O segredo profissional na era digital

Quando a comunicação entre o profissional e o seu cliente passa por um canal tecnicamente inadequado, o segredo não se quebra no dia da filtração. Quebrou-se muito antes, no momento de escolher a ferramenta.

Um problema que quase ninguém vê

Um advogado recebe no seu telefone um documento sensível de um cliente. Um médico discute com um colega um diagnóstico delicado. Um psicólogo coordena com um psiquiatra o tratamento de um paciente. Um consultor fiscal envia os dados de uma declaração pendente de revisão. Todos o fazem por mensagens instantâneas. E quase nenhum se detém a pensar onde acabam realmente essas mensagens.

A resposta, na maioria dos casos, é a mesma: num servidor que o profissional não controla, num país cuja legislação não necessariamente conhece, gerido por uma empresa cujo modelo de negócio é — em termos económicos diretos — acumular dados. A mensagem pode estar cifrada em trânsito. Mas, uma vez que chega ao servidor, é uma cópia armazenada na infraestrutura de um terceiro, sujeita às decisões operacionais, jurídicas e comerciais desse terceiro. Não do profissional.

O que a legislação diz

O Regulamento Geral de Proteção de Dados europeu é inequívoco no seu artigo 32: quem tratar dados pessoais deve aplicar medidas técnicas e organizativas "apropriadas" para garantir um nível de segurança adequado ao risco. A adequação das medidas não se avalia contra "o que a app diz que faz", mas contra o risco real. Se os dados de um cliente acabam num servidor cuja jurisdição não garante um nível de proteção equivalente ao do Espaço Económico Europeu, o responsável pelo tratamento — ou seja, o profissional — está a assumir um risco de que provavelmente não está totalmente consciente.

E não é apenas o RGPD. O segredo profissional, regulado de forma específica para advogados, médicos, psicólogos, auditores, jornalistas e outros, exige que a comunicação com o cliente seja confidencial. Não "confidencial na medida do possível". Confidencial sem matizes. Se o canal técnico utilizado não puder garanti-lo, o profissional está a assumir um risco que a deontologia da sua profissão não permite assumir.

O paradoxo é que o risco é invisível. Ninguém audita as mensagens do escritório. Ninguém pede o contrato de processamento de dados do fornecedor do chat. O risco emerge apenas quando já é tarde: uma filtração, uma quebra publicada, uma ordem judicial cumprida noutro continente sem notificação ao utilizador.

O que um profissional necessita tecnicamente

O que um profissional com segredo profissional necessita é, na realidade, surpreendentemente simples do ponto de vista dos requisitos:

- Um canal onde as mensagens vão diretas do dispositivo do emissor para o do recetor, sem passar por um servidor intermédio que armazene cópias.

- Uma infraestrutura cuja jurisdição e políticas estejam alinhadas com o RGPD por construção, não por declaração.
- Uma forma de se identificar com o interlocutor sem ter de entregar a um terceiro os contactos profissionais (nomes de clientes, números de telefone, agenda).
- Algum sistema verificável — não baseado na palavra do fornecedor — para confirmar que a mensagem chegou à pessoa correta.

Não é uma lista exigente. É, na realidade, o que se dava por certo na comunicação profissional pré-digital. Uma carta registada cumpria todos esses critérios. Uma chamada telefónica da central telefónica do escritório para a do cliente, também. O estranho não é que se peçam estas garantias hoje: o estranho é que se tenham perdido ao passar para o canal digital, sem que ninguém se apercebesse.

A diferença entre cifrar e não armazenar

Há uma metáfora útil. Cifrar uma mensagem e guardá-la num servidor é equivalente a meter um documento num cofre e deixar o cofre em casa de um desconhecido. O cofre é bom. O documento, em princípio, não pode ser lido. Mas o documento *continua a estar em casa de outro*. E esse outro pode receber uma ordem judicial, pode sofrer um ataque informático, pode alterar as suas condições de serviço, pode ser comprado por outra empresa com outra ética, pode desaparecer amanhã.

A alternativa estrutural — não procedimental, não por confiança — é que o documento nunca saia do escritório. Que viaje diretamente da mesa do profissional para a mesa do cliente, sem passar por nenhum intermediário. É isso que faz tecnicamente a comunicação ponto a ponto entre dispositivos: elimina o intermediário. Não é que o intermediario seja mau. É que, para o caso do segredo profissional, o intermediário é *desnecessário*. E o desnecessário, em qualquer sistema que aspire a ser seguro, deve ser eliminado por princípio.

A questão da responsabilidade

No final, a pergunta que todo o profissional com dever de segredo deveria poder responder com um sim rotundo é a seguinte:

> Se amanhã for filtrada uma conversa com um dos meus clientes e um tribunal ou uma ordem profissional me perguntar como giro a confidencialidade, posso demonstrar tecnicamente que o canal que utilizei não armazena cópias em infraestruturas de terceiros? Posso provar que os dados nunca saíram dos dispositivos das duas pessoas que participaram na conversa? Posso demonstrar, sem depender da palavra de uma empresa de outro continente, que a confidencialidade estava garantida pela arquitetura e não por uma promessa?

Si a resposta for não, o problema não é a ferramenta em concreto. O problema é que se delegou numa ferramenta uma responsabilidade que a ferramenta não foi desenhada para suportar. É como meter processos confidenciais num envelope transparente e confiar que o carteiro não olha.

A ferramenta que um profissional escolhe para se comunicar com os seus clientes diz muito sobre como valoriza a sua confiança. Há ferramentas desenhadas para que essa confiança não dependa de promessas, mas da arquitetura. E há ferramentas que não o estão. Conhecer a diferença faz parte do trabalho.

Quadro normativo citado

- Regulamento UE 2016/679 (RGPD), especialmente arts. 5, 25 (proteção de dados desde o desenho) e 32 (segurança do tratamento).
- Legislação nacional sobre estatutos profissionais relativamente ao dever de segredo profissional.
- Legislação sobre autonomia do doente e confidencialidade da informação de saúde.

- Códigos deontológicos das ordens profissionais relativamente à confidencialidade e ao segredo profissional.

← AnteriorCifrar não é ser privado: o que os metadados contam sobre siSeguinte →RGPD e mensagens profissionais: por que a maioria incumpre sem saber

Leituras recentes

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Leve este artigo para onde precisar.

↓ Markdown ↓ Texto simples ↓ PDF

O arquivo é descarregado no seu dispositivo. A partir daí, pode guardá-lo, importá-lo no Solo2 ou partilhá-lo onde quiser. Cuadernos não decide o destino por si.

Selo de lacre · SHA-256 a76c157e0ffa72dabbe56994441595e7642ea7790c2916745ecdd3cb13b06924

Cuadernos Lacre · Uma publicação da Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada pela equipa do Solo2.