NEWSLETTER 数据合规

2020 第一期 /总第十四期

数据合规时事速递

北京市环球律师事务所

2020 年 1 月 7 日

目录

前 言

随着《网络安全法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。帮助客户迎接数据时代的机遇与挑战。

环球律师事务所
GLOBAL LAW OFFICE

团队介绍：

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业境内外数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律与咨询服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告合规领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。

孟洁
合伙人律师
直线：86-10-6584-6768
总机：86-10-6584-6688
邮箱：
mengjie@glo.com.cn

一、新规速递

1. 四部门联合发布《App 违法违规收集使用个人信息行为认定方法》正式稿

隐私规则模糊不清、收集甚至贩卖个人信息……部分 App 违法违规收集使用用户个人信息的行为屡遭诟病，但具体判断的标准难以界定。12 月 30 日，国家网信办等四部门联合发布《App 违法违规收集使用个人信息行为认定方法》(下称《方法》)，为 App 运营者自查自纠和网民社会监督提供指引。“如进入 App 主界面后，需多于 4 次点击等操作才能访问到，则可被认定为‘未公开收集使用规则’”等具体细则纳入《方法》。

明确 31 种行为属违法违规

12 月 30 日，App 个人信息保护工作研讨会也在京举办。App 专项治理工作组成员何延哲介绍，工作组建立了微信公众号“App 个人信息举报”，截至目前，收到网民举报信息 1.23 万条，涉及 2300 余款 App，工作组选取了其中用户量大，与民众生活相关的 App 进行了评估，委托 14 家测评机构对 1000 余款 App 进行了技术测评，督促问题严重的近 300 款 App 进行整改，整改问题达 800 余个。

《方法》共明确了 App 违法违规收集使用个人信息的 31 种行为。其中，收集使用规则、明示收集个人信息的目的等都是认定的重点。

具体来看，“未公开收集使用规则”包括以下四种行为，如在 App 中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；在 App 首次运行时未通过弹窗等明显方式提示；或隐私政策等收集使用规则难以访问，如进入 App 主界面后，需多于 4 次点击等操作才能访问到；隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

“未经用户同意收集使用个人信息”也明确了 9 种行为，如征得用户同意前就开始收集个人信息；或是用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用。默认同意、私下更改设置、实际收集与所述不符、欺诈诱骗用户同意收集个人信息等行为也被列入黑名单。

此外，“必要原则”的具体内涵也得到了明确。“违反必要原则，收集与其提供的服务无关的个人信息”的行为包括收集类型与现有业务无关；频次超过实际需要；因用户不同意收集非必要内容而拒绝提供业务功能；用户因不同意新增功能所要收集的个人信息，致使原功能无法使用；以及仅以改善服务质量、提升用户体验、定向推送信息等为由，强制要求用户同意收集个人信息。

2019 年已查处 683 款 App

2019 年以来，多轮针对 App 违法违规收集个人信息的整治行动展开。公安部组织开展“净网 2019”专项行动，截至 12 月已依法查处违法违规采集个人信息的 App 共 683 款。

如 11 月以来，公安部加大打击整治侵犯公民个人信息违法犯罪力度，组织开展 App 违法违规采集个人信息集中整治，深入推进 App 违法违规采集使用个人信息专项整治行动。此次集中整治，重点针对无隐私协议、收集使用个人信息范围描述不清、超范围采集个人信息和非必要采集个人信息等情形，下架整改 100 款违法违规 App，责令限期整改 27 款，处以警告处罚 63 款，处以罚款处罚 10 款，另有 2 款被立为刑事案件开展侦查，相关案件正在侦查中。

在百款下架的 App 中，不乏微店、房天下、晋江小说阅读、某海淘等常用应用，天津银行、天津农商银行、光大银行等金融类应用，中华会计网校、小学语文一年级上等多款学习类应用也位居其中。北京商报记者通过应用商城搜索发现，上述几款 App 均已重新上架，但未能得知具体整改内容。

对此，《方法》对“公布投诉、举报方式等信息”也做出了具体要求。未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理的，均可被视为违法违规。

尚待“国标”出台联合发力

具体违法违规行为虽已进一步细化，专项行动也频频发力，但从实际来说，为勾选隐私条款而无法使用 App 的情况也颇为常见。“必要原则”的内涵明确后，“有关信息”和“无关信息”的边界也困扰着用户。

2019 年 5 月，App 专项治理工作组对下载量大的 100 款 App 申请权限以及强

制开启的权限进行过分析统计，包括对常见应用具体收集个人信息的权限，让公众直观了解常用 App 申请收集使用个人信息权限情况。

此外，2019 年 8 月开始征求个人意见的《信息安全技术 移动互联网应用(App)收集个人信息基本规范(草案)》中，也明确规定了 21 种常用 App 类型可收集的最少信息，如明确可收集的最少信息中包含个人身份信息的 App 类型只有网络约车、网络支付、交通票务等；而输入法、安全管理、浏览器类的 App，所能收集的用户信息仅有网络日志。

APP 治理工作组也于 10 月公布了优化更新后的国家标准 GB/T35273《信息安全技术个人信息安全规范》，对目前 APP 强制索权、注销难等问题给出了明确的意见。而彻底规范 APP 收集个人信息，为个人隐私提供更全面的保障，有待多份文件联合发力。[1]

《App 违法违规收集使用个人信息行为认定方法》全文参见：

http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm

2. 中国人民银行发布《金融消费者权益保护实施办法（征求意见稿）》

为进一步规范金融机构经营行为，切实保护金融消费者合法权益，中国人民银行起草了《金融消费者权益保护实施办法（征求意见稿）》（以下简称《征求意见稿》），27 日起开始向社会公开征求意见。

《征求意见稿》包括 7 章 69 条，对金融机构行为规范、消费者金融信息保护、金融消费争议解决、监督与管理机制等作出明确规定。

大数据时代，金融机构可以利用消费者的金融信息精准推销金融产品或服务，但与此同时，消费者金融信息保护也亟待完善。

《征求意见稿》明确，金融机构收集、使用消费者金融信息，应当遵循合法、

[1] 北京商报。

正当、必要原则，经金融消费者明示同意。金融机构不得收集与业务无关的消费者金融信息，不得采取不正当方式收集信息，不得变相强制收集消费者金融信息。

《征求意见稿》强调要保护金融消费者的个人信息以及隐私，在目前的情况下非常有针对性和必要性。下一步，应该制定个人信息保护的相关法律法规，进一步加强金融消费者个人信息的保护。

金融消费发生争议时，《征求意见稿》明确，先向金融机构投诉。金融消费者应当依法通过正当途径客观、理性反映诉求，不扰乱正常的金融秩序和社会公共秩序。董希淼表示："《征求意见稿》还进一步明确了金融消费者投诉的渠道、纠纷的解决机制，即使碰到了一些问题，金融消费者也可以非常方便快捷地向央行以及金融监管部门进行投诉，投诉之后还有相应的投诉处理的机制。这样更加畅通了消费者投诉的渠道，能够更好地解决金融消费的纠纷。"

针对网络犯罪一定程度存在的再犯现象，《解释》规定，对拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动的罪犯可以依法宣告职业禁止和禁止令。对于实施《解释》规定的犯罪被判处刑罚的，可以根据犯罪情况和预防再犯罪的需要，依法宣告职业禁止；被判处管制、宣告缓刑的，可以根据犯罪情况，依法宣告禁止令。[2]

《金融消费者权益保护实施办法（征求意见稿）》全文参见：

http://www.moj.gov.cn/news/content/2019-12/27/zlk_3238869.html?from=timeline&isappinstalled=0

3. 网信办审议通过《网络信息内容生态治理规定》

2019 年 12 月 20 日，国家互联网信息办公室发布《网络信息内容生态治理规定》正式稿。

规定出台的背景

出台规定主要基于两个方面的考虑。一是建立健全网络综合治理体系的需要。

[2] 央广网。

党的十九届四中全会决定提出，建立健全网络综合治理体系，加强和创新互联网内容建设，落实互联网企业信息管理主体责任，全面提高网络治理能力，营造清朗的网络空间。加强网络生态治理，培育积极健康、向上向善的网络文化，有利于建立健全网络综合治理体系。

二是维护广大网民切身利益的需要。网络空间天朗气清、生态良好，符合人民利益。网络空间乌烟瘴气、生态恶化，不符合人民利益。网络信息内容生态治理需要政府、企业、社会、网民等多方主体参与，共同构建良好的网络生态。制定实施规定，有利于进一步明确治理任务，动员全社会共同参与网络信息内容生态治理，营造良好网络生态。

规定明确的网络信息内容生产者要求

规定明确了正能量信息、违法信息和不良信息的具体范围。鼓励网络信息内容生产者制作、复制、发布含有正能量内容的信息。明确网络信息内容生产者应当遵守法律法规，遵循公序良俗，不得损害国家利益、公共利益和他人合法权益，不得制作、复制、发布违法信息；应当采取措施，防范和抵制制作、复制、发布不良信息。

为了使网络信息内容服务平台更好履行信息内容管理主体责任，规定提出具体要求

规定明确，网络信息内容服务平台应当履行信息内容管理主体责任，建立网络信息内容生态治理机制。明确了平台运行环节管理要求，包括建立健全算法推荐的人工干预和用户自主选择机制、广告管理制度、平台公约和用户协议制度、举报制度、年度报告制度等。明确了平台的信息安全管理义务，包括不得传播违法信息，应当防范和抵制传播不良信息，鼓励在重点环节传播正能量信息，不得在重点环节呈现不良信息等。

规定对网络信息内容服务使用者作出要求

规定明确，网络信息内容服务使用者发布信息和参与网络活动时应当文明互动，理性表达，不得发布违法信息，防范和抵制不良信息。鼓励通过投诉、举报等方式对网上违法和不良信息进行监督。明确网络群组、论坛社区版块的建立者和管理者应当履行管理责任，依法依约规范群组、版块内信息发布等行为。明确网络信息内容服务使用者和生产者、平台不得开展网络暴力、人肉搜索、深度伪造、流量造假、操纵账号等违法活动。

对违反规定要求的网络信息内容生产者、网络信息内容服务平台、网络信息内容服务使用者，明确法律责任

规定明确了网络信息内容生产者、网络信息内容服务平台、网络信息内容服务使用者的法律责任，同时完善了民事、行政和刑事法律责任相衔接的体系化规定。违反本规定，给他人造成损害的，依法承担民事责任；构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由有关主管部门依照有关法律、行政法规的规定予以处罚。[3]

《网络信息内容生态治理规定》全文参见：

http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm

4. 民法典(草案)提请全国人大常委会会议审议，个人信息和隐私保护专章规定

2019 年 12 月 23 日至 28 日,第十三届全国人大常委会第十五次会议在北京举行,备受关注的民法典(草案)首次整体亮相,提请审议。

公民个人信息保护纳入公益诉讼

近日,江西省吉安县民政局在公示时,详细公布了公民的完整身份证号、家庭住址、银行账号、联系电话等隐私信息,引发公众关注。当前,个人信息泄露、过度搜集个人信息的情况屡见报端。回应公众关切,民法典(草案)强化了对隐私权和个人信息的保护,部分与会人员也进一步提出了修改意见。

为了规范网络经营者的行为,全国人大常委会委员李飞跃建议人格权编第一千零三十五条增加一款作为第三款,内容为:“除法律、行政法规另有规定外,向不特定公众提供普遍信息、接入、浏览、访问、营销、推广等网络服务的经营者,不得收集与其提供服务无关的个人信息,不得以使用人拒绝提供相关信息而限制或者拒绝其享受普遍服务。”

[3] 新华社。

隐私权被侵犯,当事人如何求偿?全国人大常委会副委员长曹建明建议对第一千零三十八条进一步完善,增加一款,即“信息收集者、控制者有下列行为,损害社会公共利益的,法律规定的机关和组织可以依据《中华人民共和国民事诉讼法》等法律规定,向人民法院提起诉讼:(一)违反法律规定获取公民个人信息;(二)泄露、篡改其收集、存储的个人信息;(三)未经被收集者同意,非法将个人信息提供给他人;(四)未采取合理措施,致使公民个人信息遗失。”

曹建明副委员长还提到,由于受害人人多面广且分散,维权成本高,违法成本低,违法势头长期得不到有效遏制。实践中,一些地方消费者协会、检察机关以公益诉讼方式对公民个人信息安全的保护进行了有益的探索和实践,得到了好评,建议在民法典中增加相关条文,加强对公民个人信息的司法保护力度。[4]

5. 法工委:2020 年将制定《个人信息保护法》和《数据安全法》

12 月 20 日,全国人大常委会法工委举行第三次记者会。全国人大常委会法工委发言人岳仲明表示,中国 2020 年将制定《个人信息保护法》、《数据安全法》等。

岳仲明介绍,按照《中华人民共和国立法法》的规定,全国人大常委会编制年度立法工作计划,围绕党和国家中心任务,回应人民群众关切,统筹安排立法工作,具体工作由法工委负责。立法工作计划已经在全国人大常委会第四十四次委员长会议原则通过,对 2020 年的立法工作作出预安排。

2020 年,全国人大常委会计划修改《个人信息保护法》、《数据安全法》、安全生产法等重要领域立法工作,同时将对需要立改废释和作出授权决定的,适时安排审议。

据了解,《个人信息保护法》在 2019 年 3 月已经纳入十三届全国人大常委会的立法规划,与之相关的《儿童个人信息网络保护规定》已经颁布,《数据安全管理办法》《个人信息出境安全评估办法》已经完成了公开征求意见。

我国立法要经过四个阶段:法律案的提出、法律案的审议、法律案的表决和法律的公布。立法规划属于第一阶段也就是法律案的提出阶段,后续还需要经过审议、

[4] 新浪新闻。

表决和公布。

立法规划包含三类项目，第一类项目为：条件比较成熟、任期内拟提请审议的法律草案；第二类项目为：需要抓紧工作、条件成熟时提请审议的法律草案；第三类项目为：立法条件尚不完全具备、需要继续研究论证的立法项目。

在 2019 年 3 月公布的立法规划中，《个人信息保护法》和《数据安全法》属于第一类项目，也就是说，在 2020 年《个人信息保护法》和《数据安全法》或将进入审议阶段并迅速出台。

据统计，目前已有 100 多个国家制订了个人信息保护方面的法律。欧盟《一般数据保护条例》已于 2018 年 5 月 25 日开始实施。美国马里兰州在 2008 年通过《个人资料保护法》，2019 年加利福利亚州通过《加利福利亚消费者隐私法案》。日本 2005 年制定《个人信息保护法》，并于 2015 年进行修订、2017 年 5 月开始实施。加拿大在 2019 年 10 月颁布了《个人信息保护与电子资料法》。

随着网络信息技术和数字经济的快速发展，因个人信息不当收集、滥用、泄露，导致公民权益受到侵害的事件时有发生。通过立法加强个人信息保护已成为保护公民隐私和生命财产安全、规范网络健康有序发展的必然要求。

2019 年工信部、公安部、网信办等部门不断行动，打击个人信息犯罪，加强个人信息保护。相信随着 2020 年《个人信息保护法》和《数据安全法》的制定，我国个人信息保护将进入全新阶段。[5]

6. 央行：2020 年将出台个人金融信息保护等系列监管规则

日前，人民银行金融科技委员会会议在北京召开。会议总结 2019 年金融科技工作，研究部署 2020 年重点工作。人民银行党委委员、副行长范一飞主持会议并讲话。

会议认为，2019 年人民银行认真贯彻落实党中央、国务院决策部署，坚持“守正创新、安全可控、普惠民生、开放共赢”原则，全面发力、多点突破，推动金融科技工作开创新局面。加强顶层设计与统筹指导，出台《金融科技（FinTech）发展

[5] 每日经济新闻。

规划（2019—2021 年）》。健全金融科技监管基本规则体系，着力打造包容审慎的金融科技创新监管工具。会同发展改革委、科技部等组织金融科技应用试点，引导金融机构运用科技手段赋能金融提质增效。将金融科技产品纳入国家统一推行的认证体系，以标准落地实施为手段，强化金融科技安全与质量管理。不断优化移动支付生态体系，进一步提升支付便民利企服务水平。积极推进数据治理，加快“数字央行”建设。

会议强调，2020 年要坚持发展与监管“两手抓”，持续推动金融科技行稳致远。一是跟踪发展规划实施，引导金融机构加快体制机制改革、推进数字化转型，进一步发挥技术、数据等生产要素的重要作用，助力纾解小微企业融资难融资贵问题，增强金融服务实体经济能力。二是加强金融数据治理，加快推动涉企信息的安全共享，促进数据资源有效整合和规范利用，提升金融惠民服务能力。三是加大金融科技监管力度，出台个人金融信息保护、区块链等金融科技系列监管规则，发挥标准规则、检测认证作用，构建涵盖行业监管、社会监督、协会自律、机构自治的金融科技创新管理“四道防线”。四是加强数字化监管能力建设，健全多层次、系统化的金融科技风险治理体系，增强风险的态势感知、分析评估和预警处置水平。五是推动金融 APP 备案全覆盖，规范开放应用程序接口管理，提升线上金融服务渠道安全应用水平。六是推动金融与科技产用对接，加强金融业关键共性技术联合攻关和成果转化，提升金融业先进信息技术应用能力，为金融高质量发展注入创新活力和科技动力[6]。

7. 旧金山准备修改其禁止面部识别技术的禁令

2019 年 5 月，美国旧金山监事会通过一条新禁令，决定禁止该市所有单位使用人脸识别技术，包括警察局等政府部门。旧金山也成为全球首个推出人脸识别禁令的城市。

“地处全球对科技包容性最高以及科技最为发达的区域”，旧金山的这一做法难免产生风向标效应。随后，微软删除了其最大的公开人脸识别数据库，萨默维尔和奥克兰等美国城市也宣布加入禁止人脸识别技术的行列。

不过，时隔半年，情况开始发生变化。根据外媒最新报道，旧金山准备修改其禁止面部识别技术的禁令。上周旧金山监事会一致通过了这项豁免政策，预计将于本月获得批准。该修正案适用于城市功能所必需的设备，其面部识别技术嵌入或存

[6] 中国人民银行。

储方式意味着无法删除。

旧金山的禁令主要针对的是政府机构购买和使用人脸识别技术，并未禁止普通商家或居民使用（如监控摄像机）。此次修订也应该主要是调低公共部门使用人脸识别技术的门槛。至于具体的松动尺度有多大，还有待相关法令的最终公布。不过，如同此前禁令出台时所引发的关注一样，此次修订，也将释放出对人脸识别技术应用的包容信号。

面对隐私风险应考虑针对性优化而非绝对禁止

人脸识别作为人工智能的一个重要应用，目前在全世界范围内都处于推广、普及的阶段，这种全球性的技术发展趋势，已经很难被逆转。事实上，旧金山的禁令，在一开始就备受争议。如有专业人士表示，面对可能出现的隐私风险，应该思考的是如何予以针对性的优化，而不是绝对禁止。从这个角度来说，禁令的最终修订，其实完全在意料之中，也可以说是对技术发展浪潮的一种顺应。

技术创新不同于理论创新，它必须通过实践应用的不断摸索才能继续推进，如果仅因为实施过程中可能存在一定的风险，就予以全盘否定、禁用，在当前这样一个技术应用日新月异的社会，确实不是最理想的解决方案。它一方面不利于相关技术研究和行业的发展，乃至限制技术进步带来的社会福利，另一方面也不利于激发社会的创新创造活力。这方面时常被拿来举的一个反面例子就是欧洲。由于在隐私保护观念上的“强传统”，以及相关法律法规的过于“保守”，目前整个欧洲都缺乏具有全球影响力的互联网科技公司。

当然，任何技术都利有弊，对于弊端的预防并非多余，关键是适度。在中国，人脸识别技术的应用推广，应该说是走在了前列。除了一般的扫脸支付等消费方面的应用，人脸识别已经覆盖金融、公共安全监控、乃至打拐等多个社会治理领域。如张学友的演唱会成了逃犯的梦魇、北大弑母案嫌犯在重庆江北机场被抓、最新的劳荣枝案，等都有人脸识别技术的大功劳。

人脸识别理当有更高的应用门槛

不过，与此同时，人脸识别的“滥用”风险也并非杞人忧天。如杭州野生动物世界引进人脸识别技术，启动“刷脸”入园，被消费者以合法性、安全性不足告上法庭；甚至上个月，央视还报道有人脸信息在网上被公开兜售，5000 多张人脸，打包只要 10 元。应用上的“无远弗届”之势与人脸信息保护上的巨大漏洞，确实不得不让人反思该技术的应用边界和风险管控问题。

人脸识别应用，具有非接触性采集信息的特点，效率更高，信息也更稳定，但一旦滥用和信息保护不力，所带来的风险也更高。由此，人脸识别技术相比一般的传统信息采集方式，理当有更高的应用门槛。人脸识别应有更多的前置规范，包括哪些主体有资格使用、哪些场景下可以使用、采集后的信息如何储存和保护、权益受害者如何有效维权等等，都应有清晰界定，比如哪些公共场所安装了人脸采集系统，应有透明的信息公示。

探索技术与隐私保护兼容之道

针对个人信息采集的规范，其实并不缺乏法律规定。如网络安全法、《信息安全技术个人信息安全规范》，但是这些法规所提出的都是原则性要求，具体如何实施，缺乏足够有效的现实指导性和约束力。因此，针对人脸识别应用方面的专门立法，应加快跟进，为行业发展划定更科学的“航道”。

不只是人脸识别，在应用技术大发展的今天，平衡好创新与风险、技术进步与个人权益保护的关系，并不比技术创新本身更简单。2019 年 7 月，《国家科技伦理委员会组建方案》发布，释放了将组建国家科技伦理委员会的信号，其目的就是加强统筹规范和指导协调，推动构建覆盖全面、导向明确、规范有序、协调一致的科技伦理治理体系。人脸识别技术的应用，显然也应该有科学的伦理审视。

从绝对禁止到有限放开，旧金山对人脸识别技术态度的转变，示范了一种谨慎、务实的姿态。但并不意味着我们可以放松对该技术应用风险的警惕。只有探索出一条技术与隐私保护、人文关怀的兼容之道，技术进步才能最大程度“趋利避害”，实现技术创新的初衷。[7]

[7] 朱昌俊。

二、监管动态

1．公安部发布《2019 年网络犯罪治理防范白皮书》

12 月 13 日，第十届中国信息安全法律大会暨密码法治高端论坛在京召开。会上，公安部第三研究所网络安全法律研究中心与百度联合发布了《网络犯罪治理防范白皮书》（下称《白皮书》）。

《白皮书》显示，2018 年每分钟因网络犯罪导致的经济损失高达 290 万美元，其中侵犯公民个人信息的获取手段从诱骗、脱库向非法爬取数据等方式转变，而新型网络犯罪如 AI 类黑灰产也已经大量为不法分子所用。因此，网络黑产治理需从共享资源、提升技术等多方面共同治理。

2018 年每分钟导致经济损失 290 万美元

根据最高人民法院近日发布的《司法大数据专题报告之网络犯罪特点和趋势》，2016 年至 2018 年，人民法院审结网络犯罪案件 4.8 万余件，案件量及在全部刑事案件总量中的占比均呈逐年上升趋势。其中，2018 年网络犯罪案件量显著增加，同比升幅为 50.91%。

放眼全球，网络黑产的总体规模极为庞大。

《白皮书》显示，2018 年每分钟因网络犯罪导致的经济损失高达 290 万美元，每分钟泄露的可标识数据记录为 8100 条，而头部企业每分钟为网络安全漏洞所付出的成本则达到 25 美元。

从传统的网络犯罪类型看，常见的包括电信诈骗、侵犯公民个人信息、恶意程序、流量劫持、DDoS 攻击和侵犯商业秘密。

其中侵犯公民个人信息已经逐渐形成了“源头-中间商-非法使用”的庞大地下黑色产业链。《白皮书》指出，相较于传统个人身份识别类静态个人信息，个人活动类动态个人信息的比重开始增加；获取手段也从诱骗、脱库向非法爬取数据等方式转变。

在 2018 年 4 月底警方破获的一起案件中，非法平台通过在网站添加劫持代码，非法获取并存储公民的手机号码、搜索关键词、手机型号、所在地区等信息 1000 万余条，最终相关人员被判处有期徒刑三年。

除了非法数据利用者，企业内鬼、数据中间商也在这条黑色产业链中扮演着重要角色。数据服务商从企业内鬼和数据中间商处获取数据，用于商业行为；而数据中间商则负责对数据进行清洗、验证，然后出售给下游的非法数据利用者，由他们实施敲诈勒索、暴力催收等犯罪。

9 月以来，多家大数据公司被查。据媒体披露，不少案件都跟提供非法爬虫服务有关。

《白皮书》指出，这类涉及网络爬虫的黑灰产的典型场景是 P2P 网贷、互联网小贷、资金中介等互联网金融机构无法接入央行征信等系统，只能转而与第三方大数据公司合作，由后者通过爬虫技术采集个人或企业在互联网留下的数据信息。

色情类 AI 换脸视频占比高达 96%

随着新技术、新业态的不断涌现，网络犯罪也呈现出新的犯罪类型及特点。

2019 年 8 月，一款横空出世的 AI 换脸应用“ZAO”引发公众热议。它可以把用户的脸嫁接在视频片段中的人物身上，让用户过一把戏瘾。但与此同时，对 AI 换脸、AI 换声等新型技术被用于黑灰产的担忧也如影随形。

2017 年，有国外网友发布了一个虚假的淫秽视频，将色情明星的脸与知名度高的大众明星的脸进行了更换，从而引发巨大争议。

还有犯罪团伙通过 3D 软件合成“假脸”认证网络平台账号，在受害人不知情的情况下，进行虚假注册、刷单、薅羊毛、诈骗等不法行为。

阿姆斯特丹网络安全公司 Deeptrace 的一份报告显示，从 2018 年 12 月至 2019 年 7 月，网上的 AI 换脸视频数量几乎翻了一倍，达 14,678 部，其中绝大多数是色情视频，占比高达 96%。

在网络流量排名前五的 Deepfakes 色情网站中，女性成最大受害者，换脸对象

占比达 100%。

新型网络犯罪还包括直播类黑灰产、短视频类黑灰产、黑公关类黑灰产、回退劫持类黑产等。《白皮书》提到，产业链利益关系复杂且发展迅速、存证取证难、犯罪跨平台且资金流向分散、内外勾结等特点共同构成了网络黑产的治理困境。

《白皮书》建议，治理网络黑产需遵循“生态治理”和“防治结合”。对外要形成黑灰产治理联盟，共享黑产情报、黑产人员和技术数据库，自身也要把打击和防御相结合，通过个案及时优化风控策略。

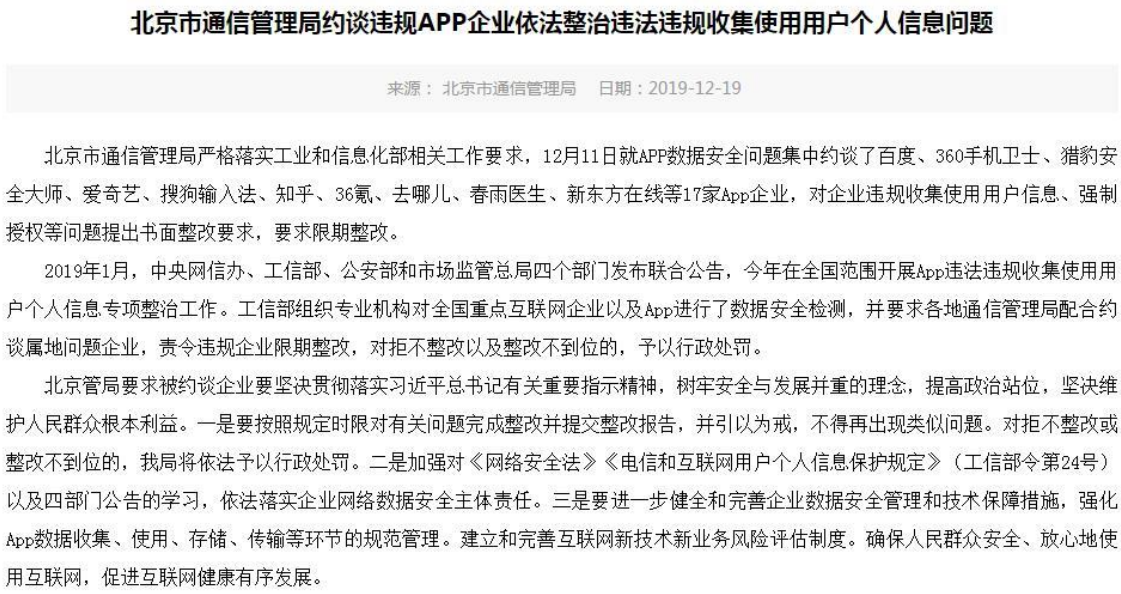
此外，监管机关也要与企业形成联动，同时做好群众普法教育工作，形成“社会公治”。最后，还需打造发现、取证、对抗黑产的创新性技术、工具、平台，从技术上正面对抗网络犯罪。[8]

《2019 网络犯罪治理防范白皮书》全文参见：

https://jing.baidu.com/h5/cybersecurityresearch.html?from=singlemessage&isappinstalled=0

[8] 南方都市报。

2. 北京通信局发布公告，约谈新东方在线等 17 家企业 APP 违法违规收集使用用户信息



北京市通信管理局约谈违规APP企业依法整治违法违规收集使用用户个人信息问题

来源： 北京市通信管理局　日期：2019-12-19

北京市通信管理局严格落实工业和信息化部相关工作要求，12月11日就APP数据安全问题集中约谈了百度、360手机卫士、猎豹安全大师、爱奇艺、搜狗输入法、知乎、36氪、去哪儿、春雨医生、新东方在线等17家App企业，对企业违规收集使用用户信息、强制授权等问题提出书面整改要求，要求限期整改。

2019年1月，中央网信办、工信部、公安部和市场监管总局四个部门发布联合公告，今年在全国范围开展App违法违规收集使用用户个人信息专项整治工作。工信部组织专业机构对全国重点互联网企业以及App进行了数据安全检测，并要求各地通信管理局配合约谈属地问题企业，责令违规企业限期整改，对拒不整改以及整改不到位的，予以行政处罚。

北京管局要求被约谈企业要坚决贯彻落实习近平总书记有关重要指示精神，树牢安全与发展并重的理念，提高政治站位，坚决维护人民群众根本利益。一是要按照规定时限对有关问题完成整改并提交整改报告，并引以为戒，不得再出现类似问题。对拒不整改或整改不到位的，我局将依法予以行政处罚。二是加强对《网络安全法》《电信和互联网用户个人信息保护规定》（工信部令第24号）以及四部门公告的学习，依法落实企业网络数据安全主体责任。三是要进一步健全和完善企业数据安全管理和技术保障措施，强化App数据收集、使用、存储、传输等环节的规范管理。建立和完善互联网新技术新业务风险评估制度。确保人民群众安全、放心地使用互联网，促进互联网健康有序发展。

近日，北京通信局发布公告称，北京市通信管理局严格落实工业和信息化部相关工作要求，12 月 11 日就 APP 数据安全问题集中约谈了 17 家 App 企业，对企业违规收集使用用户信息、强制授权等问题提出书面整改要求，要求限期整改。

2019 年 1 月，中央网信办、工信部、公安部和市场监管总局四个部门发布联合公告，2019 年在全国范围开展 App 违法违规收集使用用户个人信息专项整治工作。工信部组织专业机构对全国重点互联网企业以及 App 进行了数据安全检测，并要求各地通信管理局配合约谈属地问题企业，责令违规企业限期整改，对拒不整改以及整改不到位的，予以行政处罚。

北京管局要求被约谈企业要坚决贯彻落实习近平总书记有关重要指示精神，树牢安全与发展并重的理念，提高政治站位，坚决维护人民群众根本利益。一是要按照规定时限对有关问题完成整改并提交整改报告，并引以为戒，不得再出现类似问题。对拒不整改或整改不到位的，我局将依法予以行政处罚。二是加强对《网络安全法》《电信和互联网用户个人信息保护规定》（工信部令第 24 号）以及四部门公告的学习，依法落实企业网络数据安全主体责任。三是要进一步健全和完善企业数据安全管理和技术保障措施，强化 App 数据收集、使用、存储、传输等环节的规范管理。建立和完善互联网新技术新业务风险评估制度。确保人民群众安全、放

心地使用互联网，促进互联网健康有序发展。[9]

3. 中国信通院发布《互联网法律白皮书（2019）》

为总结梳理过去一年国内外互联网领域重要立法、执法、司法活动，总结网络法治要点，展望未来法治趋势，由中国信息通信研究院（以下简称“中国信通院”）主办的“互联网法律研讨会（2019）”于 2019 年 12 月 19 日在北京举行。

会上，中国信通院发布了《互联网法律白皮书（2019）》。这是继 2017、2018 年之后，中国信通院第三次发布互联网法律白皮书，内容涵盖我国互联网立法进程梳理、国内外互联网法治热点追踪、未来趋势展望等多个方面。

白皮书目录

一、国际互联网立法进展

（一）提升网络安全保障，构建数据管辖规则

1.完善网络安全机制，丰富治理手段

2.确立数据长臂管辖，授权司法调取

3.数据本地化立法频繁，探索数据规则衔接

（二）聚焦网络内容治理，落实平台责任

1.集中加强恐怖主义等内容管理

2.多措并举应对虚假新闻和网络暴力

[9] 和讯网。

3.加强网络版权保护，明确平台责任

（三）完善个人信息保护立法，增强全面执法能力

1.个人信息保护专门立法持续出台

2.关键环节、特殊客体具体保护规则不断完善

3.全球个人信息执法活动愈加频繁

（四）鼓励和规范新技术新业务发展

1.积极推动新技术新业务发展

2.探索新技术新业务监管规则

二、国内互联网法治进展

（一）构建网络空间法律体系

1.完善网络安全立法体系

（1）推进网络安全制度建立

（2）促进云计算服务安全可控

（3）持续强化数据安全管理

2.规范互联网信息服务活动

（1）丰富互联网内容治理架构

（2）加强互联网金融信息管理

（3）规范网络视听节目传播秩序

3.推进网络社会管理立法

（1）修改完善电子商务相关法律法规

（2）加强未成年人权益保护

（3）构建网络信用管理体系

（4）引导新技术新业务发展

（二）互联网执法力度持续加大

1.积极开展网络安全治理行动

2.清理整治网络违法有害信息

3.打击侵犯知识产权行为

4.集中处理电子商务违法行为

（三）互联网司法更加能动

1.互联网法院建设取得积极成效

2.司法与科技深度融合高效便民

3.积极探索涉网案件裁判规则

（四）网络法治研究逐步深入

三、未来趋势展望

（一） 立法持续充实，重点逐步转移

1.网络空间立法适应新形势变化

2.向网络社会管理立法逐步倾斜

3.数据治理成为未来网络治理核心

（二）执法能力稳步提升，司法改革全面推进

（三）多方参与国际合作，构建网络空间命运共同体

《互联网法律白皮书（2019）》全文参见：

http://www.cbdio.com/image/site2/20191223/f42853157e261f6aa36c44.pdf

4. 中国信通院发布《移动应用（App）数据安全与个人信息保护白皮书（2019 年）》

2019 年 12 月 26 日，2020 中国信通院 ICT 深度观察报告会“电信网络诈骗治理与网络空间安全分论坛”在北京国家会议中心举办。会上，中国信通院安全研究所发布了《移动应用（App）数据安全与个人信息保护白皮书（2019 年）》，内容涵盖 App 最新发展趋势及社会经济影响、当前 App 存在的主要数据安全隐患、国内外 App 数据安全管理实践、App 数据安全综合治理建议和用户热切关注的安全防范技巧等多个方面。

移动应用（以下简称“App”）是数字经济下的重要产品。随着移动网络和智能手机全面覆盖，App 种类和数量增长迅猛。从社交到出行、从网购到外卖，从办公

到娱乐，App 已全面渗透用户生活，成为大众生活必需品，并因此汇集大量衣食住行、社交关系等用户个人信息。App 逐渐成为承载网络应用和信息数据的核心载体。

App 在满足用户美好数字生活需要，助力消费升级和经济转型发展方面发挥了不可替代的作用，但也暴露出违法违规收集使用个人信息、用户个人信息泄露与滥用等数据安全问题。App 数据安全关乎个体层面的隐私权利保护，产业层面的健康发展，以及国家层面的全球数字竞争力。欧美等移动互联网发展较早的国家，在移动互联网安全制度构建方面已较为领先。近年来，我国也高度重视 App 数据安全与个人信息保护工作，从法规标准、专项治理、企业自律等方面多管齐下，加大治理力度。

本白皮书在研判 App 发展趋势及社会经济影响的基础上，重点分析目前主流 App 存在的数据安全隐患，系统梳理总结国内外 App 数据安全治理现状，最后从政府、企业、行业三个维度研究提出了我国 App 数据安全与个人信息保护综合治理建议，并从用户视角总结提出了用户安全使用技巧。

白皮书目录

[10] 中国信通院 CAICT。

《移动应用（App）数据安全与个人信息保护白皮书（2019 年）》全文参见：

http://www.caict.ac.cn/kxyj/qwfb/bps/201912/P020191230332039577332.pdf

5. 中国信通院发布《数字经济治理白皮书（2019）》

2019 年 12 月 26 日，中国信通院发布《数字经济治理白皮书（2019）》，主要包括：

一、数字经济治理的形势与挑战

（一）数字经济成为经济高质量发展的重要动能

（二）国家治理对数字经济治理提出新要求

（三）全球数字经济治理话语权博弈日趋激烈

（四）数字经济新特征带来四大治理挑战

二、数据治理的态势与特点

（一）全球个人信息保护制度与执法实践不断丰富

（二）数据跨境流动领域国家间主权冲突问题凸显

（三）非个人信息自由流动规则助力建构数字市场

（四）中国积极推进个人信息保护立法与实践

三、算法治理的态势与特点

（一）算法价值观问题受到全球各国关注

（四）全球数字经济治理规则博弈正在加剧

《数字经济治理白皮书（2019）》全文参见：

http://www.caict.ac.cn/kxyj/qwfb/bps/201912/P020191226515354707683.pdf

三、相关案例

1. 57 款 App 被点名整改：因不当收集使用个人信息

近日，APP 专项治理工作组发布《关于 61 款 APP 存在收集使用个人信息问题的通告》，点名存在问题的 APP，要求相关 APP 运营者对存在的问题进行整改。

关于61款App存在收集使用个人信息问题的通告

App治理工作组 App个人信息举报

近期，App专项治理工作组在评估中发现，57款App存在收集使用个人信息问题（名单及问题见附表），建议相关App运营者对存在的问题进行整改，并自即日起30日内向工作组反馈整改情况。30日后工作组将对整改情况予以核验，并将核验结果提交相关部门，建议依法予以处置。

7月至10月，App专项治理工作组根据评估中发现的收集使

值得注意的是，57 款被点名的 APP 中，金融领域属“重灾区”，占比近半数，涵盖银行（信用卡）、网贷、支付等领域。

信用卡业界发展的标杆——某银行信用卡专属 APP 也榜上有名。通告显示，该 App 存在未明示收集用户个人信息的目的方式范围、收集用户敏感信息、收集个人信息频度超出业务功能实际需要等多个问题。

此外，该 APP 还存在用户不同意收集非必要的个人信息就拒绝提供“周边游”业务功能，以默认选择同意隐私政策的非明示方式征求用户同意等问题。

同时，该 APP 未经用户同意，也未做匿名化处理，就通过客户端嵌入的个推、

神策数据、微博等 SDK 向第三方提供设备 IMEI 号等个人信息。

国家相关部门对个人信息保护和数据治理问题越来越重视，并将持续开展整治活动。

人民银行相关人员表示，人民银行正与中国互联网金融协会合作推动金融类 APP 规范化，比如从技术使用规范、数据使用规则等方面提出一定要求，推动生物识别技术在金融领域的安全应用等。下一步，人民银行还将进一步推进技术检测工作。

公安部相关负责人则表示，公安部 2020 年将继续开展“净网 2020”专项行动，与网信办、人民银行等多部门综合施策，形成监管合力，继续打击违法违规乱象。同时，以促进发展、规范管理为主要目标，促进 APP 企业合法合规运营。对不履行义务要求的，要坚决依法整改查处。对拒不履行义务和为违法犯罪和网络黑产提供支持的，将坚决依法打击。[11]

App 专项治理工作组整改通告全文参见：

https://mp.weixin.qq.com/s/lwPtpaYfwB5dlEc7YffQnQ

2. 江苏 11 款 App 侵害个人信息被查

2019 年 12 月 30 日，江苏网警发布了案情通报。根据公安部通报线索，江苏苏州、南通、扬州、淮安等地公安网安部门对属地 App 运营单位上线的 11 款生活服务类 App 应用进行检查。

经查，这 11 款 App 存在侵害个人信息行为，有的未告知用户、未获得用户允许非法获取用户设备敏感权限，有的首次运行未通过弹窗等明显方式提示用户阅读隐私政策，有的用户隐私协议缺失，有的超范围收集用户手机联系人、位置信息、短信信息，有的超范围申请用户系统“读取短信内容”“录音”等权限。

依据《网络安全法》第 41 条、第 64 条规定，江苏各属地警方分别对涉事运营

[11] 财经国家周刊。

单位予以警告，并责令限期整改，对部分直接负责的主管人员还予以罚款处罚。[12]

3. 吉林磐石市政府官网泄露居民个人信息，回应：立即通知整改

吉林省磐石市人民政府门户网站页面 “通知公告”栏目近年来陆续发布了数条名单公示，绝大多数名单未对居民个人隐私进行处理。

例如《关于磐石市 2019 年申请由租赁补贴转实物配租的家庭名单公示的通知》其中附有一份名单。该公示附件中的名单将 44 条相应人员的姓名、身份证号码、家庭人口数完整公示出来，对身份证号码未做任何模糊处理，且公示期早已过去，但截至记者检索时，相应信息仍在网上对外公布。

而该网站近年来发布的各类名单公示超过 10 份，涉及由租赁补贴转实物配租、危房改造计划对象、扶贫对象动态管理工作新识别贫困户等内容，且均在涉及居民个人身份证信息等方面未做模糊处理，涉嫌泄露个人隐私数百条。

12 月 25 日上午，磐石市政务公开网站工作人员接受采访时表示：“因公示是各个部门提供并经由领导签字盖章，只负责上传工作，不太清楚有相关规定。会立即通知各个部门，马上进行整改处理，日后注意。”

在 2018 年，国务院办公厅在印发的《2018 年政务公开工作要点》中曾明确提出，政府信息公开前要依法依规严格审查，特别要做好对公开内容表述、公开时机、公开方式的研判，避免发生信息发布失信、影响社会稳定等问题。要依法保护好个人隐私，除惩戒公示、强制性信息披露外，对于其他涉及个人隐私的政府信息，公开时要去标识化处理，选择恰当的方式和范围。

2017 年底曾集中报道了多起政府网站泄露公民个人隐私信息事件。两年过去了，各级政府网站在公示公告中泄露公民个人隐私信息的情况依然严重。[13]

[12] 现代快报。
[13] 澎湃新闻。

4. 员工离职后从公司非法下载并出售个人信息获利 49 万余元

12 月 26 日，广西壮族自治区柳州市柳江区检察院对被告人李某涉嫌侵犯公民个人信息罪依法提起公诉。

2018 年 8 月份至 2019 年 8 月份,被告人李某在柳州市柳江区拉堡镇基隆综合区一民房、柳州市鱼峰区蝴蝶山路一民房内，通过电脑登陆原工作单位广州某信息科技有限公司收集用户咨询信息数据汇总的网址、公司数据主管彭某的工作 QQ 进入该公司的工作 QQ 群，非法下载公民个人信息,后其通过个人微信号联系买家并出售公民个人信息。

公安机关网络安全保卫总队在进行网络巡查时发现李某有买卖远程监控软件的嫌疑。经侦查后，2019 年 8 月 29 日 19 时,李某在其蝴蝶山路住处被民警抓获,并查获其用于作案的电脑、手机等物品。经查，李某电脑中储存的公民个人信息达 6000 余条,李某通过微信号向他人出售公民个人信息非法获利人民币 49.37 万元。经审讯,李某对犯罪事实供认不讳。

经依法审查后,该院认为，被告人李某违反国家有关规定,向他人出售公民个人信息,非法获利达人民币 49.37 万元，情节特别严重，其行为已触犯刑法，犯罪事实清楚，证据确实充分，应当以侵犯公民个人信息罪追究其刑事责任。[14]

5. 《数据泄露典型判例分析报告》：泄密者八成是内鬼

近日发布《数据泄露典型判例分析报告》中指出，当前数据泄露途径呈现出多元化和隐蔽化的特点，数据实战监控面临挑战。同时分析发现，数据泄露风险主要来自于内部人员，占比高达八成，而牟利是造成数据泄露的主要动机。

以中国裁判文书网自 2011 年-2019 年 10 月发布的所有与数据泄露相关的典型判例(包含侵犯公民个人信息、网络安全法、非法获取公民个人信息等关键字)的 150 份裁判文书样本数据，从泄露数据类型、泄露人身份、泄露动机和泄露渠道等维度对样本数据进行解读整理，还原泄露过程，识别关键因素，形成了该报告。

[14] 正义网。

报告首先将数据泄露类型分为 5 大类，分别是用户数据、客户数据、源代码、商业机密数据和政企涉密文件。其中，用户数据是数据泄露重灾区，占数据泄露 35%，其次为商业机密数据和客户数据。

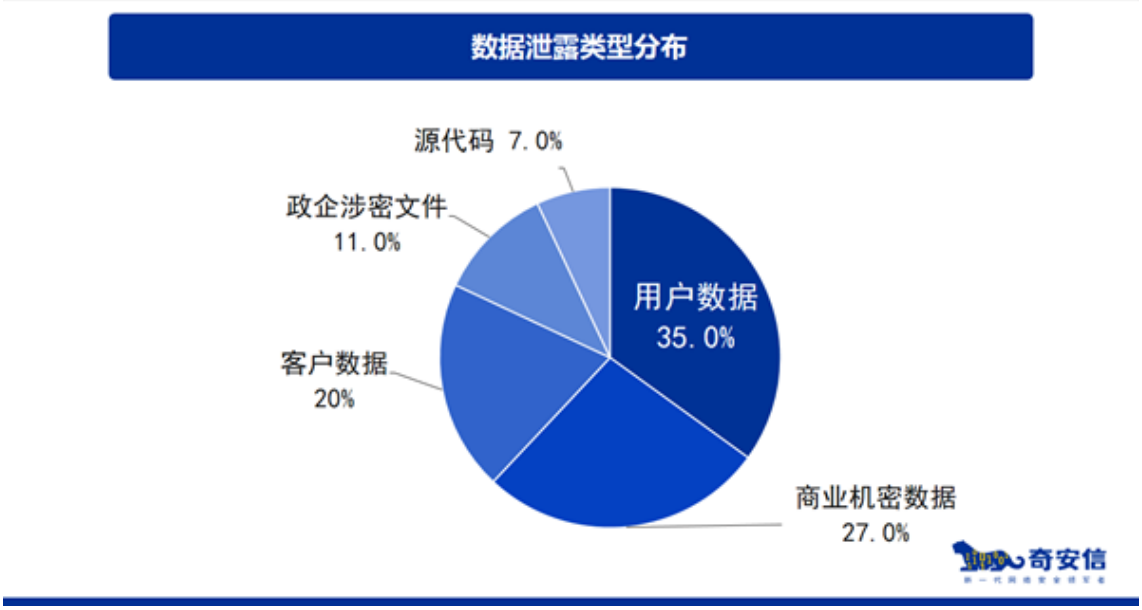


图 1：数据泄露类型分布 用户数据占比高达 35%

报告同时也对对判例样本中的数据泄露人身份角色进行了分类，发现泄露人员角色主要分为 2 大类 7 子类，一类是内部人员，一类是外部人员。其中内部人员又分为在职普通岗位、在职重要岗位、在职技术人员、待离职人员、离职人员;外部分为合作伙伴和黑客。

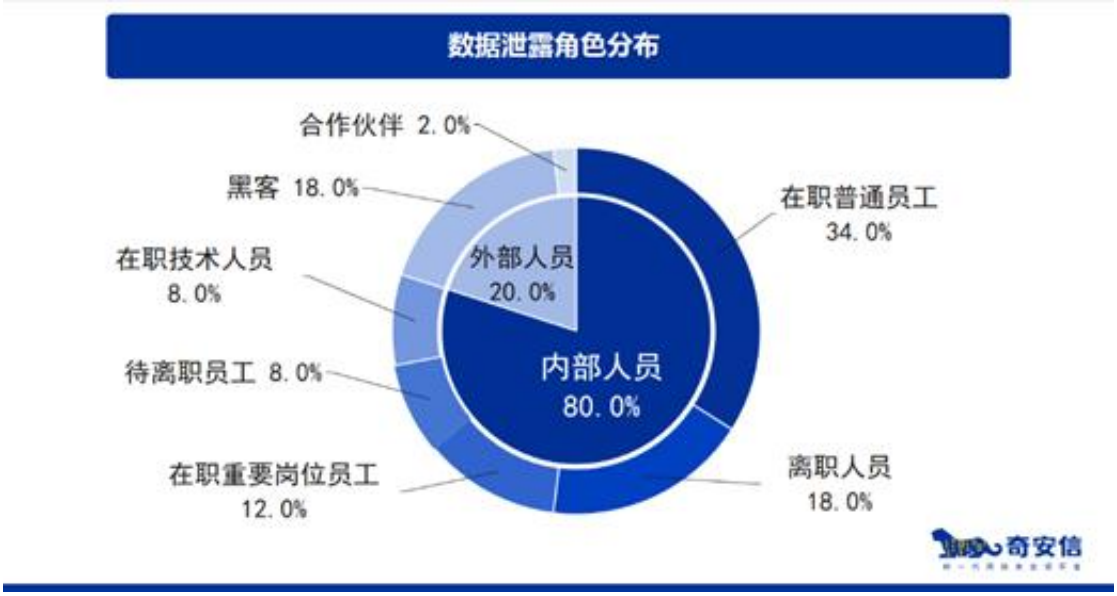


图 2：数据泄露角色分布 泄密者八成是“内鬼”

从泄露角色分布图可以看出，泄露的发生无外乎外部人员的主动攻击和内部人员的有意或无意泄露。其中数据泄露角色 80%来自内部人员，外部人员中 90%的攻击来源是黑客，黑客利用漏洞直接脱库，或者开展社会工程学攻击，获取高权限的账户直接对数据库进行操作，从而达到数据窃取的目的。

外部人员中第三方合作伙伴也是最常见数据泄露角色，由于业务合作需要共享数据，而下游合作厂商的数据保护意识或数据保护能力存在偏差从而导致数据泄露，这也是近年来攻击者更愿意从数据产业链的下游发起攻击，从而窃取数据的原因。

报告同时指出，牟利永远是数据窃取的最强原动力。牟利、增加求职筹码及不正当利用造成了 80%的数据泄露案件。

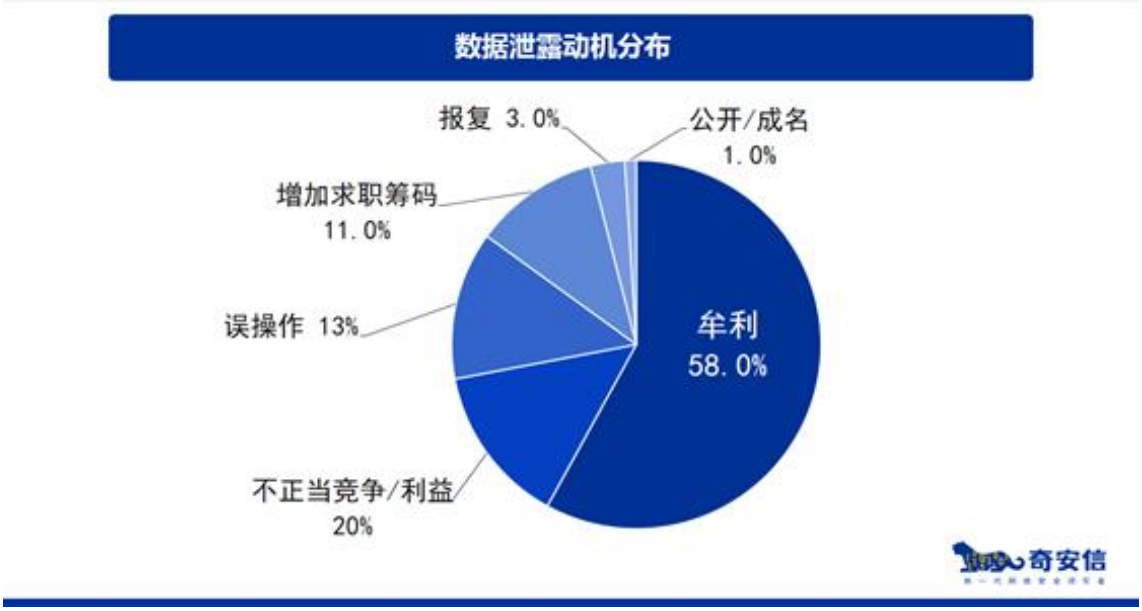


图 3：牟利成为数据窃取的最强动力，占比近六成

报告最后分析发现，移动存储介质(U 盘/移动硬盘/存储卡)占据近半壁江山，也符合其拷贝量大、传输速度快的特点。其次即时通讯、网盘类工具、邮件也常用于数据外发或数据备份，拍照常见于不能直接获取到此类数据，只具备查看权限的案例，例如拍照生产车间关键设备的参数数据。

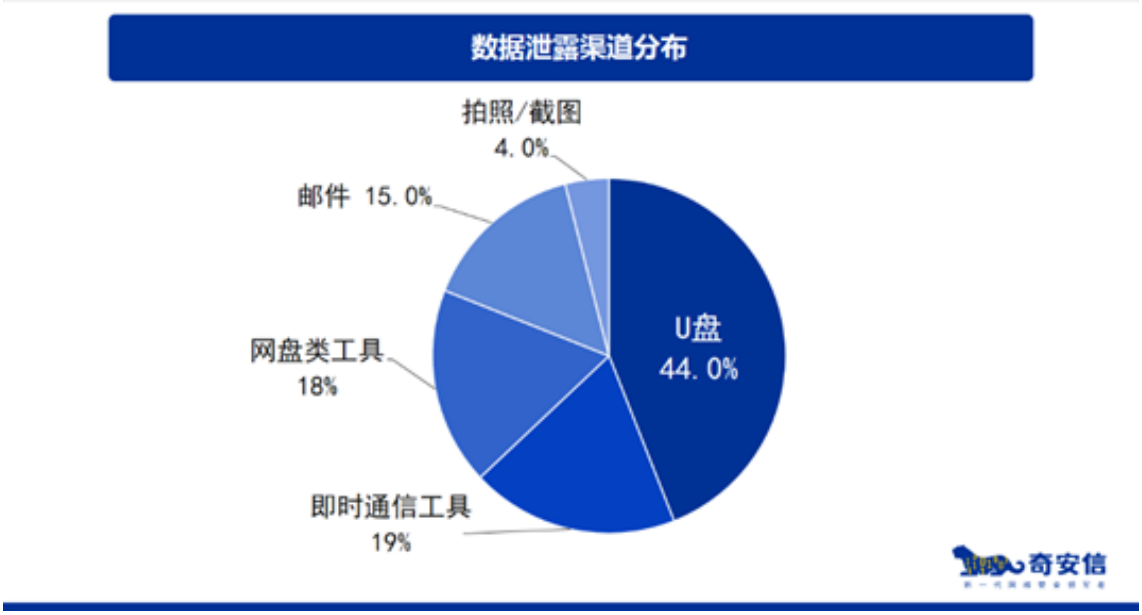


图 4：移动存储介质(U 盘)是数据泄露的主要渠道

近年来，数据安全已经成为网络安全行业聚焦点最高的一个细分领域。随着“云大物移智”的快速发展，数据已经成为企业的重要生产资料，数据驱动业务决策也成为实践业务创新的核心手段。随着数据交易的常态化，勒索软件开发市场的规模化，数据衍生服务的体系化，在低成本高收益的诱惑下，政府，企业的核心数据保护均面临着来自内外部的巨大风险。[15]

《数据泄露典型判例分析报告》全文参见：

https://www.qianxin.com/threat/reportdetail/37?type=report_apt_list

6. Facebook 再曝隐私危机，逾 2.6 亿用户个人资料外泄

社交媒体网站 Facebook12 月 19 日表示，他们正在调查一则贴文，这则贴文指出，一个数据库暴露在网络上，当中含有超过 2.67 亿“脸书”用户的姓名与电话号码等数据。

根据英国数据研究公司 Comparitech 网站上一则贴文，数据库上周被放上一个在线黑客论坛供人下载，这个论坛显然隶属于某个犯罪集团。

Facebook 发言人说:“我们正在调查此事，但我们认为，取得这些信息的时间，可能是在‘脸书’过去几年为加强保护用户信息而做出改变之前。”

Comparitech 网站指出，安全研究人员狄亚申科(Bob Diachenko)发现这个对外开放的数据库，当中含有“脸书”用户的姓名、用户名称和电话号码。

报道指出，Facebook 正努力重建大众对他们的信任，并缓和外界对这个社交网站个人资料保护的疑虑，却在此时发生这件事。

而 Facebook 在隐私泄露方面已经算是“惯犯”了。

[15] 奇安信。

2018 年 4 月，Cambridge Analytica（剑桥分析公司）被指控非法获取 Facebook 平台上的用户信息，覆盖人数高达 5000 万。在此丑闻爆发后，Facebook 立刻限制了相关软件的应用，但据官方表示，较多外部开发人员通过 API 来保留访问用户基础信息的时间，导致 Facebook 采取的举措无法完全对用户信息进行重新保护。

2019 年 7 月，Facebook 与美国联邦贸易委员会（FTC）达成了和解，并针对 2018 年剑桥分析的隐私泄漏丑闻进行高达 50 亿美元的罚款。而令人咋舌的是，在 Facebook 传出接受罚款的消息后，其公司的股价上升 1.81%，公司市值增长 104 亿美元，所收获的利润远远超过了罚款金额。

2019 年 11 月 4 日，Facebook 又被曝隐私泄露，在平台开始限制相关用户信息后的几个月，与之合作的 100 多个第三方应用可能已经通过 Facebook 工程组的编程界面访问了用户的个人数据。这些可能涉及泄漏的信息包括了用户的姓名和个人图片，但 Facebook 方并没有透露受到波及的具体用户人数。

而这样的结果并没有意味着 Facebook 在隐私丑闻上彻底脱身，对于社交平台来说，信息保护的路并不好走。[16]

7. 物联网供应商 Wyze 确认服务器发生泄露

据外媒 ZDNet 报道，Wyze 是一家销售安全设备（如安全摄像头、智能插头，智能灯泡和智能门锁）的公司，该公司周日证实发生了服务器泄露，大约 240 万客户的详细信息遭泄露。Wyze 联合创始人在圣诞节期间发表的论坛帖子中说，泄露是在内部数据库意外在线暴露之后发生的。

该公司表示，公开的数据库-一个 Elasticsearch 系统-不是生产系统；但是，服务器正在存储有效的用户数据。Elasticsearch 服务器是一种用于支持超快速搜索查询的技术，旨在帮助该公司对大量用户数据进行分类。

该公司表示，为了帮助管理 Wyze 的快速增长，最近启动了一个新的内部项目，以寻找更好的方法来衡量基本的业务指标，例如设备激活，连接失败率等。公司从主要生产服务器复制了一些数据，并将其放入更灵活的数据库中，以便于查询。最初创建此新数据表时，该表受到了保护。但是，Wyze 员工在 12 月 4 日使用此数据库时犯了一个错误，并且该数据的先前安全协议已删除。公司仍在调查此事件，

[16] 中国新闻网。

以找出原因和发生方式。

Wyze 确认泄露的服务器暴露了详细信息，例如用于创建 Wyze 帐户的客户电子邮件地址，分配给 Wyze 安全摄像机的昵称用户，WiFi 网络 SSID 标识符以及对于 24000 位用户而言的 Alexa 令牌，这些令牌将 Wyze 设备连接到 Alexa 设备。

Wyze 高管否认 Wyze API 令牌是通过服务器公开的。Twelve Security 在其博客文章中声称，他们找到了 API 令牌，他们说这些令牌可以使黑客从任何 iOS 或 Android 设备访问 Wyze 帐户。不过 Wyze 否认了 Twelve Security 的说法，即他们正在将用户数据发送回某知名云服务器。

就目前而言，涉及此泄露的披露三方在此特定泄露事件的细节方面似乎不一致。无论哪种方式，Wyze 都表示决定从所有帐户中强制注销所有 Wyze 用户，并且与所有第三方应用程序集成不同，这两个步骤将在用户重新登录并重新链接 Alexa 设备到 Wyze 帐户后生成新的 Wyze API 令牌和 Alexa 令牌。[17]

8. 化验室遭黑客入侵，加拿大近半人口健康检测数据或已泄露

最新消息，LifeLabs 突发通告，后台数据库被黑客攻击并勒索，1500 万名加拿大人的个人信息被盗取。所有人需要做抽血，尿检，心电图之类的检测，都必须要家庭医生开处方，然后到专门的实验室做检查，而这个检查实验室就是 LifeLabs。所以，没有人能绕开 LifeLabs。

据 LifeLabs 公开信的信息显示，近期 LifeLabs 遭受了一次网络攻击，黑客未授权访问后台数据，1500 万名用户的信息，包括姓名，地址，电子邮件，登录名，密码，生日日期，医疗卡号和实验结果等，面临暴露的威胁。不仅如此，黑客还以这些资料为要挟，要求 LifeLabs 赎回数据。

面临信息暴露的 1500 万用户，绝大多数生活在 BC 省和安省。而已经确认被泄漏检测结果的 85000 人，全位于安省，这些受害者在 2016 年以前做过的所有医学检测结果，及个人信息都已被黑客盗走。

[17] cnBeta。

这次的信息泄露是加拿大迄今为止，涉及人数最多的一次。

随着信息时代的发展，个人信息对每个人的重要性越来越明显，这次 LifeLabs 后台被黑，不仅是个人信息被泄露，所有客户登陆该网站的账号和密码都一同被暴露。

不少人因为害怕自己记不住这么多密码，常常是所有网站共享一套账号密码，这次 LifeLabs 的信息泄露，将有可能造成部分用户其他网站的账号密码一起被盗的结果，这将会是灾难性的结果。

LifeLabs 目前对外公布两种补救措施：

第一，公司已经安排专业人员和黑客谈判，希望能将数据安全地买回来；

第二，所有担心自己信息泄露的客户，可以联系 LifeLabs，他们将提供一年的免费保护：监控暗网和个人身份防盗保险。[18]

9. 美国商务部研究机构：人脸识别技术存在种族、性别偏见

脸部识别技术已逐渐融入人们的生活，许多智能手机用户选择开启“刷脸”功能，方便自己的生活。此外，人脸识别技术也相继被应用于执法机构和政府部门。

不过近日，美国商务部一研究机构指出，脸部识别技术存在“种族、性别偏见问题”，一些在美国开发的算法“错误率很高”。

研究人员发现，面部识别软件对黑人和亚洲人的识别错误率高于白人，大约高出 10 到 100 倍。系统对于女性的识别错误率也高于男性，美国原著民的识别错误率最高。

此外，不同软件和算法的错误率有明显差别。对此，部分提供软件识别技术的公司并不认同，他们称研究人员“没有正确使用软件”或“用了过时的算法”。

[18] 天泷。

美国商业内幕网(Business Insider)20 日消息，美国国家标准技术研究所(National Institute of Standards and Technology 属于美国商务部)当地时间周二声明称，一项针对脸部识别的研究显示，相比识别男性和白人，一些脸部识别软件对女性和有色人种的识别能力相对较弱。

报道称，该研究选取了 99 个公司作为实验对象，其中包括因特尔、微软、松下等等知名品牌。研究团队用超过 800 万人的 1800 万张照片对这些脸部识别系统进行了测试。

美国《华盛顿邮报》报道称，对亚洲人、非洲裔美国人、印第安人和太平洋岛民进行“一对一”搜索时，一些在美国开发的算法错误率很高。这类搜索对机场登机等功能至关重要，错误可能会让冒名顶替者更容易钻空子。

该媒体还指出，这种情况在警方查案时经常出现，非裔美国女性的面孔经常被警方使用的人脸识别软件认错。

但值得注意的是，亚洲公司生产的面部识别软件不太可能误认亚洲面孔。

“虽然针对算法作出声明通常来说是不合理的，但我们确实发现了一些事实证据证明，我们研究的人脸识别算法中，存在人种差异。”美国国家标准技术研究所研究院帕特里克.格罗瑟(Patrick Grother)、报告的首席作者说道，“这些数据对议员、开发者以及终端用户来说，会很有价值。他们能够以此来考量一些算法的局限和合理使用性。”

报道称，在过去的一年中，美国各地的执法机构已经开始采用面部识别技术，作为跟踪任务和识别嫌疑人的工具。

这一举动，遭到美国公民自由主张者(Civil-liberties advocates)的反对，一些城市开始禁止执法部门使用面部识别技术。

美联社 2019 年 5 月 15 日报道称，旧金山是美国第一个禁止警方使用脸部识别技术的城市。紧随其后的还有奥克兰、萨默维尔和布鲁克林。

到了 2019 年 10 月，美国公民自由联盟(ACLU)起诉美国司法部、联邦调查局(FBI)和缉毒局(DEA)，要求它们提供与使用监控技术有关的文件。美国知名财经媒体石英财经网(Quartz)指出，这其中，就涉及亚马逊和微软向政府客户提供的面部

识别软件。

早在 2019 年 2 月，有关人脸识别技术存在种族识别问题的研究就闹到的沸沸扬扬。

美联社报道称，当时，麻省理工的研究人员发现，亚马逊的面部识别软件 Rekognition 对有色人种的误认率高于白人，对深色皮肤的女性的识别错误尤为突出。

然而，亚马逊公司并不认同实验结果，并称研究人员“没有正确使用软件”或“用了过时的算法”。

美国商业内幕网指出，美国国家标准技术研究所本次 99 个实验对象公司中，并没有亚马逊的名字，而且该公司没有为这项研究提供任何软件支持。[19]

10. 美国公司破解人脸识别，安全风险有几何？

2019 年 12 月 12 日，美国《财富》杂志报道，美国圣地亚哥的一家人工智能公司 Kneron 用高清 3D 面具和照片，在世界多地成功欺骗了包括中国的微信、支付宝以及中国的火车站。由此，引发了关于人脸识别安全性的一些讨论。

3D 面具破解人脸识别更多是测试行为，而非实际风险

从身份验证的技术上来看，常常是多个维度共同约束、同时验证一个人的身份的。我们的手机支付，实际上就有三重保护。首先，人不会把手机给其他人，会保护好；其次，手机通常都会设置一个开机密码。这些开机密码提供的保护很强，像苹果的隐私保护机制，就连 FBI、CIA 也没办法。这些关都过了，最后才是微信与支付宝的人脸识别。而这背后还有潜在常行为信息、常用地点、常在时间等保护，支付金额限制等保护措施。所以，这个破解，前面几关都是用户配合，然后直接进入测试人脸识别。所以，从安全性上看，更多的是一个测试行为，而非一个实际风险。所以，从实际生活务实层面，消费者也不必过虑。

[19] 观察者网。

不过，由此扩展开的一些务虚的思索，不妨“过虑”一些。

此前，杭州一家动物园要把之前的指纹入园认证改为人脸识别认证，已经办理年卡的浙江理工大学的一位教授就把公园告上法庭，理由是：凭什么你没征求我的意见，就默认我们都同意把面部信息提供给你？公园最初还颇为疑惑，为什么指纹电话号码大家觉得问题不大，但一谈到“人脸识别”大家都惊呼“我的隐私数据被盗了”。

人脸识别具有更高的数据保护需求

大众态度的差别，是直觉性的，因为人脸识别技术最新，人一般对新东西的怀疑会更大。不过，从客观来看，人脸识别的风险也远胜于电话号码，甚至也高于同为生物信息的指纹、虹膜、声纹等。

密码泄露，只需要改变密码即可，但指纹、人脸信息是无法改变的，一旦被盗用，被有意识的窃取，被窃取者除了改变其他安全方式之外，没有其他办法。所以，人脸信息更加敏感。

而且，DEEPFAKE 技术的出现，使得人脸信息可以被用来“换头”移植到其他视频中。Deepfake，是由“deep machine learning”（深度机器学习）和“fake photo”（假照片）组合而成，是深度学习模型在图像合成、替换领域的一次成功应用。不久前，轰动一时的“ZAO”换脸 APP 风波，就是基于 DEEPFAKE 技术。所以，对于普通人来说，人脸识别会带来一个全新的风险：一般来说，密码泄露，只会损失被密码保护的东西，但是，人脸信息的扩散，很可能影响到生活。

所以，欧盟地区的数据保护法《通用数据保护条例》（“GDPR”）的规定，面部图像（facial image）构成特殊类型个人数据下的“生物识别数据”，进而相较于一般个人数据受制于更高的保护要求。

中国国家网信办，11 月 29 日发布的《网络音视频信息服务管理规定》也规定从 2020 年 1 月 1 日起，AI 造假视频不得随意发布。新规定中关于 AI 造假音视频的规定主要有四条：“按照国家有关规定开展安全评估”、“以显著方式予以标识”非真实音频信息、不得利用 AI 造假技术发布虚假新闻、部署 AI 造假音视频鉴别技术和健全辟谣机制等。

安全与破解安全的斗争是自然科学的规律所在

不过，人脸识别虽然更加敏感，但也有其自身的优势。

第一，人脸识别具有很大的方便性。

很大程度上来说，人脸识别并不是一个基于安全考量的技术。我们平常用的密码，比如支付密码、银行卡密码，都是藏在用户的心里的，不会有被盗取的可能。如果是基于非对称 RSA、对称 AES 等加密算法，只要密码稍微复杂一些，不是简单的单词，混合字符、字母、数字，基本上是不可破解的。所以，在一些对安全有着非常严格的场景下，都是采用的字符密码。

当然，也可能在输入密码的时候被盗取，但相比之下，人脸不可能被藏起来，明晃晃的显示在公共场合之中，可以获取的手段就太多了，甚至在朋友圈、社交网站上都可以搜到。

所以，人脸识别并不是一个完全基于安全的发明。但是，另一方面，人的需求多种多样，安全并不是如很多人认为的那样，始终是第一位的。打个比方说，人们为了出行方便，在预算约束下会去买电瓶车，如果说这种安全上的折中是无奈的话，那么，还有人出于爱好，花十几万买摩托，而不买轿车。所以，安全并不是压倒一切的需求，方便等需求也很重要。所以，在既有安全需求，也有方便需求的场景下，人脸识别就是一个非常好的解决方案，在小额支付、公司门禁、家庭门禁、考勤打卡、智能家居上还是有很大的发展前景的。

第二，人脸识别的防范对象更广。

人脸识别、指纹识别等生物学安全措施，相对密码识别等方案，基于自身的生物学特征，也有一些自己独特的优势。比如，密码要假冒的话，只需告诉别人就可以了。但人脸识别，指纹识别，要想假冒就更难一些，人脸和指纹的原主人，总不能在任何时候都到场。所以，人脸识别不仅防的是其他人侵犯本人的权益，某种程度上，也可以防住人脸的主人。比如，滴滴顺风车、快递小哥的人脸识别，就是平台为了防止作弊。

制作换脸视频和识别换脸就像一场猫鼠游戏，道高一尺魔高一丈，安全与破解安全的矛盾一直存在。两者之间的斗争，从人类发明机械锁就开始了。从更深层次的层面看，安全与自由也始终是一对矛盾。当安全达到极致的时候，自由也必然丧失，也保不住安全，所以，人脸识别被假冒，本身也是社会发展，乃至自然科学的

规律所在。[20]

四、环球评论

1. 简析《民法典（草案）》——个人信息保护部分

近日，《中华人民共和国民法典（草案）》（后文简称“民法典（草案）”）对外发布，其中对与人格权部分进行了详细的规定，本文主要介绍个人信息保护方面的相关规定。

《中华人民共和国民法总则》（以下简称“民法总则”）仅在第一百一十一条对个人信息的保护进行了规定，即“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”此条款明确了个人信息收到法律保护，同时强调了获取方的两点核心义务：1.依法获取和使用个人信息；2.保障信息安全”。

《民法典（草案）》在涵盖了上述要点的基础上，对个人信息保护做出了更加细致的规定。 第一千零三十四条沿用了《民法总则》第一百一十一条“自然人个人信息收到法律保护”的表述，没有单独将个人信息保护列为一项具体人格权，而本条中的第三款“个人信息中的私密信息,同时适用隐私权保护的有关规定。”明确了个人信息与个人隐私之间存在一定范围内的重合。但是，关于“私密信息”的范围《民法典（草案）》中没有给出清晰的界定，还有待于相关立法机关的进一步解释。

同时，此条的第二款明确定义了个人信息的范围，与 2017 年生效的《中华人民共和国网络安全法》（后文简称“网络安全法”）的界定一致，而纵观《民法典（草案）》个人信息保护部分的规定与《网络安全法》中的规定较为相似，我们总结了其中的相似条款及条款对应的核心要点，详见下表：

《网络安全法》	《民法典（草案）》	核心要点

[20] 刘远举。

第四十条至第四十五条	第一千零三十四条	➢ 自然人个人信息受到法律保护；
第四十一条	第一千零三十五条	➢ 收集、处理个人信息应当遵循合法、正当、必要的原则； ➢ 公开收集、使用的规则； ➢ 明示收集、处理信息的目的、方式和范围； ➢ 收集、处理个人信息应当征得被收集者的授权同意； ➢ 不得违反法律法规及双方的约定。
第四十三条	第一千零三十六条	➢ 访问权 ➢ 更正权 ➢ 删除权 《民法典（草案）》明确规定了个人信息主体拥有依法抄录或者复制其个人信息的权利。
第四十二条	第一千零三十八条	➢ 未经同意不得向他人提供个人信息，但经处理无法识别特定个人且

		不能复原的除外； ➢ 信息收集者、控制者应当采取技术措施，保障个人信息的安全； ➢ 一旦发生安全事件，应当及时采取补救措施，并按规定向被收集者和主管部门告知
第四十五条	第一千零三十九条	➢ 国家机关及工作人员对于履行职责中知悉的自然人的隐私和个人信息,应当予以保密,不得泄露或者向他人非法提供。

除上述条款外，《民法典（草案）》第一千零三十七条明确规定了责任豁免的情形，当收集、处理自然人的个人信息符合下列情况之一，行为人无需承担民事责任：

- 在该自然人或者其监护人同意的范围内实施的行为;
- 处理该自然人自行公开的或者其他已经合法公开的信息,但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外;
- 为维护公共利益或者该自然人合法权益,合理实施的其他行为。

《民法典（草案）》第一千零三十七条首次从法律层面规定了收集、处理个人信息的责任豁免情形，并且明确了除征得同意外，收集、处理个人信息的其他合法性事由。

综上所述，在个人信息保护方面，《民法典（草案）》是在《民法总则》基础上的延伸，整体的延伸体系仍是以《网络安全法》中的规定作为主线向外扩展，融入了《信息安全技术 个人信息安全规范》的相关内容，从法律层面上进一步完善了个人信息保护的权利义务体系，为个人信息主体依法维权、企业合规措施的落地提

供了明确的指导意见。[21]

《民法典（草案）》全文参见：

http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/node_35174.htm

2. 最新《App 违法违规收集使用个人信息行为认定方法》简要对比分析

从整体来看，2019 年 12 月 30 日公布的正式生效版《App 违法违规收集使用个人信息行为认定方法》（以下简称“《认定方法》”）对了 2019 年 5 月 5 日的征求意见稿（以下简称“《征求意见稿》”）做了较大幅度的更改。首先，《认定方法》删除了原有的“七、侵犯未成年人在网络空间合法权益的情形”的规定，结合上文第一部分对未成年人网络保护新规解读的探讨，笔者认为《认定方法》普适于各类 App 运营方，同时保护各类个人信息主体。对于特殊类别的保护人群，将由特殊法律与部门规章进行特别保护即可。而其他六条则在具体行为认定情形的层面上做出了或多或少的修改，下文将做具体介绍。

1. 可被认定为“未公开收集使用规则”的行为

首先，《认定方法》删除了“App 中没有用户协议”或“用户协议没有收集使用规则”这一行为属于“未公开收集使用”的情形，明确要求 App 必须有隐私政策。同时，它强调和明确了隐私政策中包含的收集使用规则应是针对个人信息的收集使用规则。其次，《认定方法》强调了 App 通知用户阅读隐私政策应在**首次运行时**，同时删除了之前 App 可以通过链接等方式通知的选项；再次，它排除了将隐私政策链接无效或文本无法正常显示的情形归为未公开收集使用规则的行为。但相比于《征求意见稿》，《认定方法》扩大了对隐私政策等使用规则难以访问的范围，只将“多于 4 次点击才能访问隐私政策”的情形作为其中一个例子。此外，《认定方法》删除了之前征求意见稿的“其他情形”这一兜底条款，改为“难以阅读隐私政策等收集使用规则”这一情形，并且进行了相应的举例说明。因此，App 的开发者应当制定单独的隐私政策，并且以在产品设计上通过合理的方式给予用户直接且方便的访问途径，使得用户能够快速的找到并且清晰明确的了解该 App 收集、

[21] 作者：孟洁、陈子谦，孟洁律师团队律师。

使用用户个人信息以及所采取的保护措施等内容。

2. 可被认定为“未明示收集使用个人信息的目的、方式和范围”的行为

《认定方法》与《征求意见稿》相比，对这一情形的规定作了较大的修改，不光通过举例等方式对原有条文进行了更准确的解释和说明，在条文篇幅和整体结构上也形成了成体系的条文规定：

- 收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等。（《认定方法》第二节第 2 条）

- 有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。（《认定方法》第二节第 4 条）

- 在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解。（《认定方法》第二节第 3 条）

此外，《认定方法》在原有基础上还新增了一个情形：

- 未逐一列出 App(包括委托的第三方或嵌入的第三方代码、插件)收集使用个人信息的目的、方式、范围等。（《认定方法》第二节第 1 条）

这说明我国目前已经意识到了第三方主体对于 App 收集个人信息活动的比重逐渐加大，另有在实践中 SDK 隐瞒收集个人信息的问题泛滥。为在立法保护层面上与实践同步，《认定方法》明确指出违规行为的形态，有利于对 App 开发者收集个人信息活动的全面保护。此规定也更好的帮助了 SDK 的提供方履行合规义务，多数的运营商在收集用户个人信息时，无法直接从用户处取得授权，需要请求 App 的开发者进行协助，而《认定方法》从监管的要求上强制要求 App 开发者履行此项告知义务，对于 SDK 提供方履行合规义务、App 开发者降低合规风险以及用户行使知情权等多个维度起到了良好的规制和帮助作用。

3. 可被认定为“未经用户收集使用个人信息”的行为

首先，《认定方法》在这一类别下针对“打开可收集个人信息权限”这一情形新增了以下几类违规行为：

- 征得用户同意前就打开可收集个人信息的权限；
- 用户明确表示不同意后，打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；
- 实际打开的可收集个人信息权限超出用户授权范围；以及
- 未经用户同意更改其设置的可收集个人信息权限状态，如 App 更新时自动将用户设置的权限恢复到默认状态。

其次，在涉及用户使用或者同意方面会被认定为“未经用户收集使用个人信息”的行为，《认定方法》也另外做出了补充，新增了：

- 以默认选择同意隐私政策等非明示方式征求用户同意；
- 以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；
- 未向用户提供撤回同意收集个人信息的途径、方式；
- 违反其所声明的收集使用规则，收集使用个人信息；以及
- 利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项。

2019 年我国对于 App 违法违规收集个人信息的监管力度不断加强，为了更好地规制监管行动中所发现的违法违规情形以及为企业提供明确性的指导意见，《认定方法》在原《征求意见稿》的基础上，重点从用户行为的角度补充了 App 开发者存在违规收集个人信息的数类情形。明确要求 App 开发者不得通过默认勾选隐私政策等非明示的方式征求用户授权同意，充分保障用户自主选择的权利。同时，由于此前部分 App 开发者利用产品更新的契机通过技术手段在 App 更新后自动将未获得用户授权的权限开启或者直接将用户选择的权限状态恢复到默认状态，并且直接收集用户信息。这些都属于未经用户同意的违规收集情形，侵犯了用户的知

情权。《认定方法》在进一步保障用户主体权益的同时也对 App 开发者在隐私产品设计上提出了更严格的要求，要求 App 开发者应当通过合理的隐私产品设计履行合法合规收集个人信息的义务，并赋予用户合理的行权途径。同时，本条款在原《征求意见稿》规定的基础上，要求 App 开发者应当为用户提供“撤回同意”的途径和方式，并且要给予用户可通过其画像向其个性化展示与非基于其画像进行普通广告展示的选项，充分保障了用户对自身个人信息的控制权。

4. 可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”的行为

与上文类似，《认定方法》同样在这一类别下针对“打开可收集个人信息的权限”这一情形新增了收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能；以及要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用这些行为。其次，《认定方法》也新增了将仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息这一行为认定为违反必要原则，收集与其提供的服务无关的个人信息的情形。上述修改更加严格落实了《网络安全法》的必要性原则，对 App 肆意的收集以及滥用用户个人信息，导致用户个人信息甚至隐私被泄露的违规乱象起到了针对性地规制作用。

5. 可被认定为“未经同意向他人提供个人信息”的行为

《认定方法》并未对这一类别进行太大的改动。首先，这两条在实质上并未做太大的改动：“既未经用户同意，也未做匿名化处理，App 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息”，以及“既未经用户同意，也未做匿名化处理，数据传输至 App 后台服务器后，向第三方提供其收集的个人信息”。但新增了“App 接入第三方应用，未经用户同意，向第三方应用提供个人信息”这一情形，体现了监管机关对于平台类 App 以及集成了多个第三方服务 App 在个人信息共享方面合规性的监管力度，相应 App 的开发者应当予以重视。

6. 可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”的行为

《认定方法》首先将“未公布投诉、举报方式等信息”这一类别融合到了第六

节中，与原有的“未按法律规定提供删除或更正个人信息功能”并列，一同进行了规定。其次，具体规定层面上，现行版本新增了两个情形：为更正、删除个人信息或注销用户账号设置不必要或不合理条件；以及未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理的。与此同时，《认定方法》也在保留的行为情形中进行更准确的解释或说明：强调未提供更正、删除个人信息及注销用户账号功能应为“有效的功能”；将人工处理中增加“承诺时限不得超过 15 个工作日”这一时限规定；以及在更正、删除个人信息或注销用户账号等用户操作已执行完毕这一行为上，新增了“但 App 后台并未完成的”这一前提条件，明确了 App 开发者应当在前端和后端同时履行相应的更改或删除义务。企业应当严格依照法律法规要求，响应用户所提出的请求，真正落实对用户个人信息的更正或删除的处理行为。

总体来看，《认定方法》的修改结合了当下监管中发现的 App 违法违规的具体情形，从原则性要求及实践性要求两个维度完善了 App 开发者保障用户个人信息安全所应承担的合规义务。同时《认定方法》更注重于落地性以及行为的有效性层面，对组织提供了明确的合规指引，有利于组织层面对具体措施的落实与实施；同时也体现了现在国家无论在立法还是执法层面上均注重日新月异的科学技术发展，这进一步也确保了对最新科学技术的有效运用与合规管理。[22]

《App 违法违规收集使用个人信息行为认定方法》全文参见

http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm

3.《中国人民银行金融消费者权益保护实施办法》2019 与 2016 版消费者金融信息保护部分简要对比分析

2019 年 12 月 27 日，中国人民银行为进一步规范金融机构经营行为，切实保护金融消费者合法权益起草了《金融消费者权益保护实施办法》，并公开对外征求意见（以下简称“2019 版《征求意见稿》”）。2019 版《征求意见稿》包括 7 章 69 条，对金融机构行为规范、消费者金融信息保护、金融消费争议解决、监督与管理机制等做出了明确规定。

相较于 2016 版《实施办法》的《金融消费者权益保护实施办法》（以下简称

[22] 作者：孟洁、王程，孟洁律师团队律师。

“2016 版《实施办法》”），2019 版《征求意见稿》的消费者金融信息保护部分条款，在内容本身以及条款的排序上，均发生了较大变化。以下，我们将列出 2019 版《征求意见稿》存在的八大变化：

1. 将个人金融信息明确为消费者金融信息

2019 版《征求意见稿》的一个变化是术语变化：2016 版《实施办法》用词为“个人金融信息”，2019 版《征求意见稿》变更为“消费者金融信息”。这一变化精准了法规的保护群体定义，更加有利于金融机构在实践工作中的落实。

2. 收集、使用消费者金融信息应当征得消费者的明示同意。

《征求意见稿》明确要求金融机构在收集、使用消费者金融信息前应当征得消费者的明示同意，意味着无论是在线上还是线下，金融机构均应当在消费者通过书面、口头等方式主动做出纸质或电子形式的声明，或者自主做出肯定性动作后，方可收集、使用消费者的金融信息。

3. 删除了“至少每半年排查一次个人金融信息安全隐患”的要求

2016 版《实施办法》要求金融机构应当严格落实国家网络安全和信息技术安全有关规定，采取有效措施确保个人金融信息安全，至少每半年排查一次个人金融信息安全隐患。2019 版《征求意见稿》则删除了此规定，从而减少了金融机构的此项义务。

4. 信息安全事件 72 小时告知金融消费者

2019 版《征求意见稿》要求金融机构在确认信息发生泄漏、毁损、丢失等安全事件时，应当在 72 小时以内采取补救措施并告知金融消费者。但值得注意的是，2019 版《征求意见稿》相较于 2016 版《实施办法》删去了发生安全事件向有关主管部门报告的义务。

2019 版《征求意见稿》删除向主办部门报告义务的原因以及目的尚不明确。笔者认为 2019 版《征求意见稿》在发生对消费者金融信息风险极高的安全事件时，增强了对消费者的报告义务，却同时降低了向主管部门的报告义务，这一点不利于

提高金融机构的安全责任意识。虽然 2019 版《征求意见稿》加强了金融机构对金融消费者的保护责任，但笔者认为保留金融机构向主管部门报告的义务则有助于落实金融机构对消费者保护责任的实施。

5. 将消费者金融信息用于营销，需要提供拒绝权

2016 版《实施办法》要求金融机构不得将金融消费者授权或者同意其个人金融信息可用于营销作为与金融消费者建立业务关系的先决条件，但该业务关系的性质决定需要预先做出相关授权或者同意的除外。而 2019 版《征求意见稿》则删除这一例外情景，并明确要求金融机构向消费者提供自主选择是否同意将金融信息用于营销的目的。消费者不同意将其个人信息用于营销的，金融机构不得因此拒绝提供金融产品或服务，**即需要给予消费者对其金融个人信息用于营销时的拒绝权。**

6. 外包服务结束时，需要外包服务提供商删除金融信息

2016 版《实施办法》和 2019 版《征求意见稿》均对金融机构将其部分服务外包的要求进行规定，但 2019 版《征求意见稿》额外要求合作关系终止后，金融机构应当监督外包服务供应商及时销毁从金融机构获取的消费者金融信息，从而避免金融信息被第三方非法、超期持有。

7. 增加了对消费者金融信息的权利保护机制

2019 版《征求意见稿》相较于 2016 版《实施办法》新增加了第三十三条、第三十六条关于消费者对其金融信息的权利主张，包括消费者对其金融信息的删除权、更正权以及将个人信息转移至指定机构的权利，与《网络安全法》、《信息安全技术 个人信息安全规范（征求意见稿）》（10.22 版）的规定基本保持一致。

值得重点关注的是，《个人信息安全规范（征求意见稿）》第 7.14 条所规定的获取个人信息副本权包含了两种情形，即直接向个人信息主体提供副本，或者将副本传输给个人信息主体指定的任何第三方。2019 版《征求意见稿》第三十条仅规定了第二种情形，即将其金融信息转移至金融消费者指定的其他金融机构，即并非完整意义上的获取个人信息副本权。

8. 跨境合规性要求趋于完善

《征求意见稿》在《实施办法》规定的基础上，对消费者金融信息可以出境的情形进行了体系化的规定，明确了消费者金融信息由于跨境业务出境时应当满足的具体条件，删除了《实施办法》中“除法律法规及中国人民银行另有规定外，金融机构不得向境外提供境内个人金融信息。”的表述，详细列出了消费者金融数据可以出境的前提条件，为公司在处理跨境业务中如何保证消费者金融数据出境的合规性提供了清晰的指引，也保证了国家重要利益与安全。[23]

2016 版的《金融消费者权益保护实施办法》，2019 版在消费者金融信息保护部分条款对比如下：

2016 版	**2019 版**
第三章 ~~个人~~金融信息保护	**第三章 消费者金融信息保护**
第二十七条 本办法所称个人金融信息，是指金融机构通过开展业务或者其他渠道获取、加工和~~保存~~的个人信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他~~反映特定个人某些情况的信息~~。	**第二十七条** 本办法所称消费者金融信息，是指金融机构通过开展业务或者其他合法渠道获取、加工和存储的消费者信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或服务相关的信息。
~~第二十八条第一款~~ ~~金融机构应当严格落实国家网络安全和信息技术安全有关规定，采取有效措施确保个人金融~~	**删除此条款**

[23] 作者：孟洁、张淑怡，孟洁律师团队律师。

~~信息安全，至少每半年排查一次个人金融信息安全隐患。~~	
第二十八条第二款 收集个人金融信息时，应当遵循合法、合理、必要原则，按照法律法规要求和业务需要收集个人金融信息，不得收集与业务无关的信息或者采取不正当方式收集信息，不得非法存储个人金融信息；应当采取符合国家档案管理和电子数据管理规定的措施，妥善保管所收集的个人金融信息，防止信息遗失、毁损、泄露或者篡改。在发生或者可能发生个人金融信息遗失、毁损、泄露或者篡改等情况时，应当立即采取补救措施，及时告知用户并向~~有关主管部门报告~~。 金融机构及其相关工作人员应当对业务过程中知悉的个人金融信息予以保密，不得非法复制、~~非法存储、非法使用~~、向他人出售或者以其他非法形式泄露个人金融信息。	**第二十八条第一款** 金融机构收集、使用消费者金融信息，应当遵循合法、正当、必要原则，经金融消费者明示同意。金融机构不得收集与业务无关的消费者金融信息，不得采取不正当方式收集信息，不得变相强制收集消费者金融信息。 **第三十二条第一款、第二款** 金融机构应当按照国家档案管理和电子数据管理规定，采取技术措施和其他必要措施，妥善保管和存储所收集的消费者金融信息，防止信息遗失、毁损、泄露或者篡改。 金融机构及其工作人员应当对消费者金融信息严格保密，不得泄露或者非法向他人提供。在确认信息发生泄漏、毁损、丢失时，金融机构应当在 72 小时以内采取补救措施并告知金融消费者。
第二十九条 金融机构应当建立个人金融信息数据库分级授权管理机制，根据个人金融信息的重要性、敏感	**第三十一条第一款** 金融机构应当建立以分级授权为核心的消费者金融信息使用管理制度，根据消费者

度及业务开展需要，在不影响其履行反洗钱等法定义务的前提下，合理确定本机构员工调取信息的范围、权限~~及程序~~。	金融信息的重要性、敏感度及业务开展需要，在不影响其履行反洗钱等法定义务的前提下，合理确定本机构员工调取信息的范围、权限。
第三十条 金融机构通过格式条款取得个人金融信息书面使用授权或者同意的，应当在条款中明确该授权或者同意所适用的向他人提供个人金融信息的范围和具体情形，应当在协议的醒目位置使用通俗易懂的语言明确向金融消费者提示该授权或者同意的可能后果。 ~~金融机构不得以概括授权的方式，索取与金融产品和服务无关的个人金融信息使用授权或者同意。~~	**第二十九条** 金融机构应当履行《中华人民共和国消费者权益保护法》规定的明示义务，并保留有关证明资料。 金融机构通过格式条款取得消费者金融信息收集、使用同意的，应当在条款中明确收集的目的、方式、内容和使用范围，并在协议中以显著方式尽可能通俗易懂地向金融消费者提示该同意的可能后果。
没有规定	**第三十条** 金融机构应当按照法律法规的规定和双方约定的用途使用消费者金融信息，不得超出范围使用。
第三十一条 金融机构不得将金融消费者授权或者同意其将个人金融信息用于~~营销、~~对外提供等作为与金融消费者建立业务关系的先决条件，但该业务	**第二十八条第二款、第三款** 金融机构不得将金融消费者同意其将金融信息用于对外提供作为与金融消费者建立业务关系的先决条件，但该业务关系的性质决定需要预先同意的除外。

关系的性质决定需要预先做出相关授权或者同意的除外。	金融机构收集消费者金融信息用于营销、用户体验改进或者市场调查的，应当以适当方式供金融消费者自主选择是否同意金融机构将其金融信息用于上述目的。金融消费者不同意的，金融机构不得因此拒绝提供金融产品或服务。
第三十二条 金融机构应当建立个人金融信息使用管理制度。因监管、审计、数据分析等原因需要使用个人金融信息数据的，应当严格内部授权审批程序，采取有效技术措施，确保信息在内部使用及对外提供等流转环节的安全，防范信息泄露风险。	**第三十一条第二款** 金融机构应当严格落实信息使用授权审批程序，采取有效技术措施，确保消费者金融信息安全。 **第三十二条第一款** 金融机构应当按照国家档案管理和电子数据管理规定，采取技术措施和其他必要措施，妥善保管和存储所收集的消费者金融信息，防止信息遗失、毁损、泄露或者篡改。
第三十三条 在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，金融机构不得向境外提供境内个人金融信息。 境内金融机构为处理跨境业务且经当事人授权，向境外机构(含总公司、母公司或者分公司、	**第三十四条** 在中国境内收集的消费者金融信息的存储、处理和分析应当在中国境内进行。因业务需要，确需向境外提供消费者金融信息的，应当同时符合以下条件： （一）为处理跨境业务所必需； （二）经金融消费者书面授权；

子公司及其他为完成该业务所必需的关联机构)传输境内收集的相关个人金融信息的，应当符合法律、行政法规和相关监管部门的规定，并通过签订协议、现场核查等有效措施，要求境外机构为所获得的个人金融信息保密。	（三）信息接收方为完成该业务所必需的关联机构（含总公司、母公司或者分公司、子公司等）； （四）通过签订协议、现场核查等有效措施，要求境外机构为所获得的消费者金融信息保密； （五）符合法律法规和其他相关监管部门的规定。
第三十四条 金融机构保护消费者个人金融信息安全的义务不因其与外包服务供应商合作而转移、减免。 金融机构应当充分审查、评估外包服务供应商保护个人金融信息的能力，在相关协议中明确外包服务供应商保护个人金融信息的职责和保密义务，并采取必要措施保证外包服务供应商履行上述职责和义务。	**第三十五条** 金融机构保护消费者金融信息安全的义务不因其与外包服务供应商合作而转移、减免。 金融机构应当充分审查、评估外包服务供应商保护消费者金融信息的能力，在相关协议中明确外包服务供应商保护消费者金融信息的职责和保密义务，并采取必要措施监督外包服务供应商履行上述职责和义务。合作关系终止后，金融机构应当监督外包服务供应商及时销毁从金融机构获取的消费者金融信息。
没有规定	**第三十三条** 金融消费者发现金融机构违反法律法规、监管规定或者双方的约定收集、使用其金

	融信息的，有权要求金融机构停止使用并删除前述金融信息；发现金融机构收集、存储的消费者金融信息有错误的，有权要求金融机构予以更正。金融机构应当采取措施予以删除或者更正。法律、行政法规另有规定的除外。
没有规定	**第三十六条** 鼓励金融机构在技术可行的前提下，基于金融消费者的请求，将其金融信息转移至金融消费者指定的其他金融机构。

中国人民银行《金融消费者权益保护实施办法（征求意见稿）》全文参见：

http://www.gov.cn/gongbao/content/2017/content_5213211.htm

4. 未成年人网络保护系列规定（2019 年 10 月 1 日/11 月 1 日/11 月 5 日/11 月 13 日）

2019 年不容忽略的一个法律热点就是国家加大了对未成年人的保护力度。首先，在儿童个人信息保护方面，国家互联网信息办公室于 8 月 22 日审议通过了《儿童个人信息网络保护规定》，该规定于 10 月 1 日起正式生效。其次，11 月 1 日，由全国人民代表大会常务委员会发布了《未成年人保护法》和《预防未成年人犯罪法》两部法律的修订草案；其中，《未成年人保护法（修订草案）》还设立了“网络保护”专章。紧接着，国家新闻出版署于 11 月 5 日下发了《关于防止未成年人沉迷网络游戏的通知》；教育部办公厅于 11 月 13 日印发了《教育移动互联网应用程序备案管理办法》。下半年来，对未成年人（含儿童）保护方面法律的系列出台，是国家对危害未成年人行为的频频亮剑，体现出对未成年人网络保护的重视和关注。下文我们以《未成年人保护法（修订草案）》中的网络保护专章为分析维度，结合其他未成年人保护相关新规，简要评述未成年人网络保护的合规重点。

1. 明确各方职责与义务

《儿童个人信息网络保护规定》明确了儿童监护人、互联网行业组织、网络运营者各方的职责。《未成年人保护法（修订草案）》进一步明确了国家、学校和家庭在未成年人网络保护方面的义务。根据《未成年人保护法（修订草案）》第五十七条和第五十九条规定，国家保护未成年人依法使用网络的权利，鼓励和支持有利于未成年人健康成长的网络内容的创作和传播，鼓励和支持以未成年人为服务对象、适合未成年人身心发展的技术和产品。

根据《未成年人保护法（修订草案）》第五十八条，家庭和学校应当开展网络安全和网络文明教育，提高未成年人安全合理使用网络的意识和能力，增强未成年人的自我保护意识。《儿童个人信息网络保护规定》第五条规定了监护人的职责，正是对《未成年人保护法（修订草案）》中家庭管教义务的呼应。

值得注意的是，鉴于教育类 App 的受众及使用对象多为未成年人，对于此类 App，教育部新颁布的《教育移动互联网应用程序备案管理办法》要求网络运营者对教育类 App 进行备案，也体现了国家对于网络运营者，关于其与未成年人相关的产品与服务，国家有统一管理的要求。因此，建议相关企业，应当根据该管理办法尽早进行 ICP 以及网络等级保护备案的工作。

2. 上网保护软件

根据《未成年人保护法（修订草案）》第六十条和第六十一条，网络产品和服务提供者、智能终端产品制造者和销售者、为未成年人提供公益性互联网上网服务设施的学习、社区、图书馆等场所的组织需要履行特别的义务。其中，为未成年人提供公益性互联网上网服务设施的场所，例如学校、社区、图书馆、文化馆、青少年宫等，应当安装未成年人上网保护软件。智能终端产品制造者和销售者也应当安装此类软件，或者采用显著方式向用户告知安装渠道和方法。

3. 适龄内容提示

《未成年人保护法（修订草案）》第六十二条禁止利用网络制作、复制、发布、传播含有法律法规禁止内容的信息。对于有可能影响未成年人身心健康的信息，相关组织和个人应当在信息展示前予以提示。根据国家新闻出版署发布的《关于防止未成年人沉迷网络游戏的通知》，在网络游戏场景下，网络游戏企业必须探索适龄

提示制度，根据游戏功能和内容的对抗激烈程度与使用者心里可接受程度等多维度综合进行衡量，做出适合不同年龄段用户的提示。

4. 个人信息保护

《未成年人保护法（修订草案）》第六十三条新增网络产品和服务提供者的义务，即应当提示未成年人用户保护自身个人信息，并对其使用个人信息进行保护性限制。此外，该条还呼应了已生效的《儿童个人信息网络保护规定》，要求依照有关规定收集、使用、保存未成年人个人信息，并经过监护人同意。对于这一点，如此前文章【新规】《儿童个人信息网络保护规定》正式发布和《儿童个人信息保护实证调研篇》及 YOUTUBE 被罚案例解读所述，如何有效识别未成年人以及如何征得监护人同意，是整个合规落地过程中需要思考的问题。目前，很多企业已经结合了自身情况，加大对儿童个人信息的保护力度。例如，不少企业已在隐私政策中增加了未成年人个人信息保护相关条款，或者设置了单独的儿童隐私保护指引。根据我们的调研，对于识别未成年人年龄以及征求监护人同意方面，企业也做出不少努力，目前的操作模式大体上分为以下几种：

1）用户自认。要求用户在注册账号时填写出生年月，如用户填写的年龄小于 14 周岁，则无法注册。

2）要求用户提供年龄证明文件。在实名制要求的前提下（例如游戏行业），用户在创建账号时需提供身份证号码，以此来判断用户年龄。有些情况下，企业还可以要求提供监护人邮箱进行验证，或者根据用户面部特征和使用行为进行综合判断，但采取这类方法的，还是建议谨慎操作，并且需要提前做出个人信息影响评估，不然反而会增加收集用户个人信息的范围。

3）监护人代为创建账号。将儿童的账号与监护人的账号进行关联，如某些产品的用户虽为儿童，但需要监护人通过自己的账号帮助儿童创建儿童账号，这样，监护人就可以通过自身账号对儿童的使用行为进行监控与保护。

5. 家长控制模式

《未成年人保护法（修订草案）》第六十四条要求网络产品和服务提供者避免提供可能诱导未成年人沉迷的内容，并设置相应功能，为监护人预防和干预未成年人沉迷网络提供便利。根据我们的调研，在产品设计方面，目前很多企业都设置了单独的未成年人模式，例如抖音、腾讯、bilibili 等提供了“时间锁”、“儿童/青少年

模式”、“亲子平台”、“成长守护平台”、青少年模式等功能。如前所述，通过这些功能，家长可以查询、控制儿童使用时长，筛选适合儿童阅读的内容，限制儿童充值消费等，实现对儿童使用行为的管理。爱奇艺还专门为儿童设计了儿童版 App，为儿童提供适合儿童阅读和观看的内容。

此外，针对网络游戏场景，《未成年人保护法（修订草案）》第六十五条还做出了特别规定，主要涉及两方面的内容：1）内容管理。即不得让未成年人接触不适宜其接触的游戏或游戏功能；2）时间管理。在该方面，国家新闻出版署在近日发布的《关于防止未成年人沉迷网络游戏的通知》中提到，**每日 22 时至次日 8 时，网络游戏企业不得以任何形式为未成年人提供游戏服务。网络游戏企业在法定节假日向未成年人提供游戏服务每日累计不得超过 3 小时，其他时间每日累计不得超过 1.5 小时。**这一举措也因此与网络游戏中的实名制要求相关。根据教育部于 2007 年 4 月 15 日发布了《关于保护未成年人身心健康实施网络游戏防沉迷系统的通知》，所有网络游戏运营企业必须在其运营的所有网络游戏中，按新闻出版总署及相关组织制定的《网络游戏防沉迷系统实名认证方案》实施实名制认证，而根据《网络游戏防沉迷系统实名认证方案》中的流程示意图，识别成年人及未成年人则是实名认证流程的重要一环。

6. 禁止网络欺凌

《未成年人保护法（修订草案）》第六十六条禁止任何组织和个人通过网络侮辱、诽谤、威胁未成年人或者恶意扭曲、损害未成年人形象。如发现前述情况的，监护人可要求网络信息服务提供者及时删除相关内容。

7. 举报投诉机制

《未成年人保护法（修订草案）》第六十七条要求网络产品和服务提供者结合自身提供未成年人相关服务，通过显著方式公示举报途径和举报方法，并配备与服务规模相适应的专职人员及时受理并处置相关举报。这一点要求可能与《儿童个人信息网络保护规定》要求企业需要确保有员工能够负责处理未成年人保护相关的投诉和举报以及未成年人个人信息保护的相关事宜一脉相承。

综上可见，未成年人网络保护这一话题涉及防沉迷、适龄分级分类、个人信息保护等诸多方面的内容。其中，在儿童个人信息保护方面，《儿童个人信息网络保护规定》已生效 3 月有余，并且对未履行要求规定了明确的罚则。建议相关企业，特别是专门为儿童提供产品与服务或者涉及儿童个人信息处理的企业，以此为契

机，重视未成年人保护这一问题，尽早采取合规举措。[24]

《儿童个人信息网络保护规定》全文参见：

http://www.cac.gov.cn/2019-08/23/c_1124913903.htm

《未成年人保护法（修订草案）》全文参见：

http://www.npc.gov.cn/npc/wcnrbhfxdca/wcnrbhfxdca.shtml

《预防未成年人犯罪法（修订草案）》全文参见：

http://www.npc.gov.cn/npc/yfwcnrfzfxdca/yfwcnrfzfxdca.shtml

《教育移动互联网应用程序备案管理办法》全文参见：

http://www.gov.cn/fuwu/2019-11/27/content_5456067.htm

5.《网络音视频信息服务管理规定》（2019 年 11 月 29 日）简要评析

2019 年 11 月 29 日，国家互联网信息办公室、文化和旅游部、国家广播电视总局联合印发了《网络音视频信息服务管理规定》（以下简称《规定》），以促进网络音视频信息服务健康有序发展，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益。《规定》自 2020 年 1 月 1 日起正式施行，包含以下几个方面的主要内容：

1. 明确网络音视频信息服务提供者的资质要求

《规定》明确网络音视频信息服务提供者是指向社会公众提供网络音视频信息服务的组织或者个人。网络音视频信息服务提供者应当依法取得法律、行政法规

[24] 作者：孟洁、殷坤，孟洁律师团队律师。

要求的相关资质。

2. 明确网络音视频信息服务使用者身份认证要求

网络音视频信息服务提供者应当依照《中华人民共和国网络安全法》的规定，对用户进行基于组织机构代码、身份证件号码、移动电话号码等方式的真实身份信息认证。用户不提供真实身份信息的，网络音视频信息服务提供者不得为其提供信息发布服务。

3. 明确网络音视频信息服务提供者的安全管理主体责任

首先，《规定》明确了信息内容安全管理责任承担的主体为网络音视频信息服务提供者，即谁经营谁负责。其次，《规定》要求网络音视频信息服务提供者建立内部管理制度体系，包括建立健全用户注册、信息发布审核、信息安全管理、应急处置、从业人员教育培训、未成年人保护、知识产权保护等制度。

从技术层面来看，《规定》要求网络音视频信息服务提供者具有与新技术、新应用发展相适应的安全可控的技术保障和防范措施，能有效应对网络安全事件，防范网络违法犯罪活动，并维护网络数据的完整性、保密性和可用性。

4. 明确对基于深度学习、虚拟现实等新技术新应用的要求

1）安全评估要求

网络音视频信息服务提供者基于新技术新应用上线具有媒体属性或者社会动员功能的音视频信息服务，或者调整增设相关功能的，应当按照国家有关规定开展安全评估。

2）标识要求

网络音视频信息服务提供者和网络音视频信息服务使用者利用新技术新应用制作、发布、传播非真实音视频信息的，应当以显著方式予以标识。

3）明确新闻信息管理要求

“深度伪造”音视频不得制作、发布、传播虚假新闻信息。转载音视频新闻信息的，应当依法转载国家规定范围内单位发布的音视频新闻信息。

4）明确违法违规信息管理要求

网络音视频信息服务提供者应当部署应用违法违规音视频以及非真实音视频的鉴别技术，发现音视频信息服务使用者制作、发布、传播法律法规禁止的信息内容的，应当依法依约停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关部门报告。

5）建立辟谣机制

网络音视频信息服务提供者发现网络音视频信息服务使用者利用基于深度学习、虚拟现实等的虚假图像、音视频生成技术制作、发布、传播谣言的，应当及时采取相应的辟谣措施，并将相关信息报主管部门备案。

5. 通过协议明确用户与网络音视频信息服务提供者的权利责任

为了明确双方的权利和义务，《规定》要求服务提供者和用户签订服务协议。除建立下文的投诉机制以外，《规定》要求服务提供者对于违法违规使用服务的用户依法应采取警示整改、限制功能、暂停更新、关闭账号等措施，保存有关记录并向相关部分进行报告。

6. 明确受理投诉举报机制

《规定》要求网络音视频信息服务提供者应当自觉接受社会监督，设置便捷的投诉举报入口，公布投诉、举报方式等信息，及时受理并处理公众投诉举报。

《规定》创设了多项管理制度，及时回应了当前网络音视频信息服务及相关技术发展面临的问题，规定了从事网络音视频信息服务应当遵守的管理要求，为促进网络音视频信息服务健康有序发展提供了重要指引，为保护公民、法人和其他组织

的合法权益，维护国家安全和公共利益提供了有力保障。[25]

《网络音视频信息服务管理规定》全文参见：

http://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm

6. 《网络信息内容生态治理规定》（2019 年 12 月 15 日）简要评析

2019 年 12 月 15 日，国家互联网信息办公室正式发布《网络信息内容生态治理规定》（以下简称“《规定》”），是对 2019 年 9 月 10 日颁布的征求意见稿(我们此前也进行过相关解读)的进一步调整，同时也对具体内容进行了强化与突出，主要呈现出以下几点特征：

1. 强调规制网络信息内容，弘扬社会主义核心价值观

根据《规定》第二条，《规定》以网络信息内容为主要治理对象，这一点与征求意见稿一致。特别地，《规定》在标题及条文的表述中增加了“信息内容”（即《网络**信息内容**生态治理规定》）四个字以示强调，彰显了本次立法对实践中网络信息内容乱象进行整治的核心目的。

此外，《规定》第二条、第五条、第二十六条等强调，《规定》以培育和践行社会主义核心价值观为根本，倡导网络信息内容生产者、网络信息内容服务平台、网络信息内容使用者唱响主旋律，弘扬正能量，反对违法信息，防范和抵制不良信息。我们理解，整治网络信息内容乱象、维护清朗的网络环境、建立良好的网络生态，将有利于建设文明、和谐、自由、平等、诚信、友善的社会风气，是对践行社会主义核心价值观的积极响应。

2. 扩大规制主体范围，增多承担责任主体

根据《规定》第四十一条，“**网络信息内容生产者**”的内涵扩大，不仅指制作网络信息内容的**组织或个人，复制、发布网络信息内容的组织或个人**也将包括在规制范围内。据此，网络信息内容使用者可能更容易转换身份为网络信息内容生产

[25] 作者：孟洁、崔卫红，孟洁律师团队律师。

者，例如，普通网民复制、转发网络信息的行为都可能视为生产网络信息，需要承担网络信息生产者相应的义务。

此外，《规定》第二十一条至第二十五条尽管落入了第四章“网络信息服务使用者”一节，但是规定了**网络信息服务生产者、服务平台及使用者三方**都应承担不侮辱诽谤、散布谣言，不利用网络信息、网络技术侵害他人合法权益、破坏网络生态等责任。这一点改变了征求意见稿只要求网络信息服务生产者承担该部分责任的局面，对网络信息乱象的治理更为全面。

3. 强调网络信息服务平台管理职责，加强行业组织自治力量

《规定》第九条、第十五条要求网络信息服务平台建立网络信息内容生态治理机制，制定本平台**网络信息内容生态治理细则、平台管理规则和平台公约，并完善用户协议**。与征求意见稿相比，《规定》除了要求订立用户协议外，还强调制定平台生态治理细则、平台管理规则、平台公约，重点突出平台对用户行为的监督和管理作用。此外，《规定》还要求平台在重点环节对网络信息内容进行审核、建立应急处置方案、对平台从业人员进行考核，提升整体素质等。

《规定》新增第二十六条，鼓励行业组织发挥服务指导和桥梁纽带作用。与征求意见稿相比，《规定》除了要求建立行业自律机制外，第二十七条还鼓励行业组织制定网络信息内容生态治理行业规范和自律公约、内容审核标准细则，指导会员单位建立健全服务规范。这一规定进一步细化了行业组织制定自治规范的要求，并强调其对会员单位的指导作用。

这一动向也体现了弱化政府直接监管的思路，符合政府一直以来倡导的“放管服”的监管目标--要求网络信息内容平台和行业组织承担更多的责任，缓解政府监管压力的同时，取得更高效的监管效果。

4. 建立用户账号信用管理制度，与建构社会信用体系理念相一致

目前，我国正在加快社会信用体系的建设。《国务院办公厅关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见》（2019.07.09）指出，国家要以依法依规、改革创新、协同共治为基本原则，以加强信用监管为着力点，创新监管理念、监管制度和监管方式，不断提升监管能力和水平。关于个人信用，《国务院办公厅关于加强个人诚信体系建设的指导意见》（2016.12.23）等法律文件亦强调了个人诚信体系建设和个人信用水平提高等。

值得注意的是，《规定》第十五条、第二十九条规定，网络信息内容服务平台应当建立**用户账号信用管理制度**，行业组织应当推动**行业信用评价体系建设**。针对用户和企业建立信用管理及评价制度，体现了立法对社会信用体系建设方针的贯彻。同时提及用户账号信用、行业信用评价体系的建设，有利于推动监管机关的监管水平，促进网络信息内容治理效率的提升。[26]

《网络信息内容生态治理规定》（正式稿）与《网络生态治理规定》（征求意见稿）对比分析：

网络生态治理规定 **（征求意见稿）**	**网络信息内容生态治理规定** **（正式发布稿）**
第一章 总则	**第一章 总则**
第一条 为了~~加强网络生态治理，维护良好网络秩序~~，保障公民、法人和其他组织的合法权益，~~构建天朗气清的网络空间~~，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》~~《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》~~，制定本规定。	**第一条** 为了营造良好网络生态，保障公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《互联网信息服务管理办法》等法律、行政法规，制定本规定。
第二条 中华人民共和国境内的网络生态治理，适用本规定。~~法律、行政法规另有规定的，遵照其规定~~。	**第二条** 中华人民共和国境内的网络信息内容生态治理活动，适用本规定。
本规定所称网络生态治理，是指政府、企业、社会、网民等主体，以网络信息内容为主要治理对象，以~~营造文明健康的良好生态为目标~~，开展的弘扬正能量、处置违法和不良信息等相关活动。	本规定所称网络信息内容生态治理，是指政府、企业、社会、网民等主体，以培育和践行社会主义核心价值观为根本，以网络信息内容为主要治理对象，以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，开展的弘扬正能量、处置违法和不良信息等相关活动。
第三条 国家网信部门负责统筹协调网络生态治理和相关监督管理工作。~~国家新闻出版部门和国务院教育、电信、公安、文化、市场监督~~	**第三条** 国家网信部门负责统筹协调全国网络信息内容生态治理和相关监督管理工作，各有

[26] 作者：孟洁、颜婷婷，孟洁律师团队律师。

~~管理、广播电视等~~有关主管部门依据各自职责做好网络生态治理工作。	关主管部门依据各自职责做好网络信息内容生态治理工作。
地方~~各级~~网信部门依据职责负责统筹协调本行政区域内网络生态治理和相关监督管理工作。地方~~各级新闻出版部门和教育、电信、公安、文化、市场监督管理、广播电视等~~有关主管部门依据各自职责做好本行政区域内网络生态治理工作。	地方网信部门负责统筹协调本行政区域内网络信息内容生态治理和相关监督管理工作，地方各有关主管部门依据各自职责做好本行政区域内网络信息内容生态治理工作。
第二章 网络信息内容生产者	**第二章 网络信息内容生产者**
第四条 网络信息内容生产者应当遵守法律法规，遵循公序良俗，~~加强网络文明建设~~。	**第四条** 网络信息内容生产者应当遵守法律法规，遵循公序良俗，不得损害国家利益、公共利益和他人合法权益。
第五条 鼓励制作含有下列内容的信息：	**第五条** 鼓励网络信息内容生产者制作、复制、发布含有下列内容的信息：
（一）宣传习近平新时代中国特色社会主义思想，全面准确生动解读中国特色社会主义道路、理论、制度、文化的；	（一）宣传习近平新时代中国特色社会主义思想，全面准确生动解读中国特色社会主义道路、理论、制度、文化的；
（二）宣传党的理论路线方针政策和中央重大决策部署的；	（二）宣传党的理论路线方针政策和中央重大决策部署的；
（三）展示经济社会发展亮点，反映人民群众伟大奋斗和火热生活的；	（三）展示经济社会发展亮点，反映人民群众伟大奋斗和火热生活的；
（四）弘扬社会主义核心价值观，宣传优秀道德文化和时代精神，充分展现中华民族昂扬向上精神风貌的；	（四）弘扬社会主义核心价值观，宣传优秀道德文化和时代精神，充分展现中华民族昂扬向上精神风貌的；
（五）有效回应社会关切，解疑释惑，析事明理，有助于引导群众形成共识的；	（五）有效回应社会关切，解疑释惑，析事明理，有助于引导群众形成共识的；
（六）有助于提高中华文化国际影响力，向世界展现真实立体全面的中国的；	（六）有助于提高中华文化国际影响力，向世界展现真实立体全面的中国的；
（七）其他含有讴歌真善美、促进团结稳定等~~积极内容的~~。	（七）其他讲品味讲格调讲责任、讴歌真善美、促进团结稳定等的内容。

第六条 ~~禁止制作~~含有下列内容的违法信息：	**第六条** 网络信息内容生产者不得制作、复制、发布含有下列内容的违法信息：
（一）~~违反~~宪法所确定的基本原则的；	（一）反对宪法所确定的基本原则的；
（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；	（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
（三）损害国家荣誉和利益的；	（三）损害国家荣誉和利益的；
（四）歪曲、丑化、亵渎、否定英雄烈士~~及其~~事迹和精神~~的~~；	（四）歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的；
（五）宣扬恐怖主义、极端主义，~~煽动民族仇恨、民族歧视，破坏民族团结~~的；	（五）宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；
	（六）煽动民族仇恨、民族歧视，破坏民族团结的；
（六）破坏国家宗教政策，宣扬邪教和封建迷信的；	（七）破坏国家宗教政策，宣扬邪教和封建迷信的；
（七）散布~~虚假信息~~，扰乱经济秩序和社会秩序的；	（八）散布谣言，扰乱经济秩序和社会秩序的；
（八）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；	（九）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
（九）侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；	（十）侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；
（十）含有法律、行政法规禁止的其他内容的。	（十一）法律、行政法规禁止的其他内容。
第七条 ~~不得制作~~含有下列内容的不良信息：	**第七条** 网络信息内容生产者应当采取措施，防范和抵制制作、复制、发布含有下列内容的不良信息：
（~~八~~）使用夸张标题，内容与标题严重不符的；	（一）使用夸张标题，内容与标题严重不符的；

（~~四~~）~~过度~~炒作~~明星~~绯闻、~~娱乐八卦~~的；	（二）炒作绯闻、丑闻、劣迹等的；
~~（三）宣扬炫富拜金、奢靡腐化等生活方式的；~~	
（~~六~~）~~调侃恶搞~~自然灾害、重大事故等灾难的；	（三）不当评述自然灾害、重大事故等灾难的；
（~~二~~）带有性暗示、性挑逗、~~性诱惑~~的；	（四）带有性暗示、性挑逗等易使人产生性联想的；
（~~三~~）展现血腥、惊悚等致人身心不适的；	（五）展现血腥、惊悚、残忍等致人身心不适的；
（~~七~~）煽动人群歧视、地域歧视等的；	（六）煽动人群歧视、地域歧视等的；
（~~五~~）~~使用粗俗语言、展示恶俗行为、宣扬低俗内容的~~；	（七）宣扬低俗、庸俗、媚俗内容的；
（~~九~~）~~对未成年人身心健康造成不良影响的~~；	（八）可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等的；
（~~十~~）其他~~含有危害社会公德等破坏网络生态内容的~~。	（九）其他对网络生态造成不良影响的内容。
第三章 网络信息内容服务平台	**第三章 网络信息内容服务平台**
第八条 网络信息内容服务平台应当~~切实~~履行网络生态治理主体责任，加强本平台生态治理工作，积极培育向上向善的网络文化。	**第八条** 网络信息内容服务平台应当履行信息内容管理主体责任，加强本平台网络信息内容生态治理，培育积极健康、向上向善的网络文化。
第九条 网络信息内容服务平台应当建立网络生态治理机制，健全信息发布审核、跟帖评论审核、版~~（页）~~面生态管理、实时巡查、应急处置、网络谣言~~处置、网络黑产线索~~处置等制度。网络信息内容服务平台应当设立网络生态治理负责人，配备与服务规模相适应的工作人员，~~并~~加强~~教育~~培训。	**第九条** 网络信息内容服务平台应当建立网络信息内容生态治理机制，制定本平台网络信息内容生态治理细则，健全用户注册、账号管理、信息发布审核、跟帖评论审核、版面页面生态管理、实时巡查、应急处置和网络谣言、黑色产业链信息处置等制度。 网络信息内容服务平台应当设立网络信息内容生态治理负责人，配备与业务范围和服务规模

	相适应的专业人员，加强培训考核，提升从业人员素质。
第十条 网络信息内容服务平台应当加强对其用户发布信息的管理，~~发现法律、行政法规禁止发布或者传输的信息的~~，应当立即停止传输该信息，采取消除等处置措施，~~防止信息扩散，~~保存有关记录，并向有关主管部门报告。	**第十条** 网络信息内容服务平台不得传播本规定第六条规定的信息，应当防范和抵制传播本规定第七条规定的信息。 网络信息内容服务平台应当加强信息内容的管理，发现本规定第六条、第七条规定的信息的，应当依法立即采取处置措施，保存有关记录，并向有关主管部门报告。
网络信息内容服务平台对网信部门和有关部门依法实施的监督检查，应当予以配合。	
第十一条 网络信息内容服务平台禁止~~复制、发布、~~传播本规定第六条规定的信息。	
第十二条 网络信息内容服务平台不得~~复制、发布、传播~~本规定第七条规定的信息。	
第十三条 ~~网络信息内容服务平台应当加强以人工编辑、机器算法等方式推荐、呈现信息环节的管理，营造积极健康~~的版（页）面生态~~，包括但不限于以下~~重点环节（服务类型、位置板块）：	**第十一条** 鼓励网络信息内容服务平台坚持主流价值导向，优化信息推荐机制，加强版面页面生态管理，在下列重点环节（包括服务类型、位置版块等）积极呈现本规定第五条规定的信息：
（一）互联网新闻信息服务首页~~（屏）~~、弹窗和重要新闻信息内容页面等；	（一）互联网新闻信息服务首页首屏、弹窗和重要新闻信息内容页面等；
（二）互联网用户公众账号信息服务~~文章列表标题、封面图及~~精选、热搜等；	（二）互联网用户公众账号信息服务精选、热搜等；
（三）微博客信息服务热门推荐、榜单类及基于地理位置的信息服务板块等；	（三）博客、微博客信息服务热门推荐、榜单类、弹窗及基于地理位置的信息服务版块等；
（四）互联网信息搜索服务热搜词、热搜图及默认搜索等；	（四）互联网信息搜索服务热搜词、热搜图及默认搜索等；
（五）互联网论坛社区服务首页~~（屏）~~、榜单类等；	（五）互联网论坛社区服务首页首屏、榜单类、弹窗等；
（六）互联网音视频服务首页~~（屏）~~、发现、精选、榜单类~~、封面~~、弹窗等；	（六）互联网音视频服务首页首屏、发现、精选、榜单类、弹窗等；

	（七）互联网网址导航服务、浏览器服务、输入法服务首页首屏、榜单类、皮肤、联想词、弹窗等；
（七）网络~~文学（~~动漫~~）~~服务首页~~（~~屏~~）~~、精选、榜单类、~~封面~~等；	（八）数字阅读、网络游戏、网络动漫服务首页首屏、精选、榜单类、弹窗等；
（八）网络游戏~~服务场景、角色、道具及公共聊天室~~等；	
（九）生活服务平台首页~~（~~屏~~）~~、热门推荐等；	（九）生活服务、知识服务平台首页首屏、热门推荐、弹窗等；
（十）电子商务平台首页~~（~~屏~~）~~、推荐区~~、商品列表封面~~等；	（十）电子商务平台首页首屏、推荐区等；
（十一）移动智能终端预置应用软件首屏、推荐区~~、弹窗~~等；	（十一）移动应用商店、移动智能终端预置应用软件和内置信息内容服务首屏、推荐区等；
（十二）以未成年人为服务对象的网络信息内容~~服务~~。	（十二）专门以未成年人为服务对象的网络信息内容专栏、专区和产品等；
	（十三）其他处于产品或者服务醒目位置、易引起网络信息内容服务使用者关注的重点环节。
	网络信息内容服务平台不得在以上重点环节呈现本规定第七条规定的信息。
第十五条 网络信息内容服务平台采用个性化算法推荐技术推送信息的，应当~~建立体现主流价值导向~~的推荐模型，建立健全人工干预机制~~，建立~~用户自主选择机制。	**第十二条** 网络信息内容服务平台采用个性化算法推荐技术推送信息的，应当设置符合本规定第十条、第十一条规定要求的推荐模型，建立健全人工干预和用户自主选择机制。
第十四条 鼓励网络信息内容服务平台开发适合未成年人使用的模式~~。~~ ~~网络信息内容服务平台提供网络游戏、网络文学、网络动漫、网络直播、网络音视频及其他各类服务时，应当采取措施防止未成年人接触违法和不良信息。~~	**第十三条** 鼓励网络信息内容服务平台开发适合未成年人使用的模式，提供适合未成年人使用的网络产品和服务，便利未成年人获取有益身心健康的信息。

第十六条 网络信息内容服务平台应当对本平台~~推送或者展示的广告内容和位置加强审核监看，~~对发布违法广告的，应当予以~~制止~~。	**第十四条** 网络信息内容服务平台应当加强对本平台设置的广告位和在本平台展示的广告内容的审核巡查，对发布违法广告的，应当依法予以处理。
第十七条 网络信息内容服务平台应当完善用户~~服务~~协议，明确用户相关权利义务，并依法依约履行相应管理职责。 网络信息内容服务平台应当建立用户账号信用~~档案~~，根据用户账号的信用~~等级~~提供相应~~的~~服务。	**第十五条** 网络信息内容服务平台应当制定并公开管理规则和平台公约，完善用户协议，明确用户相关权利义务，并依法依约履行相应管理职责。 网络信息内容服务平台应当建立用户账号信用管理制度，根据用户账号的信用情况提供相应服务。
第十八条 网络信息内容服务平台应当在~~首页、账号页面、信息内容页面等~~显著位置设置便捷投诉举报入口，公布投诉举报方式，~~细化网络生态违法和不良信息举报分类，~~及时受理处置公众投诉举报并反馈处理结果。	**第十六条** 网络信息内容服务平台应当在显著位置设置便捷的投诉举报入口，公布投诉举报方式，及时受理处置公众投诉举报并反馈处理结果。
第十九条 网络信息内容服务平台应当编制网络生态治理工作年度报告，包括网络生态治理工作情况、网络生态治理负责人履职情况、社会评价情况等内容。	**第十七条** 网络信息内容服务平台应当编制网络信息内容生态治理工作年度报告，年度报告应当包括网络信息内容生态治理工作情况、网络信息内容生态治理负责人履职情况、社会评价情况等内容。
第四章 网络信息内容服务使用者	**第四章 网络信息内容服务使用者**
第二十条第二款 网络信息内容服务使用者应当文明健康使用网络，按照法律法规的要求和用户协议约定，切实履行相应义务，在以发帖、回复、留言、弹幕等形式参与网络活动时，~~积极弘扬正能量，~~不得~~复制、~~发布~~、传播违法~~信息~~，自觉~~抵制不良~~信息。	**第十八条** 网络信息内容服务使用者应当文明健康使用网络，按照法律法规的要求和用户协议约定，切实履行相应义务，在以发帖、回复、留言、弹幕等形式参与网络活动时，文明互动，理性表达，不得发布本规定第六条规定的信息，防范和抵制本规定第七条规定的信息。
第二十一条 网络群组、论坛社区版块建立者和管理者~~，~~应当履行群组、版块管理责任，依据法律法规、用户协议和平台公约等，规范群组、版块内信息发布等行为。	**第十九条** 网络群组、论坛社区版块建立者和管理者应当履行群组、版块管理责任，依据法律法规、用户协议和平台公约等，规范群组、版块内信息发布等行为。

第二十条第一款 鼓励网络信息内容服务使用者积极参与网络生态治理，~~以~~投诉、举报等方式~~加强~~对网上违法和不良信息~~的~~监督，共同~~建设~~良好网络~~环境~~。	**第二十条** 鼓励网络信息内容服务使用者积极参与网络信息内容生态治理，通过投诉、举报等方式对网上违法和不良信息进行监督，共同维护良好网络生态。
第二十二条 网络信息内容服务使用者不得利用网络和相关信息技术，实施侮辱、诽谤、威胁~~以及恶意泄露他人隐私、散布谣言、人肉搜索等网络侵权、网络暴力~~行为，~~侵害其他组织或者个人名誉权、财产权等~~合法权益。	**第二十一条** 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用网络和相关信息技术实施侮辱、诽谤、威胁、散布谣言以及侵犯他人隐私等违法行为，损害他人合法权益。
第二十三条 网络信息内容服务使用者不得通过发布、删除信息~~等~~干预信息呈现的手段谋取不正当利益。	**第二十二条** 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得通过发布、删除信息以及其他干预信息呈现的手段侵害他人合法权益或者谋取非法利益。
第二十四条 网络信息内容服务使用者不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动。	**第二十三条** 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动。
第二十五条 网络信息内容服务使用者不得通过~~人力~~或者技术手段实施流量造假、流量劫持以及虚假注册账号、~~批量买卖~~账号、操纵用户账号等行为，破坏网络生态秩序。	**第二十四条** 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得通过人工方式或者技术手段实施流量造假、流量劫持以及虚假注册账号、非法交易账号、操纵用户账号等行为，破坏网络生态秩序。
第二十六条 网络信息内容服务使用者不得利用党徽、国旗、国徽等代表党和国家形象的标识，或者借~~党和国家领导人名义及~~国家重大活动、重大纪念日等，违法违规开展网络商业营销活动。	**第二十五条** 网络信息内容服务使用者和网络信息内容生产者、网络信息内容服务平台不得利用党旗、党徽、国旗、国徽、国歌等代表党和国家形象的标识及内容，或者借国家重大活动、重大纪念日和国家机关及其工作人员名义等，违法违规开展网络商业营销活动。
第五章 网络行业组织	**第五章 网络行业组织**
	第二十六条 鼓励行业组织发挥服务指导和桥梁纽带作用，引导会员单位增强社会责任感，唱响主旋律，弘扬正能量，反对违法信息，防范和抵制不良信息。

第二十七条 鼓励行业组织~~推进~~行业自律，~~建立健全网络生态治理行业准则~~，指导~~、督促~~会员单位~~及从业人员~~依法提供网络信息内容服务。	**第二十七条** 鼓励行业组织建立完善行业自律机制，制定网络信息内容生态治理行业规范和自律公约，建立内容审核标准细则，指导会员单位建立健全服务规范、依法提供网络信息内容服务、接受社会监督。
第二十八条 鼓励行业组织开展网络生态治理教育培训和宣传引导工作，提升会员单位、从业人员治理能力，增强全社会共同治理意识。	**第二十八条** 鼓励行业组织开展网络信息内容生态治理教育培训和宣传引导工作，提升会员单位、从业人员治理能力，增强全社会共同参与网络信息内容生态治理意识。
第二十九条 鼓励行业组织~~建立相应~~评价奖惩机制，~~支持会员单位开展网络生态治理，~~加大对会员单位激励和惩戒力度。	**第二十九条** 鼓励行业组织推动行业信用评价体系建设，依据章程建立行业评议等评价奖惩机制，加大对会员单位的激励和惩戒力度，强化会员单位的守信意识。
第六章 监督管理	**第六章 监督管理**
~~**第三十条** 地方各级网信部门应当会同有关部门，切实履行属地管理责任，做好本行政区域内网络生态治理工作。~~	
第三十二条 各级网信部门会同有关部门，建立健全信息共享、会商通报、联合执法、案件督办等工作机制，协同开展网络生态治理工作。	**第三十条** 各级网信部门会同有关主管部门，建立健全信息共享、会商通报、联合执法、案件督办、信息公开等工作机制，协同开展网络信息内容生态治理工作。
第三十三条 各级网信部门对网络信息内容服务平台履行~~生态治理主体~~责任情况开展监督检查，对~~问题突出的~~平台开展专项督查~~，及时向社会公开检查情况及查处结果~~。	**第三十一条** 各级网信部门对网络信息内容服务平台履行信息内容管理主体责任情况开展监督检查，对存在问题的平台开展专项督查。
第十条第二款 网络信息内容服务平台对网信部门和有关部门依法实施的监督检查，应当予以配合。	网络信息内容服务平台对网信部门和有关主管部门依法实施的监督检查，应当予以配合。
第三十四条 各级网信部门建立网络信息内容服务平台违法违规行为台账管理机制，根据台账依法依规进行相应处理。	**第三十二条** 各级网信部门建立网络信息内容服务平台违法违规行为台账管理制度，并依法依规进行相应处理。
第三十一条地方各级网信部门建立~~社会各界~~共同参与的监督评价机制，定期对本行政区域内	**第三十三条** 各级网信部门建立政府、企业、社会、网民等主体共同参与的监督评价机制，

网络信息内容服务平台生态治理情况进行评估。	定期对本行政区域内网络信息内容服务平台生态治理情况进行评估。
第七章 法律责任	**第七章 法律责任**
第三十五条 网络信息内容生产者违反本规定第六条规定的，网络信息内容服务平台应当依法依约采取警示整改、限制功能、暂停更新、关闭账号等处置措施，及时消除违法信息内容，保存记录并向有关主管部门报告。~~由有关主管部门依法采取相应措施。~~ ~~违反本规定第六条规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。~~	**第三十四条** 网络信息内容生产者违反本规定第六条规定的，网络信息内容服务平台应当依法依约采取警示整改、限制功能、暂停更新、关闭账号等处置措施，及时消除违法信息内容，保存记录并向有关主管部门报告。
第三十六条第二款 网络信息内容服务平台违反本规定第十二条规定的，由网信等有关主管部门依据职责~~采取约谈、责令限期改正等管理措施。拒不改正或者情节严重的，依法给予警告、罚款、责令停业整顿直至吊销许可证；构成犯罪的，依法追究刑事责任~~。	**第三十五条** 网络信息内容服务平台违反本规定第十条、第三十一条第二款规定的，由网信等有关主管部门依据职责，按照《中华人民共和国网络安全法》《互联网信息服务管理办法》等法律、行政法规的规定予以处理。
	第三十六条网络信息内容服务平台违反本规定第十一条第二款规定的，由设区的市级以上网信部门依据职责进行约谈，给予警告，责令限期改正；拒不改正或者情节严重的，责令暂停信息更新，按照有关法律、行政法规的规定予以处理。
~~**第三十六条第一款**网络信息内容生产者违反本规定第七条规定的，网络信息内容服务平台应当依法依约采取警示整改、限制功能、暂停更新等处置措施，保存有关记录，并向有关主管部门报告。由有关主管部门依法采取相应措施。~~	
第三十八条 网络信息内容服务平台违反本规定第九条、第十条第二款、第十三条、第十五条、第十七条至第十九条规定的，由网信~~等有关主管部门~~依据职责采取约谈、责令限期改正~~等管理措施~~。拒不改正或者情节严重的，~~依法~~	**第三十七条** 网络信息内容服务平台违反本规定第九条、第十二条、第十五条、第十六条、第十七条规定的，由设区的市级以上网信部门依据职责进行约谈，给予警告，责令限期改正；拒不改正或者情节严重的，责令暂停信息

~~给予警告、罚款、~~责令~~停业整顿直至吊销许可证；构成犯罪的，依法追究刑事责任。~~	更新，按照有关法律、行政法规的规定予以处理。
第三十七条 网络信息内容服务平台违反本规定第十六条规定的，由有关主管部门依照相关法律、行政法规的规定处理。 **第三十九条** 违反本规定第二十一条至第二十六条规定的，依照相关法律、行政法规的规定处理。	**第三十八条** 违反本规定第十四条、第十八条、第十九条、第二十一条、第二十二条、第二十三条、第二十四条、第二十五条规定的，由网信等有关主管部门依据职责，按照有关法律、行政法规的规定予以处理。
第四十条 网信部门根据相关法律法规规定，会同有关部门建立健全网络信息服务严重~~违规~~失信联合惩戒机制，对严重违反本规定的网络信息内容服务平台、网络信息内容生产者和网络信息内容使用者依法依规实施限制从事网络信息服务、网上行为限制、行业禁入等惩戒措施。	**第三十九条** 网信部门根据法律、行政法规和国家有关规定，会同有关主管部门建立健全网络信息内容服务严重失信联合惩戒机制，对严重违反本规定的网络信息内容服务平台、网络信息内容生产者和网络信息内容使用者依法依规实施限制从事网络信息服务、网上行为限制、行业禁入等惩戒措施。
	第四十条违反本规定，给他人造成损害的，依法承担民事责任；构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由有关主管部门依照有关法律、行政法规的规定予以处罚。
第八章 附则	**第八章 附则**
第四十一条 本规定所称网络信息内容生产者，是指制作网络信息内容的组织或者个人。	**第四十一条** 本规定所称网络信息内容生产者，是指制作、复制、发布网络信息内容的组织或者个人。
本规定所称网络信息内容服务平台，是指提供信息内容~~复制、发布、~~传播~~等~~服务的网络信息服务提供者。	本规定所称网络信息内容服务平台，是指提供网络信息内容传播服务的网络信息服务提供者。
本规定所称网络信息内容服务使用者，是指使用网络信息内容服务的组织或者个人。	本规定所称网络信息内容服务使用者，是指使用网络信息内容服务的组织或者个人。
~~**第四十二条** 网络信息内容服务平台应当依据本规定，制定本平台网络生态治理具体标准和工作细则。~~	

~~地方网信部门可结合本地实际，制定实施细则。~~	
第四十三条 本规定自 ~~2019~~ 年 月 日起施行。	**第四十二条** 本规定自 2020 年 3 月 1 日起施行。

《网络信息内容生态治理规定》全文参见：

http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm

中国首家律师事务所

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层 邮编: 100025
15 & 20/F Tower 1, China Central Place,
No. 81 Jianguo Road Chaoyang District,
Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市黄浦区湖滨路150号企业天地
5号楼26层 邮编: 200021
26F, 5 Corporate Avenue,
No. 150 Hubin Road, Huangpu District,
Shanghai 200021, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区铜鼓路39号大冲国际中心
5号楼26层B/C单元 邮编: 518055
Units B/C, 26F, Tower 5,
Dachong International Center, No. 39 Tonggu Road,
Nanshan District, Shenzhen 518055, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987