

平台企业个人信息保护合规研究

刘文静

北京外国语大学法学院, 北京

收稿日期: 2022年7月4日; 录用日期: 2022年7月27日; 发布日期: 2022年8月23日

摘要

《中华人民共和国个人信息保护法》出台后, 个人信息保护进入新时代, 对隐私政策也提出了更为精准和严格的要求。在对于个人信息安全要求日益提高的大数据时代, 个人信息的保护不仅仅停留在设置更详细的隐私政策并获得个人信息主体的同意, 实务中, 平台企业收集、储存、处理个人信息的业务模式有多种, 需遵守最小、必要和公开透明原则, 企业更应该关注个人信息收集、储存、使用全过程中的保护及合规风险, 关注企业个人信息保护合规义务, 以及企业内部风控体系的建立与真正执行, 以避免企业因个人信息保护问题而带来的法律责任及企业商誉损失。

关键词

平台企业, 个人信息保护义务, 企业合规

Research on Personal Information Protection Compliance of Internet Companies

Wenjing Liu

Law School, Beijing Foreign Studies University, Beijing

Received: Jul. 4th, 2022; accepted: Jul. 27th, 2022; published: Aug. 23rd, 2022

Abstract

After the promulgation of the "Personal Information Protection Law", personal information protection has entered a new era, and more precise and strict requirements have been put forward for privacy policies. In the era of big data with increasing requirements for personal information security, the protection of personal information is not limited to setting more detailed privacy policies and obtaining the consent of the subject of personal information. In practice, there are

many business models of Internet companies collecting, storing and processing personal information, and the principles of minimum, necessity and openness and transparency must be followed. Enterprises should pay more attention to the protection and compliance risks in the whole process of personal information collection, storage, and use, and pay attention to the compliance obligations of enterprises' personal information protection, as well as the internal risk control system of enterprises. The establishment and real implementation of the company's personal information protection can avoid legal liability and loss of corporate goodwill caused by personal information protection issues.

Keywords

Internet Companies, Personal Information Protection Obligations, Corporate Compliance

Copyright © 2022 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

《中华人民共和国个人信息保护法》(以下简称“个人信息保护法”)于2021年11月1日正式生效,该法的出台旨在最大程度保护个人信息安全,其中明确规定了对个人信息采集、存储、处理、使用、传输、删除等全过程的保护要求,同时还对大数据自动决策、人脸信息等敏感个人信息的处理作出特别规定,并建立了个人信息保护投诉、举报工作机制。该法不仅关乎个人信息权益的保护,更关乎个人、企业和社会三方利益的平衡。随着互联网技术的不断革新,新的商业模式不断涌现,个人信息成为一种极具价值的丰富资源,其价值是通过允许他人使用而体现出来的。然而,在个人信息处理过程中,个人信息频繁被泄露,个人权益屡屡遭到侵犯,引发了很多侵犯个人信息的事件及案例。面对新的法律规定和合规监管要求,平台企业在其经营过程中需要落实个人信息保护要求,需要不断修复运营系统中的个人信息保护漏洞,使企业能够在符合个人信息保护的监管新形势下更平稳、高效地运营。本文将结合最新法律法规,参照国内的实务经验,对当下处在《个人信息保护法》背景下的平台企业收集、储存、处理个人信息进行研究,旨在强化大型互联网平台企业个人信息保护义务,探索平台处理个人信息合规的新路径,促进数字经济健康发展。

2. 企业收集处理个人信息的合规风险

互联网的迅速发展,使得人们处在大数据时代,个人信息传输、转移显得更加平常。实务中,平台企业收集处理个人信息的商业模式是多样的,有些平台企业会选择请数据分析公司提供数据分析服务,有些企业则是需要与物流公司等平台合作共享个人信息,更有部分企业因为集团公司内部的需要需将个人信息传输到境外的关联公司。平台企业应该关注个人信息保护全过程的合规风险,收集处理个人信息需要取得明确同意,亦不得超越权限处理个人信息,应当防范存储个人信息遭遇泄露的风险,平台企业删除个人信息应当详细的法律规定。

2.1. 未经明确同意即开始收集个人信息是否合规

此种情况是指企业由于自身的运营、日常工作的需要,开始收集用户的公民个人信息,如收集用户的人脸头像、身份信息、地理位置等,此种情况下收集公民个人信息,并没有明确征得用户的同意。实

务中有些企业在制作 APP 等应用程序时,可能是复制了其他企业的 APP 的源代码,对于启动应用程序时即开始收集用户的公民个人信息的情况并不知情,当然主观上也不存在违法违规的目的,但是,如果未经用户同意即开始收集个人信息,无论是过失还是故意,都同样需要承担合规法律责任。例如,2019 年 12 月 19 日、2020 年 7 月 2 日,在工信部分两次公布的未完成整改的 56 款 APP 所涉及的 8 项整改内容之中,涉及“私自收集公民个人信息”的 APP 数量达到了 29 款。根据通知要求,企业若未整改完成,则会被工信部门采取如 APP 下架、纳入失信名单等严厉的惩罚; [1] 2020 年 6 月 23 日,深圳市公安局网警部门对“一花斗地主 APP”未公开收集使用规则、未经用户同意收集使用个人信息作出了警告、罚款 3000 元并暂停开展新业务 7 天的行政处罚等等。¹

2.2. “超越权限”处理个人信息的合规风险

所谓的“过度索取权限”,是指用户在使用平台企业的应用软件时,几乎都需要注册账号,并会被索取定位、访问设备照片、访问手机通讯录等权限,如果用户选择“拒绝”,则可能意味着无法正常使用,有些应用软件甚至存在“不同意授权会闪退”等情况。[2]此种情况下,平台企业可能涉嫌“超范围收集个人信息”,不符合收集公民个人信息的最小必要原则,触犯到《中华人民共和国网络安全法》(以下简称“网络安全法”)、《中华人民共和国电信管理条例》等法律法规的规定,可能承担法律责任。例如,2019 年 12 月 19 日、2020 年 7 月 2 日,在工信部分两次公布的未完成整改的 56 款 APP 所涉及的 8 项整改内容之中,涉及“过度索取权限”及“超范围收集个人信息”的 APP 数量合计达到了 31 款。[3]另外,2017 年生效的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(以下简称“《解释》”)对涉嫌非法出售公民个人信息罪的入罪标准列举了详细的规定,该《解释》第五条第八项规定非法出售 25 条公民个人信息即可能被追究刑事责任。因此,将收集得来的公民个人信息“私自共享给第三方”,可能导致的刑事责任风险非常高,必须引起企业的高度重视,近几年来国家重点打击的涉及侵犯公民个人信息的刑事犯罪的案例不胜枚举。[4]

2.3. 企业存储与删除公民个人信息存在的合规法律风险

平台企业若控制个人信息,则其便有保障所储存的信息安全的法定义务,因此如果储存的相关个人信息遭到泄漏等严重后果,那么信息控制主体则应当对于泄漏的部分承担责任。我国《网络安全法》第四十二条规定了网络运营者的应即使补救和报告的义务,第六十四条再次确认了应承担的法律后果,情节严重的则会处以停业整顿、吊销营业执照等处罚。另外,平台企业的存储管理措施不到位,导致公民个人信息外泄,造成公民个人信息主体损失的,根据《中华人民共和国消费者权益保护法》、《中华人民共和国侵权责任法》(2021 年 1 月 1 日以后为《中华人民共和国民法典》)等相关法律法规的规定,企业可能需要承担损害赔偿等民事责任。更加值得人们关注的是,公司一旦被恶意软件入侵、互联网上的病毒影响和黑客攻击,那么平台企业所存储的用户个人信息将会不同程度的泄漏或损失,公司业绩下滑很难避免,继而也会导致公司的市场名誉受损。

企业在删除用户个人信息时,在《数据安全管理办法(征求意见稿)》第三章“数据处理使用”对信息控制主体即平台企业删除信息作了详细的规定,比如该法第二十条,则运营商应该在收集使用规定的保存期限内保存个人信息,当用户注销后运营者应当协助用户及时删除,经处理仍不能复原且无法关联该用户的是例外。此外,当用户提出信息查询、修改、删除及注销个人账户的请求时,网络运营者应当在合理的范围内予以配合和帮助等等。个人信息的控制主体不应当给用户请求删除或注销账号的渠道设置任何障碍,在接到用户的删除或注销账号的合理请求后,应当及时给用户删除或注销账号的服务。

¹<https://3g.163.com/dy/article/FGI438R105129QAF.html> (最后一次访问时间 2022 年 7 月 30 日)。

实务中,也不乏因未履行及时删除义务而被责令改正甚至被处罚的案例。[5] 2019年12月19日、2020年7月2日,在工信部分两次公布的未完成整改的56款APP所涉及的8项整改内容之中,涉及“注销账户难”的APP数量合计达到了16款。[3]需要说明的是,《数据安全管理办法(征求意见稿)》虽然没有正式实施,但是也代表国家有关部门的立法倾向,可以作为企业履行数据合规义务的重要参考。

3. 平台企业个人信息保护义务

近年来,国家加快了互联网和数字经济方面的立法,先后颁布了《中华人民共和国数据安全法》和《个人信息保护法》。《个人信息保护法》的出台为个人权益的保护构建了较为完善的法律框架,也为各类企业,尤其是数据产业的企业提供了更为具体的合规指引。在习近平法治思想指导下,这些重要法律的制定和颁布,强化了以人民权利保护为中心的法治理念,用这样的理念促进数字经济的健康发展。《个人信息保护法》平台企业至少应该从以下几个义务方面关注合规风险。

3.1. 平台企业对个人信息保护应该承担信义义务

网络用户因为信赖平台组织而产生信义利益,在社会组织中,当一方与另一方的关系不对等时,强势一方如果明示或暗示发出了令人信任的邀请,而弱势一方接受了该邀请时便产生了信义关系。强势一方对因接受其信任邀请而处于特殊不利地位的人具有关照、保密和忠诚义务。平台组织是一种新的信任网络,网络用户因为对该平台组织的信任而加入其中,产生并向平台组织交出个人信息,网络企业对网络用户要承担信义义务。以网络企业的信义义务来保护个人信息有以下优点:其一,可以避免通过个人私权利或者政府公权力直接保护个人信息所造成的信息失灵问题。其二,可以保障网络企业对平台组织的经营自由。其三,可以更好地照顾网络企业追求利益与网络用户个人信息保护之间的关系。其四,可以更好地促进个人信息在不同平台组织之间的转移和利用。[6]

3.2. 平台企业对个人信息安全监管义务

平台企业是网络社会的关键节点,掌握着用户与网络的连接桥梁,网络运营者的行为在很大程度上影响着用户的信息安全,甚至会影响整个网络社会的安全状态。网络运营者提供的服务具有公共产品的属性,这一属性随着现代信息技术的不断渗透而被强化,其安全状态对整个社会的安全具有重大而深远的影响。

我国在网络政策上主张“谁接入,谁负责”、“谁运营,谁负责”,网络运营者在提供网络服务和产品的过程中获取了经济收益,那么就应当负有相应的防止危害发生的安全保护义务。[7]在全球网络安全问题日益复杂且严峻的情况下,提升网络运营者的安全意识,明确网络运营者的义务责任,是实现国家和社会稳定的必然要求。作为网络运营者,应当依照法律、行政法规的规定和国家标准的强制性要求,采取技术措施和其他必要措施,保障网络安全、稳定运行,有效应对网络安全事件,防范网络违法犯罪活动,维护网络数据的完整性、保密性和可用性。应依照《网络安全法》等行政法律法规承担行政法律责任。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,符合法定情形的,构成拒不履行信息网络安全管理义务罪,依法承担刑事责任。

3.3. 平台企业对个人信息保护应该承担告知义务

《个人信息保护法》规定了“告知-同意”原则,该原则充分保护了用户的知情权,此即相关互联网企业处理个人信息的一般合法性基础,平台经营者的处理行为应当恪守合法、正当、必要原则,不得以捆绑服务、强制停止使用等不正当手段变相胁迫、强制用户提供具体范围不够明确个人信息的行为,不得违反我国法律有关处理个人信息的正当性原则,理想的告知同意规则的落实,是建立在运营者清晰、

明确的写明了所有个人信息处理行为及告知事项。^[8]同时《个人信息保护法》对于企业违反信息泄露通知义务的罚则有所不同。根据《个人信息保护法》，除对企业处以罚款外，监管部门还可以对企业直接负责的主管人员和其他直接责任人员处以罚款，且也可对企业及企业负责人员处以其他行政处罚。基于《个人信息保护法》第66条的规定，违反信息泄露通知义务的企业可被处以1百万元以下罚款。情节严重的，将被处以5千万元以下或上一年度营业额5%以下的罚款。对企业负责人员，其也可能被处以1万元以上10万元以下罚款，情节严重的，处以10万元以上1百万元以下罚款。此外，根据情节严重程度，未能履行信息泄露通知义务的个人信息处理者有可能被处以责令改正、给予警告、没收违法所得、责令暂停相关业务、停业整顿、吊销相关业务许可或者吊销营业执照等处罚。企业负责人员可被禁止在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

3.4. 平台企业特别和专门的个人信息保护义务。

当前，我国互联网的发展进入了新的阶段，即互联网企业发展从“野蛮生长”到合法合规健康发展的阶段。从世界范围看，法治目前从两个方面强化互联网或者说数字经济的治理：一是反垄断、反不正当竞争，二是数据安全与个人信息保护。平台企业是个人信息保护的“守门人”，这体现在《个人信息保护法》为大型互联网平台企业设定了特别保护义务上。《个人信息保护法》除了规定平台企业应当遵守一般的信息处理者的义务外，还对平台企业规定了特别和专门的个人信息保护义务。这种理念也充分体现在《个人信息保护法》第58条中，同时对平台企业个人信息保护合规义务提出了更高的要求。《个人信息保护法》第58条第1项²不仅要求平台企业建立健全个人信息保护合规的制度体系，还要求其应当建立独立机构来进行更直接有效的监督。第2项关于制定平台个人信息保护规则的内容主要考虑到大型互联网企业有可能将这个义务滥用为垄断或者对平台商户进行不正当竞争操作的工具。因此，立法部门采用“遵循公开、公平、公正的原则”对这一重要内容作出了限定，旨在约束互联网大型平台企业在履行这一义务时不滥用本条文。第3项对严重违法处理个人信息的行为，要求平台企业停止提供服务。第4项鼓励社会监督的机制，并要求平台企业定期发布社会责任报告。

4. 企业收集处理个人信息合规的相关建议

平台企业需要建立健全有效个人信息保护体系，除建立完备的隐私政策外，还需要全面适用“告知同意”规则，对第三方信息披露要进行合理限制，存储与删除应当遵守相关法律法规规定，将可以打造出一个数据安全、个人信息保护到位的高效运营体制。

4.1. 企业需要建立内容完备的隐私政策

不同行业的企业因其自身的业务特性，会在实践中逐渐形成一套隐私政策文本，之后可根据政策变动和业务更迭进行具体内容的更新。目前人们基本按照《信息安全技术个人信息安全规范》(标准号:GB/T 35273-2020)来构建隐私政策的框架并且确立其具体内容。其条目可以定位到《个人信息保护法》第17条，包含《个人信息保护法》所要求的告知内容，如列明个人信息处理者的名称、姓名、联系方式，处理信息的种类、目的和方式，以及个人行使法定权利的方式。当然其他法律法规有规定的事项都可以在政策中不同程度的标注列明。

《个人信息保护法》之所以要求隐私政策完备，并对需要公开的事项做出规定，是基于对个人信息²《个人信息保护法》第58条：“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：(一)按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；(二)遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；(三)对严重违反法律、行政法规处理个人信息的产品或者服务提供者，停止提供服务；(四)定期发布个人信息保护社会责任报告，接受社会监督。”

处理实际情况和风险性的考量。企业首先需向用户明确个人信息处理者，其次要让用户了解目标信息、处理原因和处理方式，从法律层面来说这是对公开透明原则的遵循，从潜在风险而言，是为了让用户了解可能涉及个人信息处理行为的主体、对象和方式，保证隐私政策这项协议所涉行为的合法合理性。^[9]如果企业对隐私政策的制定不够完备，个别条款存在遗漏或瑕疵，将可能导致用户个人信息保护风险的增加。如未告知向关联第三方同步用户个人信息，则可能涉嫌侵害用户的知情权、选择权；如未明示信息侵权的争议解决渠道，则可能导致信息漏洞无法接收用户反馈，导致用户个人信息权益受损。^[10]

因此，隐私政策相关内容的缺失将可能直接导致企业对个人信息的使用或处理超越了用户知情同意的范畴而构成侵权，企业针对个人信息的处理行为可能会因为未获得“告知同意”的权利基础而失去合法性，不仅面临罚款、赔偿风险，还会被记入信用档案，不利于企业长期健康发展。

4.2. 企业应当全面适用“告知同意”规则

《个人信息保护法》中依然坚持了以“告知同意”为核心的个人信息的处理规则，这一规制与个人信息处理者需遵循的公开透明原则相互映照，使用户充分了解个人信息的处理规制，从而有效地保障其知情权和选择权。“告知”行为是以企业制定、发布为主，用户查看为辅，对应的是知情权；而在“告知”后进行的“同意”中，则是由用户主动做出选择，即个人在知情权被保障的基础之上，又进行了选择权的行使。隐私政策是落实告知同意规则的主要方式，但隐私政策本身并无法涵盖所有需要告知同意的情形，^[11]针对不同的场景有如下几种不同的告知同意模式：

4.2.1. 一般同意

取得用户同意是企业合法合理处理和使用个人信息的前提，因此告知同意是个人信息保护的基本规则。依据《个人信息保护法》第13条的规定，除部分例外情形外，“取得个人同意”是个人信息处理者处理个人信息的合法性基础和前提条件。实践中，企业为了规避违法违规处理个人信息可能出现的法律风险，大多是在进行收集、存储、使用、提供、加工、传输、公开个人信息的行为时，信息处理者以取得“取得个人同意”的方式获得处理用户信息的授权。

要想获得用户的一般同意，企业需要在隐私政策等需要授权的文本中，列明其处理个人信息的方式和规则，并由用户主动勾选同意等方式，完成上述步骤该企业才能处理个人信息。可见，隐私政策是获得用户一般同意的常见方式，通过隐私政策，平台方可以将涉及个人信息保护的行为和内容进行充分解释，让用户全面了解其信息可能将以什么方式被使用和保护。在保障用户选择权的基础上，即用户主动勾选确认/同意隐私政策，即视为用户全面了解和认可了隐私政策的内容，事后如用户以隐私政策为格式文本等理由主张不认可隐私政策内容的，一般不会得到支持。

但是，如果告知同意的默示存在问题，即使隐私政策再完备也可能涉嫌违规，如让用户勾选同意隐私政策的过程必须充分保障用户的选择权，而不能默认选择同意，同意的选项应当是用户主动选择的结果。^[12]另外，如用户选择不同意的，企业不能拒绝提供服务，如隐私政策的内容与平台的核心功能直接相关，如果用户拒绝隐私政策就不能使用平台的，即便用户不同意该隐私政策，企业应当提供仅浏览模式，而不是直接退出或完全无法使用平台任何功能。同时企业应当在《隐私政策》中写明：如果您拒绝该政策，可能无法使用本公司相关的服务和产品，但不影响使用该网站的基础性功能，

4.2.2. 重新同意

在信息处理者处理信息的目的、方式以及处理信息的种类发生变动的情况下，信息处理者应当重新取得用户的同意。由于取得用户原始同意时要区分一般同意和特殊同意的情况，因此在取得用户的重新同意时，获得用户特殊同意的也应当重新获得用户的特殊同意，以便与原始同意保持对应。^[13]

鉴于互联网行业日新月异的发展特点,企业需根据行业实务和政策变动不断更新隐私政策,这就意味着个人信息处理规则也会发生变更。《个人信息保护法》对此做出规定,要求个人信息处理者在个人信息处理规制发生变更时需分别重新进行“告知同意”。如果因业务变动等原因,企业要将基于某一特定目的收集来的个人信息应用于其他目的,或者要将信息应用于隐私政策所载明的用途之外时,应当事先获得用户的另外授权同意。这就好比合同事项发生了变动,双方需要重新磋商,而更新后的隐私政策在经过用户同意后就相当于一个补充协议,[14]以其新条款约束平台与用户。平台保存和处理经过匿名化处理的信息无需争得同意,共享、转让经匿名化处理的个人信息也不属于对外共享、转让及公开披露个人信息的范畴。

4.2.3. 书面同意

针对何为书面同意,根据《民法典》第 469 条³的规定,书面形式除合同书等能够有形表现所载内容的形式之外,还包括电子数据交换、电子邮件等方式,并可以随时调取查用数据电文。按照这一定义,用户点击、勾选“同意”等按钮,会作为网络操作记录,以数据形式存储在服务器,事后可以随时调取查用,也符合书面形式要求。[15]书面同意的情形主要体现在个保法第二十九条。⁴

敏感个人信息主要是指个人生物信息、账户信息、医疗数据等重要信息,泄露或非法使用敏这类信息,可能会导致个人受到歧视或者人身、财产安全受到严重危害。收集或者处理个人信息应当取得书面同意,如《药物临床试验质量管理规范》第 23 条规定要求,受试者应当签署书面的知情同意书。

4.3. 与第三方的合同或协议要约定明确

首先,明确收集来的用户的公民个人信息的所有权归企业所有,原则上第三方除用于授权的用途之外,不得共享给其他任何第四方;确有必要共享的,应当再次获得用户的明确授权;其次,可以对提供给第三方的公民个人信息进行匿名化处理,并约定第三方不得利用反向识别或复原公民个人信息;[16]再次,对第三方信息披露进行合理限制,要求其严格遵守保密义务。最后,设置免责条款。

4.4. 存储与删除应当遵守相关法律法规规定

企业在存储收集的用户的个人信息时,应当严格遵循法律对信息等级保护制度的要求,防止用户个人信息泄露或被窃取、篡改,同时也要符合存储大数据的互联网数据中心的建设标准,采用技术手段等必要措施,保证企业收集、保管合法以及用户个人信息的安全。另外,企业也应当提供相应的更正或删除个人信息的功能,并且公布投诉方式和举报方式等信息。另外,平台需要建立并公布个人信息安全投诉、举报通道并建立必要的删除、更改个人信息的服务,不得设置修改、删除个人信息不必要或不合理条件,及时响应用户相应需求,并在承诺时限内完成审查和处理。[17]

5. 结语

这是一个信息爆炸的时代,个人信息保护立法和网络经济的发展相辅相成,前者为网络平台创造经济新天地,后者将个人信息价值推上时代的风口浪尖。然而,个人信息保护的完善无法一蹴而就,隐私政策的起草发布也不能一劳永逸。从企业的角度,当下社会的政策经济环境以及企业的自身经营状况可能会发生变化,产品功能、企业架构和主营业务等都有可能发生变化,对个人信息处理规则也需要根据实际情况作及时的相应调整,以达到保护个人信息的发展目的。平台的个人信息处理活动不仅涉及公

³《中华人民共和国民法典》第四百六十九条:“当事人订立合同,可以采用书面形式、口头形式或者其他形式。书面形式是合同书、信件、电报、电传、传真等可以有形地表现所载内容的形式。以电子数据交换、电子邮件等方式能够有形地表现所载内容,并可以随时调取查用的数据电文,视为书面形式。”

⁴《中华人民共和国个人信息保护法》第二十九条:“处理敏感个人信息应当取得个人的单独同意;法律、行政法规规定处理敏感个人信息应当取得书面同意的,从其规定。”

民权益保护,而且事关产业创新发展与网络传播秩序,与公共利益息息相关。平台只有将保护个人信息的要求,贯穿到信息收集、使用、披露与提供的全过程,切实履行事前预防侵权与事后监管救济的基本责任,才能有助于公民权益保障和平台经济健康发展。

参考文献

- [1] 陈绚,王思文. 新闻传播与媒介法治年度研究报告[M]. 北京: 中国人民大学出版社, 2021: 199.
- [2] 阿热孜古丽·麦合木提. 手机应用软件索取用户信息的法律边界[J]. 法制与经济, 2021, 30(11): 83-89.
- [3] 工信部下架 106 款侵害用户权益 App [J]. 中国信息化, 2021(12): 30-31.
- [4] 彭文华, 姚建龙, 王娜, 刘崇亮, 骆群, 金冀翔. 人工智能的刑法规制及其相关法律问题[M]. 北京: 中国政法大学出版社, 2019: 430.
- [5] 刘艳红. 网络犯罪的法教义学研究[M]. 北京: 中国人民大学出版社, 2021: 375.
- [6] 吴伟光. 平台组织内网络企业对个人信息保护的信义义务[J]. 中国法学, 2021(6): 45-60.
<https://doi.org/10.14111/j.cnki.zgfx.2021.06.001>
- [7] 张逸凡. 互联网平台企业社会责任法律制度研究[D]: [博士学位论文]. 上海: 华东政法大学, 2020.
<https://doi.org/10.27150/d.cnki.ghdzc.2020.001555>
- [8] 俞灵灵. 移动电商领域不正当竞争案件的司法裁判研究[D]: [硕士学位论文]. 杭州: 中国计量大学, 2018.
- [9] 高富平. 个人信息处理: 我国个人信息保护法的规范对象[J]. 法商研究, 2021, 38(2): 73-86.
<https://doi.org/10.16390/j.cnki.issn1672-0393.2021.02.006>
- [10] 罗力. 新兴信息技术背景下我国个人信息安全保护体系研究[M]. 上海: 上海社会科学院出版社, 2020: 176.
- [11] 田宇申. 互联网保险中个人信息保护的法制规制——以个人信息保护政策为切入[J]. 兰州学刊, 2021(9): 116-134.
- [12] 马民虎, 黄道丽, 郭世杰. 网络法典型案例评析[M]. 北京: 中国民主法制出版社, 2018: 321.
- [13] 陈吉栋. 人工智能与法律的对话[M]. 上海: 上海人民出版社, 2020: 395.
- [14] 李伟, 蒋文杰. 隐私协议用户知情同意的认定[J]. 中国检察官, 2021(2): 3-15.
- [15] 李晗. 大数据时代网上银行的信息安全保障义务研究[J]. 法学杂志, 2021, 42(4): 53-66.
<https://doi.org/10.16092/j.cnki.1001-618x.2021.04.005>
- [16] 齐英程. 我国个人信息匿名化规则的检视与替代选择[J]. 环球法律评论, 2021, 43(3): 52-66.
- [17] 商希雪. 侵害公民个人信息民事归责路径的类型化分析——以信息安全与信息权利的“二分法”规范体系为视角[J]. 法学论坛, 2021, 36(4): 100-111.