ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

3 NOVEMBRE 2021

La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo *nomofilattico* del Comitato europeo per la protezione dei dati personali

di Francesco Parodo
Magistrato ordinario

La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo *nomofilattico* del Comitato europeo per la protezione dei dati personali*

di Francesco Parodo
Magistrato ordinario

Abstract [It]: L'articolo esamina i mezzi di tutela amministrativi e giurisdizionali posti a presidio del diritto alla protezione dei dati personali, focalizzando l'attenzione sia sui contenuti normativi che sull'effettività dei rimedi. Alla luce della rete di interazioni fra i Garanti della *privacy* nazionali, tra cui in particolare il Comitato europeo per la protezione dei dati, si ritiene che in tale materia si sia verificato un rimarchevole sviluppo dell'integrazione europea.

Abstract [En]: The article deals with the right to the protection of personal data and its administrative and judicial safeguards, focusing on both normative and empirical problems. Because of the bonding among the national supervisory authorities, improved also by the European Data Protection Board, the A. concludes that a remarkable development of the european integration happened.

Parole chiave: diritto alla protezione dei dati personali; tutela amministrativa e giurisdizionale; meccanismi di cooperazione e di coerenza; Comitato europeo per la protezione dei dati personali; integrazione europea
Keywords: right to the protection of personal data; administrative and judicial safeguards; Cooperation and consistency mechanisms; European Data Protection Board; european integration

1. Il processo di integrazione europea attraverso la lente della *Data protection*

La pervasività della rete Internet, la moltiplicazione dei dispositivi in grado di raccogliere dati personali, l'avanzamento tecnologico di *software* e algoritmi in grado di processarne imponenti quantità[1], sono le

* Articolo sottoposto a referaggio.

[1] In riferimento a tali dispositivi, v. la lungimirante riflessione già contenuta in S. RODOTÀ, *Prefazione*, in *Libera circolazione e protezione dei dati personali*, R. Panetta (a cura di), tomo 1, Milano, Giuffrè, 2006, pp. XIII e XIV. *Cfr.*, altresì, F.

cause principali dell'incremento esponenziale dei dati relativi a ogni persona[2]. L'analisi di tali informazioni[3], spesso raccolte in grandi insiemi – i *Big data*[4] – può fornire indicazioni, finanche in chiave predittiva[5], sui comportamenti individuali e collettivi. Questo patrimonio informativo – dotato peraltro di inestimabile valore economico[6] e potenzialmente utilizzabile per influenzare le consultazioni elettorali[7]

GIOVANELLA, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, p. 1213 e ss.

[2] Su tutti questi aspetti v. S. CALZOLAIO, L. FEROLA, V. FIORILLO, E.A. ROSSI, M. TIMIANI, *La responsabilità e la sicurezza del trattamento*, in *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, L. Califano, C. Colapietro (a cura di), Napoli, Editoriale Scientifica, 2017, p. 137 e ss. Per una illustrazione dei tre livelli in cui si sviluppa il processo di datificazione della società (c.d. *datification*), v. S. CALZOLAIO, *Protezione dei dati personali*, in *Dig. disc. pubbl., aggiornamento*, Torino, Utet, 2017, pp. 598 e 599. Più in generale sul concetto di *datification* v. R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, p. 65 ss.

[3] I termini "dati" e "informazioni" personali, spesso usati come sinonimi, indicano in realtà oggetti diversi. A stretto rigore, come precisa efficacemente S. CALZOLAIO, *Protezione dei dati personali*, cit., pp. 598, «*Il dato (informatico) non è che una consecuzione, in forma elettronica, di bit. L'informazione, invece, rappresenta il significato che si può trarre a partire dalla osservazione di uno o più dati connessi*». Sulla distinzione fra dati e informazioni v. anche C. DEL FEDERICO, A.R. POPOLI, *Disposizioni generali*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. Finocchiaro (a cura di), Torino, Zanichelli, 2017, p. 60.

[4] Il termine "*Big data*", secondo S. CALZOLAIO, *Protezione dei dati personali*, cit., p. 599, non ha ad oggi un significato «*univoco e accettato*». Fra le caratteristiche generalmente riconosciute all'espressione, comunque, vi sono l'elevatissima quantità di dati e l'alta capacità di elaborarli e analizzarli. La produzione scientifica in materia è vasta, di seguito si segnalano alcuni contributi sufficienti, quantomeno, per inquadrare il problematico rapporto fra riservatezza e *Big data*: A. MANTELERO, *La privacy all'epoca dei Big Data*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019; L. CALIFANO, *Brevi riflessioni su privacy e costituzionalismo al tempo dei big data*, in *Federalismi.it*, 3 maggio 2017; A BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *Media Laws*, n. 3/2018; M. COPPOLA, F. GUERRIERI, *Art. 4. Definizioni*, in *GDPR e normativa privacy. Commentario*, G.M. Riccio, G. Scorza, E. Belisario (a cura di), Milano-Vicenza, Wolters Kluwer, 2018, p. 47 e ss.; G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, Giappichelli, 2017; E. GIOVANNINI, *La rivoluzione dei big data a sostegno dell'Agenda 2030*, in *Equilibri. Rivista per lo sviluppo sostenibile*, n. 1/2016; L. BOLOGNINI, *Principi del trattamento*, in *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, L. Bolognini, E. Pelino, C. Bistolfi, Milano, Giuffrè, 2016, p. 103 e ss.; M. MAGGIOLINO, *Big data e prezzi personalizzati*, in *Concorrenza e mercato*, fasc. n. 1/2016; I.S. RUBINSTEIN, *Big Data: The End of Privacy or a New Beginning?*, in *International Data Privacy Law*, vol. 3, n. 2/2013.

[5] S. CALZOLAIO, *Protezione dei dati personali*, cit., pp. 599, 603 e 605.

[6] Come sottolineato da C. D'CUNHA, *Idee di Giovanni Buttarelli, trascritte da Christian D'Cunha*, in *Privacy 2030. Una nuova visione per l'Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, novembre 2019, reperibile al *link* garanteprivacy.it, p. 27, «*I flussi digitali oggi impattano sulla crescita economica ben più degli scambi commerciali*». Sul valore economico dei dati personali v. anche: G.M. SALERNO, *Le origini ed il contesto*, in *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, L. Califano, C. Colapietro (a cura di), Napoli, Editoriale Scientifica, 2017, p. 71; G. BUSIA, *Le frontiere della privacy in Internet: La nuova corsa all'oro per i dati personali*, in *Internet: Regole e tutela dei diritti fondamentali*, O. Pollicino, E. Bertolini, V. Lubello (a cura di), Roma, Aracne, 2013, pp. 29 e 30; M.C. MENEGHETTI, *Trasferimenti di dati personali verso Paesi terzi o Organizzazioni internazionali*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. Finocchiaro (a cura di), Torino, Zanichelli, 2017, p. 424; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, p. 23 e ss.; A. DE FRANCESCHI, *Il «pagamento» mediante dati personali*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, p. 1381 e ss.

[7] In proposito v., fra i tanti: K. MANHEIM, L. KAPLAN, *Artificial Intelligence: Risks to Privacy and Democracy*, in *Yale Journal of Law & Technology*, vol. 21, 25 ottobre 2018, p. 133 e ss.; M. FASAN, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *Rivista di BioDiritto*, n. 1/2019, p. 101 e ss.; B. CARAVITA, *Social network, formazione del consenso, istituzioni politiche: quale regolamentazione possibile?*, in *Federalismi.it*, 23 gennaio 2019; D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "*Cambridge Analytica*"*, in

– è concentrato nella disponibilità di poche multinazionali informatiche[8], le quali, gestendolo in regime di oligopolio e su scala mondiale, detengono un immenso potere[9]. L'influenza del fenomeno descritto

Federalismi.it, 24 ottobre 2018; S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, Luiss University Press, 2019; L. CALIFANO, *Autodeterminazione vs. eterodeterminazione dell'elettore: voto, privacy e social network*, in *Federalismi.it*, 7 agosto 2019, *passim*; B. KAISER, *La dittatura dei dati*, Milano, HarperCollins, 2019; P. MARSOCCI, *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?,* in *Rivista AIC*, n. 1/2015; E. ASSANTE, *Cosa ci può insegnare il caso Cambridge Analytica*, in *Federalismi.it*, 25 aprile 2018; L. CALIFANO, *Brevi riflessioni su privacy e costituzionalismo al tempo dei big data*, cit.; P. CIARLO, *Democrazia, partecipazione popolare e populismo al tempo della rete*, in *Rivista AIC*, n. 2/2018. Come ha efficacemente scritto S. RODOTÀ, *Data Protection as a Fundamental Right*, in *Reinventing Data Protection?*, S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, S. Nouwt (a cura di), Springer, 2009, p. 82, «*any changes affecting data protection impact on the degree of democracy we all can experience*».

[8] Si concentra invece sul potere di sorveglianza degli Stati M. ROTENBERG, *Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection*, in *European Law Journal*, 11 settembre 2020, p. 1 e ss., reperibile al *link* onlinelibrary.wiley.com. Sulle potenzialità dell'analisi dei dati personali per l'elaborazione di politiche pubbliche v. G. ORSONI, E. D'ORLANDO, *Nuove prospettive dell'amministrazione digitale: Open Data e algoritmi*, in *Istituzioni del Federalismo*, n. 3/2019, p. 593 e ss.

[9] C. SARTORETTI, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in *Federalismi.it*, 3 luglio 2019, p. 5; M. MIDIRI, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in *Federalismi.it*, 13 maggio 2020, p. 209 e ss.; M.E. STUCKE, *Should We Be Concerned About Data-opolies?*, in *Georgetown Law Technology Review*, vol. 2, n. 2/2018, p. 275 e ss. Come osserva R. BIN, *Critica della teoria dei diritti*, Milano, Franco Angeli, 2018, p. 133, con la globalizzazione sembrano rinnovarsi rivendicazioni proprie del passato, come la richiesta dei privati di una tutela pubblica contro lo strapotere di altri (dominanti) privati. S. ZUBOFF, *Molte sfaccettature di un solo diamante*, in *Privacy 2030. Una nuova visione per l'Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, novembre 2019, reperibile al *link* garanteprivacy.it, p. 48, definisce le grandi multinazionali di Internet – l'A. menziona espressamente Google, Facebook, Amazon e Microsoft – «*capitalisti della sorveglianza*». V. *amplius* anche IID., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, cit., *passim*. In proposito v. anche C. CASONATO, *Potenzialità e sfide dell'intelligenza artificiale*, in *Rivista di BioDiritto*, n. 1/2019, p. 177 e ss.

sulla sfera pubblica (oltre che su quella privata)[10] ha indotto ad affermare che sia oggi in corso una «*rivoluzione digitale*»[11] in grado di inaugurare una nuova stagione del costituzionalismo[12].

In questo quadro, la protezione dei dati personali si rivela uno strumento fondamentale per consentire il libero sviluppo della personalità individuale[13]: esso, difatti, preserva nel nuovo millennio l'esercizio incondizionato dei diritti su cui si basa la cittadinanza democratica[14]. Ma quali istituzioni possono assicurarne l'effettività? Può lo Stato-nazione garantire ancora una tutela del diritto nell'era della globalizzazione informatica? E quale ruolo avrà in futuro l'Unione europea nella protezione dei dati personali?

La ricerca di risposte a tali quesiti deve muovere, in via preliminare, dallo studio dei principali strumenti apprestati dall'ordinamento per la tutela del diritto in esame. Una volta analizzato il regime giuridico e il funzionamento in concreto dei rimedi, occorrerà soffermare l'attenzione sui meccanismi introdotti dal regolamento (UE) 2016/679 per assicurare, sul piano applicativo, l'uniformità della disciplina europea di *Data protection* in tutto il territorio dell'Unione[15]. Alla luce di questi elementi, infine, sarà possibile valutare l'*iter* del processo di integrazione europea in questa materia, e tentare di immaginarne i possibili sviluppi.

---

[10] La *Data protection* ha infatti una duplice rilevanza quale diritto soggettivo e, al contempo, interesse della collettività. Quest'ultimo non attiene al solo piano nazionale, coinvolgendo altresì l'esistenza di un interesse pubblico europeo alla regolazione dei dati personali: in proposito v. S. CALZOLAIO, *op.cit.*, pp. 626 e 635; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, vol. 2, Torino, Giappichelli, 2016, p. 4. L'importanza del diritto in esame in una dimensione collettiva è legata al contrasto di eventuali derive *orwelliane* verso società del controllo digitale: in questo senso, S. RODOTÀ, *Data Protection as a Fundamental Right*, cit., p. 82, ha evidenziato: «*reinventing data protection is an unrelenting process that is indispensable not only to afford adequate protection to a fundamental right but also to prevent our societies from turning into societies of control, surveillance and social selection*». *Conf.* anche: F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, vol. 1, Torino, Giappichelli, 2016, p. 12; S. RODOTÀ, *Prefazione*, cit., pp. VII e X; S. ZUBOFF, *Molte sfaccettature di un solo diamante*, cit., p. 47. Evidenzia i problemi della «*società sorvegliata*» anche S. CALZOLAIO, *op.cit.*, pp. 602 e 603. In letteratura nessun rimando può essere più efficace, per una rappresentazione della sorveglianza come strumento di controllo totale della società, di G. ORWELL, *1984*, Milano, Oscar Mondadori, 2002.

La duplice rilevanza del diritto – in realtà valida, nei sistemi democratici, per tutti i diritti fondamentali – risulta essere particolarmente marcata per quello alla protezione dei dati personali. *Cfr.* su questo punto: S. RODOTÀ, *Data Protection as a Fundamental Right*, cit., p. 82; S. CALZOLAIO, *op.cit.*, p. 611 e 612.

Sul rapporto fra il potere e la conoscenza che deriva dalle informazioni, infine, v. A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, in *I diritti fondamentali e le corti in Europa*, S.P. Panunzio (a cura di), Napoli, Jovene, 2005, p. 377 e ss. Più in generale, sui mutamenti dei meccanismi democratici e della sfera pubblica indotti dall'influenza di Internet v. G. GIACOMINI, *Potere digitale. Come Internet sta cambiando la sfera pubblica e la democrazia*, Milano, Meltemi, 2018.

[11] A. SIMONCINI, *Sovranità e potere nell'era digitale*, in *Diritti e libertà in Internet*, T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), Le Monnier Università, 2017, p. 20. L'A., peraltro, condivide che la performatività della Rete, l'aumento dei dispositivi in grado di raccogliere dati personali e lo sviluppo di *software* e algoritmi di analisi dei dati siano alla base della *rivoluzione digitale* in corso.

[12] *Ibidem*.

[13] Così S. RODOTÀ, *Data Protection as a Fundamental Right*, cit. pp. 80 e 82. *Conf.*: S. CALZOLAIO, *op.cit.*, p. 603; C. D'CUNHA, *Idee di Giovanni Buttarelli, trascritte da Christian D'Cunha*, cit., *passim*.

[14] S. RODOTÀ, *op.cit.*, pp. 80 e 82.

[15] Sull'evoluzione nel tempo della disciplina euro-unitaria della protezione dei dati personali v. G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Bruxelles, Springer, 2014. Sulla normativa

In quest'ordine di idee, i parr. 2, 3 e 4 analizzeranno i diversi mezzi di tutela – esperibili in modo alternativo[16] – posti a presidio del diritto alla protezione dei dati personali. Più specificamente, i tre principali rimedi invocabili in caso di violazione del diritto sono il reclamo all'autorità di controllo, il ricorso innanzi a un giudice avverso le decisioni di tale autorità, e il ricorso *diretto* all'autorità giurisdizionale ordinaria[17].

Sulla scorta dell'insegnamento dottrinale secondo cui la conoscenza dei contenuti normativi deve essere affiancata, ove possibile, allo studio della realtà pratico-applicativa[18], si tenterà di indagare il profilo dell'effettività dei predetti strumenti di tutela mediante l'elaborazione con tabelle e grafici delle informazioni ricavabili dalle relazioni del Garante della *privacy* relative agli anni dal 2009 al 2019[19]. L'interesse di una indagine empirica discende altresì dalla considerazione che, come già da tempo sottolineato in letteratura, la collaborazione fra le autorità indipendenti è un indice dell'avanzamento dell'integrazione europea[20]. Dalle relazioni annuali, peraltro, emerge come l'autorità di controllo nazionale – a cui gli artt. 8, par. 3, Carta di Nizza e 16, par. 2, TFUE affidano espressamente il compito di sorvegliare il rispetto delle regole sulla *Data protection*[21] – abbia assunto un ruolo centrale nella salvaguardia del diritto attraverso lo svolgimento di una pluralità di attività, segnatamente di natura consultiva, regolatoria, para-

attualmente vigente v. per tutti V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019.

[16] Art. 140 *bis*, co. 2 e 3, Codice della *privacy*. Sull'alternatività dei rimedi v. C. CIMAROSSA, *Artt. 77-79*, in *GDPR e normativa privacy. Commentario*, G.M. Riccio, G. Scorza, E. Belisario (a cura di), Milano-Vicenza, Wolters Kluwer, 2018, p. 583; A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di Internet*, in *Europa e Diritto Privato*, fasc. n. 4/2017, *passim*.
Secondo la giurisprudenza (Cass. Civ., Sez. L., sentenza 7 aprile 2016, n. 6775) «*In materia di trattamento di dati personali, il principio dell'alternatività del ricorso all'Autorità giudiziaria rispetto al ricorso al Garante, previsto nell'ipotesi in cui entrambe le suddette iniziative abbiano il "medesimo oggetto", per essere compatibile con l'art. 24 Cost. deve essere inteso nel senso che può applicarsi solo quando le due domande siano tali che, in ipotesi di contestuale pendenza davanti a più giudici, potrebbero, in via generale, essere assoggettate al regime processuale della litispendenza o della continenza. Ne consegue che il detto principio non opera tutte le volte in cui, in sede giurisdizionale, si faccia valere l'inottemperanza, da parte del gestore del trattamento dei dati personali, ai provvedimenti assunti dal Garante, o venga proposta una domanda di risarcimento del danno, riservata all'esame del giudice ordinario e che ha "causa petendi" e "petitum" autonomi e diversi*».

[17] Fa riferimento a tale rimedio come tutela giurisdizionale «*diretta*» anche R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, pp. 1001 e 1011. V. anche A. CANDINI, *Gli strumenti di tutela*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. Finocchiaro (a cura di), Torino, Zanichelli, 2017, p. 570. Il diritto a un ricorso effettivo e a un giudice imparziale di cui all'art. 47 Carta di Nizza, è attuato dall'art. 152 decreto legislativo 30 giugno 2003 n. 196 con l'attribuzione all'autorità giudiziaria ordinaria delle controversie concernenti la *Data protection*. Sul punto v. *amplius infra* parr. 3 e 4.

[18] U. DE SIERVO, *Tutela dei dati personali e riservatezza*, in *Diritti, nuove tecnologie, trasformazioni sociali. Scritti in memoria di Paolo Barile*, Padova, Cedam, 2003, *passim*, secondo il quale è necessario che il giurista ponga alla base delle proprie valutazioni sia il dato positivo, sia le prassi applicative e le dinamiche conflittuali che ne derivano.

[19] Fonte dei dati: relazioni annuali del Garante per la protezione dei dati personali degli anni 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, reperibili al seguente *link* garanteprivacy.it.

[20] Così P. BILANCIA, F.G. PIZZETTI, *Aspetti e problemi del costituzionalismo multilivello*, Milano, Giuffrè, 2004, p. 154.

[21] Già l'art. 28 direttiva 95/46/CE disponeva l'istituzione in ciascun Paese membro di tali autorità di controllo.

giurisdizionale, ispettiva, sanzionatoria, di cooperazione sovranazionale e internazionale, nonché di studio e divulgazione[22].

Nei parr. 5, 6, 7 e 8, invece, si studierà come la tutela del diritto non si esaurisca in una dimensione esclusivamente nazionale, ma piuttosto coinvolga, in una prospettiva integrata, anche il livello euro-unitario. I rimedi amministrativi e giurisdizionali, infatti, si trovano al centro di una rete di interazioni fra i livelli statale ed europeo: saranno specificamente analizzati – sul piano amministrativo – l'istituto dell'autorità di controllo capofila, i meccanismi di cooperazione (artt. 60, 61 e 62 GDPR[23]) e quelli di coerenza (artt. 63, 64, 65, 66 e 70 GDPR) e – sul piano giurisdizionale – il rinvio pregiudiziale alla Corte di Giustizia (art. 267 TFUE e *considerando* n. 144 GDPR[24]) e la disciplina della sospensione delle azioni proposte presso diverse autorità giurisdizionali dei Paesi membri (art. 81 GDPR)[25]. Nel par. 9, infine, si tenterà di formulare alcune conclusioni in merito al rapporto fra la protezione dei dati personali e il processo di integrazione europea.

---

[22] Sull'essenziale ruolo del Garante della *privacy* nella protezione dei dati personali v.: F. PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in *Media Laws*, n. 1/2018, p. 1 e ss.; A. PATRONI GRIFFI, *L'indipendenza del Garante*, in *Federalismi.it*, 14 febbraio 2018; M. VIGGIANO, *L'attività cd. para-giurisdizionale nella casistica dei ricorsi proposti dinanzi al Garante per la protezione dei dati personali*, in *Rassegna di diritto pubblico europeo. Autorità indipendenti e tutela giurisdizionale nella crisi dello Stato*, n. 1-2/2015, p. 273 e ss.; M. CUNIBERTI, *Autorità indipendenti e libertà costituzionali*, Milano, Giuffrè, 2007, p. 221 e ss.; E. GUARDIGLI, *Le Autorità di controllo*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. Finocchiaro (a cura di), Torino, Zanichelli, 2017, p. 513 e ss.; C. DEL FEDERICO, A.R. POPOLI, *Disposizioni generali*, cit., p. 77; M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, in *Giornale di Diritto Amministrativo*, n. 4/2018, *passim*; M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. Finocchiaro (a cura di), Torino, Zanichelli, 2017, p. 516 e ss.; P. BILANCIA, F.G. PIZZETTI, *Aspetti e problemi del costituzionalismo multilivello*, cit., p. 143 e ss. e 165 e ss.; L. CALIFANO, *La protezione dei dati personali e il ruolo del Garante in ambito pubblico*, in *Media Laws*, n. 1/2018, p. 1 e ss. Più in generale, sulle autorità amministrative indipendenti v. per tutti: M. SANINO, *La tutela giurisdizionale nei confronti degli atti delle autorità indipendenti*, Milano, Padova, Wolters Kluwer, Cedam, 2019, p. 3 e ss.; AA.VV., *Le autorità indipendenti tra funzione regolativa e* judicial review, C. Iannello (a cura di), Napoli, Edizioni Scientifiche Italiane, 2018; M. SANINO, *L'approdo dell'esperienza delle autorità indipendenti a oltre venti anni dalla loro istituzione*, Padova, Cedam, 2015; F. MERUSI, M. PASSARO, *Le autorità indipendenti*, Bologna, Il Mulino, 2011; M. CUNIBERTI, *Autorità indipendenti e libertà costituzionali*, cit.

[23] In letteratura si suole fare riferimento al regolamento (UE) 2016/679 anche con l'acronimo GDPR (*General Data Protection Regulation*).

[24] Secondo l'opinione assolutamente maggioritaria, i *considerando* – ossia la serie di proposizioni che precedono l'articolato normativo – non hanno forza giuridica vincolante, ma sono essenziali per orientare l'interpretazione del testo normativo: ne costituiscono infatti parte integrante e ne spiegano la *ratio*. Anche nella giurisprudenza della Corte di Giustizia, peraltro, è ricorrente il principio secondo cui l'attività ermeneutica delle disposizioni deve avvalersi dei principi espressi dai *considerando*. Per approfondimenti si rinvia a: L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, cit., pp. 21 e 22; V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, pp. 11 e 12; C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., p. 91.

[25] Si tratta di istituti, molti dei quali introdotti dal regolamento (UE) 2016/679, principalmente volti a garantire l'uniformità applicativa della nozione europea di *Data protection*.

2. La tutela amministrativa del diritto alla protezione dei dati personali: il reclamo di cui all'art. 77 regolamento (UE) 2016/679 e l'abrogato ricorso *ex* art. 145 Codice della *privacy*

Fra i rimedi esperibili dall'interessato, il primo contemplato dal regolamento (UE) 2016/679 è il reclamo all'autorità di controllo[26]. L'art. 77 GDPR prevede, infatti, una tutela amministrativa azionabile dinnanzi all'Autorità Garante per la protezione dei dati personali, la quale può dispiegarsi avverso i trattamenti che non rispettino la disciplina sulla *Data protection*. L'individuazione dell'autorità di controllo competente è rimessa all'interessato, il quale può liberamente scegliere fra quella dello Stato membro in cui egli risiede abitualmente[27] o lavora, oppure quella del luogo ove si è verificata la presunta violazione[28].

In ogni caso, la proposizione del reclamo pone in capo all'autorità adita l'obbligo di informare il reclamante dello stato o dell'esito del procedimento, oltre che della possibilità di avvalersi del ricorso giurisdizionale di cui all'art. 78 GDPR. Inoltre, ai sensi dell'art. 140 *bis* co. 3 Codice della *privacy*, la presentazione del reclamo al Garante preclude la proponibilità all'autorità giudiziaria di una domanda tra le stesse parti e per il medesimo oggetto, salvo che sia inutilmente decorso il termine previsto per la decisione del reclamo o per informare l'interessato dello stato del procedimento[29].

Dal punto di vista contenutistico, il reclamo deve includere l'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate, delle misure richieste e degli estremi identificativi del titolare o del responsabile del trattamento, ove conosciuto[30]. Deve contenere, inoltre, la sottoscrizione dell'interessato o, su suo mandato, di un soggetto abilitato, la documentazione utile ai fini della sua valutazione, l'eventuale procura e l'indicazione di un recapito per l'invio delle comunicazioni ad esso relative[31]. Il reclamo cui difettino uno o più requisiti, in ossequio al principio generale di libertà delle forme, può comunque essere analizzato dall'autorità di controllo a titolo di segnalazione[32].

---

[26] R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1003 e ss.; A. CANDINI, *Gli strumenti di tutela*, cit., p. 571 e ss.

[27] Sulla nota distinzione fra domicilio, residenza e dimora nel diritto civile v., per tutti, F. GAZZONI, *Manuale di diritto privato*, XVI ed., Napoli, Edizioni Scientifiche Italiane, 2013, pp. 131 e 132. La giurisprudenza ha definito la residenza abituale «*il luogo del concreto e continuativo svolgimento della vita personale, e non quello risultante da un calcolo puramente aritmetico del vissuto*» (Cass. Civ., Sez. Un., sentenza 18 marzo 2016, n. 5418).

[28] L'opzione normativa del criterio di prossimità all'interessato è sottolineata da A. CANDINI, *Gli strumenti di tutela*, cit., pp. 575 e 576. L'A., a p. 577 e ss., evidenzia altresì la differenza fra il luogo di verificazione della violazione e il luogo in cui il danno si è verificato, concludendo che il primo, unico rilevante *ex* art. 77 GDPR, coincida con quello di stabilimento del titolare o del responsabile del trattamento.

[29] Così dispone l'art. 10 co. 4 decreto legislativo 1 settembre 2011, n. 150.

[30] R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1006.

[31] Così prevede l'art. 142 Codice della *privacy*.

[32] In questo senso A. CANDINI, *Gli strumenti di tutela*, cit., p. 572. Le segnalazioni, in forza dell'art 144 Codice della *privacy*, possono essere valutate dal Garante per l'emanazione dei provvedimenti di cui all'art. 58 GDPR.

L'art. 143 Codice della *privacy* disciplina il procedimento innanzi al Garante per la protezione dei dati personali[33], il quale di regola si conclude con prescrizioni rivolte al titolare e al responsabile, oppure con un non luogo a provvedere[34]. Rispetto al ricorso giudiziario, il reclamo all'autorità di controllo presenta vantaggi rilevanti sia con riferimento alla velocità dell'*iter* procedimentale, sia per quanto concerne i relativi costi[35]. Tuttavia, tale rimedio non può essere esperito per ottenere il risarcimento del danno patito a causa del trattamento illegittimo, dovendo l'interessato necessariamente esperire, a questo fine, lo strumento di cui all'art. 79 regolamento (UE) 2016/679[36].

Stante il contenuto lasso di tempo intercorso dall'ingresso nel nostro ordinamento del reclamo quale mezzo di tutela del diritto alla protezione dei dati personali[37], la sua effettività non risulta ancora, allo stato, adeguatamente verificabile. È possibile, tuttavia, in una prospettiva più ampia, valutare l'utilizzo della tutela amministrativa del diritto facendo riferimento al ricorso all'Autorità indipendente previsto, prima dell'abrogazione disposta dal decreto legislativo 10 agosto 2018 n. 101, all'art. 145 Codice della *privacy*[38].

La disciplina di questo strumento di tutela alternativo a quello giurisdizionale, in vigore dal 1 gennaio 2004 al 18 settembre 2018, consentiva al Garante di ordinare al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie per salvaguardare i diritti dell'interessato e assegnando altresì un termine per la loro adozione[39]. Avverso il provvedimento espresso

[33] Il terzo comma dell'art. 143 Codice della *privacy*, in particolare, individua i termini del procedimento. A questo proposito è importante segnalare che qualora sia attivato il meccanismo di cooperazione di cui all'art. 60 regolamento (UE) 2016/679 – su cui v. *infra* par. 5 – il termine previsto rimane sospeso per la durata di tale collaborazione. Scopo della disposizione è consentire ai Garanti della *privacy* dei vari Paesi membri coinvolti di avvalersi pienamente della cooperazione in vista della congiunta definizione della questione relativa al trattamento transfrontaliero di dati personali. *Cfr.* A. CASELLI, *Artt. 58-67*, in *GDPR e normativa privacy. Commentario*, G.M. Riccio, G. Scorza, E. Belisario (a cura di), Milano-Vicenza, Wolters Kluwer, 2018, p. 516.

[34] A. CANDINI, *Gli strumenti di tutela*, cit., p. 573.

[35] A. CANDINI, *op.cit.*, p. 587.

[36] R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1006; A. CANDINI, *op.cit.*, p. 588. Sulla responsabilità risarcitoria da illecito trattamento dei dati personali e sul ricorso giudiziario *ex* art. 79 regolamento (UE) 2016/679 v. *infra* par. 4.

[37] Avvenuta, con l'entrata in vigore del regolamento (UE) 2016/679, il 25 maggio 2018.

[38] L'autorità garante ha evidenziato, a p. 153 della relazione annuale 2018, che la scelta dell'abrogazione del ricorso *ex* art 145 Codice della *privacy* non fosse inevitabile, in quanto l'art. 77 regolamento (UE) 2016/679 «*avrebbe, in astratto, consentito di fare salvi meccanismi di tutela che, pur disciplinati dalla normativa nazionale, non risultassero incompatibili con il disegno complessivamente desumibile dalla lettura del testo normativo europeo*». La *snellezza* procedimentale di questo ricorso e le garanzie riconosciute alle parti avrebbero integrato, ad avviso del Garante, i requisiti minimi di tutela richiesti dal GDPR.

[39] Così disponeva l'abrogato art. 150 decreto legislativo 30 giugno 2003, n. 196. Nella relazione annuale 2017 Garante per la protezione dei dati personali, p. 134, l'Autorità ha precisato che nonostante la sua abrogazione «*L'istituto del ricorso, tuttavia, lascia un'importante esperienza nel nostro Paese che l'Autorità cercherà di non disperdere sia sotto il profilo procedurale che sotto quello del* modus operandi*, improntato a principi di effettività, deburocratizzazione e accesso facilitato agli interessati/ricorrenti*».

o il rigetto tacito del Garante, il titolare o l'interessato potevano proporre opposizione con ricorso all'autorità giudiziaria ordinaria[40].

Osservando i dati tratti dalle relazioni pubblicate annualmente dall'Autorità indipendente, emerge come questo rimedio di natura amministrativa abbia avuto un continuo impiego nel tempo. I ricorsi *ex* art. 145 Codice della *privacy* sono cresciuti esponenzialmente fino al 2004, per poi subire successivamente un tendenziale decremento[41]. Più in particolare, prendendo in esame le informazioni ricavabili dalle relazioni dell'Autorità garante relative agli anni dal 2009 al 2018, è rilevabile un lento ma progressivo decremento dei ricorsi proposti.

Tabella n. 1: numero di ricorsi decisi *ex* art. 145 Codice della *privacy* dal Garante per la protezione dei dati personali[42].

Anno	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018 I°sem**
Numero ricorsi decisi	360	349	257	233	222	306	307	277	276	130

È da sottolineare che il numero di ricorsi decisi relativo all'anno 2018 si riferisce al solo primo semestre dell'anno di riferimento, poiché, come già chiarito, il ricorso *ex* art. 145 Codice della *privacy* è stato abrogato e sostituito dal reclamo di cui all'art. 77 regolamento (UE) 2016/679. Per tentare di ricostruire il dato completo in relazione all'ultimo anno considerato, si può immaginare di proiettare la quantità di ricorsi decisi nel primo semestre anche nel secondo, ottenendo così, in via di prima approssimazione, il risultato di 260 ricorsi decisi nell'intero anno 2018[43]. Alla luce di questa considerazione si può meglio apprezzare la trasposizione in forma grafica dei dati riportati nella tabella n. 1.

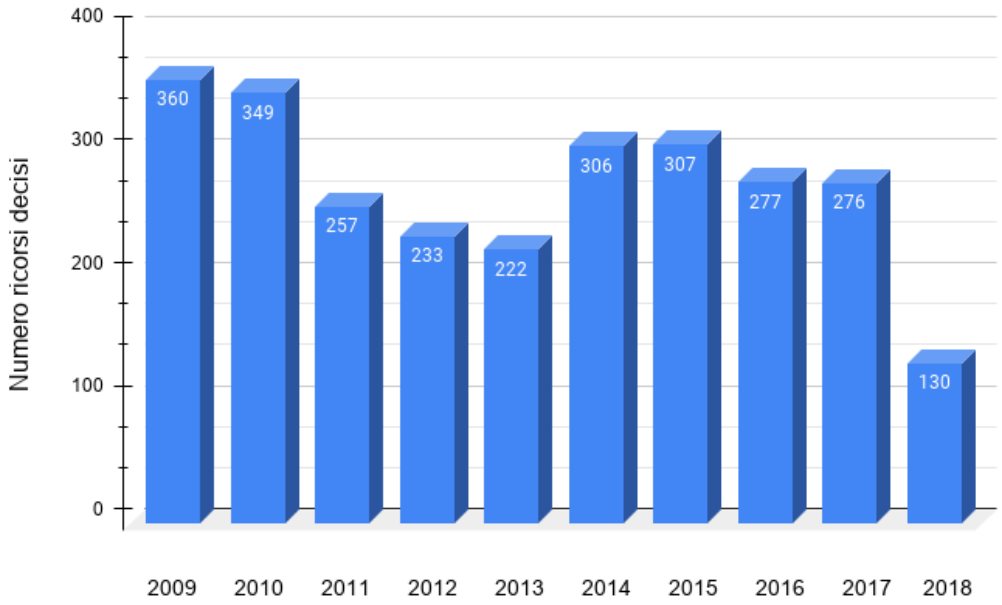
[40] Per ulteriori specificazioni sulla disciplina positiva di tale rimedio si rinvia alla lettura della sezione III, capo I, titolo I, parte III Codice della *privacy*, nella versione antecedente l'intervento riformatore compiuto dal decreto legislativo 10 agosto 2018 n. 101.

[41] Relazione annuale 2018 Garante per la protezione dei dati personali, p. 154.

[42] Fonte dei dati: relazioni annuali del Garante per la protezione dei dati personali degli anni 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, reperibili al seguente *link* garanteprivacy.it.

[43] Questo calcolo non può che essere una approssimazione in quanto, come rileva il Garante a p. 154 della relazione annuale 2018, al dato dei 130 ricorsi decisi «*sono da aggiungere gli atti la cui istruttoria è stata avviata, ma non conclusa alla data del 25 maggio 2018 (pari a 5), nonché quelli, pari a 34, che, essendo pervenuti a ridosso di tale data, non sono stati gestiti secondo il rito procedimentale dei ricorsi, ormai prossimo alla cessazione, ma trattati sulla base di disposizioni diverse. Sulla base di queste informazioni si può pertanto ragionevolmente ritenere che, se l'arco temporale preso a riferimento fosse stato l'intero anno, il numero complessivo dei ricorsi avrebbe molto probabilmente avuto, in confronto con gli anni passati, un sensibile aumento*».

Grafico n. 1: numero di ricorsi decisi *ex* art. 145 Codice della *privacy* dal Garante per la protezione dei dati personali.



L'esame del numero dei ricorsi decisi dal Garante *ex* art. 145 Codice della *privacy* nel decennio considerato conferma un andamento leggermente decrescente dell'utilizzo di questo strumento. Segnala, al contempo, un impiego piuttosto costante del rimedio, che dunque è stato percepito ed esperito quale concreta alternativa alla tutela giurisdizionale.

La menzionata cesura normativa – che ha sostituito il ricorso *ex* art. 145 Codice della *privacy* con il reclamo di cui all'art. 77 GDPR – non consente di dare continuità temporale all'analisi statistica delle forme di tutela amministrativa del diritto alla protezione dei dati personali. La differenza dei due rimedi, infatti, ha indotto l'autorità indipendente a modificare altresì la rendicontazione del loro utilizzo all'interno delle sue relazioni annuali[44]. Si ritiene tuttavia di poter concludere che, nonostante una tendenza lievemente discendente nel decennio considerato, l'impiego della tutela amministrativa del diritto abbia avuto nel tempo una discreta fortuna[45], forse anche in considerazione della possibilità, esaminata nel paragrafo seguente, di ottenere eventualmente un controllo giurisdizionale sull'esito del procedimento.

[44] *Cfr.* Relazioni annuali 2019 e 2018 (e precedenti) Garante per la protezione dei dati personali.
[45] Relazione annuale 2018 Garante per la protezione dei dati personali, p. 154.

3. Il controllo giurisdizionale sui provvedimenti del Garante della *privacy*, fra effettività del rimedio e integrazione europea

L'art. 78 regolamento (UE) 2016/679, come anticipato, disciplina il rimedio del ricorso giurisdizionale contro i provvedimenti del Garante per la protezione dei dati personali[46]. L'esperibilità di questo mezzo di tutela è una delle «*garanzie adeguate*»[47] a cui l'art. 58 par. 4 GDPR subordina l'esercizio dei poteri conferiti all'autorità amministrativa indipendente. Si tratta, pertanto, di uno strumento di difesa che tanto le persone fisiche quanto quelle giuridiche[48] possono esperire avverso le decisioni giuridicamente vincolanti formulate nei loro confronti dall'autorità di controllo[49]. In particolare, i provvedimenti vincolanti del Garante della *privacy* suscettibili di impugnazione sono quelli prescrittivi (e le ordinanze-ingiunzione) adottati all'esito di procedimenti di contestazione di violazioni amministrative, nonché quelli di rigetto o di archiviazione di reclami[50]. Il ricorso avverso questi ultimi deve essere proposto, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento[51].

Inoltre, qualsiasi interessato può avvalersi di tale ricorso qualora l'autorità di controllo competente non abbia trattato un reclamo proposto, oppure non abbia informato il reclamante entro tre mesi dello stato o dell'esito dello stesso[52]. Qualora dopo la proposizione del ricorso all'autorità giudiziaria sopraggiunga tardivamente la definizione del reclamo da parte del Garante possono verificarsi le seguenti ipotesi: in caso il reclamo sia deciso prima della pronuncia sul ricorso, il giudice dovrebbe dichiarare la cessazione della materia del contendere[53]; nell'eventualità in cui, invece, sia la statuizione giudiziaria a precedere la definizione del reclamo, l'Autorità di controllo dovrebbe dichiarare il non luogo a provvedere[54].

---

[46] Sul rapporto fra la magistratura e il Garante per la protezione dei dati personali v. anche F. SORRENTINO, *Il controllo del garante per la protezione dei dati personali e l'autorità giudiziaria secondo le più recenti norme eurounitarie*, in *QuestioneGiustizia.it*, 15 febbraio 2018. In generale sui rimedi giurisdizionali esperibili avverso gli atti delle *Authorities* v.: M. SANINO, *La tutela giurisdizionale nei confronti degli atti delle autorità indipendenti*, cit.; R. MANFRELLOTTI, *Autorità indipendenti e giurisdizione esclusiva del giudice ordinario*, in *Rassegna di diritto pubblico europeo. Autorità indipendenti e tutela giurisdizionale nella crisi dello Stato*, n. 1-2/2015, p. 155 e ss.

[47] L'art. 58 par. 4 regolamento (UE) 2016/679 prevede infatti: «*L'esercizio da parte di un'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione e degli Stati membri conformemente alla Carta*».

[48] Quindi, come precisa E. GUARDIGLI, *Le Autorità di controllo*, cit., p. 502, sia l'interessato, sia il titolare e il responsabile del trattamento.

[49] L'art. 78 regolamento (UE) 2016/679, comunque, fa salva la possibilità di esperire «*ogni altro ricorso amministrativo o extragiudiziale*».

[50] A. CANDINI, *op.cit.*, p. 583.

[51] Oppure, ai sensi dell'art. 10 co. 3 decreto legislativo 1 settembre 2011, n. 150, entro sessanta giorni se il ricorrente risiede all'estero.

[52] Così l'art. 78 par. 2 regolamento (UE) 2016/679. R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1008, definisce tale fattispecie «*silenzio-inadempimento*» del Garante della *privacy*.

[53] A. CANDINI, *op.cit.*, p. 585, reputa che l'autorità giudiziaria adita debba pronunciare una sentenza di non luogo a procedere, salva ogni statuizione sulle spese di lite.

[54] *Ibidem*.

L'art. 78 GDPR non pone particolari problemi in ordine all'individuazione dell'autorità giudiziaria da adire[55]. I ricorsi ivi disciplinati – che, come chiarito, non si riducono al solo ricorso avverso la decisione sfavorevole del Garante, estendendosi anche ai casi di mancata trattazione del ricorso – vanno difatti presentati innanzi ai giudici dello Stato nel quale opera l'autorità amministrativa indipendente[56]. In questo senso, l'individuazione dell'autorità di controllo competente fra quelle istituite all'interno dell'UE è propedeutica all'identificazione del giudice a cui proporre il ricorso[57].

Per quanto concerne il procedimento applicabile al giudizio, esso è regolato dall'art. 10 decreto legislativo 1 settembre 2011 n. 150[58]. L'ultimo comma della disposizione, in particolare, dopo aver sancito l'inappellabilità della sentenza che definisce il giudizio[59], consente al giudice ordinario di prescrivere le misure necessarie, anche in deroga al divieto di cui all'art. 4 legge 20 marzo 1865, n. 2248, allegato E), in relazione all'atto del soggetto pubblico titolare o responsabile dei dati. La legge prevede in modo espresso, quindi, che il giudice ordinario possa annullare gli atti e i provvedimenti del Garante oggetto di impugnazione[60]. Essendo quello alla protezione dei dati personali un diritto della personalità, appare condivisibile la scelta legislativa di riconoscerne la cognizione al giudice ordinario[61].

Sembra importante soffermare l'attenzione, altresì, sull'effettività in concreto del rimedio esaminato, verificando, quindi, l'utilizzo nel tempo del ricorso giurisdizionale contro i provvedimenti del Garante della *privacy*. Come anticipato, si reputa infatti che sia utile per il giurista affiancare allo studio teorico degli strumenti di tutela quello pratico-applicativo concernente il loro concreto utilizzo nella prassi[62]. In questa

---

[55] In proposito, il *considerando* n. 147 regolamento (UE) 2016/679 recita: «*Qualora il presente regolamento preveda disposizioni specifiche in materia di giurisdizione, in particolare riguardo a procedimenti che prevedono il ricorso giurisdizionale, compreso quello per risarcimento, contro un titolare del trattamento o un responsabile del trattamento, disposizioni generali in materia di giurisdizione quali quelle di cui al regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio non dovrebbero pregiudicare l'applicazione di dette disposizioni specifiche*». Una ampia ricostruzione della correlazione fra giurisdizione e territorio, anche alla luce dell'evoluzione normativa e giurisprudenziale a livello unionale, è compiuta da A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di Internet*, cit.

[56] C. CIMAROSSA, *Artt. 77-79*, cit., p. 583; R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1009.

[57] A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di Internet*, cit.

[58] Recante disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione. In proposito v. le riflessioni di R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., pp. 1012 e 1013.

[59] Secondo R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1012, l'inappellabilità della sentenza non compromette l'effettività del rimedio.

[60] V. già l'analisi di G. COSTANTINO, *La tutela giurisdizionale dei diritti al trattamento dei dati personali (Note a prima lettura dell'art. 152 d.lgs. 30 giugno 2003, n. 196)*, in *Studi di diritto processuale civile in onore di Giuseppe Tarzia*, tomo 3, Milano, Giuffrè, 2005, p. 2265 e ss. A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di Internet*, cit., peraltro, evidenzia come l'oggetto del giudizio di opposizione ai provvedimenti del Garante della *privacy* sia identico a quello introdotto in assenza di reclamo, ossia attraverso il ricorso diretto all'autorità giudiziaria di cui all'art. 79 GDPR. Su quest'ultimo strumento di tutela si rinvia *infra* al par. seguente.

[61] *Conf.* R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1010 e bibliografia ivi indicata.

[62] Questo approccio metodologico generale è suggerito U. DE SIERVO, *Tutela dei dati personali e riservatezza*, cit., *passim*.

prospettiva, si sono posti a confronto i dati pubblicati nelle ultime dieci relazioni annuali dell'autorità di controllo, redigendo la seguente tabella.

Tabella n. 2: numero di opposizioni definite a provvedimenti e a ordinanze-ingiunzione del Garante per la protezione dei dati personali[63].

Anno	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
Opposizioni (definite) a provvedimenti del Garante	65	72	73	67	80	85	80	73	101	109
Opposizioni alle ordinanze-ingiunzione	19	45	34	38	44	45	35	38	59	50

La tabella n. 2, oltre a indicare le opposizioni trattate a provvedimenti del Garante, specifica, nella terza riga orizzontale, quante di queste sono state opposizioni a ordinanze-ingiunzione. Questa precisazione, presente in ogni relazione del decennio considerato, si giustifica probabilmente per la particolare natura sanzionatoria propria delle ordinanze-ingiunzione[64], la quale è assente, di converso, nei provvedimenti di rigetto o di archiviazione di reclami oppure nelle ipotesi, precedentemente menzionate, di inerzia dell'autorità indipendente. Per avere una idea del rapporto fra le ordinanze-ingiunzione adottate dal Garante e le opposizioni proposte avverso tali provvedimenti, si riportano nella tabella n. 3 i dati relativi alle ordinanze-ingiunzione adottate negli anni 2014-2019. Non si è potuto considerare il periodo 2010-2013, invece, poiché l'informazione non era contemplata nelle relazioni annuali relative a quegli anni.

[63] Fonte dei dati: relazioni annuali del Garante per la protezione dei dati personali degli anni 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, reperibili al seguente *link* garanteprivacy.it.

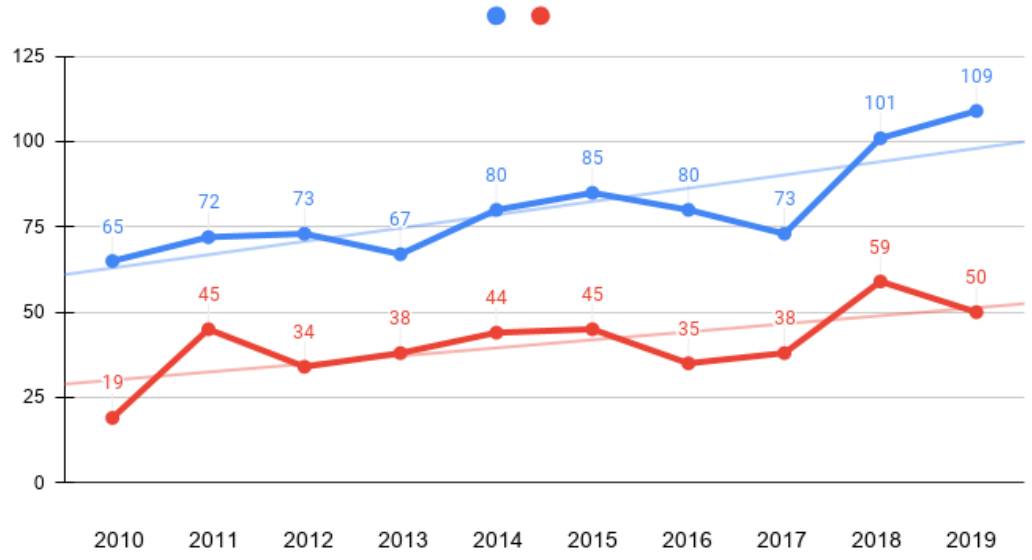
[64] In generale sui poteri sanzionatori del Garante per la protezione dei dati personali v.: S. ANTONIAZZI, *Le sanzioni amministrative*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, p. 1093 e ss.; M. RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. Finocchiaro (a cura di), Torino, Zanichelli, 2017, p. 595 e ss.

Tabella n. 3: numero di ordinanze-ingiunzione adottate dal Garante per la protezione dei dati personali[65].

Anno	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
Ordinanze-ingiunzione adottate	142	206	122	116	159	36

Per meglio cogliere l'andamento dell'utilizzo del ricorso giurisdizionale contro i provvedimenti del Garante nel lasso di tempo considerato sembra proficuo trasporre in forma grafica i dati riportati nella tabella n. 2. Sull'asse delle ordinate si sono riportate le opposizioni definite avverso i provvedimenti (in colore blu) e le ordinanze-ingiunzione (in colore rosso) adottate dal Garante, mentre nell'asse delle ascisse si sono indicati gli anni di riferimento.

Grafico n. 2: numero di opposizioni definite a provvedimenti e a ordinanze-ingiunzione del Garante per la protezione dei dati personali.



Osservando la linea di colore blu nel periodo 2010-2017 appare evidente una sostanziale stabilità, benché caratterizzata da un lieve incremento, del numero delle opposizioni definite, cui segue un marcato aumento nell'ultimo biennio. La linea rossa, pur essendo nel *trend* abbastanza sovrapponibile a quella

[65] Fonte dei dati: relazioni annuali del Garante per la protezione dei dati personali degli anni 2014, 2015, 2016, 2017, 2018, 2019, reperibili al seguente *link* garanteprivacy.it.

blu[66], presenta un andamento maggiormente oscillatorio, rendendo più difficile trarre delle conclusioni sull'evoluzione delle opposizioni alle ordinanze-ingiunzione.

In entrambe le analisi, a ben vedere, si rivela d'ausilio la valutazione delle linee di tendenza, rappresentate in colore celeste e rosa. Queste rivelano che, nel decennio considerato, si registra una crescita progressiva delle opposizioni tanto ai provvedimenti, quanto alle ordinanze-ingiunzione. Si ritiene di poter inferire[67] da questi elementi che, quantomeno dal 2010 al 2019, l'utilizzo del rimedio esaminato abbia avuto un graduale sviluppo, confermando la rilevanza, anche sistematica, della possibilità di esercitare un controllo giudiziario sui provvedimenti amministrativi del Garante.

Appare importante sottolineare, conclusivamente, come l'esigenza di fornire una interpretazione uniforme in tutta l'Unione europea del diritto alla protezione dei dati personali abbia condotto a precisare una limitazione di tale controllo giurisdizionale e, più specificamente, del potere di annullamento del giudice.

Deve essere premesso che, ove sia esperito il ricorso contro una decisione dell'autorità indipendente precedentemente oggetto di un parere o di una decisione del Comitato nell'ambito del meccanismo di coerenza[68], il Garante è oggi tenuto a trasmettere tale parere o decisione all'autorità giurisdizionale adita[69]. Lo scopo di questa previsione del GDPR è di consentire al giudice di valutare la fattispecie concreta sottoposta alla sua attenzione alla luce degli indirizzi ermeneutici di provenienza unionale.

In questo quadro, il *considerando* n. 143 regolamento (UE) 2016/679 contiene una indicazione interpretativa sui poteri – e i relativi limiti – di cui è investito il giudice ordinario adito. Infatti, qualora una decisione del Garante della *privacy* che attua una decisione del Comitato sia impugnata dinanzi all'autorità giudiziaria, e sia in questione la validità della decisione del Comitato, l'autorità giurisdizionale non può invalidare quest'ultima decisione. Ove la reputi non valida, piuttosto, è tenuta a deferire la questione alla Corte di giustizia – quale *giudice naturale* della validità degli atti delle istituzioni europee – ai sensi dell'articolo 267 TFUE[70].

---

[66] Ciò si spiega anche con la semplice considerazione che l'ordinanza-ingiunzione è una *species* del *genus* costituito dai provvedimenti adottati dal Garante della *privacy*.

[67] Sull'utilizzo giurisprudenziale dei concetti di inferenza, abduzione e deduzione si rimanda a Cass. Pen., Sez. Un., sentenza 11 settembre 2002, n. 30328.

[68] Sul meccanismo di coerenza v. *infra* par. 8.

[69] Così dispone l'art. 78, par. 4, regolamento (UE) 2016/679.

[70] Il *considerando* n. 143 GDPR così prosegue: «*Tuttavia, un'autorità giurisdizionale nazionale non può deferire una questione relativa alla validità di una decisione del comitato su richiesta di una persona fisica o giuridica che ha avuto la possibilità di proporre un ricorso per l'annullamento di tale decisione, specialmente se direttamente e individualmente interessata da siffatta decisione, ma non ha agito in tal senso entro il termine stabilito dall'articolo 263 TFUE*». La *ratio* di questa puntualizzazione, evidentemente, è quella di evitare l'aggiramento dei termini decadenziali previsti dallo stesso art. 263 par. 6 TFUE. Benché l'art. 267 TFUE non contenga alcun riferimento al termine di due mesi contemplato dall'art. 263 TFUE, la giurisprudenza della Corte di Giustizia ha evidenziato lo stretto nesso fra le due disposizioni, ritenendo che la certezza del diritto comporti la necessità di escludere la proponibilità del rinvio pregiudiziale relativo a una questione di validità per la quale era inutilmente decorso il termine di impugnazione con ricorso di annullamento. V. in proposito Corte Giust., sentenza 9 marzo 1994, causa C-188/92.

Così come non può annullare o disapplicare[71] la decisione del Comitato, essendo un organismo dell'Unione europea[72], è ragionevole ritenere che il giudice adito non possa caducare il provvedimento del Garante nazionale che ne costituisce coerente attuazione. Ne risulterebbe elusa, altrimenti, la portata precettiva del meccanismo di coerenza, che si sostanzia proprio nel vincolare la scelta dell'autorità di controllo nazionale assicurando, così, l'omogeneità applicativa della disciplina europea in tutti i Paesi membri. L'accentramento del potere decisionale a livello europeo proprio del meccanismo di coerenza, combinandosi con l'esclusività del sindacato della Corte di Lussemburgo sulla validità degli atti degli organi dell'Unione europea, si traduce, quindi, in una riduzione del potere di annullamento del giudice ordinario in tutti i casi in cui l'impugnato provvedimento del Garante nazionale sia attuativo di una precedente decisione del Comitato.

In altri termini, l'obbligatorietà che il provvedimento del Garante della *privacy* attui la decisione del Comitato – sottraendosi di conseguenza alla possibilità di un annullamento da parte del giudice nazionale – unitamente alla necessità che le questioni di validità che la riguardano siano rimesse alla Corte di Giustizia, sembrano essere indici di una riduzione delle prerogative del potere pubblico nazionale, e del corrispondente accrescimento di quelle del potere pubblico allocato a livello dell'Unione europea[73].

4. Il ricorso giurisdizionale di cui all'art. 79 regolamento (UE) 2016/679 e la responsabilità risarcitoria da illecito trattamento dei dati personali

La tutela diretta innanzi l'autorità giudiziaria può essere invocata anche a prescindere dal precedente esperimento di rimedi di natura amministrativa[74]. L'art. 79 del regolamento (UE) 2016/679, infatti, prevede che l'interessato possa proporre un ricorso giurisdizionale qualora reputi di avere subito, a seguito dell'attività di trattamento, una lesione del diritto alla protezione dei dati personali.

Per la determinazione del foro competente, il legislatore europeo ha individuato due criteri alternativi: le azioni contro il titolare o il responsabile del trattamento possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui questi hanno uno stabilimento, oppure dinanzi a quelle del Paese

[71] A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della aterritorialità") di Internet*, cit., nota n. 45.

[72] Il primo comma dell'art. 68 regolamento (UE) 2016/679 recita, infatti, che il Comitato europeo per la protezione dei dati «*è istituito quale organismo dell'Unione ed è dotato di personalità giuridica*».

[73] A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della aterritorialità") di Internet*, cit., osserva al par. 6 come, in tali fattispecie, la Corte di Giustizia assuma sostanzialmente la funzione di regolare la ripartizione della giurisdizione fra i giudici dei diversi Paesi dell'Unione, escludendo, in ambito interno, l'esercizio dell'analoga funzione da parte della Corte di Cassazione.

[74] C. CIMAROSSA, *Artt. 77-79*, cit., p. 582 e ss; A. CANDINI, *op.cit.*, p. 586 e ss.; R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1011 e ss. V. anche F. VALERINI, *Le novità processuali in materia di privacy dopo il Reg. 679/2016 (GDPR) e il D.lgs. 101/2018*, in *Judicium. Il processo civile in Italia e in Europa*, 23 ottobre 2018, disponibile a: http://www.judicium.it/wp-content/uploads/2018/10/Valerini.pdf.

in cui l'interessato risiede abitualmente, salvo, in tale seconda ipotesi, che il titolare o il responsabile sia un'autorità pubblica di uno Stato nell'esercizio dei pubblici poteri[75]. L'esatto significato di questi criteri merita di essere approfondito: invero, alla luce delle indicazioni interpretative contenute nel *considerando* n. 147 GDPR[76], essi sono destinati a prevalere – quale *lex specialis* – sulle disposizioni generali dettate dagli atti normativi dell'UE in materia di giurisdizione[77].

Il primo criterio sembra condurre all'individuazione del medesimo foro che sarebbe riconosciuto avendo riferimento al luogo della condotta, poiché il trattamento è posto in essere usualmente ove il titolare o il responsabile del trattamento hanno il proprio stabilimento[78]. L'art. 79 par. 2 regolamento (UE) 2016/679, tuttavia, non puntualizza se lo stabilimento debba essere quello principale del soggetto attivo del trattamento[79], o se debba necessariamente identificarsi con lo stabilimento in cui è avvenuto il trattamento che ha condotto al ricorso giurisdizionale[80]. Il secondo modo di determinazione del foro competente, invece, troverebbe la propria giustificazione nella sussunzione del diritto alla protezione dei dati personali fra i diritti della personalità, alla cui violazione si ricollega il criterio del centro di interessi: questo, usualmente, viene localizzato nel luogo della residenza abituale dell'interessato[81].

I due criteri speciali descritti trovano applicazione per le azioni esperite dall'interessato contro il titolare o il responsabile del trattamento, mentre quelle di accertamento negativo del titolare o del responsabile verso l'interessato – così come il contenzioso fra i soggetti attivi del trattamento – resterebbero disciplinate dal regolamento (UE) 2012/1215 (c.d. *Bruxelles I-bis*)[82].

---

75 Così dispone l'art. 79, par. 2, regolamento (UE) 2016/679. V. inoltre l'art. 10, co. 2, decreto legislativo 1 settembre 2011, n. 150.

76 Il *considerando* n. 147 regolamento (UE) 2016/679 recita testualmente: «*Qualora il presente regolamento preveda disposizioni specifiche in materia di giurisdizione, in particolare riguardo a procedimenti che prevedono il ricorso giurisdizionale, compreso quello per risarcimento, contro un titolare del trattamento o un responsabile del trattamento, disposizioni generali in materia di giurisdizione quali quelle di cui al regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio non dovrebbero pregiudicare l'applicazione di dette disposizioni specifiche*».

77 A questo proposito, l'art. 67 regolamento (UE) 2012/1215, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, dispone che «*Il presente regolamento non pregiudica l'applicazione delle disposizioni che, in materie particolari, disciplinano la competenza, il riconoscimento e l'esecuzione delle decisioni e che sono contenute negli atti dell'Unione o nelle legislazioni nazionali armonizzate in esecuzione di tali atti*».

78 F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel Regolamento "*Bruxelles I-bis*"*, in *Cuadernos de Derecho Transnacional*, vol. 9, n. 2/2017, p. 453.

79 A. CANDINI, *op.cit.*, p. 587 propende per la soluzione negativa.

80 F. MARONGIU BUONAIUTI, *op.cit.*, p. 453.

81 C. CIMAROSSA, *Artt. 77-79*, cit., p. 584. Per approfondimenti v. F. MARONGIU BUONAIUTI, *op.cit.*, pp. 455, 456 e 457.

82 F. MARONGIU BUONAIUTI, *op.cit.*, p. 451. L'A., inoltre, precisa che le disposizioni del regolamento (UE) 2012/1215 disciplinerebbero altresì i casi di concorso di processi introdotti da interessati secondo le regole dettate dal regolamento (UE) 2016/679 ed eventuali procedimenti instaurati dal titolare o dal responsabile del trattamento in base alla disciplina del regolamento (UE) 2012/1215.

Il ricorso *ex* art. 79 GDPR, in ogni caso, introduce una ordinaria azione civile[83], attraverso la quale l'interessato può chiedere il risarcimento del danno patito e l'interruzione delle condotte del titolare o del responsabile del trattamento che non siano conformi al regolamento (UE) 2016/679[84].

In particolare, ai sensi dell'art. 82 GDPR, chi ha subito un danno materiale o immateriale cagionato da una violazione del regolamento (UE) 2016/679 ha diritto al suo risarcimento da parte del titolare o del responsabile del trattamento[85]. Questi ultimi, tuttavia, sono esonerati dalle rispettive responsabilità se forniscono prova che l'evento dannoso non gli è in alcun modo imputabile[86]. Si tratta, all'evidenza, di una gravosa prova liberatoria, che si inscrive nell'alveo del *favor* legislativo nei confronti dell'interessato a cui i dati personali si riferiscono[87].

---

[83] L'art. 152 decreto legislativo 30 giugno 2003 n. 196, infatti, attribuisce all'autorità giudiziaria ordinaria le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli artt. 78 e 79 regolamento (UE) 2016/679, quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, e quelli relativi al diritto al risarcimento del danno *ex* art. 82 GDPR. *Cfr.* sul punto R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1011 e ss.

Nella giurisprudenza di merito si è posto il problema concernente la possibilità, da parte del titolare dei diritti autorali violati da utenti della rete Internet attraverso sistemi di condivisione dei file (quali *file-sharing net-works* e reti *peer-to-peer*), di ottenere dal Tribunale un provvedimento cautelare *ex* art. 700 c.p.c. che ordini all'Internet *service provider* – svolgente un ruolo di *mere conduit* a favore dei propri abbonati – di comunicare *ex* art. 156 *bis* legge 22 aprile 1941 n. 633 i dati identificativi dei soggetti titolari degli indirizzi IP e delle porte TCP: di fornire, in altre parole, alcuni dati personali riferibili agli intestatari dei contratti di fornitura per l'accesso e l'utilizzo della rete Internet. Con ordinanza dell'8 giugno 2020 (N. R.G. 1363/2020) il Tribunale di Cagliari – alla luce dell'interpretazione congiunta degli artt. 14 co. 1 decreto legislativo 9 aprile 2003 n. 70, 156, 156 *bis* e 156 *ter* legge 22 aprile 1941 n. 633, 4 n. 2), 6 e 23 GDPR, e 132 decreto legislativo 30 giugno 2003 n. 196 – ha ritenuto, valorizzando specialmente il contenuto di tale ultima disposizione, che il nostro ordinamento non consenta al ricorrente di ottenere attraverso un provvedimento d'urgenza *ex* art. 700 c.p.c. la condanna del resistente alla consegna dei dati personali identificativi degli utenti che si assume abbiano leso i suoi diritti autorali.

Per approfondimenti sulla disciplina della responsabilità civile degli Internet *service providers* nel decreto legislativo 9 aprile 2003 n. 70, che ha recepito la direttiva 2000/31/CE, v. M. GAMBINI, *Gli hosting providers tra doveri di diligenza professionale e assenza di un obbligo generale di sorveglianza sulle informazioni memorizzate*, in *Costituzionalismo.it*, fasc. n. 2/2011 "Diritto e Internet".

[84] C. CIMAROSSA, *Artt. 77-79*, cit., p. 585.

[85] Il par. 2 dell'art. 82 GDPR distingue, tuttavia, l'ampiezza della responsabilità del primo rispetto al secondo. Prevede infatti: «*Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento*». Per un esame più approfondito della responsabilità da illecito trattamento dei dati personali si rimanda a: M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, p. 1017 e ss.; E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in *Danno e responsabilità*, n. 4/2020, p. 433 e ss.

[86] Art. 82, par. 3, regolamento (UE) 2016/679. Sull'inversione dell'onere probatorio nelle ipotesi di responsabilità oggettiva v., in generale, F. GAZZONI, *Manuale di diritto privato*, cit., p. 726 e ss., e, con particolare riferimento al criterio di imputazione dell'illecito nella responsabilità per l'esercizio di attività pericolose, G. CHINÈ, M. FRATTINI, A. ZOPPINI, *Manuale di diritto civile*, V ed., Roma, Neldiritto Editore, 2014, p. 2296 e ss.

[87] G.M. RICCIO, *Art. 82*, in *GDPR e normativa privacy. Commentario*, G.M. Riccio, G. Scorza, E. Belisario (a cura di), Milano-Vicenza, Wolters Kluwer, 2018, p. 598; E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, cit., *passim*. Per maggiori riflessioni sulla prova liberatoria rinvio a M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, cit., p. 1060 e ss.

Il descritto regime giuridico di imputazione della responsabilità da illecito trattamento, a ben vedere, non differisce sostanzialmente da quello che era sancito dalla normativa nazionale previgente[88]. L'oggi abrogato art. 15 decreto legislativo 30 giugno 2003 n. 196[89], infatti, prevedeva un criterio di imputazione oggettivo o semi-oggettivo[90], essendo il danneggiante, in forza del rinvio all'art. 2050 c.c., chiamato a fornire la prova liberatoria «*di avere adottato tutte le misure idonee a evitare il danno*»[91]. Quella da illecito trattamento, dunque, costituirebbe una responsabilità extracontrattuale tipizzata e speciale rispetto all'art. 2043 c.c.[92].

La continuità dei principi che regolano questa forma di responsabilità civile induce a ritenere che, nell'ermeneutica del vigente dettato normativo, sia possibile avvalersi delle interpretazioni giurisprudenziali e dottrinali precedentemente elaborate in relazione all'art. 15 Codice della *privacy*[93]. Così, può ritenersi che ai sensi dell'art. 82 GDPR spetti all'interessato[94] provare l'evento dannoso, il pregiudizio subito per effetto del trattamento dei suoi dati personali e il nesso causale con l'attività di trattamento[95]. Egli non dovrebbe fornire la prova, invece, del dolo o della colpa del convenuto, ricadendo piuttosto su quest'ultimo l'onere dimostrativo di aver adottato tutte le misure idonee a evitare il danno[96].

Più in dettaglio, il danno patito deve essere provato secondo le regole ordinarie, in quanto l'illecito trattamento di dati personali non giustifica l'accoglimento della pretesa risarcitoria azionata in via automatica[97], ma solo a condizione che sia dimostrata dall'interessato l'esistenza del pregiudizio sofferto

[88] G.M. RICCIO, *Art. 82*, cit., pp. 597 e 598. Sulle diverse possibili interpretazioni del criterio di imputazione della responsabilità da illecito trattamento di dati personali v., però, M. RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, cit., p. 618 e ss. *Ibidem*, pp. 624 e 625: l'A. confronta la disciplina della direttiva 95/46/CE e del regolamento (UE) 2016/679 in relazione alla responsabilità derivante da illecito trattamento dei dati personali.

[89] Il primo comma della disposizione, sino all'abrogazione compiuta dal decreto legislativo 10 agosto 2018 n. 101, prevedeva: «*Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*».

[90] G.M. RICCIO, *Art. 82*, cit., p. 598. In generale, sulla fattispecie tipica di responsabilità civile di cui all'art. 2050 c.c. v. F. GAZZONI, *Manuale di diritto privato*, cit., pp. 728 e 729; G. CHINÈ, M. FRATTINI, A. ZOPPINI, *Manuale di diritto civile*, cit., p. 2294 e ss.

[91] Così testualmente l'art. 2050 c.c., rubricato «*Responsabilità per l'esercizio di attività pericolose*».

[92] E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, cit., *passim*.

[93] In questo senso anche G.M. RICCIO, *Art. 82*, cit., pp. 598 e 599.

[94] Per maggiore correttezza va precisato che, come rileva M. RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, cit., p. 616, tutti i soggetti che siano stati danneggiati dal trattamento dei dati personali, e quindi non solo l'interessato, hanno diritto al risarcimento del pregiudizio patito. *Amplius* sul punto v. M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, cit., p. 1027 e ss.

[95] Cass. Civ., Sez. 1, sentenza 5 febbraio 2016, n. 2306.

[96] Cass. Civ., Sez. 6, sentenza 5 settembre 2014, n. 18812.

[97] La giurisprudenza di legittimità – facendo applicazione di un principio generale, ribadito recentemente anche da Cass. Civ., Sez. 6, ordinanza 12 novembre 2019, n. 29206 – nega che si possa desumere dal mero illecito trattamento di dati personali la sussistenza *in re ipsa* del danno, essendo invece necessaria la specifica allegazione del pregiudizio patito. Contro tale impostazione opina invece E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, cit., *passim*, secondo il quale, in particolare, la mera violazione delle regole di condotta conformativa previste dal GDPR comporterebbe *in re ipsa* l'applicazione dell'ingiustizia del danno.

quale sua conseguenza[98]. Il danno risarcibile, inoltre, consiste in quello «*materiale o immateriale*»[99], ossia, secondo l'opinione preferibile, tanto in quello patrimoniale quanto in quello non patrimoniale[100].

Il concetto di danno, secondo il *considerando* n. 146 regolamento (UE) 2016/679, dovrebbe essere interpretato in senso lato, in modo da realizzare gli obiettivi, specie di tutela dell'interessato, che sottendono il GDPR. Tuttavia è da ritenere di perdurante valore l'orientamento giurisprudenziale, antecedente l'entrata in vigore del regolamento (UE) 2016/679, che limita la risarcibilità del danno da illecito trattamento – in applicazione dei principi contenuti in Cass. Civ., Sez. Un., sentenza 11 novembre 2008, n. 26972 – alle sole ipotesi di superamento della soglia di tollerabilità della lesione minima. Il bilanciamento con il principio solidaristico di cui all'art. 2 Cost., infatti, comporta che *non tutti* i danni non patrimoniali debbano essere oggetto di risarcimento, ma solo quelli che abbiano cagionato un pregiudizio effettivamente grave[101].

Infine resta da precisare che tutti i soggetti attivi del trattamento, se coinvolti nelle medesime operazioni di trattamento e responsabili del pregiudizio prodotto, sono tenuti in solido al risarcimento dell'intero ammontare del danno, ferma restando l'esperibilità, da parte di chi abbia pagato oltre la propria quota, dell'azione di regresso verso gli altri condebitori[102]. L'espressa enunciazione di questa disciplina nei parr. 4 e 5 dell'art. 82 GDPR, se utile nella prospettiva di omogeneizzare in tal senso gli ordinamenti di tutti i Paesi membri, si rivela ultronea nel sistema giuridico italiano, nel quale, ai sensi dell'art. 1294 c.c.[103], vige una presunzione di solidarietà dei condebitori[104].

---

98 Cass. Civ., Sez. 3, sentenza 3 luglio 2014, n. 15240; Cass. Civ., Sez. 6, sentenza 5 settembre 2014, n. 18812. Fra gli strumenti probatori utilizzabili a questo fine dall'attore, la giurisprudenza di legittimità ricomprende anche la prova testimoniale e le presunzioni semplici (v. Cass. Civ., Sez. 6, ordinanza 26 settembre 2013, n. 22100 e Cass. Civ., Sez. 3, sentenza 15 ottobre 2015, n. 20890).

99 L'espressione è contenuta nell'art. 82 par. 1 GDPR:

100 M. RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, cit., pp. 615 e 616; E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, cit., *passim*; G.M. RICCIO, *Art. 82*, cit., p. 601; M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, cit., p. 1067 e ss.

101 Cass. Civ., Sez. 6, sentenza 11 gennaio 2016, n. 222; Cass. Civ., Sez. 3, sentenza 15 luglio 2014, n. 16133, di cui riporto la massima: «*Il danno non patrimoniale risarcibile ai sensi dell'art. 15 del d.lgs. 30 giugno 2003, n. 196 (cosiddetto codice della privacy), pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 della CEDU, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost., di cui il principio di tolleranza della lesione minima è intrinseco precipitato, sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del codice della privacy ma solo quella che ne offenda in modo sensibile la sua portata effettiva. Il relativo accertamento di fatto è rimesso al giudice di merito e resta ancorato alla concretezza della vicenda materiale portata alla cognizione giudiziale ed al suo essere maturata in un dato contesto temporale e sociale. (In applicazione di tale principio la S.C. ha cassata la decisione di merito che, sulla base del mero disagio, aveva ritenuto risarcibile il danno alla privacy, caratterizzato dalla possibilità, per gli utenti del "web", di rinvenire agevolmente su internet - attraverso l'uso di un comune motore di ricerca - generalità, codice fiscale, attività di studio, posizione lavorativa e retributiva della parte attrice)*».

102 Nella ripartizione delle responsabilità fra i condebitori possono assumere rilievo eventuali accordi fra loro intercorsi ai sensi degli artt. 26 e 28 regolamento (UE) 2016/679.

103 L'art. 1294 c.c. recita testualmente: «*I condebitori sono tenuti in solido, se dalla legge o dal titolo non risulta diversamente*».

104 G.M. RICCIO, *Art. 82*, cit., p. 603. M. RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, cit., p. 623, reputa che trovino applicazione, altresì, l'art. 1298 c.c. e i commi 1 e 2 dell'art. 1299 c.c.: tali disposizioni

Conclusivamente si rileva che l'art. 34 decreto legislativo 1 settembre 2011 n. 150 ha abrogato, fra l'altro, il co. 7 dell'art. 152 Codice della *privacy*, contenente l'obbligo di notifica al Garante dei ricorsi proposti all'autorità giudiziaria. A seguito della modificata apportata dall'art. 17 decreto legislativo 10 agosto 2018 n. 101, il vigente art. 10 co. 6 decreto legislativo 1 settembre 2011 n. 150 ha nuovamente disposto in capo al ricorrente l'obbligo di notificare (anche) al Garante il decreto con il quale il giudice fissa l'udienza di comparizione delle parti[105]. Tali modifiche normative non hanno consentito all'autorità garante di raccogliere dati completi e attendibili sull'effettivo numero di ricorsi esperiti negli ultimi dieci anni, ragione per la quale non è stato possibile svolgere un'analisi dell'utilizzo nel tempo del rimedio di cui all'art. 79 regolamento (UE) 2016/679[106].

5. La tutela del diritto nei trattamenti transfrontalieri dei dati personali: l'istituzione dell'autorità di controllo capofila e il procedimento "*one stop shop*"

Dall'analisi finora condotta è emerso che, nell'arco temporale considerato, la tutela amministrativa del diritto ha goduto di un effettivo successo, essendo stata utilizzata in concreto quale alternativa a quella giudiziaria. Quest'ultima, specie intesa come controllo giurisdizionale sull'esito del procedimento innanzi al Garante nazionale[107], d'altra parte, ha guadagnato nel tempo un crescente favore, di talché l'intero *spettro* delle tutele azionabili risulta essere stato realmente esperito. In questo senso, l'eterogeneità degli strumenti di difesa del diritto apprestati dal legislatore può considerarsi sufficientemente variegata.

Ma come si declina il descritto compendio rimediale nelle fattispecie in cui le operazioni di trattamento coinvolgono una pluralità di Paesi membri, ossia in caso di trattamento transfrontaliero dei dati personali[108]?

---

prevedono, rispettivamente, «*Nei rapporti interni l'obbligazione in solido si divide tra i diversi debitori o tra i diversi creditori, salvo che sia stata contratta nell'interesse esclusivo di alcuno di essi. Le parti di ciascuno si presumono uguali, se non risulta diversamente*» e «*Il debitore in solido che ha pagato l'intero debito può ripetere dai condebitori soltanto la parte di ciascuno di essi. Se uno di questi è insolvente, la perdita si ripartisce per contributo tra gli altri condebitori, compreso quello che ha fatto il pagamento*». In generale, sulla solidarietà passiva nel rapporto obbligatorio v. F. GAZZONI, *Manuale di diritto privato*, cit., p. 613 e ss.

[105] Per i termini della notifica si rimanda allo stesso art. 10 co. 6 decreto legislativo 1 settembre 2011, n. 150.

[106] Il Garante della *privacy*, nelle relazioni annuali pubblicate dal 2012 al 2017, e precisamente nelle parti dedicate al contenzioso giurisdizionale, ha ricorrentemente valutato in modo negativo la scelta legislativa di abrogare l'obbligo di notificargli i ricorsi proposti all'autorità giudiziaria.

[107] Si ribadisce, infatti, l'impossibilità di valutare l'utilizzo del ricorso giurisdizionale *diretto* dovuta all'assenza di dati in proposito: v. *supra* par. 4.

[108] In proposito v. V. RIZZO, *Artt. 55-56*, in *GDPR e normativa privacy. Commentario*, G.M. Riccio, G. Scorza, E. Belisario (a cura di), Milano-Vicenza, Wolters Kluwer, 2018, p. 463 e ss. Il presente contributo non si occupa, invece, dei trasferimenti di dati personali verso Paesi terzi od organizzazioni internazionali, cui è dedicato il capo V del regolamento (UE) 2016/679. Per approfondimenti su tale argomento si rinvia a: F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, cit., p. 89 e ss.; M.C. MENEGHETTI, *Trasferimenti di dati personali verso Paesi terzi o Organizzazioni internazionali*, cit., p. 423 e ss.; L. VALLE, L. GRECO, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, in *Diritto dell'Informazione e dell'Informatica*, fasc. n. 2/2017, p. 168 e ss.; F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina*

Tali ipotesi sono significativamente aumentate nel tempo a causa dell'incremento della circolazione di dati fra gli Stati dell'Unione dovuto allo sviluppo delle reti di comunicazione[109]. D'altronde, la creazione di un mercato interno digitale nel quale i dati potessero fluire liberamente era, come noto, uno dei principali obiettivi della direttiva 95/46/CE[110]. La crescita del numero di questa tipologia di trattamenti ha indotto il legislatore europeo a dedicare loro una specifica disciplina.

È opportuno premettere che la definizione normativa contenuta nell'art. 4 n. 23 regolamento (UE) 2016/67 configura due fattispecie di trattamento transfrontaliero[111]. La prima comprende le operazioni, compiute da un titolare o responsabile del trattamento stabilito in più di un Paese membro, che si svolgono in stabilimenti spazialmente collocati in diversi Stati dell'Unione. La seconda riguarda i trattamenti posti in essere in un unico stabilimento da un titolare o responsabile, ma che incidono – o possono probabilmente incidere – in modo sostanziale su interessati che si trovano in più di uno Stato membro. In sintesi, il trattamento può essere definito "transfrontaliero" ogniqualvolta gli interessati oppure gli stabilimenti del titolare o responsabile si trovino in più di un Paese dell'UE.

Al fine di garantire la conformità dei trattamenti transfrontalieri alla normativa sulla protezione dei dati personali[112], l'art. 56 par. 1 regolamento (UE) 2016/679 ha istituito la figura dell'autorità di controllo capofila[113]. Essa ha un ruolo centrale nel coordinare, nelle modalità previste dall'art. 60 GDPR, la collaborazione fra tutte le autorità amministrative indipendenti coinvolte[114].

---

*contenuta nel Regolamento "*Bruxelles I-bis*"*, cit., p. 453 e ss.; S. CALZOLAIO, L. FEROLA, V. FIORILLO, E.A. ROSSI, M. TIMIANI, *La responsabilità e la sicurezza del trattamento*, cit., p. 195 e ss.; F. BORGIA, *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, p. 961 e ss.; C. DEL FEDERICO, A.R. POPOLI, *Disposizioni generali*, cit., p. 75 e ss.

Merita comunque di essere sottolineato che tecnicamente il termine «*trattamento transfrontaliero*» si riferisce solo alle operazioni di trattamento che coinvolgono Paesi membri dell'Unione europea, e non anche ai trasferimenti di dati personali verso Stati terzi od organizzazioni internazionali. Nella versione in lingua inglese del GDPR, il trattamento transfrontaliero di dati personali è chiamato «*cross-border processing*».

[109] Lo rileva anche il *considerando* n. 5 regolamento (UE) 2016/679, secondo il quale «*L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta L'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese*».

[110] La quale, come ricordano la sua stessa rubrica e il suo primo articolo, riconosceva alla libera circolazione dei dati personali una importanza assolutamente centrale, come testimoniato altresì dai *considerando* nn. 3, 6, 8 e 9 direttiva 95/46/CE.

[111] Le due ipotesi di trattamento transfrontaliero sono così formulate dall'art. 4 n. 23 regolamento (UE) 2016/679: «*a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure*

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro».

[112] C. DEL FEDERICO, A.R. POPOLI, *Disposizioni generali*, cit., p. 77; A. CASELLI, *Artt. 58-67*, cit., p. 507.

[113] «*Lead supervisory authority*» nella versione in lingua inglese del regolamento (UE) 2016/679. Una deroga importante alla competenza dell'autorità di controllo capofila è sancita dal secondo paragrafo dell'art. 56 GDPR, ai sensi del quale: «*Se il trattamento è effettuato da autorità pubbliche o organismi privati che agiscono sulla base dell'articolo 6, paragrafo 1, lettera c) o e), è competente l'autorità di controllo dello Stato membro interessato. In tal caso, non si applica l'articolo 56*».

[114] Sul punto v.: E. GUARDIGLI, *Le Autorità di controllo*, cit., p. 511; M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 521; M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro*

Più in particolare, la cooperazione coordinata dall'autorità capofila fra i Garanti nazionali interessati – che si sostanzia nello scambio di informazioni utili[115], nell'assistenza reciproca e nelle operazioni congiunte[116] – è finalizzata a raggiungere un consenso circa il provvedimento finale da adottare[117]. A questo scopo, l'autorità capofila è tenuta a trasmettere alle altre autorità di controllo interessate un progetto di decisione, e a valutare adeguatamente il parere da loro espresso su di questo[118].

In tale ottica, qualora entro il termine di quattro settimane[119] dalla sua consultazione una delle altre autorità di controllo sollevi una obiezione «*pertinente e motivata*»[120] al progetto di decisione, l'autorità capofila si trova innanzi alla seguente alternativa. Se non reputa di dare seguito all'obiezione pertinente e motivata – oppure se ritiene che difettino questi requisiti[121] – essa deve sottoporre la questione al meccanismo di coerenza. Qualora, invece, l'autorità capofila intenda dare seguito all'obiezione, è tenuta a modificare il progetto di decisione e a trasmetterlo alle altre autorità di controllo interessate, così da ottenere il loro parere anche sulla versione riveduta[122].

L'adeguata valutazione dell'opinione delle altre autorità di controllo da parte dell'autorità capofila costituisce, quindi, un elemento fondamentale del procedimento che conduce all'adozione del provvedimento finale. Essa non viene meno neanche nell'ipotesi in cui nessun Garante sollevi obiezioni[123] al progetto di decisione trasmesso: in tal caso, infatti, si presume che tutte le autorità coinvolte siano d'accordo sul progetto, che diviene per loro vincolante in forza di tale implicito consenso[124].

---

del general data protection regulation, cit., *passim*; P. BALBONI, E. PELINO, L. SCUDIERO, *Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation*, in *Computer Law & Security Review*, vol. 30, n. 4/2014, p. 392 e ss. In proposito, v. anche i *considerando* nn. 125 e 126 regolamento (UE) 2016/679. Nella letteratura spagnola v. A. RALLO LOMBARTE, R. GARCÍA MAHAMUT, J.A. VIGURI CORDERO, *Cooperación y coordinación entre autoridades de proteccion de datos*, in *Hacia un nuevo derecho europeo de protección de datos*, A. Rallo Lombarte, R. García Mahamut, (a cura di), Valencia, Tirant lo Blanch, 2015, p. 739 e ss.

115 Lo scambio di informazioni, come richiede l'art. 60 par. 12 regolamento (UE) 2016/679, deve avvenire attraverso mezzi elettronici e utilizzando moduli standard.

116 Sull'assistenza reciproca e le operazioni congiunte fra autorità di controllo v. *amplius* il par. successivo.

117 Art. 60, parr. 1 e 2, regolamento (UE) 2016/679. In proposito v. anche A. CASELLI, *Artt. 58-67*, cit., p. 509.

118 Il terzo paragrafo dell'art. 60 regolamento (UE) 2016/679, infatti, utilizza l'espressione «*tiene debitamente conto delle loro opinioni*».

119 Una completa ricostruzione dei termini nella procedura di cooperazione *ex* art. 60 GDPR e dei principi che la ispirano si trova in A. CASELLI, *Artt. 58-67*, cit., pp. 510 e 511.

120 Art. 60, par. 4, regolamento (UE) 2016/679. La definizione normativa di «*obiezione pertinente e motivata*» è contenuta nell'art. 4 n. 24 GDPR, ai sensi del quale consiste in una «*obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione*». Tale concetto, secondo A. CASELLI, *Artt. 58-67*, cit., p. 513, necessita comunque di essere ulteriormente chiarito ad opera del Comitato europeo per la protezione dei dati.

121 E che l'obiezione, dunque, non sia pertinente o motivata.

122 Ai sensi dell'art. 60 par. 5 regolamento (UE) 2016/679 il progetto di decisione così riveduto è sottoposto, entro il termine di due settimane, alla procedura di cui all'art. 60 par. 4 GDPR.

123 Entro il termine di cui all'art. 60 parr. 4 e 5 regolamento (UE) 2016/679.

124 L'art. 60 par. 6 regolamento (UE) 2016/679 difatti prevede testualmente: «*Se nessuna delle altre autorità di controllo interessate ha sollevato obiezioni al progetto di decisione trasmesso dall'autorità di controllo capofila entro il termine di cui ai paragrafi 4 e 5,*

L'adozione della decisione finale, nonché la sua notifica allo stabilimento principale o unico dei soggetti attivi del trattamento, è un'altra essenziale prerogativa dell'autorità capofila. L'art. 60 par. 8 regolamento (UE) 2016/679 contempla però una deroga a tale conclusione del procedimento, statuendo che, in caso di archiviazione o di rigetto di un reclamo, sia compito dell'autorità di controllo cui esso è stato proposto adottare la decisione finale, notificarla al reclamante, e informare il titolare del trattamento[125]. La *ratio* dell'eccezione è di consentire, anche in tali casi, l'esercizio del diritto a un ricorso giudiziario effettivo sancito dall'art. 47 Carta di Nizza[126].

Se l'archiviazione o il rigetto del reclamo fosse disposta dall'autorità capofila, infatti, l'impugnazione avverso il suo provvedimento dovrebbe essere proposta innanzi all'autorità giudiziaria del Paese membro ove essa è ubicata, e quest'ultimo potrebbe essere diverso da quello proprio del reclamante[127]. Il controllo giurisdizionale sull'attività provvedimentale dell'autorità amministrativa indipendente, così, diverrebbe più difficoltoso, rischiando di compromettere l'effettività del rimedio di cui all'art. 78 GDPR. Per tale motivo il legislatore europeo ha congegnato la deroga descritta, la quale, imponendo che spetti all'autorità di controllo cui è stato proposto il reclamo disporne l'archiviazione o il rigetto, permette di esperire il ricorso avverso tale decisione davanti a un giudice del medesimo Paese membro del reclamante, assicurando la prossimità della tutela giurisdizionale[128].

La complessa articolazione del procedimento di cui all'art. 60 GDPR, anche definito "sportello unico" o "*one stop shop*"[129], è sintomatica della difficoltà di bilanciare le prerogative delle autorità di controllo

si deve considerare che l'autorità di controllo capofila e le autorità di controllo interessate concordano su tale progetto di decisione e sono da esso vincolate».

125 Una disciplina ulteriormente differenziata, inoltre, è posta dall'art. 60 par. 9 regolamento (UE) 2016/679 in relazione ai casi in cui l'autorità capofila e le autorità di controllo interessate convengano di archiviare o rigettare parti di un reclamo, ma di intervenire su altre parti del medesimo reclamo: in siffatte ipotesi deve essere adottata una decisione separata per ciascuna di tali parti. Più in particolare, «*L'autorità di controllo capofila adotta la decisione per la parte riguardante azioni in relazione al titolare del trattamento e la notifica allo stabilimento principale o allo stabilimento unico del responsabile del trattamento o del responsabile del trattamento sul territorio del suo Stato membro e ne informa il reclamante, mentre l'autorità di controllo del reclamante adotta la decisione per la parte riguardante l'archiviazione o il rigetto di detto reclamo, la notifica a detto reclamante e ne informa il titolare del trattamento o il responsabile del trattamento*». La *ratio* della previsione è la medesima descritta nel corpo del testo con riferimento all'art. 60 par. 8 regolamento (UE) 2016/679. Per ulteriori approfondimenti si rinvia a A. CASELLI, *Artt. 58-67*, cit., p. 515.

126 A. CASELLI, *Artt. 58-67*, cit., p. 514. L'art. 47 della Carta dei diritti fondamentali dell'Unione europea recita: «*Ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo.*

Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni persona ha la facoltà di farsi consigliare, difendere e rappresentare.

A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese dello Stato, qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia».

127 A. CASELLI, *Artt. 58-67*, cit., pp. 514 e 515. Circa il controllo giurisdizionale sui provvedimenti del Garante della *privacy* v. *supra* par. 3.

128 In ossequio, dunque, all'art. 47 della Carta di Nizza, oltre che all'art. 6 CEDU e a tutte le disposizioni costituzionali dei Paesi membri che prevedono il diritto a un equo processo. *Cfr.* A. CASELLI, *Artt. 58-67*, cit., pp. 514 e 515.

129 M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 524.

nazionali con l'innovativo ruolo dell'autorità capofila[130]. La decisione di quest'ultima, come visto, di regola si sostituisce a quelle che avrebbero potuto adottare – nell'ambito delle rispettive competenze territoriali – i diversi Garanti nazionali[131], di modo che la condivisione dell'*iter* decisionale costituisce il necessario contraltare per il ridimensionamento del loro potere deliberativo quali autorità singole[132].

Dal punto di vista funzionale, l'adozione di una decisione congiunta da parte dei Garanti della *privacy* assicura l'omogeneità applicativa della disciplina della *Data protection* e, quindi, la certezza del diritto dell'Unione[133]. Contribuisce a questo fine anche l'obbligo per il titolare o il responsabile di adottare, a seguito della notifica della decisione dell'autorità capofila, tutte le misure necessarie per garantire la conformità a essa di ogni trattamento realizzato nei propri stabilimenti all'interno dell'UE[134]. In tal modo, infatti, il meccanismo "*one stop shop*" consente l'estensione degli effetti della decisione in tutti i Paesi membri in cui operano i soggetti attivi che ne sono destinatari[135].

Inoltre, l'autorità capofila costituisce l'unico Garante con cui il titolare o il responsabile del trattamento sono tenuti a interagire in relazione al trattamento transfrontaliero effettuato[136]. L'identificazione, fra le diverse autorità indipendenti potenzialmente interessate, di un solo interlocutore dei soggetti attivi del trattamento rappresenta, invero, una notevole semplificazione rispetto al sistema previgente[137], ed è volta ad agevolare lo sviluppo del mercato digitale all'interno dell'UE.

In merito all'individuazione dell'autorità capofila fra i diversi Garanti nazionali interessati, a ben vedere, occorre tenere distinte due fattispecie[138]. Qualora vi sia una molteplicità di stabilimenti collocati in più Stati dell'Unione, essa è identificata in quella competente in relazione al luogo in cui è situato lo

130 F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, cit., p. 165 e ss.

131 M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 525.

132 Sulla riduzione dei margini di indipendenza verticale dei Garanti nazionali della *privacy* dovuti alla nascita dei meccanismi di cooperazione v. M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, cit., *passim*.

133 In proposito v.: V. RIZZO, *Artt. 55-56*, cit., p. 469; M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., pp. 521 e 524.

134 Ai sensi del decimo paragrafo dell'art. 60 GDPR, inoltre, il titolare o responsabile del trattamento è tenuto a notificare all'autorità capofila le misure adottate per conformarsi alla sua decisione. L'autorità capofila, invece, deve trasmettere tali informazioni alle altre autorità di controllo interessate.

135 V. RIZZO, *Artt. 55-56*, cit., p. 469; M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 528.

136 Dispone infatti l'art. 56 par. 6 regolamento (UE) 2016/679: «*L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare del trattamento o responsabile del trattamento*». In proposito v. anche M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, cit., *passim*.

137 M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 525.

138 Sul tema v. più ampiamente: V. RIZZO, *Artt. 55-56*, cit., p. 471 e ss.; M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, cit., *passim*. Dal punto di vista normativo, l'individuazione dell'autorità capofila è disciplinata dall'art. 56 par. 1 regolamento (UE) 2016/679.

stabilimento principale[139] del soggetto attivo del trattamento[140]. Allorché la qualificazione del trattamento come transfrontaliero discenda, invece, dall'esistenza di effetti che coinvolgono interessati che si trovano in diversi Paesi membri, l'autorità capofila viene individuata in quella dello Stato in cui è collocato l'unico stabilimento del titolare o del responsabile[141]. Ove l'oggetto dei reclami o delle violazioni del regolamento riguardi unicamente uno stabilimento situato in uno Stato membro, oppure incida in modo sostanziale solo su interessati ivi ubicati, la competenza spetta, in deroga alla disciplina sopra esposta, all'autorità garante di quel Paese[142]. Resta fermo, tuttavia, anche in tali fattispecie, l'obbligo di cooperazione fra autorità amministrative indipendenti, come puntualmente descritto dai parr. 3, 4 e 5 dell'art. 56 regolamento (UE) 2016/679[143].

Secondo una parte della letteratura, le modalità per l'individuazione dell'autorità capofila introdotte dal regolamento (UE) 2016/679 avrebbero ridotto il rischio, rispetto al previgente assetto normativo delineato dalla direttiva 95/46/CE, che si verifichi il fenomeno del c.d. *forum shopping*[144]. In seguito all'entrata in vigore del GDPR, infatti, la disciplina applicabile dipenderebbe solo per la minor parte dal

---

[139] Sul concetto di "stabilimento principale" si rimanda alla definizione normativa contenuta all'art. 4 n. 16 regolamento (UE) 2016/679 e alle indicazioni interpretative contenute nei *considerando* nn. 22 e 36 GDPR. Sulla giurisprudenza euro-unitaria relativa alla nozione di stabilimento, in gran parte recepite nel dato positivo regolamentare, invece, v.: C. COLAPIETRO, A. IANNUZZI, *op.cit.*, p. 93; A. SPANGARO, *L'ambito di riferimento materiale del nuovo regolamento*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. Finocchiaro (a cura di), Torino, Zanichelli, 2017, p. 44; G.M. SALERNO, *Le origini ed il contesto*, cit., p. 72; S. CALZOLAIO, *op.cit.*, p. 622; V. FIORILLO, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, n *Federalismi.it*, 26 luglio 2017, p. 22; G. DE GREGORIO, *Social network, contitolarità del trattamento e stabilimento: la dimensione costituzionale della tutela dei dati personali tra prospettive passate e future*, in *Diritto dell'Informazione e dell'Informatica*, fasc. n. 3/2018, p. 462 e ss.; G.M. RICCIO, *Titolarità e contitolarità nel trattamento dei dati personali tra Corte di Giustizia e regolamento* privacy, in *La nuova giurisprudenza civile commentata*, n. 12/2018, p. 1805 e ss.; L. VALLE, L. GRECO, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, cit., p. 168 e ss.; O. POLLICINO, M. BASSINI, *Art. 8*, in *Carta dei Diritti fondamentali dell'Unione europea*, R. Mastroianni, O. Pollicino, A. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), Milano, Giuffrè, 2017, p. 158; M. BASSINI, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, n. 3/2016, p. 588.

[140] Ipotesi di cui alla lett. a) dell'art. 4 n. 23 regolamento (UE) 2016/679.

[141] Ipotesi di cui alla lett. b) dell'art. 4 n. 23 regolamento (UE) 2016/679. V. anche C. DEL FEDERICO, A.R. POPOLI, *Disposizioni generali*, cit., p. 77.

[142] Così prevede l'art. 56 par. 2 regolamento (UE) 2016/679.

[143] V. *amplius* A. CASELLI, *Artt. 58-67*, cit., p. 512. Per approfondimenti sulla disciplina applicabile ai reclami in queste ipotesi si rinvia a: M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., pp. 523 e 524; V. RIZZO, *Artt. 55-56*, cit., p. 473 e ss.

[144] Così P. BALBONI, E. PELINO, L. SCUDIERO, *Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation*, cit., p. 400. Con l'espressione «*forum shopping*» si fa usualmente riferimento alla possibilità per una parte di incardinare un processo – o, come in questo caso, un procedimento amministrativo – presso l'autorità – giudiziaria o amministrativa – che si dimostra più favorevole all'accoglimento delle istanze o delle interpretazioni giuridiche che si intendono far valere, selezionando, in questo modo, la sede più propizia per vedere riconosciute le ragioni che si perorano. Nell'ambito della protezione dei dati personali, il fenomeno del *forum shopping* si sostanziava soventemente nella scelta societaria di radicare il proprio stabilimento principale in Paesi membri la cui l'autorità di controllo prediligeva riconoscere, in linea generale, la prevalenza dei diritti dei titolari e responsabili del trattamento su quelli degli interessati. E. TOSI, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, cit., menziona il rischio che, in tema di responsabilità risarcitoria da illecito trattamento dei dati personali, sorga un *forum shopping* normativo fra i diversi Paesi membri.

luogo di stabilimento della società, essendo dettata direttamente a livello unionale[145]. In tal senso paiono deporre anche le linee guida adottate dal Gruppo art. 29 in data 13 dicembre 2016, le quali affermano radicalmente che «*Il regolamento non consente il* "forum shopping"»[146]. L'identificazione dell'autorità capofila, invero, sarebbe ancorata a criteri oggettivi e a elementi probatori, non potendosi invece fondare esclusivamente su dichiarazioni rese dalla società: sui titolari e responsabili del trattamento, così, ricadrebbe l'onere di provare che lo stabilimento svolga un «*esercizio reale ed effettivo di attività gestionali o decisionali rispetto al trattamento di dati personali*»[147]. L'individuazione della capofila, inoltre, spetterebbe in ultima istanza al Comitato europeo, e non al singolo Garante che reclami tale ruolo[148].

Tirando le fila del discorso fin qui compiuto, pare rilevante sottolineare come il procedimento dello sportello unico di cui all'art. 60 regolamento (UE) 2016/679 costituisca non solo «*una assoluta novità nel panorama della protezione dei dati europea*»[149], ma altresì una componente importante del processo di integrazione europea in questa materia.

La transizione dalla direttiva 95/46/CE al regolamento (UE) 2016/679 ha implicitamente modificato il ruolo dei Garanti della *privacy*, chiamati non più a vigilare sul rispetto di legislazioni nazionali – sia pure attuative di regole comunitarie – ma sull'osservanza di norme poste direttamente dal GDPR[150]. La coerente applicazione della disciplina comune in tutti i Paesi membri – di cui il meccanismo "*one stop shop*" è un tassello fondamentale – è indispensabile per non minare l'uniformità della *Data protection* nell'Unione europea[151]. La nozione unionale di diritto alla protezione dei dati personali, difatti, non può prescindere dall'esistenza di un *enforcement* che ne assicuri in concreto l'effettiva unitarietà[152].

6. Assistenza reciproca, operazioni congiunte e principio generale di leale collaborazione: una verifica, anche empirica, della cooperazione fra autorità di controllo

Quella prevista nell'ambito del meccanismo "*one stop shop*" non è l'unica forma di cooperazione fra autorità di controllo disciplinata dal regolamento (UE) 2016/679. Animato dall'intento di garantire una omogenea applicazione della disciplina unionale in tutti i Paesi membri, il legislatore europeo ha infatti tipizzato

145 P. BALBONI, E. PELINO, L. SCUDIERO, *Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation*, cit., p. 400.
146 Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento, versione emendata e adottata in data 5 aprile 2017, p. 8.
147 Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento, cit., p. 8.
148 *Ibidem*.
149 A. CASELLI, *Artt. 58-67*, cit., p. 506.
150 E. GUARDIGLI, *Le Autorità di controllo*, cit., p. 493.
151 F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, cit., p. 103.
152 M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 519.

ulteriori modelli di collaborazione tra Garanti della *privacy* nazionali[153]: l'assistenza reciproca e le operazioni congiunte[154].

Si tratta di strumenti fondamentali per rispondere alla sfida di tutelare i diritti degli interessati nei rispettivi Paesi membri, indipendentemente dalla collocazione degli stabilimenti dei titolari e responsabili del trattamento[155]. All'interno di una cornice normativa condivisa, d'altronde, è il principio stesso della certezza del diritto a richiedere che ogni autorità amministrativa indipendente conosca come la comune disciplina viene applicata dalle altre[156].

La mutua assistenza si concreta, in particolare, nelle richieste di informazioni, autorizzazioni, consultazioni preventive[157], nonché di effettuare ispezioni e indagini[158]. L'istanza deve illustrare lo scopo e i motivi che sottendono la richiesta, e le informazioni scambiate devono essere utilizzate necessariamente ai soli fini per cui sono state domandate[159].

L'autorità destinataria delle richieste deve darvi seguito senza ingiustificato ritardo[160], se non ritiene di doverle rigettare[161]. Il rifiuto di prestare assistenza è consentito, ai sensi dell'art. 61 par. 4 regolamento (UE) 2016/679, qualora il Garante destinatario non sia competente per trattare l'oggetto della richiesta o per adottare le misure di cui è domandata l'esecuzione, oppure ove l'accoglimento della richiesta violi le disposizioni del GDPR, il diritto dell'Unione o quello del Paese membro a cui è soggetto. In ogni caso, l'autorità di controllo ricevente è tenuta a informare la richiedente – entro un mese dal ricezione

153 M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 529. Sul punto v. anche: A. RALLO LOMBARTE, R. GARCÍA MAHAMUT, J.A. VIGURI CORDERO, *Cooperación y coordinación entre autoridades de proteccion de datos*, cit., p. 739 e ss.; D. BARNARD-WILLS, C. PAUNER CHULVI, P. DE HERT, *Data protection authority perspectives on the impact of data protection reform on cooperation in the EU*, in *Computer Law & Security Review*, vol. n. 32/2016.

154 L'assistenza reciproca e le operazioni congiunte non sono strumenti alternativi al procedimento dello "sportello unico", disponendo anzi l'art. 60 par. 2 regolamento (UE) 2016/679 che essi possono essere attivati in qualsiasi momento durante la cooperazione. Tali istituti sono espressione, come si spiegherà nel corso di questo par., del principio generale di leale collaborazione fra autorità di controllo. *Conf.* sul punto A. CASELLI, *Artt. 58-67*, cit., p. 519. L'assistenza reciproca e le operazioni congiunte, inoltre, rinvengono un ancoraggio nel diritto primario dell'Unione all'art. 197 par. 2 TFUE.

155 J. POLONETSKY, *Molto più del rispetto delle norme*, in *Privacy 2030. Una nuova visione per l'Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, novembre 2019, reperibile al *link* garanteprivacy.it, p. 40.

156 V. RIZZO, *Artt. 55-56*, cit., p. 469.

157 Art. 36 regolamento (UE) 2016/679.

158 Art. 61 par. 1 regolamento (UE) 2016/679. Sulla delimitazione delle richieste avanzabili attraverso lo strumento dell'assistenza reciproca codificato all'art. 61 GDPR v. più diffusamente A. CASELLI, *Artt. 58-67*, cit., p. 520 e ss.

159 M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 529 e ss.

160 E in ogni caso, ai sensi dell'art. 61 par. 2 regolamento (UE) 2016/679, entro un mese dal ricevimento della richiesta. A. CASELLI, *Artt. 58-67*, cit., p. 519.

161 In tale ipotesi, il rigetto della richiesta di assistenza deve essere motivato dall'autorità di controllo cui essa è indirizzata.

dell'istanza – dell'esito o dei progressi delle misure adottate[162]. Per incentivare lo scambio di informazioni, inoltre, l'attività di assistenza non può comportare spese a carico dell'autorità richiedente[163].

Infine è da sottolineare la natura obbligatoria dell'assistenza reciproca, che la distingue dai generici inviti alla cooperazione contenuti, invece, nell'art. 28 par. 6 direttiva 95/46/CE[164]. La portata vincolante dell'art. 61 regolamento (UE) 2016/679 ha indotto parte della dottrina a suggerirne un utilizzo ponderato, prediligendo piuttosto la collaborazione deformalizzata prevista dall'art. 57, par. 1, lett. g) GDPR[165].

Le operazioni congiunte delle autorità di controllo consistono invece in azioni comuni, incluse indagini e misure di contrasto, cui prendono fisicamente parte membri o personale dei Garanti della *privacy* di altri Paesi[166].

A queste attività, in caso di trattamenti transfrontalieri di dati personali[167], hanno diritto di partecipare le autorità degli Stati dell'UE in cui il titolare o il responsabile ha degli stabilimenti, oppure quelle dei Paesi membri in cui vi sia la probabilità che il trattamento abbia un «*impatto negativo sostanziale*» su un «*numero significativo di interessati*»[168]. L'autorità capofila competente *ex* art. 56, parr. 1 o 4 regolamento (UE) 2016/679, pertanto, è tenuta a rispondere in modo celere alle richieste di intervento[169], e a invitare le altre autorità di controllo interessate[170] a partecipare alle operazioni congiunte. Queste possono essere condotte, tuttavia, anche al di fuori dei suddetti casi obbligatori, ogniqualvolta una autorità di controllo ritenga proficuo avvalersi del supporto di un'altra per azioni da condurre sul proprio territorio[171].

---

162 L'ottavo paragrafo dell'art. 61 GDPR individua le regole applicabili nel caso in cui l'autorità di controllo destinataria dell'istanza non fornisca le informazioni domandate. M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 530.

163 In circostanze eccezionali, ai sensi dell'art. 61 par. 7 regolamento (UE) 2016/679, «*Le autorità di controllo possono concordare disposizioni di indennizzo reciproco per spese specifiche risultanti dalla prestazione di assistenza reciproca*». V. anche il *considerando* n. 120 GDPR.

164 A. CASELLI, *Artt. 58-67*, cit., pp. 518 e 519; M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, cit., *passim*.

165 A. CASELLI, *Artt. 58-67*, cit., p. 521. L'A. fonda tale opinione anche sull'applicabilità, nell'ipotesi di mancata assistenza *ex* art. 61 par. 8 GDPR, dell'art. 66 regolamento (UE) 2016/679.

166 A. CASELLI, *Artt. 58-67*, cit., p. 524; M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., pp. 529 e 531. Sul risarcimento dei danni cagionati nel compimento delle operazioni congiunte v. in particolare i parr. 4, 5, e 6 dell'art. 62 regolamento (UE) 2016/679.

167 A. CASELLI, *Artt. 58-67*, cit., p. 524.

168 Così prevede l'art. 62 par. 2 regolamento (UE) 2016/679. In relazione all'ipotesi di violazione di questo articolo, il settimo par. dello stesso art. 62 GDPR stabilisce che: «*Qualora sia prevista un'operazione congiunta e un'autorità di controllo non si conformi entro un mese all'obbligo di cui al paragrafo 2, seconda frase, del presente articolo, le altre autorità di controllo possono adottare misure provvisorie nel territorio del loro Stato membro ai sensi dell'articolo 55. Si considera, in tal caso, che urga intervenire ai sensi dell'articolo 66, paragrafo 1, e che siano necessari un parere o una decisione vincolante d'urgenza da parte del comitato a norma dell'articolo 66, paragrafo 2*».

169 M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., pp. 531 e 532.

170 A. CASELLI, *Artt. 58-67*, cit., p. 525 illustra come la nozione di autorità di controllo interessata in caso di partecipazione a operazioni congiunte sia differente rispetto a quella propria del meccanismo "*one stop shop*".

171 A. CASELLI, *Artt. 58-67*, cit., pp. 524 e 525.

Ai membri o al personale del Garante che partecipano alle operazioni congiunte possono essere conferiti poteri – anche di indagine – dall'autorità di controllo ospite, in conformità al diritto dei Paesi membri e previa autorizzazione dell'autorità di controllo ospitata[172]. Se l'ordinamento dello Stato in cui opera l'autorità ospite lo permette, essa può inoltre consentire ai soggetti ospitati di esercitare i poteri d'indagine loro riconosciuti dal diritto del Paese da cui provengono[173]. La finalità dell'art. 62 regolamento (UE) 2016/679, invero, sembra essere quella di favorire e sollecitare l'uso delle operazioni congiunte[174].

Le disposizioni che il regolamento (UE) 2016/679 dedica alla cooperazione, quindi, sono numerose, al punto che non appare improprio sussumere l'esistenza di un principio generale di leale collaborazione fra autorità di controllo.

Oltre agli artt. 60, 61 e 62 regolamento (UE) 2016/679 si considerino, a questo proposito, le indicazioni di carattere sistematico contenute negli artt. 51, par. 2[175], e 57, par. 1, lett. g)[176], GDPR, nonché nei *considerando* nn. 123 e 133 GDPR. In rapporto alla direttiva 95/46/CE, a ben vedere, il regolamento (UE) 2016/679 dedica maggiore spazio ai meccanismi di cooperazione fra Garanti nazionali: a fronte dell'unica disposizione specificamente riservata a questo tema nel primo atto normativo (art. 29 direttiva 95/46/CE), vi sono ben diciassette articoli nel secondo[177].

Il procedimento "*one stop shop*", l'assistenza reciproca e le operazioni congiunte, in quanto nuove[178] estrinsecazioni del generale principio di leale collaborazione fra autorità di controllo, costituiscono un significativo passo in avanti nel processo di integrazione europea della *Data protection*[179].

L'importanza delle concrete interazioni fra le *Authorities* nazionali[180] ha spinto la presente ricerca a verificare l'esistenza – anche sul piano empirico, oltre che normativo – di una maggiore integrazione nello svolgimento delle loro attività. A questo scopo, si è confrontato il numero annuale degli incontri di lavoro delle autorità di controllo nel corso del decennio 2010-2019.

---

172 Art. 62 par. 3 regolamento (UE) 2016/679.

173 L'art. 62 par. 3 regolamento (UE) 2016/679 precisa, tuttavia, che «*Tali poteri d'indagine possono essere esercitati unicamente sotto il controllo e in presenza di membri o personale dell'autorità di controllo ospite*» e che comunque «*I membri o il personale dell'autorità di controllo ospitata sono soggetti al diritto dello Stato membro dell'autorità di controllo ospite*».

174 A. CASELLI, *Artt. 58-67*, cit., p. 526.

175 L'art. 51 par. 2 regolamento (UE) 2016/679 dispone: «*Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII*».

176 Secondo l'art. 57 par. 1 lett. g) regolamento (UE) 2016/679 ogni autorità di controllo sul proprio territorio «*collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento*».

177 Artt. 60-76 regolamento (UE) 2016/679, cui si sommano le altre diposizioni menzionate nel corso di questo contributo. Su questi aspetti v. anche M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 516 e ss.

178 Sottolinea la loro innovatività A. CASELLI, *Artt. 58-67*, cit., p. 506 e ss.

179 M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 516 e ss.

180 Su cui si sofferma anche J. POLONETSKY, *Molto più del rispetto delle norme*, cit., p. 40.

Più in particolare, utilizzando le relazioni annuali pubblicate dal Garante della *privacy*, si sono conteggiate le riunioni del c.d. "Gruppo art. 29"[181] e, dopo la sua sostituzione nel corso del 2018, del Comitato europeo per la protezione dei dati personali[182]. L'indagine analizza altresì gli incontri dei sottogruppi di lavoro, prima nell'ambito del Gruppo art. 29 e poi del Comitato europeo, in quanto la cooperazione fra le autorità di controllo si sviluppa e si consolida anche al di fuori delle sessioni plenarie[183]. Più specificamente, i sottogruppi di lavoro si concentrano sull'approfondimento di settori specifici della protezione dei dati personali, fra cui a titolo esemplificativo: *Border Travel Law Enforcement; Compliance*, *E-Government and Health*; *Financial Matters*; *Technology*; *Social Media Working Group*.

Tabella n. 4: numero di riunioni e partecipazioni a sottogruppi di lavoro nell'ambito del Gruppo art. 29 e, successivamente alla sua istituzione, del Comitato europeo per la protezione dei dati personali[184].

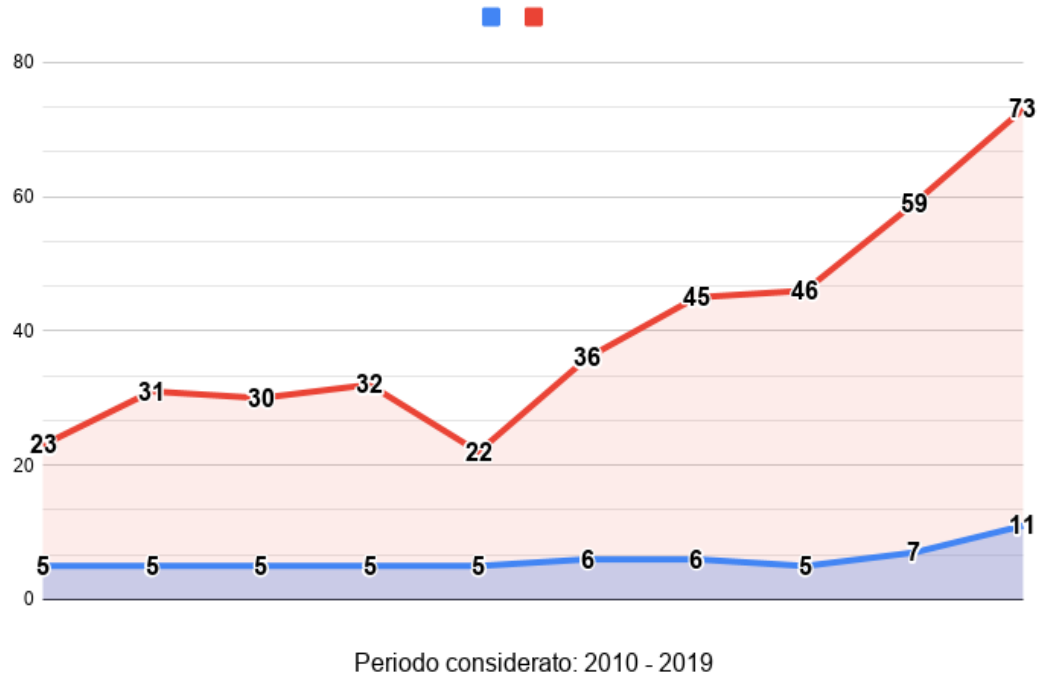
Anno	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
Riunioni del Gruppo art. 29 o Comitato europeo	5	5	5	5	5	6	6	5	7	11
Partecipazioni a sottogruppi di lavoro	23	31	30	32	22	36	45	46	59	73

La tabella n. 4 indica: nella prima riga orizzontale, il numero delle riunioni del Gruppo art. 29 e del Comitato europeo per la protezione dei dati personali, che lo ha sostituito nel corso del 2018; nella seconda riga orizzontale, il numero delle partecipazioni a sottogruppi di lavoro nell'ambito prima del Gruppo art. 29, e poi del Comitato europeo per la protezione dei dati personali.
La ricerca non si estende, invece, agli altri incontri internazionali cui ha preso parte il Garante della *privacy*, come quelli presso il Consiglio d'Europa e l'Organizzazione per la cooperazione e lo sviluppo economico.

[181] Tale organo, istituito dalla direttiva 95/46/CE, si componeva di rappresentanti delle autorità di controllo designate dagli Stati membri e di un rappresentante della Commissione europea. Il gruppo – avente carattere consultivo e indipendente – non costituiva un superiore gerarchico dei Garanti nazionali, fungendo piuttosto come sede di confronto delle esperienze nazionali e di consulenza. V. in proposito A. DI MARTINO, *op.cit.*, p. 427.
[182] Sull'importante ruolo del Comitato europeo per la protezione dei dati personali v. *infra* par. 8.
[183] *Cfr.* il giudizio espresso in proposito dal Garante per la protezione dei dati personali nelle relazioni degli anni 2010-2019.
[184] Fonte dei dati: relazioni annuali del Garante per la protezione dei dati personali degli anni 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, reperibili al seguente *link* garanteprivacy.it.

Il *focus* dell'indagine, infatti, non è la cooperazione fra poteri pubblici a livello globale, ma bensì la sua evoluzione all'interno dell'Unione europea. Per agevolare la riflessione sui dati raccolti si è elaborato il seguente grafico, che riporta sull'asse delle ordinate sia le riunioni del Gruppo art. 29 o del Comitato europeo (in colore blu) sia gli incontri dei sottogruppi di lavoro (in colore rosso).

Grafico n. 3: numero di riunioni e partecipazioni a sottogruppi di lavoro nell'ambito del Gruppo art. 29 e, successivamente alla sua istituzione, del Comitato europeo per la protezione dei dati personali.



Osservando il grafico n. 3 colpisce, innanzitutto, l'andamento della linea rossa. Le partecipazioni a sottogruppi, sempre comprese fra 22 e 32 nel periodo 2010-2014, registrano un deciso aumento nella seconda metà del grafico, passando dalle 36 del 2015 alle 73 del 2019. L'incremento è particolarmente significativo negli ultimi due anni – 2018 e 2019 – nei quali si sono aggiunti rispettivamente 13 e 14 incontri rispetto all'anno precedente. Per comprendere la portata di quest'ultima crescita si consideri che, rispetto al 2017, nel 2019 vi sono state 27 partecipazioni a sottogruppi in più, pari al numero degli incontri tenutisi nell'arco di un intero anno, in media, fra il 2010 e il 2014[185].

Senz'altro meno appariscente è la rappresentazione, tracciata dalla linea blu, delle riunioni del Gruppo art. 29 o del Comitato europeo. Preso atto della stabilità del *trend* in quasi tutto il decennio considerato,

[185] (23 + 31 + 30 + 32 + 22) / 5 = 27,6.

va comunque rimarcato che nel 2019 si sono tenute il doppio delle riunioni rispetto a quelle che si svolgevano annualmente dal 2010 al 2017. Una più attenta analisi, inoltre, conduce a rilevare che nei cinque anni fra il 2010 e il 2014 vi sono state in totale 25 riunioni del Gruppo art. 29 o del Comitato europeo (con la media di cinque all'anno), mentre nel successivo quinquennio 2015-2019 si sono registrate in totale 35 sessioni plenarie (media di sette all'anno). Seppur in modo molto più contenuto, quindi, anche la tendenza della linea blu può essere considerata ascendente.

L'intensità della frequenza degli incontri fra Garanti permette un costante controllo delle decisioni e degli orientamenti interpretativi delle autorità omologhe, le cui attività quindi assumono, anche indirettamente, un rilievo sovranazionale[186]. All'esito dell'esame della tabella n. 4 e del grafico n. 3 quindi si manifesta, anche sul piano pratico-applicativo, un aumento dell'integrazione europea nell'attività amministrativa di protezione dei dati personali. In questo senso, appare progressivamente realizzarsi uno degli obiettivi che, con il regolamento (UE) 2016/679, si era prefissato il legislatore dell'Unione europea: quello di incrementare la collaborazione fra Garanti della *privacy* nazionali.

L'intensificarsi delle relazioni fra le autorità di controllo dei diversi Stati membri, pertanto, ha condotto alla formazione di un *network* di sorveglianza a presidio del diritto in esame e dell'uniformità della sua tutela[187]. In questo quadro, ciascuna autorità amministrativa indipendente preposta alla tutela della *privacy* – avendo peraltro assunto la capacità di adottare decisioni vincolanti anche al di fuori del territorio nazionale in cui opera – riveste ormai il ruolo di Garante della protezione dei dati personali su scala europea[188].

Conseguentemente, in questi ultimi anni appare essersi rafforzata la c.d. «*dimensione orizzontale*»[189] del costituzionalismo multilivello, intesa come l'insieme dei legami e degli strumenti di coordinamento fra le pubbliche amministrazioni statali – nonché fra le magistrature dei Paesi membri, come emergerà *infra* al par. seguente – all'interno dell'Unione europea. Si è assistito, infatti, non solo all'astratta previsione normativa di nuovi e vincolanti strumenti di collaborazione, ma altresì a una maggiore interazione in concreto fra le autorità di controllo nazionali.

---

[186] I. PERNICE, *The Treaty of Lisbon: Multilevel Constitutionalism in Action*, in *Columbia Journal of European Law*, vol. 15, n. 3/2009, 2009, pp. 382 e 383, pone l'accento sull'importanza che riveste, nel quadro della dimensione orizzontale del costituzionalismo multilivello, l'interesse delle persone di un Paese membro per le politiche che vengono applicate in un altro.

[187] M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 519. Più in generale v. P. CRAIG, *EU Administrative Law*, Third Edition, Oxford University Press, 2018.

[188] In questo senso v. M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, cit., *passim*, i quali infatti utilizzano l'espressione «*autorità decentrata di esecuzione del diritto europeo*».

[189] I. PERNICE, *The Treaty of Lisbon: Multilevel Constitutionalism in Action*, cit., pp. 379-383. *Cfr.* R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, cit., p. 61 e ss.

7. Gli strumenti di coordinamento della tutela giurisdizionale: il rinvio pregiudiziale alla Corte di Giustizia e la sospensione delle azioni *ex* art. 81 regolamento (UE) 2016/679

L'ordinamento europeo, come anticipato, oltre ai meccanismi amministrativi di cooperazione e coerenza, contiene altresì degli strumenti che consentono di agevolare la tutela giurisdizionale *integrata* del diritto alla protezione dei dati personali. A questo proposito, i due principali istituti previsti dal diritto dell'Unione sono il rinvio pregiudiziale alla Corte di Giustizia (art. 267 TFUE) e la sospensione delle azioni pendenti innanzi a giudici di diversi Paesi membri (art. 81 GDPR)[190]. Entrambi assolvono alla funzione di favorire sul piano giudiziario l'omogeneità della *Data protection* e, con essa, la certezza del diritto e lo sviluppo del mercato interno dei dati.

Il rinvio pregiudiziale alla Corte di Lussemburgo costituisce il primo strumento, avente carattere generale, volto ad assicurare l'unitarietà della nozione europea di protezione dei dati personali nell'applicazione giurisprudenziale[191]. Come noto, avvalendosi di tale mezzo il giudice nazionale può – e, se di ultima istanza, deve[192] – sottoporre le questioni relative alla validità o all'interpretazione degli atti adottati da istituzioni, organi od organismi dell'Unione, oltre che quelle concernenti l'interpretazione dei Trattati. Questo istituto dunque mira a garantire, in chiave nomofilattica[193], l'uniforme applicazione del diritto dell'UE, operando al contempo, nell'ambito dell'integrazione dei sistemi giuridici, come *trait d'union* fra i livelli nazionale e unionale[194]. È stato efficacemente definito, difatti, lo «*strumento principe*»[195] della connessione fra i due ordinamenti.

Come anticipato *supra* al par. 3, in tema di *Data Protection* il rinvio pregiudiziale assume un peculiare rilievo nei casi di trattamento transfrontaliero, qualora avverso un provvedimento dell'autorità di controllo – che sia attuativo di una decisione del Comitato – venga proposta impugnazione. In siffatta ipotesi, il

---

190 Sull'applicabilità dell'art. 81 regolamento (UE) 2016/679 in luogo della disciplina generale dettata dal regolamento (UE) 2012/1215 v. *infra* in questo stesso par. Sul rapporto fra giudici ordinari e integrazione europea v. *amplius* R. CONTI, *La giurisdizione ordinaria nel processo di integrazione europea*, in *Le trasformazioni istituzionali a sessant'anni dai Trattati di Roma*, A. Ciancio (a cura di), Torino, Giappichelli, 2017, p. 75 e ss.

191 Sui caratteri generali del rinvio pregiudiziale si rimanda, per tutti, a: C. SCHEPISI, *Rinvio pregiudiziale obbligatorio ed effettività della tutela giurisdizionale*, Trieste, Edizione Università Trieste, 2003; E. D'ALESSANDRO, *Il procedimento pregiudiziale interpretativo dinanzi alla Corte di Giustizia. Oggetto ed efficacia della pronuncia*, Torino, Giappichelli, 2012; R. CONTI, *Il rinvio pregiudiziale alla Corte di giustizia: dalla pratica alla teoria*, in *QuestioneGiustizia.it*, 7 maggio 2013; T. GUARNIER, *Ruolo e funzioni del rinvio pregiudiziale nell'interpretazione delle direttive dell'Unione europea: il caso della relazione fra giudici italiani e Corte di Giustizia*, in *Federalismi.it*, 17 febbraio 2017; G. TESAURO, *Sui vincoli (talvolta ignorati) del giudice nazionale prima e dopo il rinvio pregiudiziale: una riflessione sul caso* Avastin/Lucentis *e non solo*, in *Federalismi.it*, 18 marzo 2020.

192 Art. 267 par. 3 TFUE. V. anche G. TESAURO, *Sui vincoli (talvolta ignorati) del giudice nazionale prima e dopo il rinvio pregiudiziale: una riflessione sul caso* Avastin/Lucentis *e non solo*, cit., p. 195 e ss.

193 Evidenzia la funzione nomofilattica del rinvio pregiudiziale, nonché la sua essenziale importanza nel processo di integrazione europea, A. CIANCIO, *Perché un diritto costituzionale europeo? Quattro brevi risposte a partire dalle elezioni del 2019*, in *Federalismi.it*, 5 giugno 2019, p. 5.

194 T. GUARNIER, *Ruolo e funzioni del rinvio pregiudiziale nell'interpretazione delle direttive dell'Unione europea: il caso della relazione fra giudici italiani e Corte di Giustizia*, cit., p. 2. *Cfr.* G. TESAURO, *Sui vincoli (talvolta ignorati) del giudice nazionale prima e dopo il rinvio pregiudiziale: una riflessione sul caso* Avastin/Lucentis *e non solo*, cit., p. 192 e ss.

195 M. LUCIANI, *Interpretazione conforme a Costituzione*, in *Enc. dir.*, Annali, IX, Milano, 2014, p. 453.

giudice adito, ancorché non reputi la decisione del Comitato conforme alla normativa unionale, non può disporne l'annullamento o disapplicarla[196] – in quanto è emessa da un organismo dell'UE – ma deve deferire la questione di validità alla Corte di Giustizia attraverso l'art. 267 TFUE[197]. Non sembra improprio sostenere che il giudice investito dell'impugnazione non possa, tantomeno, annullare il provvedimento dell'autorità di controllo che attua la decisione del Comitato. Opinando diversamente, invero, sarebbero aggirate sia il carattere vincolante della decisione del Comitato, sia la funzione uniformatrice propria del meccanismo di coerenza[198].

Anche la speciale disciplina della sospensione delle azioni giurisdizionali, contenuta all'art. 81 regolamento (UE) 2016/679, contribuisce all'uniforme applicazione della *Data protection*. Come già esposto *supra* al par. 4, sulla base del *considerando* n. 147 regolamento (UE) 2016/679 e dell'art. 67 regolamento (UE) 2012/1215, le norme contenute nell'art. 81 GDPR derogano – in quanto *lex specialis* – quelle del regolamento *Bruxelles I-bis*[199]. In caso pendano contemporaneamente una pluralità di azioni innanzi a giudici di diversi Paesi membri, quindi, il primo riferimento normativo dell'interprete non è il regolamento (UE) 2012/1215, ma bensì il regolamento (UE) 2016/679[200]. Resta fermo, beninteso, che per gli aspetti non disciplinati da quest'ultimo atto troverà residualmente applicazione il regolamento *Bruxelles I-bis*[201].

Tanto premesso, è da chiarire che la sospensione delle azioni giurisdizionali si articola in tre diverse iniziative, tutte finalizzate a prevenire o evitare conflitti fra giudicati[202].

La prima vincola l'autorità giurisdizionale competente di uno Stato dell'UE a prendere contatto con l'autorità giudiziaria dell'altro Paese membro, al fine di confermare l'eventuale esistenza di più azioni

196 A. BARLETTA, *La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della aterritorialità") di Internet*, cit., nota n. 45.

197 A. BARLETTA, *op.cit.*, par. 5. V. anche *considerando* n. 143 regolamento (UE) 2016/679.

198 V. *amplius* sul tema *supra* par. 3.

199 F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel Regolamento "*Bruxelles I-bis*"*, cit., p. 458 e ss. L'A., in particolare, non giudica opportuna la scelta del legislatore europeo di discostarsi dalla disciplina generale posta nel regolamento (UE) 2012/1215, dubitando della rispondenza di tale opzione legislativa alla finalità di assicurare una tutela giurisdizionale effettiva del diritto alla protezione dei dati personali. V. anche L. CANNADA-BARTOLI, *Considerazioni su alcune norme in materia di giurisdizione contenute nel regolamento generale sulla protezione dati n. 2016/679*, in *Europa e Diritto Privato*, fasc. n. 3/2018, p. 1021.

200 *Cfr.* A. BARLETTA, *op.cit.*, *passim*.

201 F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel Regolamento "*Bruxelles I-bis*"*, cit., pp. 461 e 462.

202 A. PEDUTO, *Art. 81*, in *GDPR e normativa privacy. Commentario*, G.M. Riccio, G. Scorza, E. Belisario (a cura di), Milano-Vicenza, Wolters Kluwer, 2018, p. 593. In proposito v. anche: A. CANDINI, *op.cit.*, p. 591 e ss.; R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1014 e ss.

pendenti[203]. L'obbligo in capo al giudice investito della controversia si attiva quando egli ha conoscenza[204] di azioni concernenti lo stesso oggetto, relativamente al trattamento dello stesso titolare o responsabile, pendenti presso un'autorità giurisdizionale appartenente a un differente Stato dell'Unione[205]. È posto, così, un generale obbligo di informazione reciproca tra le autorità giudiziarie dei Paesi dell'Unione[206].

Discostandosi dal modello del regolamento (UE) 2012/1215, il legislatore europeo ha deciso di non distinguere le ipotesi della litispendenza e della connessione, delineando così, nel coordinamento tra procedimenti paralleli, un regime giuridico ibrido[207]. L'art. 81 par. 1 GDPR, peraltro, non richiede il rispetto di particolari formalità nell'interazione fra autorità giurisdizionali, di talché appaiono utilizzabili i punti di contatto della Rete giudiziaria europea di cui alle decisioni 2001/470/CE e 568/2009/CE[208]. Questa prima iniziativa, invero, è propedeutica all'attivazione delle soluzioni applicabili dal giudice qualora realmente sussistano più azioni[209].

Nell'ipotesi in cui l'azione – avente il medesimo oggetto relativamente al trattamento dello stesso titolare o responsabile – penda effettivamente presso un'altra autorità giurisdizionale in un diverso Paese membro, l'art. 81 par. 2 GDPR prevede la possibilità, per qualunque giudice competente adito successivamente, di sospendere il processo di cui è investito. Tale seconda iniziativa, a differenza della prima, ha natura facoltativa, essendo rimessa all'autorità giudiziaria successivamente adita la valutazione

[203] La natura obbligatoria della previsione, contenuta nel primo par. dell'art. 81 GDPR, si desume dell'uso dell'indicativo presente nella versione italiana («*prende contatto*»), e del verbo ausiliario «*shall*» nella versione inglese. *Conf.* A. PEDUTO, *Art. 81*, cit., p. 595.

[204] Autonomamente o attraverso l'attività informativa delle parti: così A. PEDUTO, *Art. 81*, cit., p. 594.

[205] Il mutare dell'oggetto dell'azione oppure del titolare o del responsabile del trattamento, quindi, preclude l'applicabilità della disciplina della sospensione delle azioni *ex* art. 81 regolamento (UE) 2016/679. Una indicazione interpretativa in merito al legame che deve esistere fra le azioni pendenti è desumibile dal *considerando* n. 144, ultimo periodo, regolamento (UE) 2016/679, ai sensi del quale «*Le azioni sono considerate connesse quando hanno tra loro un legame così stretto da rendere opportuno trattarle e decidere in merito contestualmente, per evitare il rischio di sentenze incompatibili risultanti da azioni separate*». A. PEDUTO, *Art. 81*, cit., p. 595, evidenzia come il riferimento alla connessione fra le azioni, contenuto nel suddetto *considerando*, non debba intendersi in senso tecnico, ma piuttosto in modo ampio. Dello stesso avviso è anche R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit. p. 1014.

[206] A. BARLETTA, *op.cit.*, *passim*, ma in particolare par. 4.

[207] F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel Regolamento "*Bruxelles I-bis*"*, cit., pp. 459 e 460. L'A., a p. 461, rileva comunque come il coordinamento tra procedimenti paralleli previsto dall'art. 81 GDPR presenti una maggiore affinità con la disciplina della connessione, piuttosto che della litispendenza. Per un approfondimento sui requisiti dell'identità del titolo e dei soggetti v. *ibidem*.

[208] La condivisibile intuizione è di A. PEDUTO, *Art. 81*, cit., p. 594. Sulla struttura e le funzioni della Rete giudiziaria europea in materia civile e commerciale v. la Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle attività della rete giudiziaria europea in materia civile e commerciale del 10 marzo 2016, reperibile al *link* eur-lex.europa.eu. Sul futuro della Rete dopo la pandemia di Covid-19, v. anche L. PERILLI, *La pandemia cambierà anche la formazione internazionale?*, in *QuestioneGiustizia.it*, 4 maggio 2020.

[209] A. PEDUTO, *Art. 81*, cit., p. 594.

dell'opportunità di procedere, o meno, con la sospensione, in attesa che il giudice precedentemente investito definisca la controversia[210].

L'ultima soluzione contemplata in caso sussista realmente una pluralità di azioni davanti a giudici di più Stati membri è, ai sensi dell'art. 81 par. 3 GDPR, la dichiarazione della propria incompetenza (o meglio, del difetto di giurisdizione[211]) da parte dell'autorità giudiziaria adita in un secondo tempo. Questa misura presuppone l'esistenza di alcuni requisiti: occorre, infatti, che le azioni siano pendenti in primo grado, e che una parte del processo abbia presentato la richiesta di dichiarare l'incompetenza del giudice. Inoltre, è necessario che «*l'autorità giudiziaria adita per prima sia competente a conoscere delle domande proposte*»[212], e che la normativa nazionale applicata dal primo giudice permetta la riunione dei processi[213]. Se l'autorità giurisdizionale adita per prima non si ritiene competente, quella investita successivamente può riassumere il processo[214].

La disciplina posta dall'art. 81 regolamento (UE) 2016/679, confrontata con quella generale dettata dal regolamento (UE) 2012/1215, non presenta un elevato grado di completezza e sistematicità[215], sicché il concreto coordinamento tra processi paralleli relativi alla protezione dei dati personali necessiterà, con ogni probabilità, di fare riferimento in chiave integrativa alle regole contenute nel regolamento *Bruxelles I-bis*[216].

Alla luce delle considerazioni sinora svolte, emerge che la sospensione delle azioni – consentendo alle autorità giudiziarie di declinare la propria giurisdizione a vantaggio di giudici di un diverso Stato dell'Unione – si inscrive pienamente nel quadro del coordinamento fra le autorità giudiziarie dei Paesi membri[217]. Si tratta di uno strumento utile in un'ottica di economia processuale, consentendo lo svolgimento congiunto delle attività di trattazione, istruzione e decisione delle azioni[218]. Ma soprattutto, in considerazione dell'aumento dei casi di trattamento transfrontaliero di dati personali[219], può consentire

---

210 A. CANDINI, *op.cit.*, p. 592; R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit. p. 1016; A. BARLETTA, *op.cit.*; F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel Regolamento "*Bruxelles I-bis*"*, cit., p. 461.

211 R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit., p. 1015.

212 Così l'art. 81, par. 3, regolamento (UE) 2016/679.

213 A. PEDUTO, *Art. 81*, cit., p. 595.

214 R. GIORDANO, *La tutela amministrativa e giurisdizionale dei dati personali*, cit. p. 1016.

215 F. MARONGIU BUONAIUTI, *La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel Regolamento "*Bruxelles I-bis*"*, cit., p. 463.

216 A questo proposito, secondo F. MARONGIU BUONAIUTI, *op.cit.*, p. 463, sarebbe stato preferibile l'inserimento da parte del legislatore europeo, nel testo dell'art. 81 GDPR o a chiusura del capo VIII GDPR, di «*specifiche disposizioni di coordinamento atte a chiarire in quali termini le regole in questione siano destinate ad essere integrate dalle disposizioni pertinenti del regolamento "Bruxelles I-*bis*"*».

217 A. PEDUTO, *Art. 81*, cit., p. 595. Sul piano normativo, v. il menzionato regolamento (UE) 2012/1215.

218 A. CANDINI, *op.cit.*, p. 592. Anche A. BARLETTA, *op.cit.*, *passim*, evidenzia l'utilità di non disperdere vanamente attività processuali finalizzate alla tutela del diritto alla protezione dei dati personali.

219 Sul punto si rinvia *supra* par. 5.

di ovviare ad alcuni problemi derivanti dall'applicazione del meccanismo "*one stop shop*" di cui all'art. 60 GDPR.

L'individuazione dell'autorità capofila, infatti, se elimina l'incertezza intorno al Garante cui domandare la tutela amministrativa del diritto, può tuttavia comportare una insicurezza in relazione all'esercizio della tutela giurisdizionale[220]. Si pensi al caso in cui, avendo l'autorità capofila e gli altri Garanti interessati convenuto di archiviare o rigettare parti di un reclamo e di intervenire su altre parti dello stesso, venga adottata una decisione separata per ciascuna di tali parti[221]. In questo caso spetta all'autorità di controllo adita dal reclamante adottare la decisione per la porzione riguardante l'archiviazione o il rigetto del reclamo, e all'autorità capofila adottare la decisione per la parte concernente l'accoglimento del reclamo, che quindi prevede le azioni in relazione al titolare del trattamento[222]. Conseguentemente, ben può verificarsi che il reclamante impugni la decisione del Garante nazionale che archivia o rigetta il reclamo innanzi al giudice del proprio Stato membro, e che il titolare impugni la decisione dell'autorità capofila, per la componente che accoglie il reclamo, davanti al giudice del Paese dell'autorità capofila[223].

La sospensione delle azioni può costituire un rimedio efficace contro tali incertezze. Le autorità giudiziarie potrebbero evitare, mediante lo scambio di informazioni e il confronto reciproco, la pronuncia parallela di decisioni dal contenuto confliggente. Ma perché lo strumento di cui all'art. 81 GDPR possa funzionare al meglio, a ben vedere, occorre che l'interazione fra le autorità giudiziarie sia agevole ed efficiente. A questo scopo, serve una solida Rete giudiziaria europea in materia civile e commerciale[224].

8. Il meccanismo di coerenza e la funzione *nomofilattica* del Comitato europeo per la protezione dei dati

Qualora le forme di cooperazione amministrativa fra Garanti nazionali[225] non conducessero a una soluzione condivisa in merito alla decisione da adottare, l'ordinamento europeo prevede l'attivazione del meccanismo di coerenza[226]. Tale procedimento si pone, dunque, quale eccezione rispetto alla regola del

[220] M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, cit.; A. CASELLI, *Artt. 58-67*, cit., pp. 515 e 516.

[221] Art. 60, par. 9, regolamento (UE) 2016/679. V. anche *supra* par. 5.

[222] Sui corrispondenti obblighi di notifica e di informazione v. ancora l'art. 60, par. 9, regolamento (UE) 2016/679.

[223] Ai sensi dell'art. 78 par. 3 regolamento (UE) 2016/679, infatti, «*Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita*». Sul problema appena esaminato v. A. CASELLI, *Artt. 58-67*, cit., pp. 514, 515 e 516.

[224] Anche per conseguire tale obiettivo è stato recentemente istituito il portale https://aldricus.giustizia.it/#.

[225] Illustrate *supra* ai parr. 5 e 6.

[226] Poiché coinvolge, oltre le autorità di controllo, anche il Comitato e la Commissione europea, il meccanismo di coerenza si pone al di sopra delle forme di cooperazione fra Garanti di cui agli art. 60 e ss. regolamento (UE) 2016/679: così anche M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 538.

consenso contenuta nell'art. 60 par. 1 GDPR[227], ed è finalizzato ad assicurare l'omogeneità applicativa in tutta l'Unione della disciplina comune sulla protezione dei dati personali[228]. Il rafforzamento della rete europea delle autorità amministrative indipendenti, pertanto, si sostanzia altresì in una procedura che consente di addivenire, in caso di contrasto fra le diverse *Authorities* coinvolte, a una decisione vincolante assunta dal Comitato sul tema dibattuto[229].

Più in particolare, il Comitato dovrà adottare una decisione vincolante se l'obiezione «*pertinente e motivata*»[230] sollevata da un'autorità di controllo interessata avverso il progetto di decisione dell'autorità capofila (così come descritto all'art. 60 par. 4 GDPR[231]) sia da questa ritenuta non pertinente o non motivata, oppure ove l'autorità capofila non dia seguito all'obiezione[232]. La decisione deve essere approvata dalla maggioranza qualificata di due terzi dei membri del Comitato e deve vertere su tutte le questioni oggetto dell'obiezione pertinente e motivata[233].

Il provvedimento finale del Comitato, adottato entro un mese dal deferimento della questione[234] da parte dell'autorità capofila[235], deve inoltre essere motivato e trasmesso sia a quest'ultima, sia a tutte le altre autorità di controllo interessate[236]. Ad esse – allo scopo di assicurare la certezza del diritto, l'effettività della scelta del Comitato e la sua funzione nomofilattica – è negata la possibilità di adottare decisioni sulla

---

227 A. CASELLI, *Artt. 58-67*, cit., p. 512. L'A., a p. 529, ribadisce la funzione residuale del meccanismo di coerenza rispetto a quello di cooperazione.

228 M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 533. V. anche l'art. 63 regolamento (UE) 2016/679.

229 In proposito v.: A. CASELLI, *Artt. 58-67*, cit., p. 527 e ss.; P. BALBONI, E. PELINO, L. SCUDIERO, *Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation*, cit., p. 397 e ss.; M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, cit., *passim*; M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 533 e ss.; A. RALLO LOMBARTE, R. GARCÍA MAHAMUT, J.A. VIGURI CORDERO, *Cooperación y coordinación entre autoridades de proteccion de datos*, cit., p. 739 e ss.

230 Art. 60, par. 4, regolamento (UE) 2016/679. Su tale nozione v. *supra* par. 5.

231 Sul procedimento per l'adozione della decisione dell'autorità capofila nell'ambito dei meccanismi di cooperazione v. *supra* par. 5.

232 Artt. 65, par. 1, lett. a) e 65, par. 2, regolamento (UE) 2016/679. V. anche M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 544 e ss. e A. CASELLI, *Artt. 58-67*, cit., p. 541, il quale evidenzia come la decisione del Comitato non possa travalicare i limiti dell'obiezione sottoposta alla sua attenzione.

233 A. CASELLI, *Artt. 58-67*, cit., p. 538, sottolinea come tale decisione sia direttamente impugnabile dai soggetti interessati dinnanzi alla Corte di Giustizia dell'Unione.

234 Ai sensi dell'art. 65 par. 2 regolamento (UE) 2016/679, questo termine, in considerazione della complessità della questione, può essere prorogato di un mese. Il terzo paragrafo dell'art. 65 GDPR, tuttavia, contempla una ulteriore possibilità di proroga ove il Comitato non sia stato in grado di adottare una decisione entro i suddetti termini. In tal caso, «*il comitato adotta la sua decisione entro due settimane dalla scadenza del secondo mese di cui al paragrafo 2, a maggioranza semplice dei membri del comitato. In caso di parità di voti dei membri del comitato, prevale il voto del presidente*».

235 L'art. 60 par. 4, regolamento (UE) 2016/679 prevede, infatti, che sia compito dell'autorità capofila sottoporre la questione controversa al meccanismo di coerenza.

236 Art. 65 par. 2 regolamento (UE) 2016/679. Il quinto paragrafo dell'art. 65 GDPR precisa poi che spetta al presidente del Comitato il compito di notificare, senza ingiustificato ritardo, la decisione vincolante, nonché di informare di essa la Commissione europea. La decisione del Comitato, peraltro, deve essere pubblicata senza ritardo sul suo sito *web*, «*dopo che l'autorità di controllo ha notificato la decisione definitiva di cui al paragrafo 6*».

questione sottoposta al meccanismo di coerenza prima della scadenza dei termini per la formulazione della decisione vincolante[237].

A seguito della notifica della decisione vincolante da parte del Comitato, l'autorità capofila – o, se del caso, l'autorità di controllo a cui è stato proposto il reclamo – è tenuta ad adottare, senza ingiustificato ritardo e al più tardi entro un mese dalla ricezione della notifica, la sua decisione definitiva[238]. Quest'ultima deve basarsi sulla decisione vincolante, a cui deve conformarsi[239] e fare espresso riferimento[240]. La decisione del Comitato, per di più, deve essere allegata al provvedimento definitivo dell'autorità capofila[241]. Il procedimento per l'adozione della decisione definitiva delle autorità di controllo interessate è il medesimo dettato dai parr. 7, 8 e 9 dell'art. 60 regolamento (UE) 2016/679[242], già descritto *supra* al par. 5, a cui dunque si rinvia.

Sino a oggi il Comitato ha pronunciato una sola decisione vincolante[243], sicché le autorità di controllo sono riuscite, finora costantemente, a raggiungere un accordo nonostante l'eventuale esistenza di divergenze interpretative[244].

Oltre all'ipotesi in cui fallisse il meccanismo di cooperazione consensuale fra Garanti, il descritto procedimento di composizione delle controversie – che vede il Comitato incarnare il ruolo di «*decisore ultimo*»[245] – trova applicazione anche quando vi sia un contrasto di opinioni circa la competenza delle autorità di controllo interessate per lo stabilimento principale[246] (art. 65, par. 1, lett. b) GDPR), oppure ove un'autorità di controllo competente non richieda il parere del Comitato o non si conformi a esso[247] (art. 65, par. 1, lett. c) GDPR).

---

237 Art. 65 par. 4 regolamento (UE) 2016/679.

238 Ai sensi dell'art. 65 par. 6 regolamento (UE) 2016/679, l'autorità capofila, o l'autorità di controllo a cui è stato proposto il reclamo, è tenuta a informare il Comitato sulla data in cui la decisione definitiva viene notificata all'interessato e al titolare o al responsabile del trattamento. Lo scopo di questo sistema di notifiche, come rileva A. CASELLI, *Artt. 58-67*, cit., pp. 543 e 544, è di consentire l'eventuale impugnazione *ex* art. 263 TFUE davanti alla Corte di Lussemburgo della decisione del Comitato.

239 M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 547.

240 Con la precisazione, richiesta dall'art. 65 par. 6 regolamento (UE) 2016/679, che la decisione vincolante del Comitato sarà pubblicata sul suo sito *web*.

241 Art. 65 par. 6 regolamento (UE) 2016/679. Sul carattere giuridicamente vincolante di queste decisioni del Comitato v. anche il *considerando* n. 136 regolamento (UE) 2016/679.

242 Art. 65 par. 6 regolamento (UE) 2016/679.

243 Si tratta della decisione adottata il 9 novembre 2020. Sul caso concreto si rinvia al sito ufficiale edpb.europa.eu.

244 Lo constata lo stesso Comitato europeo nel suo 2018 *Annual Report*, *Cooperation & Transparency*, p. 13, reperibile al seguente *link* edpb.europa.eu.

245 La medesima espressione è utilizzata da A. CASELLI, *Artt. 58-67*, cit., p. 538, e da V. ZAMBRANO, *Il Comitato europeo per la protezione dei dati*, in *I dati personali nel diritto europeo*, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Torino, Giappichelli, 2019, p. 999.

246 Per un approfondimento del tema si rimanda ad A. CASELLI, *Artt. 58-67*, cit., pp. 541 e 542.

247 In tale ipotesi, come chiarisce l'ultimo periodo dell'art. 64 par. 1 lett. c) GDPR, la questione può essere comunicata al Comitato da qualsiasi autorità di controllo interessata o dalla Commissione europea.

Il parere del Comitato costituisce un ulteriore importante strumento per assicurare la coerenza applicativa della disciplina europea sulla protezione dei dati personali[248]. L'art. 64 par. 1 regolamento (UE) 2016/679 elenca tassativamente[249] le misure per la cui adozione da parte dell'autorità di controllo competente[250] è obbligatorio, innanzitutto, comunicare il progetto di decisione al Comitato[251] e, in secondo luogo, ottenere il suo parere al riguardo[252].

Tale parere, tuttavia, può anche essere discrezionalmente richiesto[253] – da parte di qualsiasi autorità di controllo, della Commissione europea o del presidente del Comitato[254] – in merito a questioni di applicazione generale, o che possono produrre effetti in più di uno Stato membro. In queste ipotesi, dunque, sottoporre i problemi interpretativi all'esame del Comitato è facoltativo, e non obbligatorio.

In ogni caso il parere del Comitato deve essere adottato[255] entro otto settimane[256] e a maggioranza relativa dei membri dell'organismo. Per garantire la completezza degli elementi utili ai fini della formulazione dell'opinione del Comitato, le autorità di controllo e la Commissione devono comunicargli[257] una sintesi dei fatti, il progetto di decisione, le ragioni per le quali è necessaria l'attuazione della misura e i pareri delle altre autorità di controllo interessate[258].

---

[248] Sul punto v.: M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 540 e ss.; A. CASELLI, *Artt. 58-67*, cit., p. 530 e ss.

[249] Sull'esaustività dell'elenco di cui all'art. 64 par. 1 GDPR v. A. CASELLI, *Artt. 58-67*, cit., pp. 532 e 533.

[250] In caso di trattamento transfrontaliero di dati personali l'autorità di controllo competente è da individuarsi nell'autorità capofila *ex* art. 60 regolamento (UE) 2016/679. V. *amplius* sul punto A. CASELLI, *Artt. 58-67*, cit., pp. 533 e 534.

[251] Il progetto di decisione trasmesso ai membri del Comitato in conformità all'art. 64 par. 5 GDPR si considera accolto dai membri dell'organismo che non hanno sollevato obiezioni entro il termine indicato dal presidente del Comitato. In proposito v. l'art. 64 par. 3 regolamento (UE) 2016/679.

[252] Fra le varie ipotesi enumerate dall'art. 64 par. 1 GDPR, si segnala per la sua importanza quella contenuta nella lett. a), che richiede la comunicazione del progetto di decisione al Comitato, allo scopo di ottenerne il parere, qualora la decisione dell'autorità di controllo sia «*finalizzata a stabilire un elenco di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4*». M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 542, rileva come tutte le misure delle autorità di controllo per cui è obbligatoriamente richiesto il previo parere del Comitato riguardino ipotesi in cui a queste ultime è riconosciuto un potere di attuazione della normativa unionale.

[253] L'art. 64, par. 2 regolamento (UE) 2016/679 precisa «*in particolare se un'autorità di controllo competente non si conforma agli obblighi relativi all'assistenza reciproca ai sensi dell'articolo 61 o alle operazioni congiunte ai sensi dell'articolo 62*».

[254] Sul carattere discrezionale di tali richieste v. A. CASELLI, *Artt. 58-67*, cit., p. 532, e M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., pp. 540, 542 e 543.

[255] Sempre che non abbia precedentemente emesso un parere sulla medesima questione, nel qual caso il Comitato ha la possibilità di rifiutarsi di adottarlo. *Cfr.* M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 543, e A. CASELLI, *Artt. 58-67*, cit., pp. 535 e 536.

[256] Il termine, ai sensi dell'art. 64 par. 3 regolamento (UE) 2016/679, può essere prorogato di sei settimane, tenendo conto della complessità della questione. A. CASELLI, *Artt. 58-67*, cit., pp. 534 e 535, si interroga sull'individuazione del *dies a quo* a partire dal quale decorre il computo del termine, e auspica un chiarimento sul punto da parte del regolamento del Comitato.

[257] Attraverso un modulo *standard* e per via elettronica. Agli obblighi informativi verso i membri del Comitato, la Commissione europea e l'autorità di controllo che gravano in capo al presidente del Comitato è dedicato il par. 5 dell'art. 64 GDPR, cui si rinvia per i relativi approfondimenti.

[258] Art. 64, par. 4, regolamento (UE) 2016/679.

L'autorità di controllo competente – che, ai sensi dell'art. 64 par. 1 GDPR, è obbligata a comunicare il progetto di decisione al Comitato per ottenerne il parere – non può adottare la decisione finale prima della formulazione dello stesso[259]. Successivamente all'emissione del parere, tale autorità, pur dovendo tenere «*nella massima considerazione*»[260] l'opinione del Comitato, può deliberare con motivazione pertinente di non conformarsi, in tutto o in parte, al medesimo[261]. In altre parole, l'autorità di controllo può stabilire di mantenere o modificare il progetto di decisione, anche in senso contrario al parere espresso dal Comitato. Questa scelta deve essere comunicata al presidente del Comitato e, come anticipato, conduce all'applicazione del procedimento di composizione delle controversie *ex* art. 65 regolamento (UE) 2016/679[262].

Il meccanismo di coerenza, così come la procedura consensuale di cui all'art. 60 GDPR, può subire delle deroghe[263] qualora sussistano delle circostanze eccezionali[264]. Ai sensi dell'art. 66 regolamento (UE) 2016/679, infatti, un'autorità di controllo interessata può adottare in modo immediato delle misure provvisorie, se reputa urgente intervenire per tutelare i diritti e le libertà degli interessati dal trattamento. Queste misure sono intese a produrre effetti giuridici nel territorio del Garante che le adotta, e il loro periodo di validità, necessariamente determinato nel tempo, non può superare i tre mesi[265].

Inoltre l'autorità che ha adottato i provvedimenti, se ritiene che sia urgente adottare misure definitive oltre a quelle provvisorie, può richiedere, motivando la richiesta, un parere d'urgenza o una decisione vincolante d'urgenza del Comitato[266]. In caso di inerzia dell'autorità di controllo competente nella

[259] Art. 64, par. 6, regolamento (UE) 2016/679.

[260] Così testualmente l'art. 64 par. 7 GDPR: sull'interpretazione di questa espressione v. A. CASELLI, *Artt. 58-67*, cit., p. 535.

[261] Art. 64, par. 8, regolamento (UE) 2016/679. Così anche M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 545.

[262] Ossia del procedimento per la composizione delle controversie da parte del Comitato. Sul procedimento per l'adozione del parere da parte del Comitato v. specificamente i parr. 7 e 8 dell'art. 64 GDPR e M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 543 e ss.

[263] Ad avviso di A. CASELLI, *Artt. 58-67*, cit., p. 545, stante la sua natura derogatoria, la procedura d'urgenza deve essere interpretata in chiave restrittiva.

[264] M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 547 e ss. L'A. condivide l'idea che, terminata la situazione di urgenza, i provvedimenti temporanei adottati non precludano il normale funzionamento dei meccanismi di cooperazione e di coerenza.

[265] Così prevede l'art. 66, par. 1, regolamento (UE) 2016/679, il quale altresì pone in capo all'autorità di controllo l'obbligo di comunicare senza ritardo agli altri Garanti interessati, al Comitato e alla Commissione le misure adottate e la loro motivazione.

[266] Art. 66, par. 2, regolamento (UE) 2016/679. Sul termine e il *quorum* per l'adozione di questi atti da parte del Comitato v. il par. 4 dell'art. 66 GDPR. Più in generale su questo tema v. M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., pp. 548 e 549. L'A. evidenzia, in particolare, come anche nell'ambito della procedura d'urgenza risulti rispettato il principio di collaborazione fra autorità di controllo.

situazione emergenziale, infine, i suddetti atti del Comitato possono essere domandati da qualsiasi autorità di controllo, attraverso una richiesta motivata con specifico riferimento al profilo dell'urgenza[267].

Poiché secondo il *considerando* n. 138 regolamento (UE) 2016/679 l'applicazione del meccanismo di coerenza «*dovrebbe essere un presupposto di liceità di una misura intesa a produrre effetti giuridici adottata dall'autorità di controllo nei casi in cui la sua applicazione è obbligatoria*», il mancato rispetto del meccanismo da parte di un'autorità di controllo comporta l'illegittimità della misura da questa adottata[268].

Al termine del succinto esame del meccanismo di coerenza di cui all'art. 63 e ss. regolamento (UE) 2016/679, è possibile apprezzare l'importanza del ruolo assunto dal Comitato nel quadro dell'uniformazione del diritto alla protezione dei dati personali all'interno dell'Unione[269].

L'obiettivo di superare le divergenze normative createsi fra Paesi membri durante la vigenza della direttiva 95/46/CE[270] ha infatti in questo nuovo organismo dell'Unione un fondamentale baluardo[271]. Al Comitato, in ragione della sua autorevole composizione[272], è attribuita una funzione di nomofilachia[273] che si esprime nel suo potere decisorio di ultima istanza[274]. La grande rilevanza del Comitato nell'architettura della *Data protection* europea è testimoniata, inoltre, dall'incremento dei suoi compiti e poteri rispetto al preesistente Gruppo art. 29[275]. In definitiva esso, come è stato efficacemente osservato, costituisce «*elemento unificatore armonizzante*»[276] e «*organo di chiusura del sistema*»[277] di protezione dei dati personali.

---

267 Art. 66, par. 3, regolamento (UE) 2016/679.

268 A. CASELLI, *Artt. 58-67*, cit., p. 529.

269 *Amplius* sul tema, comunque, v.: V. ZAMBRANO, *Il Comitato europeo per la protezione dei dati*, cit., p. 985 e ss.; L. PATTI, *Artt. 68-71*, in *GDPR e normativa privacy. Commentario*, G.M. Riccio, G. Scorza, E. Belisario (a cura di), Milano-Vicenza, Wolters Kluwer, 2018, p. 549 e ss.; M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 536; C. IPPOLITI MARTINI, *Comitato Europeo per la protezione dei dati*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, G. Finocchiaro (a cura di), Torino, Zanichelli, 2017, p. 552 e ss.

270 V. sul punto S. CALZOLAIO, *op.cit.*, p. 626, nonché i *considerando* nn. 9 e 10 regolamento (UE) 2016/679.

271 M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 534.

272 Il Comitato è composto dalle figure apicali dell'autorità di controllo di ciascun Paese membro e dal Garante europeo della protezione dei dati.

273 Parla di funzione e di attività «*nomofilattica*» del Comitato anche A. CASELLI, *Artt. 58-67*, cit., pp. 532 e 538.

274 Sull'atipicità dello schema dei meccanismi di cooperazione e coerenza nel quadro dell'integrazione amministrativa europea, caratterizzata da una maggiore verticalità in luogo della condivisione orizzontale delle scelte, si rimanda a M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, cit., *passim*. Gli AA. rilevano, in particolare, «*la tendenza a privilegiare un'attuazione decentrata del diritto europeo attraverso centri decisionali nazionali*».

275 M.S. ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, cit., p. 535; V. ZAMBRANO, *Il Comitato europeo per la protezione dei dati*, cit., p. 985. *Cfr.*, a questo proposito, il numero di disposizioni dedicate dalla direttiva 95/46/CE e dal regolamento (UE) 2016/679 rispettivamente al Gruppo art. 29 e al Comitato europeo per la protezione dei dati.

276 A. CASELLI, *Artt. 58-67*, cit., p. 529.

277 F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, cit., p. 104.

9. La protezione dei dati personali, una storia di integrazione europea

Alla luce dei risultati dell'indagine compiuta, si ritiene che le istituzioni statali possano tuttora assicurare la tutela del diritto[278], ma necessariamente in una cornice di crescente coordinamento all'interno dell'Unione europea: l'esistenza di una disciplina sostanzialmente unitaria, infatti, richiede che sia i Garanti nazionali, sia le autorità giurisdizionali addivengano a interpretazioni coerenti del comune dettato normativo. In questo senso, le predette novità introdotte dal regolamento (UE) 2016/679 sul piano rimediale hanno comportato, invero, un passo in avanti nel processo di integrazione europea nella protezione dei dati personali[279].

Si consideri, a tal proposito, l'innovatività[280] del procedimento dello sportello unico di cui all'art. 60 GDPR, il quale, mediante la cooperazione fra le autorità di controllo coinvolte, tenta di assicurare l'omogeneità della *Data protection* nell'Unione[281]. Ancora, la tipizzazione dell'assistenza reciproca e delle operazioni congiunte – istituti finalizzati a tutelare i diritti degli interessati nei rispettivi Paesi membri, indipendentemente dalla collocazione territoriale dei titolari e responsabili del trattamento[282] – mira a superare i confini nazionali, assumendo una prospettiva di protezione euro-unitaria[283].

La transizione dalla direttiva 95/46/CE al regolamento (UE) 2016/679, inoltre, ha implicitamente modificato il ruolo delle autorità indipendenti, le quali, essendo chiamate a vigilare sull'osservanza di norme poste direttamente dal GDPR[284], e avendo assunto la capacità di adottare decisioni vincolanti anche al di fuori del territorio statale in cui operano[285], rivestono ormai il ruolo di Garanti della protezione dei dati personali su scala europea[286].

In sintesi, rispetto all'assetto antecedente la riforma del 2016, la disciplina vigente presenta più estese forme di cooperazione consensuale fra Garanti nazionali e, in caso di loro fallimento, nuove soluzioni

---

278 Come emerso nei parr. 2, 3 e 4, infatti, i rimedi previsti dall'ordinamento (reclamo all'autorità di controllo, ricorso innanzi a un giudice avverso le decisioni di tale autorità, ricorso giurisdizionale *diretto*) non sono rimasti relegati su un piano meramente teorico, ma sono stati concretamente esperiti nel corso del tempo, a riprova dell'effettività della tutela che attraverso di essi veniva accordata.

279 Come già precedentemente chiarito, questa riflessione è limitata, pertanto, alla disciplina generale sulla protezione dei dati personali prevista dal regolamento (UE) 2016/679. Altre forme di collaborazione fra autorità di controllo nazionali sono contenute, per esempio, nella direttiva 2016/680/UE (artt. 50 e 51).

280 Sottolinea la portata innovativa del meccanismo "*one stop shop*" A. CASELLI, *Artt. 58-67*, cit., p. 506. V. anche M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 516 e ss.

281 F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, cit., p. 103.

282 J. POLONETSKY, *Molto più del rispetto delle norme*, cit., p. 40.

283 Come rileva V. RIZZO, *Artt. 55-56*, cit., p. 469, all'interno di una cornice normativa condivisa è il principio stesso della certezza del diritto a richiedere che ogni autorità amministrativa indipendente conosca come la comune disciplina viene applicata dalle altre.

284 E non più, invece, sul rispetto di legislazioni nazionali, sia pure attuative di regole comunitarie. *Cfr.* E. GUARDIGLI, *Le Autorità di controllo*, cit., p. 493.

285 V. in proposito *supra* par. 5.

286 V. M. MACCHIA, C. FIGLIOLIA, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, cit., *passim*, i quali infatti ricorrono all'espressione «*autorità decentrata di esecuzione del diritto europeo*».

per comporre le divergenze interpretative tra loro insorte. Nonostante la difesa del diritto rimanga in larga misura prerogativa delle istituzioni nazionali[287] – si pensi al reclamo all'autorità di controllo, al ricorso innanzi a un giudice avverso le decisioni di tale autorità, al ricorso giurisdizionale *diretto*, precedentemente analizzati – si registra quindi, specie in caso di trattamento transfrontaliero di dati personali, un accresciuto rilievo del livello ordinamentale europeo. La disciplina comune unionale della protezione dei dati personali, come già chiarito, non può d'altronde prescindere dall'esistenza di un *enforcement* che ne assicuri l'effettiva unitarietà in concreto[288].

All'avanzamento dell'integrazione sul piano normativo si aggiunge, peraltro, un incremento delle interazioni fra autorità di controllo sul piano pratico-applicativo, come risulta dall'esame della tabella n. 4 e del grafico n. 3[289]. L'intensità della frequenza dei loro incontri, infatti, permette un controllo regolare delle decisioni e degli orientamenti interpretativi delle autorità omologhe, le cui attività quindi assumono, anche indirettamente, un rilievo sovranazionale. La costanza delle relazioni reciproche genera, altresì, un *network* di sorveglianza a presidio del diritto e dell'uniformità della sua tutela[290].

Tali considerazioni inducono a rilevare che, in questa materia, le relazioni fra i Garanti della *privacy* dei diversi Paesi membri – ma anche fra le autorità giurisdizionali, come descritto *supra* al par. 7 – si sono rafforzate sia dal punto di vista normativo, sia da quello pratico-applicativo, contribuendo così all'implementazione della c.d. «*dimensione orizzontale*»[291] del costituzionalismo multilivello.

Resta da scoprire, tuttavia, se l'Unione sarà all'altezza di competere con i modelli alternativi di salvaguardia accolti dalle altre super-potenze pubbliche[292], nonché come si rapporterà con i forti interessi privati perorati dalle grandi multi-nazionali dell'informatica[293]. In altre parole, riuscirà l'UE a difendere il suo modello di tutela nello scacchiere globale? L'elevato *standard* di garanzia predisposto dalla normativa

[287] Giova ricordare anche qui che una eccezione a questa regola è costituita dalle operazioni di trattamento poste in essere dalle istituzioni e dagli organi dell'Unione: per la tutela del diritto, in queste ipotesi, è infatti competente il Garante europeo della protezione dei dati.

[288] M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 519.

[289] Per il loro esame si rinvia *supra* al par. 6. Nella tabella n. 4 e nel grafico n. 3 si è messo a confronto il numero annuale degli incontri di lavoro dei Garanti nazionali nel corso del decennio 2010-2019. Le fonti dei dati ivi raccolti sono, anche in questo caso, le relazioni annuali del Garante per la protezione dei dati personali degli anni 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, reperibili al seguente *link* garanteprivacy.it.

[290] *Cfr.* M.S. ESPOSITO, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., p. 519.

[291] I. PERNICE, *The Treaty of Lisbon: Multilevel Constitutionalism in Action*, cit., pp. 379-383.

[292] I due sistemi di protezione dei dati fino a oggi concorrenti sono stati quelli statunitense ed europeo – il confronto fra essi è emerso icasticamente, sul piano giurisprudenziale, nelle sentenze della Corte di Giustizia del 6 ottobre 2015, causa C-362/14, e del 16 luglio 2020, causa C-311/18 (cc.dd. sentenze Schrems I e II) – ma il confronto sembra essersi ormai allargato anche all'impostazione adottata dalla Repubblica Popolare Cinese. V. in proposito M. ROTENBERG, *Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection*, cit., p. 10 e ss.

[293] In proposito v.: S. ZUBOFF, *Molte sfaccettature di un solo diamante*, cit., p. 48; IID., *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, cit., *passim*.

europea[294] si affermerà come paradigma di riferimento mondiale o, invece, resterà isolato nel panorama internazionale[295]?

L'Unione, a ben vedere, sembra avere le potenzialità per assurgere a protagonista nella competizione fra modelli di protezione dei dati personali[296], come peraltro traspare dall'influenza già esercitata oltre i confini europei, in forza del «*Brussels effect*»[297], dal regolamento (UE) 2016/679. Perché divenga realmente un baluardo internazionale nella difesa del diritto[298], tuttavia, è indispensabile che l'UE garantisca concretamente in tutti i Paesi membri l'uniformità applicativa della disciplina comune.

A tal fine, è necessario che il percorso di integrazione prosegua ulteriormente nella direzione intrapresa, mediante l'implementazione degli strumenti di coordinamento della tutela giurisdizionale[299] e, in special modo, dei meccanismi amministrativi di cooperazione e coerenza[300]. In questo quadro, è probabile che il Comitato europeo divenga sempre più il centro unificatore dell'interpretazione della *Data protection*, in quanto «*decisore ultimo*»[301] delle questioni controverse fra i Garanti nazionali. Anche nel prossimo futuro, in definitiva, quella del diritto alla protezione dei dati personali dovrà essere una storia di integrazione europea.

---

294 Sul punto, fra i tanti, v.: G. BUTTARELLI, *The EU GDPR as a clarion call for a new global digital gold standard*, in *International Data Privacy Law*, vol. 6, n. 2/2016, p. 77; A. PISAPIA, *La tutela multilivello garantita ai dati personali nell'ordinamento europeo*, in *Federalismi.it*, 31 gennaio 2018, p. 2; L. VALLE, L. GRECO, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale*, cit., p. 168 e ss.

295 *Conf.* G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, cit., pp. 2 e 3.

296 Di questo stesso avviso è R. PANETTA, *Privacy 2030: diamo una chance al genere umano*, in *Privacy 2030. Una nuova visione per l'Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, novembre 2019, reperibile al *link* garanteprivacy.it, p. 46, secondo il quale: «*L'Unione Europea ha senza dubbio la potenza di fuoco politica, legislativa e decisionale per affrontare il problema (o i problemi), ma dovrebbe crescere e assumere il ruolo di terzo attore tra i diversi blocchi economici e politici, un attore autorevole, forte e autonomo nella partita a scacchi internazionale*». In tal senso appare orientata, peraltro, la recente proposta del c.d. *Data Governance Act* da parte della Commissione europea: v., in proposito, il *link* ec.europa.eu.

297 Secondo la tesi del «*Brussels effect*», l'Unione europea vanterebbe la capacità di influenzare unilateralmente non solo le normative di Stati terzi, ma anche il commercio globale e le istituzioni internazionali. Tale (sottostimata) attitudine dell'Unione sarebbe dovuta al suo estesissimo mercato interno e al forte potere regolatorio dei suoi organi. In proposito v. *amplius*: A. BRADFORD, *The Brussels effect*, in *Northwestern University Law Review*, vol. 107, n. 1/2012; U. PAGALLO, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Torino, Giappichelli, 2014, p. 270.

G. BUTTARELLI, *The EU GDPR as a clarion call for a new global digital gold standard*, cit., p. 77, ha osservato che, in conseguenza del *Brussels effect*, «*Over half the countries in the world now have a data protection and/or privacy law, and most are strongly influenced by the European approach*».

298 H. HIJMANS, *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Springer, 2016, *passim*.

299 V. *amplius supra* par. 7.

300 In proposito si rinvia *supra* i parr. 5, 6 e 8. In questo quadro, è probabile che il Comitato europeo divenga sempre più il centro unificatore dell'interpretazione della *Data protection*, in quanto «*decisore ultimo*» – l'espressione è utilizzata da A. CASELLI, *Artt. 58-67*, cit., p. 538, e da V. ZAMBRANO, *Il Comitato europeo per la protezione dei dati*, cit., p. 999 – delle questioni controverse fra i Garanti nazionali, oltre che in ragione della sua autorevole composizione.

301 L'espressione è utilizzata da A. CASELLI, *Artt. 58-67*, cit., p. 538, e da V. ZAMBRANO, *Il Comitato europeo per la protezione dei dati*, cit., p. 999.