

网络安全及数据合规动态（2020年1月-6月）：重要事件

作者：傅鹏

本动态涵盖对2020年1月至6月网络安全和数据合规领域的重要事件简述。

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、人民法院作出的典型判例

我们总结了2020年1月以来，人民法院在网络安全以及数据合规领域作出的具有代表性意义的如下司法判例：

认定事实	裁判依据及结果	简要评析
原告通过某支付软件开通个人征信服务，同时与被告签订了服务协议，原告授权被告可以向合法提供其用户信息的主体采集信息。后原告收到被告通过网络发出的执行案件信息。原告认为被告侵犯其隐私权，要求被告删除该信息，并赔偿其个人征信损失50000元。被告辩称，被告采集的被执行人信息来源为某高院，属于可公开内容，且被告提供的被执行人信息仅原告本人可以查阅，未侵犯原告隐私权。	法院经审理认为，被告向原告提供的服务是基于双方签署的服务协议，被告收集使用原告主体信息是在已取得原告同意的情况下进行的，且采集原告系被执行人的信息来自其他已合法公开的个人信息，并仅向原告本人提供了有关信息，属于对个人征信数据的合理化商业使用，不构成侵犯个人隐私权。	本案明确了商业使用用户数据的边界，对于收集于合法公开渠道的个人征信数据，可以被合理化的商业利用，既明确滥用个人征信数据的法律责任，也保护了信用经济的发展。
原告腾讯计算机公司、腾讯科技公司分别是微信软件的著作权人和微信产品的经营者。被告浙江某网络公司、杭州某科技公司开发、运营的“某群控软件”，利用Xposed外挂技术将该软件中的“个人号”功能模块嵌套于个人微信产品中，为购买该软件服务的微信用户在微信平台开展商业活动提供帮助。主要表现为：自动化、批量化操作微信的行为；监测、抓取微信用户账号信息、好友关系链信息以及用户操作信息（含朋友圈点赞评论、支付等）存储于其服务器，攫取数据信息。	杭州市互联网法院认为，被控侵权软件批量化操作微信、发布商业活动信息异化了个人微信产品的作为社交平台的服务功能，给用户使用微信产品造成了明显干扰，同时危及了微信平台的安全、稳定、效率，已妨碍、破坏了两原告合法提供的网络产品与服务的正常运行，属于《反不正当竞争法》第十二条第二款第四项所规定的妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为，构成不正当竞争。因此，判令两被告停止涉案不正当竞争行为，赔偿两原告经济损失及合理费用260万元，并为其消除影响。	该案由微信群控软件引发，系杭州互联网法院宣判的首例涉及微信数据权益认定的不正当竞争案。该案判决明确了网络平台对于其所控制的平台数据享有不同性质的数据权益，即网络平台对基于自身长期经营、投入形成的数据资源整体享有竞争权益，当该资源受到破坏性使用时，可以获得赔偿；而对单一数据个体权益而言如单一微信用户数据，尽管网络平台控制着该数据，其他方仍可在遵守“合法、正当、必要、不过度、征得同意”的前提下，使用该数据，网络平台不对该数据权益享有专有权。

二、市场监督管理部门的执法活动

我们总结了2020年1月以来，全国各地市场监督管理部门在网络安全以及数据合规领域作出的具有典型意

义的如下执法活动：

认定事实	处罚依据及结果	简要评析
江阴市某教育培训机构通过不明渠道获得涉及全市97所各类学校学生的个人信息14万余条。该培训机构还以在学校门口发放小礼品的方式采集学生姓名、家长电话等个人信息并拨打电话推销商业性教育培训服务， <u>部分未事先征得学生家长同意。</u>	依据《江苏省消费者权益保护条例》第六十二条的规定对当事人处以罚款30万元。此外，因涉案公民个人信息数量巨大，江阴市市场监管局依法将此案件线索移交当地公安局。	随着互联网的飞速发展，消费者个人信息逐渐成为一种重要资源，但是企业收集和使用消费者个人信息必须充分告知消费者使用目的、规则等内容，并获得其授权同意。
杭州某商务信息咨询有限公司的法定代表人欧阳某通过其原工作的单位、房屋销售跑盘及APP下载等途径收集了18万余条个人信息，并通过软件向个人推销贷款中介业务。欧阳某收集、使用上述个人信息均未经本人同意。	处罚决定书未说明处罚依据； 杭州市江干区市场监督管理局责令涉案当事人停止违法行为并对其罚款12万元。	企业应当加强内部数据管理，限制企业内部有关部门人员对企业数据的过度访问，规避企业内与信息数据职能履行无关的员工对企业数据的访问。
青岛市北区某楼盘销售中心，在消费者不知情的情况下，收集270名登记于其他楼盘场所的消费者信息并使用前述信息开展电话推销。	依据《中华人民共和国消费者权益保护法》的有关规定，给予当事人公司作出50000元的行政处罚。	企业应当注重对消费者的个人信息保护，不得在未经消费者授权的前提下转让或共享其个人信息，企业收集消费者个人信息亦应当获得其授权同意。

三、公安机关的执法活动

(一) 公安机关就部分主体侵犯个人信息行为进行处罚

认定事实	处罚依据及结果	简要评析
犯罪嫌疑人陈某借助在中山、江门某房产公司任职的便利，违法获取公民个人信息，并向郑某、姚某出售；犯罪嫌疑人郑某、姚某实施了非法购买公民个人信息的行为。	原报道未涉及处罚依据； 经检察院批准，上述3名犯罪嫌疑人已被依法逮捕，同时，高新警方对案件涉及的4家中介公司处以行政处罚。	就企业而言，其不得收集与企业提供的服务无关的个人信息；同时，企业应当完善其内部数据治理政策，限制企业员工对于企业内部数据及收集的个人信息的不当访问。
宿豫某健身中心在收集会员个人信息时未主动告知收集、使用信息的目的、方式和范围，未按照规定采用加密等技术措施处理及保存收集的个人信息。	根据《中华人民共和国网络安全法》第四十一条、第四十二条第二款、第六十四条第一款之规定，对其处警告处罚并责令改正。	企业收集个人信息时必须告知信息主体收集、使用信息的目的、方式和范围，并按照国家法律法规或标准的要求对收集到的信息采取必要的保护措施，如对个人敏感信息应当加密存储。
郑州某中等专业学校未履行网络安全保护义务，未制定内部安全管理制度和操作规程，未按照规定留存相关网络日志六个月，并因此遭受黑客攻击。	依据《中华人民共和国网络安全法》第59条规定，对该校给予10000元罚款的行政处罚，对该校网络安全负责人给予5000元罚款的行政处罚。	企业及其负责人应当注重对于数据保护和网络安全的内部制度建设，落实网络安全等级保护制度，制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。

(二) 公安部公布十起侵犯公民个人信息违法犯罪典型案例

2020年4月，公安部公布了2019年以来公安机关侦破的10起侵犯公民个人信息违法犯罪典型案例。

案件名称	违法行为
“20191023”“暗网”侵犯公民个人信息案	在“暗网”交易平台出售银行开户、手机注册等公民个人信息500余万条
“4·2”“暗网”侵犯公民个人信息案	利用系统漏洞盗取了1400余万条居民社保数据后，伙同在柬埔寨的违法犯罪人员在“暗网”上销售个人信息
吴某“暗网”侵犯公民个人信息案	利用暴力破解手段某汽车金融服务平台网站后台管理权限后，盗取30余万条公民个人信息并在“暗网”出售
高某“暗网”侵犯公民个人信息案	利用网站漏洞非法窃取某银行等单位网站上存储的6.02万条公民个人信息，并在“暗网”出售
“12·21”侵犯公民个人信息案	买卖公民个人手机信息、征信信息（查获各类公民个人信息43万余条）
赵某等人侵犯公民个人信息案	出售公民个人信息至下游电信网络诈骗、暴力催债、网络赌博等违法犯罪人员（查获各类公民个人信息1亿余条）
徐某等人公民个人信息被侵犯案	利用工作便利非法收集学生身份信息，开设实名手机卡后，向下游网络账号注册商、手机卡倒卖商销售个人信息（查获手机卡5万余张、“12306”账号100余万个）
梅某等人侵犯公民个人信息案	倒卖股民信息至境内外网络炒股诈骗团伙，供下游诈骗分子使用股民信息实施诈骗（查获股民信息300余万条）
杨某侵犯涉疫情公民个人信息违法案件	在工作中获取了社区疫情防控人员信息后向好友发送，导致相关信息在微信中迅速扩散，造成恶劣影响
王某侵犯涉疫情公民个人信息违法案	在工作中获取“新型冠状病毒感染肺炎防控重点人员台账”文件并发布于小区微信群中，随后被层层转发，造成恶劣影响

（三）公安机关网络安全部门发布违法收集公民个人信息十大案例

2020年第一季度，全国公安机关网络安全部门依法查处违法违规收集公民个人信息APP服务单位386个，涉及信息咨询、辅助学习、文学小说、新闻资讯、娱乐播报等多个类型，并在此基础上于2020年5月发布了违法收集公民个人信息的十大案例。

经过我们的总结，本次报道中的案例存在的主要问题情况统计如下表所示：

应用类型	存在问题	处罚结果
一款手机清理应用软件	没有详细说明索取用户通讯录、通话记录等权限的行为	责令改正违法行为
一款软件知识管理工具应用	未以显著位置、显著字体申明收集用户信息数据项，未明示各数据项收集用途	责令改正违法行为并予以警告处罚
一款医疗服务软件	未明示并征得用户同意，用户服务协议及隐私声明中未明示申请权限目的，未告知收集用户个人信息的目的及使用方式	责令改正违法行为并予以警告处罚
一款学习软件	在收集信息时未明示取得用户同意	责令改正违法行为并予以警告处罚
一款汽车生活服务软件	无收集信息明示且未取得用户同意，未向用户明示收集、使用个人信息的目的、方式、范围	责令改正违法行为
一款学习辅助软件	在部分第三方SDK组件中存在调用获取任务信息和读取联系人等两项权限的情况	责令改正违法行为
一款生活类电商服务软件	用户隐私协议中未向用户明示获取用户信息的详细用途及业务关联	责令改正违法行为并予以警告处罚
一款金融软件	应用隐私政策中未明示第三方SDK插件以及收集使用个人信息的目的、方式和范围	责令改正违法行为
一款综合瑜伽服务软件	未以显著位置、显著字体申明收集用户信息数据项	责令改正违法行为
一款数字填色游戏应用软件	超范围收集用户信息	责令改正违法行为

四、工业和信息化部（“工信部”）的执法活动

（一）工信部通报下架2019年第一批侵害用户权益App名单

2019年10月，工信部依法开展专项整治活动，并于2019年12月，通报了41家存在私自收集个人信息、过度索取权限等侵害用户权益行为的App企业的名单并督促其整改，详情可参见我们的文章：[《海问观察：网络安全及数据合规动态》（2019年12月）](#)

2020年1月3日，工信部发布“关于下架第一批侵害用户权益App名单的通报”，该通报显示，截至通报发布之日，仍有3款App未按工信部要求完成整改，工信部将依法要求相关应用商店立即对名单中应用软件进行下架处理；对于已经完成整改的App，工信部亦要求其于2020年1月6日12点前，在相关渠道更新整改后的App版本。本次通报中下架的应用软件名单如下：

软件名称	企业名称	下架版本
人人视频	武汉映象网络科技有限公司	4.3.3/4.3.4
春雨计步器	北京春雨天下软件有限公司	2.5.4
微唱-原创音乐	北京精奇互动科技有限公司	1.1.0

（二）工信部通报2019年第二批存在侵害用户权益行为的App

根据工信部于2020年1月8日发布的“关于侵害用户权益行为的App（第二批）通报”，截至通报发布之

日，尚有15款App未就个人信息收集的违法违规行为完成整改。工信部要求该等App应在2020年1月17日前完成整改工作，逾期未完成的，工信部将依法依规对其进行处罚。

经过我们的总结，本次通报中的侵害用户权益App存在的主要问题及对应的存在该问题的App数量统计如下表所示：

问题类型	存在此问题的App数量	占比
私自收集个人信息	9	60%
私自共享给第三方	8	53%
不给权限不让用	6	40%
过度索取权限	3	20%
账号注销难	3	20%
强制用户使用定向推送功能	1	7%

本次通报的第二批侵害用户权益的App的主要问题类型集中于“私自收集个人信息”与“私自共享（个人信息）给第三方”，工信部亦表明后续将以专项整治行动为契机，持续加强对App的监督检查，形成常态化监管机制。

（三）某社交媒体App因数据泄露被工信部约谈

2020年3月21日，某社交媒体App因用户查询接口被恶意调用导致App数据泄露问题被工信部网络安全管理局约谈。

工信部要求某社交媒体App应按照相关法律法规要求，并对照工信部等四部门制定的《App违法违规收集使用个人信息行为认定方法》，采取有效措施，消除数据安全隐患，包括加强用户信息分类分级保护，强化用户查询接口风险控制等安全保护策略；加强企业内部数据安全治理，定期及新业务上线前要开展数据安全合规性自评估；在发生重大数据安全事件时，及时告知用户并向主管部门报告。

（四）工信部通报2020年第一批侵害用户权益行为APP

2020年5月15日，工信部通报了在其组织的检查活动中存在问题且尚未完成整改的16款APP，并要求此16款APP在5月25日前完成整改落实工作，否则将采取相关处置工作。

经过我们的总结，本次通报中的APP存在的主要问题情况统计如下表所示：

问题类型	存在问题App数量	占比
私自收集个人信息	13	81%
私自共享给第三方	5	31%
超范围收集个人信息	4	25%
不给权限不让用	5	31%
强制用户使用定向推送功能	3	19%
过度索取权限	6	38%
账号注销难	3	19%

（五）工信部通报2020年第二批侵害用户权益行为APP

2020年7月3日，工信部通报了在其组织的检查活动中存在问题且尚未完成整改的15款APP，并要求此15款APP在7月14日前完成整改落实工作，否则将采取相关处置工作。

经过我们的总结，本次通报中的APP存在的主要问题情况统计如下表所示：

问题类型	存在问题App数量	占比
私自收集个人信息	10	67%
私自共享给第三方	6	40%
超范围收集个人信息	3	20%
不给权限不让用	2	13%
强制用户使用定向推送功能	5	33%
过度索取权限	6	40%
账号注销难	2	13%

五、互联网信息办公室的执法活动

(一)天津市委网络安全和信息化委员会办公室发布疫情防控App专项通报

2020年3月，中共天津市委网络安全和信息化委员会办公室开展对疫情防控类App的专项治理活动，并于2020年3月16日对存在收集使用个人信息违规问题的7款App发布了专项治理情况通报，其中涵盖了对数款小程序违规问题情况的通报。

经过我们的总结，本次通报中的App存在的主要问题情况统计如下表所示：

问题类型	存在问题App数量	占比
收集用户个人信息时，未同步告知用户信息使用目的	7	100%
未向用户提供个人信息更正、删除功能或未提供投诉、举报渠道	7	100%
在App或小程序中无法找到隐私政策	5	71%
以默认选择同意等非明示方式取得用户对隐私政策的同意	2	29%
未通过弹窗等明显方式向用户显示隐私政策	1	14%

(二)关于防疫服务类和复工复产类App的数据安全隐患的测评结果

国家互联网信息办公室（“网信办”）对市场上出现的防疫服务类和复工复产类App进行了测评，并于2020年3月22日发布了测评结果——“助力防疫抗疫、复工复产，App数据安全不容忽视”，对该等App的典型数据安全隐患进行了分析并提出了相关建议。

经过我们的总结，防疫服务类和复工复产类App存在的主要数据安全隐患和违规问题如下表所示：

软件类型	关注要点	违规事例列举
防疫服务类 (如医药产品网购平台)	医疗和健康隐私数据的保护	某医药平台App在首次启动、登录、注册界面未以显著方式提示用户阅读隐私政策。
		某医药平台App申请收集个人信息权限未同步说明使用目的。
在线教育类	未成年人信息的保护	某在线教育App在隐私政策中提及的收集使用个人信息类型和其业务功能对应关系不清。
		某作业辅导App在申请可收集个人信息的定位、存储权限时，未同步说明目的。
		某在线教育App无明确的隐私政策更新机制及通知用户方式。
远程办公类	员工信息及企业核心数据的保护	某视频会议App在用户注册账号时，未经用户自主操作，默认勾选“阅读并同意”选项。
		某协同办公App将隐私政策夹杂在服务条款中，且未在隐私政策中逐一描述收集使用个人信息的类型、目的等规则。
		某协同办公App功能界面、客服电话、电子邮箱等各渠道均无法要求删除文档、个人信息等数据。
		某网络会议App启动、登录、注册界面均未提示用户阅读其隐私政策。

针对上述App的安全隐患，测评发布者建议移动App使用过程中可能涉及个人敏感信息、企业核心数据的，其运营公司应实现产品的快速迭代，完善产品防护机制；企业用户一方面应结合自身管理制度，规范各项工作的开展，梳理数据资产实施分类分级管理，提升企业数据安全风险管控能力；另一方面需加强员工数据安全教育培训，确保员工使用过程的数据安全，防止由于意识不到位导致的安全事件。

六、其他国家机关的立法实践或执法活动

(一)2020年度司法解释立项计划明确提出“个人信息权”概念

最高人民法院办公厅于2020年3月19日印发《最高人民法院2020年度司法解释立项计划》（法办[2020]71号），计划2021年上半年完成《关于审理个人信息权纠纷案件适用法律若干问题的解释》。

这是法律法规、司法解释中首次明确提出“个人信息权”的概念。此前，法律法规、司法解释未明文规定“个人信息权”这一法定权利。《中华人民共和国民法总则》（“民法总则”）第一百一十一条规定，“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”。该规定被视为全面开展个人信息保护立法的重要信号。尽管如此，该条款中，也未将“个人信息”明确为“个人信息权”这一法定权利，与民法总则明文规定的物权、肖像权、名誉权、荣誉权、隐私权等法定权利似有不同。本次《关于审理个人信息权纠纷案件适用法律若干问题的解释》的最终成文值得期待，其应有利于在司法审判实践中进一步加强个人信息保护，明确个人信息收集者的合规边界。

(二)国家计算机病毒应急处理中心监测发现25款违规移动应用

2020年4月10日，国家计算机病毒应急处理中心在“净网2020”专项行动中发现并公布了25款存在隐私不合规行为的外卖、医疗和在线教育类移动应用。

经过我们的总结，本次报道中的移动应用存在的主要问题情况统计如下表所示：

问题类型	存在问题App数量	占比
未向用户明示申请的全部隐私权限	21	84%
未说明收集使用个人信息规则	2	8%
未提供有效的更正、删除个人信息及注销用户账号功能	2	8%

(三)APP专项治理工作组发布《APP违法违规收集使用个人信息专项治理报告（2019）》（“《APP治理报告》”）

2020年5月26日，APP专项治理工作组发布了《APP治理报告》。《APP治理报告》指出，2019年各部门深化APP个人信息安全治理工作，其中，工信部开展的“APP侵害用户权益行为专项整治行动”，共对236款APP运营者下发了整改通知书，并公开通报56款APP、下架3款APP；公安部开展的“净网2019”专项行动，共检测评估3.1万余款APP，依法整改2090款APP，依法查处1121款APP，集中曝光了100款存在违法违规收集使用个人信息行为的APP；国家市场监督管理总局开展的“守护消费”暨打击侵害消费者个人信息违法行为专项行动，共立案查处各类侵害消费者个人信息案件1474件，查获涉案信息369万余条，罚没款1946万余元，组织执法联动4225次，开展行政约谈3536次。

《APP治理报告》还指出，2020年将持续开展APP举报受理和检测评估工作，并拟将APP治理关注范围从APP自身扩展至移动设备生产商（手机厂商）、APP分发平台（应用商店）、第三方（第三方SDK、合作伙伴）等多方主体构建成的移动生态整体。

(四)中国人民银行公布首批拟备案金融类APP名单

2019年9月，中国人民银行发布了《中国人民银行关于发布金融行业标准加强移动金融客户端应用软件安全管理的通知（银发〔2019〕237号）》，要求金融机构按照规范对APP进行整改，并向中国互联网金融协会进行备案。

2019年12月，中国互联网金融协会启动了客户端软件实名备案工作。客户端软件备案工作启动以来，各金融从业机构积极向协会登记有关备案信息。

2020年5月19日，经综合审核并结合相关机构测评和公示情况，中国互联网金融协会公布了首批拟备案的金融类APP名单，该名单涉及工商银行、支付宝、微信等33家机构73款移动金融客户端应用软件。

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的《海问观察：网络安全及数据合规动态》：

[《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）](#)

[《海问观察：网络安全及数据合规动态》（2019年10月下半月-11月）](#)

[《海问观察：网络安全及数据合规动态》（2019年12月）](#)

[《海问观察：网络安全及数据合规动态》（2020年1月-6月）：监管规则（上）](#)

[《海问观察：网络安全及数据合规动态》（2020年1月-6月）：监管规则（下）](#)

2020-08-07