Dispute Settlement 争议解决, 2026, 12(6), 164-171
Published Online June 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.126197

Hans汉斯

欧盟GDPR影响下我国数据合规的适用性问题研究

王一丹

北京工商大学法学院，北京

收稿日期：2026年5月16日；录用日期：2026年6月17日；发布日期：2026年6月26日

摘　要

随着数字化时代的飞速发展，数据已成为重要的生产要素和战略资源。《欧洲一般数据保护条例》(GDPR)自实施以来，在全球范围内产生了深远影响，成为众多国家数据保护立法与合规实践的重要参考。本文通过剖析GDPR的条文内容，探究其制度优势和不足之处，对比我国在数据合规领域的发展现状，分析目前我国在数据的流通与保护方面所面临的挑战，合理借鉴GDPR的立法理念，提出针对性的应对策略。进一步推动我国数据合规制度体系建设，为数据的合规实践提供切实参考，促进我国数字经济在安全、有序的轨道上健康发展。

关键词

数据合规，数字经济，数据保护，数据流通，个人信息

Research on the Applicability of China's Data Compliance under the Influence of the EU GDPR

Yidan Wang

Law School, Beijing Technology and Business University, Beijing

Received: May 16, 2026; accepted: June 17, 2026; published: June 26, 2026

Abstract

With the rapid advancement of the digital age, data has become a critical factor of production and a strategic resource. Since its implementation, the *EU General Data Protection Regulation* (GDPR) has had a profound global impact and has served as an important reference for data protection

文章引用: 王一丹. 欧盟 GDPR 影响下我国数据合规的适用性问题研究[J]. 争议解决, 2026, 12(6): 164-171.
DOI: 10.12677/ds.2026.126197

legislation and compliance practices in many countries. This paper analyzes the provisions of the GDPR to explore its institutional strengths and weaknesses. By comparing these with the current state of China's data compliance framework, it examines the challenges China faces regarding data circulation and protection. Drawing on the legislative principles of the GDPR, the paper proposes targeted strategies to further advance the development of China's data compliance system, provide practical guidance for compliance practices, and promote the healthy development of China's digital economy on a secure and orderly track.

Keywords

Data Compliance, Digital Economy, Data Protection, Data Circulation, Personal Information

1. 引言

在数字经济蓬勃发展的今天，数据的价值日益凸显，数据的收集、存储、使用、传输等活动贯穿于社会生活的各个领域。与此同时，数据安全与个人信息保护问题也日益严峻，数据泄露事件频发，给个人隐私保护带来了极高的风险，数据流通效率不足也给企业和公共利益带来了巨大损失。数字经济市场平稳有序运行，核心依托于数据合规与数据流通两大支柱。所谓数据合规，是指数据处理主体在数据收集、存储、处理、共享、销毁等全生命周期中，遵守法律法规、监管规则、行业标准及内部制度，确保数据活动合规安全、公开可溯，是平衡数据利用与权益保护的核心机制。合规的最终目的是保障数据在流通过程中的合法性与安全性。而数据流通则指代在各类市场主体间的流转行为，涵盖开放共享、商业交易、信息互换等多种形态。唯有将数据流转约束于法治框架之内，方能构筑规范稳健的数字经济市场格局。

欧盟 GDPR 的出台，为各国规范数据行为提供了重要参考，其立法逻辑在于加强对个人数据的保护，合理规范数据控制者和处理者的行为，从而促进个人数据的自由流通。我国积极推进数据合规的立法与实践，多年来已陆续出台了多部法律法规，初步构建起数据合规的制度体系框架。而就现实发展态势而言，我国数据合规在制度落地与行业实践层面依旧存在着现实问题与突出挑战，需结合本国国情持续探索适配本土化发展的合规路径。

2. GDPR 的制度优势及实践问题

《欧洲一般数据保护条例》简称 GDPR，是欧盟出台的个人数据保护新规，是目前全球在保护个人数据方面，规定最为严格、处罚最为严厉的法规之一。其最大的亮点在于限制了企业收集与处理用户个人信息的权限，将个人信息的最终控制权交还给用户本人。GDPR 的立法原则蕴含双重目的：一方面是保护个人数据在处理和流通过程中所涉及的自然人的基本权利与自由，尤其保护其个人信息保护权；另一方面是促进个人数据在欧盟境内的自由流通。两个截然对立的目的在 GDPR 框架下采用的逻辑关系为：统一数据保护水平，强化个人信息保护权，增强公民信心从而实现个人数据的流动利用。

2.1. GDPR 的制度优势

2.1.1. 注重数据权利主体本位

GDPR 最为突出的制度优势在于其确立了数据主体权利本位的核心立法逻辑，构建起以自然人数据

权益保护为核心的规范体系。GDPR[1]第 1 条确立的立法目标，把个人数据保护的权利视为自然人的基本权利，明确将个人数据保护上升为基本人权保障范畴。后续又规定了个人数据处理基本原则[2]、设立了数据主体同意条件[3]以及在第三章用了一整章的篇幅赋予数据主体包括知情权、访问权、更正权、删除权、数据可携权、被遗忘权在内的广泛的权利，构架起完整的数据主体权利体系，将个人对自身数据的自主控制权贯穿于数据处理全流程。

2.1.2. 建立数据全生命周期监管

传统数据监管模式[4]大多存在阶段性监管漏洞，监管重心多聚焦于数据收集环节，对后续数据的存储、使用、销毁等后续环节缺乏有效约束，极易出现“重准入、轻过程、弱收尾”的监管乱象，导致个人数据在全流程流转中面临隐私泄露的风险，也给企业监管带来极大的压力[1]。而 GDPR 突破了碎片化、节点式的监管局限，通过设定数据获取的合法性基础、严格数据存储期间的保密性要求、明确数据处理的最小必要原则、框定数据流转的边界与共享规则、强制企业遵循数据主体意志及时删除擦除个人数据等规定[5]，确立了覆盖数据收集、存储、处理、传输、共享、删除、销毁的全生命周期监管框架，将合规监管与责任约束贯穿个人数据流转的每一个环节。

此种全生命周期监管模式，打破传统碎片化监管局限，以全流程条文规制压实各方责任，全方位防范数据安全风险，显著提升数据治理的规范性与实效性。

2.1.3. 严格数据处理者责任

在数据监管方面，GDPR 重塑了数据处理的权责关系，将合规义务与举证责任主要分配给数据控制者与处理者，明确企业仅能在获得主体有效同意或具备法定正当依据的前提下开展数据处理活动。此外，条例第 28 条还设立了数据控制者与处理者之间的合约关系，严格限制了数据处理者的权利，减少了数据在多个处理者手中流转造成的安全风险。且数据主体享有在全过程中随时撤回同意的权利，有效杜绝了捆绑授权、概括授权等违规乱象。

这种以数据主体权利为核心、以企业责任义务为支撑的制度设计，极大提升了个人数据权益的保护层级，填补了传统数据治理中个人控制权缺位的制度漏洞[2]，为全球个人数据的权益保障和风险防控提供了先进范本和成熟参考，对我国数据合规制度体系建设具有丰富的借鉴意义。

2.2. GDPR 存在的实践问题

GDPR 构建起成熟、完备的数据合规机制，从制度层面确立权利本位核心导向，构筑起坚实的个人数据安全防护体系。但该条例落地实践运行后，过于严苛的保护标准逐渐显现出弊端，产生偏重个体权益保障、忽视产业发展需求的倾向，进而引发个人数据保护尺度失衡、数据市场流通受阻的现实问题。

2.2.1. 无边界的“识别”标准

GDPR 第 4 条规定了个人数据的范围，“个人数据”指的是任何已识别或可识别的自然人(“数据主体”)相关的信息；一个可识别的自然人是一个能够被直接或间接识别的个体，特别是通过诸如姓名、身份编号、地址数据、网上标识或者自然人所特有的一项或多项的身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份而识别个体。收集到的个人信息具有“识别”与“记录”两个要素，前者为实质

[1]丁晓东译：《欧洲一般数据保护条例》，载中国人民大学明德公法网，2018 年 9 月 24 日。
http://calaw.ruc.edu.cn/wxzl/xszs/d6de8d02ef9e4b22b712846b3a889d02.htm；下文中涉及 GDPR 条文的内容均引用于此。
[2]详见《欧洲一般数据保护条例》第 5 条。
[3]详见《欧洲一般数据保护条例》第 7 条。
[4]指欧盟《数据保护指令》要求机构在收集用户个人信息前，通过发布隐私声明告知用户信息的处理状况，用户在阅读声明后作出同意的意思表示，作为对个人信息收集及利用的合法授权。
[5]详见《欧洲一般数据保护条例》第 6 条、第 32 条、第 5 条、第 5 章、第 17 条等具体规定。

要素，后者为形式要素[3]，其中最主要的功能是识别个人，即可以根据这些信息对特定个人进行识别画像，切实影响到个人权利的保护。而可识别的信息与个人利益并非直接相关，如时间、地点、参与人等个人相关信息并不一定与个人有实质的联系，只是通过相关性而对识别起到辅助作用。这类信息对于主体的识别很难具有特定性，除非与直接信息一同分析，否则仅凭借这些关联性信息无法对个人进行画像，其分析得出的最多只是某类人的特点，无法精确定位到个人。例如我国在应对重大突发公共卫生事件时，会对特定时间去往特定地点的人员进行摸排工作，仅凭借时间、地点以及监控的模糊画面难以精准定位到个人，真正精准定位的是依靠健康码、高速 ETC、景点门票等绑定了个人电话号码或身份证等唯一标识的方式综合来定位的。若完全按照 GDPR 规定的宽泛的可识别性标准来认定保护范围，除了纯粹的机器、传感器和天气数据外，再也没有非个人的数据了[4]。

2.2.2. 数据流通受限于主体的“授权”

GDPR 第 6 条第 1 款(a)项将数据主体同意作为数据处理的合法性基础之一，而第 17 条规定数据主体有权撤回同意并要求控制者删除其有关个人数据。两个条款结合来看，赋予了数据主体很大的自由权。GDPR 第 6 条列出的数据处理的合法性基础，看似给予企业自主使用数据的权利，实际上适用范围相当有限，对于个人信息的利用仍受制于数据主体的个人意志，个人可以随时撤回同意，也享有在特定条件下拒绝处理、删除等权利[2]。即使存在数据控制者，基于合法性基础，在法律意义上数据主体才是这些数据的实际控制人，撤回同意规定使得 GDPR 第 6 条的合法性标准名存实亡，给了数据主体极大的自由空间，在司法裁判中容易出现数据主体方的倾向性，不利于数据市场的稳定。GDPR 作为数据保护条例，对主体权利的保护置于社会利益或数据控制者利益之上，并没有真正将数据作为社会资源，给予数据使用者应有的地位和权利。

欧盟 GDPR 构建起成熟完备的数据保护治理范式，其注重个人权利本位、数据全生命周期监管、严格问责的立法理念与制度设计具备显著参考价值，同时制度运行中暴露出过度化规制、数据流通受限的问题也具备警示意义。依托 GDPR 积累实践经验与现存问题，能够帮助厘清我国本土制度的特色优势与短板疏漏，客观审视司法实践层面存在的欠缺。

3. 我国数据合规制度管理体系

我国已形成以《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国数据安全法》(以下简称《数据安全法》)、《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》)为核心的数据合规法律体系。《网络安全法》主管网络空间运行的基础安全和整体秩序，相较于另外两部专门法而言，属于一般性法律，当数据侵权行为无法通过《数据安全法》和《个人信息保护法》进行规制时，可以依照《网络安全法》的条款进行裁判。《数据安全法》偏重数据本身，是数据安全专门法。《个人信息保护法》更关注个人私权利的保护，属于个人信息专门法。在法律适用顺位上，网安法此次做出的修改有效加强了同其他两部法律的衔接。当涉及到个人信息时，优先适用《个人信息保护法》的规定 [6]；对于关键信息基础设施的运营者违法在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的行为，依照《个人信息保护法》第 66 条、《数据安全法》第 46 条及相关法律、行政法规的规定进行处罚 [7]。既保障了规则适用精准度，亦可维系合规体系首尾闭环。

尽管三法共同构成数据合规基本框架，但彼此间存在明显衔接空白。各法律规制逻辑未能充分契合，

[6]《中华人民共和国网络安全法》第 42 条第 2 款 网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》《中华人民共和国个人信息保护法》等法律、行政法规的规定。

[7]《中华人民共和国网络安全法》第 71 条规定。中华人民共和国国家互联网信息办公室，申卫星：专家解读丨加强网络空间法治建设 依法更好保障网络安全[EB/OL]。https://www.cac.gov.cn/2026-01/02/c_1769093523876899.htm，2026-01-02。

制度协同适配性尚有提升空间。

一是数据划分标准不一致。主要体现在《数据安全法》与《个人信息保护法》对于数据类别划分标准的差异，《数据安全法》采用数据分类分级监管模式，根据数据重要程度划分为核心数据、重要数据以及未明确提出的一般数据[8]。而《个人信息保护法》则将个人数据划分为普通个人信息与敏感个人信息。当数据同时属于“重要数据”与“敏感个人信息”时，两部法律在监管领域出现了交叉，具体适用哪一部法律缺乏衔接指引，企业难以根据数据类型确定合规基准。

二是监管主体存在重叠。三部法律涉及到网信、工信、公安等部门均有监管职责，但部门间的监管协同机制尚未健全，易出现“重复监管”或“监管真空”现象，增加了数据处理主体的合规成本，不利于形成稳定统一的常态化监管治理格局[5]。

“三驾马车”的法律规范框架共同构筑起我国数据合规治理的核心法律体系，三法分工互补、协同规制，为个人信息权益保障、数据安全保护与网络空间治理提供了规范依据。但不可否认的是，这三部法律在内容规范上存在监管领域交叉、规制边界模糊的问题，立法层面的衔接瑕疵与规则冲突尚未完全消解，在司法实践过程中，仍存在法律适用争议问题亟待解决。

4. 我国数据合规的实践困境

数字产业近五年来高速发展，数据处理场景日趋多元复杂，我国数据合规体系虽已搭建完成基础法律框架，但现行法律规范之间衔接适配不足、不同层级监管主体权责存在交叉重叠等问题，使得数据合规制度在落地适用过程中逐步显现诸多的现实难题。

4.1. 个人信息界定标准模糊

我国对于个人数据的保护范围规定在《网络安全法》第 78 条第 5 款[9]对于个人信息的表述中，《个人信息保护法》第 4 条[10]将个人信息进行了一定的限缩，排除了匿名化处理[11]后的信息。有学者指出，个人信息立法目的在于保护自然人的权利而非信息本身，个人信息本身只是一个符号，只有当其可以“识别”到个人时才需要法律的介入并加以规范[6]。因此，当数据进行了匿名化处理，失去识别画像的能力，该数据就丧失了数据的“定位性”，不必要再用《个人信息保护法》进行保护。另有学者直接将无法用以识别的信息排除了个人信息的范围，认为识别性是个人信息的首要特性，不具有识别性的信息不是个人信息[7]。

尽管学界主流观点及法律的相关规定均认可匿名化处理后的个人信息不再受到《个人信息保护法》的特别保护，但实践中对于哪些数据属于匿名化数据尚无统一认定标准。司法实践中存在企业将“去标识化”[12]数据伪造成匿名化数据的现象。若不对二者加以区分，很可能导致企业滥用匿名化数据的特殊性质，造成隐私侵权风险。

[8]《中华人民共和国数据安全法》第 21 条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

[9]《中华人民共和国网络安全法》第 78 条 本法下列用语的含义：(五) 个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

[10]《中华人民共和国个人信息保护法》第 4 条 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。

[11]《中华人民共和国个人信息保护法》第 73 条 本法下列用语的含义：(四) 匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

[12]《中华人民共和国个人信息保护法》第 73 条 本法下列用语的含义：(三) 去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

我国“cookie 匿名化第一案”[13]在司法审理过程中，关于用户在浏览器的搜索轨迹是否属于匿名化数据，是否侵犯了数据主体的隐私权，一审判决和二审判决给出了不同的判决结果。一审法院判决侵权的理由主要有以下两点，一是认为网络搜索轨迹属私人活动与私密偏好，百度利用 Cookie 收集并商业使用原告搜索轨迹属于侵犯用户隐私权；二是认为百度收集数据并向用户个性化推荐的行为未征得用户的同意，违反了《个人信息保护法》的规定。这一结果本质上是法院注重人格权本位的体现，突出强调数字时代对于数据主体的隐私权保护及数据处理者应尽的义务。而二审法院改判的依据在于对浏览轨迹这一数据的认定，二审法院认为 Cookie 仅识别浏览器而非自然人，数据已与主体身份脱钩，不满足“可识别性”，不属于个人信息。且使用前已告知 Cookie 用途，并提供退出机制，用户可自主选择，因此也不再需要重新获取同意。

该案一审与二审的反转，本质是数字时代用户人格权保护与数据产业发展的价值冲突。二审判决虽在当时具有一定合理性，但暴露了我国司法在核心概念界定、侵权要件适用、利益平衡、立法衔接等方面的深层问题。2021 年《个人信息保护法》实施后，规则层面已大幅完善，但司法实践中“重产业、轻用户”的倾向仍未根本扭转，此类新型数据处理的合规边界与裁判标准仍需进一步统一与细化。

4.2. 同意授权自由度缺失

我国同样存在数据主体同意规则，并要求同意应当由个人在充分知情的前提下自愿、明确作出[14]。然而在电子产品的使用过程中，经常会出现“强制授权同意”的现象。例如北京四中院发布的马某与 A 公司网络侵权责任纠纷案，A 公司提供的词典 APP 服务页面会默认替用户选择同意“已阅读并同意服务条款和隐私政策”，且若用户取消同意，便无法使用涉案词典，存在强迫用户同意《服务条款》《隐私政策》的情形。此外，涉案词典属于具有词典翻译功能的实用工具类 APP，根据其基本服务业务功能，应当适用无须个人信息即可使用的规定。故其在用户注册时拒绝同意《服务协议》和《隐私政策》的情况下直接退出，不提供基本查词服务，应属于对基本业务的拒绝，侵犯了马某的个人信息权益[15]。

通过对该案件的分析，可以看到当前部分移动互联网的应用程序存在强制授权行为，采用直接勾选“我同意”的声明模式，避免发生无效的法律授权，侵犯了数据主体的信息自决权。从某种角度来看，在线服务商在获得用户许可之前不得擅自使用用户的数据具有合理性，但也带来了在线平台滥用合法性的法律风险，即在通过有效同意的授权之后对个人数据进行无合规性的二次加工[8]。国内电商平台用户基数庞大，每日汇聚海量个人数据，个人隐私安全隐患居高不下。这类制式授权条款应用覆盖面广，产生纠纷后多依托《民法典》条文调整，数据合规体系尚未形成完备处置方案，个人信息权益保护机制仍有待完善。

4.3. 数据过度采集乱象严峻

企业对个人信息的收集应遵循最小必要原则，具体规定在《个人信息保护法》第 6 条[16]，应采取对个人权益影响最小的方式，不得过度收集个人信息。但我国目前对于数据的采集并没有一个具体的限定

[13]详见南京市中级人民法院(2014)宁民终字第 5028 号民事判决书。
[14]《中华人民共和国个人信息保护法》第十四条 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。
[15]北京市第四中级人民法院. 马某与 A 公司网络侵权责任纠纷案[EB/OL]. https://bj4zy.bjcourt.gov.cn/article/detail/2024/04/id/7907520.shtml, 2024-04-22.
[16]《中华人民共和国个人信息保护法》第六条 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

区间，仅凭借原则性规定难以让企业真正做到合规采集数据，一些企业会超出“合同必需”范围来收集信息，造成数据侵权引发不良后果。最高院于2025年发布的265号指导性案例揭示了企业过度收集、非法获取个人信息造成的侵权行为。某公司在未征得用户罗某同意的情况下，通过线下合作体验店收集到的手机号码，擅自为罗某注册英语网站账号并推送个性化内容，其行为已远超“履行合同所必需”[17]的基本功能服务，不构成无需取得个人同意即可处理用户个人信息的法定情形，该企业的行为存在过错，已构成数据侵权[18]。监管约束力度不足，使得过度采集问题难以有效遏制，个人信息安全难以得到稳固保障，合规管控仍存在明显短板。

5. 我国数据合规实践性路径优化

我国数据合规的法治体系建设，既不能照搬GDPR模板，也不能闭门造车，需立足本土法治语境，取其精华，规避弊端，探索本土化适配路径。

5.1. 匿名化数据处理标准落地

完善匿名化数据处理标准化落地机制，是破解我国数据流通与个人信息保护矛盾、解决司法裁判尺度不一的核心路径，也是填补数据合规实践漏洞的关键举措。目前我国单从《个人信息保护法》的概念表述无法对匿名化数据和去标识化数据做出合理的区分，仅凭借企业的自主管理显然无法做到一致，需要制定统一的国家标准。一是要细化法定判定标准，构建层级化、场景化的匿名化认定体系。立法与监管部门应依托《个人信息保护法》等相关合规法律要求，结合不同行业、不同数据类型的特性，明确“无法识别、不可复原”的量化判定阈值，杜绝概括性、模糊性的合规标准，严格区分匿名化与去标识化的适用边界，从根源上杜绝企业利用概念漏洞规避合规义务，统一行政监管与司法裁判尺度，解决同案不同判的实践困境。二是强化企业数据匿名化处理的规范引导，统一行业认知与技术标准，有效规避主体理解偏差导致的技术处理差异，筑牢数据合规防线。三是建立数据处理全流程审计台账，对数据采集、匿名化处理、流通使用、销毁留存等全环节进行记录留存，确保操作可追溯、合规可核验。

5.2. 强化信息自决权的应用

针对当前网络平台普遍存在的捆绑授权、静默授权、强制一键同意等乱象，强化个人信息自决权的落地应用，是破解强制授权困境、补齐个人信息保护短板的核心治理路径。信息自决权的核心要义，在于个人有权决定何时、何地、以何种方式传递其个人信息[9]，保障个人对自身信息的全路径享有自主选择、自主把控、自主撤回的完整权利，能够从权利根源上对抗平台不合理的强制授权规则，扭转用户被动授权的弱势局面。平台应当严格遵循最小必要原则，将基础服务授权与增值服务授权、核心信息授权与非核心信息授权进行拆分，为用户提供独立、可选择的授权选项。用户可根据自身使用需求自主授予或关闭权限，无需为获取基础服务被迫妥协授权无关个人信息，从制度层面杜绝强制捆绑授权的操作空间。同时，依托监管力量压实平台主体责任，将侵害信息自决权、设置强制授权壁垒的行为纳入重点监管范畴。通过常态化巡查、专项整治与合规处罚，倒逼平台摒弃强制用户授权的粗放运营模式，尊重用户信息自主决策权利。通过全方位强化信息自决权的实际应用，彻底整治强制授权乱象，平衡平台数据利用与个人隐私保护的关系。

[17]《中华人民共和国个人信息保护法》第十三条 符合下列情形之一的，个人信息处理者方可处理个人信息：(一) 取得个人的同意；(二) 为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；……依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

[18]中华人民共和国最高人民法院。指导性案例265号：罗某诉某科技有限公司隐私权、个人信息保护纠纷案[EB/OL]。https://www.court.gov.cn/shenpan/xiangqing/474481.html，2025-08-28。

5.3. 健全监管协同与问责机制

健全监管协同与问责机制，是整治网络平台数据过度采集乱象、遏制无序数据抓取行为、筑牢数据安全底线的重要制度保障。当前网信、公安、市场监管等部门均具备数据监管职能，但各部门监管边界划分模糊，存在各自为政、信息不通、执法脱节的问题，容易出现重复监管、监管空白、权责推诿等现象。部分中小型平台及小众应用软件借助监管缝隙，无底线采集非必要个人信息，而跨部门监管联动不足、线索移送滞后，导致违规行为难以被及时发现、精准查处。对此，需构建多部门一体化监管协同体系，打破部门监管壁垒，建立常态化信息共享、线索移送、联合执法工作机制，整合各方监管资源，形成全覆盖、无死角的监管合力。针对 APP 超范围采集、静默采集、强制索权等过度采集重点乱象，开展常态化专项整治，精准排查各类违规数据处理行为。另外，需严格落实闭环问责机制，细化数据过度采集违法行为的处罚标准，依据《数据安全法》《个人信息保护法》提高违规惩戒力度，对情节严重的企业实施高额罚款、业务整改、信用惩戒等多重处罚，落实企业负责人追责制度。通过强化监管协同、压实问责惩戒，大幅提升企业违法成本，彻底整治数据过度采集行业乱象，规范市场数据处理秩序。

6. 结语

欧盟 GDPR 以其严苛的个人数据保护规则和全球性影响力，为世界各国数据合规建设提供了重要参照。我国在数字化浪潮推动下，虽已初步构建起以《网络安全法》《数据安全法》《个人信息保护法》为核心的数据合规法律框架，多部门协同监管格局逐步形成，企业合规意识与实践也在不断提升，但仍面临法规细化协调不足、司法实践经验欠缺等挑战。需要借鉴 GDPR 在强化数据主体权利、规范数据处理活动等方面的经验，结合我国数字经济发展需求和社会治理特点，进一步完善法律制度，明确数据分类分级标准，推动数据保护落地，降低企业合规负担。通过这些针对性策略的实施，健全我国数据合规体系，为企业提供清晰的合规指引，促进数据安全有序流通，推动数字经济在安全、合规的轨道上实现高质量发展。

参考文献

[1] 范为. 大数据时代个人信息保护的路径重构[J]. 环球法律评论, 2016, 38(5): 92-115.

[2] 高富平. GDPR 的制度缺陷及其对我国《个人信息保护法》实施的警示[J]. 法治研究, 2022, 141(3): 17-30.

[3] 齐爱民. 个人信息保护法研究[J]. 河北法学, 2008, 26(4): 15-33.

[4] 梅夏英. 在分享和控制之间数据保护的私法局限和公共秩序构建[J]. 中外法学, 2019, 31(04): 845-870.

[5] 褚霞. 数据产权“三权”分置的法律实现路径研究——基于《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》的体系解释与制度衔接[J]. 北京城市学院学报, 2026(1): 86-92.

[6] 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.

[7] 韩旭至. 大数据时代下匿名信息的法律规制[J]. 大连理工大学学报(社会科学版), 2018, 39(4): 64-75.

[8] 王雪乔. 论欧盟 GDPR 中个人数据保护与“同意”细分[J]. 政法论丛, 2019(4): 136-146.

[9] 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.