



文献引用格式: 马美瑶.企业数据合规的现实困境与实践路径[J].信息安全与通信保密,2022(7):150-158.

MA Meiyao.Practical Dilemma and Practical Path of Enterprise Data Compliance[J].

Information Security and Communications Privacy,2022(7):150-158.

企业数据合规的现实困境与实践路径^{*}

马美瑶

(重庆邮电大学, 重庆 40065)

摘要: 数据作为一种新生产要素,蕴藏着巨大的能量和价值,时刻影响着国家社会发展的方方面面。同时,对于企业来说,数据是其核心竞争力,数据合规是其生存发展的基石。随着信息时代的到来,企业数据合规面临着法律监管严、技术保障难、内部管理差和违规应用多等一系列现实难题,为了更好地发挥数据价值并推动企业健康发展,从国内外的数据安全立法概况出发,对我国企业数据合规的现实困境及成因展开分析,并提出解决方案,试图探索一条我国企业的数据合规实践路径。

关键词: 数据合规;数据立法;企业困境;合规路径

中图分类号: D920.4

文献标志码: A

文章编号: 1009-8054(2022)07-0150-09

Practical Dilemma and Practical Path of Enterprise Data Compliance

MA Meiyao

(Chongqing University of Posts and Telecommunications, Chongqing 40065, China)

Abstract: As a new factor of production, data contains huge energy and value, and always affects all aspects of national social development. At the same time, for enterprises, data is their core competitiveness, and data compliance is the cornerstone of their survival and development. With the advent of the information age, enterprise data compliance is facing a series of practical problems, such as strict legal supervision, difficult technical support, poor internal management and many illegal applications. In order to better play the value of data and promote the healthy development of enterprises, this paper analyzes the practical dilemma and causes of data compliance of Chinese enterprises from the perspective of the overview of data security legislation at home and abroad, and puts forward corresponding solutions, trying to explore a data compliance practical path for Chinese enterprises.

Key words: data compliance; data legislation; enterprise dilemma; compliance path

* 收稿日期: 2021-12-30; 修回日期: 2022-05-13 Received date: 2021-12-30; Revised date: 2022-05-13

0 引言

当前以大数据、云计算、人工智能等为代表的信息技术快速发展，为经济社会发展提供了巨大动力，也为人民生活带来了许多便利。其中，数据是关键生产要素。对企业来说，做好数据合规，不仅可以为企业创造巨大的商业价值，还能避免企业陷入法律风险，督促企业积极承担社会责任；对个人来说，数据合规可以防止个人信息数据泄露，保护用户隐私。在社会层面，企业数据合规可以促进数据产业的安全健康发展，营造风清气正的网络环境。企业需要在数据标准、数据分类、数据存储、数据安全、数据文化等方面做到数据合规。其目的是合法合规地引导数据资产实现价值变现。但是，在互联网时代，数据也面临着风险和危机，稍有不慎便可能成为引发个人信息保护、市场秩序、社会治理和国家安全等问题的导火索^[1]。从企业在数据合规方面的遭遇来看，数据违规收集、应用和储存使得企业面临巨额罚款甚至停产停业危机，黑客入侵、数据泄露等外部风险让企业风雨飘摇，企业合规成本高昂、内部泄密严重等让企业应接不暇，漏洞百出。面对这些风险挑战，如何让企业在竞争激烈的市场中站稳脚跟并向好发展，是企业数据合规需要完成的使命。

1 国内外数据安全立法概述

1.1 国内数据安全立法方面

以2017年《中华人民共和国网络安全法》的实施为开端，我国开始迈进数据应用和治理

法治化时代，将数据安全纳入了国家安全的范畴进行保护。2021年9月1日《中华人民共和国数据安全法》正式施行，同年11月1日《中华人民共和国个人信息保护法》开始实施，同年11月14日国家互联网信息办公室发布了《网络数据安全管理条例（征求意见稿）》（以下简称“条例”），这标志着我国数据安全立法开始走向成熟。以上述“三法一条例”的颁布实施为标志，我国的数据安全立法已经进入了快速发展时期。同时“三法一条例”也是当前企业数据合规建设的基本遵循。

具体来看，《中华人民共和国数据安全法》作为数据安全领域的专项法律，体现了国家立法层面对数据安全的高度重视，同时，对企业数据合规建设也具有重要指导意义。比如，该法的第八条规定了企业收集和使用数据应遵循的基本原则，第十九条表明企业在满足相应条件的情况下可以进行数据交易，此外，还在第四章集中列明了在中国境内从事数据处理活动的企业应当承担的基本数据合规义务。这些法条都为企业数据合规指引了方向。同样，在《中华人民共和国个人信息保护法》中也对企业数据合规提出了要求，个人信息的处理更加严格，还作出了举证责任倒置的规定，即在个人信息权益受到侵害时，大数据企业负有证明自己没有过错的义务。而“条例”则是对《中华人民共和国数据安全法》等上位法的进一步细化实施，在关于数据收集的第四章中，规定了网络运营者的数据安全合规义务，进一步明确平台规则透明度义务、平台第三方产品及服务侵权的先行赔偿责任等，在一定程度上增加了企业的合规难度。



1.2 国际数据安全立法方面

当前,以欧盟出台的《通用数据保护条例》(General Data Protection Regulation, GDPR)为契机,各国开始制定或修改本国的数据保护法规,例如,2018年6月,美国加州出台的《加州消费者隐私法案》被称为美国最全面、最严格的州数据隐私法,该法案于2018年6月28日颁布,并于2020年1月1日生效。2020年6月,日本参议院颁布了《个人信息保护法修正案》,此修正案将于2022年4月1日正式实施。本次修订扩大了个人权利,还把违规企业的罚金上限提升至1亿日元(约合人民币650万元)。2020年11月,加拿大政府推出《数字宪章实施法案》,如果通过,它将取代现有的《个人信息保护和电子文件法》,并对该国的隐私立法引入一些新的变化。据联合国贸易和发展会议数据显示,全球范围内已经有超过100个国家进行了数据安全保护相关的立法,40多个国家出台了相应的草案,可以说,当今世界已经掀起了数据安全立法的高潮,国际社会开始进入数据保护的快速发展期。各国数据安全立法主要有以下几个特点。

一是许多国家逐渐形成全方位保护的立法理念,并突出个人信息使用限制。纵观各国关于数据安全的立法,从数据的产生、收集、存储到使用、加工、传输、提供、公开等一系列环节,都有相应的法规予以保护。二是明确管辖范围,加强与数据流通密切的相关国家和地区的数据信息交流合作,共同打击数据侵权与泄露事件。现今许多国家都十分注重网络空间主权,在数据安全立法方面,都强调管辖权的重要性,长

臂管辖已成为今后的立法趋势。三是强调对个人信息与隐私的保护,大多数国家和地区均出台单独的法典对其进行规范。个人信息是数据保护中的重中之重,对个人信息的滥用、侵权等行为都将违反本国的相关法律法规,并受到相应的处罚。四是各国开始采用精细化的立法方式来保护数据安全,明确各方法律义务责任,提升数据治理效果。“数据”一词内涵丰富,这就要求立法的精准性,要能够解决形形色色的问题,做到有法可依。

从上述国际立法特点可以看出,各国对于数据和信息的管理愈加严格,这同时也意味着企业尤其是跨国企业更应当做好数据合规建设,以满足国际上对数据安全的要求。

2 企业数据合规面临的现实困境及其成因

2.1 数据应用违规,企业合规成本高昂

在网络时代,数据是数字经济的核心,是推动新经济发展的关键^[2]。数据从产生、收集到后续的使用、保存等全生命周期都会面临一系列的安全风险,稍有不慎,就会出现数据违规的现象。数据收集之初,有直接收集、间接收集和通过爬虫技术收集等方式,其中,通过爬虫技术获取其他公司数据,若严重干扰其他企业正常合法经营,违反诚实信用原则和公认的商业道德,则很有可能构成不正当竞争。例如,微博起诉超级星饭团不正当竞争案一审宣判,超级星饭团擅自抓取微博用户相关信息、非法获取微博相关数据,构成不正当竞争,被判赔偿1000多万元;若更进一步采用技术手段非法

获取计算机信息系统中存储的数据，则有可能触犯刑法，构成非法获取计算机信息系统数据罪^[3]。企业在使用数据的过程中，常常会出现滥用数据的情况，如对一些个人敏感信息不脱敏直接使用或者未征得用户同意直接使用数据等，这些都会引发企业与用户信任危机，例如，Facebook 涉嫌非法收集生物识别数据，与用户达成隐私纠纷和解，赔偿了 5.5 亿美元；谷歌因违反 GDPR 而被法国数据保护监管机构 CNIL 处以 5 000 万欧元的罚款^[4]。我国数据违规现象也层出不穷，例如，2021 年的 3·15 晚会就曝光了人脸信息被违规收集、求职简历被非法买卖、手机清理类软件恶意窃取手机内部信息等多起涉及个人信息安全的事件。

对于企业来说，数据合规最关键的两点在于：一是要求数据应用合乎法律规定（包括数据的利用、处理、使用等行为合乎法律规定，不得违反国家强制性法律规定），二是数据应用不得侵犯他人的正当合法权益，这同时也是数据合规审查的两条红线^[5]。而企业在数据应用上之所以会出现违法违规现象，很大程度上在于要做到上述两点成本十分高昂，尤其是对于小型企业，高昂的合规成本使之望而却步，似乎只有对数据的无限制使用才是其获取利润的“唯一”选择。据 Telos 最近开展的一项企业合规成本调查显示：每家企业要做到数据合规，平均需要遵守至少 13 个不同的 IT 安全或隐私法规，并且每年在合规性活动上要花费高达 350 万美元。于是许多企业抱有侥幸心理，或者说是一厢情愿地认为自己对数据的使用是合法合规的，殊不知这已经犯了企业合规经营的大忌。

2.2 企业内外数据泄露严重

随着技术的快速更迭，数据泄露的方式也多种多样，如病毒与非法入侵、系统漏洞、访问控制和权限管理不善等，这些都使得企业遭受巨大损失。企业在面对数据泄露时，常常会出现应对无措的情况。当下许多企业尤其是互联网企业都时刻面临着来自内部和外部的各种风险挑战。内部风险主要包括系统存在漏洞未及时发现、系统未及时更新、个人私密信息未使用脱敏技术、对企业核心数据未采用加密保护的技术手段等；外部风险主要是黑客出于炫耀或其他目的，利用特定的漏洞来窃取信息数据，或者是来自恶意人士的攻击，包括网络钓鱼诈骗、数据盗窃赎金勒索和鱼叉式网络钓鱼活动等，这些都给企业及个人造成了严重损害。尽管企业采用了一些安全防护手段，但是从结果来看，还远远不够。面对上述随时会发生的风险，企业防不胜防，同时在一定程度上也说明了企业在数据保护技术上的不足，使得不法分子有了可乘之机。

2.2.1 网络攻击形势严峻，外部泄露严重

据波耐蒙研究所发布的《2020 年数据泄露损失研究》评估显示，遭遇数据泄露事件的企业平均损失 386 万美元。2018 年，Facebook 公司就曾发生严重的数据泄露事件，业界称其为“数据门”事件^[6]，该事件造成了超 8 000 万用户的信息外泄。据报道，Facebook 与 GSR 公司签署了相关保密协议，但 GSR 私下违反协议，将数据转卖给了第三方剑桥数据分析公司（一家涉嫌影响美国选举的公司）。经过多年的调查，监管机构认为 Facebook 因未能保护这些数据而



违反了其较早签署的保护用户隐私协议。同年10月,英国信息专员办公室向 Facebook 处以 50 万英镑罚款,2020 年 4 月,美国联邦法院正式批准了美国联邦贸易委员会与 Facebook 达成的 50 亿美金和解协议。

网络和平研究所所长 Marietje Schaake 曾说,“尽管网络攻击是一种无声的威胁,但它们会对我们的社会产生破坏性和持久性的影响”。这对企业来说也不例外。随着物联网的发展,数以十亿计的设备接入移动互联网,网络攻击造成的威胁正在呈指数级增长。据美国高德纳咨询公司(Gartner)预测,到 2022 年左右,全球网络安全支出费用将达到 1 704 亿美元。在网络攻击不断加剧的情况下,若企业一味固守之前的应对模式,则很有可能被竞争激烈的市场淘汰。同时,相较于大型企业,中小型企业由于缺乏完备的合规体系,更容易成为网络攻击的首选对象。根据 Markel Direct 的一项调查结果显示,51% 的中小企业都曾有过网络安全漏洞,所以对中小企业来说,一旦遭遇攻击,企业将面对来自资金链断裂和核心技术泄露的双重威胁,这对企业的打击无疑是致命的^[7]。

2.2.2 内部泄密严重

数据泄露的原因除外部黑客非法窃取外,还有便是企业内部员工导致的泄露。由于数据合规的专业性较强,很多员工尚无相关的知识储备,无法意识到数据合规的重要性,会有意无意地接触到核心数据或者关键数据并使其泄露或者流失,给企业造成重大损失。内部泄露主要分为两种类型:一是内部员工因疏忽大意导致泄露而不自知,比如员工对信息数据使用

不当、安全意识差等;二是内部员工恶意泄露,比如员工将企业信息数据资产进行出售来获取非法利益或者人员报复性操作等。从现实案例来看,显然后者的危害性更大,例如,2018 年 1 月,某警方侦破了一起新生儿信息倒卖链条,经查明,是某地方卫生系统的工作人员泄露了 50 多万条新生儿和预产孕妇信息数据;2018 年 2 月,某知名企业的合作公司员工泄露防伪数据 700 万条,直接导致了该企业经济损失约 105.7 万元。这些泄密事件都给企业数据的安全性敲响了警钟,说明了企业员工的违法违规操作可能给企业数据合规造成潜在的威胁和损害。

2.3 立法管控愈严,数据处理不当的后果愈重

随着国内外对数据合规的监管不断加强,企业对数据的处理不当导致的泄露,引来监管部门的关注,在调查清楚事件后,等待的是相关执法机构的一系列处罚,其中最引起公众关注的还是不断增加的巨额罚款案例。2016 年,网约车平台 Uber 遭到黑客攻击,泄露了 60 万司机和 5 700 万用户的个人信息。该公司没有披露该事件,而是向黑客支付了 10 万美元,试图瞒天过海,该行为使公司付出了沉重的代价,在 2018 年因违反州数据泄露通知法而被罚款 1.48 亿美元^[8]。2017 年,Equifax 由于一个数据库未及时安装 Apache Struts 框架的严重漏洞补丁,损失了近 1.5 亿条个人信息和财务信息。后在 2019 年 7 月,Equifax 就此次事件,同意向美国联邦贸易委员会、消费者金融保护局以及美国 50 个州和地区支付 5.75 亿美元,可能增至 7 亿美元,并承诺采取合理的方法来保护其网络。这些都充分说明了国际立法非常重视数据安全,

同时，巨额罚款对某些企业来说是致命的打击，可能导致企业出现资金周转困难、企业信誉下降等后果，从而失去市场中的竞争力。

2020年，我国信息安全标准化技术委员会发布了53项网络安全国家标准，同时，关于数据安全与合规方面的配套制度也在不断推进，相关执法实践逐步走向常态化，诉讼案例逐渐丰富。针对企业数据违法违规方面，也分别适用了不同的法律法规予以制裁，比如《中华人民共和国刑法》《中华人民共和国民法典》《中华人民共和国网络安全法》等的配套使用。其中以《中华人民共和国网络安全法》为例，在第六章就规定了十余种法律责任及处罚措施。就罚款来说，我国开始向国际靠拢，要求建立和完善惩罚性赔偿和巨额罚款制度，让严重违法者付出高昂成本。这在很大程度上给企业造成了隐形的压力，迫使企业不得不开始注重数据合规。

2.4 合规意识淡薄，企业潜藏重大风险

数据是一个企业的生命，但是企业员工甚至企业管理者却没有意识到这一点，从而导致数据流失、数据泄露，给企业造成一笔不菲的“支出”，甚至让企业面临“死亡”的危机。在企业治理上，很多企业管理者由于没有正确认识公司治理风险的概念和种类，难以意识到合规风险的重要性，比如行业将风险分为技术风险、销售风险、产品质量风险、知识产权风险等，但是并未抓住分类的依据和意义，从而将合规风险这一重要类别忽视不管，使企业数据安全隐患大大增加。根据公司治理风险的基本理论，企业面临的主要风险可以分为3大类型：经营

风险、财务管理风险和合规风险^[9]。因此，对于企业管理层来说，只有先分清风险类别，了解数据合规的重要性，打破固有的“数据无用”观念，才能走好企业数据合规的第一步。同样，对于企业员工来说，数据合规不应是一个“新词”，成为员工自我约束的“法外之地”。在互联网时代，员工的一言一行、一举一动都会在网络上存下数据、留下痕迹，所以仅以“不知者无罪”而免除责任者“明知不可为而为之”的责任都是不可行、不可取的做法。这些都反映了企业整体合规意识的淡薄，对核心竞争力的保护力度不够。

3 企业数据合规的实践路径

3.1 国家法律支持

3.1.1 立法明晰企业类别，及时更新合规要求

从整体上看，国内外监管趋势愈加严格，我国关于数据安全立法的顶层设计也在抓紧建设中，但是在具体落实上仍存在许多法律空白。在企业数据合规方面，立法也有亟待出台和完善的地方。同时，从上述企业面临的现实困境可以看出，高昂的合规成本与短期无法得到的收益使得许多企业铤而走险，忽略了自身的数据合规问题。面对这一现象，或能采取立法手段有所消解。

立法可以根据不同行业、企业规模大小、年收益多少等将企业进行细分，再以此为前提对不同的企业规定不同的合规要求，而不是将大型企业（包括跨国企业）与小型企业等同视之，这样可以从源头上打破小型企业对数据合规成本的顾虑，从而做到精细化立法。比如在数据



安全与合规中有一个重要制度——数据分级分类管理制度，针对不同类型的企业，其数据的种类和重要程度均有所不同，因此，立法需明晰企业类型、确定数据分类和区分数据重要性，再对企业数据合规提出具体要求，让企业有法可依。同时，国家需要及时更新每个层次所对应的具有代表性的企业合规范例，鼓励其他企业学习参考及应用。

3.1.2 从理论到实践，普及数据合规知识

在数字化时代，为了使企业认识到数据合规的重要性，监管部门应该积极普及数据合规的相关知识。政府和司法部门相互配合，上到法律法规的出台，下到具体案件的审判，从正面的法律知识普及到反面的违法违规案例公开，都是促使企业认识到数据合规重要性的好方法，同时，还可以组织数据合规方面的法律宣传会议、知识演讲等，促进企业树立全面的数据合规建设思想，让企业从整体上意识到数据违法违规的危害性，从而有意识地关注并解决自身的数据合规建设问题。

3.2 政府大力扶持

政府鼓励并帮助企业进行技术升级。做好企业数据合规，离不开技术的支持。而高新技术的应用，离不开政府的大力支持。正如“市场是只看不见的手，需要政府的监督”，企业应用新技术也需要政府的帮助。首先是物质支持，政府可以参照《中华人民共和国中小企业促进法》对一些掌握核心数据的或者是前景广阔的但资金有限的企业提供财政支持，例如补贴或者无息借款，让企业能够合法合规地生存；其次是技术提供或者分享，若政府在数据合规

的某个方面具有领先于企业的技术，那么可以考虑免费或者低价提供给有需要的企业，让市场展现出最大生机活力。最后，企业是数据合规的主体，政府应发挥引导作用，通过制定发展路线图、数据合规实施纲要及建设科技示范基地等方式来推动企业数据合规的发展。

3.3 企业自身建设

3.3.1 优化企业数据合规结构，降低合规成本

“打铁还需自身硬”，对于企业而言，解决数据违规应用问题的关键在于自身数据合规体系的建立完善。除了国家层面的立法指导，政府的帮助扶持，企业也需要根据自身的整体情况，建立一套完整而有效的合规体系。考虑到合规的高成本，企业可以运用智能化的方式推进数据合规建设^[10]。智能化的合规方式可以使数据从产生之初到后续的应用等一系列行为都处于一个合法化、标准化的环境中，从而可以节省人为合规所带来的高昂成本。同时，通过算法还可以对国家法律法规进行及时的更新，以便企业能对数据合规的变化做出快速反应，将一些常见违规行为进行标记和保存，给企业以警醒的作用。而且智能化的数据合规还可以在企业日常运营中对数据进行备份和保存，一旦发生数据泄露事件，可以让企业留有充分的证据为自己辩白，减轻甚至是免除企业的责任。当然，企业也要经常关注自己行业内的、与其实力相当的、数据合规出色的企业的做法，不断学习改进修正自身的数据合规体系漏洞，争取做到低投入、高收效，降低企业数据违法违规的风险隐患。企业还需与监管部门保持良好沟通，这样不仅有助于减少误解，还可能获得

及时且恰当的指导和支持。

3.3.2 强化技术更新，严防数据泄露

企业数据泄露事件频频发生的原因之一是企业的技术保障力度不够。很多企业意识到数据的商业价值，但是由于技术有限，也无法做到数据合规。因此，对企业来说，提高数据安全保障技术刻不容缓。在企业外部防护方面，可以根据企业自身的实际情况，购买数据安全防护产品，同时注意选择最优的技术手段来巩固自己的数据系统，比如在用户隐私保护方面，可以采用差分隐私技术，差分隐私保护可以克服传统隐私保护技术应用时其安全性依赖攻击者的相关背景知识、保护效果难以用有效严格的数学方法定量化描述等缺陷，从而可在大大降低保护对象数据集隐私泄露风险的同时，尽可能保证数据集数据的可用性^[11]。在企业内部治理方面，可以采用智能敏感数据识别技术和数据脱敏风险评估技术，利用智能化的方法对数据进行识别、加工，不仅可以大大节约合规成本，还能减小企业“犯错”的可能性。在企业间数据交互方面，同样可以采用前沿性数据匿名、同态加密、安全多方计算和联邦学习等技术对重要数据进行匿名化处理或者机密保护。企业只要在技术保障上做到位，就可以遏制住大部分的数据泄露和数据滥用现象。

3.3.3 设立企业数据合规官，洞悉立法走向

在国际上，绝大多数跨国企业应业务所在国的要求设立了企业数据合规官或者数据保护官一职。“道德与合规官”一词最早出现在 20 世纪 80 年代的美国企业，其职责是研究制定企业合规经营政策，监督管理企业文化和各项治

理制度的执行与落实^[12]。在我国，360 公司是国内首家设置首席隐私官的大型互联网企业^[13]。

对于这些企业来说，数据合规官不仅管理企业日常数据保护工作，还承担着“数据外交”的职能，其姓名与联系方式需要对外披露，同时还要与监管机关、数据主体进行对接，并且时刻掌握数据合规的监管走向。由此可见数据合规官设置的必要性，这也不失为我国企业进行数据合规建设的一个好的借鉴方法。但是，值得注意的是，大型企业除了设置数据合规官，还要配置合规部门，配合数据合规官的工作，当然，中小型企业则视自身情况而定，可以设置合理人数的合规专员监督审查企业数据合规情况。

3.3.4 建立企业数据合规文化，培养合规意识

当下许多企业出现数据违法违规现象，源于企业内部对合规文化的不重视。因此，建立企业数据合规文化，培养全员合规意识成为形势所趋。

从整体上看，企业要正确定位数据合规文化的重要内涵，将其核心要义和内容渗透到企业运营理念、业绩考核等日常经营活动中，特别是涉及企业跨地区、跨国家，从员工个人到企业整体，都要具备合规意识。具体来说，一方面，针对企业内部安全、合规、审计等直接责任部门人员，要在正式入职前加强专业知识和工作能力的教育和培训，保证其在工作期间能够遵守相关法律法规和企业规章制度；另一方面，对于其他工作部门人员，则需要加强合规风险与意识的教育和培训，企业可以定期组织数据合规知识竞赛及专业人员数据安全比赛，以奖励的方式激发员工对数据保护与合规的兴趣，最终达到企



业内部人员无论职位高低,都对数据合规有较为清晰的认知和足够重视的效果。

4 结 语

在“数据为王”的时代,企业不仅要面临竞争激烈的市场角逐,还要处理好数据合规的一系列难题。通过上述分析的企业面临的合规困境及成因可见,企业若不重视起来积极寻找解决之道,则很可能有倾覆之险。与此同时,随着数字经济时代的到来,企业应当顺应数字经济化的潮流,从不同方面加强自身数据合规建设,在合法合规的前提下充分利用数据,发挥数据的最大价值,做到以数据合规促进企业更好发展,才是现代企业的生存之道。✕

参考文献:

- [1] 支振锋. 贡献数据安全立法的中国方案[J]. 信息安全与通信保密, 2020(8):2-8.
- [2] 齐力. 企业如何开展数据治理和提升数据治理水平[J]. 中国对外贸易, 2020(8):24-25.
- [3] 李姝. 超级星饭团关联公司云智联网络科技有限公司(北京)有限公司与北京微梦创科网络技术有限公司不正当竞争纠纷案[EB/OL]. (2021-07-06)[2022-07-22]. <https://baijiahao.baidu.com/s?id=1704534350293312612&wfr=spider&for=pc>.
- [4] 游侠网. 谷歌被欧盟罚款 5 000 万欧元涉及侵犯用户隐私数据[EB/OL]. (2020-06-21)[2022-04-20]. https://www.sohu.com/a/403289133_119620.

- [5] 高富平. 2016年腾讯大数据与合规峰会演讲稿[EB/OL]. (2016-11-10)[2022-07-22]. http://www.360doc.com/content/16/1108/19/11507367_604965231.shtml.
- [6] 百度百科. 脸书数据门[EB/OL]. (2019-04-08)[2022-04-20]. <https://baike.baidu.com/item/%E8%84%B8%E4%B9%A6%E6%95%B0%E6%8D%AE%E9%97%A8/2449948?fr=aladdin>.
- [7] HelpNetSecurity. Small Businesses are most Vulnerable to Growing Cybersecurity Threats[EB/OL]. (2022-01-11)[2022-04-20]. <https://www.helpnetsecurity.com/2022/01/11/small-businesses-vulnerable/>.
- [8] 李延舜. 隐私政策在企业数据合规实践中的功能定位[J]. 江汉论坛, 2020(10):136-144.
- [9] 陈瑞华. 企业合规的基本问题[J]. 中国法律评论, 2020(1):178-196.
- [10] 钟灵. GDPR 影响下我国涉欧企业的数据合规路径[J]. 经济研究导刊, 2020(21):166-167, 199.
- [11] 付钰, 俞艺涵, 吴晓平. 大数据环境下差分隐私保护技术及应用[J]. 通信学报, 2019, 40(10):157-168.
- [12] 王媛. 我国上市公司合规官制度构建研究[D]. 北京: 中国政法大学, 2018.
- [13] 卓丽. GDPR 下企业数据合规问题及对策分析[J]. 北外法学, 2020(1):182-196.

作者简介:



马美瑶(1997—), 女, 硕士研究生, 主要研究方向为信息法学、网络法学。