2022年
全国网民网络安全感满意度
调查专题报告

个人信息保护和数据安全专题

教育部哲学社会科学实验室—— 中国政法大学数据法治实验室
中国政法大学数据法治研究院

2022年10月

本报告数据来源于2022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:

2022 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

教育部哲学社会科学实验室——中国政法大学数据法治实验室

中国政法大学数据法治研究院

2022 年 10 月

目　录

一、加强个人信息保护和数据安全治理的背景

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， 全面了解网民群众对网络安全现状的看法和意见建议， 由 135 家网络安全行业协会及相关社会组织共同发起，开展了为期 10 天的 2022“网民网络安全感满意度调查活动” 。该活动是国内调查范围最广、参与人数最多的全国性、公益性网络安全社会调查。此次调查活动于 2022 年 8 月 3 日开始启动，共收集到了 303.1776 万份有效样本采集量，其中公众网民版 2469089 份，从业人员版 562687 份。

此次发布的调查主问卷共设置了九个专题二级问卷， 分别是网络安全法治社会建设、网络诚信建设、遏制网络违法犯罪行为、个人信息保护和数据安全、网络购物安全权益保护、特殊人群(未成年人、老年人等) 网络权益保护、互联网平台监管与企业自律、数字政府服务与治理能力提升、网络暴力防控与网络文明建设。其中“个人信息保护和数据安全”作为二级问卷之一， 围绕个人信息保护和数据安全问题共设置了十五个问题。 基于此次调查所获数据， 教育部哲学社会科学实验室—— 中国政法大学数据法治实验室、中国政法大学数据法治研究院围绕本专题， 分别对网民对个人信息保护和数据安全的感受情况、网民对个人信息和数据风险反馈情况、我国个人信息保护和数据安全法治建设现状、数据安全保护存在问题、 网民数据安全诉求五方面进行分析，并对如何加强网民个人信息保护和数据安全提出建议意见，最终汇总形成“个人信息保护与数据安全”专题报告。

网络空间以多种方式融入人类社会， 对全球政治、 经济、科技、文化、社会、国防军事等领域的影响越来越深刻。网络安全已成为深刻影响公民生活、个人隐私、公众经济繁荣和国家安全的根本性问题。网络安全事件可以是任何类型的计算机网络攻击、与计算机相关的犯罪以及对网络资源的滥用或误用， 可以定义为导致威胁或损害的恶意行为、事件或情况。如何防范和化解网络安全风险已成为新时代亟待解决的重大问题。

随着 5G、物联网等技术发展普及， 不断改变网络连接方式和连接对象，物

理空间和网络空间的边界不断融合、模糊，内生式网络安全问题不断产生，数据正在成为继传统安全问题之后影响网络安全的命脉。国家互联网信息办公室于2021 年 11 月 16 日颁布的《网络安全审查办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，可见作为信息化社会基本构成单位的数据对网络安全的重要性。 网络治理问题很大程度上已经凸显为数据治理问题，网络安全问题正在不断聚焦成为数据安全问题。

当前，全球大数据产业正蓬勃发展， 技术演进与应用创新并驾齐驱。非关系数据库、分布式并行计算、机器学习和深度数据挖掘等数据存储、计算和分析新技术已经出现并迅速发展。 随着数据成为一种与劳动力、 土地、资本、 技术等要素并列的新型生产要素，数据逐渐成为我国的基础性战略资源和生产基石。然而，越来越多的信息与数据安全问题暴露出来，全球发生的数据安全事件数量呈上升趋势，个人信息保护和数据安全治理已成为各国发展的重要命题。尽管各国已采取行动解决已经出现或可能出现的数据安全治理问题， 在个人信息保护、公共数据开放、流通数据监管、国家数据主权维护等多方面加强立法并落实相关措施，但数据安全威胁仍普遍存在于数据产业链的数据生成、采集、处理、共享等各个环节。其成因是复杂多方面的， 从外部攻击到内部泄露，从技术漏洞到管理缺陷，从新技术到新模式带来的新风险，以及传统安全问题都在不断地反复出现。在区块链、元宇宙、全息互联网等概念再一次席卷新的技术革命之时，如何最大程度降低数据风险、保护个人信息、 维护网络安全、 坚守国家主权， 是用户“可读可写可拥有”的 web3.0 时代必须破解的关键命题。

二、2022 年参与专题调查公众网民对个人信息保护和数据安全的感受情况

作为网络安全的重要组成部分， 信息与数据已经深入社会公众的日常生活，并切实影响公众的相关利益。公众与网民对我国个人信息保护和数据安全治理的直观印象与整体评价，是衡量与评估公民个人信息保护与数据安全治理的重要指标与参照系。

（一）参与调查的公众网民对我国个人信息保护的整体评价有所提升

根据 2022 年参与调查的公众网民对个人信息保护现状的评价数据显示，与

2021 年的“三三分”态势相比，公众网民对我国个人信息保护评价整体上呈现逐渐好转态度，40.37%的受访人群认为当前我国个人信息保护的状况“比较好”乃至“非常好”；36.7%的受访人群认为当前状况 “一般”；22.93%的受访人群认为当前状况“不太好”或“非常不好”。

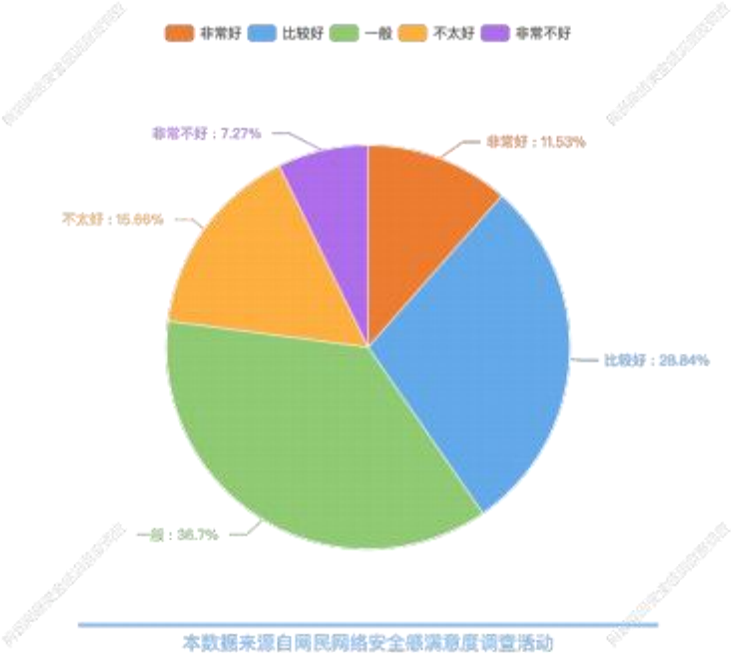

图 3-1：网民对个人信息保护现状的评价

（二）参与调查的公众网民对个人信息泄露的感知情况强烈

根据 2022 年参与调查的公众网民对个人信息泄露的感知情况数据来看，近一年来，多达 40.36%的受访人群遭遇“比较多”甚至“非常多”信息泄露；37.65%的受访人群感觉到 “有一些”信息泄露；仅有 21.998%的受访人群近一年来“没有遇到”或“很少遇到”个人信息泄露。

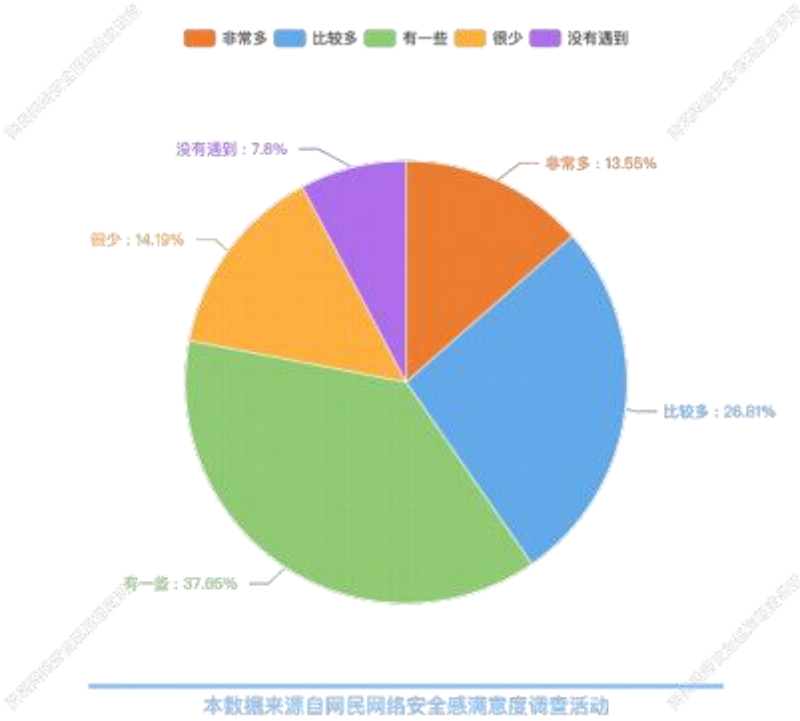

图 3-2：近一年网民对个人信息泄露的感知情况

（三）参与调查的公众网民在多场景感知到个人信息风险

由于受到不同程度骚扰，公众网民通常藉此怀疑或确认个人信息被泄露或被滥用，判断自身个人信息风险。根据 2022 年参与调查的公众网民对其所遇到的能够确认个人信息泄露的情况反馈数据，骚扰类型以非需求推销居多， 75.45%的网民表示接到各类中介的推销电话； 58.32%网民收到垃圾邮件，55.92%收到相关性的推销短信。除此以外，42.44%的公众网民还通过大数据杀熟来判断个人信息泄露，36.6%的网民认为默认勾选同意《服务协议》会导致个人信息泄露，25.53%的网民将收集信息时告知不明确视为个人信息风险来源点，22.84%的网民根据利用优势地位强制收集用户信息来推测个人信息风险，20.25%的网民认为匿名注册却被熟人加好友的情况属于个人信息泄露等。

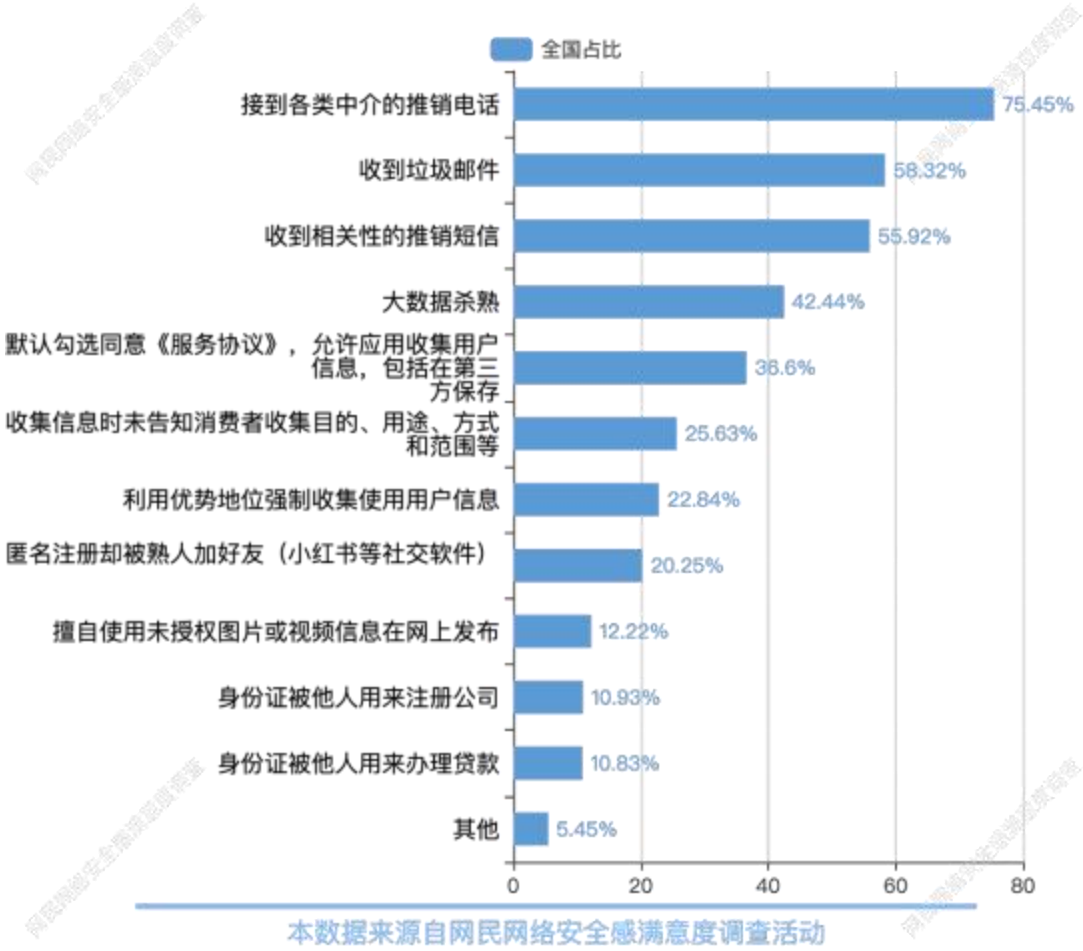

图 3-3：网民遇到的能够确认个人信息泄露的情况

（四）参与调查的公众网民对生物识别信息风险关注度提升

使用生物识别技术（如人脸识别、 身份识别）进行身份认证已成为社会生活的常态，但随着窃取个人信息手段的技术不断发展,个人生物识别信息也逐渐成为信息泄露的新内容， 网民对此类信息的利用充满忧虑。根据 2022 年参与调查的公众网民对生物识别技术泄露个人信息的主观倾向数据显示，59.16%的网民对生物识别技术的安全性“比较”或“非常”担心，较之 2021 年的 57.96%仍在上升；25.05%的网民态度“一般”，无明显倾向； 仅 15.78%的网民对生物识别技术的安全性“很少”或“没有”担心，比起 2021 年的 16.94%又进一步下降。

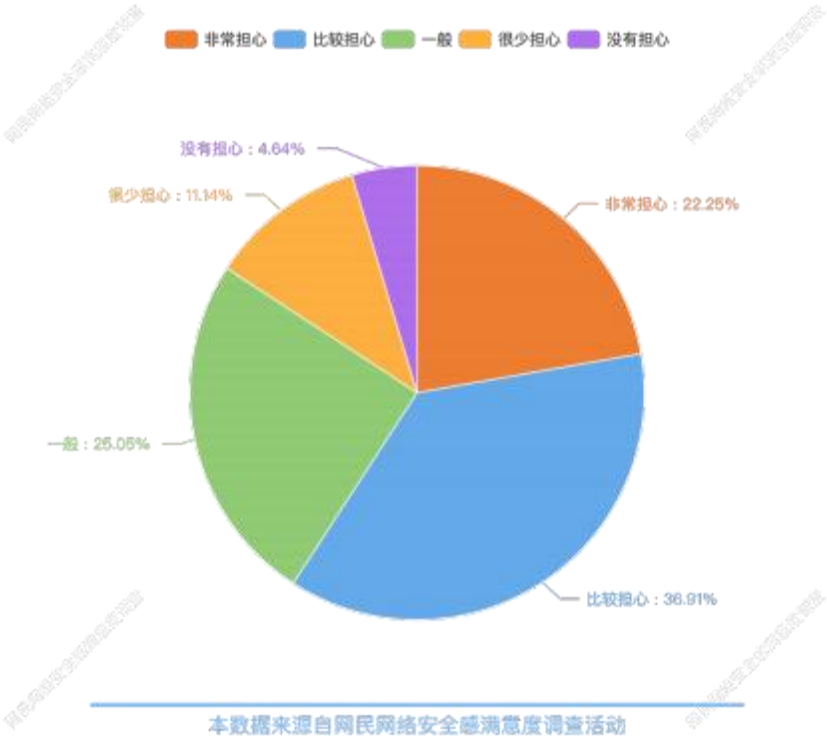

图 3-4：网民对生物识别技术泄露个人信息的主观倾向

出于对生物识别信息风险的担忧，网民在选择线上支付方式时仍主要选择非生物识别信息的支付验证方式，超过八成网民采用密码支付，仅半数采用指纹支付，只有四成采用刷脸支付，约三成采用短信验证，还有一成网民采用免密支付。

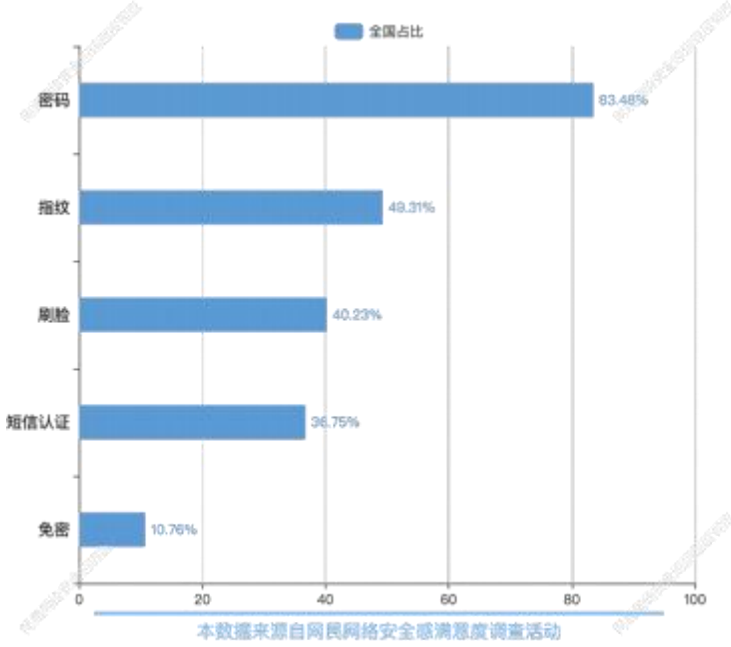

图 3-5：网民线上支付时选择的身份认证方式

（五）参与调查的逾半数网民肯定 APP 运营者对个人信息保护的改进

《数据安全法》出台后，APP 等非法采集、 滥用用户数据进一步约束，APP 运营者因此着力加强对用户的个人信息保护工作。 根据 2022 年网民网络安全满意度的调查数据， 51.43%的网民认为其工作有“明显改善”或“有所改善”，44.85%的网民认为其工作“一般”，仅有 3.72%的网民认为《数据安全法》出台后其工作反而 “有所变差”或 “明显变差”。

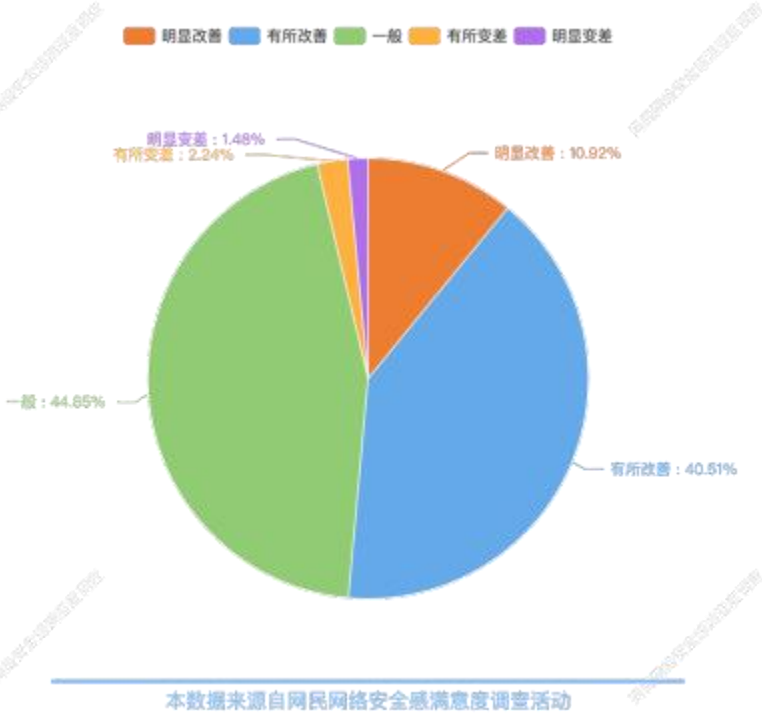

图 3-6：网民对 APP 运营者在个人信息保护方面是否改善的感受情况

三、2022 年参与专题调查公众网民对个人信息和数据风险反馈情况

（一）参与调查的网民对各类网络服务的个人信息风险感受不一

参与本次调查的公众网民认为不同类型网络服务的个人信息风险不同， 其中， 社交应用类网络服务(实时通讯、短视频等) 的个人信息风险最高，56.88%的网民认为其存在风险；同时，网民认为， 电子商务类网络服务(网络购物、网上支付、网上银行等)、网络媒体类网络服务(新闻信息、网上阅读、视频直播等)、生活服务类网络服务(搜索引擎、导航、网约车、旅游、美图)和数字娱乐类网络服务 (网络游戏、网络音乐、网络视频) 存在较高程度的个人信息风险，而健康医疗类网络服务、网上办公类网络服务以及电子政务类网络服的个人信息风险相对较低。

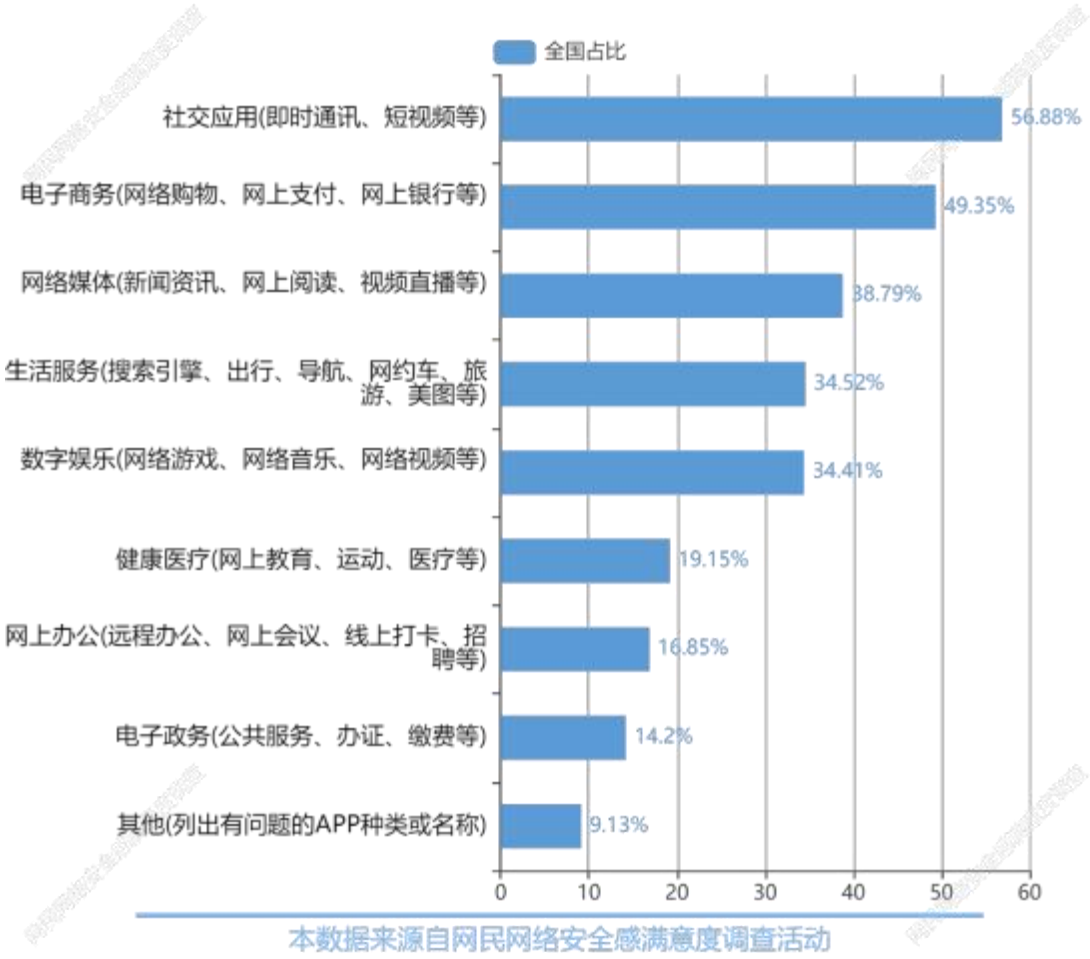

图 4-1：个人信息保护情况受关注的 APP 类型

（二）参与调查的网民认为个人信息泄露发生在多个环节

在参与调查的公众网民中，认为最可能泄露个人信息的途径是注册 APP 时，APP 要求获取相机、位置等隐私权限，占比高达 73.49%；其次， 50.3%的受访群体认为参与网上测试、投票、抽奖活动可能会导致个人信息泄露；近四成网民认为点击网上不明二维码、链接和使用公共 wife 可能会泄露个人信息。相比其他泄露个人信息的途径，注册 APP 要求开放隐私权限意味着用户陷入被动境地，并且涉及重要的个人信息， 即使违背用户意愿也不能被有效反制， 因而用户对此有更强烈的痛感。

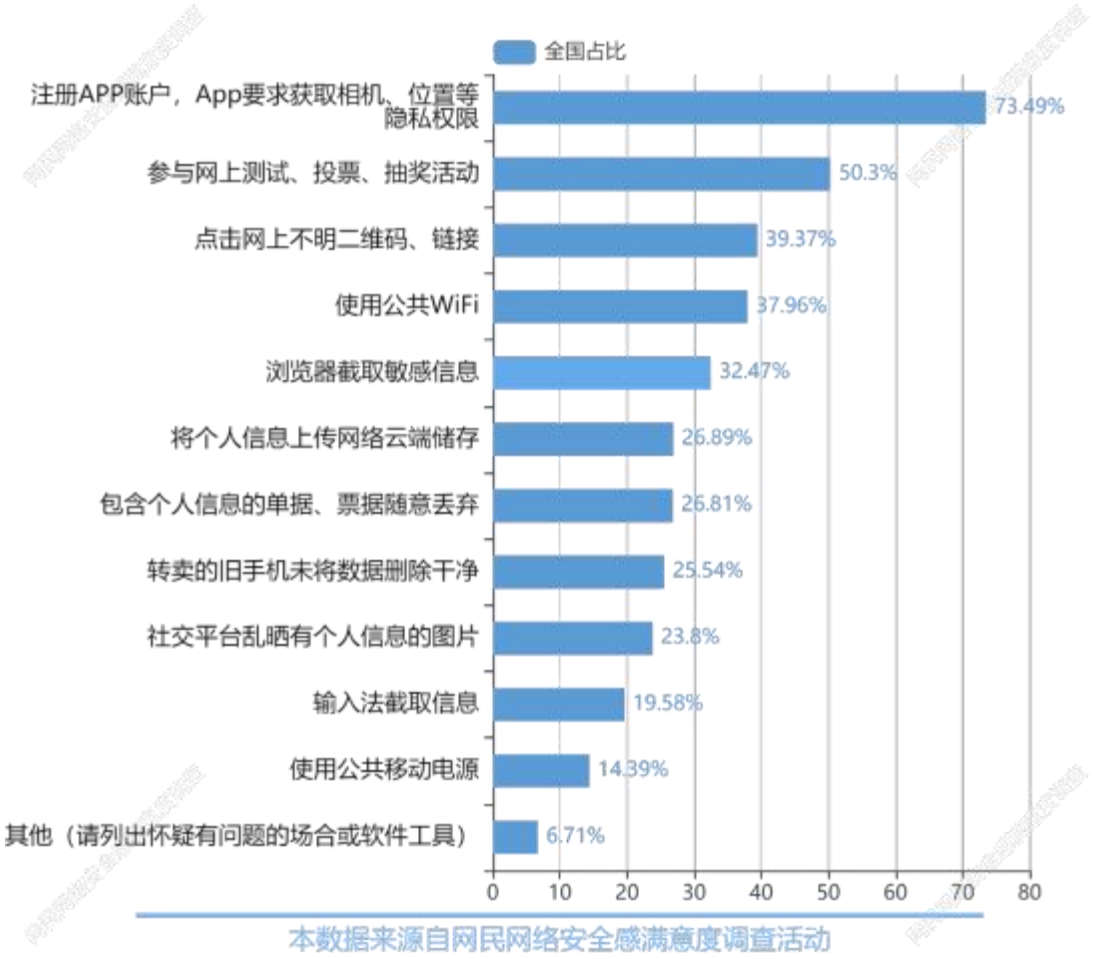

图 4-2：网民认为可能的个人信息泄露途径

（三）参与调查的网民认为 APP 存在多种违规收集个人信息问题

APP 收集信息超过必要限度， 索取无关信息和无关权限，漠视用户知情同意权，是公众网民最常遇到的问题。根据本次网民网络安全满意度调查显示，56.47%的受访群体遭遇过 APP 收集与功能无关的个人信息；53.01%的受访群体遭遇过 APP 频繁索要无关权限；47.16%的受访群体遭遇过 APP 默认捆绑功能并一揽子同意；45.28%的受访群体遭遇过 APP 强制索取无关权限，不授权就闪退。

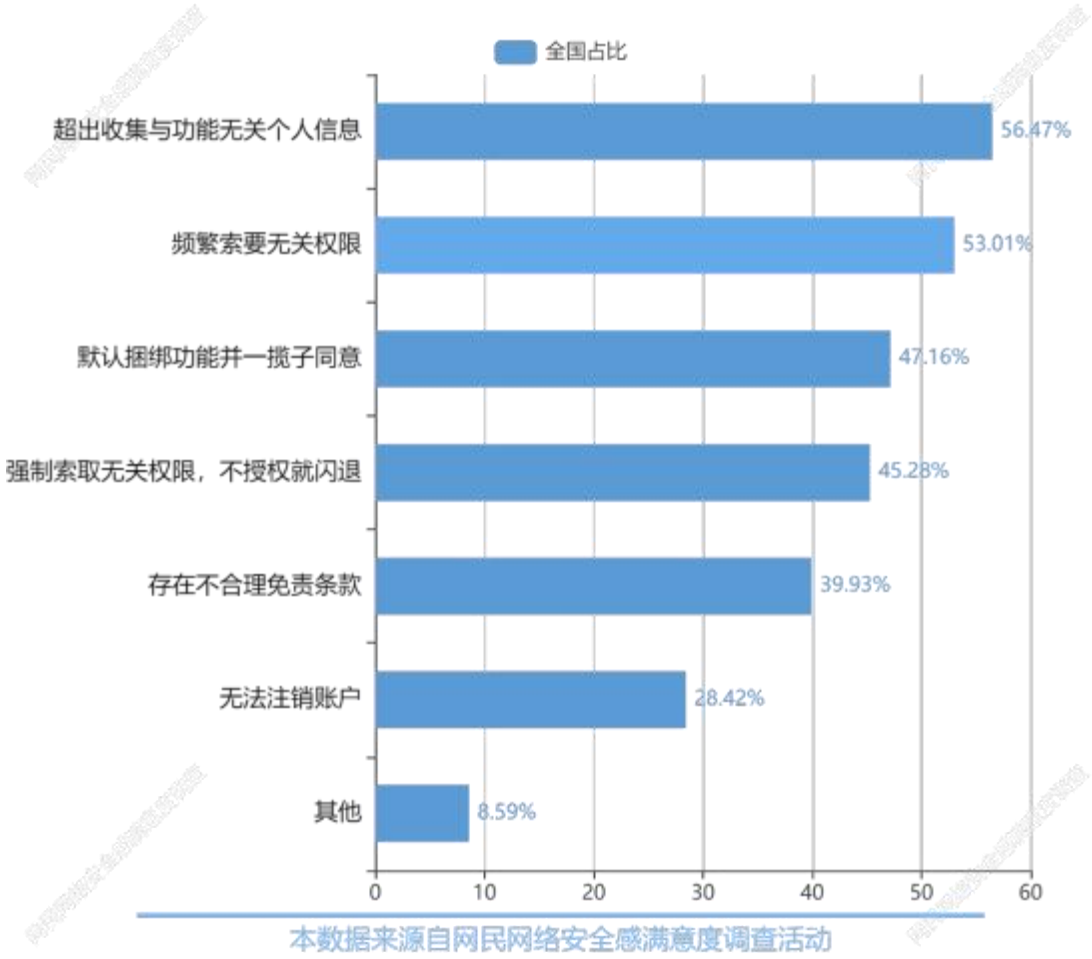

图 4-3：网民认为 APP 收集信息过程中存在的问题

（四）参与调查的网民认为精准广告推送存在重大个人信息安全隐患

大部分网民在日常上网时都会收到精准广告，精准广告需要使用用户的个人信息， 但用户的同意权是否得到了有效保障存疑。本次网民网络安全满意度调查显示， 95.04%的网民在日常上网时收到过精准广告， 13.54%的网民很少或者没有收到过精准广告。在广告推送的过程中 39.72%的网民表示网络服务经营者全部都没有征得同意即向用户发送广告；22.01%的网民表示经营者大部分都没有征得用户同意；还有 19.68%的网民不清楚发送广告是否征得过其同意。

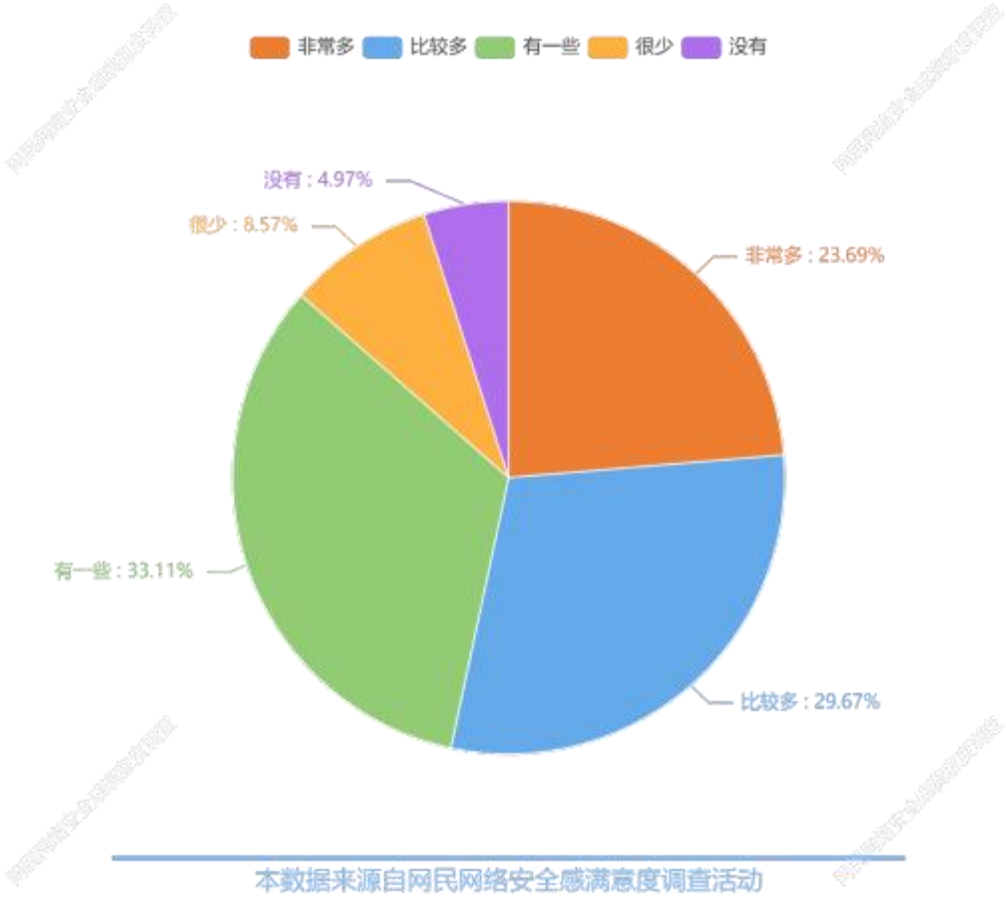

图 4-4-1：网民在日常上网时都会收到精准广告的情况

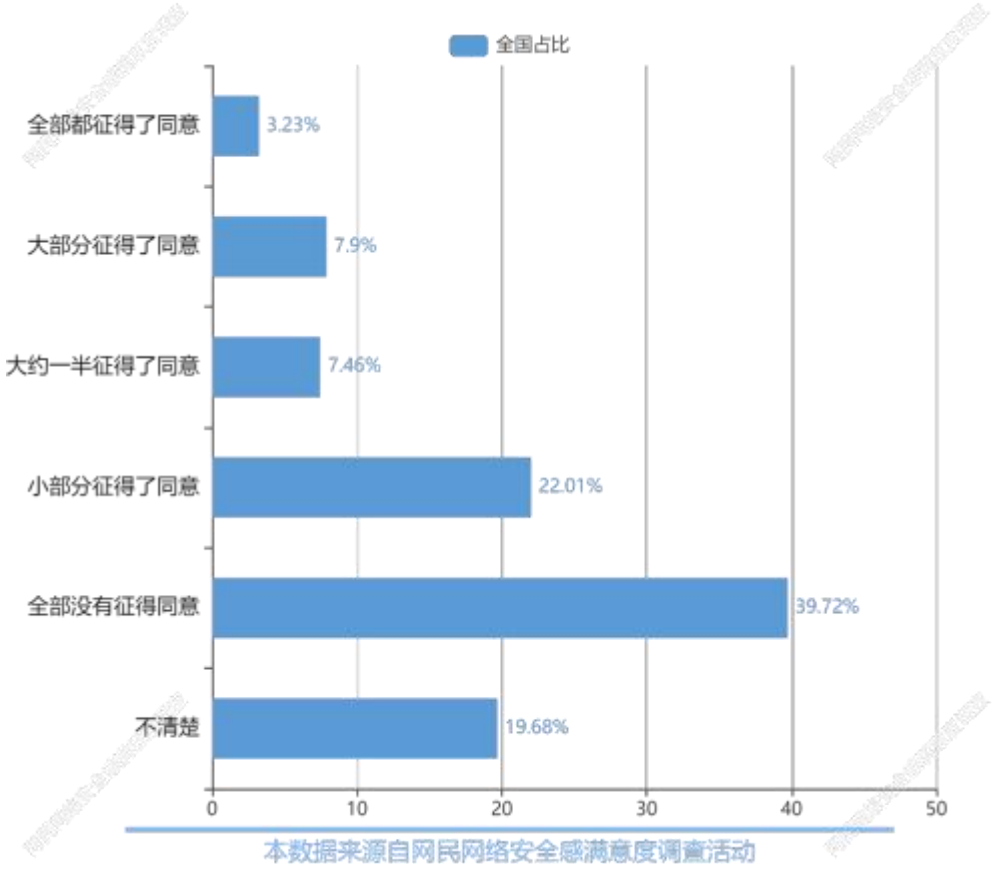

图 4-4-2：经营者发布精准广告征得网民同意的情况

不仅如此， 精准广告的退出机制缺失也对网民产生极大困扰。在参与调查的公众网民中， 31.06%的网民不清楚其收到的精准广告是否提供了退出机制；32.77%的网民表示大部分甚至全部精准广告都没有提供退出机制；11.05%的网民表示大约一半精准广告提供了退出机制。分析发现， 网络服务经营者发送精准广告大部分未征得用户同意， 并且缺乏退出机制或者未提供显著的退出机制标识，网络服务经营者不合理使用用户个人信息的情况较为严重。

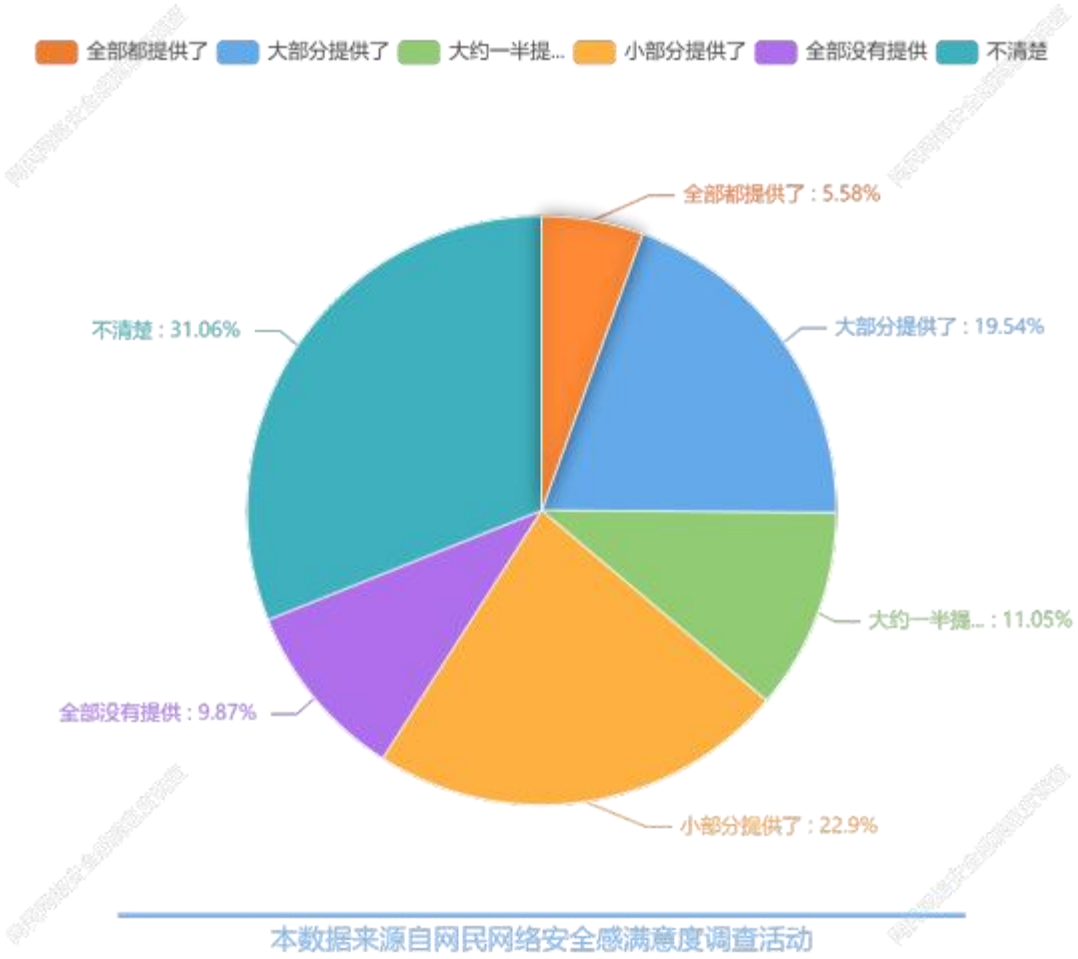

图 4-4-3：精准广告退出机制的提供情况

四、我国个人信息保护和数据安全法治建设现状

2022 年 1 月， 国务院印发《“十四五”数字经济发展规划》，部署了八方面重点任务， 其中包括“着力强化数字经济安全体系”，再次从国家顶层设计层面强化网络安全重要地位。自从 2016 年《网络安全法》出台以来， 在总体国家安全观框架下，《网络安全法》与 2021 年相继出台的《数据安全法》和《个人信息保护法》共同构成了我国数据新秩序下的三根支柱。与此同时，随着《关键信息基础设施安全保护条例》《网络安全审查办法》等法律法规正式实施，国家网信办相继对外发布《数据出境安全评估办法(征求意见稿)》《网络数据安全管理条例（征求意见稿)》等并公开征求意见，网络安全领域立法大为充实，网络安全领域配套规则逐步明确清晰，为网络安全相关工作提供了确定的指引。

在个人信息保护层面， 以《个人信息保护法》统领全局，各领域分散立法、出台规章对其进行重要补充。其一， 2021 年 8 月 20 日通过的《个人信息保护法》

对个人信息保护进行了整体安排和制度重构，立法目的既包括对个人信息的保护， 也包括个人信息合理利用，规定了个人信息处理的合法性基础、个人信息处理者的义务、个人在个人信息处理活动中的权利、个人信息保护监管体制等主要内容， 基本覆盖了个人信息保护的各个方面。 同时，《网络安全法》《民法典》以及相关行业、 领域的多部法律中都涉及到个人信息保护条款。其二， 在用户个人信息保护的关键领域，国家互联网信息办公室等四部门于 2021 年 3 月 12 日联合印发 《常见类型移动互联网应用程序必要个人信息范围规定》，明确 39 类 APP 必要个人信息范围，为开展 APP 治理提供了可靠的法律保障； 11 月 1 日， 工业和信息化部再次印发《关于开展信息通信服务感知提升行动的通知》，要求相关企业建立已收集个人信息清单和与第三方共享个人信息清单，并在 APP 二级菜单中展示，方便用户查询；2022 年 5 月 7 日， 工信部公示《APP 收集使用个人信息最小必要评估规范》等行业标准，规定了 APP 收集使用个人信息的最小必要基本原则、评估要求、评估方法以及评估流程。其三，对于个人信息跨境处理活动，国家信息安全标准化技术委员会于 2022 年 6 月 24 日公布了《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》，规定了个人信息跨境处理活动的基本要求和个人信息主体权益保障要求；6 月 30 日， 国家互联网信息办公室公布《个人信息出境标准合同规定（征求意见稿）》，规定个人信息处理者在符合条件情况下可以通过签订标准合同的方式向境外提供个人信息。其四，在司法领域，最高人民法院于 2021 年 7 月 28 日发布了《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》，从人格权和侵权责任角度，明确了滥用人脸识别技术处理人脸信息行为的性质和责任；最高人民检察院于 2021 年 8 月 21 日下发《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》，指出要深刻领会个人信息保护法设置公益诉讼条款的重要意义，推动公益诉讼条款落地落实。

在数据安全治理层面， 以统摄性的《数据安全法》与行政法规、地方性法规、政策性文件等共同构成数据安全治理法律体系。其一， 2021 年 6 月 10 日通过的《数据安全法》对数据分类分级、重要(核心) 数据管理、数据安全审查等作出了明确规定，成为我国数据安全领域基础性法律；通过各项基础制度强化对国家

利益、公共利益和个人、组织合法权益的保护， 为开展数据处理活动的组织、个人以及数据交易中介服务机构、负有数据安全保护义务的国家机关及国家机关工作人员等主体提供明确法律依据；并在《网络安全法》的基础上，完善了跨境数据流动的管理要求，回应了关键信息基础设施以外的重要数据的跨境管理诉求。其二，关于配套立法，国家互联网信息办公室于 2021 年 11 月 14 日发布《网络数据安全管理条例(征求意见稿)》，对网络数据处理活动中涉及的个人信息保护、重要数据安全管理、跨境数据流动规范等内容进行了全方位、多层次的细化规定；国家市场监督管理总局、国家互联网信息办公室于 2022 年 6 月 9 日联合公布《数据安全管理认证实施规则》，鼓励网络运营者通过认证方式规范网络数据处理活动， 加强网络数据安全保护， 规定数据安全管理认证的认证模式为：技术验证+现场审核+获证后监督。其三，在数据安全具体领域，2021 年 7 月 5 日， 国家互联网信息办公室会同国家发展和改革委员会、 工业和信息化部、公安部、 交通运输部制定出台《汽车数据安全管理若干规定（试行)》，对汽车数据处理活动中的重要数据和个人信息予以保护， 维护国家安全、数据安全和个人权益；2022 年 2 月 10 日， 工业和信息化部公布《工业和信息化领域数据安全管理办法(试行)》（征求意见稿)，规定工业和信息化领域数据处理者应当对数据处理活动负安全主体责任，对各类数据实行分级防护， 不同级别数据同时被处理且难以分别采取保护措施的， 应当按照其中级别最高的要求实施保护， 确保数据持续处于有效保护和合法利用的状态；2022 年 4 月 7 日，信安标委公布《信息安全技术 大数据服务安全能力要求（征求意见稿)》，规定了大数据服务提供者的数据服务安全能力要求，包括组织管理安全能力、数据处理活动安全能力和数据服务安全风险管理能力。其四，针对跨境数据流动规则，国家互联网信息办公室于 2022 年 5 月 19 日颁布《数据出境安全评估办法》，细化和明确了我国跨境数据安全自由流动的具体规则； 其五， 各省市加快制定地方数据条例，立足本省的数字经济发展与数据安全现状，对《数据安全法》的宏观规定加以实践性细化。

此外，对于新兴的区块链等算法技术，近年来的立法也有明显增多。 2021 年 11 月 16 日，国家网信办、工信部等四部门联合发布《互联网信息服务算法推荐管理规定》，明确算法推荐服务提供者不得利用算法虚假注册账号、非法交易

账号、操纵用户账号或者虚假点赞、评论、转发， 不得利用算法屏蔽信息、 过度推荐、操纵榜单或者检索结果排序、控制热搜或者精选等干预信息呈现， 实施影响网络舆论或者规避监督管理行为。2022 年 5 月 23 日， 最高法公布了《最高人民法院关于加强区块链司法应用的意见》，明确人民法院加强区块链司法应用总体要求及人民法院区块链平台建设要求，计划到 2025 年建成人民法院与社会各行各业互通共享的区块链联盟，形成较为完备的区块链司法领域应用标准体系。

五、数据安全保护存在问题

在本次调查的开放性反馈中，网民认为数据安全保护现阶段存在的问题主要体现在市场现状、数据结构和标准规范等方面。其中， 数据不规范以及数据市场交易市场混乱是目前最突出的问题。其次， 数据安全标准规范建设滞后、数据应用程度较低、中介服务供应不足、政府数据不开放等问题也是数据安全方面存在的重要问题。

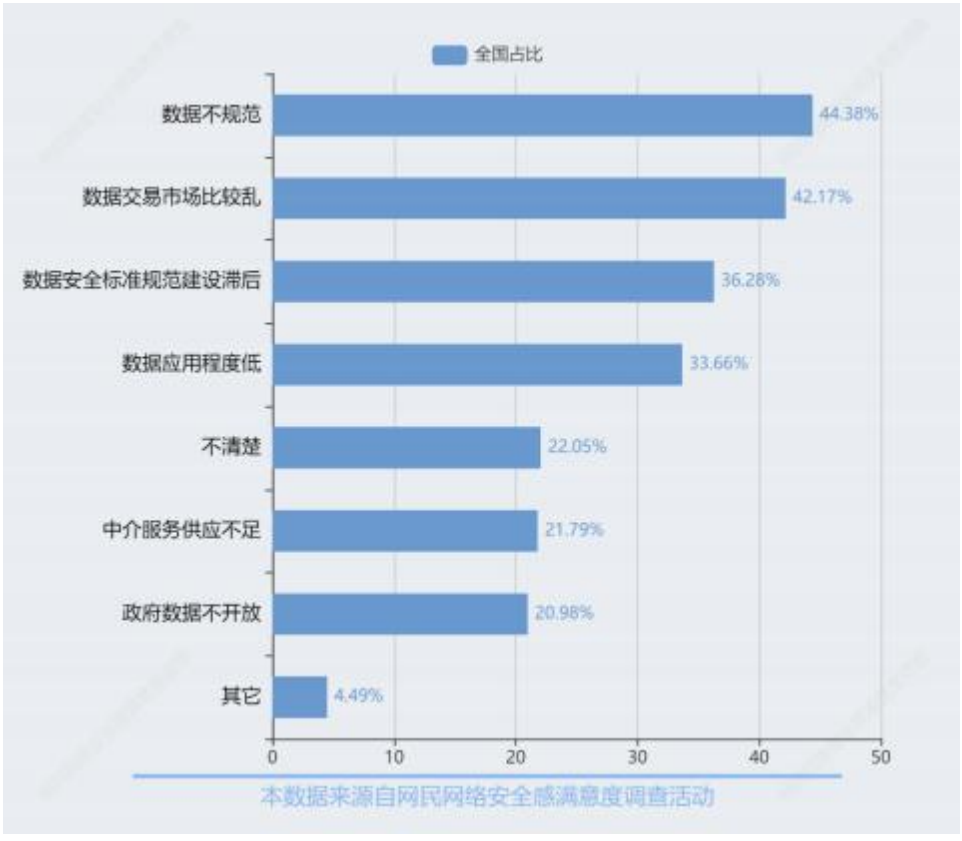

图 5-1：网民认为当前数据安全保护存在的问题

（一）数据规范是当前网民关注的首要数据安全问题

根据调查， 当前数据安全的首要问题便是数据规范问题， 占比为44.38%。

主要在于数据规范问题涵盖数据链条的多个环节，比如数据的采集、 存储、具体操作运用、数据管理协议等不规范， 数据管理平台之间竞争的不规范， 数据安全标准规范建设迟滞，以及前述数据市场交易不规范等。数据的采集、处理阶段的不规范可能会造成数据安全漏洞，使得用户数据丢失或者轻易被他人获取，数据管理者多表现为疏忽过失心态，对此需要其加强技术能力以避免安全漏洞。而数据的具体应用不规范则多表现为数据管理者对规则的不遵守，需要外部的强制手段予以保障。

（二）超四成网民认为当前数据交易市场秩序混乱

根据本次调查结果显示， 数据交易市场秩序混乱问题仅次于数据规范问题，占比 42.17%。数据交易市场秩序的混乱体现为两个层面。在内生于市场运行自身的自发秩序上，有不法分子为了限制或排除竞争，采取非法的方式获取和交易数据， 使得“数据黑市”盛行。 这是市场无法自己解决的问题， 需要其他外部手段消除市场产生的负外部性， 以维护社会公平正义。在外生于监管和法治的制度秩序上，由于目前的数据安全法治体系尚未建设完备，规范监管在数据领域尚未达到资本市场、土地市场等传统生产要素市场的标准。监管滞后是造成数据交易市场秩序混乱的主要原因。

（三）超三成网民反馈存在数据应用程度低的问题

习近平总书记强调， 要发展数字经济，加快推动数字产业化，依靠信息技术创新驱动， 不断催生新产业新业态新模式，用新动能推动新发展。 这要求我们充分发挥数据的价值，提高数据应用的效率。数据应用的程度可以分为广度和深度，必须承认当下信息的数据化已经非常充分， 数据应用的领域越来越多， 其广泛程度已经触及民众想象力的边界。但同时，数据应用的深度尚待继续挖掘。例如，在智慧城市建设发展过程中，政府推进大数据中心建设， 但未能主动促进工业的发展和大数据应用需求之间的对接，导致大数据中心通过大数据改进决策的事例鲜为人知。此外，大数据需要整个信息产业链的支撑，从底层芯片到基础软件再到应用分析软件，而新的计算平台、分布式计算架构、大数据的处理、 分析、表达等方面尚无法满足大数据在各行各业的应用需求，导致数据价值的有效利用遇到瓶颈。

（四）数据中介服务匮乏影响受访网民网络安全满意度

数据的中介服务是为了提升数据的适用性， 因为在数据平台上，中介数据体系的缺失会增加公众发现和理解数据集的难度。数据中介服务尤其对于政府数据开放有重要作用， 高质量的数据中介服务可以拓宽公众获取政府数据的管道，提升政府开放数据的利用率。虽然各级政府及其大数据管理部门正在不断深化中介服务规范管理， 推行政府购买中介服务， 但当前仍有 21.79%的受访网民认为数据中介服务缺乏，说明有关数据中介服务尚未真正方便普通民众从中获益， 有关部门应当有针对性地改进数据中介服务体系。

（五）政府数据开放程度未达到网民预期

虽然目前政府网站已经是我国各级政府及其工作部门的标配，但是仍有20.98%的受访网民认为政府数据开放不足。由此可见政府网站的服务功能没有达到部分民众的预期，政府与民众的互动尚未有效地帮助民众解决问题， 这与最大限度地发挥政府网站作为政务公开主渠道的作用仍有一段距离。

而且据统计，仅有个别地方政府网站开设“数据开放”或类似的专门栏目，绝大多数城市只是在政府网站中分散、零星地公开一些政府数据， 而没有统一设置专门栏目，导致社会成员获取或共享属于公共财产的政府数据难度很大。此外，即使是已经设置“数据开放”或类似专门栏目的地方政府，其数据开放程度还比较低，数据开放的时效性也有待提高。

六、网民数据安全诉求

参与调查的公众网民对加强数据安全保护的具体诉求体现在多个方面，包括制度供给、企业自律、建立监管和投诉机制， 以及宣传培训。其中选择最多的是加强制度供给和企业自律，显示出公众网民期望更多地从基础层面完善有关数据安全的保护体系和措施。其次是建立认证和监控制度、增加通报管道和举报平台，最后是社会组织等加强培训和宣传。即使是选择人数最少的方案（即“社会组织等加强培训和宣传”）也有超过一半的网民认可，表现出民众对数据安全治理的迫切期望。

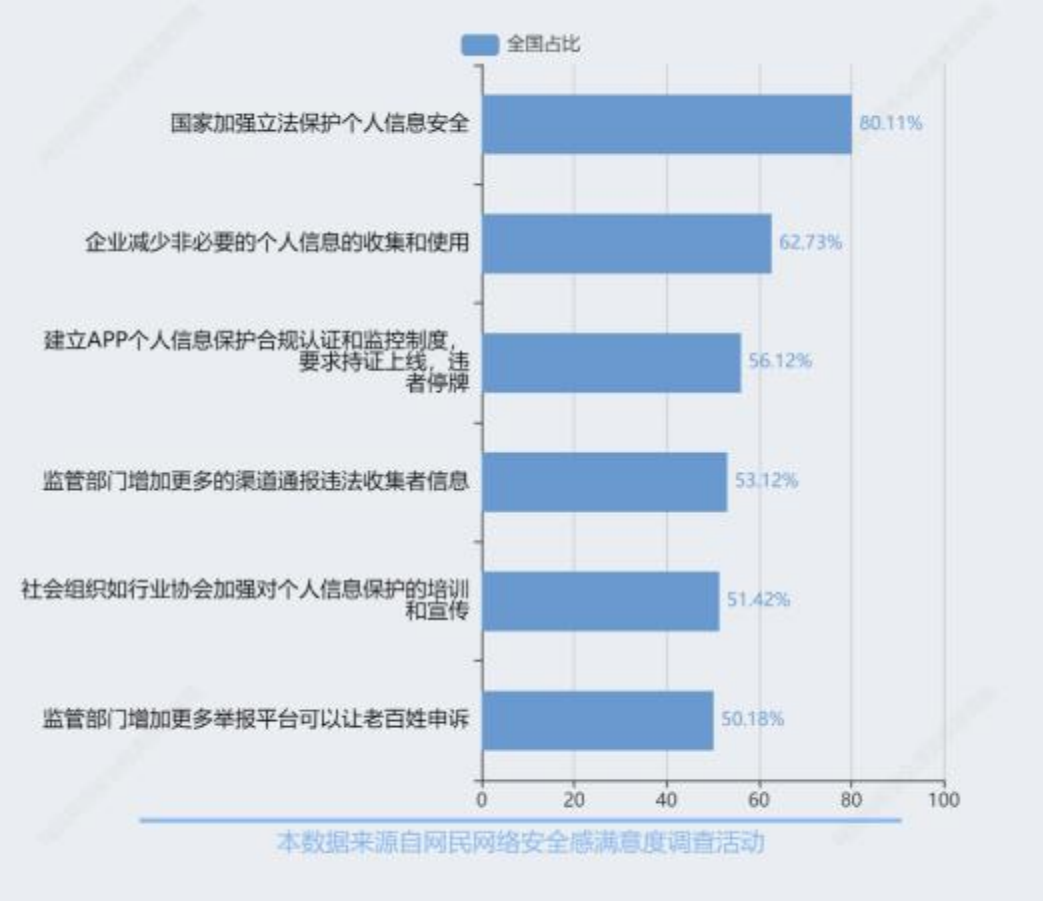

图 6-1：网民认为应重点在哪些方面加强数据安全保护

（一）制度供给层面，网民认为应当加强国家立法

从调查数据中可以看出， 公众网民在面对数据安全问题时，认为国家加强立法是首要措施。而近年来的数据安全立法态势积极，自去年出台《数据安全法》以来，《个人信息保护法》相继出台， 而且各地有关数据安全的地方性法规的制定进程也不断加快，应当认为当前的制度供给在形式上已经较为充分且趋于完备。但即使如此， 调查数据显示只有不到一半的公众网民认为《数据安全法》出台后个人信息保护现状发生改善，有超过半数的网民认为《数据安全法》的作用一般甚至对个人信息保护现状有消极影响。这说明《数据安全法》的制度设计没有解决人们希望解决的很多数据安全方面的主要矛盾，为此的确需要增强具有针对性的制度供给，使得民众能够切身体会数据安全法制在发挥作用。

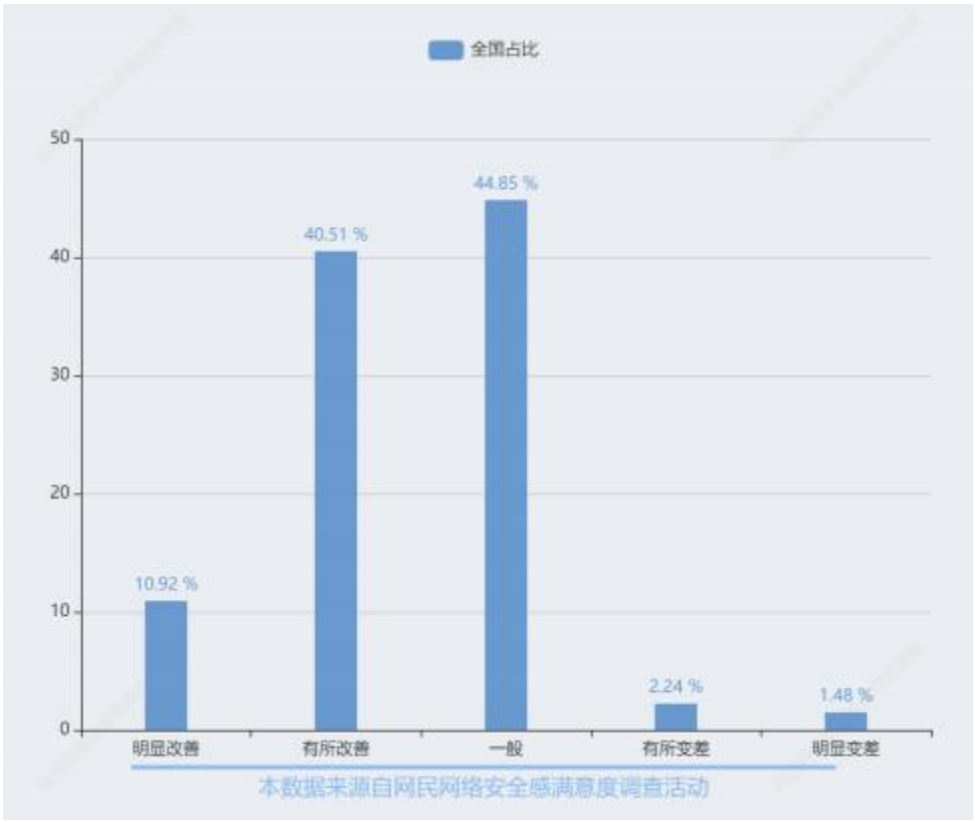

图 6-2：网民认为数据安全法出台后，APP 运营者在个人信息保护方面是否有改善

（二） 监管执法层面， 网民期待加强监管执法力度

公众网民的这一诉求实为“执法必严、违法必究”在数据安全法治中的贯彻。法律的预防效果不在于惩罚的严厉程度， 而在于执法的必然性， 因此只有保证监管执法的力度才能使完备的制度供给发挥实效。实际上《数据安全法》已经建立了一套数据安全监管制度， 明确了多方主体之间的职责分配。《数据安全法》第六条规定：“工业、 电信、 交通、金融、自然资源、 卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。”位列网民数据安全诉求第二位的“企业减少非必要的个人信息的收集和使用”难以仅仅依靠企业的自觉来实现，仍然需要在完备而强力的监管施压下才能得到保证。

（三） 救济途径层面， 网民希望增加反馈管道

前述完善制度供给和保证执法力度均是在公权力运行层面，由政府在宏观层

面为数据安全提供保障。而与之相对应的， 公众网民也十分重视个人私权在受到侵犯时有明确的救济途径，为此有 51.42%的受访网民希望监管增加更多举报平台用于申诉。增加反馈管道不仅有利于民众维权， 督促企业落实数据安全保护义务， 还可以在监管执法环节中分发挥群众的作用， 拓宽监管的范围， 也能够借此使民众对数据安全治理成效有切身感受。

（四）数据安全倡导层面， 网民认为需要加强培训与宣传

社会组织(如行业协会) 加强对数据安全保护的培训和宣传可以在多个方面发挥作用。对企业的培训可以强化企业的数据安全风险防范意识，使其重视企业自身作为数据管理者可能存在的数据安全漏洞，筑牢数据安全防线。对民众的宣传教育可以提高其对数据风险的认识，增加民众对国家的数据安全建设工作的认可度， 强化个人数据安全的防护意识，营造良好的数据法治氛围。

七、加强网民个人信息保护和数据安全的建议

（ 一）贯彻落实平台个人信息的“守门人”责任

通过对公众网民调查个人信息最有可能是从什么环节泄露进行分析，有超过70%的网民认为其个人信息是在注册 APP 账户、APP 要求获取相机、位置等隐私权限时遭到泄露。这表明，平台 APP 基于巨量的网民用户数量获取到了不计其数的个人信息甚至个人隐私数据。因此， 应当贯彻落实好《个人信息保护法》第五十八条首创的“守门人”义务，要求提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者主动承担更为严格的个人信息保护义务，把好公民个人信息上网的“入门关”。

z（二）个人信息保护难题亟需电信行业联防联控联治

个人信息泄露不仅仅存在于互联网环境当中，各类推销电话、短信暂且不论，作为网络个人数据交易黑灰产的链条之一， 在获取到个人信息后，犯罪嫌疑人通过电信渠道进行针对性的电信诈骗仍然甚嚣尘上，值得密切关注。根据数据分析，在被问及自身怀疑或确认个人信息被泄露或被滥用的具体情形时，超过七成的网民表示是接到各类中介的推销短信， 接近六成的网民表示收到了相关的推销短信。这启示，在进行个人信息保护和数据安全建设时，除了对于网络上的种种乱象要重拳出击，在网络之外的电信领域，也需要各大电信运营商的积极参与和切

实措施，保障广大公民的个人信息不受侵害。

（三）加快数据分类分级，实现数据精细化管理

通过对网民认为目前数据安全保护现状存在什么问题进行调查， 超过四成受访者认为存在数据不规范问题，接近四成受访者认为我国数据安全标准规范建设仍然滞后。数据安全治理应该从数据的安全风险着手，通过对数据进行分类分级实现数据的精细化管理和风险可控。全国人大常委会法制工作委员会对《数据安全法》的立法说明中， 便将数据分类分级管理制度作为国家数据安全管理制度和体系中的首要制度。 考虑到数据分类分级是数据安全中的基础，在数据分类分级过程中， 尤其需要平衡精细化管理与落地实施。只有通过数据的分类分级、制定既符合我国国情，又吸收国际先进经验的数据安全规范标准，才能促进数据产生、流转、利用全过程的规范化、精细化、标准化。

（四）加快建立数据交易市场

有超过四成网民认为当前数据安全保护存在的主要问题是数据交易市场秩序混乱，因此有必要建立统一的国家数据交易平台。建立国家统一的数据交易平台可以充分发挥激活数据资源的财产价值，促进数据资源在全国范围内实现最大程度的自由交易和流通，极大推动我国数据关联产业发展；同时，还可以解决数据交易平台分布不均、数据集中度不高和数据供给区域不平衡造成数据开发应用瓶颈等问题。数据交易市场的顺畅运行还需依托统一的交易准则，交易准则需要在数据产品分类标准和数据产品的定价标准上达成统一。数据产品的分类标准可根据整体数据目录与重要数据目录进行确定；数据产品的定价标准可由国家价格管理部门会同行业协会、企业共同研究制定，具体应包含数据产品基本价格指标体系和数据产品调整价格指标体系两部分。

网安联微信公众号

网安联秘书处

官网：www.iscn.org.cn

电话：020-8380 3843/13911345288

邮箱：cinsabj@163.com