

2019 网民网络安全感满意度 “网络安全法制建设”专题调查报告

2019 年 9 月

公安部第三研究所网络安全法律研究中心

目 录

前言.....	1
一、我国网络安全法制建设历程.....	2
二、“网络安全法制建设”网民安全感满意度调查分析.....	5
(一) 调查过程和数据基本情况.....	5
(二) “网络安全法制建设”满意度调查发现.....	7
1. 满意度调查结论.....	7
2. 满意度调查结论分析.....	8
1) 网民网络安全感有所提升，对网络安全法制建设满意度较高.....	8
2) 网络安全法制宣传教育成效显著，主渠道作用不可替代.....	11
3) 网络骚扰行为、违法有害信息内容、侵犯个人信息以及网络违法犯罪成为公众最常见的四大网络安全问题.....	14
4) 虚假广告、网络谣言和淫秽色情信息成为最常见的三类网络违法有害信息.....	20
5) 加强网络安全法制建设成为社会解决网络安全问题的首选途径.....	23
6) 个人信息保护、网络平台责任和数据安全保护成为三大核心诉求.....	24
7) 公众从知法到用法的需求觉醒，权利救济途径有待拓宽.....	26
8) 未成年人和老年群体用网环境亟待改善.....	28
9) 网络安全治理架构成为 5G 安全关注重点.....	30

10) 等保基础价值得到充分认可, 落实推进仍需加强.....	32
11) 平台责任落实不到位, 主体责任仍需加强.....	37
12) 网络安全执法工作满意度较高, 执法力度得到认可...	40
三、“网络安全法制建设”网民安全感满意度调查结论和建议....	44
(一) 立足核心诉求问题, 实施精准立法策略.....	44
(二) 深化网络生态治理, 净化网络空间环境.....	45
(三) 关注新技术新应用, 创新安全治理路径.....	46
(四) 加快等保配套出台, 持续推进宣传贯彻.....	47
(五) 加强企业合规指引, 推进平台责任落实.....	48
附件: 我国网络安全相关战略、立法及配套分类总览.....	49

前 言

作为 2019 年国家网络安全周的重要组成部分，由公安部网络安全保卫局指导、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 2019 网民网络安全感满意度调查活动于 2019 年 8 月 13 日启动。本活动持续 10 天，共收回问卷 221266 份，经数据清洗消除无效数据后，有效问卷 198588 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，设置七个专题二级问卷，分别是网络安全法制建设、个人信息保护、遏制惩处网络违法犯罪、网络购物、未成年人网络权益保护、网络平台企业安全监管、数字政府安全服务。“网络安全法制建设”作为二级问卷之一，围绕我国网络安全立法设置五个问题。

为全面分析我国网络安全法制建设情况，基于发起单位调查所得的数据，公安部第三研究所网络安全法律研究中心围绕“网络安全法制建设”专题及与网络安全法制建设相关的其他调查问题，分析得出十二项调查结论，汇总形成本报告。

一、我国网络安全法制建设历程

大数据、云计算、人工智能等新一代信息技术的蓬勃兴起与发展在全球范围内掀起了新一轮的科技革命与产业变革。信息化成为当今世界发展的主要趋势，也成为推动经济发展和社会变革的重要力量。经过 20 多年的发展，进入新世纪特别是党的十八大以来，我国国家信息化发展能力显著提升。以习近平同志为核心的党中央坚持从发展中国特色社会主义、实现中华民族伟大复兴中国梦的战略高度，系统部署和全面推进信息化工作，推动我国网信事业取得历史性成就。截至 2019 年 6 月，我国网民规模已达 8.54 亿，互联网普及率达 61.2%，成为名副其实的网络大国。¹随着国家“互联网+”、数字化转型战略的深化推进，网络与人民群众的生产生活深度融合，网络在政治、经济、文化等各个领域中的作用愈发凸显。

与此同时，信息化带来的网络安全风险范围和内容也不断扩大和演化，网络安全形势不容乐观。当前，我国网络信任危机加剧、数据泄露和滥用事件频发、网络虚假信息泛滥、电信诈骗和跨境赌博等安全风险治理态势未得到有效扭转，数据跨境主导竞争激烈，网络舆情背后情势复杂，网络意识形态渗透加剧，国家政治、经济、文化、社会安全面临新的威胁。此外，围绕下一代通讯技术架构的物联网、人工智能、区块链等新技术引发信息传输在范围、频度的基础性变革，新技术新应用潜在风险的不确定性也影响着新时代的网络安全。

纵览全球，各国纷纷将网络安全提升到国家战略高度，国际网络

¹ 数据来源：中国互联网络信息中心（CNNIC）第 44 次《中国互联网络发展状况统计报告》。

安全相关政策立法也呈爆发趋势，纷纷建立全方位、更立体、更具弹性与前瞻性的网络安全法律体系，不断推动关键信息基础设施保护、个人信息保护、网络内容与平台治理、网络安全审查、反恐与情报、网络监控和执法、物联网安全、密码管理、犯罪和刑罚等“行动域”的立法进程。

从国内情况来看，一方面，由于网络的无国界性，我国面临着全球同步的网络安全风险和威胁。另一方面，由于我国网民体量、网络基础设施建设水平、区域发展以及政治、经济、文化、法律环境等诸多因素，我国面临着更为复杂的安全隐患。这些都深度影响着我国网络安全生态建设，成为影响人民幸福感、获得感、安全感的重要因素。

为全面提升网络安全保障能力，筑牢网络安全防线，近年来，以总体国家安全观和网络强国战略思想为指导，我国网络空间治理不断开创新局面，走出了一条既与国际接轨，又不乏中国特色的网络安全法治之路。从 1994 年国务院 147 号令《计算机信息系统安全保护条例》，到 2000 年《全国人民代表大会常务委员会关于维护互联网安全的决定》，再到 2016 年《网络安全法》及其配套法规的不断优化，我国网络安全法治建设取得了良好成效，关键信息基础设施、网络安全等级保护、个人信息保护、数据出境安全评估、网络安全审查等重要制度基本建立，整体上实现了网络安全立法从无到有，从碎片式到体系化，从粗放式到精细化的转变，为我国互联网健康、有序的发展奠定了基础。

作为网络空间安全保障的基本法，《网络安全法》正式施行 2 年

多以来，不断赋能保护行动、配套制度、行政执法和司法实践，为全面提升人民群众的上网安全感和满意度发挥了重要作用。电力、能源、水利、教育、医疗、金融等行业的网络安全保护行动全面铺开；《网络安全等级保护条例》《关键信息基础设施安全保护条例》《数据安全管理办法》《个人信息出境安全评估办法》等重要配套制度加紧推进；区块链、人工智能等新技术新应用领域的网络安全制度规范也开始初步探索。除国家顶层制度不断完善外，贵州、天津、上海等地也充分结合本地区的特点、优势及工作实际，积极开展网络安全相关制度建设的地方试点；执法方面，围绕《网络安全法》及配套规范的执法能力提升和规范化建设工作不断强化，数据治理、“净网”行动、“护网”行动等空前有力；司法层面，全面发挥司法在推动网络经济创新发展、保障网络安全、构建互联网治理体系方面的职能作用，以设立互联网法院为标志的智慧司法不断取得新成果。

整体来看，我国网络安全法制建设整体向好，但仍然存在着规则有待细化和统一、主体责任有待加强、网络安全意识有待提升等问题。此外，由于技术、经济和社会发展的不确定性和国际博弈的波谲云诡，新技术、新应用、新业态、新规则不断冲击既有的法治理念与监管规则。如何预判新技术新应用的潜在安全风险，以法的强制性、稳定性更好地应对技术的不确定性挑战，提升网络空间长治久安的法制效力，成为新时代、新业态亟待解决的重要议题。我国网络安全法制建设之路，任重道远。

二、“网络安全法制建设”网民安全感满意度调查分析

2019 年网民网络安全感满意度调查作为国家网络安全周系列活动的一部分，得到社会大力支持。在广泛调研和收集网民网络安全感满意度的基础上，对我国网络安全法制建设现状进行分析，从而提出针对性建议，为我国网络空间治理提供支撑。

（一）调查过程和数据基本情况

此次活动设置的调查问卷分为公众版和从业人员版，其中从业人员版中根据所面向群体不同，将从业人员分为八类，分别是：1）网络服务提供者中从事网络安全相关工作的从业人员；2）网络服务提供者中从事非网络安全相关工作的从业人员；3）网络安全产品、服务提供者的从业人员；4）网络行业协会的从业人员；5）政府网络安全监督管理部门的从业人员；6）国有企事业单位的从业人员；7）科研机构、大学的从业人员；8）其他联网使用单位的从业人员。

此次调查共收回问卷 221266 份，经数据清洗消除无效数据后，有效问卷 198588 份。其中公众版 189495 份，有效问卷 172075 份纳入统计；从业人员版 31771 份，有效问卷 26513 份纳入统计（八类从业人员收回的有效问卷数量见表 1）。

人员类别	人员属性	有效问卷数量
网络服务提供者中从事网络安全相关工作的从业人员	对网络安全业务比较熟悉，对业界的安全状况的实际情况比较了解	4430 份
网络服务提供者中从事非网络安全相关工作的	对网络行业的情况比较熟悉，但对专业的网络安全业务不一定了解	4645 份

从业人员		
网络安全产品、服务提供者的从业人员	熟悉安全技术和产业发展状况，对安全问题的认识比较深刻，评价一般较为保守	3705 份
网络行业协会的从业人员	对网络行业情况比较熟悉，态度比较持平	915 份
政府网络安全监督管理部门的从业人员	熟悉政府政策要求	1027 份
国有企事业单位的从业人员	主要是网络用户的身份，单位业务管理比较规范	2971 份
科研机构、大学的从业人员	熟悉安全学科和安全技术发展状况，态度比较中立	2442 份
其他联网使用单位的从业人员	主要是网络用户身份，态度比较中立	6378 份

表 1：调查的从业人员类别、属性及有效问卷数量

公众版下设立网络安全法制建设、个人信息保护、遏制网络违法犯罪行为、未成年人网络权益保护等七项二级问卷，共有 12.3 万网民参加二级问卷调查，其中 65920 人参加“网络安全法制建设专题”调查。

为全面分析我国网络安全法制建设情况，本报告围绕“网络安全法制建设”专题及与网络安全法制建设相关的其他调查问题展开，内容涉及公众和从业人员参与回答的选择题和 9656 条主观题答案。

因每项问题面向群体不同，为方便理解，本报告中“网民”指的是公众以及受调查的部分从业人员；“公众”指的是公众版问卷中参与调查的公众；“受调查从业人员”指的是从业人员版问卷中参与调查的从业人员。

（二）“网络安全法制建设”满意度调查发现

通过对调查结果进行分析，围绕我国网络安全法制建设共形成十二项结论，涉及网民网络安全感、网络安全法制宣传教育、常见网络安全问题、核心立法诉求等内容。

1. 满意度调查结论

经过调查，得出以下结论：

第一，当前，我国网络安全法制建设态势总体向好，网民网络安全感较 2018 年有所提升，对网络安全法制建设的满意度较高。

第二，在主渠道发挥核心作用的背景下，公众对《网络安全法》的了解程度稳步提高。

第三，网络骚扰行为、违法有害信息内容、侵犯公民个人信息以及网络违法犯罪成为公众最常见的四大网络安全问题。

第四，违法有害信息内容方面，虚假广告、网络谣言和淫秽色情信息成为最常见的三类违法有害信息。

第五，面对严峻的网络安全形势，加强网络安全法制建设已经成为网民解决网络安全问题的首选途径。

第六，个人信息保护、网络平台责任和数据安全保护成为三大核心诉求。

第七，公众从知法到用法的需求觉醒，个人信息保护方法、网络诈骗识别方法、病毒及木马防范方法成为公众最迫切的网络安全知识需求。

第八，未成年人上网情况日益普遍，网络游戏已经成为未成年人

最常接触的应用服务。公众对我国未成年人网络权益保护状况评价好坏参半，防沉迷成为未成年人用网安全方面的首要诉求。此外，老年群体上网安全保障也成为公众强烈呼吁的要求之一。

第九，网络安全等级保护制度作为我国网络安全基础性保障制度，作用和价值得到社会和行业认可，已成为各部门各单位开展网络安全工作的基本方法和遵循，但仍存在等保 2.0 国家标准相关要求普及程度相对不高，从业人员培训需求呼声强烈的问题。

第十，5G 应用方面，建立适应 5G 应用需要的网络安全治理架构成为最受关注的安全重点。加强 5G 网络安全技术标准体系建设、加强对 5G 网络信息安全核心技术的知识产权管理、制定针对不同应用场景的法律法规及监管措施被认为是最应重点加强的三项安全措施。

第十一，互联网企业的网络安全责任落实情况在公众的认可程度有待提高，公众对互联网企业网络安全履责情况评价不一，75%以上的公众认为互联网企业存在有意不承担或少承担网络安全责任的情况。

第十二，执法方面，公众对政府部门在遏制网络违法犯罪方面的工作成效满意度较高，网络安全执法力度得到一定认可。人员、专业技术能力被认为是制约网络安全执法能力的主要因素。

2. 满意度调查结论分析

以下对十二项调查结论进行详细分析：

1) 网民网络安全感有所提升，对网络安全法制建设满意度较高

调查显示，51.25%的公众认为网络环境是安全的，其中 11.38%

的公众认为非常安全，39.87%认为安全。

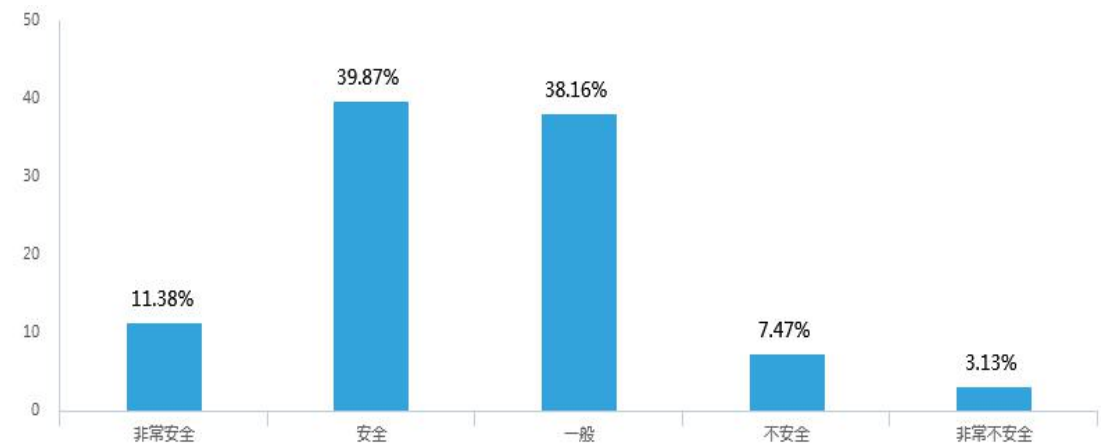


表 2：公众网络安全感评价

与 2018 年相比，48.76%的公众认为网络安全感较去年有所提升或明显提升，40.76%的公众认为较去年没有变化。

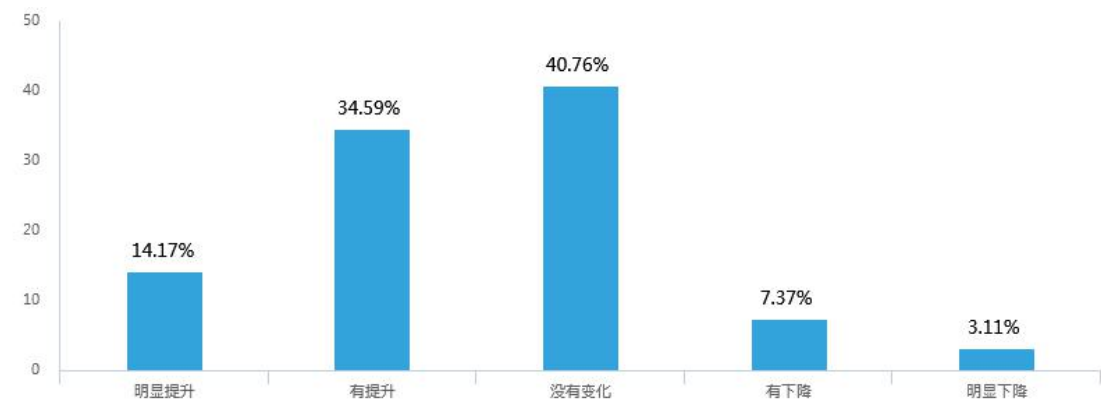


表 3：公众网络安全感较去年的变化

受调查从业人员方面，认为网络安全状况良好和一般的比例大致持平。

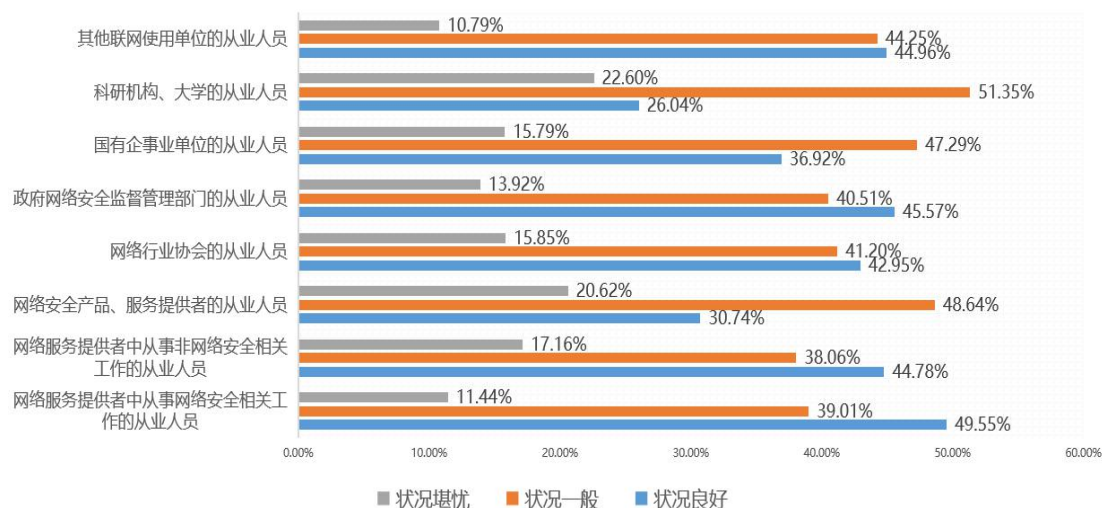


表 4：受调查从业人员对当前网络安全状况的评价²

与 2018 年相比，44.97%至 54.82%的受调查从业人员认为网络安全状况有所改善，13.07%至 37.36%认为状况明显改善，网络安全感同样有所提升。

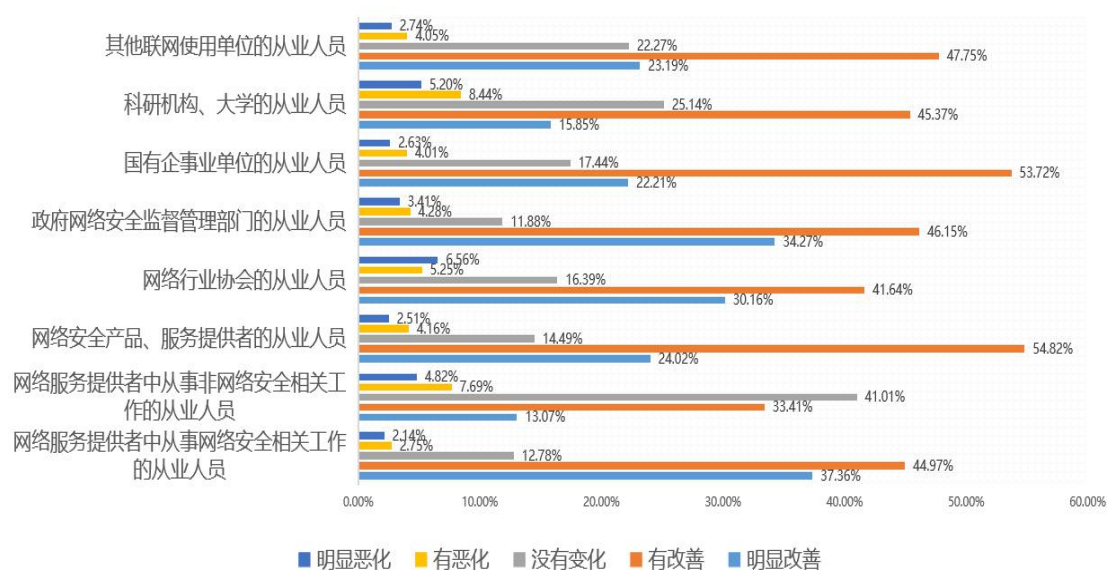


表 5：与去年相比，受调查从业人员认为当前网络安全状况的变化

网络安全法制建设满意度方面，49.79%的公众对网络安全法制建设表示满意，其中，37.06%的公众表示比较满意，12.73%的公众表示

² 为统一选项，此处将网络安全服务提供者中从事非网络安全相关工作的从业人员中的“非常安全”和“安全”统一为“状况良好”，将“不安全”和“非常不安全”统一为“状况堪忧”。

非常满意。

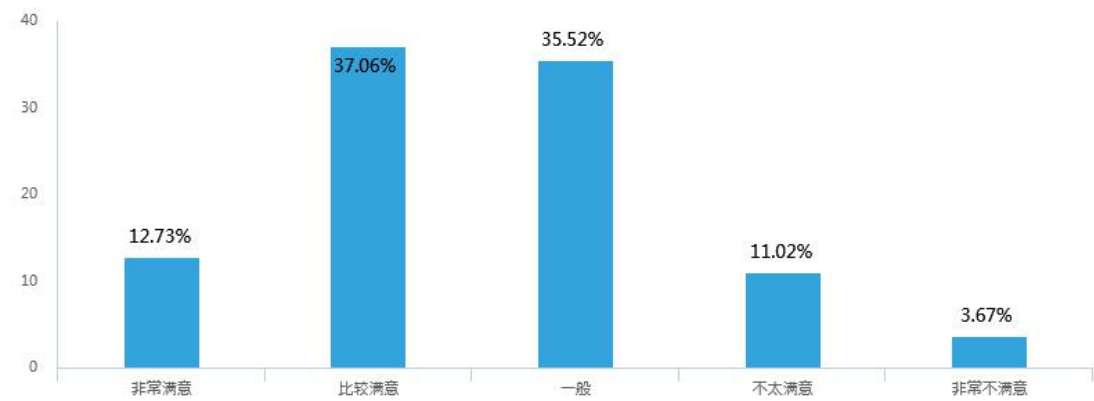


表 6：公众对网络安全法制建设的满意度

调查说明，在我国网络安全法制逐步完善、执法司法力度持续加强、网络运营者责任不断落实的综合作用下，我国网络空间治理取得较大成效，网民的网络安全感有所提升，但网络安全状况仍有持续改善的空间。

2) 网络安全法制宣传教育成效显著，主渠道作用不可替代

调查显示，网民对《网络安全法》的了解程度有所提升，20.31%的公众已了解《网络安全法》主要内容，较去年提高 5.81%；7.44%的公众表示专门学习过，对《网络安全法》非常熟悉，较去年提高 2.5%。

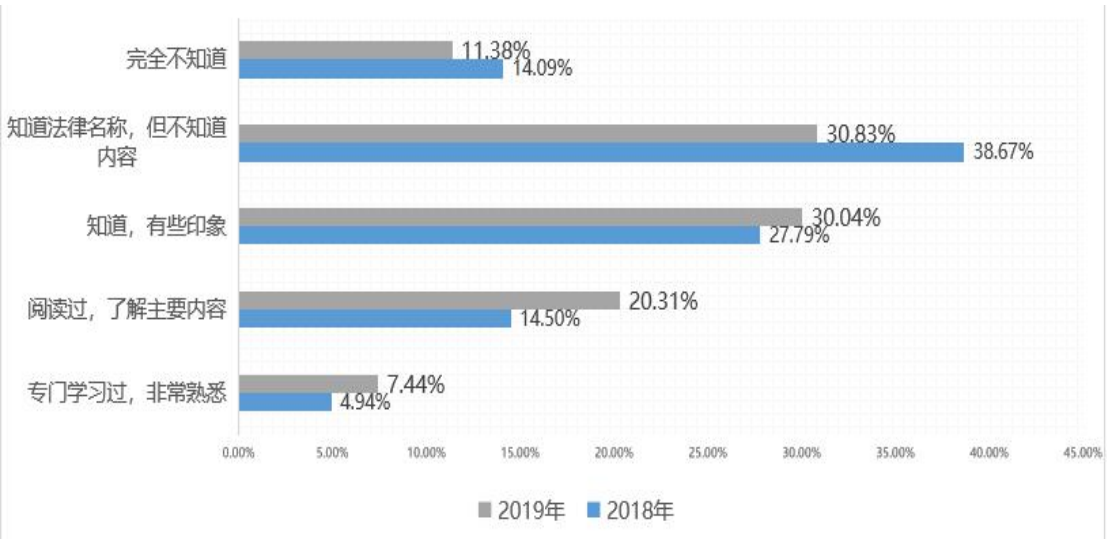


表 7：公众对《网络安全法》了解程度对比图

在此过程中，公共媒体和普法宣传活动起到的作用显著，64.48%的公众通过公共媒体了解到《网络安全法》，50.78%的公众通过普法宣传活动。

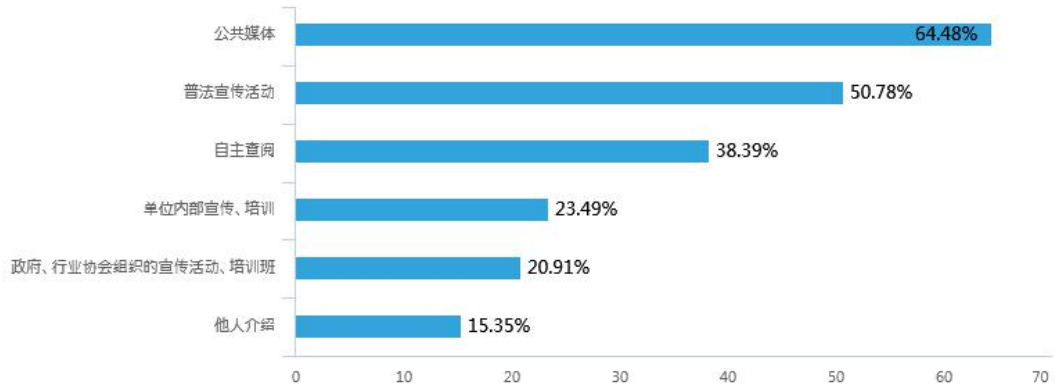


表 8：2019 年公众对《网络安全法》的了解途径

除《网络安全法》外，网民了解的其他网络安全相关立法主要集中在《国家安全法》、《消费者权益保护法》、《保守国家秘密法》、《刑法》及相关司法解释、《反恐怖主义法》等，其中《国家安全法》普及程度最高，69.1%的公众表示知道《国家安全法》，69.57%的受调查从业人员知道《国家安全法》，但对行政法规和部门规章层级的网络安全立法普遍认识不足。

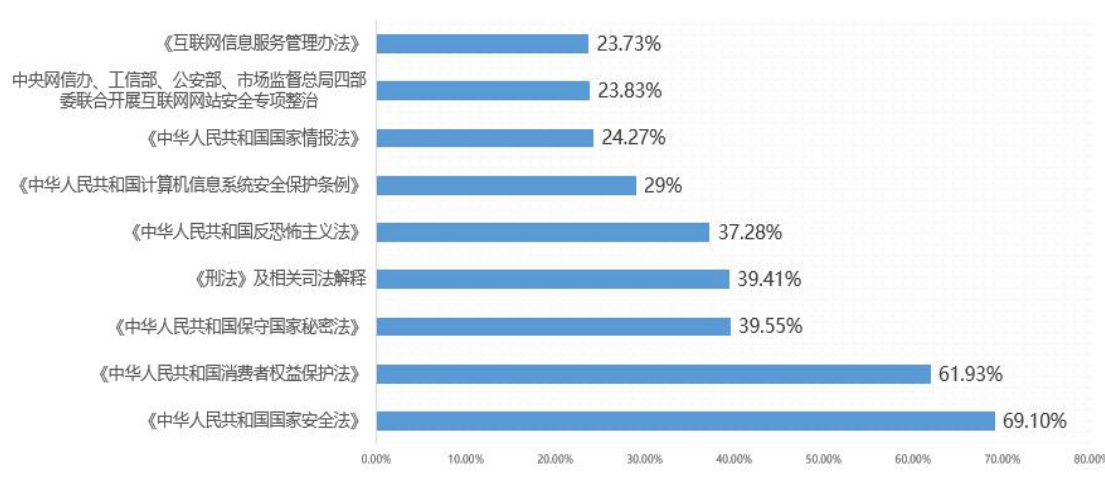


表 9：公众了解的其他网络安全法律法规、司法解释、部门规章和政策标准³

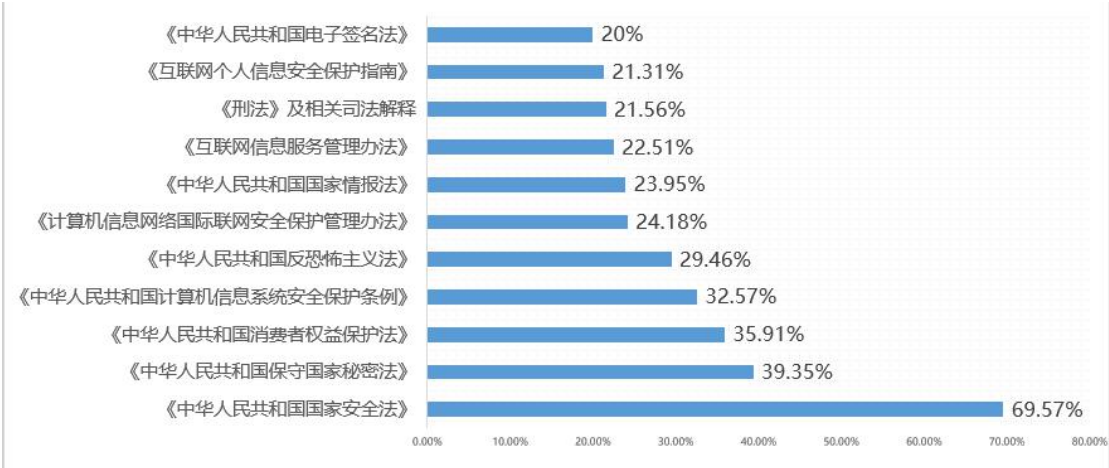


表 10：网络服务提供者中从事网络安全相关工作的从业人员了解的其他网络安全法律法规、司法解释、部门规章和政策标准⁴

网络服务提供者中从事非网络安全相关工作的从业人员与从事网络安全相关工作的从业人员，对《网络安全法》之外的立法了解情况有所区别。

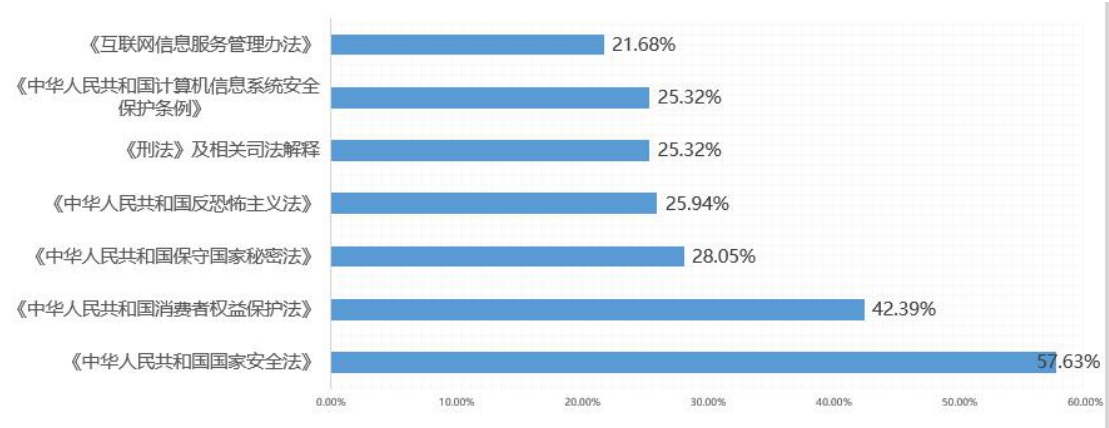


表 11：网络服务提供者中从事非网络安全相关工作的从业人员了解的其他网络安全法律法规、司法解释、部门规章和政策标准⁵

调查说明，《网络安全法》实施 2 周年以来，全社会的普及程度逐渐提高，其中主渠道在网络安全法制宣传教育方面的作用显著且不

³ 内容经过筛选，仅选取占比超过 20% 的选项
⁴ 内容经过筛选，仅选取占比超过 20% 的选项
⁵ 内容经过筛选，仅选取占比超过 20% 的选项

可替代，应持续发挥主流渠道价值，丰富宣传方式和手段，用群众喜闻乐见的方式提高网络安全法制普及程度；并重视学校教育和学科建设，贯彻网络安全为人民，网络安全靠人民的治理理念。此外，应加强基本法外相关网络安全行政法规、部门规章及规范性文件的宣传普及力度。

3) 网络骚扰行为、违法有害信息内容、侵犯个人信息以及网络违法犯罪成为公众最常见的四大网络安全问题

调查显示，网络骚扰行为、违法有害信息内容、侵犯个人信息以及利用网络实施违法犯罪成为公众最常见的四大网络安全问题，71.54%的公众表示曾遇到网络骚扰行为，66.86%表示曾遭遇违法有害信息。

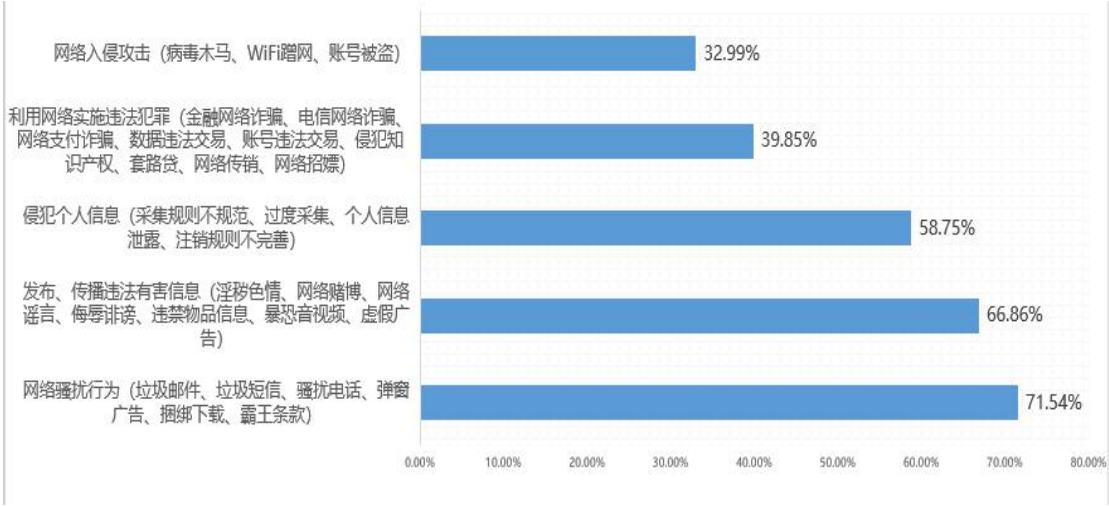


表 12：公众最常见的网络安全问题⁶

网络骚扰行为方面，垃圾短信和弹窗广告情况最为严重，88.65%的公众表示曾接到垃圾短信，87.04%的公众受到弹窗广告骚扰。

⁶ 内容经过筛选，仅选取占比最高的前五个选项

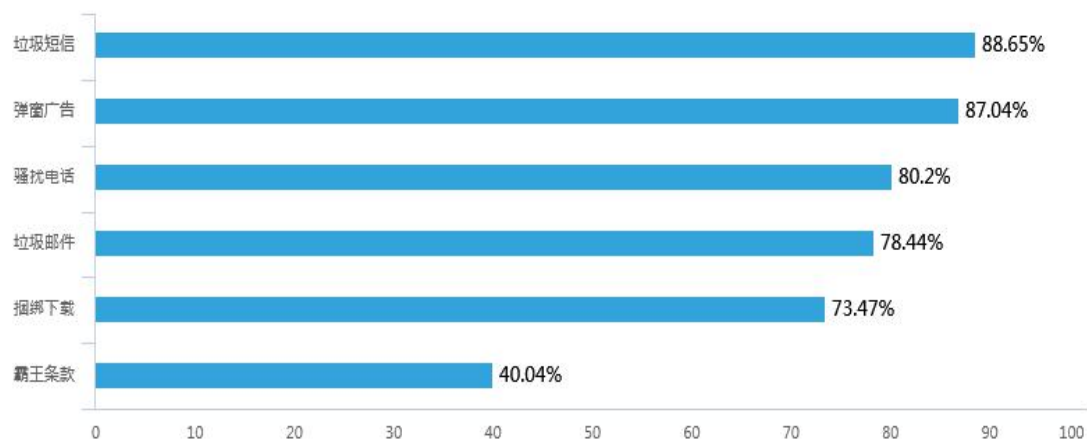


表 13：公众最常见的网络骚扰行为类型

侵犯个人信息方面，公众对个人信息保护状况评价好坏参半，33.75%的公众认为状况一般，31.98%的公众认为不太好或非常不好。

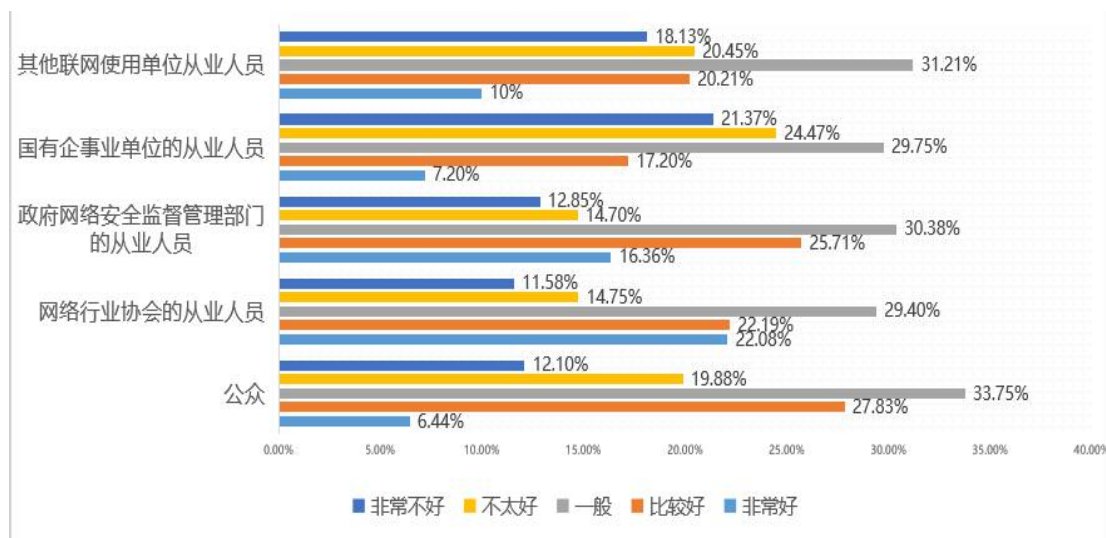


表 14：网民对当前我国网络个人信息保护状况的评价

在侵犯个人信息的具体行为方面，个人信息泄露形势最为严峻，85.36%的公众表示遭遇过个人信息泄露，37.4%的公众认为个人信息泄露情况比较多或非常多。

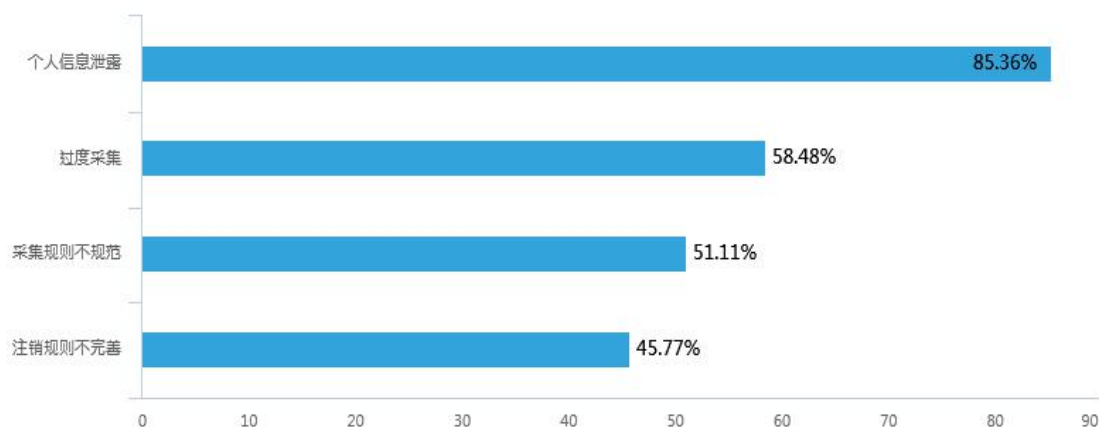


表 15：公众最常见的个人信息侵权行为

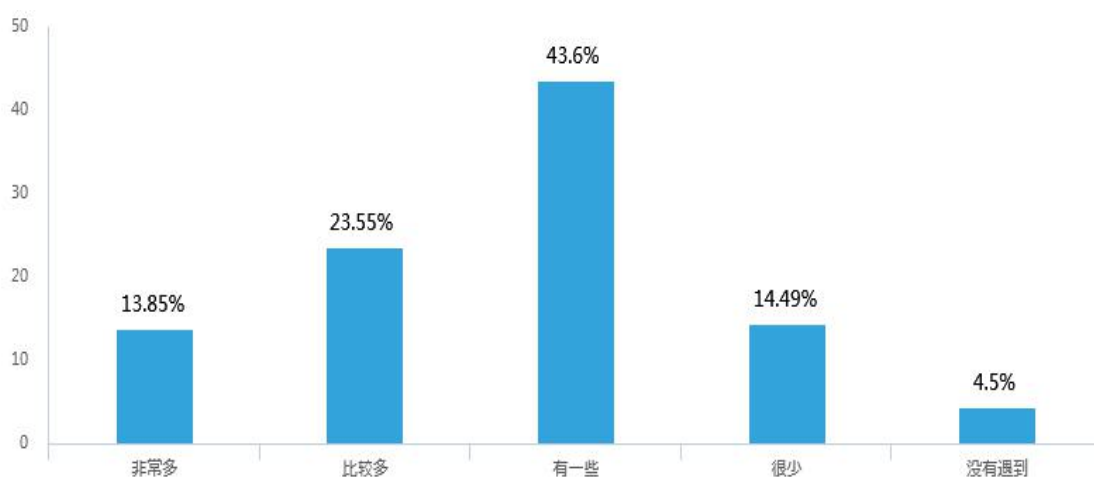


表 16：近一年，公众遇到的网络个人信息泄露情况

公众主要通过收到推销短信、接到各类中介的推销电话、收到垃圾邮件等情况怀疑或确认自己的个人信息被泄露或滥用。



表 17：公众怀疑或确认个人信息被泄露或被滥用的情形

在具体应用方面，过半数公众认为社交应用和网络购物应用的个人信息保护能力最差，对中小平台或新进入的平台安全感最低，54.24%的公众在使用中小平台或新进平台时感到不安全，29.9%认为各平台之间没有明显差别，15.86%表示对大平台或拥有一定市场地位的平台也感到不安全。

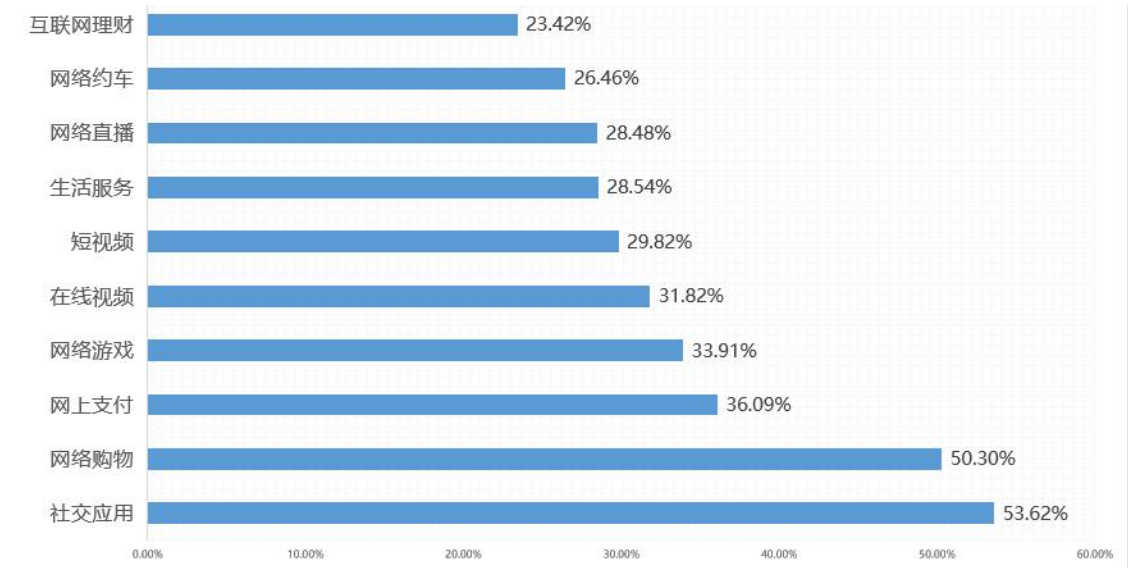


表 18：公众的个人信息保护差评应用榜⁷

利用网络实施入侵方面，63.14%的公众表示发生过账号被盗的情况，59.09%的公众遭遇过病毒木马的入侵，50.95%遭遇过 Wi-Fi 蹭网。

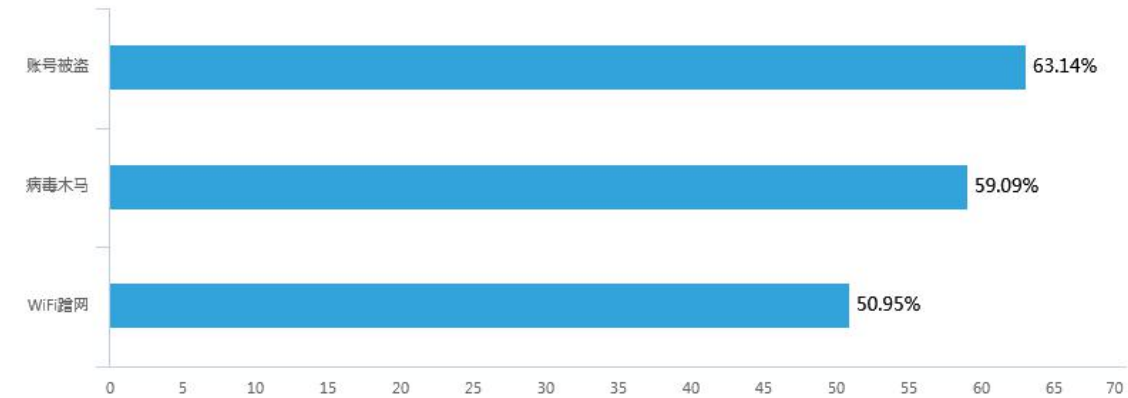


表 19：公众遭遇的网络入侵情况

⁷ 内容经过筛选，仅选取占比超过 20%的选项

利用网络实施违法犯罪方面，主要集中在电信网络诈骗、网络支付诈骗、金融网络诈骗、网络传销、账号违法交易等，其中 61.73% 的公众表示遭遇过电信网络诈骗。

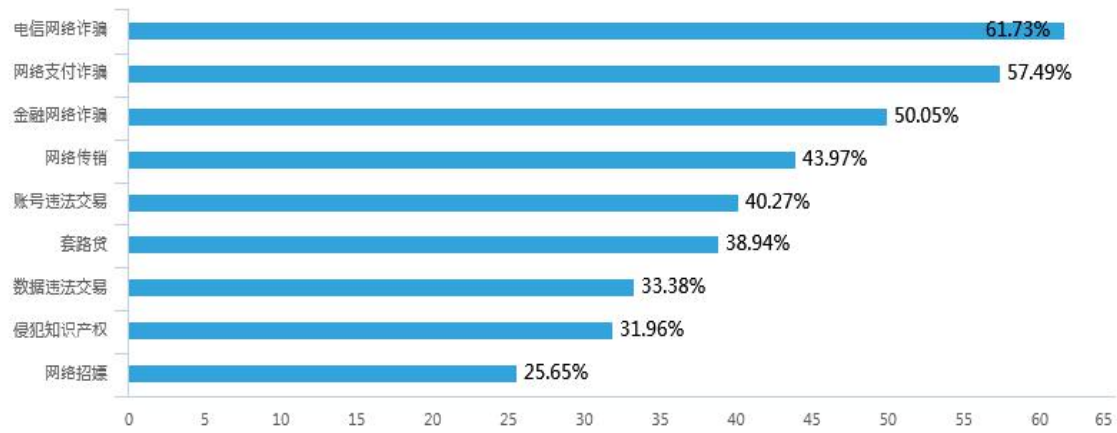


表 20：公众遇到的网络违法犯罪情况

在电信网络诈骗中，最常见的类型包括兼职刷单类、代办信用卡及贷款诈骗类、投资理财诈骗类、QQ 和微信冒充老板、亲友诈骗类等，其中以兼职刷单类诈骗最多，占 57.81%。

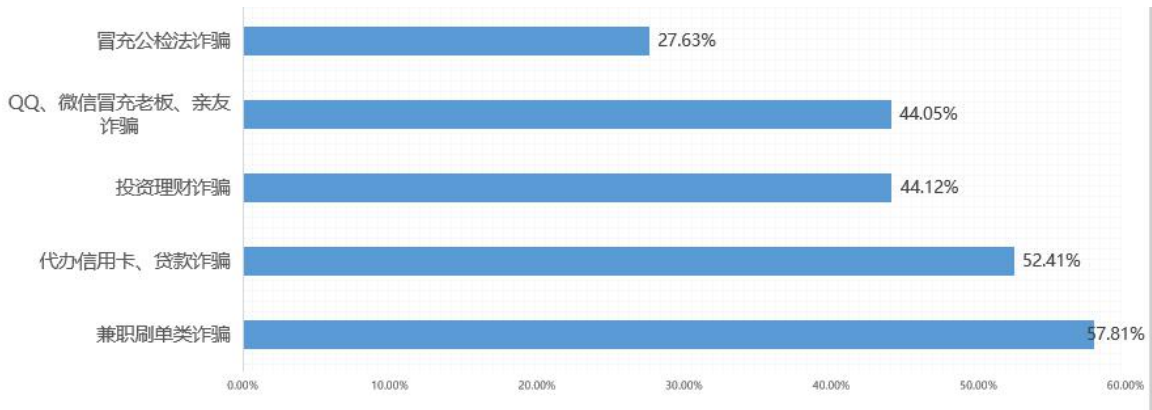


表 21：公众遇到的电信网络诈骗行为统计⁸

针对从业人员的调查中，个人信息或单位敏感信息泄密、网络篡改、病毒木马（含勒索病毒）和网络负面舆情是网络服务提供者中从事网络安全工作的从业人员认为网络服务提供者最常遭遇的网络安

⁸ 内容经过筛选，仅选取占比最高的前五个选项

全问题。其中，64.06%的受调查从业人员表示曾遭遇个人信息或单位敏感信息泄密，59.46%表示曾遭遇网站被篡改，58.24%表示曾遭遇含勒索病毒在内的病毒木马。

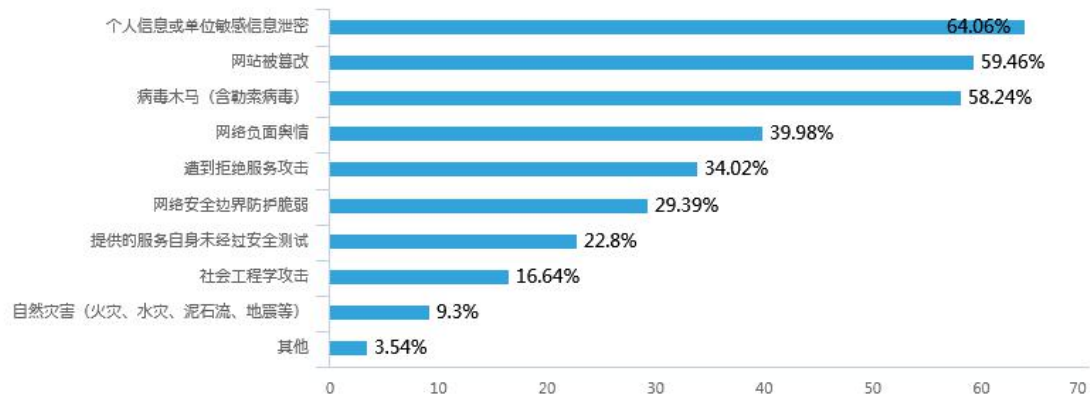


表 22：网络服务提供者中从事网络安全工作的从业人员认为网络服务提供者最常遭遇的网络安全问题

在互联网黑灰产业方面，近半数受调查从业人员认为数量有所增加或大幅增加，14.55%到 25.62%不等的受调查从业人员认为数量大幅增加。在电信网络诈骗方面，三分之一的受调查从业人员认为数量较过去有所减少，半数左右表示没什么区别或者比过去还多。

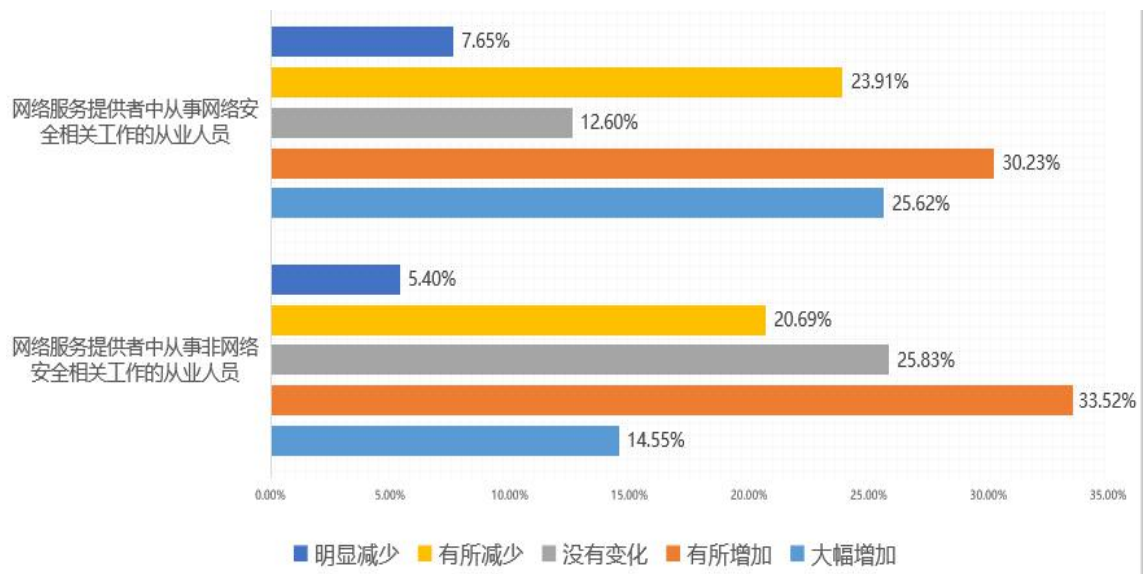


表 23：受调查从业人员对近年来网络数据、账号违法交易等互联网黑灰产业的

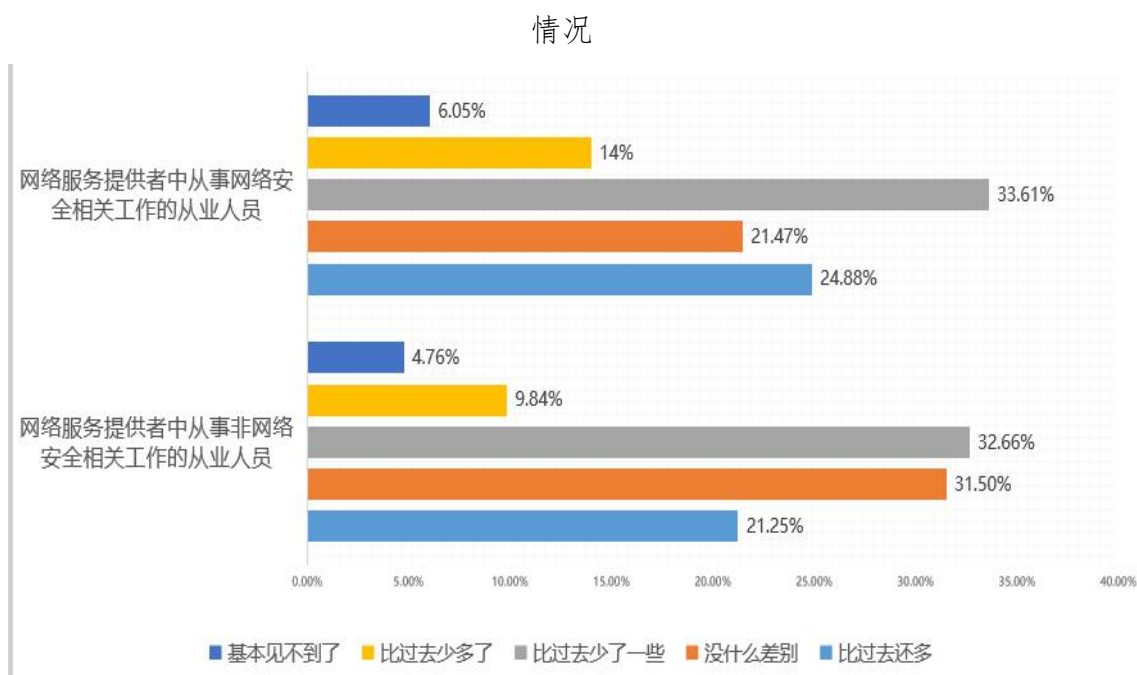


表 24：受调查从业人员对近一年，电信网络诈骗情况的评价

调查说明，公众和从业人员面临的网络安全问题各有侧重，但个人信息安全是两者共同面临的主要安全问题之一。保护个人信息、治理网络骚扰行为、遏制违法有害信息内容、打击黑灰产、电信诈骗的网络违法犯罪应成为治理重点。

4) 虚假广告、网络谣言和淫秽色情信息成为最常见的三类网络违法有害信息

调查显示，虚假广告、网络谣言和淫秽色情信息是公众最常遇到三类网络违法有害信息，79.89%的公众表示曾遇到虚假广告，64.75%表示曾遇到网络谣言，64.68%曾遇到淫秽色情信息。

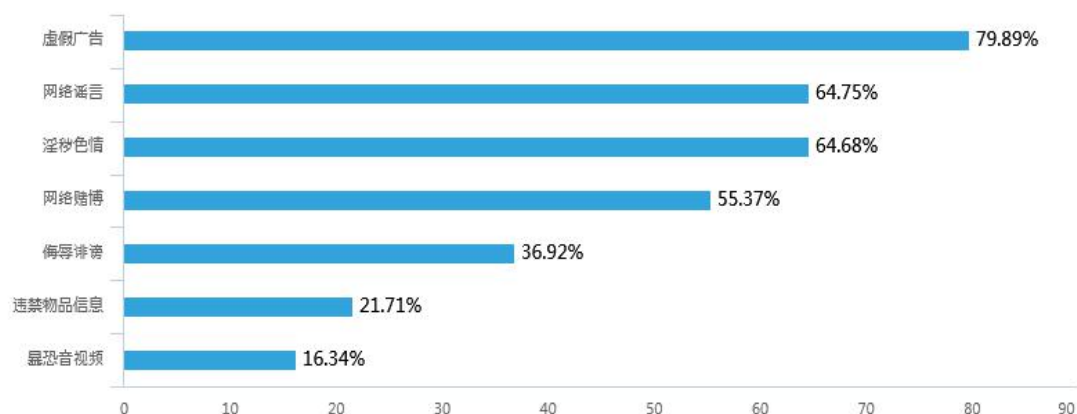


表 25：公众遇到的网络违法有害信息种类

就近一年遇到的低俗网络信息数量而言，26.86%的公众认为数量没有区别，22.54%的公众认为有所增加或明显增加，41.86%的公众认为有所减少或明显减少；在受调查从业人员中，30%左右表示数量比过去少了一些，19%至 29%不等的受调查从业人员认为数量没什么区别，15%至 19%认为有所增加。

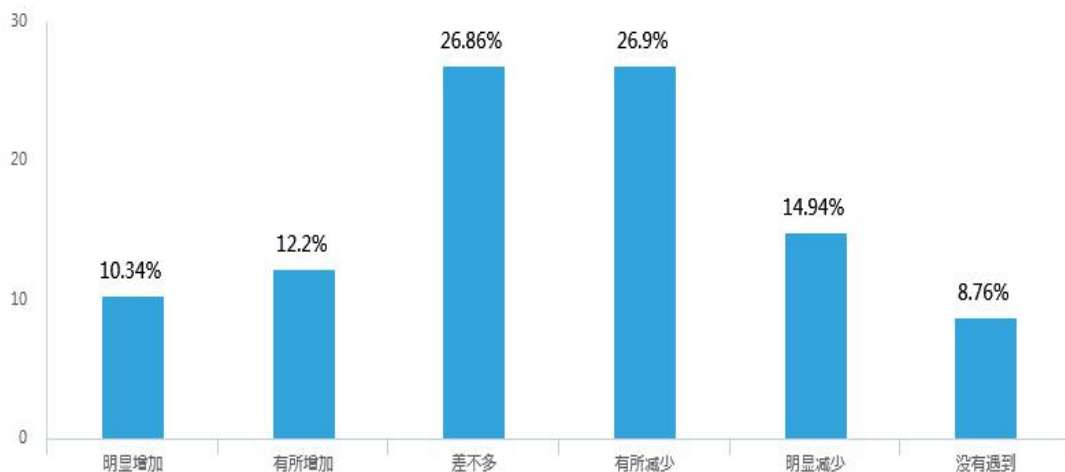


表 26：近一年公众遇到的色情暴力等低俗网络信息数量

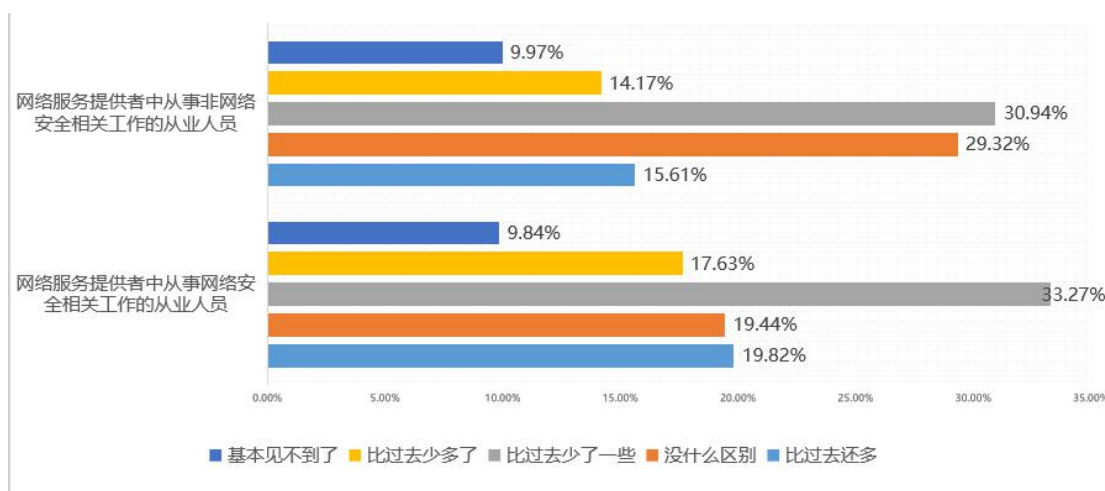


表 27：受调查从业人员遇到的低俗网络信息数量

遇到低俗网络信息后，43.55%的公众表示会直接忽略，9.54%的公众表示会告知熟悉的人，其余公众表示遭遇低俗网络信息后会通过向网站投诉、向监管部门举报、向公安部门报警等方式进行反馈，其中向网站投诉的占比最高，达到 45.41%

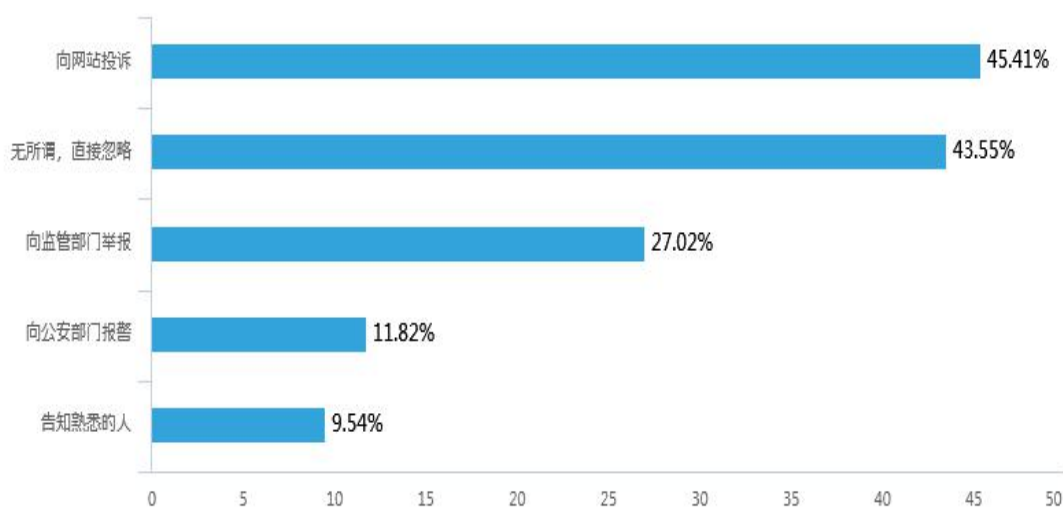


表 28：公众遇到色情暴力等低俗网络信息后的应对

调查说明，我国信息内容治理取得一定成效，大部分公众向网站投诉的结果表明，网络运营者在治理低俗网络信息方面的角色和作用难以替代。

5) 加强网络安全法制建设成为社会解决网络安全问题的首选途径

调查显示，公众认为应采取的网络安全保障措施包括加强网络安全法制建设、严厉打击网络违法犯罪行为、强化网络安全监管、将网络失信行为纳入信用管理等，其中，加强网络安全法制建设为首选途径，占比 71.77%。

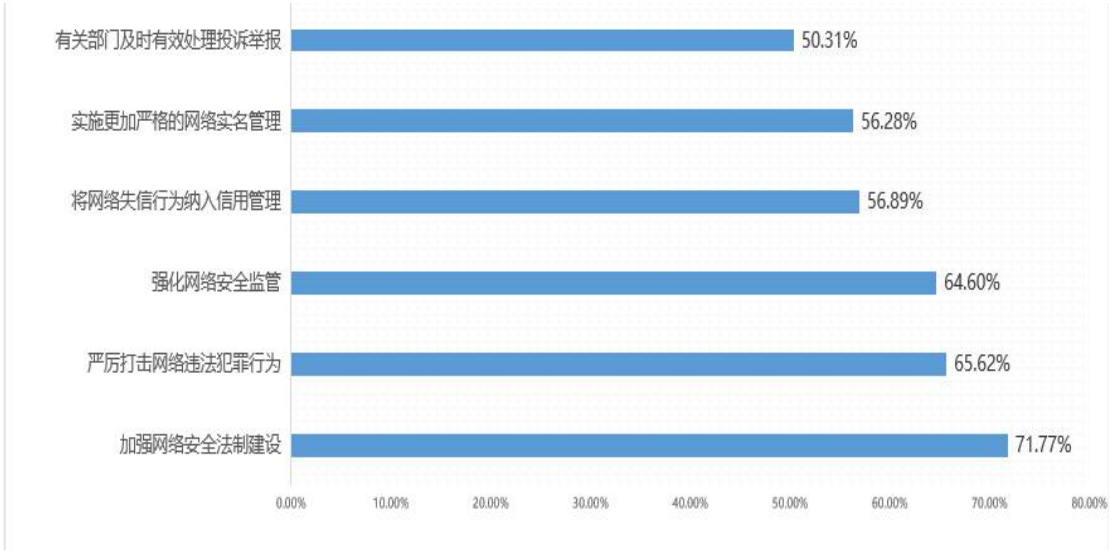


表 29：公众认为维护网络安全应采取的措施⁹

从业人员方面，网络服务提供者中从事网络安全相关工作的从业人员认为应采取的网络安全保障措施包括加强网络安全法制建设、强化网络安全监管、提升网络安全问题的发现能力、落实网络平台主体责任等。其中，与公众选择相同，加强网络安全法制建设成为首选途径，占比 71.94%。

⁹ 内容经过筛选，仅选取比例超过 50%的选项

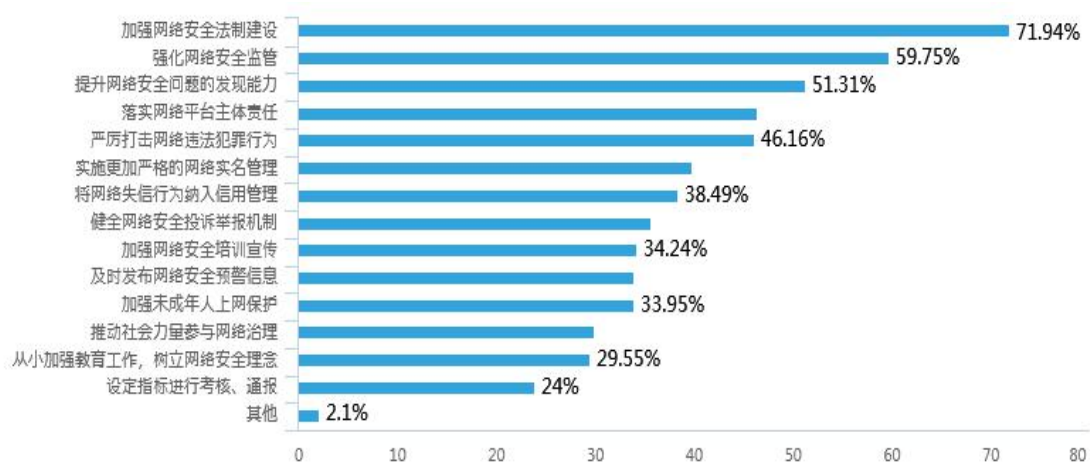


表 30：网络服务提供者中从事网络安全相关工作的从业人员认为维护网络安全最需要采取的措施

调查说明，加强网络安全法制建设成为社会解决网络安全问题的首选途径。我国以《网络安全法》为核心的网络安全法制建设取得网民一致认可，网络安全法制在保障网络安全方面的效能得到充分体现。

6) 个人信息保护、网络平台责任和数据安全保护成为三大核心诉求

调查显示，个人信息保护、网络平台责任和数据安全保护是网民在网络安全立法方面的三大核心诉求。其中，82.61%的公众认为需加强个人信息保护立法，73.36%的公众认为需加强网络平台责任立法，63.69%的公众认为需加强数据安全立法。

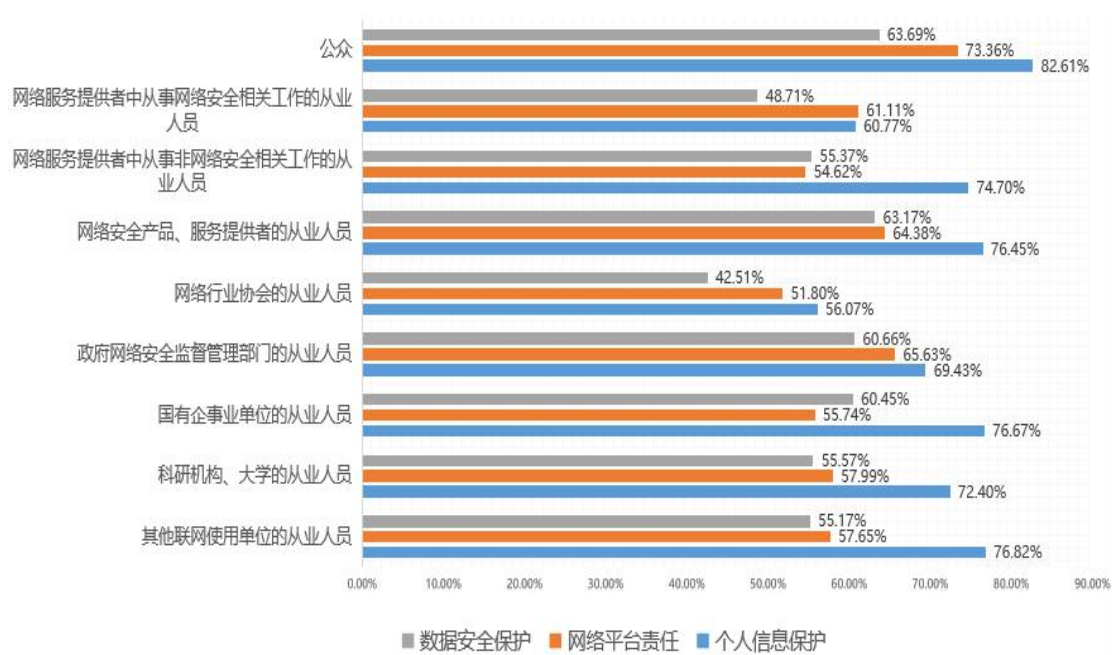


表 31：网民认为最应加强的网络安全立法¹⁰

其中，出台专门的个人信息保护立法成为公众的迫切需求，31.26%的公众认为需要出台个人信息的专门立法，30.81%的公众认为需要出台个人信息保护的强制标准。

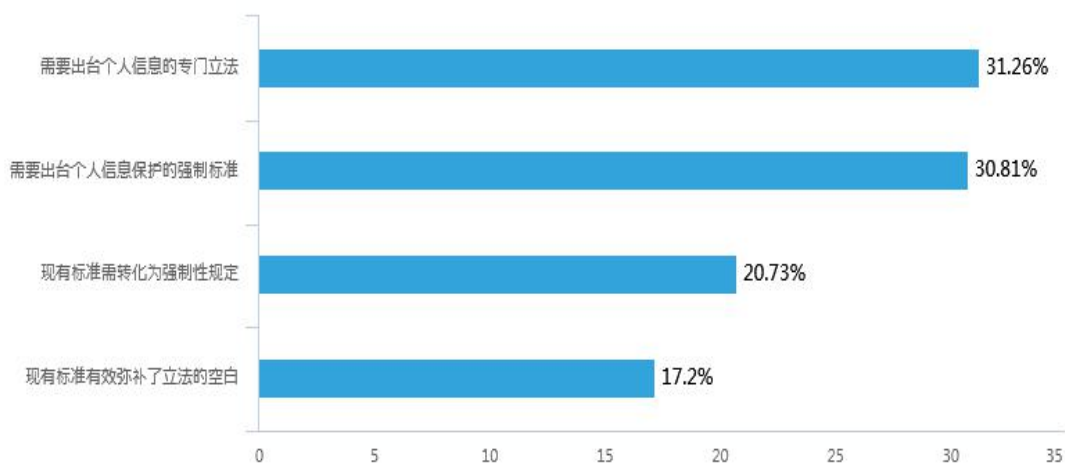


表 32：公众对国家个人信息保护立法的看法

在具体立法规范中，个人信息保护协议、个人信息采集和个人信息共享要求是公众认为最需重点规范的行为，88.08%的公众认为需要重点约束个人信息保护协议。

¹⁰ 内容经过筛选，仅选取占比最高的三个选项

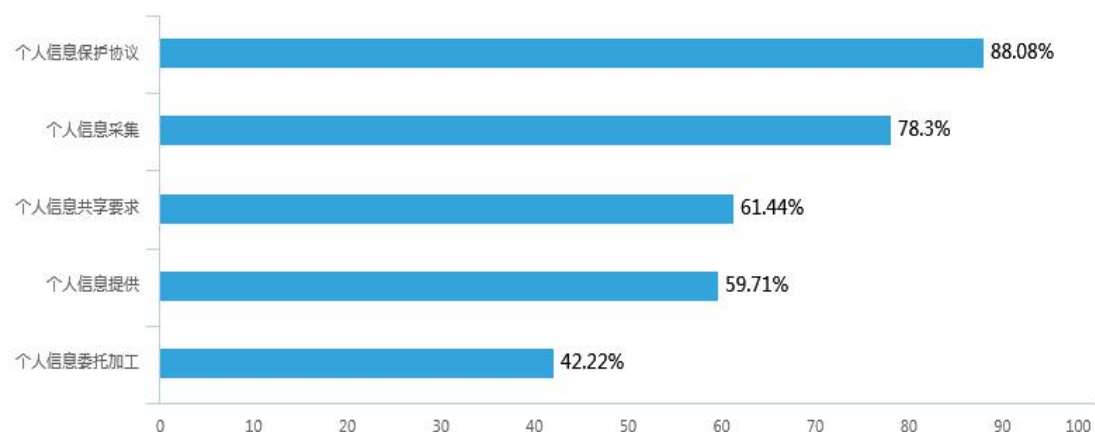


表 33：公众认为立法时需重点规范的行为

调查说明，当前规模化数据泄露和滥用事件高发频发的背景下，数据安全与个人信息保护成为人民群众的核心关切，通过加强网络安全法制建设，完善个人信息保护和数据安全立法、强化网络平台责任成为网民主要诉求。

7) 公众从知法到用法的需求觉醒，权利救济途径有待拓宽

调查显示，公众仍存在一定的不安全上网行为，45.8%的公众会在公共场所登录 Wi-Fi, 45.51%的公众会打开来源不明的电子邮件或网站链接。

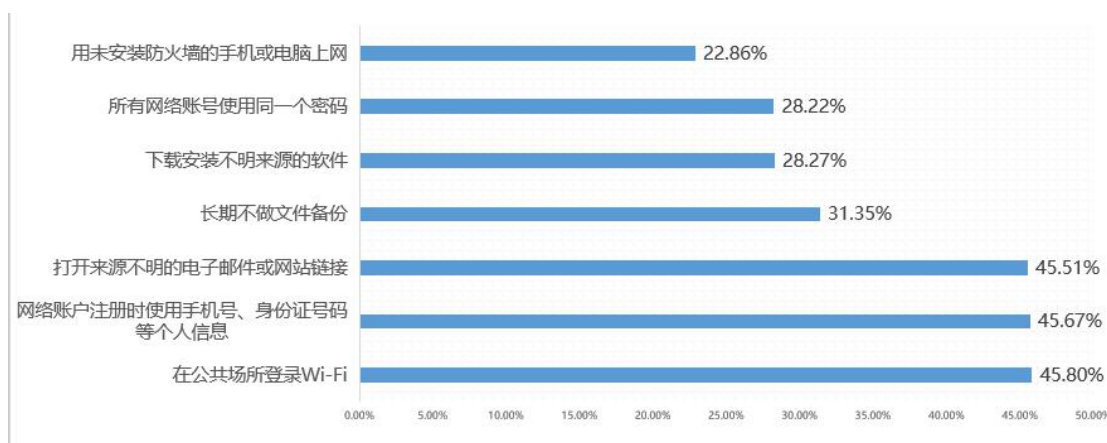


表 34：公众的网络不安全行为¹¹

¹¹ 内容经过筛选，仅选取占比超过 20%的选项

调查显示，公众普遍反映处于知法但不会用法的阶段，通过主流媒体等宣传渠道，知晓自身拥有的网络安全相关权利，但在权利受到侵犯后的权利救济方面仍存在模糊，72.51%的公众认为需加强个人权益保护宣传。

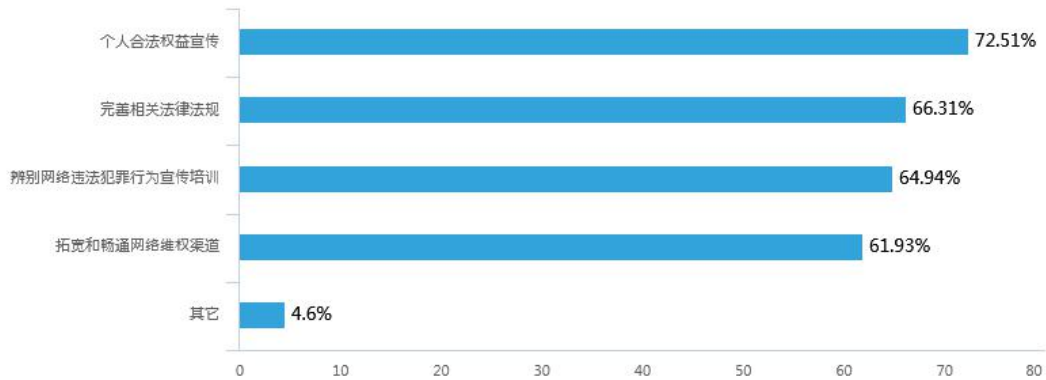


表 35：公众认为应加强的网络安全工作

个人信息保护方法、网络诈骗识别、病毒及木马防范方法是公众在网络安全知识方面的三大需求，其中 69.78%的公众表示想了解个人信息保护方法。

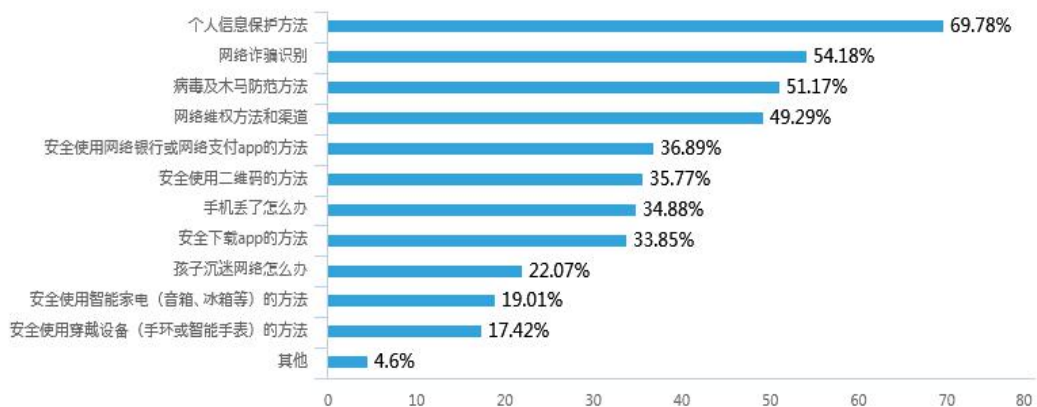


表 36：公众的网络安全知识需求

调查说明，在后续网络安全宣传教育过程中，应将重点从知法逐渐过渡到用法，提高网民的权利救济能力，拓宽权利救济途径，畅通监督举报方式，对网民强烈反映的问题及时作出回应。

8) 未成年人和老年群体用网环境亟待改善

调查显示，未成年人上网情况非常普遍，73.19%的公众表示家庭中存在未成年人上网情况。其中，网络游戏、在线视频、短视频是未成年人最常使用的网络应用，超过80%的未成年人接触过网络游戏。

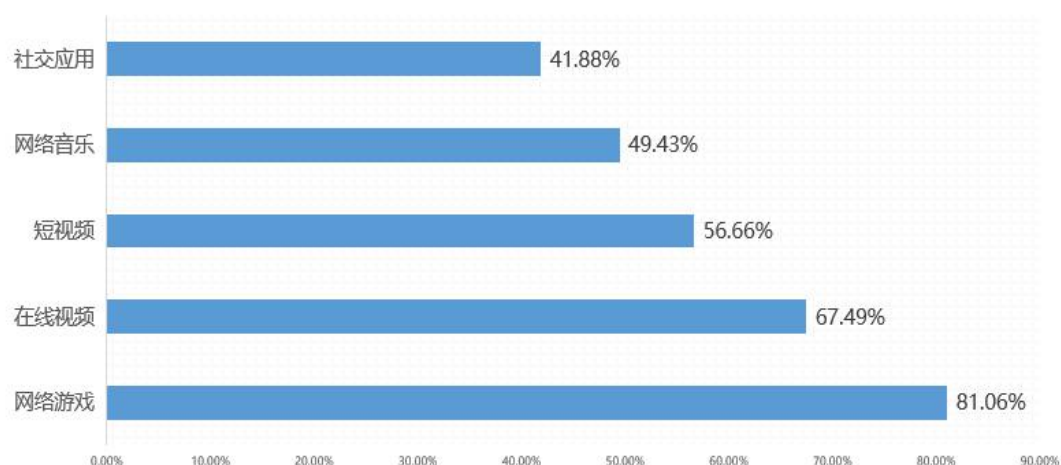


表 37：未成年人主要使用的应用服务¹²

对当前未成年人网络权益保护状况，公众评价好坏参半。41.36%的公众表示比较或非常满意，36.16%认为保护状况一般，22.47%认为不满意或非常不满意。

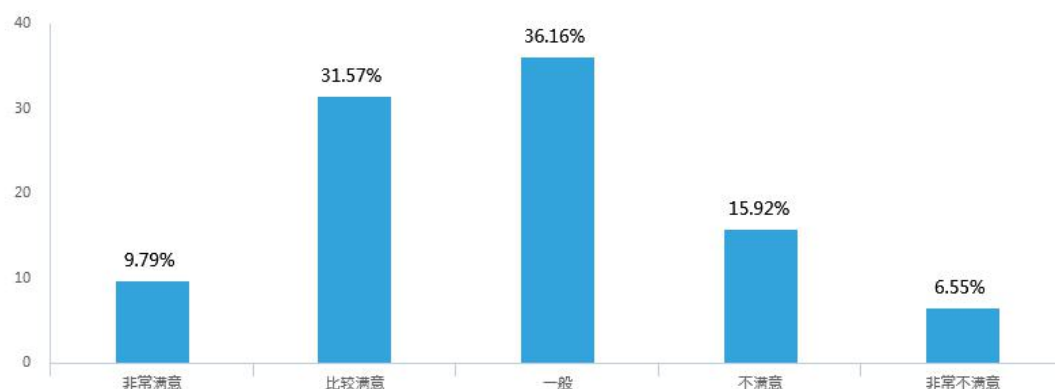


表 38：公众对未成年人网络权益保护状况的满意度

在看待未成年人上网行为方面，公众态度也较为理性，60.9%的公众认为不应当反对，应合理安排上网时间，避免因未成年人缺乏辨

¹² 内容经过筛选，仅选取占比最大的前五个选项

识能力，被网友欺骗，或沉迷网络游戏和网络聊天。

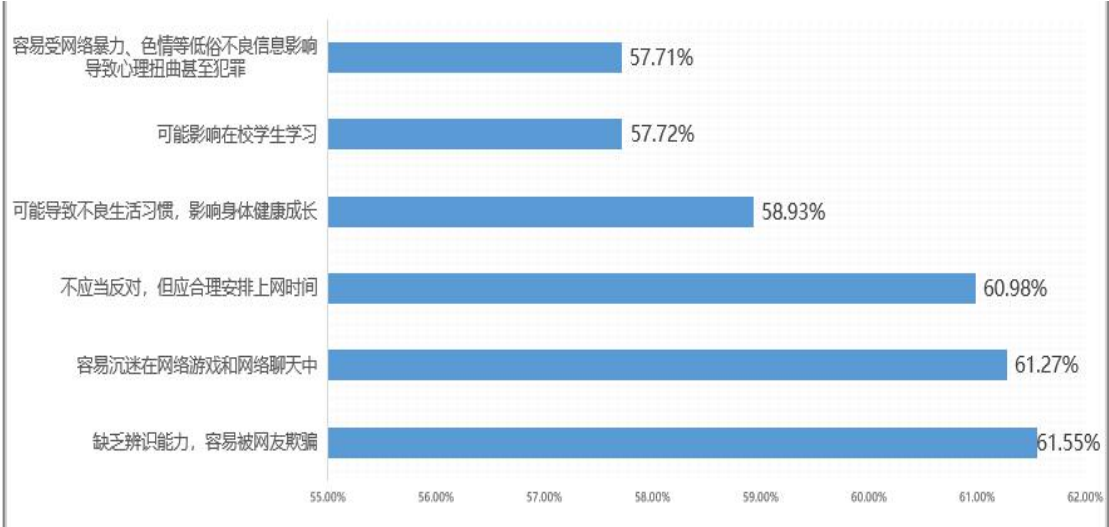


表 39：公众对未成年人上网的态度¹³

防止网络沉迷成为公众最为关心的未成年人用网健康问题，37.11%的公众最为关心网络沉迷问题，23.42%最为关心未成年人接触色情暴力信息。

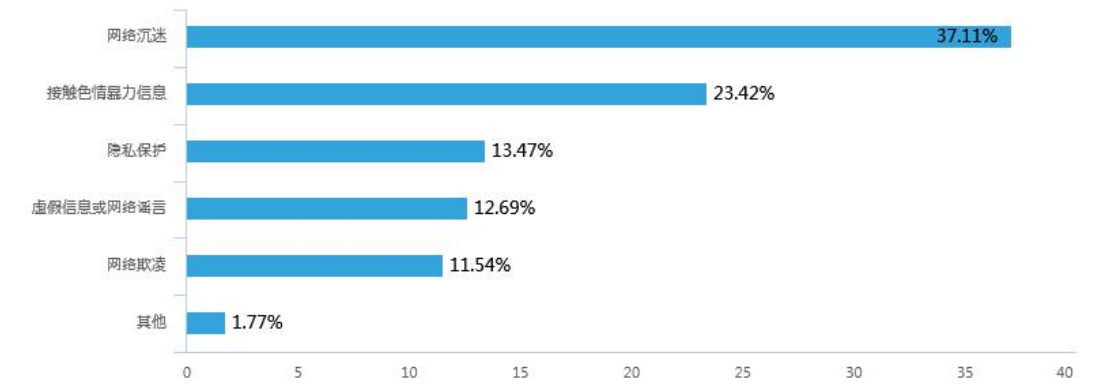


表 40：公众最关心的未成年人用网安全问题

66.11%的公众认为应限制未成年人浏览不适宜的网站和信息，57.2%的公众认为应限制上网时间和时长，55.75%认为学校应进行宣传教育并采取适当措施，52.24%认为父母应对未成年子女上网进行监督约束。

¹³ 内容经过筛选，仅选取占比超过 50%的选项

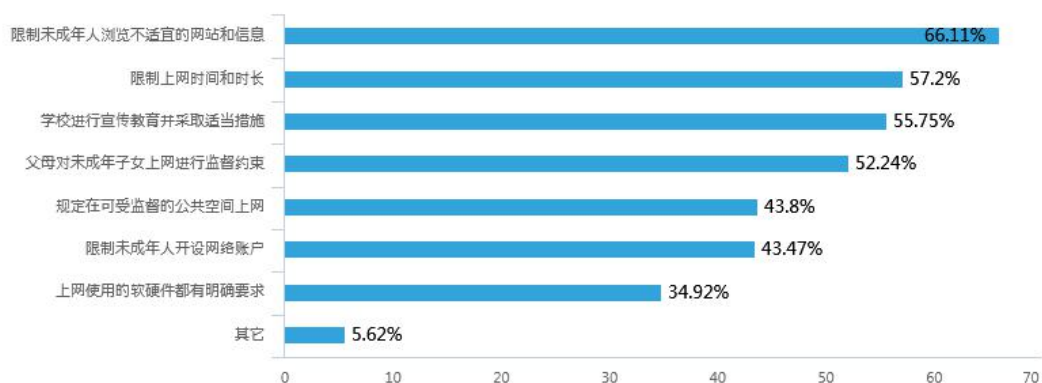


表 41：为防止网络沉迷，公众认为最有效的措施

调查说明，未成年人上网已成趋势，单纯禁止和片面限制已不能满足未成年人用网的现实需求，应将重点转向治理未成年人用网环境，采取措施防止未成年人沉迷网络，整治网络不良信息以及保障未成年人信息安全等方面。此外，老年群体对网络应用、网络违法犯罪手段不敏感，使用网络过程中易受到网络虚假信息、电信诈骗等网络违法犯罪行为侵扰，在重视未成年人用网健康的同时也需加强对老年群体的保障。

9) 网络安全治理架构成为 5G 安全关注重点

调查显示，60%左右的受调查从业人员关注过 5G 安全问题，其中网络服务提供者中从事网络安全相关工作的从业人员有 61.49%关注过 5G 安全问题。

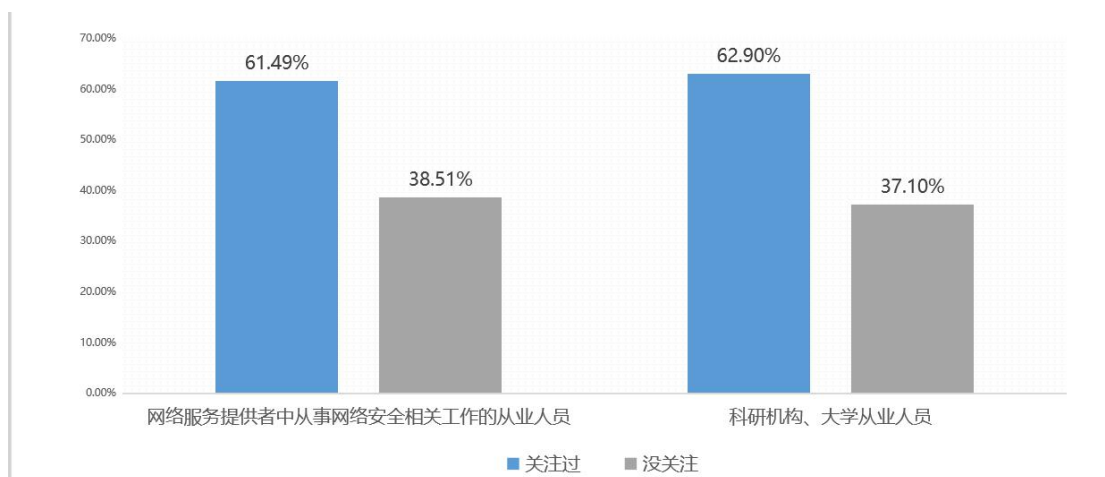


表 42：受调查从业人员是否关注过 5G 安全问题

在关注 5G 安全问题的受调查从业人员中，适应 5G 应用需要的网络安全治理架构，满足 5G 要求的车联网、物联网等应用场景的安全产品以及 5G 移动终端安全成为最受关注的三大问题。

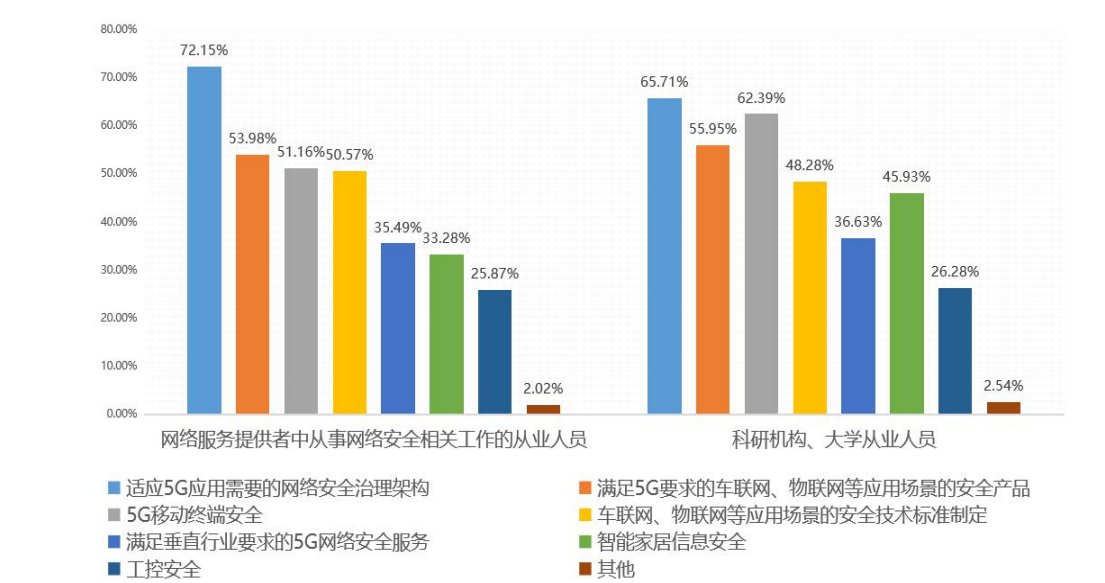


表 43：受调查从业人员最关注的 5G 安全重点

受调查从业人员认为加强 5G 网络安全技术标准体系建设，加强对 5G 网络信息安全核心技术的知识产权管理，制定针对不同应用场景的法律法规及监管措施是最应重点加强的三项安全措施。66%至 71% 不等的受调查从业人员认为应加强 5G 网络安全技术标准体系的建设。其余应重点加强的安全管理措施还包括进一步加强对运营商承载

5G 标准的多类型海量数据网络等关键信息基础设施保护；以数据为中心加强对 5G 应用新业态的网络安全管理；针对网络安全场景大量增加的情况，加强政府网络安全监管协调能力和执法能力。

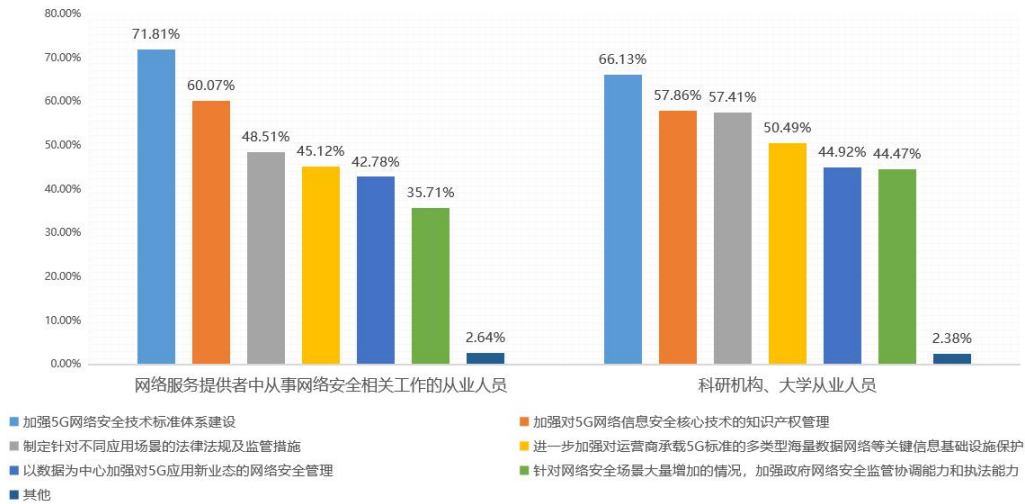


表 44：受调查从业人员认为 5G 需重点加强的安全管理措施

调查说明，5G、物联网、人工智能、区块链等新一代信息技术带来的安全问题已经引发普遍关注，建立网络安全治理框架和相应的技术标准体系成为规范新一代信息技术发展的首要诉求。

10) 等保基础价值得到充分认可，落实推进仍需加强

调查显示，网络安全等级保护制度在我国施行二十余年以来，其价值和作用已经得到社会和行业普遍认可。68%至 79%不等的受调查从业人员认为等保是国家网络安全领域的基本保障和基本制度，过半数受调查从业人员将等保视为各部门各单位开展网络安全工作的基本方法和遵循。

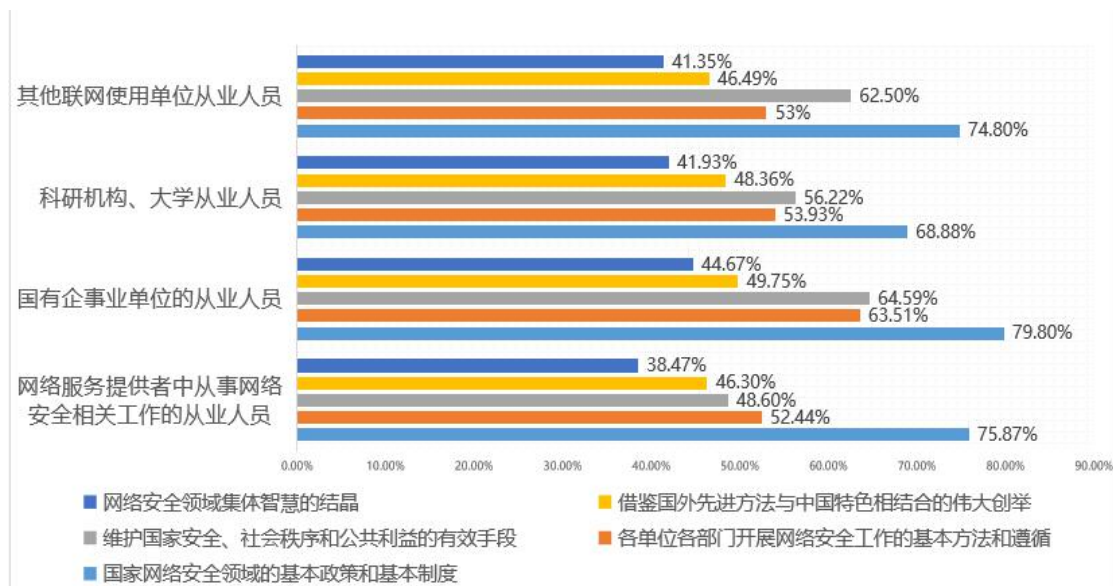


表 45：受调查从业人员认为网络安全等级保护制度的重大意义

受调查从业人员普遍认为等保制度对社会发展的推动作用很大，其中 60%以上的受调查从业人员认为等保对经济、社会发展的推动作用很大，认为等保制度用处不大的占比均不超过 10%。

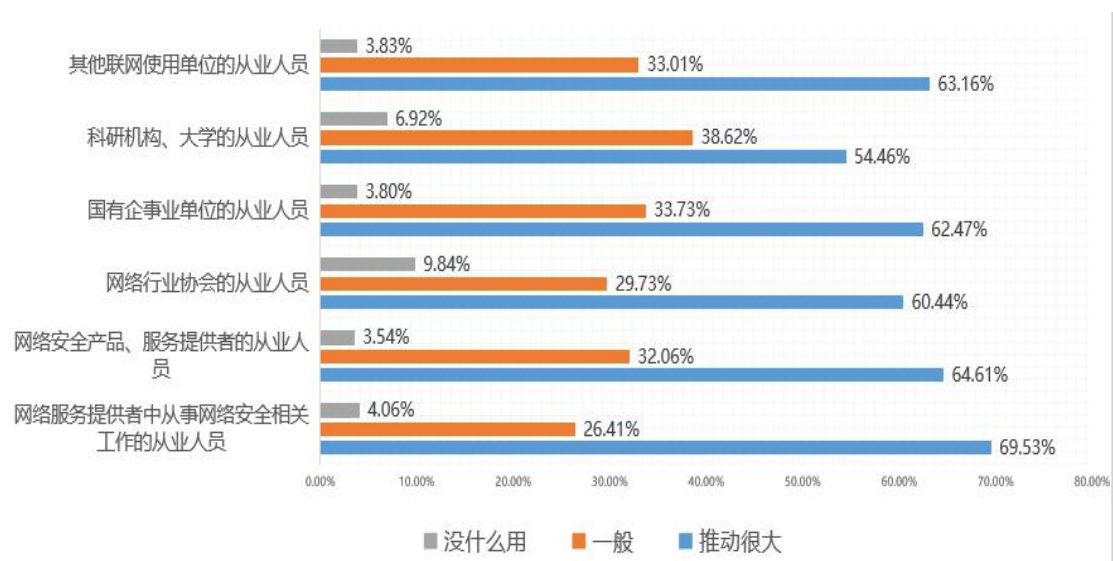


表 46：受调查从业人员认为网络安全等级保护制度对产业、企业发展的作用

我国等保工作开展状况良好，大多数受调查从业人员表示已经开展等保相关工作，但仍有 10%至 20%不等的受调查从业人员表示没有开展等保工作。

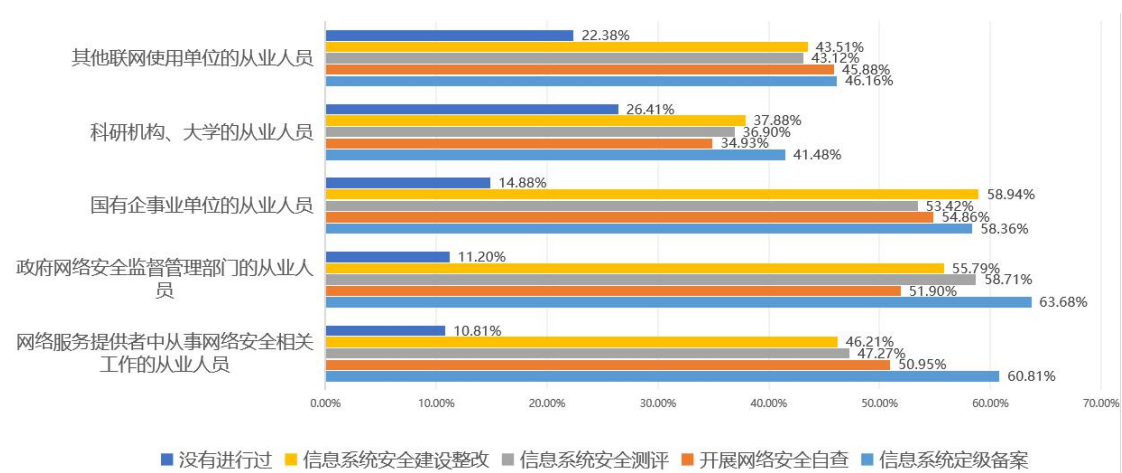


表 47：受调查从业人员开展网络安全等级保护工作的情况

作为等保工作的重要一环，测评机构的满意度整体向好，67.72%的网络安全服务提供者中从事网络安全工作的从业人员对测评机构表示满意，但仍有 30%至 50%不等的受调查从业人员对测评机构的评价一般。

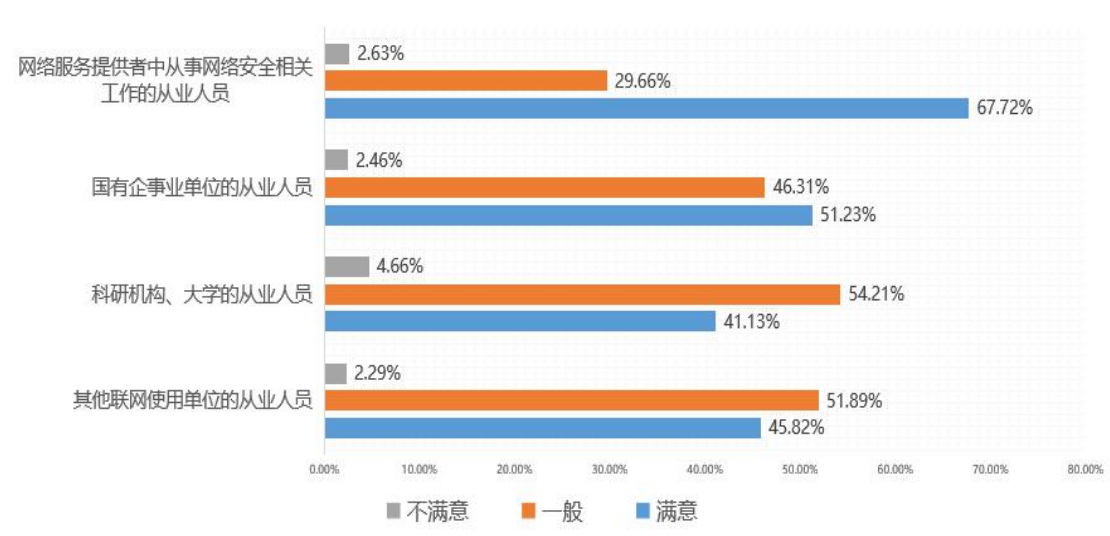


表 48：受调查从业人员对测评机构的满意程度

等保的义务单位方面，政府部门、事业单位、国有企业、互联网企业和私营单位等网络运营者作为等保义务主体已得到普遍认可，但仍有 25%至 50%不等的受调查从业人员认为家庭和个人也要履行等保义务。

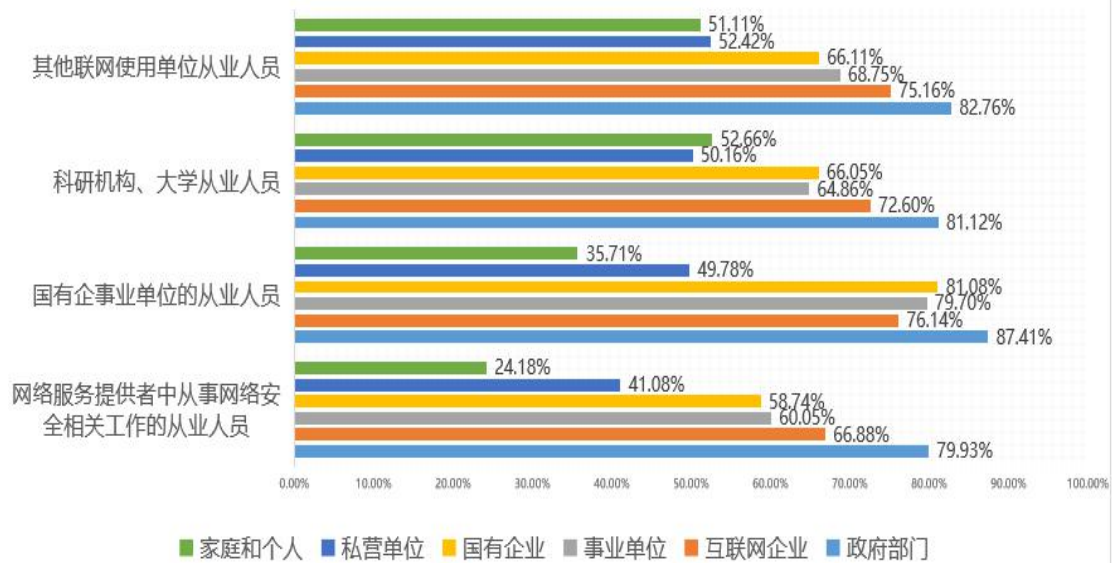


表 49：受调查从业人员认为哪些机构应开展网络安全等级保护制度

等保的目标系统方面，关键信息基础设施、行业专网和业务信息系统等作为等保目标系统也已得到普遍认可，但仅有 24%至 39%不等的受调查从业人员认为除家庭和个人自建自用以外的所有网络都需开展等保工作。

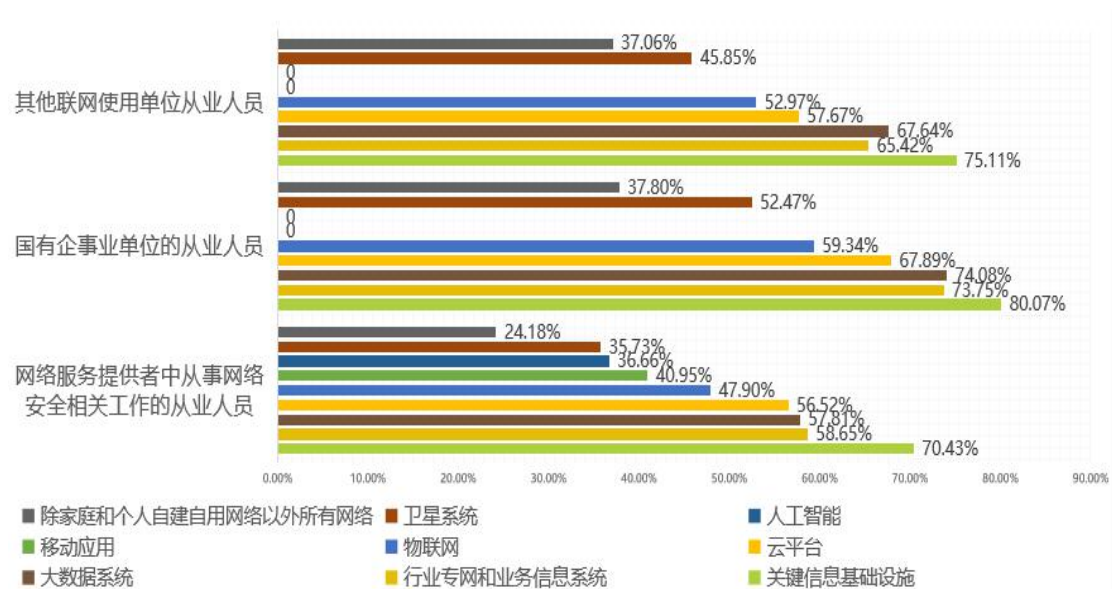


表 50：受调查从业人员认为哪些系统应开展网络安全等级保护制度¹⁴

在等保 2.0 的相关调查中，仅有 23%至 60%不等的受调查从业人

¹⁴ 图中数字 0 表示，针对该类从业人员的答案选项中没有这一项

员知道等保 2.0 国家标准的相关要求，有 76.71% 的其他联网使用单位从业人员不知道等保 2.0 要求，70.76% 的科研机构 and 大学从业人员不知道等保 2.0 要求。

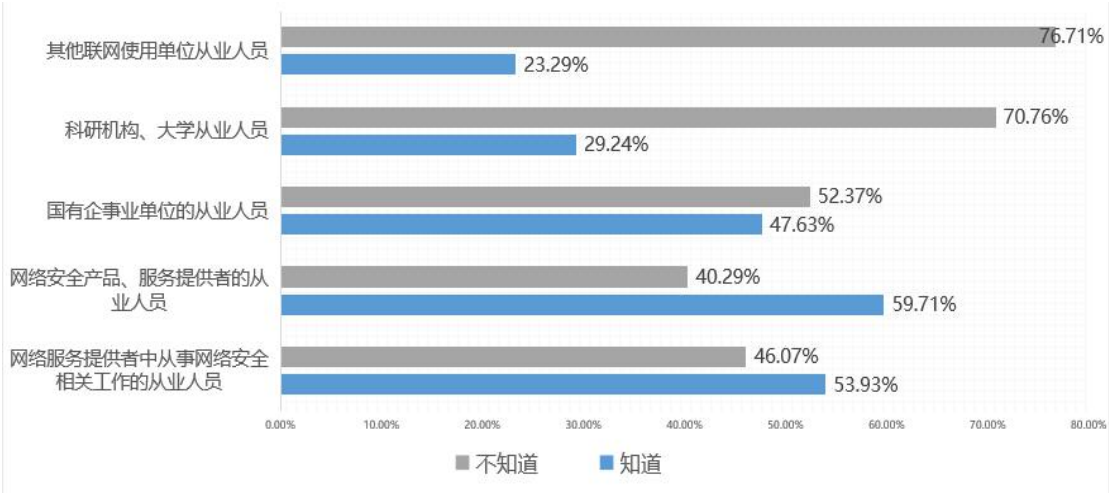


表 51：受调查从业人员对等保 2.0 国家标准要求的了解程度

在宣传等保 2.0 过程中，行业专业论坛和单位、政府组织的培训作用最为显著。47% 以上的受调查从业人员通过行业专业论坛知道等保 2.0 要求。

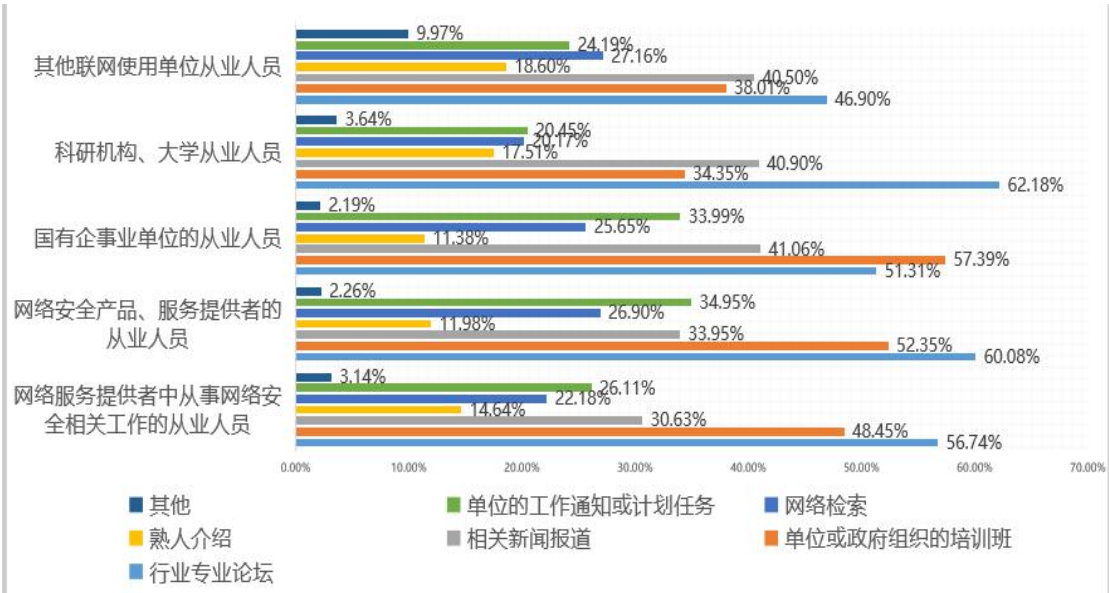


表 52：受调查从业人员知道等保 2.0 国家标准要求的途径

调查说明，网络安全等级保护制度在保障网络安全、夯实行业基

础安全方面的价值已经得到充分认可，大部分网络运营者将等保作为开展网络安全工作的基本方法和遵循，但仍有部分单位未开展任何等保相关工作，测评机构的社会满意度也仍待提高。

11) 平台责任落实不到位，主体责任仍需加强

调查显示，互联网企业网络安全责任落实方面，37.13%的公众认为落实情况非常好或比较好，37.29%的公众评价一般，19.69%认为不太好或非常不好。

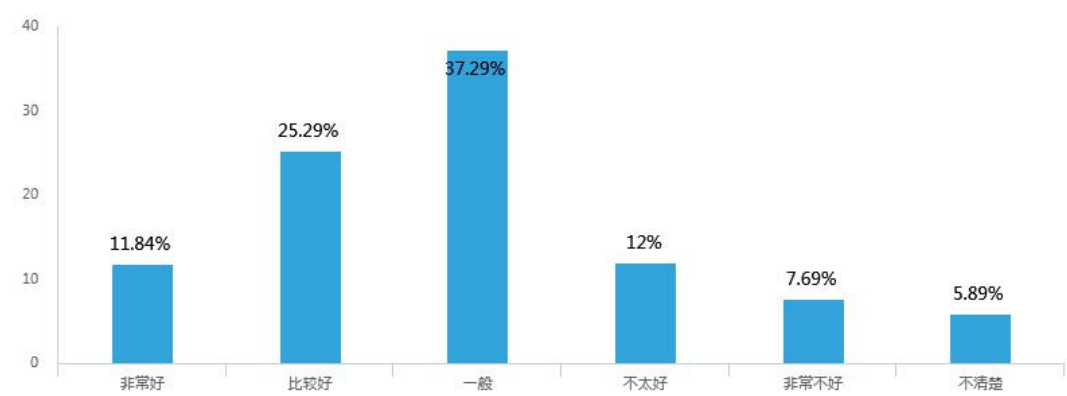


表 53：公众对互联网企业网络安全履责的评价

有意不承担或少承担网络安全责任、网络安全管理水平低下以及网络安全责任意识不强是公众给予负面评价的三大主要原因，其中77.78%的公众认为互联网企业有意不承担或少承担网络安全责任，60.52%认为互联网企业网络安全管理水平低下，57.76%认为其网络安全责任意识不强。

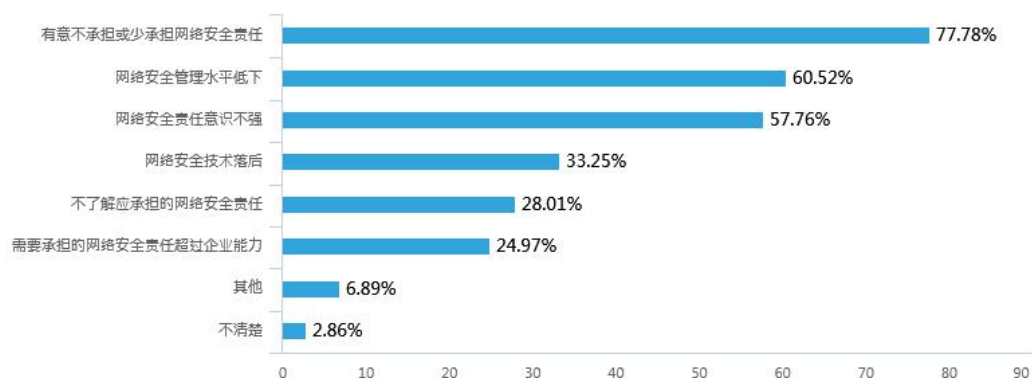


表 54：公众对互联网企业网络安全负面评价的原因

在信息内容监管方面，公众对网络平台对其自媒体平台 and 短视频平台信息内容监管措施的评价总体向好，47.67%的公众认为对自媒体平台的监管措施比较有效或非常有效，32%认为效果一般；44.66%的公众认为对短视频平台的监管措施比较有效或非常有效，34.93%认为效果一般；在群主对网络群组的监管措施方面，39.51%的公众认为比较有效或非常有效，33.65%认为效果一般。

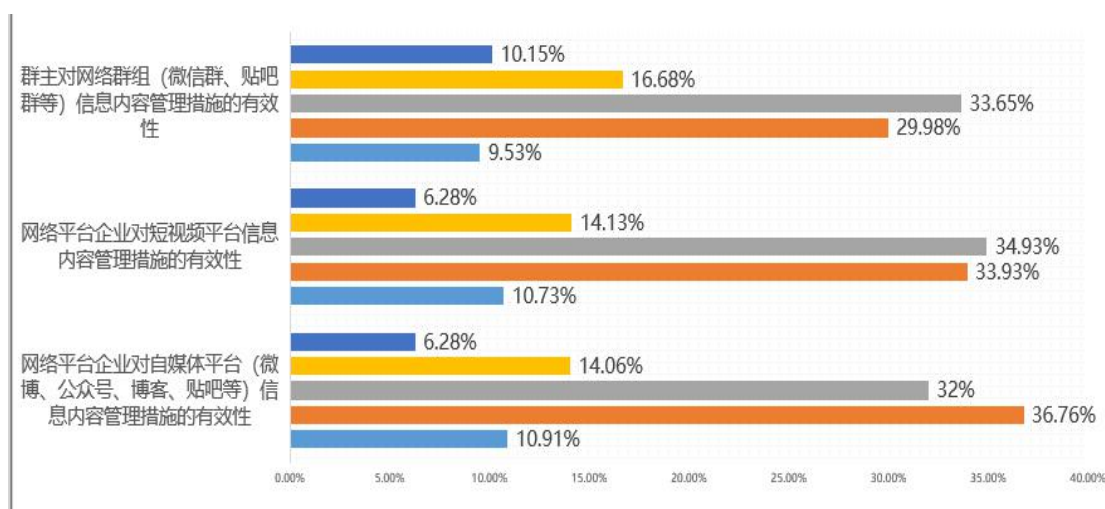


表 55：公众对平台和群主监管措施有效性的评价

在公众遭遇的信息内容不合规问题方面，网络谣言与诽谤、网络色情、个人隐私信息泄露是最常遭遇的三大问题，过半数公众表示曾遭遇过上述问题。

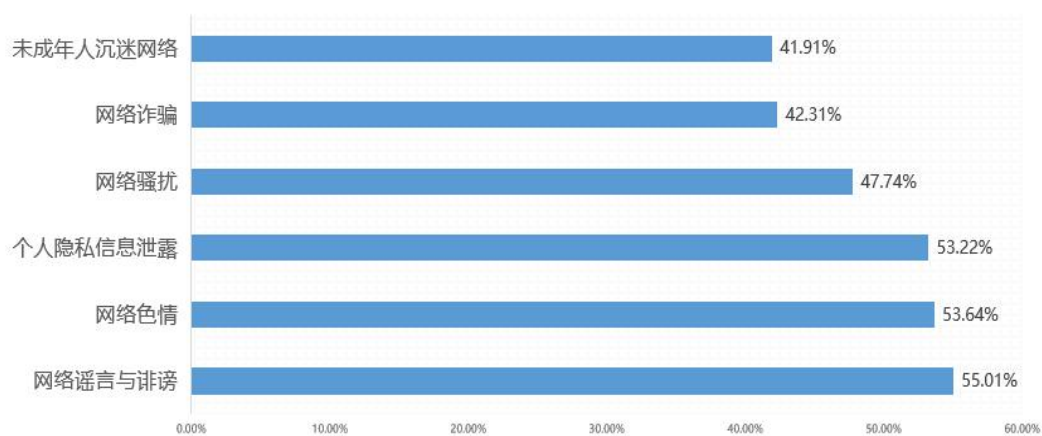


表 56：公众在自媒体平台、短视频平台、网络群组中遇到的不合规问题¹⁵

问题发生后，向网络平台投诉的占比持平，55.34%的公众表示会向平台投诉。公众认为平台接到投诉后的响应速度一般，仅 17.52% 的公众认为速度很快，31.78% 的公众认为响应速度很慢；对于投诉结果，62.46% 的公众表示对结果不满意，56.27% 的公众认为投诉处理周期长。

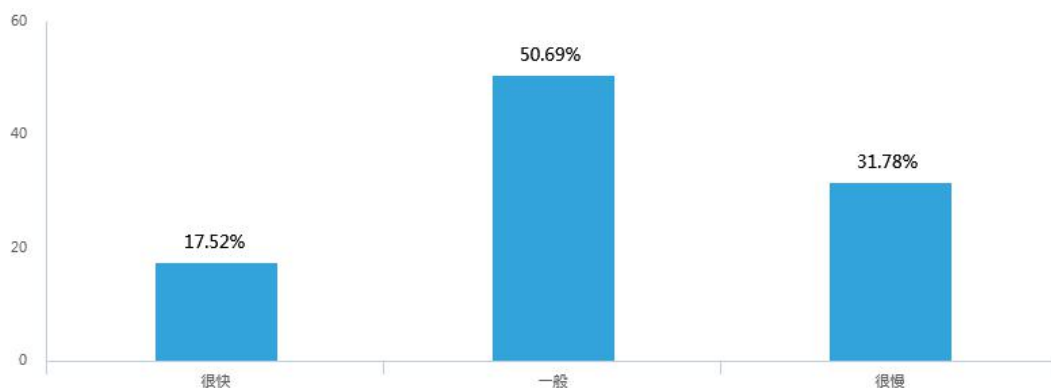


表 57：公众认为投诉后平台的响应速度

¹⁵ 内容经过筛选，仅选取占比超过 40% 的选项

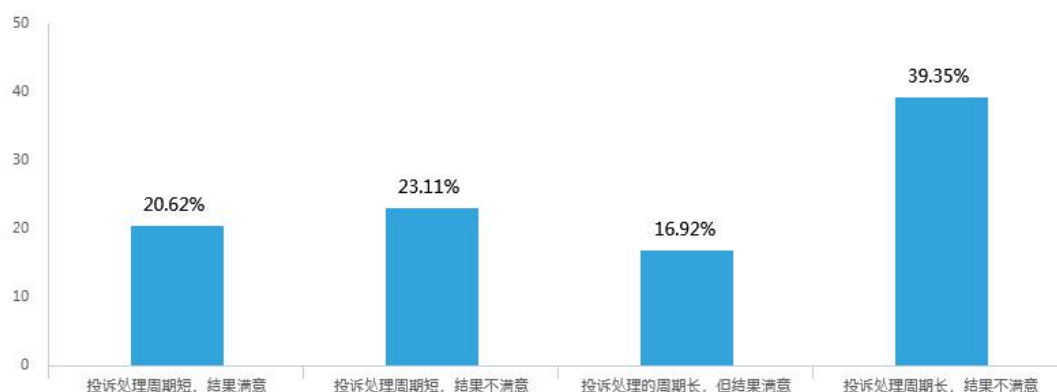


表 58：公众对投诉结果的满意程度

调查说明，网民对互联网企业在网络安全方面的履责评价一般，网民认为互联网企业有意不承担或少承担网络安全责任，但平台在信息内容治理方面的管理措施在一定程度上得到网民认可。互联网企业的网络安全合规和保障能力亟待提升，处理网民投诉建议的水平有待提高。

12) 网络安全执法工作满意度较高，执法力度得到认可

调查显示，受调查从业人员认为网信、公安和工信是最常见的网络安全执法部门，占比最高的前五个部门分别是网信、公安、工信、国安和保密部门。

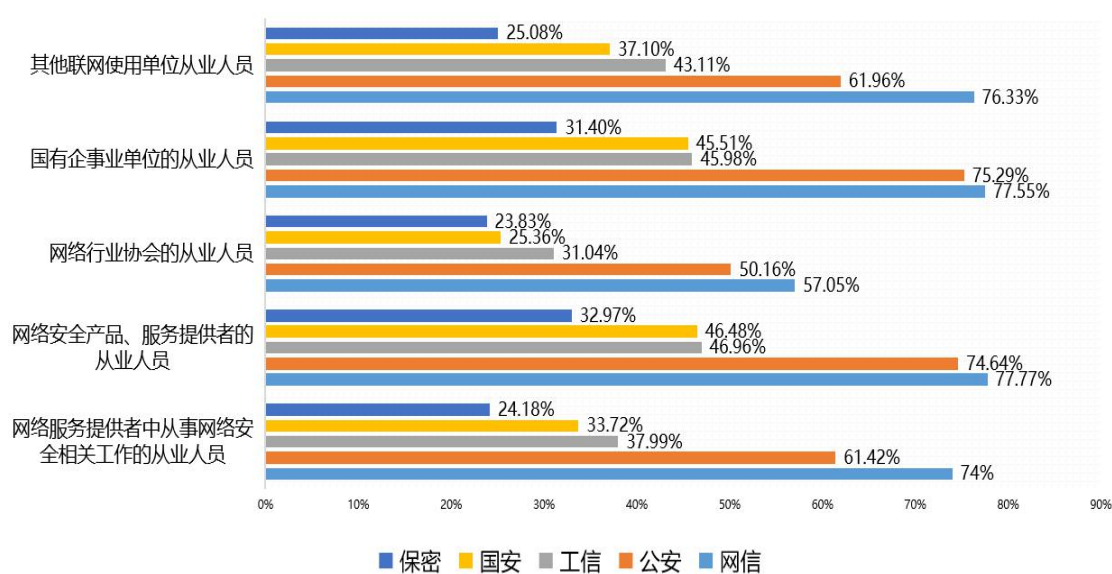


表 59：受调查从业人员认为哪些政府部门是网络安全行政执法部门¹⁶

在执法满意度方面，公众对政府部门在遏制网络违法犯罪工作方面的工作成效满意度较高，35.87%的公众表示基本满意，43.35%的公众认为非常满意或比较满意。

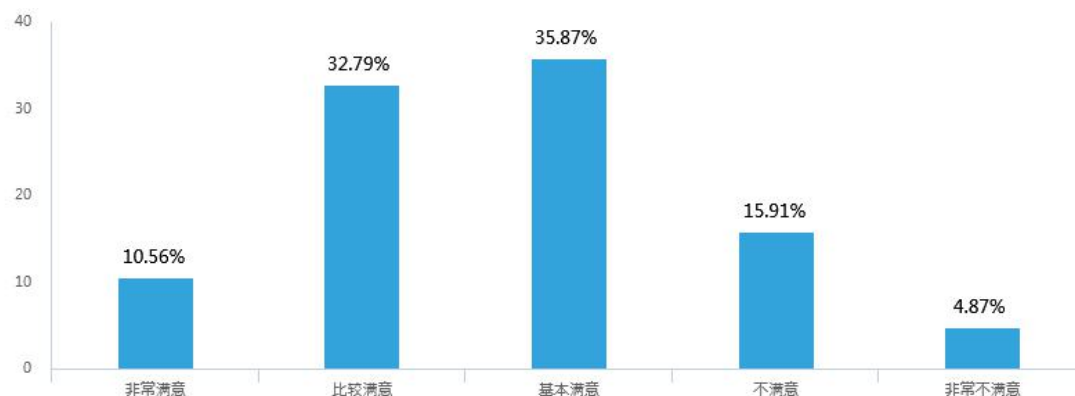


表 60：公众对遏制网络违法工作成效的评价

从业人员方面，半数受调查从业人员认为政府部门的执法力度强或比较强，三分之一左右的受调查从业人员认为力度一般。

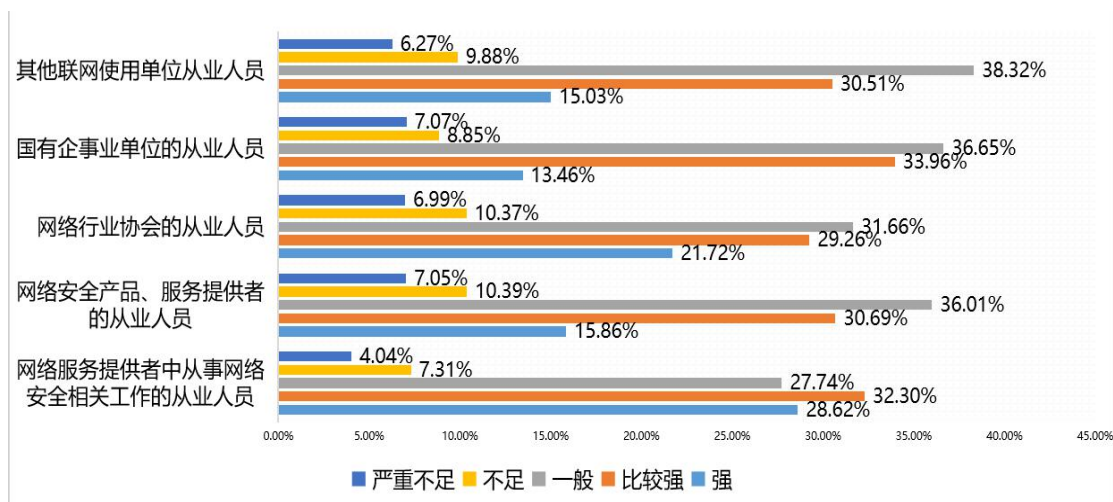


表 61：受调查从业人员对政府部门在网络安全方面的执法力度的评价

对公安执法满意度方面，从业人员满意度较高，59.89%的网络服务提供者中从事网络安全工作的从业人员对公安执法表示满意，但仍有 21.20%的其他联网使用单位中的从业人员表示未参加过公安执法

¹⁶ 内容经过筛选，仅选取占比最高的五个选项

检查。

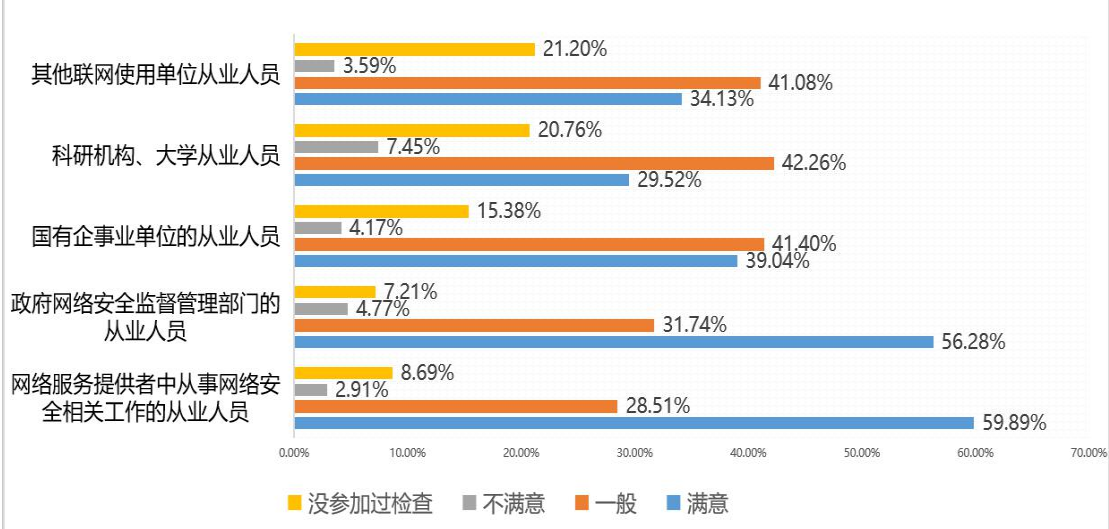


表 62：受调查从业人员对公安执法的满意度

在制约网络安全执法能力方面，受调查从业人员认为人员、包括取证能力和检测能力在内的专业技术能力、以及法律素质是主要制约因素。

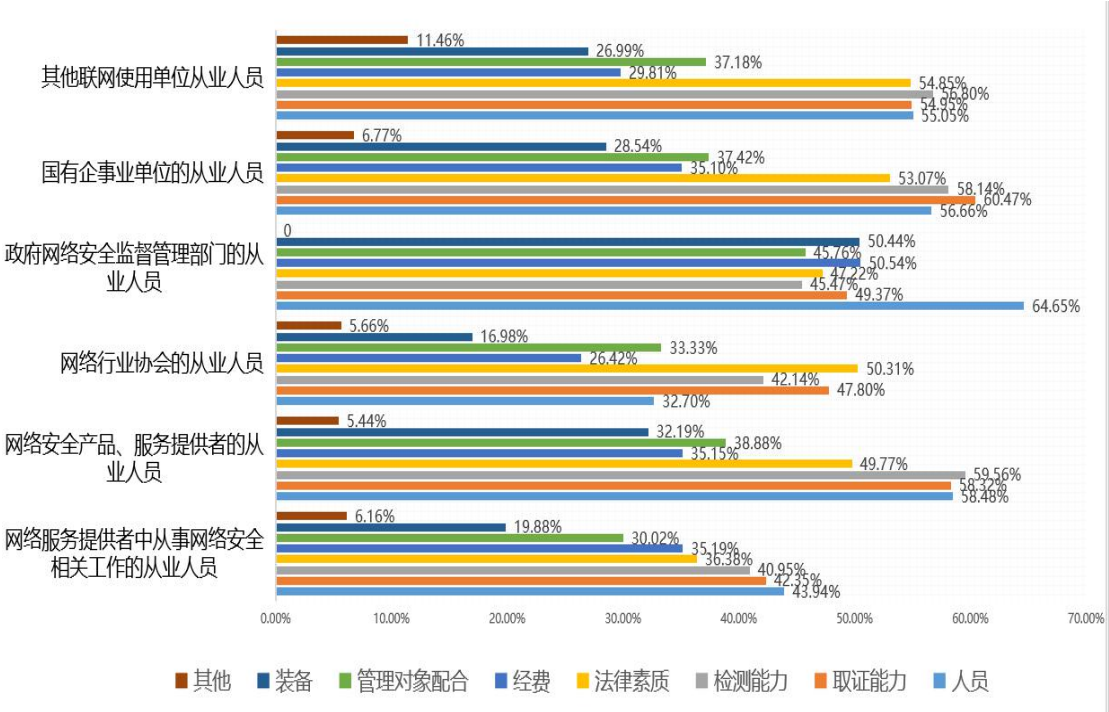


表 63：受调查从业人员认为网络安全执法能力的制约因素

在针对政府网络安全监管部门从业人员的专项调查中发现，

62.12%的从业人员认为我国当前网络安全执法依据较为充足；在政府部门的网络安全执法力度方面，56.57%认为还需加强。此外，64.65%认为人员是制约网络安全执法的首要因素，在检测、检查、取证和应急工具方面的装备还需加强。

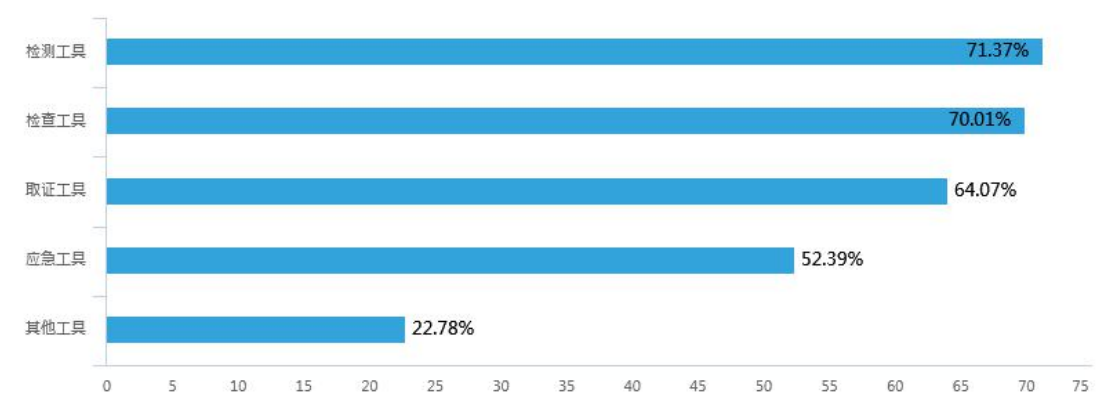


表 64：政府网络安全监督管理部门的从业人员认为在政府网络安全执法中还需加强哪些装备

调查说明，《网络安全法》正式施行以来，我国网信、公安、工信等部门通过执法大检查、“净网”、“护网”等专项行加强网络安全执法力度，社会满意度较高。

三、“网络安全法制建设”网民安全感满意度调查结论和建议

经调查分析可知，我国网民网络安全感有所提升，对网络安全法制建设满意度也较高，但仍需立足社会核心诉求，围绕完善立法、深化网络生态治理、创新安全治理路径、加快等保配套出台、推进平台责任落实等方面持续推动我国网络空间治理。

（一）立足核心诉求问题，实施精准立法策略

加强网络安全法制建设已成为社会解决网络安全问题的首选途径，我国网络安全法制建设肩负着维护网络安全，保障网络空间主权和国家利益的艰巨历史使命。

从社会的强烈诉求可以看出，在后续制度建设过程中，应以解决网络安全核心和突出问题为首要任务，实施精准立法策略，加快个人信息保护、网络平台责任和数据安全保护立法进程。

当前，我国已将《个人信息保护法》《数据安全法》纳入十三届全国人大常委会的立法规划，同属条件比较成熟、任期内拟提请审议的法律草案；配套制度层面，《数据安全管理办法》《个人信息出境安全评估办法》正在制定过程中；地方上，天津正式发布《数据安全管理办法（暂行）》，贵州正式发布《贵州省大数据安全保障条例》，围绕数据生命周期安全、数据跨境安全评估等问题先试先行，尤其是自贸区数据安全管理制度设计成为热点。网络平台责任方面，主要从加强网络信息内容治理、落实网络安全等级保护和关键信息基础设施重点保护责任、强化数据安全保障义务等方面夯实网络运营者责任。

（二）深化网络生态治理，净化网络空间环境

随着信息化与社会各领域的深度融合，移动互联网、物联网快速发展，未成年人上网已成普遍现象。网络游戏的兴起、自媒体时代的到来使得网络游戏、在线视频和短视频成为未成年人使用最多的三类应用。但网络游戏内容良莠不齐，涉及血腥、暴力、色情等违法有害信息的情况屡见不鲜；短视频行业快速兴起的同时监管尚不到位，存在导向不正、片面追求流量和用户黏性的倾向。对此，我国高度重视对未成年人影响较大的网络游戏和网络信息内容监管。

政策立法方面，2010年，我国发布《网络游戏管理暂行办法》，要求网络游戏经营单位应当按照国家规定，采取技术措施，禁止未成年人接触不适宜的游戏或者游戏功能，限制未成年人的游戏时间，预防未成年人沉迷网络；2017年，我国公布《未成年人网络保护条例（送审稿）》，要求加强网络信息内容建设和网络权益保障，在预防和干预方面，要求禁止未成年人接触不适宜其接触的游戏或游戏功能，限制未成年人连续使用游戏的时间和单日累计使用游戏的时间，禁止未成年人在每日0：00至8：00期间使用网络游戏服务；2018年，国家网信办和公安部联合发布《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》，要求包括微博客、短视频、网络直播在内的互联网信息服务提供者开展安全评估，重点评估个人信息以及防范违法有害信息传播扩散、社会动员功能失控风险的技术措施；2019年，国家网信办发布《儿童个人信息网络保护规定》，保障不满十四周岁未成年人的个人信息安全；2019年9月10日，国家互联网信息办公室

发布《网络生态治理规定（征求意见稿）》，加强网络生态治理，构建田朗气清的网络空间。

执法方面，2018、2019 年，国家网信办、工信部、公安部、国家新闻出版广电总局等多部门在各自职权范围内加强对内容相关行业的执法力度，多次通过约谈、专项行动等方式加强平台监管。

行业自律方面，2019 年，中国网络视听节目服务协会发布《网络短视频平台管理规范》和《网络短视频内容评审标准规则》，要求网络短视频平台实行节目内容先审后播制度。平台上播出的所有短视频均应经内容审核后方可播出，包括节目的标题、简介、弹幕、评论等内容。

此外，老年群体对新技术新应用发展不敏感，对手段不断翻新的网络违法犯罪防范能力较差，应加强针对老年群体的防网络诈骗、虚假信息宣传普及，在监管部门持续打击网络违法犯罪的同时，提升老年群体的自我防范意识和自我保护能力。

（三）关注新技术新应用，创新安全治理路径

以 5G、人工智能为代表的新技术新应用发展已成为社会关注的焦点。5G 正式商用在即，构建适应 5G 应用需要的网络安全治理架构成为领域内最受关注的重点内容。

在推动 5G 应用发展的同时，我国须重视 5G 引入的新型风险，加强 5G 网络安全技术标准体系建设，加强对 5G 网络信息安全核心技术的知识产权管理，制定针对不同应用场景的法律法规及监管措施。

（四）加快等保配套出台，持续推进宣传贯彻

目前，网络安全等级保护制度已围绕《网络安全法》形成了法律、行政法规、部门规章和技术标准等相对完善的等保 2.0 体系。2018 年 6 月，公安部《网络安全等级保护条例（征求意见稿）》正式向社会公开征求意见；2018 年公安部发布规范性文件《网络安全等级保护测评机构管理办法》，全面规范测评机构行为。2018 年 12 月，国家网络安全等级保护工作协调小组办公室根据 2018 年度全国网络安全等级保护测评机构监督检查和测评能力验证工作情况，按照有关规定，责令多家测评机构开展为期 3-12 个月不等的整改，整改期间暂停开展等级测评业务；国家标准方面，2019 年 5 月，部分等保 2.0 系列标准（《网络安全等级保护基本要求》《网络安全等级保护测评要求》《网络安全等级保护安全设计技术要求》）正式出台，2019 年 12 月 1 日正式施行；2019 年 8 月 30 日，等保 2.0 标准之《网络安全等级保护实施指南》正式发布，2020 年 3 月 1 日正式施行。

在行政执法方面，大量的网络安全等级保护执法案例体现了等级保护制度要求进入网络安全基础立法后的强制性，“以案为鉴”强化了法律威慑力，提升了责任主体的网络安全法律意识，也有力督促了其它网络运营者依法履行网络安全保护义务。

经调查发现，除家庭和个人自建自用的网络外，所有网络运营者都是等保义务主体的这一制度要求尚未得到全面贯彻，实践中仍存在模糊。此外，网络安全测评机构虽然规模、能力等存在差异，但其出具的等级测评结果却有同样的法律效力。调查发现，提高测评机构满

意度和服务能力也是网民十分关注的问题，应进一步加强对测评机构的质量控制、能力提升、诚信执业等规范化管理工作。

等保 2.0 国家标准宣贯工作广泛实施，在全社会范围内效果明显，进一步推动了网络安全等级保护制度的落实。但相较于国家网络安全保护基本制度这一法律定位，等保 2.0 宣贯范围仍有待扩大，应充分利用行业、专业论坛、媒体等多渠道持续推动宣传教育和培训工作。

（五）加强企业合规指引，推进平台责任落实

网络运营者是落实《网络安全法》，夯实网络安全保障义务的重要主体，但网络运营者目前的网络安全履责能力在公众方面的认可程度仍待提高。

面对数据泄露和滥用事件频发、网络违法有害信息泛滥的网络安全形势，面对 77.78% 的公众认为网络运营者有意不承担或少承担网络安全责任的调查结果，网络运营者应持续提高合规能力，全面落实网络安全责任，保障用户信息安全，净化网络信息内容。

附件：我国网络安全相关战略、立法及配套分类总览

文件名称	发布机关	生效时间	法律状态
国家战略			
国家网络空间安全战略	国家互联网信息 办公室	2016-12-27	现行有效
网络空间国际合作战略	外交部、国家互联 网信息办公室	2017-03-01	现行有效
基础性立法			
中华人民共和国刑法	全国人民代表大 会	1997-10-01	现行有效
中华人民共和国保守国家 秘密法	全国人民代表大 会常务委员会	1989-05-01	现行有效
中华人民共和国人民警察 法	全国人民代表大 会常务委员会	1995-02-28	现行有效
全国人民代表大会常务委 员会关于维护互联网安全 的决定	全国人民代表大 会常务委员会	2000-12-28	现行有效
中华人民共和国电子签名 法	全国人民代表大 会常务委员会	2005-04-01	现行有效
中华人民共和国治安管理 处罚法	全国人民代表大 会常务委员会	2006-03-01	现行有效
全国人民代表大会常务委 员会关于加强网络信息保 护的决定	全国人民代表大 会常务委员会	2012-12-28	现行有效
中华人民共和国反间谍法	全国人民代表大 会常务委员会	2014-11-01	现行有效
中华人民共和国国家安全 法	全国人民代表大 会常务委员会	2015-07-01	现行有效

中华人民共和国反恐怖主义法	全国人民代表大会常务委员会	2016-01-01	现行有效
中华人民共和国网络安全法	全国人民代表大会常务委员会	2017-06-01	现行有效
中华人民共和国国家情报法	全国人民代表大会常务委员会	2017-06-28	现行有效
出口管制法(草案征求意见稿)	商务部	2017-06-16	正式版尚未发布, 尚未生效
密码法(草案)	全国人民代表大会常务委员会	2019-07-05	正式版尚未发布, 尚未生效
网络安全相关行政法规、部门规章及规范性文件			
网络安全管理			
中华人民共和国计算机信息系统安全保护条例	国务院	1994-02-18	现行有效
中华人民共和国计算机信息网络国际联网管理暂行规定	国务院	1996-02-01	现行有效
计算机信息系统安全专用产品检测和销售许可证管理办法	公安部	1997-12-12	现行有效
计算机信息网络国际联网安全保护管理办法	公安部	1997-12-30	现行有效
计算机病毒防治管理办法	公安部	2000-04-26	现行有效
中华人民共和国电信条例	国务院	2000-09-25	现行有效
互联网安全保护技术措施规定	公安部	2006-03-01	现行有效
公安机关互联网安全监督检查规定	公安部	2018-11-01	现行有效
云计算服务安全评估办法	国家互联网信息	2019-07-02	现行有效

	办公室、国家发展和改革委员会、工信部、财政部		
网络安全漏洞管理规定(征求意见稿)	工信部	2019-06-18	正式版尚未发布, 尚未生效
网络安全等级保护与关键信息基础设施保护			
信息安全等级保护管理办法	公安部、国家保密局、国家密码管理局、国务院信息工作办公室	2007-06-22	现行有效
工业控制系统信息安全事件应急管理工作指南	工信部	2017-07-01	现行有效
工业控制系统信息安全防护能力评估工作管理办法	工信部	2017-09-01	现行有效
网络安全等级测评机构管理办法	公安部	2018-03-23	现行有效
网络关键设备和网络安全专用产品安全认证实施规则	认监委	2018-06-27	现行有效
水利网络安全管理办法(试行)	水利部	2019-08-16	现行有效
关键信息基础设施安全保护条例(征求意见稿)	国家互联网信息办公室	2017-07-12	正式版尚未发布, 尚未生效
网络安全等级保护条例(征求意见稿)	公安部	2018-06-27	正式版尚未发布, 尚未生效
网络关键设备安全检测实施办法(征求意见稿)	工信部	2019-06-05	正式版尚未发布, 尚未生效
网络安全审查			
网络产品和服务安全审查	国家互联网信息	2017-06-01	现行有效

办法（试行）	办公室		
网络安全审查办法（征求意见稿）	国家互联网信息 办公室	2019-05-21	正式版尚未发布，尚未生效
个人信息保护与数据安全			
电信和互联网用户个人信息保护规定	工信部	2013-09-01	现行有效
科学数据管理办法	国务院办公厅	2018-03-17	现行有效
人类遗传资源管理条例	国务院	2019-07-01	现行有效
儿童个人信息网络保护规定	国家互联网信息 办公室	2019-10-01	尚未生效
数据安全管理办法（征求意见稿）	国家互联网信息 办公室	2019-05-28	正式版尚未发布，尚未生效
个人信息出境安全评估办法（征求意见稿）	国家互联网信息 办公室	2019-06-13	正式版尚未发布，尚未生效
互联网信息服务严重失信主体信用信息管理办法（征求意见稿）	国家互联网信息 办公室	2019-07-22	正式版尚未发布，尚未生效
网络信息内容安全			
互联网信息服务管理办法	国务院	2000-09-25	现行有效
互联网视听节目服务管理规定	国家新闻出版广电总局、信息产业部	2008-01-31	现行有效
规范互联网信息服务市场秩序若干规定	工信部	2012-03-15	现行有效
即时通信工具公众信息服务发展管理暂行规定	国家互联网信息 办公室	2014-08-07	现行有效
互联网危险物品信息发布管理规定	公安部、国家互联网信息办公室、工信部、环境保护	2015-02-05	现行有效

	部、国家工商行政管理总局、国家安全生产监督管理总局		
互联网用户账号名称管理规定	国家互联网信息办公室	2015-03-01	现行有效
互联网新闻信息服务单位约谈工作规定	国家互联网信息办公室	2015-04-28	现行有效
互联网信息搜索服务管理规定	国家互联网信息办公室	2016-08-01	现行有效
移动互联网应用程序信息服务管理规定	国家互联网信息办公室	2016-08-01	现行有效
互联网直播服务管理规定	国家互联网信息办公室	2016-12-01	现行有效
网络表演经营活动管理办法	文化部	2017-01-01	现行有效
互联网新闻信息服务管理规定	国家互联网信息办公室	2017-06-01	现行有效
互联网新闻信息服务许可管理实施细则	国家互联网信息办公室	2017-06-01	现行有效
互联网信息内容管理行政执法程序规定	国家互联网信息办公室	2017-06-01	现行有效
互联网跟帖评论服务管理规定	国家互联网信息办公室	2017-10-01	现行有效
互联网论坛社区服务管理规定	国家互联网信息办公室	2017-10-01	现行有效
互联网用户公众账号信息服务管理规定	国家互联网信息办公室	2017-10-08	现行有效
互联网群组信息服务管理规定	国家互联网信息办公室	2017-10-08	现行有效

规定	办公室		
互联网新闻信息服务新技术新应用安全评估管理规定	国家互联网信息 办公室	2017-12-01	现行有效
互联网新闻信息服务单位内容管理从业人员管理办法	国家互联网信息 办公室	2017-12-01	现行有效
微博客信息服务管理规定	国家互联网信息 办公室	2018-03-20	现行有效
具有舆论属性或社会动员能力的互联网信息服务安全评估规定	国家互联网信息 办公室、公安部	2018-11-30	现行有效
金融信息服务管理规定	国家互联网信息 办公室	2019-02-01	现行有效
区块链信息服务管理规定	国家互联网信息 办公室	2019-02-15	现行有效
网络生态治理规定（征求意见稿）	国家互联网信息 办公室	2019-09-10	正式版尚未发布，尚未生效
密码安全			
商用密码管理条例	国务院	1999-10-07	现行有效
新技术新应用			
网络预约出租汽车经营服务管理暂行办法	交通运输部、工信部、公安部、商务部、工商总局、质检总局、国家网信办	2016-11-01	现行有效
网络预约出租汽车监管信息交互平台运行管理办法	交通运输部	2018-03-01	现行有效
智能网联汽车道路测试管	工信部、公安部、	2018-05-01	现行有效

理规范（试行）	交通运输部		
地方性立法			
贵州省大数据安全保障条例	贵州省人民代表大会常务委员会	2019-10-01	尚未生效
天津市数据安全管理办法（暂行）	天津市互联网信息办公室	2019-08-01	现行有效

表 65：我国网络安全相关战略、立法及配套制度