深度解读《政务数据共享条例》

《政务数据共享条例》已于 5 月 28 日发布，2025 年 8 月 1 日起施行。这是一件大事，将全面提升政府数字化治理能力和政务服务效能。也正是由于这事非常重要，有必要深度解读一下这个重要的条例(以下简称条例)。

一、 出台《条例》的必要性和重要性

《条例》的发布，旨在构建全国一体化政务大数据体系，推动数据资源融合应用，赋能社会治理和产业生态发展。该条例通过明晰权责、规范共享流程，重点解决跨层级、跨地域、跨系统的数据壁垒问题，同时强调数据安全与高效利用并重。

《条例》的发布，填补了法规的空白，强制破除政府部门数据垄断，并且厘清了权责和防控安全风险，将提升政府治理能力，优化政务服务效能，激活数据要素价值，构建数字治理新范式。

二、 防止政务数据被篡改、破坏、泄露，只有 HTTPS 加密才能做到

《条例》第三条定义了何为“政务数据共享”，是指政府部门因依法履行职责需要，使用其他政府部门的政务数据或者为其他政府部门提供政务数据的行为。属于政府部门之间的政务数据共享，这个共享就是甲部门的政务数据会通过网络方式共享给乙部门，所以，第三十五条要求政府部门应当采取技术措施和其他必要措施，防止政务数据被篡改、破坏、泄露或者非法获取、非法利用。

那么，采取何种技术措施和必要措施才能防止政务数据在网络传输过程中不会被非法篡改和泄露呢？这个条例中并没有指出，但是稍有网络安全常识的读者一定能正确给出答案，那就是 HTTPS 加密技术。HTTPS 加密技术是唯一一个能保障数据传输安全的技术，只需数据提供方的 Web 服务器支持 HTTPS 加密，则数据需求方就可以使用 HTTPS 方式安全地获取数据。这个技术方案是最简单和最省钱的解决方案，政府部门无需为了数据共享而采购专门的数据加解密设备，只需在数据提供 Web 服务器上部署 SSL 证书即可，如果已经部署了 SSL 证书，则无需做任何额外操作和额外投资，就能保障共享数据的传输安全，确保政务数据在共享传输过程中不会被非法篡改，不会被非法窃取而泄露。

但是，如果采用 HTTP 明文传输协议，则是非常容易被非法篡改和非法窃取的。如果数据

提供方不能以 HTTPS 加密方式为数据需求方提供数据共享服务，则数据传输安全失职方是数据提供方。而如果数据需求方不以 HTTPS 加密方式访问数据提供 Web 服务器获取数据，则数据传输安全失职方是数据需求方。而如果数据提供方设置数据提供服务为强制 HTTPS 方式，则双方都不会有责任，因为双方只能通过 HTTPS 加密方式实现政务数据共享。

三、 只有实现 SSL 证书自动化管理，才能可靠地实现 HTTPS 加密

要实现 HTTPS 加密，必须在 Web 服务器上部署 SSL 证书，这本不是难事，也不费几个钱。但是，为了保障 HTTPS 加密安全，国际标准已于 5 月 16 日制定了逐步缩短 SSL 证书有效期的时间表，从 2026 年 3 月 15 日开始，SSL 证书有效期缩短为 200 天，2027 年 3 月 15 日起缩短为 100 天，2029 年 3 月 15 日起缩短为 47 天。这个强制标准给实现 HTTPS 加密大大增加了实施难度，不能每个月去 CA 申请 SSL 证书并人工部署到 Web 服务器上。

怎么办？唯一解决方案只有实现 SSL 证书自动化管理，就是自动化为数据提供 Web 服务器申请和部署 SSL 证书，自动化实现 HTTPS 加密。全球范围内已经有超过 80%的网站系统已经实现了 SSL 证书自动化管理，但是这是国际算法 SSL 证书的自动化，需要在 Web 服务器上安装一个第三方客户端软件才能实现 SSL 证书的自动化申请和部署。我国需要满足《密码法》《网络安全法》和《数据安全法》，以及《互联网政务应用安全管理规定》等法律法规的要求，采用商用密码技术来实现 HTTPS 加密，从而切实保障 HTTPS 加密技术的安全实施。这就是为何第三十四条要求政务数据共享主管部门应当会同同级网信、公安、国家安全、保密行政管理、密码管理等部门共同推进政务数据共享安全管理制度建设。

也就是说，必须在 Web 服务器上部署国密 SSL 证书实现商用密码算法的 HTTPS 加密，这就要求 Web 服务器改造以支持商用密码算法，只有这样才能真正实现可靠的政务数据共享，才能真正保障政务数据共享的数据传输安全，因为国际上已经发生过 RSA 算法 SSL 证书被断供和被吊销的安全事件，只有采用我国 CA 签发的国密 SSL 证书才能真正保障政务数据共享的安全。

四、 微改造的国密 HTTPS 加密自动化解决方案才是最佳选择

要实现政务数据共享 Web 服务器的 HTTPS 加密，需要解决两大技术难题：一是国密 SSL 证书的自动化管理，二是 Web 服务器的国密算法支持，这就是大家常听到的国密改造难，因为整合 IT 系统生态都只默认支持 RSA 密码体系，不支持国产密码体系。

零信技术历时三年多打造了国密 HTTPS 加密自动化管理解决方案，这是一个原 Web 服务

器零改造的方案，只需在政务数据提供 Web 服务器前面部署国密 HTTPS 加密自动化网关即可，由网关来实现国密 SSL 证书和国际 SSL 证书的自动化申请和自动化部署，自动化实现自适应密码算法的 HTTPS 加密，政务数据需求部门的数据获取服务器就可以以国密 HTTPS 加密方式获取位于网关后的数据提供服务器的政务数据，数据提供方无需考虑如何向 CA 申请 SSL 证书和安装 SSL 证书，只需专注于搞好政务数据共享管理工作即可。

零信技术国密 HTTPS 加密自动化管理解决方案是一个端云一体的解决方案，国密 HTTPS 加密自动化网关会自动化连接零信云 SSL 服务系统，自动化为网站系统申请和部署双算法 SSL 证书，自动化实现国密 HTTPS 加密，只要数据获取服务器上的数据获取程序已国密 HTTPS 加密方式连接数据提供服务器即可，真正采用国密算法实现 HTTPS 加密数据安全传输，不怕国际 SSL 证书断供，因为默认配置的国际 SSL 证书仅用于不支持国密算法的 HTTPS 连接。

最后总结一下，要想落实《条例》要求的安全保障措施，防止政务数据被篡改、破坏、泄露或者非法获取、非法利用，唯一可行的技术措施就是为数据提供服务器实现国密 HTTPS 加密，而实现国密 HTTPS 加密唯一可行的解决方案只有部署国密 HTTPS 加密自动化网关，零改造自动化实现 HTTPS 加密和 WAF 防护，自动化满足相关法律法规的安全保障要求，真正落实《条例》，推进政务数据安全有序高效共享利用，提升政府数字化治理能力和政务服务效能。

王高华

2025 年 6 月 9 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 215 篇(共 63 万 7 千多字)和英文 92 篇(12 万 3 千多单词)。