Il segreto professionale nell'era digitale

Quando la comunicazione tra il professionista e il suo cliente passa attraverso un canale tecnicamente inadeguato, il segreto non si rompe il giorno della fuga di notizie. Si è rotto molto prima, al momento della scelta dello strumento.

Un problema che quasi nessuno vede

Un avvocato riceve sul proprio telefono un documento sensibile da un cliente. Un medico discute una diagnosi delicata con un collega. Uno psicologo coordina con uno psichiatra il trattamento di un paziente. Un consulente fiscale invia i dati di una dichiarazione in attesa di revisione. Tutti lo fanno tramite messaggistica istantanea. E quasi nessuno si sofferma a pensare dove finiscano realmente quei messaggi.

La risposta, nella maggior parte dei casi, è la stessa: in un server che il professionista non controlla, in un paese la cui legislazione non necessariamente conosce, gestito da un'azienda il cui modello di business è — in termini economici diretti — accumulare dati. Il messaggio può essere crittografato in transito. Ma una volta arrivato al server, è una copia archiviata nell'infrastruttura di un terzo, soggetta alle decisioni operative, giuridiche e commerciali di quel terzo. Non del professionista.

Ciò che dice la legislazione

Il Regolamento Generale sulla Protezione dei Dati europeo è inequivocabile nel suo articolo 32: chiunque tratti dati personali deve applicare misure tecniche e organizzative "appropriate" per garantire un livello di sicurezza adeguato al rischio. L'adeguatezza delle misure non viene valutata rispetto a "ciò che l'app dice di fare", ma rispetto al rischio reale. Se i dati di un cliente finiscono su un server la cui giurisdizione non garantisce un livello di protezione equivalente a quello dello Spazio Economico Europeo, il titolare del trattamento — ovvero il professionista — si assume un rischio di cui probabilmente non è del tutto consapevole.

E non è solo il GDPR. Il segreto professionale, regolamentato in modo specifico per avvocati, medici, psicologi, revisori, giornalisti e altri, esige che la comunicazione con il cliente sia riservata. Non "riservata per quanto possibile". Riservata senza sfumature. Se il canale tecnico utilizzato non può garantirlo, il professionista si assume un rischio che la deontologia della sua professione non consente di assumere.

Il paradosso è che il rischio è invisibile. Nessuno esegue audit sulla messaggistica dello studio. Nessuno richiede il contratto di elaborazione dei dati al fornitore della chat. Il rischio emerge solo quando è troppo tardi: una fuga di notizie, una violazione pubblicata, un ordine del tribunale eseguito in un altro continente senza notifica all'utente.

Ciò di cui un professionista ha tecnicamente bisogno

Ciò di cui ha bisogno un professionista con segreto professionale è, in realtà, sorprendentemente semplice dal punto di vista dei requisiti:

- Un canale dove i messaggi vadano direttamente dal dispositivo del mittente a quello del destinatario, senza passare per un server intermedio che archivia copie.
- Un'infrastruttura la cui giurisdizione e le cui politiche siano allineate al GDPR per costruzione, non per dichiarazione.
- Un modo per identificarsi con l'interlocutore senza dover consegnare a terzi i contatti professionali (nomi dei clienti, numeri di telefono, rubrica).
- Qualche sistema verificabile — non basato sulla parola del fornitore — per confermare che il messaggio sia arrivato alla persona corretta.

Non è un elenco esigente. È, in realtà, ciò che si dava per scontato nella comunicazione professionale pre-digitale. Una lettera raccomandata soddisfaceva tutti quei criteri. Anche una telefonata dal centralino dello studio a quello del cliente. La cosa strana non è che queste garanzie vengano richieste oggi: la cosa strana è che siano andate perdute passando al canale digitale, senza che nessuno se ne accorgesse.

La differenza tra crittografare e non archiviare

C'è una metafora utile. Crittografare un messaggio e archiviarlo su un server equivale a mettere un documento in una cassaforte e lasciare la cassaforte a casa di uno sconosciuto. La cassaforte è buona. Il documento, in linea di principio, non può essere letto. Ma il documento *rimane a casa di qualcun altro*. E quel qualcun altro può ricevere un ordine del tribunale, può subire un attacco informatico, può cambiare le proprie condizioni di servizio, può essere acquistato da un'altra azienda con un'altra etica, può scomparire domani.

L'alternativa strutturale — non procedurale, non basata sulla fiducia — è che il documento non lasci mai lo studio. Che viaggi direttamente dalla scrivania del professionista alla scrivania del cliente, senza passare per alcun intermediario. Questo è ciò che fa tecnicamente la comunicazione punto a punto tra dispositivi: elimina l'intermediario. Non è che l'intermediario sia cattivo. È che, per il caso del segreto professionale, l'intermediario è *non necessario*. E ciò che non è necessario, in qualsiasi sistema che aspiri a essere sicuro, deve essere eliminato per principio.

La questione della responsabilità

Alla fine, la domanda a cui ogni professionista con dovere di segreto dovrebbe poter rispondere con un sì categorico è la seguente:

> Se domani trapelasse una conversazione con uno dei miei clienti e un tribunale o un ordine professionale mi chiedesse come gestisco la riservatezza, posso dimostrare tecnicamente che il canale che ho usato non archivia copie su infrastrutture di terzi? Posso dimostrare che i dati non hanno mai lasciato i dispositivi delle due persone che hanno partecipato alla conversazione? Posso dimostrare, senza dipendere dalla parola di un'azienda di un altro continente, che la riservatezza era garantita dall'architettura e non da una promessa?

Se la risposta è no, il problema non è lo strumento specifico. Il problema è che è stata delegata a uno strumento una responsabilità che lo strumento non era progettato per supportare. È come mettere fascicoli riservati in una busta trasparente e confidare che il postino non guardi.

Lo strumento che un professionista sceglie per comunicare con i propri clienti dice molto di come valuta la loro fiducia. Ci sono strumenti progettati affinché tale fiducia non dipenda da promesse, ma dall'architettura. E ci sono strumenti che non lo sono. Conoscere la differenza fa parte del lavoro.

Quadro normativo citato

- Regolamento UE 2016/679 (GDPR), in particolare gli artt. 5, 25 (protezione dei dati fin dalla progettazione) e 32 (sicurezza del trattamento).

- Normativa nazionale sull'ordinamento delle professioni regolamentate e sul dovere di segreto professionale.
- Legge sulla tutela del paziente e sulla riservatezza delle informazioni sanitarie.
- Codici deontologici degli ordini professionali riguardanti la riservatezza e il segreto professionale.

← PrecedenteCrittografare non significa essere privati: ciò che i metadati dicono di teSuccessivo →GDPR e messaggistica professionale: perché la maggioranza è inadempiente senza saperlo

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 4b64e8cfac9e5169992c8956765dbff41b94bad6ae7bd788c4b69af7a7610687

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