# رازداری حرفه‌ای در عصر دیجیتال

وقتی ارتباط بین متخصص و مشتری او از طریق یک کانال از نظر فنی نامناسب انجام شود، راز در روز لو رفتن فاش نمی‌شود. خیلی زودتر، در لحظه انتخاب ابزار فاش شده است.

## مشکلی که تقریباً هیچ‌کس نمی‌بیند

یک وکیل روی گوشی خود سندی محرمانه از یک مشتری دریافت می‌کند. یک پزشک با یک همکار درباره تشخیص حساس بحث می‌کند. یک روانشناس با یک روانپزشک درمان یک بیمار را هماهنگ می‌کند. یک مشاور مالیاتی داده‌های اظهارنامه‌ای را که منتظر بازبینی است می‌فرستد. همه این کارها را از طریق پیام‌رسان‌های فوری انجام می‌دهند. و تقریباً هیچ‌کس مکث نمی‌کند تا فکر کند که آن پیام‌ها واقعاً به کجا ختم می‌شوند.

پاسخ در اکثر موارد یکسان است: روی سروری که متخصص بر آن کنترلی ندارد، در کشوری که لزوماً قوانین آن را نمی‌شناسد، تحت مدیریت شرکتی که مدل تجاری آن – در اصطلاح اقتصادی مستقیم – انباشت داده است. پیام ممکن است در حین انتقال رمزنگاری شده باشد. اما به محض رسیدن به سرور، این یک کپی ذخیره شده در زیرساخت شخص ثالث است که تحت تأثیر تصمیمات عملیاتی، قانونی و تجاری آن شخص ثالث قرار دارد. نه متخصص.

## قانون چه می‌گوید

مقررات عمومی حفاظت از داده‌های اروپا در ماده ۳۲ خود صریح است: هر کسی که داده‌های شخصی را پردازش می‌کند باید اقدامات فنی و سازمانی «مناسب» را برای تضمین سطح امنیتی متناسب با ریسک اجرا کند. تناسب اقدامات با «آنچه اپلیکیشن ادعا می‌کند انجام می‌دهد» سنجیده نمی‌شود، بلکه با ریسک واقعی سنجیده می‌شود. اگر داده‌های مشتری به سروری ختم شود که حوزه قضایی آن سطح حفاظتی معادل منطقه اقتصادی اروپا را تضمین نمی‌کند، مسئول داده‌ها – یعنی متخصص – ریسکی را می‌پذیرد که احتمالاً کاملاً از آن آگاه نیست.

و این فقط GDPR نیست. رازداری حرفه‌ای که به طور خاص برای وکلا، پزشکان، روانشناسان، حسابرسان، روزنامه‌نگاران و دیگران تنظیم شده است، ایجاب می‌کند که ارتباط با مشتری محرمانه باشد. نه «تا حد امکان محرمانه». بلکه محرمانه بدون قید و شرط. اگر کانال فنی مورد استفاده نتواند این را تضمین کند، متخصص ریسکی را می‌پذیرد که اخلاق حرفه‌ای او اجازه پذیرش آن را نمی‌دهد.

پارادوکس اینجاست که ریسک نامرئی است. هیچ‌کس پیام‌رسانی دفتر را ممیزی نمی‌کند. هیچ‌کس قرارداد پردازش داده‌ها را از ارائه‌دهنده چت نمی‌خواهد. ریسک تنها زمانی آشکار می‌شود که خیلی دیر شده است: یک لو رفتن، یک نفوذ منتشر شده، یک حکم دادگاه که در قاره‌ای دیگر بدون اطلاع کاربر اجرا شده است.

## یک متخصص از نظر فنی به چه چیزی نیاز دارد

آنچه یک فرد دارای وظیفه رازداری به آن نیاز دارد، از نظر الزامات در واقع به طور شگفت‌انگیزی ساده است:

- کانالی که در آن پیام‌ها مستقیماً از دستگاه فرستنده به دستگاه گیرنده می‌روند، بدون عبور از سرور واسطه‌ای که کپی‌ها را ذخیره می‌کند.

- زیرساختی که حوزه قضایی و سیاست‌های آن از طریق طراحی با GDPR همسو باشد، نه از طریق ادعا.
- روشی برای شناسایی با مخاطب بدون نیاز به تسلیم مخاطبان حرفه‌ای (نام مشتریان، شماره تلفن‌ها، دفترچه تلفن) به شخص ثالث.
- یک سیستم قابل تأیید – نه بر اساس حرف ارائه‌دهنده – برای تأیید اینکه پیام به فرد صحیح رسیده است.

این یک لیست دشوار نیست. در واقع همان چیزی است که در ارتباطات حرفه‌ای پیش از دیجیتال بدیهی فرض می‌شد. یک نامه سفارشی تمام این معیارها را داشت. تماس تلفنی از مرکز تلفن دفتر به مرکز تلفن مشتری نیز همین‌طور. عجیب این نیست که امروزه این تضمین‌ها خواسته می‌شوند: عجیب این است که در انتقال به کانال دیجیتال بدون اینکه کسی متوجه شود، از دست رفته‌اند.

## تفاوت بین رمزنگاری و عدم ذخیره‌سازی

یک استعاره مفید وجود دارد. رمزنگاری یک پیام و ذخیره آن روی سرور معادل قرار دادن یک سند در گاوصندوق و گذاشتن گاوصندوق در خانه یک غریبه است. گاوصندوق خوب است. سند اصولاً قابل خواندن نیست. اما سند *همچنان در خانه فرد دیگری است*. و آن فرد می‌تواند حکم دادگاه دریافت کند، دچار حمله سایبری شود، شرایط خدمات خود را تغییر دهد، توسط شرکت دیگری با اخلاق متفاوت خریداری شود یا فردا ناپدید شود.

جایگزین ساختاری – نه رویه‌ای، نه بر اساس اعتماد – این است که سند هرگز دفتر را ترک نکند. اینکه مستقیماً از روی میز متخصص به روی میز مشتری سفر کند، بدون هیچ واسطه‌ای. این همان کاری است که ارتباط نقطه-به-نقطه بین دستگاه‌ها از نظر فنی انجام می‌دهد: واسطه را حذف می‌کند. نه اینکه واسطه بد باشد. فقط در مورد رازداری حرفه‌ای، واسطه *غیرضروری* است. و آنچه غیرضروری است باید در هر سیستمی که به دنبال امنیت است، از نظر اصولی حذف شود.

## مسئله مسئولیت

در نهایت، سوالی که هر متخصص دارای وظیفه رازداری باید بتواند با یک «بله» قاطع به آن پاسخ دهد، این است:

> اگر فردا گفتگویی با یکی از مشتریان من لو برود و دادگاه یا یک صنف حرفه‌ای از من بپرسد که چگونه محرمانگی را مدیریت می‌کنم، آیا می‌توانم از نظر فنی ثابت کنم که کانالی که استفاده کردم کپی‌ها را در زیرساخت اشخاص ثالث ذخیره نمی‌کند؟ آیا می‌توانم ثابت کنم که داده‌ها هرگز دستگاه‌های دو فرد شرکت‌کننده در گفتگو را ترک نکرده‌اند؟ آیا می‌توانم بدون تکیه بر حرف شرکتی از قاره‌ای دیگر، ثابت کنم که محرمانگی توسط معماری تضمین شده بود و نه با یک وعده؟

اگر پاسخ منفی است، مشکل به طور مشخص ابزار نیست. مشکل اینجاست که مسئولیتی به ابزاری واگذار شده است که ابزار برای پشتیبانی از آن طراحی نشده بود. این مثل قرار دادن پرونده‌های محرمانه در یک پاکت شفاف و اعتماد به این است که پستچی داخل آن را نگاه نخواهد کرد.

ابزاری که یک متخصص برای ارتباط با مشتریانش انتخاب می‌کند، حرف‌های زیادی درباره نحوه ارزش‌گذاری او برای اعتماد آن‌ها می‌زند. ابزارهایی وجود دارند که طوری طراحی شده‌اند که این اعتماد به وعده‌ها بستگی نداشته باشد، بلکه به معماری وابسته باشد. و ابزارهایی هستند که این‌طور نیستند. شناخت تفاوت، بخشی از کار است.

### چارچوب هنجاری ذکر شده

- مقررات (اتحادیه اروپا) 2016/679 (GDPR)، به ویژه مواد ۵، ۲۵ (حفاظت از داده‌ها از مرحله طراحی) و ۳۲ (امنیت پردازش).
- قوانین محلی درباره رازداری حرفه‌ای (مانند قوانین وکالت، قوانین حقوق بیمار، و مقررات حرفه‌ای پزشکان).
- قوانین کیفری محلی مربوط به افشای اسرار حرفه‌ای.
- منشورهای اخلاقی کانون‌های حرفه‌ای در رابطه با محرمانگی و رازداری حرفه‌ای.

← السابقرمزنگاری به معنای حریم خصوصی نیست: متادیتا درباره شما چه می‌گویدالتالي → GDPR و پیام‌رسانی حرفه‌ای: چرا اکثر مردم ندانسته قوانین را نقض می‌کنند

## قراءات حديثة

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

این مقاله را هر کجا که نیاز دارید همراه خود ببرید.

↓ مارک‌داون ↓ متن ساده ↓ PDF

فایل در دستگاه شما دانلود خواهد شد. از آنجا می‌توانید آن را ذخیره کنید، به Solo2 وارد کنید یا در هر کجا که می‌خواهید به اشتراک بگذارید. Cuadernos مقصد را برای شما تعیین نمی‌کند.

ختم شمعي · SHA-256 d31db087197dd2f9b4ecef6b5a6eed84eb364fbd076238c137010878759d6473

Cuadernos Lacre · نشريّة من Menzuri Gestión S.L. ·
كتبها R.Eugenio · حرّرها فريق Solo2.