分析 · 2026年5月20日

← 上一页·下一页 →

自毁开关 (Kill switch) 与机构俘获

保留撤回可能性的保护承诺。只要开关存在，终究会有人按下它。

通俗地说： 例如，WhatsApp 可以随时删除你的消息。目前的合同并不禁止这一点，而且明天他们就可以更改合同。法院命令、新政策、政府要求——然后你发现这些消息从来都不真正属于你。

建立在撤回可能性之上的承诺

2017 年飓风“厄玛”期间，佛罗里达州的几位特斯拉车主发现，他们的汽车在收到制造商的远程更新后，续航里程突然增加了。他们并没有为此付费。电池一直具备提供这些里程的能力；制造商为了细分市场，决定不向客户开放。在紧急情况下，特斯拉临时激活了全部容量。紧急情况过后，又将其禁用。

新闻中描述的慷慨之举，仔细研读后其实是另一回事。车主从未真正拥有过他们付费购买的完整产品。制造商保留了一种技术能力——远程扩展或减少功能——并选择在那个特定案例中行使该能力以造福客户。他们本可以选择相反的做法。这个故事讲的不是善举，而是权力的架构。

本文探讨的就是这种架构。按照行业惯例，我们称之为 *kill switch*（自毁开关）：允许运营商远程禁用、修改或撤回用户已认为属于自己的产品、服务或设备功能的远程开关。问题不在于运营商是否诚实，而在于当他们不再诚实，或者有人强迫他们向另一个方向使用开关时，会发生什么。

到底什么是 kill switch

这个术语源自英语，翻译起来颇为困难：*interruptor de muerte*（死机开关）显得过于戏剧化；*interruptor remoto*（远程开关）又显得过于中性。定义 kill switch 的不是戏剧性，而是一个简单的属性：由使用者以外的人掌握的、从远程禁用某物的技术能力。它可以是完全关闭——无法启动的汽车、被删除的文件、被冻结的账户；也可以是部分关闭——消失的功能、缩短续航的电池、被中断的订阅。

并非所有的远程控制都是 kill switch。用户在安装产品时授权的常规安全更新就不是。所有者在手机被盗时可以自行激活的防盗系统也不是。从严格意义上讲，kill switch 具有三个特征：其使用由运营商而非用户决定；激活时不要求受影响者的即时同意；并且作用于用户已经认为完全属于自己的产品或服务。

欧洲现役开关博览

Tesla 经常重复这一模式，且在其案例中有据可查：对易主的二手车实施合同约定的续航降级，在许可证撤销后收回辅助驾驶功能，在不同固件版本之间单方面修改产品行为。多年来，John Deere 一直处于欧洲和美国关于维修权辩论的中心：购买拖拉机包含一个软件层，其服务依赖于制造商的官方网络；当该网络拒绝注册时，拖拉机会减少基本功能。BMW 在 2022 年曾提议通过月度订阅来激活已经物理安装在车内的座椅加热功能；公众压力迫使其撤回了该模式，但技术能力依然存在。

在软件层面，这种模式是结构性的。Adobe Creative Cloud 在订阅未续费时会撤回月度许可证，导致用户使用这些工具创建的文件无法使用。Microsoft 可以禁用其认为非正版的 Windows 副本，且用户没有实际的补救措施。Google 为执行法院命令或内部决定会从 Play Store 中移除应用程序；被卸载的应用程序也会从已安装的手机中消失。Apple Pay 于 2022 年 3 月在俄罗斯被禁用，因为 Apple 履行了国际制裁：在这种背景下是合法的，但该程序始终处于可用状态。

制造商方面的合法理由

设计这些系统的人通常会提供完全合理的论点：

1. **防止盗窃。** 如果我的汽车或手机被盗，我非常感激制造商能够从远程使其失效。
2. **防止欺诈。** 未付款的订阅需要一种切断机制；如果没有这种机制，商业模式就会崩溃。
3. **防止滥用。** 落入坏人之手的危险工具可以受益于能够被撤销的能力。
4. **合规性。** 某些法律命令迫使运营商删除内容、禁用功能或暂停账户，而没有开关的系统是无法遵守这些命令的系统。

这四个论点都是正确的。任何一个都没有改变事情的本质。kill switch 确实有利于防止盗窃；同样真实的是，这种能力也可以用来胁迫活着的客户，而不仅仅是损害小偷的利益。订阅模式确实需要一个切断机制；同样真实的是，由于合同规定以外的原因，明天就可以对现有客户执行切断。问题不在于 kill switch 是否具有合法用途。问题在于，一旦它存在，它的用途就不限于初始文件中预见到的那些。

制度俘获

这里引入了文章标题的概念。制度俘获（Institutional capture）是指一个参与者——私营公司、行政部门、监管机构——最终行使了它为有限目的而获得或被授予的能力，用于更广泛、不同或坦率地说与原始目的相反的目的。政治经济学在金融监管领域认识到这一现象已有数十年。科技行业正亲手发现这一点。

机制如下。公司出于合法目的设计 kill switch：防盗、订阅管理、合规。公司在其使用条款、隐私政策、公开信息中记录了这些目的。岁月流逝。政府根据新立法发布命令；公司被迫在一个其原始文件中未描述的方向上使用开关。一位激进股东进入董事会并修改商业政策；开关存在，并根据新政策应用。公司被更大的公司收购；服务条款被单方面重写，并提前三十天通知。在每种情况下，为了记录的目的而信任开关的客户发现，开关仍然在那里，但它响应的是其他利益。

欧洲读者的典型案例：2016年 San Bernardino 的 Apple 对 FBI 案。在加利福尼亚发生袭击事件后，FBI 要求 Apple 解锁肇事者的 iPhone。Apple 拒绝了，部分基于原则论点，部分基于技术论点：系统在设计

上不允许公司自己在不重写基础软件的情况下解锁设备。最坚固的防御不是道德上的，而是架构上的。Apple 不依靠不按下开关的承诺；它依靠开关的不存在。其他在架构中存在开关的公司，在同等压力面前无法维持同样的立场。

欧洲监管轨迹

在上一届立法任期内，欧洲法律一直在推动更多的远程控制能力，而非更少。自2024年2月起全面实行的《数字服务法案》（DSA）要求平台必须能够根据主管部门的命令启用快速内容移除机制；如果没有底层的技术能力，这些机制就不可能存在。自2024年8月起分阶段生效的《人工智能法案》（AI Act）要求某些高风险人工智能系统的提供者必须具备允许其停用或进行重大人工监管的措施：这是一种强制性 kill switch 的监管形式。相比之下，《数字市场法案》（DMA）引入了互操作性义务：这是一股限制锁定效应的反向潮流。

对于欧洲专业人士来说，诚实的理解应该是：由于法律要求，针对“运营商能否为我停用此服务？”这一问题的肯定回答每年都在增加，而非减少。这并不是在质疑监管的合法性——DSA是为了解决现实问题——但它确实强化了一点：相信运营商不会使用开关，还需要额外相信未来任何法律义务都不会强迫其在当今尚未预见的领域使用开关。这种信任不仅取决于公司，还取决于整个监管环境。

极少被提出的设计问题

大多数当代的技术设计都假设开关将存在，然后承诺不滥用它。存在另一种选择，虽然要求更高但完全可行：在假设开关不应存在的前提下进行设计。这不是一个口号。它意味着具体的决策：分布式架构而非中心化架构、用户设备上的权利而非源自账户的权利、使用运营商不掌握的密钥加密内容而非使用运营商保留的密钥加密内容、用户的加密身份而非由运营商管理的身份。每一个决策都有实际的技术成本和商业后果。但它们都有一个共同的特性：一旦做出决策，它们就消除了将某些法律命令作为可行对象的可能性。无法执行的事情，就无法命令执行。

致专业读者

在采用任何关键专业服务之前，应向提供商提出的五个问题，这些问题的顺序按照业务连续性检查员提出的顺序排列：

1. 供应商是否具备远程暂停、阻止、删除或降级我的服务、数据或产品的技术能力？
2. 在哪些合同声明的情况下，供应商可以行使该能力？
3. 在哪些未声明的情况下——司法命令、国际制裁、单方面政策变更、公司收购——他们也可能行使该能力？
4. 如果行使该能力，我有多少专业活动持续时间，以及有哪些退场计划可用？
5. 是否存在一种架构方案，使得问题一的答案是因为结构设计而非承诺而为“不”？

第五个问题的答案并不总是可用或成比例的。个人电子表格可能不值得提出这种要求。但一份活跃的法律文件、一名患者的病历、税务会计、一段受职业道德保护的对话，则需要。比例性是一项专业决策；

对第一个问题的诚实解读则不是：要么开关存在，要么不存在。

保留撤回可能性的保护不是结构性保护；它是更名后的信任。正如我们在另一本《笔记本》中提到的，信任在授予值得信任的人时是一种有效的社会解决方案，但在第一次转手时它是脆弱的。最干净的结构性防御是无法撤回的防御，因为它从一开始就不存在。正如建筑中的所有事物一样：这是一种设计选择，而不是营销决策。

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。

来源及延伸阅读

- 特斯拉 — 2017年9月的更新，在飓风艾尔玛期间暂时扩大了佛罗里达州S型和X型车的电池续航里程。这一案例在专业媒体以及随后关于合同续航里程撤销的报告中得到了广泛记录。
- 欧盟《数字服务法》(DSA) 2022/2065 — 自2024年2月17日起全面适用。第16条和第9条，关于通知与行动机制以及主管当局的命令。
- 欧盟《人工智能法案》(AI Act) 2024/1689 — 自2024年8月1日起生效，分阶段实施至2026年8月。关于高风险系统的人力监督和强制性缓解措施的条款。
- 美国地方法院 — Apple, Inc. (2016年2月16日)。关于刑事调查中获取 iPhone 访问权的“圣贝纳迪诺”案件文件。
- 美国联邦贸易委员会 (FTC) — 关于维修权 (2021-2024) 的备忘录，特别提到了约翰迪尔 (John Deere) 和农业部门；并由关于促进商品维修的欧盟指令 (EU) 2024/1799 补充。

← 上一页SHA-256 究竟是什么下一页 →端到端加密，真正的原理解析

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。

火漆印章 · SHA-256 f1b723b0c1bc1d33368119c03ced4f3dc17fc1fd847c341199abbc319d30dfcd

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

本网站不使用 Cookie，不加载第三方资源。使用自托管的匿名访问计数器（位于我们欧洲服务器上的 Umami）和用于页眉两个控制项（亮色或暗色主题，以及语言选择器）所需的最小 JavaScript。无追踪器，无用户画像，无数据共享。如果您想关注我们：RSS。