Open Journal of Legal Science 法学, 2023, 11(5), 3355-3359
Published Online September 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.115479

Hans汉斯

浅析政务数据开放下的数据安全法律问题

胡瑞竹

贵州大学公共管理学院，贵州 贵阳

收稿日期：2023年6月2日；录用日期：2023年6月20日；发布日期：2023年8月24日

摘　要

政务数据作为社会生产的新兴要素与信息载体，进入开放环境中政务数据的安全保障必然会显得更加艰巨。随着数据重要性和价值的愈加凸显，政务数据开放所面临的数据安全风险逐渐上升，对政务数据安全立法需求越发迫切。本文将以政务数据开放的现状为背景，梳理总结现在政务数据开放面临的安全问题，分析加强立法的必要性以及完善建议，以便更好地提高数据安全意识。

关键词

数据开放，政务数据，数据安全

Analysis on the Legal Issues of Data Security under the Opening of Government Data

Ruizhu Hu

School of Public Administration, Guizhou University, Guiyang Guizhou

Received: Jun. 2nd, 2023; accepted: Jun. 20th, 2023; published: Aug. 24th, 2023

Abstract

As an emerging factor and information carrier of social production, the security guarantee of government data in an open environment is bound to be more difficult. As the importance and value of data become more and more prominent, the data security risks faced by the opening of government data gradually rise, and the need for government data security legislation becomes more and more urgent. Starting from the current situation of government data opening, this paper will sort out and summarize the current security problems faced by government data opening, analyze the necessity of strengthening legislation and suggestions for improvement, so as to better improve the awareness of data security.

文章引用: 胡瑞竹. 浅析政务数据开放下的数据安全法律问题[J]. 法学, 2023, 11(5): 3355-3359.
DOI: 10.12677/ojls.2023.115479

Keywords

Data Opening, Government Data, Data Security

1. 引言

在信息技术和互联网飞速发展的背景下，人类的活动场域从现实空间被扩展到了一个网络空间。政府所获取的数据飞速增长，公众由网络渠道所得到的信息量也正呈指数型爆炸增长，政府不应该仅自己可见的保有大量数据和信息，而是选择开放政务数据。2015 年《国家安全法》第二十五条：明确规定“国家建设网络与信息安全保障，提升网络与信息安全保护能力，加强技术开发，实现对关键基础设施和重要领域信息数据的安全可控。”首次从与国家安全有关的法律层面上提出要确保数据安全，我国对数据安全问题持续关注。然而，政府在开放其所拥有的数据供各方开发和创新的同时，随着政府公开的数据日益上涨，数据所面临的安全问题和风险也随之凸显出现。

本文将基于政务数据开放方面的数据安全法律文献，以及现在最新的情况发展。从现有学者们的研究现状来看，他们都认可了政务数据开放在更大程度上的释放了数据价值，对经济和社会的发展产生了巨大的推动力，但是数据安全的问题也是不容忽视，然而既有政务数据开放又有数据安全相关法律问题关联起来研究却不多。所以，在大数据时代，政务数据的公开是必然的需求，本文以政务数据开放为背景，浅析政府在数据安全方面所面临的风险、立法的必要性以及完善建议。

2. 政务数据开放的现状

2.1. 政务数据开放的立法现状及实践

虽然，目前对于政务数据开放并没有直接以其为对象的立法，但是可以在其他的法律条文中发现关于政务数据开放的相关规定。在最初，依据《政府信息公开条例》实行政务数据的公开这项重要措施，其中明确规定了政府信息公开的范围、方式和程序以及公开的主体，一些地方在实行政务数据开放时都是以此为参考。在国家层面政务数据不予以开放的范围，主要是根据《中华人民共和国保守国家秘密法》中所规定的信息属于国家秘密以及保密的制度。在《民法典》《中华人民共和国网络安全法》(以下简称《网络安全法》)和《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)形成个人信息保护的法律体系，对个人隐私信息的范围作出了明确的规定，让包含着大量个人信息的政务数据在开放的范围中也受此约束。而 2021 年所施行的《中华人民共和国数据安全法》(以下简称《数据安全法》)共七章五十五条，其中第五章对国家机关在使用和加工以及国家机关委托他人使用和加工政务数据提出了明确的规定，而后又从政务数据平台、政务数据开放目录等做出指示，不断落实数据安全保护责任，较为系统和规范对政务数据开放制度进行了规定，同时这也意味着国家对于政务数据开放问题的紧迫重视。

2.2. 政务数据开放所面临的安全问题

2.2.1. 个人隐私数据的泄露

在大数据时代，政府拥有大量关于教育数据、不动产交易登记数据、婚姻登记数据、纳税数据、社

保数据等信息，个人隐私数据的收集、储存、传递、使用和删除过程均会面临风险。开放政府数据意味着政府部门希望节省在应用程序中开发数据以服务公众的成本，市场开发人员用数据定制以满足公众的需求，政府与数据开发人员形成合作关系。但是，使用大数据分析与挖掘技术不仅能够恢复出一个人或者一个组织机构的所有信息，借助新兴技术可以更轻松地从数据的相关关系中挖掘出个人信息或组织内部的各种信息，这些信息具有更高的隐私保护价值。个人信息数据被窃取被贩卖，对个人、对组织、对社会都将造成巨大的不良影响甚至是危害[1]。

2.2.2. 数据平台的安全防范

多部门及多组织间数据开放与共享，这样频繁且常态化流动的模式使得系统与数据安全责权边界是模糊的，出现了数据超范围共享与数据暴露面扩大等安全问题与隐患。以往政府的信息公开只为了确保公众知情的权利，而公众知道的信息都是经过加工过的数据资料，并非第一手了解，政府建立一个开放的数据平台，能够吸引社会各方根据实际需求与应用场景，整合使用开放数据。政务数据涉及在平台内的传递、使用、储存等环节，使得政务数据从隐匿状态进入到开放的环境，所以数据使用价值与数据安全风险逐渐同步上升，数据安全的确保变得至关重要。政府所开发的数据平台从设计开始以来，必须要考虑的问题是在进入数据库时的身份认证、开放数据对用户的授权等，防范薄弱的平台容易遭受到恶意破坏。同时，当政府用户在使用服务商开发的共享交换平台服务后退出平台，服务商有责任彻底清除所有备份数据以及在运行过程中所生成的用户数据，以确保数据的完整性和安全性。然而，用户数据是否被完全永久性地删除这是有待考察的，缺乏监管机制和检测机制意味着平台可能会存在完整保留或保留的风险。

2.2.3. 相关数据安全法律法规的滞后性

当前，政务数据对社会的发展已是必不可少的的生产要素，对政务数据的开放是已经在实践的过程中，而数据安全相关的法律保障则略显滞后。由前所述，政务数据开放的相关法律可以在现行的其他法律中找到，但是直接的调整对象并不是政务数据开放，这对其调整规范的效果和作用是有限的。对于《政府信息公开条例》，在很大程度上是被用作公众查阅政府信息，并对政府行为进行监管的基础依据，本条例的一些规定和内容对政务数据开放是具有参考和借鉴的价值，但是由于政府信息公开和政务数据开放的内涵有着显着区别，不能适应政务数据开放对法制保障的要求，而且很难为政务数据开发提供全面的法律依据。《数据安全法》第五章为政务数据开放进行了指导性的规定，但是仍是停留在了较为宏观的层面，要完全满足政务数据的开放还需详细完善。

3. 政务数据开放下数据安全立法的必要性

3.1. 数据安全事件的频发

国内外数据安全事件频发，数据安全风险也越来越高，加强政务数据的相关立法，才能在最大程度上实现政务数据资源地开放，确定政务敏感数据和其所包含的个人隐私数据在开放共享中的安全性。2021年，国家安全部公布了三个数据安全案例，这些案例都存在着严重的危害，我国的重要数据遭到境外网络的窃取[2]。2022 年，因为服务器使用了弱密码，南非几乎所有公民的征信数据被窃取[3]。2023 年，三星公司引入 ChatGPT 参与到修复源代码的问题中，但是在使用过程中，机密数据输入到 ChatGPT，但是之后并没有删除，数据被保留到了 ChatGPT 的平台上被服务商所获得，发生了数据泄漏事件[4]。数据泄露事件地频繁发生，数据安全需求逐步提升，必须以统一的法律标准政务数据资源的开放共享范围进行规定和限制，否则无法适应安全需求提升。

3.2. 降低政务数据开放标准的差异性

为了经济与社会发展需求，即使法律上的统一性缺失，为了加快政务数据开放的速度，一些政府已经开始推行适应本地需求的政务数据开放标准，这就造成了标准存在很多差异，很难实现统一。面对着以复杂、多元和碎片化为特征的政府数据开放领域，我们需要一种以“开放与分享”为特征的整体法律框架[5]。为了政务数据统一开放须专门制度相关法律，对每一环节只要涉及到数据的使用都必须作出严格而确定的规定，使用数据的主体方必须遵守国家在数字安全领域的各类安全相关法律法规的要求。法律规定统一政务数据的开放标准，通过一体化的管理方式，促使各公共管理主体在使用政务数据中协调一致，实现政务数据开放标准的整合。解决在政府在数据开放实践上标准不统一的困境，可切实促进政务数据的开放，有必要加强政府数据资源相关立法，推动数据资源开放共享法规的制定，确保政府敏感数据和用户个人数据在开放共享中的安全[6]。

3.3. 提升数据开放的质量

科学、统一和完善的政务数据开放立法，全方位多维度对数据安全保护，多方利益得到了考虑，确保了政务数据能够得到最大限度的安全公开。但是具体需要开放哪些种类的政务数据、怎么实现开放，范围、内容、方式等可能主要还是取决于地方政府所施行的数据开放条例。而其他一些地方政府对数据开放仍然只是处于在重视的水平上，缺乏清晰的方针和实质性的作为。统一的数据开放立法有利于将地方分散立法所产生的问题消除，如果过度偏重于数据安全保护，那么就会限制数据开放所能带来的红利，反之，过度的数据开放，那么数据安全的风险就会上升，所以统一立法才能找到数据安全和数据红利之间的平衡。

4. 政务数据安全立法的建议

4.1. 朝着精细化方向完善立法

《数据安全法》虽然对接下来的政务数据开放与安全保护指明了方向和提供法律保障，但是内容仍是不太完善，只是进行了广泛的规定，按照此要求实践，只是较为原则性、规范性地实现政务数据开放，仍旧是政务数据开放在前，安全保护措施处于滞后。《数据安全法》第三十九条所要求“国家机关建立政务数据安全管理制度，落实数据安全保护责任，保障政务数据安全”，在此条文中，针对的对象是国家机关应该履行数据安全的职责，但是对于政务数据安全管理的标准也没有进一步地做出精确地指导，由于内容粗略性和系统性地表述，让《数据安全法》在真正的实践中，反而会稍显单薄，使得地方仍旧会习惯于用地方条例来保障数据安全，《数据安全法》并未对政务数据管理制度做出具体可操作性的要求和细则。

4.2. 提高制度的可实践性

细化相关的法律制度，提高在数据安全保护中的可操作度和实践性，这是我国政务数据安全立法中的一大改进途径。针对政务数据安全法律的细化，可以在《数据安全法》第三章的基础上进一步的深化。

对于政务数据安全重要的是风险评估机制完善，虽然《数据安全法》提出了国家要建立统一的数据风险评估机制，但是应当针对政务数据为目标明确评估制度的有效性，需要明确评估主体、明确评估范围、规范评估标准、合理程序等相关内容，才能确保政务数据安全评估机制的有效性。由于数据具有动态变化的特性，政务数据的流动性和安全防护需求呈现出相对静态、固化的风险评估方式，难以满足不同环境、不同目标下的安全评估需求。需要在不同场景、阶段采取具体的相关措施，以确保数据的安全性，围绕数据资产的重要程度、数据存储、处理、共享、开放与授权运营等全过程信息，进行场景化收

集、统计和监测，从不同维度动态评估风险状况，进行数据合规稽核[7]。由风险评估机制的程序得出一个评估结果，才能实现既对已知的风险进行监测，又对未知的风险进行预测和关联，得以建立适用于特定政务数据应用场景的全天候、多方位的政务数据安全策略。

4.3. 健全政务数据安全分级分类

合理地将数据分类分级进行不同类型不同等级的数据安全保障是实现数据安全精准控制的基础。政务数据分级分类制度避免了按照一个标准对所有数据采取无差异化的安全措施，监管力量和风险防范实现重点集中，降低数据安全的治理成本。《数据安全保护法》第二十一条规定，“国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。”由此可见，政务数据分类分级保护制度作为数据安全保障的先决条件，针对不同种类与等级的数据采用不同的安全保护措施，并将安全和监控力量的措施集中在关键数据和关键数据上。政务数据分级分类制度作为政务数据安全其他制度得以开展的核心，健全政务数据安全分级分类制度便尤为重要，但目前我国虽然提出建立政务数据安全分类分级制度，却并没有对其进行落实[8]。

5. 结语

数据安全是保障政府、市场、社会运用数据创新开发的重要基石，现在数据安全甚至会影响到国家安全，持续完善数据安全的法律法规迫在眉睫，尤其是政务数据包含着如此巨量和重要的个人数据，必须为政务数据开放构建一个构健康、安全的环境。政务数据安全方面的基础性法律，《数据安全法》体现了它的重要性，应以此不断完善政务数据的安全保障，保护政府部门等重要数据符合各种数据安全法律法规的最新要求也是各级政务数据管理运营等的重点工作。只有加强法律法规的推行，才能实现全国的政务数据开放依法行动，激发数据潜能，跟上数字时代的新需求完成数据红利与数据安全之间的平衡。

参考文献

[1] 高志华. 浅析数据安全与《数据安全法》[J]. 数字通信世界, 2022(1): 185-187.

[2] 刘奕湛, 刘硕. 国家安全部公布三起危害重要数据安全案例[EB/OL]. http://finance.people.com.cn/n1/2021/1101/c1004-32269793.html, 2021-11-01.

[3] 互联网安全内参. 南非几乎所有公民征信数据泄露: 弱密码惹祸预计损失超百亿元[EB/OL]. https://www.secrss.com/articles/40484, 2022-03-21.

[4] 赵昊. 三星员工被曝不当使用 ChatGPT 半导体机密数据直传美国[EB/OL]. https://www.thepaper.cn/newsDetail_forward_22573364, 2023-04-03.

[5] 高何渊. 政府数据开放的整体法律框架[J]. 行政法学研究, 2017(6): 58-68.

[6] 叶润国, 陈雪秀. 政府数据开放共享安全保障问题与建议[J]. 信息技术与标准化, 2016(6): 22-25+34.

[7] 宋华琳, 郑琛. 论政府数据开放中的数据安全保护制度[J]. 中国司法, 2022(3): 48-54.

[8] 王泽宇. 政务数据安全立法问题研究[D]: [硕士学位论文]. 成都: 西华大学, 2022.