Doi:10. 11835/j. issn. 1008-5831. fx. 2021. 09. 001.

欢迎按以下格式引用:唐林,张玲玲. 个人信息泄露通知制度中自由裁量的规制研究[J]. 重庆大学学报(社会科学版),2022(3):219-229. Doi:10. 11835/j. issn. 1008-5831. fx. 2021. 09. 001.

Citation Format: TANG Lin, ZHANG Lingling. Research on discretion regulation in personal information breach notification system[J]. Journal of Chongqing University (Social Science Edition),2022(3):219-229. Doi:10. 11835/ j. issn. 1008-5831. fx. 2021. 09. 001.

个人信息泄露通知制度中自由裁量的规制研究

唐　林,张玲玲

(上海交通大学 法学院,上海　200030)

摘要:我国《个人信息保护法》第57条首次确立了个人信息泄露通知制度,规定了个人信息处理者在发生信息泄露后向有关部门与个人履行通知的义务。个人信息的泄露往往给个人信息主体带来持续性、衍生性的危害,涉及人身、财产安全以及精神损害等方面,故而及时有效的泄露通知能够更好地保护个人信息权益。在涉及履行个人信息泄露通知的义务上,处理者被赋予了一定的自由裁量空间,即采取措施能够有效避免相关危害的,可以不通知个人。基于此,该自由裁量主要存在两个挑战:一是损害了泄露通知引发的声誉制裁有效性,企业在预见到泄露通知带来的巨大商业风险与社会责任时,往往选择内部"消化"处理已经发生的泄露事件,破坏声誉制裁的运行机制;二是个人信息处理者与行政机关之间的信息不对称以及基于显性监管指标的"规制捕获",导致企业以最容易实现合法外观的方式来满足监管要求,降低合规成本。关于如何规制该制度的自由裁量空间以及如何构建监管部门与商业组织之间协调机制的讨论并未停止。妥当地规制"自由裁量"空间,是个人信息泄露通知制度有效运行的关键。通过借鉴欧美等国个人信息泄露通知制度中关于触发标准、阈值分布等方面令人瞩目的立法政策,基于行政法中第三方义务理论框架分析了企业声誉制裁体系及其正当性基础和自由裁量的适用条件;同时,从戴维斯提出的"结构化自由裁量"角度切入,提出我国个人信息泄露通知制度在细化完善方面应当注重自由裁量的常态化监督,持续性介入个人信息处理者在自由裁量方面的审核;在泄露通知方式上采取双层化处理,即原则上发现信息泄露应当立即通知监管机构,而对于个人信息主体的通知设定较高触发阈值;在显性监管指标方面进行协同性弱化,主要职责部门在收到自由裁量决定后与其他相关部门协同审查,弱化显性监管指标概念;在泄露通知有效性方面,强化通知的具体内容设计以及发送通知的方式,

基金项目:国家重点研究计划"全流程管控的精细化执行技术及装备研究"(2018YFC0830400)

作者简介:唐林,上海交通大学凯原法学院,人工智能治理与法律研究中心,Email: tonygilbert92@ sjtu. edu. cn;张玲玲,上海交通大学凯原法学院,Email: lawyerzhang@ sjtu. edu. cn。

致谢:北京师范大学法学院吴沈括教授对本文关于《个人信息保护法》研究予以精心指导,上海交通大学凯原法学院杨力教授为本文写作与修改提出宝贵意见,谨此致谢!

严格规范泄露通知所能包含内容的范围,禁止任何商业推广危害通知的可阅读性。

关键词:泄露通知;第三方义务;自由裁量;个人信息保护

中图分类号:D922.16 **文献标志码**:A **文章编号**:1008-5831(2022)03-0219-11

一、问题的提出

伴随着我国当下个人信息泄露事件的频发,个人信息保护引发社会各界广泛关注,成为网络空间法治建设的重要议题。2021年8月20日,全国人大常委会发布《中华人民共和国个人信息保护法》(以下简称"个保法"),其中第57条首次确立了我国个人信息泄露通知制度,明确了个人信息处理者在个人信息泄露后向有关部门与个人履行通知的义务①。本质上,个人信息泄露通知机制的主要目的在于保护公民免于受到由于个人信息泄露可能带来的持续性危害,包括但不限于身份冒用、财产损失、精神损害,以及社会生活中的其他负面影响②。个人信息泄露通知制度是我国个人信息法律保护之路上的里程碑事件,但在具体细节规定方面尚显不足,质言之,我国"个保法"第57条所构建的泄露通知制度主要面临两大挑战:其一,如何规制在个人信息泄露通知方面的自由裁量,激励信息处理者第一时间将信息泄露事件通知到职责部门与个人;其二,如何完善监管部门与商业组织的协调机制,打破监管职责部门与商业组织之间因在长期监管互动过程中形成的共识而造成流于形式的监管审查,以期最大程度地降低信息泄露后对于个人的持续性危害。

(一)自由裁量与声誉制裁之间的悖论

本质上,泄露通知制度主要通过对涉事个人信息处理者进行声誉打击、降低社会评价的方式来激励相关行业在个人信息保护上的治理与投入。声誉制裁的有效性就在于,无论是个人、企业还是其他社会组织,都较大程度受制于其自身先前行为的信息披露带来的社会影响[1]。在当下金融资本高度发达的社会中,尤其对于上市企业而言,信息泄露事件的曝光导致的声誉受损,可能会给其股价带来严重挫折[2],以及大量现有、潜在客户的快速流失[3]。而关键行业领域中的信息泄露,甚至会危害国家安全,影响社会稳定与发展[4]。"个保法"第57条第二款规定在"有效避免危害"的基础上,赋予个人信息处理者不予履行通知的自由裁量空间。一方面,对于以企业为代表的个人信息处理者来说,履行泄露通知意味着承担经济损失、潜在的商业诉讼以及政府的严格审查。由此,企业在被赋予自由裁量空间之后,预见到潜在的巨大商业风险与社会责任,往往选择在内部"消化"处理已经发生的信息泄露事件,且信息泄露事件本身往往牵扯到一系列企业组织,很难追溯信息泄露的源头[5]。发生在产业链下游企业的核心信息泄露传导到产业上游,继而引发更大规模的信息泄露事件。信息泄露的源头一旦保持沉默,信息泄露的压力最终全部由上游头部企业承担,以此形成恶性循环,严重挫伤企业履行泄露通知义务的积极性[4]。另一方面,声誉制裁的潜在理论假设是,商业组织是经济理性的,追求利润最大化,需要在信息安全建设投入与信息泄露通知带来的经济损

①我国《个人发信息保护法》第57条,"发生或者可能发生个人信息泄露、篡改、丢失的,个人信息处理者应当立即采取补救措施,并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项:(一)发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害;(二)个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施;(三)个人信息处理者的联系方式。个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的,个人信息处理者可以不通知个人;履行个人信息保护职责的部门认为可能造成危害的,有权要求个人信息处理者通知个人"。

②欧盟《通用数据保护条例》(General Data Protection Regulation), Recital 85.

失之间衡量成本与收益[6]。故而声誉制裁带来的负面影响越大,信息安全的投入也就需要相应的加强。但事实上,企业背后的决策者、管理者在谋求经济利润时的疯狂与短视常常颠覆了理性经济人的假设。一项涉及企业环境保护方面的社会调查统计表明,200 多家企业中合规部门负责人对于企业在环境污染方面将会面临的具体处罚一无所知,绝大多数是依靠粗略的估算和日常经验[7]。

(二)个人信息处理者自由裁量的监管困境

此外,面对信息泄露事件,个人信息处理者在作出不予通知个人的决定时,必然会在其组织内部形成一系列流程化制度,用来正当化“个保法”第 57 条第二款规定“采取措施能够有效避免信息泄露、篡改、丢失造成危害”的要求,以此应对行政机关的事后审查。尽管“个保法”第 57 条第二款同时也赋予了行政机关对于个人信息处理者自由裁量的最终决定权,但现实情况是,个人信息处理者往往掌控着大规模的信息存储基础设施、网络平台的实际运维等,涉及个人信息收集、存储、传输、使用、销毁等全生命流程[8]。相较于行政监管机关,个人信息处理者近乎处于知识、信息的绝对垄断地位。一方面,以互联网企业为代表的个人信息处理者利用信息不对称的优势以最容易实现合法外观的方式来满足行政监管,降低企业合规成本。表面上受监管的互联网企业作出的合规调整似乎优先考虑个人信息保护问题,但实际上对其内部工作方式没有什么改变;另一方面,迫于大型互联网企业的绝对影响力,行政机关的显性监管指标在长期监管互动的过程中,易被其“捕获”,即被吸收进企业的例行公事化信息,融入日常合规流程,最终造成浮于表面的形式化事后审查。

因此,本文拟从分析借鉴欧美等国个人信息泄露通知制度中关于触发标准、阈值分布等立法政策出发,同时结合我国行政法中第三方义务的自由裁量与声誉制裁,探讨我国个人信息泄露通知制度的完善和细化方案,以期促进我国网络空间法治建设的健康、有序发展。

二、欧美国家的泄露通知制度梳理与分析

(一)加州《数据安全泄露通知法》

加州的信息泄露通知制度源于 2002 年颁布的《数据安全泄露通知法》(Data Security Breach Notification Law)。该法案规定,在加州开展业务的个人或企业,如果拥有或被许可使用包括个人信息在内的未加密、计算机存储的信息,则在其发现信息泄露后,应向加州居民披露信息泄露的情况[9]。一般而言,加州的信息泄露通知阈值较低,其只要求客观上或有理由相信发生了个人信息泄露事件,那么拥有该信息的组织就必须向个人发出通知,并且没有任何内部协调机制来减少泄露事件发生后可能对个人带来的后续危害风险。且个人信息泄露带来的一个较为严重的危害就是身份盗窃,并可能因此造成巨大的经济损失。相较于个人信息泄露的事后补救,加州更多地强调企业履行泄露通知义务,以声誉制裁的方式迫使商业组织投入更多的资源用于信息安全的防护。此外,加州的泄露通知法案同时也针对一些特殊情况设置了泄露通知的替代性方案:当提供信息泄露通知到个人的成本高于 25 万美元时,或者遭遇信息泄露的群体数量超过 50 万人时,并且该组织缺乏相应的联系方式,则其有义务采取替代性通知方案[10]。替代性通知方案主要包含以下三种:其一,给个人信息遭遇泄露的用户发送电子邮件;其二,在其企业运营的官方网站上发布通知;其三,通知所在州内的新闻媒体[10]。替代性通知方案的主要问题在于其只是向社会提供泄露事件的宏观描述,用户无法知晓自己的个人信息是否被泄露。然而据统计,该法案导致总部设在加州,且使用的网络服务器软件保持更新到最近版本的公司只占 1.8%~2.8%。尽管加州的个人信息泄露通知法案近

年来受到了相当大的关注,但其对州内的企业在网络服务器安全方面的投资影响却收效甚微[11]。

(二)美国《机构间应急方案指南》

美国财政部货币监理署(Office of the Comptroller of the Currency,Treasury),美联储(Board of Governors of the Federal Reserve System),美国联邦存款保险公司(Federal Deposit Insurance Corporation)以及美国财政部储蓄机构管理局(Office of Thrift Supervision,Treasury)四大机构,依据 Gramm-Leach-Bliley Act 第 501 条,针对金融机构监管制定了《机构间应急方案指南》(以下简称"指南")[12]15736。相较于加州,该"指南"提供的信息泄露通知制度赋予了受监管的金融机构更多的自由裁量空间,但同时针对泄露通知的阈值采取两级分层机制:第一层低阈值要求,当机构发生了个人信息泄露事件,则应当通知到监管部门;第二层高阈值要求,仅当发现存在被泄露的个人信息有被滥用的可能性时,金融机构才须向个人发出通知[12]15736。该阈值分层制度的核心在于通过赋予金融机构在高阈值情况下的自由裁量权来化解信息过载的问题。正如"指南"在序言中表述到,监管机构不希望用户接收到对其毫无意义的泄露通知[12]15743。换言之,由金融机构来判断信息泄露事件是否触发高阈值,即存在相应的事实表明被泄露的个人信息存在被滥用可能性。否则只需要即时向监管机构告知信息泄露事件,无需承受潜在的声誉制裁。相比于加州强制通知模式,指南提供的制度方案在于通过赋予有条件的自由裁量权来平衡声誉制裁造成的寒蝉效应。

(三)欧盟《通用数据条例》

欧盟的泄露通知制度,首先在《电子隐私指令》(e-Privacy Directive)中确立,其后被《通用数据条例》(以下简称"条例")所修订取代③。条例第 33 条和第 34 条分别规定了面向监管机构的泄露通知与面向个人信息主体的泄露通知:在监管机构层面,个人信息控制者(controller)应当在知晓泄露事件(至迟在 72 小时之内)后向监管机构报告;在个人信息主体层面,当泄露事件很可能给自然人的权利和自由带来高风险时,个人信息控制者应当及时向个人信息主体发出泄露通知④。由此观之,欧盟采取了与美国的《机构间应急方案指南》同样的两级分层机制,二者之间判断标准只是存在表述上的差异,即欧盟的标准是"泄露事件给自然人的权利和自由带来高风险",而美国的标准是"被泄露的个人信息有被滥用的可能性",但本质上都是以泄露事件是否会给个人信息主体带来潜在的高风险伤害为判断依据。

三、基于第三方义务理论的泄露通知制度

(一)传统领域中企业声誉制裁体系及其影响

当下,我国针对企业的违法行为已经建立起以政府网站常态化公开,信用档案归集以及企业既往表现的负面标签化三位一体的声誉制裁体系[13]。一方面,公权力主体在执法过程中,依据《行政

③《电子隐私指令》(Directive 2009/136/EC)为欧洲议会和欧盟理事会关于对有关电子通讯网络通用服务和用户权利的 2002/22/EC 号指令,有关电子通讯方面的个人数据处理和隐私保护的 2002/58/EC 号指令,以及有关负责消费者保护法律执法方面的国家有关机构间合作的(EC) No. 2006/2004 号条例进行修订的指令。

④参见 General Data Protection Regulation, Article 33, Notification of a personal data breach to the supervisory authority; Article 34, Communication of a personal data breach to the data subject.

处罚法》《政府信息公开条例》以及《企业信息公示暂行条例》,需主动公开行政处罚等相关信息⑤;另一方面,通过企业信用信息公示系统、行业领域内的信用档案和国家公共信用信息平台形成完整的企业信用档案数据库,同时依据前述企业信用档案信息,以“经营异常目录”“严重违法失信企业名单”“失信联合惩戒对象名单”等负面标签方式,深化声誉制裁力度[14]。本质上,目前针对企业的声誉制裁体系是建立在政务信息公开、企业信息公示和社会信用体系基础之上的。由做出负面评价的公权力主体通过既有的社会信用信息平台,将企业的声誉信息广泛传播至相关市场领域及社会之中,这是理解声誉制裁运行机制的关键。根据信用风险分类监管理论,行使市场监督职能的行政主体、提供信贷的金融机构以及消费者群体对于企业的声誉信息有着极高的依赖性[15]。建立在企业信息公示、社会信用信息体系之上的企业声誉信息,直接反映了企业的合规风险和经营状态,从而能够促进市场的信息流通,以及社会公众对于交易稳定性的预期[16]。企业声誉制裁体系的负面影响在于制裁效果可能过重。负面标签等方式能够作为其他行政活动的直接依据,即只要企业被纳入负面标签序列,共享社会信用信息平台的所有相关政府部门都将对其采取相应的限制措施,没有任何的自由裁量余地。

(二)第三方义务模式下声誉制裁的正当性

“个保法”第57条规定的泄露通知制度,意在通过向职责部门与个人履行通知义务,从而实现对泄露信息的个人信息处理者进行声誉制裁。实质上,该泄露通知义务属于公法上的通知义务,即个人信息处理者以私主体的身份,对其收集、保有的个人信息承担泄露通知义务。从法律性质观之,该公法通知义务是行政法上的第三方义务,个人信息处理者作为私主体,以参与行政过程的方式履行法律强制要求的通知义务[17]。行政法中第三方义务的一个主要特征是违法行为人与该违法行为的责任主体是割裂的[18],即在泄露通知制度的语境下,非法获取个人信息的行为人与该违法行为的责任主体分离。换言之,第三方义务要求私权利主体参与到行政过程中扮演“守门人”的角色。按照“守门人”理论,衡量是否赋予私主体“守门人”的角色,主要从私主体的阻止违法行为的能力、成本收益分析、现有的激励机制,以及行政执法的缺位等因素来进行评判[11]。在个人信息保护领域,以企业为代表的个人信息处理者往往收集了大量的个人信息,无论是从阻止信息泄露的能力,还是阻止违法行为的成本上分析,其无疑是作为“守门人”的最佳方案。一方面,当下人们的生活对互联网的依赖程度越来越高,开启了信息空间中的“网络化生存方式”;另一方面,伴随着大数据分析技术的快速发展,商业组织通过结合结构化与非结构化数据,更加精准地发掘消费者的潜在需求与市场趋势,其对于个人信息的需求量也呈现指数级增长[19]。与之相较,面对种类繁多的被监管实体,行政机关无法针对大规模汇集个人信息的市场风险形成统一的监管规则,一刀切的方式更是难以应对多样化的风险[20];加之,监管机构无法比从事生产活动的商业组织掌握更多的信息,其将注意力转移到事先的预防,不再着重强调结果导向的监管细节。监管机构很大程度上将落实公共管理目标具体细节的自由裁量权交给被监管主体,利用被监管方自身的专业知识和判断力来决定实现监管目标的手段,以及在特定情况下这些目标的定义和对实现管理目标的监督。此外,不同于传

⑤2021年1月22日修订通过的《行政处罚法》第48条,“具有一定社会影响的行政处罚决定应当依法公开”;2019年4月3日修订的《政府信息公开条例》第20条,“行政机关应当依照本条例第十九条的规定,主动公开本行政机关的下列政府信息:……(六)实施行政处罚、行政强制的依据、条件、程序以及本行政机关认为具有一定社会影响的行政处罚决定”;《企业信息公开暂行条例》第6条、第7条、第8条分别规定工商行政管理部门、其他政府部门以及企业应当在行政处罚等信息产生之日起20个工作日内予以公开。

统领域中基于社会信用信息系统构建的声誉制裁体系,泄露通知制度保留了相当的自由裁量余地,给个人信息处理者采取措施避免危害,豁免其遭受声誉制裁的机会空间。触发该自由裁量的条件是“个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成的危害”,此时个人信息处理者可以不通知有关职责部门与个人。同时,作为对自由裁量的控制和制约,履行保护职责的部门认为信息泄露可能对个人造成危害的,亦有权要求个人信息处理者履行通知义务。

(三)自由裁量的触发条件与“加密避风港原则”

1. 自由裁量的触发条件

“个保法”第57条第二款规定了在公法通知义务下的豁免规则,即“个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的”,其可以不通知到个人,换言之,这是个人信息处理者在基于公法义务的豁免规则设定,获得了选择“不通知”的自由裁量空间。在传统领域下的声誉制裁体系中,负面标签作为核心打击手段“结构性”压缩了自由裁量空间;依托于社会信用基础上的信息交换,以普遍、自动化的方式将声誉制裁的影响扩展至一系列公权力主体、相关市场以及社会群体中。但类似于“经营异常名录”“严重违法失信企业名单”的负面标签是存在移出机制的⑥,其保留了一定程度的激励、宽容空间。而在泄露通知制度中,个人信息处理者一旦履行了信息泄露通知义务,网络的“记忆”是无法被抹去的,其消除负面影响、挽回社会声誉的可能性微乎其微。因此“个保法”考量到声誉制裁的严厉性和不可修复性,在公法通知义务的基础上设定了豁免规则,给予个人信息处理者一定条件下“不通知”的自由。

作为自由裁量的触发条件,“有效避免信息泄露、篡改、丢失造成危害”中“有效”的边界是在监管机构与企业互动过程中逐步发现的,是一个长期的实践过程,即监管机构利用监管过程中企业的信息披露来获取知识,进而提供可客观衡量“有效”的标准。然而在泄露通知制度创立初期,将一种需要长期实践检验才能够发现的标准作为个人信息处理者自由裁量的触发条件,无异于架空其公法通知义务。即使“有效”的标准是能够被公权力主体准确认知的,信息泄露造成的危害也依然是未知的,客观上无法被准确认知。大规模的个人信息泄露之后,通常是流入地下市场,亦即暗网,进行流通买卖,之后再被转手用作他途,如金融信贷催收、营销等领域[21]。这意味着从个人信息泄露到实际危害发生之间存在一个时间差。在这段时间内,信息泄露造成的危害是未知的,客观上是无法被评估衡量的。故而,我国泄露通知制度需要设定具有可操作性的自由裁量触发条件。由美国财政部联合美联储、美国联邦存款保险公司制定的《机构间应急方案指南》提出,仅当发现存在被泄露的个人信息有被滥用的可能性,金融机构才须向个人发出泄露通知。发现个人信息有被滥用的可能性之标准在现实中是具备可操作性的,譬如,金融机构监测到被泄露的个人信息开设了伪造账户。

2. 加密避风港原则

加密避风港原则意指,作为个人信息处理者的组织机构,其遭遇泄露的信息若已经过加密处理,则免于履行泄露通知义务[22]。在制度实践层面,该原则在美国以三种形式存在:豁免规则,可反

⑥参见《严重违法失信企业名单管理暂行办法》第9条:“企业自被列入严重违法失信企业名单之日起满5年未再发生第五条规定情形的,由有管辖权的工商行政管理部门移出严重违法失信企业名单。工商行政管理部门依照前款规定将企业移出严重违法失信企业名单的,应当作出移出决定,并通过企业信用信息公示系统向社会公示。移出决定应当包括企业名称、统一社会信用代码/注册号、移出日期、移出事由、作出决定机关。”

驳的推定(rebuttable presumption),以及损害的分析要素[23]。豁免规则源于加州 2002 年颁布的《数据安全泄露通知法》,其规定:如果加州的商业组织被未经授权的第三方获取了没有加密且由计算机存储的个人信息,则必须发出泄露通知[9]。但该法案没有对"加密"进行定义,而是由加州隐私保护办公室(California Office of Privacy Protection)制定了进一步的政策指引,解释何为可接受的加密技术和其他信息安全措施。可反驳的推定意指,该避风港原则建立了一种推定,即如果泄露的是加密数据,就不存在风险;如果发现相反的证据,就可以推翻这种假设,无需发出泄露通知[24]。例如美国国会在 2009 年颁布的《数据问责与信任法案》(Data Accountability and Trust Act)第三章信息安全泄露通知中规定,如果一个组织能够证明已对所泄露的个人数据进行了有效的加密,那么就可以推定,泄露事件不会触发身份盗用的重大风险。这一明确的推定可以通过证明"加密方法已经或可能遭到破坏"而被推翻;而作为危害的分析要素,加密只是"用于确定破坏行为是否为造成危害的因素"[25]。由此观之,加密避风港原则作为合理降低泄露通知数量,减少信息过载与企业合规成本的一种方式,具有直观的可操作性与衡量性。加密避风港可视为泄露通知制度中自由裁量的一种技术化表现形式,但具有强烈的场景适用限制性。面对海量的个人信息存储量,所有应用场景进行数据加密在时间与资源成本上都是不现实的。

四、我国个人信息泄露通知制度的结构化完善

(一)常态化监督的自由裁量

首先,常态化监督下的自由裁量权应当建立在具有操作性、可衡量的标准之上,即不仅仅要求个人信息处理者去判断其采取的措施是否能够"有效"避免信息泄露造成的危害,更需要借鉴是否存在"滥用泄露的个人信息的风险"的标准。例如以金融系统为起点,将被泄露个人信息的主体列入"监管"名单,监控个人信息被"滥用"的活动,以此作为探索在其他生活领域监控个人信息"滥用"活动的蓝本。其次,常态化监督要求职责部门持续介入个人信息处理者在自由裁量方面的审核。以企业为代表的个人信息处理者,在面对行政监管与公司目标之间的冲突时,企业内部既定的惯例和思维方式促使其以最容易实现合法外观的方式来进行合规调整,同时尽量减少企业因合规调整带来的负外部性[26]。因此,监管机构需要常态化介入企业关于泄露通知方面自由裁量的决定过程,让企业知晓职责部门始终在监督,并将严格审查其作出关于泄露通知的决定。常态化介入方式可以借鉴《萨班斯奥克斯利法案》第 302 条与第 404 条,分别关于上市公司在年报中提供内部控制与程序报告,与内部控制程序存在的缺陷⑦。个人信息处理者也应当就其作出自由裁量决定过程中涉及的相关程序、人员职责分配,以及可能带来的误判风险提供详细的说明,并以周期性的方式向职责部门进行汇报。此外,个人信息处理者还应当就"不同周期的自由裁量决定报告中类似的信息泄露事件作出不同的处理方式"提供详细的说明,从而迫使企业面对信息泄露事件作出的自由裁量决定是经过有效的评估决策,而非流于形式的合规。

(二)双层泄露通知制度

根据"个保法"第 57 条第一款,我国个人信息保护领域采取的是单一泄露通知制度,即原则上

⑦参见 Sarbanes-Oxley Act § 302 §404, 15 U.S.C. § 7262.尽管该法案主要是规制上市企业,但其提供的监管方式,即内部控制和程序报告以及内部控制程序存在的缺陷,依然能够为如何有效审查一般企业作出自由裁量决定提供借鉴。

对于监管机构与个人信息主体,不加以区分地履行通知义务。通过对美国《机构间应急方案指南》与欧盟《通用数据保护条例》中双层泄露通知制度的梳理,可以发现监管机构与个人信息主体的通知阈值是有差别的。换言之,监管机构与个人信息主体在接受、处理信息能力上有巨大的差异。监管机构有强大的人力资源和信息加工处理能力,故而原则上只要发生了或有迹象表明发生了信息的泄露、篡改、丢失,个人信息处理者就应当向监管机构履行通知义务;而个人信息主体,其背后是信息接受、处理能力参差不齐的社会公民、消费者,其时时刻刻面临着严重的信息过载,将直接导致泄露通知被信息主体选择性忽略。鉴于监管机构与个人信息主体在信息接受、处理能力上的差异,我国个人信息泄露通知制度建议采取分层机制,即原则上,个人信息处理者发现信息泄露,立即采取补救措施之后,应当通知监管机构;而对于个人信息主体的通知应当设定较高触发阈值。

(三)显性监管指标的弱化

当下互联网企业依托平台和技术优势,已经成为个人信息的主要存储与管理组织。面对市场上占据优势地位的互联网企业,地方职责部门往往在与其监管互动过程中形成共识,导致企业合规流于形式。因为企业在接收职责部门的监管过程中,逐渐了解如何能够满足具体监管指标,并将这些例行公事化的信息融入企业的日常合规流程,加剧了形式化监管的现状[27]。“个保法”第57条以“履行个人信息保护职责的部门”负责监督审核个人信息处理者的自由裁量决定,在一定程度上为日后弱化显性监管指标留下制度空间。以企业为代表的个人信息处理者,在作出自由裁量决定,选择不履行通知义务后,应当就其决定涉及的内部程序、考量的相关因素作出报告,提供给主要职责部门以备监管审查。由于被监管主体的形式多样,审查众多企业的自由裁量决定涉及的专业知识往往超出单一职责部门的监管能力。因此,建议主要职责部门在收到自由裁量决定后与其他相关部门共享,就个人信息处理者的自由裁量决定协同审查,弱化显性监管指标概念。换言之,正是由于多部门的协同审查使得以企业为代表的个人信息处理者无法在监管互动过程中摸清职责部门的监管倾向。尤其是考虑到需要就自由裁量决定过程中涉及的相关内部程序和潜在的风险评估向职责部门进行阐述和解释时,企业将会考虑双边的论点和证据,以便为来自各方的批判意见做好准备。弱化外在监管指标促使企业管理层在面对不同的信息泄露事件削弱对既有的“知识结构”的依赖,使其根据不断变化的社会现状改善、提升企业在个人信息保护方面的制度措施。

(四)个人信息泄露通知内容的有效性

“个保法”第57条第一款罗列了通知应当包含的若干事项,包括发生或可能发生的个人信息泄露、篡改、丢失的信息种类、原因以及可能造成的危害,个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施,以及个人信息处理者的联系方式。在讨论具体通知内容之前,有必要强调接收通知的个人的受教育水平。职责部门在规定通知具体内容的事项上,不能仅以监管者视角看待通知的组成架构,更应当站在信息遭遇泄露、篡改、丢失的个人视角上“急人之所急”,充分知晓我国当下依然存在很大一部分群体运用智能技术困难的现状。泄露通知制度的实行很大程度上会被诈骗团伙所利用,导致更加不可估量的财产损失等后果。此外,泄露通知无论是以短信还是电子邮件的方式发送告知,在当下信息过载的时代,有相当一部分群体会以垃圾短信或者垃圾邮件的方式过滤泄露通知,导致该制度的有效性大打折扣。在泄露通知的具体事项方面,“个保法”只规定应当包含什么,没有规定不能额外包含何种事项。这将导致发送泄露通知的企业借机推广其网络安全相关的商品等,以“夹带私货”的方式损害了泄露通知的可阅读性。关于泄露通知的第一项内容,即

个人信息泄露、篡改、丢失的原因,信息泄露往往牵扯到整个产业链,下游企业的安全漏洞可能最终在上游头部企业"引爆"巨大的信息泄露事件。简单地要求涉事企业公布个人信息泄露的原因往往适得其反,掩盖了问题真正的根源。综上,在信息泄露通知的具体内容设计以及发送通知的方式上,应更多地允许企业以及所在行业制定准则,提交给监管部门审批,鼓励行业借助信息技术开发创新有效的方式来克服既有的通知方面的缺点。还要严格规范泄露通知所能包含内容的范围,禁止任何商业推广危害通知的可阅读性。

五、结语

在个人信息保护形势日趋严峻的当下,个人信息泄露通知制度的细化和完善显得极为迫切。我国《个人信息保护法》第 57 条赋予个人信息处理者的自由裁量空间在很大程度上影响着泄露通知机制的有效性。行政法上第三方义务赋予个人信息处理者的自由裁量与"结构化自由裁量"在权力的行使方式上都面临着如何规制自由裁量主体在信息和权力上的垄断问题。鉴于个人信息处理者在知识、信息上的优势地位,促使其自由裁量权的行使更加公平、合理的程序性机制主要集中在信息披露这一维度。据此,本文提出四点完善细化建议:在常态化监督方面,进一步建立具有操作性、可衡量的触发自由裁量的标准,且职责部门需持续性介入个人信息处理者在自由裁量方面的审核;在双层泄露通知方面,原则上,个人信息处理者发现信息泄露、篡改、丢失,立即采取补救措施之后,应当通知监管机构,而对于个人信息主体的通知应当设定较高通知触发阈值,即发现泄露、篡改、丢失的个人信息有被滥用的可能性,会给个人信息主体带来潜在的危害;在显性监管指标的弱化方面,对个人信息处理者的自由裁量决定进行多部门的协同审查;在泄露通知内容的有效性方面,鼓励行业准则的制定,严格规范泄露通知所能包含内容的范围,提升泄露通知内容的可阅读性。

参考文献:

[1]CHARNY D. Nonlegal sanctions in commercial relationships[J]. Harvard Law Review,1990,104(2):373-467.

[2]中国财经网. 圆通速递泄露 40 万条个人信息被约谈股价跌 1.71%[EB/OL]. (2020-11-26)[2021-08-16]. http://finance.china.com.cn/stock/ssgs/20201126/5440347.shtml.

[3]BBC News. Cathay Pacific data hack hits 9.4 million passengers[EB/OL]. (2018-10-25)[2021-08-16]. https://www.bbc.com/news/business-45974020.

[4]刘金瑞. 数据安全范式革新及其立法展开[J]. 环球法律评论,2021(1):5-21.

[5]PARK S. Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records[J]. International Review of Law and Economics,2019,58:132-145.

[6]CARTWRIGHT P. Publicity, punishment and protection: The role(s) of adverse publicity in consumer policy[J]. Legal Studies,2012,32(2):179-201.

[7]THORNTON D, GUNNINGHAM N A, KAGAN R A. General deterrence and corporate environmental behavior[J]. Law & Policy,2005,27(2):262-288.

[8]高富平. 个人信息保护:从个人控制到社会控制[J]. 法学研究,2018(3):84-101.

[9]California Data Security Breach Notification Law,California Civil Code s. 1798.29(a)[EB/OL]. (2021-01-01)[2021-08-16]. https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml? lawCode=CIV&sectionNum=1798.29.

[10]California Data Security Breach Notification Law,California Civil Code s. 1798.82(g)[EB/OL]. (2021-01-01)[2021-08

-16]. https://leginfo. legislature. ca. gov/faces/codes_displaySection. xhtml? lawCode=CIV&sectionNum=1798. 82.
[11]MURCIANO-GOROFF R. Do data breach disclosure laws increase firms' investment in securing their digital infrastructure [EB/OL]. (2019-05-20) [2021-08-16]. https://weis2016. econinfosec. org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_33. pdf.
[12]Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[EB/OL]. (2005-03-29) [2021-08-16]. https://www. federalregister. gov/documents/2005/03/29/05-5980/interagency-guidance-on-response-programs-for-unauthorized-access-to-customer-information-and.
[13]王瑞雪. 声誉制裁的当代图景与法治建构[J]. 中外法学,2021(2):446-464.
[14]熊樟林. 行政处罚的种类多元化及其防控:兼论我国《行政处罚法》第 8 条的修改方案[J]. 政治与法律,2020(3):77-93.
[15]沈岿. 社会信用体系建设的法治之道[J]. 中国法学,2019(5):25-46.
[16]BLACK J,BALDWIN R. Really responsive risk-based regulation[J]. Law & Policy,2010(2):181-213.
[17]姚志伟. 技术性审查:网络服务提供者公法审查义务困境之破解[J]. 法商研究,2019(1):31-42.
[18]KRAAKMAN R H. Gatekeepers:The anatomy of a third-party enforcement strategy[J]. The Journal of Law,Economics,and Organization,1986(1):53-104.
[19]胡朝阳. 大数据背景下个人信息处理行为的法律规制:以个人信息处理行为的双重外部性为分析视角[J]. 重庆大学学报(社会科学版),2020(1):131-145.
[20]SUNSTEIN C. Administrative substance[J]. Duke Law Review,1991,41:607-646.
[21]郭航. 警惕暗网欺诈和个人信息违法交易[J]. 中国金融家,2019(8):126-127.
[22]BURDON M, LANE B, VON NESSEN P. Data breach notification law in the EU and Australia—Where to now?[J]. Computer Law & Security Review,2012,28(3):296-307.
[23]BURDON M,REID J,LOW R. Encryption safe harbours and data breach notification laws[J]. Computer Law & Security Review,2010,26(5):520-534.
[24]U. S. National Conference of State Legislature. Security breach notification laws[EB/OL]. (2021-04-15)[2021-08-16]. https://www. ncsl. org/research/telecommunications-and-information-technology/security-breach-notification-laws. aspx.
[25]U. S. Congress. Data Accountability and Trust Act of 2009[EB/OL]. (2009-12-09)[2021-08-16]. https://www. congress. gov/bill/111th-congress/house-bill/2221.
[26]U. S. Congress. Sarbanes-Oxley Act of 2002[EB/OL]. (2002-07-30)[2021-08-16]. https://www. congress. gov/bill/107th-congress/house-bill/3763.
[27]SCHWARTZ P,JANGER E. Notification of data security breaches[J]. Michigan Law Review,2006,105:913-984.

Research on discretion regulation in personal information breach notification system

TANG Lin, ZHANG Lingling

(*KoGuan Law School*, *Shanghai Jiao Tong University*, *Shanghai 200030*, *P. R. China*)

Abstract: Article 57 of Personal Information Protection Law of the People's Republic of China established the personal information breach notification system for the first time, which stipulates the obligation of personal information processor to perform notifications to relevant departments and individuals after the leakage of information. The leakage of personal information often brings continuous and derivative harm to the subject of personal information, involving personal and property safety as well as mental damage, so timely and effective breach notification can better protect the rights and interests of personal information. In relation to the

obligation to breach notification, the processor is given a certain amount of discretion, i. e., if measures can effectively avoid the relevant harm, the individual may not be notified. Correspondingly, there are two main challenges to this discretion: first, it undermines the effectiveness of the reputational sanctions triggered by the breach notification, as companies, anticipating the potential huge commercial risks and social responsibilities, often choose to "digest" the breach events that has already occurred internally, undermining the operational mechanism of reputational sanctions; second, the information asymmetry between the personal information processor and administrative authorities, and the "regulatory capture" based on explicit regulatory indicators lead companies to meet regulatory requirements in the easiest way to achieve legal appearance and reduce compliance costs. Discussions on how to regulate the discretionary scope of the system and how to build a coordination mechanism between regulators and business organizations have not stopped. Properly regulating the discretionary space is the key to the effective operation of the breach notification system. The paper analyzes the system of corporate reputation sanctions, its justification basis and discretionary trigger conditions based on the theoretical framework of third-party obligations in administrative law by drawing on the remarkable legislative policies of breach notification systems in Europe and the United States in respect of triggering criteria and threshold distribution. At the same time, from the perspective of "structured discretion" proposed by Davis, it is proposed that the breach notification system in China should be refined and improved by focusing on the normal supervision of discretion and continuous intervention in the review of processors' discretion; adopting a two-tier approach in the breach notification system, i. e., in principle, information leakage should be immediately notified to the regulator, and a higher trigger threshold should be set for the notification of personal information subjects; the explicit regulatory indicators should be weakened in terms of synergy, and the main responsible department should collaborate with other relevant ones to review the discretionary decision after receiving it, so as to weaken the concept of explicit regulatory indicators; in terms of the effectiveness of the breach notification, the specific content design of the notification and the way of sending the notification should be strengthened and the scope of the content that can be included in the breach notification should be strictly regulated ensuring any commercial promotion that jeopardizes the readability of the notice is prohibited.

Key words: breach notification; third-party responsibility; discretion; personal information protection

(责任编辑　胡志平)