

Cittadinanza digitale

Sicurezza Informatica

Sanità digitale

Industry 4.0/Innovazione in azienda

Infra

PRIVACY

Autorità nazionali, EDPB e GEPD: dentro la rete europea dei Garanti

[Home](#) > [Sicurezza Digitale](#) > [Privacy](#)Partecipa al dibattito 

La rete europea dei Garanti, creata per superare frammentazione normativa e assenza di una visione unitaria della privacy, costituisce il fulcro della governance del GDPR, assicurando uno spazio giuridico comune con regole uniformi e un controllo coordinato e multilivello

Pubblicato il 19 feb 2026

Veronica Montozzi

dottoranda di Ricerca in Discipline Giuridiche Pubblicistiche, curriculum Discipline Pubblicistiche, Internazionalistiche ed Europee presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tre



Dinanzi alla «**assenza di una visione globale di privacy e della sua tutela universalmente condivisa**»[1], l'Unione europea si è posta l'obiettivo di creare uno spazio dove garantire a pieno i diritti della persona rispetto a chiunque ne gestisca, tramite i dati, l'identità[2].

A tal fine, recependo e razionalizzando l'esperienza maturata in Europa negli ultimi vent'anni[3], il **Regolamento europeo n. 2016/679 sulla protezione dei dati (d'ora in poi GDPR)** si caratterizza per l'intento di perfezionare l'assetto amministrativo che assicuri livelli uniformi di tutela del diritto alla protezione dei dati nello spazio giuridico europeo[4], istituendo una serie di organismi, che nel loro insieme formano una rete, la **rete europea dei Garanti dei dati personali**, denominazione con la quale si fa riferimento all'insieme di varie istituzioni che cooperano tra loro al fine di assicurare un'effettiva e coerente applicazione della disciplina contenuta nel **GDPR**.

Indice degli argomenti ▾

Dalla direttiva 95/46 al GDPR: omogeneità e certezza del

I motivi che hanno guidato il legislatore europeo nel delineare il nuovo sistema di governance, basato sul collegamento tra diversi organismi, sono essenzialmente due.

★ WHITE PAPER

Scopri le modalità di Backup più adatte per la continuità operativa della tua azienda

- # Gestione Dati
- # Sicurezza informatica

NETWORK₃₆₀

ZeroUno

BACKUP: cos'è, a cosa serve, come e quando farlo



[Leggi l'informativa sulla privacy](#)

E-mail aziendale*

Acconsento alla comunicazione dei miei dati a terzi affinché li trattino per proprie finalità di marketing tramite modalità automatizzate e tradizionali di contatto.

SCARICA ORA

Il primo motivo, di carattere formale, concerne la tipologia dello **strumento normativo scelto** per regolare la materia della privacy: in luogo di una direttiva (la c.d. **Direttiva "madre" 95/46/CE**), infatti, viene adottato un **Regolamento**, ossia un atto di portata generale, direttamente applicabile in tutti gli Stati membri dell'Unione europea, il quale, pur prevedendo diverse clausole di flessibilità[5], impone a tutti gli Stati membri l'applicazione omogenea di una medesima disciplina.

Il GDPR, infatti, fermo restando la validità degli obiettivi e dei principi stabiliti dalla precedente direttiva 95/46, nasce dalla necessità di porre rimedio alla **frammentazione della disciplina sulla protezione dei dati personali** nell'Unione europea e dalla rilevazione della **diffusa incertezza giuridica** concernente l'applicazione della normativa[6].

L'adozione di una **disciplina omogenea** come quella offerta dal Regolamento della privacy è apparsa, quindi, funzionale a garantire in tutta l'Unione un **elevato livello di tutela dei diritti e delle libertà fondamentali** della persona fisica, con riguardo al trattamento dei dati personali.

Il GDPR infatti comporta in primo luogo una medesima regolazione in tutto il territorio dell'Unione europea al fine di tutelare un diritto che, assumendo la veste di **diritto fondamentale**, sancito dall'**art. 8 della Carta dei diritti fondamentali dell'Unione europea** e dall'**art. 16 TFUE**, richiede omogeneità di regolazione nei confronti di tutti coloro che risiedono nel suo territorio[7]; in secondo luogo, persegue l'obiettivo di **incentivare la libera circolazione dei dati** per il tramite di una ragionevole certezza delle modalità con le quali tale regolazione è in concreto applicata, creando uno «**spazio fisico comune**» entro cui sono dettate le medesime regole[8].

Tecnologie digitali e bisogno di una rete europea dei Garanti

Il secondo motivo, di carattere sostanziale, attiene invece al **contesto** nel quale si sono inserite le diverse fonti[9].

Rispetto dunque all'assetto antecedente la riforma del 2016[10], caratterizzato dall'assenza di **social network** e **motori di ricerca**, aventi quale principale caratteristica quella di rendere il mondo interconnesso, nell'odierno mondo digitale si rende evidente la necessità di assicurare un'**omogenea applicazione della disciplina sulla privacy** su tutto il territorio dell'Unione europea e di creare un **network di sorveglianza** a presidio del diritto alla protezione dei dati e dell'omogeneità della sua tutela, essendo chiaro che l'esigenza di uniformità

della normativa non possa prescindere da un **enforcement** in grado di assicurare l'effettiva coerenza da parte delle singole legislazioni nazionali[11].

La **dematerializzazione degli strumenti di circolazione delle informazioni** e l'assenza di confini geografici del web impongono, infatti, la concertazione di decisioni delle autorità per assicurare un'efficace attuazione del GDPR e «realizzare un **clima di fiducia del pubblico** che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno»[12].

I soggetti della rete europea dei Garanti e le autorità nazionali

La rete europea è stata quindi elaborata dal legislatore europeo al quale è apparsa evidente, fin da subito, l'esigenza di un **meccanismo di armonizzazione** che, da un lato, cogliesse le diversità inevitabili tra le posizioni delle Autorità dei paesi firmatari, le quali risultavano assai differenti tra di loro a causa delle normative a loro volta differenti le une dalle altre, e dall'altro, soddisfacesse l'esigenza di una **necessaria applicazione coerente** della disciplina.

Sebbene l'applicazione del GDPR abbia rappresentato un **successo** sin dai primi anni della sua entrata in vigore, avendo rafforzato la protezione dei dati come diritto fondamentale e armonizzato l'interpretazione dei principi in materia[13], grazie anche – e soprattutto – al nuovo **sistema di governance** istituito, di recente è stato rilevato l'insufficiente livello di **cooperazione tra le Autorità** dovuto alla frammentazione delle procedure e delle prassi nazionali, che determina «incertezza del diritto e aumenta i costi per le imprese (ad esempio a causa della necessità di produrre documenti differenti nei vari Stati membri), perturbando la libera circolazione dei dati personali nell'UE, pregiudicando le attività commerciali transfrontaliere e ostacolando la ricerca e l'innovazione in relazione a sfide sociali urgenti»[14].

Nei paragrafi che seguono, dunque, si cercherà di illustrare il complesso funzionamento della **rete europea dei Garanti**, partendo da un inquadramento dei

soggetti che ne fanno parte e dei diversi strumenti che ne assicurano la cooperazione e il dialogo, analizzando, infine, quali sono le criticità che attualmente impediscono l'efficace funzionamento del sistema predisposto dal legislatore europeo nel GDPR e le **prospettive di riforma**.

Le autorità di controllo indipendenti: compiti e poteri nel GDPR

Nella realizzazione di un sistema europeo prodromico ad un'omogenea tutela dei dati personali, un ruolo fondamentale è coperto dalle **autorità indipendenti nazionali**, in quanto, da una parte, sorvegliano l'attuazione e la corretta implementazione delle regole sovranazionali nei rispettivi territori, dall'altra, garantiscono, attraverso **meccanismi di coerenza** e di stretta cooperazione, **standard uniformi di tutela** in tutto il territorio europeo[15].

L'art. 51 del Regolamento dispone l'istituzione di una o più **autorità pubbliche di controllo indipendenti** in ciascun Stato membro, aventi il compito di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento, e di **agevolare la libera circolazione dei dati personali** all'interno dell'Unione.

Occorre osservare che le **Autorità di controllo in tema di privacy** avevano già fatto il loro ingresso nella normativa europea con la Direttiva 95/46/CE, la quale, all'art. 28, disponeva che ciascuno Stato membro dovesse dotarsi di un soggetto pubblico, incaricato di sorvegliare, nel proprio territorio, l'applicazione delle disposizioni di attuazione della Direttiva.

Nella Direttiva in esame, le Autorità erano investite soprattutto di **poteri consultivi**, svolgendo però, fin dalla loro comparsa, anche il compito di sviluppare, all'interno degli Stati membri, una «costante attività di implementazione della cultura della protezione dei dati personali»[16].

Il ruolo delle **Autorità indipendenti** è stato implicitamente modificato nella transizione dalla direttiva 95/46/CE al regolamento (UE) 2016/679, poiché il

paradigma introdotto da quest'ultimo statuisce un **rapporto diretto tra Autorità indipendenti di controllo e Regolamento**, esigendo che siano immediatamente applicabili le funzioni di sorveglianza e controllo sulle disposizioni ivi contenute.

Ciò ha determinato la **centralità del ruolo dei Garanti nazionali**, nel dare piena e coerente attuazione alle previsioni del regolamento e delle conseguenti norme interne di adeguamento, avendo peraltro assunto la capacità di adottare **decisioni vincolanti anche al di fuori del territorio statale** in cui operano.

In questa pianificazione, il legislatore europeo lascia agli Stati membri **margini di manovra** per disciplinare l'adozione delle previsioni di adeguamento al Regolamento in modo da renderle compatibili con l'ordinamento interno. Conseguentemente, dunque, ogni Autorità è competente anche per l'applicazione della **legislazione nazionale** nelle materie in cui il GDPR consente al legislatore dello Stato membro di legiferare.

Al fine di eseguire il compito fondamentale di «sorvegliare» la corretta applicazione del Regolamento, l'art. 58 investe le Autorità di controllo di una serie di **poteri** che possono distinguersi in tre categorie: **poteri di indagine** (art. 58, par. 1), **poteri correttivi** (art. 58, par. 2) e **poteri consultivi** (art. 58, par. 3).

A tali poteri si affianca la facoltà, statuita con l'art. 83 del Regolamento, di infliggere **sanzioni amministrative pecuniarie**, individuate sulla base di criteri di effettività, proporzionalità e dissuasività[17].

In riferimento all'**ambito territoriale di competenza** di ciascuna Autorità di controllo[18], l'art. 55 del Regolamento stabilisce che esse esercitano i propri poteri ed eseguono i propri compiti nel territorio dello Stato cui appartengono, mentre il Considerando n. 122 precisa i confini della giurisdizione avendo riguardo al trattamento esaminato.

La lead authority nei trattamenti transfrontalieri di dati personali

La presenza sul territorio dell'Unione di una o più Autorità di controllo per ciascun Stato membro, nonché la possibilità per le singole autorità di essere investite di poteri ulteriori, determinano tuttavia il rischio di **applicazioni difformi della normativa** nei diversi Stati, soprattutto nelle fattispecie in cui le operazioni di trattamento coinvolgono una **pluralità di Paesi membri**, ossia in caso di trattamento **transfrontaliero** dei dati personali[19].

In queste due diverse tipologie di casi, si rende evidente il rischio che una pluralità di Autorità nazionali diverse si pronunci, in modo anche comprensibilmente difforme, sulla conformità al GDPR di trattamenti di dati operati in più stabilimenti in diversi Paesi o che, pur effettuati da un unico stabilimento situato in un solo Paese, riguardino dati di interessati appartenenti ad altri Stati.

In considerazione quindi dell'esigenza di **uniformità dell'applicazione della disciplina**, è apparso ragionevole cercare di evitare che trattamenti di dati svoltisi sul territorio di uno Stato, ma aventi effetti anche in altri, possano essere sottoposti al sindacato di diverse Autorità di controllo – ciascuna competente per gli effetti provocati sul proprio territorio – prevedendo invece che, in caso di trattamenti che comportino la **circolazione transfrontaliera di dati**, la competenza a controllare i trattamenti stessi sia affidata a un'**unica Autorità competente**.

A tal riguardo, il Regolamento istituisce all'art. 56 un altro componente della rete europea, la c.d. **Autorità di controllo "capofila" (Lead Supervisory Authority)**, ossia l'autorità competente nel caso di trattamento di dati personali a carattere transfrontaliero, in deroga al criterio di imputazione territoriale della competenza di cui al par. 1 dell'art. 55, la quale assume in tali ipotesi un **ruolo chiave** essendo chiamata a coordinare la cooperazione con le altre Autorità appartenenti agli Stati membri interessati in modo da assicurare **coerenza nell'applicazione del Regolamento, certezza del diritto e omogeneità nella sua attuazione** anche laddove siano coinvolti più Stati[20].

Individuazione dello stabilimento principale e casi borderline

Nell'individuazione dell'Autorità capofila fra i diversi Garanti nazionali interessati, a ben vedere, occorre tenere distinte le due fattispecie di trattamento transfrontaliero.

Allorché infatti la qualificazione del trattamento come transfrontaliero discenda dalla circostanza che esso produca 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**.

Qualora, invece, il trattamento dei dati assuma la qualifica di transfrontaliero in quanto vi sia una **molteplicità di stabilimenti** collocati in più Stati dell'Unione, l'Autorità capofila è identificata in quella competente in relazione al luogo in cui è situato lo **stabilimento principale del soggetto attivo del trattamento**, inteso come lo stabilimento che effettivamente prende le **decisioni in ordine a finalità e mezzi del medesimo**, avendone per statuto il potere[21].

Spetta, poi, al **titolare/responsabile** l'onere di provare che lo stabilimento, individuato come "principale", svolga un «esercizio reale ed effettivo di attività gestionali o decisionali rispetto al trattamento di dati personali», ancorando la prova a criteri oggettivi e a **elementi probatori dimostrabili**, non potendosi invece fondare esclusivamente su dichiarazioni rese dalla società[22].

In caso di opposizione di un Garante che reclami tale ruolo, l'individuazione della capofila spetta in ultima istanza al **Comitato europeo**.

Possono esserci casi "borderline" in cui è difficile stabilire quale sia lo stabilimento principale o determinare dove siano assunte realmente le decisioni inerenti al trattamento dei dati, come ad esempio l'ipotesi in cui un'impresa abbia più stabilimenti in Europa, nessuno dei quali sia la sede dell'amministrazione centrale e in nessuno di essi si prendano decisioni sul trattamento.

In tali ipotesi, il GDPR non fornisce soluzioni chiare, prevedendo che spetti alla società indicare lo stabilimento che funge da **stabilimento principale** e, nel caso in cui non fosse possibile, sarà compito dell'Autorità di controllo del territorio interessato procedere all'individuazione dello stesso[23].

A fronte di difficoltà interpretative già nell'individuazione dell'Autorità Capofila, il testo del Regolamento adottato circonda questo istituto di molte **garanzie e limitazioni**, come dimostrano i complessi passaggi che compongono i **meccanismi di cooperazione** descritti negli artt. 56 e 60, nonché quelli relativi ai **meccanismi di coerenza**.

Comitato europeo e Garante europeo nella governance della privacy

Accanto alle autorità nazionali, le esigenze di **armonizzazione delle regole** che governano la protezione dei dati personali hanno assunto una rilevanza tale da suggerire al legislatore l'opportunità di istituire un organismo dotato di compiti più ampi e pregnanti, quale il **Comitato europeo per la protezione dei dati** (di seguito, Comitato), o **European Data Protection Board (EDPB)**.

Composizione e funzioni del Comitato europeo per la protezione dei dati

Esso è un organismo dell'Unione, dotato di **personalità giuridica** (art. 68, par. 1 GDPR), avente dunque la titolarità di tutte le situazioni giuridiche attive e passive e una responsabilità diretta per gli atti compiuti nell'esercizio delle sue funzioni, e si configura come un ente di diritto pubblico europeo, **indipendente**.

Il Comitato sostituisce, senza soluzione di continuità, il precedente **Gruppo di lavoro ex art. 29** (Working Party on Article 29), ossia l'organismo istituito dalla Direttiva che annoverava e coordinava la cooperazione tra le diverse Autorità indipendenti. Tuttavia, lungi dall'essere un mero successore, esso si differenzia in quanto dispone di **maggiori poteri** e della personalità giuridica, non prevista per il precedente organo[24], che gli consentono di ricoprire meglio il ruolo di

«organo di chiusura del sistema»[25], il cui principale compito consiste nel **vigilare sulla coerente applicazione delle norme del Regolamento**, coordinando le diverse Autorità di controllo[26].

Come previsto ai sensi dell'art. 68, par. 3 – e specificato dal Considerando n. 139 – il Comitato è composto dalle figure **apicali delle Autorità di controllo** di ciascuno Stato membro (ad oggi 27), le quali partecipano con diritto di voto, nonché dal **Garante europeo della protezione dei dati** o dai relativi rappresentanti, aventi diritti di voto specifici e limitati.

Inoltre, partecipano alle attività del Comitato anche la **Commissione europea** e i rappresentanti delle autorità dell'**Area Economica Europea** (Islanda, Liechtenstein e Norvegia), avendo il diritto di esprimere le proprie posizioni su tutte le questioni discusse, ma restando privi del diritto di voto.

Il Comitato adotta i propri atti a **maggioranza, qualificata o semplice**, rendendoli così reale espressione della volontà dell'istituzione e non dei singoli componenti, in modo tale che essi siano fortemente incentivati a rispettare l'indirizzo concordato.

In ragione di tale autorevole composizione, al Comitato viene riconosciuta, dunque, una funzione di **nomofilachia**, essendo stato istituito con la principale finalità di **monitorare e assicurare la coerente applicazione del Regolamento** (art. 70, par. 1).

In questa prospettiva il GDPR gli assegna una serie di **poteri e compiti**, assolti dall'organo in piena indipendenza (art. 69), e tutti convergenti nell'indirizzare le pratiche delle singole Autorità di controllo di tutti gli Stati membri verso un'**applicazione coerente** delle norme sulla protezione dei dati, promuovendone al contempo la **cooperazione**[27].

Il Comitato dunque esercita una costante attività di **sorveglianza** relativa all'applicazione corretta del Regolamento, non limitandosi all'esercizio di semplici funzioni consultive, come nel caso dei **pareri** emessi ai sensi dell'art.

64, ma espletando anche un **potere decisionale**, previsto dall'art. 65, in relazione alle controversie che possono sorgere tra le diverse Autorità di controllo.

In quest'ottica, il Comitato detiene anche il potere di **orientare le attività della Commissione**, organo esecutivo e promotore del processo legislativo nell'Unione, nella direzione di un'omogenea applicazione del regolamento, svolgendo un'attività consultiva nell'ambito della quale fornisce ad essa indicazioni in merito a qualsiasi questione inerente alla protezione dei dati personali.

Sempre con riguardo allo scopo di assicurare l'applicazione coerente del Regolamento, ai sensi dell'art. 70, par. 1, lett. e, il Comitato svolge l'ulteriore e fondamentale compito di **elaborare orientamenti generali**, esaminando, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, questioni relative all'applicazione del Regolamento stesso, pubblicando, di conseguenza, **linee guida, raccomandazioni e migliori pratiche** per chiarire e promuovere una **comprensione comune** delle leggi sulla protezione dei dati dell'UE.

Il Garante europeo della protezione dei dati tra controllo e consulenza

Tra i soggetti che compongono la rete europea dei Garanti, deve infine annoverarsi anche il **Garante europeo della protezione dei dati** (di seguito, GEPD), o anche **European Data Protection Supervisor (EDPS)**, che opera quale **autorità di sorveglianza indipendente**, istituita con il Regolamento (CE) n. 45/2001, e nominato dal Parlamento e dal Consiglio dell'Unione europea per **mandati rinnovabili di cinque anni**.

Esso svolge il primario compito di garantire che le **istituzioni e gli organi dell'UE** rispettino il diritto dei cittadini alla **vita privata** e alla **protezione dei dati** in sede di trattamento dei dati personali e di elaborazione di nuove politiche.

Attualmente, i doveri e i poteri del Garante europeo della protezione dei dati, nonché la sua l'indipendenza istituzionale in qualità di autorità di controllo, sono definiti nel **regolamento (UE) 2018/1725**, che ha abrogato il precedente regolamento e che stabilisce altresì le norme relative alla protezione dei dati nelle istituzioni dell'UE.

Il GEPD assolve diversi compiti, tra cui in primis, quello di **sorvegliare il trattamento dei dati personali** da parte dell'amministrazione dell'UE allo scopo di assicurare il rispetto delle norme sulla privacy, in cooperazione con i **responsabili della protezione dei dati** presenti in ogni istituzione o organismo comunitario.

Il Garante europeo collabora, inoltre, con le **amministrazioni nazionali dei paesi dell'UE** per assicurare la **coerenza** nell'ambito della protezione dei dati, ricoprendo il ruolo di **membro del Comitato europeo** con diritti di voto specifici e limitati all'adozione di decisioni che riguardano **principi e norme applicabili** ad istituzioni, organi, uffici e agenzie dell'Unione[28].

Meccanismi di cooperazione nella rete europea dei Garanti

Come anticipato, per far fronte all'inevitabile rischio di **applicazioni difformi della normativa** nei diversi Stati pericolo e assicurare l'**uniforme applicazione** della disciplina in materia di protezione dei dati personali, l'art. 51, par. 2, specificando quanto previsto nel Considerando n. 123, richiede che le autorità di controllo si impegnino a contribuire alla **coerente applicazione** del presente regolamento in tutta l'Unione, cooperando tra loro e con la Commissione, «così da tutelare le persone fisiche in relazione al trattamento dei loro dati personali e facilitare la **libera circolazione** di tali dati nel mercato interno».

In vista di tale scopo nel Capo VII, rubricato, «Cooperazione e Coerenza», il legislatore europeo disciplina i rapporti tra le Autorità per il tramite di due meccanismi: il **meccanismo di cooperazione** – finalizzato a garantire un necessario e continuo dialogo tra le Autorità di controllo interessate, al fine di

individuare una soluzione congiunta che assicuri l'uniforme applicazione della disciplina – e il **meccanismo di coerenza** che, ponendosi al di sopra del primo[29], interviene in tutti i casi in cui, nonostante il dialogo instauratosi tra le Autorità di controllo capofila e le singole Autorità interessate, ovvero, tra le singole Autorità interessate, non si riesca a pervenire ad una decisione condivisa, coinvolgendo anche la **Commissione europea** e il **Comitato**.

Il meccanismo one stop shop e il procedimento ex articolo 60 GDPR

A differenza della direttiva 95/46/CE, che in un'unica disposizione (art. 28 direttiva 95/46/CE), imponeva alle autorità unicamente di scambiarsi «ogni informazione utile», il Regolamento (UE) 2016/679 dedica numerose disposizioni alla **cooperazione** al punto che non appare improprio sussumere l'esistenza di un **principio generale di leale collaborazione** fra autorità di controllo[30].

Quali nuove estrinsecazioni di tale principio, il Regolamento prevede precisi strumenti volti a garantire un concreto e costante dialogo tra le singole autorità di controllo. Essi sono il procedimento **“one stop shop”**, l'**assistenza reciproca** e le **operazioni congiunte**, che costituiscono un significativo passo in avanti nel processo di integrazione europea della **data protection**.

Il meccanismo **one stop shop**, detto anche «meccanismo dello sportello unico», è un meccanismo di cooperazione, stabilito dall'art. 60 GDPR, che disciplina i rapporti tra l'**Autorità Capofila** e le altre autorità di controllo.

Esso si sostanzia in un meccanismo di **co-decisione**, dove vi è un'unica autorità con cui l'impresa si interfaccia, la c.d. Autorità capofila, la quale è competente a emanare nei suoi confronti la (unica) **decisione finale**, essendo però obbligata a interpellare tutte le **Autorità interessate** prima di assumere qualsiasi provvedimento che riguardi un titolare o responsabile, al fine di raggiungere un **consenso condiviso** in merito alla misura da adottare e garantire così la **coerenza**.

L'iter procedurale prende avvio su iniziativa di un **interessato**, il quale può proporre **reclamo** nello Stato dove risiede o dove lavora, denunciando la violazione di norme in materia di protezione dei dati personali da parte di un titolare del trattamento.

Ricevuto il reclamo e riscontrato il carattere **transfrontaliero del trattamento**, l'Autorità nazionale si rivolge all'Autorità capofila competente che, nel termine di tre settimane, deve decidere se **trattare il caso** (art. 56.4) secondo la procedura di cooperazione, oppure **non trattare il caso** (art. 56.5) rimettendolo alla competenza dell'Autorità di controllo nazionale (che ha ricevuto il reclamo).

Nel caso in cui la Capofila decida di attivare la procedura di cooperazione, è tenuta a **condividere** con le altre autorità interessate tutte le **informazioni utili** sulla questione e a trasmettergli un proprio **progetto di decisione**, valutando adeguatamente il parere da loro espresso su di esso.

Entro il termine di quattro settimane, ciascuna autorità di controllo può, infatti, sollevare una **obiezione «pertinente e motivata»**[31] al progetto di decisione (art. 60, par. 4), ponendo l'autorità capofila innanzi alla seguente alternativa: se non reputa di dare seguito all'obiezione pertinente e motivata – oppure se ritiene che difettino questi due requisiti – essa deve sottoporre la questione al **meccanismo di coerenza**, di cui all'art. 63; qualora, invece, l'autorità capofila intenda dare seguito all'obiezione, è tenuta a **modificare il progetto di decisione** e a trasmetterlo nuovamente alle altre autorità di controllo interessate, così da ottenere il loro parere anche sulla versione riveduta.

L'adeguata valutazione dell'opinione delle altre autorità di controllo da parte dell'autorità capofila costituisce, infatti, un passaggio fondamentale del procedimento che conduce all'adozione di un **provvedimento finale condiviso** da tutte le Autorità[32].

Tale valutazione non viene meno neanche nell'ipotesi in cui nessun Garante sollevi obiezioni al progetto di decisione trasmesso dall'Autorità capofila, in

quanto, in tal caso, si presume che tutte le autorità coinvolte siano d'accordo sul progetto, che diviene per loro **vincolante in forza di un consenso implicito**.

L'Autorità capofila adotta poi la **decisione finale** e la notifica allo stabilimento principale o allo stabilimento unico, informando le altre Autorità interessate, tra cui l'autorità nazionale che ha ricevuto il reclamo, che deve darne notizia al reclamante (art. 60.7).

La complessa articolazione del procedimento di cui all'art. 60 GDPR, è espressione della difficoltà di **bilanciare le prerogative delle autorità di controllo nazionali** con l'innovativo ruolo dell'Autorità capofila, in quanto la decisione di quest'ultima, di regola, si sostituisce a quelle che avrebbero potuto adottare – nell'ambito delle rispettive competenze territoriali – i diversi Garanti nazionali, venendo così assicurata l'**omogeneità applicativa** della disciplina della data protection e, quindi, la **certezza del diritto dell'Unione**[33].

A questi fini, è previsto a carico del titolare o del responsabile, destinatario della decisione dell'autorità capofila, l'obbligo di garantire la **conformità** a essa di ogni trattamento realizzato in tutti i propri stabilimenti all'interno dell'UE (art. 60, par. 10).

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[34].

Il meccanismo appena descritto non si applica, tuttavia, nel caso in cui 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, spettando così la competenza a decidere all'autorità garante dello Stato in cui si trovano lo stabilimento o gli interessati (art. 56, par. 2), fermo restando anche in tali fattispecie, l'**obbligo di cooperazione** fra autorità amministrative indipendenti, per il tramite di altri strumenti previsti dal Regolamento.

Il Considerando n. 128, inoltre, nega la competenza dell’Autorità Capofila, e dunque l’applicazione del meccanismo dello sportello unico, nei casi in cui il trattamento, oggetto del reclamo, sia effettuato da **autorità pubbliche** o da organismi privati nell’interesse pubblico, rimanendo quindi competente in queste ipotesi l’Autorità di controllo dello Stato in cui sono stabiliti l’autorità pubblica o l’organismo privato.

Assistenza reciproca e operazioni congiunte tra autorità di controllo

Occorre notare che, 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, in quanto, animato dall’intento di **garantire una omogenea applicazione della disciplina europea** in tutti i Paesi membri, il legislatore europeo ha tipizzato ulteriori strumenti di collaborazione tra Garanti della privacy nazionali, quali l’**assistenza reciproca** e le **operazioni congiunte**[35].

L’assistenza reciproca, disciplinata ai sensi dell’art. 61 GDPR, si concretizza, in particolare, nelle **richieste di informazioni** e misure di controllo (quali le richieste di autorizzazioni e consultazioni preventive) e le **richieste di effettuare ispezioni e indagini** in un diverso Stato membro, da parte di un’Autorità alle altre.

L’autorità destinataria delle richieste deve darvi seguito senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta (par. 2).

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.

È pertanto previsto un esplicito **divieto di rifiuto** per le autorità destinatarie delle richieste, salvo due casi tassativamente descritti dalla norma al par. 4[36].

Al di fuori di queste ipotesi, qualora l’A. richiesta non trasmetta alcun riscontro nei termini previsti, l’Autorità di controllo richiedente può adottare “**misure**

provvisorie”, analoghe a quelle di cui all’art. 66, par. 1 GDPR, destinate ad operare all’interno del proprio territorio.

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 appartenenti alle Autorità di controllo di altri Stati membri.

A queste attività, in caso di trattamenti transfrontalieri di dati personali, 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» ai sensi dell’art. 62 GDPR.

Entrambi questi strumenti possono essere utilizzati, tuttavia, anche al di fuori dei suddetti casi obbligatori, ogniqualvolta un’autorità di controllo ritenga **proficuo avvalersi del supporto** di un’altra per azioni da condurre sul proprio territorio.

Il meccanismo di coerenza e il ruolo decisorio dell’EDPB

A tutela dell’**uniformità di azione** da parte delle diverse Autorità di controllo, riprendendo quanto espresso dal Considerando n. 135[37], l’art. 63 sancisce che «al fine di contribuire all’applicazione coerente del presente regolamento in tutta l’Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il **meccanismo di coerenza** stabilito nella presente sezione».

Qualora, infatti, le forme di cooperazione amministrativa fra Garanti nazionali non conducessero a una soluzione condivisa in merito alla decisione da adottare, l’ordinamento europeo prevede l’instaurazione di un **dialogo** tra le Autorità nazionali e la Commissione, dialogo che si svolge nell’ambito del **Comitato europeo per la protezione dei dati personali** che assume un **ruolo centrale**[38].

Il legislatore europeo ha dedicato un'apposita sezione del Regolamento al meccanismo di coerenza (Sezione II del Capitolo VII, rubricata «Coerenza»), intendendo, con il termine «coerenza», tanto il meccanismo quanto l'obiettivo da raggiungere tramite esso, che si ricerca in fase di applicazione delle misure da parte dell'Autorità di controllo per la protezione dei dati.

Tale meccanismo è infatti composto da diversi **strumenti**, posti nelle mani del Comitato europeo, tramite i quali svolge la funzione di **coordinare le attività** delle autorità di controllo dei diversi Stati membri e della Commissione[39].

Pareri del Comitato europeo ex articolo 64: quando sono obbligatori

Il primo strumento, previsto dall'art. 64, si estrinseca nel potere del Comitato di adottare **pareri** che consentono di individuare una soluzione unitaria in merito a determinate questioni che possono presentarsi nel caso concreto.

L'articolo si compone di due paragrafi: nel paragrafo n. 1 vengono contemplate le **ipotesi tassative** in cui il parere da parte del Comitato deve essere obbligatoriamente richiesto.

In particolare, esse concernono tutte le decisioni delle autorità di controllo rese nell'ambito di fattispecie in cui è consentito ai singoli Stati membri mantenere un **ampio margine di manovra** rispetto all'applicazione del Regolamento (elenco di trattamenti soggetti al requisito di una valutazione di impatto, conformità al Regolamento di codici di condotta, requisiti per accreditamento di organismi, clausole contrattuali, ecc.), rendendo evidente dunque che in questo caso l'intervento del Comitato sia diretto ad assicurare la **coerenza delle decisioni** assunte dalle diverse autorità nazionali.

Nel paragrafo n. 2, invece, si attribuisce al Comitato un generico potere di **adozione di pareri** che possono essere discrezionalmente richiesti da parte di qualsiasi autorità di controllo, dalla Commissione europea o dal Presidente del Comitato, in merito a **questioni di applicazione generale** della normativa, ovvero

questioni destinate a produrre effetti in più di uno Stato membro, come ad esempio nell'ipotesi in cui un'autorità di controllo competente non si conformi agli obblighi relativi all'**assistenza reciproca** di cui all'art. 61, o allo svolgimento di **operazioni congiunte** ai sensi dell'art. 62.

In entrambe le ipotesi previste dall'articolo, il Comitato può **rifiutarsi di emettere il parere** qualora rilevi di essersi già pronunciato in passato su una questione analoga (art. 64, par. 3).

Decisioni vincolanti e procedure d'urgenza ex articoli 65 e 66

Sempre alla luce del più generale obiettivo di garantire la **coerente applicazione del Regolamento**, l'art. 65 GDPR prevede un altro strumento, ossia il potere del Comitato di **dirimere le controversie** che possono sorgere tra le diverse Autorità, adottando una **decisione giuridicamente vincolante** nelle ipotesi espressamente previste al par. 1, e nello specifico:

lett. a) qualora, nell'ambito dell'attuazione del principio dell'one stop shop, vi sia un **contenzioso** sul progetto delineato dalla Lead Authority, in quanto l'obiezione «pertinente e motivata» sollevata da un'autorità di controllo interessata avverso il progetto di decisione dell'autorità capofila (così come descritto all'art. 60) sia da questa ritenuta non pertinente o non motivata, oppure ove l'autorità capofila non dia seguito all'obiezione;

lett. b) vi sia un **contrasto di opinioni** tra le Autorità di controllo interessato per l'individuazione dello «stabilimento principale», specie nell'art. 56, relativo al meccanismo dell'Autorità di controllo capofila;

lett. c) un'autorità di controllo competente non abbia richiesto il **parere del Comitato** nei casi di cui all'articolo 64, paragrafo 1, o non si conformi (in tutto o in parte) ad esso.

L'art. 65, par. 2 delinea altresì il **procedimento** cui il Comitato deve conformarsi nell'adozione della «decisione vincolante».

Nello specifico si prevede che, entro un mese^[40] dal deferimento della questione da parte dell'autorità interessata (o capofila, nell'ipotesi di cui alla lett. a), il Comitato dovrà adottare una decisione vincolante, approvata dalla **maggioranza qualificata di due terzi** dei membri del Comitato.

Il provvedimento finale del Comitato adottato deve essere **motivato** e trasmesso sia all'autorità che ha sollevato la questione, sia a tutte le altre autorità di controllo interessate.

A seguito della notifica della decisione vincolante da parte del Comitato, l'Autorità controllo – o, se del caso, l'autorità capofila – è tenuta ad adottare, senza ingiustificato ritardo e al più tardi entro un mese dalla ricezione della notifica, la sua **decisione definitiva**, la quale deve basarsi sulla decisione vincolante del Comitato, **conformandosi** ad essa e facendone espresso riferimento.

Dall'analisi di queste ipotesi si comprende come la risoluzione delle controversie da parte del Comitato, configuri uno **strumento di ultima istanza** che interviene dopo una serie di fisiologiche fasi progressive (l'applicazione dei meccanismi di cooperazione ai sensi degli artt. 60-62, e l'emissione di un parere ai sensi dell'art. 64), delineate dal Regolamento, che avrebbero già dovuto condurre al raggiungimento del consenso tra i soggetti coinvolti^[41].

Il par. 4, art. 65 specifica poi che, nelle more dell'adozione della decisione da parte del Comitato, le Autorità devono **astenersi dall'adottare misure** sulla questione sottoposta al meccanismo di coerenza, per evitare di vanificare lo sforzo del Comitato con misure potenzialmente problematiche.

Ai sensi dell'art. 66 GDPR, è tuttavia possibile **sopperire** ai meccanismi sinora descritti (di cooperazione e di coerenza) a causa del sopravvenire di un'**urgenza**.

In circostanze eccezionali, infatti, ove sussista un **rischio grave e immediato** per i diritti e le libertà degli interessati, le Autorità che ritengano urgente provvedere, possono:

a) derogare al **meccanismo di cooperazione**, adottando immediatamente **misure provvisorie**, le quali produrranno effetti giuridici unicamente nel proprio territorio per un periodo non superiore ai 3 mesi, di cui ne danno comunicazione alle altre Autorità interessate, all'EDPB e alla Commissione;

b) richiedere al Comitato **pareri e decisioni vincolanti d'urgenza**, ossia i medesimi atti disciplinati rispettivamente dagli artt. 64 e 65, che tuttavia fruiscono di una particolare **procedura accelerata**, in quanto richiedono l'approvazione a maggioranza semplice (degli aventi diritto al voto all'interno del Comitato) e nel più breve termine di due settimane.

Criticità della rete europea dei Garanti e proposta di riforma

Federalismo esecutivo e limiti dell'attuale rete europea dei Garanti

Come visto sinora, la c.d. **rete europea dei Garanti** per la protezione dei dati è stata costruita dal legislatore europeo al fine di evitare l'instaurarsi delle **geometrie variabili** nei diversi Stati membri (ossia evitare che il Regolamento sia interpretato ed applicato diversamente negli Stati membri) e di assicurare l'**omogeneità dei trattamenti** in una prospettiva di armonizzazione del diritto alla protezione dei dati personali e di **funzionamento del mercato interno** su tutto il territorio dell'Unione.

Il modello del legislatore europeo, disegnato in considerazione del bene oggetto di tutela, non è esente da **criticità** in quanto all'istituzionalizzazione di forme di collaborazione tra le autorità di controllo, tramite i meccanismi di cooperazione e coerenza, non ha fatto seguito l'**armonizzazione di procedure amministrative e di interpretazioni dei concetti** nell'ambito di tali meccanismi[42] con la conseguenza che le singole autorità nazionali rappresentano ancora i **principali attori responsabili** dell'esecuzione della disciplina europea sulla tutela dei dati personali, dando luogo ad un **federalismo esecutivo**[43], da cui derivano effetti pregiudizievoli all'**efficace tutela del diritto**[44].

L'applicazione coerente del GDPR dipende infatti dall'**efficace funzionamento del sistema** preposto alla sua applicazione transfrontaliera[45].

Tuttavia, benché l'EDPB abbia adottato delle **Linee guida** sull'applicazione dell'articolo 60 al fine di «fornire orientamenti sull'applicazione concreta delle disposizioni»[46] relative alla procedura di cooperazione e sull'applicazione dell'art. 65, paragrafo 1, lettera a), volte a chiarire «il quadro giuridico applicabile e le fasi principali della procedura»[47], le **differenze procedurali**, che continuano a caratterizzare l'operato delle autorità di protezione dei dati, ostacolano il regolare ed effettivo funzionamento dei **meccanismi di cooperazione e di composizione delle controversie** del GDPR nei casi transfrontalieri, rimettendo il concreto utilizzo delle forme di coordinamento alla determinazione delle diverse autorità nazionali coinvolte[48].

La proposta di regolamento 2023 sulla gestione dei casi transfrontalieri

Per far fronte a tali difficoltà e sulla base delle **criticità rilevate dal Comitato**[49], nel 2023 la Commissione ha elaborato una **proposta di Regolamento** contenente norme aggiuntive all'applicazione del GDPR[50], prodromiche a consentire la **convergenza degli approcci procedurali** adottati dalle autorità di protezione dei dati e rendere più efficiente e armonizzata la gestione dei **casi transfrontalieri** in tutta l'UE.

La proposta di Regolamento è dunque tesa a definire più chiaramente le regole in diversi settori, tra cui i **reclami transfrontalieri**, il **coinvolgimento del reclamante**, i **diritti della difesa** delle parti oggetto dell'indagine (titolari del trattamento e responsabili del trattamento) e, soprattutto, la **cooperazione tra le autorità di protezione dei dati**[51].

Pertanto, in merito ai reclami, la proposta fornisce un **modulo** che specifica le informazioni richieste per tutti i reclami ai sensi dell'articolo 77 GDPR relativi al trattamento transfrontaliero, al fine di evitare che le autorità di protezione interpretino in modo diverso le prescrizioni relative alla **forma di un reclamo**, al

coinvolgimento dei reclamanti nella procedura e al **rigetto degli stessi**, e dunque che il trattamento dei reclami vari a seconda del luogo in cui il reclamo viene proposto o di quale autorità di protezione dei dati sia l'autorità capofila per un determinato caso.

Per quanto attiene la procedura di cooperazione di cui all'articolo 60 GDPR, invece, la proposta di Regolamento si occupa di **rafforzare la sinergia** tra le Autorità nei casi transfrontalieri, avendo dimostrato la recente esperienza nell'applicazione del GDPR in tali ipotesi l'insufficiente coordinamento tra autorità dei dati prima della presentazione di un **progetto di decisione dell'autorità capofila**, dal momento che la procedura di cui all'art. 60 è descritta a grandi linee, prevedendo unicamente che le autorità di protezione dei dati sono tenute a **scambiarsi le "informazioni utili"** nell'adoperarsi per raggiungere un consenso, salvo successivamente poter sollevare «**obiezioni pertinenti e motivate**» al progetto di decisione dell'autorità capofila.

Tali obiezioni, data anche la differenza di forma e struttura con cui vengono proposte e l'assenza di un **coordinamento ex ante** tra le Autorità, aumentano però la probabilità di ricorso al **meccanismo di composizione delle controversie** di cui all'art. 65 GDPR, che, sebbene rappresenti un elemento essenziale per garantire un'**interpretazione coerente della normativa privacy**, dovrebbe essere riservato a **casi eccezionali**.

La proposta dunque delinea strumenti per raggiungere più agevolmente un **consenso condiviso** intorno alla misura da adottare nei casi transfrontalieri, assegnando **maggior concretezza all'obbligo di cooperazione** e condivisione di informazioni utili da parte di autorità di controllo interessate, specificando i documenti compresi nelle informazioni che le autorità sono tenute a condividere nel corso dell'operazione transfrontaliera e consentendogli di **comunicare le loro opinioni già nelle prime fasi** della procedura di indagine[52], in modo da incidere in modo significativo sull'indagine in corso, utilizzando anche tutti gli strumenti previsti dal GDPR, quali le **indagini congiunte** e l'**assistenza reciproca**.

Verrebbe così ridotta la probabilità di **divergenze** nelle fasi successive della procedura che richiederebbero il ricorso al meccanismo di composizione delle controversie.

Verso un quadro più solido e coerente di tutela della privacy

Il Regolamento appena esaminato – ancora presente allo stato di **mera proposta** – mette in luce gli **aspetti critici** della rete europea dei garanti, tentando, al contempo, di porre rimedio alla tendenza delle Autorità nazionali di ricorrere ad **interpretazioni giuridiche** per «eludere» il **principio di cooperazione** con il fine ultimo di attrarre innanzi a sé la competenza per poter garantire più velocemente la tutela dei «propri» interessati.

L'effettivo **rafforzamento della rete europea** garantirebbe infatti maggior tutela dei diritti e il conseguente **recupero della fiducia nelle istituzioni europee** circa la capacità di regolare efficacemente l'evoluzione digitale.

Come ricorda il Regolamento al Considerando n. 7, per far fronte alle sfide che la **rapida evoluzione tecnologica** e la **globalizzazione** presentano per la protezione dei dati personali, è più che mai indispensabile «un **quadro più solido e coerente**» a tutela della privacy nell'Unione, «affiancato da efficaci misure di attuazione», e che «la **certezza giuridica e operativa** sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche».

A tal fine, è necessario che proceda il **percorso di integrazione** intrapreso mediante l'implementazione dei **meccanismi amministrativi**.

Note

[1] C. Sartoretti, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in *Federalismi*, n. 13/2019.

[2] Sul punto, 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, 77.

- [3] V. Cuffaro, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. Cuffaro – R. D’Orazio – V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Giappichelli, 2019.
- [4] Per un approfondimento v. *ex multis*: F. Pizzetti, *Privacy e diritto europeo alla protezione dei dati personali*, I e II, Torino, 2016.
- [5] Ad esempio, l’età minima per il consenso dei minori in relazione ai servizi della società dell’informazione (articolo 8, paragrafo 1, del GDPR).
- [6] G. Finocchiaro, *Introduzione al Regolamento Europeo sulla protezione dei dati*, in *Nuove leggi civ.*, 2017, 1 ss.
- [7] Sul punto si vedano le riflessioni di F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, 1, *Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016, 140 ss.
- [8] In proposito, P. Passaglia, *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in *Consulta Online*, III, 2016, 334 ss, evidenzia che il Regolamento «risponde all’esigenza di strutturare uno *jus commune* europeo».
- [9] E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, n. 1/2018, 107 osserva che: «l’esigenza di una riforma della materia è sorta anche (e forse soprattutto) dalla continua evoluzione degli stessi concetti di *privacy* e di *data protection*, dovuta principalmente all’incessante progresso dei servizi *on line*».
- [10] 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.
- [11] M. S. Esposito, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla*

privacy e sulla protezione dei dati personali, Bologna, Zanichelli, 2017, 519.

[12] V. Considerando n. 7 GDPR.

[13] Parlamento europeo, *Proposta di risoluzione sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione*, (2020/2717(RSP)).

[14] Commissione europea, *Seconda relazione sull'applicazione del regolamento generale sulla protezione dei dati*, COM(2024) 357 final.

[15] **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, 423 ss.

[16] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, 1, cit, 113.

[17] Sul regime sanzionatorio e i relativi principi si v., M. Ratti, *Il regime sanzionatorio previsto dal Regolamento per l'illecito dei trattamenti dei dati personali*, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 595 ss.

[18] Sulla competenza dell'Autorità di controllo, si v., E. Guardigli, *Il Garante per la protezione dei dati e la cooperazione fra Autorità Garanti*, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 489 ss.

[19] Ai sensi dell'art. 4, p.to 23, si definisce «trattamento transfrontaliero»: 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;

[20] E. Guardigli, *Il Garante per la protezione dei dati e la cooperazione fra Autorità Garanti*, cit., 511; in proposito v. anche **V. Rizzo, Artt. 55-56, in G.M. Riccio – G. Scorza – E. Belisario (a cura di), GDPR e normativa privacy. Commentario, Milano-Vicenza, Wolters Kluwer, 2018, 463 ss.**

[21] V. art. 4, p.to 16 GDPR.

[22] V. EDPB, *Linee guida 8/2022 sull'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento*, 28 marzo 2023. Secondo una parte della letteratura, le modalità per l'individuazione dell'autorità capofila introdotte dal regolamento (UE) 2016/679 avrebbero ridotto il rischio, diffuso invece nel previgente assetto normativo delineato dalla direttiva 95/46/CE, del così detto fenomeno del forum shopping, ossia del fenomeno per cui alcune imprese sceglievano di insediare loro stabilimenti nel territorio degli Stati che, pur rispettando la Direttiva, avessero una legge nazionale particolarmente lasca rispetto ai vincoli di tutela degli interessati. Così 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, 400; v. F. Parodo, *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*, in **Federalismi, n. 25/2021**, nota 144: «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».

[23] C. Del Federico – A. R. Popoli, *Disposizioni generali*, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 78.

[24] In proposito v. V. C. Ippoliti Martini, *Comitato europeo per la protezione dei dati*, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 554, definisce il WP29, strumento di “raccordo permanente” tra le Autorità nazionali. Sulla funzione svolta dal WP29, cfr. G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati personali*, cit.

[25] Espressione utilizzata da F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, 2, *Il regolamento europeo 2016/679*, Giappichelli, Torino, 2016, 106.

[26] Sulla struttura del Comitato e le sue funzioni si veda, C. Bistolfi, *I soggetti di controllo e verifica*, in C. Bistolfi – L. Bolognini – E. Pelino (a cura di), *Il Regolamento privacy europeo*, Milano, Giuffrè, 2016, 665 ss; V. C. Ippoliti Martini, *Comitato europeo per la protezione dei dati*, cit., 552 ss.

[27] **G. Della Morte, Art. 70**, in R. D’Orazio – G. Finocchiaro – O. Pollicino – G. Resta (a cura di), *Codice della privacy e Data Protection*, Milano, Giuffrè, 2021, 830.

[28] Sul ruolo del Garante europeo della protezione dei dati all’interno del Comitato v. G. Della Morte, *Art. 70*, cit., 822.

[29] Così M. S. Esposito, *Il meccanismo di coerenza. Comitato europeo per la protezione dei dati personali*, in G. Finocchiaro (opera diretta da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 538.

[30] M. S. Esposito, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., 521.

[31] La definizione normativa di «*obiezione pertinente e motivata*» è contenuta nell'art. 4 n. 24 RGPD, 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».

[32] In questo senso v. F. Parodo, *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*, cit., 24.

[33] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, 1, cit., 165 ss.

[34] In tal senso si esprime F. Parodo, *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*, cit., 130; v. anche V. Rizzo, *Artt. 55-56*, cit., 469; M.S. Esposito, *Il trattamento transfrontaliero e la cooperazione tra Autorità Garanti*, cit., 528.

[35] Per un approfondimento su questi strumenti v. F. Cardarelli, *Artt. 60-62*, in R. D'Orazio – G. Finocchiaro – O. Pollicino – G. Resta (a cura di), *Codice della privacy e Data Protection*, cit., 754 ss.

[36] V. Art. 61, par. 4: «L'autorità di controllo richiesta non deve rifiutare di dare seguito alla richiesta, salvo che: a) non sia competente per trattare l'oggetto della richiesta o per le misure cui deve dare esecuzione; b) l'accoglimento della richiesta violi le disposizioni del presente regolamento o il diritto dell'Unione o dello Stato membro cui è soggetta l'autorità di controllo che riceve la richiesta».

[37] Cfr. Considerando n. 135, ai sensi del quale «È opportuno istituire un meccanismo di coerenza per la cooperazione tra le autorità di controllo, al fine di

assicurare un'applicazione coerente del presente regolamento in tutta l'Unione. Tale meccanismo dovrebbe applicarsi in particolare quando un'autorità di controllo intenda adottare una misura intesa a produrre effetti giuridici con riguardo ad attività di trattamento che incidono in modo sostanziale su un numero significativo di interessati in vari Stati membri. È opportuno che il meccanismo si attivi anche quando un'autorità di controllo interessata o la Commissione chiede che tale questione sia trattata nell'ambito del meccanismo di coerenza. [...]»

[38] *Amplius* sull'importanza del ruolo del Comitato nel quadro dell'uniformazione del diritto alla protezione dei dati v., V. Zambrano, *Il Comitato europeo per la protezione dei dati*, in V. Cuffaro – R. D'Orazio – V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 985 ss.

[39] M.S. Esposito, *Il meccanismo di coerenza. Comitato europeo per la protezione dei dati personali*, cit., 539.

[40] Il termine, ai sensi dell'art. 65 par. 2 regolamento (UE) 2016/679, può essere prorogato di un altro mese, tenendo conto della complessità della questione.

[41] Così si **esprime F. Lubian, Art. 65**, in R. D'Orazio – G. Finocchiaro – O. Pollicino – G. Resta (a cura di), *Codice della privacy e Data Protection*, cit., 793; M.S. Esposito, *Il meccanismo di coerenza. Comitato europeo per la protezione dei dati personali*, cit., 547.

[42] V. EDPB, *Contribution of the EDPB to the evaluation of the GDPR under Article 97*, 18 febbraio 2020.

[43] Di "federalismo esecutivo" discutono M. Macchia – C. Figliolia, *Autorità per la privacy e Comitato europeo nel quadro del General Data Protection Regulation*, cit., 2.

[44] Emblematica delle criticità derivanti dalle interpretazioni divergenti del GDPR da parte delle autorità di protezione dei dati è stata la decisione dell'Autorità di

controllo francese (CNIL) del 2021, che ha sanzionato Facebook (oggi Meta) e Google per non aver rispettato la normativa sui *cookie* e sulla protezione dei dati personali, omettendo di attivare il meccanismo di cooperazione richiesto dal GDPR in presenza di trattamenti transfrontalieri. Entrambe le imprese hanno infatti opposto alla CNIL una questione relativa al c.d. one-stop-shop, eccependo che la CNIL non avrebbe avuto competenza per giudicare le condotte delle società, in quanto quest'ultime avrebbero la sede europea in Irlanda, a Dublino. Secondo le società statunitensi, dunque, la CNIL avrebbe dovuto adire l'Autorità di controllo irlandese, in quanto avente il ruolo di Autorità di controllo capofila. La CNIL ha tuttavia ritenuto di non dover applicare il GDPR, fondando la decisione su due ordini di ragioni: da una parte, il ruolo di *lex specialis* della direttiva ePrivacy per il trattamento dei dati risultanti da servizi della società dell'informazione, rispetto al GDPR che nel Considerando n. 173 specifica come il Regolamento non si applichi al trattamento dei dati personali di cui alla direttiva ePrivacy, le cui disposizioni precisano e integrano la direttiva 95/46/CE (oggi, GDPR) (art. 1, par. 2 Direttiva ePrivacy); dall'altra parte, la CNIL chiarisce che il trattamento sanzionato si esaurisce nel completamento dell'installazione dei cookie sul terminale dell'utente, non coinvolgendo il trattamento oltreconfine da parte degli stabilimenti in Irlanda, che consiste nel vero e proprio utilizzo commerciale dei dati degli utenti e che configura dunque un "trattamento successivo".

[45] In questo senso v. la Commissione europea nella *Comunicazione della commissione al Parlamento europeo e al Consiglio, La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati*, COM(2020) 264 final, la quale evidenzia come «Al fine di realizzare il pieno potenziale del regolamento generale sulla protezione dei dati, è importante creare un approccio armonizzato e una cultura europea comune della protezione dei dati, nonché promuovere una gestione maggiormente efficiente ed armonizzata dei casi transfrontalieri».

[46] Cfr. EDPB, *Linee-guida 02/2022 sull'applicazione dell'articolo 60 del regolamento generale sulla protezione dei dati*, 14 marzo 2022.

[47] Cfr. EDPB, *Linee-guida 3/2021 sull'applicazione dell'articolo 65, paragrafo 1, lettera a), GDPR*, 24 maggio 2023.

[48] Come rilevato di recente anche dalla Commissione europea nella *Seconda relazione sull'applicazione del regolamento generale sulla protezione dei dati*, COM(2024) 357 final.

[49] V. EDPB, *Letter to the EU Commission on procedural aspects that could be harmonised at EU level*, 10 ottobre 2022, che tra gli aspetti procedurali che necessitano di armonizzazione ha selezionato i seguenti: «*the status and rights of the parties to the administrative procedures; procedural deadlines; requirements for admissibility or dismissal of complaints; investigative powers of Supervisory Authorities; and the practical implementation of the cooperation procedure*».

[50] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme procedurali aggiuntive relative all'applicazione del regolamento (UE) 2016/679 (COM(2023) 348 final).

[51] Secondo la Commissione, infatti, «l'armonizzazione di tali aspetti procedurali favorirebbe il tempestivo completamento delle indagini e l'offerta di rimedi rapidi alle persone» (*Seconda relazione sull'applicazione del regolamento generale sulla protezione dei dati*, cit.).

[52] Cfr. Capo III, della proposta di Regolamento, rubricato "Cooperazione a norma dell'articolo 60 del regolamento (UE) 2016/679".

Innovare la sanità è possibile: ecco come farlo in modo sostenibile

Intelligenza Artificiale # Sanità



[Leggi l'informativa sulla privacy](#)

E-mail aziendale*

Acconsento alla comunicazione dei miei dati a terzi affinché li trattino per proprie finalità di marketing tramite modalità automatizzate e tradizionali di contatto.

SCARICA ORA

@RIPRODUZIONE RISERVATA

Valuta la qualità di questo articolo



Veronica Montozzi

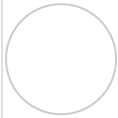
dottoranda di Ricerca in Discipline Giuridiche Pubblicistiche, curriculum Discipline Pubblicistiche, Internazionalistiche ed Europee presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tre

Seguimi su

Leggi anche:

- [Registrar TLD e NIS 2, le novità per i gestori di registri di nomi di dominio](#)
- [Blackout spagnolo: chi muove i fili dell'instabilità globale?](#)

- **Algoritmi predittivi: il futuro della sicurezza passa dal diritto**



Lasciaci il tuo parere!

B *I* U

Nome

Email*

Sito web

Commenta

0 COMMENTI

WHITEPAPER

Agenda Digitale e coesione: come gli investimenti europei stanno plasmando il futuro digitale dell'Italia

02 Lug 2025



Scaricalo gratis!

DOWNLOAD

WHITE PAPER

AI Officer: il ruolo chiave per governare l'intelligenza artificiale in azienda

30 Lug 2025

Scaricalo gratis!

DOWNLOAD

Argomenti

o su Cyber Security

T Tutto su GDPR

Canali

P Privacy

S Sicurezza digitale

Con o Senza – Galaxy AI per il business

Galaxy AI 

 Filtra per topic



CON SENZA l'AI in ufficio?

L'AI delle piccole cose: micro-task automatizzati per più strategia

LA SOLUZIONE

Meno tempo sui micro-task e più focus sulle attività a valore aggiunto: l'AI mobile a supporto della produttività

InnovAttori



L'IA alleata degli chef: così aiuta a innovare e a sprecare meno

19 Feb 2026



Tracciabilità supply chain, come Erp e cloud spingono la competitività

14 Nov 2025



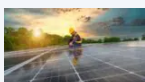
Manifattura elettronica, come salvare il settore con la gestione smart degli impianti

31 Ott 2025



Cybersecurity nel manifatturiero, perché puntare sulle persone: il ruolo di policy e formazione

01 Ott 2025



AI per il lavoro in condizioni estreme, quali tecnologie scegliere

27 Ago 2025

[Vedi tutti gli approfondimenti >](#)

Articoli correlati




LA GUIDA

Registrar TLD e NIS 2, le novità per i gestori di registri di nomi di dominio

07 Ago 2025

di Federica Maria Rita Livelli

Condividi 



SICUREZZA

Blackout spagnolo: chi muove i fili dell'instabilità globale?

09 Mag 2025

di Marco Calamari

Condividi 





WHITE PAPER

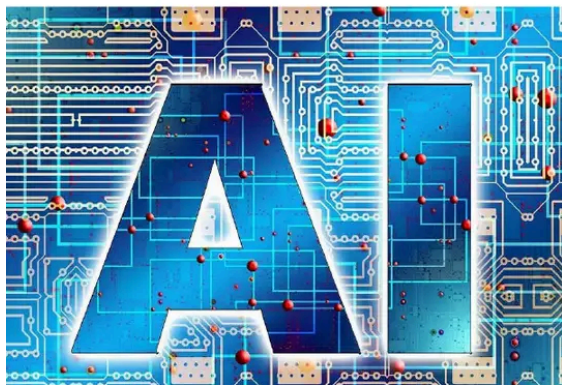
AI Officer: il ruolo chiave per governare l'intelligenza artificiale in azienda

30 Lug 2025

NETWORK₃₆₀

**AI OFFICER: UN PRESIDIO
DI LEGALITÀ PER L'USO
RESPONSABILE DELL'AI**

Pietro Boccaccini
Director, Deloitte Legal



Scaricalo gratis!

DOWNLOAD