Open Journal of Legal Science 法学, 2021, 9(3), 295-302
Published Online May 2021 in Hans. http://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2021.93041

Hans汉斯

隐私权视角下手机APP过度收集利用个人信息的法律规制

郑兆钧，马　锐，宋阁阁，张钰松

温州大学，浙江　温州
Email: mr124578@163.com

收稿日期：2021年3月25日；录用日期：2021年4月6日；发布日期：2021年5月12日

摘　要

APP对用户个人信息的过度收集利用已经成为当代侵犯公民个人隐私的重要因素，甚至诱发诸如信息贩卖、信息网络诈骗等违法犯罪行为。而APP过度收集个人信息原因包含信息的经济利益链条驱使、法律法规尚未完善、司法救济尚不成熟、行政监管难以到位以及民众维权意识尚浅等因素。为了保护公民对个人信息的隐私权，应当加强行政监管，集中监督权力、提高监督效力，建立黑名单制度，设立民事公益诉讼制度，帮助用户维护合法权益，同时完善和补充刑法关于侵犯公民个人信息罪的规定，加强宣传教育，建立行业协会，更好地对APP行业发展进行引导和规制。

关键词

个人信息，过度收集，隐私权

The Legal Regulation of Over Collection and Utilization of Personal Information by Mobile APP from the Perspective of Privacy

Zhaojun Zheng, Rui Ma, Gege Song, Yusong Zhang

Wenzhou University, Wenzhou Zhejiang
Email: mr124578@163.com

Received: Mar. 25th, 2021; accepted: Apr. 6th, 2021; published: May 12th, 2021

文章引用: 郑兆钧, 马锐, 宋阁阁, 张钰松. 隐私权视角下手机APP过度收集利用个人信息的法律规制[J]. 法学, 2021, 9(3): 295-302. DOI: 10.12677/ojls.2021.93041

Abstract

The excessive collection and utilization of user's personal information by APP has become an important factor that infringes citizens' privacy, and even leads to illegal and criminal behaviors such as information trafficking, information network fraud and so on. The reasons for the excessive collection of personal information by APP include the drive of economic interest chain, the imperfection of laws and regulations, the immature judicial relief, the difficulty of administrative supervision and the shallow awareness of people's rights protection. In order to protect citizens' right to privacy of personal information, we should strengthen administrative supervision, centralize supervision power, improve supervision effectiveness, establish blacklist system, establish civil public interest litigation system, help users safeguard their legitimate rights and interests, improve and supplement the provisions of criminal law on the crime of infringing citizens' personal information, strengthen publicity and education, and establish industry associations, so as to better promote the development of APP industry to guide and regulate.

Keywords

Personal Information, Over Collection, Rights of Privacy

1. APP 对于公民个人信息收集及处理现状

(一) 过度收集个人信息屡禁不止

截至 2021 年 1 月 22 日，工信部共发布 10 批“关于侵害用户权益行为的 APP”报，在最近五期共 512 个被通报的 APP 名单中，“违规收集个人信息”占 82.65%，“违规使用个人信息”占比 25.89%，“APP 强制、频繁、过度索取权限”占比 23.79%，其中不乏存在芒果 TV、京东、腾讯动漫等高知名度和受众的 APP 违规收集或使用个人信息问题。在开展的问卷调查中，60%的用户表示上述三个问题均有遇到，且有 81%的用户认为常用的 APP 存在过度收集隐私的问题。

APP 为了尽可能多地获取相关信息，往往通过对隐私条款笼统概括、频繁索取权限，限制使用功能等手段诱使用户授权大量与所提供服务无直接关联的个人信息[1]。虽有相关监管部门不断加大对 APP 的监管力度，规范 APP 授权范围和方式，但目前我国关于此类信息安全尚未形成完善的法律规制体系，司法救济途径尚未完全成熟，再加上 APP 市场庞大的使用基数，使得过度收集个人信息的现象屡禁不止。

(二) 个人信息利用不当的现象屡见不鲜

部分 APP 过度收集个人信息的目的并非简单地获取相应权限服务用户，而将其作为信息共享牟利的手段。个人信息的不当利用主要有两种。一种是信息共享：在工信部公布的第三期 58 个违规 APP 名单，31 个 APP 存在私自共享给第三方，如速聘 58 赶集网、B612 咔叽、荔枝新闻等。而在问卷中也有 78%的人表示遇到过 APP 使用记录共享(如在浏览器搜索的物品会被购物软件及时推荐)。一种是信息贩卖：2020 年 1 月 23 日镇江丹阳警方侦破一起重大个人信息贩卖案件，涉案 6 亿条个人信息，获利 800 余万。南方周末曾于 2019 报道中提及以非法获取公民个人信息为上游，以买卖公民个人信息为中游，以利用公民个人信息实施网络诈骗等为下游，已经形成了一条完整的网络侵犯公民个人信息黑灰产业犯罪链条。除 APP

自身有收集信息贩卖之嫌，黑客攻破 APP 数据库获取其过度收集的个人信息并将其不断倒卖也是个人隐私泄露的一条重要途径，而这条灰色产业链下的个人信息若落入不法分子手中，也会进一步导致大规模电话诈骗的出现，严重危害社会稳定和人民群众生命财产安全。

(三) 个人信息存在不可撤销风险

公民在不再使用软件时可以选择及时注销账号信息甚至注销其授权的个人信息，是保护个人信息的重要措施。工信部虽然要求电信业务经营者、互联网信息服务提供者应当严格遵守国家法律法规要求，在用户终止使用服务后，为用户提供注销账号的服务。然而部分 APP 提供的该功能形同虚设，例如通过不断设置卡顿、闪退、限制性条件等障碍，使用户陷入“找不到”、“注销难”的窘境不得不放弃注销，更遑论注销其授权的个人信息。个人信息的授权是单向且不可逆的，而个人信息的撤回是困难甚至难以实现的，而公民个人信息的过度收集是不当利用甚至难以撤销的起点，因而制约 APP 过度收集公民个人信息具有现实性和紧迫性。

2. APP 过度搜集公民个人信息原因分析

APP 过度收集个人信息，不仅侵害其隐私权，更是助长信息贩卖黑色链条的壮大，甚至进一步导致利用信息的诈骗犯罪。APP 过度收集利用公民个人信息本身已然成为社会痛点，究其原因主要包含以下方面。

(一) 公民个人信息的经济利益链条驱使

大多数 APP 以商业化运营为功能导向，必然需要用户大量的身份、位置、资金、喜好等信息，甚至包含银行账户密码等。同时，个人信息被不法利用的现象难以被信息所有者本人发觉，隐蔽的侵权方式与之巨大的利润空间形成鲜明的对比，使得大量 APP 打起信息买卖的主意，其中小众 APP 更是严重。而信息贩卖存在传导，上下游之间的信息传递使得信息泄露的规模如同滚雪球，越来越大，这也是如今破获的犯罪中动辄几千万甚至上亿条信息被转手贩卖的原因。其次，此类信息经过加工处理，信息又会被以个人画像的形式二次出售，使得每个单一的用户隐私均受到极大侵害。对于不法分子而言，成熟的上、中、下游信息交易产业链以及其产生的巨大灰色收入成为部分不法 APP 公司敛财的手段甚至是主要收入来源。

(二) 相关部门对违规 APP 监管难以到位

根据工信部最新资料显示，截至 2020 年 11 月末，我国国内市场上监测到的 APP 数量为 346 万款。其中游戏类应用规模保持领先，占全部 APP 比重为 25%，日常工具类、电子商务类和社交通讯类 APP 数量占全部 APP 比重分别为 14.6%、10%和 8.7%，其他生活服务、教育等 10 类 APP 占比为 41.6% [2]。而最容易被曝光发生侵权问题的也是这些类别的软件。

在软件具有的高速更新改版特点的背景下，面对如此庞大的 APP 市场，行政部门的监管便显得困难重重。目前对 APP 的主要监管部门为工信部，其主要通过 APP 违规收集个人信息的方式主要在于通报违法侵害公民信息 APP 名单和下架未及时整改的 APP，并发布相关部门工作文件等途径解决问题。如 2019 年 11 月 28 日四部门发布《关于印发<APP 违法违规收集使用个人信息行为认定方法>的通知》、2020 年 7 月工信部开展纵深推进 APP 侵犯用户权益专项整治行动。随后 2020 年 9 月《全国信息安全标准化技术委员会秘书处关于发布<网络安全标准实践指南——移动互联网应用程序(APP)系统权限申请使用指南>的通知》。而行政处罚的力度较小，处罚难度较大，且法律依据效力较低，再加上部分地区 APP 进入市场的审核不够严苛，导致 APP 仍旧有较大侵权空间。

(三) 相关法律法规尚不够完善

虽然我国有关个人信息安全的法律法规和行业规范均有部分涉及，但能够起到提纲挈领和体系协调

作用的“个人信息保护法”尚未出台，公民个人信息权益保护方面的立法任务仍然任重道远。体现在对于APP经营者有关个人信息保护的法律义务缺乏明确规定，以及各法律关于该领域规定存在诸多不衔接、不协调问题[3]。

目前与个人信息保护相关的法律主要但不局限于以下几位：《网络安全法》要求对个人信息收集的最小限度原则；《民法典》第1035条规定的处理个人信息应当遵循合法、正当、必要的原则，并应征得同意。《刑法》第253条之一规定违反国家有关规定，向他人出售或者提供公民个人信息将依法受到处罚，并将其从特定主体扩大为一般主体。司法解释又将“公民个人信息”，界定为以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括账号密码、行踪轨迹等[4]。除上述外还包括尚文提及的各项部委文件、以及各种国家行业标准等。

法律体系的不成熟，使得出现APP过度侵害公民个人信息以至于侵害公民隐私权救济缺乏明确的法律依据，虽然专项立法已列入2021年度立法计划，但在正式法律确立并颁布施行前，公民个人信息被侵害仍无明确的处罚标准，足够的惩罚力度，虽有刑法253条之一对贩卖个人信息的犯罪行为进行处罚，但是对于不同APP之间的信息共享显然仍处于尴尬的境地。

(四) 相关个人信息隐私权认定及司法救济尚不成熟

首先是隐私权侵权行为的认定，隐私权原则上仅保护具有隐私属性的“个人信息”，而APP收集的用户信息为经权利人许可而获得，暗含权利人放弃其隐私，视为明知个人信息将被不特定的主体收集、挖掘、分析之意。而司法裁判往往也排除仅侵害个人信息自决权的侵权行为。其次，隐私权侵权认定要求对个人隐私权存在明显实质侵害。但APP侵害个人用户隐私权行为过于隐秘，往往难以察觉和被证明，法院也难以仅就过度收集个人信息便认定侵犯其隐私权，并且司法实践将关联APP个人信息共享行为排除在规制范畴之外。

但是法律的价值在于维护和实现公平正义，而企业违法收集利用个人信息，却可以侥幸逃脱其本应承担的法律责任。一方面为诉讼中发现被侵权难、取证难、成本高、获赔难。个人诉讼成本高、证据取得难、同时司法审判成本也高，而相关集体诉讼或者代表诉讼方式尚未被发掘。另一方面即使胜诉，若因APP已及时纠正违法行为或者赔礼道歉就可以免于处罚，那么已经受到隐私权损害的用户来说，既往的损失仍在，受损的利益也未得到有效赔偿[5]。因此司法救济动力不足也成为APP侵害和非法利用个人信息的重要原因。

(五) 个人对于权利的自我保护意识薄弱

我国民众目前对APP侵害个人隐私权的行为缺乏维权意识，用户自愿起诉公司侵权的行为更是少之又少。不知被侵权、取证难、侵权成本高等问题使用户即使知道被侵权也会选择忍耐。而个人对抗企业存在实力的巨大差异，这也大大打击个人权利保护的自信心。其次，面对互联网世界大数据的共享及获取，被侵权已成为常态，长期未得到有效解决的现状使得用户习惯性妥协，甚至在潜移默化中接受了“互联网世界没有隐私”的观点。即使明知APP侵权，但基于需求仍会继续使用，或者难以承受频繁索取权限而接受APP授权请求。总之，个人对APP收集个人隐私的不重视，以及无奈妥协，使得APP过度收集个人隐私更加肆无忌惮。APP侵权存在侵害规模大、胜诉比例低、诉讼动力不足的特点，个人信息司法救济路径受阻，用户个人信息维权存在多重阻碍[6]。

3. 公民个人信息和隐私保护途径探究

(一) 重点加强对APP市场的行政监管

1) 集中监管权力，提高执法效率

当前我国对于APP个人信息收集使用的监管主要分布在网信办、工业和信息化部、公安部和国家市

场监管总局四个部门，除此之外国家发改委等十余个部门在这方面也具有行政监管权与执法权[7]，部门与部门之间的权责界线不够清晰，执法尺度和标准不完全统一，很难保证不会出现责任推诿或重复监管的情况，这不仅给用户权益的保护增加难度，也容易对 APP 开发者造成不必要的负担。因此应当将监管权力集中在一个部门机构或者建立专门的监管机构，设置明确的执法规则和标准，定期检查与不定期抽查的方式相结合，及时发布检查公告达到警示 APP 开发者和提高用户警惕性的目的，一旦发现 APP 的违法违规行为，行政部分自行处理，刑事部分可交由公安部门或者双方联合处理，提高执法效率。

2) 严格 APP 上架审查机制，从源头控制问题出现

由于当前我国缺乏对 APP 收集个人信息的详细标准和审查规定，因此大多数 APP 采取的都是所谓的“一揽子授权”，即“一次授权、全部授权、长期有效”，这样的授权模式显然对用户是不公平的，因此可以参考欧盟《通用数据保护条例》(GDPR)的规定，通过行政法规明确限制法律认可的数据收集的合法性事由，迫使 APP 企业在收集信息之初就必须符合法律规定的条件，且不能在用户授权后随意更改所依据的使用目的。其次采取“专项专用”模式，即基于一种法定原因的授权仅仅适用于该收集目的，对于其他的应用方面并不是先天成立的，需要针对性的再次申请授权。

同时需要配备相应的审查制度，即建立 APP 上架个人信息收集报备制度，由开发者列明需要收集的信息并对必要性和需求性进行说明，为什么要收集这些隐私信息，如果可能的话，哪些第三方可能会分享这些收集到的隐私信息[8]，经审查认为违规或确无必要责令其进行修改，修改合格后准予上架，除此之外 APP 之后的更新如涉及到与报备信息不同之处需要及时进行补充报备，以防 APP 假借更新之名逃避监管，侵犯用户隐私。

3) 完善黑名单制度，加大违法成本

不仅要设置 APP 黑名单，同时可以设置开发者黑名单。例如目前有部分开发者在 APP 被责令下架整改之后，将 APP 的名称、图标、域名等更换再次上架，相当于给 APP“换了件衣服”，但实质内容并无变化；或者开发的多款 APP 基本都存在侵犯用户隐私的情况，甚至整改之后依旧不合格，因此黑名单制度不仅要包括 APP 黑名单，同时还要对其开发者进行及时追踪，一旦发现背后的开发者具有上述行为或者其他类似行为，则将开发者加入黑名单并进行警告或处分，同时加大惩罚力度，例如增加罚款数额，要根据收集的信息规模或者非法收益等进行罚款，使得开发公司看到数额就望而却步，同时如果 APP 开发主要负责人没有尽到审慎检查注意的义务，还要对其个人追究行政责任，根据情节进行行政警告、行政罚款等。

(二) 完善 APP 侵权的民事救济途径

1) 当前 APP 侵犯公民隐私权的民事救济困境

用户难以知晓自身权益受到侵犯，取证难度大。通常情况下 APP 收集到信息之后的任何操作和处理用户都是一无所知的，如果掌握信息的开发公司真的将用户信息泄露出去甚至进行非法买卖交易，用户也无从知晓。而且我们所使用的每一个 APP 都可能是信息泄露的源头，但却难以确定泄露个人信息的具体 APP，既难以意识到侵权行为的存在，又没有充分有效的证据证明就是该 APP 侵犯了用户隐私，维权的难度自然十分巨大。

2) 走出困境的途径——参照公益诉讼制度

长久以来 APP 用户维权难的问题主要来自于双方的实力不对等，一方是普通的 APP 个人用户，一方是掌握技术的 APP 开发公司，实力和地位的差距显而易见，因此首先要解决的问题就是缩小双方在诉讼中的实力差距，对此我们可以参照现行法律中有关公益诉讼的规定。

当前我国缺少针对 APP 开发者的民间组织，然而 APP 开发者及产品众多，APP 侵犯用户隐私的现象屡禁不止，只靠行政部门的监管是远远不够的。因此，需要政府帮助和扶持建立相关的民间组织，既

能减轻行政部门的监管压力，同时民间组织的灵活性使其能够发现行政部门难以观察到的死角，二者共同对 APP 进行监督，更好的维护用户的合法权益。

首先此类民间组织应当以保护 APP 用户合法权益为设立宗旨，对 APP 开发者行为的合理性合法性进行监督和引导，同时对于用户个人起诉 APP 开发公司或者集体诉讼的案件应当积极地提供帮助，例如派专人出庭或者提供专业的诉讼指导和法律意见，帮助用户撰写法律文书等，开通举报热线和网上举报途径，经主动监督和用户举报一旦发现和查实 APP 侵犯公民合法权益的现象就启动以下途径：

第一，向社会发出公告，告诫广大用户群体提高警惕，同时向行政部门进行报告，行政部门接到报告之后根据实际情况和相关法律法规对违法违规的 APP 开发者进行处理，并将处理结果向社会公布。

第二，参照《消费者权益保护法》中公益诉讼相关规定代表用户提起公益诉讼。APP 侵犯用户隐私权的案件一般具有以下特点，即通常情况下用户难以发现自身权益受到侵犯，即使意识到了很多用户也会因为自身和 APP 公司之间的差距以及诉讼难度而放弃起诉，长此以往将导致 APP 侵犯用户隐私权的现象愈发猖獗，这些特点与商家侵犯消费者权益的案件具有相似性，因此可以参考消法中有关公益诉讼的规定，由实力可以与 APP 开发公司抗衡的民间组织代表广大用户对 APP 公司提起诉讼，维护用户合法权益，有效遏制此类现象的发生。

除此之外还可以由检察院作为提起诉讼的补充主体，对于没有公民、法人或其他组织提起的 APP 侵犯用户隐私权的案件可以由检察院提起公益诉讼。

(三) 完善 APP 侵犯公民隐私权的刑法相关规定

我国刑法第 253 条之一对侵犯公民个人信息犯罪做出了规定，针对这一规定学界目前正在进行广泛的探讨，各路学者观点的碰撞也较为激烈，在此选取两个与本文联系密切的重要问题进行讨论并提出建议。

1) “向他人提供”的范围界定

刑法 253 条之一第一款规定“违反国家有关规定，向他人出售或者提供公民个人信息，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；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金”。那么如果两个不同的 APP 同属一家开发公司，用户只注册了其中一个，该 APP 向另一个 APP“共享”了用户个人信息是否属于这里的“向他人提供”？《消费者权益保护法》等相关法律法规均未做明确规定，收集、使用公民个人信息者，未经本人同意不得提供给他人，其中也当然包括本案中 APP 运营公司内部之间的所谓“共享”行为，这种“共享”其实是过度滥用或不当泄露，既不正当又不合法[9]。归根结底用户只对一个 APP 进行了授权，当然只允许被授权的 APP 收集和使用个人信息，提供信息的一方没有获得用户的同意，以侵犯用户知情同意权的方式将用户个人信息提供给另一个 APP，无论是否同属一个公司都是侵犯了用户的隐私权，具有侵权行为性质，情节严重的可能构成犯罪。

2) 过度收集与过失泄露个人信息能否成为入罪理由

《个人信息刑案解释》设定了侵犯公民个人信息罪“情节严重”“情节特别严重”的定罪标准，采取了“混合型”认定模式，列举了包括个人信息的类型、数量、用途，犯罪行为违法所得等诸多方面，其中不乏人身危险性、社会影响恶劣等要素[10]。如果只是单纯的过度收集个人信息，但没有将其提供给任何第三方并进行妥善保管，那么此种行为因缺乏社会影响所以不应该入罪；如果是合理收集用户个人信息但因过失导致信息泄露，例如遭遇黑客攻击，那么因 APP 开发公司缺乏危险性所以也不该入罪；然而假如 APP 既过度收集了用户的个人信息又使得信息泄露，即使是过失也应当入罪，因为在此种情况下 APP 过度收集个人信息本身具备危险性，同时信息泄露可能会对用户造成不利后果，具有比较恶劣的社会影响，因此如果 APP 开发者过度收集个人信息后又遭信息泄露，那么可以参照刑法 253 条之一的规定，对单位和主要负责人进行处罚。

(四) 其他方式和途径

1) 加大宣传力度，提高用户警惕

解决 APP 侵犯公民隐私权的问题需要多方共同努力，不仅需要有关部门对开发者的严格有效监管，同时也需要用户提高警惕。当前用户对“互联网世界无隐私”这一情况的默认无疑助长了 APP 侵犯隐私权的嚣张气焰，政府部门、各大媒体以及其他相关组织应当积极宣传和号召，提高用户在使用 APP 时的隐私保护意识，向用户普及一些基本常识，例如哪些类型的 APP 最容易出现过度收集信息的情况？各类 APP 收集哪些个人信息是必要的？哪些是不必要的？什么类型的个人信息在授权时是需要谨慎思考和注意的等等。这些问题很多用户在使用时由于缺乏专业知识和警惕性，在 APP 请求授权时甚至连内容都没有仔细观看就一股脑的全部授权，这显然是不利于用户隐私权的保护。因此需要对用户加强宣传教育的力度，提升用户的隐私保护意识，在下载 APP 时仔细筛选是否有更好的同类 APP 可以替代，在使用时要注意浏览阅读隐私政策，对每一条授权内容都要仔细思考其必要性后再做决定，坚决不能一次性全部授权，打破“互联网世界无隐私的”错误常态。

2) 成立行业协会，引导行业发展

互联网行业迅猛发展的今天 APP 开发公司犹如雨后春笋般不断涌现，截至 2020 年 11 月末我国国内市场上监测到的 APP 数量为 346 万款，这一数字在未来还会不断扩大，面对如此庞大的规模需要一个有力的组织帮助和引导行业始终走在正确的发展方向，基于 APP 开发的专业性，成立专业且权威的行业协会并由行业协会引导 APP 开发行业的发展无疑是最佳选择。

行业协会应当明确告知 APP 开发者将用户的体验感受放在首位，坚决杜绝过度收集和利用用户个人信息的行为，坚决打击霸王条款，即用户必须进行一次性全部授权的行为，除进行行业自查外配合行政部门或者联合其他组织对 APP 进行监督和检查，一旦发现违规行为向社会公告并进行相应的行业处罚，例如取消年度评优资格、APP 上架限制即几年内不得上架新的 APP 或者数量限制等；制定行业标准引导 APP 正向发展，设立相关奖项奖金和 APP 优秀名单，定期审查更新名单并向社会公布，不仅能鼓励开发者做出更优秀的产品，同时为广大用户提供参考和选择。

4. 结语

APP 市场的繁荣的确为人们的生活提供了很大的便利，但是繁荣的背后所蕴藏的风险绝对不能忽视，APP 对用户个人信息过度收集和利用的现象屡见不鲜却又屡禁不止，归根结底是其投入成本低、风险低但收益高，因此才会有众多 APP 开发者“前赴后继”，不顾企业的名誉不断侵犯用户合法权益，因此我们必须加重违法成本，严厉打击其嚣张气焰，引导行业向更加合理合法的正确方向发展。隐私权作为宪法赋予每个公民的权利，遏制 APP 侵犯公民隐私权的现象就是保护公民的宪法权利，就是在维护宪法的权威。

参考文献

[1] 郜江丽. 关于 APP 收集个人信息实务及规范研究[J]. 北京航空航天大学学报(社会科学版), 2019(4): 7.

[2] 工信部. 2020 年 1-11 月互联网和相关服务业运行情况[EB/OL]. https://www.miit.gov.cn/gxsj/tjfx/zh/art/2021/art_a88cae7dcb564ea89e8459663c9dbe47.html, 2021-01-20.

[3] 张勇. APP 个人信息的刑法保护: 以知情同意为视角[J]. 法学, 2020(8): 113-126.

[4] 孙道萃. 非法获取 APP 数据行为的刑法教义学分析[J]. 人民检察, 2018(7): 32-36.

[5] 戴龙. 论数字贸易背景下的个人隐私权保护[J]. 当代法学, 2020, 34(1): 148-160.

[6] 陈晨, 李思頔. 个人信息的司法救济——以 1383 份“APP 越界索权”裁判文书为分析样本[J]. 财经法学, 2018(6): 102-113.

[7] 郜江丽. 关于 APP 收集个人信息实务及规范研究[J]. 北京航空航天大学学报(社会科学版), 2019, 32(4): 7-12.
[8] 高荣林. 手机 APP 侵犯用户隐私的规制——来自美国的经验[J]. 云南警官学院学报, 2016(4): 79-84.
[9] 张勇. APP 个人信息的刑法保护: 以知情同意为视角[J]. 法学, 2020(8): 113-126.
[10] 石聚航. “侵犯公民个人信息罪情节严重”的法理重述[J]. 法学研究, 2018, 40(2): 62-75.