Open Journal of Legal Science 法学, 2025, 13(8), 1890-1896
Published Online August 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.138262

Hans汉斯

民法典实施背景下个人非必要信息收集的规制路径

叶诗韵

中国政法大学刑事司法学院，北京

收稿日期：2025年7月17日；录用日期：2025年7月30日；发布日期：2025年8月27日

摘　要

数字经济化背景下，平台通过格式条款的概括性授权，超出比例原则收集用户非必要信息，而现有规制路径面临概念界定模糊、格式条款效力判定困难、裁判标准不一的问题，致使司法实践难以有效遏制侵权行为。非必要信息收集的规制路径，不能局限于被动化的诉讼救济手段，而应当以《民法典》《个人信息保护法》的必要性要求和告知同意规则为基石，构建格式条款“同意”的实质化审查标准，确立平台信息交互的多重授权机制，细化信息风险披露的内容，实现从被动救济到主动防护的治理转型。

关键词

个人非必要信息，个人信息保护，守门人制度

The Regulatory Path of Personal Non-Essential Information Collection in the Context of Civil Code Implementation

Shiyun Ye

School of Criminal Justice, China University of Political Science and Law, Beijing

Received: Jul. 17th, 2025; accepted: Jul. 30th, 2025; published: Aug. 27th, 2025

Abstract

Under the background of digital economy, platforms collect users' non-essential information through general authorization terms and the principle of over-authorization. However, existing regulatory frameworks face challenges such as ambiguous conceptual definitions, difficulty in determining the validity of format terms, and inconsistent adjudication standards. This makes it difficult to effectively

文章引用: 叶诗韵. 民法典实施背景下个人非必要信息收集的规制路径[J]. 法学, 2025, 13(8): 1890-1896.
DOI: 10.12677/ojls.2025.138262

curb the infringement in judicial practice. The regulatory framework for the collection of non-essential information should not be limited to passive litigation remedies, instead, should be based on the necessity requirements and notification of consent rules outlined in the Civil Code and the Personal Information Protection Law. This framework should construct substantive review standards for the "consent" in standard form contracts, establish a multi-layered authorization mechanism for information exchange on platforms, and refine the content of information risk disclosures. These measurements aim to facilitate a shift from passive to active consent. Additionally, a multi-layered authorization mechanism for information exchange on platforms has been established, and the content of information risk disclosure has been refined, thereby achieving a governance transformation from passive relief to proactive protection.

Keywords

Personal Non-Essential Information, Personal Information Protection, Gatekeeper System

1. 引言

在全面数字化浪潮的深刻影响下，移动应用程序(APP)的广泛普及与深度渗透，给我国目前的个人信息保护网带来了挑战：相当一部分 APP 运营主体在收集用户信息时，不能遵守“必要性”原则，过度收集与处理用户数据，明显违背比例原则的内在要求。虽然我国《数据安全法》《个人信息保护法》相继出台，个人信息保护法律体系已初具规模，但现行框架仍有待完善：在理论层面，核心概念如“个人信息”“非必要个人信息”的内涵与外延不甚明晰，导致法律适用的基础存在模糊地带；在司法实践层面，对 APP 用户协议中格式条款效力的司法判定标准尚未统一，数据处理者与数据主体之间的权利义务边界缺乏清晰界定。这些实践层面的困境，直接导致了个人信息侵权诉讼裁判标准不一的难题。

诚然，通过诉讼寻求司法救济为个人信息受侵害的主体提供了重要的维权渠道。然而，这种传统的事后救济模式本身难以克服其固有的滞后性与被动性缺陷。因此，亟待构建科学、高效且兼具预防性与救济性的个人信息保护路径。如何构建科学、高效的个人信息保护路径，不应仅仅依赖于个案裁判的公正性，更需以《民法典》《个人信息保护法》为依托，构建救济路径的前端预防体系，实现从被动救济到主动防护的治理转型。

2. 个人非必要信息的内涵和外延

概念是认识事物性质的基础和前提，也是解决法律问题所必需的工具。个人信息与个人非必要信息二者构成包含与被包含的逻辑关系：前者构成后者的概念母集。所以，对于“个人非必要信息”的解读应当以“个人信息”的概念为基础。“个人信息”作为属概念，其法定定义强调“以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息”的核心特征；而“个人非必要信息”作为一种概念，其本质应被理解为：超出特定服务场景功能实现所必需范围，且与数据处理目的不存在实质关联性的个人信息子集。

(一) 个人信息的内涵和外延

根据《个人信息保护法》的界定，个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。

首先，个人信息和个人数据的概念需要进一步界定。“可识别性”是个人信息的本质特点，而不具有直接识别属性的数据则称为个人数据。因此，个人信息强调信息的个性化特征，个人数据则是在无限丰富的数据中运用归纳思维，抽象出一般性的规律。除此之外，个人信息强调实质内容，而个人数据侧重形式载体，两者是内容与形式的关系[1]。

其次，个人信息与个人隐私并非同一概念。个人信息与个人隐私存在交叉关系：部分个人隐私以个人信息的形式表现出来，如加密照片、录音等；另外一部分隐私内容如账户密码等则属于个人数据与个人隐私交叉的范畴。除此之外，个人信息具有客观性，而对个人隐私的判断则具有主观性，这种主观性导致以客观性为保护基准的刑法难以对个人隐私展开保护[2]。从概念的开放性来看，个人信息相对开放，注重其识别性，强调信息的自由流动；而个人隐私相对封闭，注重保密性，限制其自由流动。总而言之，个人信息相比个人隐私而言范围更广，个人隐私比个人信息敏感度强。

(二) 个人非必要信息的内涵和外延

当前收集个人信息的必要性取决于是否存在特定、明确、合法的目的，且这个目的可以是商业目的、实现合同所必需、公共利益、履行法定义务。由此可见，非必要性是一个综合企业商业功能或政府管理目的和用户使用目的的相对定义。

出现这样的相对定义，主要原因有二。第一，现代网络社会中，信息处理主体已超越传统自然人、法人与非法人组织的范畴；与此同时，信息处理者与信息主体在技术资源、经济地位及信息掌控层面存在显著权力失衡[3]。第二，个人信息承载着多种需要协调的利益[4]。既有自然人对其个人信息的支配，以免人格尊严及人身财产权益受到侵害或遭受损失的需要；亦涉及营利法人基于营业自由通过信息处理获取数据价值的诉求。若片面强调信息主体的绝对对世权而漠视企业的合理需求，或为追求经营效率与行政便利过度压缩信息主体的支配权，均将阻碍个人信息的有效保护与经济社会可持续发展。

可见，非必要信息属于动态概念，同一种信息在不同的场合下会在必要和非必要之间来回切换，所以需要根据适用的不同场域展开具体分析判断。

3. 个人非必要信息收集的规制问题

个人相对于平台，无论是在信息占有还是技术掌握上的弱势地位都导致其权利根基不牢，难以在第一时间察觉其数字权利是否被侵害[5]。个人为获得平台提供的必要服务让渡必要信息的部分权利无可厚非，但对于非必要信息而言，个人显然享有拒绝让渡的权利，但事实却并非如此。

(一) 个人非必要信息收集的规制现状

虽然我国的个人信息保护体系逐步完善，多部法律、规范性文件对个人信息收集、处理进行了相应规制：如《网络安全法》第 41 条中规定“网络运营者不得收集与其提供的服务无关的个人信息”，《信息安全技术个人信息安全规范》中则明确规定了企业收集个人信息的最小必要。但分散式立法保护使得信息主体权利不完整、信息处理者法律责任不到位；在救济路径方面，刑法的被动保护不过是面对危害后果的应急反应[6]，个人信息民法保护相对贫乏，民事侵权的司法救济偏向事后补偿，但就信息保护而言，对于已经泄露或被处理的信息而言，未免无效。这种救济路径的缺失，也在司法实践中暴露出相应的问题：相当一部分用户在注册社交软件账户时，即使明确阅读隐私协议中对于信息收集相关的条款，也会迫于获取服务的目的，放弃争夺非必要信息的权属。

在现存救济路径力所不逮的情况，部分学者从宏观角度思考非必要信息保护路径的框架，认为可以通过对格式条款的效力研究分析，在前置环节维护用户的个人信息权益；另一部分学者则认为在保护用户的个人信息时，应当从法经济学角度考量企业效益发展、资源配置最优化，允许适当扩大信息收集、处理的范围。是固守用户权益的边界，还是允许企业延伸信息收集的范围，两种观点的博弈将直接导向

实践中用户个人权益保护的问题。

(二) 个人非必要信息收集的实践规制难点

个人非必要信息的收集问题是用户与平台之间诉讼纠纷的根源，格式条款概括性授权、平台关联企业信息交互、平台信息泄露等问题直接侵害用户的个人信息保护权益。

在司法实践的具体操作中，由于个人非必要信息性质复杂、界定模糊，法官的价值判断与自由心证，对判决结果具有较大的影响，难以切实通过司法实现对用户个人信息保护权益的救济。这种救济保障的不足主要体现在以下两个方面：个人信息收集格式条款的强制同意、信息关联授权的隐蔽操作。

1) 个人信息收集格式条款的强制同意

平台依据法律授予的“规则制定权”，制定相应的平台自治规则和协议，个人信息收集格式条款属于平台协议的下位概念，所以由平台掌握主动权：通常以处理者提供格式条款、用户同意的形式签订。

然而，实践中平台利用格式条款迫使用户捆绑同意非必要信息收集的情况颇为普遍[7]。网络平台通过“概括性同意”的策略，大量获取用户信息。APP 用户“知情”的门槛被设置为勾选“同意”，一旦用户不“同意”，用户将放弃所有的使用权限，此时设置的“不同意”选项更类似于形式化的选择，用户只能被迫捆绑接受非必要信息的收集。纵然有学者认为，对于“必要”的认定，不应当局限于传统观念中实现具体业务功能的目的，而应当扩展为“在其个人信息处理的综合影响正面，且给信息主体造成的损害有限的情况下，可以在合理的必要范围内处理非敏感的和敏感度低的个人信息”[8]。但实际上，何为“合理”、何为“损害有限”，这些问题都难以得到确切的答案，贸然扩大必要性的范畴显然不当，网络平台在当前不能也不应当收集用户的非必要信息。

用户遭到了权益损害，与此同时救济路径也并不乐观。我国当前对于格式条款效力的审查较为被动，一方面，出于对平台自治的尊重和遵循“不告不理”原则，法院不会主动审查平台协议规则，通常只在当事人提出或需要适用具体平台规则时，才进行有关审查[9]。另一方面，在司法审查的过程中，法院倾向于仅判定格式条款形式层面的提醒义务，却不能注意到格式条款当中捆绑同意的困局，并未实质化对用户意思表示自愿性的审查(见表 1)。

Table 1. Case analysis of the ownership definition of personal information
表 1. 个人信息的权属界定的案例分析

议题	争议焦点	典型案例	案件概述	裁判要旨
个人信息的权属界定	格式条款规定的利用主体	王某与某计算机公司个人信息保护纠纷 [1]	王某 2019 年 4 月首次登录某 APP 时，授权其获取微信好友关系。而后卸载重新下载安装时，王某拒绝了 APP 关于公开地区、性别和微信好友等信息的要求，未再授权 APP 使用其微信好友关系，但该 APP 仍然显示其微信好友浏览信息。	该 APP 收集、使用王某“地区、性别”信息，同时又允许用户随意更改和填写该信息，其收集处理该信息不符合必要性原则。在王某重新下载安装且未予授权的情况下，继续使用其微信好友关系不符合正当性要求。

2) 信息关联授权的隐蔽操作

平台未经授权过度收集、擅自分享给第三方是个人信息泄露的重要源头，也是用户最为关注的焦点问题。相当一部分互联网企业在收集用户信息后，并未在后台进行信息脱敏处理，而是直接将收集的用户个人信息全部移转给关联公司。关联企业，是指与其他企业之间存在直接或间接控制关系或重大影响

[1]参见广东法院网：《广东法院个人信息保护典型案例》，载 https://www.gdcourts.gov.cn/gsxx/quanweifabu/anlihuicui/content/mpost_1388509.html，最后访问日期：7 月 27 日。

关系的企业。关联企业在法律上可表现为由控制公司和从属公司构成，如腾讯与微信读书之间的关系便可以概括为关联关系。当作为运营商的一方收集用户个人信息后，具有关联关系的公司在一定程度上会获得部分“共享资源”——企业内部共通的用户信息。随之而来的是用户与企业之间、企业与企业之间的信息授权问题。(见表 2)

Table 2. Typological analysis of case studies on information use and associated authorization
表 2. 信息使用关联授权的案例类型化分析

议题	争议焦点	典型案例	案件概述	裁判要旨
信息使用的关联授权	抓取数据使用权限	淘宝(中国)有限公司诉安徽美景信息科技有限公司不正当竞争[2]	“生意参谋”为淘宝旗下平台。美景公司系“咕咕互助平台”软件、“咕咕生意参谋众筹”网站的开发商与运营商。美景公司在“咕咕生意参谋众筹”网站上推广“咕咕互助平台”软件，引导已订购淘宝公司“生意参谋”产品的淘宝用户下载“咕咕互助平台”客户端，通过该软件相互分享、共用子账户。	网络大数据产品不同于原始网络数据，其提供的数据内容虽然同样源于网络用户信息，具有用户的明显偏好，但经过网络运营者大量的智力劳动成果投入，经过深度开发与系统整合，最终呈现给消费者的数据内容，已独立于网络用户信息、原始网络数据之外，是与网络用户信息、原始网络数据无直接对应关系的衍生数据。网络运营者对于其开发的大数据产品，应当享有自己独立的财产性权益。
		HIQ 诉 LinkedIn 不正当竞争纠纷[3]	hiQ Labs 就雇员职业发展角度，为雇主提供基于数据的咨询服务；LinkedIn 运营全球最大的职场社交网络。原告服务依赖于对被告数据的抓取。被告对自身网站爬虫协议有严格限制，仅限特定主体抓取。被告允许用户采取灵活的隐私设置，亦采取爬虫识别系统、黑名单等多种手段限制数据爬取。	要求 hiQ 向 LinkedIn 赔偿 50 万美元，并在法律允许的最大范围内通过了一项永久禁令，包括禁止：在未经同意下直接或间接通过自动化方式访问或复制数据，根据从领英获取数据而产生的开发、使用、销售等行为，永久删除所拥有、保管和控制的领英会员资料数据，等共计六项禁止行为。

过往学界对于信息二次处理的探究主要侧重于刑法层面的规制：对于已经公开的公民个人信息如果再次进行处理是否涉及侵犯公民个人信息罪[10]。与此同时，《民法典》第 1046 条则为上述信息处理者提供了豁免路径：行为人在“合理处理”已公开信息的前提下不承担民事责任。由此类推，对于非必要信息的收集与处理也必须围绕“合理处理”展开。那么需要面对的两个问题就是：非必要信息能不能转二次授权；非必要信息的二次处理如何才能控制在合理范围之内。但我国当前并不存在较为具象的规制路径，而这正是探索用户非必要信息规制路径的关键。

4. 民法典实施背景下个人非必要信息收集的规制路径

针对非必要信息收集的规制，现行探索已经证明被动式诉讼救济的局限性。一案一议的个案处理，并不能作为处理该类案件的指导。规制路径应当回归《民法典》与《个人信息保护法》确立的必要性原则及告知同意规则，推动治理模式由被动的事后救济向主动的事前防护转变。

[2](2017)浙 8601 民初 4034 号判决书。
[3]HiQ Labs, Inc. v. LinkedIn Corp,938 F.3d 985 (9th Cir. 2019)。该案始于 2017 年，于 2019 年 9 月 9 日由美国联邦第九巡回法院作出上诉判决：维持加州北区联邦法院就 hiQ Labs 诉 LinkedIn 案颁布的诉中禁令。最高院后来基于 Van Buren v. United States 案的判决结果，就 CFAA (the Computer Fraud and Abuse Act)的未经授权的争议焦点，撤销了上诉法院的判决，发回重审。2022 年 4 月 18 日，再审支持一审、二审判决。

(一) 格式条款的“同意”的实质化

个人信息收集格式条款的告知事项在实质意义上，构成了处理者处理行为的正当性基础，是用户作出真正知情同意的必要前提。为了落实《个人信息保护法》第 14 条、确保用户“同意”的实质化，而非流于形式，必须在以下两个关键维度进行强化：

首先，格式条款告知内容的具体化。《个人信息保护法》要求告知事项需“以显著方式、清晰易懂的语言真实、准确、完整地向个人告知”，可见这是格式条款形式合规的起点。个人信息处理者通过制定公开的处理规则告知部分事项时，不仅需要“公开、便于查阅和保存”，更应与具体场景中的即时告知形成有效衔接，避免用户因规则复杂而无法实际知悉。

其次，在对用户“同意”的实质化审查中，司法机关应超越形式审查，增加用户自愿选择权的考量。当前用户基于获取服务的需求，被迫让渡自身的信息权益，但用户对于非必要信息应当享有具体、明确且自由的选择权。在审查的过程中，司法机关应当突破传统视角下对格式条款形式的表面审查，转向对用户是否自愿“同意”的审查：用户拒绝非必要信息收集、处理后，是否能无障碍地获得服务，用户是否因担心服务受限而被迫“同意”，处理者是否利用其市场优势地位变相剥夺了用户的选择自由？通过对用户选择权实际行使空间和自由度的审查，确保用户意思表示真实无瑕疵，实现“同意实质化”。

此外，还应当对格式条款中的“同意”进行多层级设置[11]，为已经公开的信息设置例外。对格式条款的实质化审查，是为了实现对用户个人信息权益的保护，但不应机械地将第 27 条所规定的“明确拒绝”和“重新同意”的机制理解为信息主体可任意限制或拒绝[12]。如果个人非必要信息属于用户已经公开的信息范畴，此时则应当根据《民法典》的豁免条款，对该部分信息进行豁免处理。

(二) 关联企业信息披露的多重授权机制

针对平台未经授权过度收集、擅自分享给第三方的情况，当前法律学术界和行业公认的规则为“三重授权原则”。“三重授权原则”，包括“用户授权 + 平台方/公司授权 + 用户授权”，即平台直接收集、使用用户数据需获得用户授权，第三方开发者通过开放平台接口间接获得用户数据，不仅需获得平台方授权，还需要用户的二次授权，未经用户的二次授权，不得随意将收集的用户信息分享给第三方。但“三重授权原则”的适用当前尚缺乏一定的可操作性。首先，根据现行规定，我国法律并未明文规定二次授权，使得二次授权的法理基础存在欠缺；其次，从实际操作性而言，互联网领域内数据的海量性、数据处理的复杂性，使其很难细化到对用户个人一一授权，可操作性较差，对于企业而言会导致资源的过度浪费与不合理配置。

关联企业信息披露本质上是企业非理性决策的产物，企业外部的生存环境直接影响企业社会责任决策[13]，在数据竞争的背景下，企业通过处理收集的用户非必要信息，进行数据加工与产出从而实现生产资源的再塑造。既然“三重授权原则”的操作性仍然存在不足，不如从生产资源的再塑造入手——从脱敏信息的角度简化处理模式，如平台在对用户信息进行收集时，必须注重对个人敏感信息的保护，进行必要、安全化程度高的脱敏化处理，严格划分其使用权限，并建立完善的内外部监督机制。无论是用户自愿转移的个人信息，还是权利归属于平台的、经过处理之后的信息，平台必须严格按照用户授权进行，不得滥用用户为获得服务而被收集的信息，使用户的社会关系链条、个人必要与非必要信息泄露于外。

(三) 信息披露的风险防控细化

在个人事先授权的情况下，个人信息出于商业目的被收集、处理是合理且合法的。但由于个人信息具有隐私性，故而企业在个人信息处理中具有风险披露义务。

我国法律中明确规定了个人信息处理者的一般告知义务以及有关个人敏感信息的事先告知规则。但我国对个人信息处理者的义务规定主要倾向于宏观层面的规定，并没有针对信息的分级处理标准，也没有对信息处理者的资质进行更为细化的规定。在比较法的视野下，欧盟法和美国法在风险披露方面可以

提供一定的镜鉴。欧盟 GDPR 规定，在信息被处理之前，数据主体在必要时可以向“数据保护专员”请求帮助。我国法律虽然也存在“个人信息保护负责人”，但缺乏对相关人员资格、能力、具体业务范围的规定，不利于发挥其实质作用，相比之下，GDPR 的规定更加细致，我国也可以在现存“个人信息保护负责人”的背景下展开对从业资格的要求，设置信息保护门槛。美国加州法则通过要求企业提供对于消费者信息披露的类别和具体情况的清单，而我国当前只对广义上“处理信息”规定了处理者的记录义务，可以从更为细致的角度展开立法，进一步披露“信息处理”“信息类别”的目录，在规制违规信息处理的同时，何为“必要信息”、何为“非必要信息”也不言自明，非必要信息违规收集的问题也会得以遏制。

5. 结语

个人信息兼具人格利益与财产法益，涉及用户、APP 运营商、第三方，对互联网法治的可持续发展影响深远。无论是片面地从道德论的角度认定信息权属于用户，还是纯粹的效率视角，将信息权属划归为平台，都稍欠妥当。非必要信息收集的有效规制，须超越传统被动救济模式，以《民法典》与《个人信息保护法》的必要性原则及告知同意规则为基准，通过建构格式条款的实质审查标准、确立分层动态授权机制、强化风险披露义务，衡平个人与企业间的法益冲突，促成用户、平台与第三方在数据合规流动中的协同治理共赢。

参考文献

[1] 杨惟钦. 价值维度中的个人信息权属模式考察——以利益属性分析切入[J]. 法学评论, 2016, 34(4): 66-75.
[2] 凌萍萍, 焦冶. 侵犯公民个人信息罪的刑法法益重析[J]. 苏州大学学报(哲学社会科学版), 2017, 38(6): 66-71.
[3] 程啸. 论我国个人信息保护法中的个人信息处理规则[J]. 清华法学, 2021, 15(3): 55-73.
[4] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.
[5] 徐明. 个人数字权利实现的立体均衡逻辑[J]. 法学评论, 2025, 43(4): 134-145.
[6] 张丽霞. 论侵犯公民个人信息罪的“违反国家有关规定” [J]. 河北法学, 2025, 43(9): 124-142.
[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+191.
[8] 武腾. 最小必要原则在平台处理个人信息实践中的适用[J]. 法学研究, 2021, 43(6): 71-89.
[9] 孙颖. 平台协议规则的外部审查机制研究——以私权力规制为中心[J]. 湖北社会科学, 2025(5): 138-146.
[10] 王华伟. 已公开个人信息的刑法保护[J]. 法学研究, 2022, 44(2): 191-208.
[11] 萧鑫. 个人信息处理的多元同意规则——基于同意阶层体系的理解和阐释[J]. 政治与法律, 2022(4): 158-176.
[12] 杨芳. 个人信息三元权益论的教义学展开与体系衔接[J]. 交大法学, 2025(4): 52-66.
[13] 何青松, 王慧, 孙艺毓. 企业社会责任决策中的锚定效应[J]. 社会科学研究, 2019(6): 32-40.