Quaderni giuridici

Gli sviluppi tecnologici del diritto societario

a cura di M. Bianchini, G. Gasparri, G. Resta, G. Trovatore, A. Zoppini

23

maggio 2022

CONSOB
COMMISSIONE NAZIONALE
PER LE SOCIETÀ E LA BORSA

L'attività di ricerca e analisi della Consob intende promuovere la riflessione e stimolare il dibattito su temi relativi all'economia e alla regolamentazione del sistema finanziario.

I **Quaderni di finanza** accolgono lavori di ricerca volti a contribuire al dibattito accademico su questioni di economia e finanza. Le opinioni espresse nei lavori sono attribuibili esclusivamente agli autori e non rappresentano posizioni ufficiali della Consob, né impegnano in alcun modo la responsabilità dell'Istituto. Nel citare i lavori della collana, non è pertanto corretto attribuire le argomentazioni ivi espresse alla Consob o ai suoi Vertici.

I **Discussion papers** ospitano analisi di carattere generale sulle dinamiche del sistema finanziario rilevanti per l'attività istituzionale.

I **Quaderni giuridici** accolgono lavori di ricerca volti a contribuire al dibattito accademico su questioni di diritto. Le opinioni espresse nei lavori sono attribuibili esclusivamente agli autori e non rappresentano posizioni ufficiali della Consob, né impegnano in alcun modo la responsabilità dell'Istituto. Nel citare i lavori della collana, non è pertanto corretto attribuire le argomentazioni ivi espresse alla Consob o ai suoi Vertici.

I **Position papers,** curati dalla Consob anche in collaborazione con altre istituzioni, illustrano ipotesi di modifiche del quadro regolamentare o degli approcci di vigilanza e ricognizioni di aspetti applicativi della normativa vigente.

Progetto Grafico

Studio Ruggieri Poggi

Stampa e allestimento

Tipografia Eurosia srl (Roma)

http://www.tipografiaeurosia.it

Consob

00198 Roma – Via G.B. Martini, 3

t 06.8477.1

f 06.8477612

e studi_analisi@consob.it

ISSN 2281-5236 (online)
ISSN 2281-5228 (stampa)

Gli sviluppi tecnologici del diritto societario

a cura di M. Bianchini, G. Gasparri, G. Resta, G. Trovatore, A. Zoppini (*)

Abstract

Il lavoro affronta il tema dell'introduzione delle tecnologie digitali negli assetti organizzativi e nei meccanismi di *corporate governance* delle società quotate, passando in rassegna gli ambiti in cui si sono registrate le novità più promettenti e interrogandosi sul corretto equilibrio tra benefici attesi e rischi potenziali. Dopo una premessa di carattere generale sulla trasformazione digitale delle imprese, l'attenzione è rivolta all'esame degli sviluppi tecnici in materia di accesso e gestione delle informazioni finanziarie da parte degli emittenti quotati e ai relativi impatti sull'informativa societaria. Muovendo dalla constatazione che lo stato emergenziale dovuto alla diffusione del COVID-19 ha recentemente indotto il legislatore a prevedere misure eccezionali, dirette ad agevolare lo svolgimento delle assemblee societarie da remoto, si procede ad analizzare i problemi applicativi posti dall'impiego di tecnologie digitali nel procedimento assembleare, scrutinando l'opportunità o meno di aggiornare a tali novità l'impostazione normativa ordinaria. L'indagine si sofferma altresì sulla possibile utilizzazione delle tecnologie a registri distribuiti nel sistema di controllo interno e di gestione dei rischi, illustrando le forme di impatto che le stesse tecnologie generano sui meccanismi di controllo interno ed evidenziando il contributo che tali soluzioni potrebbero apportare in termini di benefici sulla sicurezza e sul miglioramento dei processi di identificazione e valutazione dei rischi aziendali. Il lavoro ripercorre, in conclusione, le principali criticità in tema di protezione dei dati personali generate dall'impiego di meccanismi digitali all'interno dei modelli organizzativi delle società.

(*) Margherita Bianchini - Assonime, Direttore dell'Area del Diritto Societario e Vicedirettore Generale;
Giorgio Gasparri - CONSOB, Divisione Studi, Ufficio Studi Giuridici;
Giorgio Resta - Università degli Studi Roma Tre, Ordinario di Diritto Privato Comparato;
Gianfranco Trovatore - CONSOB, Divisione Studi, Responsabile dell'Ufficio Studi Giuridici;
Andrea Zoppini - Università degli Studi Roma Tre, Ordinario di Diritto Privato.

Si ringraziano Anna Sciortino (ESMA) e Marcello Bianchi (Assonime, Direttore dell'Area del Mercato dei Capitali e società quotate e Vicedirettore Generale) per la partecipazione costante e il contributo offerto. Le opinioni espresse nel lavoro sono attribuibili esclusivamente agli autori e non impegnano in alcun modo la responsabilità dell'Istituto. Nel citare il presente lavoro non è, pertanto, corretto attribuire le argomentazioni ivi espresse alla CONSOB o ai suoi vertici. Errori e imprecisioni sono imputabili esclusivamente agli autori.

Indice

5 L'interferenza della digitalizzazione nei processi di *governance* con il regime di protezione dei dati personali

C. Giustolisi – E. Ruzzi – F. Ruggeri (*)

5.1 Premessa

Nell'attuale contesto socioeconomico, i modelli di *business* e i sistemi di *corporate governance* sono al centro di una profonda e rapida trasformazione, trainata dall'adozione di nuove e sempre più sofisticate soluzioni tecnologiche.

L'impiego degli strumenti digitali porta con sé la promessa di semplificare i processi decisionali all'interno delle organizzazioni complesse, ma pone altresì dubbi e incertezze sull'impatto che tali strumenti – sovente completamente indipendenti dall'intervento dell'uomo – possono avere sui diritti e sulle libertà delle persone fisiche, segnatamente in materia di protezione dei dati personali.

La dottrina ha cercato di individuare quali compiti, tra quelli attualmente svolti dagli amministratori di società, possano beneficiare dell'apporto reso dalle nuove tecnologie. Già da tempo queste ultime sono, infatti, ampiamente utilizzate per facilitare e accelerare lo svolgimento di compiti di carattere amministrativo (dalla semplice gestione dell'agenda al coordinamento del personale), così permettendo di sbloccare risorse – su tutte, il tempo – verso altre attività strategiche per una società.

In particolare, l'utilizzo di *software* o sistemi (più o meno riconducibili nel paradigma dell'intelligenza artificiale) in grado di individuare e selezionare informazioni rilevanti all'interno di vasti *set* di dati "grezzi" consentirebbe al *top management* di diminuire sensibilmente la quantità di tempo e risorse dedicati alla formazione di un adeguato bagaglio informativo sulla gestione sociale e sulle iniziative da intraprendere.

In tal senso, ben può ritenersi che l'impiego delle capacità analitiche e predittive dell'intelligenza artificiale – in grado di processare enormi quantità di dati per rivelare informazioni o *pattern* non immediatamente ricavabili – rappresenti un valido strumento per agevolare e rafforzare il dovere istruttorio nelle relazioni endosocietarie e nell'esercizio delle funzioni gestorie[155], diminuendo considerevolmente il rischio che le proposte o le decisioni siano viziate da *deficit* informativi, in un'ottica di efficientamento dell'attività di *governance*.

(*) Claudia Giustolisi - Università degli Studi Roma Tre;
Edoardo Ruzzi - Università degli Studi Roma Tre;
Federico Ruggeri - Sapienza Università di Roma.

155 In proposito, si veda Montagnani, *Flussi informativi e doveri degli amministratori delle società per azioni ai tempi dell'intelligenza artificiale*, in *Persona e Mercato*, 2, 2020, 98.

Non si tratta, peraltro, di scenari meramente ipotetici, essendo già esistenti sul mercato diverse soluzioni *software* progettate per ottimizzare il sistema degli scambi informativi e il lavoro consiliare. Ci si riferisce, in particolare, ai cosiddetti *board management softwares*, le cui funzionalità spaziano dalla semplice organizzazione da remoto delle attività collegiali all'offerta di strumenti di *analytics* per semplificare l'elaborazione dei piani finanziari e la pianificazione operativa e strategica[156], contribuendo a una sostanziale riduzione delle asimmetrie informative e dei costi di agenzia tipici delle organizzazioni complesse[157].

In ogni caso, il funzionamento di nuove e sofisticate tecnologie digitali non di rado presuppone l'utilizzo di enormi *dataset* e l'elaborazione di dati personali, nel qual caso si rende necessario che le società adeguino gli strumenti informatici agli obblighi normativi imposti dal Regolamento (UE) 2016/679 (*GDPR*) e dalla normativa interna di attuazione (D. lgs. n. 101/18).

5.2 *Digital transformation* delle società quotate: profili di rischio nel trattamento dei dati personali

La società che compie operazioni di trattamento di dati personali assume *ex lege* la qualifica di titolare del trattamento, come indicato dall'art. 4, § 1, n. 7, *GDPR*. Tale figura, riferita tanto alle persone fisiche quanto a quelle giuridiche, determina le finalità e le modalità del trattamento ed è, al contempo, responsabile dell'ottemperanza al quadro normativo in materia di protezione dei dati personali.

Naturalmente, nell'ambito di una compagine societaria è il legale rappresentante *pro tempore* il soggetto chiamato a farsi carico delle azioni e delle responsabilità attive e passive discendenti dalle attività di trattamento dei dati personali poste in essere nell'esercizio delle funzioni e nel perseguimento dello scopo della stessa società.

Non di rado avviene, però, che il titolare ritenga di delegare, per ragioni sostanzialmente organizzative, le attività di trattamento dei dati ad uno o più soggetti esterni – i cosiddetti responsabili del trattamento[158] – che opereranno quale *longa manus* e che, conseguentemente, svolgeranno il proprio ruolo in via strumentale e dipendente dalla figura del titolare. Difatti, essi sono completamente privati di qualsiasi margine di autonomia decisionale, per ciò che concerne le finalità del trattamento dei dati degli interessati (ovvero delle persone fisiche interessate dal trattamento), che restano una prerogativa assoluta del titolare.

156 Montagnani, *Flussi informativi*, cit., 91.

157 Cfr. Phillips-Wren, *AI Tools in Decision Making Support Systems: A Review*, in *International Journal on Artificial Intelligence Tools*, vol. 20, n. 10, 2012, 1.

158 Dal tenore della normativa, si attende che tale figura possieda delle competenze specialistiche di natura sia giuridica che tecnico-informatica in materia di trattamento, con particolare riferimento ai profili di sicurezza dello stesso (Mantelero, *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it.*, 12, 2019, 2801.

La nomina del responsabile del trattamento costituisce, pertanto, una forma di espressione del principio di *accountability*, che scandisce ogni attività compiuta dal titolare del trattamento, in virtù degli obblighi in capo ad esso posti dal *GDPR*[159], e a cui il titolare è tenuto ad adeguarsi (oltre a dover dimostrare di aver pienamente rispettato la normativa *privacy* vigente[160]).

L'accertamento dei soggetti attivi nelle operazioni di trattamento dei dati personali consente altresì di individuare i responsabili di un eventuale trattamento effettuato in violazione dei diritti degli interessati (ad esempio, quando siano messe a repentaglio la sicurezza e l'integrità dei dati personali raccolti). Tali soggetti sono, infatti, tenuti ad adottare, prima ancora di procedere al trattamento in senso stretto, adeguate misure tecniche e organizzative che risultino concretamente idonee ad annullare o almeno a mitigare il rischio connesso a ciascuna attività di raccolta, elaborazione o diffusione di dati (art. 32, *GDPR*).

In questo senso, si è soliti riferirsi al principio della *privacy by design* cristallizzato dal legislatore europeo nell'art. 25, *GDPR*, inteso come dovere di introdurre, sin dalla fase di progettazione del trattamento, un elevato *standard* di protezione dei dati degli interessati.

La corretta applicazione della *privacy by design* richiede al titolare di intervenire tanto sugli aspetti tecnici quanto su quelli organizzativi. Con riferimento alle misure tecniche, ci si riferisce all'utilizzo di strumenti idonei a tutelare efficacemente i dati trattati (ad esempio, l'adozione di *software* in grado di realizzare automaticamente la pseudonimizzazione dei dati oppure la predisposizione di processi di registrazione *on-line* che rispettino la riservatezza delle identità personali coinvolte). Sotto il profilo organizzativo, il titolare è chiamato alla predisposizione di procedure aziendali a garanzia del trattamento dei dati, in particolare determinando l'organigramma dei soggetti deputati a eseguirlo, anche alla luce della trasversalità della materia, che interessa, al contempo, le funzioni legali, tecniche e commerciali della società (ad esempio, stabilendo regole di utilizzo dei dispositivi elettronici da parte dei dipendenti o prevedendo diversi profili di accesso ai dati personali nell'ambito dell'organizzazione aziendale[161]).

159 Tale principio, generalmente tradotto come principio di rendicontazione o di responsabilità, impone al titolare del trattamento di valutare la correttezza dello stesso, anche al di là di ciò che concerne i suoi requisiti di liceità. Il titolare deve valutare la natura dei dati che tratta, il contesto, i rischi e i costi dello svolgimento della sua attività, così da poter individuare le più opportune misure di sicurezza da adottare, che a loro volta costituiranno oggetto di un monitoraggio costante affinché rimangano sempre proporzionate e adeguate allo scopo. Per esempio, in relazione all'acquisizione del consenso dell'interessato al trattamento dei dati che lo riguardano, il titolare è espressamente chiamato a verificare i rischi insiti nel trattamento eseguito nel caso concreto, le misure più idonee a contrastarli o le modalità di utilizzo dei dati, e ciò alla luce di una concezione dinamica della liceità del trattamento che richiede una costante attività di verifica e aggiornamento a tutela del diritto alla protezione dei dati personali delle persone coinvolte.

160 Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *NLCC*, 1, 2017, 11.

161 Ratti, *Art. 25 GDPR – Commento*, in D'Orazio, Finocchiaro, Pollicino, Resta (a cura di), *Codice della privacy e Data protection*, Milano, 2021.

Nel momento in cui l'ampio utilizzo di sistemi e soluzioni digitali totalmente automatizzati (si pensi, a titolo esemplificativo, ai sistemi d'intelligenza artificiale impiegati nella selezione del personale) può incidere direttamente sulla sfera giuridica soggettiva del singolo, deve comunque considerarsi il rischio che, per ragioni imprevedibili nella fase di progettazione, possano scaturire conseguenze lesive sui diritti e sulle libertà dell'interessato[162].

Sul punto, va segnalato un certo grado di diffidenza da parte del legislatore dell'UE nei confronti dei processi decisionali totalmente demandati alle macchine: la disposizione, infatti, sancisce un generale divieto di sottoporre le persone fisiche a una decisione «*basata unicamente sul trattamento automatizzato che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona*». Non si tratterebbe, tuttavia, di un divieto assoluto, in quanto il secondo paragrafo dello stesso articolo contempla alcune ipotesi di carattere eccezionale per cui è ammesso il ricorso all'*automated decision-making*, nelle ipotesi in cui: ciò sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento; il processo decisionale automatizzato sia ammesso in forza del diritto dell'UE ovvero dello Stato membro cui il titolare è soggetto; l'interessato presti il suo consenso esplicito a tale modalità di trattamento. In ogni caso, deve necessariamente sussistere la specificazione di adeguate misure a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, come «*il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*» (art. 22, § 3, *GDPR*). Si tratterebbe, in proposito, di un diritto a una decisione elaborata non unicamente sulla base di ragionamenti logico-matematici, ma anche sull'impiego della sensibilità necessaria per cogliere le sfumature tra gli interessi e le circostanze in gioco: si pensi al rispetto di diritti fondamentali come la dignità, che sottostanno alla scelta di trattamento e che non sono sempre traducibili nel codice di programmazione dei *software*[163].

La norma sembra così conservare la stessa *ratio* di cui al previgente art. 15 della Direttiva 95/46/CE, che, pur non vietando in modo assoluto il ricorso a meccanismi totalmente automatizzati, intende comunque evitare che gli elementi così elaborati «*esauriscano la base conoscitiva degli atti che presuppongono una valutazione dell'interessato e che incidono, anche indirettamente, sulla relativa sfera personale*»[164].

Il dato normativo, tuttavia, non chiarisce il contenuto delle misure appropriate a tutela dell'interessato, piuttosto limitandosi a prevedere un generico "intervento umano". Sotto un profilo operativo, sono, dunque, le linee guida del *Gruppo dell'articolo 29 per la tutela dei dati* (*Article 29 Working Party* o *WP29*), dedicate all'art. 22, *GDPR,* a evidenziare come l'intervento soddisfi le condizioni del *GDPR* e sia,

162 Troisi, *AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla 'intelligibilità' dell'algoritmo*, in *European Journal of Privacy Law & Technologies*, 1, 2018.

163 Falletti, *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in *Dir. informaz. informatica*, 2020, 2, 179.

164 Così Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997, 342-343.

perciò, qualificabile come "umano", laddove sia realizzato da un soggetto supervisore che abbia i poteri e le competenze per modificare l'esito della decisione automatizzata, in ciò venendo meno l'ipotesi di un controllo dell'uomo che sia meramente simbolico[165].

Tanto prima dell'implementazione quanto nello svolgimento delle sue funzioni, per un *software* che esegua il trattamento di dati personali devono, in ogni caso, disporsi delle «*misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento*» (art. 24, *GDPR*). Tale operazione è, ovviamente, affidata alle figure del titolare del trattamento, che determina le finalità, e del responsabile del trattamento. A tal fine è, dunque, essenziale che il titolare del trattamento compia una preventiva valutazione circa i rischi che potrebbero intercorrere per le persone fisiche interessate dalla procedura.

Sebbene la normativa europea non abbia provveduto a fornire un'elencazione tassativa delle «*misure tecniche ed organizzative*» di gestione del rischio, come anche un qualsiasi riferimento a generali criteri di individuazione dei possibili strumenti di intervento, per alcune specifiche ipotesi gli artt. 35 e 36, *GDPR*, sopperiscono a tale mancanza, definendo apposite regole procedurali[166].

L'art. 35 *GDPR* descrive, innanzitutto, un procedimento formalizzato di valutazione del rischio (*Data Protection Impact Assessment - DPIA*) per il caso in cui il trattamento, per come progettato, possa seriamente compromettere i diritti e le libertà delle persone fisiche, a tal fine dovendosi tenere conto della natura, dell'oggetto, del contesto e delle finalità dello stesso. Valutazione che, in particolare, assume i caratteri dell'obbligatorietà, laddove il trattamento dei dati personali sia realizzato con l'implementazione di nuove tecnologie (art. 35, § 3, *GDPR*). Peraltro, rispetto alla formulazione maggiormente restrittiva di cui al citato art. 22 *GDPR*, è richiesto il ricorso alla *DPIA* non solo laddove il trattamento sia interamente automatizzato, bensì anche nel caso in cui il processo decisionale sia soltanto in parte eseguito da una macchina[167].

La valutazione in questione trova luogo già in fase di progettazione del sistema di trattamento dei dati personali, in ossequio al ricordato principio della *privacy by design*, così da garantirne la conformità al dettato normativo. Gli sviluppatori e i soggetti concretamente responsabili della gestione dei dati dovranno, pertanto, collaborare in stretta sinergia, sin dalle prime fasi di realizzazione del progetto, anche in considerazione dei maggiori costi che andrebbero sostenuti a fronte della necessità

165 WP29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679*, 2018, 20.

166 Mantelero, *La gestione del rischio*, in Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, 492.

167 Come specificato in WP29, *Linee guida*, cit., 29.

di modificare radicalmente le operazioni di trattamento in conseguenza dell'esito della valutazione di impatto[168].

In particolare, il *WP29* ha specificato che la valutazione di impatto non si esaurisce nella fase anteriore al trattamento, ma rappresenta un processo continuo, diretto a influenzare i processi decisionali aventi a oggetto il trattamento stesso. Tale analisi non deve, dunque, ridursi a un mero report *ex ante*, dovendo piuttosto rappresentare una progressiva valutazione che si sviluppi anche nella fase di implementazione del trattamento.

Laddove dalla valutazione di impatto emergano elevati profili di rischio e il titolare del trattamento non ritenga che le misure adottate o adottabili siano idonee alla riduzione dei suddetti rischi ovvero «*il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione*»[169], lo stesso, prima di procedere al trattamento, è tenuto a consultare l'autorità di controllo, ai sensi dell'art. 36 *GDPR*.

In tal caso, la disciplina richiede, dunque, che il Garante per la protezione dei dati personali, riscontrata l'effettiva impossibilità del titolare di provvedere adeguatamente da sé, proceda con l'emanazione di un parere entro il termine – di regola – di otto settimane. Tale intervento, di natura soltanto eventuale, si riferisce miratamente a una casistica che presenti particolari elementi di complessità e rischio, in ciò potendosi comprendere l'attribuzione in capo all'autorità di una funzione di *gate keeper*, e dunque di controllore ultimo, a chiusura del sistema, della sussistenza di motivi a violazione del *GDPR*[170].

5.3 L'informatizzazione del procedimento assembleare: i presìdi a tutela della riservatezza dei dati personali

L'attuale emergenza sanitaria ha reso di stretta attualità il tema delle possibili interferenze tra i presìdi a tutela della riservatezza dei dati personali e lo svolgimento delle assemblee delle società quotate con modalità di collegamento da remoto.

Non si tratterebbe, d'altro canto, di un'assoluta novità in ambito societario, in quanto, già a partire dalla riforma del 2003, le disposizioni codicistiche ammettono la sostituzione della partecipazione all'assemblea mediante presenza fisica con la partecipazione attraverso mezzi di telecomunicazione[171].

168 Mantelero, *La gestione del rischio*, cit., 504-505.

169 Così il *considerando* n. 94 del GDPR.

170 Sartore, *La valutazione d'impatto nel GDPR*, in Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Giuffrè, Milano, 2019, 345.

171 In dottrina, *inter alia*, Salafia, *L'intervento nell'assemblea della s.p.a. e della s.r.l.*, in *Soc.*, 2004, 672 ss.; Turelli, *Assemblea di società per azioni*, cit., 116 ss.; Id., *Assemblee di società per azioni ed esercizio del diritto di voto*, cit., 445 ss. e, da ultimo, Magliulo, *Le nuove tecnologie informatiche ed il rispetto del metodo collegiale*, in *Notariato*, 2019, 378 ss.

Come già illustrato in precedenza al cap. 3, l'impiego delle tecnologie informatiche nell'assemblea della società per azioni trova la sua disciplina primaria negli artt. 2370, comma 4, c.c. e 127, TUF[172], i quali, rispettivamente, prevedono la possibilità che lo statuto contempli l'intervento in assemblea mediante mezzi di telecomunicazione oppure l'espressione del voto in via elettronica e, con riferimento alle sole società quotate, demandano alla CONSOB il compito di determinare con regolamento le modalità di svolgimento dell'assemblea nelle ipotesi indicate.

Peraltro, il crescente ricorso a strumenti telematici in tale ambito ha fatto sì che la disciplina in esame, da ipotesi alternativa all'ordinaria modalità di svolgimento delle assemblee tradizionali, sia diventata, nel tempo, modalità effettiva di svolgimento delle assemblee *on-line*, sollevando una serie di questioni applicative a cui la disciplina di riferimento non ha ancora trovato soluzione. Si pensi, ad esempio, agli aspetti – già menzionati *supra* – relativi l'identificazione degli azionisti collegati; ai requisiti di sicurezza del sistema informatico; alla tutela della riservatezza dei lavori assembleari; alle conseguenze dell'interruzione del collegamento remoto durante lo svolgimento della riunione; alla registrazione della riunione[173].

Lo scoppio della pandemia e l'introduzione delle misure di sicurezza volte a prevenire gli assembramenti e lo svolgimento di riunioni fisiche, in luoghi pubblici e privati, ha fatto nuovamente emergere alcune delle criticità esposte, soprattutto in ragione dell'impossibilità assoluta di svolgimento delle assemblee con le modalità tradizionali. Si è già più sopra riferito che l'art. 106, D.L. n. 18/20, ha introdotto alcune misure emergenziali che incidono sulle modalità di svolgimento delle assemblee delle società di capitali e cooperative, concedendo, tra l'altro, la possibilità che queste si svolgano anche ove non sussista un'apposita previsione statutaria[174].

La disciplina emergenziale in materia ha dato altresì risalto ad alcune questioni interpretative attinenti alla tutela della *privacy*, per lo più di natura applicativa, che, seppur emerse a seguito dello scoppio della pandemia, prescindono da

172 Modificati entrambi modificati dal d. lgs. 27/2010 di attuazione della *SHRD*.

173 Per un approfondimento sul rapporto tra assemblea tradizionale ed assemblea a distanza v. Cabras, *L'assemblea in videoconferenza nelle società di capitali*, in *Vita not.*, 2001, 577 ss.; Demuro, *Partecipazione virtuale alle riunioni collegiali di società,* in *Giur. comm.*, 2002, II, spec. 399, nt. 3 e 407, nt. 36; Marchetti, *La "prudente innovazione" dell'assemblea virtuale*, in *Notariato*, 2001, 221 ss.; Palmieri, *Diritto societario virtuale: la videoassemblea diventa realtà*, in *Contr. e impr.*, spec. 830, nt. 1 e 833, nt. 9. In senso analogo, Cian, *L'intervento*, cit., 1074 ss.; Pederzini, *Intervento del socio*, cit.

174 La disciplina emergenziale ha previsto inoltre: (*i*) le società possono prevedere, mediante apposita indicazione contenuta nell'avviso di convocazione, che il voto sia espresso in via elettronica o per corrispondenza e che la partecipazione possa avvenire mediante mezzi di telecomunicazione anche in deroga a diverse disposizioni statutarie (art. 106, comma 2, prima frase); (*ii*) le società possono altresì prevedere che la partecipazione avvenga esclusivamente mediante mezzi di telecomunicazione, senza necessità che il presidente e il segretario o il notaio si trovino nel medesimo luogo (art. 106, comma 2, seconda frase); (*iii*) le società quotate possono avvalersi del rappresentante designato ai sensi dell'art. 135-*undecies* TUF anche in deroga a diverse disposizioni statutarie (art. 106, comma 4, prima frase); (*iv*) le società quotate possono altresì prevedere, mediante apposita indicazione contenuta nell'avviso di convocazione, che la partecipazione dei soci avvenga esclusivamente mediante il rappresentante designato ai sensi dell'art. 135-*undecies* TUF, con facoltà di attribuire al medesimo anche le deleghe o subdeleghe c.d. ordinarie di cui all'art. 135-*novies* TUF (art. 106, comma 4, seconda frase). Per una disamina approfondita sulla disciplina emergenziale cfr. Marchetti, Notari, *Diritti dei soci*, cit., 428.

quest'ultima, posto che la digitalizzazione del procedimento assembleare sembra un fenomeno accolto con apprezzamento da più parti.

Per quanto concerne il trattamento dei dati personali degli azionisti che partecipano da remoto all'assemblea, il tema è per lo più connesso con quello dell'identificazione di quest'ultimi, al fine di consentire la partecipazione in assemblea. La questione, tuttavia, non ha sollevato particolari criticità con riferimento ai presìdi posti a tutela di tali dati personali. Le società sono, infatti, tenute all'osservanza delle medesime prescrizioni in tema di "*Informativa e consenso al trattamento dei dati personali*".

Un aspetto che ha, invece, sollevato perplessità in termini di tutela riguarda il tema della registrazione delle assemblee tenute a distanza in video-conferenza, nell'ipotesi in cui dalle stesse risultino desumibili dati personali che possano ricondurre all'identità personale dei partecipanti. Il codice civile non fa, infatti, alcun accenno alla possibilità di registrare le riunioni con strumenti elettronici. Pertanto, lo statuto sociale può consentire o vietare le registrazioni delle riunioni. Se lo statuto tace sul punto, non essendo dettata una specifica disciplina sulle registrazioni delle riunioni societarie tenute a distanza, sembrerebbe trovare applicazione la disciplina generale sulla *privacy* con gli interventi chiarificatori del Garante per la protezione dei dati personali[175] e della Corte di cassazione[176] su questioni analoghe sollevate per le riunioni condominiali.

Pertanto, in conformità alle disposizioni in materia di *privacy*, la società per non incorrere in condotte illecite ha l'obbligo di informare preventivamente sulle finalità del trattamento dei dati che verranno raccolti (art. 13, *GDPR*), raccogliendo il consenso alla registrazione della riunione da parte dei partecipanti, soprattutto nell'ipotesi in cui la registrazione non avvenga per fini di ausilio alla verbalizzazione, ma per consentire la diffusione della registrazione stessa[177].

Gli azionisti devono, quindi, essere informati delle finalità del trattamento dei dati che verranno raccolti, se i dati verranno pubblicati o diffusi in qualsiasi modo, se verranno salvati su supporti di qualsiasi specie e se e quando verranno distrutti, precisando altresì che gli stessi saranno trattati nel rispetto delle misure tecniche e

175 La questione è stata affrontata dal Garante per la protezione dei dati personali in materia condominiale nel vademecum "*Il condominio e la privacy*", con statuizioni valide anche per le riunioni societarie. Il Garante, in tale sede, ha affermato che «*L'assemblea condominiale può essere videoregistrata, ma solo con il consenso di tutti i partecipanti. La documentazione, su qualsiasi supporto, deve essere conservata al riparo da accessi indebiti*».

176 V. Cass. pen., sez. III, Sent., 13/05/2011, n. 18908, e Cass. pen., sez. III, Sent., 03/02/2017, n. 5241.

177 Il Garante per la protezione dei dati personali e la Cassazione hanno, inoltre, affrontato l'ipotesi in cui la registrazione sia effettuata dal singolo intervenuto alla riunione a distanza senza la previa autorizzazione degli altri intervenuti. In tale caso, il Garante ha sostenuto che la condotta non è considerata illecita, se viene effettuata per fini esclusivamente personali, ossia se la stessa rimane conservata nella sfera della persona che ha registrato come memoria storica dei fatti avvenuti durante la riunione e non travalichi detta sfera con la comunicazione e la diffusione ad altri della registrazione (Provvedimento Garante 8 novembre 2002, n. 1067292). Analogamente, le Sezioni Unite della Corte di Cassazione hanno ritenuto che, nell'ipotesi di cui sopra, non sussista lesione della *privacy*, poiché la registrazione non dà luogo alla «*compromissione del diritto alla segretezza della comunicazione, il cui contenuto viene legittimamente appreso solo da chi palesemente vi partecipa o assiste*» (Cass. pen., SS.UU., Sent., 24/09/2003, n. 36747).

organizzative adeguate, secondo quanto previsto dall'art. 32, *GDPR*, e che il trattamento viene svolto ad opera di soggetti appositamente istruiti e autorizzati, in ottemperanza a quanto previsto dall'art. 29, GDPR.

La protezione della *privacy* non si potrà, invece, esaurire nella sola raccolta del consenso degli intervenuti, richiedendo anche il rispetto da parte della società delle norme in ordine alla conservazione delle informazioni raccolte sui supporti fisici o digitali, nonché l'indicazione del titolare del trattamento e del responsabile. La diffusione delle registrazioni senza il consenso dei presenti realizza, infatti, la fattispecie del "*trattamento illecito di dati*" previsto dall'art. 167, D. lgs. n. 196/2003, salvo che la registrazione audio o audio-video sia prodotta per far valere o difendere un diritto in sede giudiziaria o per svolgere investigazioni difensive[178].

5.4 Il trattamento dei dati personali degli azionisti

L'interferenza della digitalizzazione con i sistemi di *governance* delle società quotate necessita una particolare riflessione in merito alle modalità con cui le società procedono alla raccolta dei dati degli azionisti[179].

Questi ultimi sono tenuti a fornire alla società un flusso di dati necessari per il concreto esercizio dei diritti e degli obblighi derivanti dalla partecipazione sociale, nonché per consentire alla società di eseguire i propri obblighi di natura amministrativa, contabile, di gestione delle assemblee o per rispondere a richieste derivanti dal ruolo di azionista, anche mediante tecniche di comunicazione a distanza. In tale ipotesi, la base giuridica del trattamento va proprio ricercata nell'esecuzione di un vincolo contrattuale e il periodo di conservazione degli stessi corrisponde alla durata del rapporto o della singola operazione.

In ambito societario la raccolta e il trattamento dei dati degli azionisti vengono effettuati anche per finalità ulteriori rispetto al mero adempimento di obblighi derivanti dal rapporto società-azionista, in particolare per finalità legate all'assolvimento di obblighi previsti dalla legge (si pensi all'aggiornamento e gestione del libro soci), da regolamenti, dalla normativa dell'UE, nonché da disposizioni impartite da autorità di vigilanza o in ossequio a richieste avanzate dall'Autorità giudiziaria. La base giuridica del trattamento, in tali ipotesi, è da ricercare nell'adempimento di un obbligo legale, rendendosi, anche in questo caso, la prestazione del consenso da parte dell'azionista non necessaria.

La mancata, parziale o inesatta comunicazione dei suddetti dati da parte dell'azionista può, pertanto, generare come conseguenza l'impossibilità di svolgere le

178 Cass. pen., sez. III, Sent. 03/02/2017, n. 5241.

179 Per un approfondimento più ampio sul tema v. Abriani, *La* corporate governance *nell'era dell'algoritmo. Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla* corporate governance, in *Dir. soc.*, 1, 2020, 173.

attività richieste dalla legge e precludere alla società di adempiere agli obblighi normativi ad essa applicabili[180].

I dati personali riferibili agli azionisti che le società quotate raccolgono e trattano per il raggiungimento delle finalità sopra indicate saranno, a titolo esemplificativo, i dati anagrafici dell'azionista, i dati di contatto, le informazioni relative ai titoli azionari posseduti e a eventuali vincoli presenti su di essi, nonché tutti gli altri dati personali strettamente necessari alla partecipazione all'assemblea degli azionisti.

Anteriormente alla raccolta di tali dati, le società provvedono a sottoporre preventivamente agli azionisti la cosiddetta "*Informativa sul trattamento dei dati personali degli Azionisti*", al fine di renderli edotti sulle modalità di trattamento dei suddetti dati, circa i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati e i relativi diritti dell'azionista-interessato.

Per quanto concerne, più nello specifico, le modalità di trattamento, preme evidenziare che, grazie all'impiego di nuovi *software* e altre soluzioni telematiche per l'organizzazione dell'attività assembleare, i dati personali vengono raccolti e processati in modo dinamico, anche mediante l'ausilio di procedimenti automatizzati (art. 4 *GDPR*)[181]. La completa automazione del trattamento, tuttavia, non può giustificare differenti livelli di tutela dei soggetti interessati, in virtù del principio di "neutralità tecnologica". Al contrario, è opportuno ribadire come, anche nell'ipotesi in cui il dato venga trattato mediante tecnologie automatizzate, il titolare del trattamento non è dispensato dall'obbligo di rispettare le regole in materia di *privacy*, che, anzi, in questi casi, risultano in certa misura rafforzate[182].

Si tratta di un ambito che, pur avendo subìto un certo spicco a seguito del crescente ricorso a forme di digitalizzazione delle comunicazioni in conseguenza della recente pandemia[183], era già stato oggetto di una riflessione da parte del Comitato

180 Al riguardo, seppur datato, si ricorda il provvedimento del Garante per la protezione dei dati personali "*Divulgabili i dati sull'identità degli azionisti*", del 5 ottobre 1999, con il quale il Garante ha affermato che «[l]*a divulgazione delle informazioni sulle attività economiche, comprese quelle relative agli azionisti delle società, non contrasta con la legge sulla privacy che tende, semmai, a favorire la trasparenza e la circolazione di tali informazioni*». Richiamando quanto già affermato in due diversi pareri forniti all'Autorità Antitrust e alla Consob, il Garante ha ribadito che l'impostazione generale della legge sulla *privacy* è volta a favorire il flusso di informazioni sullo svolgimento di attività economiche da parte di terzi interessati.

181 Cfr. Angelini, *Intelligenza Artificiale* e Governance. *Alcune riflessioni di sistema*, in Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 293 ss.

182 V. il *considerando* n. 15 del *GDPR*: «*al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio*».

183 Un aspetto di particolare rilievo, emerso con il dilagare della pandemia, riguarda i profili di tutela della *privacy* in seno allo svolgimento delle Assemblee degli azionisti con modalità virtuali. In particolare, con riferimento alla registrazione dell'adunanza assembleare, in assenza di manifestazione del consenso da parte degli azionisti intervenuti. Per non incorrere in condotte illecite la società è tenuta a informare preventivamente sulle finalità del trattamento dei dati che verranno raccolti (art. 13 *GDPR*) e per far ciò è opportuno che la società predisponga una modulistica sulla *privacy*, che la comunichi ad ogni persona legittimata a partecipare alla riunione e che raccolga il consenso di tutti prima dell'inizio dei lavori, in mancanza non potrà procedersi alla registrazione della riunione. a protezione della *privacy* non si esaurisce nella sola raccolta del consenso *privacy* degli intervenuti e richiede anche il rispetto da parte della società delle norme in ordine alla conservazione delle informazioni rac-

per la *Corporate Governance* in sede di approvazione del nuovo Codice di *Corporate Governance*. Il particolare, tale Codice, seppur non incentrando la propria analisi sul solo trattamento dei dati personali degli azionisti, ha dettato princìpi applicabili anche a quest'ultimi, invitando gli emittenti ad adottare specifici presìdi per proteggere i dati oggetto dei flussi informativi e inserirli in un regolamento interno[184].

Il Comitato ha infatti ritenuto che, in virtù del rilevante impatto che la digitalizzazione sta avendo in ambito societario, la protezione dei dati aziendali contenenti dati personali sia da ritenersi sempre più una responsabilità dell'impresa. A tal fine, il Codice ha invitato le società quotate a dotarsi di regole societarie sul trasferimento dei dati, elaborando *policies* interne in cui delineare le modalità con cui viene effettuato lo scambio di informazioni, le piattaforme digitali utilizzate, nonché le misure di sicurezza adottate in atto in conformità all'art. 32 *GDPR* (art. 3, principio IX e raccomandazione n. 11)[185], tenendo conto dell'oggetto, del contesto, delle finalità e dei rischi connessi al trattamento, prevedendo, inoltre, l'attuazione di programmi di *security awareness*[186].

5.5 Trattamento illecito dei dati personali e profili di responsabilità nelle società quotate

Il problema dell'uso di sistemi digitali per il trattamento di dati personali all'interno dei processi di *governance* societaria suscita alcune considerazioni in termini di responsabilità, ove il trattamento degli stessi risulti illecito.

In particolare, l'impiego di algoritmi per fini organizzativi – che è, peraltro, alla base della cosiddetta *RegTech* – unitamente all'utilizzo di sistemi informatici, quale veicolo di diffusione di dati e informazioni, pongono alcuni interrogativi circa il corretto bilanciamento tra la tutela del diritto alla *privacy* e l'obbligo di trasparenza prescritto in capo alla società quotate[187].

Il tema del bilanciamento tra siffatti interessi è da sempre rilevante, posto che la definizione dei rispettivi confini non sempre è apparsa chiara e, molto spesso,

colte sui supporti fisici o digitali, nello specifico le registrazioni in audio o in videoconferenza delle riunioni, nonché l'indicazione del titolare del trattamento e del responsabile. Sul punto si è espresso il Garante *Privacy*, su un tema affine quale quello relativo all'assemblea condominiale, precisando che «[l]'assemblea condominiale può essere videoregistrata, ma solo con il consenso di tutti i partecipanti. La documentazione, su qualsiasi supporto, deve essere conservata al riparo da accessi indebiti». Tale principio trova applicazione per ogni tipologia di riunioni, tra le quali vi rientrano anche le riunioni in ambito societario.

184 Al riguardo il Codice, oltre a affrontare il tema della digitalizzazione del dato sotto il profilo della *privacy*, si sofferma altresì anche sui dati contenuti nei flussi informativi che potrebbero qualificarsi come informazioni privilegiate, sottolineando come il fine perseguito sia quello di evitare che la *disclosure* che comportino violazioni ai sensi del regolamento UE sugli abusi di mercato.

185 Amato, Benvenuto, *L'Organo amministrativo nel Codice di* Corporate Governance*: funzionamento, nomine ed autovalutazione*, in *Dir. Banc.*, 2020.

186 Al riguardo si veda il *Rapporto Clusit sulla sicurezza ICT in Italia*, 2020, 78, disponibile al link: https://clusit.it/rapporto-clusit.

187 Agostino, *Intelligenza artificiale e processi decisionali. La responsabilità degli amministratori di società, in Merc. Conc. Reg.*, 2020, 2, 371 ss.

ha visto il diritto alla protezione dei dati personali cedere il passo a interessi di natura pubblicistica, reputati di rango superiore, come nel caso della trasparenza in materia societaria a favore dei soci[188].

Uno degli aspetti su cui si è maggiormente concentrata l'attenzione della giurisprudenza e della dottrina concerne la pubblicazione sul sito *web* della società di particolari categorie di dati personali, riconducibili a esponenti del C.d.A., in osservanza delle disposizioni di cui all'art. 125-*ter* TUF[189]. Il tema attiene alla ricerca del corretto equilibrio tra l'interesse all'informazione del pubblico dei risparmiatori, soci presenti e futuri ed eventuali creditori, tutelato dalla legge, con i diritti di rango costituzionale, tra cui il diritto alla *privacy*.

In considerazione della rilevanza dell'argomento in esame, non è mancato il coinvolgimento del Garante, il quale, in passato, si è più volte espresso sul tema, per lo più rigettando le richieste dei ricorrenti tese ad ottenere la cancellazione dei dati personali contenuti nel registro delle imprese o un'accessibilità limitata ai libri sociali, sulla base del fatto che non sussistessero comprovati elementi che permettevano di giudicare come non compatibile la disciplina codicistica sulla tenuta del registro delle imprese con la disciplina in materia di *privacy*[190].

Tenuto conto dell'attualità del fenomeno della pubblicazione sul web di informazioni rilevanti volte a ledere l'integrità e la moralità dei soggetti coinvolti, il Garante è nuovamente intervenuto sul tema nel 2014, pubblicando le "*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati*"[191]. Il Garante, seppur facendo riferimento, nello specifico, alla pubblicazione di atti e documenti amministrativi, ha precisato che, sulla base del principio di pertinenza e non eccedenza, è «*consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto*». Pertanto, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione *on-line*.

Alla medesima conclusione, peraltro, si giunge anche esaminando la disciplina dettata dal *GDPR*, ove è previsto che il titolare del trattamento debba porre in essere misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Alla stregua di quanto sinora esposto, appare corretto riconoscere in capo alla società uno speciale dovere di agire con cautela e, comunque, nel pieno rispetto

188 Pappalardo, *Obblighi di trasparenza per le società quotate: la pubblicità a mezzo Internet e la tutela della privacy*, in *Dir. merc. fin.*, 2018, 2, 187 ss.

189 Cfr. Trib. Torino, Sez. IV, 12 giugno 2017.

190 Da ultimo, v. Garante *Privacy*, Provvedimento del 19 dicembre 2000, e anche Assonime, *Diritto di ispezione del libro soci e tutela della* privacy, *Il Caso*, n. 8, 28 ottobre 2009, in www.assonime.it.

191 Garante *Privacy*, Provvedimento n. 243 del 15 maggio 2014, pubblicato sulla G.U. 12 giugno 2014, n. 134.

del principio di minimizzazione dei dati personali, ogni qualvolta la stessa proceda alla diffusione di informazioni personali di soggetti terzi attraverso le piattaforme *web* della società[192].

5.6 L'apparato sanzionatorio delle violazioni

Il mancato rispetto degli obblighi imposti dalla normativa in materia di trattamento dei dati personali comporta, come prima e diretta conseguenza, l'esposizione dei soggetti attivi del trattamento a un ampio ventaglio di misure rimediali o di carattere sanzionatorio, selezionate sulla base di differenti criteri, elencati dal *GDPR*, ai quali le autorità di controllo faranno riferimento per esercitare i poteri correttivi di cui all'art. 58, *GDPR*. Si tratta di poteri riconosciuti in capo al Garante ed evidentemente caratterizzati dalla duplice finalità dissuasiva e repressiva rispetto alla commissione di un illecito, che si affiancano a quelli di competenza dell'AGO con riferimento agli illeciti di natura sia civile (art. 82, *GDPR*) sia penale (art. 84, *GDPR*).

Innanzitutto, si menziona l'istituto del reclamo all'autorità *ex* art. 77, *GDPR*, strumento di impulso dell'attività ispettiva del Garante che si pone su un piano di carattere ripristinatorio della correttezza del trattamento, a tempestiva tutela della persona fisica interessata, alla quale è comunque riconosciuto il doppio binario del ricorso giurisdizionale per chiedere il risarcimento del danno «*materiale e immateriale*» patito dall'illecito trattamento (art. 82, *GDPR*)[193]. Il risarcimento del danno non si limita a considerare i danni di natura patrimoniale, comprendendo altresì quelli non patrimoniali, a prescindere dall'eventuale accertamento di una fattispecie di reato e per il solo fatto di violare le norme del *GDPR*[194]. Sul punto, il *considerando* n. 146 del *GDPR* precisa che il titolare e il responsabile del trattamento sono responsabili *in solido* del danno cagionato dal trattamento illecito, a meno che non dimostrino che l'evento dannoso non sia loro imputabile.

Quanto alle sanzioni vere e proprie – come accennato – l'autorità di controllo gode di una certa discrezionalità nella scelta della misura sanzionatoria, nel rispetto di una serie di parametri valutativi tipizzati dall'art. 83 *GDPR*, per la cui interpretazione è utile affiancare le precisazioni contenute nelle Linee guida del *WP29* in materia di sanzioni amministrative[195].

Anzitutto, la valutazione del Garante sull'opportunità di procedere all'irrogazione di una sanzione amministrativa, oltreché, eventualmente, sul suo importo, deve tener conto della natura, della gravità e della durata della violazione

192 Finocchiaro, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. informaz. informatica*, 2012, 3, 383 ss.

193 Califano, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in Califano, Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, 41.

194 Tosi, *La responsabilità civile per trattamento illecito dei dati personali*, in Tosi (a cura di), Privacy *Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, Milano, 2019, 651.

195 WP29, *Linee guida*, cit., 2017, 9 ss.

(art. 83, § 2, lett. a, *GDPR*). La formulazione della disposizione, che, nei §§ da 4 a 6, fissa due diversi massimali per quantificare l'entità delle sanzioni amministrative pecuniarie (10 o 20 milioni di euro, ovvero fino al 2% o 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore), fornisce immediatamente l'indicazione di quelle disposizioni (ad esempio, quelle riguardanti i fondamenti della *data protection*, di cui agli artt. 12-22, *GDPR*) la cui violazione è considerata particolarmente pregiudizievole e, in quanto tale, meritevole di una maggior tutela.

La natura della violazione e «*l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito*» forniscono un'indicazione della gravità della violazione. E, laddove in un singolo caso siano contestualmente commesse più violazioni di diversa natura, l'autorità di controllo applicherà le sanzioni amministrative pecuniarie che risultino effettive, proporzionate e dissuasive, benché, in ogni caso, nei limiti della violazione più grave (art. 83, § 3, *GDPR*). A tal fine, assumono particolare rilevanza: il numero degli interessati coinvolti; la finalità del trattamento; l'entità del danno eventualmente subìto dagli interessati.

Quanto alla durata dell'infrazione, invece, essa rileva in quanto utile a fornire un'indicazione, ad esempio, sull'abitualità del comportamento adottato dal titolare del trattamento, sulla predisposizione di adeguate misure preventive del compimento di un illecito oppure sull'incapacità del titolare di attuare quanto richiesto a livello tecnico-organizzativo dalla disciplina sulla sicurezza del trattamento.

L'elenco dei parametri di cui all'art. 83 *GDPR* si riferisce, alla lett. *b*), all'elemento soggettivo dell'illecito, ovverosia al carattere doloso o colposo della violazione, rispetto al quale la valutazione dell'autorità riprende strettamente le categorie proprie del sindacato giurisdizionale[196].

Rilevano, poi, «*le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati*» (lett. *c*), in considerazione di un vero e proprio obbligo in capo a tali soggetti di tentare quantomeno di ridurre le conseguenze della violazione per il destinatario del trattamento. In tal senso, il Garante tiene conto del grado di responsabilità assunto dai soggetti attivi del trattamento, sia sotto il profilo della scelta della sanzione da irrogare, sia per ciò che concerne il suo ammontare. Tale elemento acquista rinnovata centralità anche con riferimento all'esecuzione del trattamento stesso, nell'ottica di verificare se il titolare o il responsabile abbiano adottato le adeguate misure tecniche e organizzative a garanzia della sicurezza del trattamento, come previsto nel complesso dal *GDPR* (lett. *d*).

Rilevano, inoltre, eventuali altre precedenti violazioni commesse dal titolare o dal responsabile del trattamento relativamente allo stesso oggetto (lett. *e*) e, in caso, il rispetto dei relativi provvedimenti emessi dal Garante (lett. *i*); il grado di

196 Califano, *op. cit.*, 45.

cooperazione con l'autorità per porre rimedio alla violazione e attenuare, per quanto possibile, gli effetti negativi realizzati (lett. *f*); le categorie di dati personali interessate dalla violazione (lett. *g*).

Ancora, assume rilevanza anche la modalità con cui il Garante abbia avuto conoscenza della violazione (lett. *h*), in quanto il titolare del trattamento ha l'obbligo di notificare all'autorità le eventuali violazioni dei dati personali realizzate in sede di esecuzione del trattamento. Assumono effetti particolarmente sfavorevoli nell'individuazione della natura della sanzione non solo l'incauta assenza della notifica, ma anche la sua eventuale incompletezza della descrizione[197].

La lett. *j*) si riferisce, poi, all'adesione ai codici di condotta o ai meccanismi di certificazione approvati, rispettivamente, ai sensi degli artt. 40 e 42 *GDPR*[198].

Da ultimo, rilevano gli «*eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso*» (lett. *k*), rispetto ai quali la stessa disposizione propone, a titolo esemplificativo, il caso in cui il titolare del trattamento abbia tratto profitto (conseguendo benefici finanziari ovvero evitando perdite) in modo diretto o indiretto proprio dalla violazione del *GDPR*.

In considerazione di tutti questi criteri di valutazione, il Garante, se ritiene che sussista la violazione di una o più disposizioni regolamentari, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni, trasmettendo al titolare o al responsabile del trattamento una comunicazione con la quale indica le violazioni loro ascrivibili. Nei trenta giorni successivi a tale comunicazione i destinatari possono replicare, presentando apposita documentazione difensiva, potendo altresì richiedere di essere ascoltati. Alla luce di tali osservazioni, spetta poi al Garante emettere il proprio provvedimento ed eventualmente irrogare la sanzione, contro la quale è possibile proporre opposizione mediante ricorso dinanzi all'AGO[199].

197 WP29, *Linee guida*, cit., 2017, 16.

198 In argomento si veda Poletti, Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in Tosi (a cura di), *Privacy Digitale*, cit., 374 ss.

199 Aterna, sub *art. 83 GDPR*, in Riccio, Scorza, Belisario (a cura di), *GDPR e Normativa* Privacy. *Commentario*, Milano, 2018, 608 ss.