Dispute Settlement 争议解决, 2025, 11(11), 176-185
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.1111358

Hans汉斯

数据平台对个人信息的侵权责任研究

岳钰淇

青岛科技大学法学院，山东 青岛

收稿日期：2025年10月19日；录用日期：2025年11月13日；发布日期：2025年11月21日

摘　要

随着大数据时代的到来，数据平台作为当下个人信息的主要处理者，在商业实践中广泛收集、存储、分析个人信息。然而，数据平台因商业需求对个人信息处理的不断扩大，导致个人信息侵权事件不断发生。近年来，个人信息泄露、滥用、深度伪造等案件频发，引发了公众对个人信息安全的广泛关注，但这一关注下却存在损害认定难、举证责任难、认定主体难、赔偿标准不一等问题。本文主要分为四个部分，第一部分主要分析个人信息的概念和类型，并对本文所述个人信息侵权概念和类型进行区分。第二部分论述个人信息侵权责任的构成要件，包括行为人存在过错，行为人实施违法行为即行为违法性，被侵权人权益受损即损害事实，损害与加害行为间的因果关系。第三部分是我国现有个人信息侵权责任制度中存在的不足，包括损害认定难、举证责任难、责任主体认定难，损害赔偿计量难。第四部分是对个人信息侵权责任制度的完善建议。

关键词

个人信息，侵权责任，构成要件，损害救济

Research on Liability for Infringement of Personal Information in Data Platform

Yuqi Yue

Law School, Qingdao University of Science and Technology, Qingdao Shandong

Received: October 19, 2025; accepted: November 13, 2025; published: November 21, 2025

Abstract

With the advent of the big data era, data platforms have become primary processors of personal information, extensively collecting, storing, and analyzing such data in commercial practices. However, as data platforms expand their processing of personal information for commercial purposes, cases of personal information infringement have become increasingly frequent. In recent years,

文章引用: 岳钰淇. 数据平台对个人信息的侵权责任研究[J]. 争议解决, 2025, 11(11): 176-185.
DOI: 10.12677/ds.2025.1111358

incidents of personal information leaks, misuse, and deepfakes have sparked widespread public concern about personal information security. Yet beneath this concern, challenges persist in determining damages, burden of proof, identification of liable parties, and inconsistent compensation standards. This paper is divided into four sections: The first section analyzes the concept and types of personal information, distinguishing between the infringement concepts and categories discussed in this paper. The second section examines the constitutive elements of personal information infringement liability, including the actor's fault, the illegality of the act, the infringement of the aggrieved party's rights, and the causal relationship between the damage and the harmful act. The third section identifies shortcomings in China's existing personal information infringement liability system, including difficulties in damage assessment, burden of proof, identification of liable parties, and compensation calculation. The fourth section proposes recommendations for improving the personal information infringement liability system.

Keywords

Personal Information, Tort Liability, Constitutive Elements, Damage Relief

1. 个人信息的概念和界定

1.1. 个人信息的概念和定义

1.1.1. 个人信息的概念

个人信息这一概念是在上世纪西方国家引入计算机办公后，逐步将大量公民基本个人信息纳入政府数据库后产生的，从文义解释来看，信息是指音讯、消息系统传输和处理的对象，泛指人类社会传播的一切内容，故而在此之前对“个人信息”这一概念更多的被理解为带有公民个人特色的、能够传播个人情况的内容。随着个人信息这一概念的提出，对这一概念的争论也从未停止。

国内学界对个人信息概念的传统理论界定主要有三种模式，即“隐私型”、“关联型”、“识别型”三类，进入数字时代后还有学者提出了场景理论。传统理论中“隐私型”界定模式认为个人信息和隐私是两种概念，但出于认可个人信息的隐私利益，主张以隐私权保护为基点的个人信息保护途径[1]。“关联型”界定模式认为与主体存在一定程度的关联信息就是个人信息[2]。“识别型”界定模式认为个人信息概念问题实质上就是讨论“可识别”问题[3]。场景理论则认为个人信息权益不能与场景割裂开来，合理的做法是将个人信息权益保护置于共同体或某种关系网中加以思考，结合具体场景判断该情形是否侵犯个人信息权益[4]。

当今世界，个人信息的概念在绝大多数国家都采用“识别型”界定模式，我国立法上也同样采取了“识别型”界定模式作为个人信息概念的界定方式，即个人信息应当是可以通过内容特征的识别来确认个人情况内容的信息。2016 年颁布的《网络安全法》在附则第 76 条第 5 款中将“个人信息”界定为可以单独或者与其他信息结合识别出自然人身份且被记录下来的各种信息 [1]。《民法典》则在此基础上重申了个人信息是能被识别出特定自然人身份的信息，并且将个人信息权益与隐私权作出了区分，极大幅度减少了国内对个人信息权益与隐私权混同使用的情况。2021 年颁布的《个人信息保护法》第 4 条规定：“个

[1]详见《网络安全法》第 76 条第 5 款。

人信息是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，不包括匿名化处理后的信息。”该项规定重申了个人信息的“可识别性”特征。结合我国立法状况来看，“识别性”是个人信息相关法律所保护的个人信息的基本要求，个人信息的概念也可以理解为能够识别自然人身份的信息。

1.1.2. 个人信息的定义区分

个人信息与个人数据不同。从个人信息的定义来看，此前学界存在将个人信息与个人数据混用、混同等情况，认为个人信息等于个人数据。但事实上，个人数据和个人信息存在完全不同的定义。就技术层面来看，数据本质上是计算机运行中代码“0”和代码“1”的堆叠和排列，而信息则是人类社会中传播的内容。从个人信息与个人数据这一子概念来看，个人信息应当是能够被识别的，且能够识别出特定自然人身份的信息；而个人数据则侧重于由个人在计算机上形成的代表特定含义的代码。早期有学者认为：“英文中信息是指经过加工后的数据，能影响接收者的行为，对接收者的决策亦有价值意义，即知识或消息”[5]。但事实上，信息在计算机上被人为加工、整理、组合后才成为数据，其本身并不会直接成为数据，这也意味着数据通过信息的加工而成为信息的载体，信息则在加工后成为数据的内涵，从这一点来看二者虽然不同但也互为表里，故而不可将个人信息与个人数据混为一谈。《民法典》第 111 条和 127 条对个人信息与数据的分别规定也论证了这一观点。

个人信息与隐私不同。上文提到对个人信息的概念曾有“隐私型”界定，主张以隐私权保护个人信息，但随着《民法典》的颁布，个人信息与隐私被区分开来。从信息保护这一角度来看，个人信息强调对自然人身份识别的保护，即保护自然人身份不被轻易识别、认出；而隐私则强调信息的私密性，隐私的所属人其在主观上不愿意该信息被大众所知，更遑论被识别出，故而在定义上要区分个人信息与隐私。当然，随着互联网的发展，数据平台对个人信息的收集、储存、分析难免涉及到个人的隐私，包括出行记录、酒店记录、活动轨迹、医疗信息等，此时对个人信息和隐私的保护就会存在一定交叉，但实践中的交叉并不影响定义上区分，对二者仍不能混同。

1.2. 个人信息侵权的概念和类型

1.2.1. 个人信息侵权的概念

我国并未在法律层面明确规定个人信息侵权的概念和类型，但可以从个人信息保护的角度出发，反向梳理和提炼个人信息侵权的概念。《个人信息保护法》第 1 条规定：“为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。”第 10 条规定：“任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。”从以上条文可以看出，个人信息保护法的宗旨并非个人信息自决权，而是防范抽象的人格侵害或财产侵害的危险[6]。具体而言，个人信息的非法处理行为可能导致个人隐私的泄露、人格权财产权的受损，甚至非法获取的个人敏感信息可能被用于电信诈骗、网络诈骗等违法犯罪。故而，笔者认为可以将个人信息侵权的概念定义为，个人信息控制者(数据平台)或者第三人非法收集、使用、加工、传输他人个人信息，非法买卖、提供或者公开他人个人信息，侵犯个人信息主体的人格权益或对个人信息主体造成财产侵害的行为。

从该概念定义来看，个人信息侵权所造成的人格侵权和财产侵权与传统人格权益侵权和财产权益侵权有着明显不同。传统的人格权和财产权其侵权风险是可预测的，其侵权后果是可预估的，侵权行为直接触及到被侵权人并对其造成损害结果。个人信息侵权并不直接触及人格权和财产权，而是依靠个人信息为媒介进行穿透，通过个人信息可识别的特性来穿透到具体的个人人格权和个人财产权，而个人信息的可识别性特征分别决定了个人信息长期内的稳定性，导致个人信息在侵权人掌握后将长期处于风险之中，并且无法预测损害结果何时发生。

1.2.2. 个人信息侵权的类型

从个人信息侵权的行为性质来看，个人信息侵权可分为个人信息非法收集、个人信息非法传播、个人信息非法使用三个维度。个人信息的非法收集主要侵犯个人信息主体的知情权和同意权，在个人信息主体没有知情且同意授权的情况下收集个人信息主体的个人信息明显超出一般信息收集的限度，此时的非法收集就为后续个人信息泄露埋下伏笔。个人信息的非法传播则会带来个人隐私泄露的风险，前文提到互联网时代个人信息与个人隐私往往交叉于一起，而隐私权作为人格权就可能因为个人信息的泄露导致人格尊严受到侵犯。而个人信息的非法使用则影响着个人信息主体对个人信息的自决权，当个人无法控制自身身份信息的使用时，那么必然造成其名誉、尊严、财产等众多方面的损失。个人信息非法收集、个人信息非法传播、个人信息非法使用这三个维度并非是独立存在的，而是形成一个完整的闭环。例如，某母婴 App 涉黄案件中，当孕妇在该 App 完成注册后，就会被 App 收集各类个人信息并链接到丈夫的相关信息，随后就会出现丈夫的手机被涉黄短信精准轰炸的情况。此时的逻辑闭环是，孕妇注册后个人信息被非法收集即被盗取或被贩卖，随后大量相关信息被非法传播即被下游买家购买，最后这些信息被非法使用即不法分子将涉黄短信精准发出。

从个人信息侵权的损害后果来看，个人信息侵权可分为财产权益损害和人格权益损害。财产权益损害是指个人信息被非法收集、传播、使用后，个人信息主体被诈骗、盗取财产所带来的经济损失。而人格权益损害则是个人信息被非法利用或传播导致的名誉受损、尊严受侵犯等。从发生阶段来看可以分为直接损害和间接损害。直接损害是指数据平台直接对个人信息的处理导致个人信息受到损害，而间接损害则是作为个人信息处理者的数据平台与数据主体之外的第三人的介入行为导致的“下游损害”[7]。第三人从个人信息处理者处获取个人信息的方式有两种，一种为合意方式，即通过订立承揽、买卖等合同合法获取，另一种为非合意方式，即非法盗取个人信息处理者的数据库而获取[7]。无论哪种方式，第三人都存在不法滥用或因储存、保管不善导致人格权益或财产权益受到侵害的可能，这种损害并不直接来自数据平台这一处理者，而是由第三人介入引起的，故而为间接损害。

2. 个人信息侵权责任构成要件

2.1. 侵权行为人的过错

我国《民法典》第 1165 条规定，我国的过错侵权责任主要分为一般过错侵权责任和过错推定侵权责任，而一般侵权中多适用一般过错侵权责任，只有法律明文规定时才适用过错推定责任。过错推定责任一般依据法律特殊规定，直接依照侵权行为所造成的损害后果来推定行为人的过错[8]。过错推动责任多适用于行为人难以证明自己过错的公共问题上，例如建筑悬挂物脱落、动物园动物致人损害等情况。而网络空间中个人信息的处理问题也是数据平台之上的公共问题，数据平台相较于用户而言存在着明显的信息优势和技术优势，当数据平台处理其收集、储存、分析的个人信息时，用户的个人信息对数据平台呈现单方透明的态势，用户难以知晓自己的个人信息处于何种保护状态，处于哪一处理环节，从平衡数据平台与用户之间的公平角度出发，数据平台应当对其处理的个人信息负有基本保护义务，如果个人信息在平台处理环节中出现损害就应当推定数据平台负有过错责任。

在《个人信息保护法》出台之前，由于《民法典》没有特别作出个人信息侵权的相关规定，因而此时对个人信息侵权适用的是一般过错责任。但实际实践中发现，个人信息受到侵权后由于举证难度较大，个人信息主体很难向法院证明侵权人在侵犯个人信息主体的个人信息权益时存在过错，从而导致个人信息主体受到侵权时难以维护自己的合法权益。考虑到个人信息主体对过错要件所承担的举证责任，《个人信息保护法》中明确规定数据平台对个人信息侵权行为适用过错推定原则，即数据平台不能证明自己已经尽到保护个人信息主体的个人信息义务或者证明自己不存在非法处理个人信息时，就可以认定数据

平台具有过错，需要就个人信息的损害后果承担责任。

2.2. 侵权行为人实施违法行为

侵权责任的另一构成要件是行为人实施了侵害他人权益的违法行为。就个人信息侵权层面具体来说，是指侵权行为人实施了法律规定以外的违法行为，侵犯了个人信息主体的个人信息权益。《个人保护法》第 2 条规定：“自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益”[2]。因此，当行为人实施了法律允许以外的行为侵害到自然人的个人信息权益时，行为人就满足侵权责任中的违法行为要件。

从违法行为的行为方式来看，违法行为分为作为的违法行为和不作为的违法行为。作为的违法行为通常是指，行为人通过积极的作为行为对自然人的个人信息权益造成了侵害。例如，《个人信息保护法》第 10 条规定：“任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动”[3]，该条规定了一些禁止性行为，而作为的违法行为通常就是积极的作为了这些禁止性行为，违法了法律所规定的禁止性规定和义务，因而这些行为都具备违法性。不作为的违法行为则是指消极履行或不履行法律规定的保护个人信息的义务。例如，《个人信息保护法》第 51 条规定：“个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：(一) 制定内部管理制度和操作规程；(二) 对个人信息实行分类管理；(三) 采取相应的加密、去标识化等安全技术措施；(四) 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；(五) 制定并组织实施个人信息安全事件应急预案；(六) 法律、行政法规规定的其他措施。”，该条就明显规定了数据平台在处理个人信息时应该负有的安全保护义务，倘若数据平台以消极的态度履行或不履行该条款，那么其怠于履行义务的行为必然构成不作为的违法行为。

2.3. 被侵权人的损害事实

损害是行为人承担责任的前提条件，无损害则无救济[9]。尽管学界中对损害的讨论包括广义和狭义两种，即现实侵害及危险状态和现实损害后果，但就个人信息侵权而言，一般采取广义上的损害概念。因为个人信息侵权往往具有非即时性的特征，对损害结果的发生有时并不是立刻显现的，或者通过客观存在来显现出来。例如，京东员工利用职务便利贩卖用户的个人信息，贩卖数量高达 50 亿条，其中一些用户甚至至今仍不知道自己的个人信息被贩卖。因此，在个人信息侵权这一领域的损害结果适用广义上的损害更为符合个人信息保护的实际需求。此外，正如前文所言《个人信息保护法》防范的是抽象的财产损失和人格侵害，所以个人信息侵权所造成的损害事实不仅仅包括财产上的直接损害，也包括为了维权时花费的调查、诉讼等合理费用，还包括因个人信息侵权而带来的人格权益受损。另外，由于个人信息侵权的非即时性特征，对于潜在的风险也应当纳入到损害范围内，需要数据平台承担消除危险的侵权责任。综上所述，对于损害事实而言，不能仅因其没有立即显现出来就认为没有造成损害事实，并且损害事实不仅包括财产上的物质损害事实，也包括人格权益等精神上的损害事实。

2.4. 违法行为与损害事实之间存在因果关系

违法行为与损害事实之间的因果关系是指，行为人实施的违法行为造成了个人信息主体的损害结果这一损害事实，或违法行为与损害结果之间存在关联关系，只有当这种因果关系成立时，行为人的侵权

[2]详见《个人信息保护法》第 2 条。
[3]详见《个人信息保护法》第 10 条。

责任才能正式成立。学界主流观点认为只要违法行为与损害事实之间存在一般社会观念或经验认同的牵连关系时，就可以认为该违法行为与损害事实之间存在因果关系。需要注意的是，在个人信息处理过程中，数据平台除了自身对个人信息进行收集、储存、分析等处理外，还可能存在第三方主体因与数据平台签订承揽、买卖等合同，为数据平台提供储存、分析、加工、共享等服务，故而个人信息侵权行为在众多环节、不同主体之间都有可能发生，个人信息侵权的手段也多种多样，因此个人信息侵权中违法行为与损害事实的因果关系也相当复杂，甚至出现一因多果、多因一果，多因多果的情况。由于司法实践中，因果关系的大小直接关系到数据平台对个人信息主体所承担的侵权责任大小，因此个案中很难对因果关系进行统一标准的划分，需要通过个案中的实际情况来判断。

3. 数据平台对个人信息侵权中现有制度的不足

3.1. 损害认定难问题

传统侵权责任理论中，就财产的损害认定而言，一般采用的是“差额说”，即将假设受害人在损害事故发生前应享有的财产总额减去损害事故发生后受害人现有财产，如果所得差额为负值，则存在损害，如果无差额或差额为正，则不存在损害[10]。就非财产的损害认定而言，通说认为只有在法律上特别规定的情形才可以请求损害赔偿[11]。需要注意的是，无论是财产损害还是非财产损害，理论上均要求这些损害已经发生或确有证据证明其将要发生[12]，而不能是不确定的，或不能证明将要发生的。但这些对传统损害的认定在个人信息侵权中显得有些水土不服，个人信息侵权的非即时性特征使得损害往往并不能被立刻确定或者被证明即将发生，个人信息侵权中对财产的损害往往会以因个人信息泄露后不定时间内出现的精准诈骗或财产盗窃作为表征；非财产损害会以个人信息泄露后未来风险和精神紧张等为表征。此外，侵权损害的范围也具有扩张性，数据平台除了收集个人信息主体的姓名、住址、电话等常规信息外，还会收集浏览记录、聊天记录、网购记录等，一旦个人信息遭受侵权还可能受到身份盗用、算法歧视、关系控制等进一步风险，而初步风险与进一步风险的发生时间往往具有高度的不确定性。并且由于人格权益侵害中，精神损害、紧张、焦虑等具有较强的主观性，加之我国对精神损害赔偿的规定较为严格，法院很难对个人信息侵权中的精神损害进行认定。故而，不论是物质层面还是精神层面，损害的认定问题都是我国个人信息侵权责任制度中较为突出的问题。

3.2. 举证责任难问题

为了缓解个人侵权中过错证据举证证明困难的问题，我国在《个人信息保护法》第 69 条规定：“处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。”但是，即便是采用过错推定责任，个人信息主体仍需要就信息控制者具备过错承担一个初步的证明责任[13]。此时，初步举证的要求使得个人信息主体有时难以踏出诉讼的第一步，首先，数据平台作为运营者必然掌握着超越一般个人信息主体的网络处理技术，个人信息主体面对数据平台存在技术壁垒；其次，个人信息处理的流程繁杂且数据平台和第三人参与者众多，难以确定违法行为具体出现在哪一流程和环节；再次，自动化的处理技术和算法黑箱也具有不透明性和不可解释性，个人信息主体难以取得有效力的证据。而且，在证据偏在状态之下，信息控制者可以用多种方式证明其采取了符合法律法规以及强制性标准的保障个人信息安全的必要措施[14]。例如，在个人信息主体使用该平台时所勾选的隐私政策声明或告知同意条款中就存在数据平台的免责声明，而数据平台的集中又促使出现赢者通吃的局面，个人信息主体缺乏替代选择时就不得不接受数据平台的免责声明，在这种情况下更加剧了个人信息主体的举证困难。

3.3. 责任主体认定难

正如前文所述，在个人信息处理过程中，除了数据平台之外，还可能存在第三方主体因与数据平台

签订承揽、买卖等合同，为数据平台提供储存、分析、加工、共享等服务，故而个人信息处理过程中存在众多环节和不同主体。在个人信息侵权案件中往往存在数据平台、第三方主体、个人信息主体共同持有个人信息的情况，而第三方主体的数量并不固定，甚至可能大量存在，那么个人信息侵权究竟出现在哪一环节，由哪一主体实施也就难以得知。例如，外卖点餐中买家通过外卖平台向卖家购买商品，此时买家的家庭住址信息就被卖家得知，而买家的家庭住址信息又是通过外卖平台传达给卖家，那么外卖平台也就随之收集了买家的家庭住址信息，之后的送餐环节又被外卖员得知。此时，卖家、外卖平台、外卖员等每一主体都存在非法收集、泄露买家个人信息的风险。正因如此，在司法实践中一旦发生个人信息泄露，很难通过一般手段确定个人信息侵权的责任主体。即便是个人信息主体可以确定自己的信息被哪一数据平台所收集，但是难以提供证据证明个人信息泄露行为是由数据平台链条下游的哪一主体所造成的。

3.4. 损害赔偿计量难

与一般侵权中的损害赔偿不同，个人信息侵权中的损害赔偿往往与个人信息的数量密度呈正相关，单个或单一的个人信息在互联网时代的价值并不高，甚至不会出现单一个人信息侵权的情况，加之个人信息不具有物理上的实质，不存在损耗可以多次传播、传递，因此个人信息的泄露一般呈现泄露信息数量巨大、非法获取主体众多、泄露信息关联性强等特征，就此而言，这些特征带来的损害很难估计，也就计量损害赔偿。例如，数据平台可以利用 Cookies 等技术分析个人信息主体的浏览记录、地理位置等信息，进而对个人信息主体进行精准的推送服务，而如果这些信息被泄露，那么个人信息主体还可能收到大量无关的推销电话、推销信息等，而侵权人就是通过为这些推销电话、推销信息提供用户个人信息来获取利益。但是，单个、零散个人信息主体的相关信息所产生的经济利益难以计算，故而数据平台非法使用单个、零散个人信息所获得的收益及其承担侵权责任时的损害赔偿也难以计算。

就非财产类的精神损害赔偿而言，个人信息主体在发现自己的个人信息泄露后，可能会产生紧张焦虑、担心担忧等精神痛苦。而这些痛苦通常是担心自己未来遭受身份盗用、算法歧视或者敲诈勒索等风险而产生的，不依附于任何人身伤害和精神性人格权受损而存在，具有较强的主观性和抽象性，较之一般的精神损害更难被直观地感知，也更不易计量[15]。

从立法上来看，《个人信息保护法》第 69 条第 2 款规定：“前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。”根据这一条文加之前文分析可以看出，由于个人受到的损失难以计量加之数据平台获利难以确认，因此在实际司法实践中只能依靠法院酌定的方式确定个人信息侵权损害赔偿的数额。这种酌定的自由裁量主要依靠法官的主观判断来确定赔偿，缺乏具备可操作的指引和统一的衡量标准，显然不利于个人信息相关利益的保护。

4. 个人信息侵权责任制度的完善建议

4.1. 明确损害的认定标准

目前《个人信息保护法》中仅规定在信息主体遭受侵害的情况下才能获得个人信息侵权损害赔偿，但无论是财产损害还是非财产损害，都存在不能立刻显现损害后果的非即时性特征，这使得个人信息侵权的损害认定在法律适用层面呈现出“全有”或“全无”的状态来进行认定。因此笔者认为，应当细致划分个人信息的不同类型，考虑不同类型个人信息损害的特殊性来判断不同个人信息侵权造成的损害和损害的大小。

从现有法律来看，法律对个人信息进行分类保护模式。目前个人信息从私密程度来划分可分为公开

个人信息和私密个人信息，从敏感程度来看可分为敏感个人信息和一般个人信息。《民法典》第1034条第3款规定：“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。”因此，对私密个人信息的保护应当采取隐私权优先的政策，因为隐私比一般个人信息所蕴含的人格自由和尊严成分比较多，其受保护程度比后者更强[16]。而《个人信息保护法》第28条对敏感个人信息的概念做出了界定，其规定：“敏感个人信息一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。”并且在第二款中说明了敏感个人信息的处理规则：“只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。”故而，对敏感个人信息的保护要更为严格，此时对敏感个人信息的侵权认定标准要更低一些，并且赔偿的力度也应该比一般个人信息更大。

在司法实践中，可以建立动态认定体系，根据不同个人信息类型、不同适用场景、不同后果可能性来进行处理，避免对损害的认定出现“全有”或“全无”的僵化。例如，建立三级信息认定体系，从三级一般个人信息，二级私密个人信息，一级敏感个人信息为基准，对可能存在的损害风险进行分类，划定为信息骚扰风险、人格侵害风险、财产损失风险、重大信息安全风险四类，以此确定损害的认定体系，尽可能避免个人信息侵权损害认定的僵化适用。

4.2. 完善证据调取规则

由于我国《个人信息保护法》规定，我国个人信息侵权案件中适用过错推定责任，所以举证的主要责任在于信息控制者即数据平台。但是，即便大部分举证责任不在个人信息主体身上，但当信息主体提起个人信息侵权诉讼时，仍需要就信息控制者具备过错承担一个初步证明责任。但这一责任的证明往往被数据平台通过各类隐私政策条款或者告知同意条款中的免责条款所规避，同时由于数据平台面对个人信息主体时的技术优势、算法黑箱等原因，数据平台可以用多种方式证明自己采取了符合法定标准的安全保障义务。故而，仅依靠个人信息主体自行获取证据显然不利于个人信息利益的保护。

因此，笔者认为应该适当扩大个人信息保护影响评估(PIA)的评估范围和参与主体，将履行个人信息保护职责的部门和《个人信息保护法》第58条所述的“互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”的外部成员独立监督机构进行链接，在个人信息泄露事件后第一时间进行介入审查，及时通知到可能涉及个人信息泄露、滥用等非法行为的个人信息主体。并且保存数据平台储存用户个人信息被泄露、滥用等情况的相关证据，在个人信息主体未来遭受个人信息侵权时，提供相应的初步证明证据。

4.3. 规范责任主体认定

互联网时代，数据的最大价值在于共享流通，而个人信息在大量汇聚后形成数据，随着数据的流通，个人信息也在不同数据平台之间流转，个人信息更容易被不同数据平台所收集。个人信息通过各种平台的处理和交换，使信息处理的效率大大提升，但随着数据的不断汇聚和传播，信息的保护面临的挑战也日益严峻，尤其是以风险发生概率的角度来看，收集个人信息的数据平台越多，出现个人数据泄露、滥用等侵权行为的可能性越高，并且这种风险不是成倍数上涨而是成指数上涨，一如前文所说，每一数据平台都可能链接着大量第三方主体，因此，每当个人信息在不同平台间流转时，风险也随之扩大，涉及的目标责任主体更加复杂。这不仅增加了个人信息保护的风险范围，也使得在发生目标时，如何认定责任主体成为一大难题。数据平台和第三方的交互环节导致了责任链条中的线索行为更加模糊，个人信息案件中往往很难通过某一线索准确地找出责任主体，甚至在某些情况下难以明确哪个数据平台、哪个第

三方主体在信息泄露或滥用中起到了决定性作用。

笔者认为，在这一点上可以参照《民法典》第1170条中对于共同危险行为侵权责任中责任主体的认定方式。即，如果可以确定侵权责任的主体时，该主体对侵权责任负责；如果无法确定侵权责任的主体时，则由所有可能参与共同危险行为侵权的主体共同承担侵权责任[17]，并且按照《个人信息保护法》第69条第1款确立的过错推定责任原则，如果有某一共同危险行为主体能够证明自己不存在过错责任，没有侵权责任的，可以不承担共同侵权责任，否则就应承担。这一机制可以有效地平衡各方的责任，将侵权责任归于实际参与和负有过错的数据平台和第三方主体，避免个人信息受到侵害时无法找到责任主体。

4.4. 完善侵权损害赔偿标准

目前我国《个人信息保护法》中对个人信息侵权中的信息主体遭受的损失和侵权行为人的侵权获利数额是难以确认的，因此需要尽快完善个人信息侵权的损害赔偿标准。在损害标准的认定中，笔者建议以不同类型的个人信息来划分损害标准，在损害赔偿中也应当沿用这一标准，即针对不同类型的个人信息损害情况，给予不同的损害赔偿数额起点，在划分好基本层次后由法院根据实际案情酌定判断个人信息侵权损害赔偿的数额。同时，对于法院的“酌定”可以从以下几个因素进行参考：首先，个人信息侵权可能对个人信息主体造成的风险性之大小，通过对后续风险的评估来控制在数额起点后的赔偿数额。其次，评估侵权责任主体对应负责的个人信息主体数量，通过侵权损害主体的数量判断侵权责任可能产生风险和损害的大小，以此控制损害赔偿数额。

需要注意的是，在无法查明个人信息主体的实际损失和数据平台的侵权获益的情况下，也可以参照《消费者权益保护法》中的最低赔偿额标准的相关规定，设立最低的个人信息侵权损害赔偿，如前文所述损害认定体系中，一般个人信息的信息骚扰风险，设置最低损害赔偿500元。也就是说，即便在单个、零散个人信息侵权时由于数据平台侵权获益的数额较小，无法估计的情况下，个人信息主体仍可以通过最低数额的损害赔偿来保障自己的最基本个人信息权益，这样有利于激发个人信息主体对自身个人信息权益的维护意识，同时可以增加数据平台的侵权成本，倒逼数据平台加强对用户个人信息的保护，提升其信息安全保障义务的履行。

5. 结论

个人信息的保护不仅仅关系到个人的信息安全，同时也关系国家公共利益的维护，明确个人信息侵权责任制度，有助于划好个人信息保护义务的红线，使得数据平台可以在红线内，最大程度地发挥自己处理信息的功能，使更多的信息成为流动的数据资源，推动社会大数据经济的增长。因此，本文分析了个人信息的概念和界定，对个人信息侵权的构成要件进行了解析，并针对目前数据平台对个人信息侵权制度中存在的损害认定难、举证责任难、责任主体认定难， 损害赔偿计量问题进行了分析，并从不同角度给出了笔者所认为的解决路径。笔者相信随着个人信息保护的不断深入发展，个人信息侵权责任制度也必将不断完善。

参考文献

[1] 徐明. 大数据时代的隐私危机及其侵权法应对[J]. 中国法学, 2017(1): 130-149.

[2] 汤啸天. 网络空间的个人数据与隐私权保护[J]. 政法论坛, 2000(1): 8-12.

[3] 程德理, 赵丽丽. 个人信息保护中的“识别”要素研究[J]. 河北法学, 2020, 38(9): 44-54.

[4] 丁晓东. 个人信息私法保护的困境与出路[J]. 法学研究, 2018, 40(6): 194-206.

[5] 梅绍祖. 个人信息保护的基础性问题研究[J]. 苏州大学学报, 2005(2): 25-30.

[6] 杨芳. 个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体[J]. 比较法研究, 2015(6): 22-33.

[7] 谢鸿飞. 个人信息处理者对信息侵权下游损害的侵权责任[J]. 法律适用, 2022(1): 23-36.
[8] 程啸. 论侵害个人信息的民事责任[J]. 暨南学报(哲学社会科学版), 2020, 42(2): 39-47.
[9] 程啸. 侵害个人信息权益的侵权责任[J]. 中国法律评论, 2021(5): 66-67.
[10] 曾世雄. 损害赔偿法原理[M]. 北京: 中国政法大学出版社, 2001: 119.
[11] 王泽鉴. 侵权行为[M]. 北京: 北京大学出版社, 2017: 224.
[12] 王利明. 侵权行为法研究(上卷) [M]. 北京: 中国人民大学出版社, 2004: 355.
[13] 王雷. 民法证据规范论: 案件事实的形成与民法学方法论的完善[M]. 北京: 中国人民大学出版社, 2022: 277.
[14] 蒋丽华. 无过错归责原则: 个人信息侵权损害赔偿的应然走向[J]. 财经法学, 2022(1): 41.
[15] 莫杨桑. 个人信息权益侵权法保护的动态体系论[J]. 人权, 2024(1): 119-144.
[16] 王利明. 和而不同: 隐私权与个人信息的规则界分和适用[J]. 法学评论, 2021, 39(2): 15-24.
[17] 叶名怡. 个人信息的侵权法保护[J]. 法学研究, 2018, 40(4): 83-102.