

# 大数据视域下个人信息的民法保护

薛博文

(辽宁工程技术大学公共管理与法学院, 辽宁阜新 123000)

摘要: 随着社会的不断发展和进步, 我国在关于个人信息保护方面的法律建设取得了一定的成果。从2017年《民法总则》实施到2021年《民法典》的颁布, 都对公民个人信息保护提出了明确的法律规定。然而, 尽管如此, 公民个人信息保护依旧面临诸多挑战。比如说存在举证困难、赔偿责任划分等问题。因此, 为了更好地保护公民的合法权益应不断加强法律建设, 加强数据监管, 通过多种方式和手段, 更好地保护公民个人信息安全。本文就大数据视域下核心信息的民法保护进行简要分析, 希望为广大读者提供一些有价值的借鉴和参考。

关键词: 大数据; 个人信息; 民法保护

## 一、民法对个人信息保护的进程分析

在2017年, 我国公布并实施了《民法总则》, 其中对个人信息方面提出了明确的规定, 以此保护我国公民的个人信息隐私安全。随着这一法律的出台, 也成功标志着我国在个人信息保护方面迈出了重要一步。《民法总则》中不仅对个人信息的法律地位进行了明确的规定, 同时还对个人信息收集、使用、传输等方面做出了相应规定, 要求信息处理者必须获得信息主体的批准和同意, 才能够对个人信息进行相关操作。

随着信息技术的飞速发展和广泛运用, 个人信息保护工作的重要性愈发凸显。各种网络平台和应用在给人们的生活带来巨大便利的同时, 也非常容易造成个人信息泄露的风险。《民法总则》的颁布和实施, 为公民个人信息保护方面提供了法律保障, 使他们在面对个人信息遭受侵害时, 能够使用相关法律武器来维护自身的合法权益。

为了进一步落实《民法总则》中关于个人信息保护方面的规定, 我国又出台了一系列配套法律法规。比如说2019年, 国家互联网信息办公室印发了《个人信息出境安全评估办法(征求意见稿)》; 2021年, 我国实施了《民法典》。由此可以看出我国在个人信息保护方面的工作正在逐步进行。《民法典》的实施不仅为个人信息保护提供了更为全面的法律依据, 同时还对个人信息进行了精准的定义, 明确权利主体的权利和信息处理者的应尽义务。除此之外, 为了更好地执行这些法律法规, 相关部门陆续出台了多项细则, 以此确保相关法律具有可操作性和可执行性。

总之, 当前, 我国在个人信息保护方面已经建立了相对比较完善的法律体系, 公民的个人信息受到了有效的保护。

## 二、个人信息受民法保护的必要性分析

首先, 有利于保护信息主体的财产安全和人身安全。在大数据背景下, 随着大数据技术的创新发展和广泛运用, 给人们的生活带来了极大的便利, 同时这也使得每个人逐渐消减了个人信息的控制力量, 非常容易发生个人信息泄露事件, 给信息主体的个人合法权益和财产利益造成极大的损害。通过大数据技术, 能够对信息主体的各种信息进行收集和汇总, 构建出一个完整的、详细的画像。在这种情况下, 个人隐私往往不复存在, 与个人信息紧密相连的交易信息也变得更加透明, 这必将会对个体的财产安全和合法权益造成严重的威胁。不法分子可以利用个人信息从事违法犯罪活动, 甚至对信息主体的人身安全造成直接的威胁。因此, 为了保护公民的信息安全, 维护他们的合法权益, 民法必须确认并保护公民的个人信息, 逐渐完善个人信息法律法规建设, 以此为公民个人信息安全提供有效保障。

其次, 有利于阻止个人信息泄露。在大数据时代背景下, 个人信息被相关企业采集之后, 应对其进行安全存储和保护, 避免发生信息隐私泄露。近些年来, 我国出现一些个人信息被非法收集、利用、分享等事件, 甚至一些企业通过合法渠道收集公民合法信息后存在非法滥用的情况, 这些事件、行为给公民个人信息安全造成了严重的威胁, 在一定程度上影响了公民的正常的生活秩序。公民的个人信息发生泄露, 极易使信息主体产生恐慌情绪, 严重阻碍了社会的经济发展和进步。对此, 为了保障公民的个人信息安全, 提升信息安全意识, 有效遏制个人信息泄露情况的发生, 个人信息受民法保护是非常有必要的, 同时也是法治社会发展的必然之路。

最后, 有助于打击违法犯罪活动。在巨额利益的驱动下, 部分企业个人非法收集公民的个人信息的行为、合法收集信息违法滥用、非法使用虚假个人信息进行诈骗、违法犯罪等, 这些行为将会给信息主体的合法权益造成严重的损害, 同时也会给社会的和谐稳定造成影响。尽管我国刑罚已经对个人信息犯罪进行了明确的规定, 但由于刑罚的谦抑性原则, 只有少数严重的行为才能够受到刑法的制裁。因此, 非常容易导致犯罪分子逍遥法外。助长了他们的违法气焰。与刑法相比, 民法更具灵活性, 在保护公民信息安全方面发挥着重要的作用, 能够有效地制裁个人信息违法行为, 弥补受害者损失, 提升打击犯罪效果。

## 三、民法保护个人信息过程中存在的问题分析

### (一) 传统个人信息保护模式效果不明显

在对个人信息保护方面, 传统的保护模式更加强调信息主体的自我控制, 也就是要求信息主体主要负责个人信息保护。然而在大数据时代背景下, 大数据技术被广泛地运用, 信息主体自身的控制力度被严重削减。然而由于我国当前在个人信息保护方面的工作并不完善, 法律体系并未健全, 缺乏系统性、全面性、专门性的法律体系。因此, 在处理个人信息侵权案件时, 往往根据隐私权方面的法律法规进行处理, 但这些法律条文在一定程度上很难覆盖大数据环境下个人信息保护的复杂性和多样性, 且个人信息的范围远大于隐私信息范围, 非常容易导致发生保护不力的情况出现。而我国《民法典》对个人信息和隐私进行了明确的定义, 并且其中也明确表明获取信息主体的个人信息需要得到其明确授权。然而在大数据时代背景下, 这种授权缺乏一定的真实性和必要性, 无法应对大数据技术广泛运用所带来的挑战。在法院处理相关个人信息侵权案件时, 当前的隐私权保护机制的作用已经不再显著, 个人信息保护也无法过于依赖它。因此, 在大数据时代背景下, 有必要制定相关法律, 对公民的个人信息进行全面保护,

从而避免发生个人信息侵权事件的发生。

## （二）技术发展导致举证困难

举证困难主要体现在多个方面。首先是取证难。在大数据时代背景下，当公民的个人信息遭受不法侵害时，他们维权所需要面对的是实力强大、背景深厚的公司、企业或者相关组织，它们往往以专业技术的方式侵害公民的个人信息，很多侵害个人信息的证据很难获取，只能依靠公权的力量获取个人信息遭受侵害的证据，但此过程也并未一帆风顺。由于技术的专业性和复杂性，公权部门在调查取证过程中往往需要耗费大量的时间和精力，此外，即使这些侵害个人信息的证据被成功获取，但如何证明其真实性和合法性，能够在法庭上被正确理解和采纳，也是一个需要解决的难题。同时，在信息主体丧失信息控制后，一旦发生个人信息侵害案件，由于法律体系并不健全，《民法典》中也并未对个人信息侵权的归责进行特殊标注。因此，法院在审理相关案件时往往采取谁主张，谁举证的原则。也就是说信息主体不仅要证明确实存在有侵权行为的发生，并且该侵权行为对自身的合法权益造成严重的损害，同时还需要证明主要是相关企业的技术存在一定风险，导致自身合法权益遭受损害，即要证明过错与合法权益损害结果之间存在关系。若无法成功举证，则将要大概率承担诉讼失败的后果。然而由于原告与被告之间存在着一定的差距，它们之间的信息、认知能力等方面存在着一定的不对称，且侵权方式、侵权地点存在着隐蔽性、虚拟性等特点，这导致受到侵害的一方很难获取相关证件，质证也无从谈起。

## （三）侵害个人信息赔偿责任不明确

在处理具体的司法案件过程中，关于个人信息侵权案件，法官往往以侵犯隐私权、人格权等方式予以处理。一般情况下，要求侵权方立即停止个人信息的侵害行为，判决其进行赔礼道歉，这些行为都能够得到有效的执行。然而，一旦涉及财产性赔偿和精神损害赔偿等相关问题时，这些判决往往无法有效执行。在研究关于个人信息侵权的相关案件时，值得注意的是，受害者在精神损害赔偿方面，法院的判决标准相对较低，他们能够获取的经济培养或者其他形式的赔偿相对有限。显然，这种补偿程度对受害者来讲是远远不够的。个人信息不仅强烈的人身属性，同时它的财产价值也不应被忽视。由于个人信息财产价值确实客观存在，尤其是在大数据时代下，这一观点被广泛认同。当个人信息受到不法侵害，他们的信息被滥用，除了给信息主体造成经济损失之外，还会对他们的精神生活造成严重损害。若无法给予受害者一定赔偿，这不仅无法体现出法律的公平性和公正性特点，无法为公民提供全面、有效的法律保护，同时也无法对侵害者形成一种强力震慑，有效阻止后续类似事件的发生。因此，有必要明确赔偿机制，以此更好地保障公民的个人信息安全，从而营造良好的社会环境。

## 四、个人信息民法保护的完善措施

首先，应统筹资源，构建统一的信息监管机构。为更好地应对个人信息遭受侵害问题，应建立统一的信息监管机构，通过这样的方式，更好地保护公民的个人信息免受不法侵害，同时加强企业信息监管，促使其更好地履行责任和义务，防止企业滥用个人信息。机构应对企业数据利用进行重点监管，充分发挥自身的监管、审批职能，充分协调个人信息保护工作与相关部门的关系，确保其在知法地位在法律层面得到认可。机构可以设置为地方性和全国性两种，分别负责地方区域和全国范围内的个人信息保护工作。地方性机构需要定期向中央性机构汇报工作进展情况，并

积极配合其指导。同时加强对地方企业数据信息采集、利用等方面的监管。

同时，在大数据时代背景下，作为数据利用企业，也应该紧跟时代发展趋势，积极成立相关部门或机构，由制定员工或专门机构负责与个人信息监管机构进行对接。相关企业需要定期向监管机构汇报信息保护方案以及具体措施。相关工作人员应为企业提供有效的个人信息业务方案，并积极参与到个人信息采集、使用、存储等工作中。此外，企业应加强关于个人信息方面的人才培训和审查工作，定期组织和开展自查活动，及时发现隐藏风险和隐患，并及时进行处理，避免公民个人信息遭受侵害，从而影响公司的正常运行。

其次，优化举证责任。在司法具体实践过程中，举证责任可以通过过错推定方式进行分配。具体来讲，当原告的合法权益受到不法侵害时，有证据表明侵害是由被告造成的，若被告无法提供相应证据证明自身并无如何过错，则可以推定被告应承担相应的民事责任。采用过错推定原则的原因在于：作为自然人，公民无法详细了解相关企业、机构的运营、生产以及销售等情况，这使得他们难以获取有效证据。因此，在证据收集过程中，自然人往往处于弱势一方，面临显著的不利条件，若要求自然人提供证据证明企业在处理个人信息过程中存在一定的过错，是难度较大的。这显然无法体现出法律的公平性和公正性。

因此，法院采取过错推定的原则，通过这样的方式，能够最大程度上避免由于原告无法提供相应证据而导致诉讼失败的情形发生。同时，对于企业经营者来讲，对信息主体造成事实损害也就意味着其已经违反了相关法律，此时就可以认定企业是过错方，侵害用户的合法权益，进一步推动相关案件的快速处理。

最后，采取惩罚性赔偿制度，提升违法成本，形成有力震慑。采用这一制度在处理个人信息案件、减少同类案件的发生、更有效地维护信息主体合法权益方面具有重要的现实意义。当相关企业发生侵犯公民个人信息时，有必要对它们采取严格的惩罚措施，尽管会在一定程度上影响企业的正常运营，但也能够发挥出警示作用，使相关企业更加重视和关注公民个人信息保护意识和合法利用意识。此外，在进行惩罚性赔偿时，也应该充分考虑案件的实际情况，结合主观恶性性，避免出现不合理判罚，从而对企业发展造成严重影响。

## 五、结束语

总之，在大数据时代背景下，对个人信息方面的保护尤为重要。当前，我国逐渐完善了相关法律法规，但依旧存在着一些问题。对此，为了更好地保护公民的个人信息安全，应不断完善法律法规，并成立相关监管机构，对相关企业、机构等进行定期监管。同时也要优化举证责任分配，并采取惩罚性赔偿制度，提升违法成本，对相关违法企业、个人等形成有力震慑，以此更好地维护公民的合法权利，构建和谐、安定的社会环境。

## 参考文献：

- [1] 王浩然，施小焱. 大数据视域下未成年读者个人信息保护研究[J]. 南海法学，2023，7（04）：33-43.
- [2] 林秀梅. 大数据时代背景下个人信息的民法保护研究[J]. 法制博览，2023（22）：79-81.
- [3] 汪瑞. 大数据下个人信息的民法保护研究[D]. 安徽财经大学，2022.