

海问观察：网络安全及数据合规动态（2019年10月下半月-11月）

作者：傅鹏

本动态涵盖2019年10月下半月至11月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政策规定及规则（部分政策规定或规则，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）。

本动态仅作为本所对网络安全及数据合规相关的近期话题的一般性探讨，不构成本所正式法律咨询意见。

一、监管规则

（一）《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》（法释〔2019〕15号）（下称“《信息网络犯罪司法解释》”）

发布时间：2019年10月21日

发布单位：最高人民法院和最高人民检察院

数据合规看点：

1、对“拒不履行信息网络安全管理义务罪”的细化规定

a. 拒不履行信息网络安全管理义务罪

《刑法》第二百八十六条之一规定，网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：

- （一）致使违法信息大量传播的；
- （二）致使用户信息泄露，造成严重后果的；
- （三）致使刑事案件证据灭失，情节严重的；
- （四）有其他严重情节的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

b. 明确了“网络服务提供者”的范围

《信息网络犯罪司法解释》规定，“网络服务提供者”指提供以下服务的单位和个人：网络接入、域名注册解析等信息网络接入、计算、存储、传输服务；信息发布、搜索引擎、即时通讯、网络支付、网络预约、网络购物、网络游戏、网络直播、网站建设、安全防护、广告推广、应用商店等信息网络应用服务；利用信息网络提供的电子政务、通信、能源、交通、水利、金融、教育、医疗等公共服务。

c. 明确了“监管部门责令采取改正措施”和“拒不改正”的具体含义和情境

《信息网络犯罪司法解释》规定，“监管部门责令采取改正措施”，是指网信、电信、公安等依照法律、行政法规的规定承担信息网络安全监管职责的部门，以责令整改通知书或者其他文书形式，责令网络服务提供者采取改正措施。认定“经监管部门责令采取改正措施而拒不改正”，应当综合考虑监管部门责令改正是否具有法律、行

政法规依据，改正措施及期限要求是否明确、合理，网络服务提供者是否具有按照要求采取改正措施的能力等因素进行判断。

d.明确或量化了其他入刑要素

《信息网络犯罪司法解释》对“致使违法信息大量传播”、“致使用户信息泄露，造成严重后果”当中的“造成严重后果”、“致使刑事案件证据灭失，情节严重的”的“情节严重”以及“有其他严重情节的”的具体含义进行了详细的规定。

2、对“非法利用信息网络罪”的细化规定

a.非法利用信息网络罪

《刑法》第二百八十七条之一规定，利用信息网络实施下列行为之一，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金：

- （一）设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；
- （二）发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；
- （三）为实施诈骗等违法犯罪活动发布信息的。

b.阐明“违法犯罪”的行为性质

《信息网络犯罪司法解释》规定，为实施诈骗等违法犯罪活动发布信息的，情节严重可认定为本罪，此处“违法犯罪”包括犯罪行为和属于刑法分则规定的行为类型但尚未构成犯罪的违法行为。上述规定，从侧面反映了，对于刑法未规定、仅在治安管理处罚法或者其他法律法规规定的行政违法行为不宜认定为本罪名中的“违法犯罪”行为。

c.释明了三类具体情节

《信息网络犯罪司法解释》释明了“用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组”的一项具体情境；释明了“为实施诈骗等违法犯罪活动发布信息”当中的“发布信息”的一项具体情境；详细释明了哪些情形可以构成“情节严重”。

3、对“帮助信息网络犯罪活动罪”的细化规定

a.帮助信息网络犯罪活动罪

《刑法》第二百八十七条之二规定，明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

b.明确了“明知他人利用信息网络实施犯罪”的情形

《信息网络犯罪司法解释》规定了如下情形可以认定为“明知他人利用信息网络实施犯罪”：经监管部门告知后仍然实施有关行为的；接到举报后不履行法定管理职责的；交易价格或者方式明显异常的；提供专门用于违法犯罪的程序、工具或者其他技术支持、帮助的；频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份，逃避监管或者规避调查的；为他人逃避监管或者规避调查提供技术支持、帮助的；其他足以认定行为人明知的情形。

c.明确了“情节严重”的情形

《信息网络犯罪司法解释》明确了一系列情形可认定为帮助信息网络犯罪活动罪入刑要素中要求的“情节严重”。

4、职业禁止和禁止令规定

《信息网络犯罪司法解释》明确，对于实施拒不履行信息网络安全管理义务罪、帮助信息网络犯罪活动罪、非法利用信息网络罪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。

简评：《信息网络犯罪司法解释》对《刑法修正案（九）》增设的三类网络信息犯罪，即拒不履行信息网络安全管理义务罪、非法利用信息网络罪和帮助信息网络犯罪活动罪的定罪量刑提供了具体的适用规范。就《信息网络犯罪司法解释》中为各项罪名划定的入刑要素看来，门槛的设置较低，同时适用的犯罪主体和犯罪行为也较为广泛。

（二）《密码法》

发布时间：2019年10月26日（2020年1月1日起施行）

发布单位：全国人民代表大会常务委员会

数据合规看点：

1、密码的分类管理制度：根据密码保护信息的不同将密码划分为核心密码、普通密码和商用密码并制定不同的管理规则，其中核心密码、普通密码用于保护国家秘密信息；商用密码用于保护不属于国家秘密的信息。

2、商用密码领域外资准入的国民待遇：商用密码科研、生产、销售、服务、进出口业务并不属于外商投资的负面清单中，即不属于禁止或限制外商投资的业务。

3、商用密码产品和服务的认证要求：商用密码产品涉及国家安全、国计民生、社会公共利益的，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供；商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。

4、关键信息基础设施的商用密码保护：法律法规要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，并应开展商用密码应用安全性评估；关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定完成国家安全审查。

5、商用密码的进口许可和出口管制制度：涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制；大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

简评：《密码法》是我国密码管理领域的第一部综合性法律，在其颁布前，相关规范仅零散地分布于各项法规及其他规定当中。《密码法》中“密码”不同于日常生活中个人使用的“密码”，是特指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务，目前多应用于电子商务领域的安全认证以及金融交易的加密传输中，其未来预期也可能将对如区块链服务等网络信息领域的服务起到更深层次的规范作用。

（三）《网络安全威胁信息发布管理办法》（征求意见稿）

发布时间：2019年11月20日
发布单位：国家互联网信息办公室

数据合规看点：

1、发布网络安全威胁事件信息或报告前，应履行事先报告义务：

信息、报告内容	通报机关
网络和信息系统被攻击破坏、非法侵入等网络安全事件信息	事件发生所在地地市级以上公安机关，公安机关报同级网信部门和上级公安机关
地区性的网络安全攻击、事件、风险、脆弱性综合分析报告	涉及地区地市级以上网信部门和公安机关
涉及公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的网络安全攻击、事件、风险、脆弱性综合分析报告	行业主管部门
全国性或跨地区、跨行业领域的综合分析报告	国家网信部门和国务院公安部门

2、征求同意的义务：发布具体网络和信息系统存在风险、脆弱性情况，应事先征求运营者书面意见，但已提前30日向主管部门举报和相关风险、脆弱性已被消除的两种情形除外。发布的“具体网络和信息系统”的情况指内容包含名字、位置、域名、IP地址等信息，若不涉及具体信息，无法定位到具体网络和信息系统，则无需征求运营者同意。

3、平台运营者、举办单位的监督义务：通过各个公共平台发布信息的，平台运营者、主办单位发现有违反本办法的行为和内容，应及时采取处置措施，并向地市级以上网信部门、公安机关报告。

简评：本办法对网络安全威胁信息发布行为进行了较为详细的规范，特别有利于平衡和减轻信息发布行为对运营者的负面影响。在过往的许多事件中，不论是黑客对网络安全威胁信息的恶意发布，还是“白帽子”对特定系统网络安全漏洞进行侦测后基于善意进行的信息发布，都有可能因为披露不当而对披露信息指向的目标系统的运营者造成负面影响。极端情况下，个别“白帽子”也曾因漏洞挖掘和披露行为受到处罚甚至刑事追诉。本办法的发布，有利于提示、规范“白帽子”的信息发布和报告活动，对在法律允许的框架内进一步鼓励“白帽子”的漏洞挖掘和合法报告/发布活动提供有益的帮助。

（四）《网络音视频信息服务管理规定》

发布时间：2019年11月18日
发布单位：互联网信息办公室，文化和旅游部，广播电视总局

数据合规看点：

1、再次强调实名制认证要求：网络音视频信息服务提供者应当对用户进行真实身份信息认证；用户不提供真实身份信息的，不得为其提供信息发布服务。

2、深度学习、虚拟现实等新技术新应用的相关要求：

a.安全评估义务：服务提供者基于该技术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调整增设相关功能的，应当开展安全评估。

b.标识义务：服务提供者和使用者基于该技术制作、发布、传播非真实音视频信息的，应当以显著方式予以标识。对不符合显著标识要求的信息内容，应当立即停止传播，经纠正后方可继续传输。

c.不得用于生成、传播虚假新闻：服务提供者和使用者不得利用该技术制作、发布、传播虚假新闻信息。

d.辟谣及备案义务：服务提供者应当建立健全辟谣机制，发现利用基于该技术的虚假图像、音视频生成技术制作、发布、传播谣言的，应当及时采取辟谣措施，并向相关部门备案。

3、部署鉴别技术的义务：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鉴别技术。

简评：除本规定对非真实音视频信息的标识义务进行明确规定外，《数据安全管理办法（征求意见稿）》也提出了类似的标识要求。《网络音视频信息服务管理规定》回应了新技术发展面临的问题，对服务提供者的安全意识、管理措施和技术保障能力提出新的要求，强调服务提供者的安全管理义务。

（五）《信息安全技术 个人信息安全规范》（最新版征求意见稿）

发布时间：2019年10月24日

发布单位：国家市场监督管理总局，国家标准化管理委员会

数据合规看点：

1、对描述进行优化：该规范补充并完善了部分定义，优化部分专业词汇和基本原则的描述。

2、对内容进行更新：该规范对个人信息收集事项中“不得强迫接受多项业务功能”、“征得授权同意”部分，个人信息使用事项中“个性化展示的使用”部分，以及“个人信息共同控制者的要求”等内容进行更新。

3、补充具体要求：该规范针对注销难问题，补充注销机制要求。对委托处理、共享、转让等事项中受委托者和接收方的管理要求进行补充。

（六）《信息安全技术 移动互联网应用程序（APP）收集个人信息基本规范》（草案）

发布时间：2019年10月24日

发布单位：国家市场监督管理总局，国家标准化管理委员会

数据合规看点：

1、明确最小必要信息的范围：将“法律法规等规范性文件要求必须收集的个人信息”修改为“法律法规要求必须收集的个人信息”，明确了必须收集的个人信息范围情形之一仅限于“法律法规”，而非宽泛地指向其他规范性文件。

2、增加运营者的定义：在“移动互联网应用程序的所有者、管理者”的基础上，增加了一项“移动互联网应用程序服务的提供者”。此前，实践中，一般理解移动互联网应用的“运营者”可以是在应用商店发布该应用的发布者（publisher），或者可以是应用软件著作权的所有者（copyright owner）。但在一些应用中，发布者并不必然是所有者；更重要的是，在发布者、所有者以外，应用的全部或部分服务可能是其他实际提供服务的主体提供，因此

在定义中加入“服务的提供者”有助于让规定更符合实践中的情形。

3、新增首次运行有义务告知最小必要信息规则：最新稿新增要求APP首次运行时应通过弹窗等明显方式告知收集最小必要信息规则。

4、细化APP运营者承担第三方代码、插件的责任范围：最新稿中明确APP运营者应确保第三方代码或插件履行个人信息安全保护义务，并防止第三方代码或插件收集无关的个人信息。这一规定相比于旧稿的“App应对其使用的第三方代码、插件的个人信息收集行为负责”这一宽泛的规定，提出了更为明确的要求、划分了更为清晰的责任承担范围。

5、完善部分服务类型所需最小必要信息的范围和使用要求：

a. 博客论坛：个人信息类型中新增仅对使用信息发布功能的该用户收集，包括操作时间等。使用要求为《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》。

b. 网络支付：个人信息类型中新增身份基本信息，包括国籍、性别、职业、住址、联系方式。使用要求为《支付机构反洗钱和反恐怖融资管理办法》。

c. 网上购物：功能定义新增“客服售后”，所需个人信息中收货人信息的使用要求新增“完成客服与售后需要”。

d. 餐饮外卖：所需客人信息中联系人信息的使用要求，从“姓名可无需真实”变更为“姓名无需保证真实”。

e. 金融借贷：个人信息类型中新增“偿付能力、贷款用途”。所需个人信息中将“个人征信信息”改为“个人信用信息”。使用要求为《小额贷款公司网络小额贷款业务风险专项整治实施方案》、《个人贷款管理暂行办法》。

f. 运动健身：个人信息类型中新增：基本健康资料，包括性别、年龄、身高、体重。使用要求为基本健康资料结合个人运动信息可以更好地给出运动或健康建议。

g. 网页浏览器：浏览器的功能定义变更为“为用户提供通过输入网址或站点导航浏览网上信息资源功能的服务”。

二、案例事件

（一）北京市通信管理局开展APP网络数据安全检查

2019年12月4日，北京市通信管理局发布通告，针对APP违规收集用户信息、强制授权、过度索权等社会热点问题，组织开展了为期两个月的移动应用APP网络数据安全检查。

本次检查选取了具有影响力的50款APP，覆盖了社交、网租房和汽车服务、线上教育、金融、线上医疗、基础电信企业等6个领域。主要发现问题有：用户拒绝授权时，未明确告知服务使用受限的范围；用户拒绝授权时，影响其他业务功能的使用；收集使用用户个人敏感信息时，未同步说明目的等。就该次检查，北京市通信管理局也在通告中要求严格落实《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）。

（二）国家市场监督管理总局召开“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动专题新闻发布会

2019年11月18日，国家市场监督管理总局（“市场监管总局”）召开“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动专题新闻发布会。

此前，市场监管总局于2019年3月印发《关于开展“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动的通知》，决定自4月1日至9月30日开展为期6个月的“守护消费”暨打击侵害消费者个人信息违法行为专项执法行动。通知表明，针对房产租售、小贷金融、教育培训、保险经纪、美容健身等多个侵害消费者个人信息违法问题突出的行业和领域开展专项执法行动，重点打击以下违法行为：未经消费者同意，收集、使用消费者个人信息；泄

露、出售或者非法向他人提供所收集的消费者个人信息；未经消费者同意或者请求，或者消费者明确表示拒绝的，向其发送商业性信息等违法行为。

行动期间，全国市场监管部门共立案查办各类侵害消费者个人信息案件1474件，查获涉案信息369.2万条，罚没款1946.4万元，移送公安机关案件154件；组织执法联动4225次；开展行政约谈3536次；开展宣传活动10653次。从查办案件的情况来看，当前侵害消费者个人信息违法行为，主要高发的行业领域和最突出的违法行为见下表：

	类别	案件数量及占比	涉案信息数量及占比	罚没款及占比
行业领域	房产租售行业	273 (18.5%)	153.2万 (41.5%)	428.2万 (22%)
	装饰装修行业	234 (15.9%)	34.5万(9.3%)	176.7万 (9.1%)
	教育培训行业	133 (9%)	126.2万 (34.2%)	475.7万 (24.4%)
违法行为	未经消费者同意，收集、使用消费者个人信息	710 (48.2%)	276.3万 (74.8%)	1006.3万 (51.7%)

（三）工信部开展APP侵犯用户权益专项整治行动

2019年10月31日，工信部发布《关于开展APP侵害用户权益专项整治工作的通知》（工信部信管函[2019]337号）。通知表明，依据《网络安全法》、《电信条例》、《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第20号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号）和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管[2016]407号）等法律法规和规范性文件要求，工信部开展专项整治工作：

1、整治行为

四个方面	八种类型
违规收集用户个人信息方面	私自收集个人信息
	超范围收集个人信息
违规使用用户个人信息方面	私自分享给第三方
	强制用户使用定向推送功能
不合理索取用户权限方面	不给权限不让用
	频繁申请权限
	过度索取权限
为用户账号注销设置障碍方面	账号注销难

2、整治对象

整治对象	检查内容
APP服务提供者	是否存在前述8类问题
APP分发服务提供者（含应用商店、基础电信企业营业厅等承担APP分发功能的各类企业）	是否落实《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管[2016]407号）

3、整治时间

阶段	时间段	内容安排
企业自查自纠阶段	通知印发之日起至11月10日	APP服务提供者认真开展自查，及时整改； APP分发服务提供者组织对所分发APP进行全面检查，督促整改，对拒不改正予以下架处理。
监督抽查阶段	2019年11月11日至11月30日	工信部组织第三方检测机构进行技术检测和检查。针对群众反映强烈的APP，将组织相关机构开展用户和专家评议。
结果处置阶段	2019年12月1日至12月20日	对存在问题的APP统一进行通报和处理。

（四）公安机关集中整治违法采集个人信息，100款APP被下架

2019年11月，公安部组织开展APP违法违规采集个人信息集中整治。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，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，正在开展侦查。公安部组织开展“净网2019”专项行动以来，已依法查处违法违规采集个人信息的APP共683款。

国家网络安全通报中心就此次整改发布了四起典型案例：

违法行为	查处机关	法律依据	处罚结果
“健康天津”APP涉嫌无隐私协议收集用户位置信息	天津市公安局武清分局网安支队	《网络安全法》第四十一条、第六十四条	行政警告并责令限期整改
“趋势密码”APP未经用户同意收集使用精准定位等个人信息，涉嫌超范围收集用户信息	上海市公安局徐汇分局网安支队	《网络安全法》第六十四条第一款	行政警告
“折疯了海淘”APP未明示数据项采集用途，涉嫌违规收集用户信息	杭州市公安局西湖分局	《网络安全法》第六十四条第一款	行政警告并责令限期整改
“简讯”APP涉嫌无隐私协议收集用户位置信息	成都市公安局网安支队	《网络安全法》第六十条第一款	行政警告并处罚款贰仟元

后记：

海问在网络安全、数据合规领域积累丰富的经验，亦持续关注不断更新的法律法规及与数据合规有关的时事热点。您可通过如下链接浏览此前发布的文章：

[《海问观察：网络安全及数据合规动态》（2019年9月上半月）](#)

[《海问观察：网络安全及数据合规动态》（2019年9月下半月-10月上半月）](#)

实习生朱安琪对本文亦有贡献。