

探究大数据视角下个人信息安全风险及执法监管策略

史林鹭 丁利明

(大连民族大学文法学院, 辽宁 大连 116000)

【摘要】在大数据时代, 个人信息安全面临着越来越严重的风险。本文从大数据视角出发, 分析了个人信息安全风险的主要来源, 并探究了执法监管策略。首先, 个人信息泄露主要来自于信息系统安全漏洞、网络攻击和非法获取等途径。其次, 执法监管策略应该围绕着建立完善的法律法规体系、提高执法监管效率、加强行业自律、推动信息安全技术创新等方面进行。最后, 需要全社会共同参与, 加强信息安全意识和自我保护能力。

【关键词】大数据; 个人信息安全; 风险; 执法监管; 法律法规体系; 信息安全技术

一、个人信息安全风险的现状和特点

(一) 个人信息泄露的现状和危害

个人信息泄露已经成为一个普遍存在的问题, 不同行业和领域都存在这种问题。从国际上看, Facebook、Yahoo 等知名企业曾经因为个人信息泄露事件而受到了质疑和谴责。在国内, 近年来也频繁发生个人信息泄露事件, 比如某些互联网企业被曝光出售用户信息, 导致大量用户的个人信息遭到泄露。

个人信息泄露对个人和社会都造成了巨大的危害。个人信息泄露可能导致个人财产受到损失, 个人隐私遭到侵犯, 甚至会引发身份盗窃等问题。对于社会来说, 个人信息泄露可能引发社会治安问题, 比如犯罪分子利用泄露的个人信息实施诈骗、恐吓等行为。

(二) 大数据时代下的个人信息安全特点

大数据时代的到来, 使得个人信息安全面临新的挑战。一方面, 大数据技术的应用使得个人信息的采集、存储和传输变得更加容易和快速, 个人信息泄露的风险也随之增加。另一方面, 大数据技术的应用使得对个人信息的分析和利用变得更加精细和准确, 从而对个人隐私造成更大的侵害。

大数据时代下的个人信息安全还表现出以下几个特点: 第一, 个人信息的数据量巨大, 泄露的影响范围也更加广泛; 第二, 个人信息的价值更加高昂, 不仅能够用于商业活动, 还能够用于政治斗争等活动; 第三, 个人信息的获取渠道更加多样, 不仅来源于个人主动提供, 还来源于网络爬虫、黑客攻击等途径。

(三) 个人信息安全风险的成因和分类

个人信息安全风险的成因主要包括以下几个方面: 第一, 个人信息保护意识不足, 主动泄露个人信息; 第二, 个人信息管理不当, 信息被恶意获取; 第三, 网络安全设施不完善, 被黑客攻击; 第四, 组织机构内部员工泄露信息。

根据成因不同, 个人信息安全风险可以分为以下几类: 第一类是由个人自身原因导致的个人信息安全

风险, 比如个人在使用互联网时过于随意地泄露个人信息、过于相信不明来源的信息等; 第二类是由外部恶意攻击导致的个人信息安全风险, 比如黑客攻击、病毒感染等; 第三类是由组织机构内部员工泄露信息导致的个人信息安全风险, 比如某些公司员工出于利益考虑恶意泄露用户信息。

此外, 根据个人信息使用目的不同, 个人信息安全风险还可以分为商业用途、政治用途、犯罪用途等不同类型。商业用途指企业利用个人信息开展商业活动; 政治用途指政府或政治组织利用个人信息开展政治活动; 犯罪用途则是指黑客、犯罪分子等利用个人信息实施诈骗、恐吓等犯罪行为。

总之, 个人信息安全风险的成因复杂, 分类也多样化。在大数据时代, 个人信息安全面临的风险更加复杂和严峻, 需要采取更加全面和有效的措施加以防范和解决。

二、大数据视角下的个人信息保护执法监管现状

(一) 个人信息保护法规及执法监管机构

我国已经制定了一系列个人信息保护法规和规范性文件, 为个人信息保护提供了法律保障。其中, 最重要的是《中华人民共和国网络安全法》, 该法明确规定网络运营者应当采取技术措施和其他必要措施, 保障个人信息的安全, 并明确规定了个人信息泄露的违法责任和处罚。

除了法律法规, 国家也设立了一些执法监管机构来保护个人信息安全。其中, 最重要的是国家互联网信息办公室、公安机关等机构。这些机构负责监督网络运营者和个人信息处理者的合法合规行为, 对个人信息泄露和违法行为进行打击和惩罚。

(二) 执法监管的主要问题和挑战

执法监管的主要问题和挑战包括以下几个方面。第一, 法规制定和执法监管的滞后性。虽然我国制定了多项个人信息保护法规, 但是在具体的执法监管方面, 很多法规还存在较大的漏洞和不完善的地方。第

二，执法监管的难度较大。随着大数据技术的应用，个人信息泄露的手段和方式越来越多样化和隐蔽化，执法监管机构难以完全掌握和监管所有的个人信息泄露情况。第三，执法监管的成本较高。执法监管机构需要花费大量的人力、物力和财力来监管个人信息的安全，这对于一些小型企业和个人来说是一个较大的负担。

（三）执法监管的进展和成效

近年来，我国在个人信息保护方面的执法监管取得了一定的进展和成效。一方面，政府加强了对个人信息保护的宣传和教育，提高了公众的个人信息保护意识。另一方面，执法监管机构对个人信息泄露和违法行为进行了严格打击，一些违法企业和个人受到了法律的制裁。例如，近年来，国家互联网信息办公室针对一些网络企业存在的个人信息泄露问题，对其进行了严格处罚。

总体来说，我国在个人信息保护执法监管方面的进展还有一定的空间和挑战。为了进一步提高个人信息保护水平，政府需要不断加强法规制定和执法监管的力度，完善现有的法律法规和执法手段。同时，执法监管机构需要不断提升技术水平和能力，采用更加有效的监管手段和技术，加大对个人信息泄露的打击和处罚力度，以保障个人信息安全。

另外，社会各方面也需要共同参与到个人信息保护执法监管中来。企业需要建立健全的个人信息保护机制和体系，加强对员工的培训和管理，规范个人信息处理流程，加强安全措施，保护个人信息不被泄露。个人也需要增强个人信息保护意识，不轻易泄露自己的个人信息，不轻易相信未知来源的信息和链接，避免个人信息被不法分子利用和侵害。

三、大数据视角下的个人信息安全风险防范策略

个人信息保护是大数据时代的重要问题，如何保障个人信息安全是每个企业和个人必须面对的挑战。本文将从技术措施、管理措施和法律措施三个方面探讨个人信息安全风险的防范策略。

（一）个人信息安全的技术措施

1. 加强数据加密

数据加密是一种基础的信息安全保护措施，它可以有效防止数据在传输或储存过程中被窃取或篡改。企业和个人在使用网络服务时，应该采取 SSL 加密协议等技术手段来保护个人信息的安全。

2. 实施访问控制

访问控制是一种限制系统或应用程序对敏感数据的访问的技术措施。企业和个人应该采用访问控制技术，限制未经授权的人员访问敏感数据，例如通过密码、生物特征等方式验证身份，并设置角色权限，对不同人员进行不同的访问限制。

3. 采用数据备份和灾备技术

数据备份和灾备技术是防范数据丢失或损坏的重要措施。企业和个人应该采用数据备份和灾备技术，将重要数据备份到不同的地点或云端，以防止数据损坏或丢失，同时备份数据也可以保护数据隐私。

（二）个人信息安全的管理措施

1. 建立内部管理制度

企业和个人应该建立内部管理制度，明确个人信息处理的流程和规范，加强对员工和业务合作伙伴的监督和管理，确保个人信息的安全和保护。

2. 加强员工教育和培训

企业和个人应该加强员工的安全意识和保密意识培训，加强员工对信息安全和保护的认识和理解，减少因员工疏忽或不当行为造成的个人信息泄露风险。

3. 进行定期的信息安全评估

企业和个人应该定期对信息系统和应用程序进行安全评估，及时发现和解决可能存在的安全漏洞和风险，加强信息安全保障。

（三）个人信息安全的法律措施

1. 合规运营

企业和个人应该遵守国家和地方相关的个人信息保护法律法规，开展合规运营。例如，在收集、使用、存储和处理个人信息时，应该获取明确的授权同意，并遵循必要和合法的原则。同时，应该定期对个人信息处理的合规性进行自查和审查，及时纠正不合规的行为。

2. 建立个人信息保护机制

企业和个人应该建立个人信息保护机制，采取有效的技术和管理措施，保护个人信息不被泄露、篡改或损坏。在个人信息处理过程中，应该确保信息安全和保护，同时也要及时履行信息披露和通知义务。

3. 维护个人信息主体权益

个人信息保护的核心在于保护个人信息主体的权益。企业和个人应该尊重个人信息主体的知情权、选择权和参与权等基本权益。当个人信息主体要求删除、更正或访问其个人信息时，应该及时响应并给予必要的支持和帮助。

四、执法监管策略优化建议

在大数据时代，保护个人信息安全是至关重要的。尽管国家已经出台了相关法规和规范，但是一些企业或个人仍然存在个人信息泄露或滥用的行为。因此，建立健全的个人信息保护执法监管体系、加强执法监管的技术手段和能力、加强行业自律和监管合作等方面的优化建议非常必要。

（一）建立健全个人信息保护执法监管体系

1. 加强法规和规范的制定

个人信息保护法规和规范应当与时俱进，并保持与国际标准的一致性，以适应快速发展的科技环境。同时，要加强对违法行为的明确界定，确保执法监管

的准确性和公正性。

2. 建立信息举报和投诉渠道

建立举报和投诉渠道，让公众可以方便地举报和投诉个人信息泄露、滥用等违法行为。相关部门应该对举报和投诉进行及时处理，确保个人信息的安全和保护。

3. 加强监管机构的能力建设

加强监管机构的能力建设，提高执法监管人员的专业技能和执法能力。建立多部门联合执法的机制，加强监管力度，打击违法行为。

（二）加强执法监管的技术手段和能力

1. 引入新技术

引入新技术，如人工智能、大数据等技术手段，提高执法监管的效率和准确性。通过数据挖掘和分析，可以更好地发现和打击个人信息泄露和滥用等违法行为。

2. 建立信息安全监管平台

建立信息安全监管平台，对个人信息采集、存储、使用、交换等全过程进行监管。采用先进的技术手段，监测企业或个人的网络活动，及时发现并处理违法行为。

3. 加强数据共享和整合

加强执法部门之间的数据共享和整合，避免信息孤岛，提高执法监管的协同能力和效率。同时，加强数据安全保护，防止信息泄露和滥用。

（三）加强行业自律和监管合作

1. 建立行业自律机制

建立行业自律机制，加强对企业的监督，促进企业自觉遵守个人信息保护相关法规和规范。行业自律应当成为企业日常经营和管理的一部分，从源头上遏制个人信息泄露和滥用的行为。

2. 加强监管部门和企业的合作

监管部门应当加强与企业的合作，共同推进个人信息保护工作。建立定期交流机制，加强对企业的指导和监督，帮助企业建立健全的个人信息保护管理制度和技术手段。同时，企业也应当积极配合监管部门的工作，共同推进个人信息保护的工作。

3. 加强国际合作和交流

个人信息保护已经成为国际社会关注的焦点。加强国际合作和交流，吸收国际先进经验和技术，促进我国个人信息保护工作的进一步发展。

五、未来研究的重点和方向

未来，个人信息安全和执法监管仍然是一个长期而复杂的工作，需要不断地进行研究和探索。未来研究的重点和方向可以从以下几个方面进行展开：

（一）技术手段的应用和创新

人工智能、大数据等新技术的不断发展和应用，将给个人信息安全和执法监管带来更多的机遇和挑

战，需要进一步研究技术手段的应用和创新。

（二）法规和规范的完善和升级

随着个人信息安全风险的不断变化和升级，需要及时跟进和完善相应的法规和规范，保证执法监管的有效性和合法性。

（三）国际合作的加强

随着跨境数据流动的加速和国际合作的深入，需要加强国际间的执法合作和信息共享，建立跨国合作机制和流程，共同应对个人信息安全问题。

（四）用户意识的提高和教育

个人信息安全不仅是政府和企业的责任，也需要用户自身的意识和教育。需要加强用户对于个人信息安全的意识和知识，提高用户的自我保护能力和防范意识。

总之，个人信息安全和执法监管是一个长期且不断变化的工作，需要政府、企业和用户共同努力，采取多种手段和策略，才能更好地保护个人信息安全和隐私。未来研究需要关注技术手段的应用和创新、法规和规范的完善和升级、国际合作的加强以及用户意识的提高和教育，为个人信息安全和执法监管提供更好的支持和保障。

参考文献：

- [1] 文禹衡，于琳. 我国个人信息法律保护现状，主要问题及完善路径——基于《中华人民共和国个人信息保护法》的词频统计与分析[J]. 图书馆理论与实践，2022(4):11.
- [2] 倪楠王敏. 人脸识别技术中个人信息保护的法规规制[J]. 人文杂志，2022(2):121-131.
- [3] 何培瑞，唐炜钧，雷歆怡. 大数据时代个人信息保护的法律责任[J]. 网络安全技术与应用，2022(8):3.
- [4] 刘继瑶. 《一般数据保护条例》对完善我国个人信息保护的启示[J]. 齐齐哈尔师范高等专科学校学报，2022(4):4.
- [5] 陈宇照. 网络平台个人信息保护责任的法律经济学分析[J]. 北京社会科学，2022(10):9.

基金项目：大连民族大学大学生创新创业计划（202212026029）资助。

作者简介：

史林鹭，出生年月：2002年11月，性别：女，民族：汉族，籍贯：辽宁省丹东市，大连民族大学文法学院法学专业，本科；

丁利明，出生年月：1971年12月，性别：男，民族：回族，籍贯：内蒙古赤峰市，大连民族大学文法学院，职称：教授，学位：博士，研究方向：国际法。