思考 · 2026年5月16日

← 上一页·下一页 →

数字时代的职业秘密

当专业人士与其客户之间的沟通通过技术上不合适的渠道进行时，秘密并非在泄露之日被打破。在选择工具的那一刻，秘密就已经被打破了。

通俗地说： 律师通过 WhatsApp 发送客户的合同。医生通过 Telegram 评价诊断结果。没人觉得有什么奇怪。但职业秘密并不是在泄密发生的那天破裂的——而是在选择该通讯渠道的那一刻就已经破裂了。

几乎没有人意识到的问题

一名律师在手机上收到客户发来的机密文件。一名医生与同事讨论敏感的诊断结果。一名心理咨询师与精神科医生协调患者的治疗。一名税务顾问发送等待审计的申报数据。他们都在通过即时通信完成这些工作。几乎没有人停下来思考这些消息最终究竟去了哪里。

在大多数情况下，答案都是一样的：去往专业人士无法控制的服务器，去往其未必熟悉的法律管辖下的国家，由一家其商业模式——从直接经济角度而言——是积累数据的公司管理。消息在传输过程中可能被加密。但一旦到达服务器，它就是存储在第三方基础设施中的副本，受该第三方的运营、法律和商业决策支配。而非受专业人士支配。

法律规定

欧洲《通用数据保护条例》（GDPR）第 32 条规定得非常明确：任何处理个人数据的人必须采取“适当的”技术和组织措施，以确保与风险相适应的安全水平。措施是否适当不是根据“应用宣称其所做的”来衡量，而是根据实际风险来衡量。如果客户数据最终进入一个其司法管辖权无法保证与欧洲经济区同等保护水平的服务器，那么数据控制者——即专业人士——就承担了一个他可能并未完全意识到的风险。

而且这不仅仅是 GDPR 的问题。针对律师、医生、心理咨询师、审计师、记者等特定人群规定的职业秘密义务，要求与客户的沟通必须保密。不是“尽可能保密”，而是无条件的保密。如果所使用的技术渠道无法保证这一点，专业人士就承担了其行业道德所不允许的风险。

矛盾之处在于，风险是不可见的。没有人审计办公室的即时通信。没有人向聊天软件提供商索要数据处理合同。风险只有在为时已晚时才会显现：一次泄露、一次被公布的安全漏洞、一次在未通知用户的情况下在另一个大洲执行的法院命令。

专业人士在技术上需要什么

从需求的角度来看，负有保密义务的人所需要的其实非常简单：

- 一个消息能直接从发送者设备传输到接收者设备，而无需经过存储副本的中间服务器的渠道。
- 一个在设计上（by design）而非靠声明与 GDPR 保持一致司法管辖权和政策的基础设施。
- 一种在无需向第三方交付职业联系人（客户姓名、电话号码、通讯录）的情况下与对方进行身份识别的方法。
- 一个可验证的系统——而非基于服务商的言辞——来确认消息已送达正确的人员。

这并不是一份苛刻的清单。实际上，这在数字时代之前的职业沟通中是被视为理所当然的。一封挂号信就能满足所有这些标准。从办公室总机到客户总机的电话通话亦然。奇怪的不是今天要求这些保证，而是奇怪在向数字渠道过渡的过程中，这些保证在无人察觉的情况下丢失了。

“加密”与“不存储”的区别

有一个很有用的比喻。加密消息并将其存储在服务器上，相当于将一份文件放入保险箱，然后将保险箱留在陌生人家中。保险箱很好，文件原则上无法阅读。但文件*仍然在别人的家里*。而那个人可能会收到法院命令，可能会遭受网络攻击，可能会更改其服务条款，可能会被另一家具有不同价值观的公司收购，或者明天就可能倒闭。

结构性的替代方案——不是程序上的，也不是基于信任的——是文件从未离开办公室。文件直接从专业人士的桌面传输到客户的桌面，不经过任何中介。这正是设备间点对点通信在技术上所做的事情：它消除了中介。并不是说中介就是邪恶的。只是在职业秘密的情况下，中介是*多余的*。而在任何追求安全的系统中，多余的东西原则上都必须被消除。

责任问题

最终，每一位负有保密义务的专业人士都应该能够以响亮的“是”来回答以下问题：

> 如果明天我与某位客户的对话被泄露，而法院或专业协会询问我如何管理保密性，我能否从技术上证明我所使用的渠道没有在第三方基础设施中存储副本？我能否证明数据从未离开过参与对话的两个人的设备？我能否在不依赖于另一大洲某家公司言辞的情况下，证明保密性是由架构而非承诺来保证的？

如果答案是否定的，那么问题并不具体在于某个工具。问题在于将一项工具本身无法支持的责任委托给了该工具。这就像把机密卷宗放进透明信封，并相信邮递员不会看一眼一样。

专业人士选择与其客户沟通的工具，很大程度上说明了其对客户信任的重视程度。有些工具的设计初衷就是让这种信任不依赖于承诺，而是依赖于架构。而有些工具则不然。了解其中的区别是工作的一部分。

编者按： 当本 Cuadernos 提及公司或产品名称时，并非为了指责。这些产品的开发者所做的工作被数百万人使用和欣赏。我们指出的是结构性问题——是模式问题，而非品牌问题。品牌作为例子出现，是因为读者熟悉它们。

引用的监管框架

- 条例 (EU) 2016/679 (GDPR)，特别是第 5、25 条（从设计阶段开始保护数据）和第 32 条（处理安全）。
- 关于职业秘密的各国国内法律（如律师法、医疗伦理规章等）。
- 刑法及相关法规中关于泄露职业机密的规定。
- 关于保密和职业秘密的专业协会职业道德守则。

← 上一页加密不等于隐私：元数据揭示了您的哪些信息下一页 →GDPR 与专业即时通信：为何大多数人都在不知情中违规

最近阅读

- 分析 · 2026年5月18日 真实隐私 vs 表象隐私：你应该问自己的问题
- 分析 · 2026年5月18日 作为专业实践的自托管 (Self-hosting)
- 概念 · 2026年5月18日 24 个单词：什么是加密身份

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 c6e4364cd889e31d979c3c0ec08d864ecfc842cbeb04c595634842c96ae440e4

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