

RE-JUS CASEBOOK

CASEBOOK ITALIANO IN MATERIA DI DIRITTI DI PROTEZIONE DEI DATI PERSONALI



THE RE-JUS PROJECT IS CO-
FUNDED BY THE JUSTICE
PROGRAMME OF THE
EUROPEAN UNION

(JUST/2015/JTRA/AG/EJTR/8703)

Pubblicato nell'ambito del progetto:

Roadmap To European Effective Justice (Re-Jus):

Judicial Training Ensuring Effective Redress To Fundamental Rights Violations.

Partner coordinatore:

Università di Trento (Italia)

Partners principali:

Università di Versailles Saint Quentin-en-Yvelines (Francia)

Istituto di Scienze Giuridiche dell'Accademia delle Scienze Polacca. (Polonia)

Università di Amsterdam (Olanda)

Partners associati:

Scuola Superiore della Magistratura (Italia)

Consejo General del Poder Judicial (Spagna)

Institutul National al Magistraturii (Romania)

Pravosudna Akademija (Croazia)

Ministrstvo za pravosodje Republika Slovenije (Slovenia)

Judicial Studies Committee of the Irish Judiciary (Irlanda)

Coordinatore scientifico del progetto Re-Jus:

Fabrizio Cafaggi

Coordinamento:

Paola Iamiceli (*scientific coordination of Re-Jus teams*)

Chiara Patera (*Project Manager*)

Coordinamento del team di esperti in Data Protection:

Federica Casarosa e Martina Flamini

Coautori:

Martina Flamini

Francesca Capotorti

Federica Casarosa

Nota sugli esperti ed i collaboratori nazionali:

Il *team* Re-Jus ringrazia tutti i magistrati, gli esperti ed i collaboratori che hanno contribuito alla realizzazione del progetto e alla stesura del presente *Casebook* attraverso la segnalazione di pronunce giurisprudenziali nazionali ed europee (in ordine alfabetico):

Roberta Brusco

Nicole Di Mattia

Sommario

INTRODUZIONE

| | |
|---|---|
| Diritto alla protezione dei dati personali nel quadro del diritto europeo e nazionale | 4 |
| L'impatto della Carta in materia di protezione dei dati | 5 |
| Il dialogo fra le corti | 5 |
| Tutela amministrativa e tutela giurisdizionale | 6 |
| Le nuove sfide del Regolamento 2016/678 | 7 |

1. BILANCIAMENTO TRA DIRITTI FONDAMENTALI

| | |
|--|----|
| 1.1 Premessa | 9 |
| 1.2 Il contesto europeo e quello italiano. L'individuazione dei beni protetti: il diritto alla manifestazione del pensiero, il diritto ad informare ed il diritto ad essere informati, il diritto alla tutela della riservatezza. | 10 |
| 1.3 La questione | 12 |
| 1.4 Il caso: Tribunale di Roma, 3 dicembre 2015, n. 23771 | 13 |
| 1.5 La giurisprudenza italiana. Un focus su una decisione di merito | 15 |
| 1.6 La giurisprudenza europea | 16 |
| 1.7 Questioni aperte | 18 |
| 1.8 Le novità del D.Lgs. 101/2018 | 19 |
| 1.9 Rilievi conclusivi | 20 |

2. EFFETTIVITÀ DELLA TUTELA, PROPORZIONALITÀ E MISURE CORRETTIVE

| | |
|---|----|
| 2.1 Premessa | 22 |
| 2.2 Tipologia di poteri e rimedi della pubblica amministrazione | 22 |
| 2.3 Poteri e rimedi dell'autorità giudiziaria | 25 |

3. EFFETTIVITÀ DELLA TUTELA, PROPORZIONALITÀ E SANZIONI

| | |
|---|----|
| 3.1 Premessa | 31 |
| 3.2 Principi generali in materia di illeciti amministrativi: le applicazioni nella giurisprudenza con riguardo ai provvedimenti del Garante Privacy | 31 |
| 3.3 L'elemento soggettivo dell'illecito | 31 |
| 3.4 La responsabilità dell'Ente | 32 |
| 3.5 Termine di decadenza per la contestazione dell'illecito e l'irrogazione della sanzione | 33 |
| 3.6 Il doppio binario sanzionatorio | 34 |
| 3.7 La giurisdizione del G.O. | 36 |
| 3.8 Il controllo dell'AGO sui provvedimenti sanzionatori | 38 |

4. EFFETTIVITÀ DELLA TUTELA, PROPORZIONALITÀ E TUTELA RISARCITORIA

| | |
|---|----|
| 4.1 Premessa | 43 |
| 4.2 Risarcibilità del danno per violazione dei dati personali | 43 |
| 4.3 Nuove prospettive dell'azione collettiva | 46 |
| 4.4 La legittimazione ad agire | 46 |
| 4.5 La competenza territoriale | 47 |
| 4.6 Effetti delle decisioni | 48 |
| 4.7 Rilievi conclusivi | 49 |

INTRODUZIONE

Diritto alla protezione dei dati personali nel quadro del diritto europeo e nazionale

Dal 1995, il legislatore europeo ha affrontato la necessità di proteggere i dati dei cittadini europei allo scopo di facilitare i trasferimenti transfrontalieri dei dati all'interno dell'UE. La necessità di armonizzare la legislazione tra gli Stati membri è stata stimolata dalla presenza di standard di protezione diversi presenti in normative nazionali all'epoca in vigore, capaci di ostacolare il libero flusso di dati personali. Di conseguenza, la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, era stata adottata al fine di armonizzare la protezione dei diritti fondamentali delle persone rispetto alle attività di trattamento dei dati personali. La base giuridica dell'intervento legislativo era dunque fondata sulla libera circolazione e sulla tutela dei diritti individuali.

L'attuazione a livello nazionale richiesta dalla direttiva, tuttavia, ha dimostrato di non avere raggiunto l'obiettivo di armonizzare la legislazione sulla protezione dei dati all'interno dell'UE.

Nel frattempo sono stati adottati altri strumenti giuridici per risolvere le questioni emergenti in quelle aree in cui la protezione dei dati convergeva con gli sviluppi tecnologici e con altri settori specifici del diritto, come la direttiva 2002/58/CE relativa al trattamento dei dati personali e la protezione della vita privata nel settore delle comunicazioni elettroniche, la decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione di polizia e giudiziaria in materia penale e la direttiva 2004/82/CE del Consiglio 29 aprile 2004 sull'obbligo dei vettori di comunicare i dati dei passeggeri.

Alla luce del livello di frammentazione molto elevato e di divergenze tra le normative di implementazione negli Stati membri, l'UE ha avviato un'ampia riforma nei settori della protezione dei dati. Il lungo processo di negoziazione ha portato all'adozione, nel 2016, del Regolamento generale sulla protezione dei dati n. 2016/678 (GDPR). La scelta del regolamento era finalizzata al raggiungimento dell'armonizzazione totale, essendo il regolamento immediatamente applicabile. Sono tuttavia ancora presenti norme aperte che lasciano spazio alle specificità nazionali. Si tratta dunque di un livello di armonizzazione superiore a quello previsto dalla direttiva previgente ma non completo; le divergenze interpretative dovranno quindi essere risolte attraverso forme di cooperazione amministrativa e giudiziaria.

Con riguardo ai soggetti deputati all'enforcement, coesistono diverse autorità. A tal proposito, occorre ricordare come sin dall'inizio dell'intervento europeo tutela amministrativa e tutela giurisdizionale siano state previste, ancorché il loro coordinamento sul piano nazionale sia stato affidato al diritto dei singoli paesi e sul piano europeo nessuna disposizione vi abbia provveduto. La natura potenzialmente transfrontaliera delle violazioni e soprattutto dei loro effetti nei casi in cui siano coinvolti operatori globali avrebbe invece richiesto un coordinamento sia sul piano della repressione che su quello degli strumenti di tutela.

A livello nazionale, il GDPR ha portato all'adozione di un decreto legislativo di adeguamento della normativa nazionale in materia di protezione dei dati personali e per la precisione il **d.lgs. n. 101 del 10 agosto 2018** pubblicato il 4 settembre sulla G.U. n. 205/2018 – in vigore dal 19 settembre 2018 - che ha provveduto ad adeguare le disposizioni del d.lgs. n.196/2003 al GDPR . Le disposizioni di tale

decreto legislativo – che hanno profondamente innovato la previgente disciplina – verranno, in questa sede, solo indicate con riferimento agli aspetti oggetto della presente trattazione.

L'impatto della Carta in materia di protezione dei dati

Con l'entrata in vigore del trattato di Lisbona, la Carta dei diritti fondamentali dell'UE (CDF) è diventata vincolante e il diritto della protezione dei dati personali sancito dall'articolo 8 della Carta ha acquisito un riconoscimento e un'autonomia nei confronti del diritto al rispetto della vita privata. Questi diritti fondamentali peraltro impongono agli Stati Membri di predisporre rimedi efficaci. Sebbene la CGUE abbia affrontato esplicitamente solo in alcune occasioni il coordinamento tra le due disposizioni della Carta, in numerosi altri casi la Corte ha giudicato sulla base del principio di effettività, orientando l'interpretazione verso standard elevati per la protezione dei dati. In particolare, il principio di effettività ha innescato l'innovazione nelle norme sostanziali riguardanti la definizione di trattamento dei dati, nonché il concetto di “stabilimento”, consentendo all'autorità di vigilanza nazionale di esercitare le sue competenze in materia transfrontaliera casi e imponendo l'obbligo di cooperare con le autorità di vigilanza estere.

Occorre anche ricordare che un ruolo importante hanno svolto e continuano a svolgere le disposizioni della Convenzione europea dei diritti dell'Uomo (CEDU) così come interpretate dalla Corte di Strasburgo e dalla Corte di giustizia. A tal riguardo, si possono richiamare i diversi effetti delle decisioni della CGUE e della Corte EDU: le prime sono immediatamente vincolanti non solo per il giudice nazionale di rinvio, ma anche per gli altri tribunali degli Stati membri; la decisione della Corte CEDU può esigere un procedimento di attuazione più lungo, e vi è una maggiore discrezionalità degli Stati contraenti riguardo al ruolo della giurisprudenza della CEDU negli ordinamenti nazionali (vi sono paesi in cui la giurisprudenza della Corte EDU è legalmente vincolante, e altri ordinamenti in cui si tratta solo di uno strumento interpretativo). Tuttavia, in entrambi i casi, le corti nazionali devono considerare parte del loro contesto interpretativo di riferimento gli standard forniti dalle Corti europee. Ed è proprio la presenza di fonti europee diverse, nonché la molteplicità dei loro interpreti, che ha generato un interessante dialogo tra le corti con un significativo impatto sulle giurisprudenze nazionali.

A tal riguardo, bisogna sottolineare che l'applicazione della CDF, da parte della CGUE, sta promuovendo cambiamenti sostanziali e procedurali nell'area della protezione dei dati. L'art 47 CDF ha avuto un impatto sul piano del diritto sostanziale come parametro per valutare la validità di norme di diritto europeo che si sono dimostrate inadeguate e sul piano del diritto processuale come base per valutare se le norme relative all'ammissibilità delle prove, che possono influire sull'effettivo accesso alla giustizia. Inoltre, la CGUE ha sviluppato sulla base della Carta una metodologia molto precisa che si basa sul principio di proporzionalità al fine di bilanciare i diritti e gli interessi fondamentali in conflitto.

Il dialogo fra le corti

Il *casebook* esamina l'influenza del diritto europeo su quello nazionale alla luce del dialogo giudiziario tra i tribunali europei ed italiani nell'applicazione della normativa sulla protezione dei dati. Questa metodologia consente di analizzare l'intero ciclo di un caso, partendo dal rinvio pregiudiziale (e potenzialmente dal conflitto con la giurisprudenza nazionale che ha innescato l'emergere della questione giuridica su cui si chiede l'intervento della Corte di Giustizia), alla sentenza della CGUE, alla decisione del giudice remittente (*follow up*), e all'impatto di quest'ultima decisione in uno SM diverso da quello

del rinvio. Questa analisi fornisce un quadro sull'interazione tra i tribunali europei e nazionali, mostrando se e in che modo lo strumento di rinvio pregiudiziale sia utilizzato strategicamente dalle corti; ad esempio, la CGUE può riformulare la questione presentata dal giudice nazionale in modo da affrontare una questione più generale sulla compatibilità delle leggi nazionali con il diritto dell'UE, al fine di svincolarsi dalla specificità del caso nazionale e fornire indicazioni a tutti gli Stati membri. Analogamente, le corti nazionali possono decidere di presentare un rinvio pregiudiziale non solo per risolvere un conflitto di interpretazione della disposizione di diritto europeo, ma possono anche collegarlo all'obiettivo di modificare la giurisprudenza esistente sulla disposizione in questione.

La decisione *follow-up*, quindi, è rilevante in quanto consente di verificare se e in che modo il giudice del rinvio abbia interpretato le linee guida fornite dalla CGUE e, se disponibile, l'impatto della stessa decisione in altre giurisdizioni in cui i giudici hanno svolto il difficile esercizio di interpretazione della decisione, adattandolo al proprio contesto legale.

Il dialogo verticale tra le corti può anche sovrapporsi al dialogo orizzontale tra corti europee e tra corti nazionali. In particolare, questo può emergere quando le corti europee affrontano questioni simili nelle loro decisioni. Si aggiunge dunque un ulteriore livello di analisi, e spesso un ulteriore sforzo interpretativo per le corti nazionali.

Sotto un diverso profilo, la crescente natura transfrontaliera del trattamento dei dati attraverso mezzi tecnologici richiede un elemento aggiuntivo che è solo rapidamente affrontato dall'articolo 81 GDPR, secondo cui, in caso di reclami da parte di titolari dei dati situati in diversi Stati membri contro lo stesso comportamento, vi è la possibilità per il tribunale di sospendere il procedimento. Di fronte a possibili problemi di coordinamento, nonché ad una eventuale decisione di sospendere i procedimenti o di proseguirli, si imporrà lo scambio di informazioni fra le corti dei diversi paesi in merito all'esistenza di tali casi. Un ulteriore tema è quello della possibile incidenza di decisioni straniere sul procedimento in corso in ambito nazionale.

Questioni simili riguardano le autorità amministrative per la protezione dei dati personali. In relazione a tali aspetti, non sono state previste dal Reg. 2016/678 regole specifiche per disciplinare il coordinamento tra le decisioni dell'autorità di protezione dei dati di uno Stato Membro rispetto alle corti di un altro Stato Membro. L'applicabilità dell'art. 81 Reg. 2016/678 a questi casi probabilmente genererà rinvii pregiudiziali verso la CGUE.

Tutela amministrativa e tutela giurisdizionale

Il coordinamento tra tutele amministrative e tutele giurisdizionali ha avuto risposte diverse: in taluni casi è previsto un meccanismo di alternatività (come in Italia, attraverso la previsione dell'art. 152 D.Lgs. 196/2003) in altri casi è possibile una scelta con l'obbligo/facoltà di una delle due autorità di sospendere il proprio procedimento in attesa della decisione dell'altro organo. In altri casi si prevede che autorità amministrative e organi giurisdizionali possano procedere parallelamente in autonomia assumendo il rischio di decisioni contrastanti. In linea generale, si può notare come al momento quasi tutti gli Stati membri prevedono due meccanismi di tutela concorrenti con sovrapposizioni parziali, lasciando spazio a risultati divergenti, ad esempio laddove, di fronte alla medesima condotta le autorità nazionali di vigilanza riconoscano una violazione della legge sulla protezione dei dati, e al tempo stesso l'autorità giudiziaria la neghi.

Tale questione, non perfettamente risolta neppure a livello europeo, ha portato a diversi interventi della

CGUE in merito al rispetto di un'efficace tutela giudiziaria di fronte a una procedura amministrativa obbligatoria. Si è infatti chiarito che il coordinamento delle tutele deve essere affrontato e risolto sulla base dei principi dell'articolo 47 CDF (cfr. CGUE, caso Puskar).

Le questioni ancora aperte sono le seguenti:

- In caso di sequenza obbligatoria tra procedimento amministrativo e giudiziario, tale sequenzialità è compatibile con il diritto a un ricorso effettivo e in particolare con l'accesso al tribunale?
- Nel caso positivo, quali sono i requisiti per il coordinamento tra i procedimenti amministrativi e giudiziari al fine di garantire un'efficace tutela giurisdizionale?
- Quali sono le forme di coordinamento in merito ai rimedi disponibili in ciascun meccanismo di controllo?
- Qual è il livello di coordinamento tra le autorità nazionali di vigilanza in caso di violazione transfrontaliera della legge sulla protezione dei dati?

Le nuove sfide del Regolamento 2016/678

Come accennato, un evidente aspetto innovativo del Regolamento 2016/678 è il potenziamento dei poteri delle Autorità di protezione dei dati.

Nella direttiva 95/46, le decisioni circa i poteri delle autorità nazionali di vigilanza e le misure sanzionatorie sono state lasciate quasi completamente agli Stati membri sia in termini di organizzazione istituzionale che di regolamentazione delle procedure. Da un lato, l'articolo 28 Dir. 95/46 aveva fornito solo uno standard minimo per quanto riguarda i poteri assegnati all'autorità di vigilanza nazionale (necessaria); dall'altro, l'art. 22 dir. 95/46 aveva lasciato agli Stati Membri la scelta di introdurre diversi tipi di sanzioni (amministrative o risarcitorie) in caso di violazioni della normativa sulla protezione dei dati.

L'approccio del Reg. 2016/678 è radicalmente diverso: rispetto alla direttiva previgente, il Regolamento alloca poteri sanzionatori più ampi sulle autorità di vigilanza nazionali e fornisce una definizione più dettagliata delle sanzioni (amministrative) in caso di violazioni della protezione dei dati.

In particolare, l'art. 58 Reg. 2016/678 richiede che le autorità nazionali di vigilanza debbano disporre di una serie di poteri investigativi, correttivi, consultivi e di autorizzazione, e tra questi in particolare la possibilità *“di imporre una sanzione amministrativa ai sensi dell'art. 83, in aggiunta o in sostituzione delle misure di cui al presente paragrafo, a seconda delle circostanze dei casi”*. Nell'art. 83 Reg. 2016/678, quindi, le sanzioni amministrative sono ampiamente definite, anche rispetto ad un'ampia serie di criteri in grado di indirizzare la decisione in base ad un test di proporzionalità (ad esempio: comportamento attuale (e precedente) di chi commette la violazione, livello di collaborazione con la nazionale autorità di controllo). Inoltre, al fine di assicurare coerenza e coordinamento tra gli Stati membri, l'art. 70 Reg. 2016/678 comprende tra i compiti del Comitato europeo per la protezione dei dati (ex Gruppo di lavoro art. 29) la possibilità di elaborare linee guida relative alle sanzioni amministrative definite nell'art. 83 Reg. 2016/678. Da un lato, il Regolamento mira a fornire una soluzione rispetto alla mancanza di rimedi efficaci nella protezione dei dati; dall'altra, segue le prassi della Commissione in relazione alle sanzioni definite diritto della concorrenza di cui all'articolo 23 capoverso 2 lettera lit. a) Reg. n. 1/2003 del Consiglio, che rafforza il coordinamento e l'armonizzazione delle sanzioni negli Stati

membri.

La modifica della struttura istituzionale secondo le linee definite dal Regolamento 2016/678 richiederà diversi passaggi all'interno di ciascun ordinamento nazionale, imponendo una riformulazione, anche a livello istituzionale, fra *enforcement* amministrativo e giudiziario.

Un altro aspetto innovativo è la possibilità di ricorso collettivo in caso di violazione della normativa sulla protezione dei dati. Il Reg. 2016/678 prevede diversi meccanismi di *enforcement* sia attraverso procedimenti amministrativi e giudiziari.

Ai sensi dell'articolo 77 Reg. 2016/678, l'interessato può presentare reclamo per la violazione della protezione dei dati dinanzi all'autorità di vigilanza in cui ha la propria residenza, il luogo di lavoro o il luogo della presunta violazione. In caso di violazione, l'autorità di vigilanza può imporre diverse misure correttive al responsabile del trattamento dei dati (cfr. Articolo 58 Reg. 2016/678) e, come detto sopra, può anche imporre sanzioni amministrative a norma dell'articolo 83 Reg. 2016/678. L'ammontare specifico della sanzione sarà determinato dalle autorità di vigilanza caso per caso e seguirà i principi di efficacia, proporzionalità e dissuasività in ogni singolo caso.

Ai sensi dell'art. 78 Reg. 2016/678, l'interessato (e anche il responsabile del trattamento dei dati) può ricorrere contro una decisione dell'autorità di vigilanza dinanzi al tribunale presso il quale è stabilita tale autorità. Il diritto a un ricorso effettivo si estende anche al caso in cui l'autorità di vigilanza non gestisce un reclamo o non informa l'interessato entro 3 mesi sullo stato di avanzamento o sull'esito del reclamo. In questo caso, il tribunale eserciterà piena giurisdizione, che dovrebbe includere la sua competenza per esaminare tutte le questioni di fatto e di diritto rilevanti per la controversia.

Infine, ai sensi dell'art 79 Reg. 2016/678, l'interessato può chiedere di accertare la violazione delle disposizioni sulla protezione dei dati anche dinanzi al tribunale in cui il responsabile del trattamento o l'incaricato del trattamento ha uno stabilimento o, in alternativa, dove l'interessato ha la propria residenza abituale.

Va notato che, ai sensi dell'articolo 80 Reg. 2016/678, l'interessato può esercitare i propri diritti anche attraverso il mandato ad un organismo, un'organizzazione o un'associazione non a scopo di lucro che selezionerà il meccanismo giudiziario o di esecuzione amministrativa o entrambi. Sebbene questa disposizione non preveda esplicitamente un ricorso collettivo, può promuovere un maggiore coinvolgimento di organizzazioni o associazioni per raccogliere e coordinare le richieste degli interessati. Di conseguenza, si potrebbe ottenere un ampliamento della tutela degli interessati, in quanto gli incentivi a far rispettare i diritti individuali potrebbero essere più elevati attraverso l'intermediazione di organizzazioni che porta con sé costi inferiori per le controversie. Data la mancanza di indicazioni dettagliate nel Regolamento 2016/678, gli Stati membri avranno discrezionalità riguardo alla possibilità di consentire reclami coordinati dinanzi alle autorità di vigilanza e ai tribunali. Nel nostro sistema sono applicabili alternativamente. Occorrerà, tuttavia, valutare la compatibilità dell'articolo 152 d.lgs. 196/2003 con l'articolo 47 CDF e con il regolamento.

Le questioni che emergono in tal caso sono le seguenti:

- Esiste la possibilità di aggregare le azioni da parte di diversi titolari dei dati provenienti da diversi paesi sulla base della stessa condotta (cioè contro lo stesso convenuto)? o sussiste una differenza nel caso in cui gli interessati siano residenti in un unico SM?

- Esiste la possibilità di aggregare le azioni da parte di un singolo interessato che ha sofferto della violazione in diversi paesi sulla base della stessa condotta (cioè contro lo stesso convenuto)?
- Quali sono i rimedi giudiziari disponibili in caso di in caso di azioni transfrontaliere aggregate?
- Esiste una differenza tra le norme relative alla liquidazione dei danni dinanzi all'autorità nazionale di vigilanza e dinanzi alle corti in caso di azioni aggregate?
- Esiste una differenza tra i rimedi definiti dalle autorità nazionali di vigilanza e quelli forniti dalle corti nazionali in caso di cause transfrontaliere aggregate?

1 BILANCIAMENTO TRA DIRITTI FONDAMENTALI

1.1 Premessa

Verranno esaminate due ipotesi ricorrenti. La prima in cui una pluralità di diritti di cui è titolare lo stesso soggetto siano stati contestualmente violati. Le tutele possono essere diverse ed il loro contemperamento effettuato alla luce del principio di effettività e del diritto ad una tutela giurisdizionale effettiva (art. 47 CDF). La seconda in cui vi possa essere un conflitto fra diritti legati alla protezione dei dati e libertà come quella di manifestazione del pensiero, di espressione, o di stampa, di cui diversi soggetti sono titolari.

In sintesi, ci si soffermerà sui seguenti aspetti:

- Il diritto alla protezione dei dati personali come diritto non assoluto;
- Violazione di più diritti fondamentali e bilanciamento;
- Bilanciamento tra diritti e rimedi esperibili.

Come previsto dall'art. 1 del Regolamento 2016/678, il GDPR *“stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali”*.

L'art. 1 del c.d. Codice Privacy (come modificato dal D.lgs. 101/2018) all'art. 1 significativamente prevede che *“Il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito «Regolamento», e del presente codice, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona”*.

In ragione della peculiare natura del diritto alla protezione dei dati personali e delle caratteristiche dei diritti potenzialmente con esso confliggenti, accade sovente che, in conseguenza di un trattamento dei dati, si verifichi sia una lesione del diritto alla protezione dei detti dati che una lesione del diritto all'onore, alla reputazione o all'immagine.

L'esatta individuazione dell'oggetto della domanda – in fase amministrativa prima e giurisdizionale poi – appare imprescindibile al fine di individuare le autorità competenti, i poteri esercitabili dalle dette autorità, il tipo di procedimento da intraprendere ed i rimedi invocabili dall'interessato e concedibili dalle autorità.

In tal senso, appare molto significativo quanto affermato dalle Sezioni Unite della Corte di Cassazione, nella **pronuncia n. 23469/2016**. Nella sentenza, le Sezioni Unite – chiamate a valutare l'ammissibilità

di un ordine di cancellazione e/o oscuramento di una singola o di più pagine di stampa di testate telematiche, attraverso il ricorso all'inibitoria *ex art. 700 c.p.c.* al fine di elidere l'aggravamento del danno patrimoniale e non patrimoniale derivante all'onore ed alla reputazione dalla pubblicazione *on line* di articoli diffamatori – hanno chiarito che quando si invoca una tutela civilistica cautelare preventiva contro i giornali telematici con cui sia commessa una lesione all'onore o alla reputazione e non si prospetta, invece, una lesione del diritto alla protezione dei dati personali, vi è una forte compressione dei rimedi esperibili. In particolare, le Sezioni Unite hanno precisato che:

- *“il solo diritto alla reputazione e all'onore (cioè, a prescindere da altri diritti di pari od eventualmente poziore rango, tutelati da altre discipline, la cui applicazione - è bene ribadirlo - è lasciata impregiudicata), benché certamente anch'esso fondamentale in quanto inerente in modo diretto alla personalità od alla dignità dell'individuo, **deve intendersi recessivo dinanzi alla tutela della libertà di stampa**, sia pure nella fase a cognizione sommaria di un giudizio civile quale quella cautelare finalizzata all'adozione di misure urgenti (v. Corte Cost. 122/70, cit.), di qualunque contenuto, ripristinatorio o inibitorio o analogo”;*
- sono precluse, e quindi non ammissibili quale oggetto di qualsiasi provvedimento cautelare o equiparato del giudice civile, tutte le misure, comunque denominate, che tendano ad impedire la persistenza nella rete o l'ulteriore circolazione o diffusione dell'articolo - o equipollente - di giornale telematico ritenuto diffamatorio; misure tra cui devono comprendersi anche quelle indicate come deindicizzazione o ad esse analoghe o di contenuto o soprattutto effetto corrispondente;
- *“la tutela piena, con il risarcimento in forma specifica o per equivalente e soprattutto con strumenti che spetterà al giudice che avrà conosciuto in modo non sommario della vicenda e dei suoi effetti individuare anche in ordine alle conseguenze della particolare diffusività degli strumenti adoperati, andrà riservata al momento, necessariamente successivo, del riconoscimento - con pronuncia almeno esecutiva, se non definitiva ed irretrattabile - dell'effettiva violazione del diritto individuale all'onore od alla reputazione, il quale solo potrà eventualmente ribaltare la valutazione di prevalenza tra i due diritti fondamentali”.*

Alla luce delle considerazioni che precedono, si deve precisare che l'esame delle questioni relative ai poteri ed ai rimedi delle autorità, amministrative e giurisdizionali, verrà compiuto con riferimento alle fattispecie di lesione del diritto alla protezione dei dati personali (nonché ai casi di interazione tra un tale diritto ed altri diritti, caratterizzata dal fatto che la lesione di diversi diritti costituzionali è allegata come conseguenza della violazione del diritto alla protezione dei dati personali).

1.2 Il contesto europeo e quello italiano. L'individuazione dei beni protetti: il diritto alla manifestazione del pensiero, il diritto ad informare ed il diritto ad essere informati, il diritto alla tutela della riservatezza.

Così come il diritto alla protezione dei dati personali anche la libertà di espressione è un diritto fondamentale riconosciuto uniformemente da tutte le fonti europee ed internazionali. La sua importanza e il suo ruolo sono riconosciuti come fondamento della democrazia, e come base per garantire la protezione di altri diritti fondamentali.

Sia la CEDU che la Carta dei diritti fondamentali UE includono la libertà di espressione, e la giurisprudenza delle rispettive corti ha progressivamente delineato i contenuti e i confini che caratterizzano tale diritto fondamentale. Poiché si tratta di un diritto espressamente riconosciuto come

non assoluto, la libertà di espressione può subire compressioni sia in caso di limiti derivanti dalla legislazione nazionale, sia in caso di bilanciamento fra diritti fondamentali confliggenti.

Secondo la giurisprudenza della Corte di Strasburgo, le limitazioni alla libertà di espressione devono

- essere previste per legge;
- perseguire un obiettivo legittimo previsto dall'art 10 CEDU;
- essere necessarie per garantire la democrazia.

Laddove tali condizioni siano soddisfatte, la limitazione deve sottostare ad un test di proporzionalità che verifichi se la normativa adottata è appropriata rispetto all'obiettivo perseguito, e non vi siano misure alternative che permettano di raggiungere tale obiettivo senza imporre tale limitazione.

È importante notare che nel quadro della giurisprudenza della Corte CEDU i casi relativi a *Von Hannover n. 1 e n. 2* e *Axel Springer* hanno permesso di verificare come conciliare due diritti conflittuali, vale a dire la libertà di espressione e il diritto alla vita privata, e sono di rilievo anche per le diverse modalità di applicazione del principio di proporzionalità. La Corte CEDU in tali casi ha dato priorità al diritto alla vita privata (in questo caso di personalità pubbliche). Esaminando tale giurisprudenza emerge peraltro il potenziale del dialogo giudiziale fra corti nazionali ed europee: la Corte di Strasburgo ha aggiunto nuovi elementi (i cosiddetti criteri) al suo test, anche per superare le ambiguità delle sue precedenti decisioni e alla luce della reazione nazionale. Questi casi evidenziano che non è sempre facile garantire una giurisprudenza coerente sull'interpretazione e l'applicazione dei criteri della Corte CEDU in materia di equilibrio tra libertà di espressione e diritto alla privacy. Gli elementi decisivi del test della Corte CEDU in questi casi sono il contributo dato dalla pubblicazione contestata ad un dibattito di interesse generale e l'applicazione dei criteri del test di valutazione da parte dei giudici nazionali.

A livello nazionale, la libertà di pensiero, di espressione (e il diritto all'informazione) e di stampa - significativamente accostate - è stata proclamata solennemente dalla Costituzione della Repubblica al suo art. 21, il quale recita: "*Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. La stampa non può essere soggetta ad autorizzazioni o censure....*".

La Corte Costituzionale, sin da risalenti pronunce ha asserito che tale libertà «è tra le libertà fondamentali proclamate e protette dalla nostra Costituzione, una di quelle [...] che meglio caratterizzano il regime vigente nello Stato, condizione com'è del modo di essere e dello sviluppo della vita del Paese in ogni suo aspetto culturale, politico, sociale» (sentenza n. 9 del 1965), sottolineando che il diritto previsto dall'art. 21 Cost. è «il più alto, forse,» dei «diritti primari e fondamentali» sanciti dalla Costituzione (sentenza n. 168 del 1971). La libertà di manifestazione del pensiero rientra quindi, secondo la Corte, tra i «diritti inviolabili dell'uomo» di cui all'art. 2 Cost. (sentenza n. 126 del 1985), con la conseguenza, da un lato, che la Repubblica ha il dovere di garantirla anche nei confronti dei privati (nel senso che «non è lecito dubitare che la libertà [in parola] debba imporsi al rispetto di tutti, delle pubbliche autorità come dei consociati, e che nessuno possa arrecarvi attentato», sentenza n. 122 del 1970) e, dall'altro, della non sopprimibilità della stessa (anche se non, sembra doversi ritenere, dell'immodificabilità della formulazione attuale dell'art. 21 Cost.). Ancora, il giudice delle leggi ha accentuato il rapporto tra libertà di manifestazione del pensiero e regime democratico, affermando che la prima è «pietra angolare dell'ordine democratico» (sentenza n. 84 del 1969), «cardine di democrazia nell'ordinamento generale» (sentenza n. 126 del 1985). In senso analogo, anche le sentenze: n. 11 del

1968, che definisce il diritto di cui all'art. 21 Cost. «*coessenziale al regime di libertà garantito dalla Costituzione*»; n. 98 del 1968, secondo cui la «*libertà di manifestazione del pensiero [...] è ordine dell'ordinamento democratico*»; n. 126 del 1985, ove si ribadisce «*la rilevanza centrale [...] che la libertà di manifestazione del pensiero, anche e soprattutto in forma collettiva, assume ai fini dell'attuazione del principio democratico*».

I diritti riconosciuti dall'art. 21 Cost. possono venire in conflitto con altri diritti della persona, costituzionalmente garantiti. Così come previsto anche dalla giurisprudenza CEDU, in ipotesi di conflitto è necessario operare un bilanciamento, tenendo presente che, secondo la giurisprudenza di legittimità, il diritto ex art. 21 Cost. tendenzialmente prevale rispetto ai diritti personali alla reputazione ed alla riservatezza, nel senso che questi ultimi, solo ove sussistano determinati presupposti, ne configurano un limite. La Corte di Cassazione ha chiarito che tale prevalenza si evince dal dettato dell'art. 1, comma 2 della Cost. (che evidenzia la funzionale correlazione della informazione con l'esercizio della sovranità popolare, che solo in presenza di una opinione pubblica compiutamente informata può correttamente dispiegarsi) e dalle disposizioni della legislazione ordinaria (artt. 25 legge n. 675 del 1996, 20 d.lgs. n. 467 del 2001, 12 d.lgs. n. 196 del 2003) che, appunto, riconducono reputazione e "privacy" nell'alveo delle "eccezioni rispetto al generale principio di tutela della informazione (cfr. Cass. n. 16236/2010).

La Corte di Cassazione, nella pronuncia appena citata, ha evidenziato che sia la stampa che la privacy sono entrambi beni costituzionali, ma la tutela della stampa prevale sulla tutela della riservatezza. La tutela della privacy, infatti, vale come «*eccezione*» rispetto «*al diritto insopprimibile e fondamentale della libertà di informazione e di critica*», diritto che garantisce l'esplicazione della «*sovranità popolare*». La Corte espressamente afferma che: «*l'attività di informazione è chiaramente prevalente rispetto ai diritti personali della reputazione e della riservatezza, nel senso che questi ultimi, solo ove sussistano determinati presupposti, ne configurano un limite*».

Nell'individuazione del bene protetto, occorre tenere presente che, molto spesso, il diritto all'identità personale e il diritto alla privacy sono strettamente connessi con il diritto all'onore e alla reputazione.

Il bilanciamento svolto fra i diritti confliggenti ha poi effetto anche sulla scelta dei rimedi applicabili, poiché il giudice si troverà vincolato in primo luogo ad una scelta derivante dall'individuazione del bene protetto (cfr. Cass. S.U. 23469/2016), in secondo luogo dovrà individuare quale fra i rimedi disponibili può rispondere in modo efficace e proporzionale alla violazione sofferta e allo stesso tempo evitare ulteriori compressioni rispetto al diritto fondamentale soccombente nel bilanciamento.

Questo aspetto appare evidente anche nel caso della tutela del diritto all'oblio, in cui si presenta un conflitto fra diritto alla protezione dei dati e libertà di espressione.

1.3 La questione

In caso di bilanciamento di diritti fondamentali contrapposti, in che modo la selezione dei rimedi può conformarsi al principio di effettività della tutela e all'art. 47 CDF?

Al fine di garantire un rimedio efficace agli interessati, il diritto dell'Unione europea deve essere interpretato nel senso che implicitamente include il diritto di essere cancellati dall'elenco dei risultati visualizzati dai motori di ricerca, che gli interessati possono opporsi ai responsabili del trattamento per obbligarli a rimuovere dall'elenco dei risultati visualizzati dai motori di ricerca i link a pagine web

pubblicate da terzi, anche qualora i dati disponibili - la cui pubblicazione era lecita - non siano stati cancellati in precedenza o contemporaneamente da tali pagine web?

1.4 Il caso: Tribunale di Roma, 3 dicembre 2015, n. 23771

Il Tribunale di Roma, dovendosi pronunciare sui *links* rinvenibili sul motore di ricerca Google contenenti il riferimento a notizie di cronaca circa una vicenda giudiziaria in cui l'attore era rimasto coinvolto nel 2012-2013 unitamente ad altri personaggi romani, alcuni esponenti del clero ed altri riconducibili alla criminalità della cd. banda della Magliana, relativamente a presunte truffe e guadagni illeciti realizzati dal sodalizio criminoso, ha innanzitutto inquadrato la vicenda in esame nel trattamento dei dati personali e nel cd. diritto all'oblio, il quale, *“ove ritenuto sussistente, impedisce il protrarsi del trattamento stesso (e quindi l'indicizzazione, con la conseguente fondatezza della domanda di deindicizzazione nei confronti del gestore del motore di ricerca), per come risultante anche dalla recente pronuncia in materia resa dalla Corte di Giustizia Europea (Grande Sezione del 13.5.2014 nella causa C-131/12, sentenza Costeja), oltre che dalle, conformi, successive decisioni del Garante per la protezione dei dati personali”*.

Secondo la citata pronuncia, in sintesi, gli utenti - in caso di ricerca nominativa su Google - non possono ottenere dal gestore del motore di ricerca la cancellazione dai risultati di una notizia che li riguarda se si tratta di un fatto recente e di rilevante interesse pubblico: il diritto all'oblio, infatti, deve essere bilanciato, ad avviso della corte, con il diritto di cronaca e con l'interesse pubblico alla conoscenza dei fatti acquisibili per il tramite dei *links* forniti dal motore di ricerca.

Ad avviso della Corte *“occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta. Se indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica”*.

In altri termini, *“dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi”*.

Ed ancora *“i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale*

persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi".

E' dunque necessario, spiega la Corte, *"verificare in particolare se l'interessato abbia diritto a che l'informazione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome"*.

Il Tribunale, a tale ultimo proposito, ricorda che il 26 novembre 2014 l'Article 29 Data Protection Working Party (organo consultivo indipendente istituito in conformità all'articolo 29 della Direttiva 95/46/CE sulla protezione dei dati personali) ha pubblicato delle linee guida per l'implementazione della menzionata pronuncia della Corte di Giustizia (causa C-131/12), le quali per quel che qui specificamente interessa contengono una serie di criteri per orientare l'attività delle autorità nazionali nella gestione dei reclami degli interessati a seguito del mancato accoglimento, da parte del motore di ricerca, delle richieste di deindicizzazione, chiarendo che nessun criterio è di per sé determinante. Tra di essi, figura in primo luogo quello della natura del richiedente (in particolare, la circostanza per cui il richiedente rivesta un ruolo di rilievo pubblico, come nel caso di personaggi politici, dovrebbe tendenzialmente orientare verso il diniego della richiesta di deindicizzazione).

Il Tribunale osserva poi che *"il trascorrere del tempo, ai fini della configurazione del diritto all'oblio, si configura quale elemento costitutivo, come risultante anche dalla condivisibile sentenza n. 5525/2012 della Suprema Corte, nella quale questo viene configurato quale diritto "a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino oramai dimenticate o ignote alla generalità dei consociati"*, presupposto nella specie assolutamente insussistente, risalendo i fatti al non lontano 2013 (o al più al luglio 2012, secondo due dei risultati della ricerca) ed essendo pertanto gli stessi ancora attuali.

Del resto, la medesima appare di sicuro interesse pubblico, riguardando un'importante indagine giudiziaria che ha visto coinvolte numerose persone, seppure in ambito locale-romano, verosimilmente non ancora conclusa, stante la mancata produzione da parte dell'istante di documentazione in tal senso (archiviazioni, sentenze favorevoli...).

I dati personali riportati risultano quindi trattati nel pieno rispetto del principio di essenzialità dell'informazione.

Né può in questa sede il ricorrente dolersi della falsità delle notizie riportate dai siti visualizzabili per effetto della ricerca a suo nome, non essendo configurabile alcuna responsabilità al riguardo da parte del gestore del motore di ricerca (nella specie Google), il quale opera unicamente quale "caching provider" ex art. 15 d.lgs. n. 70/2003: in tale prospettiva pertanto il medesimo avrebbe dovuto agire a tutela della propria reputazione e riservatezza direttamente nei confronti dei gestori dei siti terzi sui quali è avvenuta la pubblicazione del singolo articolo di cronaca, qualora la predetta notizia non sia stata riportata fedelmente, ovvero non sia stata rettificata, integrata od aggiornata coi successivi risvolti dell'indagine, magari favorevoli all'odierno istante (il quale peraltro deduce di non aver riportato condanne e produce certificato negativo del casellario giudiziale).

Ancora, il Tribunale evidenzia come l'odierno ricorrente sia avvocato, circostanza che consente di ritenere che questo eserciti un "ruolo pubblico" proprio per effetto della professione svolta e dell'albo professionale cui è iscritto, laddove tale ruolo pubblico non è attribuibile al solo politico (cfr. linee guida del 26.11.20014) ma anche agli alti funzionari pubblici ed agli uomini d'affari (oltre che agli iscritti in

albi professionali).

1.5 La giurisprudenza italiana. Un focus su una decisione di merito

La giurisprudenza italiana ha affrontato diversi aspetti relativi al contemperamento fra la libertà di espressione e tutela dei dati personali, riconoscendo fra i criteri per valutare la conformità del trattamento dei dati personali in caso di svolgimento dell'attività giornalistica, sia l'essenzialità dell'informazione, sia il ruolo pubblico svolto da parte del titolare dei dati, l'attualità della notizia in relazione al trascorrere del tempo. In quest'ultimo caso appare rilevante la decisione del Tribunale di Mantova, 28 Ottobre 2016 circa l'applicazione del principio di proporzionalità in relazione al canone della necessità, valutata in relazione al periodo di tempo in cui il dato è diffuso.

Il Tribunale di Mantova, chiamato a pronunciarsi sul caso di un articolo pubblicato dal Gazzettino di Mantova, sia nell'edizione cartacea che sul sito web on-line, (tuttora diffuso in rete) dal titolo "Magnacavallo: Truffa Smascherata — Diagnosi falsa per piazzare l'apparecchio — Pensionata raggirata, denunciati un medico e due tecnici dell'udito", asseritamente lesivo, oltre che della reputazione degli attori, anche del loro diritto all'oblio, con riferimento a quest'ultimo profilo ha preliminarmente rilevato che ogni libertà civile trova il proprio limite in quella altrui e nell'interesse pubblico idoneo a fondare l'eventuale sacrificio dell'interesse del singolo, per cui la tutela del diritto alla reputazione (nel caso di specie commerciale) va contemperata con il diritto di e alla informazione, nonché con il diritto di cronaca, e che il soggetto interessato ha diritto a che l'informazione che lo riguarda e oggetto di trattamento risponda ai criteri di proporzionalità, necessità, pertinenza allo scopo, esattezza e coerenza con la sua attuale ed effettiva identità (c.d. principi di proporzionalità, pertinenza e non eccedenza) e ciò sia alla stregua dei principi desumibili dalla legislazione vigente che in virtù del principio di correttezza (quale estrinsecazione di quello generale di solidarietà sociale desumibile dall'art. 2 Cost.). Con riguardo alla legislazione vigente, si può far riferimento agli artt. 11 e 7 del d.lgs. 196/2003 precisandosi che soggetto interessato al trattamento dei dati deve ritenersi anche la persona giuridica o l'ente collettivo (cfr. Cass. 1-8-2013 n. 18443; Cass. 8-7-2005 n. 14390), e al diritto all'oblio, che in presenza di specifiche condizioni, trova ora positivo riconoscimento, anche in relazione ai soggetti collettivi, nell'art. 17 del regolamento europeo sulla protezione dei dati personali n. 2016/679.

Il tribunale ritiene dunque che *“occorre pertanto procedere a un bilanciamento fra i contrapposti interessi consistenti da un lato nel diritto all'informazione (v. art. 21 Cost.) e dall'altro in quello all'oblio in capo a colui al quale i dati (che possono essere anche quelli pubblicati: cfr. Cass. 8-7-2005 n. 14390; Cass. 25-6-2004 n. 11864) si riferiscono affinché non vengano ulteriormente divulgate informazioni (potenzialmente) lesive in quanto divenute prive di interesse rispetto alla collettività, sia pure locale, stante il lasso di tempo intercorso dall'accadimento del fatto che ne costituisce l'oggetto sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione della propria attività”*. Sul diritto all'oblio e sul suo fondamento si possono richiamare le seguenti pronunce: Corte di Giustizia Europea del 13-5-2014 nella causa C-131-12; Cass. 24-6-2016 n. 13161; Cass. 26-6-2013 n. 16111; Cass. 5-4-2012 n. 5525; Cass. 9-4-1998, n. 3679).

Il trattamento dei dati non può avvenire per un periodo superiore a quello necessario agli scopi per i quali essi sono stati raccolti e trattati; in proposito occorre notare che la rete internet costituisce una realtà ove le informazioni non sono archiviate (e cioè organizzate e strutturate) ma solo memorizzate senza limiti e senza tempo, poste tutte al medesimo livello, senza una valutazione del relativo peso, prive di contestualizzazione e di collegamento con altre informazioni pubblicate: di qui appunto il diritto

del soggetto cui le informazioni si riferiscono (che può anche essere una persona giuridica o un ente collettivo) ad ottenere la cancellazione delle informazioni che, pur se lecitamente diffuse, risultano inutilmente lesive in ragione della loro perdita di attualità.

Il tribunale ritiene dunque, in considerazione del fatto che la vicenda risale al 2011 e che è mancato un accertamento in sede giudiziaria delle circostanze narrate nell'articolo pubblicato, ritiene fondata la pretesa della società attorea di ottenere la cancellazione dal sito web del giornale "Gazzetta di Mantova" dell'articolo pubblicato il 27-2-2011 con il titolo "Diagnosi falsa per piazzare l'apparecchio".

1.6 La giurisprudenza europea

Così come citato nel caso principale del Tribunale di Roma, il punto di riferimento nella giurisprudenza europea è il caso *Google Spain* in cui la CGUE ha affrontato la questione posta dalla *Audiencia nacional* nel caso del conflitto tra un cittadino spagnolo e il noto motore di ricerca Google. Il caso concerneva un ricorso contro la decisione dell'autorità nazionale per la protezione dei dati secondo la quale veniva ordinato al gestore del motore di ricerca di eliminare dall'elenco dei risultati i link a pagine web pubblicate da terzi e contenenti informazioni che riguardano il cittadino spagnolo che venivano visualizzati sul motore di ricerca a seguito di una ricerca effettuata in base al nome del cittadino stesso.

Google, che il giudice riconosce come responsabile del trattamento ha sostenuto che, in virtù del principio di proporzionalità, tale richiesta di rimozione delle informazioni non doveva essere rivolta al gestore del motore di ricerca, ma all'editore del sito web in cui erano disponibili le informazioni visualizzate dal motore di ricerca.

L'Audencia National aveva presentato, fra le altre, le seguenti questioni pregiudiziali:

“(2) (c): *Se la [AEPD], che tutela i diritti sanciti dall'art. 12, lett. b) e dall'art. 14, primo comma, lett. a), della direttiva 95/46, possa imporre direttamente a [Google Search] l'obbligo di ritirare dai suoi indici un'informazione pubblicata dalla [Google Search]. a terzi, senza rivolgersi preventivamente o contemporaneamente al titolare della pagina web su cui si trovano tali informazioni?*

(d): 2. In caso di risposta affermativa alla precedente questione, se, in caso di risposta affermativa, il titolare del sito web su cui si trova l'informazione. l'obbligo dei motori di ricerca di proteggere tali diritti è escluso quando le informazioni che contiene i dati personali che sono stati legalmente pubblicati da terzi e che sono conservati sul sito web dell'azienda. pagina web da cui proviene?

(3) Per quanto riguarda la portata del diritto di cancellazione e/o del diritto di opposizione, in relazione all'applicazione del diritto di cancellazione e/o del diritto di opposizione, in relazione alla "derecho al olvido" (il "diritto all'oblio"), si deve considerare che i diritti di la cancellazione e il blocco dei dati di cui all'articolo 12, lettera b), e il diritto di opposizione, a condizione che poiché, ai sensi dell'articolo 14, primo comma, lettera a), della direttiva 95/46, si estende a consentire all'interessato di indirizzarsi ai motori di ricerca per evitare l'indicizzazione delle informazioni che lo riguardano personalmente, pubblicate su pagine web di terzi, invocando il suo desiderio che tali informazioni non siano note agli utenti di Internet quando egli stesso ritiene che ciò possa essere pregiudizievole per lui o che egli desideri che sia consegnato all'oblio, anche se le informazioni in questione sono state legalmente pubblicate da terzi”.

La Corte risponde separatamente alla questione n. 2, lett. c) e d), e alla questione n. 3. Per quanto riguarda la questione della portata della responsabilità dell'operatore di un motore di ricerca, la Corte

ricorda anzitutto quali sono gli obblighi dei responsabili del trattamento e dei responsabili del trattamento dei dati personali, e i diritti delle persone interessate ai sensi della legislazione dell'UE. In particolare, viene considerato il diritto degli interessati di ottenere dal responsabile del trattamento la rettifica, la cancellazione o il blocco di trattamenti di dati che non sono conformi alla normativa UE, “*in particolare*” perché incomplete o imprecise. L'uso dell'espressione “*in particolare*” implica, per il giudice, che l'elenco non è esaustivo; dunque, nel caso di non conformità del trattamento si configura il diritto dell'interessato di ottenere la cancellazione dei dati.

Valutando il ruolo dei motori di ricerca, la Corte osserva che il trattamento dei dati attraverso i motori di ricerca crea un impatto aggiuntivo (rispetto alla pubblicazione originale dei dati) sui diritti delle persone interessate di la vita privata e la protezione dei dati:

“il trattamento dei dati [.....] effettuato dal gestore di un motore di ricerca può pregiudicare in modo significativo i diritti fondamentali alla privacy e alla protezione dei dati personali quando la ricerca mediante tale motore è effettuata sulla base del nome di una persona, poiché tale trattamento consente a qualsiasi utente di Internet di ottenere attraverso l'elenco dei risultati una panoramica strutturata delle informazioni relative a tale persona che si possono trovare su Internet - informazioni che potenzialmente riguardano un gran numero di aspetti della sua vita privata e che, senza il motore di ricerca, non avrebbero potuto essere interconnesse o avrebbero potuto esserlo solo con grandi difficoltà - e quindi di stabilire un profilo più o meno dettagliato di lui. Inoltre, l'effetto dell'interferenza con tali diritti dell'interessato è accentuato dall'importante ruolo svolto da Internet e dai motori di ricerca nella società moderna, che rendono ubiquitarie le informazioni contenute in un siffatto elenco di risultati” (§ 80).

La Corte conclude pertanto che le autorità di vigilanza o giudiziarie possono ordinare al gestore del motore di ricerca di eliminare dall'elenco dei risultati visualizzati a seguito di una ricerca effettuata sulla base dei link nominativi di una persona a pagine web pubblicate da terzi contenenti informazioni relative a tale persona, senza che un'ordinanza in tal senso presupponga la precedente o simultanea rimozione di tale nome e informazioni - di propria iniziativa dell'editore o su ordine di una di tali autorità - dalla pagina web in cui sono state pubblicate. Per la Corte, tale diritto di essere cancellato dall'elenco si fonda sul principio di effettività, in quanto “la facilità con cui le informazioni pubblicate su un sito web possono essere replicate su altri siti e il fatto che i responsabili della loro pubblicazione non sono sempre soggetti alla legislazione dell'Unione europea, una protezione efficace e completa degli utenti dei dati non potrebbe essere realizzata se questi ultimi dovessero ottenere prima o parallelamente la cancellazione delle informazioni che li riguardano dagli editori di siti web”.

Per quanto riguarda la terza questione, la Corte analizza in modo più approfondito la “*portata dei diritti dell'interessato*” e osserva che il diritto dell'interessato di opporsi al trattamento dei dati che lo riguardano si applica non solo ai dati inesatti, ma anche a quelli che sono inadeguati, irrilevanti o eccessivi rispetto alle finalità del trattamento. In particolare, la Corte ritiene che si debba tener conto del corso del tempo: anche un trattamento legittimo, in un primo tempo, di dati esatti può diventare incompatibile con la tutela prevista dalla normativa dell'Unione, qualora tali dati non siano più necessari per le finalità per le quali sono raccolti. La Corte chiede pertanto che le autorità nazionali garantiscano un equilibrio degli interessi tenendo conto della durata della disponibilità dei dati. Nella fattispecie, la Corte conclude che la sensibilità dei dati e il fatto che la pubblicazione sia avvenuta 16 anni prima, implica che l'interessato ha il diritto che le informazioni che lo riguardano non siano più collegate al suo nome nell'elenco dei risultati visualizzati dal motore di ricerca.

In determinate circostanze, e in particolare a seguito di un bilanciamento di interessi, l'interessato ha il diritto di essere cancellato dall'elenco dei risultati visualizzati da un motore di ricerca. In particolare, tale diritto può essere opposto al motore di ricerca anche nel caso in cui il nome o le informazioni non siano state cancellate in anticipo o contemporaneamente dalle pagine web a cui l'elenco si collega, e anche quando la pubblicazione su tali pagine sia legittima. L'interessato può chiedere di essere cancellato dall'elenco senza dover dimostrare che l'inserimento delle informazioni nell'elenco dei risultati gli arreca un pregiudizio, ma per l'unica ragione che, dato il tempo trascorso dalla pubblicazione, le informazioni che lo riguardano non dovrebbero più essere fornite, in considerazione del tempo trascorso dalla pubblicazione, a meno che, dato il ruolo svolto dall'interessato in materia di vita pubblica, tale interferenza con i diritti fondamentali possa essere giustificata dall'interesse preponderante di offrire al pubblico l'accesso alle informazioni in questione.

Il caso di *Google Spain*, nella misura in cui crea il diritto di essere cancellato dall'elenco, ha sollevato importanti dibattiti e nuove questioni.

Il 26 novembre 2014, il Gruppo di lavoro articolo 29 per la protezione dei dati (G29) ha adottato “*linee guida per l'attuazione della sentenza della CGUE su Google Spain*”.

Il parere del Gruppo di lavoro articolo 29 consta di due elementi principali: un'interpretazione della decisione e una definizione dei criteri per la valutazione dei reclami presentati alle autorità nazionali dalle persone interessate. Per il Gruppo di lavoro articolo 29, non dovrebbe esserci alcun limite al diritto di cancellazione. Inoltre, i motori di ricerca non hanno bisogno di informare le fonti del fatto che una delle loro pagine è inaccessibile a causa del c.d. *delisting*. Per quanto riguarda i criteri, il Gruppo di lavoro articolo 29 definisce tredici requisiti che devono essere applicati dalle autorità nazionali di vigilanza, sulla base delle “*norme generali*”.

1.7 Questioni aperte

Uno degli aspetti ancora non risolti dalla giurisprudenza europea è quello della portata del diritto alla de-indicizzazione. Infatti, uno dei più recenti rinvii pregiudiziali appunto stimolati dalla decisione *Google Spain* è quello del Consiglio di Stato francese nel caso C-507/17. In questo caso la CGUE si troverà a decidere di un ricorso contro un provvedimento dall'autorità garante francese *Commission Nationale de l'informatique e des Libertés* (CNIL) di fronte al *Conseil d'État*, in cui in primo luogo si chiede se il motore di ricerca sia tenuto ad eseguire l'operazione di cancellazione su tutti i nomi di dominio del suo motore, indipendentemente dal luogo dal quale veniva effettuata la ricerca avviata sul nome del richiedente, e anche al di fuori dell'ambito di applicazione territoriale della direttiva del 24 ottobre 1995.

Appare utile notare che con provvedimento n. 557 del 21.12.2017 il Garante per la Privacy, ritenendo ammissibile un ordine di c.d. deindicizzazione globale, ha ordinato ad un motore di ricerca di rimuovere gli URL deindicizzati fra i risultati di ricerca ottenuti digitando il nome e cognome del ricorrente, sia nelle versioni europee che extraeuropee.

Nel caso in esame, un professore universitario iscritto all'Anagrafe degli italiani residenti all'estero (AIRE) ha chiesto al Garante Privacy di ordinare a Google la deindicizzazione di 26 link, non limitata esclusivamente al territorio europeo, che sostiene facciano riferimento a contenuti gravemente offensivi della sua dignità e della reputazione. Il motore di ricerca, opponendosi al ricorso, ha evidenziato che la questione sulla deindicizzazione globale è attualmente all'esame della Corte di Giustizia dell'Unione

Europea nella causa C-507/17.

Il Garante per la Privacy, accogliendo il ricorso, ha ritenuto che la perdurante reperibilità sul web dei contenuti indicati in ricorso avesse un impatto "*sproporzionatamente negativo*" sulla sfera del ricorrente, anche in ragione del trattamento di dati potenzialmente sensibili che lo riguardano, tanto da non poter essere considerati in linea con quanto disposto dall'art. 11 del Codice e dalle Linee Guida sull'attuazione della sentenza *Costeja* emanate dal WP29 il 26 novembre 2014. In ossequio al principio della tutela effettiva, e tenuto conto del fatto che il ricorrente risiedeva fuori dell'Unione Europea, il Garante ha ritenuto opportuno estendere l'attività di rimozione degli URL in questione anche alle versioni extraeuropee del motore di ricerca.

Il predetto provvedimento, impugnato dal motore di ricerca dinanzi al Giudice Ordinario, è stato riformato dal Tribunale di Milano che, con sentenza dell'11.7.2018 (sentenza n. 7846/2018), ha ritenuto insussistenti i presupposti per la tutela del c.d. diritto all'oblio del ricorrente (e dunque non ha accolto l'istanza di deindicizzazione, a prescindere dalla questione relativa all'ambito territoriale del rimedio invocato).

1.8 Le novità del D.Lgs. 101/2018

1.8.1 [Base giuridica per l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri](#)

L'art. 2 del d.lgs 101/2018 introduce l'articolo 2-ter al codice in materia di protezione dei dati personali, il quale specifica che per quanto riguarda i trattamenti effettuati per "*l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*" la base giuridica per i trattamenti aventi ad oggetto dati personali "*comuni*" sia da rinvenirsi esclusivamente in una norma di legge o di regolamento. L'articolo si presenta come una riformulazione del previgente articolo 19 del Codice, il cui ambito di applicazione soggettivo viene, però, esteso al fine di adeguarsi all'impostazione adottata dal Regolamento. Nel Regolamento, infatti – come può leggersi nella relazione - **scompare la distinzione basata sulla natura pubblica o privata dei soggetti che trattano i dati, rilevando unicamente la finalità del trattamento perseguita, vale a dire se la finalità concerne un interesse pubblico o privato**. L'articolo quindi deve intendersi applicabile ai soggetti che trattano i dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a prescindere dalla loro natura soggettiva (art. 6, par. 1, lett. e, Reg. 2016/678).

1.8.2 [Individuazione degli interessi pubblici](#)

In relazione al trattamento di particolari categorie di dati viene stabilito l'obbligo di previsione normativa ed è individuato un elenco di trattamenti che si considerano effettuati per "*motivi di interesse pubblico rilevante*" (art. 2-sexies in relazione all'art. 9 del Regolamento concernente i dati che il Codice previgente definiva "dati sensibili"). Il regime normativo per tali trattamenti è sostanzialmente rimasto inalterato rispetto a quello previsto dal Codice per i trattamenti effettuati da soggetti pubblici (art. 20) e, in particolare, l'elenco predetto è tratto dalle diverse disposizioni del Codice riferite ai trattamenti effettuati per finalità di rilevante interesse pubblico (ad es. artt. 64-73, che il decreto abroga). Ovviamente, mutato il criterio per delimitare l'ambito applicativo di tale regime, le disposizioni in parola riguardano i trattamenti effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a prescindere dalla natura soggettiva del titolare del trattamento.

1.8.3 Libertà di stampa, libertà di espressione

Il titolo XII del codice aveva la seguente rubrica: “*Giornalismo ed espressione letteraria ed artistica*”. Tale rubrica è stata ora sostituita come segue: “«*Giornalismo, libertà di informazione e di espressione*»

In merito ad ipotesi di conflitto tra diritti fondamentali e, in particolare, di ipotesi di conflitto con il diritto all’informazione (che implica il trattamento di dati relativi a condanne penali e reati) rileva il contenuto dell’art. 2 *octies*. L’art. **2-octies (Principi relativi al trattamento di dati relativi a condanne penali e reati)** al comma 1 prevede che: “*Fatto salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell’articolo 6, paragrafo 1, del Regolamento, che non avviene sotto il controllo dell’autorità pubblica, è consentito, ai sensi dell’articolo 10 del medesimo regolamento, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati*”.

È fatto salvo, ovviamente, quanto stabilito dal d.lgs. n. 51 del 18 maggio 2018 che ha recepito in Italia la direttiva UE 2016/680 (che detta norme in materia di trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse, da parte sia dell’autorità giudiziaria, sia delle forze di polizia).

1.8.4 Salvaguardia dei codici di deontologia e buona condotta

Il d.lgs. n. 101/2018 introduce anche l’articolo 2-*decies* che conferma l’inutilizzabilità dei dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali (cfr art. 12, comma 2, d. lgs. 196/2003). Nell’articolo 2-*quater* è fatta salva l’adozione di “regole deontologiche” negli ambiti in cui il Regolamento riserva la materia agli Stati membri: a) (trattamenti necessari per adempiere un obbligo legale; b) trattamenti necessari per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri; c) trattamento di dati genetici, biometrici o relativi alla salute; d) talune specifiche situazioni di trattamento di cui al Capo IX). Tale disposizione trova la propria *ratio* nella scelta di conservare le regole stabilite nei “Codici di deontologia e di buona condotta”, previsti all’articolo 12 del previgente Codice che sino ad oggi hanno costituito una rilevante fonte di riferimento per i settori a cui sono diretti; ciò, però, solo nelle materie oggetto di “riserva” normativa interna agli Stati membri (art. 6, par. 2, Reg.).

1.9 **Rilievi conclusivi**

Le considerazioni appena svolte consentono di concludere evidenziando come il diritto alla libertà di manifestazione del pensiero e l’attività di informazione rappresentino diritti prevalenti rispetto ad altri diritti della persona con essi confliggenti, sopra esaminati. In ipotesi di conflitto, nel bilanciamento, alla luce delle indicazioni provenienti dalle Corti sovranazionali e dalla Corte di Cassazione, dovrà essere valutata la sussistenza di determinati presupposti, quali la tipologia di informazione in esame, l’essenzialità o meno della stessa, le caratteristiche dei dati trattati e l’attività svolta dal soggetto i cui dati vengono trattati.

Quando, invece, il diritto alla protezione dei dati personali entra in conflitto con diritti diversi dal diritto alla libertà di manifestazione del pensiero, il giudice si troverà a bilanciare i diritti in modo diverso, con conseguenze immediate anche in punto di scelta dei rimedi.

2 EFFETTIVITÀ DELLA TUTELA, PROPORZIONALITÀ E MISURE CORRETTIVE

2.1 Premessa

Nel presente capitolo, attraverso l'esame di casi giurisprudenziali, verranno analizzate alcune delle questioni relative al procedimento amministrativo ed al giudizio conseguente ad una violazione dei dati personali, con particolare riferimento all'onere di allegazione, all'onere della prova, alla scelta dei rimedi ed ai poteri officiosi del giudice.

Ci si soffermerà, in particolare, sui poteri dell'autorità amministrativa di controllo e sul rapporto tra l'esercizio di tali poteri ed il successivo sindacato svolto dall'autorità giurisdizionale. Con riferimento a tale aspetto, ci si interrogherà in concreto su come i rimedi del giudice civile possano interferire con quelli dell'autorità amministrativa di controllo. Nel settore della protezione dei dati, infatti, il ruolo del giudice civile è esercitato essenzialmente in sede di sindacato giurisdizionale dei provvedimenti dell'autorità garante (i casi nei quali il soggetto danneggiato adisce direttamente il giudice per chiedere esclusivamente il risarcimento del danno non sono, infatti, molto numerosi).

Dal principio di alternatività delle tutele, caratteristico del sistema italiano, si passerà poi ad esaminare le principali tipologie di provvedimenti emessi dal Garante, nonché i rimedi esperibili dinanzi al giudice ordinario. Un'attenzione particolare verrà, inoltre, dedicata alle modifiche introdotte dal Regolamento ed alle possibili conseguenze in merito ai rapporti tra tutela amministrativa e tutela giurisdizionale.

2.2 Tipologia di poteri e rimedi della pubblica amministrazione

In primo luogo, occorre chiarire la natura dei provvedimenti emessi dall'Autorità Garante.

La Suprema Corte (Cass. 20.5.2002 n. 7341) ha da tempo chiarito che l'ordinamento non conosce un *tertium genus* tra amministrazione e giurisdizione, alle quali la Costituzione riserva rispettivamente, per distinguerne e disciplinarne le attività, gli art. 111 e 97 e che non vi è nel sistema costituzionale una figura di paragiurisdizionalità a sé stante, distinta dalle due predette. Ritenuti non dirimenti i requisiti relativi all'oggetto del decidere (giacché alle pubbliche amministrazioni è dato di provvedere su diritti in forme definite giustiziali dalla dottrina), all'interesse pubblico costituente il riferimento fondamentale del giudice (atteso che la P.A. provvede in considerazione di un interesse pubblico generale) ed al rispetto del contraddittorio, la Corte di Cassazione (anche in ossequio al disposto dell'art. 29, comma 7, della legge n. 675 del 1996 – con disposizione ora prevista all'art. 10, comma 6, del D.lgs. 150/2011 – in forza della quale il Tribunale adito in opposizione alla decisione del Garante provvede anche in deroga al divieto di cui all'art. 4 della legge 2248 del 1865, all. E) ha accertato la natura amministrativa (e non giurisdizionale) dell'organo e del relativo procedimento, che non pone il Garante nella stessa posizione di terzietà assicurata dal giudice nel processo (cfr. Cass. n. 7341/2002 e n. 11864/04).

In merito a tale aspetto, la Corte di Cassazione ha poi precisato che: *“il ricorso al Giudice ordinario in opposizione al provvedimento del Garante non può essere inteso che come primo rimedio giurisdizionale a disposizione del soggetto che si pretende leso dall'atto del Garante”*. La Corte ha inoltre sottolineato che *“il Garante partecipa al giudizio di impugnativa di un suo atto quale sia stato*

il procedimento che lo ha preceduto per far valere davanti al giudice lo stesso interesse pubblico in funzione del quale essa è predisposto, ed in tale attività resta legato all'obbligo di imparzialità proprio perché l'interesse pubblico suddetto non gli è estraneo” (Cass.7341/2002) .

Le controversie previste dal D.Lgs. n. 196 del 2003, art. 152, sono regolate dal rito del lavoro e, ove non diversamente disposto, dal D.Lgs. 1° settembre 2011, n. 150, art. 10, che prevede la trattazione in unico grado di merito dinanzi al Tribunale. La controversia pertanto non si configura come gravame, rispetto al provvedimento adottato dal Garante in sede amministrativa, ma come opposizione, ed è proprio la natura amministrativa della fase svoltasi dinanzi al Garante che determina l'inidoneità del relativo provvedimento a passare in giudicato (cfr. Cass. n. 13151 del 25/05/2017; Cass. N.16061 del 18/06/2018).

Il codice privacy attribuisce al Garante per la Protezione dei dati personali il potere, non solo, di ordinare *"la cessazione del comportamento illegittimo" e di prescrivere "le misure necessarie a tutela dei diritti dell'interessato"* (art. 150, comma 2), al fine di *"rendere il trattamento conforme alle disposizioni vigenti"* (art. 143, lett. b, e art. 154, lett. c), ma anche di adottare ogni altro provvedimento necessario quando vi sia comunque un *"concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati"* (art. 143, lett. c). Il Garante è, più in particolare, competente all'emanazione di provvedimenti di natura preventiva, inibitoria o conformativa, potendo sospendere, modificare o far cessare il trattamento illegittimo dei dati personali, mentre la domanda risarcitoria ha causa petendi e petitum totalmente diversi, per i quali, è assicurata la riserva esclusiva di giurisdizione ordinaria.

L'art. 58 del Reg. 2016/678 specifica ed individua le tre tipologie dei poteri di indagine, dei poteri correttivi e dei poteri consultivi ed autorizzativi.

2.2.1 [La questione](#)

Come può incidere il principio di effettività sulla modulazione dei poteri dell'Autorità Garante?

2.2.2 [Il caso: Corte di Cassazione \(sezione I\), nella sentenza n. 7755 del 16 aprile 2015](#)

La Corte di Cassazione (sezione I), nella sentenza n. 7755 del 16 aprile 2015, si è soffermata sui poteri dell'Autorità Garante, precisando i limiti e le caratteristiche del potere di blocco del trattamento, ritenuto illecito, dei dati personali.

Nel caso in esame una casa editrice aveva presentato ricorso al Tribunale competente al fine di sentire dichiarare l'illegittimità del provvedimento con cui il Garante aveva vietato la diffusione, su una rivista di gossip, dei dati sanitari riferiti ad un noto personaggio pubblico che aveva perso la vita in un incidente stradale. Attraverso l'inibitoria l'Autorità Garante mirava ad evitare la divulgazione di dati clinici dettagliati, con allegato bozzetto autoptico, relativo alle ferite riportate in occasione del sinistro mortale, in quanto non necessarie per la completezza dell'informazione giornalistica. Il Tribunale, nel rigettare il ricorso, aveva ritenuto l'azione del Garante corretta nella misura in cui la stessa aveva impedito la divulgazione di dati sensibili non essenziali per la completezza dell'informazione, con conseguente illegittimità del relativo trattamento.

Soffermandosi in particolare sui poteri dell'Autorità, la Suprema Corte ha affermato che vietando alla casa editrice di diffondere i dati personali di carattere sanitario relativi al noto personaggio pubblico, *"non si era trattato di una tutela anticipata rispetto a una pubblicazione futura e incerta, ma di una pubblicazione già avvenuta, rispetto alla quale il Garante ha esercitato il potere, riconosciutogli*

dall'art. 143, lett. c), e art. 154, lett. c) e d), del codice privacy di vietare o disporre il blocco del trattamento dei dati personali che risulti illecito o non corretto, anche a causa della violazione delle prescrizioni del codice deontologico nell'esercizio dell'attività giornalistica (art. 139, comma 5, del codice privacy, artt. 6 e 10 del codice deontologico, approvato con provvedimento del Garante del 29 luglio 1998, con riguardo all'essenzialità dell'informazione e alla tutela della dignità della persona)".

2.2.3 La giurisprudenza italiana

La giurisprudenza nazionale ha affrontato in diversi casi il ruolo e i poteri dell'autorità garante per esempio nella decisione della Suprema Corte n. 11140/2016, depositata il 30.5.2016. Nel caso in esame, il Garante aveva avviato un'istruttoria in merito alla procedura adottata dalla RAI al fine di raccogliere i dati personali degli acquirenti da parte dei rivenditori di apparecchi radiotelevisivi, anche mediante richiesta di informative e documenti rivolta alla stessa RAI e all'Agenzia delle Entrate. All'esito di tale procedura, nel 2001 il Garante aveva emesso un provvedimento con il quale aveva censurato la procedura e segnalato all'Agenzia delle Entrate (quale titolare del trattamento dei dati) e alla RAI (quale responsabile del trattamento dei dati) la necessità di *«interrompere la raccolta ed il trattamento dei dati personali [...] e di astenersi dal loro ulteriore trattamento»*. Nella sentenza in esame, la Prima Sezione della Corte di Cassazione, accogliendo il ricorso del Garante ha affermato che l'atto impugnato *«si sostanziava in manifestazione d'intento non direttamente autoritativo ed interdittivo ma persuasivo»* (contenente una segnalazione motivata dell'opportunità di abbandonare una procedura illegittima di trattamento dei dati personali). Tale atto ha quindi assunto la veste tipica del provvedimento, rientrando tra i compiti del Garante quello di *«segnalare ai relativi titolari o responsabili le modificazioni necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti»* (cfr. art. 31, comma 1, lett. c), l. n. 675/1996, vigente all'epoca dei fatti).

2.2.4 La giurisprudenza europea

Il ruolo e i poteri delle autorità garanti sono state affrontati in dettaglio nel caso *Weltimmo* (C-230/14), in cui la CGUE si trovava ad affrontare la questione relativa alla possibilità che l'autorità ungherese per la protezione dei dati potesse esercitare il potere, conferitole dalla legge ungherese, di infliggere un'ammenda ad una società che, pur essendo registrata in Slovacchia, gestiva un sito web per il commercio immobiliare riguardante proprietà site in Ungheria. Il rinvio pregiudiziale si riferiva in realtà alla questione circa il campo di applicazione territoriale della legge, e se l'autorità ungherese avrebbe potuto esercitare i propri poteri contro una società registrata in Slovacchia.

Tuttavia, la Corte ha ritenuto che, prima di trattare l'ambito di applicazione territoriale dei dati nazionali poteri dell'autorità di protezione, *"è necessario esaminare quali sono i poteri di tale autorità di controllo"*. alla luce dell'articolo 28, paragrafi 1, 3 e 6, della direttiva 95/46".

Per la Corte, dall'art. 28, n. 1, della direttiva 95/46 risulta che ciascuna autorità di controllo istituita da uno Stato membro deve garantire il rispetto, all'interno del territorio di tale Stato membro, delle disposizioni adottate in applicazione della direttiva 95/46. Inoltre la Corte osserva che, ai sensi dell'art. 28, n. 3, della direttiva 95/46, tali autorità di controllo si trovano a essere dotati in particolare di poteri investigativi, quali i poteri di raccolta di tutte le informazioni necessari per l'esercizio delle loro funzioni di vigilanza e di effettivi poteri d'intervento, quali come potere di ordinare il blocco, la cancellazione o la distruzione dei dati, di imporre un'azione temporanea o il divieto definitivo di trattamento o di avvertire o ammonire il responsabile del trattamento dei dati. La Corte sottolinea che tale elenco di poteri non deve essere considerato esaustivo e che, tenuto conto del tipo di potere discrezionale di cui

dispongono gli Stati membri in materia di recepimento della direttiva 95/46, si deve considerare che tali poteri di intervento possono comprendere il potere di sanzionare il responsabile del trattamento dei dati imponendogli, se del caso, un'ammenda. La Corte aggiunge che tale potere dovrebbe essere esercitato conformemente al diritto processuale dello Stato membro a cui appartiene l'autorità di controllo.

La decisione della Corte può essere letta come implicitamente riferita al principio di effettività, in quanto il ragionamento della Corte si basa sull'idea che, essendo le autorità di controllo nazionali di controllo istituite per garantire il rispetto del regolamento sulla protezione dei dati, essi dovrebbero essere dotati di poteri necessari a tal fine, anche se tali poteri non sono espressamente elencati nella direttiva 95/46.

L'autorità di controllo ungherese può esercitare il potere di infliggere un'ammenda a un responsabile del trattamento, anche se tale potere non è espressamente incluso nella direttiva. Tuttavia, tale potere dovrebbe essere esercitato secondo il diritto procedurale dello Stato membro cui appartiene l'autorità di controllo, e solo sul territorio di tale Stato membro (cfr. capitolo 2 sull'ambito di applicazione territoriale).

Nel più recente caso *Holstein* C-210/16, la CGUE riprende i principi affermati in *Weltimmo* per affermare che la competenza può essere esercitata dall'autorità garante dello Stato membro in cui la società responsabile del trattamento è stabilita, anche non è il soggetto che opera concretamente il trattamento all'interno del gruppo societario, ma soltanto quello che opera la vendita di spazi pubblicitari e le altre attività di marketing.

Se le autorità di vigilanza devono cooperare tra loro nella misura necessaria per l'esecuzione del progetto dei loro compiti, in particolare attraverso lo scambio di tutte le informazioni utili, la direttiva non prevedeva criteri di priorità circa l'intervento di un'autorità di vigilanza rispetto ad un'altra, né prevedeva l'obbligo per un'autorità di controllo di uno Stato membro di rispettare la posizione espressa dall'autorità di controllo di un altro Stato membro. Occorre a tal proposito ricordare che le autorità nazionali di controllo sono responsabili, ai sensi dell'articolo 8, paragrafo 3, CDF per il controllo del rispetto delle norme UE concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali.

Nel Regolamento 2016/679 i poteri delle autorità di controllo indipendenti sono definiti in modo più ampio rispetto alla direttiva previgente. Tra questi, il potere di "*imporre un'ammenda amministrativa ai sensi dell'articolo 83, in aggiunta o in luogo delle misure di cui al presente paragrafo, a seconda delle circostanze di ogni singolo caso*" è esplicitamente indicato come potere obbligatorio per le autorità di controllo.

Il legislatore dell'UE ha pertanto tenuto conto dell'esito del dialogo giudiziario svoltosi in seno alla CGUE in decisioni, come quelle qui commentate, in cui la Corte ha interpretato esplicitamente o implicitamente la direttiva 95/46 alla luce del principio di efficacia. Attualmente questo principio è esplicitamente menzionato all'articolo 83 del Regolamento, insieme ai principi di proporzionalità e dissuasività (par. 1).

2.3 Poteri e rimedi dell'autorità giudiziaria

2.3.1 [Il rapporto tra procedimento amministrativo e procedimento giurisdizionale. La disciplina previgente](#)

L'art. 145, commi 2 e 3, del Codice Privacy fissava il principio dell'alternatività secondo il quale

a) il ricorso al Garante non poteva essere proposto se per il medesimo oggetto e tra le stesse parti è stata

già adita l'autorità giudiziaria;

b) la presentazione del ricorso al Garante rendeva improponibile un'ulteriore domanda davanti all'autorità giudiziaria ordinaria tra le stesse parti e per lo stesso oggetto.

L'alternatività riguardava esclusivamente le domande aventi un identico oggetto, ovvero quelle che, se pendenti contestualmente davanti a più giudici, potessero, in via generale, essere assoggettate al regime processuale della litispendenza o della continenza. Si tratta delle domande che richiedono interventi di natura preventiva, inibitoria o conformativa, potendo il Garante indicare modalità concrete di cessazione del trattamento illecito dei dati. La domanda di risarcimento del danno patrimoniale o non patrimoniale ha *causa petendi* e *petitum* radicalmente divergenti da quelle sopra esaminate ed era destinata ad una declaratoria d'inammissibilità se proposta davanti al Garante; in numerose pronunce (*ex multis* 19/2/2002 doc. web. 1063674; 5 ottobre 2006 doc. web. 135919), il Garante ha ritenuto inammissibile il ricorso contenente una domanda risarcitoria, ritenendosi privo di competenza al riguardo.

Come chiaramente affermato dalla Suprema Corte, *“l'accoglimento del ricorso, totale o parziale, da parte del Garante può, in conclusione, facilitare il ricorso alla tutela risarcitoria davanti all'autorità giudiziaria ordinaria, ma non escluderla. Diversamente ragionando, dovrebbe ritenersi alternativamente che scelta la strada della tutela inibitoria (e preventiva), sia negata quella risarcitoria, oppure che, nonostante il riconoscimento del trattamento illecito dei dati personali, la parte sia tenuta ad un'impugnazione del provvedimento del Garante al solo fine di richiedere il risarcimento del danno e non incorrere nella sanzione di tardività dell'azione. Quest'ultima soluzione è in netto contrasto con il canone costituzionale della ragionevolezza. La prima introduce un impedimento all'ottenimento della tutela piena di un diritto fondamentale quale quello in gioco, del tutto incompatibile con l'art. 24 Cost. Diversa è la soluzione in caso di rigetto del ricorso da parte del Garante. In tale ipotesi, condicio sine qua non per adire l'autorità giudiziaria è l'impugnazione tempestiva del provvedimento di diniego, con conseguente facoltà di proporre la connessa domanda risarcitoria unitamente a quella relativa all'accertamento della illiceità del trattamento dei dati”* (Cass. 17.9.2014 n. 19534; cfr. anche Cass. Sez. lav. 7.4.2016 n. 6775).

[2.3.2 Le novità del D.Lgs. 101/2018 in materia di rapporto fra procedimento amministrativo e procedimento giurisdizionale](#)

L'art. 145 del codice in materia di dati personali è stato abrogato dal d.lgs 101/2018. Il GDPR detta alcune norme rilevanti per comprendere i rapporti fra procedimento amministrativo e giurisdizionale. In particolare, si prevedono:

- il reclamo all'autorità di controllo

L'articolo 77 GDPR prevede il diritto di proporre reclamo all'autorità di controllo. Si prevede che, *“fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il (...) regolamento ha il diritto di proporre reclamo a un'autorità di controllo”*. Si prevede poi che *“l'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale”*.

- il ricorso giurisdizionale effettivo contro le decisioni dell'autorità di controllo

L'art. 78 GDPR prevede *“fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda”* nonché nel caso in cui *“l'autorità di controllo che sia competente (...) non tratti un reclamo o non lo informi entro tre mesi dello stato o*

dell'esito del reclamo”.

- il ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento

L'art. 79 GDPR prevede il diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento, che è esercitabile “*fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile*”.

Occorre infine sottolineare che per quanto riguarda il risarcimento del danno, l'art 82 GDPR prevede la competenza dell'autorità giurisdizionale.

2.3.3 Le novità del D.Lgs. 101/2018 in merito al procedimento giurisdizionale

L'art. 17 del D.Lgs 101/2018 sostituisce l'art. 10 del D.lgs. 150/2011. In sintesi:

- è prevista la competenza, in via alternativa del tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero del tribunale del luogo di residenza dell'interessato;
- il comma 5 prevede che l'interessato possa dare mandato a un ente del terzo settore soggetto alla disciplina del decreto legislativo 117/2017, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali di esercitare per suo conto l'azione, ferme le disposizioni in materia di patrocinio previste dal codice di procedura civile;
- il comma 9 dispone che nei casi in cui non sia parte in giudizio, il Garante può presentare osservazioni, da rendere per iscritto o in udienza, sulla controversia in corso con riferimento ai profili relativi alla protezione dei dati personali. Il giudice dispone che sia data comunicazione al Garante circa la pendenza della controversia, trasmettendo copia degli atti introduttivi, al fine di consentire l'eventuale presentazione delle osservazioni

L'art. 154-ter (Potere di agire e rappresentanza in giudizio). 1. Il Garante è legittimato ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali. 2. Il Garante è rappresentato in giudizio dall'Avvocatura dello Stato, ai sensi dell'articolo 1 del regio decreto 30 ottobre 1933, n. 1611.

3. Nei casi di conflitto di interesse, il Garante, sentito l'Avvocato generale dello Stato, può stare in giudizio tramite propri funzionari iscritti nell'elenco speciale degli avvocati dipendenti di enti pubblici ovvero avvocati del libero foro”.

2.3.4 La questione

Nei casi di protezione dei dati, qual è il ruolo del diritto a un ricorso giurisdizionale effettivo (articolo 47 CDFUE) nel definire il rapporto tra esecuzione amministrativa e giudiziaria?

Atteso che l'art. 47 della Carta riguarda non solo i diritti degli individui, ma anche il rapporto tra tutela giurisdizionale e tutela amministrativa, può ritenersi che l'art. 140 *bis* sopra citato costituisca uno strumento che garantisce all'interessato una tutela effettiva dei suoi diritti?

2.3.5 La giurisprudenza italiana

(i) Corte di Cassazione italiana in Cass. civ. Sez. III, n. 17408/2012

Nel caso di procedimenti alternativi riguardanti la stessa domanda, la Corte di Cassazione italiana si è

occupata del rapporto tra il ruolo dell'autorità di controllo e quello dei tribunali nei procedimenti giudiziari. La causa si è concentrata su una situazione complessa in cui l'interessato ha presentato un ricorso in primo luogo dinanzi a un tribunale e in secondo luogo dinanzi all'autorità di controllo. L'autorità di controllo, erroneamente, non ha dichiarato la domanda irricevibile a causa dell'avvio dell'azione giudiziaria e ha deciso il caso dinanzi al tribunale di primo grado ha concluso il procedimento. Successivamente, il tribunale di primo grado, ignorando la decisione dell'autorità di controllo, ha deciso il caso. L'attore ha quindi impugnato dinanzi alla Corte di Cassazione la decisione del tribunale di primo grado per erronea applicazione dell'art. 145 del Codice della protezione dei dati personali.

La Corte Suprema ha affrontato la questione chiarendo che l'alternativa tra i due meccanismi di esecuzione non impone nel caso specifico che l'azione giudiziaria debba essere dichiarata inammissibile, essendo quest'ultima iniziata prima della richiesta all'autorità di protezione dei dati. Nel caso specifico, sono i procedimenti dinanzi all'autorità di controllo che avrebbero dovuto essere considerati inammissibili. Tuttavia, dato che la decisione dell'autorità per la protezione dei dati è stata presa prima della conclusione del procedimento giudiziario e non è stata impugnata dalle parti, essa spiega i suoi effetti solo rispetto alle argomentazioni delle parti.

(ii) Corte di Cassazione nella Cass. civ. n. 13151/2017, 25 maggio 2017

Anche in questa decisione, la Corte di Cassazione ha affrontato l'impatto della decisione dell'autorità nazionale di controllo nei confronti del procedimento giudiziario relativo al risarcimento dei danni. La Corte ha affermato che la decisione dell'autorità di controllo non può vincolare il tribunale civile in quanto una tale decisione non acquisirà mai lo *status* (e avrà gli effetti) di cosa giudicata, dato che l'autorità di protezione dei dati è un organo amministrativo.

2.3.6 La giurisprudenza europea

Il caso europeo più rilevante sul rapporto relativo al rapporto fra ricorso amministrativo e giudiziario è *Puškár*, C-73/16.

Il sig. Puškár è una persona fisica che ha presentato un ricorso alla Corte Suprema della Repubblica slovacca chiedendo alla Direzione Finanza, a tutti gli uffici fiscali sotto il suo controllo e alla Direzione Finanze Ufficio amministrativo penale di rimuovere il suo nome da un elenco, precedentemente redatto dalla Direzione Finanza, che non era diffuso al pubblico, e di cui era entrato in possesso senza il consenso della Direzione Finanza. Tale elenco conteneva il Numero di Identità e il Codice Fiscale del sig. Puškár; questi fa valere una violazione dei suoi diritti chiedendo la rimozione del suo nome e di ogni riferimento a lui dall'elenco e da altri elenchi analoghi, nonché dal sistema informatico dell'autorità finanziaria. La Corte suprema respinge la domanda poiché il sig. Puškár non aveva esaurito i rimedi dinanzi alle autorità amministrative nazionali. Il sig. Puškár ha quindi presentato ricorso alla Corte costituzionale della Repubblica slovacca.

La Corte costituzionale slovacca si è concentrata principalmente sulla giurisprudenza relativa all'articolo 6, paragrafo 1, della CEDU in relazione all'articolo 46 della Costituzione slovacca. La Corte si è occupata in particolare dell'obbligo dei tribunali di giustificare la loro decisione tenendo conto di tutti i fatti e gli elementi giuridici pertinenti. Tale obbligo è stato considerato una condizione preliminare per l'esercizio del diritto delle parti a un ricorso effettivo. In questo senso, la Corte costituzionale interpreta l'articolo 46, paragrafo 1, della costituzione slovacca, conformemente all'articolo 6, paragrafo 1, della CEDU e sulla base della giurisprudenza della Corte europea dei diritti dell'uomo. In questo senso, la

Corte costituzionale ha affermato che per soddisfare i requisiti dell'articolo 46 Cost. (e dell'articolo 6 della CEDU), l'analisi della Corte suprema avrebbe dovuto tener conto di tutte le circostanze del caso rispetto al livello di protezione dei dati personali garantito dall'articolo 46 Cost. Costituzione e il livello di protezione della privacy garantito dalla CEDU. Così, la Corte costituzionale ha concluso che la Corte di Cassazione non aveva preso in considerazione gli argomenti di fatto e di diritto e, cosa più importante, aveva mancato di fornire una decisione in merito a quali condizioni la protezione dei dati personali avrebbe dovuto essere rispettata nel caso del trattamento dei dati da parte delle autorità fiscali. La Corte costituzionale ha poi affermato che la Corte suprema ha violato i diritti fondamentali del ricorrente, vale a dire il diritto a un ricorso effettivo e a un processo equo, il diritto alla privacy e il diritto alla protezione dei dati personali. Pertanto, la Corte costituzionale ha rinviato la causa alla Corte suprema.

A questo punto, la Corte suprema, ritenendo che la Corte costituzionale non avesse tenuto conto della giurisprudenza della Corte di giustizia dell'Unione europea, ha deciso di adire tale Corte per una pronuncia pregiudiziale.

La prima questione mirava a verificare se il procedimento amministrativo preliminare obbligatorio adottato dal legislatore slovacco nel caso in questione è conforme al diritto dell'UE e in particolare all'articolo 47 CDF.

Dopo aver dichiarato che i dati personali raccolti a fini fiscali rientrano nell'ambito di applicazione della direttiva n. 95/46, poiché sono trattate dall'articolo 13, paragrafo 1, di tale direttiva, la CGUE esamina le questioni pregiudiziali.

Per quanto riguarda la prima questione pregiudiziale, la Corte ricorda che l'obbligo di esaurire i rimedi amministrativi, pur non vietato dalla direttiva n. 95/46, deve essere esaminato alla luce dell'Articolo 47 CDF, articolo 4, paragrafo 3 del TUE (principio di leale cooperazione) e articolo 19, paragrafo 1 del TUE (principio di leale cooperazione). Poiché l'obbligo di esaurire i mezzi di ricorso amministrativi supplementari costituisce una limitazione del diritto ad un'effettiva il ricorso giurisdizionale può essere giustificato secondo i criteri stabiliti a norma dell'articolo 52 (1) CFREU, ossia solo quando:

- i) sia previsto dalla legge;
- ii) rispetti dell'essenza del diritto;
- iii) conforme al principio di proporzionalità;
- iv) rispetti gli obiettivi di interesse generale riconosciuti dall'UE o la necessità di tutelare i diritti dei cittadini europei. diritti e libertà altrui.

La Corte si è concentrata in particolare sugli ultimi due criteri. Per quanto riguarda l'esistenza di obiettivi di interesse generale, la Corte ha riconosciuto che la l'obbligo di presentare un reclamo amministrativo prima di avviare un'azione legale può avere un positivo effetto deflattivo del contenzioso, permettendo la definizione delle controversie in tempi più rapidi e incrementando l'efficienza dell'autorità giudiziaria. Pertanto, l'obbligo generale persegue obiettivi di interesse generale. Per quanto riguarda il test di proporzionalità, la Corte si è basata sul parere dell'AG e sulle decisioni *Alassini* (da C-317/08 a C-320/08) e *Menini* (C-75/16). In particolare, ha fatto esplicito riferimento ai criteri individuati nella decisione *Alassini*, (par. 67) ai fini della valutazione della proporzionalità. Tali pronunce, rese in materia consumeristica, prevedono che non siano contrarie al principio della tutela giurisdizionale effettiva quelle norme che subordinano la proposizione di un ricorso giurisdizionale al previo esperimento di procedure di conciliazione e di mediazione extragiudiziali, a condizione che:

1. Le procedure non danno luogo ad una decisione vincolante per le parti;
2. Le procedure non causano un ritardo sostanziale ai fini dell'introduzione di un'azione legale. Procedure;
3. I procedimenti sospendono il termine di prescrizione;
4. Le procedure non danno luogo a costi - o a costi molto bassi - per le parti;
5. La procedura non sono previste solo per via elettronica;
6. Le procedure prevedono misure provvisorie in casi eccezionali in cui l'urgenza della situazione lo richiede.

Sulla base di queste argomentazioni, la CGUE stabilisce dunque che *“l'articolo 47 della Carta dei diritti fondamentali dell'Unione europea deve essere interpretato nel senso che esso non osta a una normativa nazionale che subordina la possibilità di esperire un ricorso giurisdizionale, da parte di una persona che afferma sia stato violato il suo diritto alla tutela dei dati personali (...), al previo esaurimento dei rimedi disponibili dinanzi alle autorità amministrative nazionali, a condizione che le modalità concrete di esercizio di detti rimedi non pregiudichino eccessivamente il diritto ad un ricorso effettivo dinanzi a un giudice (...). È importante, in particolare, che l'esaurimento dei rimedi disponibili dinanzi alle autorità amministrative nazionali non comporti un ritardo sostanziale per la proposizione di un ricorso giurisdizionale, produca la sospensione della prescrizione dei diritti considerati e non provochi costi eccessivi”*.

2.3.7 Rilievi conclusivi

L'esame dei poteri dell'autorità di controllo e dell'autorità giudiziaria, in materia di tutela conseguente alle violazioni del diritto alla protezione dei dati personali, nonché l'analisi della tipologia dei provvedimenti emessi evidenzia come l'autorità giudiziaria – anche quando venga adita in sede di opposizione avverso i provvedimenti del Garante - sia sovente chiamata alla scelta di un rimedio che, nel rispetto dei principi di effettività e proporzionalità, garantisca una tutela effettiva. In sede di sindacato sull'atto dell'autorità di controllo - sicuramente più esteso nel caso del giudice ordinario, rispetto a quello amministrativo – come si traducono le importanti novità introdotte dal Regolamento, in materia di rimedi, sul versante dei poteri del giudice civile?

Il rispetto del principio della domanda, l'onere della prova, le preclusioni istruttorie sono solo alcuni dei temi sui quali, all'indomani dall'entrata in vigore del Regolamento, la giurisprudenza sarà chiamata a confrontarsi.

3 EFFETTIVITÀ DELLA TUTELA, PROPORZIONALITÀ E SANZIONI

3.1 Premessa

Occorre premettere che, sebbene la giurisprudenza che ha affrontato le problematiche attinenti alle sanzioni amministrative irrogate dal Garante per la Privacy in caso di violazione del diritto alla protezione dei dati personali e del relativo controllo da parte dell'autorità giurisdizionale, abbia raramente posto, a fondamento delle proprie decisioni, in modo esplicito, i principi di effettività della tutela e di proporzionalità, alcune delle soluzioni fornite dalle decisioni che saranno citate nel prosieguo rispondono chiaramente all'esigenza di garantire una tutela effettiva degli interessati anche sul piano sanzionatorio, così come altre garantiscono anche in questa fase il rispetto del principio di proporzionalità, che assume qui particolare rilievo. Le decisioni in questione saranno dunque analizzate in quest'ottica.

3.2 Principi generali in materia di illeciti amministrativi: le applicazioni nella giurisprudenza con riguardo ai provvedimenti del Garante Privacy

Prima di esaminare le questioni relative all'irrogazione delle sanzioni da parte del Garante, è utile innanzitutto svolgere qualche considerazione sui principi generali che regolano la disciplina delle sanzioni amministrative e che hanno trovato applicazione da parte della giurisprudenza anche nell'ambito della tutela della privacy.

Al riguardo può citarsi innanzitutto Cassazione civile, sez. I, 11 giugno 2014, n. 13219, che, dovendo valutare l'incidenza della modifica legislativa favorevole successiva ai fatti oggetto del provvedimento del Garante, ossia il caso in cui il trattamento illecito fosse avvenuto prima dell'entrata in vigore della norma più favorevole, ha fatto applicazione del principio valevole in tema di illeciti amministrativi secondo cui *“l'adozione dei principi di legalità, irretroattività e divieto di analogia, di cui alla L. n. 689 del 1981, art. 1, comporta l'assoggettamento del fatto alla legge del tempo del suo verificarsi, con conseguente inapplicabilità della disciplina posteriore eventualmente più favorevole, a nulla rilevando che detta più favorevole disciplina, successiva alla commissione del fatto, sia entrata in vigore anteriormente all'emanazione del provvedimento di accertamento”* (Sez. I, n. 1105/2012).

3.3 L'elemento soggettivo dell'illecito

Chiamata a pronunciarsi sul provvedimento del Garante per la protezione dei dati personali che aveva sanzionato l'Agenzia delle Entrate per aver diffuso, sul proprio sito internet, i redditi dichiarati da tutti i contribuenti per l'anno 2005, Cassazione civile, sez. I, 11 giugno 2018, n. 15075, in merito alla censura attinente alla violazione dell'art. 3, L. n. 689 del 1981, facendo valere parte ricorrente che il comportamento contestato all'Agenzia non era stato dalla stessa posto in essere dolosamente o colposamente e che comunque il Garante non aveva dato prova di tale elemento soggettivo, ha ritenuto, quanto al riparto degli oneri probatori con particolare riguardo all'elemento soggettivo, che, *“in tema di sanzioni amministrative, la L. 24 novembre 1981, n. 689, art. 3, in presenza del compimento della condotta proibita, pone una presunzione di colpa a carico dell'autore del fatto vietato, riservando a questi l'onere di provare di aver agito senza colpa (cfr. Cass. n. 2406 del 2016; Cass. n. 27432 del*

2013), con la conseguenza che la sentenza impugnata ha correttamente soffermato la propria attenzione sulla sussistenza dell'elemento oggettivo della violazione (nella specie, del D.Lgs. n. 196 del 2003, art. 13), ricadendo sulla predetta odierna ricorrente l'onere probatorio di cui si è detto”, onere nella specie rimasto inadempito. D'altro canto, ha specificato la Corte, “in tema di violazioni amministrative, l'errore sulla liceità del fatto giustifica l'esclusione della responsabilità solo quando risulti inevitabile, occorrendo, a tal fine, un elemento positivo, estraneo all'autore dell'infrazione, idoneo ad ingenerare in lui la convinzione della stessa liceità, oltre alla condizione che, da parte sua, sia stato fatto tutto il possibile per osservare la legge e che nessun rimprovero possa essergli mosso, così che l'errore sia stato incolpevole, non suscettibile, cioè, di essere impedito dall'interessato con l'ordinaria diligenza (cfr. Cass. n. 19759 del 2015)”.

3.4 La responsabilità dell'Ente

La garanzia di una tutela effettiva degli interessati passa anche dalla previsione della possibilità di infliggere le sanzioni previste *ex lege* al titolare del trattamento, sia esso persona fisica o giuridica.

In questo senso spunti interessanti possono trarsi da Cassazione civile, sez. II, 5 luglio 2016, n. 13657, che ha affrontato la questione della “identificazione” del soggetto titolare del trattamento e della imputabilità delle sanzioni, interrogandosi sui limiti di compatibilità del rinvio alla L. n. 689 del 1981 da parte del D.Lgs. n. 196 del 2003, art. 166. Si è domandata, infatti, se sia possibile in quest'ambito infliggere la sanzione amministrativa prevista *ex lege* anche ad un Ente (quale, in ipotesi, la Provincia) oppure solo ad una persona fisica.

Al riguardo la Corte ha preliminarmente osservato che “il richiamo al noto principio della imputabilità personale della sanzione, di cui alla L. n. 689 del 1981, non può giustificare - come ritenuto nella decisione gravata - la sostanziale irresponsabilità dell'Ente tenuto al trattamento dei dati sensibili protetti dalla legge. Non è corretto, in particolare, il richiamo, operato dalla sentenza impugnata, al dictum di Cass. n. 12664/2007 e, quindi, al principio (in essa pure richiamato) della natura personale della responsabilità e dei conseguenti profili della imputabilità, dell'elemento soggettivo della violazione, delle cause di esclusione della responsabilità e del concorso di persone.

Giova al riguardo evidenziare che quanto affermato dalla citata decisione di questa Corte attiene, più propriamente, al regime sanzionatorio considerato dalla generale legge di depenalizzazione.

Quest'ultima preesisteva alla normativa sanzionatoria specifica del Codice e quest'ultimo, pur richiamando (al suo art. 166) la L. n. 689 del 1981 rende possibile la configurabilità di una responsabilità solidale della persona giuridica, ma non esclude di per sé la possibile autonoma responsabilità della stessa siffatta persona quanto al successivo e specifico regime sanzionatorio previsto dal predetto Codice stesso.

Infatti la diversa natura giuridica delle sanzioni amministrative contenute nel Codice in materia di protezione dei dati personale (D.Lgs. n. 196 del 2003) è confermata dal tenore della norma di cui all'art. 162, comma 2-bis (aggiunto ex D.L. n. 207 del 2008 conv. in L. n. 14 del 2009) del detto codice laddove si prevede testualmente che: “in caso di trattamento di dati personali effettuato in violazione...delle disposizioni indicate nell'art. 167 è altresì applicata in - sede amministrativa, in ogni caso, la sanzione del pagamento di una somma....”.

Insomma, con l'anzidetta norma di legge si prevede una sanzione amministrativa che si aggiunge a quella penale, con un regime proprio ed autonomo e che scatta in ogni caso e, quindi, anche nei confronti

di un Ente e non solo della persona fisica.

Peraltro la suddetta previsione appare in linea proprio con l'inquadramento generale dato dal citato Codice quanto alla configurazione dei soggetti (persone fisiche o giuridiche) titolari del trattamento dei dati. Difatti, ai sensi dell'art. 4 del predetto Codice, è considerato titolare del trattamento dei dati non solo la persona fisica, ma espressamente anche *“..la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono...”*.

D'altra parte questa Corte, già con nota pronuncia (Cass. civ., Sez. 6-2, Ord. 8 aprile 2014, n. 8184), ha già avuto modo di affermare che *“il titolare del trattamento è la persona giuridica, come tale perfettamente sanzionabile ai sensi della normativa in materia di trattamento dei dati personali”*.

3.5 Termine di decadenza per la contestazione dell'illecito e l'irrogazione della sanzione

Un criterio di proporzionalità sembra essere stato adoperato dalla giurisprudenza per stabilire il momento a partire dal quale decorre il termine di decadenza per la contestazione dell'illecito e l'irrogazione della sanzione da parte del Garante Privacy: è principio consolidato, infatti, quello per cui spetta al giudice di merito considerare quale sia il tempo ragionevolmente necessario per le indagini dell'Autorità, guardando alla maggiore o minore difficoltà del caso concreto e alla necessità delle indagini stesse.

Più nel dettaglio, in via generale, secondo la giurisprudenza, se da un lato, *“è irrilevante la suddivisione dell'Amministrazione in una pluralità di snodi organizzativi in materia di accertamento ed irrogazione di sanzioni amministrative e la distinzione tra gli organi, deputati, rispettivamente, alla constatazione ed alla valutazione dei fatti costituenti violazioni amministrative, è ininfluente ai fini della decorrenza del termine da rispettare per la contestazione degli illeciti”*, dall'altro lato, *“nel caso di mancata contestazione immediata della violazione, l'attività di accertamento dell'illecito non coincide con il momento in cui viene acquisito il fatto nella sua materialità, ma deve essere intesa come comprensiva del tempo necessario alla valutazione dei dati acquisiti ed afferenti agli elementi (oggettivi e soggettivi) dell'infrazione e, quindi, della fase finale di deliberazione, correlata alla complessità delle indagini tese a riscontrare la sussistenza dell'infrazione medesima e ad acquisire piena conoscenza della condotta illecita sì da valutarne la consistenza agli effetti della corretta formulazione della contestazione; compete, poi, al giudice di merito determinare il tempo ragionevolmente necessario all'Amministrazione per giungere a una simile, completa conoscenza, individuando il dies a quo di decorrenza del termine, tenendo conto della maggiore o minore difficoltà del caso concreto e della necessità che tali indagini, pur nell'assenza di limiti temporali predeterminati, avvengano entro un termine congruo essendo il relativo giudizio sindacabile, in sede di legittimità, solo sotto il profilo del vizio di motivazione (Cass. Sez. 2, Sentenza n. 25916 del 2006)”*.

Il Consiglio di Stato – chiamato a pronunciarsi sull'arco di tempo entro il quale l'Autorità garante concorrenza e mercato deve provvedere alla notifica della contestazione, ma con principi che ben possono trovare applicazione nel settore della protezione dei dati personali – ha affermato che, ai sensi dell'art. 14 l. 689 del 1981, il detto arco di tempo *“è collegato non già alla data di commissione della violazione, ma al tempo di accertamento dell'infrazione, da intendersi in una prospettiva teleologicamente orientata e quindi non già alla notizia del fatto sanzionabile nella sua materialità, ma all'acquisizione della piena conoscenza della condotta illecita, implicante il riscontro dell'esistenza e della consistenza della infrazione e dei suoi effetti; pertanto, il fatto che l'Autorità Antitrust delibere*

l'avvio dell'istruttoria a distanza di vari mesi dalla segnalazione della possibile infrazione non può in alcun modo essere considerato come una violazione dei diritti delle imprese coinvolte, né un superamento dei termini procedurali, in quanto la stessa valutazione dell'esigenza di avviare o meno l'istruttoria può presentarsi complessa; di conseguenza, il termine di novanta giorni previsto dal comma 2 dell'art. 14 della legge n. 689 del 1981 inizia a decorrere solo dal momento in cui è compiuta - o si sarebbe dovuta ragionevolmente compiere, anche in relazione alla complessità della fattispecie - l'attività amministrativa intesa a verificare l'esistenza dell'infrazione, comprensiva delle indagini intese a riscontrare la sussistenza di tutti gli elementi soggettivi e oggettivi dell'infrazione stessa" (Consiglio di Stato 22.7.2014 n. 3986 e, più di recente, Consiglio di Stato 1.6.2016 n. 2328).

I predetti principi sono stati confermati e applicati dalla Suprema Corte anche con specifico riferimento all'attività ispettiva e sanzionatoria di competenza del Garante per la Protezione dei Dati Personali con sentenze n.17143 del 17/08/2016 e del 6 giugno 2018, n. 14678, secondo cui *“In caso di mancato rispetto della privacy, il termine di 90 giorni previsto per la notifica della violazione decorre dal momento in cui l'Autorità Garante, all'esito della attività istruttoria, abbia acquisito piena conoscenza della condotta illecita”*. La Corte di Cassazione ha in questo modo fissato un parallelo con quanto già previsto per gli accertamenti e le sanzioni Consob, respingendo il ricorso di Edipro nella vicenda che riguardava la cessione di oltre 15 milioni di posizioni anagrafiche a Fastweb senza aver prima raccolto il consenso degli interessati e condannando, dunque, la società, a pagare la sanzione amministrativa decisa dal garante anche se la notificazione della violazione era arrivata oltre i 90 giorni, vista la difficoltà dell'accertamento.

3.6 Il doppio binario sanzionatorio

Un problema attinente al rispetto del principio di proporzionalità, inteso qui come adeguatezza della sanzione, che consiste nella valutazione della scelta finale in termini di tollerabilità della restrizione o incisione nella sfera giuridica del destinatario del provvedimento, si pone in relazione alla tematica del doppio binario sanzionatorio.

A tal proposito risulta di un certo interesse Cassazione civile, sez. VI, 6 marzo 2018, n. 5341, che, nel pronunciarsi sul ricorso del Garante Privacy avverso la sospensione ex art. 295 c.p.c. del giudizio di opposizione ad una sanzione amministrativa inflitta dal Garante per un illecito trattamento di dati personali, disposta dal Tribunale di Palermo per essere pendente un giudizio penale avente ad oggetto i medesimi fatti, ha riconosciuto la regola del “doppio binario” punitivo tra procedimenti concernenti i medesimi fatti.

Al riguardo la Corte ha osservato che *“l'art. 162, comma 2 bis, nel disporre la sanzionabilità “altresì”, a titolo di illecito amministrativo (con riferimento al trattamento di dati personali effettuato in violazione delle misure indicate nell'art. 33 o delle disposizioni indicate nell'art. 167), introduce una ipotesi di doppia punibilità, con conseguente applicazione del cumulo materiale fra sanzioni di specie diversa, in deroga al principio di specialità di cui al primo comma della L. n. 689 del 1981, art. 9.*

Infatti, come già affermato da questa Corte, l'identità della condotta materiale integrante le fattispecie amministrativa e penale esclude quindi che l'esistenza del reato dipenda dall'accertamento della violazione amministrativa, e quindi la sussistenza della connessione obiettiva per pregiudizialità di cui alla L. n. 689 del 1981, art. 24, richiesta per radicare la competenza del giudice penale nell'accertamento della responsabilità per l'illecito amministrativo (nello stesso senso v. Sez. 2,

Sentenza n. 28381 del 22/12/2011 Rv. 620361 in fattispecie del tutto assimilabile, in cui pure si discuteva di doppia punibilità in relazione ad una condotta sottoposta a sanzioni amministrative e sanzioni penali). Ha dunque errato il Tribunale a ritenere sussistente caso di pregiudizialità penale di cui all'art. 24, di cui alla citata legge”.

Il doppio binario sanzionatorio pone numerose questioni problematiche.

In particolare è opportuno citare l'ordinanza di rinvio del 15 novembre 2016, n. 23232, con cui la seconda sezione della Corte di Cassazione, dovendosi pronunciare in materia di abuso di informazioni privilegiate, in un caso in cui le persone fisiche coinvolte erano state sottoposte dalla CONSOB a sanzione pecuniaria ex art. 187-bis t.u.f., pur essendo state assolve, in sede penale, dall'imputazione per il delitto di cui all'art. 184 t.u.f., ha posto alla Corte di giustizia i seguenti quesiti pregiudiziali: 1) se l'art. 50 della carta dei diritti fondamentali dell'Unione debba essere interpretato nel senso che, in presenza di un accertamento definitivo dell'insussistenza della condotta che ha integrato l'illecito penale, sia precluso, senza necessità di procedere ad alcun ulteriore apprezzamento da parte del giudice nazionale, l'avvio o la prosecuzione per gli stessi fatti di un ulteriore procedimento che sia finalizzato all'irrogazione di sanzioni che per la loro natura e gravità siano da qualificarsi penali; 2) se il giudice nazionale, nel valutare l'efficacia, proporzionalità e dissuasività delle sanzioni, ai fini del riscontro della violazione del principio del ne bis in idem di cui all'art. 50 della carta dei diritti fondamentali dell'Unione, debba tener conto dei limiti di pena posti dalla direttiva 2014/57/UE.

La Corte di giustizia, con sentenza del 20 marzo 2018, *Di Puma*, cause riunite C 596/16 e C 597/16, ha risposto alla prima questione (così come riformulata: “*se l'articolo 14, paragrafo 1, della direttiva 2003/6 osti a una disposizione nazionale, quale l'articolo 654 c.p.p., che estende al procedimento inteso all'irrogazione di una sanzione amministrativa pecuniaria l'autorità di cosa giudicata di tali affermazioni in punto di fatto, operate nel contesto del procedimento penale*”) statuendo che “*l'articolo 14, paragrafo 1, della direttiva 2003/6, letto alla luce dell'articolo 50 della Carta, va interpretato nel senso che esso non osta a una normativa nazionale in forza della quale un procedimento inteso all'irrogazione di una sanzione amministrativa pecuniaria di natura penale non può essere proseguito a seguito di una sentenza penale definitiva di assoluzione che ha statuito che i fatti che possono costituire una violazione della normativa sugli abusi di informazioni privilegiate, sulla base dei quali era stato parimenti avviato tale procedimento, non erano provati*”.

Tenuto conto della risposta data alla prima questione, il Giudice di Lussemburgo ha ritenuto che non occorresse procedere alla soluzione della seconda.

È interessante notare in proposito come la Corte sia giunta alla predetta conclusione guardando anche al rispetto del principio di proporzionalità (ragionamento che potrebbe essere replicato anche in materia di sanzioni del Garante Privacy). Osserva, infatti, che: “*l'obiettivo di proteggere l'integrità dei mercati finanziari e la fiducia del pubblico negli strumenti finanziari è tale da giustificare un cumulo di azioni come quello previsto dalla normativa nazionale oggetto del procedimento principale, ove tali azioni e sanzioni siano intese, in vista del conseguimento di detto obiettivo, a fini complementari aventi ad oggetto, eventualmente, aspetti diversi del medesimo comportamento costitutivo dell'infrazione in oggetto (v., in tal senso, sentenza pronunciata in data odierna, *Garlsson Real Estate*, C 537/16, punto 46). Tuttavia, la prosecuzione di un procedimento inteso all'irrogazione di una sanzione amministrativa pecuniaria di natura penale, come quello oggetto del procedimento principale, in esito alla definizione del procedimento penale è assoggettata al rigoroso rispetto del principio di proporzionalità (v., in tal*

senso, sentenza pronunciata in data odierna, Garlsson Real Estate, C 537/16, punto 48). (...) Orbene, in una situazione come quelle oggetto del procedimento principale, la prosecuzione di un procedimento inteso all'irrogazione di una sanzione amministrativa pecuniaria di natura penale eccederebbe manifestamente quanto necessario per conseguire l'obiettivo di cui al punto 42 della presente sentenza, una volta che esiste una sentenza penale definitiva di assoluzione che dichiara l'assenza degli elementi costitutivi dell'infrazione che l'articolo 14, paragrafo 1, della direttiva 2003/6 è inteso a sanzionare" (punti 42-44).

3.7 La giurisdizione del G.O.

La giurisdizione del g.o. sui provvedimenti (anche sanzionatori) del Garante, per come costruita, assume un ruolo determinante nel garantire una tutela effettiva dei diritti degli interessati: si tratta, infatti, di una giurisdizione esclusiva e di merito, che, quindi, da un lato, assicura che tutte le posizioni soggettive siano trattate dinanzi al medesimo giudice e, dall'altro lato, una cognizione piena sull'atto amministrativo.

3.7.1 Giurisdizione esclusiva

Se alla giurisdizione esclusiva del g.o. facevano già riferimento alcune pronunce del Consiglio di Stato, che avevano giudicato inammissibile il ricorso straordinario al Presidente della Repubblica avverso i provvedimenti del GPDP (Consiglio di Stato, parr. n. 4468 del 2007 e n. 3754 del 2008) e dichiarato la propria carenza di giurisdizione sui provvedimenti del GPDP (Consiglio di Stato, VI, 2 ottobre 2007, n. 5091), questa è stata definitivamente stabilita da Cass. civ., sez. un., 14 aprile 2011, n. 8487, che ha sancito la possibilità per il g.o. di conoscere anche degli interessi legittimi che possono venire in rilievo. In particolare, la Suprema Corte non ha condiviso quanto sostenuto dalla pronuncia del Consiglio di Stato oggetto di ricorso, secondo cui l'art. 152 D.Lgs. n. 196 del 2003 avrebbe lasciato fermo il tradizionale criterio di riparto della giurisdizione, fondato sulla distinzione tra diritti ed interessi, cosicché la giurisdizione del giudice ordinario, in tema di dati personali, potrebbe dirsi sussistente solo quando si controverta su diritti fondamentali (ad es., quelli al corretto trattamento od alla cancellazione dei dati), e non anche quando si controverta su interessi legittimi.

I giudici di legittimità, in proposito, hanno evidenziato come le norme del Codice non lascino *“marginari dubbi circa l'intentio legis di attribuire l'intera materia alla cognizione dell'AGO, senza eccezioni di sorta e senza che a ciò risulti di ostacolo la norma costituzionale di cui all'art. 103, più volte evolutivamente interpretata sia da questa stessa corte di legittimità (Cass. ss.uu. 3521/1994), sia dallo stesso Giudice delle leggi nel senso che anche alla predetta autorità giudiziaria è consentito, per effetto di conforme disposizione del legislatore ordinario, di conoscere di interessi legittimi, di conoscere ed eventualmente annullare un atto della P.A., di incidere conseguentemente sui rapporti sottostanti secondo le diverse tipologie di intervento giurisdizionale previste”* (Cort cost. ord. 140, 165 e 275/2001; 525/2002, mentre l'affermazione contenuta nella sentenza 204 del 2004, a mente della quale la cognizione degli interessi legittimi *“sarebbe riservata al giudice amministrativo”* sembra in realtà compiuta incidenter tantum, avendo la stessa Corte, con la sentenza 377 del 2008, espressamente riconosciuto al legislatore ordinario un margine di apprezzamento in materia di riparto di giurisdizione tra giudice ordinario e giudice amministrativo).

La Corte aggiunge anche che *“la scelta del legislatore ordinario, sicuramente inequivoca nella sua chiara espressione lessicale, appare poi, nel merito, perfettamente ragionevole, poiché la materia dell'accesso ai dati personali e dei costi di esercizio di tale diritto presenta una indiscutibile, reciproca,*

inestricabile interferenza di diritti e interessi legittimi, nella quale, peraltro, netta appare la prevalenza dei primi rispetto ai secondi. Nel caso di specie, oltretutto, non par lecito discorrere nemmeno di vera discrezionalità amministrativa, poiché il garante è chiamato ad operare un bilanciamento tra interessi privati (quelli degli interessati ai dati trattabili e quelli delle imprese detentrici), e non tra interesse privato e interesse pubblico”.

Spunti molto significativi possono trarsi anche da Cassazione civile, sez. VI, 2014, n. 18812/2014, che ha ribadito il carattere esclusivo della giurisdizione del g.o. nel caso di specie, laddove ha ricordato che il processo in tema di sanzioni amministrative secondo la legge n. 689 del 1981 “è costruito come processo di impugnazione di un atto amministrativo qual è l’ordinanza-ingiunzione, che è manifestazione di un caso di giurisdizione esclusiva (anche su interessi legittimi) dell’A.G.O. ai sensi dell’art. 113 Cost., u.c., e dunque come processo oppositivo. Come tale il processo nasce e la giurisdizione comincia con il ricorso in opposizione. Anteriormente vi è solo un procedimento di carattere amministrativo, sebbene a contenuto c.d. giustiziale, ma ad esso non possono applicarsi i principi in tema di notificazione alla parte costituita tramite difensore nel processo”.

3.7.2 Giurisdizione di merito: il giudizio sul rapporto e non sull’atto

Con riferimento alla configurabilità di una giurisdizione di merito, appare molto significativo quanto affermato da Cass. civ., 5 novembre 2012, n. 18929. Nella citata sentenza la Suprema Corte ha chiarito che, per quanto attiene alle controversie che riguardano l’applicazione del d.lgs. 196/03, come si evince dall’art. 152, comma 12, del suddetto decreto, si è in presenza di un’ipotesi di giurisdizione di merito del g.o. Il controllo giudiziale quindi non deve ritenersi limitato al mero sindacato di legittimità del provvedimento, ma deve riguardare il rapporto, su cui al giudice dell’opposizione spetta una cognizione piena [funzionale, quindi, ad una tutela effettiva].

Tanto è in linea con quanto affermato, più in generale, in merito al giudizio di opposizione al provvedimento sanzionatorio. Una siffatta opposizione, infatti, non configura un’impugnazione dell’atto amministrativo, ma introduce un ordinario giudizio sul fondamento della pretesa dell’autorità amministrativa. Pertanto l’opposizione alla pretesa anzidetta, una volta proposta, devolve al giudice adito la piena cognizione circa la legittimità e la fondatezza della pretesa stessa, con l’ulteriore conseguenza che, in virtù dell’art. 23 della legge n. 689 del 1981, il giudice ha il potere-dovere di esaminare l’intero rapporto, con cognizione che non è limitata alla verifica della legittimità formale dell’atto, ma si estende – nell’ambito delle deduzioni delle parti – all’esame completo del merito della pretesa fatta valere con l’ingiunzione, per stabilire se essa sia fondata o no e se lo sia in tutto o in parte.

In tale cognizione, ha specificato la Corte, rientra anche la determinazione dell’entità della sanzione, secondo i criteri stabiliti dall’art. 11 della legge, con apprezzamento discrezionale insindacabile in sede di legittimità se congruamente motivato e immune da errori logici o giuridici (così Cassazione civile, sez. II, 2/4/2015, n. 6778; v. anche Cass. n. 6020 del 2003).

In questo senso significativa è anche Cassazione civile, sez. II, 5 luglio 2018, n. 17665, la quale, proprio partendo dalla premessa che il giudice è chiamato alla ricostruzione dell’intero rapporto sanzionatorio e non soltanto alla valutazione di legittimità del provvedimento irrogativo della sanzione (cfr., sia pure con riferimento alla L. 24 novembre 1981, n. 689, art. 23, comma 6, *ratione temporis* applicabile, Cassazione civile, sez. 6, 11/03/2015, n. 4898), ha tratto la conclusione che “nel giudizio di opposizione a sanzione amministrativa, grava sull’amministrazione opponente l’onere di provare gli elementi costitutivi dell’illecito, ma la sua inerzia processuale non determina l’automatico accertamento

dell'infondatezza della trasgressione”.

3.8 Il controllo dell'AGO sui provvedimenti sanzionatori

3.8.1 Premessa: distinzione tra provvedimenti sanzionatori ed altri provvedimenti

Prima di affrontare alcune questioni attinenti ai poteri di controllo giurisdizionale circa la misura della sanzione, appare utile ricordare che, al fine di stabilire la disciplina applicabile nonché i soggetti legittimati all'azione, il giudice di merito è preliminarmente chiamato a verificare se il provvedimento impugnato possa effettivamente rientrare nel novero dei provvedimenti sanzionatori.

Al riguardo, si può fare riferimento a Cassazione civile, sez. I, 4 febbraio 2016, n. 2196, che, in relazione alla misura assunta dal Garante, il quale, al fine di eliminare o ridurre il disagio derivante dal fenomeno delle telefonate “mute”, aveva imposto a Enel Energia s.p.a., quale titolare del trattamento, di adottare tutte le misure, anche di carattere tecnico, idonee a garantire che il sistema impedisse la reiterazione di chiamate di tal genere (escludendo specificamente la possibilità di richiamare la singola utenza per un intervallo di tempo pari almeno a trenta giorni), ha ritenuto *“una prescrizione simile, tesa a contrastare fenomeni considerati lesivi del diritto al trattamento dei dati personali o a ridurre l'impatto in ambiti considerati fisiologici, non integra una sanzione amministrativa, e il soggetto legittimato all'opposizione non è qualunque titolare del trattamento, ma lo specifico titolare al quale la prescrizione sia stata imposta. Questo perché il rimedio oppositorio è diretto a sottoporre al controllo giurisdizionale la situazione soggettiva sulla quale il provvedimento ha inciso”*.

Ne consegue, secondo la Corte, l'inesistibilità in via automatica al provvedimento delle disposizioni della L. n. 689 del 1981, non essendosi dinanzi a una sanzione amministrativa.

Anche Cassazione civile, sez. I, 30 maggio 2016, n. 11140, ha avuto modo di affrontare la tematica in questione in relazione al provvedimento cautelare dell'Autorità Garante per la protezione dei dati personali che censurava la procedura adottata dalla RAI Radiotelevisione italiana S.p.A. per procurarsi i dati personali degli acquirenti al fine di ottenere nuovi abbonamenti. In particolare, il Garante, a fronte di una attività di raccolta e trattamento dei dati personali in violazione di legge (acquisiti e trasmessi dai commercianti alla RAI anziché al titolare) aveva adottato un provvedimento cautelare di natura non sanzionatoria, segnalando al titolare ed al responsabile le modifiche opportune al fine di rendere il trattamento conforme alle disposizioni vigenti.

La Corte ha rilevato che *“come sostenuto dal Garante ed irreprensibilmente accertato dal Giudice di primo grado, il provvedimento in questione, dato in primis il relativo tenore letterale, si sostanziava in manifestazione d'intento non direttamente autoritativo ed interdittivo ma persuasivo, attraverso la motivata segnalazione, reputata necessaria e rivolta all'Agenzia delle Entrate ed alla società RAI, la prima quale titolare e la seconda quale responsabile dei trattamenti - qualità coerenti con la normativa di riferimento e pure evidenziate dalle concessioni tra l'Amministrazione delle Finanze e la RAI di cui ai decreti del Ministro delle Finanze del 23.12.1988 e del 23.07.1999 – dell'opportunità di desistere dall'iniziativa di non consentite modalità e dall'ulteriore trattamento dei dati personali così raccolti; in tale funzione l'atto aveva in effetti legittimamente assunto la veste tipica del provvedimento (già previsto dalla L. n. 675 del 1996, art. 31 lett. c) (e non l)), (cfr anche l'art. 16, del regolamento di cui al D.P.R. n. 501 del 1998)”*. Il provvedimento, pertanto, non poteva ritenersi atipico, né viziato nel merito, per eccesso di potere o per violazione delle regole legali che presiedevano alla relativa adozione.

3.8.2 Le valutazioni del giudice di merito circa la misura della sanzione amministrativa in funzione dell'effettività della tutela e del principio di proporzionalità

La giurisprudenza è costante nell'affermare che la valutazione in ordine alla congruità della sanzione in concreto comminata dall'autorità di vigilanza per gli illeciti amministrativi contestati è attività rimessa in via esclusiva al giudice del merito (Cassazione civile, sez. II, 2/4/2015, n. 6778)

Quanto ai parametri indicati dall'art. 11, l. n. 689 del 1981, Cassazione civile, sez. II, 7 marzo 2018, n. 5357 (in risposta al motivo di ricorso che denunciava la violazione della L. n. 689 del 1981, art. 11 in relazione alla mancata considerazione del concreto esito dell'operazione ai fini della sanzione irrogata dalla Consob), ha riaffermato da ultimo il principio secondo cui *“nel procedimento di opposizione avverso le sanzioni amministrative pecuniarie, il giudice ha il potere discrezionale di quantificarne l'entità, entro i limiti sanciti dalle relative disposizioni di legge, allo scopo di commisurarla all'effettiva gravità del fatto concreto, globalmente desunta dai suoi elementi oggettivi e soggettivi, senza che sia tenuto a specificare i criteri seguiti, dovendosi escludere che la sua statuizione sia censurabile in sede di legittimità ove quei limiti siano stati rispettati e dalla motivazione emerga come, nella determinazione, si sia tenuto conto dei parametri previsti dalla L. n. 689 del 1981, art. 11 quali la gravità della violazione, la personalità dell'agente e le sue condizioni economiche (Cass. 28.2.2016 n. 2406)”*.

Si tratta di un principio consolidato nella giurisprudenza della Suprema Corte: al riguardo, basti citare Cassazione civile, sez. II, n. 765/2017, con riferimento ad un'opposizione avverso l'ordinanza ingiunzione con la quale il Ministero dell'Economia e delle Finanze aveva applicato una sanzione pecuniaria, che a sua volta richiama le sentt. nn. 5877/04, 9255/13, 6778/15, nonché Cassazione civile, sez. I, 8 febbraio 2016, n. 2406, che ha statuito su di una sanzione amministrativa pecuniaria irrogata dalla Banca d'Italia per violazione della legge bancaria.

Nella giurisprudenza di merito, un'applicazione della valutazione della sanzione alla luce del principio di proporzionalità può rinvenirsi nella decisione del Tribunale Cagliari, sez. I, 6 giugno 2017, n. 1569, che si è pronunciato su un provvedimento con cui il Garante aveva imposto alla società ricorrente (succeduta ad un'altra società in veste di titolare del trattamento) di richiedere nuovamente a tutti gli interessati un nuovo consenso al trasferimento dei loro dati personali e genetici.

Il ricorso faceva valere che il provvedimento rendesse oltremodo gravoso l'esercizio da parte della ricorrente di un'attività grazie alla quale trovano attuazione nell'ordinamento diritti e valori fondamentali aventi rango costituzionale, tra cui la dignità sociale (art. 3 Cost.), la ricerca scientifica (art. 9 Cost.) e il diritto alla salute (art. 32 Cost.).

La sproporzione tra la misura imposta e l'attività richiesta risultava, secondo la società ricorrente, ancor più evidente in considerazione del fatto che la banca dati oggetto di causa conteneva dati e informazioni su circa 11.700 persone, sparse in dieci comuni della Sardegna, con tutta una serie di problematiche relative, tra le altre, alla necessità di individuare l'attuale residenza o domicilio degli interessati ovvero il nome e la residenza o il domicilio dei loro eredi. Ricontattare tutti i soggetti coinvolti si prospettava dunque una soluzione estremamente difficile, se non impossibile, antieconomica e scarsamente funzionale alla tutela dei diritti degli interessati.

Il Tribunale ha ritenuto fondate le censure riguardanti l'assenza dei presupposti per l'adozione della misura del blocco e l'omesso bilanciamento degli interessi che vengono in rilievo nel caso concreto:

l'imposizione della misura del blocco del trattamento, motivata dalla necessità di acquisire una nuova

manifestazione del consenso, oltre che non prevista da alcuna disposizione avente carattere normativo, *“appare, ad avviso dello scrivente giudice, esorbitante rispetto alle finalità perseguite, di tutela dei soggetti che lo hanno originariamente prestato, tenuto conto di tutte le circostanze del caso concreto di cui si è detto (e quindi: a) del fatto che Società X persegue le medesime finalità di Shar DNA; b) del fatto che Società X è una società operante in campo internazionale nell'ambito della ricerca scientifica; c) del fatto che Società X, attraverso la costituzione della LonGevia Genomics s.r.l., si propone di operare stabilmente nel territorio sardo, per la prosecuzione del programma di ricerca scientifica, allo stato interrotto; d) del fatto che non vi è ad oggi motivo di ritenere che Società X o LonGevia Genomics s.r.l. si rendano responsabili di violazioni di norme di legge in materia di trattamento dei dati; e) del fatto che il singolo interessato può pur sempre esercitare i propri diritti in conformità alle disposizioni del Codice)”*.

3.8.3 Insindacabilità in sede di legittimità della valutazione discrezionale del giudice di merito

Con specifico riferimento all'entità delle sanzioni irrogate dal Garante Privacy, si può prendere in esame la sentenza della Corte di Cassazione n.17143/2016, in cui la Corte ha ritenuto inammissibile il motivo relativo alla entità della sanzione in concreto irrogata dall'Autorità *“perché diretto ad operare un sindacato sull'esercizio di un potere giurisdizionale discrezionale qual è quello della concreta verifica e validazione della quantità di sanzione applicabile al caso”*.

A fondamento di siffatta statuizione la Suprema Corte ha citato Cass. Sez. II, sentenza n. 6778 del 2015, che aveva chiarito come, in tema di opposizione a sanzione amministrativa, *“nel caso di contestazione della misura della stessa, il giudice è autonomamente chiamato a controllarne la rispondenza alle previsioni di legge, senza essere soggetto a parametri fissi di proporzionalità correlati al numero ed alla consistenza degli addebiti, e può reputare congrua l'entità della sanzione inflitta in riferimento ad una molteplicità di incolpazioni anche qualora escluda l'esistenza di alcune di esse, purché motivi in ordine all'apprezzamento della sostanziale ininfluenza sulla complessiva gravità dei fatti di quelle ritenute insussistenti”*. I giudici di legittimità fanno riferimento altresì a Cass. Sez. I, Sentenza n. 2406 del 2016 (su cui v. supra), valorizzando, pertanto, la necessità di commisurare la sanzione all'effettiva gravità del fatto concreto, che si realizza attraverso il potere discrezionale del giudice, da esercitare nel rispetto dei limiti posti dalla legge.

3.8.4 Applicazione del principio del concorso di violazioni continuate

Si può citare qui la pronuncia della Corte di Cassazione, del 24 giugno 2014, n. 14326, in cui la Corte era chiamata a pronunciarsi sulle sanzioni irrogate dal Garante a fronte della spedizione di messaggi promozionali da parte di una società in assenza di consenso. La Suprema Corte ha rigettato la tesi prospettata dalla ricorrente, secondo cui, anche a voler ritenere che i suoi comportamenti fossero distintamente sanzionabili, in quanto in violazione sia dell'art. 13 del codice sia degli artt. 23 e 130, il Garante avrebbe dovuto fare necessariamente applicazione del principio del concorso di violazioni continuate, con necessità dunque di applicazione della sanzione più grave aumentata fino ad un terzo.

La Suprema Corte ha in proposito ricordato che *“in tema di sanzioni amministrative, la L. n. 689 del 1981, art. 8 prevede che - salve le ipotesi di cui al comma 2, in materia di violazione delle norme previdenziali ed assistenziali - la sanzione più grave alimentata fino al triplo può essere irrogata nei soli casi di concorso formale, senza che possa ritenersi applicabile il medesimo meccanismo sanzionatorio alla fattispecie della continuazione di cui all'art. 81 c.p., comma 2, (Cass., Sez. 2, 8*

agosto 2007, n. 17347; Cass., Sez. 2, 4 marzo 2011, n. 5252)”.

3.8.5 [L'aggravante di cui all'art. 164 bis del D.Lgs. 196 del 2003](#)

Ai sensi dell'art. 164 bis, comma 3, *“In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni di cui al presente Capo sono applicati in misura pari al doppio”*.

La Corte di Cassazione, con pronuncia del 27 luglio 2017, n. 18619, in un caso che atteneva alla comunicazione a terzi di banche dati aventi ad oggetto dati personali avvenuta in assenza di informativa e consenso degli interessati, ha sancito l'applicabilità dell'aggravante di cui all'art. 164 bis del D.Lgs. 196 del 2003, nella parte in cui prevede l'aggravamento delle sanzioni per l'ipotesi in cui la violazione coinvolga numerosi interessati, a prescindere dal concreto impiego dei dati contenuti nel database.

Così statuendo i giudici di legittimità hanno riformato la pronuncia del Tribunale di Milano 5 febbraio 2014, n. 1748, che aveva invece ridotto la sanzione irrogata dal Garante, ritenendo inapplicabile al caso di specie l'aggravante di cui all'art. 164 bis, in quanto dall'istruttoria non era emerso l'effettivo numero di utenti raggiunti dagli sms elettorali. Il Tribunale, nella rideterminazione della misura della sanzione, aveva inoltre tenuto conto della limitata rilevanza economica del contratto intercorso tra le due società, dell'assenza a carico dell'autore della violazione di precedenti violazioni delle disposizioni in tema di trattamento dei dati personali, nonché delle condizioni economiche dell'agente

La Suprema Corte, dopo aver constatato che oggetto della sanzione era la *“cessione non autorizzata del database”* in assenza di preventiva informativa e del consenso degli interessati alla cessione dei loro dati, e non il successivo utilizzo delle utenze, hanno affermato che *“diviene quindi irrilevante, ed esula dall'oggetto dell'illecito contestato, la circostanza che poi i titolari dei dati ceduti siano stati effettivamente raggiunti da sms elettorali”*.

Ai fini dell'applicazione dell'aggravante di cui all'art. 164 bis, c. 3 del Codice in ipotesi di trasferimento di banca dati in assenza di consenso ed in violazione degli obblighi di informativa è sufficiente dunque la potenzialità del coinvolgimento di più soggetti interessati, a nulla rilevando l'effettivo utilizzo dei dati illecitamente ottenuti.

3.8.6 [Modifiche apportate dal D.Lgs. 101/2018](#)

A fronte di elevatissime sanzioni amministrative dettate dal regolamento, si è ritenuto di non potere mantenere alcune delle sanzioni penali le quali si sarebbero sovrapposte a quelle amministrative violando così il principio del *“ne bis in idem”*.

L'aspetto sanzionatorio è stato così ristrutturato: è stato rimodulato l'impianto il reato di *“trattamento illecito di dati”* (art. 167), sono state introdotte nuove fattispecie di reato (*“Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala”* e la *“Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala”*, declinata sempre in relazione a un numero rilevante di persone offese: cfr. artt. 167-bis e 167-ter); è stata confermata la fattispecie di cui all'articolo 168 (*“Falsità nelle dichiarazioni al Garante”*) e sostituito l'art. 170 relativo all'inosservanza di provvedimenti del Garante. Peraltro, il comma 2 dell'art. 168 punisce la condotta di interruzione o turbativa della regolarità di un procedimento innanzi al Garante o degli accertamenti svolti dall'Autorità ove si richiede un dolo intenzionale. Per quanto attiene alle misure minime di sicurezza, non più previste dal Regolamento, è stato abrogato l'art. 169: ne deriva che la violazione delle disposizioni in materia di

sicurezza sarà sanzionata con misure di carattere amministrativo-pecuniario, ai sensi degli art. 83, par. 5 del Regolamento. È prevista, poi, la cooperazione tra autorità giudiziaria e il Garante, che è competente per l'irrogazione delle sanzioni amministrative eventualmente coincidenti con l'area della rilevanza penale: qui interviene, peraltro, la disposizione del comma 6 (mutuata dall'art. 287-terdecies d.lgs. n. 58/1998) volta a disciplinare la possibile convergenza sul medesimo fatto di responsabilità e sanzioni penali e amministrative. Ed infatti, è stato previsto che *«quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita»*.

3.8.7 Rilievi conclusivi

Il giudice ordinario – adito in seguito all'impugnazione di un provvedimento emesso dall'autorità di controllo – è chiamato, a prescindere dai vizi relativi alla legittimità formale dell'atto, a valutare il merito dell'intero rapporto.

L'autorità di controllo, prima, ed il giudice civile, dopo, devono applicare il principio di proporzionalità anche per decidere se irrogare o meno una sanzione e non solo per determinare il *quantum* della stessa. Come previsto dal Considerando 148 del Regolamento, infatti, nei casi di violazione minore, la sanzione pecuniaria potrebbe essere sproporzionata e potrebbe essere proporzionato, invece, l'ammonimento. Occorre, comunque, interrogarsi sul potere del giudice di disporre l'ammonimento, anche se non richiesto dalla parte. L'applicazione dei principi di effettività e di proporzionalità chiede al giudice di rivalutare la scelta fatta dalla parte ed eventualmente, porre alle parti la questione ai sensi dell'art. 101 c.p.c., così da stimolare le parti sulla possibilità di scegliere un rimedio più proporzionato alla violazione commessa.

4 EFFETTIVITÀ DELLA TUTELA, PROPORZIONALITÀ E TUTELA RISARCITORIA

4.1 Premessa

Occorre premettere che il legislatore italiano non dà una definizione dei principi di effettività, proporzionalità e dissuasività. Il giudice si trova, in sede di scelta del rimedio e di valutazione sull'entità o la tipologia dello stesso, dinanzi alla necessità di motivare sugli elementi che portino a ritenere un determinato rimedio rispettoso dei tre predetti principi.

Nel presente capitolo, i principi di effettività e di proporzionalità verranno analizzati prendendo in esame le specificità dell'azione collettiva (con particolare riferimento alle questioni relative alle azioni esperibili, alla competenza per territorio ed alla legittimazione ad agire), nonché i profili relativi alla tutela risarcitoria. Proprio con riferimento a tale ultima questione, particolare attenzione verrà riservata all'esame del rapporto tra tutela ripristinatoria e tutela risarcitoria, nonché ai profili relativi all'onere della prova, ai criteri di determinazione dei danni ed alla valutazione della gravità della lesione ed alla serietà del danno.

4.2 Risarcibilità del danno per violazione dei dati personali

4.2.1 La questione

Al fine di garantire l'effettiva protezione dei dati personali all'interno dell'Unione europea e il pieno risarcimento delle vittime si può configurare l'esistenza di un "danno *in re ipsa*"?

4.2.2 La normativa previgente e le novità del D.Lgs. 101/2018

L'art. 15 del d.lgs. 30 giugno 2003, n.196 intitolato "*danni cagionati per effetto del trattamento*", prevedeva che: "*Chiunque cagiona danni ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'art. 11*". L'art. 11 della direttiva disciplinava le "*modalità del trattamento e requisiti dei dati*".

Tale disposizione è stata abrogata dall'art. 27 del D.Lgs. 101/2018 e l'art. 82, GDPR prevede che chiunque abbia subito un danno materiale o morale a seguito di una violazione del regolamento sulla protezione dei dati ha il diritto di ottenere dal responsabile del trattamento o dall'incaricato del trattamento il risarcimento dei danni subiti. Disposizioni più precise seguono la distinzione tra la responsabilità del responsabile del trattamento e quella dell'incaricato del trattamento. L'onere della prova relativo alla mancanza di responsabilità è posto a carico del responsabile del trattamento, analogamente a quanto disposto dalla direttiva 95/46/CE.

A differenza di altri atti legislativi dell'UE (ad esempio, la direttiva sui risarcimenti antitrust), il principio del risarcimento completo non viene richiamato. Per contro, il risarcimento del danno morale è

specificamente previsto.

4.2.3 [La giurisprudenza relativa alla normativa previgente](#)

La Suprema Corte, dopo aver chiarito che il significato della congiunzione "anche" utilizzata dal comma 2 del previgente art. 15 d.lgs. 196/2003 è quello di non confinare la risarcibilità del danno non patrimoniale alle ipotesi di pregiudizio conseguente ai fatti incriminati dalle disposizioni previste dallo stesso codice della privacy (art. 167, sul trattamento illecito di dati), ha ribadito la necessità di valutare l'accesso al risarcimento, che il legislatore ha ancorato alla "violazione dell'art. 11", in relazione alla verifica di gravità della lesione e serietà del danno (Cass. 15.7.2014 n. 16133). Nella pronuncia appena citata, la Corte ha precisato che *“dall'ambito applicativo dell'art. 11 sono escluse talune ipotesi (trattamento effettuato per scopi esclusivamente personali e rispetto a dati non destinati ad una comunicazione sistematica o alla diffusione; trattamento effettuato da soggetto non annoverabile tra le figure, di titolare e responsabile, tipizzate dagli artt. da 28 a 30 del codice), le quali, tuttavia, possono dar luogo (rispettivamente: la prima, per effetto della esplicita previsione dell'art. 5, comma 3, del codice; la seconda, per la clausola soggettiva generale del "chiunque" di cui al comma 1 dell'art. 15 del codice) ad un danno di natura non patrimoniale, la cui risarcibilità dovrà essere vagliata, già in punto di anti giuridicità della condotta, in base alle comuni regole sulla responsabilità aquiliana”*.

La Corte di Cassazione ha, inoltre, più volte ribadito che il danno da trattamento dei dati, come ogni altro tipologia di danno, non può ritenersi *“in re ipsa”*, ma che va allegato e provato con qualsiasi mezzo, incluse le presunzioni semplici e la prova testimoniale che attesti uno stato di sofferenza fisica o psichica (Cass., 26 settembre 2013, n. 22100; Cass., 25 settembre 2012, n. 16279; Cass. 10527/11).

Tuttavia, proprio l'ampio utilizzo delle presunzioni fa sì che spesso la giurisprudenza di merito si avvicini molto al desumere il danno dall'illecito. In tal senso, esemplificativamente, Trib. Bari, 23 luglio 2010, n. 2637 (in [Giurisprudenzabarese.it](#) 2010): *“l'illecito costituito dall'erronea segnalazione di un soggetto - nella fattispecie, libero professionista – (al registro dei cattivi pagatori) costituisce un fatto illecito, il quale, ai sensi degli art. 2043 e 2050 c.c., obbliga il segnalante al risarcimento dei danni. La risarcibilità del danno non patrimoniale è configurabile allorquando il fatto lesivo incida su una situazione giuridica relativa ai diritti fondamentali della persona umana garantiti dalla Costituzione, e fra tali diritti rientra l'immagine, ossia la diminuzione della considerazione della persona. Non c'è dubbio che tanto nel caso della persona fisica, quanto nel caso della persona giuridica, l'illegittima segnalazione è fonte di discredito per il "segnalato". E in ogni caso, a prescindere dall'attività economica eventualmente esercitata dal danneggiato, si riconosce come l'illegittima segnalazione possa determinare, oltre ad un danno patrimoniale, anche una lesione di fondamentali diritti del debitore, quali quello all'immagine ed alla reputazione. Con ciò non si deve però ritenere che si tratti di danno risarcibile "in re ipsa". Infatti, ogni qual volta emerga che la notizia lesiva risulti compresa nella banca dati della Centrale per un tempo sufficiente a consentirne la percepibilità da parte di coloro che vi hanno accesso, può ritenersi verificata la presunzione di un danno non patrimoniale in capo al segnalato, per la cui determinazione può procedersi in via equitativa”*.

In merito alla necessaria valutazione della gravità della lesione e serietà del danno, appare particolarmente significativa la già citata sentenza n. 16133/2014.

Detta pronuncia trae origine da un ricorso formulato ai sensi dell'art. 152 del d.lgs. 30 giugno 2003, n. 196, da alcuni studenti specializzandi nei confronti dell'Università di Roma Tre al fine di vedersi riconoscere il risarcimento del danno non patrimoniale cagionato da una asserita lesione del loro diritto

alla protezione dei dati personali. In particolare, secondo la narrativa dei ricorrenti, l'Università di Roma Tre, violando le disposizioni del suddetto decreto, si sarebbe resa responsabile di una illecita diffusione di dati personali e, più in generale, di una violazione dei principi di correttezza, pertinenza, finalità e necessità di cui al combinato disposto degli artt. 3 ed 11 del d.lgs 196/2003. L'Università di Roma Tre, invero, aveva pubblicato sul proprio sito istituzionale un documento in formato excel contenente, oltre ai nominativi degli studenti specializzandi, ulteriori dati quali il codice fiscale, l'attività di studio, la posizione lavorativa e la posizione retributiva. Ebbene, al documento poteva accedersi oltre che dal sito istituzionale dell'Ateneo, anche attraverso l'inserimento del nome e del cognome di ciascun interessato all'interno della maschera di ricerca di "Google". In primo grado il Tribunale di Roma, ravvisando una violazione delle disposizioni del Codice in materia di protezione dei dati personali, aveva accolto il ricorso ordinando la cancellazione dei dati personali contenuti nel documento, inibendone ulteriori forme di diffusione, e condannando l'Università Roma Tre al risarcimento dei danni non patrimoniali liquidati nella somma di euro 3.000,00 in favore di ciascun ricorrente.

Nell'esaminare i motivi di impugnazione interposti dall'Università Roma Tre, la Suprema Corte ha confermato la ricostruzione dei fatti operata in primo grado, ritenendo corretta la qualificazione del trattamento dei dati personali posto in essere dall'Università come illecito per violazione dei sopra citati principi. Ciò che tuttavia desta particolare interesse nella pronuncia sono le argomentazioni spese in ordine alla lesione derivante dal fatto illecito e al conseguente risarcimento dei danni. In particolare la Corte, dopo un'attenta esamina delle disposizioni del Codice Privacy e della tipologia di rimedi esperibili, ha espressamente affermato che: *“non la mera violazione delle prescrizioni poste dall'art. 11 determinerà, quindi, una lesione ingiustificata del diritto fondamentale alla protezione dei dati personali, ma soltanto quella che ne offenda in modo sensibile (e cioè oltre la soglia di tollerabilità) la sua portata effettiva, calata in un contesto in cui si combinano strettamente i diritti e le libertà contemplate dai primi due articoli del codice, perchè il risultato sia quello di una tutela piena della persona umana a fronte di un vulnus concreto ed effettivo, che, come tale, necessita di essere ristorato”*.

4.2.4 [La giurisprudenza europea](#)

Per quanto attiene alla giurisprudenza europea meritano di essere menzionate altre decisioni dei tribunali dell'UE nel settore del risarcimento dei danni morali degli interessati. In particolare, nella causa F-46/09 (V. e GEPD/Parlamento europeo), il Tribunale della funzione pubblica dell'UE ha affrontato la questione se l'annullamento di un atto del Parlamento (ossia la decisione di rigetto di un impiego) offerta basata sul trattamento illecito dei dati medici del candidato) può costituire di per sé stesso un risarcimento adeguato e, in linea di principio, sufficiente per il danno morale e, in caso contrario, in che modo la sua mancata osservanza i danni materiali dovrebbero essere valutati. Sulla base di una giurisprudenza consolidata dell'UE, il Tribunale conclude che l'annullamento dell'atto illegittimo dell'amministrazione non può costituire un risarcimento integrale per la mancata osservanza di tale obbligo:

- i) se tale atto contiene una valutazione delle capacità e del comportamento della persona:
- ii) se tale atto contiene una valutazione delle capacità e del comportamento della persona interessato che può offenderlo (cfr. sentenza del 7 febbraio 1990 nella causa C 343/87, causa C 343/87, Racc. 1990, pag. Culin/Commissione, punti 25-29, e nella causa Pierrat/Corte di giustizia, punto 62);
- iii) quando l'illegalità commessa è particolarmente grave (sentenze del 30 settembre 2004 nella causa T 16/03 Ferrer de Moncada/Commissione, punto 68, e del 7 luglio 2009 nelle cause riunite F 99/07 e F

45/08 Bernard contro Europol, punto 106);

iv) quando l'annullamento di un atto non ha alcun effetto pratico. effetto. Poiché il danno morale al ricorrente non è interamente risarcito.

Poiché il danno morale alla ricorrente non è stato interamente risarcito dal Tribunale di primo grado delle Comunità europee (Quinta Sezione), il Tribunale procede ad un'equa valutazione dell'importo di il risarcimento che il Parlamento deve versare al ricorrente per tale danno, alla luce in particolare, delle illegalità accertate e delle loro conseguenze. Questi due elementi possono essere comparati ai criteri di valutazione utilizzati nella decisione italiana esaminata in precedenza.

4.2.5 Rilievi conclusivi e questioni aperte

Non diversamente dall'art. 23, dir. 95/46/CE, l'art. 82, GDPR prevede che chiunque abbia subito un danno materiale o morale a seguito di una violazione del regolamento sulla protezione dei dati ha il diritto di ottenere dal responsabile del trattamento o dall'incaricato del trattamento il risarcimento dei danni subiti.

Il trattamento delle perdite non materiali è una questione su cui si applicano le legislazioni nazionali degli Stati Membri, che possono portare a risultati diversi a seconda della tradizione giuridica e delle norme, sia in punto di soluzioni concrete, che delle funzioni che si attribuiscono alla responsabilità civile. È dunque compito della dottrina e della giurisprudenza interrogarsi sul ruolo che potranno svolgere in questo ambito i principi di proporzionalità, effettività e dissuasività.

4.3 Nuove prospettive dell'azione collettiva

L'art 80 Reg. 2016/679 individua tre diverse tipologie di azione:

- un'azione collettiva a base *opt-in*, in cui gli interessati hanno il diritto di incaricare un ente autorizzato di presentare un reclamo a loro nome, di esercitare le azioni definite negli articoli 77, 78 e 79 del Regolamento;
- un'azione collettiva a base *opt-in*, in cui gli interessati hanno il diritto di incaricare un ente autorizzato di esercitare il diritto a ricevere un risarcimento solo se la legislazione dello Stato membro lo consente;
- un'azione collettiva a base *opt-out*, in cui le entità autorizzate sono autorizzate ad agire per conto degli interessati senza aver ottenuto un mandato da tali soggetti in caso di violazione dei diritti di una persona interessata ai sensi del regolamento, a condizione che lo Stato membro previsto una tale possibilità. Le richieste di risarcimento sono, tuttavia, escluse da questo meccanismo.

Il d.lgs 101/2018 ha introdotto, nell'art. 142 al d.lgs 196/2003 e nell'art. 10 del d.lgs. 150/2011, la possibilità per il soggetto titolare dei dati di dare mandato ad enti del terzo settore per agire in giudizio, rispettivamente, con un reclamo di fronte all'Autorità Garante dei dati personali e con un ricorso di fronte al tribunale civile.

4.4 La legittimazione ad agire

L'art. 80 Reg. 2016/679 individua come legittimati ad agire in nome e per conto dei titolari dei dati personali le associazioni e organismi no profit. Al fine di garantire che il soggetto rappresentativo agisca nell'interesse del gruppo tutelato e non per scopi personali, la normativa europea ha imposto criteri

reputazionali minimi, prevedendo che l'associazione o organizzazione:

- debba essere senza scopo di lucro;
- debba essere regolarmente costituita, secondo le norme nazionali applicabili;
- debba essere attiva nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali.

Il legislatore italiano ha seguito la medesima definizione riconoscendo legittimazione attiva, secondo il novellato art. 142 cod. privacy e art. 10 del d.lgs. 150/2011, agli enti del terzo settore costituiti ai sensi del d.lgs. 117/2017, e che siano attivi nel settore della protezione dei dati personali.

Per quanto attiene ad altre norme relative alla rappresentanza di interessi collettivi, il terzo requisito incluso nell'art. 80 può essere interpretato in modo restrittivo, poiché in pratica impone all'associazione o organizzazione no profit non soltanto di avere nel suo statuto l'obiettivo di tutela dei dati personali, ma di avere già svolto attività che si riferiscano a tale obiettivo. Da un lato, la scelta del legislatore europeo si muove verso una maggiore garanzia di competenza e di affidabilità dei soggetti legittimati ad agire; tuttavia, tale limitazione può essere problematica laddove, per esempio, l'organizzazione sia stata costituita a tutela degli interessi di altre categorie di soggetti, come per esempio i consumatori o i lavoratori. In questi casi, la protezione dei dati personali dei consumatori o dei lavoratori potrebbe non essere né esplicitamente definita negli obiettivi statuari, né essere stata oggetto di precedente attività. Dunque, potrebbe limitarsi la legittimazione attiva nei confronti di soggetti che possono d'altronde garantire sia la competenza sia la finalità di tutela dei diritti e delle libertà degli interessati.

Sperabilmente, ulteriori elementi saranno offerti dalla decisione della CGUE nel *caso Fashion Id.* (C-40/17) in cui il rinvio della corte tedesca di Düsseldorf include una questione relativa alla legittimazione attiva delle associazioni senza scopo di lucro che si occupino della tutela degli interessi dei consumatori in caso di violazione della normativa sulla protezione dei dati personali.

4.5 La competenza territoriale

Il Regolamento tace sulle norme procedurali da applicarsi in caso di azioni collettive, lasciando al legislatore nazionale piena discrezionalità. Per quanto riguarda il foro applicabile, un'esplicita indicazione proviene dall'art. 79(2) del Regolamento, dove si prevede espressamente che i ricorsi (individuali) dinanzi alle autorità giurisdizionali debbano essere promossi nello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente.

Il legislatore italiano ha riprodotto la norma del Regolamento relativa alle azioni individuali stabilendo, nel novellato art. 10 del dlgs 150/2011 che *“Sono competenti, in via alternativa, il tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell'interessato.”* Tuttavia, nel prosieguo della norma, il legislatore ha ommesso di specificare se e come la stessa debba adattarsi al caso di azioni collettive. Infatti, in caso di plurimi soggetti mandatari rispetto all'ente del terzo settore, potrebbe essere difficilmente applicabile l'alternativa fra competenza del tribunale del luogo di residenza o stabilimento del titolare del trattamento e quella del tribunale del luogo in cui ha residenza l'interessato, poiché per esempio all'azione potrebbero partecipare soggetti aventi residenza in luoghi diversi. Dunque, salvo lasciare all'associazione libera scelta circa il tribunale

di residenza di uno o più dei mandatarî, potrebbe essere ragionevole interpretare la norma individuando la competenza del tribunale del luogo di residenza o stabilimento del titolare del trattamento.

4.6 Effetti delle decisioni

L'azione collettiva potrà dunque risultare in una decisione che affermi la violazione delle norme relative ai dati personali tale da permettere l'irrogazione di una sanzione amministrativa pecuniaria ovvero il risarcimento del danno nei confronti dei soggetti interessati.

Laddove la condotta del titolare del trattamento sia dunque qualificata come lesiva dei diritti degli interessati mandatarî dell'azione collettiva, quali effetti potrà avere tale declaratoria nei confronti dei soggetti che non hanno partecipato all'azione? Alla luce della lettera dell'art 80(2) del Regolamento, appare evidente che il legislatore europeo ha riconosciuto la possibilità che gli Stati Membri possano adottare norme che permettano la rappresentanza degli interessi indipendentemente da forme di mandato. Questo permetterebbe, dunque, alle associazioni e organismi no profit di presentare azioni declaratorie della violazione delle norme sulla protezione dei dati personali cui possano seguire azioni c.d. *follow-on* da parte dei singoli consumatori al fine di ottenere eventuale risarcimento circa i danni sofferti in ragione della violazione. Purtroppo, il legislatore italiano ha escluso tale ipotesi consentendo esclusivamente l'opzione di azioni collettive basate sul sistema *opt-in*. In tali casi, la decisione del Garante così come quella del tribunale potrà avere effetto giuridico nei confronti dei soli interessati mandatarî dell'azione.

È interessante osservare che nel quadro degli interventi europei relativi alle azioni collettive, un approccio ben più efficace è stato adottato nella proposta di direttiva relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori (COM/2018/184 final - 2018/0089 (COD)). In questo caso, infatti, l'art. 10 della proposta di direttiva afferma che, in caso di decisione definitiva di un organo giurisdizionale o amministrativo declaratoria, in sede di azione collettiva, della violazione da parte di un operatore commerciale delle norme relative alla protezione dei consumatori, tale decisione costituirà "*prova inconfutabile nelle azioni di natura risarcitoria (all'interno dello stesso Stato membro) o una presunzione relativa dell'avvenuta violazione (per le cause intentate in un altro Stato membro)*". Appare evidente che in questo caso, il legislatore ha recepito le problematiche sorte a seguito dei casi di violazione occorsi negli Stati Membri, primo fra tutti il caso *Dieseldgate*, laddove infatti la tutela collettiva degli utenti si è scontrata con la difficoltà di riconoscere degli effetti alle decisioni delle autorità garanti della concorrenza dei singoli stati rispetto alle azioni collettive relative alle medesime violazioni.

Tale diverso approccio non è però scevro di conseguenze nell'applicazione pratica, poiché possono ben presentarsi casi in cui vi sia una sovrapposizione fra lo status di consumatore e quello di titolare dei dati personali, così come ha chiaramente dimostrato il caso *Schrems II* (C-498/16) di fronte alla CGUE. Per esempio una azione collettiva focalizzata sulla vessatorietà di clausole contrattuali, quali la c.d. *privacy policy* annessa come contenuto contrattuale in numerosi termini di servizio per i servizi della società dell'informazione, potrebbe avere la possibilità di garantire sia ai partecipanti all'azione di ottenere il riconoscimento della condotta lesiva dell'operatore commerciale (e in questo caso titolare del trattamento) e conseguentemente il risarcimento per i danni provocati dalla stessa condotta, ma anche permettere ai consumatori che si trovino nelle stesse condizioni contrattuali di utilizzare la decisione quale prova inconfutabile per presentare equivalenti azioni di risarcimento dei danni sofferti. Lo stesso non potrebbe accadere invece nel caso di azioni collettive nei confronti dello stesso operatore

commerciale laddove venga contestata la violazione delle norme a tutela della protezione dei dati personali. Dunque, potrebbe emergere una situazione di disparità di tutela giurisdizionale non giustificata da differenze di natura sostanziale rilevanti.

4.7 Rilievi conclusivi

Il rimedio risarcitorio si accompagna, nel disegno del legislatore del codice, ad una tutela inibitoria composita, che rende suscettibile di graduare la risposta in funzione delle concrete esigenze di salvaguardia dell'interessato. Vi è, dunque, una sinergia tra tutela preventiva (eminentemente inibitoria) e quella risarcitoria che il legislatore, nel costruire l'apparato rimediabile, ha tenuto presente, così da far convergere la seconda là dove il pregiudizio risulti attuale, effettivo ed apprezzabile e laddove la lesione risulti seria e di apprezzabile gravità. Alla luce del principio di effettività, occorrerà interrogarsi sulla possibilità di garantire un rimedio effettivo attraverso la tutela risarcitoria, con particolare riferimento a quei casi nei quali la lesione del diritto alla protezione dei dati personali si consuma istantaneamente, con effetti destinati a moltiplicarsi in ragione del passare del tempo.

In applicazione dei principi affermati dalle Sezioni Unite in materia di nullità negoziali (cfr. Cass. SS.UU. 12.12.2014 n. 26242) il giudice potrebbe anche rilevare la non dissuasività e la non proporzionalità del rimedio?

Con riferimento alle azioni collettive, invece, solo l'esame delle prime azioni e delle successive decisioni consentirà di chiarire le peculiarità di tale strumento (solo un mezzo processuale di tutela che si aggiunge a quello ordinario spettante al singolo interessato?), il rapporto con le azioni individuali, le differenze in rito delle due forme processuali di tutela e le conseguenze in termini di tutela effettiva.