**Dispute Settlement** 争议解决, 2023, 9(5), 2007-2017
Published Online September 2023 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2023.95272

Hans汉斯

# 大数据时代下个人信息保护的法律实证研究

## ——以APP强制授权和过度授权为例

**文玉琴，林　禄**

浙江师范大学法学院，浙江　金华

收稿日期：2023年6月25日；录用日期：2023年8月19日；发布日期：2023年8月29日

## 摘　要

**随着网络技术的迅速发展，APP已成为人们使用网络信息服务必不可少的载体。但我们也应看到APP强制授权和过度授权对个人信息安全及网络安全等各方面带来的极大危害。利用国家、企业、行业协会及行业组织、用户及大众媒体四大主体之间的联动配合对其进行有效规制。国家要完善立法，加强行政监管，推动司法实践。企业要强化保护意识，采取切实可行的保护措施，积极承担不法责任。行业协会及行业组织要完善行业自律机制，加强行业监管。消费者要树立个人信息保护意识和维权意识，大众媒体要承担起媒体监督的责任，加大个人信息保护宣传力度。利用这四大主体，建立“四位一体”的规制体系，将对根治APP收集个人信息乱象产生重要意义。**

## 关键词

**APP，个人信息，强制授权，过度授权，四位一体**

# An Empirical Legal Study of Personal Information Protection in the Era of Big Data

## —Taking Mandatory Authorization and Over-Authorization of APP as an Example

**Yuqin Wen, Lu Lin**

Law School, Zhejiang Normal University, Jinhua Zhejiang

Received: Jun. 25th, 2023; accepted: Aug. 19th, 2023; published: Aug. 29th, 2023

## Abstract

**With the rapid development of network technology, APP has become an essential carrier for**

文章引用: 文玉琴, 林禄. 大数据时代下个人信息保护的法律实证研究[J]. 争议解决, 2023, 9(5): 2007-2017.
DOI: 10.12677/ds.2023.95272

**people to use network information services. However, we should also see the great harm brought by APP mandatory authorization and over-authorization to various aspects such as personal information security and network security. It is effectively regulated by the linkage among the four main bodies: the state, enterprises, trade associations and organizations, users and mass media. The state should improve legislation, strengthen administrative supervision and promote judicial practice. Enterprises should strengthen protection awareness, take practical protection measures and actively assume wrongful responsibilities. Industry associations and trade organizations should improve the industry self-regulatory mechanism and strengthen industry supervision. Consumers should establish awareness of personal information protection and rights protection, and mass media should assume the responsibility of media supervision and increase the publicity of personal information protection. The use of these four main bodies, and the establishment of the "four-in-one" regulatory system, will be important to eradicate the APP collection of personal information chaos.**

## Keywords

**APP, Personal Information, Mandatory Authorization, Over-Authorization, Four-in-One**



## 1. 前言

随着网络信息技术和数字经济的快速发展，下载使用手机 APP 已经成为人们生活中不可或缺的一部分。APP 成为用户使用网络服务重要工具的同时，其强制授权及过度授权的行为也给用户的个人信息安全带来了极大的风险——中消协调查认为 APP 已经成为个人信息泄露的重灾区[1]，因不当收集、滥用、泄露个人信息导致公民权益受到侵害的事件时有发生。在大数据时代，个人信息不能全部以识别性为核心，否则依照大数据云计算整合分析个人信息的效率，现代所有信息仿佛都属于个人信息。“动态”形式表现的个人信息在数量上急剧增加，这类特殊动态个人信息数据量大、类型多样、变化快、潜在价值大[2]。在实务中，交易贩卖此类信息并牟取利益已经成为成熟的产业链条。准确定义个人信息并明晰其范围边界是研究 APP 授权危害性、构架“四位一体”个人信息保护框架的出发点。因此，笔者将个人信息定义为：“以识别性为核心的个人身份信息、由特定个体行为所产生的足迹记录信息以及特定个体自身客观状况和主观态度的总和”。

## 2. “APP 强制授权及过度授权”含义的法律界定

准确地从法律角度界定 APP“强制授权”和“过度授权”是规制 APP 授权乱象的基础。网络时代下，数据主体有权知道与其数据将被处理的一切相关资讯，包括数据控制人的身份、拟处理数据的范围、处理依据、处理目的、处理类型、处理持续期间、后果影响、是否向他人或境外传输以及主体享有的各种权利等等。而通过对 APP 授权情况的研究，可以看出 APP 在索取授权时，并未告知或清楚告知权限的真正使用目的，权限的具体内容，以及通过授权所得到的用户个人信息使用处理的相关情况。通过授权来获取信息是一种状态，但获取“更多”的用户信息反而成为趋势，“更多”信息的获取成为企业获取授权的目的所在。如获取设备安装软件的列表权限，以此来了解用户还在同时使用那些软件，借此来了解竞争对手的市场占有率，亦或是对用户实行标签化处理，便于日后广告等营销类信息的推广[3]。在此基

础上获取的权限不仅仅是 APP 提供服务的基础，同时也可能成为 APP 开发者实现提高市场占有率、攫取资源、财富目的的工具。

新华网也曾在报道[4]中指出，某款电信营业厅 APP 在使用过程中索取读取通话记录、允许其拨打电话甚至允许修改通话记录等权限，这些应用权限与其电信服务业务并无关系，也并不必要。网络安全专家在对该 APP 进行检测时发现，初次安装使用该 APP 时仅有四项权限提示，但是其向用户主张了 70 项子权限。某款手机浏览器 APP 不开启定位权限就无法正常使用，某输入法 APP 要求收集用户的信用卡号和密码等个人信息。

根据上述对授权现状的研究，笔者对 APP 强制授权及过度授权的界定如下：APP 强制授权是指采用不授权就无法使用 APP 相关功能等强制方式，排除用户选择的主要权利，索取权限，收集和使用用户个人信息进行商业活动的行为。APP 过度授权是指 APP 要求用户提供与其功能使用无关或关系较小的权限，超出合理范围越界过度收集和使用用户个人信息进行商业活动的行为。

## 3. APP 授权的现状研究

互联网行业高速发展的同时，APP 授权乱象丛生，强制授权和过度授权现象屡禁不止。为规范 APP 不合理索取权限、收集信息的行为，更好地发掘现阶段 APP 授权存在的问题，笔者根据 APP 功能分类，对下载量大且具有代表性的 100 款 APP 进行重点统计调查，分析统计他们要求的权限以及强制开启的权限的种类和数量，并对重点权限和与个人信息收集使用密切相关的权限进行重点统计研究。由于 Android 系统和 iOS 系统在 APP 权限管理审核方面存在差异，故笔者以这 100 款 APP 为调查对象在两种系统中进行统计，发掘两大系统关于 APP 权限管理和个人信息保护方面的差异和问题，提出更为完善的规制方案。统计数据结果如下：

根据统计结果，笔者发现：不管是 Android 系统还是 iOS 系统，都存在若不同意授予 APP 部分权限就不能使用 APP 全部功能的现象，即“强制授权”；此外，部分 APP 索取权限并非基于服务需要，存在“过度授权”现象。最后，还有部分 APP 在得到授权后不按照法律法规使用，不在合理的限度里使用，不以实现其功能为目的使用，存在授权滥用的现象(比如部分 APP 在通讯录里自行添加客服电话)。通过以上调查研究，可以看出我国现阶段 APP 授权主要存在以下问题：

1) “强买强卖”，存在强制授权现象。当同一类型的绝大多数 APP 出于商业或其他目的，通过默认授权，以功能为要挟，运用功能捆绑等形式强迫用户同意不合理的授权，否则 APP 便无法使用时，用户出于使用的需要实际上没有拒绝的权利，只有选择被谁侵犯的权利。从强制授权的目的来看，尽管有些强制授权存在一定的必要性，但大多数还是为了获得用户信息。如通过“获取设备安装软件列表”权限了解到用户手机中安装了哪些软件[5]，通过这些数据进而了解竞争对手的市场占有率；或通过数据将用户标签化，进而开展所谓的大数据营销、精准营销。

调查显示，94 款 Android 版本 APP 索取“获取手机信息”这一应用权限(如见图 1)，手机信息包括设备型号、系统版本、手机型号等。该权限本身可以帮助开发者开发适配于不同手机型号的手机 APP，但现阶段此权限对于 APP 适配系统没有太大的作用——因为现阶段 Android 系统为开源性的，几乎不存在适配性问题，因此这种授权并非必要。然而大部分应用都会请求这个权限，通常采取要求用户明确同意的方式获取授权，但如若用户选择不授权，相当一部分手机 APP 会拒绝用户使用该手机 APP。

2) “得寸进尺”，存在过度索权现象。当今时代数据决胜，线上的消费者成为众多互联网相关企业争夺的重要资源，超范围攫取用户信息成为一种行业的潜规则。由于授权行为没有明确的法律边界，开发者索取与业务功能无关的权限，获取权限后再进行信息的收集和利用。部分 APP 为了获得用户个人信息在手机终端后台启动，采集用户设备信息、地理位置等个人信息。这无疑侵犯了公民的合法权利。

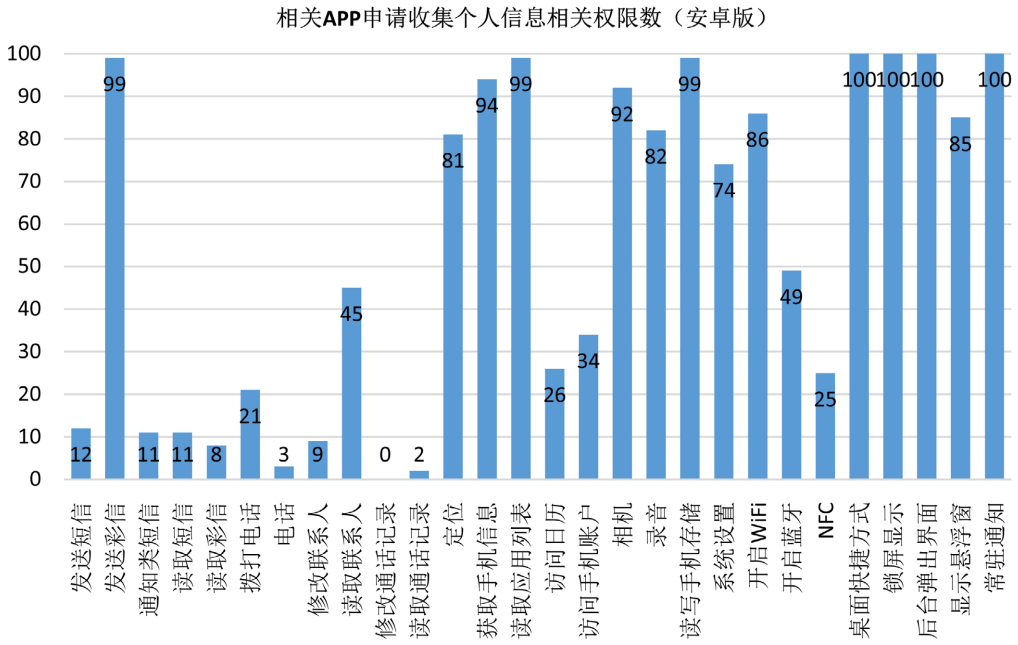


**Figure 1.** Number of relevant APPs applying for personal information-related permissions (Android version)
**图 1.** 相关 APP 申请个人信息相关权限数(安卓版)

调查显示，81 款 Android 版本 APP 要求定位权限，76 款 iOS 版本 APP 索取位置权限(如见图 2)。定位权限无疑是“明星权限”，大多数 APP 索取定位权限的理由是提供附加服务，为用户提供便利。而现实生活中往往是“一次同意，长期授权”，比如用户使用便捷定位功能填写快递单号后，定位权限仍然被赋予相关 APP，并不是“允许一次”，用户需要自行关闭；而且大多数 APP 并不必然需要定位权限，而是出于其他种种目的索取该权限。

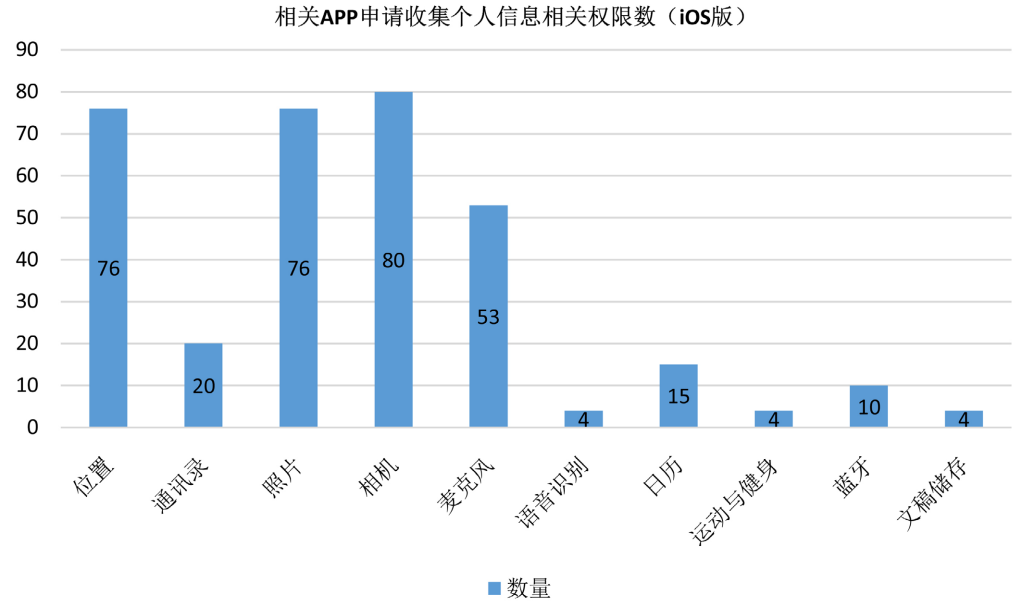


**Figure 2.** Number of related APPs applying for personal information-related permissions (iOS version)
**图 2.** 相关 APP 申请个人信息相关权限数(iOS 版)

3) “明修栈道暗度陈仓”，存在越界收集、使用个人信息的现象。APP 在获取应用权限后，超越用户授权本身的方式和范围使用权限，过度攫取用户信息，将得到的信息运用于商业用途。如地图交通类软件获取定位权限后，不仅将该权限用于道路的指引，还会自行获取用户位置信息并借助消息通知权限弹窗推荐用户所在地附近的酒店、餐厅、旅游景区等，利用用户信息实现经济价值；相册权限的赋予使得许多 APP 在实现服务功能以外，可以在后台调取用户的相册；读取联系人更是越界收集使用的“重灾区”，手机 APP 可以在得到授权后，在后台读取手机的联系人信息，可以在后台上传或者备份。部分 APP 不仅申请读取联系人权限，甚至强制捆绑了修改联系人这一权限，在用户的联系列表中直接增加该 APP 客服联系方式。

4) “含糊其辞”，隐私政策不明确。隐私政策是 APP 运营者向用户阐述他们将如何处理和保护用户个人信息以及他们为用户提供修改、删除这些信息的权利的规范性文件。隐私政策是保护用户知情权的重要手段，也是一种约束 APP 开发企业行为的重要手段。但大多数 APP 没有做好隐私政策的明示制度，开发者将隐私政策加入用户协议、使用指南等其他内容中，不以简明扼要的方式展现隐私政策的相关内容，给用户及时查阅带来了极大的不便；仅仅采取表面合法的方式，利用信息的不对称性来获取用户的应用权限并规避法律限制。此外，隐私政策对于一些涉及权限适用范围与可能带来的风险等方面的解释含糊不清，这种做法，也是行业里的公开秘密。

## 4. APP 授权乱象的原因分析

APP 授权乱象带来的个人信息保护的问题，已经开始步入“深水区”。对于个人信息保护与社会安全、产业生态创新与经济发展等方面的探讨将更加深入、复杂、具体。个人信息安全从来不是一个“孤立”的问题。但现阶段我国在这方面的工作还很不足，没有形成系统有效的规制机制。

**(一) 国家保护不足，监管力度不够。**

APP 授权乱象牵扯到的不仅是每个公民的个人利益，还有社会公共利益和社会整体利益。现阶段，关于 APP 授权乱象问题，关于个人信息保护，制度规则的制定、实施、执行等各个环节都存在问题和漏洞，给违法行为创造了生存滋长的环境。

1) 相关法律法规在司法实践中的可操作性不强。目前我国的个人信息保护主要依靠分散的法律法规予以规制(如见表 1)，虽然涉及的领域逐渐变多，但有关解决 APP 不当授权所带来的个人信息保护问题的法律较少且有局限性，相关法律对违法犯罪行为的惩治力度较低。刑法规制范围之下的犯罪行为惩处力度较小，内容存在滞后性，无法灵活应对市场经济不断发展提出的各种问题；民事方面的保护不够，APP 授权导致个人信息泄露致使用户受到侵害时，侵权人可能会由此接受刑事或行政处罚，但用户由于信息泄露导致的财产及非财产损失无法通过刑事和行政手段得到弥补；用户在市场中处于信息弱势地位，面临着举证困难的窘境，导致受案率低、审判效率低。条款内容不够具体，现有法律法规多为单一、笼统的义务介绍，而没有具体写出违反保护义务所带来法律后果，威慑力不够[6]。2) 行政机关监管力度不够。各个行政部门监管职能重合且不全面，例如我国《移动互联网应用程序信息服务管理规定》《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规中规定的互联网领域个人信息保护的行政监管机关各不相同[7]，导致用户在维权时相关行政监管机构互相推诿，无法有效保障用户个人信息权益，行政效率低；有监管职能的行政部门缺乏专业性，难以对违规收集使用用户个人信息的行为进行处罚。

**Table 1.** China’s laws and regulations on the protection of personal information
**表 1.** 我国有关个人信息保护的法律法规

| 实施时间 | 法律法规/政策名称 | 颁布主体 |
|---|---|---|
| 2021.01 | 中华人民共和国民法典 | 全国人民代表大会 |

**Continued**

| | | |
|---|---|---|
| 2021.03 | 中华人民共和国刑法 | 全国人民代表大会 |
| 2021.11 | 中华人民共和国个人信息保护法 | 全国人大常委会 |
| 2017.06 | 中华人民共和国网络安全法 | 全国人大常委会 |
| 2021.04 | 最高人民检察院发布 11 件检察机关个人信息保护公益诉讼典型案例 | 最高人民检察院 |
| 2018.11 | 检察机关办理侵犯公民个人信息案件指导 | 最高人民检察院 |
| 2021.05 | 常见类型移动互联网应用程序必要个人信息范围规定 | 国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局 |
| 2019.10 | 儿童个人信息网络保护规定 | 国家互联网信息办公室 |
| 2019.04 | 互联网个人信息安全保护指南 | 公安部 |
| 2013.09 | 电信和互联网用户个人信息保护规定 | 工业和信息化部 |

**(二) 开发企业责任意识不够，能力不足**

企业是市场经济的重要主体，也是促进资源有效利用、财富不断增长的重要动力。在市场中，部分企业为实现利益最大化，会采取一系列的不正当竞争行为，破坏市场秩序，损害社会公共利益。

1) APP 开发企业缺乏社会责任意识、法制意识。部分企业在制定和公开相应的个人信息保护政策方面做的工作不足。更有甚者枉顾商业信誉企业形象，违规违法收集、使用、出售用户的个人信息，占据市场优势地位，实现企业利益最大化。对国家相关法律法规没有正确的解读和理解，在法外寻找生存空间，违法违规收集使用用户个人信息。2) 由于技术水平的限制和市场发展带来的企业规模分化，一些小型 APP 开发企业在个人信息保护方面不具备保护的技术、能力、素质，难以凭借自身形成有效的保护机制，比如容易受到黑客攻击与病毒攻击，致使大量数据丢失，带来个人信息泄漏。3) 企业内部监管力度不足，没有建立相关合规管理体系，没有对上市的 APP 进行合规审查，没有对其可能带来的个人信息问题备有效预案，没有建立完善的监管机制。

**(三) 行业组织缺乏行业自律，监管未落到实处**

行业组织作为一个行业的中介机构，在现代市场经济运行中应承担不可代替的监督责任，对于企业而言，行业组织既是实现利益的助力，也是企业的管理者[8]。据中国消费者协会调查[1]结果，APP 的强制授权和过度授权现象已非常泛滥，《用户协议》中的相关隐私条款描述不准确不清晰，反映了手机 APP 厂商缺乏自律，企图“蒙混过关”，有目的性地收集用户个人信息，没有做到真正意义上的公开透明。而行业组织作为厂商的管理者，既没有统一的监管管理体系，也没有统一的行业标准，未尽到为消费者规避风险的责任。

1) 缺乏行业自律公约，行业组织没有统一的监管体系，也没有统一的行业标准。各责任主体之间配合不足，行业组织对企业的信用等级公开不透明，行业组织与社会公众所掌握的信息不对称，公众无法参与到企业对个人信息保护状况的监督，监管规则碎片化，全链条治理模式落实不足。无法保证监管活动有序进行，导致对厂商的监管不到位，没有尽到监管职责。2) 行业组织缺乏对企业的个人信息安全影响评估机制，导致企业不重视对用户信息的保护，更不愿意提高成本对用户信息进行保护。3) 各大网络服务提供方和各种平台作为网络信息的主要载体，没有尽到安全保障的义务。相关企业或平台对于为保证业务的顺利进行保存的个人信息缺乏必要的技术和措施，导致用户的个人信息泄露。

**(四) 用户个人信息保护意识薄弱**

随着网络信息技术和数字经济的快速发展，我们对电子产品的依赖程度越来越高，各种 APP 软件更

是改变了我们的生活方式。然而，由于用户个人信息保护意识薄弱，经常不自觉地造成个人信息的泄露。

1) 网络用户个人信息保护意识淡薄，维权意识低，且维权难度高。根据笔者前期的问卷调查，大多数用户因为隐私条款过于冗长晦涩便选择不去浏览而随意进行授权，为了免费的小礼物就盲目下载不可靠的 APP，在注册各种网络账户时，不看安全提示就随意进行个人信息输入，缺乏个人信息保护意识。由于维权取证难、成本高，消费者尽管认识到自己的信息被泄露，但自身往往处于弱势地位，难以查证侵权渠道，举证困难，败诉风险极高。维权困难变相放纵了侵权人的侵权行为。2) 个人信息数据化、庞杂化。大数据时代下，用户在 APP 上的个人信息愈发庞杂。人们在日常生活中进行网页浏览、网上购物等活动时不断被采集信息，这些活动都会产生敏感信息。而这些信息会因为相关企业保护不当、管理机制不健全而流入信息交易市场。为了实现利益最大化，部分企业和个人甚至会采取不法手段贩卖交易个人信息。

## 5. APP 用户个人信息保护的完善建议

### 5.1. 国家层面

国家是社会公权力的主体。国家利用立法、司法、行政等手段处理公共事务、维护公共秩序、增进公共利益。当个人信息的保护与公共利益发生联系时，意味着个人利益与社会公共利益之间产生了矛盾。国家有义务采取公权力的手段来维护公共利益，维护个人信息安全。立法是国家行使公权力进行治理的重要手段。司法方式是解决社会问题的最后一道防线。行政机关对规制 APP 授权乱象负有监管职责。从国家层面来讲，规制 APP 授权乱象，进而维护公民个人信息安全可以采取以下措施：

**(一) 立法方面**

1) 构建保护个人信息立法的有机协调系统，明确当前立法中较为模糊的定义与界限。例如《个人信息保护法》将个人信息区分为敏感个人信息和一般个人信息，且对其处理规则也作出明确划分，但在司法实践进行具体操作时却缺乏明确的标准，法院在审理 APP 个人信息侵权案件时，最大的难点就在于如何定性涉案个人信息的属性，如何明确强制授权过度授权的标准，而直接放入不同场景进行分析判断，极易造成“同案不同判”的现象。因此我国应结合已有的相关规定，出台针对性强、可操作性高的相关立法、司法解释作指引，颁布针对 APP 用户隐私保护的法律，从立法层面对“APP 的强制授权和过度授权”进行概念区分，针对用户被迫同意的问题，法律应明确真实知情同意的规则，禁止 APP 开发企业通过欺诈或强迫的方式获取授权，否则视为未获取同意，由于用户对 APP 企业收集信息的保存状况不知情而难以行权的现象，法律可确立证明责任倒置、复数数据控制者连带责任等规则。

2) 完善其他部门法对个人信息的法律保护机制。在刑法领域明确相应罪责及量刑标准，完善犯罪主体规范，比如像行政机关这种为公民提供相关服务而收集公民个人信息的中间机构是否构成犯罪，应当具体情况具体分析，要考察其是否具备犯罪的构成要件，即在主观方面是否具有故意，在客观方面是否实施了法律所规定的犯罪行为，应根据实际情况确定犯罪主体。就刑事处罚而言，采取“双罚制”，对犯罪 APP 企业处罚金，对相关直接负责人或者主管人处有期徒刑以上的刑法，以起到警示震慑的作用。在民法领域确定 APP 开发企业赔偿标准，除财产上的损害赔偿，还应注重对于精神损害的赔偿。从民事处罚角度而言，应当追究违规 APP 企业的违约责任以及侵权责任，使其对因数据泄露遭受损失的信息主体进行民事赔偿，并且应当提高民事赔偿的数额，以此来增加 APP 企业的违法成本，对其进行威慑。在经济法方面，将信誉罚制度推广到个人信息保护领域。违法违规收集使用用户个人信息的 APP 企业不仅要面临行政上的处罚，还要面临信誉罚。同时，建立个人信息保护领域的黑名单，将违法违规企业向社会公布。在政策上，要减少对违法违规企业的资源倾斜，降低贷款额度，加大审查力度。另一方面，从电商法领域进一步明确 APP 上市的合规要求。草案三稿明确规定：电子商务经营者根据消费者的兴趣爱

好、消费习惯等特征向其推销商品或者服务，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。

**(二) 司法方面**

完善司法救济，建立公益诉讼制度。在实务中，公民个人信息受侵害后诉至法院的效率极低且面临举证困难的窘境，无法有效维护他们的权利，因此可以将有关 APP 侵权的案件纳入公益诉讼的机制内，通过国家机关提起公益诉讼治理 APP 授权乱象，同时国家也可以允许行业协会、消费者协会等社会团体提起公益诉讼，通过程序上的完善来保障实体法的运行，从而维护消费者的个人信息安全。首先，公益诉讼机制应当根据行政机关的区划划分标准建立，保证公益诉讼机制的全面覆盖；其次，公益诉讼机制应当与行政机关内部的信息处理监管部门相区别，在专项立法中明确规定公益诉讼机制的定位，赋予其法律范围内的职责与权力；最后，对于公益诉讼机制，应当吸收社会普通民众的加入，重视普通民众的意见。

未来我国不仅应当从实体法的角度对个人信息进行保护，也要配套以相应的程序法机制，才能更好地实现统筹兼顾的目标，实现对个人信息的有效保护。此外，应该考虑个人信息侵权案件原被告实力悬殊、证据亲被告远原告、被告易于证明等因素，结合保护公共利益、倾斜保护弱者原则，降低个人信息侵权的证明标准，即原告只需证明被告掌握原告个人信息、被告存在不当使用的可能性即可，由被告举证说明其储存、利用的过程以证实其不存在滥用的行为并尽到了妥善保管的义务[9]。用户在提起民事诉讼时，应同时跟进刑事案件进程，尽早使刑事实体结果落到实处，以解决刑法和民法在个人信息案件上的矛盾摩擦，提高诉讼效率，减少诉讼成本。

**(三) 行政方面**

1) 通过法律法规明确行政部门的监管职权，授权其审查资质。如果行政部门不能进行有效的监管，那么实体性法律法规不能充分发挥作用，侵权现象也不会有所改善。借鉴外国成文法的经验可见，美国《隐私权法案》的具体规定适用于联邦部会以上的机构；日本的《个人信息保护法》主要明确了行政机构的权力结构和企业单位的权利义务范围；欧盟保护指令则可以广泛适用于行政机关和非行政机关。究其本质，这些立法条文都对个人信息行政法保护的范围加以界定，明确了权利主体的范围和权限以及行权模式。因此，在我国环境下，法律法规可以对现有的工商局等行政部门进行授权，整合各部门资源，发挥协同作用，通过法律法规使工业和信息化部、公安部、国家安全部以及所属的下级部门明确各自的职权和监管职责，加强沟通与协调，相互配合，充分发挥各部门综合效率，提升办事效率。

2) 行政部门根据法律法规制订更加详尽的具体性实施条例，采取行政强制措施。第一，借助具体性实施条例，规范现阶段 APP 授权过度化与强制性的现象，行政部门可以根据 APP 的实际功能需要，借助行政许可措施为其设定索取授权的合理范围，一方面可以避免在实际商事活动中就 APP 授权行为的合法性产生纠纷，保证商事活动顺利进行，另一方面可以防止企业泛滥收集民众个人信息，造成公民个人信息受侵害；第二，依法行政，严格执法，重视行政处罚。将 APP 授权过程中的侵权行为纳入行政处罚体系，对违法企业采取警告、罚款、没收违法所得、暂扣或者吊销许可证、营业执照、责令停产停业等处罚措施，甚至对直接负责人进行行政拘留，这样一来既惩罚了违法行为，对社会具有指导和警示作用，也提高了侵权人的违法成本，从源头杜绝违法行为的产生。第三，行政部门应当建立适当的专项优惠制度和扶持政策，为企业提高信息脱敏化处理等技术提供相应的政策和资金支持，促进 APP 企业对个人信息进行数据化处理的技术发展。

## 5.2. 开发主体企业层面

开发主体企业是 APP 授权的主体，其在规制 APP 授权乱象的过程中发挥着重要作用。企业应该承担

起社会责任和法律责任，推动个人信息保护事业的发展。

**(一) 行为管理方面**

1) 构建企业内部合规管理体系，完善合规部门的管理功能，发挥合规部门的规范作用。合规部门是识别、评估、通报、监控并报告 APP 企业合规风险的一个独立的职能部门。合规部门要做到协助 APP 企业构建合规管理体系，制订、修订有关 APP 方面的合规手册和相应的管理规章制度。此外，合规部门还需细化 APP 企业个人信息管理组织日常合规要求，具体到 APP 产品从开发到应用的每一个环节，在审查方面，合规部门应定期进行合规性审查，从形式审查深入到实质审查，同时细化审查要求，区分基本功能和拓展功能，对于 APP 获取用户权限的范围严加把控，摈弃概括同意，有效阻止不合法律规范的 APP 进入市场。

2) 强化 APP 企业的数据泄漏通知义务。一旦发现其收集的用户信息遭到泄露，APP 企业应在第一时间履行数据泄露通知义务，以此来减少甚至避免因个人信息泄露给用户、社会、国家等造成损失。就通知方式而言，应当采取“双重通知”原则，即对信息主体与监管机关都要及时履行数据泄露通知义务，且信息主体必须要先于监管机关被通知，以便信息主体能够及时采取自救措施，如立即修改相关个人信息、对涉及到的财产及时提取或转移等。当然，在信息主体无法对相关个人信息采取自救措施时，则需要尽快通过监管机关来对泄露的个人信息采取相应的保护措施，将个人信息泄露的不良影响最小化。

3) 对 APP 的有关功能进行类型化分析，主要包括两个步骤，一是分类别，二是分功能。对 APP 进行分类，必须基于该 APP 的服务范围以及服务目的。在根据服务对 APP 进行类型化分析后，才能判断其索取的授权是否与其功能实现相关，是否具有正当性、必要性、合理性。APP 功能主要包括核心功能与辅助功能两个方面。核心功能是主要功能，对于 APP 的正常运行和使用有着必要性，用户在使用 APP 时，应当允许 APP 获得与核心功能相应的授权和数据信息。而辅助功能则是次要功能，是 APP 提供的核心功能之外的其他功能，此类功能的使用很显然不具有必要性，因此其授权应当处于用户可选择的状态，即是否开启该功能完全取决于用户本身，开启该功能的时间和次数也均由用户自主选择。在用户拒绝开启相应权限时，应当可以照常使用该 APP，而不能以无法使用为由强制用户进行选择。

4) 企业内部应提高对信息处理、保存的相关技术，就信息处理技术而言，企业要努力提高将收集到的用户个人信息去隐私化的技术，不仅要使相关信息失去可识别性，还要能够做到不法分子非法获取用户个人信息之后无法通过相应的技术手段将匿名化的个人信息恢复；就信息保存技术而言，企业要提高信息存储的保密能力和防入侵、防泄露能力，使得不法分子尤其是黑客，无法非法入侵 APP 企业信息存储系统，从源头上防止用户个人信息遭受泄露，以保护用户的隐私权不受侵犯。在非例外情况下，应禁止企业对涉及健康、性生活或性取向的数据、经处理可识别特定个人的生物识别数据等用户个人敏感数据的获取。

**(二) 责任承担方面**

1) 应用商店等发行平台应当就 APP 违法违规侵害用户个人信息的行为，与违法违规的 APP 企业承担连带责任。对于此类连带责任，需根据不法行为性质的不同分为以下两个层级来处罚：一、在审核过程中存在明显疏忽大意的行为，而导致明显违规的 APP 上架的发行平台应承担较重的责任；二、对于审核时并不违规却在上架后发生违规现象的 APP，发行平台无需承担让其上架的责任，而是需要承担未能及时使其下架的责任。2) 在 APP 企业内部建立完善的问责机制。一、可以借鉴刑法对单位犯罪的“双罚制”，在追究企业自身责任的同时，加大对 APP 企业直接责任人或者主要负责人的问责力度，比如“禁业限制”，对违规 APP 企业的直接负责人或主管人实行严格的职业限制，利用设置职业门槛的方式，规定相关人员在一定期限内或者永远不得进入该行业，从事与之相关的工作。二、责任共担，数据供应链自上而下的各方都应被问责，强调数据处理者和数据拥有者共担责任。要求企业设立完善的数据保护制

度，进行文档化管理，将数据链条上的有关工作人员的数据处理活动进行实时监控，做到数据控制与流通的一举一动都有据可查，全面记载整个数据的处理全过程并及时向监管机构报备，一旦数据发生泄露等问题，可以由此找到相关责任人员，使其承担相应的责任。

### 5.3. 从行业协会、行业组织层面

1) 行业协会及组织要承担起信息安全保障义务。信息安全保障义务的承担主体应扩大到行业协会及组织。行业协会及组织要采取合理措施防止个人信息的泄露、丢失或者公开，并在出现上述情形后承担补充责任。以 APP 开发行业为例，行业协会采取的合理措施包括：第一，建立行业自律组织，加强保障机制，赋予行业自律组织制定隐私权规划和保护标准，明确政策、行为规范和保护措施，监督、检查和处理投诉等的权利义务；第二，规范网站隐私保护政策，建立行业个人信息保护标准，自我规范和约束，明确信息收集目的、方式、用途，保障用户权利，监督企业安全保障措施等；第三，技术软件研发，开展技术研发，为企业提供技术后盾，明确隐私政策技术的标准，规定技术研发的激励措施等[10]。

2) 建立行业自律组织，完善自律公约，切实从源头防范信息泄漏。所谓行业自律，指的是由公司或者行业内部制定行业的行为规章或者行为指引，为行业的隐私保护提供示范的行为模式[11]。相关行业可以借鉴美国的行业自律模式，探索建立行业自律组织，由市场上相对权威的企业牵头，强制所有企业加入，用统一权威的标准去要求 APP 企业进行企业整顿和规制，促进 APP 企业之间的相互监督和制约。另一方面，我国的行业组织不具有美国行业组织所具有的法律地位，一旦违法所得高于违法成本时，自主性就会被打破。没有法律法规的支撑，自律规范的执行措施和救济措施都得不到有效的贯彻落实，因而我国应采取立法模式与行业自律模式并重的规范模式，以促进行业自律和技术自治的生成，最终形成行业自律的良性发展市场规则，因此行业自律须与立法司法相结合，作出契合法律法规的强制性的明文规定，取得较强的约束力，用统一的标准去规范 APP 行业收集用户个人信息的行为，全面保护个人信息。

### 5.4. 从消费者及大众传媒层面

**(一) 消费者方面**

1) 消费者应增强个人信息保护意识，加强消费者自我防范意识。比如，消费者应当避免安装来历不明的软件和插件，授权时应认真阅读和理解隐私政策，坚决拒绝与功能使用无关的授权，通过个人微博微信等方式对 APP 体验感知发表评价，揭露企业的违法行为。提高消费者的自我保护意识可以从源头上有效防止个人信息泄露，进而减少 APP 企业非法利用消费者个人信息的空间。2) 消费者要提升对个人信息的控制能力。消费者在使用 APP 的过程中，一旦发现自己的信息被相关企业违法采取和使用，要立即通过合法方式告知企业停止收集和使用行为，要求企业删除已采取的信息。用户一旦发现授权会带来信息泄露风险，要及时取消授权并对此类泄露行为进行抗议，加强自身对个人信息尤其是隐私信息的控制，维护自身的合法权益。

**(二) 大众传媒方面**

1) 大众传媒要承担起新闻媒体人的责任，发挥监督作用。大众传播媒介一定要做好维护个人信息安全、保护消费者合法权益的宣传，对违规授权、违法收集个人信息、违法使用个人信息、损害消费者权益的行为进行舆论监督。大众媒体可以通过互联网、电视、广播、报纸、期刊等形式曝光 APP 企业的违法行为，曝光授权乱象，定期发布侵犯公民个人信息典型案例，以此来加强企业对个人信息的保护意识，推动企业建立严格的信息收集管理机制。2) 大众传媒要加大个人信息保护的宣传力度，提升消费者的自我保护意识和信息安全意识。大众传媒要通过互联网、电视等传播媒介，积极开展消费者教育活动，提高消费者维权意识，同时向大众宣传如何向行政机关举报、如何通过行业协会帮助自己维护合法权益、

如何进行消费者私人诉讼等维权方式，让更多的人不仅要有维权意识，还要懂得如何维权。

## 6. 结语

大数据时代背景下，使用 APP 已成为公民生活中的基本生活行为之一，其获取公民用户信息的情况无法避免。但凡事过犹不及，授权与维权的平衡已成为当务之急。在“2019 北京国际金融安全论坛”上，中国互联网金融协会副秘书长朱勇提到：“世界经济数字化转型已经是大势所趋，移动互联网时代下的数字金融前景广阔，作用积极，但也给金融监管和治理带来新挑战。当前 APP 强制授权、过度授权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出。”APP 强制授权、过度授权引发的危害现象屡见不鲜，对公民、社会乃至国家都存在着程度不一的隐患。然而，关于 APP 强制授权和过度授权的法律界定在理论上还未统一，对于此乱象的法律规制在实践中仍在探索。我们应当在厘清 APP 强制授权和过度授权法律界定的基础上，利用国家、开发企业、行业协会及行业组织、用户及大众媒体之间的联动配合，建立“四位一体”的有效规制体系，全方面、多角度、深层次地对 APP 强制授权和过度授权的乱象进行规制与整治，缓解 APP 强制授权和过度授权带来的各方矛盾与社会压力，稳定社会秩序并推动国家建设。

## 参考文献

[1] 中国消费者协会. 2018 年 APP 个人信息泄露情况调查报告[R]. https://cca.cn/jmxf/detail/28180.html

[2] 大数据战略重点实验室: 数据革命贵阳国际大数据博览会暨全球大数据时代贵阳峰会全记录 2015 版[M]. 北京: 当代中国出版社, 2016.

[3] 叶名怡. 论个人信息权的基本范畴[J]. 清华法学, 2018, 12(5): 143-158.

[4] 新华网. 中国电信这款 APP 不仅索要 70 多项权限, 还要修改你的通讯录[N]. 新华网, 2018-04-02.

[5] 京东法律研究院: 欧盟数据宪章《一般数据保护条例》(GDPR)评述及实务指引[M]. 北京: 法律出版社, 2017.

[6] 陈晨, 李思頓. 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] 高鑫钰, 邵道萍. 网络 APP 收集用户个人信息的法律规制[J]. 齐齐哈尔大学学报(哲学社会科学版), 2022(6): 72-76.

[8] 井涛. 经济法责任的独立性问题探讨——第四届经济法前沿理论研讨会综述[J]. 华东政法学院学报, 2004(1): 107-112.

[9] 刘帆. 浅析大数据时代个人信息的法律保护——以庞某诉北京趣拿公司、东航公司侵犯隐私权案为例[J]. 北方经贸, 2019(7): 63-65.

[10] 项定宜. 比较与启示: 欧盟和美国个人信息商业利用规范模式研究[J]. 重庆邮电大学学报, 2019, 31(4): 44-53.

[11] 李春芹, 金慧明. 浅论美国个人信息保护对中国的启示——以行业自律为视角[J]. 中国商界, 2010(2): 303.