财经法学 No. 3，2026
pp. 156 - 171

非合理处理已公开个人信息违法性的危险层次化判断

宗绍昊*

内容提要：非合理处理已公开个人信息行为可能触及民事、行政或刑事违法性，但不同违法性之间的界限十分模糊。目的层次化判断和危险层次化判断是区分非合理处理行为不同违法性的两种基本模式。现有目的层次化判断方案导致公开目的之查明事实无用或不能、传递或监控目的流转的成本过高、违背历史解释结论并欠缺违法性的程度区分功能。非合理处理行为违法性的判断需协调已公开个人信息的多元价值和特殊规范属性，与之相匹配的是危险层次化判断方案，该方案能以危险的程度差异实现不同违法性的判断标准配置。其中，前置违法性（民事和行政违法性）指向作为低度危险的危险升高标准，旨在将属于容许危险（“信息中介”）或危险降低（更严格的技管融合治理）的信息处理行为排除于外；刑事违法性指向作为高度危险的危险失控标准，需贯彻先形式标准后实质标准的基本路径，核心是判断信息处理者是否基于后续犯罪的意图而获取已公开个人信息，或将获取的已公开个人信息提供给可能对信息主体实施不利益行为的多数第三人。

关键词：已公开个人信息　非合理处理　违法性判断　基于危险的方法　民行刑一体化

《个人信息保护法》第13条第1款第6项及第2款规定，“依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息”的，不需取得个人同意。合法公开状态中的已公开个人信息处于保护与利用的交叉地带，各方主体均可在合理限度内自由地获取并处理相关个人信息。但这种合理限度通常被相关主体所漠视，违反合理处理规则的行为屡见不鲜，民事、行政和刑事违法性可能交叉存在。在非合理处理行为潜在地混杂着多重违法性的情况下，〔1〕需要

* 宗绍昊，中国政法大学数据法治研究院博士研究生。

〔1〕 本文所述的“非合理处理行为”特指违反《个人信息保护法》第13条第1款第6项的信息处理行为。虽然，可将其称为“违法处理行为”，但事实上，违法处理行为的指涉非常广泛，违反《个人信息保护法》其他规定处理已公开个人信息的行为仍是违法处理行为，如违反该法第21条的委托处理行为。

为不同违法性边界的划分提供方案，以令民行刑各司其职、协同共治。〔2〕但现实情况是，同一非合理处理行为极易对应不同的违法性，导致在此案中仅具有民事违法性的非合理处理行为在彼案中直接具有刑事违法性。例如，在麦某波诉北京法先生科技有限公司等网络侵权责任纠纷案中，麦某波于2022年8月发现被告微信小程序“法先生法律大数据”及其网站未经同意公开了原告的姓名、联系方式等个人信息，并编造、篡改胜诉率、执业年限等信息后公开。法院认为，该公司的非合理处理行为具有民事违法性，应当承担向原告麦某波赔礼道歉、赔偿经济损失的侵权责任。〔3〕而在李某侵犯公民个人信息案中，李某利用企查查网站下载企业信息之后，整理成含有公司名称、法人代表姓名、联系方式、公司地址、邮箱在内的企业个人信息数据并在淘宝上销售，共出售90余万条信息。法院认为，其行为已构成侵犯公民个人信息罪。〔4〕两案差异性仅体现为涉案已公开个人信息的数量，这不足以成为确认后一非合理处理行为刑事违法性的充要条件，因为在吴某侵犯公民个人信息案中，检察院对同样满足2017年5月8日最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第5条定罪数量标准的行为，最终认为其不构成犯罪并予以不起诉处理。〔5〕这种针对非合理处理行为不同违法性辨别的混乱局面势必严重侵害涉案行为人的利益。当前民行刑等各部门法主要研究合理处理规则的构造问题，而缺乏区分非合理处理行为不同违法性的系统研究。〔6〕

一、非合理处理行为违法性的目的层次化判断困境

民行刑一体化结构强调的是民法、行政法的前置性以及刑法的后置性，〔7〕由此形成不同违法性的层次化配置格局。“理论与实践之间是循环促进的动态关系”〔8〕，但从既有理论上看，非合理处理已公开个人信息违法性的层次化判断一边倒地偏向目的层次化方案，这使得司法实践的理论选择空间不足，再加之目的层次化判断自身附随的巨大弊端，导致违法性合理分配的目标不达。

（一）层次化判断的两种模式：目的层次化与危险层次化

个人信息保护存在两大基本逻辑，即“基于权利的方法”和“基于危险的方法”。〔9〕目的层

〔2〕 参见刘艳红：《民刑共治：中国式现代犯罪治理新模式》，载《中国法学》2022年第6期，第27页。

〔3〕 参见广州互联网法院（2022）粤0192民初20966号民事判决书。

〔4〕 参见江苏省扬州市中级人民法院（2020）苏10刑终79号刑事裁定书。

〔5〕 参见卢志坚、白翼轩、田竞：《出卖公开的企业信息谋利 检察机关认定行为人不构成犯罪》，载《检察日报》2021年1月20日，第1版。

〔6〕 一个有趣的现象是，刑法上合理处理的出罪机制建构占据绝对的研究主导地位，非合理处理行为的刑事违法性判断遇冷。然而，合理处理行为是前置法上典型的合法行为，不可能触犯刑法，更不必讨论出罪机制的具体构造，当前对合理处理行为所存在的构成要件该当性出罪模式和违法性出罪模式之争并无益处。这种研究的不当偏重，更加突出了本文试图建构民行刑一体化违法性判断体系的必要性。

〔7〕 参见张德权、夏伟：《侵犯公民个人信息罪的实质限缩》，载《郑州大学学报（哲学社会科学版）》2025年第5期，第71页。

〔8〕 刘艳红：《中国刑事执行法学的自主知识体系构建》，载《法律适用》2026年第1期，第13页。

〔9〕 本文将“基于风险的方法”称为“基于危险的方法”，意欲以此强调后种“危险”与信息主体实体法益的关联性，避免制度性风险等空泛理解。

次化判断和危险层次化判断是由个人信息保护基本立场衍生的、判断非合理处理已公开个人信息违法性的两大基本方案。

基于权利的方法是严格保护信息主体相关信息权利的体现，并试图为其确立一项绝对的、排他的控制性权利——个人信息自决权。这一自下而上的赋权逻辑大多为私法学者所采。〔10〕个人信息自决权的核心命题是，“由公民基于其内心、自由地决定其自身信息何时、何地、以何种方式被收集、储存、处理以及利用的权利”〔11〕。在该命题下，目的与用途限制原则（简称“目的限制原则”）成为个人信息保护的帝王条款，信息主体对目的和用途的控制性被认为是自我决定权的直接体现。目的层次化判断方案强调以信息处理者的目的与用途之于信息主体的目的与用途的违反性程度，〔12〕作为区分非合理处理已公开个人信息所对应的不同部门法违法性的手段，这恰恰是对上述命题的直接反映。其中，信息处理行为一旦违背信息主体的公开目的与用途即具备民事和行政违法性，如伊某与江苏苏州某公司侵犯个人信息权纠纷案等；〔13〕而明显违背信息主体的公开目的与用途的处理行为即构成侵犯公民个人信息罪，〔14〕如最高人民法院第 194 号指导性案例等。〔15〕因此，作为当前通说观点的目的层次化判断方案是以个人信息自决权为价值取向的产物。

新近基于危险的方法被广泛提倡，这一自上而下的规制逻辑大多为公法学者所采。〔16〕基于危险的方法强调，不必为信息主体确立一项个人信息自决权，这种权利绝对化的理论构造不仅不利于信息主体的个人信息保护，也无法与个人信息流通与利用的环境发生有效兼容。在此基础上，其一方面承认一些信息主体的工具性权利，另一方面认为只要将危险控制在可被容许、可被接受的范围之内，即不会侵害或威胁信息主体的合法权益，并可据此适当地允许个人信息的流通与利用。〔17〕基于危险的方法衍生危险层次化判断方案，即以个人信息处理行为所指向的不同程度的危险作为区分不同部门法违法性的手段，如北京互联网法院发布的 10 起个人信息保护典型案例之六：王某与北京某科技有限公司人格权纠纷案等。这一方案并未被司法实践普遍接受而仅在少数案件中出现，尚未形成危险层次化判断的系统理解。

（二）目的层次化判断的局限

我国《个人信息保护法》第 6 条第 1 款强调的是公开目的对处理目的的限制，但这种限制并非传统上的强限制，而是具有一定的宽松度，可以在直接或合理关联的范围内有限制地兼容少量其他目的（是否可兼容商业目的存在争议），因而可将其称为缓和的目的限制原则。即便如此，

〔10〕 参见王利明：《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》，载《现代法学》2013 年第 4 期，第 67 页。

〔11〕 姚岳绒：《论信息自决权作为一项基本权利在我国的证成》，载《政治与法律》2012 年第 4 期，第 72 页。

〔12〕 参见邢会强：《场景理论在〈个人信息保护法〉解释中的应用》，载《数字法治》2024 年第 2 期，第 76 页。

〔13〕 参见江苏省苏州市中级人民法院（2019）苏 05 民终 4745 号民事判决书。

〔14〕 参见周光权：《侵犯公民个人信息罪的行为对象》，载《清华法学》2021 年第 3 期，第 40 页；宋伟卫：《处理已公开个人信息的刑法边界》，载《吉林大学社会科学学报》2022 年第 6 期，第 81 页。

〔15〕 参见《最高人民法院发布第 35 批指导性案例》，载《人民法院报》2022 年 12 月 29 日，第 2 版。

〔16〕 参见王锡锌：《个人信息权益的三层构造及保护机制》，载《现代法学》2021 年第 5 期，第 105 页。

〔17〕 See Yuhong Yan, *The Risk-Based Approach to Personal Data Protection and the Response of the International Trade Law*, 14 Beijing Law Review 1250, 1256 - 1257 (2023).

非合理处理已公开个人信息违法性的目的层次化判断在方法论上仍存在若干弊端，进而促成权利泛化现象的出现。〔18〕这种理论构造的内在缺陷为层次化判断方案的转型奠定了基础。

首先，查明已公开个人信息之公开目的存在事实无价值或不能实现的两难现象。信息主体的信息公开大致发生于公共管理领域、经营消费领域和社会交往领域之中，并分别对应信息主体与国家机关、信息主体与社交软件以及信息主体与电商平台的互动关系。〔19〕但无论针对何种领域与何种关系，信息公开的目的要么因具有多样性而导致所有的处理行为均符合使用限制，要么因停留在信息主体的主观世界而不可查。例如，根据《政府信息公开条例》第1条的规定，政府信息公开的目的包括便于获取和提升透明度。而根据2016年8月29日最高人民法院《关于人民法院在互联网公布裁判文书的规定》的要求，裁判文书的公开旨在促进司法公正和提升司法公信力。可见，任何人以合法方式获取政府信息和裁判文书的行为均有利于实现其公开目的。在此基础上，诸如企查查等平台通过公开渠道汇聚了海量的数据，并有偿提供给查询者，经过企查查等平台的中转，信息公开的目的被演变为盈利。如此一来，只要查询者进行了付费服务，其便不违反使用限制的要求。如果再加上“兼容目的”，所谓的使用限制更无继续存在的意义。在不同公开目的的叠加过程中，距离第一位信息处理者越远，越不可能发生背离使用限制的现象，因为总有一项公开目的适合某位信息处理者。又如，信息主体在社交软件上公开部分个人信息，其可能系出于特定范围或直接公开式分享、交友、获取流量/知名度/经济利益等目的。面对案件中海量的信息主体，要求信息处理者逐一核查信息公开目的并不现实，且事后获得的事前公开目的亦不具有可信性。数字时代，海量数据经算法聚合和分析之后导致信息处理者查明所涉信息初始来源已力有不逮，更遑论比初始来源要具体百倍的公开目的。对此，有论者提倡以推定的同意法理解决上述问题，并认为后续的信息处理行为均在信息主体的同意范围内，〔20〕或者以信息主体的合理期待作为规制推定的同意适用边界之标准。〔21〕显然，前者不存在任何使用限制，而后者所谓的合理期待亦因前置的公开目的之极端不确定性可能制造出“虚假同意”，最终演化为“解释者的同意”并悄然转向客观判断信息处理行为的应罚性，而与公开目的不再具有任何关联性。实际上，“目的明确且正当→使用限制”构成目的限制原则的全部内容。在两个环节的关系问题上，前者是后者的逻辑起点，而后者则属于前者的直接或兼容性落实。可见，“目的限制原则依赖于一个前提条件，即信息处理目的在收集信息之时予以确定是可能的”〔22〕。这意味着，目的限制原则的两个环节应发生在同一场景之下，即信息主体和信息处理者的角色恒定不变。在已公开个人信息的场景下，因信息处理者的（多次）变更，信息主体和信息处理者之间的联系发生断裂，此时的目的明确且正当环节既无存在的空间，亦不可能实现。

---

〔18〕 参见林轲亮：《新质生产力催生下的新兴权利：类型分野、生成标准及法治保障》，载《广西大学学报（哲学社会科学版）》2025年第3期，第155页。

〔19〕 参见曹博：《个人信息可识别性解释路径的反思与重构》，载《行政法学研究》2022年第4期，第137－142页。

〔20〕 参见宁园：《“个人信息已公开”作为合法处理事由的法理基础和规则适用》，载《环球法律评论》2022年第2期，第72页。

〔21〕 参见刘双阳：《“合理处理”与侵犯公民个人信息罪的出罪机制》，载《华东政法大学学报》2021年第6期，第66页。

〔22〕 朱荣荣：《个人信息保护“目的限制原则”的反思与重构——以〈个人信息保护法〉第6条为中心》，载《财经法学》2022年第1期，第21页。

其次，传递公开目的与实施过程监控的成本过大。已公开个人信息的信息处理者与信息主体之间存在若干其他信息处理者。若其他信息处理者能够有效传递原初公开目的，使用限制仍存在实现的可能性。然而，鉴于“‘个人信息被公开时的用途’本身也是一类信息”，在缺乏法律明文规定和实际收益激励的情况下，其他信息处理者并无动力再增成本以实施该种“利他行为”。〔23〕同时，这种成本还会随着其他信息处理者或信息数量的增多而呈现出几何倍数的增大。换言之，距离信息主体越遥远的信息处理者传递公开目的的动力越低、成本越高、难度越大。“由于数字时代的法律得以建立的社会结构已开始从平面空间向立体空间变迁，传统‘点对点’的线性社会关系也开始向‘点对面’的交叉社会关系演变。”〔24〕如果说传统中心化、线性因果的环境尚且具备传递信息的条件，当前分散化、非线性的复杂环境则直接损毁了该种传递基础。在信息不间断地混合、加工的过程中，传递公开目的无疑成为一种奢望，更遑论履行“知情同意”规则。以大语言模型为例，最新的开源大模型基于纯强化学习、混合专家模型等形成推理能力并达到顿悟时刻，其中参数量级的竞争日趋激烈，其训练语料库涉及诸如书籍、文章、评论、在线对话和人工生成的数据等各项来源，互联网上公开可用的数据占据其训练语料库的大部分内容。大语言模型将这些数据进行预处理和深度挖掘之后，最终按照需求呈现给用户。在训练数据的初始搜集阶段，公开目的存在标注和未标注两种可能性。面对其中未标注公开目的的数据，大语言模型无力探索其公开目的；面对其中已标注公开目的的数据，大语言模型在耗费大量算力的基础上似乎可以实现，但这种可能性在数据清理、汇总、结构化等过程中亦归于虚无。实际上，信息传播具有不可逆性，传播者与接收者之间享有复制平等，追查在先的目的主张并不存在。此外，大数据技术的特性在于发掘存量信息的隐藏价值，这意味着在信息处理过程中随时随地均可能发生无预期的使用场景变动之情形。〔25〕这种信息处理的特征要求处理者必须对信息处理过程进行实时监控，一旦超越使用限制便立即停止使用并再次履行“知情同意”规则。这些措施（监控＋通知＋同意）不仅对于信息处理者而言代价高昂乃至不可履行，〔26〕对于信息主体而言亦具备相当大的干扰成本和“知情同意”成本，且因抑制信息竞争而可能迟滞信息处理者发展能力，〔27〕并非双方理性人的合理选择。例如，在王某侵犯公民个人信息案中，法院认为“在相关信息已经合法对外公开的情况下，要求行为人的收集、整理、交换等行为仍需得到‘被收集者同意’的要求过于苛刻也不合理”〔28〕。

再次，合理处理规则的历史沿革否认目的层次化判断。《个人信息保护法（草案）》（一次审议稿）第 28 条将“使用限制”作为判断对已公开个人信息的处理行为是否合理的核心标准。《个人信息保护法（草案）》（二次审议稿）遵循了相同的判断逻辑。但是，现行实证法完全删除了与使用限制相关的所有表述而仅保留“合理的范围”这一项限制内容。对于此次修改，全国人大

〔23〕 参见赵艺、杨洁：《论依法公开个人信息的“合理”处理》，载《人权》2023 年第 1 期，第 168 页。

〔24〕 周佑勇：《从部门立法到领域立法：数字时代国家立法新趋势》，载《现代法学》2024 年第 5 期，第 5 页。

〔25〕 参见付新华：《生成式人工智能对个人信息保护法的结构性冲击及应对》，载《法学论坛》2025 年第 6 期，第 104 页。

〔26〕 See Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 Seton Hall Law Review 995, 1006 (2017).

〔27〕 See Tal Z. Zarsky, *The Privacy-Innovation Conundrum*, 19 Lewis & Clark Law Review 115, 136 (2015).

〔28〕 江苏省苏州市姑苏区人民法院（2018）苏 0508 刑初 40 号刑事判决书。

宪法和法律委员会的理由系做好“与民法典有关规定的衔接”〔29〕。即，在《民法典》第1036条第2项未对合理处理行为进行使用限制的基础上，《个人信息保护法》不能作出多余的规定，由此实现法秩序的统一。遵此逻辑，现行实证法完全抛弃了对合理处理行为的使用限制，而非将其作为不成文的构成要件要素。诚然，基于刑事违法的相对独立性，刑法可以作出与前置法相异的概念解释结论。然而，违背使用限制的信息处理行为存在属于合理处理行为的可能性。这一结论在前两次审议稿中有所体现，其强调在用途不明确时，信息处理者仍“应当合理、谨慎地处理已公开的个人信息”。此处所谓的“用途不明确”，意味着信息处理者的处理行为可能与之相符，也可能与之相异，却均可构成合理处理行为。既然如此，非合理处理行为违法性的层次化判断方案便不能直接以之作为判断标准，否则即有可能将前置法上的合法行为误认为构成侵犯公民个人信息罪。

最后，目的层次化方案欠缺违法性的程度区分功能。非合理处理行为违法性层次化判断方案所应解决的核心问题是民事、行政违法性与刑事违法性的界分问题，因为前两者对应的违法行为距离合法行为明显更近、对于涉案行为人权益影响程度明显更小，所以通常采取宽松的违法性判断方法。目的层次化判断方案虽试图解决非合理处理行为违法性的界分困境，但其所使用的方法反而加剧了不同部门法的界限模糊状态。在已公开个人信息的情况下，目的限制原则的基底是个人信息自决权，其只能被判断是否受到了侵害，即纯粹“有无”的判断，无法确定其受到了多大程度的损害，这就为违法性的层次化判断留下了漏洞。个人信息自决权的内容非常宽泛、模糊，在强调主观重要性的同时无法提供一个精确的尺度来确定已公开个人信息处理行为是否需要刑法介入规制。事实上，各国对目的限制原则设定的一系列证明标准，均因缺乏客观内容而无法建立起与目的之间的关联性，导致同一事实在不同决策者的权衡之间最终走向不同的结局。〔30〕在此基础上，以个人信息自决权为核心的审查框架会滑向“形式数量论”，即以司法解释规定的个人信息数量标准作为区分民事、行政违法性与刑事违法性的方案。但是，良法善治的境界是形式与实质的统一。〔31〕前者并非后者的充要条件（不对应性），〔32〕并可能在唯数额论的过程中忽略其他证据的搜集（证据缺失），〔33〕导致一些案件出现违背公平正义的裁判结论。既然针对个人信息自决权的侵害本身无法被有效证明，以“明显违背”为核心的刑事违法性判断标准亦无法实现，因为只有在知悉违背对象的结构的前提下才能据此得出违反程度的判断，即后者需以前者为部分依托。例如，将已公开个人信息从公共管理领域或社会交往领域转移至经营消费领域的行为，究竟是“轻微违背”还是“明显违背”公开目的与用途？将已公开个人信息从合法领域转移至非法（含侵权、违法与犯罪）领域的行为，是否可以根据非法领域的类别确定“轻微违背”还是“明

〔29〕 江必新：《全国人民代表大会宪法和法律委员会关于〈中华人民共和国个人信息保护法（草案）〉审议结果的报告——2021年8月17日在第十三届全国人民代表大会常务委员会第三十次会议上》，载《中华人民共和国全国人民代表大会常务委员会公报》2021年第6期，第1132页。

〔30〕 See Maximilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-Based Approach, Principles, and Private Standards as Elements for Regulating Innovation*, Nomos Verlagsgesellschaft, 2018, p. 35.

〔31〕 参见周佑勇：《习近平法治思想对推进中国式法治现代化的理论创新》，载《学习与探索》2024年第6期，第6页。

〔32〕 参见陈少青：《罪量与可罚性》，载《中国刑事法杂志》2017年第1期，第53页。

〔33〕 参见张耕、黄国赛：《民刑交叉视角下商标刑事保护边界研究》，载《知识产权》2020年第12期，第51页。

显违背”？可见，该标准实际上只是对非合理处理行为刑事违法性判断中的“情节严重”要件进行了简单的词语置换，并未进一步解决罪量的实质判断标准问题，最终在充满模糊性的“明显违背”标准之间或将走向解释恣意的结局。

二、非合理处理行为违法性的危险层次化判断立场

基于现有目的层次化判断方案的一系列弊端，应提倡一种区分非合理处理已公开个人信息违法性的新立场，以实现有效识别不同部门法违法性的目标。这一立场应首先对已公开个人信息所兼具的保护和利用属性进行平衡，并据此分配非合理处理行为不同违法性的判断标准。

（一）危险层次化判断的理论优势

在围绕已公开个人信息而展开的多方权利主体之中，信息主体处于权利结构的最末端地位。为解决这种结构上的不对称性，目的层次化判断方案试图通过为信息主体设置一系列的权利来实现对信息处理者的限制。然而，其一方面在人格属性与财产价值之间因偏重前者而导致失衡。个人信息是数字经济发展的重要数据基础，其能够被商业化利用而具备财产价值，因而财产价值是个人信息的天然属性，否则侵犯公民个人信息罪中规定的出售行为便不存在实现的可能性。另一方面在个人保护与社会保障之间因偏重前者而导致失衡。其代表的自主控制范式难以规范地位不平等、不对称结构下的个人信息多方处理关系，由此引发诸如“知情同意”规则形式化、救济成本过高等保护不足现象。事实上，个人自决不能被定性为合法的“权利”，它们不是国家可以提供给个人的东西。相反，国家能够尊重个人自治，并尽可能为个人提供一些必要的条件。〔34〕在自主控制范式下，因缺乏权力机关监管责任等社会保障路径的充分介入，面对大规模、持续性、累积性的信息处理危险，个人保护反而落入下乘。据此，应选择以“危险”替代“目的”作为非合理处理已公开个人信息违法性的层次化判断理念，以矫正信息主体与信息处理者权力悬殊的力量对比。

危险层次化方案有利于建立和谐共生的已公开个人信息保护与利用的格局，防止出现“公地悲剧”和“反公地悲剧”的不良现象。“公地悲剧”强调的是在权利缺乏的情况下，信息处理者基于利益最大化原则极尽个人信息之能量而不问信息主体之利益，导致绝对开放的信息流被过度消耗；“反公地悲剧”指的是因过度权利化而引发的“权利丛林”现象，在密集的权利主张之间最终阻碍信息有效利用。目的层次化判断方案虽解决了“公地悲剧”难题，却可能在适用过程中演变为“反公地悲剧”。在已公开个人信息的场景下，目的层次化判断方案严格限制信息处理行为的目的和用途，在最小化使用的同时，极大地缩小了信息处理范围，从而阻碍了信息挖掘与创新。同时，囿于“知情同意”规则陷阱等行权障碍，其最小化使用并未实现最大化保护，“收益＜成本”的情况客观存在。相比较而言，危险层次化判断方案在两个难题的相互平衡之间提供了一条更为科学的个人信息规范路径。其并非不对信息主体赋权，而是在仅排斥一项绝对的个人

〔34〕 See Antoinette Rouvroy & Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, in S. Gutwirth ed., Reinventing Data Protection?, Springer, 2009, pp. 59－60.

信息自决权外，仍认可诸如查阅权、复制权、删除权等工具性权利。换言之，其践行的是低度赋权路径。正因如此，其并非不保护信息主体的利益，只不过是在持续不平等关系的多方主体关系中，由更具有优势地位的公权机关“自上而下”地对信息处理行为的危险进行具体、动态地调控，并同时允许信息主体以力所能及范围内的权利“自下而上”地参与信息治理过程，限制上下两端对信息处理者施加的合法性义务。“自上而下”与“自下而上”相结合，催生的是信息处理者“由内而外”地合法合规处理信息的行为。由于公权机关监管的危险控制属性，信息处理者不会因频繁的权利需求和合规需求而被拘束，可在完成信息保护义务的基础上以更加自由的状态处理个人信息。危险层次化判断方案的这一特征与个人信息规范旨在“通过合理处理规则促进信息流通与利用”的目标相契合。基于此，危险层次化判断方案无意区分自行公开和法定公开的个人信息，只要信息处理行为未产生不当风险，即应被允许。这一规则不仅能为保障信息主体权益创造环境，为拓展公共利益保护空间提供支持，更能使我们免于陷入查明目的与用途违法性的困境。

危险层次化判断方案符合已公开个人信息作为责任规则的要求。从“卡梅框架”上看，财产规则适用于平等主体之间的自愿协商情形，而责任规则强调法益转移的“定价权”并非由当事人自行协商，而是由法律“买断”或“卖断”。在责任规则下，公权机关将实施更多的干预，而个人所拥有的也并非一项“全能权利”。针对已公开个人信息的合理处理行为，属于“知情同意”规则的排除情形，二者在适用上构成并列选择关系。此时法益转移的“定价权”由法定而非意定，信息处理的实际控制者系信息处理者而非信息主体，从而完全契合责任规则的内涵。即便相关规范基础提及已公开个人信息的不同类型，其也仅属提示性规定，不足以作为反证目的限制原则的正当性依据。当然，将个人信息规范定性为责任规则或将引发事后救济不利于保护信息主体的权益的质疑。〔35〕海量个人信息的汇交融合、分析处理是大语言模型习得推理能力达到顿悟时刻的关键因素。大语言模型对个人信息的处理具有不可预见性，对个人信息的深度挖掘、数据复用等现象容易引发信息主体对隐私风险的担忧，〔36〕危险层次化方案亦面临着忽略个人信息人格属性的指责。然而，该方案以危险控制为核心，它不仅赋予个人信息人格属性及事后救济的存在空间，更强调了事中的危险防范。换言之，在信息处理的全生命周期，任何一方主体均无法在信息收集之时即排除所有的潜在危险，只能控制信息收集之后、信息处理过程中可能产生的特定危险，并对不当造成的损害予以赔偿。〔37〕这种经由设计的个人信息保护机制已将个人信息保护理念嵌入大语言模型信息处理全生命周期之内。〔38〕倘若信息主体仍担忧其信息处理可能带来不利益，亦可充分行使以删除权为代表的工具性权利，将特定个人信息彻底脱离信息处理过程。这并非忽略个人信息人格属性，而是对个人信息财产属性和人格属性予以兼容的结论。更何况，信息处理者未违反合理处理规则并不代表其信息处理行为必然合法，在经由设计的个人信息保护机制

〔35〕 参见申卫星：《数据确权之辩》，载《比较法研究》2023年第3期，第6页。

〔36〕 See Christopher Kuner et al., *Expanding the Artificial Intelligence-data Protection Debate*, 8 International Data Privacy Law 289, 290 (2018).

〔37〕 See Maximilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-Based Approach, Principles, and Private Standards as Elements for Regulating Innovation*, Nomos Verlagsgesellschaft, 2018, p. 512.

〔38〕 See Ira S. Rubinstein, *Regulating Privacy by Design*. 26 Berkeley Technology Law Journal 1409, 1423－1424 (2011).

未通过个人信息保护影响评估与合规审计等的情况下亦将招致相应的法律责任。

危险层次化判断方案是纠正最小必要处理与合理处理规则关系的合理选择。信息处理行为非“合理”性之判断需要进行各方主体之间复杂的利益衡量，而非单方面地提出非“最小”性要求。司法实践中完全可能出现这样一种现象，即对甲而言，其原本不处理已公开个人信息才是损害最小的选择，但对甲、乙双方而言，只有甲处理已公开个人信息才是对乙损害最小的选择，且该种处理行为不会造成过多的损害，此时的甲非“最小”处理却属于整体上“合理”处理的范畴。作为比最小化使用更加宽松的合理处理，其在保护与利用的平衡之间天然地偏向于后者，而这恰恰是目的层次化判断方案所无法满足的。

（二）危险层次化判断的标准配置

危险层次化判断方案能以危险的程度差异有效关联已公开个人信息指向的不同部门法违法性，可在融贯性解释的基础上合理分配不同的危险判断标准，建立起科学的违法性界分路径。基于法益概念的跨部门法属性，个人信息必须与实体法益产生关联才具有相应的现实危险性，因此，不同程度的个人信息处理行为，其危险指向的均为信息主体人身和财产法益。毫无疑问，这种与实体法益关联性的强调，至少能在判断对象上保持侵害可判断性和清晰性，再辅之以特定的程度限定词及判断方法可避免危险的泛化判断。

基于危险的方法，民法规范中提及的“侵害重大利益”体现为“处理者对合法公开的个人信息的处理将会导致信息主体的个人权益难以或无法行使，或者个人权益被侵害、妨碍等重大的不利后果”〔39〕，包括无法行使信息处理的拒绝权等。换言之，非合理处理行为只要使得信息主体的实体法益更容易、更可能受到侵害，即奠定了民事违法性基础。“危险责任的基本思想在于‘不幸损害’的合理分配，乃基于分配正义的理念”〔40〕，系因危险来源者对危险的可控制性，并基于正义的要求令其分散损害赔偿。这种因非合理处理行为而产生的危险具有低度性和可控制性的基本特质。民事违法性所采取的危险升高标准，为非合理处理行为设定了进入惩罚判断的下限，与先民后刑的基本逻辑相适应。在是否对民事违法性指向的信息主体进行数量限制的问题上，一方面仅处理少量且特定个体信息的违法场景并不常见，且限制信息主体范围亦与危险的基本属性相违，因而不应对潜在的侵害主体范围进行限制，另一方面从主张权利救济的角度上观察，原告方只能是少量且特定的个体，这一点不存在疑问。在此情况下，对于不当处理大量个人信息所造成的危险，只能依据危险程度的差异进行民行刑治理的选择，而民法仅规制其中的低度危险行为。

基于危险的方法，非合理处理行为的民事违法性与行政违法性存在关联。《个人信息保护法》第 66 条对非合理处理行为的行政责任予以规定，强调“违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务”时即成立行政责任，这明显是低度危险的直接体现，并与行政法以秩序维护为导向的基本价值相吻合。倘若信息处理者的违法行为并未招致任何危险，亦不必处罚，否则与《行政处罚法》第 33 条第 1 款轻微违法行为不罚的思想相违背。这

〔39〕 程啸：《论公开的个人信息处理的法律规制》，载《中国法学》2022 年第 3 期，第 96 页。

〔40〕 王泽鉴：《侵权行为》（第 3 版），北京大学出版社 2016 年版，第 15 页。

意味着，二者在危险判断标准上相一致，具有民事违法性的非合理处理行为也可能同时具有行政违法性。之所以强调“可能”，源于二者权利/权力运行方式的不同，是否起诉/发现均会影响责任是否/如何承担，因而二者并非“绝对一体”的关系。当然，具体侵权责任的承担可基于损害填补的原则由被告对已公开个人信息的使用方式、数量、范围、侵权持续时间等因素决定具体类型，如停止侵害、赔礼道歉、赔偿损失等，而《个人信息保护法》第69条中“造成损害”的表述也不与危险升高标准相矛盾，因为危险指向公民实体法益这一背后层法益但损害指向个人信息权益这一前置的阻挡层法益。〔41〕行政责任的承担可由轻到重依据行政相对人的危险招致与纠正情况决定具体处罚类型，如警告、罚款、没收违法所得等。民事责任和行政责任承担方式上的显著差异，决定了即便民事违法性和行政违法性的判断标准相同，亦不会引发重复处罚的冲突，而是各自拥有独立的处罚价值。

基于危险的方法，刑法应规制的非合理处理行为必须具备危险的失控性，进而才能满足侵犯公民个人信息罪的刑事违法性。这种危险失控标准，为非合理处理行为设定了最终是否予以刑事处罚的上限。一方面，立法者之所以创设刑法规范规制已公开个人信息的非合理处理行为，源于其所拥有的典型危险性，并试图将该种危险源堵截于对信息主体的人身、财产法益等重要法益发生紧迫的危险状态之前，以防止造成不可挽回的局面，因而该罪应属于前置性、预防性的抽象危险犯形态的刑事立法。另一方面，将侵犯公民个人信息罪界定为抽象危险犯，并不意味着信息处理者的非合理处理行为一经实施即构成犯罪。即，抽象危险亦需进行危险判断，这在近年已得到司法实践的普遍认可。抽象危险犯以对不特定或多数重要法益产生危险为处罚条件。〔42〕作为比迫在眉睫的具体危险更缓和的危险，其在现实化的过程中既不能过于轻微（处罚前置），也不能过于严重（处罚延迟）。而危险失控意味着信息处理者已无法控制风险的扩散，致使大量重大法益处于危殆状态。此时，行为虽已超出初始违法阶段所产生的抽象危险，也尚未达到实害发生的迫在眉睫程度，但已实质拉近了损害发生的时空距离。这种介于轻微与严重之间的中间状态，具有拦截典型危险的刑法必要性，足以奠定其刑事可罚性。“从危险控制的角度判断抽象危险，并非要求行为人事后排除危险的发生，而是考察行为人在实施构成要件行为的过程中是否掌控了危险的不发生”〔43〕，其是经过时间和空间酝酿后对危险升高时点的危险进一步发展的结果。较之于徘徊在概率精确化（数量多≠概率高）和说理恣意性困境（达到或超过75%的说理不能〔44〕）之中的可能性说而言，具有严重发散性、外溢性等特征的危险失控标准能够树立起民事、行政不法与刑事不法的鲜明界限，更易于便捷且合理地认定应受刑事处罚的非合理处理行为。

---

〔41〕 个人信息权益是形式法益概念，强调规范违反性本身，其与公民的实体法益，包括人身和财产法益存在本质区别。对个人信息权益产生损害的行为，仅能对实体法益产生特定的危险，而这处于手段与目的的关系之中。如果采用阻挡层和背后层法益的结构表达，个人信息权益属于阻挡层法益，实体法益属于背后层法益。

〔42〕 参见张明楷：《抽象危险犯：识别、分类与判断》，载《政法论坛》2023年第1期，第75页。

〔43〕 于润芝：《抽象危险犯的解构：从法益关联和危险控制展开》，载《南大法学》2022年第3期，第123页。

〔44〕 在可能性说下，抽象危险被认为是具有造成实害结果发生的高度可能性的危险。参见韩德明：《风险刑法：理论语境和论证路线》，载《江海学刊》2018年第4期，第126页。所谓高度可能性即高度盖然性，通常认为超过75%的可能性即可，允许存在一定的不确定性。

针对利益衡量变动说，〔45〕实施违法、侵权或其他行为说〔46〕以及仿比例原则说〔47〕等解释方案而言，危险层次化判断方案无疑使得部门法违法性的层次化配置更清晰。具体而言，第一种解释方案直接将侵害“重大利益”限定于敏感个人信息的场景，造成了排除规则与单独同意规则之间的冲突；第二种方案仅指明了存在不同部门法的维度，却未对实质标准进行任何阐释；第三种方案看似进行了多重正当性的相互衡量，实则其每一个环节均流于空洞，究其根源，比例原则仅提供了形式审查框架，其实质内容需要另行填补。

需要注意的是，危险与安全在某些论者看来是一体两面的概念，进而可能认为危险层次化判断方案可转译为安全法益论，但这并不合理。例如，有论者认为“打击个人信息违法犯罪的目的，是要消除违法处理给信息主体人身、财产权利带来的风险因素，使之恢复到合法安全状态”〔48〕。分析该观点，安全强调的是将相关领域违法或犯罪的发生率控制在一定范围之内的秩序状态，因而安全和秩序具有等价性。〔49〕正如卢曼所言，“绝对的安全是无法达到的……作为风险的对立概念，安全在这个概念丛中是一个空的概念，就像健康概念在患病/健康的区别之中一样”〔50〕。因其高度的易变性特征，“风险不论是具体或抽象描述的事实状态，或者只是纯粹心理的恐惧感受等，皆不断被转译成简化的安全概念”〔51〕。该论者自己也认识到，安全是一种复合型利益和抽象性不利益，无法被计算损害，〔52〕因为不存在不重要的“安全”。既然如此，安全便不能作为界定非合理处理行为不同部门法违法性的标准，否则刑法与前置法在均沦为纯粹的行为法的同时，法法衔接的界限亦将消弭，导致实质非正义。与之不同的是，危险层次化判断方案中使用的危险概念，直接指向法益侵害的危险。只要特定法益的内涵清晰且危险（具体危险 VS 抽象危险）判断的框架科学，这种危险便既可判断“质”，也可判断“量”。

三、非合理处理行为违法性的危险层次化判断方法

非合理处理已公开个人信息违法性可分为前置违法性和刑事违法性，〔53〕前者以民事违法性为核心，兼顾公权机关介入处罚特定信息处理者的情形。在此基础上，应对不同信息处理环节中的不同部门法违法性判断确立科学的判断方法。

（一）前置违法性的危险升高标准判断

非合理处理行为的民事违法性判断适用危险升高标准，即判断信息处理者的行为是否使得法

〔45〕 参见宁园：《“个人信息已公开”作为合法处理事由的法理基础和规则适用》，载《环球法律评论》2022 年第 2 期，第 83 页。

〔46〕 参见刘晓春：《已公开个人信息保护和利用的规则建构》，载《环球法律评论》2022 年第 2 期，第 63－64 页。

〔47〕 该观点的具体判断步骤如下：一是将信息主体的个人信息利益与信息处理者的合法利益、社会公共利益进行权衡比较，二是判断收集和利用方式是否正当，三是判断进一步处理的公开的个人信息与源信息在内容、结构上是否相符。参见王海洋、郭春镇：《公开的个人信息的认定与处理规则》，载《苏州大学学报（法学版）》2021 年第 4 期，第 75 页。

〔48〕 贺彤：《安全作为个人信息保护的法益》，载《财经法学》2023 年第 3 期，第 114 页。

〔49〕 参见刘艳红：《中国刑法的发展方向：安全刑法抑或自由刑法》，载《政法论坛》2023 年第 2 期，第 64 页。

〔50〕〔德〕尼克拉斯·卢曼：《风险社会学》，孙一洲译，广西人民出版社 2020 年版，第 38－39 页。

〔51〕 古承宗：《风险社会与现代刑法的象征性》，载《科技法学评论》2013 年第 1 期，第 131 页。

〔52〕 参见贺彤：《安全作为个人信息保护的法益》，载《财经法学》2023 年第 3 期，第 117－120 页。

〔53〕 参见宗绍昊：《网络平台拒不履行数据质量保证义务的刑事违法性判断》，载《法学论坛》2026 年第 2 期，第 172 页。

益更容易、更可能受到侵害。事实上，信息处理过程兼具机遇与挑战，在技术双刃剑属性的加持下，很容易通过不同概念之间的转译或关联，令某一信息处理行为较之于不处理信息的行为升高了危险。换言之，完全否定信息处理行为才可能实现所谓的安全状态，只要存在信息处理行为即增强了危险。正因如此，非合理处理行为的民事违法性判断不适宜正向证成，而应当注重反向排除，即确认没有升高危险的信息处理行为并据此排除侵权行为的成立。危险升高的反面是危险不变或危险降低，前者指向容许危险理论，后者指向危险降低理论。

容许危险理论强调的是，一个不会以意义重大的方式威胁已公开个人信息主体实体法益的举止行为，不值得处罚。〔54〕在非合理处理行为场景下，容许危险理论指向的是“信息中介”行为。“信息中介”是存在于上游 A 信息处理者与下游 B 信息处理者之间的角色，其虽实施了某种信息处理行为，但该种行为没有产生有别于现有已公开个人信息的实质价值，亦未通过对多方素材的整合加工而显著便利不法行为或不利益后果的实现，属于规范上危险不变的情形。所谓的信息深度加工，应当强调信息来源的多样性（众多不同类型信息渠道的整合）、信息获取的难度（一般主体通常无法轻易获得，可能需要技术等手段辅助）、信息排列的可用性（与实体法益相关联的列表呈现）等的综合判断。这一特征同步体现于非法公开的个人信息和合法公开的个人信息场景之中，只不过前一情形增加了非法公开主体这一新的可罚对象。例如，在梁某冰与北京汇法正信科技有限公司网络侵权责任纠纷上诉案中，梁某冰主张汇法正信公司在搜索结果及网页中呈现的梁某冰姓名、性别以及相关民事纠纷等，属于其个人信息和隐私。根据汇法正信公司陈述，其信息来源于北京法院审判信息网，梁某冰提交的公证书中显示“中国裁判文书网”也登载了涉案文书。梁某冰对上述网站登载涉案文书予以认可，但表示汇法正信公司网站不能将其进行商业应用。〔55〕分析本案，梁某冰的相关涉案信息属于个人信息而非隐私，更进一步讲，属于个人信息中的已公开个人信息，一般公民均可在特定网站上自由浏览、下载相关内容。在此情况下，汇法正信公司爬取相关信息并用于商业化活动的行为不符合容许危险理论中对信息来源的多样性、信息获取的难度等的要求，并未升高对公民人身和财产法益的危险。遵此逻辑，如果高知名度的信息平台主动将分散的已公开个人信息进行整合并在淘宝等平台出售，即便其符合信息排列的可用性标准，在不具备信息来源的多样性、信息获取的难度等的情况下亦属于容许危险的情形。

危险降低理论，即当具备结果发生可能性的信息处理行为降低了先在的结果危险（即纯正的危险降低）时，可否定其危险性。信息处理行为的危险降低需付诸较之前一阶段的信息处理行为更严格的技术治理与管理治理的协同。其中，技术治理是降低公民实体法益侵害可能性的核心手段，管理治理则为技术治理提供方案选择和资源保障。所谓更严格的治理协同，比较的对象应是已公开个人信息获取时和处理时的保护措施。例如，行为人在汇聚、整合海量已公开个人信息之后，为其设定访问控制、储存加密等，并仅服务于自己的正常商业运作，显然危险面较获取时更窄；又如，行为人在获取已公开个人信息并提供给第三人使用的过程中，借助隐私计算技术，在

〔54〕 参见〔德〕克劳斯·罗克辛：《德国刑法学总论（第 1 卷）·犯罪原理的基础构造》，王世洲译，法律出版社 2005 年版，第 249 页。

〔55〕 参见北京市第四中级人民法院（2021）京 04 民终 71 号民事判决书。

确保信息本身不对外泄露的情况下满足对方合理需求，实现信息的安全利用等。〔56〕这些均属于危险降低的情形。

在当事人明确拒绝的情况下，信息处理者的行为是否具备民事违法性尚需进一步判断。鉴于《个人信息保护法》将合理处理作为信息主体“知情同意”的排除规则，为协调《民法典》与作为特殊法的《个人信息保护法》的关系，应将“明确拒绝”解释为“侵害重大利益”的子内容，即前者是后者的必要不充分条件。这一解释结论有利于实现非合理处理行为违法性的层次化，如果将二者理解为并列关系，容易造成不同部门法违法性之间的矛盾。在信息主体“明确拒绝”的情况下仍处理已公开个人信息的行为，我国现有规范至多仅明确肯定了其民事违法性，并不意味着其具备行政违法性或刑事违法性。换言之，“明确拒绝”不具备区分不同部门法违法性的功能。信息主体明确拒绝的信息处理并非当然地属于值得禁止的危险信息处理，即便此种情形达到了相关司法解释所规定的数量标准，其仍存在实质出罪的可能性。在此基础上，司法实践中不能一出现“明确拒绝”即认定非合理处理行为的民事违法性。例如，在吴某与某公司网络侵权责任纠纷案中，原告的抖音账号主要发布国风类短视频，账号说明处标注有“没有授权任何换脸”。原告的摄影师于 2021 年 10 月 14 日在自己的抖音账号发布某“甜度超标”视频，并@原告注册的抖音账号。涉案软件中的“特效”板块中有“古装”标签，有若干模板视频供用户使用，其中包括“燕子风筝少女”换脸模板视频。法院认定，模板视频系将原告出镜的“甜度超标”视频中的原告面部替换成他人面部，通过人工智能深度合成技术生成。〔57〕本案“没有授权任何换脸”即为当事人“明确拒绝”的表达，但尚需以危险升高标准判断被告行为的民事违法性。在视频换脸市场起步阶段，一些不规范乃至违法犯罪的换脸行为频发，涉案视频换脸软件可被任何人用于任何用途，其明显具备助推危险发展的效果。在此基础上，本案被告的信息处理行为才具备相应的民事违法性。

需要注意的是，基于相同的逻辑，倘若具有民事违法性的非合理处理行为并非发生在平等私主体之间，而是发生在地位不对称的双方主体之间，公权机关亦可对信息处理者予以不同程度的行政处罚，具体处罚类型的选择在形式上可依据事前确定的行政裁量基准，在实质上需就危险类型、危险场景、技术性合规状况、既往违法行为发生频率等予以综合确定。同时，危险层次化判断方案不仅适用于非合理处理行为的违法性判断问题，也同样适用于信息处理行为是否合理的判断问题。只要不具备民事、行政违法性的信息处理行为便属于《个人信息保护法》所认可的合理处理行为。这是基于目的层次化判断方案的内在弊端而作出的科学判断。

（二）刑事违法性的危险失控标准判断

信息处理者的非合理处理行为是否造成了失控的危险，决定着其行为是否可构成侵犯公民个人信息罪。在此过程中，形式标准能够便捷地起到初次筛选和快速出罪作用，而实质标准则可进一步验证行为可罚性以维持刑法谦抑性，二者均不可或缺。同时，不同阶段的处理行为应赋予不同程度的危险要求，以契合其距离法益的远近特征。

〔56〕 参见刘艳红：《人工智能技术在智慧法院建设中实践运用与前景展望》，载《比较法研究》2022 年第 1 期，第 4 页。

〔57〕 参见北京互联网法院（2023）京 0491 民初 3821 号民事判决书。

就形式标准而言，司法解释规定的量化指标是其实体内容。理论上有方案将信息处理者是否违反“国家有关规定”作为非合理处理行为是否应受刑事处罚的形式标准。〔58〕然而，应受刑事处罚的非合理处理行为一定是违反“国家有关规定”的行为，不必单独审查。即便认为，违反“国家有关规定”的行为可能是前置法上的非合理处理行为而非刑法上的非合理处理行为，但二者的规范基础同一，且信息处理行为究竟是否“合理”，各部门法均存在认定上的模糊性。与之相对的是，以信息处理数量为代表的量化指标虽然存在不对应性、证据忽略等诸多弊端，但其弊端根源于单一性的“有无”评价，而非先天的功能性缺失，即以形式替代实质而作出错误该当的行为。同时，量化指标系司法审查的起点，存在适用上的简便性，对于提高司法效率具有显著作用，不能将其放弃。因此，量化指标应仅在第一性形式审查上起作用。值得注意的是，曾受过行政或刑事处罚又实施非合理处理行为的情形，仅能影响信息处理者的预防必要性程度高低，无法作用于法益侵害性的判断。

就实质标准而言，其要求信息处理者的处理行为合因果地引发了失控的危险时，才能构成侵犯公民个人信息罪。“刑法管控这种风险，必须出于行为能够直接导致严重危害后果的可能性这一考量。”〔59〕因此，非合理处理行为的刑事违法性指向的危险失控标准时刻关联着公民的实体法益，并以信息处理行为是否存在针对人身、财产法益的严重危害后果可能性作为核心判断依据。在此基础上，危险失控标准着重强调的是信息处理危险之于实体法益的因果性和程度性。毫无疑问，针对已公开个人信息不同处理阶段的行为显著影响着因果性和程度性的判断，因而需要对信息处理者的获取、出售和提供等不同阶段的行为进行分类讨论。

较之于出售和提供行为而言，仅获取已公开个人信息的行为因缺乏明显的因果性、现实的扩散性，其结果危险性显著低于前者。在立法者对获取、出售和提供等不同阶段的行为配置了同一法定刑的情况下，必须有其他要素补足获取已公开个人信息行为的结果危险性（二者在有责性上并无差别），才能最终达到危险失控的程度进而科处刑罚。在结果无价值论立场内部，只有目的犯中的目的以及未遂犯中的既遂故意对于结果危险性有特殊的价值，应当被例外地承认为主观违法要素。〔60〕而与信息处理者获取已公开个人信息行为的结果危险性相关联的只有目的犯中的目的。事实上，“由于不存在现实的风险外溢行为，个人信息犯罪预备行为的不法属性只能来源于主观违法要素，即后续犯罪的意图”〔61〕。因此，将侵犯公民个人信息罪的行为类型涵盖已公开个人信息获取行为的理由在于，行为人的信息处理行为“明显存在着与相应犯罪的特定联系”〔62〕。后续犯罪的意图这一不成文的构成要件要素，使对已公开个人信息的处理行为呈现出以下特征：其目标在于向外（危险外溢）侵害公民的人身或财产法益，且整个信息传播过程由行为人决定并支配信息的（拟）流向。在第三人具备多数性的基础上，由于信息的第一次传播已面向多数主体，后续主体再次传播或直接使用等的危险已无法控制。同时，为了平衡获取、出售和提供行为

〔58〕 参见远桂宝、商银涛、段厚省：《擅自处理已公开个人信息的刑法规制》，载《中国检察官》2024年第2期，第24页。

〔59〕 陈思桐：《经济刑法中抽象危险犯的处罚限度》，载《财经法学》2022年第5期，第187页。

〔60〕 参见刘艳红：《实质犯罪论》（第2版），中国人民大学出版社2022年版，第141页。

〔61〕 赵炳昊：《数字经济时代个人信息犯罪的穿透式治理》，载《中国刑事法杂志》2025年第4期，第36页。

〔62〕〔德〕乌尔里希·齐白：《全球风险社会与信息社会中的刑法：二十一世纪刑法模式的转换》，周遵友等译，中国法制出版社2012年版，第217页。

之间的危险性差距，在危险已外溢并现实化的情况下，不应要求出售和提供行为所涉及的多数第三人（少数第三人不符合危险外溢，特定与否在所不问）可能对信息主体实施犯罪行为，而只需强调其可能存在的、针对人身或财产法益的不利益行为即可，由此建立起与公民实体法益之间的因果性。至于牟利目的，则因与客观危险的增加无关联并不构成侵犯公民个人信息罪的必要条件。这一结论已被司法实践所认可。例如，在杨某甲侵犯公民个人信息案中，检察院认为，行为人购买个人信息后并未用于非法用途而仅限于推销公司的正常业务，无法对信息主体产生影响人身、财产安全等的不利后果。〔63〕这意味着，如果信息处理者基于合法经营的目的而获取已公开个人信息，其不具备向刑事犯罪发展的增量条件，不必考虑其是否构成犯罪。这种情形有别于司法解释中对于“为合法经营活动而非法购买、收受”行为的可罚性规定，因为其要么须具备获利性而不单单停留在获取阶段，要么因获取行为的非法性而不属于信息处理者的范畴。〔64〕

要言之，危险失控标准意味着，信息处理者基于后续犯罪的意图而获取已公开个人信息，或者将获取的已公开个人信息提供给可能对信息主体实施不利益行为的多数第三人。通过主观意图的加入、实际扩散行为的有无、（潜在）行为对象数量的评价和预期利益损害的类型等因素的结合，将危险失控标准指向的因果性、程度性要求再次予以清晰的具象化，能够为司法实践提供具有可操作性的非合理处理行为刑事违法性认定指南，最终实现侵犯公民个人信息罪不同行为类型的罪刑均衡。例如，在罗某期、谢某健、罗某年侵犯公民个人信息案中，罗某期等人通过企查查网站等途径收集、梳理诸如公司法人代表通信信息等已公开个人信息并据此对信息主体实施诈骗。法院认为，其行为已经构成侵犯公民个人信息罪。〔65〕分析本案，罗某期等人作为信息处理者，其基于实施后续诈骗行为的意图而实施信息处理行为，在达到司法解释规定的形式标准的条件下为被害人上当受骗（超越不利益行为的不法行为）提供了资料上的信任基础，对合因果地指向的信息主体人身和财产法益已然产生了失控的危险，达到了情节严重的程度，将其作为犯罪处理是正确的。

四、结　语

数字时代，已公开个人信息的规范目的不仅在于保护，更在于利用。正因如此，对信息处理行为是否具备违法性以及何种违法性的判断需要尤其慎重。既有观点一边倒地偏向目的与用途的限制，这一目的层次化判断路径恰恰与合理处理规则的价值相左并产生若干司法实践操作弊端，无法完成非合理处理行为违法性的层次化判断目标。在此基础上，有效平衡已公开个人信息保护和利用的危险层次化判断方案应运而生，并可依据危险的程度差异建立起民事、行政和刑事违法性的有序配置格局。当然，非合理处理行为的违法性判断问题不仅限于已公开个人信息的场合，诸如媒体为公共利益实施新闻报道、舆论监督等行为也会涉及不同部门法违法性的界定，本文的

〔63〕 参见浙江省绍兴市柯桥区人民检察院绍柯检公刑不诉〔2018〕158 号不起诉决定书。

〔64〕 这一情形实际上指的是，行为人通过非法渠道批量购得个人信息。这些个人信息之中有可能包括一部分已公开个人信息，但此处的信息处理者并非行为人，而是上游卖方。对上游卖方信息处理行为的刑事可罚性判断，仍适用本文的标准。

〔65〕 参见广西壮族自治区宾阳县人民法院（2020）桂 0126 刑初 104 号刑事判决书。

研究成果对其亦具有一定的借鉴价值。希冀未来在更加健全的合理处理机制的辅助下，信息主体能够获得更加个性化、低度危险的各项服务，“公私领域的各个社会主体协力实现国家和社会治理目标”〔66〕。

Abstract：The unreasonable processing of publicly available personal information may involve civil, administrative, or criminal illegality, though the distinctions among these types remain substantially blurred. Purpose based and risk based hierarchical assessments represent two fundamental models for distinguishing such illegality. The existing purpose-based approach leads to outcomes where identifying the purpose of disclosure is either factually ineffective or practically impossible. This approach also incurs excessive costs in transferring or monitoring purpose-driven data flows, contradicts conclusions derived from historical interpretation, and lacks the function of differentiating degrees of illegality. Assessing the illegality of unreasonable processing requires balancing the diverse values and normative attributes of publicly available personal information. The risk-based hierarchical framework is better suited for this task. It enables the configuration of distinct illegality criteria based on varying degrees of danger. Here, preceding illegality refers to civil and administrative violations. It corresponds to the elevated risk standard, representing a low level of danger. This standard excludes information processing activities that constitute permissible risk, such as those by “information intermediaries”, or activities that achieve risk reduction through stricter integrated technical and regulatory governance. Criminal illegality points to the uncontrollable risk standard, signifying a high level of danger. Its application must follow a basic path where formal criteria precede substantive assessment. The core of this analysis is to determine whether the information processor obtained publicly available information with intent to engage in subsequent criminal acts. Alternatively, it examines whether the processor provided the obtained information to multiple third parties likely to inflict harm on the data subject.

Key Words：publicly disclosed personal information, unreasonable processing, judgment of illegality, risk-based approach, integration of civil, administrative, and criminal laws

（责任编辑：简　爱）

〔66〕 周佑勇：《中国行政基本法典的精神气质》，载《政法论坛》2022年第3期，第76页。