2021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

广东新兴国家网络安全和信息化发展研究院

中国政法大学数据法治研究院

2021年12月

本报告数据来源于 2021 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：

2021 网民网络安全感满意度调查
“个人信息保护和数据安全”专题报告

广东新兴国家网络安全和信息化发展研究院
中国政法大学数据法治研究院

2021 年 12 月

目录

一、前言

为充分发挥网络安全社会组织在网络空间建设中的桥梁作用，全面提升社会组织服务国家及地方政府网络安全建设的能力和水平，促进全国网络安全事业的发展，由全国各级网信、公安、工信、市场监管等政府部门的指导和大力支持、全国135家网络社会组织共同发起，以“网络安全为人民、网络安全靠人民”为主题的2021网民网络安全感满意度调查活动于2021年8月3日启动。本活动持续10天，共收回问卷284.5235万份，经数据清洗消除无效数据后，有效问卷264.7339万份。

此次发布的调查问卷分为公众版和从业人员版。公众版从大众化的角度，设置八个专题二级问卷，分别是网络安全法治社会建设、遏制惩处网络违法犯罪、个人信息保护和数据安全、网络购物权益保护、未成年人网络权益保护、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、数字鸿沟消除与乡村振兴；从业人员版从网络从业人员的技术专业化角度，设置四个专题二级问卷，分别是等级保护实施与企业合规、行业发展与生态建设、新技术应用与网络安全、科技创新与人才培养。其中“个人信息保护和数据安全”作为二级问卷之一，围绕我国个人信息保护和数据安全设置十八个问题。

为全面分析我国个人信息保护和数据安全情况，基于发起单位调查所得的数据,由广东新兴国家网络安全和信息化发展研究院主办、中国政法大学数据法治研究院承办，围绕本专题及聚焦行业趋势，结合分析得出五项调查结论，汇总形成本报告。

2021年12月6日至10日，2021年全国网民网络安全感满意度调查报告发布周在北京面向全社会举办。《2021年网民网络安全感满意度调查“个人信息保护和数据安全”专题报告》作为发布周的重要组成

部分，不仅反映了现阶段个人信息保护和数据安全在数据要素化、可视化方向的具体实践，也为网络安全行业发展提供决策思考和可行路径，进而为网络空间建设提供有益参考。

二、加强个人信息保护和数据安全治理的背景

随着“大数据”时代的到来，“数据”开始充斥人们的生活，信息化社会的大量场景中，是数据而非我们自身决定了我们是谁，数据勾画了我们的行为轨迹，标识了我们的数字身份，界定了我们的网络关系。在由知识经济向数字经济过渡的过程中，数据也是一项重要的生产资料。中共中央、国务院于2020年3月发布《关于构建更加完善的要素市场化配置体制机制的意见》将数据作为一种新型生产要素与劳动力、土地、资本、技术等要素并列，提出要加快培育数据要素市场，探索建立统一规范的数据管理制度，提高数据质量和规范性，推动完善适用于大数据环境下的数据分类分级安全保护制度，推动数据采集标准化与政府数据开放共享。

数据的价值在于使用，若不能对收集到的海量数据进行分析利用，珍贵的数据便只是空占存储器的二进制代码。大数据的价值并非单纯来源于它的基本用途，更来自于对数据的二次利用，但与此同时，也必然产生技术发展的溢出效应，衍生各种风险。大量个人信息侵权与数据泄露案件的出现让人们的个人信息保护与数据安全需求进一步增强。为回应这一现实需求，各国纷纷出台或更新了数据保护的法案，至2021年，全球已有超过130个国家制定了个人信息保护相关法律，如欧盟的《通用数据保护条例》（GDPR）、美国的《加州消费者隐私权法案》（CCPA），我国新出台的《民法典》《个人信息保护法》《数据安全法》也对该问题做出了详细规定。尽管立法理念与模式不一，侧重点各不相同，欧盟强调保障人权，赋予个人强大的自主决定权；美国在立法与司法中均把经济与科技的发展作为重要考量。但无论是哪一种立法模式，都显示出日趋严格的个人信息保护与数据安全治理趋势，如果不解决数据安全问题，就无法进一步促进数字经济发展，驱动国家治理能力和治理体系现代化已成为各国共识。因此，如何在释放数据潜在价值的同时保护个人信息，保障数据安全，成为“时代之问”。

三、我国个人信息保护和数据安全法治建设现状

党的十八大以来，我国加快完善个人信息保护和数据安全法治体系建设，建立健全数字领域法治框架体系，有效保障了公民、法人和其他组织的合法权益。

在个人信息保护层面，我国正在形成以专门法为基础，以各领域分散立法为重要补充的个人信息保护法治体系。一是《个人信息保护法》正式出台。《个人信息保护法》确立以“告知—同意”为核心的个人信息处理一系列规则，完善了个人信息跨境提供规则，明确个人信息处理活动中个人的权利和处理者义务，根据个人信息处理的不同环节、不同个人信息种类，对个人信息的共同处理、委托处理、向第三方提供、公开、用于自动化决策、处理已公开的个人信息等提出有针对性的要求。二是现行多部法律、行政法规中都设定个人信息保护的相关条款。2012年底，全国人大常委会通过了《关于加强网络信息保护的决定》，明确规定保护公民个人及法人信息安全。同时，《网络安全法》《民法典》以及相关行业、领域的法律中都涉及个人信息保护条款。三是我国多个行业监管部门以部门规章的形式对本领域的个人信息保护问题作出了规定。工信部早在2013年就出台了《电信和互联网用户个人信息保护规定》，对电信和互联网领域个人信息保护工作作出了专门规定。此外，金融、医疗健康、电子商务等领域也作出了相应的个人信息保护规则。

在数据安全治理层面，我国在制度设计层面进一步突出数据安全问题在网络安全保护中的重要地位，以专门立法与行政法规、地方性法规为细化、补充的方式构建起数据安全治理法律体系。一是确立数据安全保护基本框架。2021年出台的《数据安全法》坚持以数据开发利用和产业发展促进数据安全，深化数据安全体制建设，正式确立了数据安全保护管理各项基本制度，明确了数据管理者和运营者的数据保护责任、政务数据的开放规范与机制，指明了数据保护的工作方向，对释放数据的生产要素价值，缓解数据安全与开放应用之间的矛盾具有重要意义。二是通过法律体系的完善，消除数据流动带来的国家安全风险。如《网络安全审查办法》，承接2017年通过的《网络安全法》，将数据处理者开展数据处理活动也纳入到了网络安全审查的范围，要求掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查；正在征求意见的《网络数据安全管理条例（征求意见稿）》更进一步，将数据分为一般数据、重要数据、核心数据，并规定对核心数据实施严格保护，数据处理者向境外提供重要数据或者关键信息

基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息，应当通过国家网信部门组织的数据出境安全评估。三是形成数据安全规范标准体系。国家标准化管理委员会和全国信息安全标准化技术委员会已针对数据安全活动制定发布了一系列标准指南，既包含《数据交易服务安全要求》、《政务信息共享数据安全技术要求》等以应用场景为划分的标准，又包含《基因识别数据安全要求》、《声纹识别数据安全要求》、《步态识别数据安全要求》等针对具体技术的标准，形成了较为完整的数据安全规范标准体系。工信部《电信和互联网行业数据安全标准体系建设指南》的制定与出台，将充分发挥标准的顶层设计和基础引领作用，为保障电信和互联网行业网络数据安全、促进网络数据合理有序流动提供进一步有力支撑。四是出台地方数据条例推动本地区数字化发展，保障数据安全。《数据安全法》出台后，各地数据条例的制定进程加快，如《深圳经济特区数据条例》将于2022年1月1日生效，天津市将《天津市数据安全管理办法（暂行）》有效期延长至2023年，2021年11月26日，上海市十五届人大常委会第37次会议表决通过《上海市数据条例》，《浙江省公共数据条例（草案）》也正在征求意见。各地制定的数据条例立足于本省市的数字经济发展与数据安全现状，弥补了作为框架性立法的《数据安全法》过于宏观，无法直接指导实践的缺点。但各省市规定的不一致，也导致了企业数据安全合规成本增加，因此地方数据条例制定过程中，除了需要考虑本省市的情况，也需做好与《数据安全法》《网络安全法》《个人信息保护法》等法律法规以及其他省市数据条例的衔接。

四、公众网民对个人信息保护和数据安全的感受情况

个人信息保护与数据安全治理，与社会公众的切身利益息息相关，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）公众网民对我国个人信息保护的整体评价

个人信息保护是当前网民广泛关注的重点问题。根据数据显示，目前网民对我国个人信息保护现状的满意度大致呈现“三三分”态势，37.52%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”；35.86%的受访人群认为当前状况“一般”；26.62%的受访人群认为当前状况“不太好”或“非常不好”。通过时间维度纵向比较来看，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。

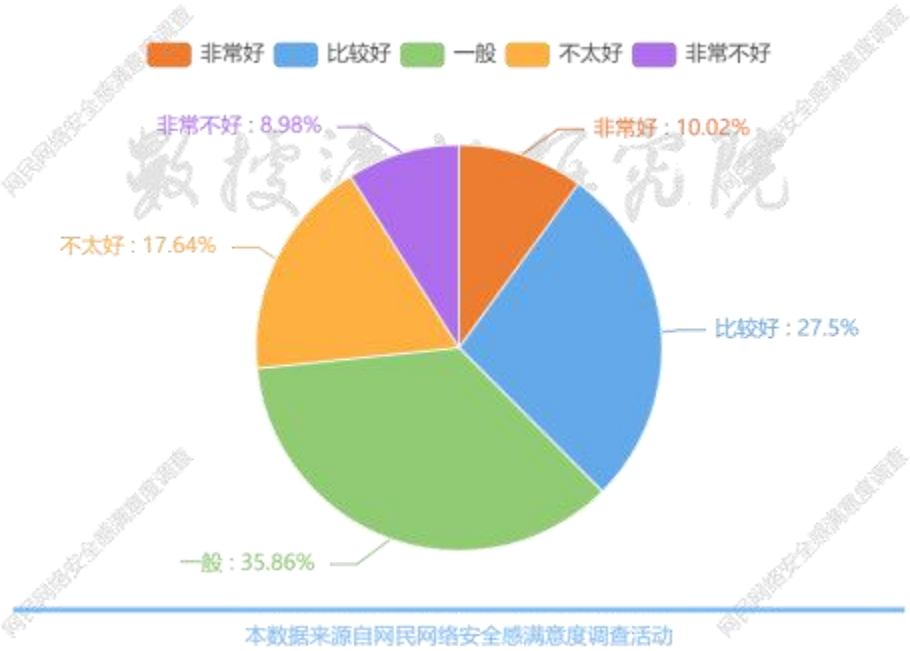

图3-1：公众网民对个人信息保护现状的评价

（二）公众网民对个人信息泄露的感受情况

公众网民对个人信息泄露情况感受强烈。调查显示，近一年来，23.08%的受访人群“没有遇到”或“很少遇到”个人信息泄露；35.66%的受访人群“有一些”信息泄露遭遇；41.25%的受访人群遭遇“比较多”甚至“非常多”信息泄露。

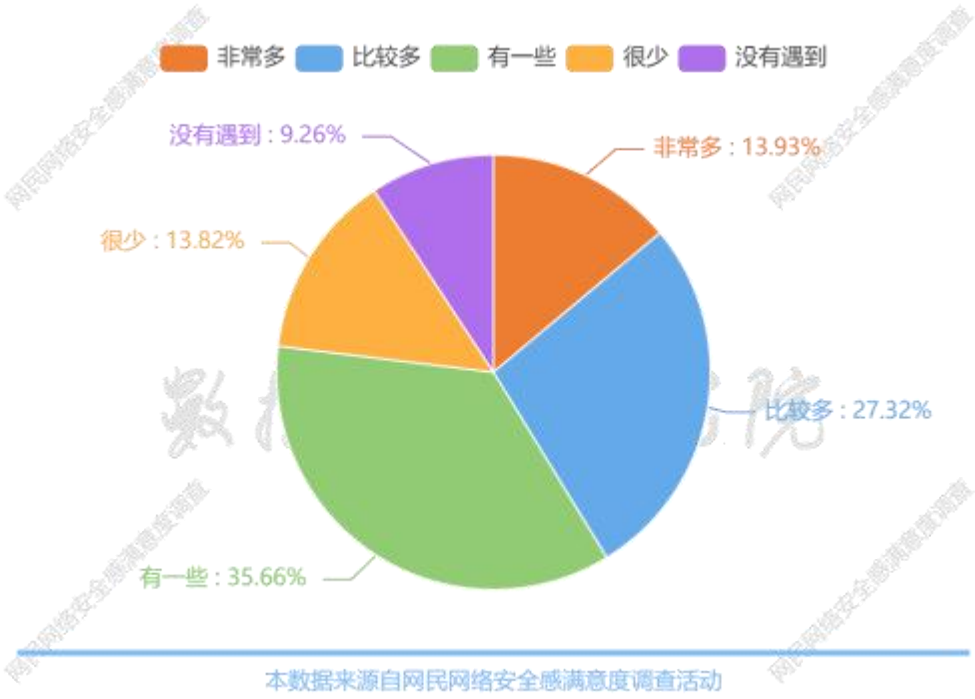

图3-2：近一年公众网民遭遇个人信息泄露情况

（三）公众网民对个人信息风险的感知情况

公众网民通常通过个人信息泄露之后接收到的各式各样骚扰来判断自身个人信息风险。近八成网民接到各类中介的推销电话；超过六成网民收到垃圾邮件；近六成网民收到相关性的推销短信。除了上述骚扰方式，公众网民还可以从其他途径推测出个人信息风险，例如超过四成网民认为遭遇大数据杀熟是因为个人信息已经泄露，近四成网民遭遇或认为，默认勾选同意《服务协议》，允许应用收集用户信息（包括被第三方保存），会导致个人信息泄露等等。

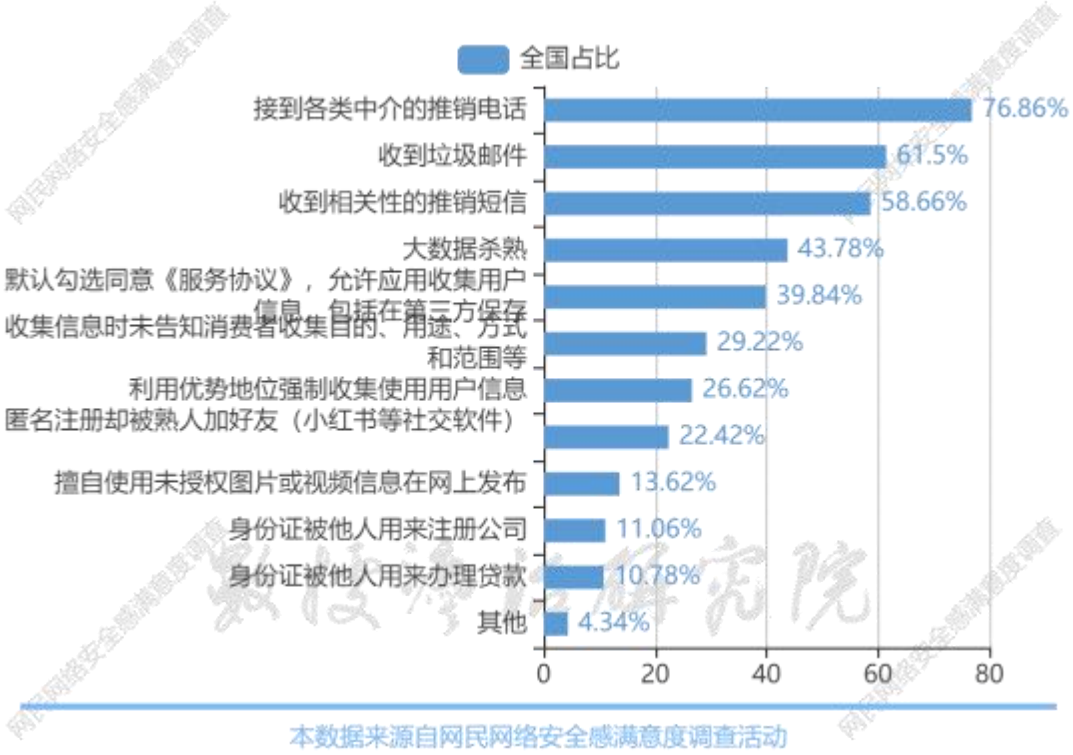

图3-3：网民遭遇的能够推知个人信息泄露的情况

（四）公众网民重点关注生物识别信息风险

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，但由于生活识别信息的不可更改特点，网民对生物识别信息的利用充满忧虑。数据显示，57.96%的网民对生物识别技术的安全性“比较”或“非常”担心；25.1%的网民态度“一般”，无明显倾向；仅16.94%的网民对生物识别技术的安全性“很少”或“没有”担心。

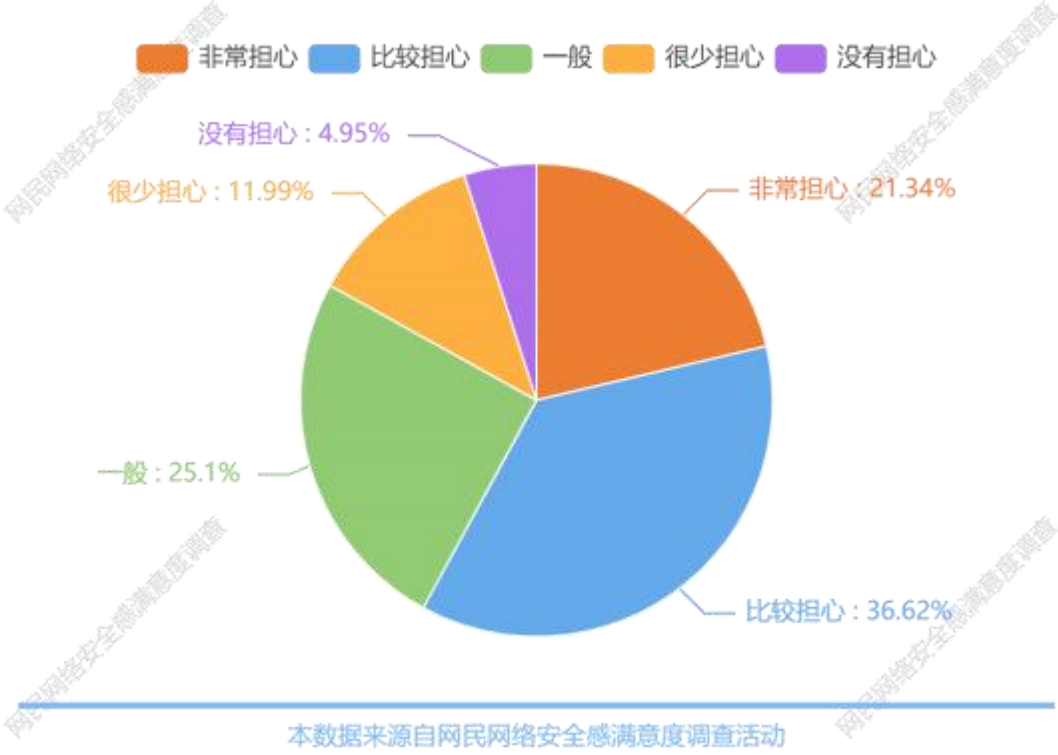

图3-4：网民对生物识别技术泄露个人信息的主观倾向

网民对于生物识别信息风险的担忧也在线上支付方式选择方面得以验证。数据显示，大多数网民采用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。

五、公众网民对个人信息和数据风险的反馈情况

（一）网民对各类网络服务的个人信息风险感受不一

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，超过六成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务的个人信息风险相对较低。

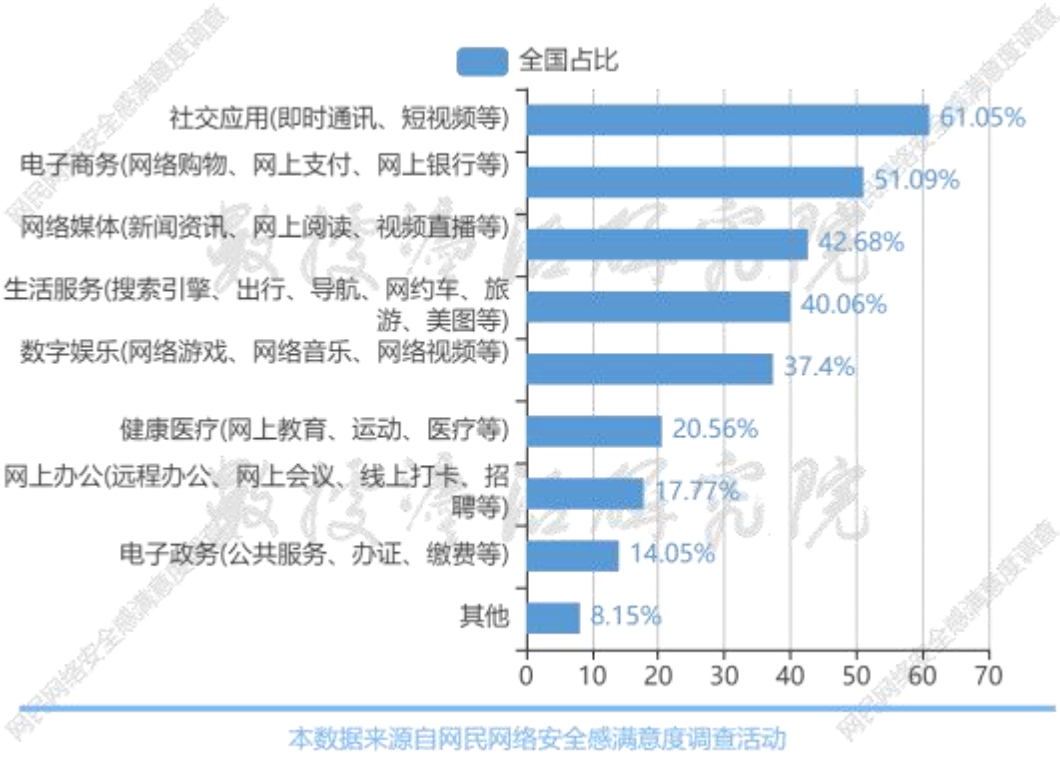

图4-1：个人信息保护情况受关注的APP类型

（二）网民认为个人信息泄露发生在多个环节

调查显示，公众网民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76.65%；其次，超过半数的受访群体认为参

与网上测试、投票、抽奖活动可能会导致个人信息泄露；超过四成网民认为点击网上不明二维码、链接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。

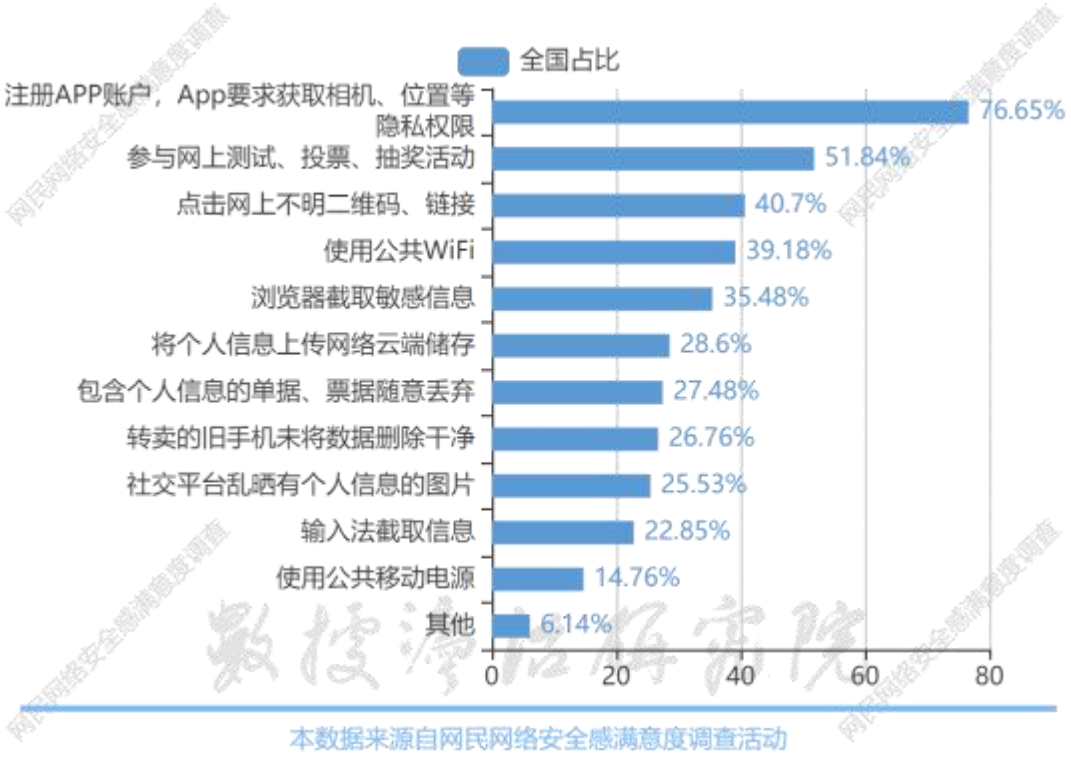

图4-2：网民认为可能的个人信息泄露途径

（三）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。调查显示，60.12%的受访群体遭遇过APP收集与功能无关的个人信息，57.78%的受访群体遭遇过APP频繁索要无关权限，50.25%的受访群体遭遇过APP强制索取无关权限，不授权就闪退，50.02%的受访群体遭遇过APP默认捆绑功能并一揽子同意。

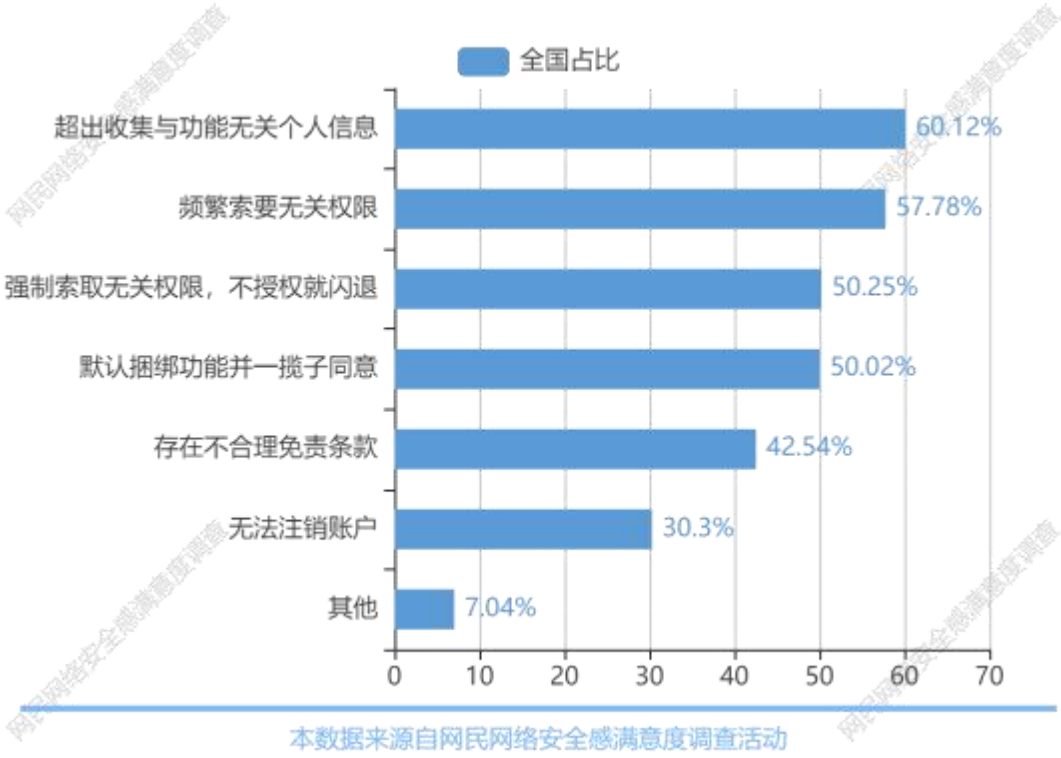

图4-3：网民认为APP收集信息过程中存在的问题

（四）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。调查显示，约九成网民在日常上网时收到过精准广告，约一成网民很少或者没有收到过精准广告。在广告推送的过程中，四成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；超过两成网民表示经营者大部分都没有征得用户同意；还有两成网民不清楚发送广告是否征得过其同意。

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。三成网民不清楚其收到的精准广告是否提供了退出机制；超过三成网民表示大部分甚至全部精准广告都没有提供退出机制；一成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。

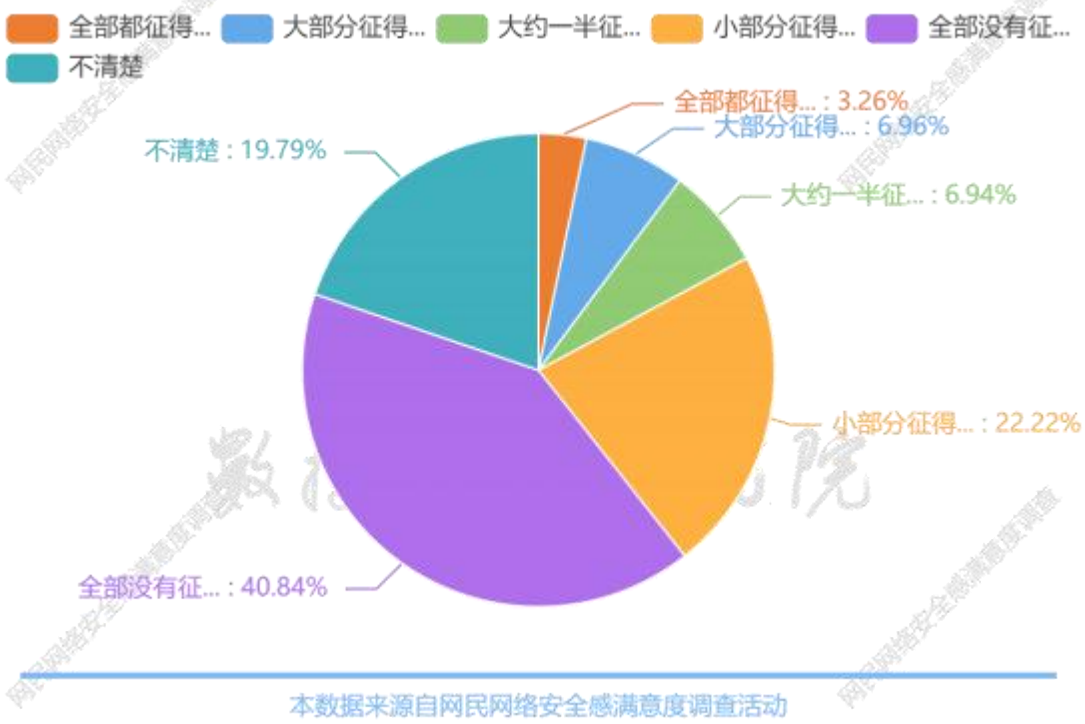

图4-4-1：经营者发布精准广告征得网民同意的情况

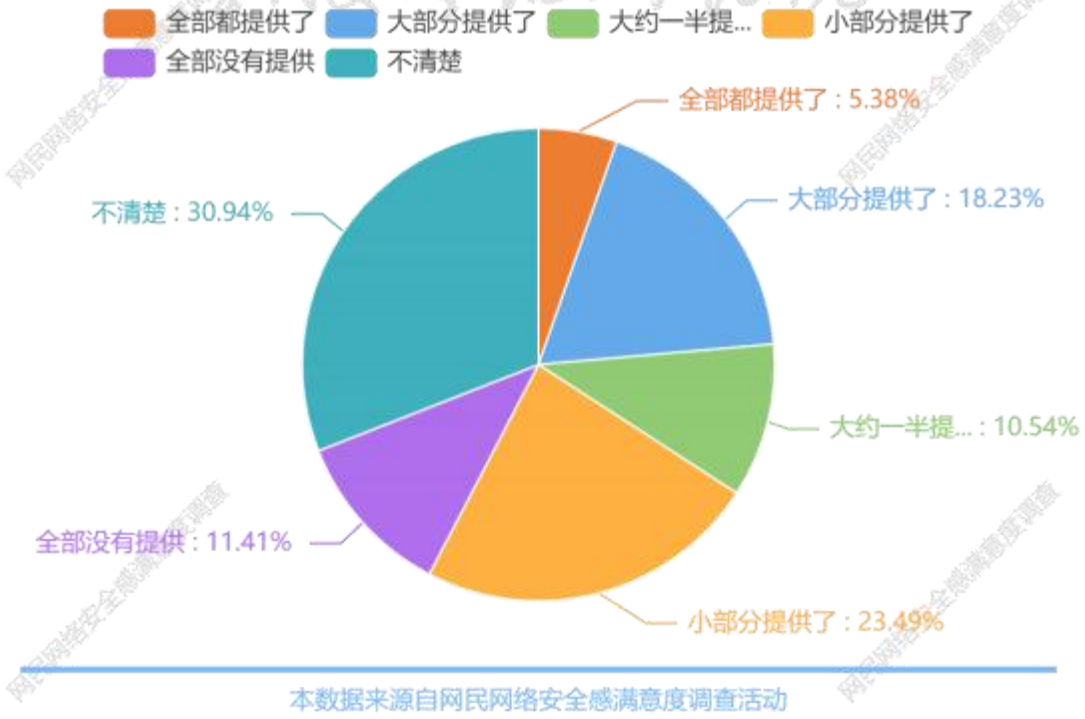

图4-4-2：精准广告退出机制的提供情况

六、数据安全保护存在的问题

在开放性反馈中，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，数据市场交易市场混乱，以及数据不规范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。

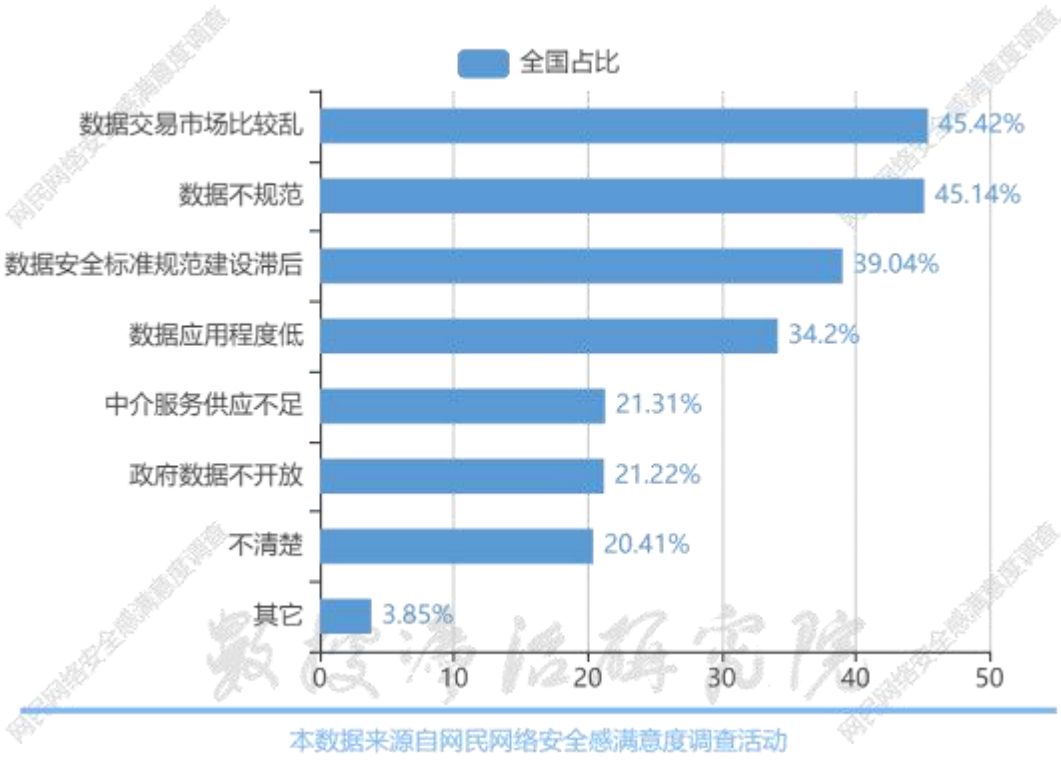

图5-1：网民认为当前数据安全保护存在的问题

（一）数据交易市场秩序混乱

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。

（二）数据规范问题

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。

（三）数据应用程度低

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）数据中介服务缺乏

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21.31%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）政府数据开放不足

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21.22%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）增强制度供给

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，自今年出台《数据安全法》以来，《个人信息保护法》相继出台，《网络数据安全管理条例（征求意见稿）》目前也开始向公众征求意见，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。

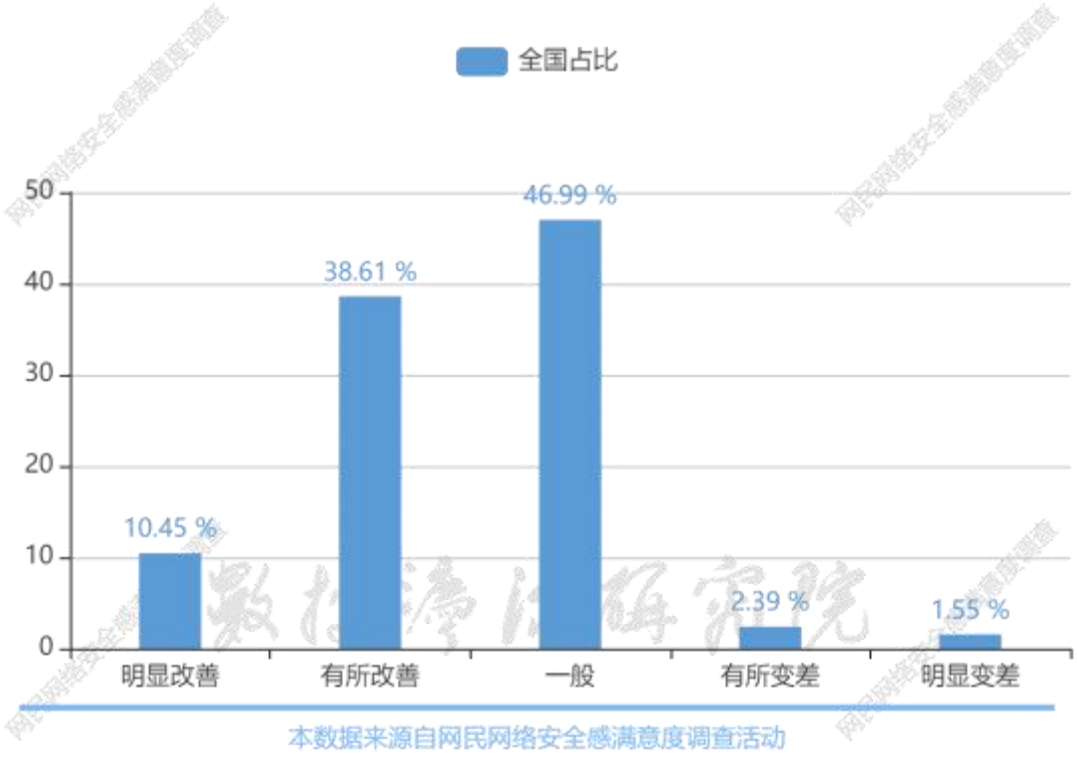

图6-2：网民认为数据安全法出台后，APP运营者在个人信息保护方面是否有改善

（二）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）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51.55%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）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）通过公权力控制维度保护个人信息

通过对公众网民对个人信息保护措施进行分析，公众网民倾向于主要通过国家立法、部门监管等公权力控制维度加强个人信息保护和数据保护。超过80%的网民认为通过国家加强立法保护个人信息安全是目前最有效的措施。这启示，可通过国家建立APP个人信息保护合规认证和监控制度，对运营者设立门槛，增设申诉管道和通报管道，通过公权力控制代表公众网民来进行个人信息保护手段的行使，借此保护个人信息和数据安全。

（二）选择低成本的网民参与个人信息泄露防范手段

网民对个人信息泄露保持着较强的警惕心理，在遭遇个人信息泄露之后会采取多种方式解决，极少数网民会对个人信息泄露情况不予理会。根据数据分析，近六成半网民会在个人信息泄露之后更换账号、密码，具有良好的个人信息安全风险意识和补救意识。近六成网民会在信息泄露之后提醒亲友，防止受骗。近四成网民会选择报警维护自身权益。超过一成网民会寻找律师维护自身权益。通过数据分析发现，个人信息泄露后，大部分具有风险意识的网民群体更倾向于选择成本较低的补救措施，对于报警和寻找律师这种成本较高的方式选择较少。这启示，未来在进行个人信息保护制度设计时，应选择低成本的，网民易于操作的个人信息泄露防范手段，例如设立专门个人信息泄露通知处理网站、设立“原则加入、明示退出”的个人信息公益诉讼参与制度，保障线民个人信息泄露带来损害的求偿权。

（三）加快制定数据分类分级目录

网络安全的核心是数据安全，数据安全的逻辑起点是数据的分类分级保护。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。以数据分类分级保障数据安全，既需要自上而下由国家建立数据分类分级保护制度，又需要自下而上由企业在组织内部对业务开展过程中获取、产生的数据进行分类分级。分

类的核心标准为数据的重要程度和数据被滥用可能给个人、社会、国家带来的风险大小。

国家根据数据重要性和风险性对数据进行分类分级后，需要以整体数据目录与重点数据目录的形式，确定每一种数据的可开放限度。对数据进行分类的方式是多维的，但为保证数据目录的可用性，避免概念上的争议，同时考虑到数据外延会随着技术的发展与计算能力的提升而不断扩大，整体数据目录与重点数据目录的制定均需遵循法律优先、规范性、体系性、稳定性、可拓展性等原则。

（四）加快建立数据交易市场

网民认为当前数据安全保护存在的最主要问题是数据交易市场秩序混乱，这反映出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数据交易平台的数据供给作用，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。

（五）构建企业内部数据安全监管体系

网民认为《数据安全法》对个人信息保护的效果有限的一个重要原因在于企业未做好内部合规，APP数据安全问题频发，因此有必要构建企业内部数据安全监管体系，以自检促合规。数据合规的意义在于，数据处理者的数据处理行为，经法律授权的官方机构或由法律授权的官方机构的委托机构认定完全符合法律规定，则即使后续出现数据泄露等问题，也应作为意外事故处理，将数据处理者所需承担的责任降至最低。根据《数据安全法》的规定，重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。并参照国家数据安全机制，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全，并定期对数据处理活动开展风险评估。在发现数据安全缺陷、

漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报

网安联微信公众号

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