海问观察：网络安全及数据合规动态（2019 年 9 月上半月）

傅鹏、赵卿梦

本动态涵盖 2019 年 9 月上半月（大致涵盖 2019 年 9 月 2 日-2019 年 9 月 15 日及其前后若干时段的期间）网络安全和数据合规领域的规定、规则及重大新闻。第一部分为我们理解值得关注的该领域的最新规定及规则（部分规定或规则，可能包含我们对其值得关注的要点或问题的简评）；第二部分为我们理解值得关注的该领域的重要事件或重大新闻（部分事件或新闻，可能包含我们对其值得关注的要点或问题的简评）。

一、 最新规定及规则

文件名称	关于引导规范教育移动互联网应用有序健康发展的意见
发布时间	2019 年 9 月 5 日
颁布单位	教育部等八部门[①]
看点	**1. 规范教育 APP 的数据管理** 教育移动应用提供者应当建立覆盖个人信息收集、储存、传输、使用等环节的数据保障机制。按照“后台实名、前台自愿”的原则，对注册用户进行身份信息认证。收集使用个人信息应当明示收集使用信息的目的、方式和范围，并经用户同意。收集使用未成年人信息应当取得监护人同意、授权。不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得收集与其提供服务无关的个人信息，不得违反法律法规与用户约定，不得泄露、非法出售或非法向他人提供个人信息。 **2. 保障教育 APP 的网络安全** 教育移动应用提供者应当落实网络安全主体责任，采取有效措施，防范应对网络攻击，保障系统的平稳、安全运行。教育移动应用和后台系统应当统一落实网络安全等级保护要求。应用商店等移动应用分发平台提供者应当加强教育移动应用上架审核管理，建立开发者真实身份信息登记制度，对教育移动应用开展安全审核，及时处理违法违规教育移动应用。鼓励教育移动应用提供者参加网络安全认证、检测，全面提高网络安全保障水平。 **3. 对教育 APP 实施备案制度** 要求教育 APP 提供者在其注册地的省级教育行政部门进行备案，并在 2019 年底完成备案工作。 **4. 对教育 APP 实施分类管理和收费限制** 针对推荐使用的教育 APP，采取自愿原则，且**不得与教学管理行为绑定，不得与学分、成绩和评优挂钩**。作为教学、管理工具要求统一使用的教育 APP，**不得向学生及家长收取任何费用，不得植入商业广告和游戏**。对于承担**招生录取、考试报名、成绩查询等重要业务**的教育移动应用，**原则上应当由教育行政部门和学校自行运行管理**。确需选用第三方应用的，**不得签订排他协议，或实际由单一应用垄断业务**。
简评	**1. 强化教育 APP 涉及的使用场景的个人信息保护** 该意见对教育 APP 的个人信息保护等数据管理工作提出了更为明确的要

	求。根据新华网 2019 年 7 月的报道，工业和信息化部组织对 100 家互联网企业的 106 项互联网服务进行抽查，发现 18 家互联网企业存在未公示用户个人信息收集使用规则、未告知查询更正信息的渠道、未提供账号注销服务等问题，并已责令相关企业整改。其中就包含市场上若干款知名教育 APP。此外，在广东省公安厅曝光的 7 月份“超范围收集用户信息 APP”整治结果中，数款教育类 APP 被曝存在超范围读取用户通话记录、短信内容，收集用户通讯录、位置信息，超权限使用设备麦克风、摄像头等突出安全问题。在其他一些主管部门组织的评测或者检查活动中，多款教育 APP 也数次被列举存在个人信息保护方面的合规问题。该意见的出台有助于进一步规范教育 APP 在个人信息保护方面存在的现有问题，提高教育 APP 在网络安全和数据合规方面的总体保护水平。 **2. 期待进一步出台的《教育移动互联网应用备案管理办法》** 业界对该意见提出的教育 APP 备案制度特别关注。根据教育部科技司司长雷朝滋的公开讲话，教育部将就备案相关工作出台《教育移动互联网应用备案管理办法》，并且该办法初稿目前已经形成，将于近期进一步征求意见，计划在 9 月底前印发该办法。相信随着该办法的出台，有关部门对教育 APP 备案的流程、内容等具体要求将以更明晰的形式呈现在教育 APP 运营者面前，便利教育 APP 运营者更好地参与、完成备案工作。

文件名称	关于加强工业互联网安全工作的指导意见
发布时间	2019 年 8 月 28 日
颁布单位	工业和信息化部等十部门[②]
看点	**1. 构建工业互联网安全管理体系** 要求围绕工业互联网安全监督检查、风险评估、数据保护、信息共享和通报、应急处置等方面建立健全安全管理制度和工作机制，强化对企业的安全监管。建立工业互联网行业分类指导目录、企业分级指标体系，制定工业互联网行业企业分类分级指南。推动工业互联网设备、控制、网络（含标识解析系统）、平台、数据等重点领域安全标准的研究制定，建设安全技术与标准试验验证环境。 **2. 提升企业工业互联网安全防护水平** 督促工业企业部署针对性防护措施，加强工业生产、主机、智能终端等设备安全接入和防护。指导工业企业、基础电信企业在网络化改造及部署IPv6、应用5G的过程中，落实安全标准要求并开展安全评估。要求工业互联网平台的建设、运营单位按照相关标准开展平台建设，在平台上线前进行安全评估，针对边缘层、IaaS层（云基础设施）、平台层（工业PaaS）、应用层（工业SaaS）分层部署安全防护措施。建立健全工业APP应用前安全检测机制，强化应用过程中用户信息和数据安全保护。 **3. 强化工业互联网数据安全保护能力** 明确数据收集、存储、处理、转移、删除等环节安全保护要求，指导企业完善研发设计、工业生产、运维管理、平台知识机理和数字化模型等数据的防窃密、防篡改和数据备份等安全防护措施，鼓励商用密码在工业互联网数据保护工作中的应用。
简评	随着工业化和信息化“两化”深度融合的全面开展，互联网在工业技术领域的应用得到了飞速发展。然而，互联网“分享”、“发现”的特点

	和工业技术系统（特别是工业控制系统）“控制”、“稳定”的特点如何进一步协调，成为监管机关及该领域从业人员一直以来关注的重点。该意见给工业互联网的安全管理体系、安全防护水平以及安全保护能力等方面提出了一系列方向性的要求。更重要的是，随着该意见的出台，可以预见将有一系列与工业互联网领域的网络安全及数据合规相关的新规定、国家新标准出台，值得工业互联网领域的从业人员持续关注。

文件名称	网络生态治理规定（征求意见稿）
发布时间	2019 年 9 月 10 日
颁布单位	国家互联网信息办公室
看点	1. 该规定在以网络信息内容为主要治理对象的基础上，将具体的治理目标分为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和网络行业组织几个方面，提出了一些具体的治理规定。 2. 对于**网络信息内容生产者**生产、制作的信息类型，该规定列举了**鼓励制作的类型**、**禁止制作的违法信息类型**以及**不得制作的不良信息类型**三个大的方面的较为详细的类型内容列表。 3. 对**网络信息内容服务平台**，该规定提出了对信息内容发布审核、以人工编辑及机器算法等方式推荐和呈现信息环节的管理、完善用户服务协议及明确用户相关权利义务、建立用户账号信用档案并根据用户账号的信用等级提供相应的服务、在显著位置设置便捷投诉举报入口、编制网络生态治理工作年度报告等方面的要求。其中关于用户账号的信用等级的相关要求，是对互联网信息内容领域的总体监管层面的较新的要求，有待进一步通过颁布实施细则等方式来细化这一方面的具体管理要求。 4. 该规定也对**网络信息内容服务使用者**提出了一系列要求。其中特别值得关注的是，在对新的技术背景和新的互联网不正当竞争及其他不当行为进行监管的背景下，要求网络信息内容服务使用者（1）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，（2）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，以及（3）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。 5. 该规定对未成年人/儿童网络保护提出了具体的要求。其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**，要求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。 6. 该规定对一系列违反该规定的行为提出了具体的罚则。此外，还明确规定网信部门将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**。

二、 案例及事件

（一） “ZAO”事件持续发酵并引发关于个人信息保护的广泛关注

1. 事件

2019 年 8 月 30 日-2019 年 8 月 31 日，ZAO APP 在短时间内引发舆论密切关注，但其用户也广泛地表达了关于照片上传后的隐私泄露风险，且 ZAO APP《用户协议》第 6 条中「不可撤销」、「永久授权」等描述使得用户的肖像权和著作权亦可能因为使用 ZAO APP 而存在法律风险。

2019 年 8 月 31 日，ZAO 主动修改用户条款[③]：删除了「不可撤销」、「永久授权」等描述方式；并且在协议的初始部分以加粗字体做了特别提示[④]，承诺该协议只用于对用户上传内容进行换脸等内容的修改操作。

2019 年 9 月 3 日，ZAO 运营团队发布声明[⑤]，澄清 ZAO 不会存储个人面部生物识别特征信息；使用“ZAO”也不会产生支付风险；并且如果用户删除信息或注销账号，ZAO 均会删除相应信息。

2019 年 9 月 3 日，工信部约谈北京陌陌科技有限公司[⑥]，要求其严格按照国家法律法规以及相关主管部门要求，组织开展自查整改，依法依规收集使用用户个人信息，规范协议条款，强化网络数据和用户个人信息安全保护。

2019 年 9 月 3 日，ZAO 更新隐私协议以及用户协议：删除了此前争议较大的要求用户将著作权和肖像权授权给 ZAO 的两段规定，并且设置了真人验证环节以保证肖像权不被滥用，并声明真人验证时不会存储面部特征信息。

2019 年 9 月 7 日和 2019 年 9 月 10 日，ZAO 分别更新了 Android 和 iPhone 商店的版本，协议内容没有变化，为帮助用户理解，添加了“隐私解释”。

2. 简评

关于 ZAO APP 事件在个人隐私保护及 AI 生成作品的版权归属等问题的讨论，请参见我们此前的文章
【https://mp.weixin.qq.com/s?__biz=MzA5MjYzNDQyMw==&mid=2658226119&idx=1&sn=8ecf72c09d3aa739644a38de341770aa&chksm=8befc39fbc984a899c542b6fb08b00d7b841ff81a713af7ee788e9d3eccc8a974a1261b5f707&token=1542179409&lang=zh_CN#rd】。

（二） 28 项全国信息安全标准化技术委员会归口国家标准获批发布

2019 年 8 月 30 日，国家市场监督管理总局、国家标准化管理委员会发布中华人民共和国国家标准公告（2019 年第 10 号），其中《信息安全技术 路由器安全技术要求》《信息安全技术 数据库管理系统安全评估准则》等 28 项国家标准为全国信息安全标准化技术委员会归口，具体清单如下：

国家标准编号	国家标准名称	代替标准号	实施日期
GB/T 18018-2019	信息安全技术 路由器安全技术要求	GB/T 18018-2007	2020/3/1
GB/T 20009-2019	信息安全技术 数据库管理系统安全评估准则	GB/T 20009-2005	2020/3/1
GB/T 20272-2019	信息安全技术 操作系统安全技术要求	GB/T 20272-2006	2020/3/1

国家标准编号	国家标准名称	代替标准号	实施日期
GB/T 20273-2019	信息安全技术 数据库管理系统安全技术要求	GB/T 20272-2006	2020/3/1
GB/T 20979-2019	信息安全技术 虹膜识别系统技术要求	GB/T 20979-2007	2020/3/16
GB/T 21050-2019	信息安全技术 网络交换机安全技术要求	GB/T 21050-2007	2020/3/17
GB/T 25058-2019	信息安全技术 网络安全等级保护实施指南	GB/T 25058-2010	2020/3/18
GB/T 37931-2019	信息安全技术 Web 应用安全检测系统安全技术要求和测试评价方法	N/A	2020/3/1
GB/T 37932-2019	信息安全技术 数据交易服务安全要求	N/A	2020/3/1
GB/T 37933-2019	信息安全技术 工业控制系统专用防火墙技术要求	N/A	2020/3/1
GB/T 37934-2019	信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求	N/A	2020/3/1
GB/T 37935-2019	信息安全技术 可信计算规范可信软件基	N/A	2020/3/1
GB/T 37939-2019	信息安全技术 网络存储安全技术要求	N/A	2020/3/1
GB/T 37941-2019	信息安全技术 工业控制系统网络审计产品，安全技术要求	N/A	2020/3/1
GB/T 37950-2019	信息安全技术 桌面云安全技术要求	N/A	2020/3/1
GB/T 37952-2019	信息安全技术 移动终端安全管理平台技术要求	N/A	2020/3/1
GB/T 37953-2019	信息安全技术 工业控制网络监测安全技术要求及测试评价方法	N/A	2020/3/1
GB/T 37954-2019	信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法	N/A	2020/3/1
GB/T 37955-2019	信息安全技术 数控网络安全技术要求	N/A	2020/3/1
GB/T 37956-2019	信息安全技术 网站安全云防护平台技术要求	N/A	2020/3/1
GB/T 37962-2019	信息安全技术 工业控制系统产品信息安全通用评估准则	N/A	2020/3/1
GB/T 37964-2019	信息安全技术 个人信息去标识化指南	N/A	2020/3/1
GB/T 37971-2019	信息安全技术 智慧城市安全体系框架	N/A	2020/3/1
GB/T 37972-2019	信息安全技术 云计算服务运行监管框架	N/A	2020/3/1
GB/T 37973-2019	信息安全技术 大数据安全管理指南	N/A	2020/3/1
GB/T 37980-2019	信息安全技术 工业控制系统安全检查指南	N/A	2020/3/1
GB/T 37988-2019	信息安全技术 数据安全能力成熟度模型	N/A	2020/3/1
GB/T 15852.3-2019	信息技术 安全技术 消息鉴别码第 3 部分：采用泛杂凑函数的机制	N/A	2020/3/1

（三） 网络预约汽车服务个人信息安全指南国家标准启动会召开

1. 事件

全国信息安全标准化技术委员会秘书处（“信安标委秘书处”）于 2019 年 8 月 31 日在北京组织召开网络预约汽车服务个人信息安全指南国家标准启动会，启动会上，信安标委秘书处介绍了网络预约汽车服务个人信息安全指南国家标准的编制工作方案和标准大纲，业内相关企

业代表均分享了各自在个人信息保护方面的实践经验，与会专家分别围绕标准定位、相关法律法规和标准具体制定工作等发表了意见建议。本次会议旨在在网约车领域落实国家数据安全管理政策，进一步促进国家标准《个人信息安全规范》在具体领域的落地实施。[⑦]

2. 简评

落实《网络安全法》规定的个人信息保护原则及《个人信息安全规范》提出的个人信息保护要求在具体业务类型或业务场景中的细化应用是个人信息保护立法及执法机构的关注点。此前，在金融、医疗等对个人信息使用高度敏感的行业，主管机关出台了基于行业及特殊业务场景的规定及国家推荐性标准（含征求意见稿）。在网络预约汽车服务领域的个人信息保护特别规定也是这一监管趋势的体现之一。相信主管机关在未来也将针对其他细分的行业领域和业务场景出台更多的规定及国家标准，规范这些具体行业领域及业务场景中的个人信息使用和保护。

（四） 上海市网信办依法处置 18 个违规网站、微信公众号

2019 年 9 月 6 日，上海网信办会同电信主管部门，针对网民举报内容启动专项整治活动，依法处置 18 个违规网站、微信公众号，其中：关闭“上海殡葬网”、“花蛇网”等 2 家传播虚假信息、发布低俗信息的严重违法违规网站；协调有关部门关闭“上海司机平安符”等 4 个散播交通执法检查情况，教唆非法客运驾驶员躲避执法检查的违规微信公众号；对一家违规转载大量境外时政新闻的英语听力 APP 作出行政处罚；指导、整改“猜豆网”等 7 家违法违规网站；约谈“上海金属网”等 4 家违法违规网站[⑧]。

（五） 广东省公安厅发文曝光“通付 MPOS”等 42 款存在违规收集信息行为的 APP

1. 事件

2019 年 9 月 5 日，广东省公安厅发文称，根据公安部“净网 2019”专项行动和中央网信办、工信部、公安部、市场监管总局四部委关于开展 APP 违法违规收集使用个人信息专项治理行动部署，广东省公安机关持续开展超范围收集用户信息 APP 清理整治专项行动，2019 年 8 月份共监测发现“通付 MPOS”等 42 款 APP 存在超范围读取用户通话记录、短信或彩信，收集用户通讯录、用户设备上已知账号，超权限使用用户设备麦克风，以及无用户协议、隐私政策或未说明业务逻辑、权限与获取用户隐私信息用途等突出安全问题，目前广东省公安机关已将有关监测情况上报公安部通报属地公安机关开展清理整治。[⑨]

2. 简评

本次广东省公安厅指出存在问题的该等APP中，与用户协议及隐私政策有关的问题主要仍集中在（1）无用户协议及/或隐私政策；或者（2）隐私政策未能适当说明业务逻辑与用户信息收集权限的关系。该等问题也是有关机关在其他评审或检查活动中核心关注并经常发现的问题，值得APP运营者在今后的用户协议和隐私政策的起草或更新过程中予以特别关注。

***实习生董琰祺对本文亦有贡献。**

---

[1] 教育部、中央网信办、工业和信息化部、公安部、民政部、市场监管总局、国家新闻出版署、全国“扫黄打非”工作小组办公室。

[2] 工业和信息化部、教育部、人力资源和社会保障部、生态环境部、国家卫生健康委员会、应急管理部、国务院国有资产监督管理委员会、国家市场监督管理总局、国家能源局、国家国防科技工业局。

[3] 修改后条款：“在您上传及/或发布用户内容时，您同意或者确保实际权利人已经同意授予「ZAO」及「ZAO」用户全球范围内免费的、可以对用户内容进行部分的修改或编辑（如将短视频中的人脸换成另一个人的人脸等）以及对修改或编辑前后的用户内容进行信息网络传播的权利。”

[4] 特别提示内容：“您提供上传/发布短视频以及利用技术对平台上的短视频进行局部修改生成新的短视频的服务，相关内容将严格按照相关法律法规的规定保留在 ZAO 上，除非为了改善 ZAO 为您提供的服务或另行取得您的再次同意，否则 ZAO 不会以任何形式或目的使用上述内容。”

[5] 信息来源请见：微博“ZAO 官方助手”于 2019 年 9 月 3 日发出的声明。

[6] 信息来源请见：工信部官网 http://www.miit.gov.cn/n1146290/n1146402/n1146440/c7392862/content.html。

[7] 信息来源请见：信安标委官网 https://www.tc260.org.cn/front/postDetail.html?id=20190905104044。

[8] 信息来源请见：上海市网信办微信公众号 2019 年 9 月 10 日发布消息 https://mp.weixin.qq.com/s?src=11&timestamp=1568645056&ver=1856&signature=9zA1jOEKbVXGyeaBuuI8zpfX0QApldFTTXV0-7Od9RKJbBeUqcohrwrDDF-wamZWp5l4NQy-hoPohjM9-vKqJkDby9bagzUe99oWK92u2xD-8SDSrjGkOh8kSZE4jtCX&new=1。

[9] 信息来源请见：广东省公安厅官网 http://gdga.gd.gov.cn/gkmlpt/content/2/2596/post_2596763.html。该等 42 款 APP 超范围收集用户信息的情况以及其用户协议及隐私政策对应的问题也可参见该信息来源。