



Stefania Calosso

Avvocato, Cultrice della materia Data Protection Law presso l'Università di Bologna, componente della Rete Giuridica AIAS



Chiara Piccaglia De Eccher

Avvocato penalista, componente della Rete Giuridica AIAS



La tutela dei dati personali a garanzia del “nuovo” whistleblower

Il D.lgs. 10 marzo 2023 n° 24 recepisce in Italia la Direttiva UE 2019/1937, la cosiddetta direttiva *whistleblowing*, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

Preliminarmente, definiamo chi è il soggetto segnalante *whistleblower*, come previsto dagli articoli 1 e 2 del D.lgs. 24/23:

“la persona che segnala, divulga ovvero denuncia all’Autorità giudiziaria o contabile, violazioni di disposizioni normative nazionali o dell’Unione Europea che ledono l’interesse pubblico o l’integrità dell’amministrazione pubblica o dell’ente privato, di cui è venuta a conoscenza in un contesto lavorativo pubblico o privato.”

Lo scopo della “nuova” disciplina è quello di:

- uniformare i diversi Stati europei al fine di tutelare i soggetti segnalanti;
- disciplinare la protezione del *whistleblower*;
- raggiungere una piena equiparazione tra settore pubblico e privato.

La norma è orientata a garantire la **riservatezza** del *whistleblower* e contrastare/prevenire condotte volte alla corruzione o cattiva amministrazione, sia nel settore pubblico sia nel settore privato.

La protezione del soggetto segnalante viene così rafforzata:

- dall’ampliamento dell’ambito soggettivo di riferimento, con l’estensione ai soggetti diversi da chi segnala (il cosiddetto **facilitatore** o le persone menzionate nella segnalazione);
- dai canali di segnalazione richiesti.

Così facendo, si conferma la volontà legislativa di rendere lo strumento della segnalazione l’elemento portante al fine di garantire la legalità e il buon andamento delle amministrazioni/enti e delle imprese private. Le principali novità, così come sintetizzate dalle nuove Linee Guida ANAC del 12 luglio 2023, sono:

- specificazione dell’ambito soggettivo con riferimento agli enti di diritto pubblico e a quelli di diritto privato;
- **ampliamento dei soggetti protetti dalla normativa;**
- estensione dell’ambito oggettivo;
- disciplina di tre canali di segnalazione e delle condizioni per accedervi: interno, esterno, nonché il canale della divulgazione pubblica;
- indicazione di diverse modalità di presentazione delle segnalazioni (forma scritta o orale);
- **disciplina dettagliata degli obblighi di riservatezza e del trattamento dei dati personali ricevuti, gestiti e comunicati da terzi o a terzi;**

- chiarimenti su che cosa si intende per ritorsione e ampliamento della relativa casistica;
- disciplina sulla protezione delle persone segnalanti o che comunicano misure ritorsive offerta sia da ANAC che dall’Autorità giudiziaria e maggiori indicazioni sulla responsabilità del segnalante e sulle scriminanti;
- introduzione di apposite misure di sostegno per il segnalante e il coinvolgimento di enti del terzo settore competenti;
- revisione della disciplina delle sanzioni applicabili da ANAC e l’introduzione da parte dei soggetti privati di sanzioni nel sistema disciplinare adottato ai sensi del D.lgs. 231/2001.

La **riservatezza**, che rappresenta il principio cardine della direttiva UE 2019/1937, postula l’imprescindibile rispetto degli adempimenti prescritti dai legislatori in ambito di privacy e protezione dei dati personali: il Regolamento UE 2016/679, GDPR, e il D.lgs. 196/2003 (il cosiddetto “codice privacy”) sono, infatti, ampiamente richiamati dal D.lgs. 24/2023, tant’è che si può dire che perseguono una tutela reciproca (l’art. 13 D.lgs. 24/2023 sancisce una clausola di generale conformità al Reg. UE 679/2016, GDPR, e al D.lgs. 196/2003).

Sotto questo profilo, infatti:

- non solo l’identità del segnalante, bensì qualsiasi altra informazione che ne consenta l’identificazione, anche indirettamente, non può essere rivelata senza il suo espresso consenso;
- il titolare del trattamento deve predisporre un’autorizzazione *ad hoc* ai sensi degli artt. 29 e 32, par. 4, GDPR, per il personale interno competente a ricevere le segnalazioni e formarlo in tal senso;
- ogni trattamento di dati e informazioni oggetto di segnalazione deve essere effettuato nel pieno rispetto dei principi di liceità, di correttezza e trasparenza, di limitazione delle finalità, di minimizzazione ed esattezza dei dati e di limitazione della loro conservazione (art. 5 GDPR);
- i dati personali non utili al trattamento di una specifica segnalazione non possono essere rac-

colti e, ove accidentalmente raccolti, devono essere immediatamente cancellati; diversamente, possono essere trattati limitatamente a quanto necessario per dar seguito alla segnalazione ed essere conservati solo per il tempo strettamente necessario alla gestione della segnalazione e, comunque, non oltre cinque anni a decorrere dalla data di comunicazione dell’esito finale della procedura di segnalazione medesima (art. 14, c. 1, D.lgs. 24/2023);

- il titolare del trattamento deve individuare, e di conseguenza implementare, misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato rispetto agli specifici rischi derivanti dai trattamenti effettuati (art. 32 GDPR, quali per esempio, strumenti di crittografia che garantiscano la riservatezza dell’identità del segnalante, del segnalato, del contenuto, dei documenti e delle persone comunque menzionate nella segnalazione), anche attraverso lo svolgimento di una valutazione d’impatto sulla protezione dei dati (art. 35 GDPR), nonché disciplinare il rapporto con eventuali fornitori esterni che trattano dati personali per suo conto (i cosiddetti responsabili del trattamento, art. 28 del GDPR).

E ancora, sempre con riferimento all’attività che deve essere svolta dal titolare, quest’ultimo è chiamato:

- al puntuale rispetto del principio di protezione dei dati personali *by design e by default* (art. 25 GDPR);
- ad aggiornare il registro dei trattamenti in base al nuovo trattamento obbligatorio;
- a redigere un’apposita informativa da fornire ai segnalanti prima che procedano alla segnalazione (artt. 12 e 13 GDPR).

In considerazione di quanto sopra occorre, pertanto, nel rispetto delle scadenze dettate dal legislatore (15 luglio 2023 e 17 dicembre 2023), adeguarsi e conformarsi parallelamente al nuovo dettato normativo e ai principi della protezione dei dati personali, al fine di garantire una piena *compliance* a entrambi i corpi normativi.