Análise · 16 de maio de 2026

← Anterior·Seguinte →

RGPD e mensagens profissionais: por que a maioria incumpre sem saber

Quase qualquer escritório, consultório ou assessoria envia documentos com dados de clientes por aplicações cujo servidor está fora do Espaço Económico Europeu. Sem má-fé, mas em muitos casos vulnerando o regulamento sem que ninguém os tenha advertido.

Para nos entendermos: A tua assessora fiscal envia-te um documento pelo WhatsApp. Chega ao teu telemóvel em Madrid, mas antes passou por um servidor no Texas. O RGPD tem algo bastante claro a dizer sobre isso — e a maioria dos escritórios anda há anos a incumpri-lo sem o saber.

O documento que viaja mais do que imagina

Uma situação quotidiana: uma assessora fiscal recebe por mensagens um documento com dados de um cliente. Um comercial reenvia por chat um orçamento a um colega. Uma médica partilha pela mesma via um relatório clínico com um colega. Ninguém pensa nisso duas vezes. É o normal. É o cómodo. É o que se faz em qualquer escritório em qualquer cidade da Europa todos os dias.

Mas esse documento, em muitos casos, acaba de viajar para um servidor nos Estados Unidos. Foi armazenado — ainda que temporariamente, ainda que "cifrado em repouso" — numa nuvem que nem o profissional nem o seu cliente controlam. Passou por sistemas que tecnicamente podem indexar metadados associados ao conteúdo. E o Regulamento Geral de Proteção de Dados europeu tem algo bastante claro a dizer sobre isso.

O que a normativa exige

O RGPD — e por extensão a jurisprudência do Tribunal de Justiça da União Europeia (em particular o acórdão Schrems II, C-311/18, de 2020) — estabelece que os dados pessoais de cidadãos europeus devem estar adequadamente protegidos. Se esses dados saem do Espaço Económico Europeu, o responsável pelo tratamento deve garantir que o destinatário oferece um nível de proteção "essencialmente equivalente" ao europeu. Na prática, isso significa que enviar dados de clientes por serviços cujos servidores estão sob jurisdição norte-americana, sem ter realizado uma avaliação de impacto e ter implementado salvaguardas suplementares — cláusulas contratuais-tipo, medidas técnicas adicionais como criptografia verificável, etc. — pode constituir uma violação do regulamento. Embora ninguém tenha dito nada ainda.

E não se trata apenas do conteúdo das mensagens. Os metadados — quem envia o quê a quem, quando, com que frequência, de onde — também são dados pessoais segundo a normativa, segundo interpretação reiterada do Comité Europeu para a Proteção de Dados. Um serviço que recolhe metadados das comunicações profissionais de um utilizador está a processar dados pessoais dos clientes desse utilizador, sem que estes tenham conhecimento disso, nem tenham prestado qualquer consentimento para tal tratamento.

O esquema mental comum — "eu só uso a app para escrever; a app não é um fornecedor de dados do meu cliente" — é juridicamente incorreto. Se os dados do cliente passam pela infraestrutura de um terceiro, esse

terceiro está a processar esses dados. E se os está a processar, deve haver uma base legal, um contrato de subcontratação do tratamento, e garantias adequadas.

Quem é responsável

A pergunta sobre quem carrega a responsabilidade jurídica não é académica. O RGPD distingue entre o *responsável pelo tratamento* (quem decide que dados são tratados e para quê) e o *subcontratante* (quem o faz materialmente, em nome do responsável). O profissional que envia documentos de clientes é o responsável. O fornecedor da app de mensagens é, em muitos casos, subcontratante de facto. Sem contrato de subcontratação — e sem a maioria das cláusulas que tal contrato deveria conter — o responsável não cumpriu a sua obrigação.

A interpretação benigna é: "a maioria dos profissionais não sabe isto". A interpretação rigorosa é: "o desconhecimento não isenta do cumprimento". E a interpretação de qualquer advogado especialista em proteção de dados consultado a este respeito é, por norma, a rigorosa.

Para quem importa isto em concreto

Para qualquer profissional ou empresa que lide, ainda que ocasionalmente, com informação pessoal de terceiros:

- Advogados que recebem documentação de clientes (contratos, processos, declarações, relatórios patrimoniais).
- Médicos e outros profissionais de saúde que partilham dados de saúde — considerados *categoria especial* pelo art. 9 RGPD, com regime reforçado.
- Consultores fiscais e gestores administrativos que movimentam dados identificativos, fiscais e bancários.
- Departamentos de recursos humanos que gerem documentação laboral e pessoal de empregados.
- Comerciais que recebem dados de contacto e, muitas vezes, informação comercial sensível de prospetos e clientes.

Em todos os casos, a informação está protegida pelo RGPD. Em todos os casos, na prática habitual, essa informação transita por canais cuja jurisdição não permite ser declarada "essencialmente equivalente" ao quadro europeu sem salvaguardas adicionais. Não por má-fé. Por costume. E por uma infraestrutura tecnológica que deu prioridade à comodidade sobre o cumprimento durante quinze anos.

O argumento "toda a gente o faz"

Convém antecipar a objeção mais frequente: "se toda a gente o faz, não pode ser um problema real". É um argumento perfeitamente compreensível e, juridicamente, não tem qualquer força. O facto de uma prática estar difundida não a torna conforme com o regulamento. As agências de proteção de dados sancionaram várias empresas nos últimos anos precisamente por usos de mensagens que pareciam inofensivos até ao momento da inspeção.

A realidade operacional atual é que o risco é baixo em termos de probabilidade — é muito pouco frequente que uma inspeção audite as ferramentas de mensagens específicas de um escritório de média dimensão —, mas alto em termos de impacto se se materializar. É um risco que a maioria assume sem saber que o está a assumir. Ou seja, sem ter avaliado se a ferramenta utilizada está alinhada com a responsabilidade jurídica do responsável pelo tratamento.

O rastro digital é retroativo

Há um segundo argumento, quase simétrico ao anterior, que convém antecipar: *"se isto fosse um problema sério, a administração já teria começado a inspecioná-lo"*. A realidade operacional atual dá-lhe razão superficial. As inspeções por uso indevido de mensagens em empresas pequenas e, sobretudo, em trabalhadores por conta

própria são hoje quase inexistentes — não porque a conduta seja permitida, mas porque a administração carece dos efetivos humanos necessários para auditar milhões de obrigados.

Isso é o que a prática observada sugere hoje. Não é o que a próxima década sugere. Dois vetores convergem para alterar o equilíbrio em prazos relativamente curtos.

Primeiro: o rastro digital é retroativo. Cada mensagem enviada por uma aplicação com servidor central fica registada — pelo menos nos metadados — numa infraestrutura que persiste. O que foi enviado há seis meses continua a ser tecnicamente auditável hoje. O que for enviado hoje continuará a ser auditável daqui a cinco anos. A ausência de inspeção presente não é uma garantia de ausência de inspeção futura. É um adiamento da avaliação, não uma isenção.

Segundo: a capacidade de auditoria administrativa vai crescer aceleradamente. A introdução de ferramentas de inteligência artificial nos processos de inspeção elimina o estrangulamento humano que até agora tem protegido as empresas pequenas e os trabalhadores por conta própria. Um sistema capaz de cruzar metadados massivos, declarações fiscais, registos comerciais e obrigações de notificação de quebras não requer inspetores: requer acesso. E o acesso, mediante requisitos a fornecedores com presença jurídica na UE, é perfeitamente exequível sob o quadro normativo atual.

A isto junta-se um fator menos técnico, mas igualmente determinante: os Estados europeus estão em processo sustentado de endividamento crescente e necessitam, quase sem exceção, de ampliar a sua base arrecadatória. A sanção administrativa derivada do incumprimento do RGPD é, em termos puramente fiscais, uma fonte de receitas crescente e politicamente cómoda. Não é conjetura: é tendência observável nos relatórios anuais das agências de proteção de dados europeias, onde o volume total de sanções tem estado em alta há vários exercícios consecutivos.

A conclusão operacional para o responsável pelo tratamento não é alarmista, mas fria: **a decisão sobre como se gere a comunicação com clientes hoje é avaliada contra a capacidade inspetora do ano em que chegue a inspeção, não contra a atual.** E essa capacidade será, em prazos razoáveis, substancialmente diferente da de hoje. Quem comece a fazer as coisas bem hoje não estará em regra apenas a partir de hoje: o rastro gerado a partir deste momento será coerente com a normativa, e isso protege retroativamente o tramo que vem. Quem continuar como até agora estará a acumular rastro auditável cuja conformidade será avaliada contra os padrões — e os recursos — dos próximos anos.

O que muda com uma arquitetura diferente

Existem alternativas técnicas em que os dados não são armazenados em infraestrutura de terceiros, mas viajam diretamente do dispositivo do emissor para o do recetor. Nessa arquitetura, o cumprimento do RGPD relativamente a transferências internacionais não depende de cláusulas contratuais-tipo, nem da boa vontade do fornecedor, nem de auditorias futuras. Depende de que *não há transferência*. E o que não existe não se pode incumprir.

Esta não é uma solução exclusiva nem a única possível. Mas é estruturalmente diferente, e o cumprimento normativo deixa de ser um anexo procedimental para se tornar uma consequência direta do design. Para um profissional que leva a sério a sua responsabilidade como responsável pelo tratamento, essa diferença importa.

A próxima edição de Cuadernos analisará em detalhe o acórdão Schrems II e as suas implicações práticas para empresas pequenas e médias que dependem de serviços cloud norte-americanos, cinco anos após a sua publicação.

Nota editorial: quando estes Cuadernos nomeiam empresas ou produtos, não é para acusar. Aqueles que os constroem fazem trabalhos que milhões de pessoas usam e apreciam. O que assinalamos é estrutural — o modelo, não a marca. As marcas aparecem como exemplo porque são as que o leitor reconhece.

Fontes e quadro normativo

- Regulamento UE 2016/679 (RGPD), especialmente capítulo V sobre transferências internacionais.
- Acórdão do TJUE C-311/18 ("Schrems II"), 16 de julho de 2020.
- EDPB — Recomendações 01/2020 sobre medidas que complementam os instrumentos de transferência.
- Agências de proteção de dados — Relatórios anuais com casuística de sanções por uso indevido de mensagens instantâneas em ambientes profissionais.

← AnteriorO segredo profissional na era digitalSeguinte →Quando não há ninguém no meio

Leituras recentes

- Análise · 18 de maio de 2026 Privacidade real vs aparente: as perguntas que convém fazer-se
- Análise · 18 de maio de 2026 Self-hosting como prática profissional
- Conceito · 18 de maio de 2026 As 24 palavras: o que é uma identidade criptográfica

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 d7e4163ad36a8287217704211adc25340232c069ec894603d4f0b7d6d1885f9d

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