2023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家网络安全行业协会及相关社会组织

牵头单位：北京网络空间安全协会

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4月

本报告数据来源于 2023 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:

2023 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

发起单位：全国 135 家网络安全行业协会及相关社会组织

牵头单位：北京网络空间安全协会

承办单位：乌镇数字文明研究院

浙江大学国际传播研究中学

互联网实验室

2024 年 4 月

目　录

一、加强个人信息保护和数据安全治理的背景

为了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 138986 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“2023 个人信息保护与数据安全”专题报告。

党的十八大以来，习近平总书记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。得益于此，网络安全政策法规体系不断健全，网络安全工作体制机制日益完善，全社会的网络安全意识和能力明显提高，广大人民群众在网络空间中的获得感、幸福感和安全感不断增强。然而，我们也应该看到，近年来，我国面临的网络安全威胁和风险日益突出，这些威胁和风险已经向政治、经济、文化、社会、生态、国防等领域渗透。因此，防范网络安全风险、维护网络空间安全，已经成为中国必须面对和解决的重大安全问题。作为网络安全的一部分，数据安全在国家安全、经济安全以及社会稳定中都有着重要地位，已连续四年被写入政府工作报告。《2024 年政府工作报告》中强调了数据资源作为新型生产要素的重要性，认为数据安全与国家安全密切相关。

2021 年《数据安全法》《个人信息保护法》落地施行，与《网络安全法》共同形成了数据治理法律领域的“三驾马车”。在此之后，相关配套法规纷纷出台，《网络数据安全管理条例(征求意见稿)》《数据出境安全评估办法》等行政法规是对三部上位法的补充、落实和细化。而 2023 年 3 月以来的《网信部门行政执法程序规定》《工业领域数据安全能力提升实施方案》，标志着数据安全监管的常态化。

数字时代，个人信息已成为一种宝贵的资源，是数字经济时代的核心资产，被广泛应用

于商业、社会和个人生活的方方面面，包括个人身份、偏好、行为等敏感信息在内的大量数据被广泛采集、存储和利用。与此同时，个人信息的泄露、滥用和不当处理也带来了严重的隐私和安全风险。在网络空间中，网络攻击、数据泄露和身份盗窃等安全威胁不断涌现，给个人信息安全带来了巨大挑战。尤其是在行业界，诸如金融、医疗、零售等领域，个人信息的泄露可能导致严重的财务损失和信任危机，对个人权利和社会稳定造成严重影响。如何最大程度保护个人信息、维护网络安全，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、2023 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评价持续提高

根据 2023 年的调查结果现实，“一般”“不太好”“非常不好”评价分别占受访人群的 34.98%，10.01%和 4.35%，都低于 2022 年的比例，其中“不太好”更是降低了 5.65%。30.97%的受访人群认为当前状况“比较好”；19.68%的受访人群认为当前状况“非常好”。这两个比例较去年都有所提升，并接近整体评价比例的“半壁江山”。

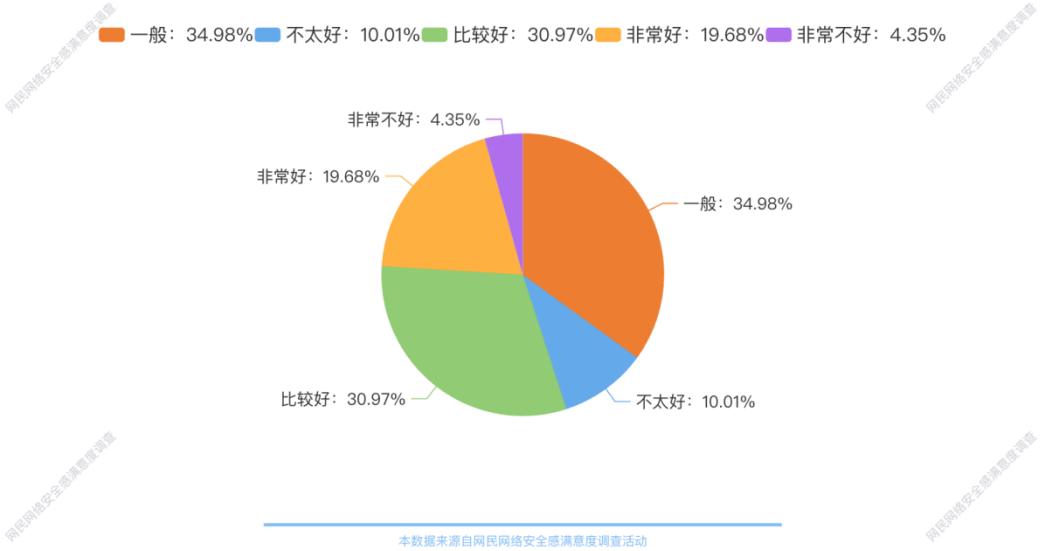

图 2-1：公众网民对个人信息保护现状的评价

（二）公众网民个人信息泄露的感知情况向两极化发展

个人信息泄露在网络环境中仍然是一个普遍存在的问题。总体上，有近九成的受访者（91.51%）在过去一年中感知到网络个人信息的泄露。“没有遇到”和“非常多”在受访人群中的比例相较于 2022 年均有上涨，分别为 8.49%和 17.52%。相对较轻微的情况（“很少”和“有一些”）比例的受访人群为 48.82%；25.16%的受访人群遇到过“比较多”的信息泄露。

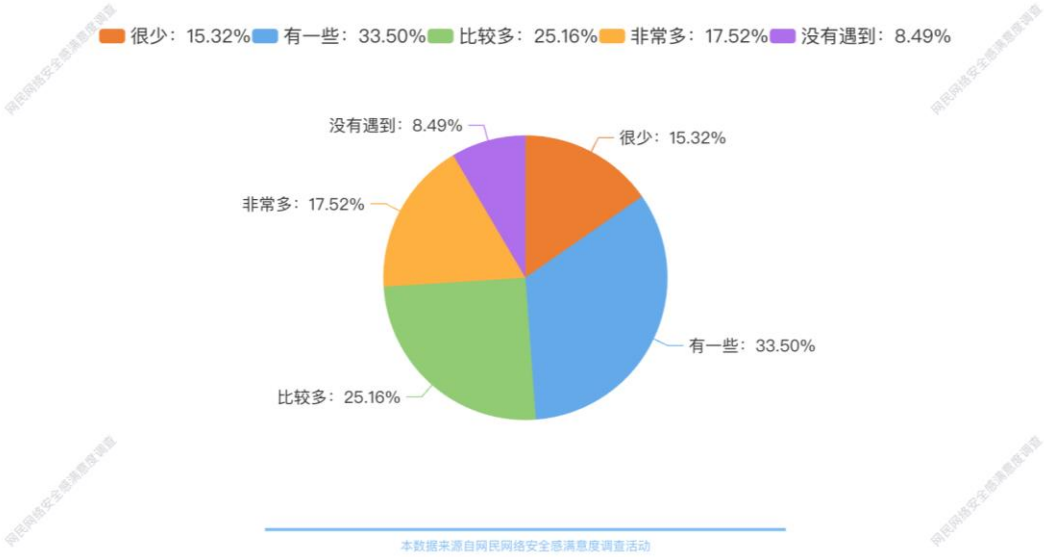

图 2-2：近一年网民对个人信息泄露的感知情况

（三）公众网民在多元场景感受到的信息泄露情况有所好转

个人信息泄露和滥用的情况在通信工具使用过程中普遍存在但较去年有所好转。根据 2023 年参与调查的公众网民反馈的数据显示，怀疑或确认个人信息被泄露、滥用的情形主要包括接到各类中介的推销电话（69.08%）、收到垃圾邮件（43.77%）、收到相关性的推销短信（41.58%）等。虽然中介推销电话较去年有所下降，但仍是占据最大比例的情形。各类 APP 也成为了个人信息泄露的主要场景，尤其是大数据杀熟（37.19%），即个人信息可能被用于定向广告或定价策略。部分 APP 默认勾选同意《服务协议》，允许应用收集（包括在第三方保存）用户信息（25.45%），一定程度上导致匿名注册却被熟人在抖音、小红书等社交软件加好友（17.85%）。也有 19.69%的受访者怀疑收集信息时未告知消费者收集目的用途、方式和范围等会导致信息泄露等。

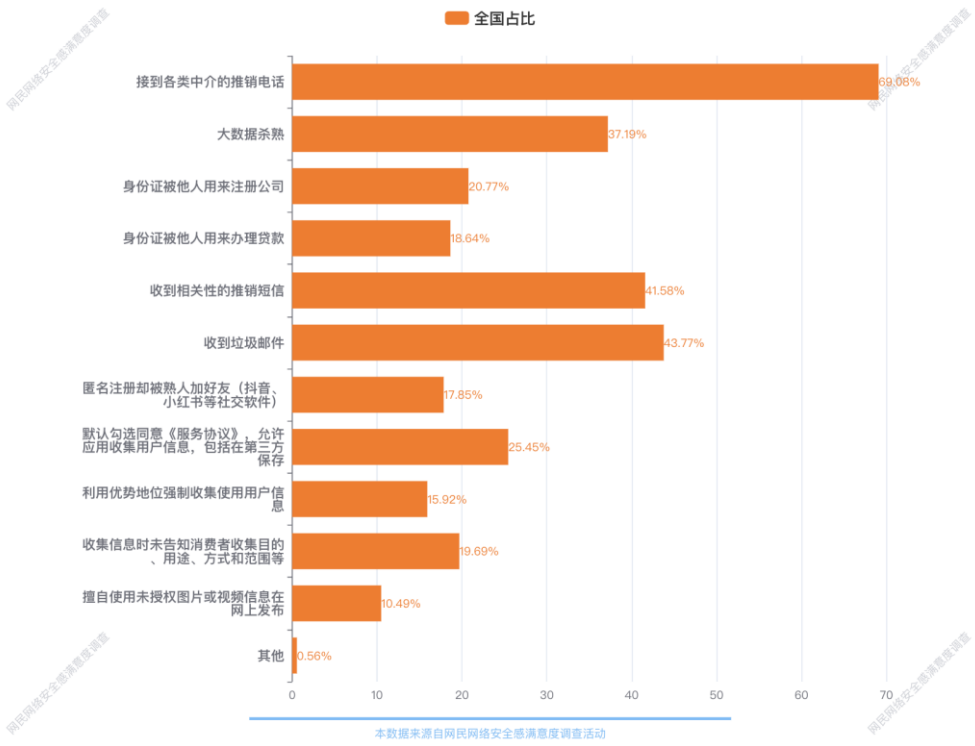

图 2-3：网民遇到的怀疑或确认个人信息泄露的情形

（四）公众网民对个人信息泄露有多种处理方式

在发现以上个人信息泄露时，不少受访者在采取措施前会对泄露信息可能带来的风险进行评估，再做出应对决策（22.61%）。也有 14.94%的受访者选择不采取行动。超过半数的受访者（52.83%）选择更换账号、密码等手段。在面对由泄漏造成个人利益受损的情况时，受访者表示会报警保护自身权益（42.39%），找律师维护自己的权益（20.32%），并且提醒身边的亲朋好友防止被骗（43.41%）。

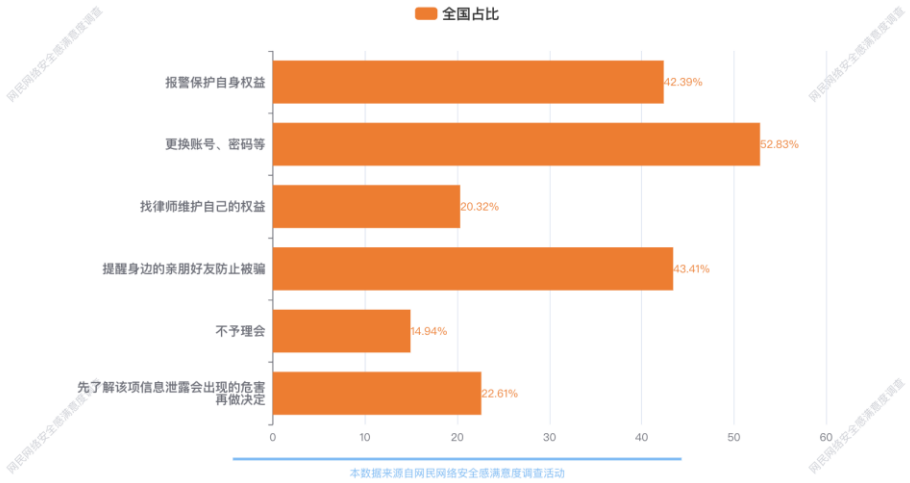

图 2-4：网民遇到个人信息泄露时的解决方式

（五）公众网民对生物识别信息风险的担忧程度提高

在使用生物识别技术进行身份认证时，仅 3.71%的受访者表示完全信任这种技术，其余受访者生物识别技术在信息安全方面都存在不同程度的担忧。“一般”与“很少担心”较去年波动不大，分别有 25.01%和 11.31%的受访者。24.94%的受访者“非常担心”生物识别风险，占据最大板块的“比较担心”有 35.03%的受访者。

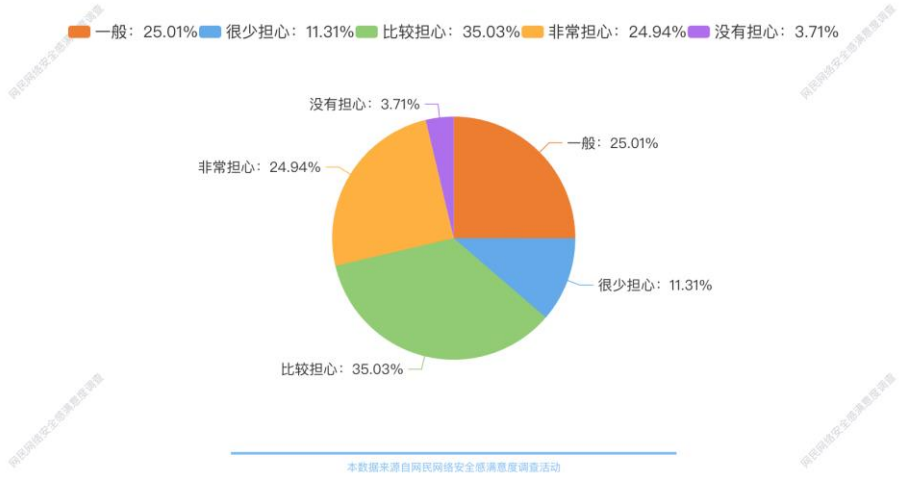

图 2-5：网民对生物识别技术泄露个人信息风险的倾向

与去年的情形略有差异，刷脸和免密支付的网民比例均有所提高，分别为 41.07%和 12.91%。在线上支付时，密码（76.04%）和指纹（48.08%）的网民比例有所下降，但仍是受访者最常采取的两种身份方式认证；还有 27.37%的受访者会采用短信认证。

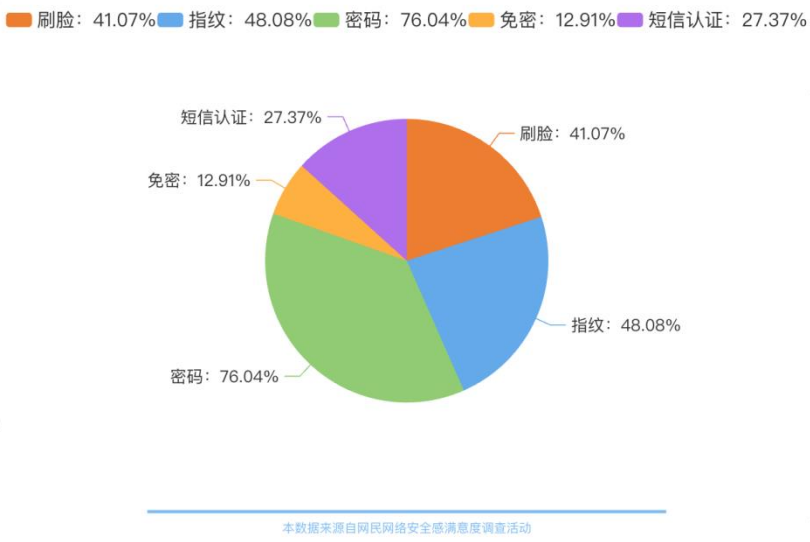

图 2-6：线上支付采用的身份认证方式

三、2023 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

公众对社交应用（即时通讯、短视频等）、网络媒体（新闻资讯、网上阅读、视频直播等）、电子商务（网络购物、网上支付、网上银行等）和数字娱乐（网络游戏、网络音乐、网络视频等）应用的个人信息保护较为担忧。其中，半数人认为社交应用保护不太好，41.21%认为网络媒体保护不佳，40.81%对电子商务应用的保护表示担忧，37.30%对数字娱乐应用也持相似看法。相比之下，健康医疗类、生活服务类、网上办公类和电子政务类应用的个人信息保护问题相对较少引起关注。

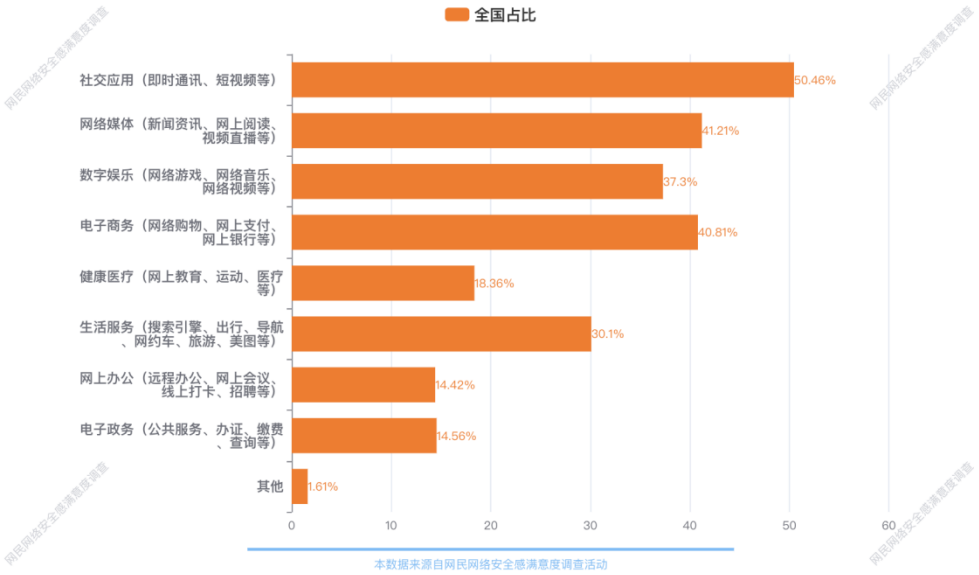

图 3-1 个人信息保护受关注的 APP 类型

另外，在使用 App 的过程中，极个别会认真阅读的受访者占到了 33.67%，是最大的一个群体。27.97%的受访者表示不会留意，还有 13.79%的受访者会根据大众使用程度，不被普遍使用的会认真看，只有接近四分之一的受访者都会认真阅读。网民对安全隐私协议的敏感度和认知度仍有待提高。

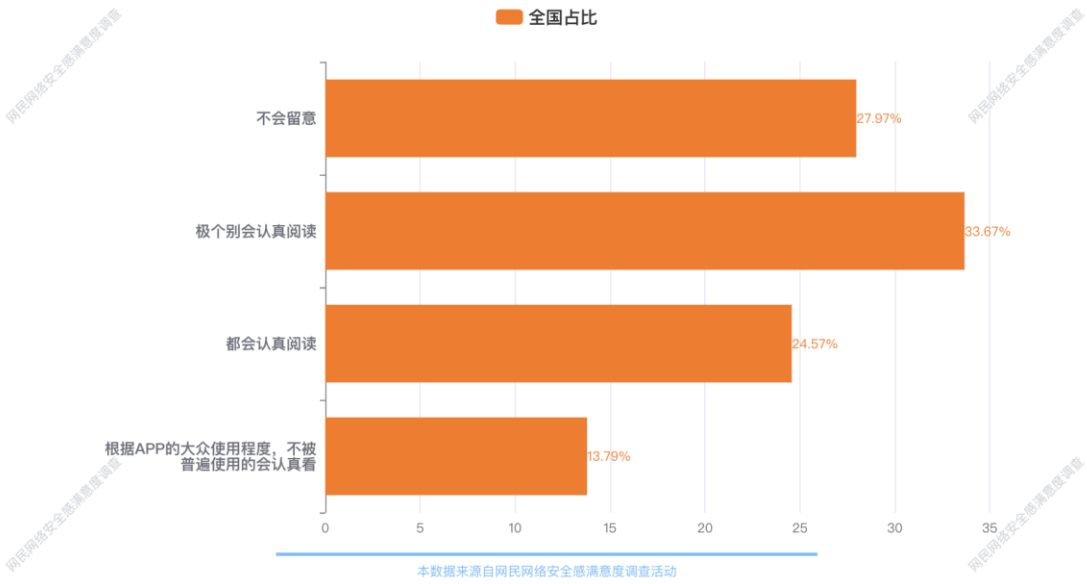

图 3-2：网民使用移动应用（APP）时阅读安全隐私协议的情况

（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，

近一年来，公众网民普遍面临着个人信息泄露的风险，主要集中在注册 APP 账户时授权隐私权限、点击不明二维码或链接以及参与网上测试、投票、抽奖活动等行为。其中，注册 APP 账户并授权隐私权限是导致信息泄露的最主要因素，占比高达 62.04%，这与现代应用程序对用户权限的要求密不可分。用户在使用应用程序时不可避免地需要授权较多的隐私权限。其次是点击网上不明二维码、链接（42.83%）以及参与网上测试、投票、抽奖活动（44.74%）。此外，将个人信息上传到网络云端储存（26.48%）和使用公共 WiFi（30.64%）也存在较大的信息泄露风险。其他途径（1.85%）的个人信息泄露可能性相对较低，但仍需要关注和加强相应的防护措施。

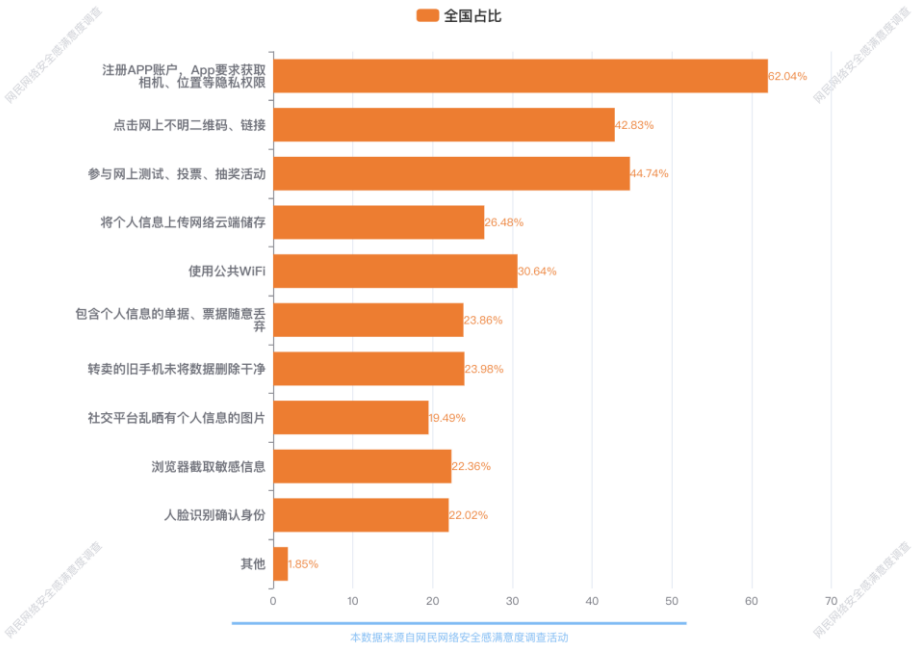

图 3-3：个人信息泄露环节

（三）网民认为 APP 使用存在的各类违规现象与问题

一些 APP 在信息收集、权限获取等方面存在超出功能需求的个人信息收集和频繁索要无关权限，分别占比 51.15%和 44.90%。这可能会影响用户对于隐私保护的信心和态度，也是公众网民最常遇见的问题。另外，38.43%的受访者表示存在不合理免责条款；34.08%的受访者表示默认捆绑功能并一揽子同意。

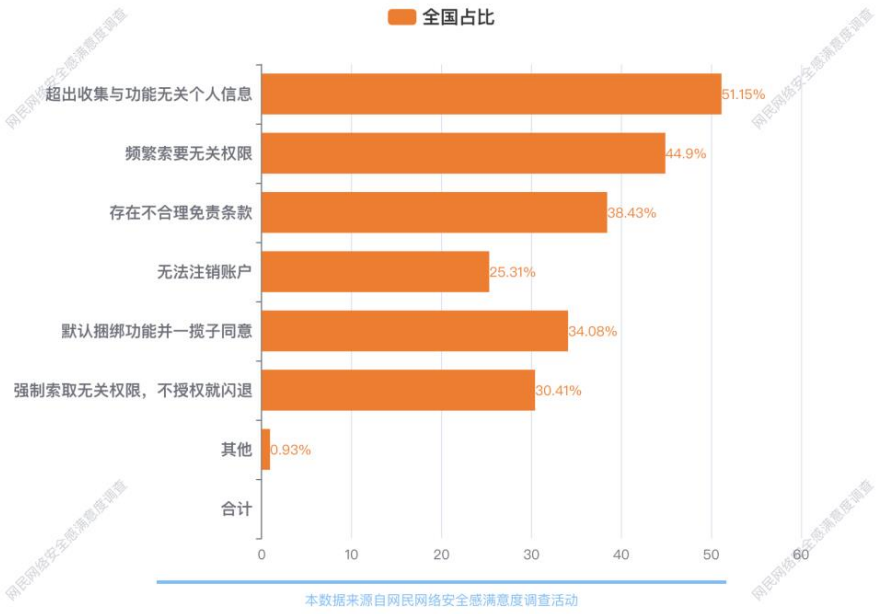

图 3-4：受访者在 APP 收集信息过程中遇到的问题

虽然有约 11.01%的受访者表示对非政府、非官方的 app 或平台注册时需要提供个人敏

感信息这件事并不在意，认为信息已处于“裸奔”时代，但大多数人仍然持谨慎态度，24.62%的受访者对此非常在意，拒绝向任何商业平台提供个人信息；41.92%的受访者只在必要情况下提供信息或者会选择换平台。纵然 APP 信息获取权限，是在 APP《安全隐私协议》合法范围下征求用户同意所进行的，但有 27.97%的人表示不会留意安全隐私协议，13.79%的人表会对不被普遍使用的 APP 才会认真看。

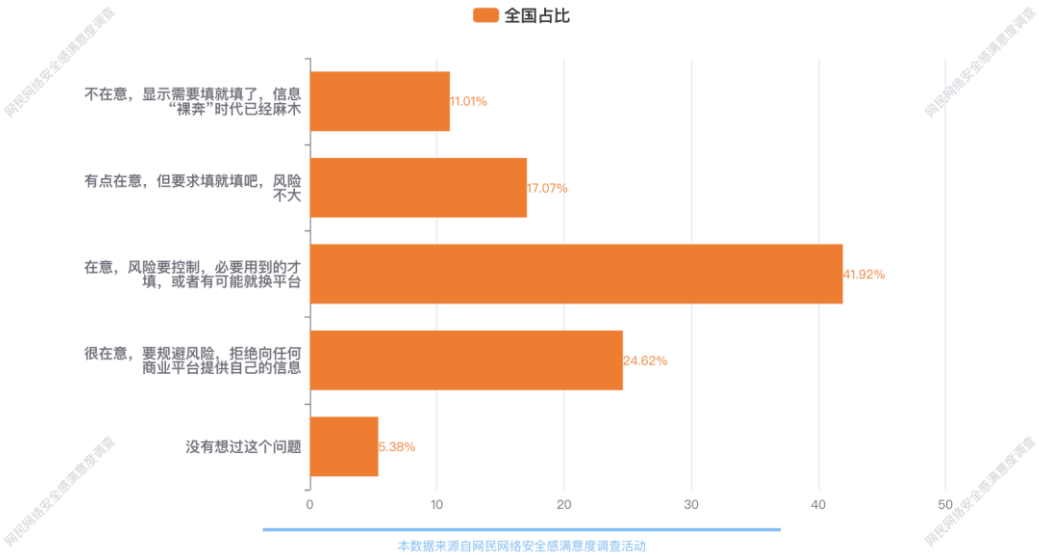

图 3-5：网民对非政府、非官方 app 需要提交敏感信息的态度

（四）经营商推送的精准广告及设置的退出机制仍需完善

互联网中的 APP 和平台，均不同程度地存在滥用个人信息，进行过度的个性化广告、信息推送或价格歧视等情况。在日常上网的过程中，有超越九成的受访者收到过精准广告的投送。只有 17.01%的网民很少或没有收到过精准广告，较去年的比例有所提高，精准广告现象有所好转。但是其中 29.14%的受访者表示经营者向他们发布精准广告时全部没有征得同意，仅不到十分之一的人表示精准广告的发布全部都征得了同意。还有 14.67%的受访者不清楚经营者发布精准广告时是否有征得过同意。

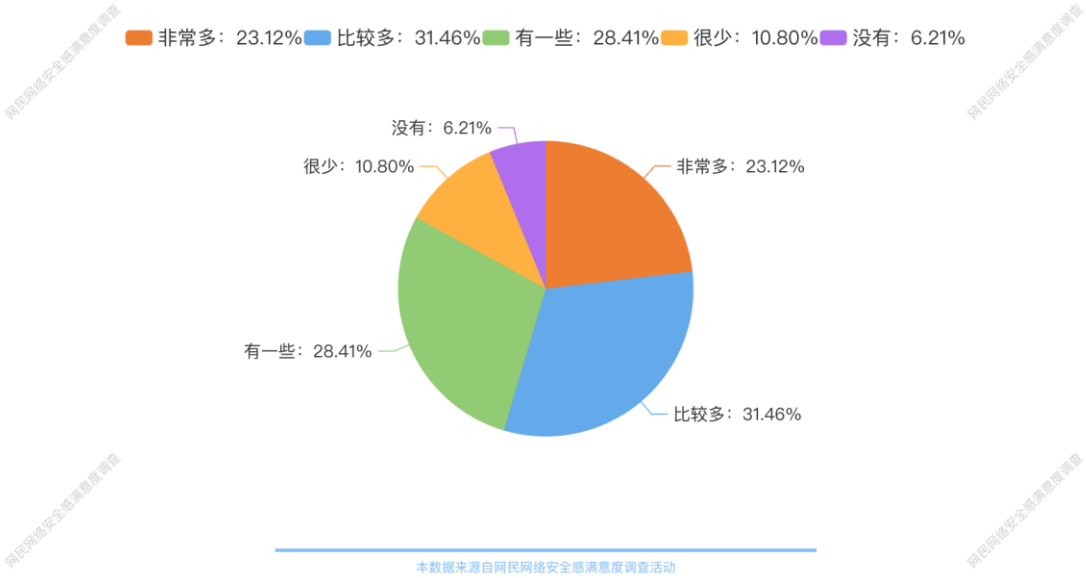

图 3-6：网民在日常上网时收到精准广告的情况

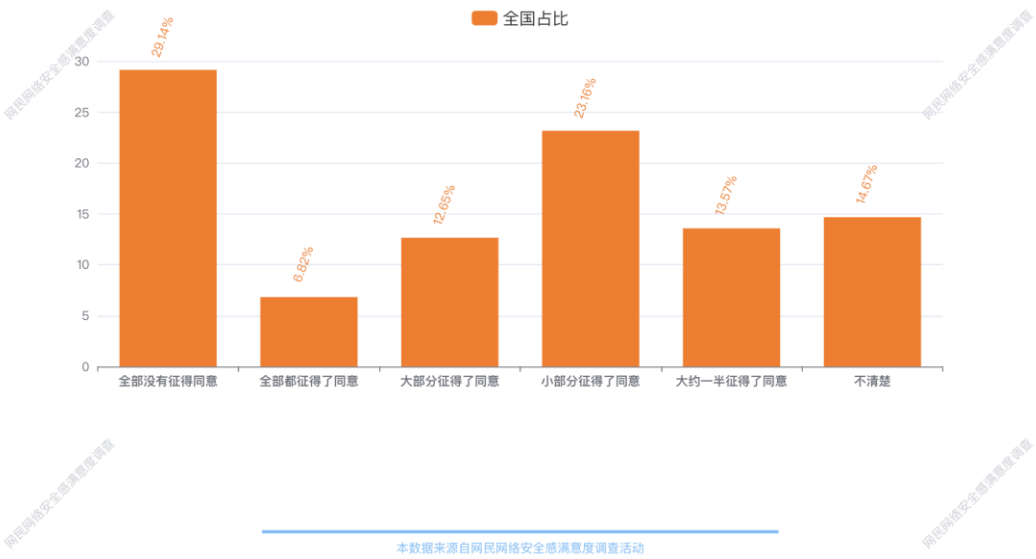

图 3-7：经营者向网民发布精准广告时征求同意的情况

此外，仍然还有五分之一的网民表示不清楚 APP 对“精准广告”提供的退出机制，较去年下降了 11.06%。但其他情况不容乐观，12.24%的受访者表示全部精准广告都没有提供退出机制，以及 24.01%的受访者认为小部分精准广告提供退出机制了，这两个比例相较于去年都有所上升。不到十分之一的受访者认为收到的精准广告全部提供了退出机制，退出机制仍需加强建设和普及。

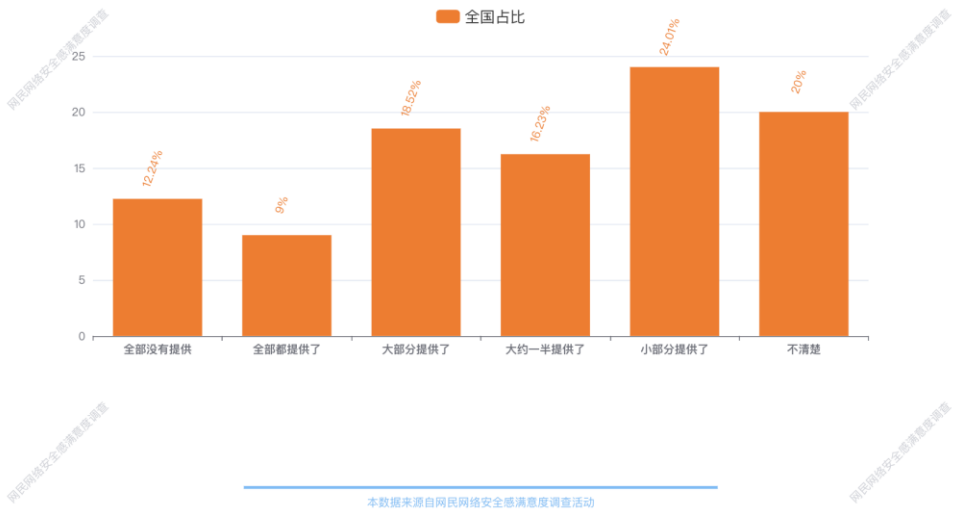

图 3-8：网民收到的精准广告退出机制的提供情况

四、2023 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）网民对相关法律法律法规的了解程度

个人信息安全保护法律法规方面，仍有较大的宣传和普及空间。大多数受访者（55.71%）是通过《中华人民共和国个人信息保护法》来了解涉及个人信息安全保护的法律法规，而对《民法典》、《数据安全法》、《未成年人保护法》和《网络安全法》中涉及个人信息安全保护的法律法规的了解程度相对较低。

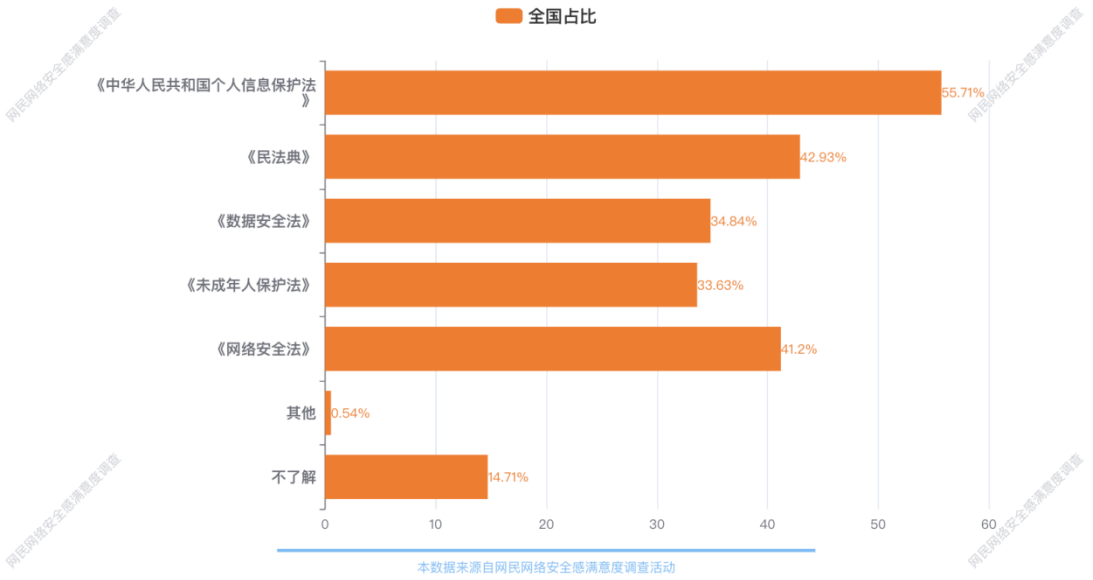

图 4-1 涉及个人信息安全保护的法律法规

对于新出台的《人脸识别技术应用安全管理规定（试行）（征求意见稿）》，一半左右的受访者还不太了解，需要进一步加强宣传和解释。

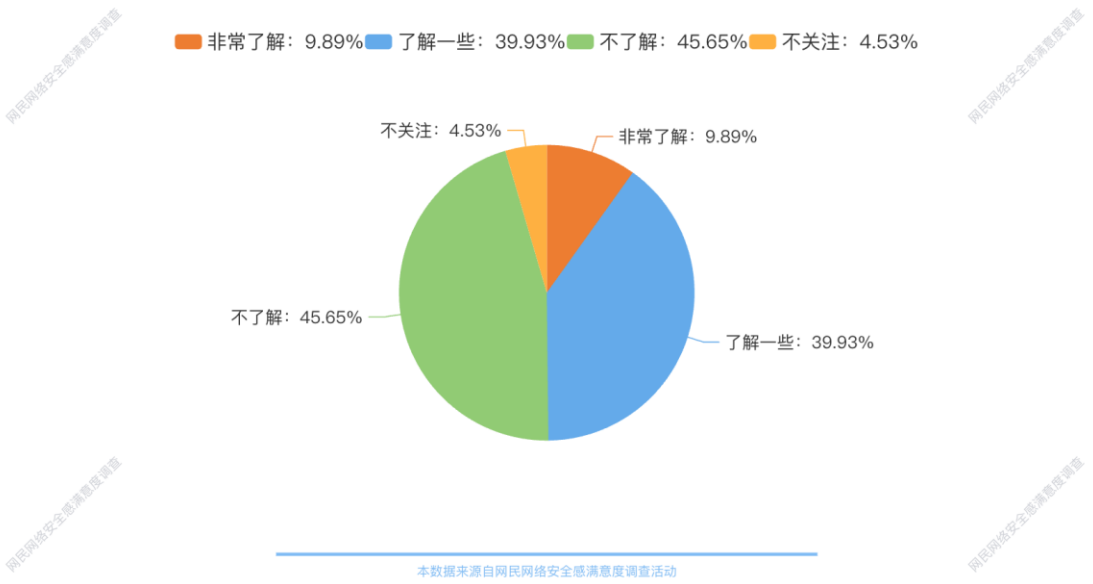

图 4-2 网民对《人脸识别技术应用安全管理规定（试行）（征求意见稿）》的了解情况

（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

仅有约三分之一的网民了解《个人信息保护法》中的新规定——个人信息保护公益诉讼制度而言，仍需要加大新规定的普及力度，加强公众的个人信息保护意识。

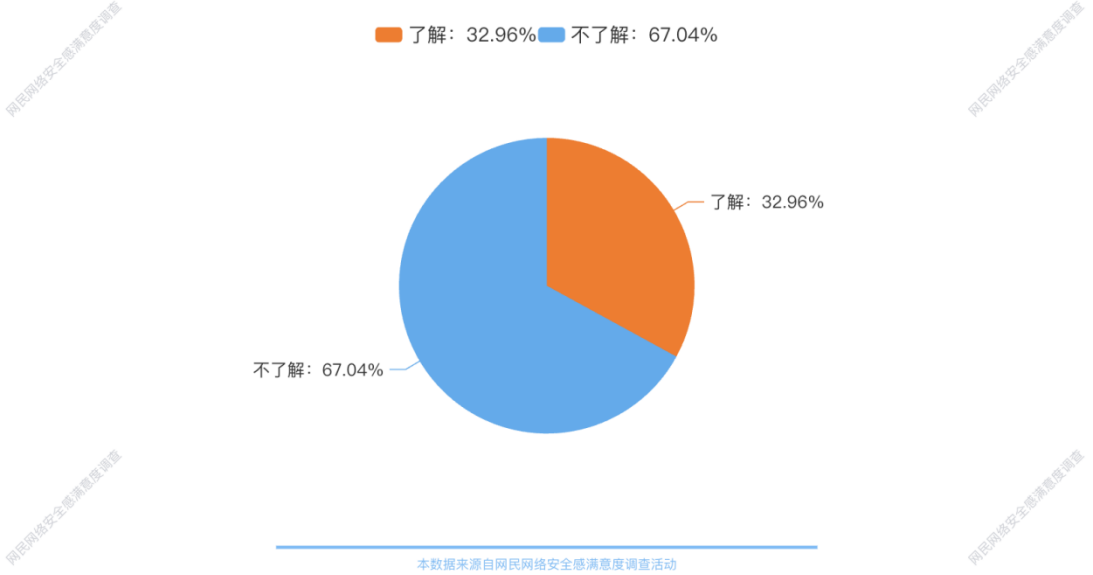

图 4-3 网民对《个人信息保护公益诉讼制度》的了解情况

个人信息保护民事公益诉讼在推行过程中可能面临维权意识不足、诉讼成本高、判决执行困难和惩罚力度不足等多个困境。近一半的受访者认为原告维权意识不足或惰于起诉，这可能源于对个人信息保护重要性认识不足、维权成本高等原因。超过一半的人认为诉讼过程漫长、耗费成本巨大，这可能与涉及到技术和法律问题的复杂性有关。由于执行力度不足、

法律程序繁琐等原因，近一半的受访者认为判决执行困难，效果欠佳。此外，法律制度和执行力度还待提高，有关约四成的人认为惩罚力度不足以消除再犯风险。

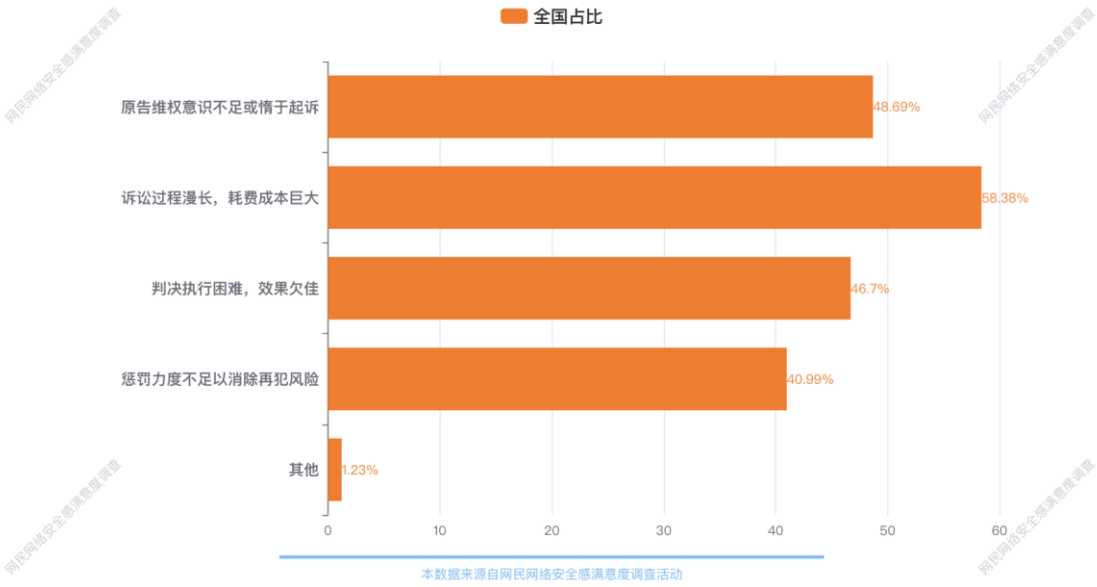

图 4-4 在个人信息保护民事公益诉讼的推行过程中会面临的困境

（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，完善公益诉讼配套制度，提高公益诉讼的效率和执行力，扩大检察机关获取侵权线索的途径：如鼓励举报、加强衔接等，以便更多的侵权行为能够被及时发现和处理；加强惩罚措施，起到更好的震慑作用，让侵权者知道触犯法律的代价。另一方面，个体力量也不可忽视。有 34.29%的受访者认为应明确个人信息保护公益诉讼主体的起诉顺位，以确保维权行为的合理性和有效性。公民个人也应该纳入公益诉讼主体（39.67%），以增强整体维权力量，让更多人参与维护个人信息安全。

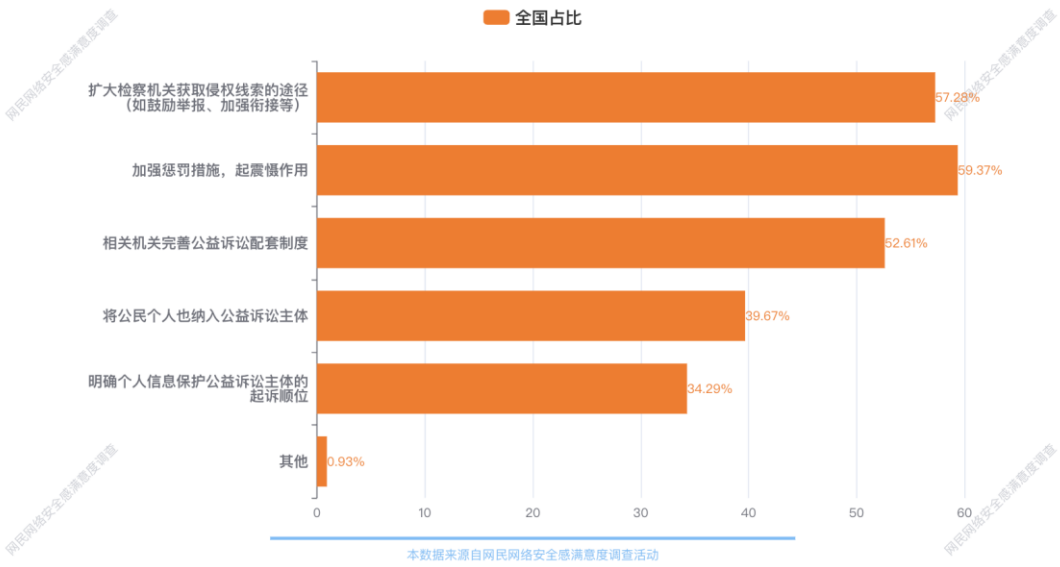

图 4-5 对个人信息保护公益诉讼的建议

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，但仍是最突出的一大问题。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。

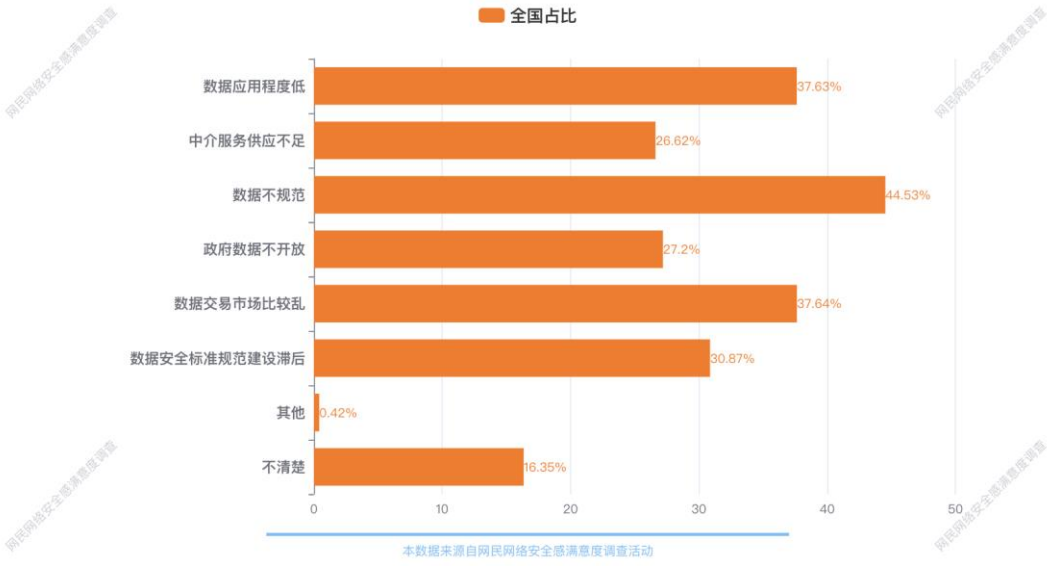

图 5-1 数据安全保护现状存在的问题

（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问题“数据不规范”在今年的受访者比例中甚至有上升的趋势，占 44.52%。该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 16.35%，较去年已下降了 5.7；同时，选择“其他”的受访者仅为 0.42%，较去年下降 4.07%。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

信息化社会中，数据的产生与流通已经变得无所不在，小到各大平台迅速收集的用户数据，大到相关产业数字化转型的加速，网络空间中数据的产生量正持续走高。然而，数据应用的效率和水平未能跟上这一步伐，这成为了制约数据价值发挥的瓶颈。。根据今年的调查发现，37.63%的受访者认为数据应用程度低，相较于去年的比例更高。这一数据反映了公众对数据应用现状的不满和期待。数据的价值并非仅仅在于其数量，更在于其质量和应用场景，如何确保数据的准确性、完整性是提升数据应用效率的关键。数据的合理合法运用不仅需要靠平台的技术、规则以及服务，也要有为用户创造足够的数据应用场景，提高用户体验。这些都需要我们从多个方面入手，全方位、多层次地推进数据全链条的建设。

（四）政府数据不开放成为网民日益关心的问题

根据调查得出，2023 年受访者的数据安全意识普遍更强，数据不仅成为了推动社会进步的重要力量，也成为了网民参与社会建设的重要途径。然而政府数据源的开放不足问题逐渐凸显，成为网民关注的焦点。27.2%的受访者认为政府数据不开放，这一比例较去年的 20.98%有了明显的提升。这一变化不仅反映了公众对数据开放需求的增加，也凸显了政府在数据开放方面存在的短板。数据开放有助于让公众了解政府的工作情况，提升政府的透明度和公信力。另外，政府可以通过开放数据激发社会的创新活力，推动各行各业的发展。但是部分政府部门对数据开放的重要性认识不足，缺乏开放数据的意识和动力，导致数据开放存在一定的困难和障碍。如何建立统一的数据开放标准和规范，加强数据安全保护，促进政府与网民之间数据的交流与沟通成为大数据时代的重要议题，

六、网民对个人信息保护和数据安全的建议和期望

（一）超半数公众网民对新法规出台持有积极态度

数据安全法、个人信息保护法等法规出台后，大多数受访者对 APP 运营者在个人信息保护方面的改善持积极态度：有 14.22%的受访者认为有明显改善，38.18%的人表示有所改善。但仍有一部分受访者（41.81%）认为改善幅度较小。尽管法规已经出台，但在实际执行中可能存在一些问题，导致个人信息保护并没有得到有效改善，甚至出现了反向的情况。

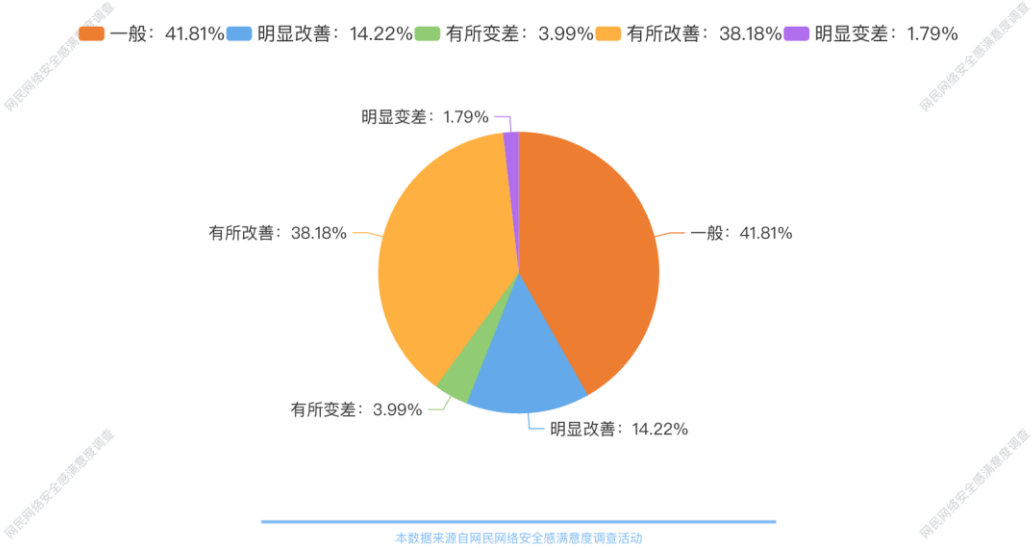

图 6-1 网民认为相关法规出台后个人信息保护的改善情况

（二）公众网民更期待宣传教育的加强与普及

受访者们对加强个人信息保护和数据治理抱有不同的期待。“加强宣传教育，提高网民维权意识和能力”和“加强执法监督力度”是受访者们最为期待的举措，分别占比 64.88%和 62.17%。还有 56.55%的受访者认为需要强化社会监督机制，49.02%的受访者认为需要完善个人信息采集和数据保护的标准规范。有关于加强措施方面，公众网民都积极地提供信息，凸显了网民法治意识以及数据安全意识的加强。

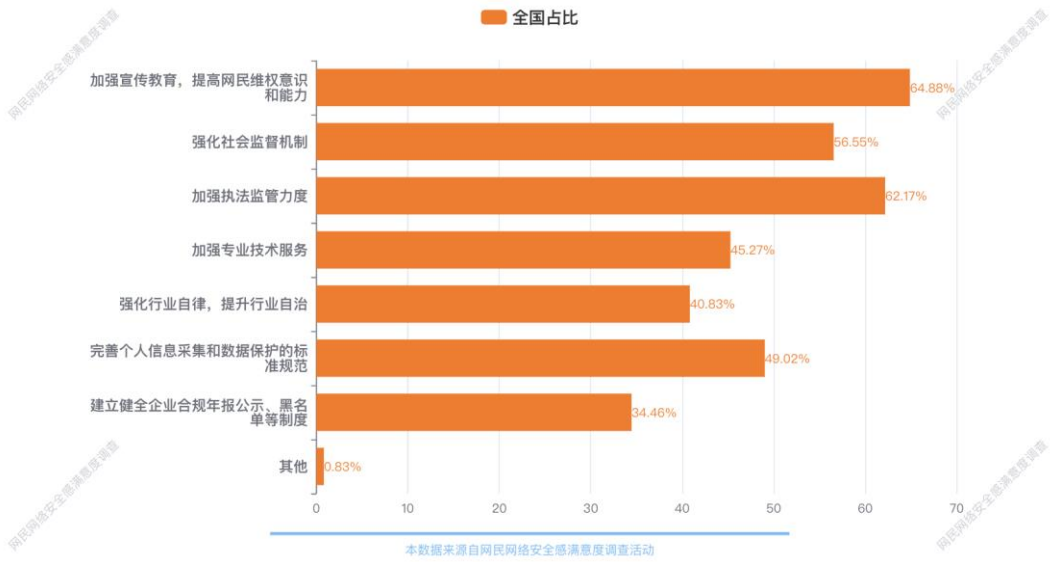

图 6-2 网民对加强个人信息保护和数据治理的期望情况

（三）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、社会、企业三个层面。政府在数据安全的保护中起到中流砥柱的作用，受访者把加强立法放在保护措施的第一位。此外，监管部门要增加更多的渠道通报违法收集者信息（45.77%）、增加更多举报平台以便老百姓申诉（42.04%），以及建立 APP 个人信息保护合规认证和监控制度，要求持证上线，违者停牌（40.03%）。半数受访者认为社会组织如行业协在个人信息保护的培训和宣传方面也应担起责任。同时，企业应减少非必要的个人信息收集和使用，同时依法保护用户信息的隐私，防止出现信息泄漏的情况。

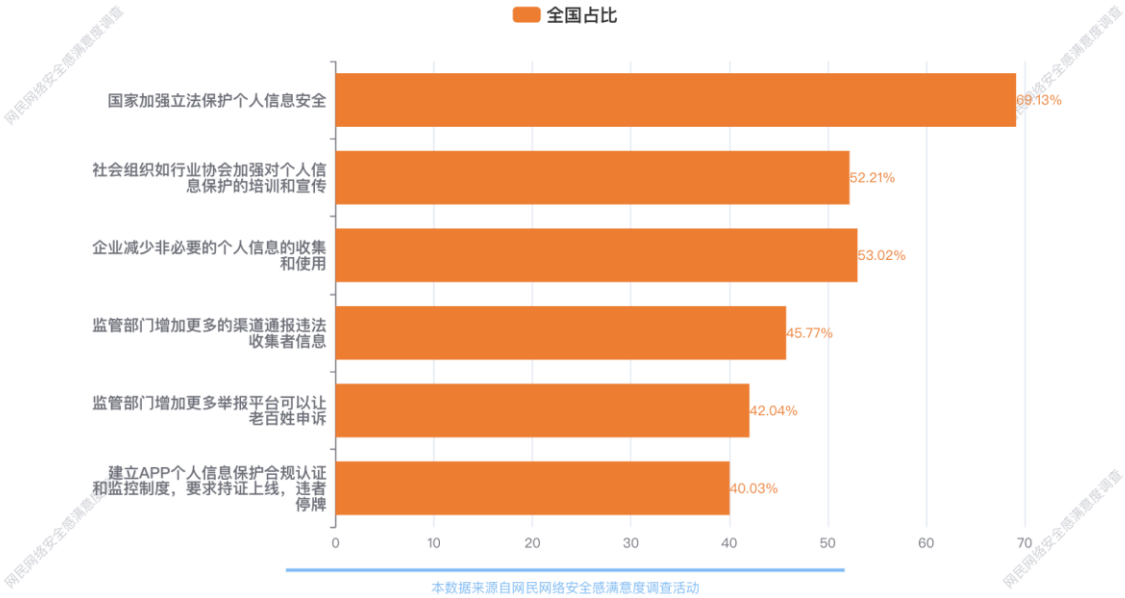

图 6-3 加强数据安全保护的重点方面

（四）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

互联网中浮现的网络诈骗、个人信息泄露、网络暴力等问题，不仅损害了网民的合法权益，也影响了互联网的健康发展。因此，更多的网民对相关法律的出台抱有积极的态度，期望通过法律手段维护自己的权益和利益，这体现了他们对互联网治理的关注和期待。因此，政府加强立法、监督力度提高、完善标准规范等规制措施是网民们关注的要点。的确，政府加大立法和监管力度能有效地遏制网络违法行为的发生，保护网民的合法权益。同时，只有制定科学、合理的标准规范，才能引导互联网健康、有序地发展。政府应积极回应公众网民的诉求，不断完善互联网法律法规体系，增强网民对互联网的信任和依赖，推动互联网行业健康、有序地发展。

五、提高网民个人信息保护和数据安全的对策

（一）全面建设数据生态，提升个人信息保护水平

数据生态不仅关乎国家竞争力的提升，也深刻影响着个人生活和社会发展的方方面面。技术的发展使个人数据逐步泛在化，每个人开始逐步拥有自己的数据存储空间，实现了去中心化的存储。数据生态是一个综合性的概念，它涵盖了数据的产生、采集、存储、处理、分析和应用等全过程。在这个过程中，各个环节相互依存，形成了一个动态平衡的系统。据调查，仍有44.53%的受访者认为数据不规范，以及37.64%的受访者认为数据交易市场比较乱，个人数据等尚未得到充分合规的利用。《个人信息保护法》和《数据安全法》都强调安全是国家利益，发展也是国家利益。我国在数据生态建设方面也主要集中在政府、企业等实体单位上。随着个人信息保护问题的凸显，严重制约了数据生态的健康发展。因此，要建立健全数据标准体系，统一数据格式和规范，提高数据的质量和可比性。其次，要加强数据共享和互通，保障数据的充分流动和有效利用。在数字经济日益成为经济增长新动能的背景下，建设数据生态不但有利于个人信息保护的完善，更是推动经济社会发展的重要力量。

（二）发展前沿数据安全技术，提高安全保障的智能化水平

数据安全的问题主要依靠安全技术来解决，而不是靠传统的人员安全、系统安全和网络安全解决。前沿数据安全技术涵盖了多个领域，包括数据加密、身份认证、访问控制、安全审计等。这些技术的不断创新与发展，为数据安全提供了有力保障。例如，刷脸和免密支付的网民比例均在不断提高，在受访者中分别达到了41.07%和12.91%。但在使用生物识别技术时，超半数以上的受访者担忧先进技术的安全性。因此前沿数据安全技术仍需不断吸收新技术、新思想，以提高安全性和效率。例如，随着人工智能技术的发展，数据安全技术也开始融入人工智能技术，形成了智能安全防护体系。通过类似的体系自动识别、分析、应对安

全威胁，提高数据安全保障的智能化水平。此外，数据安全技术涉及计算机科学、数学、密码学、网络通信等多个学科领域，需要各领域专家共同合作，形成合力。在研发技术的同时需要与法律法规、伦理道德等社会规范相结合，确保技术的合规性。

（三）企业规范数据要素市场，保障数据安全可持续发展

对于企业实践而言，需要进一步规范数据要素市场，以及数据流通、价值变现等多个环节。一个健康、规范的数据要素市场不但对于企业的长远发展至关重要，也能避免用户的数据泄露和滥用，并能够确保数据的准确性、完整性和一致性。在这样的市场中，数据的收集、存储和使用都需要遵循严格的法律法规和伦理规范。这能够有效地保护消费者的数据安全与隐私。同时，能为企业树立良好的社会形象，增强消费者的信任度。据调查显示，53.02%的受访者希望企业减少非必要的个人信息的收集和使用，以及 34.46%的受访者认为要建立健全企业合规年报公示、黑名单等制度。企业应当制定完善的数据管理制度，明确数据的来源、存储、使用和共享等方面的规范。更需要建立数据泄露应急响应机制，及时应对可能出现的数据泄露事件。最后，企业也需要透明化收集个人的数据，全面提升数据要素市场的规范化水平。这将有助于企业更好地应对数字化时代的挑战和机遇，实现可持续发展。

（四）兼顾多方监管授权，共建数据安全新框架

优质的监管手段可以兼顾政府、企业、公众。需要保护合规企业的数据授权，同时政府也能够参与监管，使用数据安全技术，密码学技术来去实现数据加密，授权企业可以正常使用个人用户、企业用户的数据源。目前很多企业已经拥有一些用户的数据，要充分考虑这些数据的脱敏或加密过程。由于在个人信息收集使用过程，公众与企业的力量明显处于不对等情况，在这种实力悬殊情况下要突出行政监管或者行政保护手段。另外，法律需要面向各领域数据权属的差异化需求，制定一些新规定。公众也需要持续提高隐私意识，并获得一定程度的数据主权。从在线购物、社交媒体到移动支付，人们的日常生活已与互联网紧密相连。个人信息不仅关乎个人隐私，还涉及到财产安全、社会信任等多个方面。一旦个人信息泄露，可能会给个人带来不可估量的损失。近年来频发的网络诈骗案件，往往都与个人信息泄露有关。51.15%的受访者认为 APP 在超出收集与功能无关的额个人信息，以及 44.9%的受访者认为在频繁索要无关权限，这些问题都可能对用户的安全造成威胁。公众也应获得更多的数据自主权，决定数据的流通的存储，从而为自己的信息负责。

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 / 139 1134 5288

邮箱：cinsabj@163.com