

# 政府数据开放中个人信息保护的优化路径

张娟

常州大学史良法学院, 江苏 常州

收稿日期: 2024年1月3日; 录用日期: 2024年1月24日; 发布日期: 2024年3月15日

## 摘要

在整个数据市场的构成中, 政府数据无疑占有着举足轻重的地位, 但是有关政府数据在开放过程中公民个人信息的保护问题, 尚缺乏严谨的制度逻辑和规范。政府数据开放过程中, 存在数据开放与目的限制原则的冲突、数据开放的识别性冲突、法律边界不明、政府监管措施欠缺、个人信息的救济机制不完善等诸多挑战。因此, 政府数据开放中个人信息保护要平衡开放和数据限制原则的冲突、构建场景化数据开放的“识别性”路径、确定政府数据开放的法律边界、调整政府数据开放使用的监管措施、构建多元救济途径。

## 关键词

政府数据, 数据开放, 个人信息保护

# Optimization Path of Personal Information Protection in Government Data Opening

Juan Zhang

Shiliang Law School, Changzhou University, Changzhou Jiangsu

Received: Jan. 3<sup>rd</sup>, 2024; accepted: Jan. 24<sup>th</sup>, 2024; published: Mar. 15<sup>th</sup>, 2024

## Abstract

In the composition of the whole data market, government data undoubtedly occupies a pivotal position, but the protection of citizens' personal information in the process of government data opening still lacks rigorous system logic and norms. In the process of government data opening, there are many challenges, such as the conflict between the principle of data opening and purpose limitation, the identification conflict of data opening, unclear legal boundary, lack of government supervision on measures, and imperfect relief mechanism of personal information. Therefore, the protection of personal information and data restriction, building the "identification" path of the

**scenario of data opening, the protection of personal information in the opening of government data should determine the legal boundary of the opening of government data, adjust the regulatory measures of the open use of government data, and build multiple relief channels.**

## Keywords

**Government Data, Data Opening, Personal Information Protection**

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## 1. 问题的提出

随着大数据与人工智能的发展，政府数据开放制度也因此应运而生。新兴的政府信息公开制度与传统的政府信息公开制度相比，政府数据公开代表着由“履行公众知情权”的“被动公开”到“构建开放政府”的“主动开放”的模式转变。政府数据公开是政府利用数字手段来治理国家的一种制度工具，旨在利用开放数据和数据创新，从而实现发展经济、提高服务、提升治理能力等有益的行政目标。但是伴随着数字政府、数字社会、数字经济的一体化发展的同时，也给国家安全和公民安全带来了许多风险和

挑战。

然而，就政府数据开放而言，目前我国还没有关于这方面的相关立法。《政府信息公开条例》于2019年4月3日修订并发布，但是它并没有提及政府数据和开放政府的相关描述，仅仅只提及了政府要依据宪法和相关法律的规定，严格的履行有关信息公开的义务和责任。《中华人民共和国个人信息保护法》自2021年11月1日起颁布施行，明确规定了本法可适用于国家机关处理个人信息的活动，并明确了“原则上国家机关不得公开或者向他人提供其处理的个人信息”，法律、行政法规另有规定或者取得个人同意的除外[1]。本文致力于分析政府数据开放中个人信息保护存在的问题，并为其提供纾解途径，使行政机关在实现自身管理目标与保护行政相对人个人信息之间达成相对平衡的状态。

## 2. 政府数据开放中个人信息保护的理论基础

### 2.1. 个人信息保护的必要性与特殊性的论证

一方面，要明确政府在数据开放中对个人信息保护的作用。一些西方自由主义法哲学家坚持“政府之恶”的理论，他们主张限制政府的权力，来确保公民的自由和权利。自由主义者普遍对国家和政府充满恐惧，因为政府之存在是对公民权利的一大威胁[2]。伴随着数字时代的到来，以大数据和新媒体为基础的互联网企业正在蓬勃发展，但是“数据垄断”“数据独裁”等不利影响正在逐步显现。相对来说，与实力雄厚的互联网企业相比，公民们则处于非常不利的地位，所以就某些方面来说公民还是需要政府的帮助的。

另一方面，在政府数据开放过程中，要秉持控权论理念，以防政府与企业的“合谋”。伴随着大数据的发展，各个地方的政府机构都将“互联网+”的发展放在首要位置，希望能通过大数据的发展促进相关产业的发展。但是，有一些地方政府试图通过处理、应用甚至是泄露政府数据开放中的个人信息从而促进相关产业的发展时，“政企合谋”的危机便会在不知不觉中产生。因此，为了更好的实现政府数据开放的目的，防止公民的个人信息沦为“政企合谋”的牺牲品，贯彻实施行政法治的控权论理念则显

得极其重要[3]。

## 2.2. 公共利益与私人利益的关系阐释

在政府数据开放的过程中，政府、企业和个人三方主体的利益相互影响，所以当下讨论的热点便是如何均衡好各方的利益。

第一，就政府数据开放的范围和内容而言，并不是政府数据开放的范围越大、内容越广越好。在数字时代的推动下，政府数据的开放观念由先前的政府信息公开发展到目前的政府数据开放，但是“以公开为常态”并不具备充分的正当性。相反，“需求导向原则”得到了理论界和实务界的更多认同[4]。这种观念的转变一方面意味着政治话语的改变，另一方面也暗含着公民们需要政府为他们提供一些基础的、可理解的数据。因而，政府数据开放的内容和范围要考虑到社会大众的接受程度，并不是越多越好。

第二，政府数据开放的过程混杂着多方利益，包括部门利益、企业利益以及个人利益，因此并不能完全代表着公共利益。从政府的层面看，“不敢开放”“不愿开放”“不会开放”的问题仍然普遍存在[5]。从企业的层面看，部分企业在参与政府数据开放利用过程中存在明显的机会主义行为，例如：部分企业索要数据为真，利用数据为假，或是利用数据进行涉及公民个人隐私的违规操作[6]。

## 3. 政府数据开放中个人信息保护的现实困境

### 3.1. 理论冲突

#### 3.1.1. 数据开放与目的限制原则的冲突

在整个大数据的背景下，经过数据处理后的政府数据和企业数据会产生额外的附加价值，所以数据也就进一步成为了企业进行营业活动和政府进行政务工作的手段和工具。因而，对于民生服务和公共管理来说，政府数据开放具有很大的实践价值，在一定程度上它暗含着由传统的管理型向新兴的服务型的政府职能理念的改变，这也满足了公共服务和公共管理的需要。但在现实生活中，政府的开放数据往往会被企业重复的开发与利用，因而在一定程度上会导致其超过政府在收集与整理数据时的目的限制。究其根源是因为政府在整理与收集信息时仅仅是为了满足自身行政事务上的需求，因而所收集的数据信息并不能都满足企业日常事务的需要。

#### 3.1.2. 数据开放的识别性冲突

对个人的信息数据进行分析、使用、处理等二次增值行为是政府数据开放最主要的价值，但是在某些特殊的开放场景下，比如通过披露等方式对个人信息进行分析、使用、处理等二次增值行为是被禁止的，因此政府数据可能会失去它的识别性。有些学者认为，就数据安全而言，政府数据开放应对个人相关数据脱敏后再开放与增值开发，即企业仅可开发去除“识别性”的“非个人数据”[7]。但与此同时，又会引发出一个新的问题，在一些特定的情况下个人信息的使用和处理需要保留其识别性，如在开放过程中，政府数据的二次增值应用或者服务目的是为了公民的日常生活服务，如果要充分实现其功能，这时就需要使用个人信息的可识别性特点。由此可见，政府数据的开放并不适用所有的二次增值应用的情况。

### 3.2. 现实挑战

#### 3.2.1. 政府数据开放中个人信息的法律边界不明

随着大数据广泛的应用，政府数据在开放的过程中也会面临一定的风险与挑战。比如，在此过程中，一旦个人信息受到法律保护的边界不明，则会导致公民的个人信息遭到泄露和侵犯。很多利益集团在实

际运营过程中也正是意识到了这一点，因而巧妙的利用了个人信息法律规定的不确定性，在政府数据开放的平台里侵犯公民的个人隐私以及非法的收集公民个人信息，从而导致公民的个人信息遭到泄露和侵犯。例如，当社会公众出于日常生活的需要而下载某些 APP 软件时，经常会因为不知道这些软件的应用程序，而误开通了“允许给自己发送通知或者推送感兴趣的内容”等操作行为。而像这种允许给自己发送通知或者推送感兴趣的内容就相当于默认了软件的一些侵权行为，这样会使得一些机构就利用了法律填补的漏洞，不仅“巧妙”的泄露了公民的个人信息，而且还逃避了法律的惩罚。

随着大数据时代的到来，个人信息权的重要性越来越明显，使得每个信息主体都意识到其拥有保护自己的个人信息不被滥用的权利，而个人信息保护制度能够运行下去正是基于这项权利的存在[8]。因此，在此过程中，政府需要明确的了解个人信息在此过程中的界限范围，才能更有效的实施政府数据开放的目的。

### 3.2.2. 政府部门监管措施欠缺

在实际工作中，政府部门本身的监管能力会对公民的个人信息保护产生一定的影响。由于政府自身的监管能力的欠缺，所以政府不可能随时随地的对公民的个人信息进行有效的监控，因而政府也很难及时的侦察到公民个人信息的泄露情况的发生。

政府部门发现公民个人信息的泄露主要有两种方法：一是依据企业自身的定期排查；二是依靠公民个人的举报。例如：万豪酒店泄露顾客的个人信息的案件。具体事件如下：在 2014 年时，万豪旗下的酒店就已经发生过泄露顾客个人信息的事件，但是当时的管理者并未严肃处理好该事件，以至于泄露个人信息的情况越演越烈，直至 2018 年已经有 5 亿顾客的个人信息的泄露甚至盗窃[9]。因为个人信息泄露自身的隐秘性，所以就算是相关的部门，有时也无法及时察觉到个人信息正在遭受泄露[9]。

其次，就是有一些政务查询业务需要用户通过登录政府网站或者下载某些特定的 APP 才能查询到自己想知道的信息，这无疑就给了某些犯罪分子可乘之机。例如，一些犯罪分子会在这些特定的 APP 或者网站中放入木马病毒或者病毒链接，一旦用户误点了这些病毒链接，就会导致个人的信息瞬间被泄露出去。当政府用来存储个人信息的载体不成熟时，也会发生个人信息泄露的情况。比如，电脑硬盘、U 盘及网络云盘等载体容易遭到攻击，这些载体会因为平台技术人才不当的管理与维护造成破坏，或者受到自然灾害、电脑病毒和不法分子的攻击等而受到破坏而造成公民的个人信息遭受泄露和侵害。

### 3.2.3. 个人信息的救济机制不完善

在我国，大多数公民的个人信息都掌握在政府手中。在政府数据开放过程中，政府也很有可能成为泄露公民个人信息的主体。所以在此过程中，完善个人信息救济机制极其重要。个人信息的救济机制不完善主要有以下原因。

一是举证艰难。如果公民在自身的个人信息遭到泄露之后，可以向法庭提供明确的证据证明自己的个人信息确实遭到他人的泄露，那么法官就会为受害者争取到最大的权益，同时也让违法者受到应有的惩罚。但是在现实生活中，大多数公民在个人信息受到侵犯后，很难向法庭提供明确的证据，证明自己的个人信息遭到他人的侵犯或者泄露，以至于无法确切的保护到自己的个人权利。导致举证艰难的主要因素有：需要具备一定的技术手段和能力才能向法庭提供明确的证据，但是一般的公民通常不具备这种能力；侵权者和被侵权者地位的不平等，被侵权者一般是公民，通常处于劣势地位。

二是举报和维权途径少。在公民的个人信息遭到泄露时，主要有以下三种举报和维权的途径。第一种，是公民个人自行发现网络上存在泄露自己的个人信息的情况，从而要求信息发布者删除有关自身的个人信息，从源头上切断了泄露自己个人信息的情况。第二种，则是要求受害者向泄露其个人信息的主管部门提出控告，但是要求损失的金额达到一定的标准才可以提出该项要求，相关的机关才会予以立案

调查。第三种，则是受害者向法院提起诉讼，要求侵权者承担应有的法律责任并赔偿自己的损失。但是这一途径，则要求受害者个人自身掌握一定的法律知识，否则就不一定可以通过这一种手段来为自己谋求到法律的保护。

## 4. 政府数据开放与个人信息保护的权利平衡

### 4.1. 平衡数据开放和目的限制原则的冲突

对于平衡数据开放和目的限制原则的冲突，究其根源是是要解决政府在整理和收集个人信息时的范围限度以及企业在进行日常经营活动时所需要采集的公民的个人信息范围的冲突。

在政府数据进行开放时，需要制定明确的限制规则，可以明确的表明哪些个人信息可以进行开放，哪些个人信息不能进行开放，即使是企业机构为了进行正常的生产生活也不能超过政府所规定的限制，这样才能在一定程度上规避企业机构做出超出目的限制原则的行为。就企业而言，一方面要加强保护个人信息的意识和增强自身的法律意识，不能为了企业的需要就过度甚至违法获得公民的个人信息，这样只会得不偿失；另一方面是要拓展企业合法化收集个人信息的途径，使得企业不仅只能依靠政府获得个人信息，还可以通过其他途径也能获得自身所需的个人信息，从而从根源上减少违背目的限制原则收集个人信息的情况。

### 4.2. 构建场景化数据开放的“识别性”路径

构建场景化的数据开放的“识别性”路径主要包括以下两个方面：一方面是加强技术方面的控制。政府部门应该充分利用大数据平台的特性，对个人信息的隐私部分进行去除识别性处理，并根据隐私情况进行私密的等级划分，再进行相应的不同程度的加密处理，从而有效的防止个人信息的泄露或者被侵犯。另一方面是对于不同场景下的个人信息进行特定的“识别性”处理。简而言之，就是在一些特定的场景下，需要利用个人信息的与众不同的特征，对其进行快速的识别，从而提高工作的效率。将日常生活中需要进行场景化识别的情况都进行一一记录和阐释，并列明具体的案例场景，也使得繁重的工作变得更加便捷。

### 4.3. 明确政府数据开放的法律边界

为了明确政府数据在开放过程中的法律边界，应重点关注以下两个方面：第一，可以参照《民法典》中有关个人信息权利保护的法律条文，明确的区分出一般个人信息和敏感个人信息。对于一般的个人信息，在政府数据开放的过程中必须要将效率原则置于首位，政府可选择匿名后再对个人信息进行开放。但是涉及到公民的敏感信息或者隐私信息时，政府则应当尊重公民的权利和自由，让公民自行决定是否开放。第二，我国可以参考其他国家的《信息公开法》，明确的列出需要将公共利益置于首位的项目，并且这些项目的实施必须由政府亲自完成，以防止一些利益集团以公共利益为名，实际上却做出侵犯公民个人信息的行为。

### 4.4. 调整政府数据开放使用的监管措施

#### 4.4.1. 完善监管体系

随着《个人信息保护法》的出台，有关个人信息保护的法律法规体系即将形成。为进一步发挥《个人信息保护法》在政府数据开放中的作用，应重点关注以下两个方面。

一方面是落实并且细化个人信息保护体系的规则。一是必须确保《个人信息保护法》在个人信息保护法律体系中的主导地位，以确保能够充分保护好个人信息。二是进一步细化政府数据在开放过程中对

个人信息的保护。《个人信息保护法》对国家机关处理个人信息的有关规定还是不太具体，可以在参考各行业特点，听取各行业有关组织建议后进行细化落实。

另一方面是加快构建由政府主导、行业辅助的个人信息保护监管制度体系。一方面，政府在监管上应发挥其主导作用，加快落实《个人信息保护法》中有关各部门监管职能的细化规则，为各行各业的个人信息保护提供准则。另一方面，在细化规则以及相关法规的指导下，倡导行业协会出台符合本行业的监管规范，实现从上而下，从里到外的监管体系。

#### 4.4.2. 提高监管技术

为了更有效的保护公民的个人信息安全，政府部门可以从提高监管技术方面进行改变。第一，培养技术人才，构建完善的监管系统。政府可以联合高校培养一批专门为政府服务的互联网人才，致力于解决政府在数据开放过程中的个人信息监管问题，比如百人计划等等；可以加强国际的交流和合作，比如与美国硅谷等高新技术企业建立合作关系，为培养高科技人才奠定了坚实的基础；如果是专门为我国的个人信息保护培养优秀的高科技人才，可以考虑和阿里巴巴等企业开展合作。第二，提供雄厚的资金支持，确保网络设备的先进性。在数据网络飞速发展的当今社会，政府应该加大投资于设备的更新，程序的升级，这样才能更好的保证国家以及个人信息网络的安全。例如，政府可以建立一个网络浏览机制，通过对公民的浏览记录进行详细的监督，从而更好的掌握在各个网络平台中，公民的个人信息的详细情况。

### 4.5. 构建多元救济途径

#### 4.5.1. 加大惩罚泄露个人信息的力度

对于个人信息救济机制不完善的问题，可以通过加大惩罚泄露个人信息的力度来解决。这在一方面可以对一些利益集团形成强有力震慑作用，从而提高他们的违法成本，另一方面也能在一定程度上起到更好的保护公民的个人信息的作用。

目前，政府可以采取的惩罚措施有：一是提高违法成本，明确金额处罚标准。随着数字时代的到来，利用网络数据犯罪的案件也变得更加频繁。在对违法犯罪者进行正常的没收违法所得收入之后，我国政府可以提高对非法泄露公民个人信息的相关人员以及公司企业的罚款，这无疑可以减少一定数量的泄露个人信息案件的发生。二是构建一支具有极高专业性的个人信息保护的处罚队伍。需要注意的是，要提高处罚人员的法律水平，进行法制思想教育，从源头提高整个队伍的法律素养。同时要赋予该队伍强有力的处罚权，使他们能够依法对泄露个人信息现象进行处罚，这样才能更好的保护个人信息的安全。加强行政处罚部门与其他部门间的沟通与合作，如减少法院申请执行的案件，这样可以提高行政执法效率，也能减轻法院的工作量。

#### 4.5.2. 拓宽个人信息举报方式和调解途径

当今，对于个人信息被侵犯或者泄露的问题，可以通过向相关的行业部门举报来解决。但是事实上，只有极少数的公民知道有哪些部门可以解决这些问题。政府需要做的是，保障公民举报违法的个人信息途径的顺利进行。例如，政府可以利用数据网络的发展，研发并实施在手机 APP 上进行举报投诉，从而使得举报方式变得更加简便。又或者可以开通微信小程序上投诉举报通道，使得举报的途径更为多样。

就调解途径而言，公民则可以选择网上调解以及诉讼平台。这种调解途径有以下几个优点：一、该平台可以记录整个调解以及诉讼的全过程，且电子版的记录比纸质版更容易保存。二、该平台可以避免当事人见面后的冲动情绪，在一定程度上避免了冲动办事<sup>[10]</sup>。三、与线下比较而言，在平台上解决问题可以更好的人力和金钱成本。

## 5. 结语

政府数据开放是一把双刃剑,利用好会促进与激发数据生产要素价值的充分释放,利益分配不当则会对信息主体的安全和隐私带来威胁[11]。所以,当政府数据开放的过程中涉及到公众的个人信息时,需要特别注意个人信息的安全以及公民的人身或财产安全。因而,在数据网络时代,政府数据开放的重心应放在保护个人信息安全与信息权利上。通过上文分析了在政府数据开放过程中个人信息保护存在的问题之后,笔者提出的相应的解决措施,期望对政府数据开放下个人信息的保护有所裨益。

## 基金项目

2023 年江苏省研究生科研与实践创新计划项目“司法大数据应用的法律规制研究”(项目编号:KYCX23\_3020)。

## 参考文献

- [1] 商希雪,韩海庭. 政府数据开放中个人信息保护路径研究[J]. 电子政务, 2021(6): 113-124.
- [2] 李强. 自由主义[M]. 台北: 东方出版社, 2015: 231.
- [3] 李谦. 互联网数据开放的中国逻辑:经济动力与政治意涵[J]. 文化纵横, 2016(1): 25-34.
- [4] 宋烁. 论政府数据开放的基本原则[J]. 浙江工商大学学报, 2021(5): 107-116.
- [5] 蒋冰晶,李少军. 包容与合作: 大数据时代政府数据开放的行政法治理念[J]. 河北法学, 2019, 37(12): 101-109.
- [6] 韩啸,陈亮. 政府数据开放价值创造缘何失败?——基于价值共同破坏视角的新解释[J]. 公共管理评论, 2021, 3(3): 92-112.
- [7] 郭明军,王建冬,安小米,等. 政务数据与社会数据平台化对接的演进历程及政策启示[J]. 电子政务, 2020(3): 32-39.
- [8] 李雪梅. 我国政府数据开放的困境及对策——基于大数据征信视角[J]. 征信, 2020, 38(9): 30-35.
- [9] 百度百科. 万豪酒店数据泄露门[EB/OL]. <https://mbd.baidu.com/ma/s/3jpkVz4P>, 2023-08-10.
- [10] 何茂玉. 论政府数据开放中个人信息的法律保护[D]: [硕士学位论文]. 长沙: 湖南师范大学, 2021.
- [11] 李政,洪莹. 基于隐私保护的政府大数据治理研究[J]. 大数据, 2020, 6(2): 69-82.