

【网络社会变革与管理】

“互联网+”时代公民信息安全的法律保护研究

张 琴

(南京邮电大学 社会与人口学院, 江苏 南京 210023)

摘 要:在“互联网+”时代,公民信息安全面临严峻挑战。分析网络条件下的公民信息安全保护的法理基础和重要性,结合“互联网+”时代信息安全保护的的特殊性,探讨我国公民信息安全保护的现状及存在问题,从法律层面及管理与技术层面提出我国公民信息安全保护法律制度的设计方案:我国应加快个人信息保护法的立法进程,进一步完善互联网立法内容和结构,形成立法、执法、司法部门合力,以提高法律保护公民信息安全的效果。同时,应加强互联网行业自律,提升个人信息保护的技术,加强公民普法宣传教育和国际合作,共筑公民信息保护的屏障。

关键词:“互联网+”;公民信息安全;网络安全法;个人信息保护法

中图分类号:D923 **文章编号:**1673-5420(2019)03-0014-10

近年来,我国制定了“互联网+”行动计划,大力推动移动互联网与其他行业融合,已逐步迈入“互联网+”时代。与此同时,作为衡量经济发展状况和现代化水平的重要指标的信息化水平也在快速提升。截至2018年12月,我国网民规模达8.29亿,互联网普及率达到59.6%^[1]。

随着互联网的快速发展,公民信息安全面临巨大的风险。个人信息泄露案件屡有发生,严重侵害了公民利益。多家互联网公司、快递公司、外卖平台、知名酒店、银行等纷纷卷入信息泄露事件。信息违法犯罪触目惊心,直接导致公民隐私、财产等权益受到侵犯。

为应对公民信息安全频受侵犯的严峻形势,党的十八届四中全会提出要加强互联网领域立法,完善网络安全保护法律法规,规范网络行为。2016年我国通过了《网络安全法》。2018年9月,《个人信息保护法》被列入十三届全国人大常委会立法规划的第一类项目,即条件比较成熟、任期内拟提请审议的法律草案。在互联网影响日益扩大的背景下,公民信息安全不仅关系到公民的切身利益,也关系到国家的经济安全和网络安全,因此,应加强对公民信息安全保护的研究。

一、网络条件下的公民信息安全保护简述

(一)公民信息的定义、特征和信息安全的法理基础

我国信息论专家钟义信认为,可以把信息定义为事物运动的状态和方式^[2]。我们可以把公民信息看作一切可以识别公民的数据、符号、特征等要素的总和,包括年龄、联系方式、身份证号码等,涉及公民的身心健康、家庭、职业等各方面。人们习惯上把公民信息称为个人信息,它具有如下特征:

1. 隐私性。个人信息与个人隐私具有密切的联系。大部分个人信息如健康、财产、私生活都可视为隐私权的内容,非经个人同意不得公开。个人信息通过累积可不断让个人的特征清晰化。

2. 经济性。个人信息具有一定的经济价值。俄罗斯、美国已经以立法的形式规定了“信息财产”。个人信息与经济利益有显而易见的关联。目前存在大量的倒买倒卖个人信息的行为,违法犯罪分子正是利用信息的信息性特征牟取非法利益。

3. 资源性。在信息时代,个人信息是做出分析决策的前提条件,是一种宝贵的资源,可以用来进行政府决策、科学研究、企业战略制定、社会调查等。例如,在公共服务领域,基础信息对掌握公共服务现状、提高公共服务水平都具有重要意义。

网络条件下的公民信息安全保护是对宪法公民基本权利的具体落实,涉及对公民人身权、财产权、隐私权等诸多权利的保护。在我国,宪法规定的“国家尊重和保障人权”是公民信息权存在的主要依据,而宪法“人格尊严”条款则提供了信息权的解释空间。信息安全体现着人性尊严与人格独立等基本权利的核心内容。综观国外宪法实践,虽然各国对个人信息保护的法律表述与实践各不相同,但将个人信息保护的权利基础确立为基本权利是必然趋势。

(二)网络条件下的公民信息安全保护的重要性

随着互联网的发展,以网络为载体的犯罪数量呈上升趋势。近年来我国已发生多

起侵犯公民信息安全的案件,涉案人数之多、手段之先进、案情之复杂,都是前所未有的。这类案件侵犯公民的财产权、人身权,甚至危及公民生命,对国家安全和社会稳定产生重大威胁。

另外,在信息时代到来之前,公民信息使用范围狭窄,仅限于某些特定领域(如刑事侦查、医疗、间谍等),也未引起人们足够的重视。进入信息时代以后,个人信息资源的使用领域日趋广泛,其资源性日益受到重视^[3]。违法犯罪分子正是看到了个人信息的巨大潜在利益,进行不法谋利。这就需要公民提高自我保护意识,主动防范信息犯罪。

网络是信息时代维护国家安全和社会稳定的重要阵地。依法保障公民信息安全对保障公民权利、维护安定团结的大好局面非常重要。

二、“互联网+”时代信息安全保护的的特殊性

“互联网+”作为一种崭新的经济发展形态,不是互联网和传统行业的简单相加,而是互联网与各行业的深度融合。在“互联网+”时代,网络技术飞速发展,信息处理、储存和检索技术以空前的速度提高,对个人信息潜在的侵犯风险不断增加。在此背景下,个人信息的保护显得尤为迫切。和普通意义上的公民信息安全相比,“互联网+”时代的公民信息安全有以下特点:

1. 复杂性。“互联网+”涉及社会各领域,由于不同行业的服务内容、形式千差万别,因此,存在多种多样的侵犯个人信息的情形,人们必须做充分的预案。例如,作为“互联网+旅游”的产物,公民经常通过网络预订酒店客房。酒店收集了住客的身份证、住址、行程等信息,如果疏于管理或被黑客攻破,这些信息就可能被大量倒卖。又如,作为“互联网+医疗”的产物,病人的疾病信息、就诊经历等隐私也可能成为信息侵权的对象。毫不夸张地说,互联网和每个行业的融合都会带来特定的信息保护问题。

2. 隐蔽性。现代信息技术使信息的处理与利用更为便捷,也使侵犯个人信息的行为变得更为隐蔽,个人信息很可能在当事人毫不知情的情况下被侵犯。例如,浙江省松阳县法院于2017年9月审理判决了一起特大侵犯公民个人信息案,超过7亿条公民信息遭泄露,8000余万条公民信息被贩卖。该案犯罪嫌疑人王某辉于2016年2月入侵某部委医疗服务信息系统,将该系统数据库内的部分公民个人信息导出,并进行贩卖^[4]。对于黑客的窃密行为,很多受害者竟浑然不觉。

3. 危险性。在“互联网+”时代,随着计算机和网络技术的发展,通过网络访问个人

数据更为便捷,侵犯公民信息的违法成本大大降低,这就增加了公民信息被滥用的潜在危险。公民在接受政府、金融、医疗、旅游、教育等机构服务的过程中,其信息被各相关单位、网站、APP等广泛占有,一旦缺乏严密保护,随时会处于“裸奔”状态。

三、公民信息安全法律保护的立法现状及存在问题

伴随着互联网的快速发展,我国加快了个人信息保护的立法步伐,初步形成了多层次的个人信息安全法律体系,由宪法、法律、行政法规、规章、司法解释、行业自律规则等构成。首先,宪法明确规定“公民个人尊严不容侵犯”,这是个人信息保护的基本依据。其次,2017年《民法总则》首次提出对个人信息权进行保护。《刑法修正案(七)》首次将侵害公民个人信息安全的行为定罪入刑,填补了刑法保护在这方面的空白。《网络安全法》作为网络安全的“基本法”,明确了政府部门、企业、社会组织和个人的网络安全权利、义务和责任,建立了国家网络安全的一系列基本制度。最后,我国还颁布实施了涉及公民个人信息保护的多部法律规范性文件,如《关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等。在立法取得成就的同时,还需重视公民信息保护的问题。

(一) 互联网立法内容不够完备

在目前的互联网立法中,一些重要概念尚不明确。例如,《网络安全法》第七十六条对网络安全的内涵进行了界定,但要想在实践中应用好这部法律,还需要明确网络安全的准确外延,这个问题是整部立法的核心所在^[5]。此外,我国互联网法律制度的可操作性有待加强。以《网络安全法》为例,整部法律中的鼓励性、支持性、促进性条款约占一半以上的篇幅,真正意义上具有法律规范逻辑结构(条件假设、行为模式、责任归结)性质的条款则占不到一半的比例,过于笼统和模糊,缺乏可操作性,难以为网络法律关系主体提供明确的、肯定的行为模式指引,也难以为司法机关直接适用,需要再次进行立法解释和司法解释^[6]。

另外,立法的“互联网+”特色不明显。“互联网+”意味着互联网与各行业的融合,这就需要制定大量的行业法律法规。如医疗行业、旅游行业、教育行业等的公民信息保护单行立法都需及时跟进。

(二) 互联网立法不成体系

近年来,我国加快了公民信息保护立法的步伐,但还远远跟不上时代需要。互联网法律缺少顶层设计及总体规划,立法零散不成体系。全国人民代表大会常务委员会执

法检查组曾指出:网络安全监管“九龙治水”的现象仍然存在,权责不清、各自为战、执法推诿、效率低下等问题尚未得到有效解决,法律赋予网信部门的统筹协调职能履行不够顺畅^[7]。由于立法部门和信息化部门之间的沟通尚不完善,法律的协调性缺乏,实践中经常出现同一行为处罚主体不同、处罚力度不一致的现象。

(三) 互联网立法层级偏低

目前,由全国人大及常委会通过的互联网立法主要有《网络安全法》《电子签名法》和《民法》《刑法》中的相关规则。除此以外,我国的互联网立法主要由规章或者规范性文件构成,带有明显的部门立法特征,法律效力较低。例如,中央在政策层面早已对信息安全等级保护制度有要求,但这个制度只是以部门规章的方式加以规定,使其权威性、严密性不足,重点不突出,信息基础设施与网络空间基本处于不设防状态^[8]。

(四) 互联网管理规定执行效果不够理想

目前互联网管理规定多以事前许可加事后处罚为主要形式,在实践中效果不理想。许多需要事前许可的领域(如互联网接入服务、内容服务的许可与备案等)未经许可的现象相当普遍。如果不改变现有管理方式,仅仅靠加强执法很难真正解决问题。事后处罚同样会在执行中遇到阻碍,行政管理的有效性无法保障^[9]。

四、网络条件下的公民个人信息保护立法的国际比较

目前世界上已有 50 多个国家和地区颁布了保护信息安全的法律。其中,比较有代表性的是美国的部门性立法模式和欧盟的统一集中立法模式。

美国采用分散立法和行业自律相结合的模式。一方面,美国采取分散立法的模式,通过制定各种单行法来规范和保护不同领域的个人信息资料。联邦和州制定隐私及安全保护的法律法规来维护公民的信息资料权利,包括《隐私权法》《电子通讯隐私法》《金融、隐私法法案》《公平信用报告法》等。还有一些法律是对特殊人群的信息资料权进行保护,如《儿童在线隐私权保护法案》保护的是 13 周岁以下儿童的个人信息资料权。另一方面,美国更注重采取行业自律模式,即通过网络从业者的自我约束来保护网络环境下的个人信息,作为对立法的补充。由于行业自律具有较强的针对性和灵活性,受到了从业者的普遍认同。行业自律主要分为三类:第一类是行业指引。许多行业联盟制定了适用于本行业的网上隐私保护准则。第二类是网络隐私认证。为便于网络用户识别,行业联盟授权达到其隐私规则的网络从业者张贴其隐私认证标志。第三类是技术保护模式。它为用户提供网络隐私保护的技术支撑。最常见的一种技术保护模式

依托于“个人隐私选择平台”,在该模式下个人能够自由选择是否提供本人信息。分散立法和行业自律这两种模式相辅相成,互为补充。

相比于美国,欧盟更注重用严密的法律规定来保护公民的信息权利,个人信息保护标准也更高。欧盟称“个人信息保护”为“数据保护”,1995年的《关于与个人数据处理相关的个人数据保护及此类数据自由流动的指令》系统地对个人数据的收集、使用、处理、转移等进行了规定。目前,欧盟在个人信息保护领域最新、最严的法律是《通用数据保护条例》(简称GDPR)。GDPR严格规定,企业在收集处理用户信息时需要事先征得同意,而且需要向用户明确说明隐私条款。GDPR对企业违法行为的惩处力度非常大,行为轻微的要罚款1 000万欧元或全年营业额的2%(取其最高值),行为严重的则要罚款2 000万欧元或全年营业额的4%(取其最高值)。如此严格的规定,迫使一部分企业因害怕承担巨额罚款而直接退出欧洲市场。GDPR规定的“自设计开始的隐私保护”原则、个人的“被遗忘权”制度等对我国立法具有借鉴意义。此外,欧洲各国也分别制定了相关法律来保护信息安全。例如,德国的《联邦资料保护法》、法国的《法国自由、档案、信息法》、英国的《数据保护法》等。

五、我国“互联网+”时代公民信息安全保护的设计方案

近年来,随着互联网的发展,公民的个人信息以互联网为载体,发生更频繁的交流往来,面临更多的被侵害风险。应对“互联网+”时代的要求,我们要不断完善个人信息保护立法,健全信息安全保障体系。

(一)法律层面

1. 加快个人信息保护立法进程

首先,在立法规划上,应把个人信息保护法纳入国家级立法规划,放在优先的位置,尽快制定专门法律。近年来,全国人大常委会委员、农工党中央专职副主席杨震等多位代表委员在全国“两会”上呼吁尽快制定个人信息保护法。目前,这部法律已被列入全国人大立法计划。笔者认为,个人信息保护法应包括以下内容:个人信息的概念、内容、保护原则,个人信息的搜集、储存、处理和利用的要求,管理部门职责,运营商职责、公民和社会组织职责,侵犯个人信息法律责任等。立法应体现公开搜集原则,对个人信息的搜集、储存、处理和利用进行公开。为防止个人信息泄露,要明确采集和存储个人信息的单位负有安全保护职责。要对云计算、大数据的使用权限进行限制。要加大对未成年人等特殊群体的信息保护。立法时还应增加涉及信息网络安全保障的相关内容^[10]。

其次,完善现有法律。例如,在完善修订《网络安全法》时,应进一步明确网络安全的外延范围,提高法律的技术含量和可操作性。同时,加快《网络安全法》的配套立法工作,结合“互联网+”各主要行业的特征,作出个人信息保护的具体规定。此外,要把对个人信息安全进行保护的观念贯彻到有关法律的修订过程中去。例如,立法机关在2005年制定《治安管理处罚法》之时,我国侵犯个人信息的现象还不严重,因此,该法对网络条件下的个人信息保护规定尚不完善。随着网络的快速发展,将来在修订《治安管理处罚法》时,应增设对侵犯个人信息违法行为的处罚,对违反行政法律法规、尚未触犯刑法的个人信息安全侵权行为视情节采取行政拘留、罚款、没收违法所得等处罚,以威慑违法分子。

最后,在公民信息保护法出台之前,可以本着循序渐进的原则,先着手制定某些急需的单行法。值得注意的是,公民信息安全管理是全国一盘棋,应以法律、行政法规为主,以确保统一性、权威性。行政规章如确属必要,可由主管部门颁布,总量要适当控制且不得违反上位法,以确保法制统一原则的实现。

2. 进一步明确个人信息权的概念和法律地位

个人信息的立法保护虽不局限于民事立法,但两大法系都把个人信息权利作为基本的民事权利纳入民法的体系中。大陆法系把人格权、英美法系把隐私权作为个人信息保护的基础。鉴于个人信息权利的重要性,将其界定为一项独立的民事权利的意义体现在:能使其受到尊重和保护,能给受害人提供直接的法律救济,能为其他法律保护提供依据,能和其他保护机制相互补充和衔接,全方位地保护个人信息。我国2017年通过的《民法总则》首次从民事基本法层面提出个人信息权,并明确了个人信息保护的基本规范,是立法的重大进步。但是,我国个人信息保护立法还不完善,主要体现为个人信息法律边界不够明确、制裁措施不够具体等。今后应当进一步明确个人信息权的概念和具体规则,巩固个人信息权利的法律地位。

3. 明确公民个人信息犯罪主体的范围和处罚规则

从社会危害性来看,个人信息犯罪比一般的个人信息违法行为后果更严重,因此必须加强相关刑事立法。《刑法修正案(七)》增设了出售、非法提供公民个人信息罪、非法获取公民信息罪等罪名,是立法的进步。我国《刑法》第二百五十三条之一根据侵犯公民个人信息行为的情节严重程度,分别设立了“情节严重”和“情节特别严重”两档法定刑,并确立了对特殊主体的从重处罚原则。但同时也存在缺憾,如公民个人信息的概念不够完善,个人信息犯罪主体的范围不够明确具体,同时缺少针对不同的犯罪情节的具体量刑规定。《刑法》第二百五十三条之一未明确规定“情节严重”和“情节特别严重”

的具体认定标准,有可能导致司法实践中产生适用标准不一或者“同罪不同罚”的现象。这个缺憾已随着2017年5月9日发布的《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》(下称《解释》)的出台得到弥补,该《解释》对侵犯公民个人信息犯罪的定罪量刑标准和有关法律适用作了规定,在实践中发挥了积极作用。

近年来,我国加大了对侵犯公民信息违法犯罪行为的打击力度。以浙江松阳特大侵犯公民个人信息案为例:2016年,浙江松阳县警方成功破获多起以“猜猜我是谁”的方式冒充单位领导实施诈骗的案件,抓获11名犯罪嫌疑人,现场缴获用于实施诈骗的全国各地公民个人信息16.7万条,涉案金额117万余元。法院审理查明,用于违法犯罪的数据库是由被告人王某辉等提供的。王某辉于2016年2月入侵某部委医疗服务信息系统,将该系统数据库内的部分公民个人信息导出并进行贩卖^[4]。对王某辉等的定罪量刑是如何掌握的呢?根据《解释》规定的“情节严重”和“情节特别严重”的具体标准,王某辉的行为符合第五条所列举的造成重大经济损失或者恶劣社会影响的,数量或者数额达到“非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五百条以上;非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五千条以上的;非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五万条以上”,应认定为“情节特别严重”,根据刑法第二百五十三条之一,应判处三年以上七年以下有期徒刑,因此法院以侵犯公民个人信息罪处王某辉等有期徒刑三年四个月到五年不等,并处罚金六万元到四十万元不等。

同样的道理,在2017年7月19日山东省临沂市中级人民法院对“徐玉玉被电信诈骗案”的审判中,对被告人陈文辉的主要定罪量刑的根据为:第一,根据刑法规定,诈骗公私财物,数额特别巨大或者有其他特别严重情节的,处十年以上有期徒刑或者无期徒刑,并处罚金或者没收财产。陈文辉以诈骗罪被判处无期徒刑。第二,根据该《解释》的规定,被告人陈文辉非法购买高考学生信息十余万条,用于实施电信诈骗犯罪,属于法律规定的“情节特别严重”情形,依法应处三年以上七年以下有期徒刑,并处罚金。根据陈文辉犯罪事实及情节,法院依法以侵犯公民个人信息罪,判处陈文辉有期徒刑五年,并处罚金三万元。对陈文辉的诈骗罪、侵犯公民个人信息罪数罪并罚,执行无期徒刑,剥夺政治权利终身,并处没收个人全部财产^[11]。

由以上案例可见,《解释》因提供了具体量化标准,对侵犯个人信息犯罪的定罪量刑起了非常大的作用。随着“互联网+”时代的发展,在刑法中进一步细化处罚规则是必然趋势。

4. 立法、执法、司法部门形成合力

立法、执法、司法机关之间要协调合作,发挥合力,有效打击此类违法犯罪行为。立法机关要深入开展调研,提高立法的民主性和科学性。“无救济则无权利。”应明确规定公民因行政主体违法收集、处理和利用个人信息的行为而遭受损害的,有权提起行政诉讼,要求行政赔偿;应明确规定公民被他人或组织侵犯个人信息的,有权提起民事诉讼甚至刑事诉讼。公安机关和网络信息监管部门要严格按法律和相关规定处理侵犯公民信息的违法分子。一旦发生严重侵犯个人信息的事件,监管部门应立即启动协调和处理机制,加大责任追究力度。当个人信息泄露时,互联网运营商应立即报告监管机关并积极配合调查;电信管理机构可依法处以警告和罚款、责令侵害方赔礼道歉、赔偿损失、甚至停业整顿;监管机关应建立服务争议的通报渠道与研判机制、应急处理机制,通过日常监测与协调处理机制及时解决相关争议。法院及检察院要秉承公平公正的原则,追究公民信息侵权行为的法律责任。对侵犯个人信息的犯罪行为,必须加大惩治力度。建议在现有刑罚的基础上适当提高针对性质特别恶劣、社会危害性特别大的信息犯罪行为的刑期设定,以达到威慑效果。

(二) 管理与技术层面

“互联网+”时代对信息安全的管理与技术提出了比以往更高的要求。为了让立法落到实处,必须建立和完善相关的配套制度。

1. 加强互联网行业自律

保护个人信息需要自律和他律双管齐下。在加强立法规制的同时,要加强行业自律。应鼓励民间组织建立行业联盟,加强自我约束,同时加强网络道德建设,净化网络环境。另外,可以设立专门机构,指导行业自律,形成政府机关与行业联盟的良好互动。可以借鉴国外隐私权标志认证的做法,提升行业自律的效果。

2. 发展保护个人信息的技术

技术可以为保护个人信息提供有效的服务。用户可以通过安装反病毒程序、还原硬盘等办法保护个人信息安全,还可以通过选择平台、加密技术、使用相关软件等维护其个人资料。网络运营商作为公民信息资料的存储者,应向消费者明确其收集、使用用户信息的情况,让消费者有足够的知情权和选择权,同时要积极改进信息保护技术。国家应加大扶持力度,鼓励科研机构参与技术研发,提高信息保护的水平。由于依靠技术改进并非一劳永逸,因此要做到多管齐下,全面保护个人信息。

3. 加强普法宣传教育和国际合作

有关部门应当加强公民信息安全普法教育宣传力度,大力普及信息安全法律知识。

要教育网络用户不要受利益驱使而泄露个人资料,提高用户保护信息的警惕性和自觉性。此外,要在用户中普及技术手段,引导他们通过合法加密、匿名参与网络活动等方式来保护自己的信息。一旦个人信息资料泄露,要能主动运用法律来保护自己。同时,应积极参与公民信息安全保护的国际合作,吸收和借鉴发达国家和地区信息立法与管理的经验,促进我国的公民信息安全保护。

美国太阳计算机公司首席执行官 Scott McNealy 曾在 1999 年惊呼:“隐私已死!”今天,我们终于深刻地体会到其中的含义^[12]。我们期待个人信息保护法早日出台,我们也相信,“互联网+”时代我国完善的公民个人信息保护法律体系一定能尽快形成!

参考文献:

- [1] 中国互联网络信息中心. 第 43 次《中国互联网络发展状况统计报告》[EB/OL]. [2019-02-28]. http://www.cnnic.net.cn/hlwfzyj/hlwzxbg/hlwjtjbg/201902/t20190228_70645.htm.
- [2] 马建峰,沈玉龙. 信息安全[M]. 西安:西安电子科技大学出版社,2013.
- [3] 徐漪,沈建峰. 个人信息的属性及立法保护的原则[J]. 产业与科技论坛,2011(6):46-48.
- [4] 浙江松阳判决一起特大侵犯公民信息案 逾 7 亿条个人信息遭泄露[N]. 法制日报,2017-09-13(08).
- [5] 蓝蓝. 当前网络安全立法工作的三个重点[J]. 网信军民融合,2018(10):30-31.
- [6] 黄志荣. 中国互联网立法研究[D]. 北京:中共中央党校,2017.
- [7] 刘金瑞.《网络安全法》实施一周年配套立法的回顾与展望[J]. 中国信息安全,2018(7):61-62.
- [8] 中国没有网络战部队 网络空间基本不设防[EB/OL]. [2019-03-02]. <http://news.sina.com.cn/c/2014-03-02/044029599472.shtml>.
- [9] 万静. 互联网法律碎片化严重多以规章形式出现,专家建议应对互联网法进行顶层设计[N]. 法制日报,2015-07-23(06).
- [10] 63.4% 个人网上活动信息曾被泄露[N]. 法制日报,2015-11-10(03).
- [11] 徐玉玉案主犯为何被判无期徒刑? 法院详解[EB/OL]. [2019-03-19]. <http://china.huanqiu.com/article/2017-07/11002182.html?agt=15438>.
- [12] 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.

(责任编辑:楼启炜)