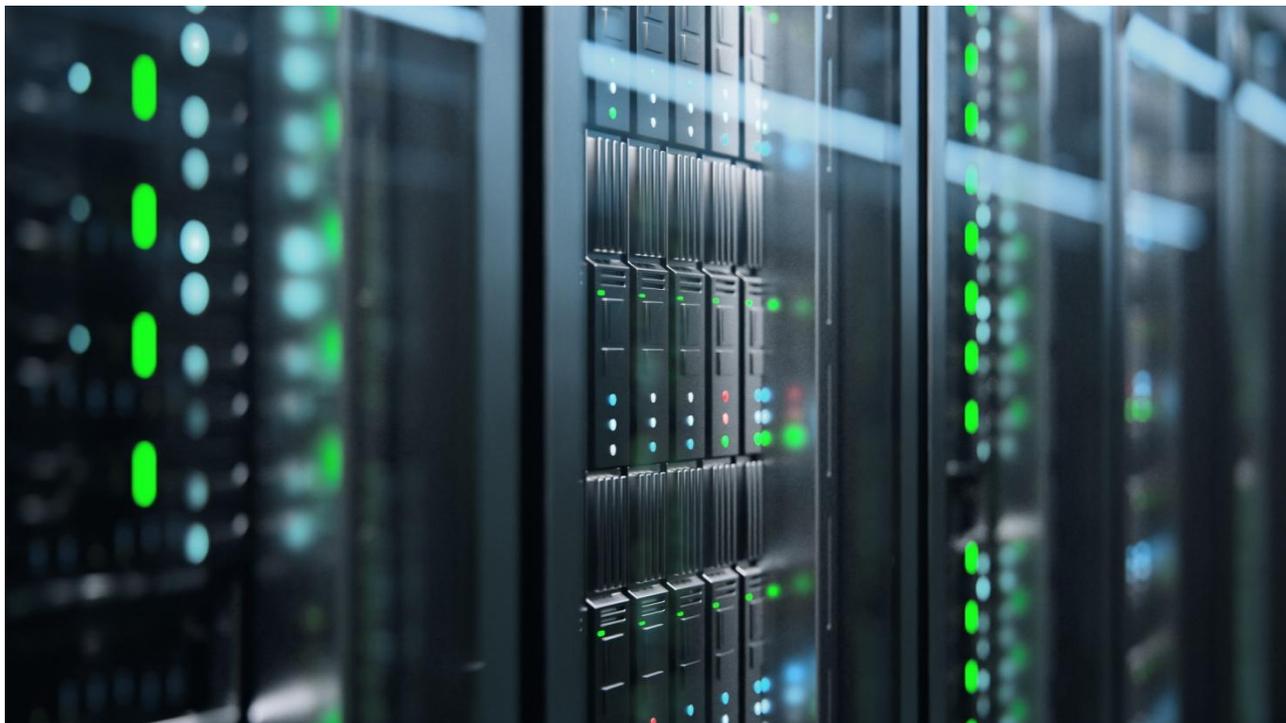


**NEWSLETTER N. 480 del 2 agosto 2021**

- [Data retention: Garante privacy, necessaria una riforma](#)
- [Rider: il Garante privacy sanziona Deliveroo Italy per 2,5 milioni di euro](#)
- [Whistleblowing: Garante, servono maggiori tutele per il segnalante](#)

---

**Data retention: Garante privacy, necessaria una riforma**

Il Garante per la protezione dei dati personali [ha inviato una segnalazione al Parlamento e al Governo](#) con la quale chiede di valutare l'opportunità di una riforma della disciplina della conservazione dei dati di traffico telefonico e telematico a fini di giustizia.

La modifica più volte sollecitata dall'Autorità si è resa ora ulteriormente necessaria a seguito della [sentenza della CGUE del 2 marzo scorso \(causa C-746/18\)](#).

Tale pronuncia, infatti, sviluppa e precisa un indirizzo già consolidato, a partire dalla sentenza Digital Rights Ireland dell'8 aprile 2014 con cui la Corte di Giustizia ha dichiarato l'illegittimità della direttiva 2006/24/Ce in materia di data retention per violazione del principio di proporzionalità nel bilanciamento tra protezione dati ed esigenze di pubblica sicurezza.

Una carenza di proporzionalità che nel caso italiano è stata ulteriormente accentuata dalla legge 167/2017 che ha esteso a sei anni il termine massimo di conservazione dei tabulati prima stabilito in due anni per i tabulati telefonici, in un anno per i telematici e in un mese per le chiamate senza risposta. Ed anche se i dati raccolti possono essere acquisiti solo per reati particolarmente gravi, come quelli di competenza delle Procure distrettuali (criminalità organizzata, mafia, terrorismo), ciò comporta comunque la conservazione generalizzata dei tabulati di tutti gli utenti per sei anni.

Il Garante invita quindi il Parlamento a riflettere sull'opportunità di una riforma della disciplina della data retention, tale da differenziare condizioni, limiti e termini di conservazione dei dati di traffico telefonico e telematico in base alla particolare gravità del reato per cui si procede, e comunque entro periodi massimi compatibili con il principio di proporzionalità, come interpretato dalla Corte di giustizia dell'Unione europea.

Secondo il Garante, occorrerebbe inoltre valutare l'opportunità di subordinare l'acquisizione dei dati di traffico telefonico e telematico all'autorizzazione del gip, ferma restando, nei casi d'urgenza, la possibilità per il pubblico ministero di provvedervi con proprio decreto, da convalidare in una fase successiva.

A fronte poi, della diversità di posizioni già espresse in alcune sentenze successive a quella della CGUE e dell'esigenza di rendere il quadro normativo interno pienamente conforme alla disciplina europea, come interpretata dalla Corte di giustizia dell'Unione europea, è dunque auspicabile – ad avviso del Garante - un intervento chiarificatore del legislatore, che assicuri quel bilanciamento, tra esigenze investigative e protezione dei dati personali, più volte invocato dalla giurisprudenza europea.

---

### **Rider: il Garante privacy sanziona Deliveroo Italy per 2,5 milioni di euro**

*Utilizzo poco trasparente degli algoritmi e raccolta sproporzionata dei dati dei lavoratori*



Prosegue l'azione dell'Autorità per la privacy a tutela dei dati dei lavoratori delle piattaforme di food delivery italiane.

Il Garante [ha ingiunto a Deliveroo Italy il pagamento di una sanzione di 2 milioni e 500 mila euro](#) per aver trattato in modo illecito i dati personali di circa 8000 rider. Per mettersi in regola, la società dovrà modificare il trattamento dei dati dei lavoratori adeguandosi, entro tempi determinati, alle prescrizioni dettate dall'Autorità. Dagli accertamenti effettuati anche presso la sede della società, che svolge attività di consegna di cibo e prodotti per mezzo di una piattaforma digitale, sono emerse infatti numerose e gravi violazioni della normativa privacy europea e nazionale, dello Statuto dei lavoratori e della recente normativa a tutela di chi lavora con le piattaforme digitali.

Gli illeciti riguardavano tra l'altro la mancata trasparenza degli algoritmi utilizzati per la gestione dei rider, sia per l'assegnazione degli ordini sia per la prenotazione dei turni di lavoro.

La società, che a fine 2020 ha dichiarato di non utilizzare più il sistema di prenotazione dei turni, dovrà fornire ai rider informazioni precise sul funzionamento del sistema di assegnazione degli ordini ed individuare misure per tutelare il diritto di ottenere l'intervento umano in grado di valutare compiutamente e, se del caso, correggere in modo sostanziale il funzionamento del sistema.

Spetta comunque alla società di verificare, con cadenza periodica, la correttezza dei risultati degli algoritmi per ridurre al massimo il rischio di effetti distorti o discriminatori.

Dalle verifiche è inoltre emerso che Deliveroo effettua anche un minuzioso controllo sulla prestazione lavorativa dei rider - attraverso la continua geolocalizzazione del loro dispositivo, che va ben oltre quanto necessario per assegnare l'ordine (ad es. rilevazione ogni 12 secondi della posizione, conservazione di tutti i percorsi per 6 mesi) - e mediante la conservazione di una elevata mole di dati personali raccolti nel corso dell'esecuzione degli ordini, tra i quali anche le comunicazioni con il customer care. Il sistema raccoglie infatti dati relativi a scostamenti di pochi minuti rispetto ai tempi stimati (ad es. ritiro dal cibo dal ristorante o consegna al cliente) o comunque predeterminati (ad es., tempo di effettivo spostamento del rider dal luogo in cui ha accettato il pick up). Tutto ciò in violazione dello Statuto dei lavoratori che, per l'utilizzo di dispositivi dai quali possa derivare anche il controllo a distanza del lavoratore, richiede, prima dell'installazione, la sussistenza di esigenze determinate (sicurezza del lavoro, tutela del patrimonio aziendale) e comunque la stipula di un accordo sindacale o l'autorizzazione dell'Ispettorato del lavoro.

L'Autorità ha concesso a Deliveroo 60 giorni di tempo per correggere le violazioni riscontrate e ulteriori 90 giorni per completare gli interventi sugli algoritmi

---

**Whistleblowing: Garante, servono maggiori tutele per il segnalante**  
*Sanzionati un datore di lavoro e il fornitore dell'applicativo*



L'identità dei whistleblower è protetta da uno specifico regime di garanzia e riservatezza previsto dalla normativa di settore per la particolare delicatezza delle informazioni trattate e per gli elevati rischi di ritorsioni e discriminazioni nel contesto lavorativo. In tale quadro, il titolare del trattamento è tenuto a rispettare i principi in materia di protezione dei dati, assicurandone l'integrità e la sicurezza.

E' quanto ribadito dal Garante privacy che, a seguito di attività ispettive sugli applicativi usati per le segnalazioni di illeciti (whistleblowing), ha sanzionato la [società Aeroporto Guglielmo Marconi di Bologna per 40.000 euro](#) e [il suo fornitore di software per 20.000 euro](#) per violazioni delle regole poste a tutela dei dati personali trattati.

Nel caso della Società aeroportuale il Garante ha accertato il mancato utilizzo di tecniche di crittografia per la trasmissione e la conservazione dei dati e la violazione del principio della privacy by design.

Nel corso dell'istruttoria è emerso infatti che l'accesso all'applicativo per l'acquisizione e la gestione delle segnalazioni di illeciti avveniva senza l'uso di un protocollo di rete sicuro (quale il protocollo https) e che l'applicativo stesso non prevedeva la cifratura dei dati identificativi del segnalante, delle informazioni relative alla segnalazione e della eventuale documentazione allegata.

La società aeroportuale, titolare del trattamento, tracciava poi, mediante i log generati dai firewall, l'accesso all'applicativo da parte dei dipendenti connessi alla rete aziendale. Ciò rendeva inefficaci le altre misure adottate per tutelare la riservatezza dell'identità dei segnalanti, considerato anche l'esiguo numero di connessioni all'applicativo in questione. Inoltre, tenuto conto della delicatezza delle informazioni trattate, dei rischi e della vulnerabilità degli interessati, la società avrebbe dovuto effettuare una valutazione di impatto.

Nel comminare la sanzione il Garante ha ribadito che il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve verificare la conformità ai principi di protezione dati impartendo le necessarie istruzioni al fornitore del servizio (ad es. disattivando le funzioni in contrasto con le norme di settore). L'Autorità ha sanzionato con un secondo provvedimento anche il fornitore dell'applicativo, nella sua qualità di responsabile del trattamento, sia per la violazione degli obblighi in materia di sicurezza, sia per la mancata regolamentazione del rapporto con altre due società che trattavano i dati per suo conto.

---

## **L'ATTIVITÀ DEL GARANTE - PER CHI VUOLE SAPERNE DI PIÙ**

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

- Semplificare le informative privacy attraverso il metodo "Creative Commons". Protocollo tra Garante Privacy e Creative Commons - [Comunicato del 26 luglio 2021](#)
- Covid 19: Il Garante privacy "avverte" la Regione Sicilia. L'ordinanza del Presidente della Regione viola le norme sulla privacy dei lavoratori - [Comunicato del 23 luglio 2021](#)
- Pegasus: il Garante privacy chiede informazioni alla società che distribuisce il software - [Comunicato del 23 luglio 2021](#)
- Anticorruzione: Firmato protocollo tra Garante privacy e associazione Aitra - [Comunicato del 22 luglio 2021](#)
- Pmi: Garante privacy e Torino Wireless insieme per promuovere la cultura della protezione dati. Firmato oggi il Protocollo d'intesa - [Comunicato del 21 luglio 2021](#)

## **NEWSLETTER**

del Garante per la protezione dei dati personali (Reg. al Trib. di Roma n. 654 del 28 novembre 2002).

Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza Venezia, n. 11 - 00187 Roma.

Tel: 06.69677.2751- Fax: 06.69677.3785

Newsletter è consultabile sul sito Internet [www.garanteprivacy.it](http://www.garanteprivacy.it)