Open Journal of Legal Science 法学, 2026, 14(4), 257-265
Published Online April 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.144115

Hans汉斯

个人信息权利的类型化保护与风险预防

杨雯靖

宁波大学法学院，浙江 宁波

收稿日期：2026年3月11日；录用日期：2026年3月26日；发布日期：2026年4月27日

摘 要

随着数据所蕴含的价值逐渐被人们发现和利用，数据权利这一概念逐渐出现在人们的视野中，数据侵权问题也开始频繁发生，首当其冲的便是个人信息权利的保护问题，并且贯穿于数据的收集、处理和输出全过程。从比例原则的角度，数据的保护并不是绝对的、完全的、无底线的，在公共利益面前，个人利益可能需要让步，在个人利益受到侵害时，企业的权限也需得到限制。因此数据保护切忌过度泛化，应注重类型化保护，个人信息权利保护切忌单一化，应基于权利束概念进行动态保护。个人信息保护与隐私权保护最大的区别在于持续不平等的数据处理关系，而个人信息保护的本质在于前置性保护规范。这意味着个人信息权利保护应从传统的被动抵制改变为主动的风险预防，这就需要建立完善的风险预防与问责机制，明确个人数据、企业数据和公共数据的保护边界，制定关于数据的类型化保护机制，从而平衡好个人信息权利保护与数据价值的关系。

关键词

个人信息保护，个人信息权利，数据权利，类型化保护，风险预防，权益冲突

Categorical Protection and Risk Prevention of Personal Information Rights

Wenjing Yang

Law School, Ningbo University, Ningbo Zhejiang

Received: March 11, 2026; accepted: March 26, 2026; published: April 27, 2026

Abstract

As the value embedded in data is gradually recognized and utilized, the concept of data rights has gradually emerged in public discourse, and data infringement issues have begun to occur frequently. Among these, the foremost concern is the protection of personal information rights, which is implicated throughout the entire process of data collection, processing, and utilization. From the perspective

文章引用: 杨雯靖. 个人信息权利的类型化保护与风险预防[J]. 法学, 2026, 14(4): 257-265.
DOI: 10.12677/ojls.2026.144115

of the principle of proportionality, data protection is neither absolute nor unlimited. In the face of public interest, individual interests may need to yield; conversely, when individual interests are infringed upon, the scope of corporate authority must also be constrained. Therefore, data protection must avoid over-generalization and instead focus on categorized protection. Similarly, the protection of personal information rights should not be uniform; rather, it should adopt a dynamic approach based on the concept of a bundle of rights. The most significant distinction between the protection of personal information and the protection of privacy lies in the sustained inequality inherent in data processing relationships. The essence of personal information protection lies in the establishment of ex-ante regulatory safeguards. This implies that the protection of personal information rights should shift from a traditional model of passive resistance to one of active risk prevention. Achieving this requires the establishment of robust risk prevention and accountability mechanisms, the clarification of boundaries between personal data, corporate data, and public data, and the development of categorized protection mechanisms for data, thereby balancing the protection of personal information rights with the value derived from data.

Keywords

Personal Information Protection, Personal Information Rights, Data Rights, Categorical Protection, Risk Prevention, Rights Conflict

1. 引言

人工智能时代，数据的使用价值可见一斑，在数据权利不断泛化的过程中，个人信息权利的侵权问题也层出不穷，对个人数据信息保护问题的讨论和争议，即使在《中华人民共和国个人信息保护法》(以下简称“《个人信息保护法》”)出台之后仍不绝于耳。在讨论的过程中，人们从对数据的泛化保护，逐渐意识到数据的类型化区别[1]；从对个人信息权利的单一化保护，发展为基于权利束概念的动态保护[2]；从类隐私权的保护模式，延伸出基于持续不平等数据处理关系的个人信息保护[3]。有学者曾提出，个人信息保护的本质在于前置性保护规范[4]。虽然我国已经出台了《个人信息保护法》，但对于个人信息权利保护的一些概念性及边界性问题在学界仍存在理解冲突，本文旨在厘清个人信息权利的概念区分问题，从法律内涵和类型化保护的视角对个人信息权利进行解读，并提出关于个人信息权利保护的风险预防措施。与欧盟《通用数据保护条例》(GDPR)及美国加州《消费者隐私法案》(CCPA/CPRA)等域外法律框架相比，本文所提出的类型化保护与风险预防方案，更注重回应我国平台经济深度渗透、数据安全与发展并重的现实情境，在制度设计上强调动态平衡而非绝对赋权，体现了本土化的理论创新。

2. 个人信息权利的侵权样态及保护困境

近年来，在人工智能、自动化、大数据等词汇被人们反复提及的同时，数据侵权一词也不绝于耳，个人信息权利的侵权样态之丰富，给人们敲响了个人信息权利保护的警钟。数据处理者对个人数据信息权益的侵害贯穿了数据的收集阶段、处理阶段到输出阶段始终，个人信息保护问题也随着数据价值的不断挖掘而不断升级。

2.1. 个人信息权利的侵权样态

在个人数据的收集环节，授权同意知情的规则已被各平台广泛使用，然而平台利用格式条款诱导用

户授权，使“同意”往往流于形式。即使个人为了获得软件的使用权限让渡了其个人数据的处理权限，但是企业对于数据的处理是否合法合规仍有待考量，例如企业将获得的大量个人敏感信息转售第三方，可能会损害社会公共利益。

除了用户同意的方式外，数据收集者可能还会采用各种技术手段完成个人数据的收集，其中不乏各种非法与合法手段，例如网络爬虫、网页 Cookies (小型文本文件)等技术手段，技术本身并不违法，其合法性实际上取决于使用的方法和目的，这就涉及数据的类型了，例如利用网络爬虫这种自动化程序，抓取个人敏感信息、商业数据等会涉及数据侵权。

在个人数据的处理与存储环节，数据可能会因为安全管理的缺陷导致数据泄漏，这种泄漏可能是因为技术上的系统漏洞，也可能是由于员工的违规操作。同时超出用户初始授权范围使用数据，滥用或篡改数据也可能会导致个人信息权益的受损。另外放任他人任意爬取用户数据不作限制，也属于不履行平台的监管责任的行为，应当承担相应责任。[5]

在个人数据的输出环节，人们常常困扰于收到垃圾短信、邮件的轰炸以及电话的骚扰，甚至诈骗集团会获取个人信息进行精准的诈骗设计，企业将个人信息商业化滥用的行为严重侵害了用户的信息权益。另外企业在进行自动化决策的过程中，利用算法技术进行算法价格歧视等也是数据在发展过程中出现的新型信息侵权样态[6]。例如“胡某某诉上海携程商务有限公司侵权责任纠纷案”[1]，原告作为平台钻石会员，通过网络平台预订酒店时支付 2889 元，而该酒店同一房型的实际挂牌价仅为 1377.63 元，差价高达 1511.37 元。法院经审理认定，平台存在未充分履行会员优惠承诺、过度采集用户个人信息、利用算法进行差异化定价等行为，违反了《消费者权益保护法》第八条关于消费者知情权、第十条关于公平交易权的规定。该案虽未直接依据《个人信息保护法》作出裁判，但法院在判决中明确指出，平台利用用户历史行为数据、消费能力画像等信息进行自动化决策，导致消费者在交易中处于信息不对称的弱势地位，价格形成机制缺乏透明度。这一司法实践充分揭示了当前法律适用中面临的“算法黑箱”认定难、消费者举证难等现实困境，亦反映出传统知情同意机制在应对持续不平等数据处理关系时的结构性局限。

2.2. 个人信息权利的保护困境

权利保护往往满足三个要件，即主体的明确性，内容的法定性和救济的可行性，而这些不断涌现的侵权样态往往会模糊我们对保护主体和内容的锁定。个人信息权利从内涵到类型依旧存在着广泛的争议，首先我国关于个人信息权利的保护的范围仍采取的是列举式规定，这就导致了新型数据权益的保护的困难[7]。另外个人信息的保护边界依旧模糊，企业和政府汇聚了大量的个人数据，其中不乏敏感的个人隐私信息，我们无法阻止数据价值挖掘的时代需求，那么因此出现的数据风险该如何预防就成了新的问题，当今个人信息保护仍停留在隐私权保护的被动抵制模式中，如何从源头把关，完成个人信息的保护是我们亟需面对的问题。

个人信息保护权利的困境，很大程度在于监管框架的模糊，在机器学习、自动化决策的使用越来越频繁的过程中，个人信息的侵权样态会越来越隐蔽，个人对侵权的证明难度和维权的成本也会越来越高，也可能会导致社会公平和群体歧视等系统性影响。人们一方面苦于数据权利泛化导致的司法操作难度，另一方面希望能将新型数据权益纳入法制的保护框架之内，同时又渴望发挥数据的最大价值。值得注意的是，本文所倡导的类型化保护与风险预防方案在落地过程中可能面临多重挑战：一是严格的风险分级可能增加企业合规成本，抑制中小创新主体的数据利用活力；二是动态评估机制对监管资源提出较高要求，需警惕“监管过载”风险；三是类型化标准与现行《民法典》和《个人信息保护法》的衔接尚需立法层面的进一步明确。

[1]胡红芳、上海携程商务有限公司侵权责任纠纷案，浙江省绍兴市中级人民法院(2021)浙 06 民终 3129 号民事判决书。

3. 个人信息权利的内涵解读

“权利”作为一个外来词汇，蕴含着可以自由支配并受到法律保护的意思表示，这种意思表示的力量来自法律的赋予，而“个人信息权利”作为一种基于“个人信息”而产生的新型权利，学界对其内涵往往有着不同的解读和归类[8]。有观点认为个人信息权利是一种新型民事权利，尤其是以王利明教授为代表的民法学家认为，个人信息权利是一种独立的人格权[9]，本文认为个人信息保护既不是传统的民事权利，也不是传统的宪法权利。

3.1. 个人信息权利与个人数据权利

在“个人信息权利”这一概念出现的同时，“个人数据权利”这一概念也应运而生，然而，我们很容易发现“数据权利”这个词模糊性，之所以会出现这种感觉，是因为数据是信息的外在形式，而信息代表的是数据的具体内容[10]。“个人数据权利”这一概念就像是对“个人信息权利”概念的一种过度延伸，正如美国社会学家萨姆纳曾说过的“一个能论证所有问题的理论实际上什么都论证不了”[11]，这种概念上的过度延伸，实际上是在削弱内容的说服力和影响力。

那么个人信息权利与个人数据权利究竟是什么样的关系，是包含关系、交叉关系，还是同一的呢？对此，学界出现了两种观点，一种是区分说，另一种是同一说。在同一说下，也存在着不同的情形，即个人信息包含个人数据的观点，个人数据包含个人信息的观点，以及二者内涵交叉而并用的观点[12]。这一观点的形成，来自个人信息和个人数据内涵的差异，其落脚点在于“信息”和“数据”。而本文认为，个人信息权利和个人数据权利的重点在于“个人”，个人信息和个人数据在外延上具有同一性，在诸多法律文件中所指代的内容也是同一的[13]，因此，应当采取“同一说”的观点。

3.2. 个人信息权利的法律内涵

厘清了个人信息权利与个人数据权利的关系之后，我们紧接着会面临个人信息权利是民事权利还是宪法上的权利的问题，对于个人信息权利属性问题的回答不仅仅是学术问题，更是制度与实践的问题，不同的答案可能会导致个人信息保护立法、执法与司法上的差异。

从个人信息所蕴含的人格性利益和财产性利益的角度来看，个人信息权利具有明显的私法属性，当个人信息权利受到侵害时，可以要求侵害人排除妨害、消除危险、赔偿损失[14]。同时人们可以直接地支配、控制个人信息，例如《个人信息保护法》中所规定的人们对个人数据的被遗忘权(删除权)、访问权、更正权、可携权、限制处理权、已公开信息的拒绝权等。[15]

但实际上，私法意义上的数据权利，也可能同时具有公法权利的性质，当人们以个人信息权利对抗公权力对个人信息的不当干预时，个人信息权利就带有了明显的公法色彩，因此，以公、私法属性的划分来定义个人信息权利是有局限性的。[1]

首先，个人信息权利是法律赋予自然人对个人信息所享受的支配力和对抗力，本质是为了避免持续不平等的信息关系而实现动态平衡的多元复合权利。如果我们以隐私权为出发点，进行对比分析，我们就能快速理解个人信息权利的本质。隐私权作为一种具体的人格权，基于人际关系，调整的是平等主体之间出现的侵害隐私权的法律关系，具有消极防御性。而个人信息保护则基于人际关系，调整的是个体与信息处理者之间的不平等关系，具有积极性与消极性、控制性与对抗性的复合性特征。[16]

基于此，我们可以发现个人信息权利的保护有一个很大的前提，即持续性、不平等的信息关系。然而从隐私权到个人信息权利的保护，为什么会出现这样一种变化呢？分析《民法典》中关于隐私权的规定，我们不难发现，在《个人信息保护法》出台前，我国已经列出了对于一些以信息方式侵犯他人隐私的行为，并将私密信息作为个人隐私权的一部分。那么既然我们可以通过主张隐私权排除他人对个人信

息的干扰，又为什么需要再设立一部个人信息保护的法律呢？答案就在于个人信息保护早已跳出了民法的框架，跳出了平等主体之间的一次性隐私权的侵害的范围，更跳出了国家与个人之间非持续性的信息侵害关系。[17]

最后我们回到个人信息权利所蕴含的支配力和对抗力特征，个人对信息的积极控制可以从上文所述的被遗忘权(删除权)、访问权、更正权、可携权等体现出来，展现的是个人对数据权利的自决权和知情同意的权利。而个人对信息的对抗效力则可以从限制处理权、已公开信息的拒绝权等角度进行理解，具体而言，可以从个体、企业和政府三个角度进行解读，即具有商业性或者专业性信息收集能力的企业或个体，以及具有专业信息收集能力的公共机构。值得一提的是，对上述的信息收集，学界存在将这种信息收集限制在自动化收集范围内[18]，以及将非自动化收集的信息包括在个人信息保护的框架内两种不同的观点，本文赞同是第二种，即只考虑个人信息收集过程是否具有专业性，是否存在持续、不平等的信息关系。

3.3. 类型化视角下个人信息权利的解读

在数据逐渐成为生产生活中的重要一环的过程中，海量数据中所蕴含的权利和利益，势必带来大量的纠纷，若我们对于数据不加以区分而直接赋予同样的法律属性、法律资格，采取同样的适用规则和保护方式，那么就可能导致权利的泛化。无论是因此导致的过多的条款配置，还是对不同主体行为的过度限制，都是与我们进行信息数据保护，在减少社会冲突的同时实现数据价值目的相背离。另外，对数据不加以区分，实际上会导致权利与利益的模糊，从而加重司法负担，提高司法操作的难度。[2]

由于个人信息所包含的人格权益、财产价值及公共管理功能，可以将数据信息分成个人信息、企业数据和公共数据三种类型，基于这样的类型化视角，我们可以对不同类型的数据使用不同的规则，从而能够更好地预防和化解冲突。当然，我们在进行权利规制和保护的过程中，会发现三种类型的数据乃至其所涉及的权利会出现一些交叉甚至冲突的情况，那么如何设计权利的保护边界，又会是一道新的命题。

由于个人信息所蕴含的权益绝不是单一、绝对的权利，我们可以借鉴“权利束”理论，将个人信息权益想象成一个包含具体的、刚性的权利和个人信息所蕴含的固有的、自然延伸的利益。基于数据活动的不同环节和不同主体的贡献，我们能将数据分解并配置不同的具体权益，再根据数据的不同类型进行差异化、功能化的制度设计，满足不同敏感度和不同位阶权利的冲突。[19]

4. 个人信息权利的保护边界

上一个章节，我们对个人信息权利的内涵进行了解读，并提到类型化视角下，敏感度不同、位阶不同乃至权益的刚柔性不同的数据会出现权益冲突的情况，需要明确权利的保护边界。个人信息数据中所蕴含的价值是不可限量的，但无论是企业数据还是公共数据，都离不开个人数据的收集，为了平衡不同位阶的权益，我们有必要对权利保护的边界进行明确。

4.1. 财产价值的受限实现

个人信息数据关联着个人隐私、财产安全等，而数据则因平台劳动而产生新的价值，但个人信息中的财产价值的实现应该是受到限制的。首先，平台收集及处理数据需要完成用户授权，且这样的用户授权是具有相对性，即用户将自己的个人信息授权给某公司使用，那么其他主体即使获得了这个数据，并不必然获得数据的使用权限，这意味着一些通过网络爬虫等方式获取的个人信息属于非用户授权数据。

当然，数据平台并不因为用户的同意授权的行为，就能免除自己所有的责任，在实践中，数据平台所提供的用户授权书中所涉及的隐私政策往往十分冗长隐蔽，且由平台单方面制定，对此用户通常无法对里面的内容完全知情，同时平台会设置不授权则禁止服务的规则，对于那些结束服务后，想要撤回授

权的用户，平台更是没有提供相应的链接或渠道[20]。因此，从数据的获取到数据的使用，都存在着很大的边界模糊，平台可能会制作一份授权范围过大的用户授权书，甚至会利用一些兜底条款越权，而信息主体往往不知道自己向平台授权了哪些信息，这就导致传统的知情同意机制被架空。因此，限制平台的权限十分重要，对于侵犯用户人格权的情况，应当严格限制，保证个人信息财产价值实现不超越用户的人格权边界。

4.2. 权利边界的弹性框定

根据上文我们知道，传统的“知情同意”模式可能会因为一些概括授权或者隐私条款模糊或者被忽视等原因而失效，在这种情况下，除了用人格权边界对个人信息进行兜底保护外，个人信息的匿名化机制构建也非常重要。通过《个人信息保护法》我们可以知道，个人信息指的是任何能够单独或结合其他信息识别出特定自然人身份的数据或记录，这就意味着，匿名化的信息将脱离个人信息的范畴。当然我国的法律依赖的是“可识别性”特点，采取的是绝对匿名化的标准，但技术的发展也可能会导致数据存在复原和再识别的风险[21]。因此，即使是匿名化的数据也应当定期评估去匿名化的风险，并考虑是否需要重新进行匿名处理。

实际上，数据也不是越匿名越好，匿名固然能更好地保护个人信息，但也可能会减损数据价值，例如一些研究，可能需要更精确的数据信息，才能获得更准确的研究成果。因此，我们可以考虑从个人信息的性质出发，对个人信息划分等级，设定匿名化处理的差别原则，从而最大限度地调和个人信息保护和利用企业信息之间的关系[22]。例如，对于无个人指向性的信息，我们可以采用无需匿名化即可流通的标准，对于一般的个人信息，我们可以采取普通的匿名化标准，对于敏感个人信息我们可以采取严格匿名化的标准[23]。最后对于一些特殊的敏感个人信息，若其流通可能产生巨大经济风险和社会安全的，我们甚至可以采取禁止流通的规定以维护国家和社会安全和利益。

当然我们在确立权利保护边界的同时，也要注重权益的横平调整，确立法定数据权利优于新型数据利益，人格性利益大于财产性利益，公共利益大于私人数据利益的三大标准。同时采取类型化视角展开制度设计，对于个人数据的保护，我们可以以人格权为基础，扩张新型权利覆盖财产性利益。对于企业数据的保护，我们可以突破传统知识产权的局限，创设有限制的处理权限，例如设立期限限制，建立企业数据的商业化及公共化规则。对于公共数据，我们可以在政府管理化的基础上，推动实现开放共享，发挥公共数据的价值，例如开放非涉密型数据，允许企业加工公共数据生产衍生数据产品。

5. 个人信息权利保护的风险防范

在个人信息保护的基础框架和边界确定之后，我们对个人信息权利的保护应当从被动制裁的逻辑转向主动预防，关键在于通过事前评估、事中防护和事后处置三个维度确定信息处理者的前置合规义务，从而保障信息处理的合规性以及安全措施的完善性，进而确定个人信息权利保护的合法性约束机制。

5.1. 数据类型化管理

上一章节我们提到了，将数据分成个人信息、企业数据和公共数据，制定不同的管理规则以实现不同的数据价值，那我们在风险防范时，需要进一步对数据进行类型化，以设定对应的预防规则。我们可以将数据依据风险程度的高低进行分级，目的是筛选出那些高风险数据，目前的个人信息保护法对于高风险数据，仅以“对个人信息权益有重大影响”进行笼统概括，但是缺少进一步的判断标准。因此，我们需要明确高风险的判断标准。

我们可以从两个角度解读高风险，即发生风险的可能性高以及风险后果的严重程度高。具体而言，当一个企业拥有大体量的个人信息数据时，一旦这些数据侵害到个人权益时，往往会伴随着较严重的后

果。而如果我们从数据的内容来看，如果这个数据主要是个人敏感数据，那么发生风险的可能性就会更高。我们以结果为导向，可以评估损害的程度，例如造成歧视，造成大额财产的损失，而以行为导向，我们可以分析风险的来源，这往往涉及数据的类型、规模以及数据处理者的目的等。我们可以考虑要求数据处理者出具前置性的数据处理合规责任书，要求数据处理者主动证明其行为和目的的合规性，并列明其数据处理所涉数据的风险类型，若涉及高风险数据，我们应当让数据处理者明确其所需承担的合规义务，严格规范数据类型化管理的规则制度。[4]

对于数据的类型划分，我们可以参考欧盟有关数据风险阈值的规定，事先设定具体的评估标准，例如用户规模、所涉业务范围等，每项指标设定不同的评分标准，根据数据所达到的风险数值将其分配到不同的类别，进行不同程度的监管，避免出现对信息保护的单一化。

5.2. 信息动态风险评估

对于信息风险的评估，实际上我国在《个人信息保护法》中也明确了对于个人敏感数据的处理，利用个人信息进行自动化决策，委托处理个人信息或者向其他个人信息处理者提供个人信息以及公开个人信息或者向境外提供个人信息等个人数据处理的情形，应当在事前进行个人信息保护影响评估。但是我们不能保证，数据在使用期间不会出现风险度增加的情况，实际上，随着数据规模和业务种类的增加，这种风险增加的情况是必然的。对此，我们可以考虑对信息进行动态的风险评估，我们可以考虑建构风险评估模型，基于数据的风险评估标准，统计风险数值的变化趋势并进行预测，实现自动化的风险管理。

同时，可以建立高风险场景清单，例如当数据处理涉及生物特征识别，大规模处理个人敏感信息、个人访问空间，进行跨境数据传输，公开个人信息等情况，应当进行风险预警，并及时进行区块链存证，若风险模型判断有数据违规处理的可能性极大，可以进行一定程度的干预，而数据处理者可以考虑证明数据处理的合规性或者提供相应程度的保证，以排除干预。初步设想，动态风险评估模型可设置多维度的量化指标，例如用户规模(日活超 500 万计 5 分、100 万至 500 万计 3 分、100 万以下计 1 分)、数据敏感度(含生物特征等高度敏感信息计 8 分、一般敏感信息计 5 分、非敏感信息计 2 分)、处理行为(跨境传输计 6 分、自动化决策计 4 分、委托处理计 3 分)以及历史合规情况(近两年有行政处罚计 5 分、有投诉未整改计 3 分、无不良记录计 0 分)，根据累计得分划定风险等级：超过 20 分纳入高风险等级监管，需实施事前审批与定期审计；10 至 20 分为中风险等级，要求定期报告与抽查；低于 10 分为低风险等级，以事中事后监管为主，以此展示模型的可操作性与分层管理逻辑。

5.3. 危机处理与问责机制

当数据风险确有出现的时候，我们不能等到损害发生时再进行挽救，这时候需要及时启动危机处理与问责机制。在公关危机中，人们往往把事件发生后的 72 小时称作黄金公关期，对于前四小时必须迅速作出反应，以控制局面，避免危机进一步恶化，在获悉危机发生后的 24 小时启动危机管理机制，做好准备工作，并在 72 小时内完成公关工作，如果超过这个时间就会失去有效处理的最佳期间。危机管理专家曾提出著名的危机公关“5S 原则”，即速度第一原则、责任承担原则、真诚沟通原则、权威证实原则和系统运行原则[24]，这些原则对我们在面对数据风险危机同样有着很大的启发。

在处理数据危机时我们也需要把握黄金时期，例如统筹管理者可以紧急限缩数据处理的权限，并进行区块链存证，努力将影响降到最低。其次要建立问责机制。同时，我们应当将数据风险动态告知用户，说明事件详情与补救措施，明示其解除相关授权或关闭网页 Cookie 等方式。另外，对于数据风险的通知，应当有权威的官方渠道，进行告知、公示或查阅等，以保障用户对数据安全的信心。最后我们要保证一

系列数据危机与问责的机制可以系统运行，对此，可以设立一定的数据保护委员会，对数据保护进行流程化的管控，对于数据处理者进行定期文化培训，对于技术人员进行技术防护培训，对不同的数据类型制作相应的合规手册。

6. 尾部

个人信息保护问题是涉及全体公民利益的问题，传统的个人信息保护范式在面对日益复杂的数据处理场景和新型数据权益侵害风险时难以发挥其效用。本文提出的个人信息权利保护的路径也非追求绝对安全，而是在精准识别风险的基础上，达到实现权益保障与释放数据价值的审慎平衡，旨在打破标准单一的数据保护，从而科学划分信息类型、识别差异化信息风险从而匹配相应的数据保护措施。数据的风险预防与动态治理的核心价值在于将数据风险识别与评估前置化、结构化，这需要形成多方协同、多维监管的合规风控机制。未来，数据一定会在更多的场景发挥其效能，技术赋能所带来的机遇与挑战需要我们进行持续的跟踪和防范。在制度层面，信息类型需要完成细化处理规则，筑牢个人信息保护的基础；在执法层面，信息监管需要强化管理的精准性与执法的专业性；在技术层面，信息保护需要形成动态评估个人信息侵权的概率模型，高效化解各种个人信息侵权风险；在观念层面，数据处理者的侵权意识和保护义务应当内化提高，确立个人信息保护的观念根基。

参考文献

[1] 段卫利. 什么是数据权利——数据权利的类型化分析[J]. 辽宁师范大学学报(社会科学版), 2024, 47(6): 136-144.

[2] 李晓宇. 权利与利益区分视点下数据权益的类型化保护[J]. 知识产权, 2019(3): 50-63.

[3] 丁晓东著. 个人信息保护原理与实践[M]. 北京: 法律出版社, 2021: 21-31.

[4] 张璐. 个人信息保护风险规范的建构机理与实现路径[J]. 江西财经大学学报, 2022(3): 126-136.

[5] 吴卫. 明确越界网络爬虫行为的刑事处罚边界[N]. 检察日报, 2022-02-15(001).

[6] 王莹. 算法侵害类型化研究与法律应对——以《个人信息保护法》为基点的算法规制扩展构想[J]. 法制与社会发展, 2021, 27(6): 133-153.

[7] 王颖. 个人信息权利保护的法律困境与完善措施[J]. 青年记者, 2021(21): 75-77.

[8] 李伟民. “个人信息权”性质之辨与立法模式研究——以互联网新型权利为视角[J]. 上海师范大学学报(哲学社会科学版), 2018, 47(3): 66-74.

[9] 王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013, 35(4): 62-72.

[10] 程啸. 论大数据时代的个人数据权利[J]. 中国社会科学, 2018(3): 102-122, 207-208.

[11] 萨姆纳, L.W. 权利的道德基础[M]. 李茂森, 译. 北京: 中国人民大学出版社, 2011.

[12] 韩旭至. 信息权利范畴的模糊性使用及其后果——基于对信息、数据混用的分析[J]. 华东政法大学学报, 2020, 23(1): 85-96.

[13] 梅夏英. 信息和数据概念区分的法律意义[J]. 比较法研究, 2020(6): 151-162.

[14] 张里安, 韩旭至. 大数据时代下个人信息权的私法属性[J]. 法学论坛, 2016, 31(3): 119-129.

[15] 丁晓东. 什么是数据权利——从欧洲“一般数据保护条例”看数据隐私的保护[J]. 华东政法大学学报, 2018, 21(4): 39-53.

[16] 丁晓东. 隐私权保护与个人信息保护关系的法理——兼论《民法典》与《个人信息保护法》的适用[J]. 法商研究, 2023, 40(6): 61-74.

[17] 丁晓东. 个人信息权利的反思与重塑论个人信息保护的适用前提与法益基础[J]. 中外法学, 2020, 32(2): 339-356.

[18] 杨芳. 我国个人信息保护法适用范围之思考——隐私权救济困境下的个人信息保护法[J]. 社会科学家, 2016(10): 112-115.

[19] 曹新舒. 数据“三权分置”法律表达的中间理路[J]. 网络法律评论, 2023, 25(0): 59-86.

[20] 周勇, 林凌. 个人信息数据保护受托机制构建研究[J]. 当代传播, 2024(5): 83-87.

[21] 王立梅. 大数据视角下的个人信息匿名化规则构建[J]. 云南民族大学学报(哲学社会科学版), 2021, 38(5): 142-150.

[22] 张新宝. 我国个人信息保护法立法主要矛盾研讨[J]. 吉林大学社会科学学报, 2018, 58(5): 45-56, 204-205.

[23] 张建文, 高悦. 我国个人信息匿名化的法律标准与规则重塑[J]. 河北法学, 2020, 38(1): 43-56.

[24] 郑成武. 媒体危机公关 5S 通用原则[J]. 中国行政管理, 2007(6): 87-88.