Secretul profesional în era digitală

Când comunicarea dintre profesionist și clientul său are loc printr-un canal inadecvat din punct de vedere tehnic, secretul nu este încălcat în ziua divulgării. A fost încălcat mult mai devreme, în momentul alegerii instrumentului.

O problemă pe care aproape nimeni nu o vede

Un avocat primește pe telefon un document confidențial de la un client. Un medic discută cu un coleg despre un diagnostic delicat. Un psiholog coordonează tratamentul unui pacient cu un psihiatru. Un consultant fiscal trimite datele unei declarații care așteaptă revizuirea. Toți o fac prin mesagerie instantanee. Și aproape nimeni nu se oprește să se gândească unde ajung de fapt acele mesaje.

Răspunsul este, în cele mai multe cazuri, același: pe un server pe care profesionistul nu îl controlează, într-o țară a cărei legislație nu o cunoaște neapărat, gestionat de o companie al cărei model de afaceri este – în termeni economici direcți – de a acumula date. Mesajul poate fi criptat în tranzit. Dar odată ce ajunge pe server, este o copie stocată în infrastructura unei terțe părți, supusă deciziilor operative, legale și comerciale ale acelei terțe părți. Nu ale profesionistului.

Ce spune legislația

Regulamentul General European privind Protecția Datelor este lipsit de ambiguitate în articolul său 32: oricine prelucrează date cu caracter personal trebuie să pună în aplicare măsuri tehnice și organizatorice „adecvate” pentru a garanta un nivel de securitate corespunzător riscului. Adecvarea măsurilor nu se măsoară după „ceea ce aplicația spune că face”, ci după riscul real. Dacă datele unui client ajung pe un server a cărui jurisdicție nu garantează un nivel de protecție echivalent cu cel al Spațiului Economic European, operatorul – adică profesionistul – își asumă un risc de care probabil nu este pe deplin conștient.

Și nu este vorba doar despre GDPR. Secretul profesional, reglementat specific pentru avocați, medici, psihologi, auditori, jurnaliști și alții, cere ca comunicarea cu clientul să fie confidențială. Nu „cât mai confidențială posibil”. Confidențială fără rezerve. Dacă canalul tehnic utilizat nu poate garanta acest lucru, profesionistul își asumă un risc pe care deontologia profesiei sale nu îi permite să îl asume.

Paradoxul este că riscul este invizibil. Nimeni nu auditează mesageria biroului. Nimeni nu cere contractul de prelucrare a datelor de la furnizorul de chat. Riscul iese la iveală abia când este prea târziu: o divulgare, o breșă publicată, un ordin judecătoresc executat pe un alt continent fără notificarea utilizatorului.

De ce are nevoie tehnic un profesionist

Ceea ce are nevoie o persoană supusă secretului profesional este, din punctul de vedere al cerințelor, de fapt surprinzător de simplu:

- Un canal în care mesajele merg direct de la dispozitivul expeditorului la dispozitivul destinatarului, fără a trece printr-un server intermediar care stochează copii.
- O infrastructură a cărei jurisdicție și politici sunt aliniate cu GDPR prin construcție, nu prin declarație.
- O modalitate de identificare cu interlocutorul fără a fi necesară predarea contactelor profesionale (numele clienților, numerele de telefon, agenda) către o terță parte.
- Un sistem verificabil – nu bazat pe cuvântul furnizorului – pentru a confirma că mesajul a ajuns la persoana potrivită.

Nu este o listă exigentă. Este, de fapt, ceea ce se considera de la sine înțeles în comunicarea profesională pre-digitală. O scrisoare recomandată îndeplinea toate aceste criterii. Un apel telefonic de la centrala biroului la cea a clientului, de asemenea. Ciudat nu este faptul că aceste garanții sunt cerute astăzi: ciudat este că s-au pierdut la trecerea la canalul digital, fără ca nimeni să observe.

Diferența dintre a cripta și a nu stoca

Există o metaforă utilă. A cripta un mesaj și a-l stoca pe un server echivalează cu punerea unui document într-un seif și lăsarea seifului în casa unui străin. Seiful este bun. Documentul nu poate fi citit, în principiu. Dar documentul *se află în continuare în casa altcuiva*. Iar acel cineva poate primi un ordin judecătoresc, poate suferi un atac informatic, își poate schimba condițiile de serviciu, poate fi cumpărat de o altă companie cu o altă etică sau poate dispărea mâine.

Alternativa structurală – nu procedurală, nu bazată pe încredere – este ca documentul să nu părăsească niciodată biroul. Să călătorească direct de pe masa profesionistului pe masa clientului, fără niciun fel de intermediar. Aceasta este ceea ce face tehnic comunicarea punct la punct între dispozitive: elimină intermediarul. Nu că intermediarul ar fi rău. Ci doar că, în cazul secretului profesional, intermediarul este *inutil*. Iar ceea ce este inutil trebuie eliminat din principiu din orice sistem care aspiră să fie sigur.

Problema responsabilității

În cele din urmă, întrebarea la care orice profesionist cu obligația de a păstra secretul ar trebui să poată răspunde cu un „da” categoric este următoarea:

> Dacă mâine se divulgă o conversație cu unul dintre clienții mei și o instanță sau un ordin profesional mă întreabă cum gestionez confidențialitatea, pot demonstra tehnic că canalul pe care l-am folosit nu stochează copii în infrastructura unor terțe părți? Pot dovedi că datele nu au părăsit niciodată dispozitivele celor două persoane care au participat la conversație? Pot dovedi, fără a mă baza pe cuvântul unei companii de pe un alt continent, că confidențialitatea a fost garantată de arhitectură și nu de o promisiune?

Dacă răspunsul este nu, problema nu este instrumentul în sine. Problema este că instrumentului i-a fost delegată o responsabilitate pe care instrumentul nu a fost conceput să o susțină. Este ca și cum ai pune dosare confidențiale într-un plic transparent și ai avea încredere că poștașul nu se va uita.

Instrumentul pe care un profesionist îl alege pentru a comunica cu clienții săi spune multe despre modul în care le prețuiește încrederea. Există instrumente concepute astfel încât acea încredere să nu depindă de promisiuni, ci de arhitectură. Și există instrumente care nu sunt așa. Cunoașterea diferenței face parte din muncă.

Cadrul normativ citat

- Regulamentul (UE) 2016/679 (GDPR), în special art. 5, 25 (protecția datelor începând cu momentul conceperii) și 32 (securitatea prelucrării).
- Legislația română privind secretul profesional (inclusiv Legea nr. 51/1995 pentru organizarea și exercitarea profesiei de avocat, Legea nr. 95/2006 privind reforma în domeniul sănătății).

- Codul Penal, art. 227 (divulgarea secretului profesional).
- Codul deontologic al avocaților privind confidențialitatea și secretul profesional.

← PrecedentA cripta nu înseamnă a avea confidențialitate: ce spun metadatele despre dumneavoastrăUrmător →GDPR și mesageria profesională: de ce majoritatea încalcă normele fără să știe

Lecturi recente

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Luați acest articol cu dumneavoastră oriunde aveți nevoie.

↓ Markdown ↓ Text simplu ↓ PDF

Fișierul se va descărca pe dispozitivul dumneavoastră. De acolo îl puteți salva, importa în Solo2 sau partaja oriunde doriți. Cuadernos nu decide destinația în locul dumneavoastră.

Sigiliu de ceară · SHA-256 c284da6ec746999931be0e99a1ce8552ac6e9210575df94cb492c5f79303e6ce

Cuadernos Lacre · O publicație a Menzuri Gestión S.L. ·
scrisă de R.Eugenio · editată de echipa Solo2.