السر المهني في العصر الرقمي

عندما يتم الاتصال بين المهني وعميله عبر قناة غير مناسبة تقنيًا، لا يتم كسر السر في يوم التسريب. لقد كسر قبل ذلك بكثير، في لحظة اختيار الأداة.

مشكلة لا يراها أحد تقريبًا

يتلقى محامٍ على هاتفه مستندًا سريًا من عميل. يناقش طبيب مع زميل تشخيصًا دقيقًا. ينسق أخصائي نفسي مع طبيب نفسيٍ علاج مريض. يرسل مستشار ضريبي بيانات إقرار ينتظر المراجعة. يفعل الجميع ذلك عبر المراسلة الفورية. ولا يتوقف أحد تقريبًا ليفكر في المكان الذي تنتهي فيه تلك الرسائل حقًا.

الإجابة في معظم الحالات هي نفسها: على خادم لا يتحكم فيه المهني، في بلد قد لا يعرف بالضرورة تشريعاته، تديره شركة نموذج عملها هو – بمصطلحات اقتصادية مباشرة – تجميع البيانات. قد تكون الرسالة مشفرة أثناء النقل. ولكن بمجرد وصولها إلى الخادم، فهي نسخة مخزنة في بنية تحتية لطرف ثالث، وتخضع للقرارات التشغيلية والقانونية والتجارية لذلك الطرف الثالث. وليس لقرارات المهني.

ماذا يقول التشريع

اللائحة العامة الأوروبية لحماية البيانات واضحة في مادتها 32: يجب على أي شخص يعالج بيانات شخصية تنفيذ تدابير تقنية وتنظيمية "مناسبة" لضمان مستوى من الأمن يتناسب مع المخاطر. لا تُقاس ملاءمة التدابير من خلال "ما يقول التطبيق إنه يفعله"، بل من خلال المخاطر الحقيقية. إذا انتهى الأمر ببيانات العميل على خادم لا تضمن ولايته القضائية مستوى من الحماية يعادل مستوى المنطقة الاقتصادية الأوروبية، فإن المسؤول عن البيانات – أي المهني – يتحمل خطرًا ربما لا يدركه تمامًا.

وهي ليست فقط GDPR. السر المهني، الذي يتم تنظيمه بشكل خاص للمحامين والأطباء والأخصائيين النفسيين والمراجعين والصحفيين وغيرهم، يتطلب أن يكون التواصل مع العميل سريًا. ليس "سريًا قدر الإمكان". بل سريًا دون تحفظ. إذا كانت القناة التقنية المستخدمة لا تضمن ذلك، فإن المهني يتحمل مخاطرة لا تسمح بها أخلاقيات مهنته.

المفارقة هي أن الخطر غير مرئي. لا أحد يدقق في مراسلات المكتب. لا أحد يطلب عقد معالجة البيانات من مزود الدردشة. يظهر الخطر فقط عندما يفوت الأوان: تسريب، اختراق منشور، أمر قضائي تم تنفيذه في قارة أخرى دون إخطار المستخدم.

ما يحتاجه المهني تقنيًا

ما يحتاجه الشخص الخاضع للسرية هو في الواقع بسيط بشكل مدهش من وجهة نظر المتطلبات:

- قناة تذهب فيها الرسائل مباشرة من جهاز المرسل إلى جهاز المستلم، دون المرور عبر خادم وسيط يخزن النسخ.
- بنية تحتية تتوافق ولايتها القضائية وسياساتها مع GDPR من خلال التصميم، وليس من خلال التصريح.

- طريقة للتعريف مع المحاور دون الحاجة إلى تسليم جهات الاتصال المهنية (أسماء العملاء، أرقام الهواتف، دفتر العناوين) لأطراف ثالثة.
- نظام قابل للتحقق – لا يعتمد على قول المزود – لتأكيد وصول الرسالة إلى الشخص الصحيح.

هذه ليست قائمة متطلبة. إنها في الواقع ما كان يُعتبر أمرًا مفروغًا منه في التواصل المهني قبل الرقمي. كان البريد المسجل يفي بكل هذه المعايير. والمكالمة الهاتفية من بدالة المكتب إلى بدالة العميل كذلك. الغريب ليس أن هذه الضمانات مطلوبة اليوم: الغريب هو أنها فقدت عند الانتقال إلى القناة الرقمية، دون أن يلاحظ أحد.

الفرق بين التشفير وعدم التخزين

هناك استعارة مفيدة. تشفير رسالة وتخزينها على خادم يعادل وضع مستند في خزنة وترك الخزنة في منزل شخص غريب. الخزنة جيدة. المستند لا يمكن قراءته من حيث المبدأ. لكن المستند *لا يزال في منزل شخص آخر*. وهذا الشخص يمكنه تلقي أمر قضائي، أو التعرض لهجوم إلكتروني، أو تغيير شروط الخدمة الخاصة به، أو أن تشتريه شركة أخرى بأخلاقيات مختلفة، أو قد يختفي غدًا.

البديل الهيكلي – ليس إجرائيًا، وليس قائمًا على الثقة – هو ألا يغادر المستند المكتب أبدًا. أن ينتقل مباشرة من مكتب المهني إلى مكتب العميل دون أي وسيط على الإطلاق. وهذا ما يفعله التواصل من نقطة إلى نقطة بين الأجهزة تقنيًا: إنه يلغي الوسيط. ليس لأن الوسيط شرير. بل ببساطة لأن الوسيط في حالة السر المهني *غير ضروري*. وغير الضروري يجب، في أي نظام يطمح لأن يكون آمنًا، أن يلغى من حيث المبدأ.

مسألة المسؤولية

في نهاية المطاف، السؤال الذي يجب أن يكون كل مهني لديه واجب السرية قادرًا على الإجابة عليه بنعم قاطعة هو التالي:

> إذا تم تسريب محادثة مع أحد عملائي غدًا وسألتني محكمة أو هيئة مهنية عن كيفية إدارتي للسرية، فهل يمكنني إثبات تقنيًا أن القناة التي استخدمتها لا تخزن نسخًا في البنية التحتية لأطراف ثالثة؟ هل يمكنني إثبات أن البيانات لم تغادر أبدًا أجهزة الشخصين المشاركين في المحادثة؟ هل يمكنني، دون الاعتماد على قول شركة من قارة أخرى، إثبات أن السرية كانت مضمونة بالبناء المعماري وليس بالوعد؟

إذا كانت الإجابة لا، فالمشكلة ليست في الأداة بشكل ملموس. المشكلة هي أنه تم تفويض مسؤولية لأداة لم يتم تصميم الأداة لدعمها. إنه مثل وضع ملفات سرية في مظروف شفاف والثقة في أن ساعي البريد لن ينظر للداخل.

الأداة التي يختارها المهني للتواصل مع عملائه تقول الكثير عن كيفية تقديره لثقتهم. هناك أدوات مصممة بحيث لا تعتمد تلك الثقة على الوعود، بل على البناء المعماري. وهناك أدوات ليست كذلك. معرفة الفرق هو جزء من العمل.

الإطار المعياري المذكور

- اللائحة (الاتحاد الأوروبي) 2016/679 (GDPR)، وبشكل خاص المواد 5 و 25 (حماية البيانات بالتصميم) و 32 (أمن المعالجة).
- التشريعات المحلية بشأن السر المهني (مثل قوانين ممارسة المحاماة، وقوانين حماية حقوق المريض، واللوائح المهنية للأطباء).
- قوانين العقوبات المحلية المتعلقة بإفشاء الأسرار المهنية.
- المواثيق الأخلاقية للنقابات المهنية فيما يتعلق بالسرية والسر المهني.

← السابقالتشفير لا يعني الخصوصية: ماذا تقول البيانات الوصفية عنكالتالي → GDPR والمراسلات المهنية: لماذا ينتهك معظم الناس القواعد دون علمهم

قراءات حديثة

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

خذ هذا المقال معك أينما احتجت إليه.

↓ ماركداون ↓ نص عادي ↓ PDF

سيتم تنزيل الملف على جهازك. من هناك يمكنك حفظه، أو استيراده إلى Solo2 أو مشاركته أينما تريد. Cuadernos لا تقرر الوجهة نيابة عنك.

ختم شمعي · SHA-256 e772632501b8bab21c65087e119b24e64bd8b0699ae99667ce0f706405599ad5

Cuadernos Lacre · منشور لشركة Menzuri Gestión S.L. ·
بقلم R.Eugenio · تحرير فريق Solo2.