

IP 属地的法律性质证成及平台责任评析

严 驰

(武汉理工大学 法学与人文社会学院, 湖北 武汉 430070)

摘 要: 国内互联网平台近日陆续上线显示用户 IP 属地功能。公开用户 IP 属地的行为存在显著的合法性争议,在如今强调网络安全和个人信息保护的大数据时代背景下,有必要从法律角度对该事件进行分析和探讨。通过对相关文献和学者观点的梳理总结,结合规范性文件和司法判例,研究认为应将 IP 属地认定为个人信息,同时谨慎考虑是否把 IP 属地界定为敏感个人信息或隐私。在平台责任的法理分析上,研究指出平台在公开用户 IP 属地前应充分履行告知同意义务,平台要求用户“一揽子同意”的行为有违最小必要原则,即使用户不同意平台也应继续提供服务。在后续发展中,平台应构建起自证清白的体系,以充分履行个人信息保护义务。

关键词: IP 属地;个人信息保护;平台责任

中图分类号: D923

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2022.05.009

引用格式: 严驰. IP 属地的法律性质证成及平台责任评析[J].网络安全与数据治理,2022,41(5):59-65.

The legal attribution of IP location and platform liability review

Yan Chi

(School of Law, Humanity and Social Sciences, Wuhan University of Technology, Wuhan 430070, China)

Abstract: The function of displaying user's IP location has recently been launched one after another on domestic Internet platforms. The act of disclosing user's IP location has significant legality controversy. In the context of the big data era, which emphasizes network security and personal information protection, it is necessary to conduct analysis and discussion of the incident from the legal perspective. By combing and summarizing relevant literatures and scholars' viewpoints, combining the relevant normative documents and judicial precedents, study believes that IP location should be recognized as personal information, while cautiously considering whether to define IP location as sensitive personal information or privacy. In the legal analysis of the platform's responsibility, study points out that the platform should fully fulfill the obligation of informing consent before disclosing the user's IP location, and the platform's act of requiring the user's "blanket consent" is against the principle of minimum necessity, platform should continue to provide services even if the users do not agree. In the subsequent development, the platform should build up a system of self-incrimination and fully fulfill the obligation of protecting personal information.

Key words: IP location; personal information protection; platform liability

0 引言

2021 年 10 月 26 日,中央网信办发布了《互联网用户账号名称信息管理规定(征求意见稿)》,其中第 12 条要求互联网用户账号服务平台以显著方式在用户账号信息页面展示 IP 属地信息。境内账号 IP 属地标注到省(区、市),境外账号 IP 属地标注到国家(地区)。2022 年 4 月 24 日,中央网信办部署开展了“清朗·网络暴力专项治理行动”,要求 18 家

网络暴力事件频发、社会影响力大的网络平台切实承担社会责任,对网络暴力行为建立事前预警、事后保护、严防扩散、曝光警示等全链条治理措施。2022 年 4 月至 5 月,今日头条、小红书、抖音、知乎、新浪微博等知名互联网平台相继上线了显示用户 IP 属地的功能^[1],引发社会舆论广泛讨论。2022 年 6 月 27 日,国家互联网信息办公室正式发布《互联网用户账号信息管理规定》(以下简称“《管理规定》”),

并于 2022 年 8 月 1 日起施行,其中第 12 条明确指出互联网信息服务提供者应当在用户账号信息页面展示合理范围内的 IP 地址归属地信息。截止到 2022 年 11 月,用户在相关平台上均不具有自主关闭或者改变 IP 属地信息的选择权。虽然显示用户 IP 属地能有效减少蹭热度、网络暴力、恶意造谣等不法行为的发生,但也引发了公众对个人信息泄漏的担忧。2021 年 11 月,《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》”)正式实施,开启了我国个人信息保护的新纪元。本文试图在法律监管缺位的情况下,结合相关法律规定和司法实践,对 IP 属地的法律性质以及平台公开用户 IP 属地应承担的法律责任进行探讨,廓清大数据时代的公民个人信息安全的概念。

1 研究基础

1.1 概念解析

互联网协议(Internet Protocol, IP)地址是实现互联网功能的基础资源,也是对网络使用者身份和网络信息追根溯源的重要工具,被称为是“网上门牌号”^[2]。和手机系统中通过 GPS 或基站定位获取位置信息的原理不同,网络用户的 IP 地址是由互联网通信协议决定的、在接入互联网时就被分配的地址,信息接收方需要通过 IP 地址才能完成信息接入。本文所探讨的 IP 属地并不等同于 IP 地址。IP 属地虽然是基于 IP 地址形成的位置信息,但又不同于 IP 地址呈现到门牌号级别的精准度,它只是对使用互联网的自然人地理位置的一种粗略显示。简单来说,IP 属地就是用户上网行为发生时的具体地理位置^[3]。IP 属地针对境内用户账号显示到省级行政区划的程度,如浙江、新疆、上海等,针对境外用户账号则只显示国家或地区,如美国等。

1.2 文献综述

此前,世界范围内在 IP 地址是否属于个人信息上已存在较大争议,如美国《信息隐私法》中认为 IP 地址属于个人信息,法国法院的相关判决中则未将 IP 地址视为个人信息。在欧盟《通用数据保护条例》(GDPR)出台前,我国有学者总结了法国、英国、德国等在 IP 地址上的相关规定,认为 IP 地址因缺乏某一特定的人的特征而不应被视为个人信息^[4]。2018 年 5 月出台的 GDPR 中把 IP 地址视为网络标识符的一种纳入个人信息的保护范畴,一定程度上终结了欧盟地区关于 IP 地址是否属于个人信息的

争议。对此我国也有学者更认可欧盟在 GDPR 中的观点,认为一般情况下静态 IP 和动态 IP 均构成个人信息^[5]。我国在相关司法实践中更倾向于把 IP 地址视为识别特定个人的信息,如熊某某与杨某某名誉权纠纷案中,法院认为被告熊某某通过原告杨某某泄漏的 IP 地址,进一步掌握到足以识别特定自然人的个人信息导致原告杨某某的名誉权受损。秦某某诽谤、寻衅滋事案中,法院通过 IP 地址和微博注册信息的对应,识别出秦某某犯罪嫌疑人的身份。

IP 属地作为新近提出的概念,尚缺乏一个明确的定义,关于其法律性质分析的文献数量较少。我国有学者结合了域外立法与实践,提出在“识别”要素判断上不宜采用过于宽泛的解释,应将其限制为实质上的或能够合理推断的可能,认为 IP 属地信息因过于模糊、无法单独识别出特定自然人而不属于个人信息^[6]。也有学者提出《管理规定》第 12 条为网络平台设定公开用户 IP 属地信息的法定义务不能通过“适当性”“必要性”及“均衡性”审查,有违比例原则,不宜成为平台公开用户 IP 属地行为的合法性依据^[7]。还有学者关注 IP 属地功能上线后引发的 IP 代理乱象^[8],认为社交平台公开 IP 属地的行为有利有弊,虽然一定程度上提升了网络用户鉴别信息真假的能力,但也可能会催生和 IP 代理相关的灰色产业链发展。如今对 IP 属地的规制体系尚付阙如,未来仍需进一步明确和发展。

2 IP 属地法律性质界定

在探讨 IP 属地相关的法律问题前,首先应明确 IP 属地的法律性质。厘清个人数据性质是规制数据活动的当务之急^[9]。如今法学界对个人信息和个人数据的概念区分众说纷纭,有学者认为个人数据权和个人信息权虽然对象重合度很高,但在主体和内容上都有所不同^[10],也有学者认为个人信息和个人数据在法学上具有一致性,在实质内容方面并无区别^[11]。从全球范围来看,欧盟、美国、日本等国家的立法中更倾向于使用“数据”的概念,未对两者加以明确区分,如 GDPR 中就采用了“Data”(数据)而非“Information”(信息)的表述。为避免相关概念的混淆,本文把个人数据和个人信息做同义语,不对两者加以区分。

2.1 IP 属地是否属于“个人信息”

2.1.1 国内立法及实践

“可识别性”是个人信息界定时的核心要素^[12]。

有学者提倡对个人信息进行宽泛的界定,认为在个人信息的“识别”要素的判断上,只要内容、目的、结果三者任一与特定自然人相关即可认定为个人信息^[13]。也有学者指出应对个人信息作狭义解释,过分扩大个人信息的范围会加重中小企业的责任义务,给企业合规带来了巨大的不确定性^[14]。《中华人民共和国网络安全法》(以下简称“《网络安全法》”)第76条把个人信息定义为以电子方式记录的能够单独或者与其他信息结合识别个人身份的信息,《个人信息保护法》第4条则把个人信息定义为以电子或其他方式记录的与识别自然人有关的信息。2019年宣判的凌某某与抖音公司的网络侵权责任纠纷一案中,北京互联网法院认为抖音公司在未征得凌某某同意的情况下通过IP地址收集原告地理位置信息,构成对原告个人信息的侵害。

2.1.2 国外立法及实践

GDPR第4条中对个人信息的定义是与已识别或可识别的自然人相关的任何信息,无限扩大了个人信息的边界。2018年6月美国加利福尼亚州(以下简称“加州”)颁布的号称“美国史上最严格数据保护立法”的《加州消费者隐私保护法案》(CCPA)中,明确把IP地址纳入个人信息的范畴。在帕特里克·布莱耶(Patrick Breyer)诉德意志联邦共和国案中,欧盟上诉法院认为确定一个人是否可以识别,应考虑到控制人或任何其他可能合理使用的所有手段来识别该人^[15],虽然动态IP地址本身不能直接识别出特定自然人身份,但是通过IP地址与其他网络平台账户数据的组合,可以达到间接识别用户的效果。同样,在纽约时报公司等诉联邦通信委员会案中,美国纽约南区联邦地区法院认为尽管IP地址不会直接透露个人可识别信息,但是可以用于帮助拼凑出能与特定自然人相关连的其他身份信息。

运营商分配给用户的IP地址是动态、共享的群体标识,而IP属地是静态、专属于自然人的个体标识,其存在基于网络连接服务的参数携带,天然指向或者关联个人。传统观点认为可识别性是个人信息首要且必要的特性,不具可识别性的匿名信息等不属于个人信息^[16]。学界多数观点指出不应在“识别”要素的认定上采取过于宽泛的解释,过分扩大个人信息范围。个人信息与自然人的人格尊严和安全密切相关,维护个人利益是个人信息保护的逻辑起点^[17]。随着数据收集和处理技术的发展,大数据

时代的个人信息受到“识别性”和“相关性”两方面的限制^[18],应重新界定个人信息保护范围,除识别信息以外,也应对相关信息加以保护。个人信息需要同时具备与特定个人相关联、反映个体特征和具有可识别性^[19]。以互联网搜索记录为例,早期的搜索记录并不属于个人信息,随着大数据分析技术的发展,如Netflix之类的新兴科技公司会通过Hadoop、Phython等程序收集海量数据,迅速了解用户习惯^[20]并根据用户反馈作出精准的广告推送。虽然IP属地不具备单独的可识别性,但其具备个人信息的相关性,通过和其他数据信息的结合,可以间接识别特定自然人。综合国内外立法及实践情况,在IP属地是否属于个人信息的判断上,宜采用广义解释将其认定为个人信息。

2.2 IP属地是否属于“敏感个人信息”

2021年12月,全国信息安全标准化技术委员会发布的《网络安全标准实践指南——网络数据分类分级指引》中把行踪轨迹定义为“基于实时地理位置形成的个人行踪和行程信息”,如精准定位信息、GPS车辆轨迹信息、出入境记录、住宿信息等,强调了行踪轨迹是个人实时地理位置的信息记录。虽然《中华人民共和国民法典》(以下简称“《民法典》”)第1034条中把行踪信息纳入了个人信息范畴,但是并未对行踪轨迹下明确的定义。IP属地作为位置信息,是自然人实时地理位置和省份移动轨迹的记录,可以看作一种行踪轨迹类信息。行踪轨迹通常被视为敏感程度较高的个人信息,这也引发了进一步的思考,即IP属地是否属于“敏感个人信息”?

2.2.1 法律规定

《最高院、最高检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》第5条中把公民个人信息归列为高度敏感信息、一般敏感信息和普通个人信息并设置了相应的入罪标准^[21]。《个人信息保护法》颁布之前,“敏感个人信息”的概念只在《信息安全技术个人信息安全规范》(GB/T35273-2020)等标准层面出现过,从未在我国法律中明确规定。《个人信息保护法》第28条中把敏感个人信息定义为“一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息”,并列举了包括行踪轨迹在内七类典型的敏感个人信息。《个人信息保护法》在落地过程中对GDPR多有借鉴,GDPR第9条中规定了对

民族起源、政治观点、宗教信仰等特定类型个人信息的保护,但并未涉及明确的“敏感个人信息”表述。日本《个人信息保护法》(APPI)第2条规定“需要特殊保护的个人信息”是指包括种族、宗教、社会地位、医疗历史、犯罪记录、因犯罪遭受损害的事实,或者其他内阁命令规定的为避免引发歧视、偏见或者其他不利而需要特殊保护的个人信息,和我国敏感个人信息的概念具有高度一致性。

2.2.2 理论争议

敏感个人信息和个人信息的关键差别就在“敏感”的判断上,我国对敏感一词的法律评价标准存在一定的模糊性。支持主观说的学者认为“敏感个人信息”是使人敏感的个人信息,个人对该信息处理表现出高反应度^[22]。支持客观说的学者则认为“敏感”一词是基于社会多数人的共同心理,与一个国家的政治、经济、文化、社会等都存在联系^[23]。也有学者认为“敏感”并非个体对某种事物主观反应度的表现,而是指法律规制的高反应度。敏感个人信息的界定要在确定敏感个人信息法律基准和法律基准具体维度的基础上再确定判定标准,个人信息在达到“敏感”的法律基准并具备强工具性和唯一识别性时才应被认定为“敏感个人信息”^[24]。《个人信息保护法》对敏感个人信息保护的立法逻辑即敏感个人信息的不当使用会对自然人的身、财产权益造成损害。由此观之,立法中采用了“敏感”即造成侵害或危害结果上的容易性的客观说^[25]。在判断个人信息是否构成敏感个人信息时,宜采取以客观权益侵害风险为基准的观点,从公众认可度、发生可能性、损害严重性三个维度来进行区分。从公众认可度的角度来说,社会公众对IP属地信息的敏感性认可度较低;从发生可能性的角度来说,IP属地信息一旦泄露或被非法利用使个人信息权益受到侵害的可能性较大;从损害严重性的角度来说,IP属地信息泄漏或不当使用的影响和危害较低,给信息主体带来损害的可能性较小。如今关于IP属地是否应被界定为敏感个人信息的讨论仍在继续,根据不同维度、不同指标会得出迥然不同的结果,尚难断言IP属地是否属于敏感个人信息。

在IP属地的法律属性判断上,还存在其是否属于个人隐私的困惑。个人信息权和隐私权之间存在一定的交叉和重合,也在性质、客体等方面存在明确的界分^[26],在此不再赘述。总体而言,一般认为敏

感个人信息属于隐私的保护范围,一般个人信息则可进行商业化利用^[27]。因此,在IP属地是否属于用户个人隐私的判断上,仍需时间给出答案。随着大数据技术的发展,个人信息的边界正在逐步泛化,一般个人信息和敏感个人信息间的区别被进一步弱化,难以实现清楚地界定。只要样本容量足够大,通过技术手段能轻易地把自然人暴露在网络上的细琐信息拼凑成完整的人物画像^[28]。采取宽严相济的定义,把IP属地纳入个人信息的保护范畴符合大数据时代个人信息保护的发展理念。同时,应谨慎考虑是否把IP属地界定为敏感个人信息或隐私,防止个人信息保护因范围过大而失去可实施性。

3 平台责任的法理分析

根据《国务院反垄断委员会关于平台经济领域的反垄断指南》第2条的定义,平台是通过网络信息技术实现双边或者多边主体规则下交互,共同创造价值的一种组织形态。大数据时代平台间的商业竞争模式更多表现为“数据战”“信息战”,对平台上用户个人信息的收集分析、加工处理实现相关产品的营销推广,是如今互联网平台的主要运营模式和核心竞争力所在^[29]。为了更好地协调信息保护和信息利用,兼顾用户信息权益和平台商业利益,有必要明确平台在公开显示用户IP属地这一行为上的法律责任。

3.1 平台行为合法性辨析

以新浪微博为例,2022年4月28日,新浪微博管理员账号发布IP属地功能升级公告,正式针对全体用户开启“IP属地”功能。截止到2022年11月,用户仍无法主动关闭IP属地展示。即使在新浪微博隐私设置的个人信息与权限中关闭系统获取定位权限后,用户主页、微博评论时仍会显示IP属地。新浪微博“先斩后奏”的做法引起了大量用户的不满,尽管IP属地只是一个模糊的省份/地区(国内)或国家(国外)信息,无法链接到具体个人,但是用户在新浪微博上呈现的信息不限于此,结合用户主页信息、微博发布情况等很容易间接识别到特定自然人,强制公布用户IP属地可能会引发后续地域歧视、广告精准投放、个性化信息推送等。

在不少平台的公告中,显示IP属地的目的是为了打造真实的线上社区,整治热点问题造谣传谣现象。常态化显示IP属地的确暴露了部分用户人设与日常内容不符的现象,一定程度上达到了保障

平台内容真实的目的。但是认为公开 IP 属地就能消弭恶意造谣、冒充身份、蹭热度等不法现象难免过于乐观。平台方作为信息传播的把关人 (Gatekeeper)^[30], 承担着重要的信息审查责任, 在未恪尽职守对用户发布内容进行筛选、过滤的情况下, 以公开用户 IP 属地的方式来维护平台环境, 有履职不当之嫌。此外,《个人信息保护法》第 15 条中规定了个人对个人信息处理者处理个人信息的撤回权。平台强制显示 IP 属地、不允许自行修改删除是对用户撤回权的限制和剥夺, 以上行为的合法性仍有待讨论。

3.2 用户告知同意原则

平台对用户 IP 属地信息的处理可以分为信息收集和信息公开两个部分。在信息收集上, 如果用户自愿为平台开放获取系统位置的权限, 在用户知情并同意的基础上, 平台获得用户 IP 属地信息的合法性自不待言。平台方作为网络服务提供商, 基于网络链接的原理, 不可避免地会在运营过程中接触和收集到用户的精准位置信息, 因此, 平台在收集用户 IP 属地信息的环节并未侵犯用户的个人信息权益。在信息公开方面, 平台对 IP 属地信息的处理属于对个人信息的处理活动。在澳大利亚, 平台方作为网络服务的提供者只有经过法院或行政机关的命令才能公开用户的 IP 地址等个人信息^[31]。《个人信息保护法》第 25 条规定, 未经个人单独同意, 个人信息处理者不得公开其处理的个人信息。平台把个人的 IP 属地信息公开在个人主页及评论界面, 理应征得用户单独同意。

告知同意原则, 是个人信息处理中的黄金原则。《民法典》第 1035 条规定, 除法律、行政法规另有规定的之外, 处理个人信息应征得该自然人或者其监护人同意。《个人信息保护法》第 13 条规定, 原则上个人信息处理者在取得个人同意后才能处理个人信息 (除非有第 2 项至第 7 项的例外情形)。《个人信息保护法》第 14 条规定基于个人同意处理个人信息的, 应在个人充分知情的前提下自愿、明确作出。平台显示用户 IP 属地的行为是平台运营者研判了相关国家政策后, 在未保证用户知情、同意的前提下, 预先为其实施作出的准备, 明显不符合第 13 条第 2 项至第 6 项的规定情形。《管理规定》也因存在有违比例原则的争议而不宜成为第 7 项兜底条款中平台未经用户同意公开 IP 属地信息的

正当性来源。《民法典》第 1036 条规定, 为维护公共利益或自然人合法权益而合理实施的处理个人信息行为, 行为人不承担民事责任。平台在显示用户 IP 属地的公告中原因各异, 主要包括维护良好传播秩序, 维护社区生态氛围, 打击造谣传谣行为等。公共利益是指不特定多数人的利益, 公开用户 IP 属地是为了维护公共利益过于牵强, 应警惕平台把公共利益异化为限缩个人信息权益的借口, 平台无法通过该条款而免责。

3.3 处理个人信息的“最小必要”原则

如今大部分网络平台只有在用户“同意”的前提下, 才可以获得预期的服务。现实中用户对其个人信息的处理行为并无充分的选择权, 平台方往往不会事先单独征得用户同意, 而是在用户协议或隐私政策中通过“一揽子同意”的方式, 要求用户同意所有有关个人信息处理的授权, 以规避擅自使用用户 IP 属地信息引发的合规风险。通过对多个平台的实测, 绝大部分平台在不同其隐私政策的情况下会直接退出无法使用。还有平台会在协议中加入默认用户同意的条款, 如《微博服务使用协议》第 4.11 条中就指出“针对某些特定的微博服务的使用规则及说明, 微博运营方通过各种方式作出的任何声明、通知、警示都将被视为是服务使用协议的一部分, 用户如使用该等微博服务默认视为用户同意”。信息时代用户和平台间的关系是不对等的, 用户希望通过平台来达成社交目的、展现个人形象或是共享交流信息, 对作为服务提供方的平台有强烈的依赖性。作为信息处理者的平台有恃无恐, 不论用户主观上是否明确理解相关规则, 只追求其客观上点击同意的结果。在面对“全有或全无”的选择时, 用户为了继续使用不得不做出“一揽子同意”, 以暴露个人信息为代价来换取平台上的发言权。对平台而言“一揽子同意”的索权能避免侵权的法律风险, 但对于用户而言其授权范围远大于所需服务。

从法律层面来说,《个人信息保护法》第 6 条规定, 处理个人信息应采取对个人权益影响最小的方式, 不得过度收集个人信息。《个人信息保护法》第 16 条规定, 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由, 拒绝提供产品或者服务; 处理个人信息属于提供产品或者服务所必需的除外。这就涉及处理个人信息时的“最小必要”原则, 在最小性的判断上, 平台要求“一揽子同意”

的行为违背了“对个人权益影响最小的方式,必要的最小范围”规定。在必要性的判断上,《常见类型移动互联网应用程序必要个人信息范围规定》第3条规定,必要个人信息是指保障 App 基本功能服务正常运行所需的个人信息。公开 IP 属地并非相关平台正常运行和提供基本功能服务所必需,平台在用户拒绝平台获取或公开该信息的情况下仍应继续提供服务,且不得降低服务质量。在全球范围内,互联网平台的告知行使义务需要得到规制已是一种共识。GDPR 第 13 条和 CCPA 第 2 条中均指出应对告知的具体内容、方式做出明确具体的规定^[32],保障个人信息处理者在法律层面履行充分告知的义务。未来有必要在《个人信息保护法》等法律或司法解释中建立完整、系统的告知程序和救济程序,明确个人信息处理者告知用户何时何种程度公开个人信息、不同情形下告知的具体内容,以及公开后出现问题时可采取哪些救济措施等。

4 结论

对 IP 属地法律性质和平台责任的研究并非小题大做,如果放任平台侵犯用户个人信息权益的现象发生,可能会引发“破窗效应”^[33],导致管理和约束的失序。各大网络平台上线显示用户 IP 属地信息的行为,可以看作是《管理规定》落地前响应国家要求改善网络环境的一种尝试。目前尚无法对 IP 属地信息的法律性质作出明确界定,平台显示用户 IP 属地信息行为的法律责任也有待商榷,提出系统化的规制措施为时过早。在对个人信息主体权益日益重视的时代背景下,网络平台方应思考如何履行好主体责任,又避免因个人信息处理不当而引发后续法律问题。《个人信息保护法》第 69 条规定,个人信息处理者处理个人信息的行为侵害个人权益时适用举证责任倒置的原则,平台因无法承担证明自己无过错的举证责任而败诉的案例已有先例。为此,平台应建立起个人信息安全保护的体系,对内可以设置《个人信息保护法》第 52 条中的“个人信息保护负责人”职位、申请 ISO27001 信息安全管理体系认证等,把个人信息保护渗透到组织架构和管理制度中,建立完备的个人信息安全合规体系。对外可以和专业第三方机构展开合作,制定完备、公开的平台隐私政策文本,把个人信息的收集、传输、共享等环节匹配到相应的系统设置中,使个人信息保护规则落到实处。

参考文献

- [1] 金晨. 亮明 IP 属地, 净化网络生态[N]. 人民日报(海外版), 2022-05-27(8).
- [2] 张宣. 你的网上门牌号—IP 地址安全吗[N]. 新华日报, 2022-05-11(13).
- [3] 孙冰. IP 属地显示后谁慌了? 安全专家提醒小心成了黑灰产“猎物”[J]. 中国经济周刊, 2022(10): 75-77.
- [4] 石佳友. 网络环境下的个人信息保护立法[J]. 苏州大学学报(哲学社会科学版), 2012(6): 85-96.
- [5] 韩旭至. 个人信息列举式规范之审视[J]. 河南财经政法大学学报, 2018(4): 46-55.
- [6] 翟嘉诗. IP 地址信息的法律属性分析—兼评微博显示用户 IP 属地信息行为[J]. 互联网天地, 2022(5): 49-53.
- [7] 王东方. 网络平台公开用户 IP 属地信息的适法性分析[J]. 新疆社会科学, 2022(5): 123-130, 180.
- [8] 姚瑶. “IP 代理”乱象该管了[J]. 法人, 2022(6): 63-64.
- [9] 周秀娟, 史雨萱. 数字经济时代个人数据携带的私法规制路径研究——以欧盟 GDPR 为视角[J]. 电子科技大学学报(社科版), 2022(2): 70-77.
- [10] 周斯佳. 个人数据权与个人信息权关系的厘清[J]. 华东政法大学学报, 2020(2): 88-97.
- [11] 余筱兰. 论法学上的个人信息与个人数据[J]. 上海法学研究, 2021(19): 135-139.
- [12] 任龙龙. 个人信息民法保护的理论基础[J]. 河北法学, 2017(4): 181-192.
- [13] 韩旭至. 个人信息概念的法教义学分析——以《网络安全法》第 76 条第 5 款为中心[J]. 重庆大学学报(社会科学版), 2018(2): 154-165.
- [14] 邓明理. 大数据背景下个人数据的监管保护[J]. 北京邮电大学学报(社会科学版), 2019(1): 19-25.
- [15] 张燕, 何雨歌. 欧洲法院个人数据保护典型案例述评[M]. 上海: 上海交通大学出版社, 2021.
- [16] 韩旭至. 大数据时代下匿名信息的法律规制[J]. 大连理工大学学报(社会科学版), 2018(4): 64-75.
- [17] 梅夏英. 数据的法律属性及其民法定位[J]. 中国社会科学, 2016(9): 164-183, 209.
- [18] 谢琳. 大数据时代个人信息边界的界定[J]. 学术研究, 2019(3): 69-75.
- [19] 王利明. 论个人信息权在人格权法中的地位[J]. 苏州大学学报(哲学社会科学版), 2012(6): 68-75, 199-200.

- [20] 刘海波, YOUNG ANN. 内容分选 平台助力 数据驱动: 大数据视阈下影视新媒体平台的发展策略——以 Netflix 为例[J]. 电影文学, 2020(15): 3-8.
- [21] 张勇. 公民个人信息刑法保护的碎片化与体系解释[J]. 社会科学辑刊, 2018(2): 86-93.
- [22] 陈海帆, 赵国强. 个人资料的法律保护: 放眼中国内地、香港、澳门及台湾[M]. 北京: 社会科学文献出版社, 2014.
- [23] 杨合庆. 中华人民共和国个人信息保护法释义[M]. 北京: 法律出版社, 2021.
- [24] 宁园. 敏感个人信息的法律基准与范畴界定——以《个人信息保护法》第 28 条第 1 款为中心[J]. 比较法研究, 2021(5): 33-49.
- [25] 程啸. 个人信息保护法理解与适用[M]. 北京: 中国法制出版社, 2021.
- [26] 王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013(4): 62-72.
- [27] 房绍坤, 曹相见. 论个人信息人格利益的隐私本质[J]. 法制与社会发展, 2019(4): 99-120.
- [28] 张里安, 韩旭至. 大数据时代下个人信息权的私法属性[J]. 法学论坛, 2016(3): 119-129.
- [29] 武腾. 最小必要原则在平台处理个人信息实践中的适用[J]. 法学研究, 2021(6): 71-89.
- [30] 张品良. 网络文化传播: 一种后现代的状况[M]. 南昌: 江西人民出版社, 2007.
- [31] 魏求月. 网络服务提供者侵权责任的障碍与解构[J]. 中国高校社会科学, 2020(2): 125-134, 160.
- [32] 丁晓东. 个人信息保护: 原理与实践[M]. 北京: 法律出版社, 2021.
- [33] 乔治·凯林, 凯瑟琳·科尔斯. 破窗效应[M]. 上海: 三联书店出版社, 2014.

(收稿日期: 2022-10-28)

作者简介:

严驰(1998-), 男, 硕士研究生, 主要研究方向: 数字法、知识产权法。

“计算法学: 数据法治与法律科技”主题征文通知

党的二十大报告指出, “全面依法治国是国家治理的一场深刻革命”, “必须更好发挥法治固根本、稳预期、利长远的保障作用, 在法治轨道上全面建设社会主义现代化国家”。随着新一代信息技术的快速崛起, 传统法学研究范式正经历深刻变革, 计算科学与传统法学已成为新的发展趋势, 数据空间、数据挖掘、人工智能设计算法、机器学习算法等越来越广泛地影响着法律的制定和实施。目前, 在智慧法院的建设中, 通过信息化手段开展人工智能辅助在线纠纷解决等实践, 为更好地服务诉讼群众, 践行司法公正, 提升国家治理体系和治理能力现代化做出了贡献。为反映计算法学领域的前沿成果和理论创新, 做学科交叉融合的催化剂, 加强基础学科培养能力, 《网络安全与数据治理》编辑部特别企划“计算法学: 数据法治与法律科技”主题征文, 向计算法学领域的专家学者发出邀请, 共同为在法治轨道上实现中国式现代化助力, 诚挚邀请相关领域的专家学者积极投稿。

一、征文主题: 计算法学: 数据法治与法律科技

主题范围包括但不限于:

- (1) 数据要素赋能社会治理研究; (2) 数据确权与数据安全研究; (3) 算法治理研究; (4) 人工智能侵权研究; (5) 个人信息保护研究; (6) 数字货币问题; (7) 大数据挖掘与机器学习; (8) NLP 技术应用; (9) 元宇宙的法治问题探究; (10) 智慧法院和在线诉讼的理论与实践。

二、特约主编

申卫星, 清华大学法学院教授、博士生导师; 国务院政府特殊津贴专家, 国家万人计划哲学社会科学领军人才, 德国洪堡学者、美国哈佛大学福布莱特访问学者。研究方向为民法学、计算法学。

三、投稿须知

论文要求为中文论文, 观点鲜明、逻辑严谨, 论据充分、方法合理、数据翔实, 能够反映计算法学领域的最新研究成果。投稿文章须未在其他期刊或者出版正式论文集的会议上刊登过, 且不在其他刊物或会议的审稿过程中, 不存在一稿多投现象; 保证文章的合法性(无抄袭、剽窃、侵权、虚假引用等不良学术行为), 字数 6000-10000 字左右。

稿件经评审合格录用后, 在《网络安全与数据治理》(正刊) 上以主题专刊形式发表。

投稿方式: 请在投稿网站 <http://www.pcachina.com> 注册、投稿。注册后请投稿在“计算法学”栏目。

稿件模板下载网址: http://files.chinaaet.com/files/Periodical/pcachina_Templates.doc。

四、时间安排

截稿日期: 2023 年 4 月 30 日

出版日期: 2023 年 6 月 15 日 第 6 期(6 月正刊)

《网络安全与数据治理》编辑部
2022 年 11 月

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com