STUDIO LEGALE
GIOVANNIPAOLOACCINNI
E ASSOCIATI

Il regolamento 2016/679/UE: GDPR

SOMMARIO: 1. Premessa – 2. Ambiti applicativi – 3. I principi fondamentali del GDPR – 4. Le figure principali: "titolare del trattamento", "responsabile del trattamento", e "DPO" – 5. Doveri e responsabilità del titolare e del responsabile del trattamento – 6. Codici di condotta e certificazioni – 7. Risarcimenti e sanzioni – 8. Autorità di controllo e relativi poteri.

* * *

1. Premessa

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il regolamento 2016/679/UE "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", ormai noto come GDPR. Il regolamento abroga la direttiva 95/46/CE, in attuazione della quale in Italia era stato adottato il d.lgs. 30 giugno 2003, n. 196 (c.d. "Codice della Privacy"). La scelta del legislatore comunitario di utilizzare il regolamento (e non più la direttiva) è intesa ad assicurare una diretta applicabilità delle norme all'interno dei singoli Stati membri, per favorire una maggior completezza, chiarezza ed uniformità di disciplina.

Il GDPR è quindi entrato in vigore il 24 maggio 2016 e gli Stati membri dovranno ora dare piena applicazione alle sue disposizioni entro (e non oltre) la data del 25 maggio 2018[1]. Nel regolamento si legge che "*la portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso*"[2] rendendo perciò opportuna la riaffermazione, a livello europeo, del principio in forza del quale "*il trattamento dei dati personali dovrebbe essere al servizio dell'uomo*"[3]. In estrema sintesi può dirsi che il regolamento introduca regole più chiare in materia di informativa e consenso, definisca i limiti al trattamento automatizzato dei dati personali, ponga le basi per l'esercizio di nuovi diritti, stabilisca criteri rigorosi per il trasferimento dei dati al di fuori dell'Unione europea e per i casi di violazione dei dati personali (c.d. *data breach*). Mentre l'obiettivo della previgente direttiva era quello di tutelare i singoli nei confronti dei responsabili del trattamento dei dati, obiettivo del nuovo regolamento in esame è per contro quello di prevenire e sanzionare (severamente) i trattamenti illegittimi, anche a prescindere dalla effettiva necessità di tutela del singolo cui i dati si riferiscono. Nella nuova normativa europea la protezione dei dati personali non è dunque più concepita unicamente come diritto fondamentale dell'individuo, ma (anche e soprattutto) come interesse della collettività.

[1] Regolamento 2016/679/UE, art. 99, comma 2.
[2] Regolamento 2016/679/UE, *considerandum* n. 6.
[3] Regolamento 2016/679/UE, *considerandum* n. 4.

2. Ambiti applicativi

Per quanto concerne l'ambito applicativo, il regolamento pone limitazioni sia sul versante "materiale", che su quello "territoriale":

- ambito di applicazione materiale (art. 2): si afferma che la normativa "*si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*". Tra i limiti di applicazione materiale vanno in particolare segnalati quelli operanti nei riguardi dei trattamenti di dati personali "*effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico*", nonché di quelli "*effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali*"[4].

- ambito di applicazione territoriale (art. 3): si legge che il regolamento si applica "*al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*". Viene poi precisato che l'applicazione è altresì estesa "*al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

3. I principi fondamentali del GDPR

Il regolamento (strutturato in 99 articoli, preceduti da 173 *consideranda*) è complessivamente informato a tre fondamentali principi:

1) il principio di trasparenza: impone che le informazioni relative all'identità del titolare del trattamento dei dati e le finalità del trattamento siano facilmente accessibili e di facile comprensione per gli interessati, sin dal momento della raccolta dei dati (grazie ad un linguaggio semplice e chiaro);

2) il diritto all'oblio: consiste nel diritto di ottenere la cancellazione dei propri dati quando sia venuta meno la finalità per la quale se ne è consentito l'uso e comunque quando non sussistano più i motivi che possono averne giustificato la diffusione. Ai fini di dare concreta attuazione a tale diritto, il regolamento prevede il "diritto di rettifica" (art. 16) ed il "diritto alla cancellazione" (art. 17);

3) il principio di *accountability*: può essere tradotto come principio di responsabilizzazione e obbligo di rendicontazione. Nasce in ambito aziendale per

[4] Regolamento 2016/679/UE, art. 2, comma 2.

indicare i doveri di trasparenza, di *compliance* e di rendicontazione di scelte, comportamenti ed azioni.

Il principio di *accountability* rappresenta un momento baricentrico della normativa e conserva siffatta propria natura anche nel contesto di un'analisi dei profili di responsabilità dei soggetti incaricati, tanto da essere richiamato all'art. 24 (rubricato per l'appunto "responsabilità del titolare del trattamento"), in cui si ingiunge al titolare del trattamento di mettere in atto "*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*".

4. Le figure principali: "titolare del trattamento", "responsabile del trattamento", e "*DPO*".

Il regolamento individua tre figure che (in misura diversa tra loro) fungono da principali destinatari delle norme ivi contenute. Stando alle definizioni fornite dallo stesso GDPR all'art. 4, si tratta in particolare del:

- Titolare del trattamento: "*la persona **fisica o giuridica**, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali***".
Il titolare del trattamento può considerarsi come figura di vertice nella gestione dei dati e nella ripartizione delle responsabilità derivanti dal trattamento dei dati personali. Ne è riprova il *considerandum* n. 74, che afferma l'opportunità di "*stabilire la **responsabilità generale** del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato **direttamente** o che altri abbiano effettuato **per suo conto***". Analogamente, l'art. 24 impone al titolare di mettere in atto "*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*", "*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*". La stessa norma prescrive inoltre che le suddette misure tecniche ed organizzative siano "*riesaminate ed aggiornate qualora necessario*"[5].
Esiste poi la possibilità di individuare più di un titolare del trattamento. A norma dell'art. 26, nel caso in cui due o più titolari del trattamento determinino congiuntamente finalità e mezzi del trattamento, essi saranno infatti considerati "***contitolari** del trattamento*". In tal caso, questi soggetti sono tenuti a determinare in modo trasparente, mediante un **accordo interno**, le rispettive responsabilità in merito all'osservanza degli obblighi stabiliti dal GDPR. I contenuti essenziali dell'accordo sono messi a disposizione dell'interessato che potrà esercitare i propri diritti *"nei confronti di e contro ciascun titolare del trattamento*", indipendentemente dalle disposizioni dell'accordo.

[5] In ciò si coglie un primo evidente parallelismo con il concetto di "modello organizzativo" proprio del d.lgs. 231/2001. Occorre poi precisare sin da ora che l'art. 32 ("Sicurezza del trattamento") pone l'onere di adottare le misure tecniche ed organizzative adeguate sia in campo al titolare, che al responsabile del trattamento, come si avrà modo di spiegare nel prosieguo.

- Responsabile del trattamento: la persona (fisica o giuridica) che "*tratta dati personali **per conto** del titolare del trattamento*".
In tema di **delega di funzioni** l'art. 28 ed il *considerandum* n. 81 del GDPR stabiliscono che, qualora il titolare deleghi il trattamento ad un responsabile, questi debba presentare "garanzie sufficienti" (soprattutto in termini di conoscenza specialistica, affidabilità e risorse) a mettere in atto le misure tecniche ed organizzative in questione[6]. Importante rammentare che, *ex* art. 28, comma 10, il responsabile che (in violazione del regolamento) determini le finalità e i mezzi del trattamento sarà considerato un "titolare" del trattamento.
Alcune precisazioni ulteriori sulla figura del responsabile del trattamento meritano quindi qui di seguito di essere evidenziate. In particolare, al responsabile è inibita la facoltà di *sub*-delega senza aver ottenuto preventiva autorizzazione scritta da parte del titolare. I trattamenti dei dati effettuati dal responsabile sono disciplinati da un contratto (o altro atto giuridico) che vincoli il responsabile al titolare e che chiarisca materia, durata, natura e finalità del trattamento. Il contratto deve poi prevedere che i dati possano essere trattati dal responsabile solo su istruzione documentata del titolare.

[N.B.: ai sensi dell'art. 27, il titolare ed il responsabile del trattamento devono designare un proprio "**rappresentante** nell'Unione" nel caso in qui questi siano stabiliti al di fuori dell'Unione, ma trattino dati di soggetti situati sul territorio dell'Unione[7]].

- Responsabile della protezione dei dati (c.d. "D.P.O." – *Data Protection Officer*): è una figura eventuale che il titolare del trattamento ed il responsabile del trattamento sono tenuti a designare, ai sensi dell'art. 37, in soli tre casi:

> - quando il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali);
>
> - quando le attività principali del titolare o del responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
>
> - quando le attività principali del titolare o del responsabile del trattamento consistano nel trattamento, su larga scala, di particolari categorie di dati personali, quali i c.d. "dati sensibili" e/o i dati relativi a condanne penali e a reati (*ex* art. 10 del regolamento).

---

[6] Il responsabile può dimostrare di disporre di tali "garanzie" mediante la propria adesione ad un codice di condotta approvato (*ex* art. 40) o ad un meccanismo di certificazione approvato (*ex* art. 42). Sui meccanismi di certificazione sulla loro valenza "scriminante" si tornerà *infra*.

[7] Per espressa previsione dello stesso art. 27, comma 2, l'obbligo di designare un rappresentante non si applica:
"*a) al trattamento se quest'ultimo è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento; oppure*
b) alle autorità pubbliche o agli organismi pubblici".

La nomina di un DPO al di fuori di tali casi rimane mera facoltà rimessa alla discrezione del titolare e del responsabile del trattamento dei dati (salvo che sia resa obbligatoria da altre fonti del diritto dell'Unione o dei singoli Stati membri). Purtuttavia, nell'ambito di un "gruppo imprenditoriale" è possibile nominare un unico DPO a condizione che questi sia "*facilmente raggiungibile da ciascuno stabilimento*"[8]. Il regolamento prescrive inoltre che il DPO sia designato "*in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati*". Il DPO può essere un dipendente del titolare e/o del responsabile del trattamento, ovvero potrà assolvere i propri compiti in base ad un contratto di servizi. I dati di contatto del DPO devono essere pubblicati e comunicati all'autorità di controllo[9].

5. Doveri e responsabilità del titolare e del responsabile del trattamento

Come già si è avuto modo di anticipare, il titolare ed il responsabile del trattamento (quest'ultimo tenuto ad assistere e collaborare con il primo) debbono adoperarsi in modo da garantire che il trattamento dei dati personali venga effettuato conformemente alle prescrizioni del GDPR e comunque in maniera tale da evitare compromissioni e lesioni dei diritti degli interessati[10]. In tal senso si segnala l'adozione di "*misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*" prescritta dagli artt. 24, 25 e 32. Quest'ultima norma precisa inoltre come le suddette misure debbano (tra l'altro) ricomprendere (se del caso): *a)* la pseudonimizzazione e la cifratura dei dati personali; *b)* la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; *c)* la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; *d)* una procedura per testare regolarmente l'efficacia delle misure adottate.

E' necessario poi chiarire i concetti di "*privacy by design*" e di "*privacy by default*" delineati all'art. 25 nei termini che seguono:

- comma 1 (**privacy by design**)[11]: "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,* ***sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso*** *il titolare del trattamento*

[8] Regolamento 2016/679/UE, art. 37. comma 2.

[9] Gli artt. 38 e 39 definiscono la posizione ed i compiti del DPO. Tra i profili più rilevanti si segnala che il DPO non deve ricevere influenze/istruzioni da parte del titolare e/o del responsabile per quel che concerne l'esecuzione dei compiti suoi propri. Il DPO è inoltre chiamato a fungere da punto di contatto tra il titolare del trattamento, i singoli interessati e l'autorità di controllo. Questi inoltre fornisce consulenza (ove richiesta) al titolare e al responsabile e coopera con l'autorità di controllo.

[10] Per evidenti ragioni di brevità non ci si soffermerà ora ad analizzare nel dettaglio le modalità prescritte dal regolamento per la raccolta ed il trattamento dei dati. In proposito basti ricordare che l'intero sistema si basa sul concetto cardine del "consenso", assunto a condizione di liceità del trattamento dei dati ai sensi degli artt. 5 e seguenti, ove si chiarisce peraltro che il titolare del trattamento deve essere in grado di comprovare il consenso prestato (in virtù del principio di "responsabilizzazione").

[11] Per espressa previsione dell'art. 25, ultimo comma, "*un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo*". In tema di certificazioni si tornerà nel prosieguo.

*mette in atto misure tecniche e organizzative adeguate, quali la **pseudonimizzazione**, volte ad attuare in modo efficace i principi di protezione dei dati, quali la **minimizzazione**, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*". Ed è quanto si intende con obbligo di "protezione dei dati fin dalla progettazione" (c.d. privacy by design);

- comma 2 (**privacy by default**): "*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che **siano trattati, per impostazione predefinita, solo i dati personali necessari** per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, **per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica***". In questi termini viene quindi definito il dovere di protezione dei dati "per impostazione predefinita" (c.d. privacy by default).

Seguono poi ulteriori adempimenti che il titolare ed il responsabile hanno il dovere di rispettare. Primo fra questi è la tenuta dei **registri delle attività di trattamento** disciplinata dall'art. 30. In buona sostanza, il titolare ed il responsabile (nonché, ove presenti, i rispettivi "rappresentanti") sono **in alcuni casi**[12] obbligati a conservare traccia delle attività di trattamento dei dati personali effettuate sotto la propria responsabilità (nel caso del titolare) o per conto di un titolare del trattamento (nel caso del responsabile). Il contenuto di tali registri è puntualmente tipizzato all'art. 30, ove vengono elencate le informazioni di cui è necessario mantenere traccia. Per espressa previsione normativa i registri vanno tenuti in forma scritta, anche in formato elettronico e, su richiesta, devono essere messi a disposizione dell'autorità di controllo a cura del titolare e del responsabile.

Ulteriore obbligo gravante sul titolare del trattamento (che si consulta con il DPO) è quello previsto dall'art. 35 che stabilisce che il titolare, prima di procedere ad un trattamento dei dati che involga l'uso di nuove tecnologie, debba svolgere una **valutazione dell'impatto** che siffatto trattamento è suscettibile di avere sulla protezione dei dati, allorquando esso presenti un elevato rischio per i diritti e le libertà delle persone fisiche. Siffatta valutazione d'impatto è volta a determinare quali siano le misure organizzative e di sicurezza da adottarsi per rispettare il disposto del nuovo regolamento. Nel caso in cui la valutazione compiuta a norma dell'art. 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare, quest'ultimo dovrà consultare l'autorità di controllo prima di procedere al trattamento, avviando così l'*iter* amministrativo disciplinato dall'art. 36 (**consultazione preventiva**).

Si giunge così alle prescrizioni di maggiore interesse, ossia quelle inerenti l'obbligo di "segnalare" eventuali violazioni di dati all'autorità di controllo ed al singolo

[12] L'obbligo di tenuta dei "registri" non si applica alle imprese od organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (vale a dire quelli c.d. "sensibili" e quelli relativi a reati e precedenti penali).

interessato[13]. In tema di "**notifica**" di una violazione dei dati personali all'autorità di controllo occorre pertanto rifarsi al disposto dell'art. 33, a norma del quale, in caso di violazione, il titolare dovrà darne notizia all'autorità di controllo competente (*ex* art. 55) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore** dal momento in cui ne sia venuto a conoscenza, "*a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*"[14]. Qualora la notifica non sia eseguita entro 72 ore deve essere corredata dei **motivi del ritardo**[15].

L'art. 33, nel tipizzare il contenuto della notifica[16], chiarisce quindi che essa deve "*almeno*":
- descrivere la natura della violazione dei dati personali, compresi (ove possibile) le categorie ed il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione (da parte del titolare del trattamento) per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire tali informazioni contestualmente alla notifica, queste potranno essere comunicate in fasi successive, ma "*senza ulteriore ingiustificato ritardo*". Si prescrive comunque al titolare del trattamento di **documentare** qualsiasi violazione dei dati personali (comprese le circostanze ad essa relative, le conseguenze ed i provvedimenti adottati per porvi rimedio). Tale documentazione consente all'autorità di controllo di verificare il rispetto delle norme contenute appunto nell'art. 33.

Altro aspetto è invece quello della "**comunicazione**" da darsi all'interessato *ex* art. 34 in caso di violazione dei dati. Questa dovrà essere fornita dal titolare all'interessato "*senza ingiustificato ritardo*" quando la violazione sia "*suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche*". La norma precisa come la comunicazione vada formulata in un linguaggio semplice e chiaro, debba descrivere la natura della violazione e contenere almeno le informazioni e le misure proprie della "notifica" all'autorità[17].

---

[13] Si parla tecnicamente di "notifica" all'autorità e di "comunicazione" all'interessato.

[14] La notifica, pertanto, non sarà sempre dovuta. Il giudizio di opportunità è rimesso allo stesso titolare del trattamento in ossequio al principio di "responsabilizzazione" cui è informato l'intero regolamento.

[15] Preme precisare che, nel caso in cui sia il responsabile del trattamento ad acquisire per primo contezza dell'avvenuta violazione, questi sarà gravato dell'obbligo di informarne il titolare "*senza ingiustificato ritardo*".

[16] Non sono ancora previste modalità dettagliate in relazione al "formato" ed alle "procedure" applicabili alla notifica in parola, rispetto alle quali il *considerandum* n. 88 si limita ad indicare alcuni punti di cui occorrerà tener conto nel darvi definizione. Da segnalarsi, tuttavia, che nel 2015 il Garante della Privacy aveva predisposto un "modello" per procedere alla comunicazione delle violazioni di dati personali (già prescritta dal Codice della Privacy) che sembrerebbe poter fungere da base di lavoro (seppure con i dovuti accorgimenti) per la redazione della notifica prevista dalla nuova normativa.

[17] Ad eccezione dell'indicazione delle categorie e del numero approssimativo di interessati in questione, nonché delle categorie e del numero approssimativo di registrazioni di dati personali in questione.

La stessa disposizione prevede poi una serie di ipotesi in cui la comunicazione non è richiesta, ovverosia quando sia soddisfatta almeno una delle seguente condizioni:
- il titolare del trattamento abbia messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure siano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la "comunicazione" richiederebbe sforzi sproporzionati. In tale evenienza, si procede ad una comunicazione pubblica (o una misura simile), tramite la quale gli interessati siano informati con analoga efficacia.

6. Codici di condotta e certificazioni

Sovente le norme del regolamento stabiliscono che l'adesione ai codici di condotta e/o il conseguimento di certificazioni possano fungere da "esimente" per il titolare del trattamento ove chiamato a rispondere di eventuali violazioni di dati o, più in generale, di illeciti trattamenti degli stessi. Per fare qualche esempio si potrebbe pensare al sopracitato art. 25 che, nel delineare gli oneri di protezione dei dati "fin dalla progettazione" e "per impostazione predefinita", al suo ultimo comma precisa che "*un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti*". Ancora, in senso analogo, si riscontra il terzo comma dell'art. 32 in cui pure si afferma che "*l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti*" previsti dal regolamento. L'elenco di norme che riconoscono questo tipo di valenza all'adesione ai codici di condotta e/o al meccanismo di certificazione sarebbe ancora lungo, passando dall'art. 35 in tema di "valutazione di impatto", per arrivare all'art. 83, regolante (come si vedrà *infra*) le "condizioni generali per infliggere sanzioni amministrative pecuniarie". Quest'ultimo, alla lettera *j*) del secondo comma, chiarisce che "*al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa* […] *si tiene debito conto* […] *dell'adesione ai codici di condotta approvati ai sensi dell'art. 40 o ai meccanismi di certificazione approvati ai sensi dell'art. 42*". Si ritiene dunque utile spendere qualche più espresso riferimento almeno al merito del disposto degli artt. 40 – 43.

(**Codici di condotta**): a norma dell'art. 40 "*le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento*". La norma, chiarendo l'*iter* da seguire, stabilisce che i codici "approvati" (e passati al vaglio delle competenti autorità) vengano pubblicati e registrati in un apposito registro da tenersi aggiornato con le eventuali modifiche ed integrazioni successivamente apportate. Esiste quindi una procedura di "monitoraggio" dei codici di condotta approvati che è affidata ad un organismo preposto in base all'art. 41. I codici così approvati, aggiornati e registrati hanno "*validità generale all'interno dell'Unione*". Possono allora dichiarare di aderire a tali codici non soltanto i titolari ed i responsabili soggetti all'applicazione del GDPR (a norma dell'art.

3), ma anche gli altri che desiderino (nondimeno) fornire le adeguate garanzie nel quadro dei trasferimenti di dati personali verso paesi terzi od organizzazioni internazionali.

(**Certificazione**): a norma dell'art. 42 viene incoraggiata l'istituzione di "***meccanismi** di certificazione della protezione dei dati, nonché di **sigilli** e **marchi** di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati*" dai titolari e dai responsabili. La norma prevede sin da ora i principii cardine cui dovranno informarsi i meccanismi di certificazione. Tra questi si segnala il fatto che la certificazione debba essere "volontaria" e "accessibile tramite una procedura trasparente". La certificazione è rilasciata al titolare e/o al responsabile del trattamento per un periodo massimo di 3 anni e può essere rinnovata a condizione che i requisiti continuino ad essere soddisfatti. Di converso, laddove siffatti requisiti non siano più soddisfatti gli organismi[18] di certificazione o l'autorità di controllo potranno revocare la certificazione. Importante tenere comunque presente che "*la certificazione* […] ***non** riduce la responsabilità del titolare del trattamento o del responsabile* […] *riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti*" (art. 42, comma 4). Come accennato *supra* l'adesione a codici di condotta o a meccanismi di certificazione potrà (e dovrà) tuttavia essere "tenuta in debito conto" al momento di decidere l'*an* ed il *quantum* della sanzione amministrativa pecuniaria (come stabilito dal già citato art. 83).

7. Risarcimenti e sanzioni

Le conseguenze di un trattamento di dati illecito si proiettano su due distinti piani: quello risarcitorio e quello sanzionatorio.

- **Risarcimento**: per quanto concerne l'analisi del primo versante occorre rifarsi all'art. 82 del regolamento. Questo sancisce il principio generale del "**diritto al risarcimento**" in forza del quale "*chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno **dal titolare del trattamento o dal responsabile** del trattamento*". La norma precisa inoltre che "*un **titolare** del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il regolamento*"; mentre "*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*". Tanto premesso, va comunque fatta salva la regola per cui il titolare ed il responsabile sono esonerati da responsabilità ove dimostrino che l'evento dannoso non sia loro "*in alcun modo imputabile*".
Lo stesso art. 82, al suo quarto comma, prevede inoltre un principio di **solidarietà passiva** tra titolari e responsabili "*coinvolti nello stesso trattamento*". In tal senso ogni titolare o responsabile del trattamento è perciò "*responsabile **in solido per l'intero** ammontare del danno*", sì da garantire l'effettività del risarcimento all'interessato. Come naturale, il titolare o il responsabile che abbia risarcito il danno per intero avrà

[18] L'art. 43 prevede che siano istituiti ed accreditati degli "organismi di certificazione" che soddisfino i requisiti ivi indicati.

poi il diritto di **agire in regresso** nei confronti dei coobbligati coinvolti per ripetere la quota di risarcimento corrispondente alla loro parte di responsabilità.

- **Sanzioni**: le norme da assumersi quale punto di riferimento per l'analisi del versante sanzionatorio sono quelle contenute nell'art. 83, rubricato "*condizioni generali per infliggere sanzioni amministrative pecuniarie*". A norma del primo comma del citato articolo, le sanzioni da irrogarsi devono rispondere ai tre requisiti di "effettività", "proporzionalità" e "dissuasività". Le stesse vanno quindi inflitte in funzione delle "*circostanze di ogni singolo caso*" e possono essere irrogate in aggiunta ovvero in sostituzione di quelle previste dall'art. 58, comma 2, lett. *a*) – *h*) e *j*)[19].
Al momento di valutare l'*an* ed il *quantum* della sanzione amministrativa pecuniaria il regolamento (art. 83, comma 2) prescrive di tenere in debito conto alcuni elementi, quali, a più significativo esempio:

- natura, gravità e durata della violazione, anche in considerazione della natura, dell'oggetto e della finalità del trattamento in questione, nonché del numero di interessati lesi e della gravità dei danni subiti;
- carattere doloso o colposo della violazione;
- misure adottate dal titolare o dal responsabile per attenuare il danno;
- **grado di responsabilità del titolare o del responsabile alla luce delle misure tecniche ed organizzative adottate** (*ex* artt. 25 e 32);
- eventuali precedenti violazioni commesse dal titolare o dal responsabile;
- grado di cooperazione con l'autorità di controllo;
- categorie di dati personali interessate dalla violazione;
- modalità con cui l'autorità di controllo ha avuto conoscenza della violazione (in particolare: **se ed in che misura è stata fatta la notifica** della violazione);
- rispetto o meno dei provvedimenti eventualmente disposti in precedenza a norma del già richiamato art. 58, comma 2;

[19] Ai sensi dell'art. 58, comma 2, "*ogni autorità di controllo ha tutti i poteri correttivi seguenti:*
a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;
b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;
c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;
d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
[…]
j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale".

- **adesione a codici di condotta** approvati (art. 40) **o ai meccanismi di certificazione** (art. 42);
- eventuali altri fattori aggravanti o attenuanti applicabili (es. benefici finanziari conseguiti o perdite evitate, direttamente o indirettamente, in conseguenza della violazione).

Urge allora una precisazione. Ai sensi dell'art. 83, comma 3, "*se, **in relazione allo stesso trattamento** o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, **varie disposizioni** del presente regolamento, l'importo totale della sanzione* […] ***non supera** l'importo specificato per la violazione più grave*". Manifesto il parallelismo tra il principio ora esposto e la previsione del primo capoverso dell'art. 81 c.p. Il motivo del recepimento di un simile principio risulterà chiaro non appena ci si avveda della "severità" delle sanzioni previste dai commi 4, 5 e 6 dello stesso articolo.

A seconda del tipo di violazione sono infatti previste due cornici sanzionatorie:

- sanzione **fino a € 10 milioni** o, per le imprese, **fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente (se superiore), nel caso in cui in cui la violazione abbia ad oggetto:

1. gli obblighi del titolare o del responsabile del trattamento previsti dagli artt. 8 (condizioni del consenso del minore), 11 (trattamento che non richiede identificazione), 25 – 39 (privacy by design e by default; norme su titolare e responsabile; registro attività di trattamento; notifiche e comunicazioni di *data breach*; valutazione d'impatto; norme sul DPO), 42 e 43 (certificazione ed organismo di certificazione);
2. gli obblighi dell'organismo di certificazione a norma degli artt. 42 e 43;
3. gli obblighi dell'organismo di controllo a norma dell'art. 41, comma 4.

- sanzione **fino a € 20 milioni** o, per le imprese, **fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente (se superiore), nel caso in cui la violazione abbia ad oggetto:

1. i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli artt. 5 (principi applicabili al trattamento), 6 (liceità del trattamento), 7 (condizioni per il consenso) e 9 (trattamento di dati c.d. "sensibili");
2. i diritti degli interessati ai sensi degli artt. 12 – 22;
3. il trasferimento di dati personali ad un destinatario in un paese terzo o ad un'organizzazione internazionale *ex* artt. 44 – 49;
4. qualsiasi obbligo ai sensi delle legislazioni dei singoli Stati membri adottate a norma del capo IX;
5. l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati emanato dall'autorità di controllo *ex* art. 58, comma 2, o il negato accesso *ex* art. 58, comma 1.

L'art. 84 si pone infine quale "norma di chiusura" dell'apparato sanzionatorio del GDPR, stabilendo che "*gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni **non***

soggette a sanzioni amministrative pecuniarie a norma dell'art. 83 […]. *Tali sanzioni devono essere effettive, proporzionate e dissuasive*"[20]. Quest'ultima previsione necessita di lettura combinata a quella del *considerandum* n. 149, secondo il quale "*l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del* ***ne bis in idem*** *quale interpretato dalla Corte di giustizia*"[21]. Ad ogni modo, sembrerebbe essere preclusa per i singoli Stati membri la possibilità di assoggettare a sanzione anche penale le condotte già tipizzate all'art. 83 del regolamento e soggette a sanzione amministrativa pecuniaria. Dovrà quindi (eventualmente) trattarsi di fattispecie afferenti a condotte (attive od omissive) altre e diverse rispetto a quelle che già fanno incorrere titolare e responsabile del trattamento nelle assai afflittive sanzioni pecuniarie di cui si è appena detto. Le sanzioni penali che gli Stati "*dovrebbero poter stabilire*" potranno riguardare tanto la violazione "diretta" di norme contenute nel GDPR, quanto quella di norme nazionali adottate negli ordinamenti domestici in virtù e nei limiti dello stesso regolamento[22].

L'introduzione di nuove fattispecie penali *ad hoc* risulta pertanto eventuale e niente affatto scontata. Secondo una certa dottrina, alla luce del mero potere di indirizzo delle istituzioni europee in materia penale, gli Stati membri potrebbero infatti adempiere ai doveri imposti loro dal regolamento anche solo limitandosi ad applicare le sanzioni amministrative pecuniarie previste dall'art. 83 e introducendo ulteriori sanzioni amministrative pecuniarie ai sensi dell'art. 84; senza insomma essere tenuti ad introdurre norme incriminatrici *ad hoc*[23]. Di avviso opposto altra corrente dottrinale, secondo cui parrebbe addirittura "inevitabile" un adeguamento della legislazione penale nel nostro ordinamento[24]. Argomentando in tal senso, quest'ultima dottrina si sofferma a valutare la possibile abrogazione delle fattispecie penali già introdotte dal Codice della Privacy (in recepimento della previgente Direttiva 95/46/CE), in base alla loro

[20] Ogni Stato membro deve poi notificare **entro il 25 maggio 2018** alla Commissione le disposizioni di legge adottate.

[21] Il riferimento sembra essere a Corte Giust. UE (Grande Sezione), 26 febbraio 2013, C-617/10, *Aklagaren c. Hans Akerberg Fransson*. In tal senso, come anche chiarito in dottrina da M. LAMANUZZI, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della* privacy *e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, in *JusOnline*, 2017, 1, p. 256, "*l'applicazione di una sanzione penale per violazioni in materia di trattamento dei dati personali applicata in un procedimento divenuto definitivo osterà all'instaurazione di nuovi procedimenti penali per lo stesso fatto, non invece all'applicazione di sanzioni amministrative, purché l'effetto punitivo complessivo non risulti eccessivo*".

[22] Sul punto bene precisare che, ai sensi del *considerandum* n. 149, le sanzioni penali "*possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso la violazione del presente regolamento*". Con ciò si potrebbe forse legittimare qualche dubbio in ordine alla "sottraibilità" dei profitti ottenuti dalla violazione di norme adottate a livello solo domestico (seppur in attuazione del GDPR) e non già da violazioni "dirette" del regolamento.

[23] In tal senso cfr. L. BOLOGNINI, *Sanzioni penali*, in L. Bolognini, E. Pelino, C. Bistolfi (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 705.

[24] Il riferimento è, ancora una volta, a M. LAMANUZZI, *cit.*, p. 254-255. L'Autrice sul punto chiosa affermando che, malgrado il regolamento non ponga limitazioni rispetto ai soggetti sanzionabili, il principio di personalità della responsabilità penale vigente nel nostro ordinamento (art. 27 Cost.) escluderebbe che siano assoggettate a sanzioni penali le persone giuridiche. In proposito, tuttavia, ci si permette notare come, alla luce del noto d.lgs. 231/2001, potrebbero ben configurarsi estensioni di responsabilità (amministrativa dipendente da reato) anche agli enti nel cui interesse o vantaggio gli illeciti siano stati perpetrati.

compatibilità con la nuova normativa. In tal modo si sostiene che le ipotesi derivanti dal combinato disposto dell'art. 167, da una parte, e degli artt. 123 e 126 del Codice della Privacy, dall'altra, sarebbero da ritenersi abrogate in quanto queste ultime due sarebbero state "superate" dalla nuova e più dettagliata disciplina del trattamento dati (comuni e sensibili) contenuta agli artt. 6 e seguenti del regolamento. Per contro, altre ipotesi delittuose potrebbero rimanere valide. Si pensi in proposito al reato disciplinato dal combinato disposto degli artt. 167 e 130, consistente nella violazione di norme in materia di *e-privacy* e comunicazioni indesiderate, o, ancora, all'ipotesi contravvenzionale di cui all'art. 169 del Cod. della Privacy che punisce l'omissione delle misure minime di sicurezza di cui all'art. 33 e di cui all'Allegato B del Codice; "*disposizioni non incompatibili con il nuovo regime di* accountability *e di sicurezza delineato dal regolamento europeo*".
Sul punto si può dunque affermare che le strade alternative percorribili dal legislatore italiano per dare attuazione alle prescrizioni europee[25], e precisamente siano tre:

1) abrogare le fattispecie penali attualmente vigenti (previste dal Cod. Privacy) ed introdurre nuove fattispecie penali conformi al GDPR;
2) abrogare le fattispecie penali attualmente vigenti (previste dal Cod. Privacy) ed introdurre nuove sanzioni amministrative;
3) riformulare le fattispecie penali attualmente vigenti nelle sole parti incompatibili con il GDPR.

Rimanendo in tema di sanzioni penali e continuando ad adottare una prospettiva *de iure condendo*, appare infine opportuna qualche rapida considerazione inerente ai c.d. "reati presupposto" fondanti la responsabilità amministrativa da reato dell'ente. In passato si è infatti già assistito ad un tentativo del legislatore di arricchire il novero dei reati presupposto con quelli previsti in materia di privacy. Il d.l. 93/2013 apportava infatti modifiche all'art. 24-*bis* del d.lgs. 231/200, ampliandone il contenuto con un richiamo (anche) ai reati previsti dal Codice della Privacy. In sede di conversione del decreto, tuttavia, la l. 15 ottobre 2015, n. 119 ha espunto il riferimento a siffatti reati. Falliva così il primo tentativo di estendere la responsabilità degli enti alle violazioni afferenti la materia oggi in esame.
Le norme di recepimento del GDPR potrebbero portare tuttavia ad una riformulazione dei reati previsti dal Codice della Privacy ed eventualmente anche alla loro introduzione nel catalogo dei reati rilevanti *ex* d.lgs. 231/2001. Le stesse potrebbero poi comportare (come detto) anche la creazione di nuove fattispecie penali in materia, anch'esse potenzialmente fonte di responsabilità amministrativa da reato[26]. Va peraltro sottolineato come l'intera architettura del nuovo regolamento europeo sembri essere progettata sulla falsa riga del d.lgs. 231/2001, con il quale condivide molteplici punti di

[25] Sotto questo profilo si è affermato che il regolamento in oggetto abbia sostanzialmente la natura di "quasi direttiva" poiché, violando formalmente l'art. 83, par. 2, TFUE, ma rispettandone di fatto la *ratio*, si limita ad esercitare un'attività di indirizzo nei confronti dei legislatori nazionali cui è demandato il compito di adottare disposizioni penali in ossequio al principio di riserva di legge vigente in materia penale.
[26] Da segnalarsi quale ulteriore profilo di criticità il fatto che, ai sensi dell'art. 4, nn. 7) e 8), sia il titolare che il responsabile del trattamento possano essere indifferentemente persone fisiche o giuridiche. Elemento che dovrà essere tenuto in doverosa considerazione in sede di eventuale formulazione di nuove fattispecie sanzionatorie, onde scongiurare un contrasto con il principio secondo cui *societas delinquere non potest*.

contatto; primo fra tutti l'onere di adottare "misure tecniche ed organizzative adeguate" che sembrano riecheggiare in tutto e per tutto la filosofia dei "modelli organizzativi".

Concludendo, pare opportuno mettere in luce un ultimo profilo problematico dato dalla dubbia conciliabilità dell'obbligo di "notifica" del *data breach* (nonché del dovere di collaborazione *ex* art. 31) con il principio processual penalistico del *nemo tenetur se detegere*. La "scivolosità" del tema appare manifesta anche alla luce del *considerandum* n. 87 (secondo cui la notifica "*può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento*"), specie ove si consideri che, ai sensi dell'art. 58 del regolamento, ogni autorità di controllo è dotata di un'ampia serie di poteri di indagine[27]. La proposizione del problema può tuttavia apparire prematura, attesa la mancanza di fattispecie penali riconducibili a quelle stesse violazioni che, per l'appunto, istaurano l'obbligo di notifica all'autorità di controllo. A voler nondimeno azzardare una prima soluzione almeno intuitiva, potrebbe (auspicabilmente) pronosticarsi la scelta del legislatore italiano di non ricorrere alla formulazione di nuove norme incriminatrici, preferendo, di converso, relegare la sanzionabilità al solo piano amministrativo.

8. Autorità di controllo e relativi poteri

Il Capo VI del Regolamento è dedicato alle c.d. "Autorità di controllo indipendenti", cui si è più volte fatto cenno *supra* nell'affrontare i diversi istituti (per tutti, la disciplina delle "notifiche" di *data breach*). Occorre quindi principiare dal richiamo all'art. 51, a norma del quale ogni Stato membro deve disporre che "***una o più** autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento*". Sicchè un primo dato da tener presente: il compito di tutelare (all'interno dei singoli Stati) i diritti e le libertà previsti dal GDPR potrà essere affidato a più di una autorità di controllo. In tal caso, tra queste dovrà essere individuata quella chiamata a rivestire il ruolo di autorità "**capofila**" e, dunque, a fungere da "*punto di contatto unico per l'effettiva partecipazione di tutte*" al c.d. "**meccanismo di coerenza**" previsto dall'art. 63. Quest'ultimo si traduce (*de facto*) in un generale principio di reciproca cooperazione cui deve informarsi l'operato delle autorità dei vari Stati membri al fine di contribuire all'applicazione coerente del Regolamento in tutta l'Unione. Il Regolamento si premura poi di indicare i principi di suddivisione delle competenze tra le varie autorità di controllo eventualmente esistenti in un singolo Paese (si vedano sul punto gli artt. 55, 56, 60 e ss.).

Tralasciando qui ogni analisi dei requisiti tecnici richiesti ai membri delle autorità di controllo, nonché i loro criteri di nomina, ci si soffermerà invece, da ultimo, sui tipi di poteri riconosciuti alle autorità per l'espletazione dei propri compiti[28].

A norma dell'art. 58, i poteri attribuiti alle autorità di controllo possono infatti ricondursi a tre distinte macro-categorie:

- "**poteri di indagine**";

[27] Cfr. *infra* par. 8

[28] L'art. 57 elenca in maniera analitica i compiti assegnati alle autorità di controllo, che, tuttavia, possono essere generalmente ricondotti al dovere di sorvegliare ed assicurare l'applicazione del GDPR, promuovendo la consapevolezza di titolari e responsabili con riguardo alle responsabilità loro proprie.

- "**poteri correttivi**"[29];
- "**poteri autorizzativi e consultivi**".

Per quel che ora maggiormente interessa, sia sufficiente ricordare che ad ogni autorità di controllo sono riconosciuti i seguenti "poteri di indagine":

a) **ingiungere** al titolare, al responsabile del trattamento e, ove applicabile, al loro rappresentante, **di fornirle ogni informazione di cui necessiti** per l'esecuzione dei suoi compiti;

b) **condurre indagini** sotto forma di attività di revisione sulla protezione dei dati;

c) effettuare un riesame delle certificazioni rilasciate in conformità all'articolo 42, co. 7;

d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;

e) **ottenere**, dal titolare o dal responsabile del trattamento, **l'accesso a tutti i dati personali e a tutte le informazioni necessarie** per l'esecuzione dei suoi compiti;

f) **ottenere accesso a tutti i locali** del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, **in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri**[30].

Opportuno precisare ancora che l'esercizio di tali poteri è comunque soggetto a "*garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo*" (art. 58, co. 4). In ossequio a tali principi, vengono previsti anche (agli artt. 77 e 78) il "*diritto di proporre reclamo all'autorità di controllo*" ed il "*diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo*". Si è inoltre stabilito che ogni Stato dovrà prevedere che l'autorità di controllo abbia per legge il potere di "*intentare un'azione o di agire in sede giudiziale o, ove del casso, stragiudiziale per la violazione del presente regolamento*". Infine, si segnala che ad ogni Paese viene rimessa la facoltà di riconoscere alla/e propria/e autorità di controllo **poteri ulteriori** rispetto a quelli già previsti dal Regolamento.

Per concludere, si pone in evidenza che il "Gruppo di lavoro per la protezione dei dati" (già istituito ai sensi dell'art. 29 della Direttiva n. 49 del 1995)[31] sta gradualmente

[29] Tra questi si rinvengono, ad esempio, quello di rivolgere ammonimenti a titolare e responsabile che abbiano violato il Regolamento, nonché quello di ingiungere al titolare di comunicare all'interessato una violazione (*data breach*) che abbia interessato i suoi dati personali.

[30] Ai singoli legislatori nazionali spetterà dunque il compito di apprestare i necessari coordinamenti con le normative nazionali, affinché venga garantito il rispetto dei principi fondamentali (specie processuali) di ciascun ordinamento.

[31] Alla luce della espressa abrogazione della Direttiva 49/95, tale Gruppo di lavoro è destinato ad essere sostituito dal "**Comitato europeo per la protezione dei dati**" introdotto dagli artt. 68 e seguenti della nuova normativa. Al "Comitato" è rimesso il compito di garantire un'applicazione coerente del Regolamento anche mediante la pubblicazione di "*linee guida, raccomandazioni e migliori prassi*" *ex* art. 70.

elaborando una serie di *guide lines* esplicative del GDPR che potranno fungere da primo momento di riferimento in sede di applicazione della nuova normativa europea.