

【法学研究】

大数据时代金融信息保护的法律制度建构

刘 斌

摘 要: 大数据技术在提高信息获取能力、降低信息处理成本的同时,也使信息安全面临严峻形势。我国缺乏完善的个人信息保护立法,金融信息保护的规范依据不足。实践中金融机构往往通过格式条款进行免责,相关行政监管措施缺失,金融信息受害人举证困难。金融信息是个人信息权的保护对象,立法上可以从合同法路径和侵权法路径对其加强保护,并将其保护范围作为一个框架性概念,保持开放性。为了加强金融信息保护,我国应当建立个人信息保护法与金融信息保护法规相辅相成的法律体系,明确将金融机构和相关组织纳入义务主体的范围,规定金融信息保护义务的内容,设置举证责任倒置制度,严格限制格式条款的免责效力,强化金融信息保护监管。

关键词: 大数据; 金融信息; 个人信息权; 安全保护义务

中图分类号: D923

文献标识码: A

文章编号: 1003 - 0751(2015) 03 - 0054 - 06

随着大数据时代的来临,金融信息安全问题日益凸显。由于采用大数据技术进行信息存储和处理的成本非常低廉,所以金融机构保存着越来越多的信息,并且有能力通过大数据分析处理获得更多二次信息。大数据技术的运用,也带来了诸多风险。实践中,银行等金融机构经常忽视客户利益,未能尽到妥善的金融信息安全保护义务,导致利用金融信息非法牟利案件频繁发生,公开贩卖客户金融信息的恶性事件不时见诸报端,甚至形成了售卖客户信息、盗取客户资金的非法利益链。有鉴于此,本文在剖析我国金融信息保护法律制度缺陷的基础上,廓清构建金融信息保护制度的基本理论,提出完善我国金融信息保护法律制度的路径和措施。

一、我国金融信息保护面临的困境

针对我国频繁出现的金融信息安全问题,相关监管部门出台了规范性文件予以应对。2005 年,中国人民银行出台了《个人信用信息基础数据库管理暂行办法》,对个人信用信息的报送、整理、查询、异议处理等作了规定。2012 年国务院通过了《征信业

管理条例》,规定了征信机构的设立条件、业务规则和监管规则。这两个规范性文件主要涉及征信信息,尚未扩及个人的全部金融信息。为了加强个人金融信息保护,中国人民银行分别于 2011 年、2012 年发布了《关于银行业金融机构做好个人金融信息保护工作的通知》和《关于银行业金融机构进一步做好客户个人金融信息保护工作的通知》,对个人金融信息进行了列举式界定,并且对金融机构的金融信息保护行为作了比较具体的列举。此外,我国《反洗钱法》、国务院颁布的《个人存款账户实名制规定》、中国人民银行与中国银行业监督管理委员会等部门联合发布的《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》、中国人民银行发布的《银行卡业务管理办法》等法律、法规、规章中,也对金融信息保护有零星规定。目前我国在立法上并未形成金融信息保护规则体系,现有规则缺乏系统性,效力层次较低,未能在法律层面解决金融机构的信息安全保护义务问题及其伴随的损害赔偿问题。由于立法缺失,目前我国金融信息保护面临以下困境。

收稿日期: 2015 - 01 - 07

作者简介: 刘斌,男,河南财经政法大学民商经济法学院讲师,法学博士(郑州 450002)。

1. 金融信息保护的规范依据不足

我国目前没有一部完整的个人信息保护法,基本立法的缺失造成以下问题:(1)金融信息的内容和范围不清。我国《商业银行法》第73条的保护对象是存款信息,《反洗钱法》第5条的保护对象是金融机构基于反洗钱义务而获得的客户身份资料和交易信息,《征信业管理条例》和《个人信息信息基础数据库管理暂行办法》主要保护个人信用和征信信息安全,这些不同层级的立法并未形成统一的金融信息权概念。(2)金融信息安全保护义务方面的规范不足。前述法律、法规和规章对金融信息保护主体的界定主要局限于金融机构,未能涵盖与金融信息有关联的其他主体;对于不履行金融信息保护的法律责任的规定,基本上停留在谈话、整改、通报、处分等行政手段上,缺乏明确的民事救济措施。

2. 缺乏有效的行政监管措施

对于侵犯金融信息的行为,除课以民事责任、刑事责任外,加强行政监管也是有效的规制措施。我国现行立法中,金融信息保护行政监管措施主要存在两方面问题。(1)监管部门的职权零散,不能对侵害金融信息的行为形成全面约束。根据我国《反洗钱法》《商业银行法》以及中国人民银行出台的规章,金融监管部门仅有权对侵害反洗钱信息、存款信息、征信信息的行为进行处罚,而无权规制其他侵害行为。(2)监管部门的职权较小,约束力弱,难以实现有效监管。我国《商业银行法》第73条规定了国务院银行业监督管理机构对商业银行非法查询、冻结、扣划个人或单位存款的行为的执法权,《反洗钱法》第32条规定了反洗钱行政主管部门对金融机构违反保密规定,泄露有关信息的行为的执法权,这两部法律的保护范围都十分有限,行政主管部门对金融信息保护并无全面的执法权。中国人民银行出台的规章效力层次低,所规定的监管措施基本上停留在谈话、通报层面,不能形成实质性约束。

3. 有关金融信息的格式合同泛滥

客户到金融机构办理业务时,经常遭遇金融机构单方提供的格式合同。在这些合同中,金融机构往往设定各种各样的条款为自己免责,这些条款对客户而言则构成金融信息保护障碍。如《中国银行股份有限公司信用卡领用合约(个人卡)》第1条规定,信用卡的申请人或持卡人同意银行向第三方了解或者披露客户的财产及资信等状况,无论申请成

功与否,银行均保留相关资料而不予退回。在客户主张金融信息保护以及请求法律救济时,金融机构往往援引此类条款予以免责,这不利于客户的金融信息权利保护。

4. 金融信息受害人举证困难

在我国,对于严重侵害个人金融信息的行为,可以按照《刑法》第253条规定的“出售、非法提供公民个人信息罪”予以处罚。然而多数情况下,金融信息受害人是通过主张民事权利而获得救济的。根据我国《民事诉讼法》第64条及相关司法解释的规定,金融信息受害人负有证明自己主张的举证责任。但实践中金融信息的非法出售和泄露行为具有很大的隐蔽性,这些行为在损害后果发生之前很难为受害人所知晓;即使在损害发生之后,受害人也很难证明侵害行为与损害后果之间存在因果关系。举证困难已经成为金融信息受害者维权的主要障碍。

二、构建金融信息保护制度的法理逻辑

构建金融信息保护制度面临权利基础和权利保护路径两方面问题。就前者而言,金融信息作为信息享有者的一种利益,尚未形成一种法律上的权利。有学者提出将金融信息纳入隐私权范畴加以保护,然而传统法律理论对隐私权有着严格界定,将金融信息纳入其中会对隐私权和金融信息两个概念都造成冲击。因此,如何界定金融信息保护的权利基础,是构建金融信息保护制度的首要问题。就后者而言,由于民法上存在侵权法与合同法的分野,所以通过合同法抑或侵权法来构建金融信息保护民事规则,就成了构建金融信息保护制度的基础性问题。

1. 金融信息保护的权利基础与相关法律规范

金融信息保护面临权利归类问题。在金融信息保护问题凸显初期,由于立法中并未预设金融信息权的概念,所以司法实践中多借助隐私权对金融信息进行保护。但是,传统立法中的隐私权范围比较狭窄,难以满足大数据时代的需求。传统意义上的隐私多通过不同的方式被泄露或获取,而在大数据时代,通过对原始信息的分析处理就可以推导出过去、现在甚至将来的相关信息。譬如,通过对转账的时间、数额、对象等信息进行大数据分析,可以得出客户的基本商业往来关系和社会交往范围。近年来,经合组织、欧盟和美国纷纷启动隐私权保护框架改革,在其中纳入网络隐私方面的内容。^①虽然个人

信息与个人隐私在内容上存在一定的重合,但整体而言,个人信息的范围远远超出隐私信息,因而在法律上应当区分个人信息权与隐私权。^②为了保证人格权立法的开放性和可操作性,我国立法对个人信息权进行详细列举更有利于对其进行保护。我国个人信息保护立法已经开始酝酿,另行制定金融信息保护法无异于叠床架屋,也将造成立法资源的浪费。当然,作为一般法,个人信息保护法并不能完全解决金融信息保护问题。金融信息保护除需借助个人信息保护法之外,还需要相应的行政法规,搭建起民事责任和刑事责任之外的行政责任体系。

2. 金融信息保护的路径

在理论上,金融信息保护可以采取合同法路径或侵权法路径。前者是指使金融机构基于明示或默示的合同关系而负担信息保护义务,若违反合同义务,则构成违约责任;后者是指在侵权法上使金融机构对金融信息负担安全保护义务,不履行此项义务者,构成对隐私权或信息权的侵害。合同法路径在逻辑上存在的问题是:(1)金融信息收集者在收集信息时对信息分析能产生何种结果并不总是知情,因而在事实上缺乏与他人合意实施金融信息侵权行为的基础。在很多情况下,大数据分析所产生的结果是超乎预料的,即使数据收集者事先向被收集方告知了相关信息,数据分析的结果也仍然可能超出告知范围。譬如,在美国一个判例中,被告通过对移动电话基站收集到的为期 60 天的数据进行分析,得出了每个通话者的具体位置。^③但是,其收集数据的目的仅在于记录通话时间等信息,在进行大数据处理之前,其并不知道能得出通话者的位置,此类二次数据的获得在逻辑上并无基于合意的可能。(2)契约能够解决存在明示或默示合同关系的当事人之间的纠纷,但对于与合同没有直接关联的其他主体缺乏约束力。譬如,金融大数据的收集方或者通过提供方的同意、授权而以正当的方式获取信息,或者以未获同意的其他方式获取信息,之后可能将信息交由第三方分析处理,最后交由第四方使用。即使数据收集方与提供方达成了某种合意,这种合意也不能对后续的数据处理者、使用者等主体构成约束。不过,契约理论并非毫无意义。若征得信息主体的同意,金融信息的来源就具备了合法性基础。

与合同法路径相比,侵权法路径面临的主要问题是,我国目前并无法定的个人信息权概念,个人信

息权保护缺乏实定的请求权基础。我国《侵权责任法》第 6 条第 1 款明确规定,侵权责任的构成是基于行为人有过错地侵害了他人的民事权益。依此,侵权法路径面临的问题是,侵犯金融信息安全者究竟违犯了何种法定义务或者侵害了何种权利。为了更好地保护金融信息安全,我国应当通过立法明确规定个人信息权以及不同主体的金融信息安全保护义务。在界定金融信息安全保护义务时,不能将侵权法路径与契约法路径相互替代,而应当设立一项概括的安全保护义务,作为民法上安全保障义务在金融法领域的延伸,以确保违犯该义务的不当行为得以制止,所生损害得以救济。

3. 金融信息保护的内容与范围

大数据时代金融信息的内容非常广泛,不但包括姓名、住址、年龄、工作单位、联系方式、亲属等基本信息,而且包括收入情况、交易对象、交易金额、交易地点等特定信息。除了这些原始信息,通过对收集到的金融大数据进行分析,还能得出大量二次信息。需要指出的是,通过大数据运算所得到的个人信息,在法律上的保护价值与原始信息并无二致,甚至由于其信息指向性明确而更加需要法律保护。在对金融信息进行界定时,不应局限于数据本身,而应综合考虑数据的产生、转换、使用、传输、储存、加密、解密、销毁等过程。在这一系列过程中,金融信息经历了不同形态的衍化,归于不同主体的管控之下,发挥着不同形式的功能。因此,金融信息在内容上应当包括两部分,一部分是通过各种方式收集到的原始信息,另一部分是通过原始信息进行分析运算而得出的二次信息。

三、我国金融信息保护的法律制度完善

为了加强个人信息保护,欧盟和美国、日本等国都制定了完善的个人信息保护法律。欧盟在 1995 年就通过了《关于涉及个人数据处理的个人保护以及此类数据自由流动的指令》,之后又通过了《关于在信息高速公路上收集和传递个人数据的保护指令》《关于与欧共体机构和组织的个人数据处理相关的个人保护以及关于此种数据自由流动的规章》等一系列法律,构建起比较完善的数据保护制度体系。与欧盟的统一立法模式相比,美国的个人信息立法呈现出多元化趋势。除了 1974 年《美国隐私法案》,联邦和各州还就具体类型的个人信息进行了

分别立法,构建起美国特色的分散立法模式。在金融法领域,美国制定了与个人信息保护相关的《公平信用报告法》《金融隐私权法》《金融服务现代化法案》等法律,消费者隐私权法案也在制定之中。借鉴国外立法经验,我国应当尽快制定统一的个人信息保护法,奠定个人信息保护的一般法基础,同时制定金融信息保护法规,采取一般法与特别法相辅相成的金融信息安全保护立法模式,构建起完整的金融信息保护制度体系。

1. 明确金融信息安全保护义务主体

金融大数据的使用者包括金融机构、金融中介组织、销售商、社会媒介、技术供应商、市场管理部门等,将金融信息保护义务局限于金融机构并不能起到良好的保护效果。这一点已为域外立法例所认可。如美国《联邦交易委员会法案》第5条对所有行业(而不局限于商业机构)都施加了数据安全保护义务。我国立法应当对负担金融信息安全保护义务的主体作扩展性规定,不停留于某一个或者某些机构,而是包括金融大数据所可能涉及的多元主体,使所有数据使用者都为自己的行为承担责任。

第一,金融机构应当对客户的金融信息负担最主要的安全保护义务。金融机构是金融大数据产生的载体和存续的直接媒介,其对金融大数据进行收集、处理的过程中,能够获得大量有利于开展金融业务、扩大市场范围、增加营业利润的信息。如果金融机构不负担金融信息安全保护义务,将导致风险与收益的偏离。并且,金融机构作为营利商人,应当承担企业社会责任。注重对客户信息的保护,不仅是金融机构长远营利的需要,也是其承担最基本的企业社会责任的要求,是其遵行诚实信用原则的体现。此外,金融机构处于控制风险的最有利地位,其最有能力控制金融信息风险。金融大数据置于金融机构管理、控制之后,信息提供方实际上已经丧失了对其进行保护的能力,技术提供商、金融中介组织、社会媒体等也往往是通过与金融机构之间的合同安排而接触和使用金融大数据的。

第二,除了金融机构,大数据技术提供商、金融管理部门和其他接触到金融大数据的主体也应当承担金融信息安全保护义务。(1) 金融机构往往并不具备数据处理专长,在多数情况下大数据技术服务是由技术提供商外包进行的,客户信息因而存在被技术提供商泄露的风险。由于金融客户与技术供应

商之间缺乏直接的合同,所以被泄露数据的当事人并不能基于合同而获得救济。因此,法律应当明确规定技术提供商的数据安全保护义务。(2) 国家公权力机构在对大量金融信息进行管理的同时,可能会出于故意或过失而造成金融信息的泄露,从而对相关利益主体造成损害。因此,金融管理部门应当对其收集和使用的金融大数据负担安全保护义务。(3) 在大数据市场交易中,市场主体可以通过不同的方式获取或占有客户金融信息。对于这些接触到金融大数据的市场主体,同样应当课以金融信息安全保护义务,以防范其对客户信息造成侵害。

2. 明确金融信息安全保护义务的内容

目前,金融机构加强大数据保护的依据其实是管理部门对其设定的技术标准。如2006年中国人民银行发文对进一步加强银行业金融机构信息安全保障工作进行指导,要求银行业金融机构加强信息安全队伍和基础设施建设等。但是,仅仅提出技术规范上的要求是不够的,还应当在立法上明确金融信息安全保护义务的具体内容,将履行法律义务作为信息安全管理合乎技术规范的判断标准和裁判依据。金融信息安全保护义务是一个开放性的概念,其包括但不限于以下内容。

第一,合法收集信息的义务。金融大数据的收集对信息主体而言往往是被动的,有些人甚至是在完全不知情的情况下,其个人账单、信用情况、交易记录、资产负债等信息被金融机构作为收集、分析对象。通过对大量数据的比对分析,金融机构对客户金融信息的了解甚至超乎客户自身。立法应当明确规定,金融机构违犯法律规定或者违背客户意志收集金融信息,构成对客户权利的侵犯。合法收集信息义务的主要内容,包括原始收集者的合法收集义务和第三方的合法收集义务,前者是指原始收集者对金融信息的收集不能违犯法律规定,也不能违背客户意愿,如客户使用加密措施来防止信息被跟踪后,网站就不能突破这种措施而收集客户信息;后者是指原始收集者意欲将数据信息与第三方共享时,相关行为应当合法且合乎客户意愿。

第二,告知或说明义务。告知或说明义务是金融机构获取金融信息的正当性基础,是客户知情权的要求。如美国1999年《金融现代化法》要求提供金融服务或产品的企业将信息收集和使用情况告知消费者,金融企业有义务向消费者解释信息收集方

式、使用方式和保护方式。有学者提出,在大数据时代,由于数据的价值很大一部分体现在二级用途上,而收集者在收集数据时并未作二次使用的考虑,所以告知与许可义务不能再起到很好的作用了。^④笔者认为,在大数据时代,告知或说明义务仍然是保护金融信息安全的一个重要措施。法律应当要求金融机构明确告知客户其收集数据的目的和用途,并且规定履行告知或说明义务不能成为免责事由。

第三,妥善管理的义务。金融机构能否妥善管理客户信息和数据,关系到客户的信息安全。美国《公平信用报告法》对涉及信用状况、保险、医疗、租赁等内容的数据的收集、披露和使用进行了严格规制。在我国,大数据技术起步较晚,金融机构对金融信息的重视程度较差,往往不能与金融资产相比。正是由于重视不够,导致金融机构收集到的金融信息存在不同程度的外泄问题。鉴于此,我国应当通过立法要求金融机构对金融信息采取适当的数据保密措施,如进行加密处理、数据脱敏等。对于外来风险,金融机构应当完善防火墙等技术措施加以防范。金融机构未尽妥善管理义务而导致金融信息外泄的,应当承担相应的法律责任。

第四,风险识别义务。大数据技术会带来信息风险,其也可以帮助金融机构发现和防治金融欺诈。通过分析客户的资金流动数据和消费状况,金融机构能够发现那些偏离既有模式的资金变动情况,进而对有问题交易采取风险防范措施。譬如,基于交易记录,金融机构如果发现某客户在同一时间分别在北京和纽约有两次刷卡消费记录,便可推测存在信用卡盗刷问题,据此可提示客户相关交易风险并及时采取防范措施。风险识别功能是大数据技术的积极效用之一,法律应当对使用大数据技术的金融机构施加风险识别义务。

第五,隐私保护义务。我国未来立法应当明确规定,金融机构对于金融大数据中涉及客户非公开信息的内容,应当予以保护,不得擅自泄露给第三方或者公众。除对既有信息进行保护外,基于大数据的预测而产生的信息同样属于金融机构隐私保护义务的内容。因为此类信息虽然并非数据收集者所直接获取,但如果收集者擅自将其披露,势必对个人隐私权造成极大破坏。并且,此类信息属于预测性隐私,不属于传统法上的隐私权保护范围。^⑤

第六,及时删除的义务。信息获得者和使用者

的及时删除义务,对应于信息提供者的“被遗忘权”。传统理论和立法将这项权利归入隐私权范畴,但在大数据时代,将其作为个人信息权的一部分进行保护更为恰当。我国立法应当明确规定,已经失去占有正当性的金融信息,相关主体应当及时予以删除,而不能永久占有、使用。

3. 明确金融信息侵权行为的民事责任

我国没有统一的个人信息保护法,在发生金融信息侵权纠纷后,当事人只能寻求侵权法上的一般救济。司法实践中金融信息受害者多数情况下只能得到停止侵害、消除影响等名誉性补偿,经济赔偿和精神损害赔偿方面的请求往往得不到司法机关支持。我国应当提高侵犯金融信息行为的违法成本,在个人信息保护法中明确规定侵犯个人信息者对其行为所生损害的经济赔偿责任,在造成受害人精神痛苦的情况下,还应进行精神损害赔偿。

4. 设置举证责任倒置制度

举证困难以及高昂的诉讼成本,已经成为金融信息受害者维权的极大障碍。从理论上讲,为了保护处于举证弱势地位的原告,可以实行举证责任倒置。我国《最高人民法院关于民事诉讼证据的若干规定》第4条规定了实行举证责任倒置的诉讼类型,包括新产品制造方法专利侵权诉讼、高危作业侵权诉讼、环境污染诉讼、建筑物致人损害诉讼等。但是,根据我国目前的立法和司法解释,举证责任倒置制度的效力范围尚未及于金融信息侵权案件。笔者认为,为了更好地满足大数据时代金融信息保护的需求,我国应当建立金融信息侵权诉讼的举证责任倒置制度。在金融信息侵权诉讼中,将相应的举证责任分配给被告(往往是金融机构和相关社会组织)不但契合金融信息保护的价值取向,而且符合有关证明责任分配的诉讼法理论。(1)就举证能力而言,较之金融消费者等信息权利主体,金融机构等组织对金融信息具有较强的占有和控制能力,其对金融行为比较了解,举证能力较强。(2)从证据法理论上讲,证明距离是进行举证责任分配的重要因素。^⑥在金融信息侵权案件中,较之金融消费者,金融机构等信息占有和使用者与待证事实之间的证明距离更近,而金融信息主体与侵害行为距离较远,难以承担相关证明责任。(3)就立法的价值取向而言,实行举证责任倒置是对当事人之间明显失衡的权利义务关系的再平衡,体现了对在财力、信息等方

面处于弱势地位的当事人的倾斜保护。在大数据时代,对金融信息侵权诉讼实行举证责任倒置制度,能够有效矫正金融消费者等信息主体与金融机构等信息占有、使用者之间的权利义务偏差。(4)就行为的可责性而言,金融信息泄露往往是金融信息占有、使用者没有(或不充分)履行信息安全保护义务的结果,在金融信息侵权诉讼中对其课以举证责任,有利于督促其将金融信息置于安全保护之下。

在针对金融信息侵权诉讼的举证责任倒置制度中,应当明确规定倒置的证明标准和证明事项。就证明标准而言,可以适用民事诉讼的盖然性标准,而不苛求金融机构等组织所提供的证据达到足以排除合理怀疑的高度。根据《最高人民法院关于民事诉讼证据的若干规定》第73条关于盖然性标准的规定,在金融信息侵权案件中,只要金融机构等组织提供的证据超出对方证据的证明程度,就认为其尽到了举证责任。就证明事项而言,金融信息侵权诉讼中并不是要求金融机构等组织承担全部待证事实的证明责任。在侵权行为、损害后果、侵权行为与损害后果之间的因果关系、主观过错这四项待证事实中,金融消费者等信息主体对损害后果更有举证便利和优势,而对其他三项的举证能力较弱,因而在举证责任分配上,金融信息主体应当就损害后果及其与金融机构交易所涉事实等承担证明责任,金融机构等组织应当就其并无侵权行为和主观过错,以及其行为与损害后果之间不存在因果关系承担证明责任。

5. 严格限制格式合同免责条款的效力

从合同法理论上讲,免责条款的运用是有悖合同法原则的,应当受到严格限制。原因在于:(1)免责条款严重损害了契约自由原则。意思自治是合同法的生命,一方通过设定格式条款进行免责,严重限制了交易对方选择合同内容的自由,无法体现合同主体的真实意思。(2)免责条款严重损害了契约公平原则。交易主体的平等性是合同公平的基础,免除单方责任的格式条款不仅损害了合同的公平性,对公共利益而言也是一种损害。我国立法关于格式合同免责条款的规定主要是《合同法》第39条、第40条、第53条以及《消费者权益保护法》第26条。《合同法》第39条第1款规定提供格式条款一方应当遵循公平原则确定当事人之间的权利和义务,并履行提请对方注意以及说明免责条款内容的义务;第40条、第53条规定了免责条款无效的情形,其中

第53条第2款“因故意或重大过失造成对方财产损失的”,可以适用于金融机构等组织提供的格式合同。在特别法上,我国《消费者权益保护法》第26条明确规定,经营者不得以格式条款等方式作出排除或限制消费者权利、减轻或免除经营者责任、加重消费者责任等对消费者不公平、不合理的限定。《消费者权益保护法》是《合同法》的特别法,其法条应当优先于《合同法》的法条予以适用。我国应在个人信息保护法中明确规定,即使金融消费合同规定了金融消费者同意金融机构向第三方披露自己信息的条款,该条款也不能成为金融机构等组织免除其损害赔偿责任的事由。

6. 强化金融信息保护监管执法

我国应当通过个人信息立法,强化金融信息保护行政监管制度。(1)赋予金融管理部门全程监管权。应当设立金融信息相关合同的事先审查机制。对具有高度技术性的金融消费合同,由金融管理部门对其格式条款进行事先审查,以促进合同的公平性。同时,加强金融信息保护的事中、事后监管。监管部门要及时对金融机构的信息保护系统建设、运行情况及其实施信息保护制度的情况进行检查、监督,对违犯个人信息保护法律和金融信息保护法规的行为进行否定性评价或行政处罚。(2)强化金融管理部门的行政执法手段。我国个人信息保护法应当在保留现有执法措施的基础上,赋予行政主管部门警告、罚款、责令停产停业、暂扣许可证等更加有力的执法手段。此外,鉴于目前金融行业“一行三会”的多头管理模式,未来立法中应当明确各监管主体的权限,以避免监管执法冲突和执法混乱。

注释

- ①Omer Tene & Jules Polonetsky, Judged by the Tin Man: Individual Rights in the Age of Big Data, 11 J. on Telecomm. & High Tech. L. 351, 2013, p. 362. ②参见王利明《论个人信息权在人格权法中的地位》,《苏州大学学报》(哲学社会科学版)2012年第6期。③In re Application of the United States of America For Historical Cell Site Data, 724 F.3d 600, http://international.westlaw.com, 2015-03-04. ④参见[英]维克托·迈尔-舍恩伯格、[英]肯尼迪·库克耶《大数据时代》,浙江人民出版社2013年,第22页。⑤Kate Crawford & Jason Schultz, Big Data And Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 B. C. L. Rev. 93, 2014, p. 96. ⑥参见汤维建:《论民事诉讼中的举证责任倒置》,《法律适用》2002年第6期。

责任编辑:邓林