



2024年全国网民网络安全感满意度 个人信息保护和数据安全 专题调查报告



发起单位: 全国135家网络社会组织及相关机构(网安联)

联合发起单位: 全国228家网安联志愿服务机构及相关志愿服务团队

牵头单位: 北京网络安全安全协会

承办单位: 乌镇数字文明研究院

浙江大学国际传播研究中心

互联网实验室

2024年10月

本报告数据来源于 2024 网民网络安全感满意度调查活动，任何组织和个人引用本报告中的数据和内容须注明来源出处。

组委会欢迎有关研究机构合作，深入挖掘调查数据价值，有需要者请与组委会秘书处联系。

报告查询(总报告及区域、专题、行业报告):网络安全共建网:www.iscn.org.cn“网安联”公众号:



2024 网民网络安全感满意度 “个人信息保护和数据安全”专题调查报告

乌镇数字文明研究院
浙江大学国际传播研究中心
互联网实验室
2024 年 10 月

目 录

一、加强个人信息保护和数据安全治理的背景..... 1

二、2024 年参与专题调查的公众网民对个人信息保护和数据安全的感受情况 3

 （一） 公众网民对个人信息保护和数据安全的整体满意度持续提高 3

 （二） 网民个人信息泄露现象加剧：公众安全感亟需提升 3

 （三） 公众网民在多元场景感受到的信息泄露情况好转 4

 （四） 公众网民对个人信息泄露多能主动进行处理 5

 （五） 公众网民对生物识别信息风险的担忧程度持续提高 6

三、2024 年参与专题调查的公众网民对个人信息保护反馈情况 7

 （一） 个人信息、数据安全保护现状以及存在的问题 7

 （二） APP 注册是网民对网络个人信息泄露环节感知中的主要环节 9

 （三） 网民认为 APP 使用存在的各类违规现象与问题 10

四、2024 年参与专题调查的公众网民对《个人信息保护法》等法制建设的认知情况 12

 （一） 网民对相关法律法规的了解程度 12

 （二） 个人信息保护民事公益诉讼推行过程中面临的困境、建议和期望 14

 （三） 网民对个人信息保护民事公益诉讼的建议 14

五、我国数据安全法制建设存在的问题与提升方向 15

 （一） 数据安全保护存在的主要问题 15

 （二） 数据规范作为首要问题仍未得到有效解决 16

 （三） 数据应用程度未能跟上发展步伐 16

 （四） 中介服务供应不足成为 2024 年网民日益关心的问题 17

 （五） 加强数据安全保护需要多方合作与责任落实 17

六、网民对个人信息保护和数据安全的建议和期望 18

 （一） 公众网民仍然期待宣传教育的加强与普及 18

 （二） 数据安全保护集中在三个层面 19

 （三） 在数据安全保护上，公众网民期待的重点是规制力度的提高 19

七、提高网民个人信息保护和数据安全的对策 20

 （一） 明确平台数据收集的限度，提升个人数据保护自主权 20

 （二） 善用人工智能等前沿技术，架构数据主动保护体系 20

 （三） 加大规范数据市场的力度，促进数据流通的合法性 21

 （四） 多渠道普及信息安全教育，疏通信息保护诉讼流程 21

一、加强个人信息保护和数据安全治理的背景

在数字化时代，个人信息保护和数据安全治理的重要性日益凸显。随着信息技术的快速发展，数据已成为关键的生产要素，对经济、政治、文化、社会和生态文明建设产生深远影响。然而，数字化转型在带来便利的同时，也伴随着个人信息泄露、数据滥用等风险，这些问题对国家安全、公共利益和个人权益构成了严重威胁。因此，加强个人信息保护和数据安全治理成为全球面临的紧迫挑战。

数据安全作为网络安全的重要组成部分，在国家安全、经济安全以及社会稳定中占据着举足轻重的地位，这一点在近年来的政府工作报告中得到了充分体现，数据安全的重要性被反复强调，并已成为国家战略规划的核心内容之一。党的十八大以来，从信息化发展大势和国内外形势出发，提出了一系列开创性的新理念、新思想、新战略，形成了关于网络强国的重要思想。在此基础上，网络安全政策法规体系不断完善，网络安全工作体制机制逐步加强，全社会的网络安全意识和能力显著提升，广大人民群众在网络空间的获得感、幸福感、安全感持续增强。然而，我们也必须清醒地认识到，随着数字化进程的加快，我国面临的网络安全威胁和风险呈现出新的特点，这些威胁和风险已经渗透到政治、经济、文化、社会、生态、国防等多个领域。党的二十届三中全会通过的《中共中央关于进一步全面深化改革、推进中国式现代化的决定》中明确提出建立高效便利安全的数据跨境流动机制，强调提升数据安全治理监管能力，为我国数据安全治理体系和能力现代化提供了纲领性指导。因此，有效防范网络安全风险、坚决维护网络空间安全，已经成为我们必须面对和解决的重大而紧迫的安全问题。

《网络数据安全条例》也宣布自 2025 年 1 月 1 日起施行。以《网络安全法》《数据安全法》《个人信息保护法》等法律为依据，聚焦网络数据，细化相关规定，完善网络数据安全规则，为提升网络数据安全治理体系和能力现代化提供了更有操作性的法治保障。条例中明确了网络数据处理者的主体责任，优化了网络数据跨境安全管理制度，并明确了网络平台服务提供者的责任义务，健全了网络数据监督管理体制机制。这些法律法规的实施，标志着我国在个人信息保护和数据安全治理方面正逐步构建起一套科学、高效、法治化的治理体系，为推进国家治理体系和治理能力现代化，实现高质量发展提供了有力支撑。

在人工智能时代，数据已成为重要的基础设施，网络数据安全性的重要性愈发凸显。随着数据驱动的技术迅猛发展，海量信息的收集和分析不仅推动了创新与效率的提升，也引发了对数据隐私和安全的前所未有的关注。AI 系统通常依赖于大量的个人和敏感数据进行训练

和优化，这使得数据安全漏洞的潜在后果变得更加严重。一旦数据遭到泄露或滥用，不仅会对个人隐私造成深刻影响，还可能导致经济损失、品牌信誉受损以及法律责任等多重危害。因此，建立强有力的数据安全框架，确保数据在存储、传输和处理过程中的安全性，已成为维护公众信任、促进可持续发展的关键任务。

为了更好贯彻落实为进一步贯彻落实习近平总书记“提升广大人民群众在网络空间的获得感、幸福感、安全感”重要指示精神，响应国家网络安全宣传周的“网络安全为人民，网络安全靠人民”的号召，全面了解网民群众对网络安全现状的看法和意见建议，135 家网络安全协会和社会组织共同进行网民网络安全感满意度调查问卷，涉及多个专题。其中个人信息保护和数据安全专题，共收集到了 123710 份有效样本采集量。基于此次调查所获数据，分别从参与专题调查的公众网民对个人信息保护和数据安全的感受情况、个人信息保护反馈情况、个人信息保护法等法制建设的认知情况、我国数据安全法制建设存在的问题与提升方向以及网民对个人信息保护和数据安全的建议和期望这六个方向展开，来有效应对个人信息保护与网络安全的挑战，分析当前面临的主要风险和威胁，提出相应的政策建议和技术解决方案，促进个人信息保护和网络安全工作的持续改善和创新发展，为构建安全、可信的数字社会做出贡献，最终汇总形成“2024 个人信息保护与数据安全”专题报告。

二、2024 年参与专题调查的公众网民对个人信息保护和数据安全的感受情况

（一）公众网民对个人信息保护和数据安全的整体满意度持续提高

2024 年的调查结果显示,网民对我国个人信息保护状况的满意度平均得分为 8.0139 分,整体呈现出较为满意的态度。根据调查评分标准:“非常不满意”得分为 1-2 分,“较不满意”3-4 分,“一般”5-6 分,“较满意”7-8 分,“非常满意”9-10 分。结果显示,评价为“一般”“较不满意”“非常不满意”的受访者比例分别为 21.41%、5.88%和 4.17%,较 2023 年均有所下降,其中“一般”评价下降了 13.57%，“较不满意”下降了 4.13%。约 33.11%的受访者对当前状况表示“较满意”，而 35.43%的受访者则给予了“非常满意”的评价，这两个比例相较去年有所提升，总和已超过整体评价的“半数”。

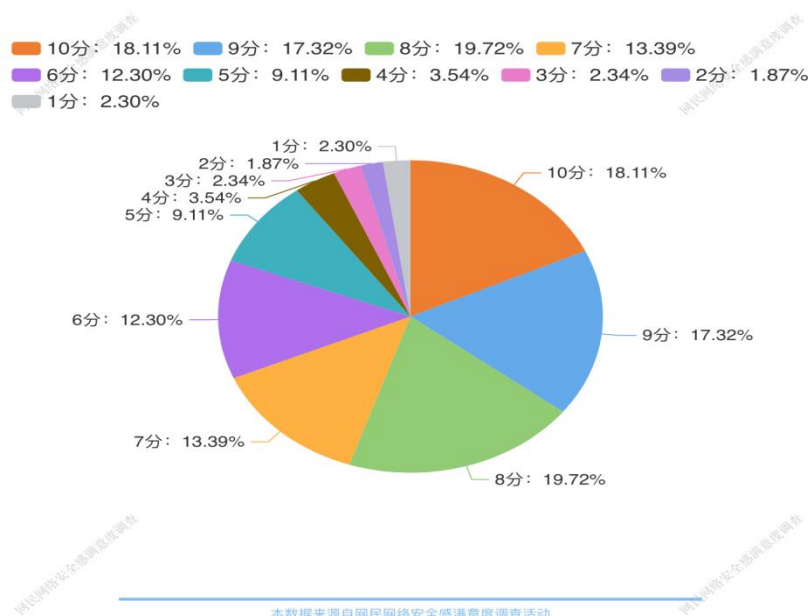


图 2-1: 公众网民对个人信息保护现状的评价

（二）网民个人信息泄露现象加剧：公众安全感亟需提升

近一年中,网络个人信息泄露的情况仍然是一个普遍存在的问题,且泄漏情况较 2023 年更为严重。约 45.5%的受访者表示遭遇了“非常多”或“比较多”的泄露(19.69%和 25.81%),而 32.37%的受访者认为自己“有一些”泄露经历。尽管 14.20%的人表示“很少”遇到泄露,7.93%的人认为“没有遇到”。但总体来看,超过 77%的受访者(“非常多”、“比较多”、“有一些”)经历了不同程度的个人信息泄露。这反映出公众对网络安全问题的高度关注和迫切需求,加强网络安全措施和个人信息保护政策以提升公众的信任和安全感任务仍然迫在眉睫。

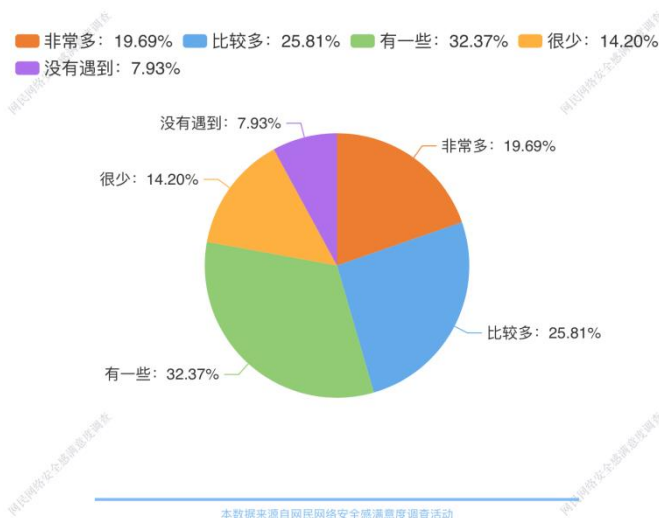


图 2-2: 近一年网民对个人信息泄露的感知情况

(三) 公众网民在多元场景感受到的信息泄露情况好转

公众在怀疑或确认个人信息被泄露或滥用的情形中，主要包括接到各类中介推销电话（64.88%）仍然是信息泄漏最主要的场景。另外，大数据杀熟现象（44.12%）较 2023 年相比有所增加，个人信息仍可能被用于不公平的定价策略。其他常见的情况还包括收到相关性推销短信（38.09%）、垃圾邮件（37.36%），以及某些应用默认勾选同意《服务协议》，允许收集用户信息（26.17%）。此外，受访者还报告了身份证被他人用来注册公司（25.54%）或办理贷款（22.45%）的情况，这些严重影响了个人权益。还有 19.71% 的受访者在匿名注册后被熟人通过社交软件加为好友，增加了隐私泄露的风险。部分受访者还担忧在信息收集过程中未被告知目的和方式（19.38%），以及在特定情境下被迫同意收集用户信息（16.16%）。此外，12.45% 的受访者表示遭遇擅自使用未授权图片或视频的问题。

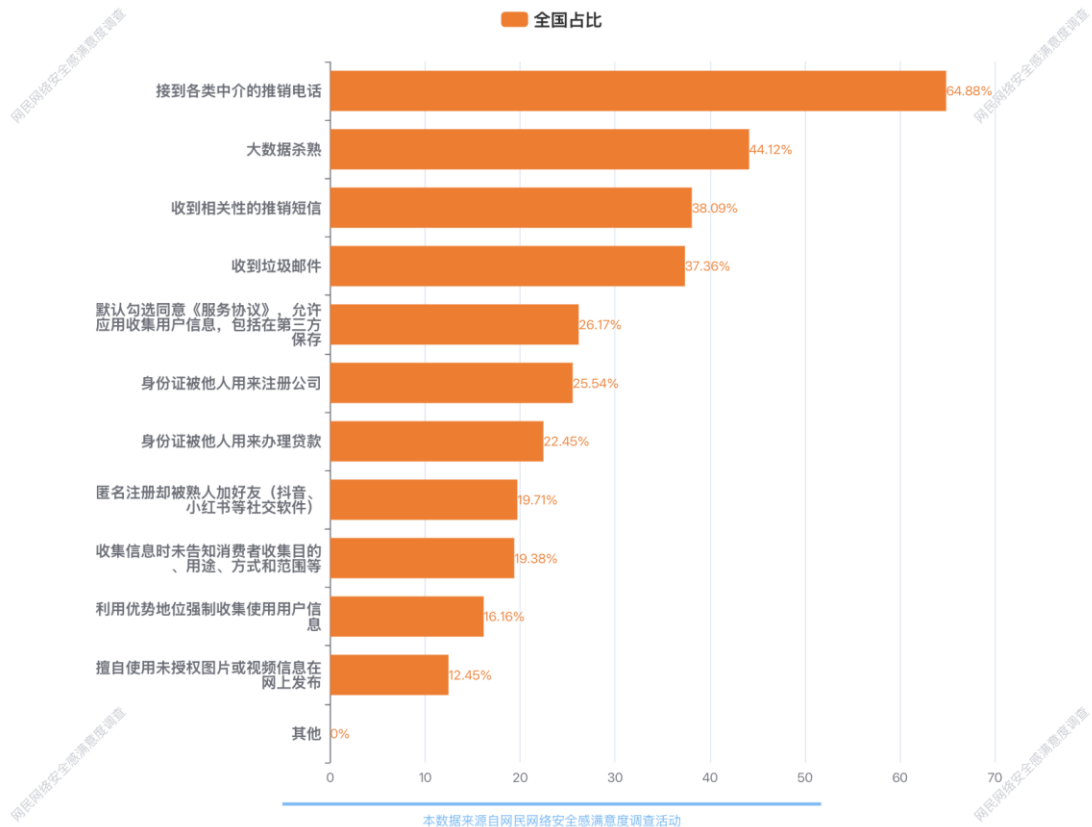


图 2-3：网民遇到的怀疑或确认个人信息泄露的情形

（四）公众网民对个人信息泄露多能主动进行处理

在发现以上个人信息泄露时，大多数受访者都会对泄露信息的情况作出不同程度的处理。主要选择立即更改账号密码（56.08%）和报警投诉（42.57%），但仍有 24.85%人感到恐慌却不知如何应对，仅 10.49%（较 2023 年有所下降）的受访者认为泄露影响不大，选择继续正常生活。而公众的应对措施主要包括：32.55%的受访者倾向于在社交媒体上分享自己的经历，以提醒他人提高警惕。甚至有 24.28%的人尝试找出泄露的源头。还有 18.43%的受访者会向家人和朋友寻求帮助，认为社会支持在此情况下很重要。

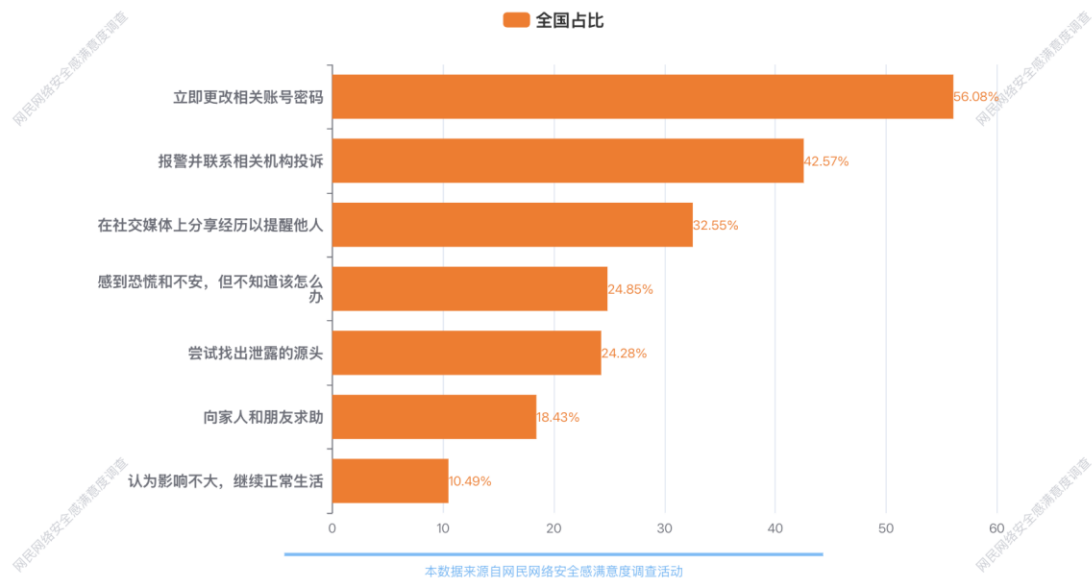


图 2-4: 网民遇到个人信息泄露时的解决方式

(五) 公众网民对生物识别信息风险的担忧程度持续提高

公众对使用生物识别技术（如人脸识别和指纹识别）进行身份认证时的信息泄露普遍存在担忧，而 2.89% 的人则表示“没有担心”，这一比例较 2023 年有所下降。具体而言，24.10% 的受访者表示“非常担心”，而 34.68% 的人“比较担心”，合计超过一半的受访者对此感到忧虑。29.48% 的受访者表示“一般”，显示出对风险的中等认知。相比之下，仅有 8.85% 的人“很少担心”。生物识别技术的普及，带来便利的同时，却让公众丧失其个人信息保护的安全感。

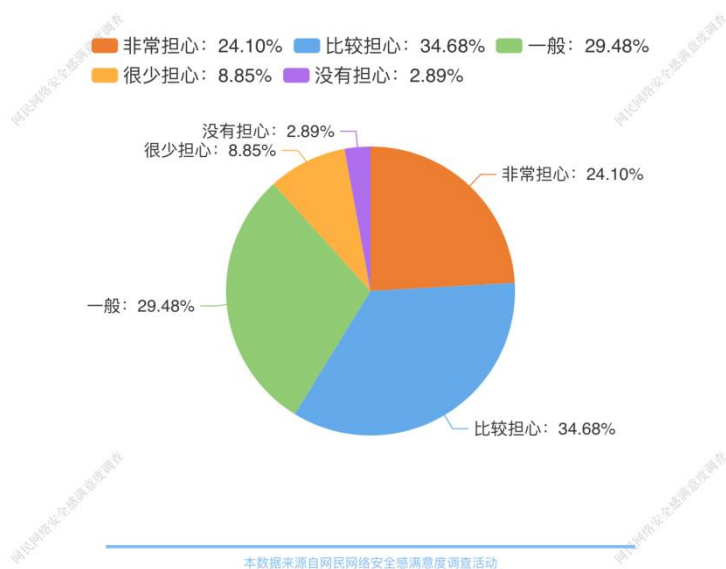


图 2-5: 网民对生物识别技术泄露个人信息风险的倾向

在生物识别技术日益普及的背景下，公众对相关政策和规定的关注度 and 理解程度尚需提升。对新出台的《人脸识别技术应用安全管理规定（试行）（征求意见稿）》的了解程度较为有限，37.26%的受访者表示“不了解”，而 4.35%的人则表示“不关注”。仅有 13.91%的受访者表示“非常了解”，而 44.47%的人“了解一些”。

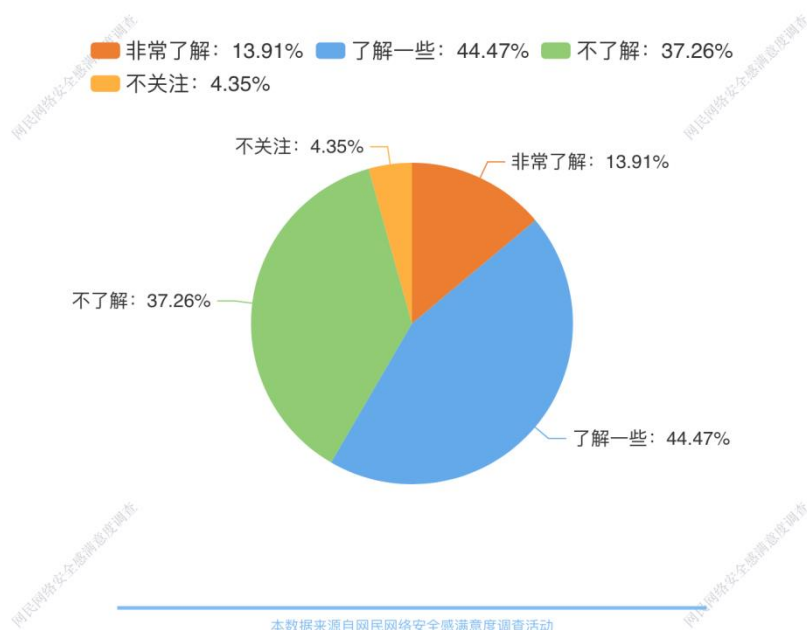


图 2-6：对《人脸识别技术应用安全管理规定（试行）（征求意见稿）》对了解程度

三、2024 年参与专题调查的公众网民对个人信息保护反馈情况

（一）个人信息、数据安全保护现状以及存在的问题

公众对个人信息保护不足的应用类型主要集中在社交应用和网络媒体，其中 51.79%的受访者认为社交应用（如即时通讯和短视频）在保护个人信息方面做得不太好，49.50%的人对网络媒体（如新闻资讯和视频直播）的保护表示不满。此外，41.82%的受访者指出数字娱乐应用（如网络游戏和音乐）也存在信息保护不足的问题，40.78%认为电子商务平台（如网络购物和网上支付）亟需加强个人信息保护。相比之下，网上办公类和电子政务类应用的个人信息保护问题的关注度相对较低，但仍有 29.53%的人表示担忧。

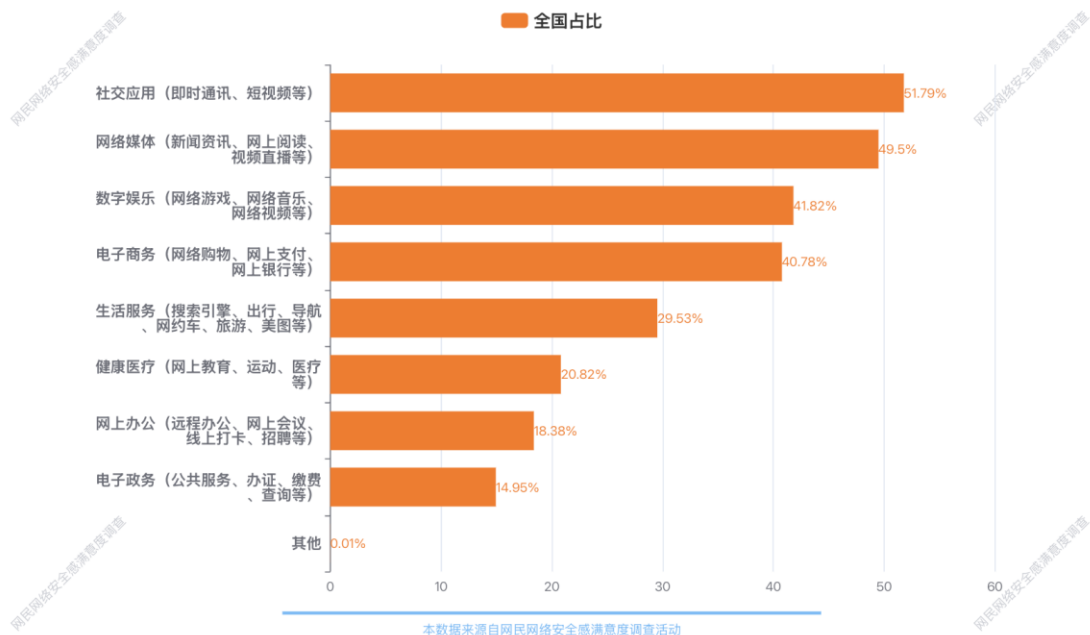


图 3-1-1 个人信息保护受关注的 APP 类型

公众在使用移动应用（APP）时对安全隐私协议的阅读态度差异明显。具体来看，26.84%的受访者表示“都会认真阅读”这些协议，显示出对隐私安全的重视。与此同时，38.89%的人表示“极个别会认真阅读”，可能只是针对特定的应用程序。相对而言，有23.02%的受访者表示“不会留意”这些协议，11.24%的受访者则表示会根据 APP 的大众使用程度进行判断，对于不被普遍使用的 APP 会认真查看协议。

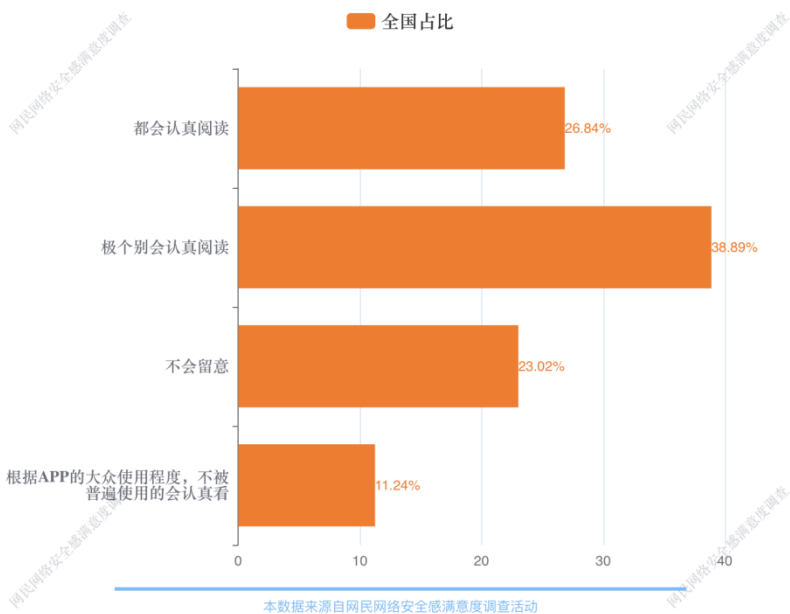


图 3-1-2：网民使用移动应用（APP）时阅读安全隐私协议的情况

而在使用移动应用时不留意安全隐私协议的主要原因是“协议太长了，没有耐心看”（42.58%）。其次，21.41%的受访者认为“平台会有各种方式获取我的信息，认真阅读也没意义”，反映出对隐私保护无力感的普遍存在。还有 14.53%的人表示“没有需要保护自己安全隐私的意识”。此外，7.64%的受访者认为“信息裸奔时代，已经不在意”，而 13.84%的人则认为“协议只是代表平台利益，用户没有选择权”，进一步凸显了对平台主导地位的不满。

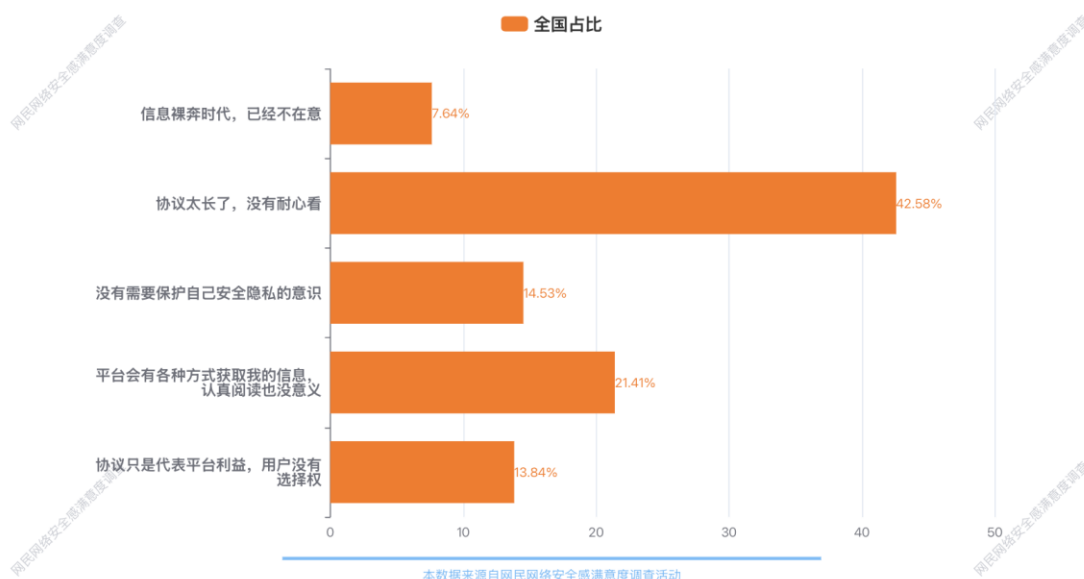


图 3-1-3:网民使用移动应用时不留意安全隐私协议的主要原因

（二）APP 注册是网民对网络个人信息泄露环节感知中的主要环节

公众对个人信息泄露的主要环节具有清晰的认识。其中，注册 APP 账户时获取隐私权限的情况被认为是最主要的泄露途径，达到 61.93%。公众对应用程序要求过多权限产生担忧，特别是在涉及相机、位置等敏感信息时，用户普遍感到不安。其他公众感知个人信息泄露的主要环节包括点击不明二维码和链接（47.34%）以及参与网上测试、投票和抽奖活动（45.89%）。此外，使用公共 WiFi（31.85%）、将个人信息上传至云端（29.93%）、随意丢弃含信息的单据（24.44%）、未彻底删除旧手机数据（23.36%）、浏览器截取敏感信息（23.00%）以及社交平台随意分享个人信息的图片（21.36%）也被认为是潜在的泄露风险。认为人脸识别确认身份的过程可能是泄露环节的网民较去年有所减少，但仍有 20.14% 的受访者视为。

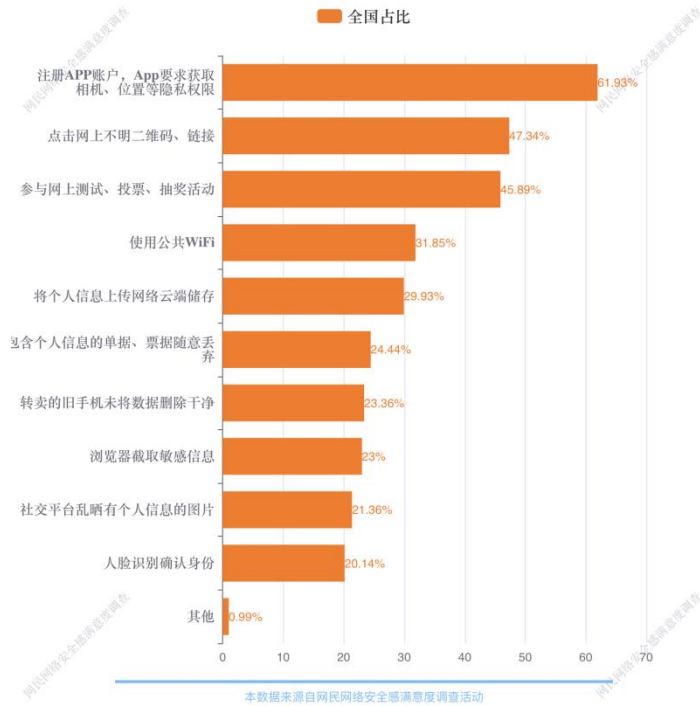


图 3-2-1：个人信息泄露环节

（三）网民认为 APP 使用存在的各类违规现象与问题

公众普遍认为多个 APP 或平台存在滥用个人信息的情况，尤其是在个性化广告、信息推送和价格歧视方面。具体来看，50%的受访者认为“抖音”存在较多的滥用情况，紧随其后的是“微信”（39.04%）和“拼多多”（39.00%）。此外，“淘宝”也有 35.16%的受访者表示担忧，其他如“百度”（28.24%）和“今日头条”（18.67%）的比例也不容忽视。

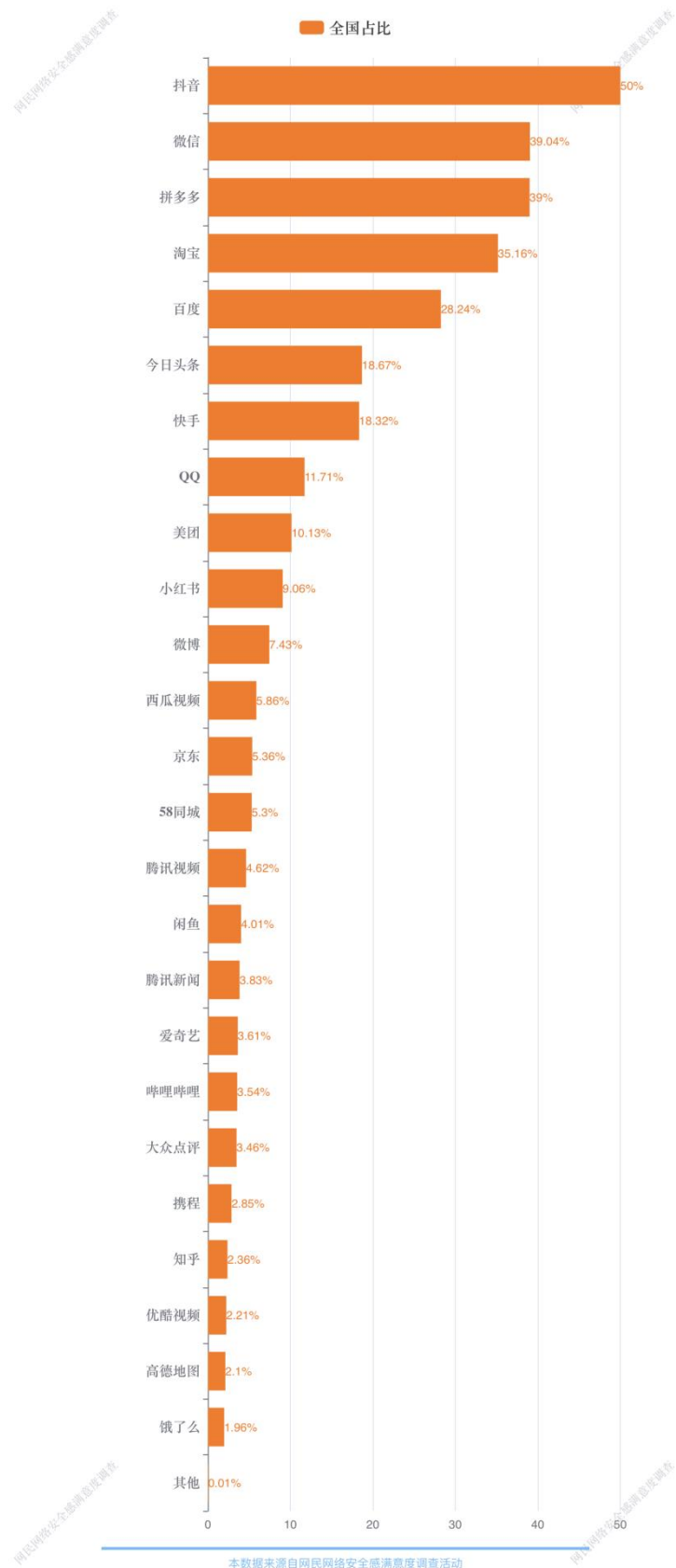


图 3-3-1:存在较多的滥用个人信息的具体平台

在数据安全法、个人信息保护法等出台后，18.42%的受访者认为 APP 运营者在这方面

“明显改善”，而 39.29% 的人表示“有所改善”，这表明法律的出台在一定程度上促进了运营者对个人信息保护的重视和改进。与此同时，有 36.89% 的受访者的态度则趋于中立，认为改善情况“一般”，这可能暗示他们对现状的期望并未完全实现。相对较少的比例中，仅有 3.98% 的人认为情况“有所变差”，而 1.42% 的受访者甚至表示“明显变差”。总体而言，公众对数据安全法和个人信息保护法实施后 APP 运营者在个人信息保护方面变化的多元看法。

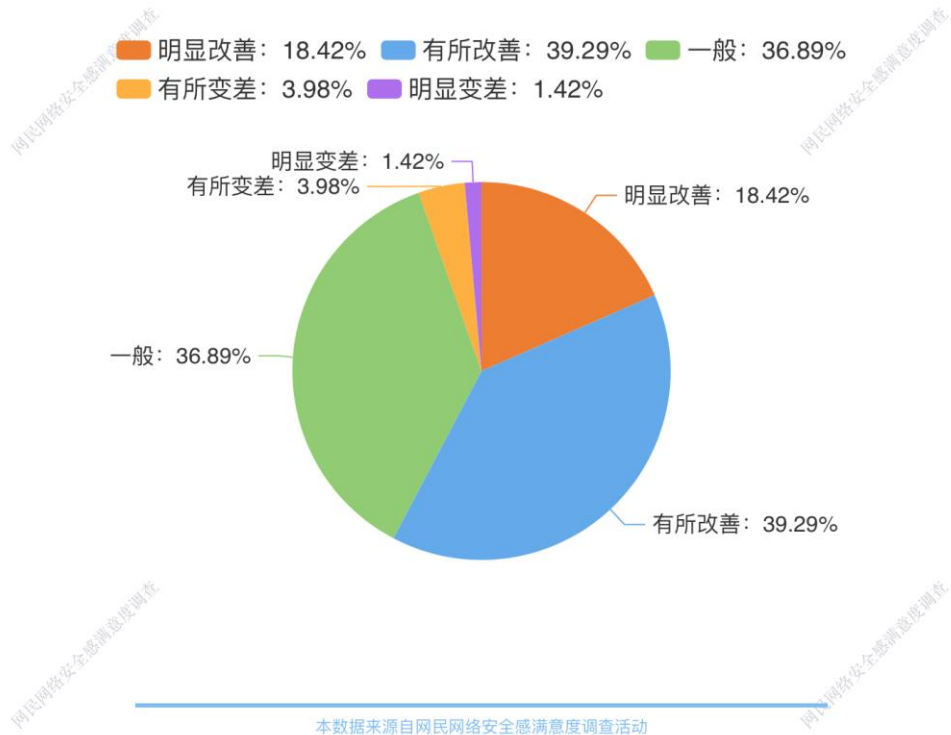


图 3-3-2：网民对非政府、非官方 app 需要提交敏感信息的态度

四、2024 年参与专题调查的公众网民对《个人信息保护法》等法制建设的认知情况

（一）网民对相关法律法规的了解程度

公众对个人信息安全保护法律法规的认知情况，展现出不同程度的了解。最引人注目的是，《中华人民共和国个人信息保护法》以 55.42% 的认知率屹立于众，成为公众最为熟知的法律。紧随其后的是《民法典》，获知率为 45.07%，以及《网络安全法》，被 41.16% 的受访者所了解。与此同时，《数据安全法》和《未成年人保护法》分别以 38.76% 和 38.18% 的认知率进入公众视野。然而，仍有 10.68% 的受访者表示对这些法律法规毫无了解。

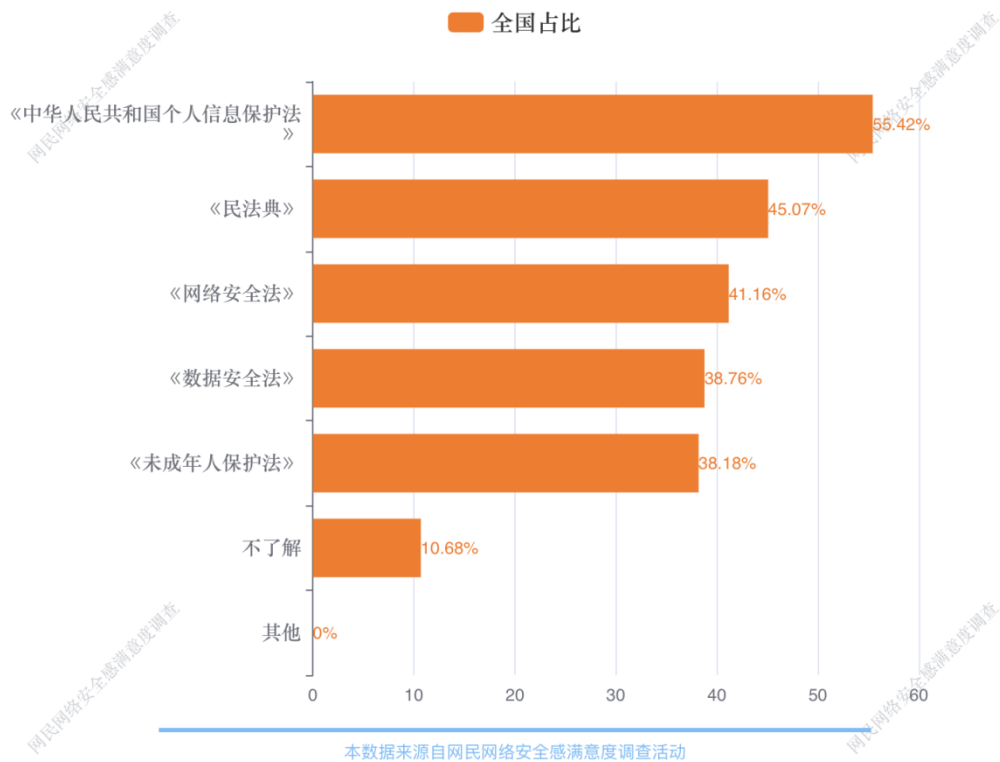


图 4-1 涉及个人信息安全保护的法律法规

而多达 64.43%的人则表示“不了解”《个人信息保护法》个人信息保护公益诉讼制度中的新规定。只有 35.57%的受访者表示了解该制度。这与 2023 年相比并且有明显提升，说明针过去对新兴法律机制的普及效果并不明显，仍需要加强。

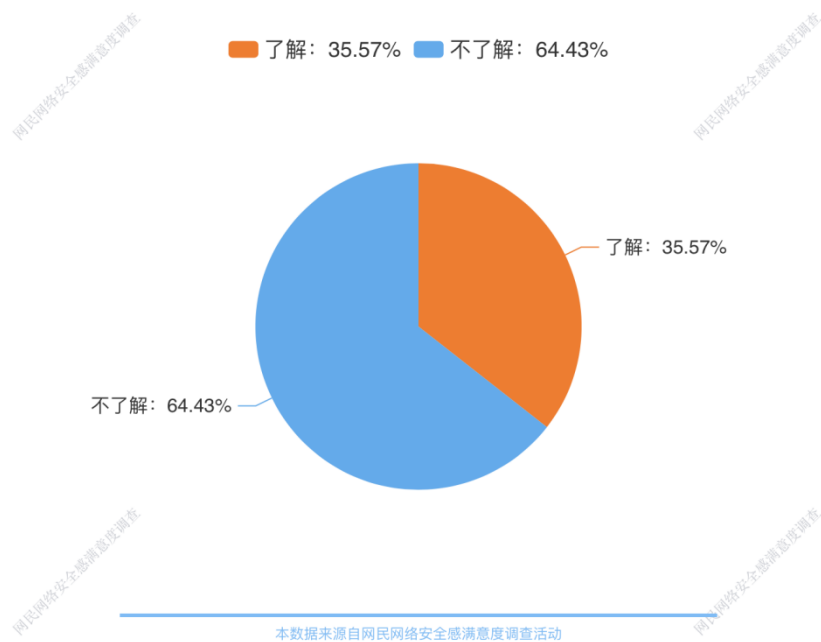


图 4-2 网民对《个人信息保护法》个人信息保护公益诉讼制度中新规定的了解情况

（二）个人信息保护民事公益诉讼推行过程中面临的困境、建议和期望

在个人信息保护民事公益诉讼的推行过程中，公众普遍认为面临多重困境。其中，57.24%的受访者指出诉讼过程漫长且成本高昂是一大主要障碍，许多人因此望而却步，难以积极参与维权。其次，52.06%的受访者认为，原告的维权意识不足，或因惰性而不愿提起诉讼，这在一定程度上削弱了公益诉讼的有效性和影响力。与此同时，46.70%的受访者反映，判决的执行困难，使得即便获得胜诉，实际效果依然有限，无法有效保护个人信息安全。此外，34.72%的人指出，现有的惩罚力度无法有效消除再犯风险，使得侵害行为屡屡得逞。

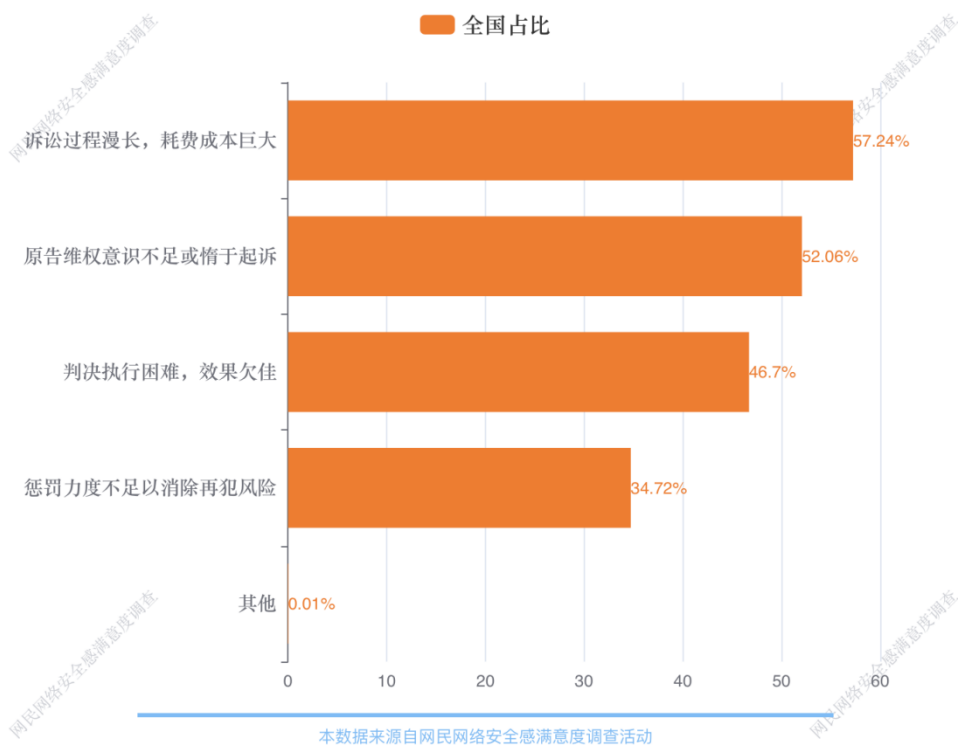


图 4-4 在个人信息保护民事公益诉讼的推行过程中会面临的困境

（三）网民对个人信息保护民事公益诉讼的建议

为了解决以上问题，超半数受访者建议从制度监管层面入手，扩大检察机关获取侵权线索的途径，例如鼓励举报和加强部门间的衔接，提高公益诉讼的效率和执行力。同时要**加强惩罚措施**，以产生更强的震慑作用，防止侵权行为的发生是提升公益诉讼效果的重要措施。完善公益诉讼配套制度（48.36%）也不容忽视。有 36.24%的人认为，应将公民个人纳入公益诉讼主体，使更多的个体能够参与到信息保护的维护中。27.71%的受访者指出，明确个人信息保护公益诉讼主体的起诉顺位，对于理顺诉讼流程、提升诉讼效率也具有重要意义。

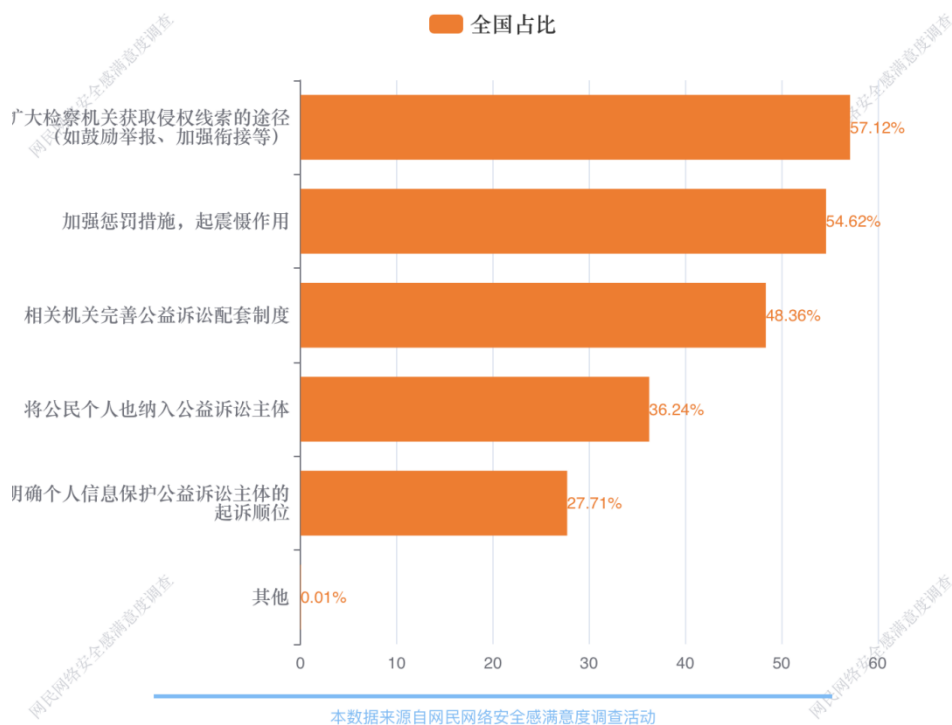


图 4-5 对个人信息保护公益诉讼的建议

五、我国数据安全法制建设存在的问题与提升方向

(一) 数据安全保护存在的主要问题

当前数据安全保护还有待加强和改进, 数据安全保护存在多方面问题。与 2023 年相比, 数据不规范和数据交易市场比较乱的情况相对来说有所好转, 但数据管理普遍不规范、数据应用程度低仍是最突出的一些问题。经市场监管总局(标准委)批准发布, 将于 2023 年 10 月 1 日起正式实施的《信息技术大数据数据资源规划》为解决数据管理标准和规范不统一的问题提供了一个良好的方向和框架。该规划在数据收集、存储、处理和分享方面制定统一的规划和标准, 从而减少各个数据管理者在这些方面存在的差异, 但执行力度和效果仍不明显。其次, 应用程度低、数据安全标准规范建设滞后、中介服务供应不足、政府数据不开放也是数据安全方面存在的重要问题。数据处理过程中的标准仍然不够明确, 尽管拥有丰富的数据资源, 但其价值未能得到充分挖掘。

同时, 数据交易市场混乱, 缺乏透明度, 也增加了潜在风险。中介服务供应不足, 影响了数据交易的安全与效率。政府在数据开放方面的不足限制了公共数据的有效利用。数据安全标准和规范的建设滞后, 使得现有保护措施无法有效应对快速发展的数据环境。

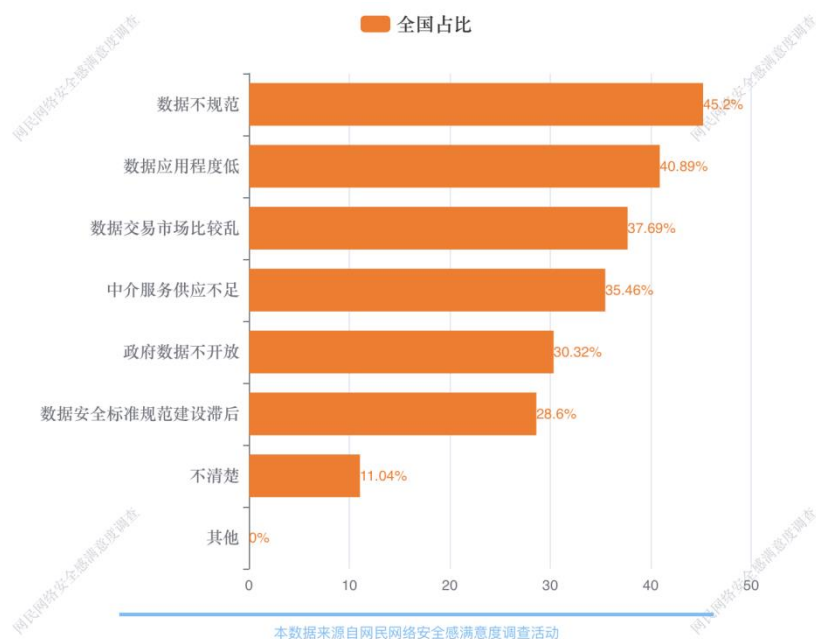


图 5-1 数据安全保护现状存在的问题

（二）数据规范作为首要问题仍未得到有效解决

根据调查结果显示，去年的首要数据安全一大问题“数据不规范”在今年的受访者比例中仍有上升的趋势，占 45.2%，数据市场仍然比较混乱，这些问题仍然是各界需要着重关注和解决的问题，主要原因在于采集、存储、使用等多项数据环节仍然没有十分清晰的边界，从而使得滥用、丢失个人数据等问题出现。另一方面也与网民的数据意识得到提高有关，今年调查中选择“不清楚”的受访者为 11.04%，较去年已下降了 5.31；同时，选择“其他”的受访者仅为 0%。数据安全的相关普及得到了提高，也使得受访群体更明晰自身受到的数据安全风险。

（三）数据应用程度未能跟上发展步伐

在信息化社会中，数据的生成与流通已无处不在。从各大平台迅速收集的用户信息，到产业数字化转型的加速，网络空间中数据的产生量持续上升。然而，数据应用的效率和水平并未与此相匹配，成为限制数据价值发挥的瓶颈，发展差距有逐渐扩大的趋势。今年的调查显示，40.89%的受访者认为数据应用程度低，较去年有所上升。这一结果反映了公众对当前数据应用状况的不满与期待。随着人工智能的快速发展，数据的价值愈加凸显，但同时也带来了新的挑战。AI 技术的广泛应用要求数据具备更高的质量和适用性，确保数据的准确性和完整性成为提升应用效率的关键。此外，AI 的决策过程往往依赖于海量数据，这使得数据的合理合规使用显得尤为重要。数据不仅仅是数量的积累，更需要创造足够的应用场景以提升

用户体验。因此，我们需要从多个角度入手，全方位、多层次地推进数据全链条的建设，以应对 AI 技术带来的机遇与挑战。

（四）中介服务供应不足成为 2024 年网民日益关心的问题

随着个人信息保护和数据安全问题的日益突出，“中介服务供应不足”问题的显著上升一个重要原因可能是网民对中介服务的需求不断上升。许多人希望通过专业中介来确保自己的数据安全，避免信息泄露或滥用。然而，市场上中介服务的供应却未能跟上这一需求，导致用户在保护个人信息时感到无助和不安。其次，数字化转型的加速使得各类应用和平台对数据处理的要求更加复杂。网民需要中介在数据交易、信息认证等方面提供专业支持，但由于中介服务的供应不足，导致用户在使用各种数字服务时面临更多风险。此外，部分中介机构的服务质量不高，缺乏有效的监管机制，使得用户对中介服务的信任度降低。这种信任缺失使得用户对中介的依赖性增强，却又因服务不足而感到失望，从而引发更大的关注和担忧。

另一方面也可以反映出：公众对数据权益保护的意识提升，促使他们更加关注中介服务的角色和功能。随着对个人信息保护法规的了解加深，网民希望中介能够在维权过程中发挥更积极的作用，以更好地保护他们的利益。

（五）加强数据安全保护需要多方合作与责任落实

在数据安全保护方面，受访者认为应重点关注以下几个方面。首先，国家应加强立法，进一步保护个人信息安全，社会组织和行业协会需要强化对个人信息保护的培训与宣传，促进公众对数据安全的认识。此外，企业也应减少对非必要个人信息的收集和使用。另外，监管部门方面，增加更多渠道以通报违法收集者信息的措施被 42.89% 的受访者认为重要。同时，设立更多举报平台，让公众能够方便地申诉。最后，建立 APP 个人信息保护合规认证和监控制度，要求持证上线并对违规者采取停牌措施。

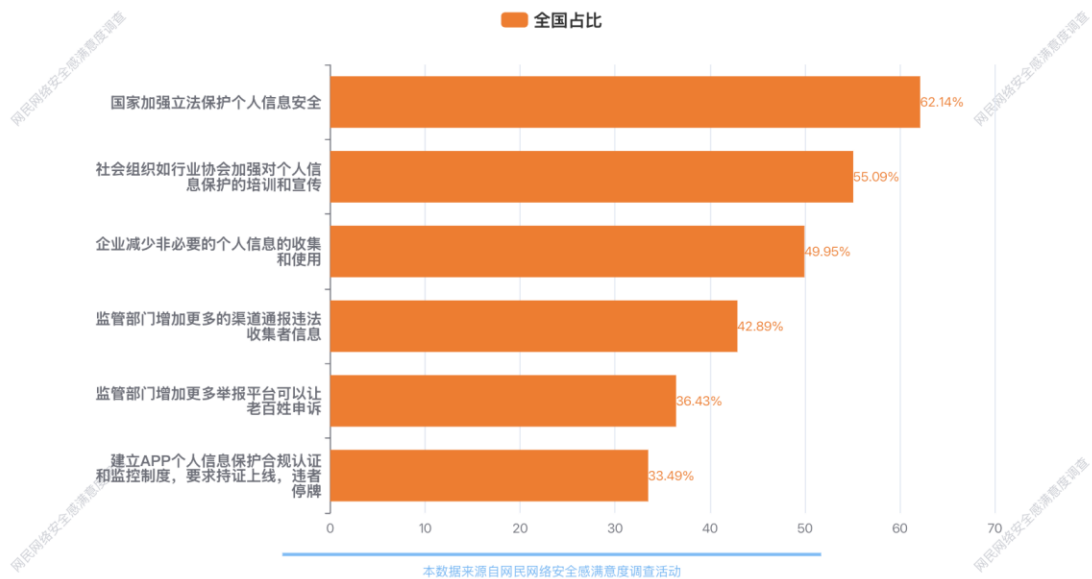


图 5-2 网民认为数据安全保护的解决方向

六、网民对个人信息保护和数据安全的建议和期望

（一）公众网民仍然期待宣传教育的加强与普及

在公众网民对于个人信息保护和数据安全治理的期望中，宣传教育的加强与普及仍然是重要的诉求。62.27%的受访者希望提升网民的维权意识和能力，这一需求反映了他们对自身权益的关注。诚然，在信息化社会中，面对日益复杂的数字环境和潜在的隐私风险，公众渴望获得更全面的知识，帮助他们识别和应对个人信息泄露和滥用的风险。同时，这种期待也是在各种数据使用场景日益普遍的背景下，对信息安全的高度重视。网民希望能够从自身出发，提升自我数字素养，从而在实际生活中采取有效的自我防护措施。

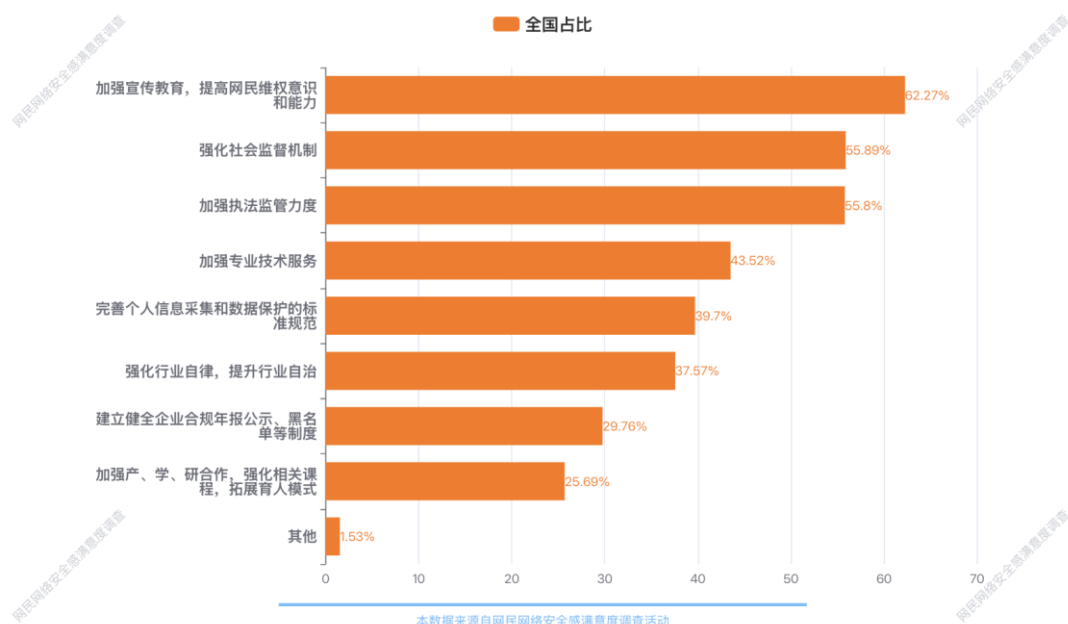


图 6-2 网民对加强个人信息保护和数据治理的期望情况

（二）数据安全保护集中在三个层面

根据调查结果，加强数据安全保护的重点应着眼于政府、企业、社会三个层面。政府在数据安全的保护中起到中流砥柱的作用。受访者把强化社会监督机制放在保护措施的第一位（55.89%）以便更有效地监督数据安全治理，55.80%的受访者强调了加强执法监管力度的重要性，认为应对违法行为采取更加严厉的措施。同时，进一步完善个人信息采集和数据保护的标准规范，以确保数据处理的规范性与合法性。

此外，建立健全企业合规年报公示、黑名单等制度，以促进企业的透明度和责任感。加强在专业技术方面的服务，以提升数据保护的技术能力。强化行业自律、提升行业自治的建议，显示出公众对行业自我管理的期待。最后，应加强产、学、研合作，强化相关课程，拓展育人模式，以培养更多具备数据安全治理能力的人才。

（三）在数据安全保护上，公众网民期待的重点是规制力度的提高

随着信息技术的快速发展和数据生成的爆炸性增长，数据泄露和滥用事件频频发生，使公众对个人信息安全的担忧加剧。在这一背景下，网民希望通过更加严格的法律法规来保护自身的隐私和数据安全，主要由于法律不仅是一种规范，更是一种保障，能够有效约束个人信息的滥用行为。随着数据泄露事件的频发和公众对个人隐私的重视，增强法律的约束力变得尤为重要。严格的法律规定能够为企业和组织设定清晰的界限，促使其在处理用户信息时遵循更高的标准。

互联网中浮现的网络诈骗、个人信息泄露、大数据宰熟等问题，不仅损害了网民的合法权益，也影响了互联网的健康发展。公众普遍对大数据环境下的个性化推送和价格歧视等现象感到不满，认为企业在获取和使用个人信息时往往缺乏透明度和责任感。这种情况下，强化监管和提高规制力度成为提升企业合规意识和社会责任的重要手段。公众的维权意识也随着对网络数据隐私安全保护知识普及日益增强，他们渴望在面对数据安全问题时拥有更多的保障和支持。互联网安全治理不仅能保护个人信息，还能为公众提供一个更安全和可信的数字环境，从而重建对互联网的信任。

七、提高网民个人信息保护和数据安全的对策

（一）明确平台数据收集的限度，提升个人数据保护自主权

在数字化深入发展的背景下，明确平台数据收集限度、提升用户对个人数据的自主控制权已成为保障网络安全与个人隐私的关键。这不仅关系到用户在数字环境中的安全感，也直接影响公众对平台、企业乃至国家治理的信任度。为避免个人信息在未经授权的情况下被滥用，数据收集的范围和限度亟需明确规范。公众对应用程序要求过多权限产生担忧，尤其是注册 APP 账户时获取隐私权限的情况，被认为是最主要的泄露途径，达到 61.93%。并且公众普遍认为社交应用和网络媒体等平台存在滥用个人信息的情况。相关平台应遵循“最小、必要”原则，严格控制收集的数据类型和范围，尤其是对敏感信息如地理位置、设备信息、生物特征等进行分级管理。通过增加数据收集的透明度，设置必要的授权提醒与撤回机制，保障用户在数字环境中随时掌控数据流向。从国家层面看，规范平台数据收集限度、保障用户数据控制权既是对《个人信息保护法》等法律法规的落实，也是提升国家数据安全治理能力的有效举措。通过构建系统性的个人数据保护框架，国家可以为用户、企业和社会建立一个安全可信的数字环境，增强网民的网络安全意识和自我保护能力。最终为实现国家数字化战略、推动数字经济高质量发展提供有力保障。

（二）善用人工智能等前沿技术，架构数据主动保护体系

人工智能前沿技术具备快速分析海量信息、精准识别威胁的强大能力，将其应用于数据安全领域，不仅可以实时检测、识别潜在的安全风险，还能自动采取相应措施以防止数据泄露和滥用。因此，善用人工智能技术架构数据主动保护体系，不仅是应对当前隐私和安全挑战的必然选择，更是保障数字经济可持续发展的关键途径。通过政府、企业、个人多方协同联动，构建能够对数据安全实施全方位的检测系统，实现个人敏感内容泄露实时检测，并支

撑实际场景下对伪造数据与不良信息的同步审查和精准溯源,及时消除对我方不利的伪造信息隐患。善用大模型的强推理能力,常态化构建漏洞储备库,归纳漏洞机理共性,全面提升我国的数据保护能力。与此同时,推进隐私计算技术的普及应用,使数据在“可用不可见”的前提下实现共享和利用,最大限度地减少对个人隐私的侵害。构建全面的智能化数据安全体系是重要的发展趋势之一。这不仅是提升网络安全治理水平的重要支撑,更是国家在全球数字化竞争中实现领先优势的有力保障。通过加大对人工智能数据安全技术的研发投入和政策支持,形成国家级的智能数据保护生态体系,进一步提升我国在数据安全治理上的话语权,为构建可信赖的全球数字经济环境贡献中国方案。

（三）加大规范数据市场的力度，促进数据流通的合法性

数据作为关键生产要素的市场价值日益凸显,数据的有效流通已成为推动创新和经济增长的重要动力。然而,根据调查结果显示,去年的首要数据安全一大问题“数据不规范”在今年的受访者比例中仍有上升的趋势,占 45.2%。公众仍能接到各类中介推销电话,占比 64.88%;大数据杀熟现象更是愈演愈烈,占到了 44.12%。这对公众的隐私安全带来了严峻挑战。要充分释放数据要素的经济潜力,必须加大对数据市场的规范力度,建立起合法、安全、有序的流通机制,确保数据交易在合法合规的前提下进行。为实现这一目标,应推动构建一套标准化的数据交易规则,明确数据采集、处理、流通的规范。强化交易数据的审核与验证机制,可以引入权威第三方机构进行监督,确保交易双方的数据来源和用途清晰合法。同时,建立数据使用溯源系统,实现对数据全生命周期的追踪管理,避免数据被用于未经授权的用途,减少违规行为。此外,探索建立数据交易的合规审查制度,使各类企业和组织在合法的框架内共享数据,实现数据资源的最大化利用。多维度规范数据市场、促进合法流通,提高数据交易的透明化和合法化,保障数据安全的同时能够提高市场信任度。国家为数据要素市场的健康发展提供了坚实的制度基础,但仍需社会各界的努力,增强自律和责任意识,共同维护数据交易市场,有力保障数据的安全流通和合理应用。

（四）多渠道普及信息安全教育，疏通信息保护诉讼流程

个人信息安全已成为公民权益的重要组成部分。然而,公众对信息安全的认知和应对能力相对不足,据调查显示,多达 64.43%的人表示“不了解”《个人信息保护法》个人信息保护公益诉讼制度中的新规定。信息保护诉讼流程亦存在流程繁琐、耗时较长等问题,难以满足公众的快速维权需求。57.24%的受访者指出诉讼过程漫长且成本高昂是一大主要障碍,许多人因此望而却步,难以积极参与维权。62.27%的受访者希望提升网民的维权意识和能力。因此,多渠道普及信息安全教育、优化信息保护诉讼流程已成为保障公民信息

权益、提升社会整体信息安全水平的关键任务。首先，应通过线上线下多种渠道普及信息安全知识，提升公众对隐私保护的意识和自我防护能力。政府、学校、企业等可通过网站、社交媒体、宣传活动等方式传播信息保护知识，帮助公众了解信息泄露的风险和应对策略，为全民构建起全面的信息安全认知体系。在此基础上，需简化并疏通信息保护诉讼的流程，降低公众维权的门槛。例如建立一体化信息安全联动平台，便于用户在信息泄露事件发生时快速投诉和维权。整合政府监管、企业自律和用户反馈功能，形成多方参与的联动机制，提升隐私事件的处理效率和透明度。通过多方合力推进信息安全知识的普及和诉讼流程的疏通，在全社会形成信息安全的广泛共识，提高公民的信息安全参与感和获得感。这一举措将为构建安全、可信的数字社会提供坚实的基础，增强公民对信息时代的信任感和安全感。



网安联微信公众号



网安联微信小程序



“网络安全共建网”官网

网安联秘书处

官网:www.iscn.org.cn

电话:020-8380 3843/13911345288

邮箱:cinsabj@163.com