GDPR e messaggistica professionale: perché la maggioranza è inadempiente senza saperlo

Quasi ogni studio, clinica o consulenza invia documenti con dati dei clienti tramite applicazioni il cui server si trova al di fuori dello Spazio Economico Europeo. Senza cattiva fede, ma in molti casi violando il regolamento senza che nessuno li abbia avvertiti.

Il documento che viaggia più di quanto pensi

Una situazione quotidiana: una consulente fiscale riceve per messaggistica un documento con i dati di un cliente. Un commerciale inoltra per chat un preventivo a un collega. Una dottoressa condivide per la stessa via un referto clinico con un collega. Nessuno ci pensa due volte. È la norma. È comodo. È ciò che si fa in ogni studio in ogni città d'Europa ogni giorno.

Ma quel documento, in molti casi, è appena viaggiato verso un server negli Stati Uniti. È stato archiviato — anche se temporaneamente, anche se "crittografato a riposo" — in un cloud che né il professionista né il suo cliente controllano. È passato attraverso sistemi che tecnicamente possono indicizzare i metadati associati al contenuto. E il Regolamento Generale sulla Protezione dei Dati europeo ha qualcosa di piuttosto chiaro da dire al riguardo.

Ciò che la normativa esige

Il GDPR — e per estensione la giurisprudenza della Corte di Giustizia dell'Unione Europea (in particolare la sentenza Schrems II, C-311/18, del 2020) — stabilisce che i dati personali dei cittadini europei devono essere adeguatamente protetti. Se quei dati lasciano lo Spazio Economico Europeo, il titolare del trattamento deve garantire che il destinatario offra un livello di protezione "sostanzialmente equivalente" a quello europeo. In pratica, ciò significa che l'invio di dati dei clienti tramite servizi i cui server sono sotto la giurisdizione statunitense, senza aver effettuato una valutazione d'impatto e aver implementato garanzie supplementari — clausole contrattuali tipo, misure tecniche aggiuntive come la crittografia verificabile, ecc. — può costituire una violazione del regolamento. Anche se nessuno ha ancora detto nulla.

E non si tratta solo del contenuto dei messaggi. Anche i metadati — chi invia cosa a chi, quando, con quale frequenza, da dove — sono dati personali secondo la normativa, secondo l'interpretazione reiterata del Comitato europeo per la protezione dei dati. Un servizio che raccoglie i metadati delle comunicazioni professionali di un utente sta elaborando i dati personali dei clienti di quell'utente, senza che questi ne siano a conoscenza, né abbiano fornito alcun consenso per tale trattamento.

Lo schema mentale comune — "uso solo l'app per scrivere; l'app non è un fornitore di dati del mio cliente" — è giuridicamente scorretto. Se i dati del cliente passano attraverso l'infrastruttura di un terzo, quel terzo sta elaborando quei dati. E se li sta elaborando, deve esserci una base legale, un contratto di nomina a responsabile del trattamento e garanzie adeguate.

Chi è responsabile

La questione su chi gravi la responsabilità giuridica non è accademica. Il GDPR distingue tra il *titolare del trattamento* (chi decide quali dati trattare e per cosa) e il *responsabile del trattamento* (chi lo fa materialmente, per conto del titolare). Il professionista che invia documenti dei clienti è il titolare. Il fornitore dell'app di messaggistica è, in molti casi, un responsabile di fatto. Senza un contratto di nomina — e senza la maggior parte delle clausole che tale contratto dovrebbe contenere — il titolare non ha adempiuto al proprio obbligo.

L'interpretazione benevola è: "la maggior parte dei professionisti non lo sa". L'interpretazione rigorosa è: "l'ignoranza non esonera dal rispetto della legge". E l'interpretazione di qualsiasi avvocato specializzato in protezione dei dati consultato al riguardo è, in genere, quella rigorosa.

Per chi conta questo in concreto

Per qualsiasi professionista o azienda che gestisca, anche occasionalmente, informazioni personali di terzi:

- Avvocati che ricevono documentazione dai clienti (contratti, citazioni, dichiarazioni, rapporti patrimoniali).
- Medici e altri operatori sanitari che condividono dati sulla salute — considerati *categorie particolari* dall'art. 9 GDPR, con regime rafforzato.
- Consulenti fiscali e gestori amministrativi che spostano dati identificativi, fiscali e bancari.
- Dipartimenti delle risorse umane che gestiscono documentazione lavorativa e personale dei dipendenti.
- Commerciali che ricevono dati di contatto e, spesso, informazioni commerciali sensibili di prospect e clienti.

In tutti i casi, l'informazione è protetta dal GDPR. In tutti i casi, nella pratica abituale, tale informazione transita attraverso canali la cui giurisdizione non consente di essere dichiarata "sostanzialmente equivalente" al quadro europeo senza ulteriori garanzie. Non per cattiva fede. Per abitudine. E per un'infrastruttura tecnologica che ha dato priorità alla comodità rispetto alla conformità per quindici anni.

L'argomento "lo fanno tutti"

Conviene anticipare l'obiezione più frequente: "se lo fanno tutti, non può essere un problema reale". È un argomento perfettamente comprensibile e, giuridicamente, non ha alcuna forza. Il fatto che una pratica sia diffusa non la rende conforme al regolamento. Le autorità per la protezione dei dati hanno sanzionato diverse aziende negli ultimi anni proprio per utilizzi della messaggistica che sembravano innocui fino al momento dell'ispezione.

La realtà operativa attuale è che il rischio è basso in termini di probabilità — è molto raro che un'ispezione controlli gli strumenti di messaggistica specifici di uno studio di medie dimensioni — ma alto in termini di impatto se si materializza. È un rischio che la maggior parte si assume senza sapere di assumerlo. Ovvero, senza aver valutato se lo strumento utilizzato sia in linea con la responsabilità giuridica del titolare del trattamento.

La traccia digitale è retroattiva

C'è un secondo argomento, quasi simmetrico al precedente, che conviene anticipare: *"se questo fosse un problema serio, l'amministrazione avrebbe già iniziato a ispezionarlo"*. La realtà operativa attuale gli dà ragione in superficie. Le ispezioni per uso improprio della messaggistica nelle piccole imprese e, soprattutto, nei lavoratori autonomi sono oggi quasi inesistenti — non perché il comportamento sia consentito, ma perché l'amministrazione manca del personale necessario per controllare milioni di soggetti obbligati.

Questo è ciò che suggerisce la pratica osservata oggi. Non è ciò che suggerisce il prossimo decennio. Due vettori convergono per alterare l'equilibrio in tempi relativamente brevi.

Primo: la traccia digitale è retroattiva. Ogni messaggio inviato tramite un'applicazione con server centrale viene registrato — almeno nei metadati — in un'infrastruttura che persiste. Ciò che è stato inviato sei mesi fa è ancora tecnicamente ispezionabile oggi. Ciò che viene inviato oggi continuerà a essere ispezionabile tra cinque anni. L'assenza di ispezioni attuali non è una garanzia di assenza di ispezioni future. È un rinvio della valutazione, non un'esenzione.

Secondo: la capacità di ispezione amministrativa crescerà rapidamente. L'introduzione di strumenti di intelligenza artificiale nei processi ispettivi elimina il collo di bottiglia umano che finora ha protetto le piccole imprese e gli autonomi. Un sistema in grado di incrociare metadati massivi, dichiarazioni fiscali, registri commerciali e obblighi di notifica delle violazioni non richiede ispettori: richiede accesso. E l'accesso, tramite richieste ai fornitori con presenza giuridica nell'UE, è perfettamente fattibile nell'attuale quadro normativo.

A ciò si aggiunge un fattore meno tecnico ma altrettanto determinante: gli Stati europei sono in un processo sostenuto di indebitamento crescente e hanno bisogno, quasi senza eccezione, di ampliare la propria base imponibile. La sanzione amministrativa derivante dall'inadempimento del GDPR è, in termini puramente fiscali, una fonte di reddito crescente e politicamente comoda. Non è una congettura: è una tendenza osservabile nei rapporti annuali delle agenzie europee per la protezione dei dati, dove il volume totale delle sanzioni è in aumento da diversi esercizi consecutivi.

La conclusione operativa per il titolare del trattamento non è allarmistica, ma fredda: **la decisione su come viene gestita oggi la comunicazione con i clienti viene valutata rispetto alla capacità ispettiva dell'anno in cui arriverà l'ispezione, non rispetto a quella attuale.** E tale capacità sarà, in tempi ragionevoli, sostanzialmente diversa da quella odierna. Chi inizia a fare le cose bene oggi non sarà in regola solo a partire da oggi: la traccia generata da questo momento sarà coerente con la normativa, e ciò protegge retroattivamente il tratto a venire. Chi continuerà come prima accumulerà una traccia ispezionabile la cui conformità sarà valutata rispetto agli standard — e alle risorse — dei prossimi anni.

Cosa cambia con un'architettura diversa

Esistono alternative tecniche in cui i dati non vengono archiviati su infrastrutture di terzi, ma viaggiano direttamente dal dispositivo del mittente a quello del destinatario. In tale architettura, l'adempimento del GDPR in merito ai trasferimenti internazionali non dipende da clausole contrattuali tipo, né dalla buona volontà del fornitore, né da ispezioni future. Dipende dal fatto che *non c'è trasferimento*. E ciò che non esiste non può essere inadempiente.

Questa non è una soluzione esclusiva né l'unica possibile. Ma è strutturalmente diversa e la conformità normativa smette di essere un annesso procedurale per diventare una conseguenza diretta della progettazione. Per un professionista che prende sul serio la propria responsabilità come titolare del trattamento, tale differenza conta.

Il prossimo numero di Cuadernos analizzerà nel dettaglio la sentenza Schrems II e le sue implicazioni pratiche per le piccole e medie imprese che dipendono da servizi cloud statunitensi, a cinque anni dalla sua pubblicazione.

Fonti e quadro normativo

- Regolamento UE 2016/679 (GDPR), in particolare il Capo V sui trasferimenti internazionali.
- CGUE C-311/18 ("Schrems II"), 16 luglio 2020.
- EDPB — Raccomandazioni 01/2020 sulle misure che integrano gli strumenti di trasferimento.
- Autorità per la protezione dei dati — Rapporti annuali con casistica di sanzioni per uso improprio della messaggistica istantanea in contesti professionali.

← PrecedenteIl segreto professionale nell'era digitaleSuccessivo →Quando non c'è nessuno in mezzo

Letture recenti

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Porta questo articolo dove ne hai bisogno.

↓ Markdown ↓ Testo semplice ↓ PDF

Il file viene scaricato sul tuo dispositivo. Da lì puoi salvarlo, importarlo in Solo2 o condividerlo come preferisci. Cuadernos non decide la destinazione per te.

Sigillo di cera · SHA-256 d91a399b754d0caecd94b78cdd62d3ce1f933501e007286c3093d9ec77523190

Cuadernos Lacre · Una pubblicazione di Menzuri Gestión S.L. ·
scritta da R.Eugenio · a cura del team di Solo2.