分析 • 2026年5月25日

← 上一页 • 下一页 →

作为专业实践的自托管

服务器不过是一台电脑。问题不在于是否应该拥有一台, 而在于你客户的数据住在哪里，谁在维护它, 以及出问题时谁来承担责任。

明确一点： 你的数据始终住在某人的电脑里：在你把一切都托付给的那个巨头的电脑里、在你管理的租用电脑里，或者在你自己的电脑里。你想要的控制权越多, 你承担的责任就越大。委托给大型第三方能让人安心，但不能免责：信息是你的（也是你客户的），而负责人是你。

云与地下室之间的问题

最好从解构一个无端吓人的词开始：服务器。服务器并不是冷却室里某种神秘的机器。它仅仅是别人的——或者是你自己的——用来保存信息并将其交付给请求者的电脑。几十年来，我们把客户的信息放在文件夹里、档案柜里、办公室桌子上，没有人因此失眠。信息并没有因为它在纸上就变得可怕；它也不必因为它在硬盘上就变得可怕。

“云”也不是虚无缥缈的。它是一家公司的电脑，几乎总是在远方，几乎总是别人的。我是在那一天无意中得知这一点的：我曾深信我的文件在 Google Drive 中非常安全，却发现我电脑文件夹里装的不是我的文档，而是指向存放在别处的文档的快捷方式。如果那个“别处”决定关闭、改价或取消服务，我的宁静也会随之而去。我不拥有我的东西；我只是拥有访问它们的许可。

由此产生了这本 Cuaderno 的问题，它说起来比答起来容易得多：你客户的数据应该存放在哪里？你自己的数据呢？公众的讨论把它摆得好像只有两个针锋相对的答案——大平台的云，或者自己动手搭建——几乎像是一个选边站的问题。但路并非两条：有三条，而且没有一条是信仰之举。慢慢读来，它们各有更多的细微之处，所要求的也比看上去的更多。

这关乎你，无论你卖什么

很容易认为保密是律师、医生或记者的事，其余的人没有什么可隐瞒的。这是一个错误, 而且是一个代价高昂的错误。几乎任何企业都会保存受法律约束的客户数据，而且许多人在不知不觉中保存了比看起来敏感得多的信息。

一家沙发店记下购买者的姓名、地址和电话；如果有分期付款，还会记下他的经济资料。一家装修或室内设计公司保存着客户家中内部的照片和住宅的完整图纸。一家清洁公司经手着它所清洁的办公室的图

纸，这些图纸常常用颜色和数字标注，指明哪个员工在什么时间、用哪把钥匙进入哪里。这一切看上去都算不上什么大事，直到有人自问它对别的什么人还有价值：那些清洁图纸，换一双眼睛去看，对想要闯进去行窃的人来说，正是一张完美的地图。

一个生意规模小，或者卖的是沙发而不是在诉讼中辩护，并不意味着它的数据没有价值，也不意味着法律不再适用于它。它只会导致其所有者倾向于少去考虑这件事。而对自己责任范围内的某件事考虑太少，正是问题开始的地方。

你的数据住在哪里？

对这个问题，本质上有三个答案。而且值得记住的是，「数据」不只是某位客户的卷宗，或那一沓发票和报价单：它也包括你与他的对话——通过 WhatsApp，通过某项专业聊天服务，通过 Solo2。接下来的三个答案，既不是纯粹程度的高低，也不是一道从好到坏的阶梯：它们是分配同一样东西——控制权与责任——的三种方式。

把一切都交托给一家供应商。 这是最常见的做法，对大多数人来说也是他们所知道的唯一做法。我把所有东西都放进 Google Workspace 或 Microsoft 365，整个交托给供应商。我交我的费用，从此不再去想它。这种做法最极端的形态，是那些你甚至根本拿不到自己数据的服务：比如某些云端开票程序，替你保管发票和报价单——而且运转得非常好——但信息活在他们的系统里，而不是你的系统里。只要你在付费，你就能访问；等到你离开的那天，你才发现把自己的历史记录带走是困难的，甚至是不可能的。把你的数据半扣作人质，对不止一家供应商而言，正是那个让你无法转投竞争对手的东西。换来便利，我交出了控制权，还有——嘴上不说——那种责任已不再是我的的感觉。这里要补上一个几乎从来没人作出的细微之分：交托并不等同于美国式。我同样可以舒舒服服地把一切交托给一家欧洲供应商——比如 Infomaniak——并一笔勾销我们在「Schrems II」中所见的关于跨国传输的大部分疑虑，而无需自己托管任何东西。这并不是美国对抗宇宙其余的一切：在纯粹的交托之内，就已经有要紧的抉择了。

租赁并管理你自己的服务器。 我拥有 Microsoft 或 Google 会提供给我的同样的东西，但我自己来搭建。我从欧洲供应商（Hetzner、OVH、Scaleway）租赁一台服务器，安装自由软件（例如用于文件的 Nextcloud），并自己管理结果。我获得了真正的控制权：我知道什么在运行、在哪里运行以及为什么运行。但机器仍然在第三方的数据库中，而且最重要的是，承担后果的人变了。通过委托，如果出了问题，你有人可以责怪。通过自己管理，错误很可能就在你身上。

存放在你自己的电脑上。 这是几乎没有人说过的选项，也是本手册的核心。你不需要一个在巨型数据中心内二十四小时运行的庞大服务器来托管你的东西。你的办公室电脑本身就是一个服务器：它为你服务。你让它在办公室开着，然后你通过客户家的笔记本电脑，或者在家里通过手机连接它。我们称之为“办公室电脑”，而不是“服务器”，但它做的正是前两个选项所做的事情。控制权是最大的，近便性也是最大的：你的数据就在你所在的地方。直白地说，另一面是责任也是最大的。如果停电了，纽伦堡没有值班技术人员：得由你来合上电闸。为了让那台电脑能从外部访问，需要某种东西在你的笔记本电脑和它之间架起一座桥梁。这不是魔法，在选择这条道路之前了解这一点是件好事。

而且甚至不必把办公室那台电脑改作他用：有一种正是为此而设计的设备，即 NAS（由 Synology、QNAP 等厂商生产）。正如我们在这些 Cuadernos 中所见的几乎一切事物一样，它内部并没有什么魔法：它是一台专用的电脑，与你会在数据中心里租用的那种机器是同一类，只不过它是为存储数据并通过网络提供数据而设计的，中间没有显示器，也没有键盘。给它接上一块屏幕和一个键盘，你就得到了一台普通的电脑；在你的 PC 上装好合适的软件，你就得到了一台 NAS。区别在于，NAS 出厂时就已就绪。你把它买下来，在家里或办公室插上电源，它就是你的了。你不用每月付费；只需一次付清，它就属于你，就像你生意里的任何其他工具一样。你开机、关机，愿意的话还能带去别处。而且因为它是你的，没有什么能阻止你拥有两台——一台放在家里，一台放在办公室——或者三台，再在一处安全的地方添置一台，让它们彼此同步：这是你自己的冗余备份，无需指望第三方来维护。归根结底，自托管并不是单一的一件事：它是设备、所有权、地点与软件的组合。

这里无可避免地要点出我们所做的事，而我们毫不遮掩地这样做：在 Solo2 中，架起那座桥的正是应用程序本身。你办公室的电脑只对你信任的设备保持可访问，而且始终处于加密之下，你其余的设备会自行重新连上它。当一位客户与你交谈时，是你的电脑——而不是第三方的——在与客户交谈。我们解决不了停电；我们解决的是那座桥。而且我们并非唯一：如今几乎对每一种需求，都存在着这样的程序——自由的或专有的——它们让你正好能做到这一点：把数据留在你自己的设备上，并从外部访问它们。我们的不过是一个例子；要紧的是这个理念，而不是这个品牌。

冗余并不是超能力

这里立刻产生了一个反对意见，而且是合理的：如果我把一切都放在办公室电脑上，如果它坏了怎么办？问得好。答案是, 我们在大型供应商那里想象的安全网比看起来要更普通, 也更容易模仿。

当我把数据留在跨国公司的数据中心时, 我相信它在几个地方都有副本。而且很可能确实有：在第二个地点, 也许在第三个地点。但那种冗余并不是无限的, 而且最重要的是, 它不是我的：它仍然是一个我不拥有的硬盘, 由我寄予了（且几乎从未核实过的）信任的某人管理。

同样的一张网我自己也能织, 而且具有决定性的优势。我的日常服务就在办公室电脑上。从那里, 我在一家友好公司的电脑（一位同行、另一个值得信赖的办公室）上保存一份加密副本, 如果我愿意, 还可以在我们提到的那家欧洲供应商那里保存另一份加密副本。区别在于一切：我留在外面的既不是我的服务, 也不是我的明文数据, 而是一份只有我能打开的加密副本。外部供应商保管着一个他没有钥匙的锁着的箱子。我没有把我的信息托付给他：我把一些如果没有我就没有任何意义的字节托付给了他。

在失去安全之前，它一直很安全

请允许我讲一个个人故事，因为它比任何论点都能更好地说明这一点。十多年来，我一直是 CrashPlan 的忠实客户，这是一家技术上非常卓越的备份服务商。我把公司和家里的所有电脑、家人的电脑——所有的一切——都备份到他们的云端，我可以按自己想要的频率恢复版本，时间可以追溯到几个月前的特定文件。在第一次完整备份后，它只传输加密和压缩后的增量数据，这让我几乎不费吹灰之力就能保持庞大备份的更新。它救过我很多次，从一份微不足道的文件到整个硬盘。这些年来价格一直在上涨，我并不在意：我付钱付得很开心。

我不知道的是，CrashPlan 算错了一笔账：他们在合同中承诺了在空间和时间上都是无限的存储。空间乘以时间——多年的历史、每隔几分钟产生的版本——会一直增长，直到变得难以为继。有一天，他们通知我们所有人服务即将停止。他们做得很优雅，给了将近一年的宽限期，并给了我们下载自己数据的手段。但是，一个带着超过十年的所有硬盘版本备份的人能去哪里呢？那时你才发现，你既没有办法全部下载，也没有地方存放，而且即便你能做到，新仓库的费用也将是一笔巨款。

我抢救出了四样必不可少的东西。其余的，在他们关掉开关时就没了。我本来很安心，我的信息是安全的……直到它不再安全。而且并非因为背叛：CrashPlan 的表现无可挑剔——与 Evernote 恰恰相反，后者多年之后表现得令人不齿——很简单，我在云端的守护天使，行使着它全部的权利，决定不再当我的守护天使了。对我来说，结果是一模一样的：我以为安全的东西，消失了。

这个故事真正教给我们的是关于人性而非技术。当有人感到某件事是自己的责任时，他会采取预防性的行动：制作副本、确保护卫、以良好的判断力保持警惕。当他（错误地）相信责任由一个庞大且有实力的第三方承担时，他就会松懈，听之任之。那种委托出去的平静并不是谨慎：说白了，它是失职的一种形式。

付钱并不等于合规

那种静悄悄的失职非常像是一对父母, 他们把儿子送进最贵的学校, 之后再为他付一笔硕士学费, 并以此认为自己尽到了责任。他们并没有尽到责任。作为父母，意味着要关心他今天学到了什么，他不理解什么，他的价值观，他的自信。如果在二十五岁时, 那个儿子既不会工作也不懂礼貌，错不在收钱的学校：而在那个委托他人并因付了钱就相信已经足够的人身上。付钱给第三方并不能免除责任。从来都没有。

数据也是一样，近来的历史印证了这一点。五十年或一百年前，一位专业人士把客户的东西收在文件夹里，放在自己的办公室或家中，并为它们感到负有责任。很少有什么东西会丢失。我们进入了数字世界，并以惊人的轻易，把一切都上传到「云」——它不过是某家跨国公司的电脑罢了——然后不再操心。而事故频频发生，有些公司丢掉了一切，于是人们便说：是 Google 的错，是 Microsoft 的错。不。信息是你的，或是你客户的，但负责的人是你。

托管自己的东西并不是技术上的心血来潮：它是找回几十年前的那种宁静，那种知道每样东西在哪里以及为什么在那里的宁静。与此同时，数据保护经历了一次剧烈的摆动——从没有任何规则、任何人都会不加思索地展示客户数据的情况，摆动到了一种对最弱小者（比如把客户电话给快递员的自由职业者）也施加不成比例严苛要求的地步。我不争论目标；我观察这种失衡。但失衡并不能赦免我们：有一天，当行政部门拥有大规模追踪和制裁的手段时，规模将不再保护任何人，在房屋未打理好之前不等待那一天的到来是明智的。将数据置于自己的控制之下有助于合规，也有助于证明合规。最重要的是，它让事物回归原位：当信息是你的，责任就完全是你的——没有可以责怪的第三方，也没有其故障会导致你暴露的第三方。

责任同样也在保护

把这件事画得没有阴影，那是不诚实的。占据中间人的位置，意味着要扛起属于这个位置的担子：让备份保持更新，安装更新，以及一份法律责任——即 RGPD 的责任——而这份责任，其实从来就没有完全不再是你的（脚注里的参考资料详列了相关条款）。有活要干，也有某一天，某样东西在不合时宜的时候出了岔子。我们并不掩饰这一点。

但围绕「责任」这个词的那种恐惧，刻度校得不对。在一项关停的云服务里弄丢你的文件，或者在 Google 相册里弄丢你的照片，要比弄丢你自己电脑里那个装着重要文件的文件夹容易得多：那个你知道它在哪儿、一旦消失你立刻就会察觉到不见了的文件夹。你感到是自己的东西，你会照看；你以为在别人手里安然无恙的东西，你会疏忽。

想想从前的相册，那些冲洗出来、收在抽屉里的纸质照片的相册。你可曾听过有谁说自己「弄丢了」家庭相册？听得到的是房子连同相册一起烧掉了；至于就这么平白丢掉，没有。然而，那些把所有照片都放在 Google 相册或 Apple 相册里、结果什么都没剩下的人：这样的故事每隔几个月就会重演一次，因为他们以为照片是安全的。Google 相册照看你的照片，当然照看；但它照看的方式，不像一对父母照看那本装着他们子女和孙辈的相册。这个差别，没有任何一座数据中心能弥补：责任，当它是你的时，不只是一副担子；它也是最好的保障。

决定前的四个问题

如果你考虑迈出这一步，无论以何种形式，最好先心平气和且诚实地回答四个问题：

1. 你的数据里，哪一部分丢了、或带不走，会让你心痛？而且要当心，别把那些「例行」的东西打发掉：发票的历史记录看上去是世上最平淡无奇的东西，直到你更换程序，才发现那些发票是供应商的，而不是你的——你顶多能把它们打印成 PDF，却再也无法在其中检索了。这不只是敏感与否的问题：而是你需要保存的东西，究竟真正属于谁的问题。
2. 哪一个选项与你真实的技术能力相称？一台养护得当的自有电脑，谁都够得着；而管理一整台服务器，就没那么简单了。对自己懂什么、不懂什么，要诚实。还要记住，在自己搭起一整台服务器和把一切都交托出去之间，有一片非常合理的中间地带：那些程序——自由的或专有的——把你的数据保存在你自己的设备上，又让你从外部访问它们。对许多人来说，这是最好的平衡。
3. 你对最糟糕的一天有什么计划？数据泄露、硬盘损坏、供应商关闭、技术人员请病假。如果计划是以“这不应该发生”开头的，那它就不是计划。
4. 如果明天对你进行检查, 你知道如何证明自己是合规的吗？做好了和能证明自己做好了，并不是一回事。法律要求的是后者。

没有普适的答案。只有一种根据所获得的利益和所继承的责任而诚实采取的、成比例的答案。而在技术之上, 有一个简单的定论：你的数据住在某人的电脑里。唯一真正重要的问题是，你希望那是谁的电脑。

自托管既不是美德也不是恶习：它是一个带有具体能力和责任印记的工具。问题从来不在于是否应该托管你自己的数据，而在于托管什么数据、如何托管以及依靠什么样的支持网络。收回对数据的控制权并不意味着回到地下室，也不意味着对一切都充满疑虑：它是回归到对属于我们的东西感到负责，就像那

些数据还存放在桌上的文件夹里一样。这种责任感，如果被正确理解，正是专业人士为客户提供的真正服务。

来源及延伸阅读

- 法规 (EU) 2016/679 — 第 28 条（处理者）、第 32 条（处理安全）、第 33 条（漏洞通知）、第 37 条（指定数据保护官）。
- 西班牙数据保护局 — *《个人数据处理风险分析实用指南》*（现行修订版）。针对承担自身技术职能的控制者的框架。
- 欧洲数据保护委员会 — *《关于基于合法利益处理个人数据的 1/2024 指南》*。同样适用于自身基础设施决策中的比例性测试。
- 欧盟委员会 — 在欧洲管辖范围内设立的信息服务供应商公共名录。识别欧洲管理托管选项的行政起点。
- Nextcloud GmbH (德国) — *Nextcloud 企业架构和合规文档*。一个记录在案的自由软件案例，包含自托管和由欧洲供应商管理的模式；可作为自 2016 年以来在欧洲管辖范围内维护的项目的技术参考。

← 上一页24 个单词：什么是加密身份下一页 →真实隐私 vs 表象隐私：你应该问自己的问题

最近阅读

- 反思 · 2026年6月29日 你并不匿名
- 思考 · 2026年5月27日 签名无法解决的问题
- 分析 · 2026年5月26日 真实隐私 vs 表象隐私：你应该问自己的问题

随身携带本文，以备不时之需。

↓ Markdown ↓ 纯文本 ↓ PDF

文件将下载到您的设备中。您可以从那里将其保存、导入 Solo2 或在任何地方共享。Cuadernos 不会为您决定文件的去向。

火漆印章 · SHA-256 e1bc1845577984c3f5c1c3b1f17eb0237a455bc0ea827851461cfd5c297e970b

Cuadernos Lacre · Menzuri Gestión S.L. 的出版物 ·
由 R.Eugenio 撰写 · 由 Solo2 团队编辑。