

数字政府安全服务的调查报告

中国电子信息产业研究院网络安全研究所

赛迪区块链研究院

2019 年 9 月

目录

一、数字政府安全服务调查背景.....	1
二、我国网民网络安全感满意度调查样本总体情况.....	3
（一）2019 年参与调查人员基本信息.....	3
1. 参与调查的网民性别分布.....	3
2. 参与调查的网民年龄分布.....	4
3. 参与调查的网民学历分布.....	5
4. 参与调查的公众网民网龄分布.....	6
5. 参与调查的公众网民职业分布.....	6
6. 参与调查的公众网民地区分布.....	7
7. 参与调查的网络从业人员从业岗位分布.....	8
8. 参与调查的网络从业人员从业时间分布.....	9
9. 参与调查的网络从业人员所在单位网络服务范围分布.....	10
（二）2019 年与 2018 年参与调查人员基本信息情况对比.....	12
1. 参与调查的网民性别分布均衡性有所提高.....	12
2. 参与调查的网民年龄阶段分布老年人占比有所增加.....	14
3. 参与调查的高学历网民人数有所扩张.....	16
三、我国网民网络安全感满意度整体情况分析.....	18
（一）2019 年过半网民认为网络总体是安全的.....	18
（二）2019 年我国网民网络安全感满意度有较大的提高.....	18
（三）从业人员对网络安全状况基本满意.....	19
四、数字政府安全服务调查分析.....	21

（一）政务各领域网上服务需要继续加强.....	21
1. 在银行领域的政府网上服务使用率最高.....	21
2. 教育、医疗等政府网上服务仍需要加强.....	22
（二）政府网上服务的便捷性仍需提高.....	23
（三）政府网上服务存在安全隐患.....	24
1. 个人隐私信息易泄露是政府网上服务的最大风险.....	25
2. 教育、医疗信息是最易泄露的的服务领域.....	26
3. 从业人员对个人信息保护满意度较低.....	28
4. 网民对国家个人信息保护的立法的态度.....	29
（四）政府网络安全监管有待完善.....	29
1. 网民对政府网络安全监管的态度.....	30
2. 从业人员对政府网络安全监管的态度.....	31
五、对我国数字政府安全服务的建议.....	34
（一）强化顶层设计，完善政务服务的制度体系.....	34
（二）进一步完善个人信息安全的保护手段.....	34
（三）优化业务流程提高政府网上服务便利性.....	35
（四）加强政府网络安全监管，营造社会良好网络安全氛围.....	36

一、数字政府安全服务调查背景

数字政府是以新一代信息技术为支撑，通过数据驱动重塑政务信息化管理架构、业务架构和组织架构，以提升政府体系和治理能力现代化为主要目标的建立在互联网上、以数据为主体的虚拟政府，是一种新型政府运行模式。数字政府既是互联网+政务深度发展的结果，也是大数据时代政府自觉转型升级的必然趋势。

“数字政府”是“数字中国”体系的有机组成部分，是推动“数字中国”建设、实现经济高质量发展、再创营商环境新优势的重要抓手和重要引擎。党中央、国务院高度重视数字政府建设，并将其作为实现国家治理体系和治理能力现代化的战略支撑，提出以电子政务为抓手，推进政府管理和社会治理模式创新，实现政府决策科学化、社会治理精准化、公共服务高效化。在2018年政府工作报告对数字政府建设提出了具体要求，“实施大数据发展行动，加强新一代人工智能研发应用，在医疗、养老、教育、文化、体育等多领域推进‘互联网+’”“深入推进‘互联网 政务服务’，使更多事项在网上办理，必须到现场办的也要力争做到‘只进一扇门’‘最多跑一次’”“加快政府信息系统互联互通，打通信息孤岛”等。

2017年以来我国政府网上政务服务能力持续提高，目前全国“互联网+政务服务”工作已初步形成良好的工作格局，一体化网上政务服务成为建设“数字政府”的战略选择。全国各地区

均大力推进高水平的网上政务服务建设，在多个方面取得了明显成效，主要体现在以下几个方面：一体化网上政务服务平台建设全面提速，平台体系基本建成；全面优化网上服务成为深化行政审批制度，体制机制逐步健全；一网服务成为发展重点，供给能力持续加强；政府网上服务协同共享，用户体验显著提升。

与此同时，目前各省级政府网上政务服务还面临着网上政务服务平台覆盖面和精细度不够、线上线下融合及多渠道服务整合不充分、政务服务信息共享和业务协同程度不高、政府网络安全监管机制不完善等问题。为了更深入了解人们对当前政府网上安全服务的态度和意见，由公安部网络安全保卫局指导，全国 135 家网络安全社会组织共同发起，调查了全国 172075 名网民和 26513 名网络从业人员对政府网上服务的看法。

二、我国网民网络安全感满意度调查样本总体情况

（一）2019 年参与调查人员基本信息

本次网络安全满意度问卷调查针对两个不同人群，分别是对网民调查和从业人员调查。网民调查共收回网民调查问卷 189495 份，经数据清洗消除无效数据后，共有 172075 份问卷数据纳入统计；从业人员网络安全满意度调查问卷有 31771 份，数据清洗消除无效数据后，有 26513 份问卷数据纳入统计。经统计，参与调查的人员基本情况如下：

1. 参与调查的网民性别分布

一是参与调查的公众网民性别分布，男性网民占比 67%，女性网民占比 33%。二是参与调查的网络从业人员性别分布，男性网民占比 70.21%，女性网民占比 29.79%，比例基本一致。

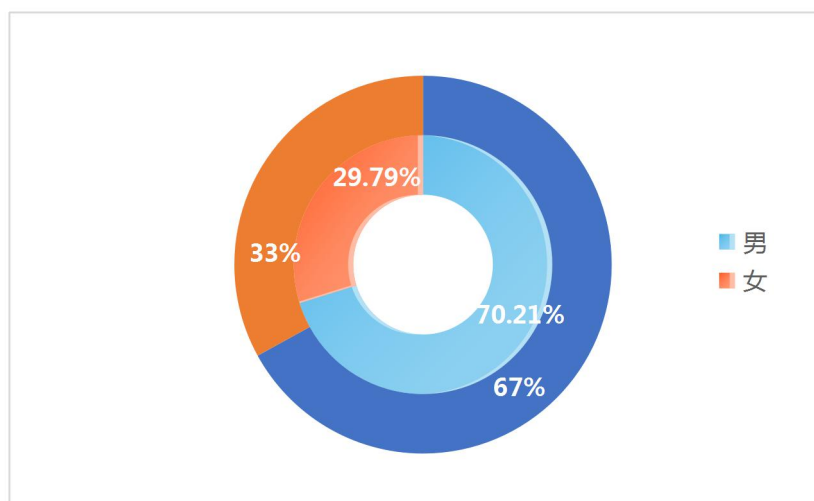


图 2-1 参与调查的公众及从业人员的性别比例

2. 参与调查的网民年龄分布

一是参与调查的公众网民年龄分布。在参与调查的公众网民中，12-18 岁年龄阶段网民占比 22.46%，19-24 岁年龄阶段网民占比 34.84%，25-30 岁年龄阶段网民占比 17.94%，31-45 岁年龄阶段网民占比 18.44%，46-60 岁年龄阶段网民占比 5.60%，60-80 岁年龄阶段网民占比 0.73%。二是参与调查的网络从业人员年龄分布。在参与调查的网络从业人员中，12-18 岁年龄阶段网民占比 4.84%，19-24 岁年龄阶段网民占比 32.82%，25-30 岁年龄阶段网民占比 32.04%，31-45 岁年龄阶段网民占比 25.31%，46-60 岁年龄阶段网民占比 3.45%，60-80 岁年龄阶段网民占比 0.55%。从年龄分布上来看，网民主要集中于青年，而参与调查的从业人员相对更年长。

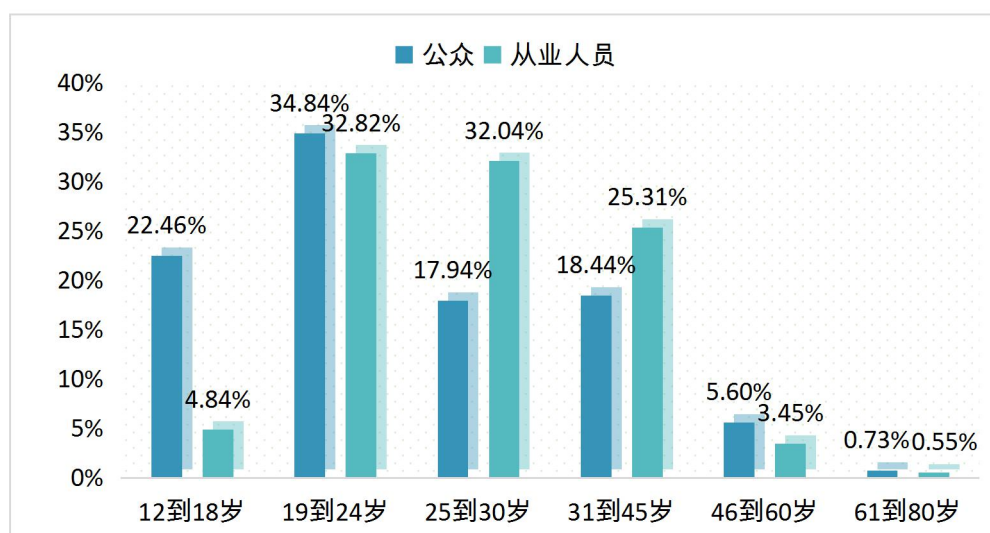


图 2-2 参与调查网民的年龄分布

3. 参与调查的网民学历分布

一是参与调查的公众网民学历分布。在参与调查的公众网民中,初中及以下学历网民占比 9.32%,高中学历网民占比 18.09%,中专学历网民占比 7.06%,大专学历网民占比 22.95%,本科学历网民占比 36.67%,硕士学历网民占比 4.27%,博士学历网民占比 1.63%。二是参与调查的网络从业人员学历分布。在参与调查的网络从业人员中,高中以下学历网民占比 4.24%,高中中专网民占比 10.22%,大专学历网民占比 24.24%,本科学历网民占比 50.08%,硕士学历网民占比 8.72%,博士学历网民占比 2.50%。从学历分布上来看,无论是参与调查的公众网民还是参与调查的网络从业人员,大学本科学历人数最多。参与调查的公众网民本科以上学历占比为 42.57%,参与调查的网络从业人员本科以上学历占比达 61.3%,相比较而言,网络从业人员的学历水平高于公众网民的学历水平。

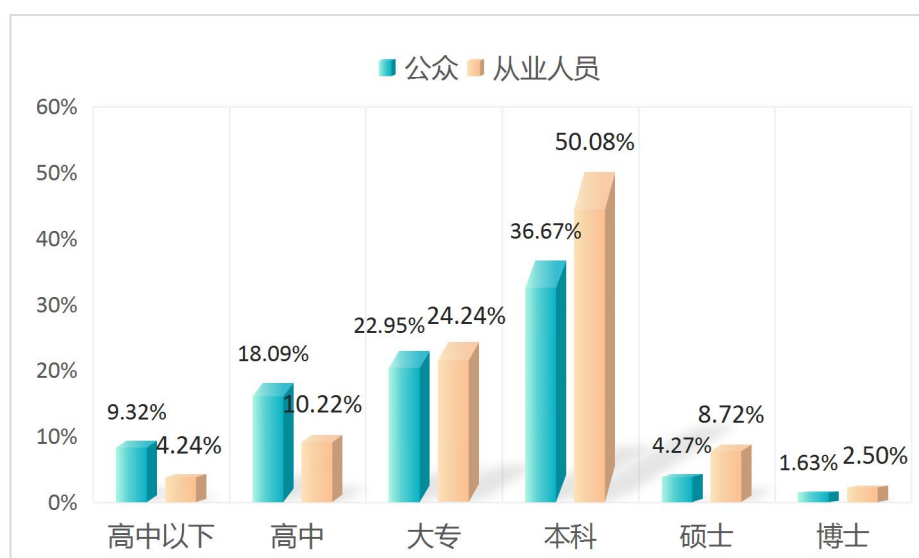


图 2-3 参与调查网民的学历分布

4. 参与调查的公众网民网龄分布

统计参与调查的公众网民的网龄分布，从网龄分布来看，网龄在 1-3 年的公众网民占比 9.18%，网龄在 4-6 年的公众网民占比 22.37%，网龄在 7-9 年的公众网民占比 18.44%，网龄在 10-12 年的公众网民占比 23.52%，网龄在 13-15 年的公众网民占比 11.13%，网龄在 16-18 年的公众网民占比 5.69%，网龄在 19-30 年的公众网民占比 9.68%。

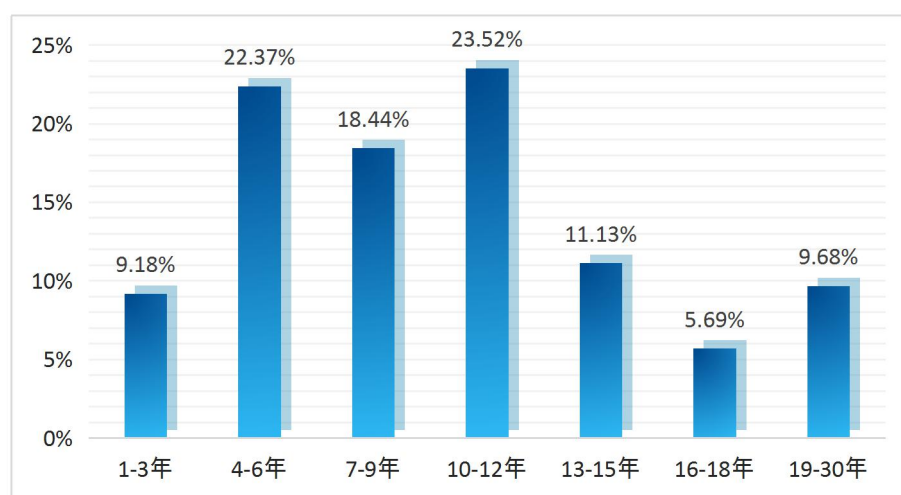


图 2-4 参与调查公众网民的网龄分布

5. 参与调查的公众网民职业分布

统计参与调查的公众网民的职业分布，从职业分布来看，在校学生占比 35%，企业一般员工占比 14.48%，教师占比 11.56%，工程技术人员占比 7.19%，企业管理人员占比 5.22%，政府公务人员占比 3.03%，医生占比 1.29%，农业人员占比 1.27%，媒体从业人员占比 1%，研究人员占比 0.54%，法律从业人员占比

0.39%。其中在校学生占比数量最高，超过企业一般员工占比的2倍之多。

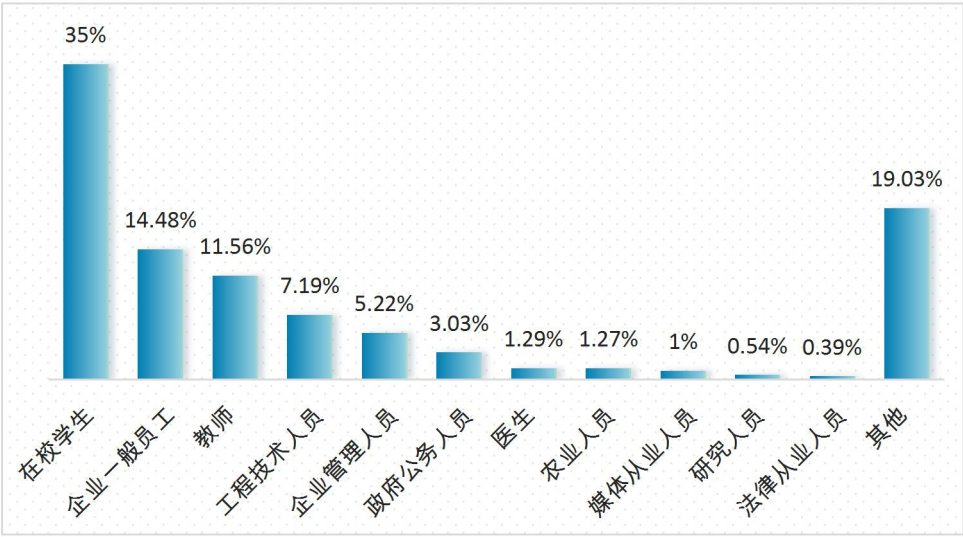


图 2-5 参与调查网民的职业分布图

6. 参与调查的公众网民地区分布

统计参与调查的公众网民的地区分布，从地区分布来看，参与调查的网民来自全国各省、市、自治区和港澳台地区，覆盖面广。网民常住地(居住满6个月)的地区分布情况如下图。从图中可以看出，浙江、广东一带的东南地区参与调查的网民占比最多，其他地区，如东北地区、西北地区、西南地区以及港澳台地区参与调查的网民占比相对较少。

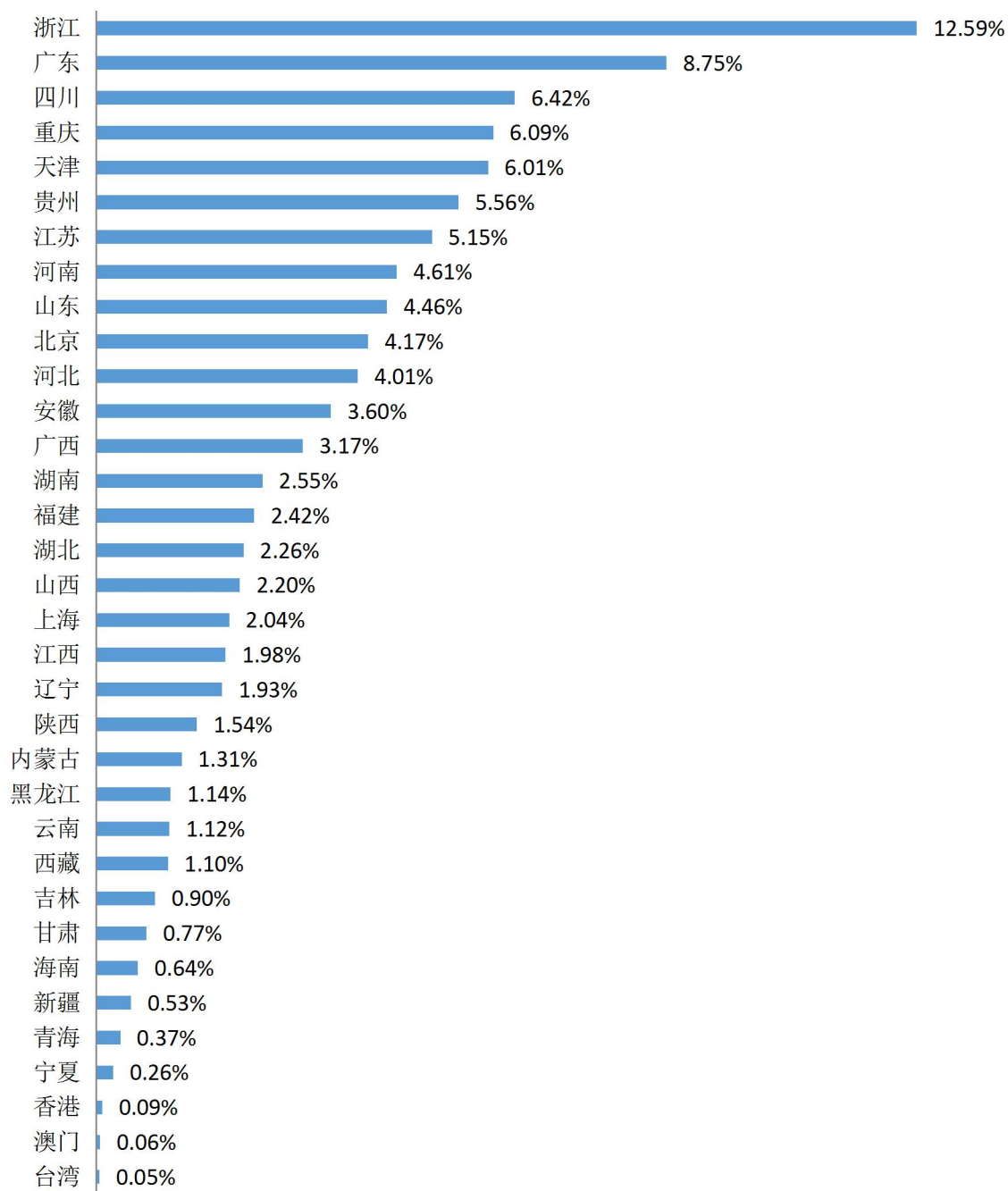


图 2-6 参与调查的公众网民的常住地区分布

7. 参与调查的网络从业人员从业岗位分布

统计参与调查的网络从业人员工作岗位分布，在采集的网络从业人员的 26513 份调查问卷中，有 4430 位网络从业人员从事

网络服务提供者的网络安全相关工作，占比 16.17%；有 4645 位网络从业人员从事网络服务提供者的非网络安全相关工作，占比 17.52%；有 3705 位网络从业人员从事网络安全产品、服务提供者相关工作，占比 13.97%；有 915 位网络从业人员在网络行业协会工作，占比 3.45%；有 1027 位网络从业人员在政府网络安全监督管理部门工作，占比 3.87%；有 2971 位网络从业人员在国有企事业单位工作，占比 11.21%；有 2442 位网络从业人员在科研机构、大学工作，占比 11.21%；有 2971 位网络从业人员从事国有企事业单位相关工作，占比 11.21%。

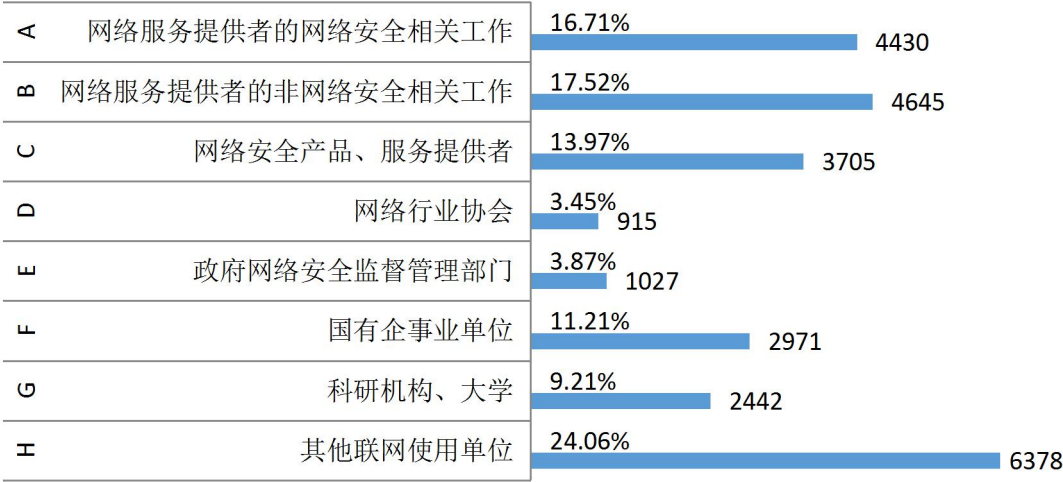


图 2-7 从业人员岗位分布

8. 参与调查的网络从业人员从业时间分布

统计参与调查的网络从业人员从业时间分布，在采集的网络从业人员的 26513 份调查问卷中，网络从业人员从业时间在 1-3 年占比 39.58%，4-10 年占比 44.48%，11-15 年占比 9.09%，16-30 年占比 6.82%。从业人员的从业时间大多在 10 年以内。其中 4-10

年区间占比最多为 44.48%，1-3 年区间占 39.58%，两者合计 84.06%。

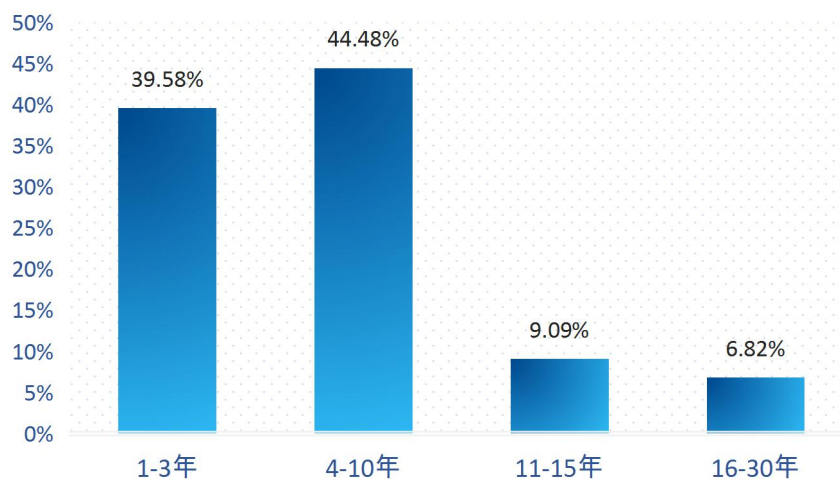


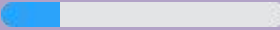
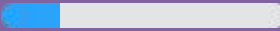
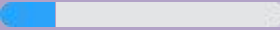
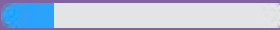
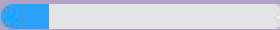
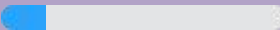
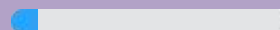
图 2-8 网络从业人员从业时间分布

9. 参与调查的网络从业人员所在单位网络服务范围分布

统计参与调查的网络从业人员所在单位网络服务范围分布，在采集的网络从业人员的 26513 份调查问卷中，以基础行业服务为主的占比 20.99%，以网络音视频为主的占比 20.65%，以网络新闻为主的占比 19.71%，以数据中心服务为主的占比 18.35%，以旅行订购为主的占比 16.41%，以云平台服务为主的占比 16.07%，以网络游戏为主的占比 15.06%，以电子商务为主的占比 13.23%，以接入服务为主的占比 10.9%，以电子邮件为主的占比 10.5%，以软件下载为主的占比 9.82%，以金融服务为主的占比 9.68%，以即时通讯为主的占比 7.67%，以搜索引擎为主的占比 7.65%，以论坛微博客为主的占比 7.38%，以内容分发服务为主的占比 7.02%，以域名服务为主的占比 6.16%，以移动应

用商店为主的占比 5.33%。从业人员所在单位提供的服务覆盖面广，提供的网络服务最多的分别是基础行业服务、网络新闻、云平台服务、电子商务等。

表 2-1 参与调查的网络从业人员所在单位网络服务范围分布

选项	比例
基础行业服务	 20.99%
网络音视频	 20.65%
网络新闻	 19.71%
数据中心服务	 18.35%
其他	 17.38%
旅行订购	 16.41%
云平台服务	 16.07%
网络游戏	 15.06%
电子商务	 13.23%
接入服务	 10.9%
电子邮件	 10.5%
软件下载	 9.82%
金融服务	 9.68%
即时通讯	 7.67%
搜索引擎	 7.65%
论坛微博客	 7.38%

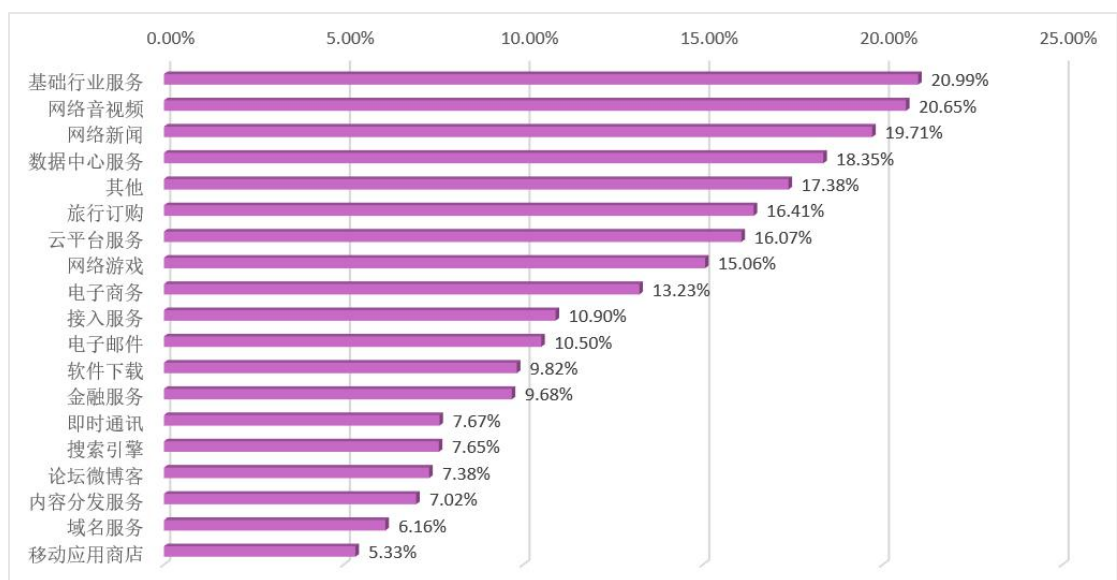
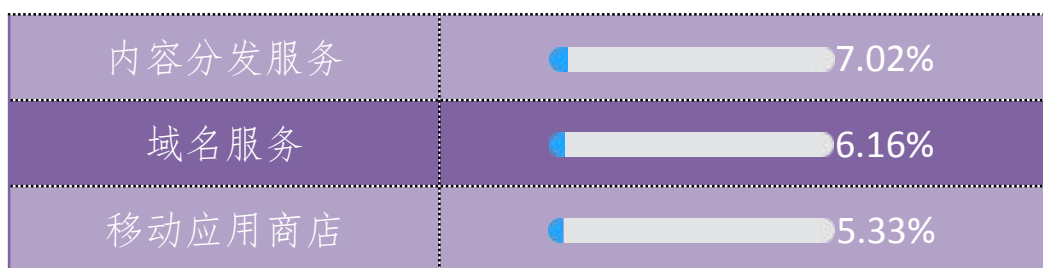


图 2-9 参与调查的网络从业人员所在单位网络服务范围分布

(二) 2019 年与 2018 年参与调查人员基本信息情况对比

1. 参与调查的网民性别分布均衡性有所提高

根据网民网络安全感满意度调查报告显示,从网民性别比例看,2018 年男性占比 77%,女性占比 23%,2019 年男性占比 67%,女性占比 33%。根据国家统计局网站数据统计,2017 年我国男性总人数 71137 万人,女性总人数 67871 万人,男性总人数与女性总人数的比例为 1.048。2018 年我国男性总人数 71351 万人,女性总人数 68187 万人,男性总人数与女性总人数的比例为 1.046。男性总人数和女性总人数均有所上升,但从增长率来看,2017

年到 2018 年男性总人数增长率为 0.30%，女性总人数增长率为 0.47%。国家男女比例逐渐平衡是本次调查样本性别比例平衡性有所提高的原因。

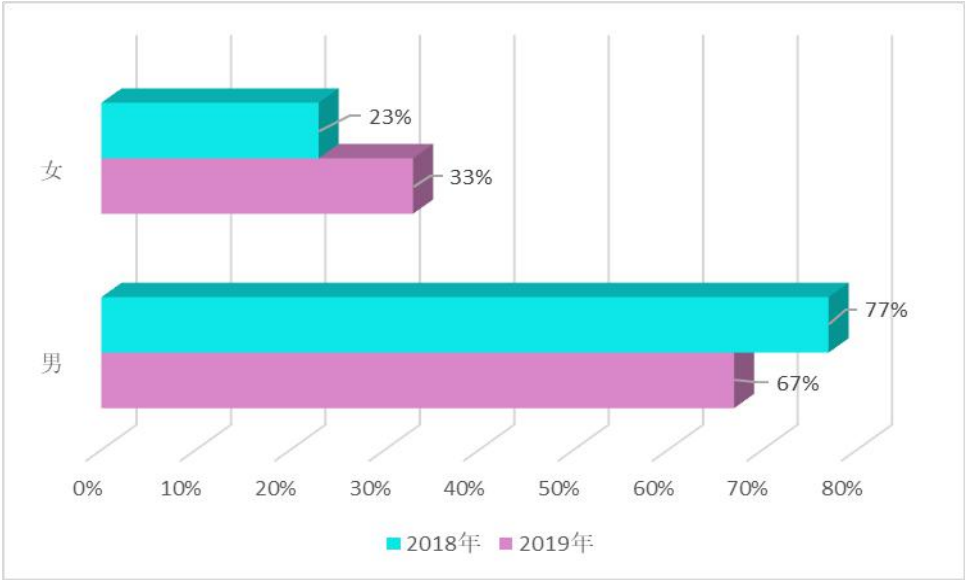


图 2-10 2018-2019 公众网民性别分布



图 2-11 2017-2018 我国男女总人数及增长率

从网络从业人员性别分布上，根据网络从业人员网络安全感满意度调查报告显示，2018 年男性占比 67%，女性占比 33%，2019 年男性占比 70%，女性占比 30%。一方面全国男性人口总数量高

于女性人口总数量，另一方面网络安全方面男性需求人数占比高于女性，导致出现 2019 年网络从业人员男性数量上升，女性数量下降。

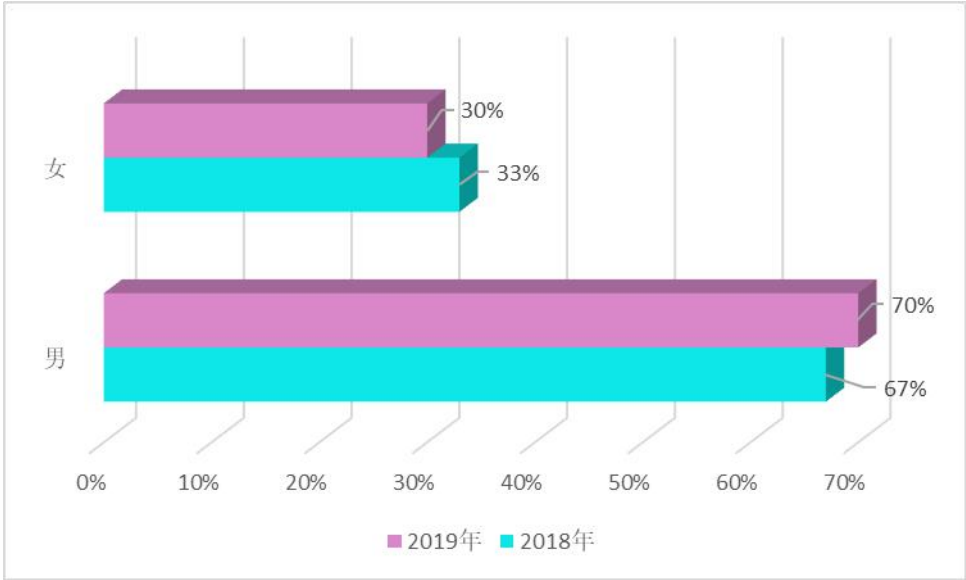


图 2-12 2018-2019 网络从业人员性别分布

2. 参与调查的网民年龄阶段分布老年人占比有所增加

根据网民网络安全感满意度调查报告显示，从年龄分段比例看，2018 年，12-18 岁网民占比 22.58%，19-24 岁网民占比 44.89%，25-30 岁网民占比 17.19%，31-45 岁网民占比 12.06%，46-60 岁网民占比 2.92%，60 岁以上网民占比 0.36%。2018-2019 年我国 12-18 岁以及 25-30 岁网民占比相差不大，19-24 岁网民占比明显下降，31 岁及以上年龄段网民数量有所增加。随着信息化时代的推动，智能手机、5G 技术的普及，以及人口老龄化趋势的发展，促进越来越多的中老年人向信息科技时代靠拢，而越来越多的年轻人更热衷于线下活动的沟通交流。

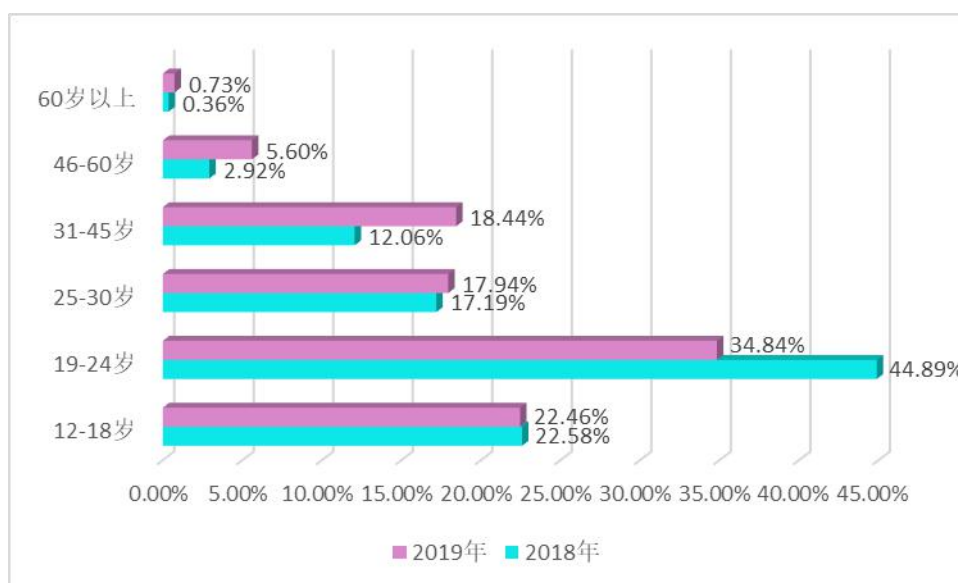


图 2-13 2018-2019 公众网民不同年龄阶段占比

从网络从业人员年龄比例分布上,根据网络从业人员网络安全感满意度调查报告显示,2018 年,12-18 岁网民占比 3.75%,19-24 岁网民占比 34.63%,25-30 岁网民占比 32.66%,31-45 岁网民占比 25.51%,46-60 岁网民占比 3.26%,60 岁以上网民占比 0.35%。在人口老龄化和科技飞速发展的趋势下,2018-2019 年我国网络从业人员网民数量在青少年和老年人阶段占比提高,而青年、中年占比减少。

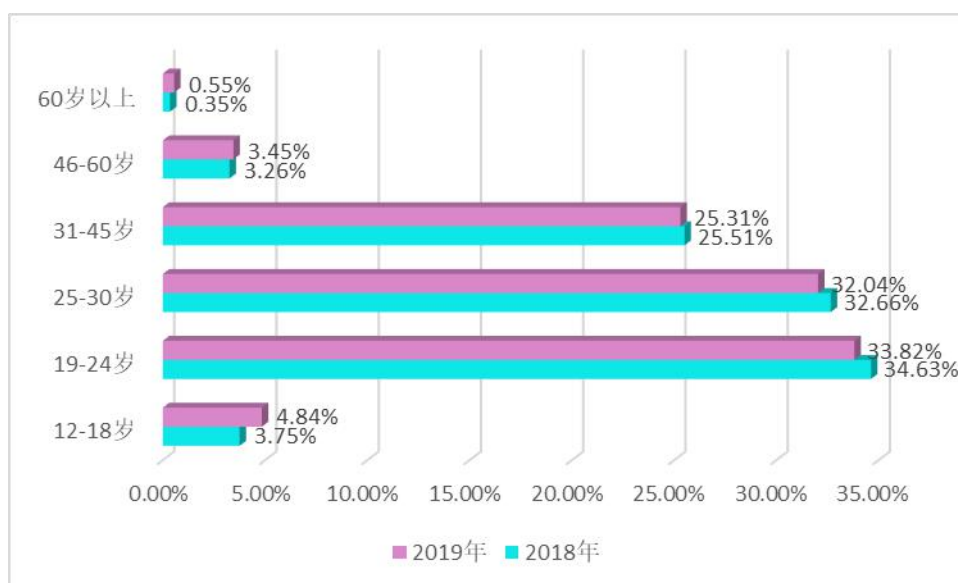


图 2-14 2018-2019 网络从业人员网民年龄分布

3. 参与调查的高学历网民人数有所扩张

根据网民网络安全感满意度调查报告显示,从学历分布比例看,2018年,初中及以下学历网民占比10.97%,高中学历网民占比18.72%,中专学历网民占比6.22%,大专学历网民占比20.08%,本科学历网民占比39.16%,硕士学历网民占比3.70%,博士学历网民占比1.34%。2019年相比于2018年初中及以下、高中、本科学历网民占比下降,中专、大专,硕士、博士学历网民占比提高。随着中国经济社会不断发展,近年来人口受教育程度越来越高,普通高等学校毕业人数越来越多,高学历网民占比相应增加。

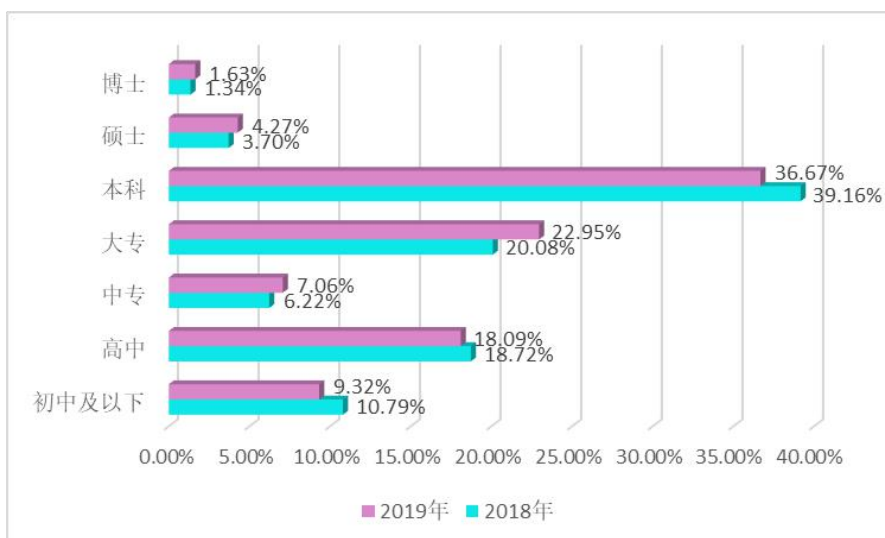


图 2-15 2018-2019 公众网民学历分布

从网络从业人员网民学历分布上,根据网络从业人员网络安全感满意度调查报告显示,2018 年,高中以下学历网民占比 4.33%,高中中专学历网民占比 17.75%,大专学历网民占比 25.75%,本科学历网民占比 45.05%,硕士学历网民占比 5.49%,博士学历网民占比 1.63%。同理,随着中国经济社会不断发展,近年来人口受教育程度越来越高,普通高等学校毕业人数越来越多,高学历网民占比相应增加。

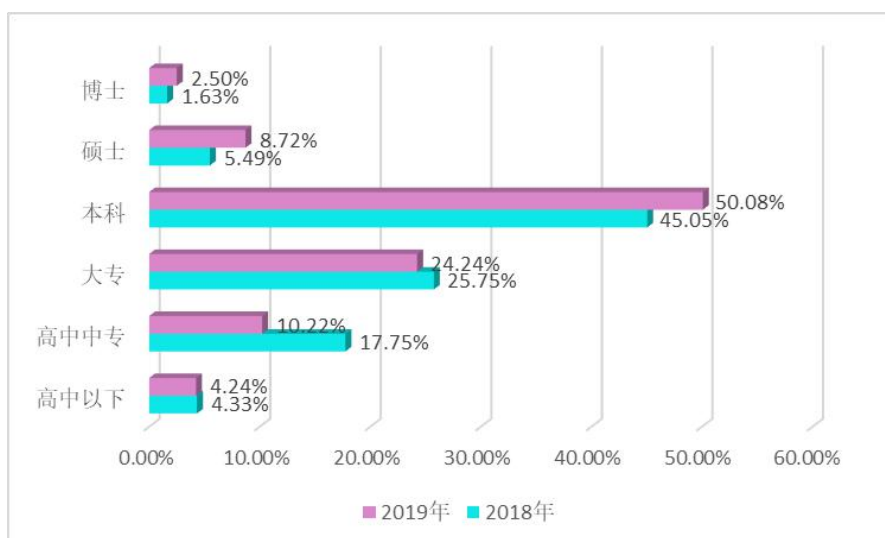


图 2-16 2018-2019 网络从业人员网民学历分布

三、我国网民网络安全感满意度整体情况分析

（一）2019 年过半网民认为网络总体是安全的

调查结果显示, 11.38%参与调查的网民对使用网络时的总体安全感觉是非常安全的, 39.87%参与调查的网民对使用网络时的总体安全感觉是安全的, 38.16%参与调查的网民对使用网络时的总体安全感觉是一般, 7.47%参与调查的网民对使用网络时的总体安全感觉是不安全的, 3.13%参与调查的网民对使用网络时的总体安全感觉是非常不安全的。其中感到安全的两者相加占比为 51.25%, 表明超过一半的网民对使用网络时的总体安全感觉是安全的。

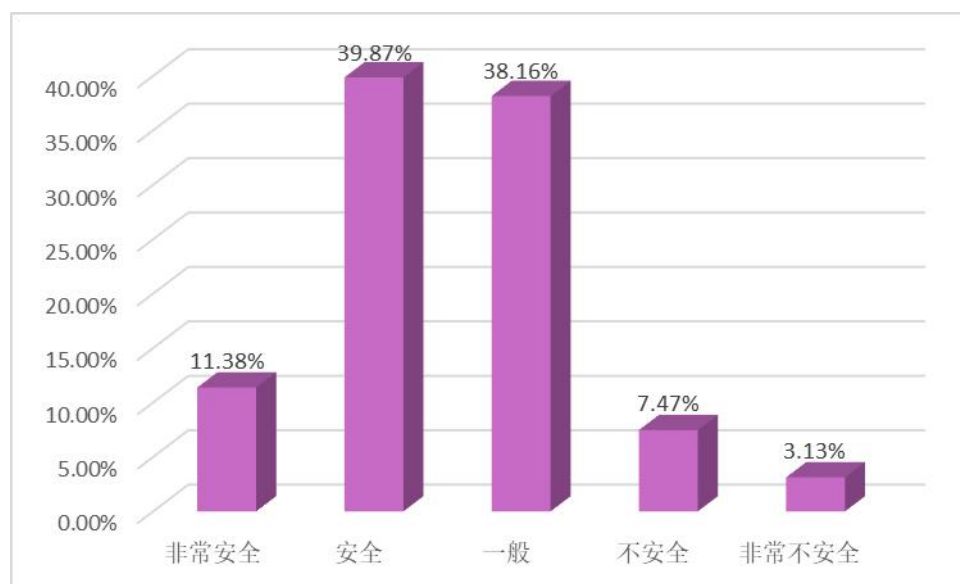


图 3-1 2019 年参与调查的网民对使用网络时的总体安全感觉

（二）2019 年我国网民网络安全感满意度有较大的提高

调查结果, 网民认为网络安全感与去年相比有较明显的提

升。其中 34.59% 的网民中认为网络安全感有提升，14.17% 网民认为有明显提升，两者相加达 48.76%，接近一半的网民认为网络安全感有提升。有 40.76% 的网民认为没有变化，10.48% 的网民认为网络安全感下降。较去年数据相比，认为网络安全感提升的民众比例显比去年增加了 16.29%，认为网络安全感下降的网民比例比去年下降了 2.82%。

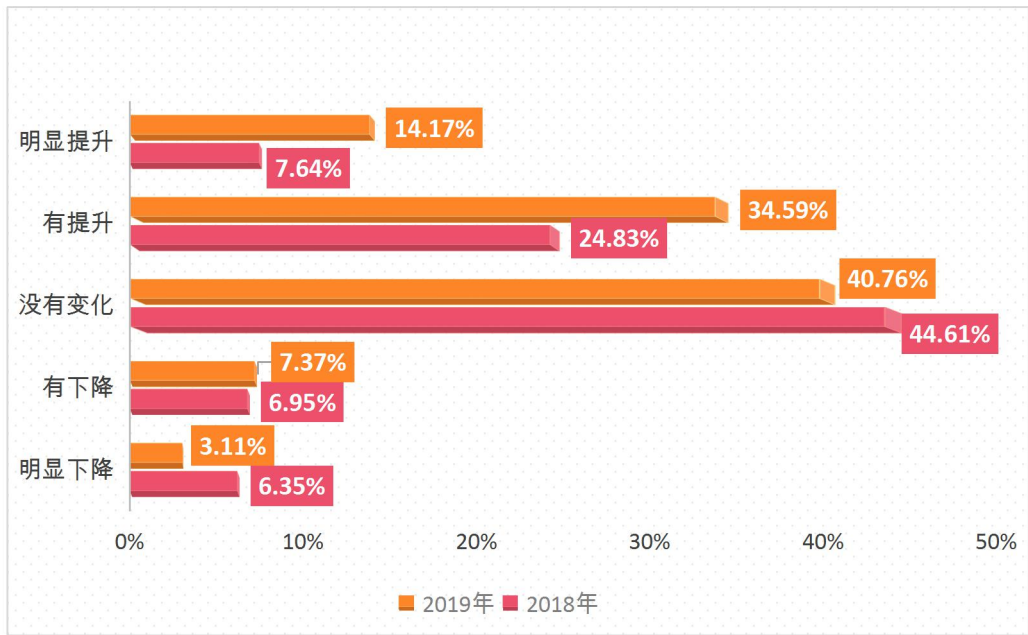


图 3-2 2018 和 2019 年网民的网络安全感变化情况

（三）从业人员对网络安全状况基本满意

图 3-3 是针对不同岗位的从业人员进行了网络安全状况态度的调查，总体上来看大多数从业人员认为状况良好或一般，认为当前网络状况堪忧的从业人员不足两成。不同岗位对网络安全的看法并不完全一致。网络行业协会、政府网络安全监督管理部门、和一般联网使用单位对网络安全的满意度超过了四成，而科

研机构、大学相关从业人员认为网络安全状况良好的网民只有26.04%。认为网络状况一般的从业人员基本都在五成左右。

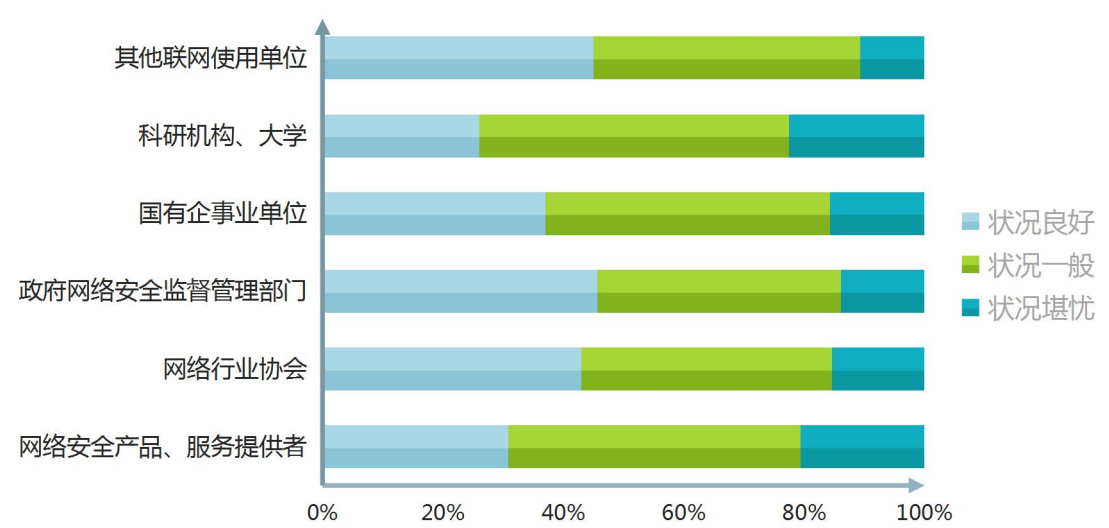


图 3-3 从业人员对网络安全感的态度

通过以上调查数据表明，当前我国各类网民对网络安全的总体状况给予了较高的评价，反映了近年来政府监管部门、行业协会、网络公司及社会各界对网络安全的重视和持续的投入取得了明显的成效，得到了广大网民的认可。这一成绩是在近年来我国网络高速发展、网络应用创新持续不断、网民数量大幅增长的情况下取得的，是政府、行业、企业和社会公众共同努力的结果，是网络共建、共享原则的具体体现。

四、数字政府安全服务调查分析

（一）政务各领域网上服务需要继续加强

总体上来看，大部分网民都使用过政府网上服务，没有使用过的网民只有 14.6%。目前政务网上服务已经覆盖银行、交通、教育、社保、医疗、旅游、就业、工商、税务、住房等多个领域。

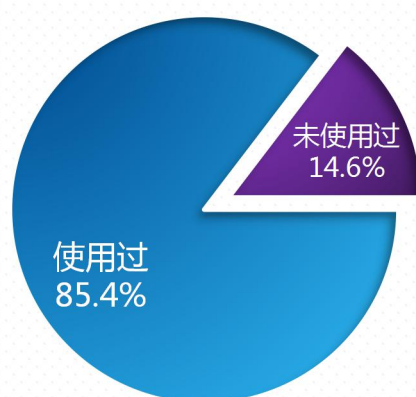


图 4-1 网民是否使用过政务网上服务分布

1. 在银行领域的政府网上服务使用率最高

根据调查结果，使用过银行服务的网友最多达到 59.58%。目前许多地区的银行网点可以受理证照申请，通过网络上传到审批局审批系统进行在线审核，最后在网点同时颁发营业执照、办学许可证等多个证照，充分利用了银行网点的分布特点，可以大大缩减注册登记一般审批事项的办理时效，让企业、个人可以在就近的银行办理各类证照。

其次是交通、教育、社保和医疗服务，分别是 50.3%、48.82%、

46.89%、44.89%，使用人数均接近五成。而在旅游、就业、工商、税务、住房等领域的使用过的人数明显减少，仅有两成左右。

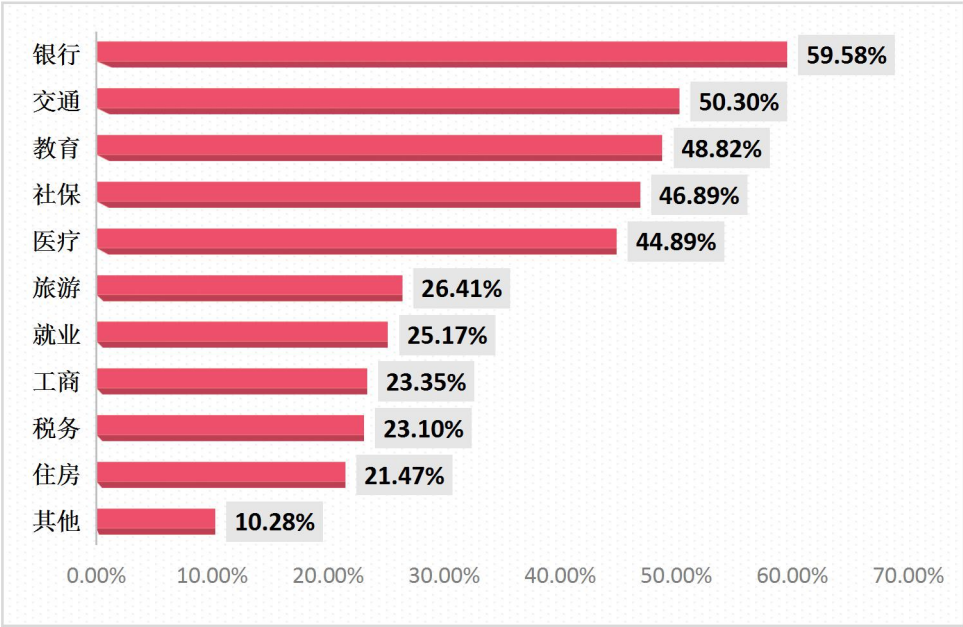


图 4-2 政府网上服务使用比例

2. 教育、医疗等政府网上服务仍需要加强

网民对政府网上服务需求强烈，有 51.35%的网友认为教育是最需要加强的政务服务。近五成网友认为医疗、交通、就业、社保网上服务仍需要加强。在教育方面，目前教育工作的透明度不高，需要通过推进教育服务公开、重点领域信息公开，包括积极做好义务教育招生信息公开，推进义务教育免费就近入学、入学流程、证件要求和办理方式公开等等。而医疗方面目前国内智慧医疗信息平台建设还不成熟，要继续解决看病“最后一公里”问题，大力支持“互联网+医疗健康”的发展。

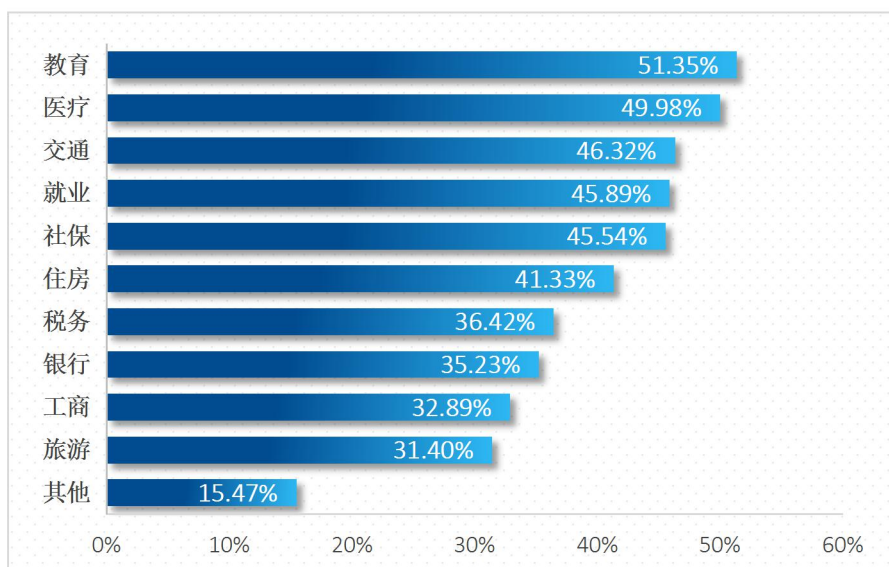


图 4-3 需要加强的政府网上服务

（二）政府网上服务的便捷性仍需提高

为实现线上线下深度融合、高效便捷政务服务新体系,以“一网通办”便利群众,我国政务网上服务一直聚焦破解政府“办事难、办事慢、办事繁”的问题,简化办事环节和手续,优化政务服务流程,提供渠道多样、简便易用的政务服务,让群众办事更方便。目前大部分网民认可政府网上服务是便利的,占 66%。

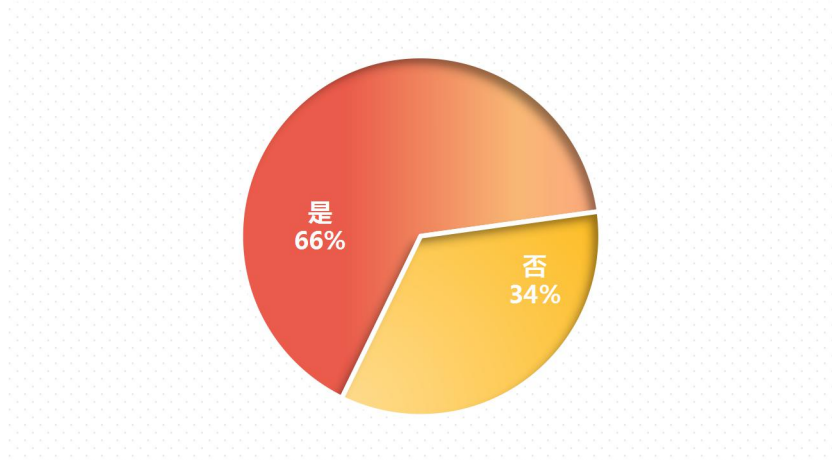


图 4-4 政府网上服务是否便捷

根据调查结果 4-5 所示，网民认为提高数字政府服务的便捷性最需要提高的是政务办理时效，占比高达 72.43%。其次是结果反馈、信息公开、资料提交和业务投诉服务，认为还需要加强网民均超过了五成，表明当前的政务服务仍有许多需要改善的地方。

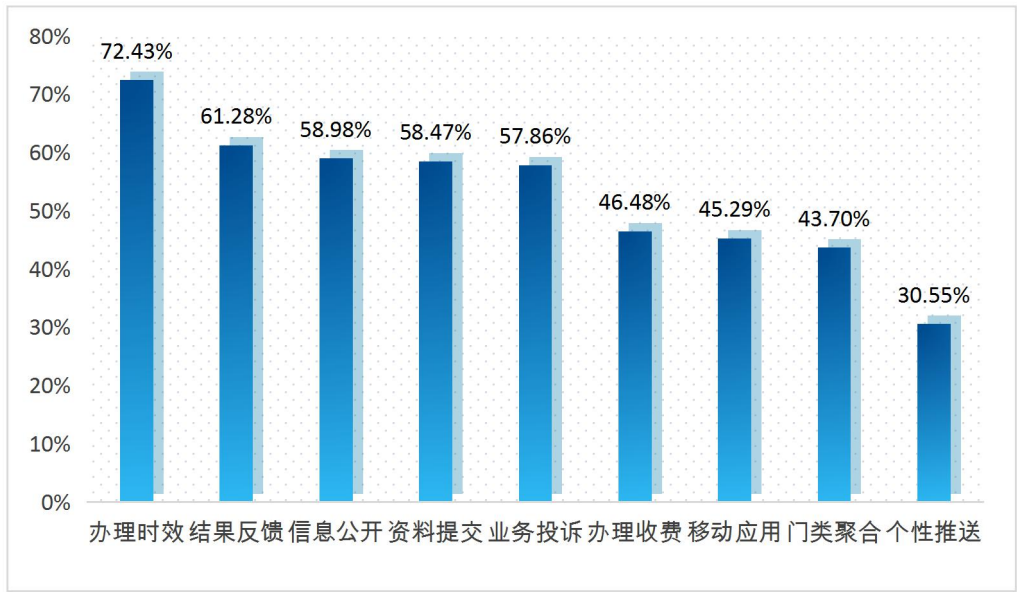


图 4-5 政府网上服务便捷性需要加强

（三）政府网上服务存在安全隐患

政务服务平台承载着亿万公民的身份信息、各企事业单位的数据资料，也是国家提供政务服务、稳定运行的重要保障，网络安全的重要性不言而喻。在当前严峻的网络安全形势下，政务网上服务也面临着巨大的威胁和挑战，如恶意破坏网络系统或数据文件、盗窃金融数据、机密文件以及其他敏感的数据信息等等。随着政务服务的不断“上网”以及新信息技术和新网上服务的应用，网络攻击方式也不断“升级”，威胁类型也呈现出新颖化、

复杂化的特征。

图 4-6 是网民对政府网上服务安全满意度的调查。目前，有 72.16% 的网民认为政府网上服务是安全的。

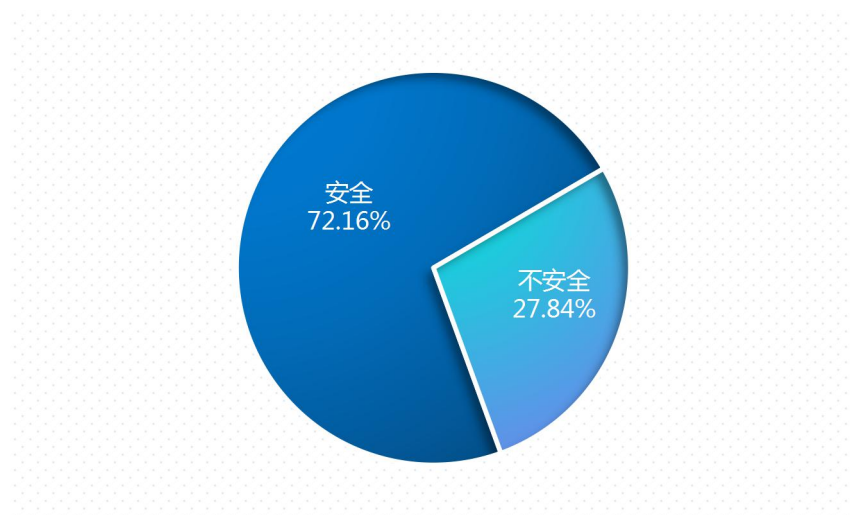


图 4-6 政府网上服务安全满意度调查

1. 个人隐私信息易泄露是政府网上服务的最大风险

政府网上服务安全风险调查如图 4-7，65.76% 网民最担忧的安全问题是个人信息泄露。由于政务系统中存在涉及公民各类隐私信息，很容易被不法分子为攫取经济价值，而医疗、教育、住房等信息的泄露跟是可能对人民的生命财产造成威胁。网络中也存在着大量假冒政府单位的钓鱼网站，利用短信、二维码、网页弹窗、搜索引擎、微信朋友圈等大肆传播，通过销售伪造认定证书、窃取个人信息、发布虚假消息牟利、假借中央部委名义监督实则敲诈勒索、一体化伪造网上政府诈骗企业财产等多种手段实施诈骗，成为民众最大的安全隐患。

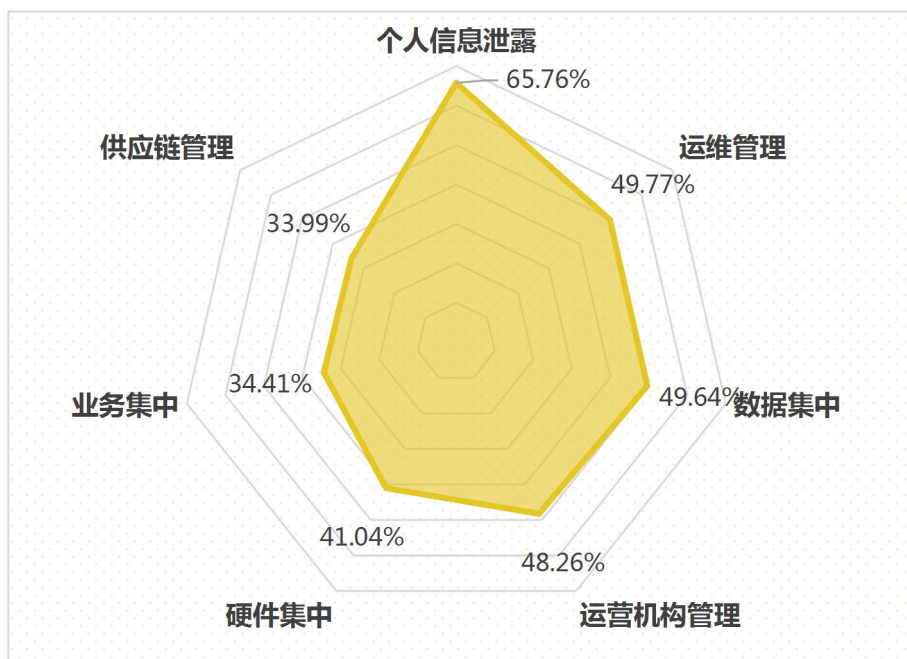


图 4-7 政府网上服务存在风险调查

接近 50%的网民认为政府运维管理、数据集中存放也是政府网上服务的重要安全隐患。在政府运维管理中，有可能出现网络故障和数据中心机房故障，并且人为操作也存在失误的可能。在当前政府采用云计算服务的过程中，政务云平台的运维管理也给数字政府的发展带来了新挑战。政务数据集中存放虽然可以充分发挥数据价值，但也承担更大的数据管理责任，面临更大的数据安全风险，如何通过制度、体系、技术创新解决安全问题将是所有地区和部委网信部门面临的共同挑战。

2. 教育、医疗信息是最易泄露的的服务领域

目前政府网上服务在各个行业均存在信息泄露的情况，如图 4-8 所示。尤其是医疗和教育行业信息泄露情况最严重，分别是 51.7%和 50.5%。其次是就业、交通和住房领域，分别是 45.33%、

44.31%、44.18%，相对来说旅游、社保、银行、工商服务信息泄露的情况更少。

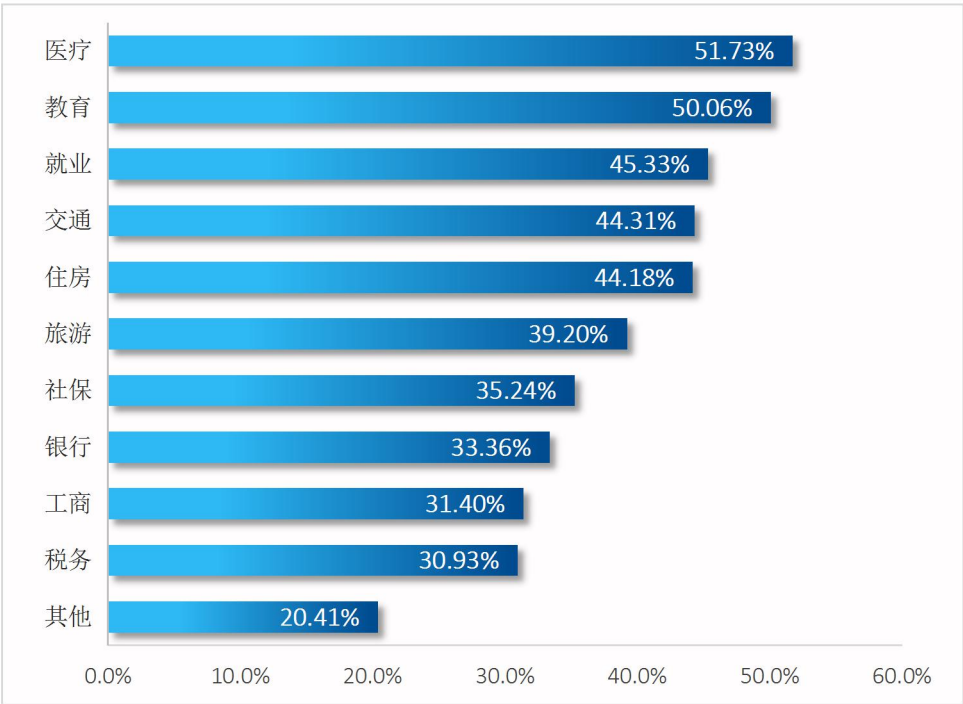


图 4-8 政府网上服务存在的风险

医疗信息除了常见的姓名、年纪、身份证、手机号等常见信息外，还包含患者的诊断、病情、就医经历等材料。医疗数据是国家重要基础性的战略资源，事关人民群众的生命安全、个人隐私。因此医疗信息的泄露，不但给个人造成很大的困扰，同时也会造成经济损失，如像基因这样特别的数据流失的话，也可能对国家安全造成威胁。

教育信息包含了老师学生家长注册登录个人信息、教学资源信息、国家教学资助信息等，如果个人信息落到不法分子手中，骚扰电话将严重影响教师、学生和家长的正常生活，更严重还有可能出现诈骗等情况，危及被诈骗人生命安全。近年来学生因个人信息泄露，被不法分子骗走学费的案例屡屡发生，因此教育行业数

据泄露问题也成为威胁社会安定团结且急需解决的问题。

3. 从业人员对个人信息保护满意度较低

面向政府网络安全监管部门、网络行业协会、国有企业事业单位，其他联网使用单位从业人员对当前网络个人隐私保护情况展开调查，如下图 4-9 所示。政府网络安全监管部门、网络行业协会的相关从业人员对个人隐私保护服务的满意度整体高于国有企业事业单位和其他联网使用单位从业人员。这可能是因为政府网络安全监管部门和网络行业协会的从业人员对于现有的政府保障个人隐私手段更加了解，满意度更高。而其他行业的人员对国家的法律和保障手段了解少，对政府监管更加不信任。

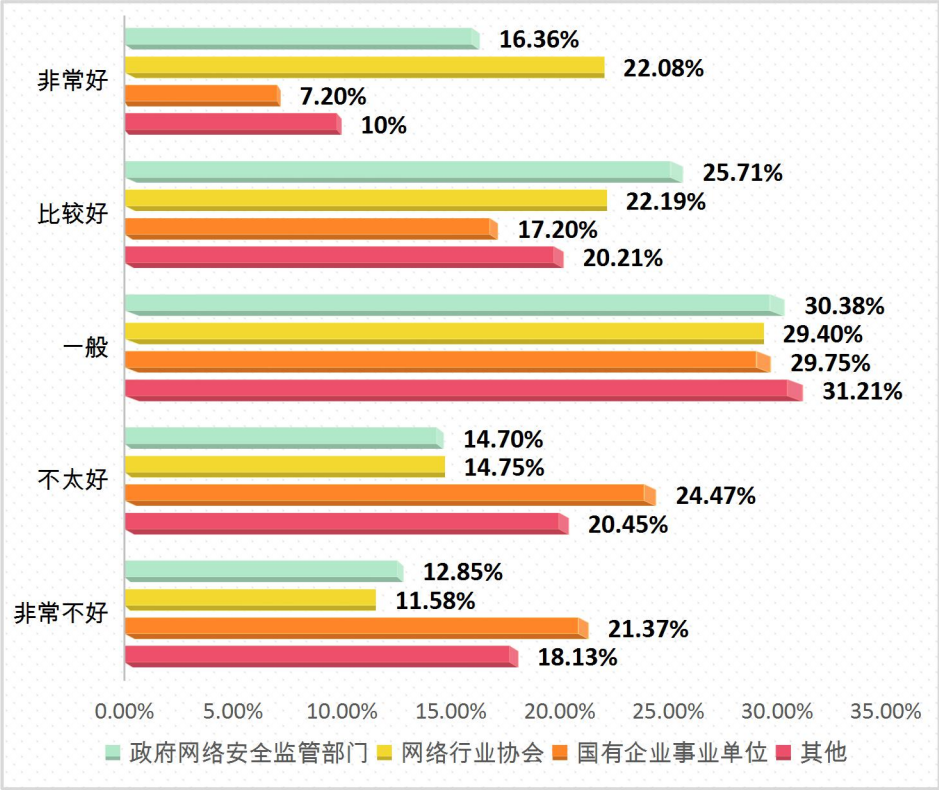


图 4-9 我国个人信息保护的状况的调查情况

4. 网民对国家个人信息保护的立法的态度

在调查中，认为现在有标准弥补了立法空白的网民仅有17.2%，大多数网民都认为我国个人信息保护在立法方面仍需完善。31.26%的网民认为需要出台个人信息的专门立法，30.81%的网民认为要继续出台个人信息保护的强制标准，20.73%的人认为需要将现有的标准转化为强制规定。

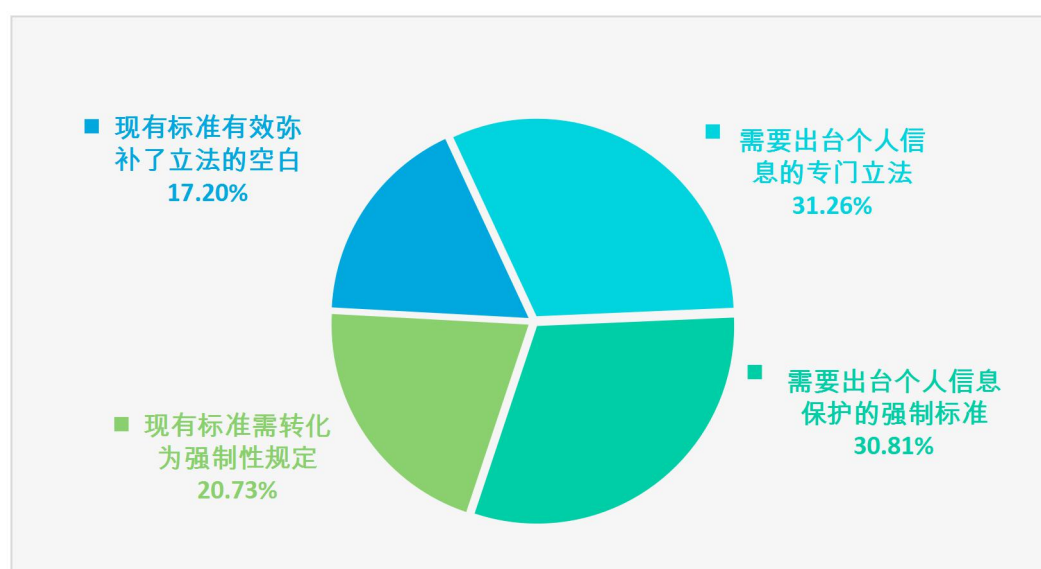


图 4-10 对国家个人信息保护的立法的看法

（四）政府网络安全监管有待完善

随着互联网的快速普及，如今我国网民规模已经突破 6 亿，手机网民规模突破 5 亿，网络使用人群数量不断增长。网络不仅影响千家万户，更是对国民经济的稳步发展有着重要作用。近年来网络安全事假时有发生，政府也非常重视网络安全监管，不断完善法律法规，提高网络安全监管力度。

1. 网民对政府网络安全监管的态度

随着全国政服务服平台一体化建设的推进，政府的网络安全服务也需要与时俱进。针对目前政府提供的网络安全服务，超过56%的网友认为，知识普及、信息查询是网民最满意的政府监管手段。在服务过程中的风险提示、免费工具使用、投诉举报等手段的满意度分别占 42.6%、38.1%、37.53%。政府通过广泛的普及网络安全相关知识，并且对当前社会发生的网络安全风险进行提醒，提供网民信息查询的平台，能有效提升人民安全意识，减少安全问题的发生。

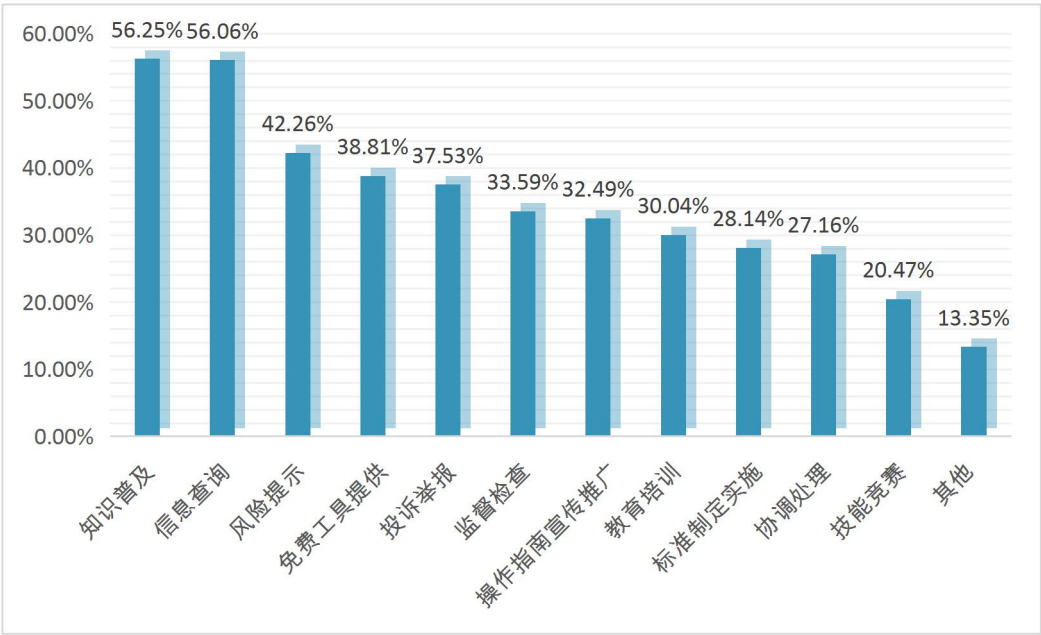


图 4-11 政府在网络安全方面服务的满意度

针对政府部门应当如何加强网络安全建设，77.96%的网友认为应该要完善法律法规，严厉打击违法犯罪。认为需要加强监管及网络平台监管、广泛宣传普及网络安全知识的网民占到了六成以上。

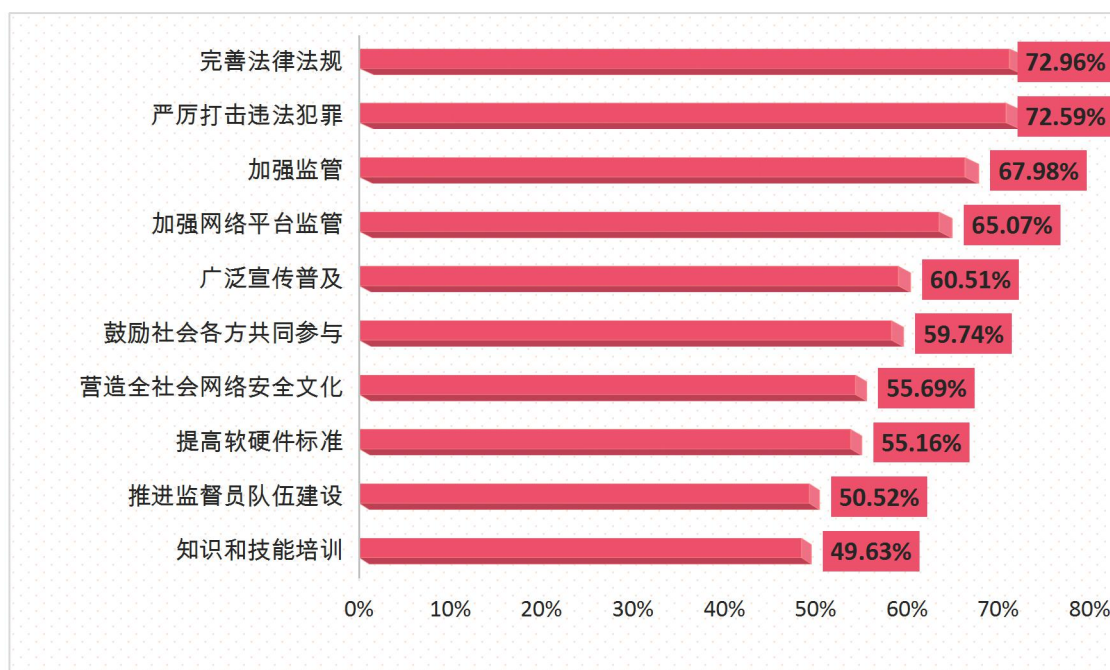


图 4-12 网民对政府部门加强网络安全建设的建议

2. 从业人员对政府网络安全监管的态度

面向政府网络安全监管部门、网络行业协会、国有企业事业单位和其他他联网使用单位从业人员对当前政府的网络安全监管工作的不足进行了调查。从业人员认为最大的不足是政府缺少网络安全专业技术人才，占比均超过五成，其中政府网络安全监督管理部门的从业人员多达 75%。其次是网络安全工作经费不足，网络安全技术与管理水平低、信息系统存在安全风险、领导重视不足等都是重要原因。

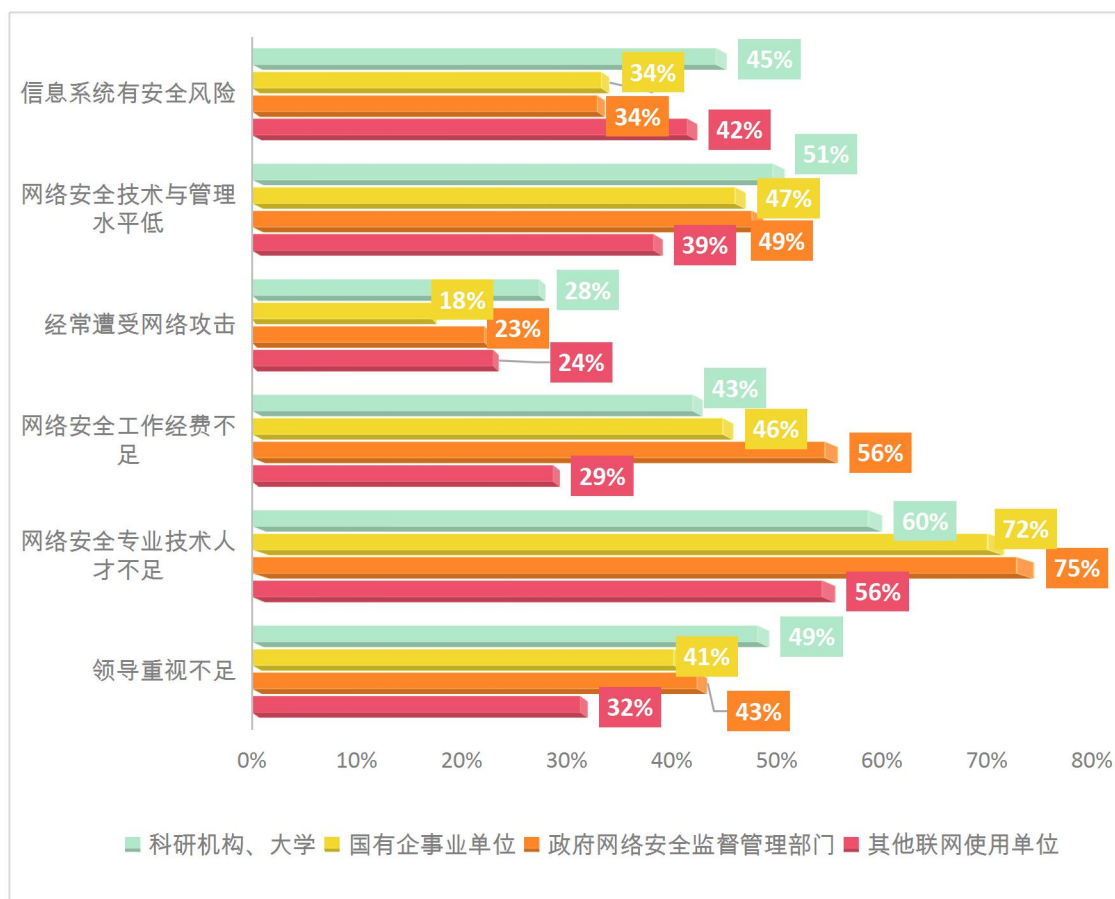


图 4-13 从业人员认为政府网络安全监管的不足

面向网络服务提供和网络安全相关工作、政府网络安全监督管理部门、网络行业协会、国有企业事业单位、研究机构和大学、其他他联网使用单位的从业人员进行了对当前网络安全立法工作的调查。大多数从业人员都认为加强公民个人信息保护的立法是当前最重要，国有企业事业单位、其他联网使用单位从业人员的占比分别是 76.67%和 76.82%。其次是网络平台责任、数据安全保护、网络安全等级保护、网络违法犯罪防治。其中网络服务提供者网络安全相关工作认为最重要的是加强网络平台责任，占比为 61.11%。政府网络安全监督管理部门相较于其他岗位的从业人员更加重视网络违法犯罪防治、关键信息基础设施保护和数据

权利的民事立法等工作。

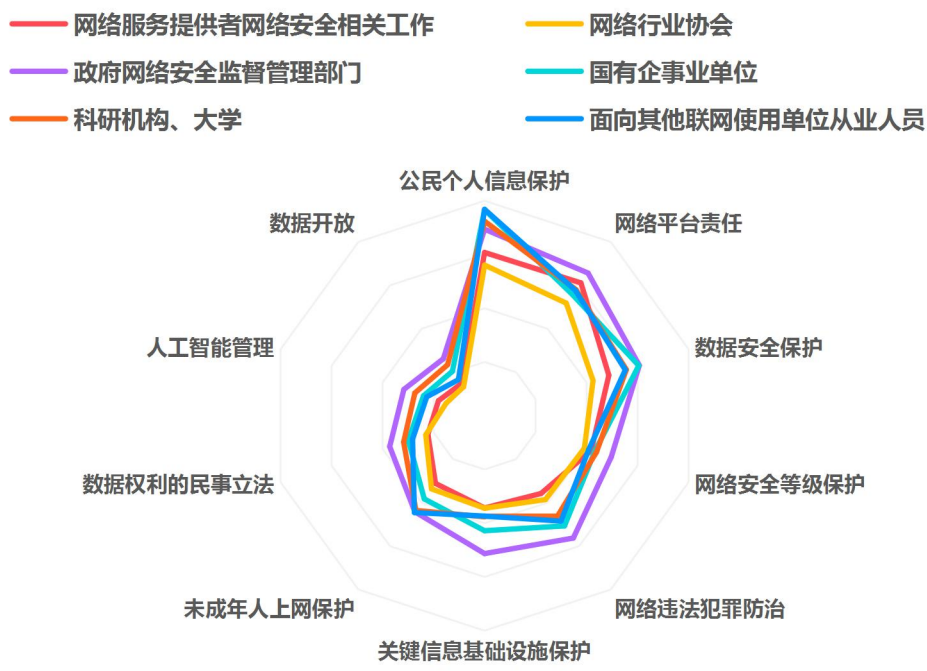


图 4-14 从业人员加强的网络安全立法的意见

五、对我国数字政府安全服务的建议

（一）强化顶层设计，完善政务服务的制度体系

数字政府作为新技术条件下政府组织和运作模式的新形态，亟需克服传统体制机制的羁绊，加速与各个行业的深度融合，提供更广泛、更便捷的服务。通过强化顶层设计，探索与“数字政府”相适应的政务信息化建设管理新体制。

一是政府部门要形成职责明确的政府信息化工作格局，确保组织体系运转顺畅，沟通协调无缝耦合；要积极推动政府数据资源共享开放，探索贯穿数据全生命周期的数据治理新路径。

二是完善政务服务的制度规范，建立各行业配套的制度体系。严格落实《网络安全法》等法律法规，研究制定政务数据的确权开放、产权保护等方面的法律法规，推动政府数据资源共享开放，强化网络安全和建设工作。

三是加速推进与群众生活更加密切的政务服务，如医疗、健康、交通等，稳步推进“一网通办”，实现审批更简、监管更强、服务更优，推进“互联网+政务服务”工作落实。

（二）进一步完善个人信息安全的保护手段

完善个人隐私安全主要是从技术和管理两个方面加强平台的建设和管理。在技术上，邀请信息安全方面的专家和相关专业力量，制定了个人信息保护的安全技术方案；采用安全网关、防火墙、入侵防护、堡垒机等各种安全加固措施抵御外部的攻击，

保障平台信息安全；建设安全风险发现预警功能，出现安全漏洞时及时预警，并能阻断数据外泄；利用国产加密算法、身份鉴权等相关技术，保障接口安全及数据的加密传输和存储安全。

在管理层面，一是制定统一的安全管理规定，明确各级机关负责的网上办理事项网站相关的主体责任，建立了上下联动相关机制，确保一体化政务平台整体信息安全。二是定期对平台进行攻防演练，发现漏洞及时修补。三是建立安全事故应急预案，一旦发生安全事故后，确保能够快速响应，并及时修复。通过将技术防护和安全管理的有效结合，着力构建全方位、多层次的纵深安全防护体系，确保“互联网+政务服务”平台的系统安全和数据安全。

（三）优化业务流程提高政府网上服务便利性

深化“放管服”改革，打造高效便民服务型政府，大力推进办事流程简化优化和服务方式创新。最大限度精简办事程序，减少办事环节，缩短办理时限，改进服务质量。加快政务大厅功能升级，推动公共服务事项全部进驻，为群众提供项目齐全、标准统一、便捷高效的公共服务。建立健全首问负责、一次性告知、并联办理、限时办结等制度，积极推行一站式办理、上门办理、预约办理、自助办理、同城通办、委托代办等服务，消除“中梗阻”，打通群众办事“最后一公里”。加强政府服务能力建设和作风建设，要从群众利益出发，设身处地为群众着想，建立健全

文明服务规则，提升运用新技术新方法为民服务的能力。加大效能评估和监督考核力度，探索运用网上监督系统，确保服务过程可考核、有追踪、受监督，办事群众可以现场或在线评价。

打造高效便民的政府政务是时代所需，更是顺应群众期待和需求的创新之举。不仅能有效提升办事部门的公众形象，更加能更好地服务群众，深化改革。在“互联网”时代背景下，我们还需探索打造更多老百姓喜爱、满意的便民服务举措，进一步便利和提高群众的受益面。

（四）加强政府网络安全监管，营造社会良好网络安全氛围

习近平总书记在网络安全和信息化工作座谈会上所指出，网络安全为人民，网络安全靠人民。要坚持网络安全和网络发展同步推进，把保障人民群众的安全和利益作为网络安全工作的根本出发点，建立良好的网络安全机制。做好网络安全执法检查工作，定期开展网络安全风险的评估工作，全面排查风险，堵塞安全漏洞，切实加强网络安全监测预警和应急处置能力，坚决防止发生重大网络安全事件事故。

维护网络安全是全社会的共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。进一步营造网络安全宣传全域化氛围，要提升居民网络安全意识，每一个网民都应当强化共同参与、积极行动的主人主体主角意识，才能汇聚维护网络安全的强大合力，构筑起网络安全的坚固长城。各政府单

位要以高度的责任感和使命感，不断总结经验，完善机制，提高民众的网络安全意识，提高政府网络安全防护能力和监管能力，让数字政府服务更好地造福人民。