Reclami e segnalazioni privacy: quali conseguenze per l'organizzazione che viene segnalata?

I DATI RELATIVI AI RECLAMI E ALLE SEGNALAZIONI PRIVACY SONO UN CAMPANELLO D'ALLARME PER ENTI ED IMPRESE: DALL'ENTRATA IN VIGORE DEL GDPR AD INIZIO 2022 SONO CRESCIUTI DEL 40%, PASSANDO DA UN TOTALE DI 2.547 (MAGGIO-SETTEMBRE 2018) A 3.519 (GENNAIO-MARZO 2022). OGNI ANNO, LA MAGGIOR PARTE DEI PROVVEDIMENTI COLLEGIALI DELL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI PRENDE LE MOSSE PROPRIO A SEGUITO DI RECLAMI O SEGNALAZIONI. QUALI CONSEGUENZE PER LE ORGANIZZAZIONI? COME PREVENIRE?

Federico Corti
Ottobre 13, 2022
Scarica PDF dell'articolo

Il GDPR ha innovato profondamente la materia dei diritti delle persone fisiche, prevedendo specifici mezzi di tutela. Il Capo VIII del Regolamento descrive i mezzi di ricorso a disposizione degli interessati, i quali possono agire innanzi all'Autorità amministrativa di controllo (in Italia, il Garante per la protezione dei dati personali), ovvero adire le vie legali innanzi al giudice ordinario.

Soffermandoci sul primo di questi mezzi di tutela, l'articolo 77, par. 1, del GDPR, prevede che "l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione". Una volta ricevuto il reclamo, l'Autorità competente "dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico". Viene quindi avviata una fase istruttoria preliminare, cui segue un eventuale successivo procedimento amministrativo formale che può portare all'adozione dei provvedimenti sanzionatori. In questo processo, l'articolo 77, par. 2, del GDPR, prevede che l'interessato sia posto nelle condizioni di ricevere tutte le informazioni relative allo stato delle indagini e all'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale.

Il Codice Privacy specifica le modalità di proposizione e le tempistiche per la gestione dei reclami da parte dell'Autorità Garante per la protezione dei dati personali: nove mesi dalla data di presentazione per raggiungere una decisione (estendibili, in caso di motivate esigenze istruttorie); tre mesi dalla data di presentazione per informare l'interessato sullo stato del procedimento. Lo stesso Codice, agli articoli 144 e 144-bis (inserito dal cd. "Decreto Capienze", convertito nella L. 205/2021), disciplina anche la segnalazione: ovvero un'ulteriore forma di tutela amministrativa attivabile da soggetti diversi dall'interessato al fine di portare all'attenzione e richiedere l'intervento del Garante in relazione a vicende anche a carattere collettivo e sociale, concernenti possibili violazioni della disciplina sulla protezione dei dati. La segnalazione, a differenza del reclamo, non è un'azione nel proprio diretto interesse, bensì nel più ampio interesse della legalità.

RECLAMI E SEGNALAZIONI RICORRENTI

Con riferimento ai ricorsi proposti all'Autorità nel corso degli ultimi anni, è facile ritrovare alcuni temi ricorrenti:

- Numerosi reclami e segnalazioni hanno ad oggetto la pubblicazione di dati personali (commenti, fotografie, etc.) sui social network, in particolare su Facebook, Instagram e YouTube;
- Le segnalazioni e i reclami in materia di marketing riguardano il cd. telemarketing selvaggio, nonché comunicazioni di natura commerciale via e-mail o sms. Con riguardo all'ambito del telemarketing, in particolare, le segnalazioni portate annualmente all'attenzione del Garante sono migliaia e costituiscono il carico di lavoro prevalente dell'Autorità;
- Molte istanze si riconnettono a trattamenti di dati personali effettuati in ambito lavorativo e, in particolare, una parte significativa dei reclami rivolti all'Autorità in materia di rapporti di lavoro continua a riguardare il persistente utilizzo, da parte del datore di lavoro, di account di posta elettronica aziendale di tipo individualizzato (contenente il nome e/o il cognome della lavoratrice o del lavoratore) anche dopo che il rapporto di lavoro, in forza del quale l'account è stato assegnato, si è interrotto;
- Sempre con riguardo ai trattamenti nel contesto lavorativo, numerosi reclami vengono rivolti nei confronti di amministrazioni, anche locali, e di altri enti, in merito alla pubblicazione sui siti web istituzionali, talvolta anche nella sezione "Amministrazione trasparente", di atti e documenti che contengono dati personali di dipendenti;
- La diffusione di dati sul web, in generale, è uno dei temi che viene spesso portato all'attenzione dell'Autorità Garante. Numerosi reclami e segnalazioni hanno ad oggetto la diffusione, sui siti web di istituti scolastici, di dati personali riguardanti alunni e personale dipendente, in assenza di una base giuridica idonea a giustificare tale diffusione;

- Diversi reclami riguardano la conformità al GDPR, in caso di produzione in giudizio delle informazioni personali;
- Parlando di informazioni connesse a procedimenti giudiziari, buona parte delle doglianze riguarda la reperibilità in rete di informazioni relative a vicende giudiziarie che hanno interessato il reclamante e che, in epoca successiva alla pubblicazione degli articoli indicati, hanno assunto contorni diversi in virtù dell'evoluzione dei relativi procedimenti.

CONSEGUENZE SANZIONATORIE, CONSEGUENZE DI IMMAGINE

Il titolo del paragrafo è auto esplicativo: iniziamo dalle conseguenze sanzionatorie.

Prendendo come riferimento i tre trimestri trascorsi del 2022 e le sanzioni comminate dalla nostra Autorità di controllo, solo il 20% circa dei provvedimenti a carattere sanzionatorio pubblicati, riguarda istruttorie partite da violazioni di dati personali o dalla diretta iniziativa dell'Autorità (nell'ambito del ciclo di controlli definito nel piano semestrale dell'attività ispettiva, di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza).

La stragrande maggioranza delle ordinanze di ingiunzione pubblicate, invece, esordisce così: *"Con reclamo del XX, presentato ai sensi dell'art. 77 del Regolamento, il reclamante [...">, ha lamentato che [...">"* oppure *"Da una segnalazione pervenuta all'Autorità [...'> è emerso che [...">"*. Talvolta il provvedimento si apre citando le numerose doglianze ricevute, portate anche all'attenzione da associazioni di rappresentanza. In casi minori sono altre Autorità a trasmettere note di segnalazione (Polizia di Stato, Questura, Guardia di Finanza).

Le conseguenze sono evidenti: al totale complessivo di sanzioni riscosse hanno contribuito in maniera determinante gli interessati stessi, mediante l'attivazione dei mezzi di tutela sopra esposti. A ciò si devono aggiungere gli effetti negativi, in termini di reputazione ed immagine, derivanti dalla pubblicazione del provvedimento. Sovente, infatti, il Garante decide di applicare la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet istituzionale.

Come prevenire che gli interessati rivolgano lamentele direttamente all'Autorità?

IL CANALE PRIVACY@

Una soluzione realmente efficace (se applicata correttamente) consiste nel mettere a disposizione degli interessati un canale dedicato alle istanze privacy. Tale canale dovrebbe essere costantemente presidiato da personale interno all'organizzazione, debitamente istruito rispetto alle modalità e alle tempistiche per fornire riscontro. Il canale di contatto potrebbe essere il classico **privacy@nomesocietà.it/com**, **assistenzaprivacy@nomesocietà.it/com**, come se si trattasse di un servizio clienti, volto a soddisfare le richieste degli interessati al trattamento dei dati. Chiaramente ciò non esclude che gli stessi possano rivolgersi al Garante, tuttavia una fase di confronto preliminare può favorire la risoluzione della doglianza.

MECCANISMI ADEGUATI E FORMAZIONE PER PREVENIRE

In ogni caso, il titolare dovrebbe essere in grado di gestire adeguatamente anche istanze che pervengono ad altri canali della società. Nelle linee guida 01/2022, il Comitato Europeo per la Protezione dei Dati raccomanda, come best practice, l'introduzione di meccanismi per migliorare le comunicazioni interne fra colleghi, in modo da facilitare l'esercizio dei diritti degli interessati e garantire, in ogni circostanza, un riscontro efficiente alle istanze. È bene quindi che tutto il personale operante all'interno dell'organizzazione, sia adeguatamente formato e consapevole dei rischi in caso di mancato riscontro, di riscontro tardivo, scortese, approssimativo o incompleto. Gli interessati hanno a disposizione un mezzo di tutela potente: essere in grado di prevenire un reclamo o una segnalazione al Garante è sicuramente meglio che trovarsi nella condizione di dover rispondere alla "richiesta di informazioni" da parte dell'Autorità, formulata ai sensi dell'art. 58 del GDPR e degli artt. 157 (Richiesta di informazioni e di esibizione di documenti) e 158 (Accertamenti) del novellato Codice Privacy.

SE NON L'HAI ANCORA FATTO, TI INVITIAMO A CONSULTARE IL CATALOGO DEI NOSTRI CORSI. LA FORMAZIONE È RICHIESTA DAL GDPR E ALLA BASE DI UNA ADEGUATA PREVENZIONE.

Labor Project®
consulenza operativa per l'impresa

Labor Project S.r.l.
Iscrizione Ufficio Registro Imprese
di Como con n. 02725120139
Cap. Soc. € 100.000 i.v.
P.I. 02725120139

CANTU'
Via Brianza, 65
22063 Cantù (CO)
Tel. +39 031 704381
info@laborproject.it

ROMA
Via Lima, 7
00198 Roma (RM)
roma@laborproject.it

MILANO
Viale Monza, 347
20126 Milano (MI)
milano@laborproject.it

LUGANO
Via Luigi Canonica,11
6900 Lugano (Svizzera)
info@privacydesk.ch