数据合规视野下个人信息保护归责标准的重构

李晓霞*

内容摘要：根据我国现行法律规范，侵犯公民个人信息属于一般侵权纠纷，如果适用传统归责标准规制，将有违公平原则和难以实现个案正义。过错应何标准而定，各国多采客观化标准。过错的客观化改变了传统依赖主观过错的考究，降低了道德的非难性，更加注重司法场域中应有客观的规范和标准。以客观过错标准为主轴来完善个人信息侵权行为归责的层阶体系，从数据的合规性判断出发，注重行为规制的客观层面，并以此作为归责的基础和重心。通过五款个人信息保护合规产品的技术与功能场景的考察，进而提炼“信息主体身份”“信息处理方式”“信息类别评估”“信息风险评估”四个合规性要素，形成客观归责认定机制和归责逻辑核心。

关键词：个人信息保护　归责标准　数据合规　客观过错标准　客观归责认定机制　侵权责任

引　言

目前，在我国个人信息保护规制体系中，公民个人信息侵权行为的责任应适用何种归责原则尚不明确。而在司法实践中，个人信息侵权案件法官多采用一般侵权纠纷的裁判思维进行责任的判定。然而，大数据背景下侵犯个人信息的行为类型多变，原告难以提供证据证明被告主观存在过错。因而个人信息侵害行为应当如何认定方能实现权益的真正保护之问题殊值探究。本文认为应采用客观过错标准予以具体化、类型化认定，以改变传统个人主义的过错责任。具体路径可从以下两个方面进行完善：一方面，借鉴域外互联网企业的个人数据保护之合规要点进行梳理，提炼出信息主体身份，信息处理方式，信息类别，信息风险四个基本评价要素；另一方面，拟通过四个要素进行同质关联、互补关联、关联例外三个层次的审查实现不同价值权益的保护。

一、现状的反思：个人信息保护传统归责原则适用功效考察

相较于其他民事侵权行为，我国个人信息侵权责任认定尚待完善。尤其是在法律归责标准的确立

*江西省会昌县人民法院三级法官。

上，仍是沿用传统的过错主观归责标准，未突出个人信息数据动态特性，就民事救济的效果而言明显动力不足。

（一）聚焦：当前个人信息侵权的归责模式

在当前的司法裁判中，对于个人信息侵权归责问题的判定倾向较为统一，主要遵循过错归责原则，但法官在过错的证成上却存在不小分歧。在样本案例〔1〕中，适用过错原则的占比75.9%，其中主观故意案件占比43.2%，主观过失案件占比32.7%，剩余19.4%和4.7%的案件分别适用的是过错推定原则和无过错原则（见图1）。

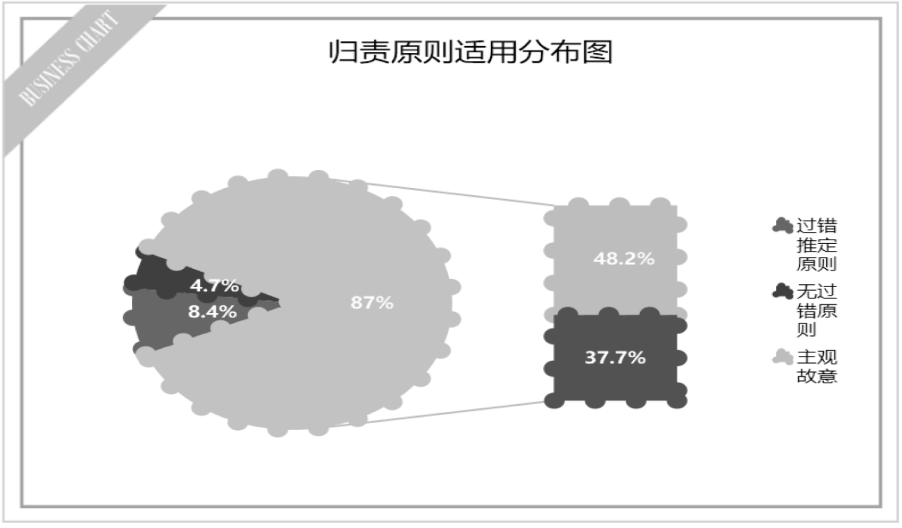

图1 归责原则适用分布图

模式一：过错责任原则

我国民法典侵权责任编第1165条第1款对个人信息侵权的归责原则确定为一般侵权的过错责任原则，即原告需证明行为人具有过错为责任认定的前提。如个案中承办法官就强调行为人的主观故意，认为“三被告事实上明知应取得用户授权，但是却径行使用了原告的个人信息，视为主观上存在故意，依法应当承担相应的侵权责任”。〔2〕而在个案中，承办法官在主观意志状态的认定上，则是以行为人的主观过失作为责任的最终划归，认为“被告未经原告同意，将标注有原告个人信息的表格在有小区业主、被告工作人员参加的会议上分发，被告存在主观过失，应承担侵权责任”。〔3〕

模式二：过错推定原则

随着大数据技术的不断广泛应用，个人信息侵权的规制难度也随之增大。仅仅适用传统侵权法的一般过错责任原则，很难真正实现个人信息保护的民事救济。2020年8月20日颁布的《个人信息保护法》第69条初步确立了过错推定原则，但具体如何适用尤其是因果关系的判断，损害结果的认定等均未明确。而在司法实践中判定行为人是否实施了侵权行为主要是从“违法性”判断。〔4〕如个案中，承办法官认为“被告的搜索行为违反了个人信息保护的相关规定，在未得到授权的情况下，造成涉案信息扩散属于违法使用个人信息的行为。”〔5〕

〔1〕笔者于2023年1月10日分别以“个人信息权”“民事案件”“判决书”“侵权”“基层法院”为关键词在裁判文书网进行检索，排除一些重复的或与本文研究无关的案例，涉及个人信息保护的民事判决书475件。

〔2〕参见北京市海淀区人民法院（2018）京0108民初13661号民事判决书

〔3〕参见宁波市镇海区人民法院（2021）浙0211民初593号民事判决书。

〔4〕参见程啸：《论侵害个人信息的民事责任》，《暨南学报》2020年第2期。

〔5〕参见北京互联网法院（2019）京0491民初10989号民事判决书。

模式三:无过错责任原则

在侵权责任认定体系中,无过错原则主要是出于维护公共利益等目的,而对拟制型的法律人格进行否定性评价。因此,在传统侵权领域上,无过错原则的运用更注重损害事实的考察,而并不关注行为人主观上过错。如个案中,承办法官认为"被告在本案审理过程中以积极方式申请将原告个人信息从网站撤下,因客观原因不能变更,被告对此无过错,但是对原告担任更高职务造成了一定的影响,故应承担一定责任。"〔6〕

(二)差异:举证责任分配情况考察

民法典将个人信息保护纠纷归总为一般侵权纠纷,举证责任分配也适用过错原则,由原告承担侵权责任构成四要件的举证责任。值得注意的是,在大多数个人信息侵权纠纷案中,往往存在原告举证难的客观情形。主要表现为原告在证明发生损害事实存在一定优势,但对包括损害行为、因果关系等在内的其他侵权责任构成要件的举证存在较大难度。如个案中原告侵权责任构成四要件的举证仅完成了存在损害事实的部分,其他构成要件的举证不能,最终导致自身诉请被法院驳回的结果。〔7〕此外,也有一些法官适当减轻原告的举证责任。在个案中,法官运用"高度盖然性"完成了存在侵权事实的合理推定,并没有要求原告承担侵权事实存在的举证责任。〔8〕类似的情况也可以在个案中得到印证,受制于客观条件并考虑到原告举证不能的合理性,法官采取举证责任倒置,要求被告就自己是否履行了个人信息保护义务进行举证。〔9〕

(三)思考:过错判断标准主观化的现实桎梏

通过样本案例的分析,不难发现在给个人信息侵权行为定性时,往往集中于是否存在主观过错。在大数据时代,此类案件侵权主体为社会公共服务提供者或者网络公司等,这些主体作为法律拟制的组织性人格主体,在造成损害结果时具体行为人并不明确,很难通过主观存在过错认定其承担法律责任。这种主观要件判断其目的本身并不明确,"故意"或者"过失"在判定时,很多时候更似一个简单的概念,并不包含具体的内容,很难确定具体的行为性质。如个案中,被告辩称"发现原告提供的数据存在滞后性,为了更好的查明原因,利用网络爬虫软件二次获取公交数据,其目的主要用于数据对比,不具有主观恶意"。〔10〕因此,如果仅从行为人信息爬取行为来看,其主观心态是"故意"或者"过失"是模棱两可的,很难将行为人的主观心态还原,尤其是拟制型法人是否具备主观故意或者过失的认定更是加重了侵权行为规制边界的模糊性。

二、思路的拓展:过错客观化判断标准的引入

过错客观化标准主要是考察行为人的致害行为,针对行为不正当性的认定。易言之,所谓过错,是内心的主观状态,对客观行为的不正当特征进行标准化的设定。

(一)起点回溯:归责方式客观化

在大陆法系的客观过错概念中,其是建立在罗马法"善良家父"的标准上,即行为人作为一个合理人所应尽到的注意义务或者行为人所作行为是违反法律作为义务标准。在这个否定性评价过程中,它所遵循的是特定场景下理性人所作的选择,而不是主观状态的探寻。在这个标准的建立上,德国法主要是通过职业或者年龄进行区分, 如果行为人作出行为之时缺乏了同职业或者同年龄段群体一般应

〔6〕参加深圳前海合作区人民法院(2018)粤0391民初4065号民事判决书。

〔7〕参加南京市玄武区人民法院(2016)苏0102民初1123号民事判决书。

〔8〕参加北京市海淀区人民法院法院(2015)海民初字第10634号民事判决书。

〔9〕参加双流县人民法院第(2014)双流民初字第5341号民事判决书。

〔10〕参加深圳市中级人民法院(2017)粤03民初822号民事判决书。

具备的心智时，则需承担不利后果。[11]而法国法则是进行一个反面推论，更加强调行为缺陷对过错所造成的影响，即过错是由于行为缺陷造成，而对于行为缺陷的认知，主张通过“理性人”与“普通人”的比较判断来认知这种缺陷。英美法系的“理性人”标准不同于这种反面比较，它倾向于普遍适用，即在不考虑个体差异、能力的情况下，如何形成一个“普适者”评价标准。但是，并不意味着普遍性之外无特殊性。英美法亦强调一种修正的“理性人”标准，即在某种特别的行为缺陷下“理性人”标准是不适用的，比如未成年人的行为缺陷。[12]

因此，过错客观标准聚焦于如何界定“理性人”，即如何通过一个“理性人”的模型去对照评价法律拟规制的对象。显然，这是一个抽象的概念，但在具体的设定以及建构中，需考虑的并不是如何假定这个理性人的所有行为都是合理的，而是要将其作为参照物，将行为者的行为与之进行比较，以此认定行为人行为的不法性，即存在过错，最终纳入法律归责范围。这种“理性人”权衡之下的过错标准，具有客观性，它要求法官摒弃主观心态的考察，从一个相对客观的立场出发，对行为人的行为对照“中立”标准逐一评价，尽量降低主观性的偏见，并作出最终的评判。因为法律谴责本身就掺杂着情感性的评判，如果仍将主观过错的判定作为基准，不免加重个人情感色彩。相较之，客观过错的判断注重行为人的不法行为的后果否定性评价，是一个相对中立的立场。同时，法官这种客观性的评判，也符合侵权责任法的要义，即比起惩罚应罚之人，让受害人受到应有的救济更有意义，这也是法律公平价值的重要体现。通过“理性人”标准的确立，普通人对于自身行为的认知有了合理的预期，不必过分把握自己的主观关注和谨慎。[13]

（二）过程演化：由积极确权模式转向行为规制模式

我国现行法律规定个人信息侵权违法的阻却事由仅包括信息主体同意这一项，并积极引导信息主体强化对个人信息的自我控制与保护，属于积极确权模式。但个人信息属性具有双重性，不仅与信息主体权益息息相关，也承担着实现社会利益最大化的任务。这既是大数据时代下个人信息法律保护的必然趋势，也是优化国家现代化治理体系的应有之义。如何实现个人信息保护最大化和社会治理最优化之间的平衡，需要合理把握过错客观化标准对行为人行为规制的尺度。[14]

个人信息因其属性模糊、外延广泛，不能满足权利对象具体、明确的规制要求。在这种情形下，应转向行为规制模式，才能为个人信息主体提供更为全面、更为适当的民事法律保护。首先，行为规制模式针对的是信息处理者在信息收集、存储等阶段的不同行为拟采取的合规控制。它可以针对不同阶段的不同行为提供更有针对性的保护措施，以实现层阶化的合法权益保护。其次，行为规制模式主张，行为规制模式与信息生命周期相结合，将信息的收集、处理、存储等行为纳入规制对象，从而形成一套完整的行为合规指引。最后，行为规制模式具有双重性。一方面它遵从法律规则，要求行为人所有信息处理行为都应遵守相应的法律规则；另一方面，在法律遵循之外，所有的信息流通环节都应符合行业规则标准，这个标准往往要严于法律控制。因为，个人信息的范围和类型非常广泛，某些特定类型的个人信息与自然人的人格密切相关，作为特定人格要件受到法律的特殊保护。在这种情况下，如果收集和使用这些具备人格要件性质的个人信息，行为人除需满足基本信息规制要求，还必须遵守更为严格的人格权的相关规定和要求，并获得权利主体的明确授权。而对于那些不具备人格要件性质的个人信息，由于法律规制强度相比更低，故而立法者更需要在信息保护与信息利用之间进行权衡，以作出更为妥当的决策。[15]此时，行为规范模式不仅能够为满足各类信息主体的救济需求，而且能够保证个人信息保护更具有层阶性和动态性，从而实现个人信息保护制度与人格权保护制度相互衔接，实现民法

〔11〕参见王泽鉴：《德国法上损害赔偿制归责原则》，中国政法大学出版社2008年版，第276页。

〔12〕参见李响：《美国侵权法原理及案例研究》，中国政法大学出版社 2004年版，第139页。

〔13〕参见李犊、张铁薇：《正义与侵权行为法归责原则的类型演进》，《学术交流》2018 年第1期。

〔14〕参见吴伟光：《大数据技术下个人数据信息私权保护论批判》，《政治与法律》2016年第7期。

〔15〕参见张勇：《敏感个人信息的公私法一体化保护》，《东方法学》2022年第1期。

保护的有机兼容。

三、要素的确立:合规性考察下个人信息侵权客观评价

在互联网企业的发展中,数据合规是重要的一环。欧美互联网公司在个人信息保护上一直走在世界的前沿。2020年Securiti.AI公司推出了五款个人信息合规产品,是当前域外互联网企业在数据合规操作上的佼佼者。笔者拟通过这五款产品的技术与功能场景的考察,进而提炼相关的合规性要素,为个人信息侵权行为的客观评价提供借鉴。

表1　Securiti.AI的5种合规产品的技术与功能场景

产品	技术操作	功能场景	涉及合规内容	要素提炼
Data Fulfillment Automation	1、构建一个或多个动态请求表单并嵌入到客户的网站中接受数据主体的请求;2、收集DSR请求,并根据用户的身份创建DSR工作流程;	针对不同的用户身份设计不同的信息处理流程;	特殊主体身份信息处理的区别	信息主体身份
	3、DSR工作流程提交给后台,后台有机器人助手Auti,可关联到用户John A.的数据,帮助完成DSR任务并且同步系统; 4、生成DSR履行的审查报告,以证明遵循隐私合规。	1、为消费者提供数据权利请求的窗口;2、收到请求立即或者在规定时间内进行响应。	履行访问权、修改权和删除权等	信息处理方式
PD Linking Automation	1、生成个人数据的关联报告; 2、跨国企业的个人数据的治理与可视化; 3、数据泄露后的及时通知受影响的数据主体。	可将企业在不同时间、不同系统收集和存储的某个数据主体相关数据进行关联。	辅助用户数据权利响应、用户的归属地管理、数据泄露用户通知产品的功能	
Assessment Automation	隐私风险评分服务	企业可邀请与合作的多个第三方组织,共同接入评估平台进行隐私风险评估。	法规CCPA和GDPR均有规定与第三方合作时,必须确保它们的隐私风险控制水平	信息类别评估
hird Party Risk Assessment	产品系统内置不同的合规性模板,如GDPR、CCPA,每一种合规性模板对应各种合规点检查列表和问题	提供了一个协作平台,内部多位安全专家可分工根据合规性模GDPR、CCP逐项检查和评估。	法规抽取出来的合规性检查列表,比如隐私条款设计的强制且明确的合规条项	信息风险评估

(一)要素一:信息主体身份

Data Fulfillment Automation在信息处理过程中,首先会收集用户的身份以及数据处理的授权,并根据用户身份建立不同的流程。如下图2,John A用户填写了个人信息身份,并对其个人信息的处理方式进行了授权。之所以要区分信息主体身份,是因为不同职业的个人信息与容忍义务相关。一般特殊职业的信息主体往往与公共利益密切相关,因此在处理个人信息时则需具备更高的容忍义务。[16]例如,医疗机构在收集和使用医疗数据时,不仅要符合一般数据合规的要求,而且在患者隐私保护和信息安全上应具备更高的要求。此外,个人信息若用于公共利益,不得视为个人信息侵权,如收集人口健

〔16〕参见丁晓东:《用户画像、个性化推荐与个人信息保护》,《环球法律评论》2019年第5期。

康信息，除非其信息处理活动超出合理范围，如因信息收集行为导致个人信息泄露而影响了信息主体的生活秩序，此时应结合具体情况进行规制。

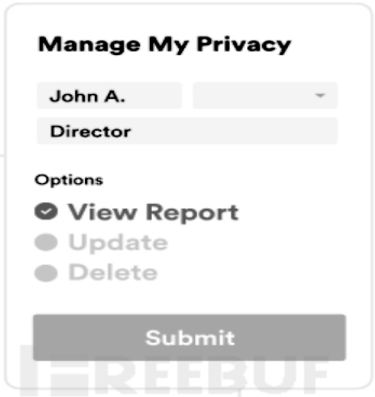

图2 Data Fulfillment Automation信息主体身份收集

（二）要素二：信息处理方式

PD Linking Automation进一步优化了当前数据收集与数据泄露时拟采取的合规性措施：个人数据地图+审查报告（见图3）。个人数据地图可将平台收集到的所有信息关联，并且明确信息处理应基于正当性且在特殊情况下的使用情形。〔17〕而审查报告则是在数据泄露后，应通过关联的信息快速告知用户，并形成处理方式的合规审查报告。从以上功能可以看出，在信息处理方式上应考量信息处理行为的目的、措施和后果等。

就行为目的于损害评价要素的层次性而言，个人信息处理越基于公共目的，信息处理的正当性就越高，法院证成损害存在的难度就越大。例如，当信息处理者是基于维护公共安全、加强社会保障和维护公共秩序的目的时，其行为具有正当性，可以成为个人信息侵权的豁免事由。

就行为措施的多样性而言，信息处理者所采取的行为方式应以公众的合理预期作为评价标准，如果超出合理预期，其所带来的损害后果的评估难度亦会加重。〔18〕由于大数据技术的日益成熟，信息处理能力也不断提高，越来越多的信息处理方法对于个人信息所造成的影响也不断扩大，相应的个人容忍义务也出现了变化。比如人肉搜索行为，这种信息处理方式是普通人无法容忍的，在信息泄露之外，其侵害的更多的是信息主体的生活秩序。在此种情境下，个人信息侵权可以推定损害。而对于那些在公众合理预期之内的信息处理方式，如利用收集信息帮助品牌门店开展精准营销，常见的场景包括：老顾客识别、顾客打标、精准触达，甚至顾客多维度精准画像等。要实现上述功能，需要将收集的顾客个人信息和其他资源融合/匹配/对碰，可能的法律风险根据数据来源、输出数据类型不同而差异较大。除应满足个人信息侵害的一般构成要件外，在事实损害的认定上，还应将实质性损害作为必要因素纳入考量。

就行为后果否定性评价而言，信息处理造成的损害结果越明显，法官就越容易证成损害已经发生。个人信息侵权的损害后果有各种表现形式，除了实际侵权的严重性之外，信息处理行为是否会增加信息主体人身、财产、生命安全的潜在风险，也是法官在损害后果认定中需要纳入考量的因素之一。〔19〕反之，如果信息处理行为所造成的损害相对较小，则属于不可弥补的轻微损害，则视为不具

〔17〕比如，用户向比如Google提出访问个人信息的请求后，Google有多个产品与系统，在浏览器服务器记录用户注册信息和Cookie信息，另外在邮件服务器中也记录了同一用户的个人信息，这两个系统存储的同一个数据主体的信息，但多数企业不会将两个系统进行关联。但GDPR和CCPA要求企业向消费者披露数据主体的相关个人信息，因此关联技术十分重要。

〔18〕参见丁晓东：《论个人信息法律保护的思想渊源与基本原理——基于"公平信息实践"的分析》，《现代法学》2019年第3期。

〔19〕参见朱芸阳：《定向广告中个人信息的法律保护研究——兼评"Cookie隐私第一案"两审判决》，《社会科学》2016年第1期。

有法律意义的损害。

图3　PD Linking Automation个人数据地图、审查报告分流

（三）要素三：信息类别评估

Assessment Automation对涉及个人信息的数据进行了类型化分析，划定了高风险与低风险的信息范围。对于高风险的信息依据相关法律规定设定了一些附加义务，增加了平台对处理此类信息行为的一些程序和环节，而对于低风险的信息，处理行为则相对简单，并豁免了部分规定。同时，针对不同的信息类别，依据私密程度的不同，形成相应的隐私评估报告（见图4）。

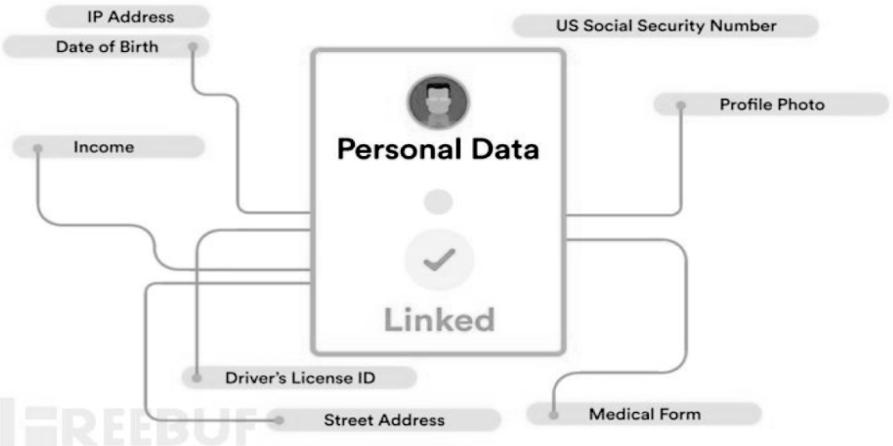

图4　Assessment Automation 个人信息分类

上述合规性操作反映出信息类别评估对信息风险的影响。个人信息的私密性程度越高，侵权造成损害的可能性就越大。依据个人信息的私密性程度，可将信息类别由低到高可依次界定为“合法公开的信息——个人普通信息——个人私密信息”，随着信息类别私密性程度的加深，损害概率也将逐渐增加。[20]依法披露的个人信息的私密性程度最低，信息处理者有权根据民法典第1036条第2款的规定对其进行处理，但信息主体明确拒绝处理或信息处理行为会侵犯其重大利益的除外。如果个人信息的私密性程度越高，则往往会涉及个人隐私权的重合，此时应优先适用隐私权的相关规定。[21]而个人普通信息私密性程度居中，其权利的减损通常要考察相应损害的发生，其保护强度亦介于合法公共信息和个人隐私信息之间。只有在过度处理的情况下，信息主体才会受到人格或财产的损害。[22]又如，基于个人信息的私密性程度，在征得个人信息主体同意的方式上，有概括同意（一揽子同意）和逐项同意

〔20〕参见陈磊：《隐私合规视角下数据安全建设的思考与实践》，《保密科学技术》2020年第4期。

〔21〕参见王利明：《民法典人格权编中动态系统论的采纳与运用》，《法学家》2020年第4期。

〔22〕参见临汾中院（2016）临民初字2429号民事判决书。

(区分产品线:一般信息和敏感信息),默示同意和明示同意之分。根据目前个人信息合规立法的趋势,逐项同意和明示同意要求越来越可能成为同意的一般合规义务。

(四)要素四:信息风险评估

hird Party Risk Assessment对照合规性标准设定不同的风险等级,并就个人授权情况形成相应的风险监管(见图5)。比如用户只授权了信息用于数据分析,但是若发现在广告推荐上利用了该信息,则会出现风险提示,要求企业立即采取相应的规制措施。

图5 hird Party Risk Assessment信息风险评估

因此,在利用网络侵害个人信息的案件中,法官可根据特定的场景,进行程度化的考量,结合个人信息风险进行评价(见图6)。首先,结合个人信息处理的具体场景,初步判定个人信息控制者的个人信息处理过程;其次,分析个人信息处理活动对个人权益造成的影响,并判定相应的影响程度;最后,根据个人信息处理活动涉及的特点、相关方、规模等进行分析,得出风险等级。

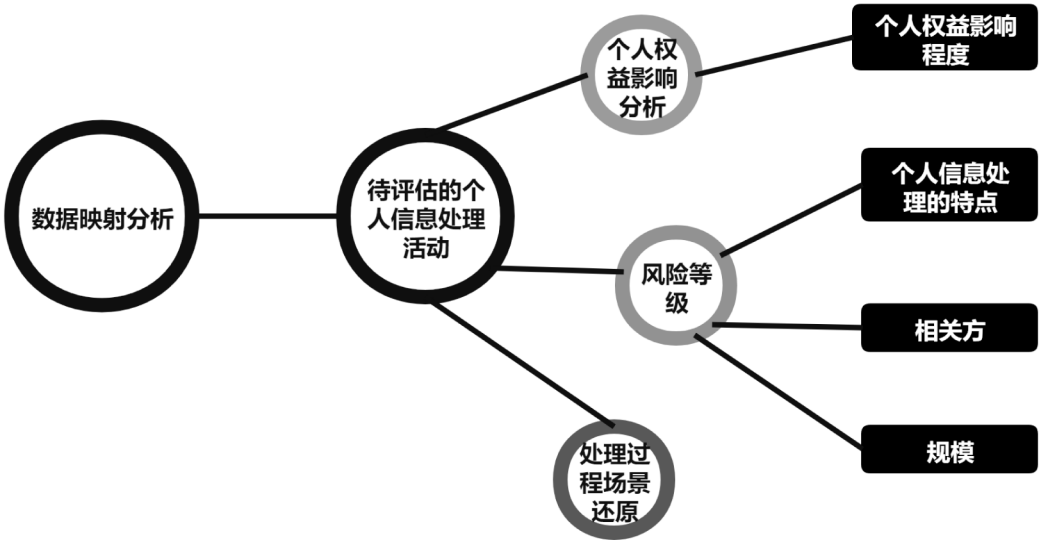

图6 个人信息侵权行为风险评估

四、具体化路径:个人信息侵权客观归责的层阶式演化

侵权责任法要义在于风险分担,弥补损害,其法律功能旨在对不同位阶价值权益的保护,而其价值的取舍会因目的性和必要性的不同而存在差别。因此,从客观性评价要素而言,个人信息侵权的价值权衡应契合其行为的特殊性,具体按照"信息主体身份——信息处理方式——信息类别评估——信息风险评估"的顺序依次进行考量。[23]而就联动关系而言,结合信息属性及其处理过程的融通性,其各个要素之间的联动耦合有赖于当前数据合规的相关规定以及司法实践的经验总结,具体可从以下三个层次进行路径演化:

(一)层次一:要素的同质关联

信息风险评估往往和其他要素有同质关联性。风险等级的高低往往与信息处理行为的目的、方式、后果紧密相关(见图7)。关于风险等级的界定,目前没有统一的标准,可参考欧盟实践,区分低风险、中风险和高风险三个等级。低风险是指风险场景干扰的可能性较低,所造成的损失很小(一般限于经济损失),数据管理方仅需采取企业内部合规措施即可;中风险是指风险场景会严重干扰到个人用户,不仅会造成中等程度经济损失,还会对个人生活造成影响,且需要数据管理方采取法律规制措施;高风险是指风险场景会对个人用户生命财产安全构成威胁,且数据管理方若不采取措施将会造成不可挽回的后果,如巨额经济损失以及公信誉丧失等。[24]

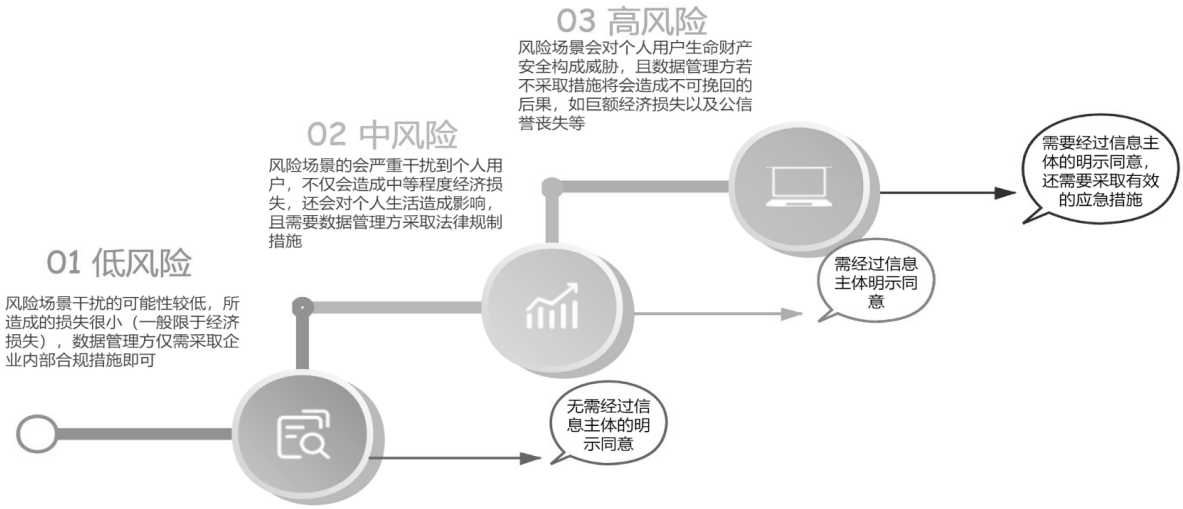

图7 个人信息风险评估与其他要素同质关联导图

若风险评估为低风险,信息处理者可以不经过信息主体的明示同意而处理;若风险评估为中风险,则需经过信息主体的明示同意,即满足①信息主体对此是知情的;②且自愿作出;③具体的声明或者用明确肯定的行为表示同意三个条件,方能视为获得了信息处理的授权;若风险评估为高风险,不仅需要经过信息主体的明示同意,还需要采取有效的应急措施。如个案中,法院认为"用户向被告所提供的姓名、地址和联系方式等个人信息是双方交易过程所必须提供,而双方在发生纠纷时,被告通过上述信息用于交易核实、纠纷调解,仍处于消费者的合理预期内,因此不构成个人信息的侵害"。[25]

〔23〕参见周晓晨:《过失相抵制度的重构———动态系统论的研究路径》,《清华法学》2018年第4期。

〔24〕参见黄春林:《网络与数据法律事务》,人民法院出版社2019年版,第187页。

〔25〕参见北京互联网法院(2019)京0491民初313号民事判决书。

该案例的风险场景为低风险，被告使用信息限于双方内部纠纷解决，因此可不经过信息主体的明示同意。

（二）层次二：要素的互补关联

根据数据的合规特点，不同的要素之间，其互补关系亦不相同。首先，信息主体身份是最首要的评价要素，它往往影响着其他要素的评估力度。一般而言，具有特殊身份的信息主体或者信息处理者归属于特殊行业，那么在其他要素的考察上，其所占比重相对于普通个人要适当酌减。比如信息处理方式的合理预期范围要高于普通个人。其次，信息风险评估与信息类别具有相互补充的关系。在信息类别与信息风险评估成正比时，如个人私密信息被扩大传播造成高风险时，其认定为个人信息侵权为理所当然。但若二者为负相关时，若个人信息为隐私信息，但其传播的范围很小，仅造成轻微损害的，其过错评价可忽略不计。若个人信息虽然是是信息主体自愿公开的信息，但是因他人传播导致范围超出合理预期，且给信息主体造成巨大损失，那视为有过错，仍应进行规制。最后，信息处理方式与信息类别具有紧密的互补关系。倘若已满足某一要素，且量化程度很高，那么尽管另外其他要素契合度更低的情况下，通常也不会影响侵权责任的成立。例如，在个案中，法院虽认定读书信息不具有私密性，但由于特定信息的目的、方式和范围知晓的清晰程度，以及作出意愿表示的自主、具体、明确程度已经超出“一般用户的合理预期”，故认定被告侵害了原告的个人信息权益。〔26〕

（三）层次三：要素关联的例外情形

大数据时代的发展，信息公共利益和个人信息利益的摩擦会更为频繁，如果这些摩擦均纳入规制范围将不利于公共利益的实现，因此应关注正当化事由和责任减免事由。根据个人信息保护法第13条之规定，可以限定为以下三个方面：其一，被收集信息者同意，包括明示同意和推定同意。比如用户在阅读隐私声明后作出的意思表示就是明示同意，而基于客观判断，能够确实的期待信息主体同意的情况下视为推定同意；其二，双方约定行为或者法定行为使用个人信息的，行为具有正当性；其三，出于公共利益或紧急的国家利益、社会利益的保护使用个人信息的可作为豁免事由。

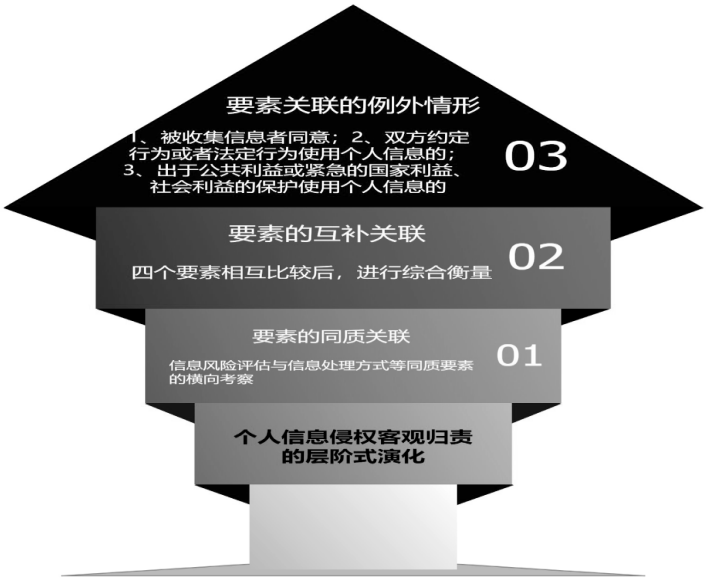

图8 个人信息侵权行为客观归责导图

综上，在发挥防卫数据爆炸时代引发的公共风险的同时，还应避免社会防卫和公共风险防卫的过度化，及其对个人正常生活空间的过度挤压。基于上述客观过错标准的确立，能够形成全方位、多样性和层次性的侵权行为评估，有助于确认规范性要素在个人信息侵权损害判断中的重要价值。

〔26〕参见北京互联网法院（2019）京049 民初16142号民事判决书。

结　语

在大数据时代，个人信息保护环境发生了巨大变化，数据安全与公民个人信息的全面防护成为当前民法领域所要面对的重要课题和挑战之一。然而通过检视当前的司法实践，传统的个人信息主观归责标准不能有效应对静态数据向动态数据演变带来的种种困境。个人信息的保护应当针对个人信息的属性、类别作出差别化规制，最大程度的实现社会信息治理功能与个人权益维护的有效平衡。过错客观化在个人信息侵权归责中具有独特的适用价值，通过行为规制模式，对客观评价要素进行总结，并进行不同层次的关联，有助于明确个人信息侵权责任的正当化边界。