

大数据时代个人信息保护的法律困境与突破

何传标

上海市华联律师事务所, 中国·上海 200001

摘要: 在大数据技术日益普及的背景下, 个人信息保护正面临前所未有的挑战。论文聚焦于大数据时代下个人信息保护在技术、行业和法律层面所遭遇的实际困境, 提出通过构建全面的信息保护法治体系来实现突破, 即整合现有法律资源, 明确细化保护标准, 并对数据跨境流动进行合理规范; 加强相关部门间的协同合作, 完善公益诉讼机制, 统一裁判尺度, 建立健全惩罚性赔偿制度等, 旨在实现大数据发展与个人信息保护之间的动态平衡, 切实保障公民的基本权益, 从而为数字经济的健康、可持续发展提供坚实支撑。

关键词: 大数据时代; 个人信息保护; 法律困境; 对策

Legal Dilemma and Breakthrough of Personal Information Protection in the Era of Big Data

Chuanbiao He

Shanghai Hualian Law Firm, Shanghai, 200001, China

Abstract: Against the backdrop of the increasing popularity of big data technology, personal information protection is facing unprecedented challenges. The paper focuses on the practical challenges faced by personal information protection in the era of big data at the technical, industry, and legal levels. It proposes to achieve breakthroughs by building a comprehensive legal system for information protection, which integrates existing legal resources, clarifies and refines protection standards, and reasonably regulates cross-border data flow; strengthening collaboration and cooperation among relevant departments, improving public interest litigation mechanisms, unifying judgment standards, establishing and improving punitive damages systems, etc., aim to achieve a dynamic balance between the development of big data and the protection of personal information, effectively safeguard the basic rights and interests of citizens, and provide solid support for the healthy and sustainable development of the digital economy.

Keywords: big data era; personal information protection; legal dilemma; countermeasure

0 前言

随着数字技术的飞速进步, 人类社会已全面迈入大数据时代, 从智能手环记录的健康信息到购物平台的个性化推荐, 个人信息已经深深融入日常生活的方方面面, 成为数据浪潮中不可或缺的一部分。这些海量数据不仅为经济社会发展注入了强劲动力, 同时也带来了严峻的安全挑战, 而传统的法律框架显然难以有效应对这一复杂局面, 深入探讨个人信息保护所面临的法律难题及其解决之道, 不仅关系到公民的基本权益, 更是构建安全可信的数字社会的关键所在。

1 数字洪流: 大数据时代的信息生态新图景

1.1 数据浪潮下的“个人信息新大陆”

大数据技术的兴起重新定义了个人信息的范畴。过去, 个人信息仅限于姓名、身份证号等明确标识。而如今, 社交媒体动态、搜索引擎关键词乃至生物识别特征都被纳入其中, 智能家居所记录的生活习惯, 以及物联网设备上传的环境数据, 也进一步拓展了个人信息的内涵。与此同时, 数据收集的主体也从单一机构扩展到电商、社交平台等多个领域, 形成了一个复杂庞大的信息网络, 基于这些海量数据构

建的用户画像, 能够精准捕捉用户的兴趣、消费偏好甚至情绪状态, 但这也使得隐私保护面临严峻挑战, 算法偏差还可能引发“数字歧视”^[1]。

1.2 信息价值裂变: 从隐秘角落到商业战场

在数据经济时代, 个人信息已成为核心生产要素, 在数据交易市场中, 经过整合的信息数据集成为炙手可热的商品, 企业通过数据共享挖掘潜在价值, 并以此构筑竞争壁垒。此外, 大数据催生了许多新型商业模式。例如, 短视频平台的内容推荐机制和共享单车的调度系统, 都依赖于对个人信息的深度分析。然而, 这种对数据的高度依赖也带来了信息泄露和滥用的风险, 威胁着用户的隐私安全。

1.3 技术双刃剑: 便利与风险的共生困境

大数据技术深刻改变了社会生活的方方面面, 在医疗领域, 通过对病理和基因数据的分析, 可以实现更加精准的诊断和治疗; 智能交通系统通过整合实时数据优化交通流量, 缓解城市拥堵; 在线教育平台则根据学生的学习情况推送个性化的学习资源。然而, 技术的另一面是不容忽视的数据安全隐患。由于数据集中存储和网络传输的特点, 黑客攻击和内部泄密事件时有发生, 此外, 企业超范围使用数据、

合成伪造信息等乱象频发,不仅威胁个人隐私,更对社会稳定构成潜在风险。

2 荆棘迷局:个人信息保护的现实困境

2.1 技术层面:数据安全防护的难题

2.1.1 数据存储与传输中的潜在风险

在大数据驱动的时代背景下,数据呈现出集中化存储和网络化传输的趋势,这对数据安全构成了严峻考验。为提升数据处理和分析效率,企业及机构通常将海量用户信息集中存放在数据中心,这种高度集中的模式使得单一安全漏洞可能引发大规模的信息泄露事件^[2]。与此同时,数据在传输过程中同样面临诸多威胁。一些企业为了节约成本,选择使用未加密或加密强度较低的协议,这为黑客窃取、篡改数据提供了可乘之机。尤其是在物联网环境中,智能设备与服务器之间的频繁数据交换增加了风险敞口。由于许多设备本身缺乏足够的安全防护能力,攻击者能够通过入侵这些终端获取用户的敏感信息,例如实时位置、健康监测数据等。

2.1.2 新型攻击方式对信息安全的冲击

随着科技的快速演进,针对个人信息的攻击手段也变得更加复杂和智能化。近年来,勒索软件成为一大突出威胁。攻击者利用恶意程序加密受害者的文件,并以公开或删除数据为要挟索取赎金^[3]。例如,2023年某医疗机构遭遇勒索软件攻击,其大量患者病历被加密,不仅导致医院蒙受巨大经济损失,还使患者的隐私暴露于危险之中。此外,人工智能技术的滥用也为信息安全带来了新的隐患。不法分子借助AI换脸、深度伪造等技术,仅需少量公开的人脸数据即可生成高度逼真的虚假内容,进而实施诈骗、身份盗用等违法行为。这类新型攻击手段往往具备较高的技术门槛和较强的隐蔽性,传统安全防护措施难以有效应对,从而给个人信息保护带来了前所未有的挑战。

2.2 行业层面:数据使用的无序状态

2.2.1 企业过度收集个人信息现象

在利益的驱使下,部分企业频繁出现超出必要范围收集用户信息的行为。许多应用程序在用户注册或使用,要求获取与其功能无关的权限。例如,某些阅读类应用会在未经用户明确同意的情况下,记录其阅读习惯和搜索记录等敏感信息。企业之所以热衷于大规模采集数据,一方面是为了更精准地描绘用户画像,从而提升商业价值;另一方面,则可能将多余的数据用于非法交易,从中牟利。这种行为不仅侵犯了用户的知情权与选择权,还显著提高了数据泄露的风险,用户往往因缺乏选择或被迫接受,而不得不交出大量个人隐私^[4]。

2.2.2 数据共享与交易的不规范问题

作为大数据产业发展的重要组成部分,数据共享与交易本应推动行业的进步,但目前该领域仍存在诸多不规范现象。在数据共享环节,企业之间的合作通常缺乏明确的规则

与有效的监管,容易导致信息被滥用。而在数据交易市场中,由于缺少统一的标准与完善的监管体系,数据的真实性和合法性难以得到保障。一些不法分子通过非法手段获取个人信息,并经过简单处理后,在地下市场进行交易,形成了一条完整的黑色产业链。这些违规操作不仅扰乱了数据市场的正常秩序,还对用户的合法权益造成了严重损害。

2.3 法律层面:保护体系的不断完善

2.3.1 法律法规滞后且欠协调

随着大数据技术的飞速发展,各类新兴应用场景和商业模式层出不穷,而法律的制定与修订却需要较长周期,难以及时适应技术进步的步伐。例如,在涉及AI生成内容的个人信息侵权问题以及元宇宙场景下的信息保护方面,现有法律尚未提供清晰的规范。同时,不同法律法规之间也存在一定的冲突和重叠。在中国,《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等多部法律均涵盖个人信息保护的内容,但在具体条款的适用范围、责任划分等方面存在差异,这不仅增加了执法和司法实践的复杂性,也使得相关问题的解决变得更加困难。

2.3.2 法律执行与监管存在阻碍

首先,个人信息侵权行为往往具有隐蔽性和跨地域性特征,这使得调查取证变得极为困难。许多数据泄露事件发生后,由于攻击者使用匿名化、加密等技术手段隐藏身份,并且数据传输可能跨越多个地区和网络节点,监管部门很难追踪到具体的责任人^[5]。其次,当前的监管力量相对薄弱,难以有效应对海量的数据处理活动。面对数量庞大的互联网企业和日益复杂的业务模式,现有的监管资源和技术手段显得捉襟见肘。最后,针对个人信息侵权行为的处罚力度普遍不足,违法成本过低,难以形成有效的震慑作用。

3 破局之道:构建信息保护的法治体系

3.1 立法优化:填补规则空白与统一规范

3.1.1 整合立法,推动专门立法

当前,个人信息保护的相关规定散见于多部法律法规中,缺乏系统性和协调性。因此,应推动在个人信息保护领域的专项立法工作,借鉴欧盟《通用数据保护条例》(GDPR)的成功经验,制定一部覆盖数据全生命周期管理的综合性法律。通过明确各条款的适用范围和优先级,解决现行规范中的矛盾问题,构建一个统一且清晰的法律框架。同时,针对新兴技术领域,如人工智能生成内容、元宇宙及物联网等场景,应及时出台配套法规,填补现有法律空白,确保对新型侵权行为的有效约束。

3.1.2 分级管理,规范跨境流动

构建个人信息分级分类管理制度,根据不同信息的敏感程度和重要性,制定差异化的跨境流动规则。对于普通个人信息,在满足特定条件的情况下可允许自由流动,而对于

高敏感信息,则需经过严格的安全评估和审批流程。同时,参考亚太经合组织(APEC)的跨境隐私规则(CBPR)框架,推动国际间的数据保护标准互认与合作,建立安全高效的跨境数据流动通道。此外,应明确数据出境主体的责任,要求其采取必要的技术和管理手段,确保境外接收方达到同等保护水平,避免因跨境流动导致的信息保护标准下降。

3.2 执法强化:创新监管模式与提升效能

3.2.1 部门协同,厘清监管职责

目前,个人信息保护监管涉及网信、公安、工信等多个部门,存在职责交叉和协调不畅的问题,为提高监管效能,应建立跨部门协同监管机制,厘清各部门在数据安全审查、违法查处和应急处置等环节的具体职责。可以参考英国信息专员办公室(ICO)的集中管理模式,设立专门的个人信息保护监管机构,统筹协调各部门工作,防止监管真空和重复执法。同时,加强与行业协会和第三方机构的合作,发挥其在行业自律和技术评估方面的作用,形成多元共治的监管格局。

3.2.2 技术赋能,全周期监测

执法部门应充分利用大数据、人工智能和区块链等先进技术,打造智能化监管平台,通过大数据分析技术,实时监测企业的数据收集、存储和使用行为,及时发现异常数据流动和潜在风险。借助人工智能算法,自动识别违规收集个人信息的应用程序和网站,显著提升监管效率。利用区块链技术实现数据操作的全程追溯,确保数据处理活动留有记录,便于调查取证。此外,还应建立风险预警机制,提前预判可能发生的数据泄露事件,并采取相应防范措施,从被动应对转向主动防控。

3.3 司法保障:畅通救济渠道与增强威慑力

3.3.1 降低门槛,完善公益诉讼

进一步完善个人信息保护公益诉讼制度,降低诉讼门槛,扩大公益诉讼主体范围,除检察机关外,可赋予消费者协会、环保组织等社会组织提起公益诉讼的权利,鼓励其代表公众利益维护个人信息安全^[6]。同时,简化诉讼程序,开辟快速审理通道,提高案件处理效率,为受害者提供更便捷的维权途径。

3.3.2 统一尺度,发布指导案例

为确保司法裁判的一致性,最高人民法院应定期发布指导性案例,明确侵权认定标准、责任划分原则以及赔偿计算方法等关键问题,通过案例指导,为各级法院提供裁判参考,提升法律适用的权威性和一致性。此外,建立案例共享

平台,促进法官之间的经验交流和学习,推动司法实践的规范化发展。

3.3.3 加大赔偿,建立惩罚机制

建立惩罚性赔偿制度,对故意或恶意侵犯个人信息的行为,在补偿受害者实际损失的基础上,施加高额惩罚性赔偿。赔偿金额可根据侵权人的违法所得、侵权行为的持续时间及影响范围等因素综合确定,显著提高违法成本。同时,加大对侵权企业的行政处罚力度,除罚款外,还可采取责令停业整顿、吊销营业执照等严厉措施,形成法律、经济和市场层面的多重威慑体系。此外,建立信用惩戒机制,将侵权企业和个人列入失信名单,限制其市场准入和经营活动,促使相关主体自觉遵守个人信息保护法律法规。

4 结语

在数字经济蓬勃发展的今天,个人信息已成为推动社会进步的重要资源,但随之而来的保护难题也不容忽视。从信息生态的剧烈变革,到技术、行业、法律层面的现实困境,个人信息保护面临着前所未有的挑战,构建完善的信息保护法治体系,是化解危机、平衡发展与安全的关键路径。通过立法优化填补规则空白、执法强化提升监管效能、司法保障增强救济力度,不仅能切实维护公民的合法权益,更能为大数据产业的健康发展筑牢法治根基。未来,随着技术的持续创新与社会需求的不断变化,个人信息保护仍需与时俱进,在实践中持续完善法律体系,推动形成政府、企业、社会协同共治的良好局面,实现数字时代个人信息保护与经济社会发展的良性互动。

参考文献:

- [1] 张衡.大数据时代个人信息安全规制研究[M].上海:上海社会科学院出版社,2020.
- [2] 杨荟康.大数据时代个人信息保护法律监管体系的重塑与思考[N].松原日报,2025-04-11(003).
- [3] 崔宇茹.人工智能时代个人信息保护法律难题与对策分析[J].法制博览,2025(3):160-162.
- [4] 冷传莉.人工智能与大数据法律问题研究[M].北京:知识产权出版社,2022.
- [5] 赵伟.大数据时代个人隐私权的法律保护[J].法制博览,2025(12):16-18.
- [6] 潘鑫鑫.大数据时代下个人信息保护公益诉讼制度研究——基于330份裁判文书的分析[J].湖北工业职业技术学院学报,2025,38(2):72-77.