# میزبانی شخصی به عنوان یک تمرین حرفه‌ای

سرور چیزی جز یک کامپیوتر نیست. سوال این نیست که آیا باید یکی داشته باشید یا نه، بلکه این است که داده‌های مشتریان شما کجا زندگی می‌کنند، چه کسی از آن‌ها نگهداری می‌کند و چه کسی در صورت خرابی مسئولیت را بر عهده می‌گیرد.

**برای اینکه متوجه منظور هم شویم:** داده‌های شما همیشه در کامپیوتر کسی زندگی می‌کنند: در کامپیوتر غولی که همه چیز را به او می‌سپارید، در یک کامپیوتر اجاره‌ای که خودتان مدیریت می‌کنید، یا در کامپیوتر خودتان. هرچه کنترل بیشتری بخواهید، مسئولیت بیشتری را می‌پذیرید. تفویض اختیار به یک شخص ثالث بزرگ آرامش‌بخش است اما سلب مسئولیت نمی‌کند: اطلاعات مال شماست —و مال مشتریانتان— و مسئول آن شما هستید.

## سوال بین ابر و زیرزمین

خوب است با خنثی کردن کلمه‌ای شروع کنیم که بدون دلیل می‌ترساند: سرور. سرور یک ماشین مرموز در یک اتاق سرد نیست. به سادگی کامپیوتر شخص دیگری —یا کامپیوتر خودتان— است که اطلاعات را ذخیره می‌کند و به کسی که درخواست می‌کند تحویل می‌دهد. برای دهه‌ها ما اطلاعات مشتریان خود را در یک پوشه، در یک فایل‌باکس، روی میز دفتر نگه داشتیم و هیچ‌کس به خاطر آن خوابش را از دست نداد. اطلاعات ترسناک نبود چون روی کاغذ بود؛ لازم نیست چون روی دیسک است هم ترسناک باشد.

«ابر» هم اثیری نیست. کامپیوتر یک شرکت است، تقریباً همیشه دور و تقریباً همیشه متعلق به دیگری. من این را ناخواسته روزی یاد گرفتم که با اطمینان از اینکه فایل‌هایم در Google Drive امن هستند، متوجه شدم که پوشه در کامپیوترم حاوی اسناد من نیست، بلکه حاوی میانبرهایی به اسنادی است که در جای دیگری زندگی می‌کردند. اگر آن جای دیگر تصمیم می‌گرفت تعطیل کند، قیمت را تغییر دهد یا اشتراک را لغو کند، آرامش من هم با آن می‌رفت. من وسایلم را نداشتم؛ اجازه دسترسی به آن‌ها را داشتم.

از همین‌جا پرسش این دفترچه زاده می‌شود، پرسشی که بیانش از پاسخ‌دادنش آسان‌تر است: داده‌های مشتریانت باید کجا زندگی کنند؟ و داده‌های خودت؟ گفتگوی عمومی آن را چنان مطرح می‌کند که گویی تنها دو پاسخ روبه‌روی هم وجود دارد — ابرِ سکوهای بزرگ یا اینکه خودت کار را به‌دست بگیری —، تقریباً مسئله‌ای جناحی. اما این دو راه نیستند: سه راه‌اند، و هیچ‌کدام عملِ ایمانِ کورکورانه نیست. اگر با تأمل خوانده شوند، ظرافت‌های بیشتری دارند و بیش از آنچه به‌نظر می‌رسد می‌طلبند.

## این به شما مربوط است، هر چه که می‌فروشید

آسان است که فکر کنیم محرمانگی موضوع وکلا، پزشکان یا روزنامه‌نگاران است و بقیه چیزی برای پنهان کردن ندارند. این یک اشتباه است، و از نوع گران‌قیمت آن. تقریباً هر کسب‌وکاری داده‌های مشتریان خود را که مشمول قانون است نگه می‌دارد و بسیاری، بدون اینکه بدانند، اطلاعاتی را نگه می‌دارند که بسیار حساس‌تر از آن چیزی است که به نظر می‌رسد.

یک مغازهٔ مبل‌فروشی نام و نشانی و تلفن خریدار را یادداشت می‌کند؛ اگر تسهیلاتی در کار باشد، اطلاعات مالی او را هم. یک شرکت بازسازی یا دکوراسیون عکس‌های داخل خانه‌های مشتریانش و نقشه‌های کامل مسکن آن‌ها را نگه می‌دارد. یک شرکت نظافتی با نقشه‌های دفترهایی که تمیز می‌کند سروکار دارد، که اغلب با رنگ‌ها و شماره‌هایی نشانه‌گذاری شده‌اند که می‌گویند کدام کارمند کجا، چه ساعتی و با کدام کلید وارد می‌شود. هیچ‌یک از

این‌ها چیز مهمی به‌نظر نمی‌رسد تا آنکه آدم از خود بپرسد برای چه کسِ دیگری ارزش دارد: آن نقشه‌های نظافت، اگر با چشمی دیگر دیده شوند، نقشهٔ کاملی است برای کسی که بخواهد برای دزدی وارد شود.

اینکه یک کسب‌وکار کوچک است یا اینکه مبل می‌فروشد به جای دفاع در دعاوی حقوقی، داده‌های آن را بی‌ارزش نمی‌کند و باعث نمی‌شود قانون در مورد آن متوقف شود. فقط باعث می‌شود صاحب آن تمایل داشته باشد کمتر به آن فکر کند. و کم فکر کردن به چیزی که مسئولیت شماست، دقیقاً همان جایی است که مشکلات شروع می‌شود.

## داده‌های شما کجا زندگی می‌کنند؟

این پرسش، در اساس، سه پاسخ دارد. و خوب است به یاد داشته باشیم که «داده‌ها» تنها پروندهٔ یک مشتری یا دستهٔ فاکتورها و پیش‌فاکتورها نیست: گفتگوهای تو با او هم هست — از طریق WhatsApp، از طریق یک سرویس گفتگوی حرفه‌ای، از طریق Solo2 —. سه پاسخی که در پی می‌آید درجات خلوص نیستند و نردبانی از خوب‌ها به بدها هم نیستند: سه شیوهٔ تقسیمِ همان یک چیزند، یعنی کنترل و مسئولیت.

**واگذاری همه‌چیز به یک ارائه‌دهنده.** این رایج‌ترین کار است و برای اکثریت تنها چیزی است که می‌شناسند. همه‌چیز را در Google Workspace یا Microsoft 365 می‌گذارم و یکسره به ارائه‌دهنده می‌سپارم. حق اشتراکم را می‌پردازم و دیگر به آن فکر نمی‌کنم. افراطی‌ترین شکل این کار سرویس‌هایی است که در آن‌ها حتی داده‌هایت را در اختیار نداری: برخی برنامه‌های صدور فاکتور ابری، مثلاً، فاکتورها و پیش‌فاکتورها را برایت نگه می‌دارند — و خیلی هم خوب کار می‌کنند —، اما اطلاعات در سیستم آن‌ها زندگی می‌کند نه در سیستم تو. تا وقتی پول می‌دهی، دسترسی داری؛ روزی که می‌روی، درمی‌یابی که بردنِ تاریخچهٔ خودت دشوار یا ناممکن است. نیمه‌گروگان‌نگه‌داشتن داده‌هایت برای بیش از یک ارائه‌دهنده دقیقاً همان چیزی است که مانع رفتنت به‌سوی رقیب می‌شود. در ازای راحتی، کنترل را تسلیم می‌کنم و — بی‌آنکه بلند بگویم — این حس را که دیگر مسئولیت با من نیست. اینجا نکته‌ای جا دارد که تقریباً هیچ‌گاه گفته نمی‌شود: واگذاری مترادفِ آمریکایی‌بودن نیست. می‌توانم همه‌چیز را با همان راحتی به یک ارائه‌دهندهٔ اروپایی بسپارم — مثلاً Infomaniak — و با یک حرکت بخش بزرگی از تردیدها دربارهٔ انتقال‌های بین‌المللی را که در «Schrems II» دیدیم حل کنم، بدون هیچ خودمیزبانی‌ای. مسئله ایالات متحده در برابر بقیهٔ جهان نیست: در همان واگذاری محض هم تصمیم‌هایی هست که اهمیت دارند.

**اجاره و مدیریت سرور خودتان.** من همان چیزی را دارم که Microsoft یا Google به من می‌دهند، اما خودم آن را راه‌اندازی می‌کنم. من یک سرور را نزد یک ارائه‌دهنده اروپایی —Hetzner, OVH, Scaleway— اجاره می‌کنم، نرم‌افزار آزاد (مثلاً Nextcloud برای فایل‌ها) نصب می‌کنم و خودم نتیجه را مدیریت می‌کنم. من کنترل واقعی به دست می‌آورم: می‌دانم چه چیزی در حال اجراست، کجا و چرا. اما ماشین هنوز در مرکز داده یک شخص ثالث است و بالاتر از همه، کسی که عواقب را تحمل می‌کند تغییر می‌کند. با تفویض اختیار، اگر چیزی شکست بخورد، کسی را دارید که سرزنش کنید. با مدیریت شخصی، به احتمال زیاد تقصیر با شما خواهد بود.

**داشتن آن روی کامپیوتر خودتان.** این گزینه‌ای است که تقریباً هیچ‌کس درباره آن نمی‌گوید و قلب این دفترچه است. شما برای میزبانی وسایل خود به یک سرور بزرگ که بیست و چهار ساعته در یک مرکز داده کلان روشن است نیاز ندارید. کامپیوتر دفتر شما در حال حاضر یک سرور است: به شما خدمت می‌کند. آن را در دفتر روشن می‌گذارید و از لپ‌تاپ در خانه مشتری یا از موبایل وقتی خانه هستید به آن متصل می‌شوید. ما آن را «کامپیوتر دفتر» می‌نامیم، نه «سرور»، اما دقیقاً همان کاری را انجام می‌دهد که دو گزینه قبلی انجام می‌دهند. کنترل حداکثری است و نزدیکی هم همین‌طور: داده‌های شما همان‌جایی است که شما هستید. طرف دیگر آن، بدون رتوش، این است که مسئولیت نیز حداکثری است. اگر برق قطع شود، هیچ تکنسین شیفت در نورنبرگ وجود ندارد: این به عهده شماست که فیوز را بالا بزنید. و برای اینکه آن کامپیوتر از بیرون قابل دسترسی باشد، به چیزی نیاز است که پلی بین لپ‌تاپ شما و آن بسازد. این جادو نیست و بهتر است قبل از انتخاب این مسیر آن را بدانید.

حتی لازم نیست رایانهٔ دفتر را دوباره به کار بگیرید: دستگاهی هست که دقیقاً برای همین کار ساخته شده است، یعنی NAS (سازندگانش Synology، QNAP و دیگران هستند). مانند تقریباً همهٔ آنچه در این Cuadernos دیده‌ایم، در درونش جادویی نیست: یک رایانهٔ تخصصی است، از همان نوع ماشینی که در یک مرکز داده اجاره می‌کردید، فقط با این تفاوت که برای ذخیرهٔ داده‌ها و عرضهٔ آن‌ها از طریق شبکه ساخته شده است، بدون نمایشگر و صفحه‌کلید. یک نمایشگر و صفحه‌کلید به آن وصل کنید تا یک رایانهٔ معمولی داشته باشید؛ نرم‌افزار مناسب را روی رایانهٔ شخصی‌تان نصب کنید تا یک NAS داشته باشید. تفاوت در این است که NAS از پیش آماده است. آن را می‌خرید، در خانه یا دفتر به برق می‌زنید و از آنِ شماست. هر ماه حق اشتراک نمی‌پردازید؛ یک‌بار پولش را می‌دهید و مال

شما می‌شود، مانند هر ابزار دیگری در کسب‌وکارتان. روشنش می‌کنید، خاموشش می‌کنید و اگر بخواهید آن را به جای دیگری می‌برید. و چون مال خودتان است، هیچ چیز مانع نمی‌شود که دو دستگاه داشته باشید —یکی در خانه و یکی در دفتر— یا سه دستگاه، با افزودن یکی در جایی امن، که با هم هم‌گام باشند: افزونگی از آنِ خودتان، بی‌آنکه به شخص ثالثی برای نگهداری‌اش وابسته باشید. میزبانی شخصی، در نهایت، یک چیز واحد نیست: ترکیبی است از دستگاه‌ها، مالکیت، مکان‌ها و نرم‌افزار.

اینجا ناگزیریم آنچه را می‌کنیم نام ببریم، و بی‌پرده می‌کنیم: در Solo2 این پل را خودِ برنامه می‌سازد. رایانهٔ دفترت تنها برای دستگاه‌های مورد اعتمادت در دسترس می‌ماند، و همیشه زیر رمزنگاری، و دیگر دستگاه‌هایت خودشان دوباره به آن وصل می‌شوند. وقتی مشتری‌ای با تو حرف می‌زند، این رایانهٔ توست — نه رایانهٔ یک شخص ثالث — که با مشتری حرف می‌زند. ما قطعی برق را حل نمی‌کنیم؛ پل را حل می‌کنیم. و ما تنها کس نیستیم: امروز برای تقریباً هر نیازی برنامه‌هایی هست — آزاد یا انحصاری — که دقیقاً همین را ممکن می‌کنند، یعنی داده‌ها روی دستگاه خودت باشند و از بیرون به آن‌ها برسی. کار ما یک نمونه است؛ آنچه مهم است ایده است، نه برند.

## افزونگی (Redundancy) یک ابرقدرت نیست

در اینجا یک اعتراض فوری مطرح می‌شود و معقول است: اگر من همه چیز را روی کامپیوتر دفترم داشته باشم، اگر خراب شود چه می‌شود؟ سوال خوبی است. پاسخ این است که شبکه امنیتی که ما نزد ارائه‌دهندگان بزرگ تصور می‌کنیم، متواضعانه‌تر —و قابل تقلیدتر— از آن چیزی است که به نظر می‌رسد.

وقتی داده‌هایم را در مرکز داده یک شرکت چندملیتی می‌گذارم، اعتماد می‌کنم که آن‌ها در چندین جا نسخه دارند. و احتمالا دارند: در مکان دوم، شاید در سوم. اما آن افزونگی بی‌نهایت نیست و بالاتر از همه متعلق به من نیست: همچنان یک هارد دیسک است که من صاحب آن نیستم، توسط کسی مدیریت می‌شود که من ایمانی به او دارم که تقریباً هرگز تأیید نمی‌کنم.

آن شبکه را خودم هم می‌توانم ببافم، و با یک مزیت تعیین‌کننده. سرویس روزانه من در کامپیوتر دفتر زندگی می‌کند. از آنجا یک نسخه رمزگذاری شده را در کامپیوتر یک شرکت دوست —یک همکار در حرفه، یک دفتر مورد اعتماد دیگر— نگه می‌دارم و یک نسخه رمزگذاری شده دیگر، اگر بخواهم، نزد همان ارائه‌دهنده اروپایی که درباره‌اش صحبت می‌کردیم. تفاوت در همه چیز است: آنچه من در بیرون می‌گذارم، سرویس من یا داده‌های آشکار من نیست، بلکه یک نسخه رمزگذاری شده است که فقط من می‌توانم باز کنم. ارائه‌دهنده بیرونی یک صندوق در بسته را نگه می‌دارد که کلید آن را ندارد. من اطلاعاتم را به او نمی‌سپارم: من چند بایت را به او می‌سپارم که بدون من هیچ معنایی ندارند.

## امن بود تا زمانی که دیگر نبود

اجازه دهید یک داستان شخصی تعریف کنم، زیرا این موضوع را بهتر از هر استدلالی نشان می‌دهد. برای بیش از ده سال من مشتری وفادار CrashPlan بودم، یک سرویس پشتیبان‌گیری که از نظر فنی فوق‌العاده بود. من از تمام کامپیوترهای خودم و خانواده‌ام —شرکتی و خانگی، همه چیز— در ابر آن‌ها پشتیبان می‌گرفتم، با نسخه‌هایی که می‌توانستم با هر فرکانسی که می‌خواهم بازیابی کنم و در زمان به یک فایل خاص از ماه‌ها قبل برگردم. بعد از اولین نسخه، فقط تفاوت‌ها را به صورت رمزگذاری شده و فشرده ارسال می‌کرد، به طوری که من یک پشتیبان عظیم را تقریباً بدون هیچ تلاشی به‌روز نگه می‌داشتم. بارها مرا نجات داد، از یک سند پیش‌پاافتاده تا یک دیسک کامل. قیمت در طول سال‌ها بالا رفت و برایم مهم نبود: با خوشحالی پرداخت می‌کردم.

چیزی که نمی‌دانستم این بود که CrashPlan در محاسبات اشتباه کرده بود: آن‌ها با قرارداد وعده فضای ذخیره‌سازی نامحدود، هم در فضا و هم در زمان را داده بودند. و فضا ضرب در زمان —سال‌ها تاریخچه، نسخه‌هایی در هر چند دقیقه— رشد می‌کند تا زمانی که ناپایدار شود. یک روز آن‌ها به همه ما اطلاع دادند که سرویس رو به پایان است. آن‌ها این کار را با ظرافت و با یک مهلت سخاوتمندانه، تقریباً یک سال، انجام دادند و وسایلی را برای دانلود داده‌هایمان در اختیار ما قرار دادند. اما یک نفر با بیش از ده سال نسخه‌های مختلف از تمام دیسک‌هایش کجا می‌رود؟ آنجاست که متوجه می‌شوید نه راهی برای دانلود همه چیز دارید و نه جایی برای گذاشتن آن، و حتی اگر می‌توانستید، هزینه انبار جدید گزاف می‌شد.

چهار چیزِ ضروری را نجات دادم. باقی وقتی کلید را خاموش کردند رفت. من آسوده بودم، اطلاعاتم در امان بود... تا آنکه دیگر نبود. و نه به‌خاطر خیانتی: CrashPlan رفتاری بی‌عیب داشت — برخلاف Evernote که سال‌ها بعد رفتاری شرم‌آور داشت —؛ به‌سادگی، فرشتهٔ نگهبانم در ابر، با تمام حق، تصمیم گرفت دیگر فرشتهٔ نگهبان نباشد. اما نتیجه برای من یکسان بود: آنچه امن می‌پنداشتم، ناپدید شد.

آنچه این داستان واقعاً می‌آموزد بیشتر با طبیعت انسانی در ارتباط است تا تکنولوژی. وقتی کسی احساس می‌کند چیزی مسئولیت اوست، به صورت پیشگیرانه عمل می‌کند: نسخه تهیه می‌کند، پشت خود را محکم می‌کند، با قضاوت درست تردید می‌کند. وقتی باور می‌کند —به اشتباه— که مسئولیت بر عهده یک شخص ثالث بزرگ و توانمند است، شل می‌شود و اجازه می‌دهد امور بگذرد. آن آرامش تفویض شده احتیاط نیست: بلکه بدون رتوش، شکلی از بی‌مسئولیتی است.

## پرداخت کردن به معنای رعایت مقررات نیست

آن بی‌مسئولیتی آرام بسیار شبیه والدینی است که پسرشان را در گران‌ترین مدرسه ثبت‌نام می‌کنند، بعد از آن هزینه مدرک کارشناسی ارشد او را می‌پردازند و با آن معتقدند که وظیفه خود را انجام داده‌اند. آن‌ها انجام نداده‌اند. والدین بودن یعنی نگران بودن از اینکه او امروز چه آموخته، چه چیزی را نمی‌فهمد، ارزش‌هایش، اعتماد به نفسش. اگر در بیست و پنج سالگی آن پسر بلد نباشد کار کند یا رفتار کند، تقصیر مدرسه‌ای نیست که پول را گرفته: تقصیر کسی است که تفویض اختیار کرده و با این باور که همین کافی است، پرداخت کرده است. پرداخت به شخص ثالث از مسئولیت سلب نمی‌کند. هرگز نکرده است.

با داده‌ها هم همین‌گونه است، و تاریخ نزدیک آن را تأیید می‌کند. پنجاه یا صد سال پیش یک حرفه‌ای چیزهای مربوط به مشتریانش را در پوشه‌هایی، در دفتر کارش یا در خانه‌اش، نگه می‌داشت و خود را مسئول آن‌ها می‌دانست. به‌ندرت چیزی گم می‌شد. به جهان دیجیتال گذر کرده‌ایم و، با سهولتی حیرت‌آور، همه‌چیز را در «ابر» بارگذاری می‌کنیم — که چیزی جز رایانهٔ یک شرکت چندملیتی نیست — و دیگر نگران نمی‌شویم. و اغلب حادثه‌ها رخ می‌دهند، و شرکت‌هایی هستند که همه‌چیز را از دست می‌دهند، و آنگاه گفته می‌شود: تقصیر Google بود، تقصیر Microsoft بود. نه. اطلاعات از آنِ توست، یا از آنِ مشتریانت، اما مسئول تویی.

میزبانی وسایل خودتان یک هوس فنی نیست: بازپس‌گیری آن آرامش دهه‌های پیش است، آرامش دانستن اینکه هر چیز کجاست و چرا. در این میان، حفاظت از داده‌ها نوسان ناگهانی پاندولی را تجربه کرده است —از نبود هیچ قانونی، زمانی که هر کسی بدون فکر داده‌های مشتری را به نمایش می‌گذاشت، تا الزامی که با سختی نامتناسب بر دوشِ کوچک‌ترین‌ها می‌افتد، فریلنسری که تلفن مشتری را به پیک می‌دهد. من در مورد هدف بحث نمی‌کنم؛ من ناهماهنگی را مشاهده می‌کنم. اما ناهماهنگی ما را تبرئه نمی‌کند: روزی که دولت ابزاری برای ردیابی و مجازات در مقیاس بزرگ داشته باشد، اندازه دیگر از کسی محافظت نخواهد کرد و عاقلانه است که با خانه‌ای نامرتب منتظر آن روز نمانیم. داشتن داده‌ها تحت کنترل خود به رعایت مقررات کمک می‌کند و به اثباتِ آن کمک می‌کند. و بالاتر از همه، چیزها را به جای خود برمی‌گرداند: وقتی اطلاعات مال شماست، مسئولیت کاملاً با شماست —هیچ شخص ثالثی برای سرزنش وجود ندارد، و نه شخص ثالثی که شکست او شما را در معرض خطر قرار دهد—.

## مسئولیت محافظت هم می‌کند

بی‌انصافی است که این را بدون سایه‌ها تصویر کنیم. نشستن به جای واسطه یعنی برداشتنِ بارِ او: نگه‌داشتن نسخه‌های پشتیبانِ به‌روز، اعمال به‌روزرسانی‌ها، و مسئولیتی قانونی — مسئولیت RGPD — که، در واقع، هیچ‌گاه به‌طور کامل از آنِ تو دست نکشید (مراجع پاورقی مواد مربوطه را شرح می‌دهند). کار هست، و روزی هست که چیزی در وقت نامناسب از کار می‌افتد. آن را پنهان نمی‌کنیم.

اما ترسی که آن واژه، مسئولیت، را در بر گرفته بد کالیبره شده است. خیلی آسان‌تر است که فایل‌هایت را در سرویس ابری‌ای که تعطیل می‌شود از دست بدهی، یا عکس‌هایت را در Google Photos، تا آن پوشهٔ مدارک مهمی را که روی رایانهٔ خودت داری: همان که می‌دانی کجاست و به‌محض ناپدیدشدنش متوجه نبودش می‌شوی. آنچه را از آنِ خود حس می‌کنی، از آن مراقبت می‌کنی؛ آنچه را در دست دیگری امن می‌پنداری، رهایش می‌کنی.

به آلبوم‌های عکس قدیم فکر کن، همان‌های کاغذیِ ظاهرشده که در کشویی نگه داشته می‌شدند. آیا هیچ‌گاه شنیده‌ای کسی بگوید آلبوم خانوادگی‌اش را «گم کرد»؟ از خانه‌ای که سوخت و آلبوم درونش بود شنیده می‌شود؛

اما گم‌کردنش همین‌طوری، نه. و در عوض، کسانی که همهٔ عکس‌هایشان در Google Photos یا Apple Photos بود و چیزی برایشان نماند: این داستان هر چند ماه یک‌بار برمی‌گردد، چون گمان می‌کردند در امان است. Google Photos از عکس‌هایت مراقبت می‌کند، البته که می‌کند؛ اما نه آن‌گونه که پدر و مادری از آلبومی مراقبت می‌کنند که فرزندان و نوه‌هایشان در آن‌اند. این تفاوت را هیچ مرکز داده‌ای درست نمی‌کند: مسئولیت، وقتی از آنِ تو باشد، تنها یک بار نیست؛ بهترین تضمین هم هست.

## چهار سوال قبل از تصمیم‌گیری

اگر در فکر برداشتن این قدم هستید، در هر شکلی از آن، خوب است ابتدا به چهار سوال با صداقت بی‌طرفانه پاسخ دهید:

1. از دست‌دادن یا نتوانستن بردنِ کدام بخش از داده‌هایت دردت می‌آورد؟ و مراقب باش آنچه را «روزمره» است دور نیندازی: تاریخچهٔ فاکتورها پیش‌پاافتاده‌ترین چیز دنیا به‌نظر می‌رسد تا آنکه برنامه را عوض می‌کنی و درمی‌یابی که آن فاکتورها از آنِ ارائه‌دهنده بودند، نه از آنِ تو — که، حداکثر، می‌توانی آن‌ها را در قالب PDF چاپ کنی، بی‌آنکه دیگر بتوانی درونشان جست‌وجو کنی —. مسئله تنها حساسیت نیست: مسئلهٔ این است که آنچه نیاز داری نگه داری، واقعاً از آنِ کیست.
2. کدام گزینه با توان فنی واقعی‌ات متناسب است؟ یک رایانهٔ شخصیِ خوب نگه‌داشته‌شده در دسترس هرکسی است؛ مدیریت یک سرور کامل، نه چندان. دربارهٔ آنچه می‌دانی و آنچه نمی‌دانی صادق باش. و به یاد داشته باش که میان برپاکردن یک سرور کامل و واگذاری همه‌چیز، زمینهٔ میانیِ بسیار معقولی هست: برنامه‌هایی — آزاد یا انحصاری — که داده‌هایت را روی دستگاه خودت نگه می‌دارند و می‌گذارند از بیرون به آن‌ها برسی. برای بسیاری بهترین تعادل است.
3. چه برنامه‌ای برای بدترین روز دارید؟ نقض داده‌ها، دیسکی که می‌میرد، ارائه‌دهنده‌ای که تعطیل می‌کند، تکنسین در مرخصی استعلاجی. اگر برنامه با «این نباید اتفاق بیفتد» شروع می‌شود، آن برنامه نیست.
4. آیا می‌دانید چگونه ثابت کنید که اگر فردا مورد ممیزی قرار گرفتید، رعایت مقررات می‌کنید؟ انجام درست کار و توانایی اثبات اینکه آن را درست انجام می‌دهید، یک چیز نیستند. قانون دومی را می‌خواهد.

پاسخ جهانی وجود ندارد. پاسخی متناسب وجود دارد که با صداقت در مورد آنچه به دست می‌آید و آنچه به ارث می‌رسد اتخاذ شده است. و بالاتر از تکنیک، یک یقین ساده وجود دارد: داده‌های شما در کامپیوتر کسی زندگی می‌کنند. تنها سوالی که واقعاً مهم است این است که می‌خواهید آن کامپیوتر متعلق به چه کسی باشد.

---

*میزبانی شخصی نه فضیلت است و نه رذیلت: ابزاری است با ردپای مشخصی از توانایی‌ها و مسئولیت‌ها. سوال هرگز این نبود که آیا داده‌های خود را میزبانی کنید یا خیر، بلکه این بود که چه داده‌هایی، چگونه و با چه شبکه حمایتی. بازپس‌گیری کنترل داده‌ها به معنای بازگشت به زیرزمین یا بی‌اعتمادی به همه چیز نیست: بلکه بازگشت به احساسِ مسئولیت نسبت به چیزی است که متعلق به ماست، درست مثل زمانی که آن داده‌ها در پوشه‌ای روی میز بودند. آن مسئولیت، اگر به درستی درک شود، خدمت واقعی است که یک حرفه‌ای به مشتریان خود ارائه می‌دهد.*

### منابع و مطالعه بیشتر

- مقررات (EU) 2016/679 — ماده ۲۸ (پردازشگر)، ماده ۳۲ (امنیت پردازش)، ماده ۳۳ (اطلاع‌رسانی نقض داده‌ها)، ماده ۳۷ (تعیین افسر حفاظت از داده‌ها).
- آژانس حفاظت از داده‌های اسپانیا — *راهنمای عملی برای تحلیل ریسک در پردازش داده‌های شخصی* (نسخه فعلی). چارچوبی برای کنترل‌گرانی که عملکردهای فنی خود را بر عهده می‌گیرند.
- شورای حفاظت از داده‌های اروپا — *دستورالعمل ۱/۲۰۲۴ در مورد پردازش داده‌های شخصی بر اساس منافع مشروع*. همچنین برای تست تناسب در تصمیمات زیرساخت شخصی قابل اعمال است.
- کمیسیون اروپا — دایرکتوری عمومی ارائه‌دهندگان خدمات اطلاعاتی مستقر در حوزه قضایی اروپا. نقطه شروع اداری برای شناسایی گزینه‌های میزبانی مدیریت شده اروپایی.
- Nextcloud GmbH (آلمان) — *معماری سازمانی Nextcloud و مستندات انطباق*. یک مورد مستند از نرم‌افزار آزاد با حالت‌های میزبانی شخصی و مدیریت شده توسط ارائه‌دهنده اروپایی؛ مفید به عنوان مرجع فنی پروژه‌ای که از سال ۲۰۱۶ در حوزه قضایی اروپا نگهداری می‌شود.

← السابق۲۴ کلمه: هویت رمزنگاری شده چیستالتالي → حریم خصوصی واقعی در مقابل ظاهری: سؤالاتی که باید از خود بپرسید

## قراءات حديثة

- تأمل · ۲۹ ژوئن ۲۰۲۶ شما ناشناس نیستید
- تامل · ۲۷ مۀ ۲۰۲۶ آنچه یک امضا نمی‌تواند اصلاح کند
- تحلیل · ۲۶ مۀ ۲۰۲۶ حریم خصوصی واقعی در مقابل ظاهری: سؤالاتی که باید از خود بپرسید

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 000c9e09fc9ebc9385c234ad3fd2a65db53a7a403f496495700a7fcba3602bcc



Cuadernos Lacre · نشریّة من Menzuri Gestión S.L. ·
کتبها R.Eugenio · حرّرها فریق Solo2.