova spazio e la tutela della riservatezza del segnalante è salvaguardata dalle disposizioni del codice di rito riguardanti il segreto, laddove invece l'anonimato potrebbe operare nel procedimento disciplinare, in cui l'identità del segnalante potrebbe essere svelata solo per garantire il diritto di difesa del segnalato,: "*l'anonimato del denunciante - che, in realtà, è solo riserbo sulle generalità, salvo ovviamente il consenso dell'interessato alla loro divulgazione - opera unicamente in ambito disciplinare, essendo peraltro subordinato al fatto che la contestazione «sia fondata su accertamenti distinti e ulteriori*

rispetto alla segnalazione», giacché, ove detta 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»: ne consegue - né potrebbe essere diversamente - che, in caso di utilizzo della segnalazione in ambito penale, non vi è alcuno spazio per l'anonimato - rectius: per il riserbo sulle generalità […]" (Cass. Pen., Sez.VI, 27 febbraio 2018, n. 9047).

Malgrado la reticenza della giurisprudenza, parrebbe comunque opportuno consentire che le procedure di segnalazione individuate dal Modello prevedano **anche la possibilità di effettuare segnalazioni anonime, al fine di poter diffondere una positiva cultura del whistleblowing e promuovere le segnalazioni stesse**. Detta conclusione risulta avvalorata anche dalla Nota Illustrativa di Confindustria sulla materia ("*La disciplina in materia di whistleblowing*", gennaio 2018), secondo cui non è da escludere che il Modello possa contemplare dei canali per l'invio di segnalazioni in forma anonima, purché le medesime siano documentate ovvero siano dettagliate al punto da "*far emergere fatti e situazioni relazionandoli a contesti determinati*": in assenza di tali precauzioni, infatti, l'anonimato della segnalazione aggraverebbe l'attività di verifica sulla sua fondatezza, "*con il rischio di alimentare denunce infondate e mere doglianze che hanno poco a che fare con la tutela dell'integrità dell'ente*". Ulteriore conferma di tale orientamento si riscontra poi nell'art. 6 della Direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, attualmente in corso di recepimento. Infatti, come viene illustrato nel Considerando 34 della Direttiva, è rimessa agli Stati membri la facoltà di: "*[…] decidere se i soggetti giuridici del settore pubblico e del settore privato e le autorità competenti devono accettare le segnalazioni anonime di violazioni rientranti nell'ambito di applicazione della presente direttiva e vi danno seguito. Tuttavia, le persone che hanno segnalato o reso pubbliche in forma anonima informazioni rientranti nell'ambito di applicazione della presente direttiva e che ne soddisfano le condizioni dovrebbero beneficiare della protezione prevista dalla presente direttiva qualora siano successivamente identificate e subiscano ritorsioni*".

Il ricorso a segnalazioni anonime potrebbe assumere rilevanza per due ragioni. Da un lato, **agevolerebbe l'emersione di condotte illecite**, posto che nel contesto culturale odierno – pubblico e privato – la cultura del *whistleblowing* non è ancora diffusa e gli individui sono restii ad esporsi, effettuando segnalazioni. Viceversa, la facoltà di segnare condotte illecite attraverso modalità che garantiscano non solo riservatezza, ma anche anonimato, potrebbe favorire il ricorso ai canali di *whistleblowing*, ferma restando l'applicabilità del sistema sanzionatorio per punire segnalazioni infondate effettuate con dolo o colpa grave.

Dall'altro, l'anonimato non contrasterebbe con la funzione intrinseca del *whistleblowing*, che rimane di allerta e non di denuncia: una volta effettuata la segnalazione, l'organizzazione ricevente sarebbe tenuta ad approfondire, accertare e verificare i fatti, anche qualora si permettesse al segnalante di restare anonimo. In proposito, **può tracciarsi un parallelismo con quanto di recente previsto dalla Suprema Corte per le denunce anonime in ambito penale**: "*Sulla base di una denuncia anonima non è possibile procedere a perquisizioni, sequestri*

e intercettazioni telefoniche […]. Tuttavia, gli elementi contenuti nelle denunce anonime possono stimolare l'attività di iniziativa del P.M. e della polizia giudiziaria al fine di assumere dati conoscitivi, diretti a verificare se dall'anonimo possano ricavarsi estremi utili per l'individuazione di una «notitia criminis»" (Cass. Pen., Sez.VI, 4 agosto 2016 n. 34450). Parimenti, **la segnalazione anonima**, pur non efficace di per sè a fondare una contestazione nei confronti del segnalato, **potrebbe fungere da "atto di impulso"** per la Società e permetterle di portare alla luce condotte illecite o perfino delittuose.

1.3. Pluralità di canali di whistleblowing: strumenti per un approccio integrato alla gestione delle segnalazioni

A prescindere dalla possibilità o meno di conservare l'anonimato del *whistleblower*, va ricordato che l'obbligo di riservatezza comporta che i dati personali dei segnalanti e di tutti gli altri soggetti eventualmente coinvolti devono essere correttamente gestiti, in conformità con la normativa applicabile anche in tema di *data protection*.

Ciò si traduce, in primo luogo, nel dovere di assicurare adeguata riservatezza ai canali di comunicazione utilizzati per rivolgere segnalazioni all'Organismo di Vigilanza (che per prassi sono costituiti da un indirizzo *e-mail* dedicato e da una o più cassette per le segnalazioni cartacee), vietandone l'accesso a tutti i soggetti che non siano componenti dell'Organismo.

Oltre a ciò, le operazioni di trattamento di segnalazioni esterne ai canali di comunicazione dell'Organismo di Vigilanza – in particolare quelle che si svolgano per mezzo di strumenti informatici – devono essere affidate a soggetti specificamente formati e informati sulle procedure aziendali di *whistleblowing* e sulle relative modalità di tutela della riservatezza. Tali soggetti devono essere inoltre chiaramente e preventivamente identificati, non solo sulla base della struttura organizzativa della Società o del Gruppo, ma anche dell'eventuale implementazione di specifiche procedure di whistleblowing ai sensi di regolamentazioni di settore.

Può infatti accadere che alcune Società abbiano predisposto, oltre alla *e-mail* dell'Organismo di Vigilanza, canali di segnalazione di Gruppo o siano interessate da normative peculiari in tema di *whistleblowing* (ad es. Società soggette al Codice Interno di Autodisciplina di Borsa Italiana, al TUB, al Codice delle Assicurazioni, alla normativa del settore pubblico ai sensi dell'art. 54-bis D.Lgs. n. 165/2001,alla normativa antiriciclaggio, ecc.): in questi casi, in assenza di informazioni, vi è il rischio che il *whistleblower* effettui la medesima segnalazione su più canali o ricorra ad un canale diretto ad un destinatario non competente, con conseguente pregiudizio della riservatezza.

In quest'ottica, è evidente l'opportunità di valutare l'adozione di meccanismi informatici integrati di *screening* delle segnalazioni, così da consentirne l'inoltro al soggetto deputato secondo la singola normativa. In tal senso depone anche la L. n. 179/2017, la quale, pur intervenendo direttamente sull'impianto del D.Lgs. 231/2001, non esplicita chi sia il destinatario delle segnalazioni né

stabilisce che lo stesso sia necessariamente l'Organismo di Vigilanza, chiamato a vigilare sull'osservanza del Modello e diretto destinatario di sole notizie concernenti condotte illecite rilevanti ai fini del D.Lgs. 231/2001 e violazioni del Modello.

Si potrebbero ipotizzare pertanto soluzioni integrate di gestione dei diversi canali di *whistleblowing* implementati all'interno del contesto aziendale, quali **l'utilizzo di piattaforme informatiche, gestite da *provider* terzi** con l'ausilio di refenti aziendali interni. La realizzazione di un tale sistema integrato consentirebbe, una volta ricevuta la segnalazione, di individuarne a monte l'ambito di applicazione, l'oggetto e il contenuto e di indirizzare la stessa al destinatario competente ai sensi della normativa applicabile.

Questa possibile soluzione costituirebbe un efficace strumento di *compliance* a tutela della riservatezza del segnalante (e del segnalato), agevolando, al contempo, le attività dell'Organismo di Vigilanza, che riceverebbe soltanto le segnalazioni di propria competenza.

2. I verbali dell'Organismo di Vigilanza: tra riservatezza e obbligo di reporting

L'art. 6 del D. Lgs. n. 231/2001 stabilisce che l'ente non risponde del reato commesso dagli apicali o dai sottoposti se prova che (*i*) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, Modelli Organizzativi idonei a prevenire reati della specie di quello verificatosi e (*ii*) il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo.

Per poter espletare adeguatamente ed efficacemente l'attività di vigilanza, l'OdV deve avere libero accesso a tutte le aree aziendali, onde ottenere i documenti e le informazioni necessari per lo svolgimento dei compiti attribuiti. Deve essere, inoltre destinatario di una serie di flussi informativi, immediati (al verificarsi di eventi di rilievo ai fini del sistema di compliance 231) o periodici, che consentano di garantire un sistema efficace, efficiente e puntuale di controllo.

Fondamentale, inoltre, che l'OdV si relazioni periodicamente con tutti gli organi e le funzioni societarie preposte ai controlli (Collegio Sindacale, RSPP, DPO, Responsabile Trasparenza e Corruzione Responsabili dei Sistemi di Gestione aziendale eccettera) per creare sinergie nell'ottica della miglior efficacia del sistema aziendale dei controlli.

Sono considerati ***strumenti operativi*** imprescindibili, anche al fine di poter dimostrare l'effettivo svolgimento da parte dell'OdV dell'attività di sorveglianza ad esso demandata: (*i*) il Piano di audit, (*ii*) i verbali delle riunioni con le risultanze delle verifiche effettuate e dei flussi pervenuti e (*iii*) la Relazione periodica.

Di immediata evidenza, quindi, l'importanza di disciplinare – tra i tanti aspetti inerenti l'azione dell'OdV – le modalità di predisposizione, i tempi di conservazione e le eventuali modalità di condivisione dei predetti strumenti operativi.

Per quanto concerne la Relazione periodica (solitamente annuale), la stessa ha ad oggetto i risultati dell'attività svolta dall'OdV con l'indicazione, tra l'altro (*i*) dei controlli effettuati e l'esito degli stessi, (*ii*) delle verifiche specifiche e l'esito delle stesse, (*iii*) dell'eventuale necessità o opportunità di aggiornamento della mappatura dei processi sensibili e del Modello e (*iv*) delle eventuali criticità riscontrate con suggerimenti e spunti per il miglioramento.

È prassi ormai diffusa e consolidata, che la Relazione periodica non solo venga inviata all'organo amministrativo, ma che venga anche sottoposta al Collegio Sindacale, direttamente dall'OdV o, più frequentemente, per il tramite dell'organo amministrativo.

Il Piano di audit (solitamente annuale) è il documento che definisce le attività che l'OdV intende effettuare nel periodo di riferimento; indica gli obbiettivi che l'OdV si prefigge, individua le attività "a rischio reato" ed i relativi processi sensibili su cui, salvo necessità emergenti, intende riservare un'attenzione prioritaria anche secondo criteri di rotazione, stabilisce il calendario degli incontri, sempre fatte salve necessità contingenti ed improvvise e, come tali, non pianificabili.

Il Piano di audit è, anch'esso, sottoposto all'organo amministrativo e talvolta, senza che ciò comporti particolari problematiche, inviato per conoscenza anche al Collegio Sindacale.

Sicuramente più delicata la questione inerente la possibilità di condivisione dei verbali dell'OdV. Non ci si riferisce, ovviamente, ai verbali redatti all'esito delle riunioni tra diversi organi di controllo finalizzati proprio, nel rispetto dell'indipendenza e dell'autonomia dei diversi ruoli e competenze, al confronto reciproco ed alla condivisione delle verifiche effettuate.

Ci si riferisce, invece, ai verbali redatti dall'OdV nell'ambito delle proprie attività.

Si pone, infatti, proprio per questi ultimi, la necessità di trovare una adeguata soluzione che, da un lato, garantisca la dovuta riservatezza e, dall'altro, consenta di assolvere all'obbligo di reporting quantomeno verso l'organo amministrativo, a cui l'OdV tenuto a riferire.

La questione diventa ancora più delicata, se si considera che l'OdV può essere destinatario delle eventuali segnalazioni circostanziate di condotte illecite rilevanti ai sensi del D. Lgs. n. 231/2001 o di violazioni del Modello Organizzativo di cui i soggetti indicati nell'articolo 5, comma 1, lettere a) e b) del predetto decreto siano venuti a conoscenza in ragione delle funzioni svolte. Rispetto a dette segnalazioni, sussiste infatti l'obbligo di garantire la riservatezza dell'identità del segnalante. Sempre allo scopo di tutelare il diritto alla riservatezza del segnalante, si considerino inoltre le limitazioni previste all'art. 2 *undecies*, lettera

f) del D. Lgs. n. 196/ 2003, che prevede che l'interessato non possa esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento UE 2016/679 qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto "*alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio*".

Proprio in ragione di quanto esposto, è diffusa la prassi di redigere uno specifico Regolamento per la gestione delle segnalazioni e di prevedere che l'intera istruttoria sia riportata in verbali appositi e specifici, distinti da quelli relativi alle normali attività di verifica dell'OdV, accessibili ***unicamente*** ai componenti dell'OdV. Terminata poi l'istruttoria, l'OdV redigerà una relazione riepilogativa delle indagini effettuate e delle evidenze emerse da sottoporre all'Organo Amministrativo per gli eventuali provvedimenti disciplinari o sanzionatori.

Con riferimento, invece, ai verbali per l'attività "ordinaria" dell'OdV, gli stessi potranno essere sottoposti all'organo amministrativo, tenuto conto del fatto che l'OdV deve garantire un adeguato sistema di reporting verso i vertici aziendali, su base continuativa, così da mantenere uno stretto contatto con l'organo a cui deve riferire.

Non si ravvisano, invece, ragioni per cui i verbali debbano essere sottoposti, né che possano essere richiesti o pretesi da altri organi (Collegio Sindacale, Revisore) o dalle diverse funzioni aziendali. Sarà, semmai l'organo amministrativo, unico possibile destinatario dei verbali dell'OdV, a valutare l'opportunità di diffondere e rendere note, nelle modalità che riterrà opportune, le evidenze emerse dalle verifiche dell'OdV al fine di sensibilizzare in merito a rilevate anomalie organizzative o comportamentali o a condotte non in linea con il Modello Organizzativo e le procedure aziendali.

3. Riservatezza e responsabilità dell'OdV

Il Modello Organizzativo e di Gestione (di seguito "MOG") è un documento complesso che contiene una serie di regole (prescrizioni, precetti, raccomandazioni, procedimenti ecc.) per la corretta gestione dell'ente cui il MOG si riferisce.

Le regole contenute nel MOG non sono uno standard valido per tutti gli enti, ma sono differenti da ente ad ente e rappresentano in via diretta o indiretta l'assetto e l'organizzazione aziendale: fattori della produzione, modalità di produzione, segreti aziendali, modalità di commercializzazione, *mark up* applicato, modalità di gestione delle risorse e così via.

Uno dei compiti dell'Organismo di Vigilanza nominato ai sensi del DLGS 231/2001 (di seguito "OdV") è quello di verificare che il Modello Organizzativo - e quindi le regole in esso contenute - sia (correttamente) applicato, aggiornato ed efficace.

Per svolgere tale funzione, l'OdV ha la necessità di accedere a tutta una serie di informazioni e documenti che possono essere anche sensibili, riservati o

relativi ad un know-how segreto (ad esempio, la stessa organizzazione aziendale potrebbe essere considerata materia riservata).

A ciò si aggiunga che la disciplina del whistleblowing ha aumentato il numero di informazioni riservate che l'OdV deve potenzialmente gestire (nomi dei segnalatori, nomi dei segnalati, circostanze riferite ecc.).

Ci si pone, quindi, la domanda: quali sono le responsabilità dell'OdV qualora le informazioni sensibili, riservate o segrete vengano riferite a terzi senza il consenso dell'ente?

Sotto il profilo della privacy, è stato escluso da parte del Garante della Privacy che l'OdV ricopra il ruolo di Titolare del trattamento, ovvero quello di Responsabile del trattamento, ai sensi del D.Lgs. 196/2003 come da ultimo modificato dal D.Lgs. 101/2018. Tuttavia, il Garante Privacy non ha escluso che i membri dell'OdV debbano collaborare all'implementazione della normativa privacy e, qualora si rendano responsabili di violazione della stessa, ne possano rispondere nei confronti dell'ente.

I membri dell'OdV, dunque, in caso di illegittima diffusione di informazioni che non siano già di pubblico dominio, saranno anche civilmente responsabili per violazione dei precetti contenuti nella normativa privacy e per inadempimento rispetto al contratto stipulato con l'ente (quello con il quale è stata accettata la carica di membro dell'OdV).

Per quanto concerne le informazioni acquisite attraverso i canali di *whistleblowing*, per il settore privato l'art. 2 della L. 79/2017 è chiaro: i membri dell'OdV se destinatari delle segnalazioni "garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione".

Se, dunque, i membri dell'OdV violano la riservatezza del segnalante, riferendo informazioni non necessarie a terzi, ancorché finalizzate alla verifica delle circostanze segnalate, saranno responsabili nei confronti dell'ente e del segnalante per i danni eventualmente subiti da questi ultimi.

Ci si domanda, a questo punto, se la responsabilità per violazione della riservatezza commessa da un solo membro dell'OdV si possa estendere all'intero collegio.

In tal senso, può essere utile ricorrere al parallelismo tra OdV e un altro organo sociale deputato a compiere attività di vigilanza sull'attività della società: il collegio sindacale.

L'articolo 2407 del Codice Civile prevede, da una parte, la responsabilità solidale dei componenti del Collegio Sindacale (con gli amministratori), laddove l'evento dannoso per la società non si sarebbe prodotto se i Sindaci avessero vigilato sull'attività degli amministratori in conformità agli obblighi della propria carica e dall'altra, la responsabilità dei sindaci in caso di violazione del proprio obbligo di conservare il segreto sui fatti e sui documenti di cui hanno conoscenza per ragione del loro ufficio.

Naturalmente, l'art. 2407 del Codice Civile non è *tout court* applicabile ai membri dell'OdV, essendo una norma speciale e specifica per il Collegio Sindacale. Peraltro, tale norma sembrerebbe prospettare una responsabilità collegiale degli organi collegiali societari, con la conseguenza che la violazione di taluni obblighi da parte anche di un solo componente comporterebbe la responsabilità dell'intero collegio.

È, dunque, possibile che in futuro il legislatore introduca una norma similare anche per i membri dell'OdV. Attualmente, in assenza di una normativa e giurisprudenza sul punto ogni tesi rimane valida.

Si è detto che l'OdV ha punti di contatto col Collegio Sindacale, ma è anche vero che ha caratteristiche profondamente differenti.

Infatti, in genere gli OdV collegiali sono composti da tre persone: due membri esterni ed uno interno (mentre il Collegio Sindacale è composto solo da membri esterni).

I c.d. "membri interni" sono persone che, oltre a far parte dell'OdV, sono anche dipendenti dell'ente stesso, mentre i c.d. "membri esterni", sono normalmente professionisti.

I membri interni, in quanto dipendenti dell'ente, sono soggetti all'obbligo di fedeltà previsto dall'art. 2105 c.c., il quale – secondo parte della dottrina e della giurisprudenza – ha valore "onnipervasivo", nel senso che l'obbligo in questione può, e deve, ricomprendere al proprio interno ogni comportamento del dipendente che può incidere sull'elemento fiduciario che contraddistingue il rapporto tra datore di lavoro e lavoratore. Palesemente, rientra tra gli obblighi del dipendente quello di non "divulgare notizie attinenti all'organizzazione" del datore di lavoro.

Il dipendente "membro interno", dunque, si trova ad avere un duplice vincolo di riservatezza rispetto all'esterno e, in maniera conflittuale con gli obblighi gravanti sui membri dell'OdV, un obbligo di trasparenza e verità dei confronti del proprio superiore gerarchico. Per il membro interno, quindi, gli obblighi di riservatezza appaiono complessi e risulta difficile individuare criteri generali per la determinazione dei limiti degli obblighi dei membri interni. Ciò anche in considerazione delle norme latamente applicabili ai membri interni, che a volte sono tra loro conflittuali.

La figura del membro esterno non è meno complessa: è, infatti, discusso se il membro esterno – quando questi è anche un professionista iscritto a un Albo ed è sottoposto a uno specifico ed autonomo codice deontologico, come ad esempio gli avvocati, - continua a rivestire il ruolo di professionista/consulente (nell'esempio, quindi, se continua a rivestire la qualità di avvocato) o se, invece, nel momento in cui svolge l'attività di membro dell'OdV si spoglia della propria qualità di professionista (avvocato) per rivestire quella di consulente atipico, senza, quindi che sia applicabile la disciplina tipica dello specifico professionista (codice deontologico, leggi specifiche ecc.).

Certo è che, se il membro esterno mantiene la qualifica professionale (ovvero mantiene la qualifica di avvocato), a tale soggetto sarà applicabile, oltre alla disciplina ordinaria sopra esaminata, anche quella tipica del professionista: si pensi ad esempio al codice deontologico, ai doveri di riservatezza, al segreto professionale, anche in caso di richiesta di testimonianza e così via.

Anche sotto il profilo assicurativo, certamente la responsabilità professionale sarà *tout court* ricompresa nella polizza assicurativa professionale del membro esterno/professionista.

Se, invece, si considera l'incarico di membro dell'OdV quale incarico estraneo all'attività professionale, allora il professionista non sarà sottoposto, nello svolgimento dello specifico incarico, alle leggi professionali (codice deontologico, doveri di riservatezza ecc.).

Forse l'orientamento più corretto è quello di ritenere che il professionista membro dell'ODV mantiene la propria qualifica originale (nell'esempio "avvocato") anche se la carica di membro dell'OdV non è tra quelle tipiche della professione.

Infatti, se si esamina la genesi del rapporto tra ente e membro esterno, appare chiaro che il professionista viene scelto come membro dell'OdV anche e soprattutto per la sua qualifica e non tanto quale consulente esterno o come soggetto meramente erudito in tema di DLGS 231/2001.

Dalla disamina sopra effettuata appare chiaro che la responsabilità dei membri dell'OdV non è stata ancora pienamente chiarita dal legislatore ed è oggi attività complessa individuare con certezza dei criteri generali di responsabilità dell'OdV e dei suoi membri, considerato anche che vi sono certamente delle differenze "qualitative" tra i membri dell'OdV (interni ed esterni) e tra il Collegio Sindacale e l'OdV.

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

Rischi tributari e riflessi sull'attività di vigilanza dell'OdV in ambito 231

SOMMARIO: 1. L'attività dell'Organismo di Vigilanza e le relative finalità – 2. L'attuale sistema di controlli: l'obbligo giuridico di attivazione – 3. L'attuazione della Direttiva PIF e l'ampliamento del novero dei reati presupposto ex D.lgs. 231/01 – 4. I reati tributari inseriti nel novero della 231/2001 ex art. 25-quinquiesdecies – 5. Le attività di Risk Assessment in relazione ai Reati Tributari richiamati dall'art. 25-quinquiesdecies D.lgs. 231/2001 – 6. Riflessione conclusiva – 7. Bibliografia

1. L'attività dell'Organismo di Vigilanza e le relative finalità

L'OdV svolge sì funzioni di controllo ma - giova ribadirlo – non in merito alla prevenzione dei reati, bensì al funzionamento e all'osservanza del MOG. È naturalmente sprovvisto dei poteri impeditivi della commissione degli illeciti, e di ciò ne è prova il fatto che non è suo compito adottare il MOG, né aggiornarlo, ma solo verificarne l'applicazione e suggerire agli organi gestori gli interventi necessari alla corretta funzionalità.

È di logica deduzione anche il requisito dell'autonomia dell'OdV (art. 6, comma l, lett. b), D.lgs. n. 231/2001) che non comporta attribuzioni di poteri di intervento sull'organizzazione dell'ente. Persino l'autonomia di spesa dell'OdV, ove prevista dallo Statuto dell'ente, è correlata al solo svolgimento dei compiti di controllo.

Nella disamina dell'art. 6 invocato dall' OdV nella sua specifica richiesta, occorre evidenziare quanto segue:

- i flussi informativi di cui all'art 6, comma 2, lett. d);
- i risultati delle attività di controllo e vigilanza di cui all'art 6, comma 1, lett. b) e d);
- eventualmente, ma tutt'altro che necessariamente, le segnalazioni di condotte illecite rilevanti ai fini del D.lgs. n. 231/2001 o di violazioni del modello, di cui all' art. 6, comma 2-bis. Iett. a).

Da questa premessa si evidenzia come l'OdV è istituito da "l'organo dirigente" (art. 6 comma 1, lett. b), il quale dovrà disciplinare gli aspetti principali relativi al funzionamento dell'OdV (cfr. Linee guida di Confindustria, pagg. 57 e 60).

Inoltre l'autonomia e l'indipendenza dell'OdV ex art. 6 D.lgs. n. 231/2001 non sono per così dire assolute, ma sono compatibili con "il riporto al massimo vertice operativo aziendale vale a dire al Consiglio di Amministrazione" (cfr. Linee guida di Confindustria, pag. 57).

Occorre, infine, evidenziare che nonostante l'art. 6 del D.lgs. n. 231/2001 individui in modo alquanto generico i compiti dell'OdV, rimane comunque indiscutibile che le generali finalità di prevenzione dei reati presupposto non possono essere confuse con le particolari finalità dei trattamenti strumentali allo svolgimento degli stessi compiti. L'esegesi dell'opinione maggioritaria muove dal fatto che il D.lgs. 231/2001 espressamente attribuisce all'OdV autonomi poteri di iniziativa e controllo (art. 6, comma 1, lett. b), nello specifico fine di adempiere al compito di vigilare sul funzionamento e sull'osservanza dei modelli e di curarne il loro aggiornamento.

Proprio sulla base di questa richiesta, si evince come il ruolo dell'OdV possa ricoprire l'azione di vigilanza ove, in sostanza, deve concretizzarsi nella "verifica della coerenza tra i comportamenti concreti ed il modello istituito" (cfr. Linee Guida di Confindustria).

In questo modo si segue una prospettiva dinamica volta al mantenimento dei requisiti di funzionalità del modello e all'aggiornamento dello stesso attraverso proposte rivolte in tal senso agli organi sociali a ciò deputati.

Non esiste un "diritto ad avere" qualsiasi tipo di informazione, celando la richiesta con il "diritto a sapere" come l'azienda impegna le sue risorse finanziarie.

Infatti, le risorse finanziarie dell'Ente, nei protocolli di prevenzione, devono essere amministrate secondo i criteri di massima trasparenza, correttezza e veridicità, in ossequio alla normativa vigente in ambito contabile e fiscale nonché alle procedure previste, in modo da consentire la ricostruzione puntuale di ogni flusso da e verso l'Ente stesso.

Le citate procedure richiamano: il Codice Etico, i poteri, le deleghe e le procure.

L'OdV ha facoltà di acquisire elementi in ordine ai vari rapporti e, ove richiesto a campione, la Società deve esibire all'OdV l'eventuale documentazione richiesta.

Nel rispetto dei poteri di iniziativa e controllo, l'OdV ha facoltà di prendere visione dei documenti concernenti i flussi finanziari al fine di verificarne la corrispondenza, la trasparenza e la univocità degli stessi., risulta infatti ignorato da un sistema di responsabilità da reato calibrato esclusivamente su un modello di società-isola non esaustivo rispetto al panorama societario attuale.

2. L'attuale sistema di controlli: l'obbligo giuridico di attivazione

L'attuale sistema dei controlli risulta così articolato:

- il potere di adottare il Modello di organizzazione, gestione e controllo è attribuito unicamente all'organo dirigente ai sensi dell'art. 2381 c.c.;
- l'obbligo di vigilare sull'adeguatezza, in termini di efficienza e idoneità, del complessivo assetto organizzativo, amministrativo e contabile dell'azienda - quindi, anche sulle procedure di prevenzione contenute nel Modello - spetta al Collegio Sindacale ai sensi dell'art. 2403 c.c.;

Cosa spetta, invece, all'OdV?

All'Organismo di Vigilanza, invece, spetta unicamente l'obbligo di vigilare sul funzionamento e l'osservanza del Modello al fine di riferire gli eventuali malfunzionamenti di una procedura o Ia necessità di un suo aggiornamento, rispettivamente, all'organo dirigente - preposto all'adozione del Modello - e al Collegio Sindacale - quale garante dell'adeguatezza dell'assetto organizzativo aziendale - affinché questi adottino le misure-necessarie.

L'OdV vanta esclusivamente poteri di sorveglianza e controllo, cosicché, una volta venuto a conoscenza di operazioni a rischio-reato, questo non può sostituirsi ai soggetti apicali, ma deve unicamente segnalare al vertice aziendale la violazione perché intervenga per bloccare l'illecito: spetterà, poi, all'organo dirigente decidere se correre o no il rischio della commissione del reato.

Del resto, l'autonomia e l'indipendenza dell'Organismo di Vigilanza dai vertici aziendali sembra cogliersi proprio in questa sua estraneità alla gestione d'azienda.

La giurisprudenza, da parte sua, ritiene che, per "*garantire efficienza e funzionalità, l'organismo di controllo non dovrà avere compiti operativi che, facendolo partecipe di decisioni dell'attività dell'ente, potrebbero pregiudicare la serenità di giudizio al momento delle verifiche*".

Sulla stessa linea interpretativa si è espressa anche Confindustria la quale ha osservato che all'OdV sono "*devoluti compiti di controllo non in ordine alla realizzazione dei reati ma al funzionamento e all'osservanza del modello, curandone, altresì, l'aggiornamento e l'eventuale adeguamento ove vi siano modificazioni degli assetti aziendali di riferimento*"[53].

53 Confindustria Linee Guida pg. 23: "*L'art. 6 nulla dispone circa l'eventuale responsabilità penale all'OdV. Il codice penale prevede una forma di estensione della responsabilità a titolo omissivo per chi, in presenza di un obbligo giuridico, non si sia attivato per impedire il verificarsi dell'evento lesivo (art. 40 cpv. c.p.). AI riguardo, pur dovendosi ritenere che l'organismo abbia compiti limitati a garantire il funzionamento del modello, con esclusione di qualsiasi obbligo di impedimento dei reati che esso mira a prevenire, è opportuno richiamare l'attenzione sui rischi connessi ai casi di dolosa inerzia rispetto a fatti delittuosi derivanti dall'inosservanza del modello di cui l'organismo sia consapevole*".

3. L'attuazione della Direttiva PIF e l'ampliamento del novero dei reati presupposto ex D.lgs. 231/01

Tra le importanti novità previste dalla legge n.157 del 19 dicembre 2019 (entrata in vigore il 25 dicembre 2019), che ha convertito il D.L. n.124/2019 (c.d."Decreto Fiscale"), vi è l'inclusione di taluni reati tributari previsti dal D.lgs. n. 74/2000 tra quelli presupposto della responsabilità amministrativa degli Enti (nuovo art.25-quinquiesdecies del D.lgs. n. 231/2001, introdotto dall'art.39, co.2, del D.L. n.127/2019).

La novella era stata auspicata anche dalla Corte di Cassazione la quale, con la sentenza "*Gubert*", in tema di confisca, suggeriva "*un intervento del legislatore volto ad inserire i reati tributari fra quelli per i quali è configurabile una responsabilità amministrativa dell'ente ai sensi del D.lgs. 8 giugno del 2001, n.231*".Ved. Cass. Pen. Sez. Un., ud. 30 gennaio 2014, dep. 5 marzo 2014, n.10561.

Segnaliamo ai lettori la pubblicazione in Gazzetta Ufficiale del D.lgs. 14 luglio 2020, n. 75 (in G.U. n. 177 del 15 luglio 2020), volto ad adeguare la disciplina penale italiana alla direttiva (UE) 2017/1371 del Parlamento europeo e del Consiglio, del 5 luglio 2017, in tema di lotta contro la frode che leda gli interessi finanziari dell'Unione (c.d."direttiva PIF" – direttiva per la protezione degli interessi finanziari).

La direttiva (VE) 2017/1371 del Parlamento europeo e del Consiglio del 5 luglio 2017 (c.d. direttiva PIF) reca norme per la "***lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale***".

La direttiva sostituisce e aggiorna la precedente Convenzione PIF, già recepita nel nostro ordinamento con l. 300/2000.

Per conformarsi alle disposizioni innovative contenute nella direttiva, il decreto presenta le seguenti principali novità, con alcuni interventi di modifica apportati al decreto in seguito alle osservazioni formulate dalle Commissioni Parlamentari e dei quali si è però tenuto conto nel redigere l'elenco seguente.

1. **Intervenendo sul codice penale**, inasprisce le pene per una serie di reati (**316**, **316-ter**, **319-quater**) quando dalla commissione degli stessi derivi una lesione degli interessi finanziari dell'Unione europea, nonché estende l'area di punibilità di taluni reati (**322-bis**, **640**) per ricomprendervi fatti offensivi dei medesimi interessi;

2. **Intervenendo sul d.lgs. 74/2000**, in relazione ai **delitti dichiarativi di cui agli artt. 2, 3 e 4** è prevista la punibilità a titolo di tentativo (precedentemente esclusa dall'art. 6, cui è ora aggiunto un comma 1-*bis*) nell'ipotesi di atti compiuti anche nel territorio di un altro Stato membro all'interno dell'Unione Europea e finalizzati all'evasione dell'IVA per un valore non inferiore ai dieci milioni di euro;

3. **Intervenendo in tema di elusione dei diritti doganali**, ripristina (dopo la depenalizzazione attuata con D.lgs. n. 8/2016) le sanzioni penali per il reato di contrabbando quando gli importi evasi sono

superiori a diecimila euro e introduce, quale aggravante del reato di contrabbando, l'ipotesi in cui l'ammontare dei diritti non pagati sia superiore a centomila euro;

4. **Intervenendo sul D.lgs. n. 231/2001**, amplia significativamente il catalogo dei reati presupposto, tra cui sono inseriti il **delitto di frode nelle pubbliche forniture**, di **frode in agricolture e di contrabbando**, alcuni **delitti contro la pubblica amministrazione (314, 316, 323)** nei casi in cui da essi derivi un danno agli interessi finanziari dell'Unione europea, nonché alcuni reati tributari non compresi nella recente riforma (l. 157/2019), cioè i delitti di dichiarazione infedele, di omessa dichiarazione e di indebita compensazione, purché rientranti nell'ambito di applicazione della direttiva (v. *supra*, punto 2).

Giova precisare la disposizione del testo normativo: l'art. 1 si limita, sulla base del criterio di delega di cui all'art. 3, comma 1 lett. j), della legge delega, ad apportare le modifiche al codice penale imposte dalla direttiva: agli articoli 316, 316 *ter* e 319 *quater* del codice penale vengono aggiunte le previsioni relative all'ipotesi in cui i fatti ivi previsti e puniti riguardino denaro o utilità sottratti al bilancio dell'Unione o ad organismi della stessa con danno superiore a 100.000 euro: in tale caso è stato previsto – conformemente alle indicazioni della direttiva - un aumento della pena edittale massima fino a quattro anni di reclusione.

In adesione alla delega contenuta nell'art. 3, comma 1 lett. d), della legge delega 4 ottobre 2019, n. 117, si è provveduto ad integrare, con un numero 5-*quinquies*), l'art. 322-*bis* del codice penale al fine di estendere la punibilità a titolo di corruzione dei pubblici ufficiali e degli incaricati di pubblico servizio di Stati non appartenenti all'Unione europea, ove i fatti siano tali da ledere o porre in pericolo gli interessi finanziari euro unitari.

Si è, infine, ritenuto di dover affiancare l'Unione Europea allo Stato ed agli altri enti pubblici quali persone offese del delitto di truffa ai sensi e per gli effetti di cui all'art. 640, comma secondo, numero 1), del codice penale, al fine di realizzare una tutela penale - con procedibilità d'ufficio - degli interessi finanziari dell'Unione nelle ipotesi non coperte dall'art. 640-*bis*.

L'art. 2 interviene, invece, sul D.lgs. 10 marzo 2000, n. 74. La necessità di un **adeguamento dei limiti edittali**, ove il fatto sia commesso anche in parte in altro Stato e l'imposta sul valore aggiunto evasa superi l'importo di dieci milioni di euro, è stata superata dalla recente approvazione di disposizioni che hanno provveduto ad aumentare le pene detentive per i reati dichiarativi, contemplati dalla direttiva.

È stato necessario, invece, **intervenire sull'art. 6 del D.lgs. n. 74/2000** per introdurre, relativamente ai delitti tributari in materia di dichiarazione compresi nell'ambito di applicazione della direttiva, la punibilità del tentativo altrimenti esclusa dal primo comma della disposizione nazionale (art. 3, comma 1 lett. c), della legge delega).

Quanto **all'art. 9 del D.lgs. n. 74/2000**, la disposizione limita la punibilità a titolo di concorso dell'emittente e dell'utilizzatore di fatture relative ad operazioni inesistenti.

Un intervento al riguardo è da ritenersi non necessario. L'esclusione del concorso di persone nel reato è stata, infatti, introdotta dal legislatore nazionale al fine di evitare che un medesimo soggetto sia chiamato a rispondere due volte per il medesimo fatto: una volta per aver emesso le fatture relative ad operazioni inesistenti ed un'altra volta per aver concorso, con l'emissione medesima, nel reato commesso con la dichiarazione fiscale dall'utilizzatore delle fatture medesime.

Poiché la direttiva **riguarda esclusivamente i delitti di dichiarazione**, va osservato che la limitazione all'operatività della regola generale del concorso di persone riguarda esclusivamente colui che è punito, peraltro con le medesime sanzioni penali, ad un differente titolo: ne consegue che non ne deriva alcun vuoto di tutela per gli interessi finanziari dell'Unione, proprio in quanto l'ordinamento italiano punisce già l'emissione delle fatture per operazioni inesistenti quale autonomo titolo di reato.

L'art. 3 apporta modifiche al decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, al fine di garantire che i reati lesivi degli interessi finanziari dell'Unione, ove i danni o i vantaggi siano considerevoli, siano puniti con pena detentiva non inferiore nel massimo a quattro anni di reclusione. Si è ritenuto di intervenire attraverso l'aggiunta di un'aggravante speciale dei delitti di contrabbando ove l'ammontare dei diritti di confine dovuti sia superiore a centomila euro, secondo i limiti fissati dall'art. 7 della direttiva ed in base al criterio di cui alla lett. f) della legge delega.

Dovendosi comunque individuare, per le ragioni esposte in premessa, i reati di contrabbando quali reati direttamente lesivi degli interessi finanziari dell'Unione europea, si è resa necessaria la criminalizzazione di condotte che erano state di recente depenalizzate: con l'art. 4 si è, dunque, inserita un'eccezione alla portata tendenzialmente generale della depenalizzazione disposta con il D.lgs. n. 8/2016 relativamente ai reati puniti esclusivamente con la pena pecuniaria. Coerentemente con quanto previsto dalla direttiva all'art. 7, paragrafo 4, si è limitata la nuova criminalizzazione delle condotte ai casi di reati rispetto ai quali i diritti di confine dovuti siano superiori alla soglia di diecimila euro.

L'art. 5 apporta modifiche al D.lgs. n. 231/2001, volte a completare il quadro della responsabilità amministrativa delle persone giuridiche nel senso indicato dalla direttiva secondo il principio dettato dalla lett. e) dell'art. 3 della legge delega.

In primo luogo è stato necessario intervenire sul terreno dei delitti contemplati dall'art. 24 del D.lgs. n. 231/2001 al fine di comprendere, tra i reati presupposto della responsabilità amministrativa degli enti, il delitto di frode nelle pubbliche forniture ed il reato di frode in agricoltura previsto dall'art. 2 della legge n. 898 del 1986.

In secondo luogo, si è ampliato il panorama dei delitti contro la pubblica amministrazione, includendovi il delitto di peculato nonché quello di abuso d'ufficio, previsti e puniti dagli artt. 314 e 316 del codice penale.

Dei due articoli è stata, conseguentemente, integrata la rubrica.

Il comma 1, lett. c), dell'art. 5 è dedicato all'integrazione delle previsioni **dell'art. 25-*quinquiesdecies* relativo alla responsabilità delle persone giuridiche da delitto tributario**: è stato necessario, infatti, prevedere la responsabilità egli enti – sempre che ricorrano le condizioni di applicazione della direttiva, ovvero la commissione del fatto in parte in territorio di altro Stato membro e un'imposta sul valore aggiunto evasa di almeno dieci milioni di euro - per i delitti non compresi nella disciplina di recente introduzione, ovvero per i delitti di dichiarazione infedele, di omessa dichiarazione e di indebita compensazione.

Con il comma 1, lett. d), infine, è stata introdotta la responsabilità delle persone giuridiche da reato di contrabbando, modulando la sanzione a seconda che il reato ecceda o meno la soglia, individuata in euro centomila, oltre la quale la lesione degli interessi finanziari dell'Unione deve ritenersi considerevole.

L'art. 6 apporta modifiche alla legge 23 dicembre 1986, n. 898 in materia di frodi comunitarie nel settore agricolo, prevedendo nel corpo dell'art. 2 della legge 23 dicembre 1986, n. 898, la fissazione della pena della reclusione fino a quattro anni qualora la somma indebitamente percepita sia superiore a 100.000 euro (art. 3, comma 1, lett. f), della legge di delegazione).

L'art. 7 apporta modifiche di carattere generale, in forza del criterio di delega di cui alla lett. b) del citato art. 3, disponendo che il riferimento alle parole "Comunità europee" dovrà essere inteso come rivolto alle parole "Unione europea".

L'art. 8, in vista della necessaria armonizzazione dei sistemi dell'Unione europea e sulla base di quanto previsto dall'art. 18 della direttiva, dispone che ogni anno il Ministero della giustizia invii alla Commissione europea una relazione contenente dati statistici relativi al numero dei procedimenti iscritti, delle sentenza adottate e dei provvedimenti di archiviazione per i reati lesivi degli interessi finanziari dell'Unione; agli importi delle somme sottoposte a confisca; al valore stimato dei beni, diversi dal denaro, sottoposti a confisca; al danno stimato per l'Unione europea e per le sue istituzioni.

L' art. 9 contiene la clausola di invarianza finanziaria.

4. I reati tributari inseriti nel novero della 231/2001 ex art. 25-quinquiesdecies

L'art. 39, comma 2 del D.L. 124/2019 ha inserito nel catalogo dei reati ex. D.lgs. n. 231/2001, **all'art. 25-*quinquiesdecies***, alcuni **reati fiscali** previsti dal D.lgs. del 10 marzo 2000, n. 74, che fanno scattare la responsabilità amministrativa dell'ente, nello specifico:

- Reato di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.lgs. n. 74/2000);
- Reati di dichiarazione fraudolenta mediante altri artifici (art. 3 D.lgs. n. 74/2000);
- Reati di emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.lgs. n. 74/2000);
- Reato di occultamento o distruzione di documenti contabili (art. 10 D.lgs. n. 74/2000);
- Reato di sottrazione fraudolenta al pagamento di imposte (art.11 D.lgs. n. 74/2000).

Con il **secondo comma** dell'art. 25-*quinquiesdecies* è poi prevista l'applicazione di una circostanza aggravante, che aumenta la pena base se risulta constatato il conseguimento di un "profitto di rilevante entità".

Infine, con il **terzo comma** dell'art 25-*quinquiesdecies*, è prevista l'applicazione, nei casi di condanna, di una sanzione interdittiva.

6. Riflessione conclusiva

Una corretta consapevolezza di una cultura di gestione e controllo deve sia essere essenziale per il perseguimento degli obiettivi di una impresa, che puntare ad un livello strategico di primario livello.

L'importanza dell'indipendenza di funzioni di controllo svolge un ruolo fondamentale in quell'obbiettivo di giudizio e di capacità di esprimere un'opinione che possa considerare totalmente e trasversalmente tutti i fattori a rischio, senza interferenze né condizionamenti esterni.

In questo modo l'attività dei componenti dell'OdV deve erigersi a baluardo di autonomia, con effettivi poteri di controllo e senza essere sottoposto alle dirette dipendenze del soggetto controllato.

7 . Bibliografia

Di GIOVINE, *Lineamenti sostanziali del nuovo illecito punitivo, rilievi critici sui modelli apicali. L'«organismo di controllo», in LATTANZI, Reati e responsabilità degli enti* - Guida al d.lgs. 8 giugno 2001, n.231, JI ed., Milano, 2010, 108

PISANI, *Controlli sindacali e responsabilità penale nelle società per azioni*, Milano, 2003, 106

PIERGALLINI, *La struttura del modello di organizzazione*, cit., 170; ID., Societas delinquere et puniri non potest: *la fine tardiva di un dogma*, in Riv. Trim. dir. pen. econ., 2002, 593

FOGLIA MANZILLO, *Nessun obbligo per l'organo di vigilanza di impedire gli illeciti penali*, in Dir. prat. Soc., 2003, 5, 38

ANTONETTO, *Il regime del rapporto e della responsabilità dei membri dell'Organismo di Vigilanza, in La responsabilità amministrativa delle società e degli enti*, n.1, 2008, 80

PEDRAZZI, *Corporate governante e posizione di garanzia: nuove prospettive*, in A.A.V.V., *Governo delle imprese e mercato delle regole*, Milano, 2002, II, 1375

SGUBBI, *Responsabilità per omesso impedimento dell'evento*, Padova, 1975.

CAPITOLO 6 di Eva Cruellas Sada, Eugenia Gambarara e Irene Picciano

Concorrenza e tutela del consumatore nell'era digitale

SOMMARIO: 1. Introduzione: verso una nuova definizione del mercato digitale europeo – 2. La proposta del Digital Markets Act – 2.1 Introduzione: il Digital Services Act Package – 2.2 La proposta del Digital Markets Act – 2.3 Gatekeepers, regolazione ex ante e nuovi poteri della Commissione – 2.4 Prospettive future, tra scenari protezionistici e "Brussels Effect" – 3. La New Competition Tool – 3.1 Quali sono i problemi di concorrenza strutturali che la NCT andrebbe a risolvere? – 3.2 Le opzioni di policy proposte per la NCT – 3.3 La consultazione, i commenti ed i prossimi passi – 4. Alcuni dei più recenti interventi delle autorità antitrust sui mercati digitali e sui data – 5. Le nuove tendenze in materia di tutela del consumatore nel mondo digital – 5.1 New Deal per i consumatori – 5.2 La Direttiva Omnibus – 5.3 La recente prassi decisionale dell'AGCM – 5.4 Take away

1. Introduzione: verso una nuova definizione del mercato digitale europeo

L'economia digitale pone nuove sfide per il diritto della concorrenza ed il diritto a tutela del consumatore, di fronte alle quali gli attuali strumenti di enforcement rischiano di risultare inadeguati o insufficienti[54]. Si pensi, a titolo esemplificativo, al crescente processo di concentrazione che sta interessando i mercati digitali, con tutti i rischi strutturali e di condotte abusive che ne conseguono e che potrebbero portare al raggiungimento del c.d. *tipping point* e alla conseguente eliminazione della concorrenza. Oltre all'impegno della Commissione Europea ("Commissione") e della Autorità Antitrust nazionali nella piena attuazione degli strumenti di enforcement antitrust già disponibili (incluso il ricorso, ove necessario, a misure cautelari e rimedi di natura strutturale), la Commissione sta portando avanti alcune proposte di riforma per integrare l'attuale disciplina a ed adattarla alle nuove sfide dell'era digitale, tramite (*i*) un set di regolamenti ex ante, volti a prevenire eventuali distorsioni concorrenziali, (*ii*) la c.d. "*New Competition Tool*", finalizzata a poter intervenire in caso di problemi strutturali di concorrenza, nonché (*iii*) l'adozione di nuove norme a tutela dei consumatori - il c.d. "*New Deal for Customers*" - volte a migliorare l'applicazione delle norme vigenti in linea con la costante evoluzione digitale di molti mercati.

54 Cfr. Discorso del Commissario Margrethe Vestager "*Competition in a Digital Age: Changing Enforcement for Changing Times*" in data 26 giugno 2020: https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/competition-digital-age-changing-enforcement-changing-times_en.

2. La proposta del Digital Markets Act

2.1 Introduzione: il Digital Services Act Package

Lo scorso 15 dicembre la Commissione ha pubblicato il testo delle due proposte d'intervento di regolazione del mercato digitale. Segnatamente, il Digital Services Act[55] ("**DSA**") e il Digital Markets Act[56] ("**DMA**") si collocano nell'ambito della nuova strategia digitale UE, tesa a introdurre nuove regole di tutela dei diritti fondamentali e dei consumi degli utenti online, oltre a nuove garanzie per lo sviluppo di un mercato dei servizi digitali equo e competitivo. Per Margrethe Vestager, vice-presidente esecutiva della Commissione e responsabile per la Concorrenza, la nuova strategia europea è infatti sviluppata con l'obiettivo di assicurare da un lato "*l'accesso e l'ampia scelta di prodotti e servici online sicuri" per gli utenti, e dall'altro "una concorrenza libera ed equa online così come offline*" per le imprese[57].

L'intento annunciato dalla Commissione è dunque quello di colmare il gap creatosi con il progressivo sviluppo tecnologico degli ultimi venti anni, durante i quali poche piattaforme hanno continuato ad ampliare i propri servizi fino a diventare veri e propri *gatekeepers*, letteralmente "guardiani" delle interazioni online tra singoli utenti e tra consumatori e imprese. Conscio delle conseguenze potenzialmente patologiche per il mercato e per le libertà degli utenti, il legislatore europeo ha delineato la proposta del *Digital Services Act* e del *Digital Markets Act*, nato, il primo, con l'intento di promuovere la trasparenza e la tutela dei diritti dei consumatori, il secondo con l'obiettivo di fornire un maggiore supporto a potenziali nuovi operatori nel mercato delle piattaforme.

2.2 La proposta del Digital Markets Act

Più nello specifico, il *Digital Markets Act* interviene per la prima volta a determinare il "quanto" le piattaforme possano spingersi ad ampliare il proprio business prima di rischiare di determinare meccanismi potenzialmente patologici per l'economia e la concorrenza del mercato unico digitale. Così facendo, il DMA inserisce una serie di elementi decisivi nel contesto di sostanziale non-regolazione che fino ad oggi ha caratterizzato l'evoluzione del Digital Single Market europeo.

55 *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. Il testo della proposta è disponibile in inglese al link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en.

56 *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*. Il testo della proposta è disponibile in inglese al link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en

57 Traduzione libera. Nel commento integrale: "*The two proposals serve one purpose: to make sure that we, as users, have access to a wide choice of safe products and services online. And that businesses operating in Europe can freely and fairly compete online just as they do offline. This is one world. We should be able to do our shopping in a safe manner and trust the news we read. Because what is illegal offline is equally illegal online.*" Si veda il comunicato stampa della Commissione europea ("**Commissione**") pubblicato il 15 dicembre 2020, disponibile all'indirizzo https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347.

È importante notare che entrambe le proposte introducono misure differenziate in relazione ai diversi *digital players*, parametrati sulle dimensioni e sulle tipologie di servizi offerti da ciascuna piattaforma. Sotto questo profilo, già in fase di presentazione dell'iniziativa del *Digital Services Act Package* (che comprende sia DSA che DMA), la Commissione aveva manifestato l'intenzione di intervenire a regolare prevalentemente le "*very large online platforms acting as gatekeepers*". Tale iniziativa deriva dalla considerazione, riportata all'interno dell'*Impact Assessment* prodromico alla pubblicazione delle due proposte[58] (e ripresa nel preambolo del DMA), che sebbene nel mercato digitale europeo operino ad oggi oltre 10,000 piattaforme online, la maggioranza del mercato è di fatto controllata da una compagine ristrettissima di grandi piattaforme, che negli ultimi venti anni hanno potuto beneficiare senza limitazioni di un effetto di rete che rivela le proprie conseguenze solo oggi. La pubblicazione delle due proposte lo scorso 15 dicembre ha rivelato dunque i parametri quantitativi individuati dalla Commissione per determinare in quali circostanze una piattaforma debba essere sottoposta al regime dei c.d. "*gatekeepers*". Se da un lato il DSA si applica a tutti gli intermediari digitali[59], prevedendo ulteriori misure per le piattaforme che risultano utilizzate da almeno il 10% dei 450 milioni di consumatori europei, il DMA si applica invece solamente ai principali provider di servizi presenti nell'ecosistema digitale. Più nel dettaglio, il DMA limita il proprio ambito di applicazione ad un elenco chiuso di otto tipi di servizi digitali, definiti direttamente nella Proposta come "*core platform*": servizi di intermediazione (es. *marketplace* o *app store*); motori di ricerca; *social network*; piattaforme di condivisione video (es. Youtube); servizi di comunicazione interpersonali indipendenti dal numero telefonico (es. Facebook Messenger); sistemi operativi (es. iOS, Android); servizi di *cloud computing*; fornitori di piattaforme pubblicitarie (es. Google AdSense)[60]. Tra i *provider* di *core platform* si individuano poi, grazie ai parametri stabiliti all'articolo 3 della proposta di Regolamento, i c.d. "*gatekeepers*". L'articolo prevede che, per essere sottoposta alle regole previste per i *gatekeepers*, una piattaforma debba:

1) Avere un impatto significativo sul mercato interno;

2) Gestire un servizio rilevante, che rappresenta cioè un punto di collegamento significativo tra utenti commerciali e utenti finali;

3) Godere di una posizione consolidata e duratura nel settore in cui opera.

58 Inception Impact Assessment "*Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the european Union's internal market*", pubblicato il 2 giugno 2020. Il documento è disponibile al link: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers.

59 Il DSA prevede che le piattaforme siano suddivise in progressivi sottogruppi, partendo dagli "*intermediary services*" fino ad arrivare alle "*very large online platforms*". Più nel dettaglio, si intendono: (*i*) *intermediary services* tutti quei servizi che offrono una infrastruttura digitale, compresi servizi di accesso alla rete e registrar di domini di primo livello; questa prima categoria a sua volta include (*ii*) *hosting services,* come *cloud* e servizi di *webhosting*, i quali a loro volta includono il sottogruppo delle (*iii*) *online platform*, come *online marketplace*, *app store* e *social media*; tra questi si riscontra poi una ristretta categoria di (*iv*) *very large online platform*, ossia quelle piattaforme che mettono a disposizione il proprio servizio ad almeno il 10% degli utenti europei (45 milioni di utenti).

60 Art. 2(2) della Proposta.

In base al regime delle presunzioni stabilite allo stesso articolo 3, il primo dei tre criteri si considera soddisfatto se l'impresa cui appartiene la piattaforma ha generato un fatturato annuo all'interno dello spazio economico europeo pari o superiore a 6,5 miliardi di euro nell'ultimo esercizio finanziario e se fornisce un servizio di piattaforma di base in almeno tre Stati membri. Il secondo requisito, relativo alla gestione di uno spazio considerato centrale per l'economia, si considera soddisfatto se la piattaforma, nell'esercizio precedente, ha fornito il proprio servizio a più di 45 milioni di utenti finali attivi mensilmente, stabiliti o situati nell'Unione, e a più di 10.000 utenti commerciali attivi aventi sede nel territorio dell'Unione. Infine, si presume che una piattaforma goda di una posizione consolidata e duratura qualora abbia fornito il proprio servizio, negli ultimi tre esercizi finanziari, a più di 45 milioni di utenti finali attivi mensili stabiliti o situati nell'Unione e a più di 10.000 utenti commerciali attivi annui stabiliti nell'Unione.

Non si tratta quindi solamente delle GAFAM (Google, Amazon, Facebook, Apple, Microsoft), ma anche di piattaforme come TikTok, eBay, Google, Expedia, Spotify, Telegram ecc. Tutte piattaforme che, al di là delle deviazioni di alcune pratiche, hanno portato incredibili benefici sia ai consumatori che alle imprese stabiliti nel territorio UE. Sotto il profilo procedurale, l'art. 3(3) della proposta prevede un obbligo di notifica in capo a quelle piattaforme che si trovino a soddisfare i requisiti di cui sopra. A questo seguirà un'aggiuntiva valutazione da parte della Commissione, alla quale viene rimesso in ultima istanza il potere di determinare la qualifica della piattaforma. In aggiunta a questi parametri indicativi, la proposta del DMA prevede anche che la Commissione avrà il potere di qualificare direttamente un *gatekeeper* come tale in seguito ad un'indagine sul mercato[61]. Qualora la Commissione si sia basata su elementi incompleti, inesatti o fuorvianti, o nel caso in cui la situazione fattuale relativa al presunto *gatekeeper* abbia subito modifiche consistenti, la Commissione potrà riesaminare la propria decisione ed eventualmente modificare la qualifica della piattaforma[62].

2.3 Gatekeepers, regolazione ex ante e nuovi poteri della Commissione

L'attuale normativa antitrust prevede un approccio correttivo puramente ex post da parte della Commissione, che può quindi intervenire soltanto dopo aver accertato la presenza di comportamenti lesivi della concorrenza, spesso al termine di indagini che possono durare interi mesi. Ne deriva una generale incapacità di reagire in maniera tempestiva alle pratiche anticoncorrenziali che fino ad oggi sono state messe in atto da alcune piattaforme. Al netto dell'analisi svolta dalla Commissione su tali criticità, la scelta è stata quella di stravolgere l'approccio normativo preesistente introducendo un sistema di regolazione ex ante, con la precisa individuazione di pratiche vietate e obblighi di trasparenza. Tale applicazione dovrebbe servire non soltanto ad accorciare i tempi di intervento delle autorità, ma anche a fornire linee guida più chiare alle grandi piattaforme che vogliono operare lecitamente nel mercato.

61 Art. 3(4) della Proposta.

62 Art. 4 della Proposta.

Più nello specifico, l'introduzione di una normativa *ex ante* prevede (al Capo III della Proposta) la definizione di una serie di condotte illecite incluse in una "*blacklist*" vincolante per tutti i *gatekeepers*. Si tratta di esempi mutuati in gran parte dalle pratiche scorrette che già in passato, come descritto nel paragrafo precedente, sono state sottoposte ad indagini e sanzionate dall'Antitrust: *self-preferencing*; utilizzo di dati raccolti sugli utenti commerciali per formulare strategie competitive contro le stesse imprese che utilizzano il servizio; ingiustificato diniego di accesso alle funzionalità della piattaforma o ai dati raccolti dall'utenza; pratiche ingiustificate di *tying* o *bundling* nell'offerta di beni o servizi; imposizione di termini poco chiari agli utenti; ecc. A queste si aggiungono una serie di obblighi (la "*whitelist*"): autorizzare l'installazione e l'utilizzo di software di terze parti; favorire soluzioni di interoperabilità; consentire agli utenti commerciali, gratuitamente, l'accesso agli indicatori di performance disponibili tramite la piattaforma; consentire agli stessi utenti l'accesso a dati aggregati e non aggregati raccolti tramite le loro interazioni sulla piattaforma; ecc. Entrambe queste categorie sono illustrate agli artt. 5 e 6 della Proposta, suddivise tra misure auto-applicative e misure che potranno essere soggette ad ulteriori specificazioni. In relazione a questa seconda categoria, l'art. 7 stabilisce un quadro di riferimento per la creazione di un meccanismo di dialogo tra *gatekeeper* e Commissione: ove le misure messe in atto dal primo per attuare gli obblighi previsti all'art. 6 siano considerate insufficienti, così come nel caso in cui lo stesso *gatekeeper* voglia sottoporre tali misure ad un vaglio di efficacia, la Commissione deve intervenire per specificare le corrette soluzioni da adottare. Le misure fino a qui previste possono essere derogate solamente in caso di sospensione richiesta in circostanze eccezionali (art. 8) o per superiori motivi di interesse pubblico (art. 9).

Le ulteriori disposizioni presenti al Capo III definiscono il meccanismo di aggiornamento dell'elenco degli obblighi previsti agli art. 5 e 6 (art. 10); precisano che gli obblighi introdotti dal Regolamento si applicano indipendentemente dal fatto che le condotte del *gatekeeper* siano di natura contrattuale, commerciale, tecnica o di qualsiasi altra natura (art. 11); ribadiscono l'obbligo di notificare qualsiasi progetto di concentrazione ai sensi del Regolamento (CE) n. 139/2004 (art. 12); e introducono infine l'obbligo per il *gatekeeper* di prevedere un audit indipendente per qualunque trattamento di profilazione dei consumatori adottato tramite la piattaforma (art. 13).

In ogni caso, la previsione di norme *ex ante* non interviene a sostituire, ma solamente ad integrare, il potere di indagine ed enforcement ex post che già la Commissione riveste in funzione di autorità antitrust europea. Gli articoli da 18 a 24 contengono infatti i requisiti procedurali per avviare un'indagine e definiscono il ruolo investigativo della Commissione, che si vede attribuire nuove funzioni e poteri. Potrà infatti intervenire direttamente in caso di individuazione di problemi competitivi strutturali, anche in assenza di un accertato illecito da parte delle società dominanti, operando con funzioni simili a quelle previste per la *Digital Market Unit* dell'autorità antitrust britannica (*Competition and Markets Authority*). Nel preambolo della proposta di regolamento, la Commissione chiarisce tuttavia che tali misure devono limitarsi a quanto necessario

e giustificato per affrontare il problema derivante dalla ricorrenza di determinate pratiche sleali perpetrate *gatekeepers* e per garantire (considerando n. 27 e 34). In linea con tale considerazione, all'art. 1 del *Digital Markets Act* si specifica che gli Stati membri non dovranno imporre ai *gatekeepers* – tramite disposizioni legislative o amministrative – ulteriori obblighi finalizzati a garantire mercati liberi e competitivi.

Per quanto riguarda le sanzioni, in caso di violazione degli obblighi previsti nel DMA le multe possono raggiungere fino al 10% del fatturato annuo mondiale della società, con penalità di mora fino al 5% del fatturato medio giornaliero. Infine, se in caso di mancata adesione alle misure sanzionatorie ordinate dalla Commissione, la violazione sistematica delle norme potrà portare anche all'applicazione di rimedi di natura straordinaria, quali l'obbligo di cessione di parte degli asset aziendali o delle proprietà aziendali (*splitting*).

2.4 Prospettive future, tra scenari protezionistici e "Brussels Effect"

Alcuni commentatori, vedono in questa strategia una esemplificazione del c.d. "Brussels Effect"[63]. Secondo questi ultimi, l'UE starebbe per ripercorrere con il *Digital Services Act Package* le stesse fasi che si sono susseguite poco dopo l'approvazione e l'implementazione del Regolamento generale per la protezione dei dati personali n. 2016/679 ("**GDPR**"), arrivando così anche in questo caso a rivestire il ruolo di "global standard maker" per i futuri interventi normativi operati all'estero[64].

Quello che in ogni caso è certo è che, come già successo con la Direttiva e-Commerce, il Digital Services Act e il Digital Markets Act, una volta approvati, comporteranno una radicale riorganizzazione del panorama digitale odierno, ridefinendo, almeno per i prossimi decenni, il rapporto tra le varie piattaforme e tra i servizi digitali e i consumatori.

Ciò che invece resta da definire, tra le altre cose, è come le disposizioni del DMA si coordineranno con le altre normative che hanno già contribuito a plasmare in maniera consistente l'assetto del mercato digitale europeo negli ultimi anni. Primo tra tutti il GDPR, fondato sul principio cardine di minimizzazione del trattamento, che subordina il trasferimento di dati a terze parti alla prestazione di un consenso libero, specifico, informato ed inequivocabile da parte degli interessati.

63 L'espressione trae ispirazione dal titolo del paper di Anu Bradford, docente della Columbia Law School (*The Brussels Effect*, 107 Nw. U. L. Rev. 1 (2012)) e divenuto successivamente un libro "*The Brussels Effect: How the European Union Rules the World*" (2019).

64 Nel caso del GDPR, l'iniziativa legislativa europea ha fornito un esempio e uno standard di regolazione che è poi stato ripreso dal California Consumer Privacy Act (CCPA) entrato in vigore il 1° gennaio 2020, ma anche da nuovi progetti di riforma che sono stati intrapresi in Brasile, Cina, India, Giappone, Corea del Sud, Thailandia e, più recentemente in Australia.

L'iter legislativo delle due proposte è ancora in una fase iniziale e senz'altro bisognerà aspettare prima di arrivare alla definizione concreta delle regole che condurranno l'Europa verso una nuova fase di regolamentazione del mondo digitale. Nel frattempo, spetterà alle autorità antitrust continuare a cercare un bilanciamento tra i vari interessi in gioco e apportare dei correttivi *ex post* alle attuali inefficienze del mercato unico digitale.

3. La New Competition Tool

Il 2 giugno 2020, la Commissione ha aperto una consultazione pubblica relativa alla proposta di introdurre un nuovo strumento normativo (la cosiddetta *New Competition Tool* o "**NCT**")[65], basato sull'articolo 103 TFUE in combinazione con l'articolo 114 TFUE, che dovrebbe essere volto a colmare le lacune delle attuali regole europee a tutela della concorrenza e a consentire un intervento tempestivo ed efficace nei confronti dei problemi strutturali di concorrenza che caratterizzano alcuni mercati, specialmente nel contesto digitale, che non possono essere risolti attraverso l'applicazione delle norme a tutela della concorrenza.

Al riguardo, Margrethe Vestager, vice-presidente esecutiva della Commissione e responsabile per la Concorrenza, ha affermato "*The world is changing fast and it is important that the competition rules are fit for that change. Our rules have an inbuilt flexibility which allows us to deal with a broad range of anti-competitive conduct across markets. We see, however, that there are certain structural risks for competition, such as tipping markets, which are not addressed by the current rules. We are seeking the views of stakeholders to explore the need for a possible new competition tool that would allow addressing such structural competition problems, in a timely and effective manner ensuring fair and competitive markets across the economy*"[66].

Nel *Inception Impact Assessment* (i.e. valutazione d'impatto iniziale), pubblicato dalla Commissione all'avvio della consultazione, si sottolinea che alla base di questa iniziativa vi sono le caratteristiche intrinseche che si riscontrano in alcuni mercati - quali economie di scala, forti effetti di rete e dipendenza dei dati - così come alcune dinamiche di mercato che favoriscono improvvise e radicali diminuzioni di concorrenza (cosiddetto "*tipping*") e scenari cosiddetti "*winner-takes-most*". Come la Commissione ha osservato in alcuni recenti casi, queste caratteristiche possono rendere molto difficile contrastare una posizione di potere di mercato o di dominanza una volta tale posizione sia stata acquisita da un'impresa (cfr., *inter alia*, M.8124 *Microsoft/LinkedIn* e AT.37.990 *Intel*).

Queste caratteristiche, peraltro, sono tipiche dei mercati digitali, ma si possono trovare anche nei mercati non digitali. Inoltre, con la generale crescente digitalizzazione dell'economia, sempre più mercati mostreranno queste caratteristiche, e le differenze tra i mercati digitali e non digitali diventeranno sempre meno evidenti.

65 Cfr. Comunicato Stampa della Commissione del 2 giugno 2020 all'avvio della consultazione sulla *New Competition Tool* al seguente Link: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_977

66 Cfr. Comunicato Stampa cit. a nota piè di pagina 12.

Infatti, sebbene la proposta di NCT sia stata inserita nel pacchetto degli interventi sui servizi digitali dell'UE (cfr. Sezione B), che raggruppa varie iniziative politiche anche di altre direzioni generali della Commissione, la NCT non sarà necessariamente limitata ai mercati digitali e abilitati digitalmente. Infatti, nel citato *Inception Impact Assessment*, si fa riferimento a possibili iniziative che riguarderebbero tutti i settori dell'economia o, almeno, i settori in cui i problemi strutturali sono visti come prevalenti. Pertanto, anche se la proposta potrebbe essere vista come un'ulteriore iniziativa per adattare la normativa alle dinamiche competitive dell'economia digitale, in realtà, se analizzata nel dettaglio, la proposta di *New Competition Tool* risulta di più vasta portata e potrebbe dare luogo ad un vero e proprio cambiamento radicale nella politica della concorrenza nell'UE.

La Commissione evidenzia nel *Inception Impact Assessment* che la crescente concentrazione dei mercati può consentire alle imprese il monitoraggio dei comportamenti dei concorrenti e ridurre la pressione concorrenziale attraverso forme di collusione tacita. La possibilità di utilizzo degli algoritmi, aumentando la trasparenza, può comportare questi rischi anche in mercati meno concentrati.

In questo contesto, potrebbero emergere problemi strutturali di concorrenza che, pur avendo un impatto negativo sulla concorrenza - potendo produrre inefficienze in termini di aumento dei prezzi, diminuzione della qualità, riduzione della scelta e dell'innovazione - resterebbero esclusi dall'ambito di applicazione delle norme a tutela della concorrenza, i.e. gli articoli 101 e 102 del Trattato sul Funzionamento dell'Unione Europea ("**TFUE**").

3.1 Quali sono i problemi di concorrenza strutturali che la NCT andrebbe a risolvere?

Nello specifico, la Commissione ha sottolineato che i suddetti problemi strutturali possono emergere in numerosi diversi scenari, che possono tuttavia essere raggruppati in **due categorie**:

- **i rischi strutturali per la concorrenza**, legati a situazioni in cui determinate caratteristiche dei mercati (ad esempio, gli effetti di rete e di scala, l'indisponibilità di *multi-homing* e gli effetti di *lock-in*), insieme alla condotta delle imprese che operano in tali mercati, creano rischi per la concorrenza. Questo è particolarmente vero per i mercati a rischio di "*tipping*", cioè di eliminazione della concorrenza sul mercato, in cui i rischi per la concorrenza derivano dalla creazione di potenti operatori di mercato con una posizione di mercato e/o di *gatekeeper* radicata che potrebbe essere prevenuta con un intervento precoce. Altri scenari che rientrano in questa categoria includono strategie unilaterali di società non dominanti per monopolizzare un mercato con mezzi anticoncorrenziali;
- **la carenza strutturale di concorrenza** (fallimento strutturale del mercato) che si riscontra in quei mercati in cui, in presenza di determinate caratteristiche sistemiche del mercato, non si sviluppa la concorrenza.

Ad esempio, i mercati possono mostrare fallimenti sistemici dovuti a determinate caratteristiche strutturali quali l'elevata concentrazione e la presenza di barriere all'entrata, il lock-in dei consumatori, la mancanza di accesso ai dati o l'accumulo di dati. Allo stesso modo, strutture di mercato oligopolistiche aumentano il rischio di collusione tacita, compresi i mercati in cui soluzioni tecnologiche basate su algoritmi determinano una maggiore trasparenza.

Di fronte a questo contesto, l'obiettivo generale della NCT è garantire una concorrenza leale e non falsata nel mercato interno, consentendo alla Commissione di intervenire laddove sussistano problemi che impediscano ai mercati di funzionare correttamente, favorendo uno o pochi concorrenti.

3.2 Le opzioni di policy proposte per la NCT

Nello specifico, nel *Inception Impact Assessment*, la Commissione delinea quattro possibili opzioni per la proposta *New Competition Tool*:

1. **Uno strumento di portata orizzontale basato sulla nozione di dominanza**, che consentirebbe di affrontare le preoccupazioni concorrenziali derivanti dalla condotta unilaterale delle imprese dominanti senza la necessità di accertare previamente una violazione dell'articolo 102 TFUE. Lo strumento si applicherebbe a tutti i settori economici e consentirebbe alla Commissione, in cooperazione con le Autorità Nazionali, di intervenire prima che un'impresa in posizione dominante possa adottare comportamenti escludenti nei confronti dei concorrenti. Lo strumento consentirebbe alla Commissione di imporre rimedi comportamentali e se del caso, rimedi strutturali. Tuttavia, la Commissione non accerterebbe alcuna violazione della normativa antitrust né imporrebbe ammende e quindi non si genererebbero diritti al risarcimento dei danni.
2. **Uno strumento basato sulla nozione di dominanza**, con caratteristiche analoghe a quello di cui all'opzione 1 ma con una portata più limitata in quanto sarebbe applicabile solo nei settori in cui emergono con più evidenza problemi strutturali di concorrenza, tra cui alcuni mercati digitali o abilitati al digitale e/o altri settori particolarmente inclini a suscitare le suddette preoccupazioni a causa della sussistenza di posizioni dominanti radicate, alte barriere all'ingresso, ecc.
3. **Uno strumento basato sulla struttura del mercato**, che consentirebbe alla Commissione di identificare e porre rimedio a problemi di concorrenza strutturale che non possono essere affrontati (affatto o in modo altrettanto efficace) in base alle regole di concorrenza dell'UE. Pertanto, a differenza delle opzioni 1 e 2, non sarebbe limitato solo alle società che sono già dominanti. Questo strumento sarebbe basato su un test che consentirebbe alla Commissione di intervenire quando un rischio strutturale per la concorrenza o una mancanza strutturale di concorrenza impedisca al mercato di funzionare correttamente.

Lo strumento consentirebbe alla Commissione di imporre misure comportamentali e, dove appropriato, rimedi strutturali. La Commissione potrebbe anche raccomandare un'azione legislativa per migliorare il funzionamento del mercato interessato. Come per le opzioni precedenti, non ci sarebbe alcun accertamento di una violazione della normativa antitrust né sarebbero imposte ammende e quindi non si genererebbero diritti al risarcimento dei danni.

4. **Uno strumento basato sulla struttura del mercato ma con portata limitata** ai settori in cui emergono con più evidenza problemi strutturali di concorrenza. Analogamente allo strumento presentato nell'opzione 3, questa opzione affronterebbe i problemi di concorrenza strutturale. Nell'opzione 4, tuttavia, l'utilizzo dello strumento sarebbe limitato ai settori in cui le problematiche identificate sono prevalenti. Questi potrebbero includere alcuni mercati digitali o abilitati al digitale e/o altri settori identificati come particolarmente inclini a suscitare le suddette preoccupazioni a causa della sussistenza di posizioni dominanti radicate, alte barriere all'ingresso, ecc.

Pertanto, la NCT potrebbe essere basata sulla posizione dominante ovvero sulla struttura del mercato, potrebbe applicarsi a tutti i settori ovvero essere limitata a settori specifici che sono particolarmente inclini a problemi di dominanza/preclusione, come i mercati digitali o abilitati digitalmente. Negli scenari basati sulla posizione dominante, la Commissione avrebbe il diritto di intervenire solo per impedire che le società in posizione dominante abusino del loro potere di mercato. Negli scenari basati sulla struttura del mercato, i poteri della Commissione sarebbero più ampi e consentirebbero di intervenire, anche in assenza di posizione dominante, in relazione a problemi di concorrenza strutturale che non possono essere affrontati sulla base delle regole di concorrenza esistenti. In tutte le possibili opzioni, la Commissione condurrebbe indagini di mercato volte a identificare problemi concorrenziali nei mercati e a imporre gli eventuali adeguati rimedi (comportamentali o strutturali), ma la Commissione non accerterebbe nessuna infrazione della normativa antitrust né imporrebbe sanzioni e, di conseguenza, non si genererebbero diritti al risarcimento dei danni.

Nel *Inception Impact Assessment*, la Commissione ha analizzato il possibile impatto delle suddette quattro opzioni sotto diversi profili (economico, sociale, ambientale, sui diritti fondamentali, sulla semplificazione del *pubblic enforcement*).

Anche se nessuna delle quattro opzioni prevedrebbe l'accertamento di una violazione della normativa antitrust o l'imposizione di ammende, e nessuna quindi potrebbe generare azioni per il risarcimento dei danni antitrust, lo strumento conferirebbe alla Commissione poteri molto ampi tra cui l'imposizione di misure comportamentali e/o strutturali.

L'intervento potrebbe quindi essere di vasta portata poiché i rimedi strutturali potrebbero includere scissioni o cessioni di azienda, e i rimedi comportamentali potrebbero implicare obblighi molti diversi, dalle modifiche alle politiche di determinazione dei prezzi e distribuzione agli obblighi di separazione interna, ad esempio. A oggi, tuttavia, la Commissione ha lasciato ampiamente aperta la possibilità di decidere quale tipo di misure applicare nella pratica.

3.3 La consultazione, i commenti ed i prossimi passi

Come sopra indicato, il nuovo strumento si baserebbe sugli articoli 103 e 114 del TFUE e richiederebbe pertanto l'approvazione del Consiglio e del Parlamento europeo. Data la significativa espansione dei poteri della Commissione che la proposta prevede e le preoccupazioni di alcuni Stati membri, la proposta sta suscitando un notevole dibattito. Nello specifico, la consultazione sul *Inception Impact Assessment* si è conclusa il 30 giugno con la partecipazione di 85 soggetti mentre la consultazione sulla proposta di NCT in generale si è conclusa il 9 settembre 2020 con la partecipazione di 188 *stakeholders*[67] e 27 autorità antitrust nazionali[68].

Molti *stakeholder* europei ritengono che la normativa attualmente in vigore sia efficace e sufficientemente flessibile per combattere i più comuni problemi di concorrenza nei mercati, compresi quelli più innovativi e digitali. Sono quindi stati espressi ragionevoli dubbi sulla reale necessità di dotare la Commissione di un nuovo strumento così ampio a tutela della concorrenza e sui rischi che tale nuovo strumento causi una situazione di eccessiva incertezza per le imprese e possa anche limitare la libertà di impresa. Infatti, è stata sottolineata la differenza significativa tra una disciplina che consenta solo di formulare raccomandazioni ai legislatori - come quella ad oggi esistente *inter alia* in Italia, dove l'Autorità antitrust italiana (Autorità Garante della Concorrenza e del Mercato "**AGCM**") può segnalare al Parlamento e al Governo le situazioni distorsive derivanti da provvedimenti legislativi o amministrativi, ai sensi dell'art. 21 Legge n. 287/90 - e un regime, come quello proposto dalla NCT, che consenta all'Autorità di concorrenza di imporre rimedi e obblighi diretti e specifici alle imprese che operano in un determinato mercato.

Anche alcune autorità antitrust nazionali hanno espresso dubbi in relazione alla proposta di NCT (si veda, ad esempio, la posizione dell'autorità antitrust spagnola[69]). Mentre, in altri paesi, invece, sono già presenti misure simili alla NCT. In particolare, il regime di indagini di mercato (*Market Investigation Regime* o "**MIR**") nel Regno Unito conferisce all'autorità antitrust in tale paese ("**CMA**") poteri molti ampi per imporre rimedi e misure ai fini di risolvere

67 Un riassunto delle contribuzioni da parte degli *stakeholders* può essere consultato al seguente link: https://ec.europa.eu/competition/consultations/2020_new_comp_tool/summary_stakeholder_consultation.pdf.

68 Un riassunto delle contribuzioni da parte delle Autorità antitrust nazionali può essere consultato al seguente link: https://ec.europa.eu/competition/consultations/2020_new_comp_tool/summary_contributions_NCAs_responses.pdf

69 Si veda al seguente link: https://www.cnmc.es/sites/default/files/editor_contenidos/Notas%20de%20prensa/2020/CNMC%20position%20paper%20on%20DSA%20and%20NCT.pdf.

problemi concorrenziali[70], che non ricadono nell'ambito della normativa antitrust, laddove sussista un cosiddetto effetto avverso sulla concorrenza (adverse effect on competition o "**AEC**")[71]. Gli insegnamenti acquisiti nel Regno Unito in relazione a questo regime fortemente contestato prefigurano il dibattito che la Commissione dovrà affrontare nell'analisi dei risultati della consultazione e anche successivamente nell'applicazione della NCT, qualsiasi sia l'opzione scelta, che sarà eventualmente adottata a seguito del completamente dell'iter legislativo a livello dell'UE.

In particolare, diverse voci hanno segnalato che laddove la NCT sia effettivamente introdotta sarà necessario fornire chiare indicazioni sui requisiti e le soglie che potranno fare scattare l'avvio di un'indagine approfondita e l'uso dei poteri previsti dalla NCT da parte della Commissione nonché sull'onere della prova in capo alla Commissione per dimostrare la sussistenza di un problema concorrenziale nel mercato e la necessità di imporre misure. Inoltre, occorrerà adottare adeguate misure per assicurare il contraddittorio e la tutela dei diritti di difesa delle imprese coinvolte nonché regole che garantiscano l'applicazione di rimedi obiettivi, proporzionali ed efficaci e provvisti da sufficiente supporto probatorio.

La Commissione aveva previsto di presentare la valutazione definitiva sull'impatto della proposta di NCT, a valle della consultazione, entro l'ultimo trimestre del 2020. Siamo dunque in attesa di conoscere le valutazioni finali della Commissione ed il perimetro e le specifiche caratteristiche della proposta definitiva di regolamento per l'introduzione della NCT che presenterà la Commissione.

4. Alcuni dei più recenti interventi delle autorità antitrust sui mercati digitali e sui data

Dopo aver illustrato le proposte di riforma elaborate dalla Commissione, sembra utile fare un breve cenno ad alcuni casi rilevanti, a livello italiano ed europeo, nei quali sono emerse le nuove problematiche concorrenziali nel contesto dell'economia digitale.

Le aziende tecnologiche hanno fino ad ora navigato in una zona grigia che per le sue caratteristiche è quasi sempre riuscita a sfuggire ai limiti tradizionalmente imposti dalla regolazione dei mercati in senso pro-competitivo. Nonostante questo, le indagini e le sanzioni imposte dalle autorità antitrust negli ultimi anni, sia a livello europeo che nazionale, avevano già indicato una radicale deviazione verso un più attento controllo delle dinamiche in atto nei mercati digitali e, in particolare, sulle piattaforme digitali.

70 Altri paesi dove le autorità garanti della concorrenza possono svolgere indagini di mercato e imporre rimedi per risolvere eventuali problemi di concorrenza risulterebbero Grecia, Islanda, Messico e Sudafrica.

71 AEC è definito come lo scenario in cui le caratteristiche o combinazione di caratteristiche presenti in un mercato limitino, impediscano o restringano la concorrenza.

Già a partire dai primi mesi di applicazione del GDPR, la lente delle autorità per la protezione dei dati personali si è concentrata sui *business model* e sulle pratiche messe in atto dalle grandi piattaforme, portando anche a sanzioni per l'ammontare di svariati milioni di euro[72]. Più recentemente, tuttavia, l'utilizzo dei dati da parte delle stesse piattaforme è stato oggetto di scrutinio anche da parte delle autorità antitrust, che hanno riscontrato nel controllo di grandi quantità di dati l'indizio di un problema sistemico all'interno del mercato digitale. Oggi, infatti, anche i dati e il loro trattamento rappresentano fattori decisivi per la concorrenza tra piattaforme online. Se per due decenni le autorità garanti dell'UE hanno scelto di non intervenire a contrastare in maniera diretta i problemi di concorrenza derivanti dalla concentrazione dei dati, d'altro canto anche i tribunali hanno metodicamente relegato l'analisi dei trattamenti operati dei *tech giant* ai soli parametri che disciplinano la protezione dei dati[73]. Più di recente, tuttavia, le autorità garanti della concorrenza a livello nazionale e sovranazionale hanno posto sempre più l'accento sull'interconnessione tra le concentrazioni di dati e i disequilibri presenti all'interno del mercato digitale.

Per fornire un esempio, la Commissione ha già riscontrato l'utilizzo di metodi anticoncorrenziali da parte di Google – tra cui *self-preferencing* e pratiche abusive di *online advertising* – prevedendo più sanzioni per un totale di 8,4 miliardi di euro comminate tra il 2017 e il 2019[74]. Più recentemente, la Commissione ha svolto delle indagini in merito all'intenzione di Google di acquisire FitBit, sollevando le criticità relative in particolare all'utilizzo per finalità di *targeted marketing* dei dati raccolti dai dispositivi indossabili.

72 Tra le più recenti, si veda le sanzioni del CNIL contro Google e Amazon per l'utilizzo di sistemi di tracciamento a fini di promozione pubblicitaria senza aver ottenuto il preventivo consenso degli utenti. L'Autorità garante francese ha sanzionato Amazon per 35 milioni di euro (https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core) e Google per un totale di 100 milioni di euro (https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland).

73 Un primo esempio in senso contrario si presentato lo scorso giugno, quando la Corte federale tedesca ha confermato l'analisi del Federal Cartel Office (Bundeskartellamt) che riscontrava nella raccolta dei dati sugli utenti operata da Facebook un indizio di abuso di posizione dominante sul mercato. L'autorità per la concorrenza tedesca aveva già ordinato a Facebook di cessare la pratica che prevedeva di combinare i dati provenienti dai diversi servizi di sua proprietà senza il preventivo consenso dell'utente allo scopo di generare dei "super profili". L'ordine del Federal Cartel Office era stato sospeso dalla Corte regionale di Dusseldorf a seguito dell'appello di Facebook, e si trova ora davanti alla Corte Federale tedesca, che ne ha confermato l'efficacia in via provvisoria in attesa di esprimersi sul merito della questione. Si veda la traduzione inglese del comunicato stampa della Corte, federale disponibile all'indirizzo https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2020/23_06_2020_BGH_Facebook.pdf?__blob=publicationFile&v=2.

74 I testi dei provvedimenti della Commissione sono disponibili ai seguenti link: • Google Shopping, 27 giugno 2017: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784; • Android, 18 luglio 2018: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581; • Google AdSense, 20 marzo 2019: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770.

La Commissione ha dato il via libera all'acquisizione lo scorso 17 dicembre, prevedendo per Google una serie di impegni che per i prossimi 10 anni (rinnovabili per ulteriori dieci) limiteranno la posizione dominante di Google sul mercato degli *smartwatch*. Tali impegni in ogni caso, come specificato dalla stessa Commissione, non esimeranno la società dalle ulteriori misure previste nella futura versione approvata del DMA[75].

Anche l'autorità antitrust italiana ha messo Google nell'occhio del mirino: il 28 ottobre scorso l'AGCM ha annunciato l'apertura di un'istruttoria contro Google per possibile abuso di posizione dominante nel mercato italiano del display advertising. In particolare, l'Autorità ha contestato un uso discriminatorio dell'enorme quantità di dati che Google raccoglie attraverso le sue applicazioni. La società controllata da Alphabet Inc., infatti, avrebbe violato l'art. 102 del Trattato limitando l'accesso dei propri concorrenti ai dati raccolti attraverso i cookie e altri strumenti di tracciamento impostati su Android e Google Chrome, che vengono poi sfruttati per la profilazione degli utenti e la diffusione di pubblicità mirata. L'azienda, secondo l'antitrust italiano, avrebbe rifiutato di fornire ai concorrenti le chiavi per decriptare l'ID Google, e avrebbe impedito a terzi di utilizzare i pixel di tracciamento indispensabili per i sistemi di pubblicità online (un mercato che nel 2019, prima dell'accelerazione dell'economia digitale dovuta all'emergenza COVID-19, valeva in Italia 3,3 miliardi). In altri termini, Google starebbe creando uno svantaggio per i propri concorrenti (che necessiterebbero di un maggior numero di passaggi per raggiungere il target degli utenti) e, contemporaneamente, starebbe utilizzando i dati tratti dai propri canali (non disponibili agli altri operatori del display advertising) per ottenere una profilazione puntuale e non replicabile. Le condotte in esame sarebbero idonee ad ostacolare lo svolgimento di una concorrenza effettiva nei mercati interessati, con preclusione dei concorrenti e con conseguenti effetti negativi per il benessere dei consumatori, sullo sviluppo tecnologico dei messaggi pubblicitari e, in ultima analisi, sull'esperienza di fruizione dei messaggi pubblicitari da parte degli utenti[76].

Anche Amazon è stata oggetto di recenti interventi investigativi da parte dell'antitrust europeo. Il 10 novembre scorso, dopo un anno e mezzo di indagini, la Commissione ha riscontrato un utilizzo sleale dei dati raccolti sugli 800.000 venditori europei attivi sul portale a vantaggio dei prodotti Amazon. Grazie al suo ruolo di intermediario tra rivenditori e consumatori, il gruppo guidato da Jeff Bezos ha infatti accesso a una grande quantità di dati non pubblici che confluiscono direttamente nei suoi sistemi automatizzati e, una volta aggregati, aiutano a calibrare l'offerta strategica di dei prodotti a marchio Amazon. Secondo la Commissione, considerando che Amazon vende i propri prodotti sulla piattaforma ed è quindi un concorrente diretto degli altri rivenditori che utilizzano il marketplace, non dovrebbe poter monitorare in maniera esclu-

75Commissione, provvedimento del 17 dicembre 2020, disponibile al link: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484.

76 AGCM, Provvedimento A542 del 20 ottobre 2020, disponibile all'indirizzo https://www.agcm.it/dotcmsdoc/allegati-news/A542_avvio%20istruttoria.pdf.

siva l'attività dei clienti di tali rivenditori (ad esempio il numero di visite e di ordini, le informazioni sulla spedizione, i reclami dei consumatori, ecc).

Inoltre, la Commissione ha iniziato ad analizzare anche le presunte pratiche anticoncorrenziali di Facebook ed Apple, con nuove indagini avviate tra la fine del 2019 e la prima metà del 2020. Nei confronti di Apple, le indagini antitrust hanno ad oggetto i meccanismi di funzionamento dell'App Store e il metodo pagamento Apple Pay. A seguito di un'indagine preliminare, la Commissione teme che le condizioni, i termini e le altre misure connesse all'integrazione di Apple Pay per l'acquisto di beni e servizi nelle app commerciali e nei siti web nei dispositivi iOS possano falsare la concorrenza e ridurre la scelta e l'innovazione. Nel caso di Facebook, invece, la Commissione aveva avviato due indagini relative alle modalità di raccolta e monetizzazione dei dati, ma la società di Zuckerberg, dopo aver presentato ricorso presso il Tribunale dell'UE, ha ottenuto una sospensione provvisoria alle indagini per il rischio che le informazioni richieste dalla Commissione violassero dati altamente sensibili degli utenti della piattaforma[77]. Nel frattempo, però, Facebook era già stata sanzionata per 110 milioni di euro per aver fornito informazioni non veritiere durante le indagini sull'acquisizione di Whatsapp, sostenendo falsamente di non essere in grado di collegare gli account del servizio di messaggistica direttamente con i profili del *social network*[78].

A livello italiano, l'autorità antitrust italiana ha avviato nel mese di luglio 2020 un procedimento nei confronti di Amazon e Apple, le quali, ad avviso dell'autorità, avrebbero concluso un accordo secondo cui, in cambio della qualifica di rivenditore ufficiale, Amazon avrebbe garantito ad Apple (e ai suoi rivenditori ufficiali) la possibilità esclusiva di vendere i prodotti Apple e Beats sul proprio marketplace italiano. Alla luce di tale accordo, Amazon avrebbe quindi rimosso dalla propria piattaforma tutti i rivenditori non ufficiali di prodotti Apple e Beats. Un simile accordo si porrebbe in violazione dell'articolo 101 TFUE in quanto potrebbe: (*i*) limitare la possibilità per i rivenditori non ufficiali di utilizzare i servizi di intermediazione offerti da Amazon e, in tal modo, raggiungere una platea più ampia, (*ii*) limitare gli incentivi di Apple e Amazon a competere tra loro sui prezzi dei prodotti Beats e Apple e (*iii*) limitare l'integrazione del mercato europeo, in quanto l'accesso alla piattaforma renderebbe più semplice la vendita all'estero per i rivenditori non ufficiali[79].

Inoltre, nel mese di novembre 2020, l'autorità antitrust italiana ha avviato un'istruttoria nei confronti dell'Associazione Nazionale fra le Imprese Assicuratrici (ANIA) relativa alla proposta di un "progetto antifrode" nei rami vita e danni, che prevedrebbe la realizzazione di banche dati e lo sviluppo di algoritmi comuni per determinare indicatori del rischio frode che le compagnie di assicurazioni potrebbero utilizzare. Ad avviso dell'autorità antitrust italiana,

77 T-451/20 and T-452/20 Facebook Ireland v Commission.

78 Commissione, provvedimento del 18 maggio 2017, disponibile all'indirizzo https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369.

79AGCM, Provvedimento I842 - Vendita prodotti Apple e Beats su Amazon Marketplace del 14 luglio 2020, disponibile al link: https://www.agcm.it/dotcmsCustom/getDominoAttach?urlStr=192.168.14.0037A9A8/$File/p28294.pdf

tale progetto presenterebbe delle criticità concorrenziali, relative non solo alla necessità di un soggetto terzo gestore del pool di dati ma anche all'aumento della trasparenza sul mercato causato dallo sviluppo di algoritmi comuni e dalla condivisione di un'ampia mole di dati, che potrebbe agevolare la collusione tra concorrenti, uniformando le scelte di strategia commerciale delle compagnie assicurative coinvolte[80]. Si noti che anche la Commissione ha avviato un'istruttoria in un caso analogo, nei confronti di *Insurance Ireland*[81].

Si tratta in ogni caso di pratiche che, oltre ad ostacolare sensibilmente la concorrenza, impediscono ai consumatori di beneficiare di una scelta più ampia e di prezzi più bassi. L'intervento delle autorità antitrust nazionali e della Commissione, dapprima correttivo e ora (da parte della Commissione) anche normativo, rappresenta la naturale reazione alle conseguenze indesiderate del processo innovativo che ha caratterizzato lo sviluppo economico degli ultimi anni. La pervasività dei servizi offerti da aziende come quelle già citate, che grazie all'incredibile quantità di dati raccolti sono in grado di fornire prodotti e servizi ormai diventati essenziali per gli utenti, avrebbe infatti creato una barriera all'ingresso per le aziende più piccole nello stesso panorama.

L'intento è dunque quello di ridimensionare il ruolo di alcune piattaforme che hanno assunto una posizione di predominio all'interno del mercato, in ragione della pervasività dei servizi offerti e della quantità di dati raccolti attraverso questi. In questo senso, il *Digital Markets Act* e la *New Competition Tool* rappresentano il capitolo finale di quella che negli ultimi mesi è stata definita come una vera e propria "*tech storm*", con il susseguirsi di numerose iniziative e indagini che già da tempo indicavano una decisa presa di posizione da parte delle istituzioni europee.

5. Le nuove tendenze in materia di tutela del consumatore nel mondo digital

5.1 New Deal per i consumatori

L'obiettivo di una maggior trasparenza nei mercati online, nei quali le piattaforme digitali hanno assunto negli ultimi anni un ruolo di rilevante importanza, ha spinto la Commissione a dotarsi di nuove norme poste a tutela dei consumatori, finalizzate a migliorare l'applicazione e ad ammodernare le norme vigenti, in linea con la costante evoluzione digitale di molti mercati. Ciò ha portato il 7 gennaio 2020 all'adozione del cosiddetto "*New Deal for Customers*"[82].

80AGCM, Provvedimento I844 - Progetto Antifrode ANIA del 3 novembre 2020, disponibile al seguente link: https://www.agcm.it/dotcmsCustom/getDominoAttach?p28435.pdf

81Disponibile al seguente link: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2509.

82 The New Deal for Consumers. What benefits will I get as a consumer?-Factsheet, Novembre 2019, disponibile a questo link https://ec.europa.eu/info/sites/info/files/factsheet_new_deal_consumer_benefits_2019.pdf. Le nuove regole entreranno in vigore a partire dal 2022. In particolare, la Digital Content Directive e la Sale of Goods Directive dal 1° gennaio 2022, la Omnibus Directive dal 28 maggio 2022. Gli Stati membri dell'UE hanno due anni di tempo per recepire queste direttive, nello specifico: fino al 1° luglio 2021 per la Digital Content Directive e la Sale of Goods Directive e fino al 28 novembre 2021 per la Omnibus Directive.

Queste nuove regole avranno un inevitabile impatto sulla compliance aziendale e sui processi interni, richiedendo alle imprese un'approfondita conoscenza della normativa posta a tutela dei consumatori nell'ottica di scongiurare il rischio di incorrere in indagini da parte delle autorità competenti e in eventuali e conseguenti sanzioni o danni reputazionali, nonché di predisporre aggiornamenti o integrazioni dei programmi di compliance già in essere, proprio al fine di considerare anche questi ulteriori aspetti e sviluppi. Il Commissario alla giustizia Diedier Reynders ha infatti pubblicamente dichiarato che l'introduzione delle nuove regole lancia un avvertimento chiaro agli operatori commerciali che sono tenuti a rispettare e non aggirare la nuova normativa. Infatti: "*le imprese che violano su larga scala le norme UE a tutela dei consumatori rischiano un'ammenda pari ad almeno il 4% del proprio fatturato annuo. Si tratta di una sanzione sufficientemente dissuasiva ed efficace per evitare che operatori commerciali disonesti possano ingannare*"[83].

Il "*New Deal for Customers*", definito come il nuovo quadro normativo "autenticamente europeo" a tutela dei consumatori, ha l'obiettivo di una maggiore armonizzazione del diritto dei consumatori, prevedendo più trasparenza e responsabilità per i fornitori, i venditori e le piattaforme. In particolare, il nuovo complesso di regole che comprende la *Ominbus Directive*[84]; la *Digital Content Directive*[85]; la *Sale of Goods Directive*[86] e la *Collective Redress Directive*[87], avrà un impatto su tutte le aziende che operano nel settore del digital. I principali aspetti su cui questo pacchetto di norme interverrà attengono: (i) alla trasparenza e responsabilità - in quanto tali elementi influenzeranno sicuramente le interfacce utente (al fine di renderle più chiare e "accessibili") - incluse tematiche quali garanzie legali/funzionalità e, soprattutto, interoperabilità; (ii) al riconoscimento dei dati come controprestazione: ciò porterà alla necessaria

Quanto alla Collective Redress Directive, non è ancora stata adottata definitivamente ma il testo è stato concordato. In questo caso oltre ai canonici due anni entro i quali gli Stati Membri devono recepire le direttive, sono stati offerti altri 6 mesi per consentire anche alle Autorità di adattarsi alle nuove regole.

83 Commissione, New Deal per i consumatori: entrano in vigore nuove norme che migliorano la tutela dei consumatori, disponibile al seguente link: https://ec.europa.eu/italy/news/20200107_nuove_norme_ue_che_tutelano_i_consumatori_it Anche il Vicepresidente responsabile per i Valori e la trasparenza, ha dichiarato: "*Le nuove norme aumenteranno la protezione dei consumatori nel mondo digitale, come è giusto che sia. Inoltre, l'UE dice NO ai prodotti venduti come identici in altri Stati membri, quando invece non lo sono. Per proteggere i consumatori dai commercianti disonesti e dagli imbroglioni on line è però necessario che le nuove norme siano applicate con rigore, invito dunque tutti gli Stati membri a garantirne l'applicazione tempestiva.*"

84 Direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori.

85 Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

86 Direttiva (UE) 2019/771 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE, e che abroga la direttiva 1999/44/CE.

87 Directive of the european Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC (non è ancora disponibile la versione in lingua italiana).

rivalutazione/categorizzazione di tutti i servizi pubblicizzati come "gratis" sia nel funzionamento che - soprattutto- nella comunicazione commerciale; (iii) alla protezione dei dati non personali attraverso l'interruzione del trattamento dei dati non personali quando l'utente si ritira/termina il rapporto contrattuale e la possibilità di renderli disponibili su richiesta; (iv) all'aggiornamento dei processi per l'esercizio del diritto di recesso, delle garanzie e dei rimedi per i consumatori. In buona sostanza, l'obiettivo è creare un "nuovo diritto contrattuale" che sia armonizzato per tutti i paesi dell'UE scongiurando il rischio di avere 27 leggi nazionali diverse. A mero titolo esemplificativo, dovrà essere prevista la possibilità di doppia firma (doppia *checkbox*) per i termini e condizioni che contengono clausole vessatorie e di modifica delle condizioni contrattuali, così come sarà necessario offrire un servizio di assistenza via e-mail e telefono (anche per i servizi gratuiti).

5.2 La Direttiva Omnibus

Merita un approfondimento particolare la Direttiva Omnibus che apporterà modifiche alla Direttiva 2005/29[88] relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno. Importanti saranno gli oneri in termini di adeguamento che graveranno sulle imprese, tenute a rivedere le condizioni generali di contratto, i rapporti con i partners commerciali e i fornitori, le informazioni veicolate tramite i siti e/o le App nonché i modelli di business, al fine di adeguarsi al nuovo quadro normativo e coglierne le opportunità.

Più nel dettaglio, le novità riguardano:

I. **L'ampliamento del novero delle pratiche commerciali scorrette e delle tutele per i consumatori**: la Direttiva prevede l'introduzione nel novero delle pratiche commerciali ingannevoli della commercializzazione di prodotti "a duplice qualità", cioè quella attività di marketing che promuove un bene in uno Stato membro, come identico a un bene commercializzato in altri Stati membri, mentre questo bene ha una composizione o caratteristiche significativamente diverse. Inoltre, gli Stati membri possono adottare disposizioni per tutelare i legittimi interessi dei consumatori rispetto a pratiche commerciali o di vendita aggressiva o ingannevole nel quadro di vendite negoziate fuori dai locali commerciali.

II. **I rimedi e le sanzioni**: la Direttiva prevede l'introduzione (attraverso l'articolo 11 *bis*) di rimedi individuali proporzionati ed effettivi, quali il risarcimento del danno, la riduzione del prezzo o la risoluzione del contratto, per i consumatori lesi da pratiche commerciali sleali. Per quanto attiene alle sanzioni, come accennato in precedenza, saranno simili a quelle previste dal GDPR, per un importo massimo almeno pari al 4% del fatturato annuo del professionista nello stato o negli stati UE interessati, o sino ad euro 2.000.000,00 in mancanza di informazioni sul

88 Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno.

fatturato, fatta salva la possibilità per ciascun Stato Membro di introdurre sanzioni più elevate[89].

III. **Una maggiore trasparenza**: la Direttiva prevede altresì maggiori obblighi di trasparenza nei confronti dei consumatori rispetto alle recensioni sui prodotti: sono proibite infatti le false recensioni. I professionisti dovranno rendere noto se hanno adottato processi/procedure idonee a garantire che le recensioni pubblicate provengano da consumatori che hanno effettivamente acquistato o utilizzato il bene in questione, ovvero se sono frutto di sponsorizzazione o comunque influenzate dall'esistenza di un rapporto contrattuale con il professionista. È altresì richiesta una maggiore trasparenza rispetto al posizionamento delle offerte commerciali all'interno dei risultati di una ricerca online: la Direttiva prevede infatti che il fornitore di funzionalità di ricerca online dovrà indicare quei risultati di ricerca che contengono "posizionamenti a pagamento" (cioè se un professionista ha pagato, direttamente o indirettamente per ottenere una classificazione migliore di un prodotto all'interno dei risultati della ricerca). Inoltre, il consumatore dovrebbe essere chiaramente informato quando il prezzo che è offerto è personalizzato sulla base della decisione automatizzata, in modo da poter tenere conto dei potenziali rischi insiti nel processo decisionale di acquisto.

5.3 La recente prassi decisionale dell'AGCM

Sempre in un'ottica di compliance aziendale, occorre sottolineare come negli ultimi anni tanto la Commissione quanto l'AGCM abbiano mostrato una particolare attenzione alle tematiche legate alla tutela del consumatore e alle pratiche commerciali scorrette nel settore digitale.

A tal proposito occorre ricordare che l'AGCM, insieme con il Garante Privacy e l'Autorità per le Garanzie nelle Comunicazioni ("**AGCOM**"), ha dedicato al settore digitale un'indagine conoscitiva[90] durata tre anni e i cui risultati sono stati pubblicati nel febbraio 2020.

In questa sede ci concentreremo su due principali filoni seguiti dall'Autorità in questi ultimi anni proprio al fine di individuare quegli aspetti cui le imprese attive (anche) nel settore digitale devono prestare maggiore attenzione. Segnatamente, l'intreccio tra tutela del consumatore e protezione dei dati personali, e le insidie derivanti dal massiccio ricorso all' e-commerce durante e (probabilmente anche dopo) l'emergenza sanitaria da Covid-19.

89 I criteri da tenere in considerazione nell'applicazione/quantificazione sono (non esaustivi): natura, gravità, entità e durata della violazione; eventuali azioni intraprese dal venditore o fornitore per attenuare il danno subito dai consumatori; eventuali violazioni commesse in precedenza dal venditore o fornitore; precedenti sanzioni inflitte al venditore o fornitore per la medesima violazione.

90 AGCM, AGCOM, Garante Privacy, Indagine conoscitiva sui Big Data, disponibile al seguente link: https://www.agcm.it/dotcmsdoc/allegati-news/IC_Big%20data_imp.pdf.

5.3.1 Dati personali e tutela del consumatore

Quanto al primo profilo occorre ricordare che l'AGCM nel 2018 ha condotto un'indagine e irrogato una sanzione di 10 milioni di euro nei confronti di Facebook per due presunte pratiche commerciali scorrette[91] aventi ad oggetto il trattamento dei dati personali degli utenti attuate sia durante la fase di attivazione dell'account sia durante la fruizione del servizio di Facebook. In particolare, Facebook ha adottato un'informativa non idonea a generare sufficiente consapevolezza negli utenti circa l'utilizzo che sarebbe stato fatto dei dati personali da loro forniti, dati destinati ad una successiva utilizzazione e/o condivisione con i terzi con finalità meramente commerciale. In altre parole, l'informativa presente nella prima pagina della piattaforma ("*Iscriviti. È gratis e lo sarà sempre*") peccava di chiarezza, immediatezza e completezza, non contenendo informazioni adeguate circa l'intento commerciale dei dati forniti e "*delle finalità remunerative che sottendono la fornitura del servizio di social network enfatizzandone la sola gratuità, così da indurre [i consumatori] ad assumere una decisione di natura commerciale che non avrebbero altrimenti preso*". La seconda condotta, qualificata come "aggressiva", ha avuto ad oggetto l'applicazione da parte di Facebook di un meccanismo volto a trasmettere i dati ad altri siti "*web-app*" di terzi per finalità commerciali. Secondo l'Autorità, il Professionista ha esercitato un indebito condizionamento nei confronti degli utenti registrati, i quali avrebbero subito, senza espresso e preventivo consenso (quindi in modo del tutto automatico e inconsapevole), la trasmissione e l'uso da parte di Facebook/terzi di dati personali per finalità commerciali.

In sede di impugnazione, il Tribunale Amministrativo Regionale per il Lazio[92], ha parzialmente accolto il ricorso presentato da Facebook avverso la decisione dell'AGCM, sancendo però un principio fondamentale e quanto mai innovativo, quello cioè legato al valore economico e commerciale dei dati personali nel mercato digitale: in altre parole tali dati sono considerati come dei veri e propri beni commerciali e controprestazioni contrattuali. L'AGCM ha ulteriormente ribadito tale principio nel recentissimo provvedimento[93] con cui ha accertato l'inottemperanza di Facebook e irrogato una sanzione amministrativa pecuniaria pari a 7 milioni di euro per non aver rimosso la pratica scorretta sull'utilizzo dei dati degli utenti e per non aver pubblicato la dichiarazione rettificativa richiesta dall'Autorità col provvedimento emesso nel novembre 2018. L'AGCM ha ritenuto che le Società[94] pur avendo eliminato il *claim* di gratuità in sede di registrazione alla piattaforma, non informassero l'utente con

91 Procedimento PS11112, Facebook – condivisione dati con i terzi, decisione del 29 novembre 2018.

92 Tribunale Amministrativo Regionale per il Lazio, sentenze n.260 e n.261 del 10 gennaio 2020. I giudici hanno riconosciuto come fondata soltanto la prima pratica commerciale scorretta, giudicando invece la seconda priva di fondamento.

93 Procedimento IP330, Facebook – raccolta utilizzo dati degli utenti, decisione del 9 febbraio 2020, disponibile al seguente link https://www.agcm.it/dotcmsdoc/allegati-news/IP330_chiusura.pdf.

94 Le condotte oggetto del procedimento sono state imputate a Facebook Ireland Ltd e alla controllante al 100% Facebook Inc, in virtù dell'applicazione del principio derivante dalla giurisprudenza antitrust della cd "parental liability" anche in materia di pratiche commerciali scorrette. L'AGCM ha motivato l'applicazione di tale principio alla luce della comune ratio dei due plessi normativi (antitrust e tutela del consumatore) volti alla tutela del mercato e della libertà di concorrenza.

chiarezza e immediatezza in merito alla finalità remunerativa della raccolta e dell'utilizzo dei dati dell'utente e, conseguentemente, dell'intento commerciale perseguito. Secondo l'Autorità, si tratterebbe di informazioni di cui il consumatore necessita per decidere se registrarsi al servizio, considerato il valore economico assunto per Facebook dai dati ceduti dall'utente, che rappresentano il corrispettivo stesso per l'utilizzo del servizio.

Il corollario di ciò è che diventa di fondamentale importanza per le società che operano nel settore digitale predisporre un'informativa ai consumatori/utenti che sia quanto mai chiara e completa e che non generi alcun dubbio circa le finalità (commerciali e remunerative) perseguite dal Professionista tramite l'uso dei dati personali, pena il rischio di pesanti ammende per violazione della normativa sulle pratiche commerciali scorrette.

L'Autorità è tornata sul tema di recente aprendo lo scorso 7 settembre 2020 un'indagine[95] nei confronti di Google (per il servizio Google Drive), Apple (per il servizio iCloud) e Dropbox, ciascuno interessato sia da un procedimento per presunte pratiche commerciali scorrette e/o violazioni della Direttiva sui diritti dei consumatori sia da presunte clausole vessatorie nei contratti. In particolare, per i profili di interesse discussi, l'indagine dell'Autorità nei confronti di Apple, Google e Dropbox riguarda proprio la mancata o inadeguata indicazione, in sede di presentazione del servizio, della finalità commerciale della raccolta/utilizzo dei dati forniti dall'utente e il possibile indebito condizionamento esercitato sui consumatori che non sarebbero in grado di esprimere il consenso all'utilizzo dei dati personali. L'apertura di un simile procedimento appare quindi sintomatica dell'importanza e centralità attribuita dall'Autorità alle tematiche in esame.

5.3.2 Il settore dell'*e-commerce*

Il secondo filone che preme qui brevemente analizzare è quello legato al settore dell'*e-commerce*, che, in assoluta controtendenza rispetto alla crisi che stanno attraversando tutti i settori dell'economia, ha conosciuto uno sviluppo notevole nell'anno dell'emergenza sanitaria.

Il ricorso massiccio alle vendite online ha attirato l'attenzione delle autorità europee e nazionali preposte alla tutela dei consumatori, che hanno svolto un'intensa attività di monitoraggio e di indagine[96]. Basti pensare che, per quanto riguarda l'Italia, all'indomani dell'emergenza sanitaria dichiarata dall'Organiz-

95 CV194-CV195-CV196-PS11147-PS11149-PS11150 - Avviate istruttorie nei confronti di Google, Apple e Dropbox per i servizi di cloud computing, comunicato stampa disponibile al seguente link https://www.agcm.it/media/comunicati-stampa/2020/9/CV194-CV195-CV196-PS11147-PS11149-PS11150.

96 In data 23 marzo 2020, il Commissario alla giustizia Didier Reynders ha indirizzato una lettera pubblica a diversi *social network*, piattaforme, motori di ricerca e *markeplace*, richiamando la normativa in materia di pratiche commerciali scorrette, menzionando indirettamente le più recenti indagini avviate dalle autorità nazionali competenti (tra cui anche la nostra), ed invitando i destinatari della lettera ad informare la Commissione, entro una settimana, delle azioni intraprese per rimuovere qualsiasi pratica commerciale scorretta dalle proprie piattaforme (disponibile qui). Le piattaforme hanno mostrato un atteggiamento collaborativo, dimostrato dal comunicato stampa pubblicato con cui la Commissione il 3 aprile 2020 ha manifestato la propria soddisfazione per le misure adottate dalle piattaforme online.

zazione Mondiale della Sanità, le piattaforme di e-commerce - dal colosso di Jeff Bezos[97] a quelle minori[98] - sono finite nel mirino dell'antitrust a causa di presunte pratiche commerciali scorrette (in alcuni casi ad opera di venditori terzi), legate proprio alla presunta pubblicità ingannevole e ai prezzi potenzialmente speculativi di mascherine e igienizzanti.

Alla luce di questa costante e crescente attenzione da parte dell'AGCM nei confronti delle piattaforme di e-commerce, che ha portato la stessa anche ad un anomalo e inconsueto utilizzo della tutela cautelare[99], tramite l'adozione di numerose misure d'urgenza immediatamente efficaci, è bene che le imprese predispongano strumenti di compliance e di sensibilizzazione per evitare di non incorrere in violazioni dei diritti dei consumatori, mediante pratiche illecite.

5.4 Take away

Sulla scorta delle modifiche normative che si accingono ad essere recepite anche in Italia e soprattutto della prassi decisionale dell'Autorità, è bene che le imprese che operano (anche) nel settore *digital* prestino particolare attenzione ad esempio a: non pubblicizzare qualità che un prodotto non possiede; non commercializzare prodotti con prezzi speculativi legati a situazioni emergenziali; non omettere informazioni circa i criteri adottati per ordinare i risultati di ricerca; vigilare sulla veridicità delle recensioni dei prodotti posti in commercio; predisporre delle *policy* trasparenti in cui vengano chiaramente indicate le finalità commerciali della raccolta dati degli utenti e a offrire dei adeguati servizi di *customer care*.

97 AGCM, procedimento PS11716, Amazon-vendita online prodotti emergenza sanitaria, provvedimento n. 28442 del 23 novembre 2020 con il quale l'Autorità ha accettato e reso vincolanti gli impegni proposti da Amazon.

98 Si veda ad esempio, AGCM procedimento PS11736, Tiger Shop – vendita online prodotti emergenza sanitaria, provvedimento n. 28446 del 10 novembre 2020.

99 Tale potere è attribuito dall'art. 27 comma 3 del Decreto Legislativo 206/2005 ("Codice del Consumo").

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 ai quali appartengono i curatori e i co-autori del Quaderno stesso, sotto specificati), ove è stata costituita nel 2003 come organizzazione apolitica senza scopo di lucro, operando in particolare nel settore del diritto d'impresa e con il fine di promuovere e diffondere la cultura e le modalità più attuali dell'esercizio della professione legale in forma associata, organizzata e certificabile.

Hanno contribuito a questo Quaderno:

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

L'Avv. **Antonio Bana**, curatore e co-autore del Capitolo 5 di questo Quaderno, dello Studio Legale Bana di Milano (www.studiobana.it)

L'Avv. **Alessandra Anselmi**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)

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

L'Avv. **Francesca Chiara Bevilacqua**, co-autrice del Capitolo 5 di questo Quaderno, dello Studio Legale Associato Gianni & Origoni (www.gop.it)

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

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

L'Avv. **Eva Cruellas Sada**, co-autrice del Capitolo 6 di questo Quaderno, dello Studio Legale Associato Gianni & Origoni (www.gop.it)

L'Avv. **Simona Custer**, co-autrice del Capitolo 5 di questo Quaderno, di A&A Studio Legale (www.albeeassociati.it)

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

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

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

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

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

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

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

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

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

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

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

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

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

Pubblicazione giuridica n° 19 di ASLA

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

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

www.aslaitalia.it

Hanno contribuito a questo Quaderno:

L'Avv. **Irene Picciano**, curatrice e co-autrice del Capitolo 6 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)
L'Avv. **Antonio Bana**, curatore e co-autore del Capitolo 5 di questo Quaderno, dello Studio Legale Bana di Milano (www.studiobana.it)

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

www.aslaitalia.it

L'Avv. **Andrea Mantovani**, co-autore del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)
L'Avv. **Marta Margiocco**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Cocuzza e Associati (www.cocuzzaeassociati.it)
L'Avv. **Guido Novellini**, co-autore del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Portolano Cavallo (www.portolano.it)
L'Avv. **Mariangela Papadia**, co-autrice del Capitolo 3 di questo Quaderno, dello Studio Legale Associato Pavia e Ansaldo (www.pavia-ansaldo.it)
L'Avv. **Alessia Placchi**, co-autrice del Capitolo 2 di questo Quaderno, dello Studio Legale Associato LCA (www.lcalex.it)
L'Avv. **Eva Reggiani**, co-autrice del Capitolo 1 di questo Quaderno, dello Studio Legale Associato Cleary Gottlieb (www.clearygottlieb.com)
L'Avv. **Josephine Romano**, co-autrice del Capitolo 4 di questo Quaderno, dello Studio Legale Associato Deloitte Legal (www.deloitte.com/it)
L'Avv. **Roberto Tirone**, co-autore del Capitolo 4 di questo Quaderno, dello Studio Legale Cocuzza e Associati (www.cocuzzaeassociati.it)

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

ASLA
Associazione Studi Legali Associati