GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

17/IT

WP 253

Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679

Adottate il 3 ottobre 2017

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL

TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 di detta direttiva,

visto il proprio regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Indice:

I. Introduzione

L'UE ha attuato una riforma globale della normativa sulla protezione dei dati in Europa. La riforma si basa su diversi pilastri (componenti fondamentali): norme coerenti, procedure semplificate, azioni coordinate, coinvolgimento degli utenti, informazioni più efficaci e rafforzamento dei poteri destinati a far rispettare le norme.

I titolari del trattamento e i responsabili del trattamento[1] hanno maggiori responsabilità nel garantire l'efficace tutela dei dati personali delle persone fisiche. Le autorità di controllo sono dotate di poteri per garantire che i principi del regolamento generale sulla protezione dei dati (di seguito "il regolamento") e i diritti delle persone interessate siano rispettati conformemente all'enunciato e alla ratio del regolamento.

L'applicazione coerente delle norme sulla protezione dei dati è fondamentale per un regime di protezione dei dati armonizzato. Le sanzioni amministrative pecuniarie rappresentano un elemento centrale del nuovo regime introdotto dal regolamento per far rispettare le norme, in quanto costituiscono un componente importante dell'insieme di strumenti di applicazione a disposizione delle autorità di controllo, congiuntamente alle altre misure previste dall'articolo 58.

Il presente documento è destinato a essere utilizzato dalle autorità di controllo per garantire una migliore applicazione e attuazione del regolamento ed espone l'interpretazione comune delle disposizioni di cui all'articolo 83 del regolamento nonché l'interazione di detto articolo con gli articoli 58 e 70 e i relativi considerando.

In particolare, ai sensi dell'articolo 70, paragrafo 1, lettera e), il comitato europeo per la protezione dei dati ha la facoltà di pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del regolamento, e l'articolo 70, paragrafo 1, lettera k), specifica che è prevista l'elaborazione di linee guida riguardanti la previsione di sanzioni amministrative pecuniarie.

Le presenti linee guida non sono esaustive e non forniscono spiegazioni in merito alle differenze esistenti tra sistemi amministrativi, civili o penali nell'imposizione di sanzioni amministrative in generale.

Al fine di adottare un approccio coerente all'imposizione di sanzioni amministrative pecuniarie, che rispecchi adeguatamente tutti i principi delle presenti linee guida, il comitato europeo per la protezione dei dati ha raggiunto un'intesa comune sui criteri di valutazione di cui all'articolo 83, paragrafo 2, del regolamento e, pertanto, il comitato e le singole autorità di controllo concordano sull'impiego delle presenti linee guida come approccio comune.

[1] NdT: La versione italiana del regolamento (UE) 2016/679 ha modificato alcuni termini della direttiva 95/46/CE (abrogata dal regolamento stesso). Per coerenza terminologica, questo testo riprende sempre la terminologia del regolamento. Pertanto "controller" è il "titolare del trattamento" ("responsabile del trattamento" nella direttiva) e "processor" è il "responsabile del trattamento" ("incaricato del trattamento" nella direttiva).

II. Principi

Una volta accertata la violazione del regolamento dopo aver valutato i fatti del caso, l'autorità di controllo competente deve individuare la o le misure correttive più appropriate per affrontare tale violazione. Le disposizioni di cui all'articolo 58, paragrafo 2, lettere da b) a j)[2], indicano gli strumenti che le autorità di controllo hanno a disposizione per far fronte a un'inadempienza da parte di un titolare del trattamento o responsabile del trattamento. Nel ricorrere a tali poteri, le autorità di controllo devono osservare i seguenti principi:

1. La violazione del regolamento dovrebbe comportare l'imposizione di "sanzioni equivalenti".

Il concetto di "equivalenza" è fondamentale nel determinare la portata degli obblighi delle autorità di controllo di garantire coerenza nel ricorso ai poteri correttivi di cui all'articolo 58, paragrafo 2, in generale e nell'applicazione delle sanzioni amministrative in particolare[3].

Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, ***il livello di protezione dovrebbe essere equivalente*** *in tutti gli Stati membri* (considerando 10). Il considerando 11 spiega che per garantire un livello equivalente di protezione dei dati personali in tutta l'Unione occorrono, tra l'altro, "*poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri*". Inoltre, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri sono considerate un modo per "*prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno*", in linea con il considerando 13 del regolamento.

Il regolamento offre una base più solida rispetto alla direttiva 95/46/CE ai fini di una maggiore coerenza, in quanto esso è direttamente applicabile negli Stati membri. Anche se le autorità di controllo agiscono in "piena indipendenza" (articolo 52) nei confronti dei governi nazionali, dei titolari del trattamento o dei responsabili del trattamento, esse devono collaborare "*al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento*" (articolo 57, paragrafo 1, lettera g)).

Il regolamento esorta a una maggiore coerenza rispetto alla direttiva 95/46/CE nell'imposizione delle sanzioni. Nei casi transfrontalieri, la coerenza deve essere garantita principalmente mediante il meccanismo di cooperazione (sportello unico) e in una certa misura tramite il meccanismo di coerenza introdotto dal nuovo regolamento.

Nei casi nazionali previsti dal regolamento, le autorità di controllo applicheranno le presenti linee guida nello spirito di collaborazione ai sensi dell'articolo 57, paragrafo 1, lettera g), e dell'articolo 63, al fine di garantire la coerenza dell'applicazione e dell'attuazione del regolamento. Sebbene continuino a essere indipendenti nello scegliere le misure correttive di cui all'articolo 58, paragrafo 2, le autorità di controllo dovrebbero evitare di scegliere misure correttive differenti in casi analoghi.

---

[2] L'articolo 58, paragrafo 2, stabilisce che è possibile rivolgere avvertimenti quando "i trattamenti previsti possono verosimilmente violare le disposizioni del regolamento". In altre parole, nel caso contemplato dalla disposizione, la violazione del regolamento non è ancora avvenuta.

[3] Anche quando i sistemi giuridici di alcuni paesi dell'UE non consentono l'irrogazione di sanzioni amministrative pecuniarie come previsto dal regolamento, l'applicazione di tali norme in detti Stati membri deve avere effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo (considerando 151). Le autorità giurisdizionali sono vincolate dal regolamento ma non sono vincolate dalle presenti linee guida del comitato europeo per la protezione dei dati.

Lo stesso principio si applica quando tali misure correttive sono imposte sotto forma di sanzioni pecuniarie.

2. Come tutte le misure correttive scelte dalle autorità di controllo, le sanzioni amministrative pecuniarie dovrebbero essere "effettive, proporzionate e dissuasive".

Come tutte le misure correttive in generale, le sanzioni amministrative pecuniarie dovrebbero rispondere adeguatamente alla natura, alla gravità e alle conseguenze della violazione, e le autorità di controllo devono valutare tutte le circostanze del caso in maniera coerente e oggettivamente giustificata. La valutazione di quanto sia effettivo, proporzionato e dissuasivo in ciascun caso dovrà anche riflettere l'obiettivo perseguito dalla misura correttiva prescelta, che è quello di ripristinare la conformità alle norme oppure di punire un comportamento illecito (o entrambi).

Le autorità di controllo dovrebbero individuare misure correttive che siano "*effettive, proporzionate e dissuasive*" (articolo 83, paragrafo 1), sia nei casi nazionali (articolo 55) che nei casi che comportano il trattamento transfrontaliero dei dati (secondo la definizione di cui all'articolo 4, punto 23).

Le presenti linee guida riconoscono che la legislazione nazionale può stabilire requisiti aggiuntivi per la procedura che le autorità di controllo devono seguire per far rispettare le norme. Essi possono consistere ad esempio in notifiche di indirizzo, moduli, termini per presentare osservazioni, appello, esecuzione, pagamento[4].

Tali requisiti non dovrebbero tuttavia ostacolare in pratica il conseguimento degli obiettivi di efficacia, proporzionalità e dissuasività.

Una determinazione più precisa dell'efficacia, della proporzionalità e della dissuasività scaturirà dalla pratica che emergerà in seno alle autorità di controllo (in materia di protezione dei dati e grazie alle esperienze acquisite in altri settori normativi) e dalla giurisprudenza relativa all'interpretazione di tali principi.

Al fine di irrogare sanzioni amministrative che siano effettive, proporzionate e dissuasive, l'autorità di controllo deve rifarsi alla definizione della nozione di impresa fornita dalla Corte di giustizia dell'Unione europea (CGUE) ai fini dell'applicazione degli articoli 101 e 102 TFUE, secondo cui il concetto di impresa **va inteso come** un'unità economica che può essere composta dall'impresa madre e da tutte le filiali coinvolte. Conformemente al diritto e alla giurisprudenza dell'UE[5], un'impresa deve essere intesa quale unità economica che intraprende attività economiche/commerciali, a prescindere dalla persona giuridica implicata (considerando 150).

[4] Ad esempio, il quadro costituzionale e la proposta legislativa in materia di protezione dei dati dell'Irlanda prevedono che, prima di valutare la portata della o delle sanzioni, si giunga a una decisione formale in merito alla violazione stessa e la si comunichi alle parti interessate. La decisione sulla violazione non può essere rivista durante la valutazione della portata della o delle sanzioni.

[5] La definizione della giurisprudenza della Corte di giustizia è la seguente: "la nozione di impresa abbraccia qualsiasi entità che esercita un'attività economica, a prescindere dallo status giuridico di detta entità e dalle sue modalità di finanziamento" (causa Höfner e Elsner, punto 21, ECLI:EU:C:1991:161). Un'impresa "dev'essere intesa nel senso che essa si riferisce ad un'unità economica, anche qualora, sotto il profilo giuridico, questa unità economica sia costituita da più persone, fisiche o giuridiche" (causa Confederación Española de Empresarios de Estaciones de Servicio, punto 40, ECLI:EU:C:2006:784).

3. L'autorità di controllo competente effettuerà una valutazione "in ogni singolo caso".

È possibile imporre sanzioni amministrative pecuniarie in risposta a una vasta serie di violazioni. L'articolo 83 del regolamento prevede un approccio armonizzato nei confronti delle violazioni di obblighi espressamente elencate nei paragrafi da 4 a 6. Il diritto di uno Stato membro può estendere l'applicazione dell'articolo 83 alle autorità e agli organismi pubblici istituiti in tale Stato membro. Inoltre, il diritto di uno Stato membro può consentire o addirittura imporre l'irrogazione di una sanzione pecuniaria in caso di violazione di disposizioni diverse da quelle citate all'articolo 83, paragrafi da 4 a 6.

Il regolamento stabilisce che ogni caso sia valutato singolarmente[6]. L'articolo 83, paragrafo 2, rappresenta il punto di partenza di tale valutazione individuale. Esso prevede che "*al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi*...". Di conseguenza, e alla luce del considerando 148[7], l'autorità di controllo ha la responsabilità di scegliere la o le misure più appropriate. Nei casi citati all'articolo 83, paragrafi da 4 a 6, tale scelta **deve** tenere conto di tutte le misure correttive, tra cui l'imposizione della sanzione amministrativa pecuniaria appropriata, sia che essa sia associata a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, oppure che sia autonoma.

Le sanzioni pecuniarie rappresentano un importante strumento che le autorità di controllo dovrebbero utilizzare nelle opportune circostanze. Le autorità di controllo sono incoraggiate a ricorrere alle misure correttive con un approccio ponderato ed equilibrato, al fine di reagire in maniera effettiva, dissuasiva e proporzionata alla violazione. Il punto non è qualificare le sanzioni pecuniarie come misure di ultima istanza, né evitare di irrogarle, bensì utilizzarle in un modo che non ne riduca l'efficacia come strumento.

---

[6] Oltre all'applicazione dei criteri di cui all'articolo 83, esistono altre disposizioni a sostegno di tale approccio quali:

- considerando 141: "*Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico*";
- considerando 129: "*È opportuno che i poteri delle autorità di controllo siano esercitati nel rispetto di garanzie procedurali adeguate previste dal diritto dell'Unione e degli Stati membri, in modo imparziale ed equo ed entro un termine ragionevole. In particolare ogni misura dovrebbe essere appropriata, necessaria e proporzionata al fine di assicurare la conformità al presente regolamento, tenuto conto delle circostanze di ciascun singolo caso..."*;
- articolo 57, paragrafo 1, lettera f): *"tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 8, e svolge le indagini opportune sull'oggetto del reclamo"*.

[7] "*Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del presente regolamento. In caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria. Si dovrebbe prestare tuttavia debita attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo*".

Il comitato europeo per la protezione dei dati, negli ambiti di sua competenza ai sensi dell'articolo 65 del regolamento, adotterà una decisione vincolante sulle controversie tra le autorità, in particolare in merito alla determinazione dell'esistenza di una violazione. Se un'obiezione pertinente e motivata mette in discussione la conformità di una misura correttiva con il regolamento generale sulla protezione dei dati, la decisione del comitato europeo per la protezione dei dati esaminerà anche in che modo la sanzione amministrativa pecuniaria proposta nel progetto di decisione dell'autorità di controllo competente rispetta i principi di efficacia, proporzionalità e deterrenza. Seguiranno separatamente orientamenti del comitato europeo per la protezione dei dati sull'applicazione dell'articolo 65 del regolamento per ulteriori dettagli sul tipo di decisione che il comitato deve adottare.

---

4. Un approccio armonizzato alle sanzioni amministrative pecuniarie in materia di protezione dei dati richiede la partecipazione attiva delle autorità di controllo e lo scambio di informazioni tra le stesse.

Le presenti linee guida riconoscono che per alcune autorità di controllo nazionali i poteri sanzionatori rappresentano una novità nel settore della protezione dei dati e sollevano numerose questioni in termini di risorse, organizzazione e procedura. In particolare, le decisioni in cui le autorità di controllo esercitano i poteri sanzionatori saranno impugnabili dinanzi ai tribunali nazionali.

Le autorità di controllo collaborano tra loro e, ove necessario, con la Commissione europea tramite il meccanismo di cooperazione, come stabilito nel regolamento, al fine di sostenere scambi formali e informali di informazioni, ad esempio attraverso seminari periodici. Tale cooperazione si concentrerà sulla loro esperienza e pratica nell'applicazione dei poteri sanzionatori al fine di raggiungere una maggiore coerenza.

Questa condivisione attiva di informazioni, insieme alla giurisprudenza emergente sul ricorso a tali poteri, potrebbe condurre a una rivisitazione dei principi o dei dettagli particolari delle presenti linee guida.

III. Criteri di valutazione di cui all'articolo 83, paragrafo 2

L'articolo 83, paragrafo 2, contiene un elenco di criteri che le autorità di controllo devono usare per valutare sia l'opportunità di irrogare una sanzione amministrativa che l'importo della sanzione. Ciò non significa che occorre ripetere la valutazione usando gli stessi criteri, bensì che si deve procedere a una valutazione che tenga conto di tutte le circostanze di ogni singolo caso, conformemente all'articolo 83[8].

Le conclusioni raggiunte nella prima fase della valutazione possono essere impiegate nella seconda parte relativa all'importo della sanzione, evitando così di dover eseguire la valutazione utilizzando gli stessi criteri due volte.

La presente sezione fornisce orientamenti alle autorità di controllo su come interpretare le singole circostanze del caso alla luce dei criteri di cui all'articolo 83, paragrafo 2.

a) la natura, la gravità e la durata della violazione

Quasi tutti gli obblighi dei titolari del trattamento e dei responsabili del trattamento previsti dal regolamento sono classificati in base alla loro **natura** nelle disposizioni di cui all'articolo 83, paragrafi da 4 a 6. Il regolamento, fissando due diversi massimali per le sanzioni amministrative pecuniarie (10/20 milioni di EUR), fornisce già un'indicazione del fatto che la violazione di alcune disposizioni del regolamento può essere più grave della violazione di altre disposizioni. Tuttavia l'autorità di controllo competente, valutando le circostanze del caso alla luce dei criteri generali di cui all'articolo 83, paragrafo 2, può decidere che in quel particolare caso vi sia una necessità maggiore o minore di reagire con una misura correttiva sotto forma di sanzione pecuniaria. Quando è scelta una sanzione pecuniaria quale misura correttiva appropriata, da sola o in aggiunta ad altre misure, si applicherà il sistema a livelli del regolamento (articolo 83, paragrafi da 4 a 6) per individuare la sanzione massima imponibile a seconda della natura della violazione in questione.

Il considerando 148 introduce la nozione di "violazioni minori". Tali violazioni possono consistere nella violazione di una o più disposizioni del regolamento elencate all'articolo 83, paragrafo 4 o 5. La valutazione dei criteri di cui all'articolo 83, paragrafo 2, può tuttavia spingere l'autorità di controllo a ritenere che nelle circostanze concrete del caso la violazione, ad esempio, non crei un rischio significativo per i diritti degli interessati in questione e non incida sull'essenza dell'obbligo in questione. In tali casi, la sanzione può essere sostituita (ma non sempre) da un ammonimento.

Il considerando 148 non prevede l'obbligo per l'autorità di controllo di sostituire sempre una sanzione con un ammonimento in caso di violazione minore ("*potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria*"), ma piuttosto una possibilità, dopo la valutazione concreta di tutte le circostanze del caso.

Il considerando 148 offre la stessa possibilità di sostituire una sanzione pecuniaria con un ammonimento qualora il titolare del trattamento sia una persona fisica e la sanzione pecuniaria che dovrebbe essere imposta costituisca un onere sproporzionato. L'autorità di controllo deve innanzitutto decidere, valutando le circostanze del caso, in merito alla necessità di irrogare una sanzione. Qualora sia favorevole a imporre una sanzione pecuniaria, l'autorità di controllo deve altresì valutare se la sanzione che dovrebbe essere imposta costituisca un onere sproporzionato per una persona fisica.

Il regolamento non fissa un importo specifico per violazioni specifiche, ma solo un massimale. Da ciò si può desumere la gravità relativamente minore delle violazioni di cui all'articolo 83, paragrafo 4,

[8] In alcuni paesi, in applicazione delle norme procedurali nazionali derivanti dai requisiti costituzionali, la valutazione della sanzione da infliggere può avvenire separatamente, in un momento successivo alla valutazione dell'esistenza della violazione. Ciò può limitare il contenuto e la quantità di dettagli di un progetto di decisione presentato dall'autorità di controllo capofila di tali paesi.

rispetto a quelle di cui all'articolo 83, paragrafo 5. La reazione effettiva, proporzionata e dissuasiva a una violazione dell'articolo 83, paragrafo 5, dipenderà tuttavia dalle circostanze del caso.

Occorre notare che, in determinate circostanze, le violazioni del regolamento che per natura dovrebbero rientrare nella categoria *"fino a 10 000 000 EUR o […] fino al 2 % del fatturato mondiale totale annuo"* conformemente all'articolo 83, paragrafo 4, potrebbero essere classificate in una categoria superiore (20 milioni di EUR). È il caso, ad esempio, di una violazione che sia stata precedentemente oggetto di un ordine[9] dell'autorità di controllo che il titolare o il responsabile del trattamento non ha rispettato[10] (articolo 83, paragrafo 6). Le disposizioni del diritto nazionale possono nella pratica ripercuotersi sulla valutazione[11]. La natura della violazione e "*l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito*" forniranno un'indicazione della **gravità** della violazione. Qualora nell'ambito di un singolo caso siano state commesse congiuntamente più violazioni diverse, l'autorità di controllo può applicare le sanzioni amministrative pecuniarie a un livello che risulti effettivo, proporzionato e dissuasivo entro i limiti della violazione più grave. Ad esempio, qualora siano stati violati l'articolo 8 e l'articolo 12, l'autorità di controllo può applicare le misure correttive di cui all'articolo 83, paragrafo 5, che corrispondono alla categoria della violazione più grave, ossia quella dell'articolo 12. Precisare ulteriori dettagli in questa fase esula dall'ambito delle presenti linee guida (un calcolo più dettagliato costituirebbe l'oggetto di un'eventuale fase successiva delle presenti linee guida).

I fattori presentati di seguito devono essere valutati combinatamente, ad esempio il numero di interessati va valutato in combinazione con le possibili ripercussioni nei loro confronti.

Occorre valutare **il numero** di interessati coinvolti, al fine di stabilire se si tratta di un evento isolato oppure del sintomo di una violazione sistemica oppure dell'assenza di prassi adeguate. Ciò non vuol dire che gli eventi isolati non debbano essere punibili, in quanto un evento isolato potrebbe pur sempre ripercuotersi su molti interessati. A seconda delle circostanze del caso, ciò dipenderà, ad esempio, dal numero totale di soggetti registrati nella banca dati in questione, dal numero di utenti di un servizio, dal numero di clienti, oppure dalla popolazione del paese, ove opportuno.

---

[9] Gli ordini, di cui all'articolo 58, paragrafo 2, sono i seguenti:

- ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal regolamento;
- ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
- ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
- imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
- 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;
- 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;
- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

[10] L'applicazione dell'articolo 83, paragrafo 6, deve necessariamente tenere conto del diritto procedurale nazionale. Il diritto nazionale determina le modalità di emissione e di notifica di un ordine, il momento di entrata in vigore e l'eventuale periodo di tolleranza per conformarvisi. In particolare, occorre tenere conto dell'effetto di un appello sull'esecuzione di un ordine.

[11] Le disposizioni di legge che pongono limitazioni potrebbero far sì che un ordine precedente dell'autorità di controllo non possa più essere preso in considerazione dopo un determinato periodo dalla sua emissione. Le norme di alcune giurisdizioni prevedono che al termine del periodo di prescrizione di un ordine non possa essere imposta alcuna sanzione pecuniaria per l'inosservanza di tale ordine a norma dell'articolo 83, paragrafo 6. Spetta all'autorità di controllo di ciascuna giurisdizione determinare le ripercussioni di tali impatti.

Occorre altresì valutare **la finalità** del trattamento. Il parere del Gruppo di lavoro sulla "limitazione delle finalità"[12] ha analizzato i due elementi fondamentali di tale principio della normativa sulla protezione dei dati: indicazione specifica della finalità e utilizzo compatibile. Nel valutare la finalità del trattamento nel contesto dell'articolo 83, paragrafo 2, le autorità di controllo dovrebbero valutare la misura in cui il trattamento rispetta i due elementi fondamentali del suddetto principio[13]. In alcuni casi, l'autorità di controllo potrebbe ritenere necessario inserire un'analisi più approfondita della finalità del trattamento stesso nell'analisi dell'articolo 83, paragrafo 2.

Se gli interessati hanno subito un **danno**, occorre considerarne l'entità. Il trattamento dei dati personali può generare rischi per i diritti e le libertà personali, come esposto al considerando 75:

> "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*."

Se dalla violazione del regolamento sono sorti o potrebbero sorgere danni, l'autorità di controllo dovrebbe tenerne conto nella scelta della misura correttiva, sebbene non abbia la facoltà di corrispondere il risarcimento specifico del danno.

L'irrogazione di una sanzione pecuniaria non dipende dalla capacità dell'autorità di controllo di stabilire un nesso causale tra la violazione e il danno materiale (si veda ad esempio l'articolo 83, paragrafo 6).

La durata dell'infrazione può fornire un'indicazione, ad esempio, dei seguenti elementi:

a) condotta intenzionale da parte del titolare del trattamento, oppure

b) mancata adozione di misure preventive appropriate, oppure

c) incapacità di attuare le misure tecniche e organizzative richieste.

b) il carattere doloso o colposo della violazione

In generale, il "dolo" comprende sia la consapevolezza che l'intenzionalità in relazione alle caratteristiche di un reato, mentre per "colposo" si intende che non vi era l'intenzione di causare la

[12] WP 203, parere 03/2013 sulla limitazione delle finalità, disponibile (in inglese) al seguente indirizzo: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[13] Vedasi anche WP 217, parere 6/2014 sul concetto di legittimo interesse del titolare del trattamento ai sensi dell'articolo 7, pagina 24, sulla questione: "Cosa rende un interesse "legittimo" o "illegittimo"?"

violazione nonostante il titolare/responsabile del trattamento abbia violato l'obbligo di diligenza previsto per legge.

È generalmente riconosciuto che le violazioni dolose, da cui emerge il disprezzo per le disposizioni di legge, sono più gravi di quelle colpose e pertanto possono verosimilmente giustificare l'applicazione di una sanzione amministrativa pecuniaria. Le conclusioni circa il dolo o la colpa dipenderanno dagli elementi oggettivi di condotta rilevati dalle circostanze del caso. Inoltre, la giurisprudenza emergente e la pratica in materia di protezione dei dati nell'ambito dell'applicazione del regolamento chiariranno le circostanze fornendo linee di demarcazione più chiare per valutare il carattere doloso di una violazione.

Tra le circostanze indicanti il carattere doloso di una violazione figura il trattamento illecito autorizzato esplicitamente dall'alta dirigenza del titolare del trattamento oppure effettuato nonostante i pareri del responsabile della protezione dei dati o ignorando le politiche esistenti, ad esempio ottenendo e trattando dati relativi ai dipendenti di un concorrente con l'intento di screditare tale concorrente sul mercato.

Altri esempi sono:

- modifica di dati personali per dare un'impressione fuorviante (positiva) circa il conseguimento degli obiettivi – episodio riscontrato nel contesto degli obiettivi relativi ai tempi d'attesa ospedalieri;
- scambio di dati personali con finalità di marketing, ossia vendita di dati come "approvati" senza verificare/ignorando il parere degli interessati circa le modalità di utilizzo dei propri dati.

Altre circostanze, quali mancata lettura e non rispetto delle politiche esistenti, errore umano, mancata verifica dei dati personali nelle informazioni pubblicate, incapacità di apportare aggiornamenti tecnici in maniera puntuale, mancata adozione delle politiche (piuttosto che la semplice mancata applicazione) possono essere sintomo di negligenza.

Le imprese dovrebbero essere responsabili dell'adozione di strutture e risorse idonee alla natura e alla complessità della propria attività. Pertanto, i titolari del trattamento e i responsabili del trattamento non possono legittimare violazioni della normativa sulla protezione dei dati appellandosi a una carenza di risorse. Le prassi e la documentazione delle attività di trattamento seguono un approccio basato sul rischio ai sensi del regolamento.

Esistono zone grigie che influenzano il processo decisionale circa la necessità di imporre o meno una misura correttiva e l'autorità potrebbe dover condurre indagini più approfondite per accertare le circostanze del caso e per garantire che tutte le circostanze specifiche di ciascun caso siano state adeguatamente considerate.

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

I titolari del trattamento e i responsabili del trattamento hanno l'obbligo di attuare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, di condurre valutazioni di impatto sulla protezione dei dati e di mitigare i rischi arrecati ai diritti e alle libertà personali dal trattamento dei dati personali. Tuttavia, quando si verifica una violazione e l'interessato ne subisce i danni, la parte responsabile dovrebbe fare quanto in suo potere per ridurre le conseguenze della violazione per il o i soggetti coinvolti. Tale comportamento responsabile (o la sua assenza) sarà preso in considerazione dall'autorità di controllo nella scelta della o delle misure correttive e nel calcolo della sanzione da imporre nel caso specifico.

Sebbene i fattori attenuanti o aggravanti siano particolarmente utili per adeguare l'importo della sanzione amministrativa pecuniaria alle particolari circostanze del caso, il loro ruolo nella scelta della misura correttiva appropriata non dovrebbe essere sottovalutato. Nei casi in cui la valutazione fondata su altri criteri lascia l'autorità di controllo nel dubbio circa l'appropriatezza di una sanzione amministrativa pecuniaria, come misura correttiva a sé stante oppure in combinazione con altre misure di cui all'articolo 58, le circostanze aggravanti o attenuanti possono aiutare a scegliere le misure appropriate spostando l'ago della bilancia in favore di quella che sembra essere la misura più effettiva, proporzionata e dissuasiva nel caso in questione.

Tale disposizione serve per valutare il grado di responsabilità del titolare del trattamento in seguito al verificarsi di una violazione. Può riguardare casi in cui è indubbio che il titolare/responsabile del trattamento non ha adottato un approccio imprudente/negligente e ha fatto quanto in suo potere per correggere le proprie azioni quando si è reso conto della violazione.

In passato, l'esperienza disciplinare delle autorità di controllo nell'ambito della direttiva 95/46/CE ha dimostrato che può essere opportuno mostrare un certo livello di flessibilità nei confronti di quei titolari/responsabili del trattamento che hanno ammesso la violazione e che si sono assunti la responsabilità di correggere o limitare l'impatto delle loro azioni. Alcuni esempi potrebbero essere i seguenti (anche se non porterebbero in tutti i casi a un approccio più flessibile):

- aver contattato altri titolari/responsabili del trattamento che potrebbero essere stati coinvolti in un'estensione del trattamento, ad esempio nel caso in cui alcuni dati sono stati erroneamente condivisi con terze parti;
- azione tempestiva adottata dal titolare/responsabile del trattamento per impedire la prosecuzione o l'espansione della violazione a un livello o a una fase che avrebbe determinato ripercussioni ben più gravi.

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

Il regolamento ha introdotto un livello ben superiore di responsabilità del titolare del trattamento rispetto alla direttiva 95/46/CE sulla protezione dei dati.

Il grado di responsabilità del titolare del trattamento o del responsabile del trattamento valutato sulla base dell'adozione di una misura correttiva appropriata può dipendere dai seguenti aspetti:

- Il titolare del trattamento ha attuato misure tecniche che seguono i principi della protezione dei dati fin dalla progettazione o per impostazione predefinita (articolo 25)?
- Il titolare del trattamento ha attuato misure organizzative che attuano i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (articolo 25) a tutti i livelli dell'organizzazione?
- Il titolare/responsabile del trattamento ha messo in atto un livello di sicurezza adeguato (articolo 32)?
- Le prassi/politiche pertinenti in materia di protezione dei dati sono conosciute e applicate al livello adeguato di gestione dell'organizzazione? (articolo 24).

L'articolo 25 e l'articolo 32 del regolamento prevedono che i titolari del trattamento tengano 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*". Anziché imporre un obbligo di risultato, tali disposizioni introducono obblighi di mezzi, il che significa che il titolare del trattamento deve condurre le valutazioni necessarie e giungere alle opportune conclusioni. La domanda cui l'autorità di controllo deve quindi rispondere è la seguente: in che misura il titolare del trattamento ha fatto quanto ci si aspettava facesse, considerando la natura, le finalità o l'entità del trattamento, alla luce degli obblighi imposti dal regolamento?

In tale valutazione, occorre tenere in debita considerazione qualsiasi procedura e metodo basati sulle migliori prassi, ove esistano e siano applicate. È importante tenere conto delle norme industriali e dei codici di condotta nel rispettivo campo o professione. I codici di condotta potrebbero fornire un'indicazione delle pratiche comuni nel settore e un'indicazione del livello di conoscenza dei diversi mezzi esistenti per affrontare le tipiche problematiche di sicurezza associate al trattamento.

Anche se le migliori prassi dovrebbero rappresentare l'ideale da perseguire in generale, nel valutare il grado di responsabilità occorre considerare le circostanze specifiche del singolo caso.

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

Tale criterio serve per valutare i precedenti dell'entità che commette la violazione. Le autorità di controllo dovrebbero considerare che la valutazione può avere una portata piuttosto vasta poiché ogni tipo di violazione del regolamento, seppur di natura diversa da quella esaminata dall'autorità di controllo, potrebbe essere pertinente ai fini della valutazione, in quanto potrebbe fornire indicazioni su un livello generale di conoscenza insufficiente o di indifferenza nei confronti delle norme sulla protezione dei dati.

L'autorità di controllo dovrebbe valutare quanto segue:

- Il titolare/responsabile del trattamento ha già commesso la stessa violazione in precedenza?
- Il titolare/responsabile del trattamento ha commesso una violazione del regolamento secondo le stesse modalità? (ad esempio a causa di una conoscenza insufficiente delle prassi esistenti nell'organizzazione, oppure in seguito a una valutazione del rischio inadeguata, non rispondendo alle richieste dell'interessato in maniera tempestiva o per un ritardo ingiustificato nel rispondere alle richieste, ecc.).

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

L'articolo 83, paragrafo 2, prevede che il grado di cooperazione debba essere tenuto in "debito conto" al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa. Il regolamento non indica con precisione come tenere conto degli sforzi dei titolari del trattamento o dei responsabili del trattamento nel rimediare a una violazione già accertata dall'autorità di controllo. Inoltre, è chiaro che i criteri saranno solitamente applicati nel calcolo dell'importo della sanzione pecuniaria da imporre.

Tuttavia, nello scegliere la misura correttiva proporzionata al singolo caso si dovrebbe tener conto anche dell'eventuale l'intervento con cui il titolare del trattamento abbia limitato o addirittura azzerato le ripercussioni negative sui diritti delle persone che si sarebbero altrimenti verificate.

Un caso in cui la collaborazione con l'autorità di controllo potrebbe essere presa in debita considerazione è il seguente:

- L'entità ha risposto in modo particolare alle richieste dell'autorità di controllo durante la fase di indagine nel caso specifico limitando in tal modo in maniera significativa le ripercussioni sulle persone?

Detto ciò, non sarebbe opportuno tenere ulteriormente conto della collaborazione già prevista per legge: ad esempio, l'entità è in ogni caso tenuta a consentire all'autorità di controllo di accedere ai locali per controlli/ispezioni.

g) le categorie di dati personali interessate dalla violazione;

Alcuni esempi di domande chiave a cui l'autorità di controllo potrebbe ritenere necessario rispondere, ove opportuno, sono i seguenti:

- La violazione riguarda il trattamento di categorie particolari di dati di cui agli articoli 9 e 10 del regolamento?
- I dati sono direttamente/indirettamente identificabili?
- Il trattamento riguarda dati la cui diffusione causerebbe immediati danni/disagi alla persona (che non rientrano nelle categorie di cui agli articoli 9 e 10)?

- I dati sono direttamente disponibili senza protezioni tecniche oppure sono criptati[14]?

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

L'autorità di controllo potrebbe venire a conoscenza della violazione in seguito a indagini, reclami, articoli di giornale, suggerimenti anonimi oppure notifiche da parte del titolare del trattamento. Il titolare del trattamento ha l'obbligo a norma del regolamento di notificare all'autorità di controllo eventuali violazioni dei dati personali. Qualora il titolare del trattamento si limiti ad adempiere a tale obbligo, la conformità ad esso non può essere interpretata come fattore attenuante/mitigante. Analogamente, qualora il titolare/responsabile del trattamento abbia agito incautamente senza notificare la violazione, o perlomeno senza notificarne tutti i dettagli, in quanto non in grado di valutarne adeguatamente la portata, l'autorità di controllo potrebbe ritenere necessaria l'imposizione di una sanzione più grave, il che significa che risulterà improbabile la classificazione quale violazione minore.

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

Il titolare del trattamento o il responsabile del trattamento potrebbe già essere nel mirino dell'autorità di controllo per la verifica della conformità in seguito a una precedente violazione. In tal caso gli eventuali precedenti contatti con il responsabile della protezione dei dati saranno stati verosimilmente numerosi e l'autorità di controllo li terrà in considerazione.

A differenza dei criteri di cui alla lettera e), questo criterio di valutazione serve solo per ricordare alle autorità di controllo di fare riferimento alle misure precedentemente emesse nei confronti del medesimo titolare o responsabile del trattamento "*relativamente allo stesso oggetto*".

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;

Le autorità di controllo hanno il dovere di *"sorveglia[re] e assicura[re] l'applicazione del […] regolamento"* (articolo 57, paragrafo 1, lettera a)). L'adesione ai codici di condotta approvati può essere utilizzata dal titolare del trattamento o dal responsabile del trattamento per dimostrare la conformità, ai sensi dell'articolo 24, paragrafo 3, dell'articolo 28, paragrafo 5, o dell'articolo 32, paragrafo 3.

In caso di violazione di una delle disposizioni del regolamento, l'adesione a un codice di condotta approvato può fornire indicazioni circa la portata della necessità di intervenire con una sanzione amministrativa pecuniaria effettiva, proporzionata, dissuasiva o altra misura correttiva da parte dell'autorità di controllo. I codici di condotta approvati conterranno, ai sensi dell'articolo 40, paragrafo 4, "*i meccanismi che consentono all'organismo (di controllo) di effettuare il controllo obbligatorio del rispetto delle norme del codice*".

Qualora il titolare del trattamento o il responsabile del trattamento abbia aderito a un codice di condotta approvato, l'autorità di controllo potrebbe ritenere sufficiente che la comunità incaricata di gestire il codice intervenga adeguatamente in prima persona nei confronti del proprio membro, ad esempio tramite i regimi di monitoraggio e applicazione del codice di condotta stesso. Pertanto, l'autorità di controllo potrebbe ritenere che tali misure siano sufficientemente effettive, proporzionate

[14] Il fatto che la violazione riguardi solo dati indirettamente identificabili oppure pseudonimi/dati criptati non dovrebbe essere sempre considerato un fattore attenuante supplementare. Per tali violazioni una valutazione complessiva degli altri criteri potrebbe offrire una moderata o netta indicazione circa l'opportunità di imporre una sanzione amministrativa.

e dissuasive in quel particolare caso senza che l'autorità di controllo stessa debba imporre misure aggiuntive. Alcune forme di sanzionamento dei comportamenti non conformi possono avvenire tramite il regime di monitoraggio, ai sensi dell'articolo 41, paragrafo 2, lettera c), e dell'articolo 42, paragrafo 4), compresa la sospensione o l'esclusione del titolare del trattamento o del responsabile del trattamento dalla comunità incaricata di gestire il codice. Ciononostante, i poteri dell'organismo di controllo si espletano "*fatti salvi i compiti e i poteri dell'autorità di controllo competente*", il che significa che l'autorità di controllo non ha l'obbligo di tenere conto delle sanzioni precedentemente imposte relative al regime di autoregolamentazione.

La non conformità con le misure di autoregolamentazione potrebbe altresì rivelare la colpa o il dolo del titolare/responsabile del trattamento.

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

La disposizione stessa fornisce esempi di quali altri elementi potrebbero essere presi in considerazione nel decidere l'appropriatezza di una sanzione amministrativa pecuniaria per una violazione delle disposizioni di cui all'articolo 83, paragrafi da 4 a 6.

Le informazioni relative ai profitti derivanti da una violazione potrebbero risultare particolarmente importanti per le autorità di controllo in quanto il guadagno economico derivante dalla violazione non può essere compensato tramite misure che non abbiano una componente pecuniaria. Pertanto, il fatto che il titolare del trattamento abbia tratto profitto dalla violazione del regolamento può costituire una chiara indicazione della necessità di imporre una sanzione pecuniaria.

IV. Conclusioni

Le riflessioni sugli aspetti esposti nella sezione precedente aiuteranno le autorità di controllo a individuare, tra i fatti pertinenti del caso, i criteri più utili per valutare se sia necessario imporre una sanzione amministrativa pecuniaria appropriata in aggiunta o in sostituzione delle misure di cui all'articolo 58. Tenendo conto del contesto fornito dalla valutazione, l'autorità di controllo individuerà la misura correttiva più effettiva, proporzionata e dissuasiva per far fronte alla violazione.

L'articolo 58 fornisce alcuni orientamenti sulle misure tra cui un'autorità di controllo può scegliere, in quanto le misure correttive di per sé hanno natura diversa e sono destinate principalmente a finalità diverse. Alcune misure di cui all'articolo 58 possono anche essere cumulate, dando così luogo a un intervento che prevede più di una misura correttiva.

Non è sempre necessario integrare la misura con un'altra misura correttiva. Ad esempio, tenuto debito conto di cosa è proporzionato al caso specifico, l'efficacia e la dissuasività dell'intervento dell'autorità di controllo potrebbero essere garantite attraverso la sola sanzione pecuniaria.

In sintesi, le autorità devono ripristinare la conformità tramite tutte le misure correttive che hanno a disposizione. Le autorità di controllo dovranno altresì scegliere il canale più appropriato per portare avanti l'intervento (potendo ricorrere, ad esempio, a sanzioni penali - ove disponibili a livello nazionale).

La pratica di applicare sanzioni amministrative pecuniarie coerentemente all'interno dell'Unione europea è una pratica in via di evoluzione. Le autorità di controllo dovrebbero collaborare costantemente per aumentare tale coerenza, ad esempio tramite regolari scambi durante seminari sul trattamento dei casi o altri eventi che consentano di confrontare i casi a livello sub-nazionale, nazionale e transfrontaliero. Al fine di sostenere questa attività continuativa si raccomanda la creazione di un sottogruppo permanente annesso a una parte pertinente del comitato europeo per la protezione dei dati.