Open Journal of Legal Science 法学, 2024, 12(7), 4765-4771
Published Online July 2024 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2024.127678

Hans汉斯

个人信息保护问题及对策研究

张小宇

新疆财经大学法学院，新疆 乌鲁木齐

收稿日期：2024年5月31日；录用日期：2024年6月19日；发布日期：2024年7月30日

摘　要

在大数据时代的背景下，因回应中国人民对个人信息保护的迫切需求，我国2021年1月1日起施行的《民法典》已明确将个人信息保护以法律形式进行明文规定；除此以外，《个人信息保护法》作为我国首部关乎个人信息保护的单行法规的颁布应运而生，自此，我国个人信息的法律保护进入全新时代。法律的出台虽然在一定程度上回应了现实的需求，但并未终结有关个人信息保护的争论。如何在个人信息保护与合理使用之间维持平衡，仍有深入研究的必要。

关键词

个人信息保护，民法，个人隐私

Research on Problems and Countermeasures of Personal Information Protection

Xiaoyu Zhang

Law School, Xinjiang University of Finance and Economics, Urumqi Xinjiang

Received: May 31st, 2024; accepted: Jun. 19th, 2024; published: Jul. 30th, 2024

Abstract

In the context of the era of big data, in response to the urgent need for personal information protection in China, the "Civil Code" implemented on January 1, 2021 has clearly stipulated the protection of personal information in legal form; in addition, the Personal Information Protection Law, as the first single law concerning the protection of personal information in China, came into being, and since then, the legal protection of personal information in China has entered a new era. Although the introduction of the law has responded to the practical needs to a certain extent, it

文章引用: 张小宇. 个人信息保护问题及对策研究[J]. 法学, 2024, 12(7): 4765-4771. DOI: 10.12677/ojls.2024.127678

has not ended the debate about the protection of personal information. How to maintain a balance between the protection of personal information and reasonable use, there is still a need for in-depth research.

Keywords

Personal Information Protection, Civil Law, Personal Privacy

1. 引言

大数据时代，个人信息泄露的情况已司空见惯，从快递包装上的信息到在网站上因公因私填写的更为详尽的信息，轻则为我们带来垃圾短信，骚扰电话的困扰，重则发生诈骗、银行账户的钱被盗、冒名办信用卡透支等案件也已屡见不鲜。然，“徒善不足以为政徒法不能以自行”个人信息的保护除却人人自身增强保护意识，法律制度的保护及惩罚的措施更为重要。虽在大数据时代的背景下，因回应中国对个人信息保护的迫切需求，我国 2021 年 1 月 1 日起施行的《民法典》已明确将个人信息保护以法律形式进行明文规定，在总则编第五章中，“自然人的个人信息受法律保护”在民事权利保护一部分中熠熠生辉；除此以外，人格权编中也在其第六章详细对个人信息的概念及保护规则进行了界定。为更能有效地保护个人信息，2021 年 8 月，《个人信息保护法》作为我国首部关乎个人信息保护的单行法规的颁布应运而生，自此，我国个人信息的法律保护进入全新时代。法律的出台虽然在一定程度上回应了现实的需求，但并未终结有关个人信息保护的争论。如何在个人信息保护与合理使用之间维持平衡，仍有深入研究的必要。

2. 个人信息概述

(一) 个人信息概念及泄露的危害

个人信息，在本文语义内是指中华人民共和国境内的公民个人信息，在形式上，广义上来说，以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息即可称作个人信息，例如公民的姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等都在此列。狭义上是指根据《个人信息保护法》第四条的规定能够纳入法律保护的个人信息，在法律条文的限缩解释内，是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，匿名化处理后的信息不能被包括在其内。

个人信息泄露，按照文义解释，是指个人的敏感信息、隐私内容在个人的社交活动中无意或有意地被第三方获取、公开或使用的行为。个人信息泄露可造成如下后果：一、易引发非法活动的发生，比如冒用他人身份后，不法分子常常以他人的名义进行金融诈骗、开展网络欺诈等违法犯罪活动。这既损害了公民个人的财产利益，又破坏了社会的信任关系；二、个人信息泄露往往会直接导致个人隐私的曝光。个人隐私是指公民个人不愿为他人所知的自己的个人生活的秘密，而个人信息的泄露往往会使这些秘密信息大白于天下，在群众目光的聚集下，人无完人，个人隐私被肆意评价往往会致使个人形象和声誉受到负面评价和攻击，对个人的社交关系和职业发展进行严重打击甚至完全摧毁；三、个人信息泄露可以

上升到威胁到国家安全和社会稳定层面，在信息化的时代，个人在网上的注册信息、所发评论、所转文章和活动轨迹等会透露个人的政治倾向、个人爱好、职业等。这些信息量庞大的数据经过精细化的分析，可以作为国与国之间外交政策、军事或非军事斗争和对外宣传的有力参考。在大数据时代，信息技术的井喷式发展和智能化应用的广泛普及使得原本难以获取的个人信息成为社会经济活动中不可或缺的资源，同时也成为黑客、网络犯罪分子等攻击的目标。因此，加强个人信息的保护显得尤为重要[1]。

(二) 域外个人信息保护的立法比较

作为联邦制国家德国，采用的是统一的个人信息立法。德国将个人信息作为法律上的基础概念纳入了人格权范围，为此制定了专门法律加以保护。《联邦个人资料保护法案》由德国国会在 1970 年开始制定，后在 1976 年被批准通过，于 1977 年正式生效。德国联邦政府与其州政府都制定了个人信息保护法，其保护范围除了政府之外，民间行业也广泛牵涉其中。1977 年，德国国会通过的《防止个人资料处理滥用法》使德国率先成为在公领域和私领域中统一立法对个人信息进行保护的国家之一。

1983 年，德国宪法法院在“人口普查法案”一案中，于判决书中首次使用了信息自决权的概念，肯定了个人信息权在德国宪法中的一席之地。此外，还将国家安全机关对个人信息的搜集与处理方法纳入法律保护范围。随后，1990 年的法律修订将非国家机构处理个人信息所形成的民事法律关系与国家机构处理个人信息形成的行政法律关系纳入同一部法律中进行统一规制，在传统立法模式上首次创新性的呈现出不同步的交叉。这种统一交叉立法模式对大陆法系造成了深远的影响，甚至对英美法系的国家也产生了较大影响[2]。

美国信息保护采取了以隐私权为基础的分散立法模式，在美国并不存在任何一部集中保护个人信息的基本法律，相关规范全部分散于不同的公共领域法律之中。美国宪法作为美国的根本大法，为公民个人信息的保护提供了坚实的基础，在公共领域，以电子监听和隐私保护为例，美国的《联邦通讯法》中，以第 605 条保护了电子通信中的信息隐私，但其范围较为狭窄，在电子通信领域之外不具有普遍适用性。直到 1968 年，《全面控制犯罪活动与街道安全法案》第 3 章才终于对美国电子监听立法进行了统一，法律的规制范围包含了联邦、州以及个人的监听行为。随着电子监听技术的发展，国会在 1986 对此部法律进行修正后，正式出台了《电子通讯隐私法》，该法案具有创新性的将电子邮件、移动通话设备的监听全部纳入保护范围，直接将截取电子通信的行为定性为犯罪，并对因此造成的对个人信息的侵犯赋予民事救济。

除上述方面，在个人信息隐私保护领域美国仍存在大量其他立法，例如：1974 年的《美国隐私法》是为规范国家机关处理个人信息的行为而设定；而《公平信用报告法》是针对私人机关的；《家庭教育权利与隐私法》；《儿童隐私保护法》是专门针对学生与家长的个人信息保护的，其中明确规定，如需收集 12 周岁以下的儿童信息，务必要征得其监护人的同意；此外，联邦政府也不能成为例外，在联邦政府接触银行内个人账户时需要遵循《金融隐私法》的规定。

美国分散立法的模式能够保证行政行为的顺利实施与商业活动的正常进行，亦能起到防止立法权力集中膨胀的作用，这种多元化格局让美国能对个人信息进行相对全方位的保护，针对不同领域制定出的不同法律能够在最大程度上将个人信息保护的细致、准确，在个人信息遭受侵害时，公民也能采取高度吻合的救济措施。然而，分散立法模式的过度分散也会带来弊端，当法律条文过于纷繁复杂，不同领域之间的立法不可避免地产生了许多矛盾和重复，使得法律本身发生冲突很难达到和谐共生[3]。

在欧洲，信息保护被认为是一项基本人权。德国联邦法院在 1984 年率先提出“信息自主权”后，欧盟于 1995 年通过了《欧盟数据保护指令》，这部法案是欧盟关于个人信息保护最主要的立法。一方面该项指令通过对收集程序、收集对象的规制防止信息控制者过度用权，设定相应义务以避免信息控制者与

信息主体之间的地位悬殊。另一方面，该指令同时赋予信息主体权利，在立法中对个人信息主体增加了强行法的保护，即个人信息保护的权利不允许当事人自行放弃。

欧盟的个人信息保护立法在全球有很大影响。例如新西兰、阿根廷等非欧盟国家和地区也参考欧盟的立法制定了个人信息保护法。

3. 个人信息保护的司法实证基础

根据沃耘，乔鹏飞所发表的文献数据[4]，在2001年以前，在知网平台上鲜少有学者以“个人信息”为主题进行发文，从1980年以来，每年以此为主题的文献两均在两位数范围内，自2001年该主题的年文献量为141篇，为二十多年来首次超过一百篇。此后，至2007年为517篇，至2010年为1259篇，至2022年已达到了5858篇。“个人信息”主题文献的井喷式增长体现了民众迫切的需求，因此《民法典》关于个人信息保护的部分及单行法规《个人信息保护法》应运而生，然而两部法律毕竟出台时间尚短，叠加法律本身具有的滞后性，司法实践中存在着诸多问题。例如在案例中自然人的自主维权为主，民事公益诉讼极少发挥作用，然批量型案例较多，民事公益诉讼制度未能得到有效发挥；因《民法典》对个人信息的界定无法进行穷尽式列举，而是根据语义采用了以“等”为示例的开放性立法，将明文列举之外的其他信息也纳入了保护范围。但并非所有以电子或者其他方式记录的信息都能直接纳入《民法典》所保护的个人信息范围，当将“可识别性”作为核心要件时，司法实践中仅有个别案例详细论述了无名个人信息保护的正当性与合理性，并未深入探究“可识别性”的标准；此外，个人信息与隐私权在司法层面的区分并不显著。相关案例的判决结果显示，非法使用和非法公开是个人信息侵权的主要表现形式，而侵权不成立的首要理由为证据不足。在大数据时代APP或网络平台因天然地位优势往往能够掌握大量信息，而公民个人处于弱势地位。除证据不足之外，不成立的主要理由为“原告知情且同意”“处理行为合法、正当、必要”和“信息不具有私密性”，。但私密信息的认定标准不详，司法实践中大多以“未涉及私人生活安宁”“未证明不愿为他人知晓”为由一笔带过。

4. 个人信息保护的困境及问题

(一) 个人隐私与个人信息范围模糊

法律需要具备一定程度上的准确性，当法律条文用词模糊，就会为实践中的案子留下太多的解释空白，实践中法官往往不敢轻易为法律没有明确规定的定义进行解释，抑或由于个人的局限性做出错误解释，个人隐私范围的界定如今并没有明确的直接来源于法律条文的标准。当政府信息涉及第三方个人隐私时，信息公开主体和法院对个人隐私与个人信息的理解经常出现分歧和混乱，从而导致出现不同的裁判结果。在新技术、大数据的快速发展下，传统的隐私概念也确实具有一定的滞后性，与实践需求不能进行很好的衔接，这也是法律文本和技术文本之间出现鸿沟的原因之一。在互联网时代，万物互联，信息技术对个人隐私保护带来的冲击显著提高了隐私保护的难度。智能终端可以跨越时空的阻隔，随时随地搜集人们的行为轨迹和生活习性等个人资料，使“隐”慢慢地消失。同时，社交平台、网络直播等媒介促使人们积极展现自己的图像和生活情景，使得“私”的界限难以把握。在大数据和人工智能强大的信息采集、整合、分析能力下，一些原本不涉及个人隐私的信息被联系到一起后，也能拼凑转换成个人不愿为人所知的隐私信息。因此，个人隐私与个人信息的界限需要根据经验上进行补足，不能因不侵害个人隐私权就认定为不侵害个人信息，同时侵害个人信息并不一定意味着侵害了个人隐私。

(二) 个人信息“可识别性”标准不明

我国《民法典》第1034条第2款以“抽象定义 + 开放列举”的方式界定了个人信息，其核心要求是“可识别性”。这种“可识别性”的要求可从两个方面予以解读：一是并非所有明文列举的信息就当

然地构成个人信息，仅有根据所列信息可以识别到特定自然人的有名信息才属于《民法典》的保护对象；二是并非其他未被列举的无名信息就不属于个人信息，有些信息看似无关紧要，但只要通过该信息能够成功对特定自然人进行识别，就应当成为《民法典》的保护对象。因此，“可识别性”标准应属司法实践重点论述的对象。绝大多数案件对于无名个人信息的认定仅以《民法典》中规定的“可识别性”之表面含义为依据，并未对“可识别性”的实质含义或要求作出解释。

(三) 公益诉讼的制度效用尚未充分发挥

计算机网络时代的到来，改变了信息通过口耳相传或档案记载等传统的信息传播方式，各类个人信息被通过各种技术、各种方式记录下来，并被用来查询和分析个人消费偏好、健康状况、征信状况等，导致个人信息具备的不仅仅是私人性特点，而是更加偏向于公共性和社会性。因此，个人信息保护也应当从个人保护转向社会保护。社会保护的有效实现机制之一就是起源于罗马法的公益诉讼。针对大规模的个人信息侵权行为，传统的私益诉讼方式难以全面保护个人信息权益。当大规模的个人信息侵权案件发生，往往出现个人受到的损害轻微，致使当事人认为不值为此提起诉讼的现象，然而受害人数众多，总体损害后果不能以轻微概论[5]，在这种情况下，作为微小个体的众多自然人需要有一个集体的权利代言人。

5. 个人信息保护问题的对策研究

(一) 厘清个人隐私、可识别性、合法正当必要等界限

目前我国民法并未将个人信息单独确立成为一项民事权利加以保护，故可考虑在“个人信息”后面加上“权”字，明确规定个人信息权。这样既可以为特别法提供上位法依据，也能够落实个人信息司法保护的需求。同时，还应当区分隐私信息和个人信息[6]。此外，还需进一步明确个人信息与公民隐私之间的界限，将二者之间的不相重合部分加以界定，以便于在司法实践中，裁判者能更好地区分具体案由归属并做出正确的、合乎具体情况的判决。

个人信息只有充分流通才能实现其所蕴含的经济价值，既要保证其有效的流通又要保证其得到良好的保护，在实践中，合法、正当、必要三项原则如何把握也关乎着个人信息保护与流通利用的平衡。为了避免各方当事人对合法、正当、必要原则出现理解偏差，应当限制使用个人信息的目的、手段、程度、内容等，使个人信息的使用呈现出程序化的特点，避免出现在把握和运用上偏向某一方当事人。所谓“合法”指收集、存储、加工、使用、提供、公开等处理活动应严格遵循法律法规的规定，这里的“法律法规”应采取广义解释，不应局限于全国人大及其常委会所制定的法律，应包括各种法律法规及规范性文件等。“正当”即指目的特定、明确、合理。对目的作出严格限制，避免失之宽，同时也应当考虑为了充分挖掘信息的流通价值，可以允许处理者根据现实需求而适当改变其目的，但是变更后的目的不得与原目的存在过大差异，需要具有一定的关联性，且不可随意变更，如履行一定的告知同意程序。目的不仅应特定、明确，还必须合理。目的合理要求公私主体在处理个人信息时，应符合公共与集体的利益和个人的合法私利[7]。“必要”是指处理活动对于实现处理目的而言是必要的，凡是不必要的都不应开展。该原则是比例原则在个人信息保护领域中的体现。在民法中，比例原则意味着“只有在以下情形当中，个人自由及其私法自治才能受到干预，即对于维护更高的利益而言这是必要的，且此种干预既适于实现预期的目标，也是实现该目的的最缓和的方式。

(二) 举证责任优化

基于消除个人信息保护争讼双方经济、科技等力量的不平等性所导致的举证责任分配的负面影响，若将过错责任原则作为唯一的归责原则，并不能满足目前的司法发展需要。对此可以借鉴域外立法模式，例如德国所采取的不同类型的主体适用各自不同的相应归责原则的模式。立足于我国国情，针对不同的

主体采取不同的归责原则，可考虑把侵权主体划定为自然人、国家机关和非国家机关，并规定自然人则采用过错责任原则，国家机关采用相对更为严格的无过错责任原则，非国家机关运用过错推定责任原则[8]。具备举证责任能力是当事人承担举证责任的前提条件，然而自然人的举证责任有限，若机械性地将举证责任分配给举证责任先天弱势的公民，相当于将诉讼流于形式直接宣告无举证能力一方败诉承担不利的法律后果[9]。在司法实践中，应当给处理者分配承担信息使用情况以及履行保证信息主体信息安全义务的举证责任。此外，《最高人民法院关于民事诉讼证据的若干规定》第四条举出了八种特殊侵权行为，并为之设置了相应的举证责任。个人信息侵权并未被纳入这八种特殊情形之中，相较于信息控制者，信息主体处于劣势地位难以证明因果关系要件，可考虑适时地将个人信息保护的举证责任纳入其中。再者，在处理民事案件时不能仅适用“谁主张，谁举证”的责任分配模式，具体问题具体分析使举证责任变得灵活在个人信息保护的案件显得格外重要。

(三) 构建惩罚性赔偿制度

前述所述，个人信息泄露导致的后果并不仅能损害个人权利，对国家集体等公共利益往往也能造成较大冲击，此种价值取向要求个人信息权益的保护不可仅仅停留在个体主义的视角上。现行个人信息损害赔偿制度将大规模个人信息受到侵害时导致的“社会性损失”排除在损害赔偿制度的赔偿范围之外。然惩罚性赔偿不仅可以填补已经造成的社会性损失，能够恢复受损的整体利益，还能作为发挥法律的惩罚功能与教化功能，震慑不法分子，防止信息社会整体利益再次受损。

(1) 主体：除却受侵害的公民个人作为个体可以提起诉讼或者选出代表进行集体诉讼，《个人信息保护法》在实质上已经授予了包括消费者组织、国家网信部门指定的组织以及人民检察院在内的相关主体权利，这些主体都可以对广泛侵害公民个人信息权益行为提起公益诉讼。

(2) 主观要件：应以故意为主观构成要件。《民法典》中的第 1185 条、第 1207 条与第 1232 条，明文规定了对于适用于惩罚性赔偿的三种案件类别都应具备侵权主体的“明知”或者“故意”等主观要件。对侵权者主观故意的考虑，不失为评估惩罚性赔偿制度适用的一项综合权衡因素[10]。带有明显故意性质的侵权人往往造成的后果严重，这种情况下，实行惩罚性赔偿显得尤为必要。在个人信息侵权案件的实践中，侵权人往往为了牟取可观的非法经济利益，故意向他人泄露或售卖大量个人信息，这种行为对大量公民的信息安全都产生了严重威胁。利用非法手段得到的个人信息可以让更多的违法犯罪分子去实施针对性极强的诈骗行为，大大增加了作案的成功率，直接后果则是涉案金额暴增，同时也给受害者带来了重大的财产损失与心灵创伤。故在个人信息权益保护相关的公益诉讼中，决定被告是否应当承担惩罚性赔偿的关键因素应为行为人是否存在明确的主观故意。

(3) 应以情节严重作为酌定要件。惩罚性赔偿的适用应当严谨审慎，考虑到惩罚性赔偿中惩戒的特性明显，情节轻微的案件不宜采取这种严厉的举措。在个人信息保护案件中，以“构成严重威胁人身或财产安全的不合理危险”作为情节严重的标准不失为一个方法[11]。

参考文献

[1] 连烨莹. 大数据时代个人信息保护问题研究[J]. 厦门科技, 2024, 30(2): 47-49.

[2] 陈清. 大数据时代个人信息法律保护路径研究[J]. 社科纵横, 2024, 39(2): 91-96.

[3] 蒋破. 国际信息政策法律比较[M]. 北京: 法律出版社, 2001: 187.

[4] 沃耘, 乔鹏飞. 《民法典》背景下个人信息保护的司法考察与制度完善[J]. 征信, 2024, 42(5): 31-42.

[5] 张新宝, 赖成宇. 个人信息保护公益诉讼制度的理解与适用[J]. 国家检察官学院学报, 2021(5): 55-74.

[6] 金辉. 建立完善的个人信息保护制度[N]. 经济参考报, 2019-12-31(08).

[7] 刘权. 论个人信息处理的合法、正当、必要原则[J]. 法学家, 2021(5): 1-15.

[8] 孙淑婷, 阿依加马丽·苏皮. 《民法典》背景下个人信息侵权举证责任探究[J]. 山西省政法管理干部学院学报, 2022, 35(1): 46-49.

[9] 秦华, 高允菁. 个人信息保护的当下困境及司法应对——以手机 APP 对个人信息的使用为切入点[J]. 天津法学, 2022, 38(2): 55-70.

[10] 高志宏. 惩罚性赔偿责任的二元体系与规范再造[J]. 比较法研究, 2020(6): 185-198.

[11] 于丰笛, 刘蓓. 论个人信息保护领域惩罚性赔偿制度的构建[J]. 长春理工大学学报(社会科学版), 2024, 37(2): 38-44.