Public Governance Research
Vol. 34, Issue 5

2022 October

The U.S. federal personal information breach notification system and its reference significance

By

Yu Zengzun

美国联邦个人信息泄露通知制度及其借鉴意义
于增尊

Recommended Citation

Zengzun, Y., 2022, October. The U.S. federal personal information breach notification system and its reference significance. Public Governance Research, Vol. 34(5).

法与治理

美国联邦个人信息泄露通知制度及其借鉴意义

于增尊
（天津师范大学　法学院，天津　300387）

摘要：美国是世界上最早确立个人信息泄露通知制度的国家，但由于两党制掣肘、联邦和州两套法律体系并行等体制性困境，时至今日在联邦层面仍然缺乏综合性的个人信息泄露通知法，仅在公共部门管理、医疗健康、金融服务等领域颁布较为完善的单行立法。我国应当重视个人信息泄露通知的综合性立法工作，允许特定行业制定个人信息泄露通知规范，构建系统明晰的个人信息泄露通知规则体系。

关键词：个人信息泄露通知；数据泄露通知；健康保险携带和责任法案；格雷姆－里奇－比利雷法案
中图分类号：D90　**文献标识码**：A　**文章编号**：2097－0072（2022）05－0082－08
DOI：10. 13975/j. cnki. gdxz. 2022. 05. 010

随着互联网、大数据等现代信息技术的大规模应用，人类社会迅速进入信息化、数字化时代。信息技术和数字产业的发展大大便利了日常生活，推动了社会经济发展。与此同时，围绕信息资源的犯罪活动持续高发，数据泄露事件层出不穷，严重损害公民合法权益和国家安全发展。如何减少数据泄露事件的发生，以及在数据泄露后将损失降到最小，成为各国面临的共同课题。为此，越来越多的国家通过法律确定了个人信息泄露通知制度或数据泄露通知制度（个人信息是数据的内容，也是数据泄露的重灾区，许多立法和表述中将二者等同，本文依循此例），力图通过事后的通知和补救措施降低数据泄露的危害。

我国近年来颁布的《网络安全法》《民法典》《个人信息保护法》《数据安全法》等法律中均规定了信息处理者或网络运营商的数据泄露通知义务，但条文数量较少，内容尚显粗疏，可操作性较差，需要借鉴域外先进经验加以完善。而作为最早确立个人信息泄露通知制度的美国则是绕不开的考察对象。美国是一个联邦和州法律系统并行的国家，国内学者目前对美国数据泄露通知制度的研究，或将联邦和各州的内容统而言之，或只针对联邦层面的特定行业立法（主要是医疗健康领域），在深入性和系统性方面稍显不足。本文拟就美国联邦个人信息泄露通知制度进行全面考察，并辨析其利弊得失，希望能对我国个人信息泄露通知制度建设有所裨益。

一、美国联邦个人信息泄露通知制度立法概况

2002 年 9 月，加利福尼亚州通过了 SB1386 号法案，并于 2003 年 7 月 1 日正式生效。这是世界上首部数据泄露通知法，在个人信息保护领域开创了新纪元。同年，参议员 Dianne Feinstein 向美国国会提出了一项联邦数据泄露通知法提案。尽管该提案经过二读后未能获得批准，但制定一部联邦数据泄露通知法律的诉求由此进入了国会的议事范畴。此后几年间，美国国会审查了多项立法提案，许多州也在呼吁国家尽快出台相关法律。在 2005 年写给国会领导人的一封信中，48 个州的检察总长敦促国会采取行动，制定联邦法规。[1] 在接下来的十年里，随着网络攻击和信息泄露愈演愈烈，一项统一的联邦立法显得愈发重要且迫切。每一届国会均为此做了尝试，甚至仅 2007 年就提出了三项数据

收稿日期：2022－06－30
基金项目：天津市教育科学规划项目《高校治理现代化视域下的学生个人信息保护问题研究》（编号：HIE210396）。
作者简介：于增尊（1986－），男，河北沧州人，天津师范大学法学院副教授，主要研究方向为数据法学。

泄露通知法案[2]，可惜始终未能正式颁行。

2015 年，奥巴马总统在国情咨文中指出，为了“更好地应对不断演变的网络攻击威胁、打击身份盗窃并保护孩子们的信息”[3]，必须解决网络安全问题，制定“个人数据通知和保护法案”（Personal Data Notification and Protection Act），建立国家层面的个人信息泄露通知标准。该法案被提交至多个联邦委员会，但与之前所有相同的努力相似，它最终也只是摆在国会面前的众多提案之一。

当然，没有关于个人信息泄露通知的综合性法律，并不意味着在联邦层面无章可循。面对不断高发的网络犯罪和信息泄露事件，一些联邦管理机构在特定行业或领域内出台了专项法规，主要包括美国公共和预算管理办公室（Office of Management and Budget）防范和应对联邦机构管理的个人信息泄露的指导意见，联邦政府及美国卫生和公众服务部（United States Department of Health and Human Services）制定的一系列健康信息泄露通知规范，美国财政部金融局（Office of the Comptroller of the Currency）、联邦储蓄委员会（Federal Reserve Board）、联邦储蓄保险公司（Federal Deposit Insurance Corporation）、联邦储蓄机构管理局（Office of Thrift Supervision）等部门制定的保护金融领域个人信息泄露的通知法规，等等。

二、联邦机构个人信息泄露通知制度

（一）主要的法律文件

基于管理和服务等目的，包括联邦机构在内的公共部门会收集许多个人信息。如何切实保护这些个人信息并防止其被泄露，对于维持政府形象、维护公众信任至关重要。2007 年 4 月，“总统的身份盗窃特别小组”（The President's Identity Theft Task Force）发布了《打击身份盗窃：战略计划》（Combating Identity Theft：A Strategic Plan），对联邦政府机构如何保护个人信息作出了规定，并建议公共和预算管理办公室向所有联邦机构和部门发布数据泄露指南和常规操作指引，以便后者在数据泄露后正确披露相关信息。[4]

为响应特别小组建议，2007 年 5 月公共和预算管理办公室为联邦机构发布名为《防范和应对个人身份信息泄露》（Safeguarding Against and Responding to the Breach of Personally Identifiable Information）的指导意见备忘录。[5]备忘录要求联邦机构在 120 天内制定并实施泄露通知政策，并在附件中概述制定泄露通知政策时必须遵循的框架。其中附件 1“防止个人身份信息被泄露”再次强调联邦机构在现有法律、行政命令、法规和政策下保护个人身份信息和培训员工的责任，并提出两项新的隐私要求和五项新的安全要求。附件 2“事故报告和处理要求”重申各联邦机构应当建立正式的信息泄露事件响应计划，并要求机构在发生任何涉及个人身份信息泄露的事件后通知有关机构。附件 3“信息泄露的外部通知”规定了联邦机构在向个人发出通知时需要考虑的因素，并详细说明了通知内容、通知方法等。附件 4“规则和后果”指导每个机构制定和实施政策，明确不遵守行为规则的后果和可以采取的纠正措施。

（二）通知之前的风险评估

在发现数据可能遭到泄露后，联邦机构应当首先对泄露事件可能造成的风险进行评估。评估应考虑五方面因素：①遭到泄露的数据元素的性质。②受影响的人员数量。③个人信息的可访问性和可用性，即被未经授权的个人使用的风险大小。④泄露事件导致损害的可能性，包括潜在危害的广泛性和损害发生的现实可能性。⑤联邦机构减轻损害风险的能力，即如何减轻泄露事件对信息系统造成的进一步损害。

（三）通知个人的规则

通知应当简洁、醒目、通俗易懂，并包括以下内容：对信息泄露的情况进行简要描述，包括泄露发生的日期和发现泄露的日期；在可能的情况下，说明泄露事件涉及的个人信息类型；说明信息是否被加密或通过其他方式保护；个人应采取哪些措施以保护自己免受潜在的伤害；联邦机构正在采取的调查和止损措施。

提供通知的方式取决于受影响的个体数量和联系信息，并应与他们需要收到通知的紧迫性相称。可考虑的通知方式包括：①邮递信件（First – Class Mail）；②情况紧急需要立即进行个别通知或受影响人数有限的，可以采用电话通知，但应与书面通知同时进行；③如通知对象已提供电子邮箱，并明确同意以电子邮件作为与机构联络的主要方式，而其收件地址并不可知，可以采取发送电子邮件的方式；④作为个别通知的补充，可以在报纸或其他公共媒体上刊登通知；⑤如果机构没有足够的联系信息提供通知，可以使用替代方式，包括在机构网站首页的醒目位置张贴通知，并通知当地主要的印刷和广播媒体。

（四）通知监管机构的规则

如果发生了未经授权的访问或涉及个人身份信息的事件，除通知受影响的个人之外，联邦机构还须向有关机构或官员履行告知或报告义务。一是遵循机构内部程序，通知包括隐私官员和监察官员在内的联邦机构官员。二是无论当时掌握信息的多寡，要在一小时内通知美国计算机应急小组（United States Computer Emergency Readiness Team），以便

其协助协调联邦机构与其他机构的沟通。三是如果数据泄露事件涉及信用卡信息，则联邦机构需要通知开户行。

（五）通知的时间与违规罚则

在发现数据泄露后，各机构应无不合理迟延地履行通知义务，除非是为了执法和国家安全的需要，或恢复受损的电脑数据系统的合理完整性。推迟通知的决定应由机构首长或其可书面指定的高级人员作出，但延误不应加重任何受影响个人面临的风险或遭受的伤害。如果相关工作人员未切实履行通知职责，可以根据法律和政策对其处以谴责、停职、罢免等处罚。

三、医疗健康领域个人信息泄露通知制度

（一）主要的法律文件

为提高健康保险的可携带性和连续性，打击医疗保险和医疗保健服务中的浪费、欺诈和滥用[6]，美国联邦政府于1996年8月颁布《健康保险携带和责任法案》（Health Insurance Portability and Accountability Act，HIPAA）。HIPAA要求卫生与公众服务部部长制定保护健康信息隐私和安全的法规。为此，卫生和公众服务部分别于2000年和2003年颁布隐私规则（Privacy Rule）和安全规则（Security Rule），对个人健康信息的使用和披露作出限制，并建立了一套保护特定健康信息的国家标准。2009年，作为《美国复苏与再投资法案》（American Recovery and Reinvestment Act，ARRA）的一部分，国会通过了《医疗信息技术促进经济和临床健康法案》（Health Information Technology for Economic and Clinical Health Act，HITECH），旨在促进和扩大健康信息技术的采用，并提升对健康信息的保护。该法案的一项重要内容是引入健康信息遭到泄露后的通知规则，包括通知主体、对象、时间、内容、罚则等。这些内容在2013年颁布的HIPAA综合规则（Omnibus Rule）中得到了修订吸收，最终形成了较为完善的健康信息泄露通知制度。

（二）主要术语的定义

HIPAA规制的主体包括“涵盖实体”（Covered Entity）及其商业伙伴（Business Associate），前者主要包括健康计划（Health Plans）、健康保健服务提供者（Health Care Providers）和健康保健信息处理机构（Health Care Clearinghouses）；后者则是向实体提供健康信息传输服务，或代表实体向他人提供个人健康记录等，因而接触和使用健康信息的组织和个人。

HIPAA保护的客体是“受保护的健康信息”（Protected Health Information，PHI），也称为HIPAA数据，是在提供医疗保健服务过程中创建、使用或披露的任何可能识别个人身份的健康信息，包括与个人过去、现在或将来的身体或心理健康状况有关的信息，向个人提供医疗保健的信息以及支付费用的信息。HIPAA列出了18项身份标识符，包括姓名、地址、电子邮箱、病例编号、生物识别标识符、全脸照片和任何可以识别个人的类似图像等，包含其中任何一项即被视为“受保护的健康信息”。

在HIPPA语境下，信息“泄露”是指“以……不允许的方式获取、访问、使用或披露受保护的健康信息，从而损害受保护健康信息的安全或隐私。”但下列情形不属于信息泄露：①实体及其商业伙伴的工作人员或授权人员出于善意，并在授权范围内无意获取、访问或使用健康信息；②被授权访问健康信息的人无意中向另一位被授权人员披露健康信息，且该信息不会被进一步不当使用或披露；③实体及其商业伙伴真诚地相信，未经授权获知健康信息的人员不可能合理地保留该信息。

（三）通知的触发条件

为了确定受保护的健康信息是否已被泄露，以及是否会对个人造成重大伤害，实体及其业务伙伴需要进行风险评估。需要考虑的因素包括：①遭到泄露的健康信息的性质和范围，包括信息类型和重新识别的可能性；②未经授权使用或收到健康信息的人；③是否实际获取或查看了健康信息；④健康信息的风险得到缓解的程度。

如果评估结果显示健康信息被泄露的可能性或者危害后果很小，实体可以决定不发出通知。但风险评估并非启动泄露通知程序的前置条件，在健康信息明显遭到泄露的情况下，实体可以在不进行风险评估的情况下，直接启动泄露通知流程。并且作为一项经营战略，没有什么可以阻止实体及其业务伙伴在不执行风险评估的情况下，就每次健康信息泄露事件发出通知。[7]

（四）通知的具体规则

根据HIPAA规则，健康信息泄露后的通知对象包括信息主体、卫生和公众服务部以及媒体三部分。

其一，在发现健康信息泄露后，相关实体必须以书面形式通知受影响的个人，除非其同意以电子方式接收此类通知。如果有10人以上的联系信息缺失或失效，则实体必须在其网站首页或受影响个人可能居住区域的主要媒体上发布通知。在通知时间方面，HIPAA要求实体尽快向个人提供通知，不得无故拖延，且在任何情况下都不得迟于发现信息泄露行为后的60天。通知必须尽可能包括以下五方面内容：①对健康信息泄露情况的简要描述，包括泄露发生的

日期和发现泄露的日期（如果已知）；②对遭到泄露的健康信息类型的描述；③个体为保护自己免受潜在伤害而应采取的措施；④对实体正在采取的调查核实、减轻伤害、防范后续泄露等措施的简要描述；⑤实体的联系信息。

其二，如果信息泄露事件涉及同一个州或者司法管辖区内500名以上居民，实体需要无不当迟延地并最迟在发现后的60天内，以新闻稿的形式通知该州或司法管辖区内的知名媒体。考虑到实体通常不会保留所有受害者的最新联系信息，通知媒体的重要性就十分凸显，是确保所有受害者都意识到个人信息遭到泄露威胁的重要举措。

其三，实体必须通过在卫生和公共服务部网站填写并提交数据泄露报告表的方式，将有关情况通知部长。如果健康信息泄露的影响范围超过500人（不论分布在几个州），实体必须无不当迟延地通知卫生和公共服务部部长，且最迟不得晚于发现泄露事件后的60天；如果健康信息泄露影响的对象少于500人，实体应当在不迟于发现泄露事件的当年结束后的60天内提交报告。

（五）违规的处罚措施

为确保实体在保护患者隐私和健康数据方面积极履行职责，对于违反HIPAA规则的行为，设置在卫生和公共服务部的民权办公室（Office of Civil Rights）和州检察长有权进行处罚。处罚结构是分层次的，OCR通常更喜欢使用发布技术指导等非惩罚性措施解决HIPAA违规行为，但如果违规行为严重、持续很长时间或者存在多种违规行为，民权办公室可能采取经济处罚措施，最高可处以每年150万美元的罚款。作为该种罚则的一部分，如果实体不恪守个人信息泄露通知义务，包括不予通知、延迟通知、通知事项不合要求等，就可能受到经济处罚。2017年，Presense Health成为第一个与民权办公室就违反HIPAA泄露通知规则的案件达成和解的实体。该公司因晚于规定时间一个多月才通知卫生和公共服务部，最终向OCR支付了47.5万美元来解决其违规行为。[8]

四、金融服务领域个人信息泄露通知制度

（一）主要的法律文件

1999年，美国国会颁布被称为“金融服务现代化法案”的《格雷姆－里奇－比利雷法案》（Gramm－Leach－Bliley Act，GLBA），旨在控制金融机构处理个人信息的方式，确保其保护从各种形式的客户记录中收集的个人身份信息的机密性。GLBA第501（b）节要求各监管机构为金融机构制定与行政、技术和物理保障相关的标准，防止此类信息的安全性或完整性受到威胁或危害。据此，2001年美国财政部金融局、联邦储蓄委员会、联邦储蓄保险公司、联邦储蓄机构管理局等机构联合制定《建立信息安全标准的机构间准则》（Interagency Guidelines Establishing Information Security Standards），要求各金融机构评估客户信息（系统）遭受违规披露、滥用、更改、破坏的威胁，以及未控制风险制定的各项政策程序的充分性，制定与信息敏感性和银行业务范围、复杂度相称的，包含行政、技术和物理保障措施的信息安全计划。[9]2005年，联邦储蓄委员会等机构又联合发布《关于客户信息被未经授权访问和通知客户的响应机制的机构间指南》（Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice），以列举形式规定金融机构的响应机制应当包括的内容，对通知客户的标准、内容、形式作出详细规定，重申银行在客户信息泄露时向联邦监管机构、执法机构报告的义务，并鼓励其在向客户发送通知之前通知消费者报告机构。[10]

（二）主要概念的定义

在GLBA系列规范体系下，需要履行数据泄露通知义务的主体是“金融机构”（financial institution）。“金融机构”是指从事1956年《银行控股公司法》第4（k）条所述金融活动的任何机构，即向个人提供贷款、投资、保险等金融产品或服务的银行、投资公司、保险公司等。作为通知对象的“客户”是与金融机构有“客户关系”的消费者，建立关系的方式包括在金融机构开立信用卡账户、提供个人身份财务信息以获得抵押贷款等。遭到泄露的“客户信息”则是由金融机构或其代表所保存的，包含客户姓名、地址、银行卡号等非公开个人信息的记录，无论其形式是纸质、电子或其他。

（三）通知客户的规则

当金融机构发现未经授权访问客户信息的事件时，应进行合理调查，以便确定该信息已被或将被滥用的可能性。如果这种可能性得到确认，金融机构应尽快通知受影响的客户，除非执法机构认为通知会干扰刑事调查并向该机构发出延迟通知的书面要求。

通知应以确保客户可以合理预期收到的方式发出，包括电话、邮件、电子邮件等。通知应包含以下内容：①概括地描述信息泄露事件，被泄露的客户信息类型，以及金融机构为保护客户信息免受进一步侵害所做的工作；②提供一个电话号码，客户可以借此获得进一步的信息和帮助；③提醒客户在未来12至24个月内保持警惕，并及时向金融机构报告涉嫌身份盗用的事件。此外，金融机构应根据情况酌情通知以下内容：①建议客户检查自己的金融账

户，并在发现可疑情况时立即告知金融机构；②对欺诈警报的描述，以及解释客户如何在其消费者报告中添加欺诈警报，以通知债权人该客户可能是欺诈的受害者；③建议客户定期从全国性的信用报告机构那里获取信用报告，并删除与欺诈交易有关的信息；④告知客户如何免费获得信用报告；⑤告知客户如何获得联邦贸易委员会（FTC）在线指南（其中涉及消费者可以采取哪些措施来防止身份盗窃），并鼓励其向 FTC 报告身份盗窃事件。[10]

（四）通知监管机构的规则

《关于客户信息被未经授权访问和通知客户的响应机制的机构间指南》要求，当金融机构发现涉及未经授权访问或使用客户敏感信息的事件时，应当通知其主要联邦监管机构。所谓“客户敏感信息”（Sensitive Customer Information）是指客户的姓名、地址或电话号码，以及客户的社会安全号码、驾照号码、帐号、银行卡号码，或允许访问客户帐户的个人账号或密码，还包括允许某人登录或访问客户帐户的客户信息元素的任意组合，例如用户名和密码或密码和帐号。

按照规则起草机构的解释，金融机构需要在开始调查时通知监管机构，以确定信息已被或将被滥用的可能性，并便于监管机构在必要时采取适当行动。但联邦监管机构不希望创建一个需要填写类似“可疑活动报告”（Suspicious Activity Report）的详细表格的复杂流程，因此最终通过的规则仅要求金融机构尽快通过电话或其他快捷方式通知主要的联邦监管机构即可。[10]

五、美国联邦个人信息泄露通知制度评析

（一）综合性立法缺位主要缘于体制性困境

无论是为了维护公民的合法利益，还是减少网络犯罪和经济损失，抑或是促进法律的完备性和权威性，一部联邦层面的综合性数据泄露通知立法都是十分必要的。十数年来不断被提出的专业性议案，也说明了美国国会对此有着清晰的认识。之所以迄今仍面临立法缺位的局面，笔者认为根源在于美国内部的体制性困境。

一是联邦法律和州法律的优先权问题。美国是一个联邦制国家，存在联邦和州两级立法架构。美国《宪法》第 6 条第 2 款规定，“本宪法及依本宪法所制定之合众国法律……为全国的最高法律”，这就确立了“联邦法优先”原则。即在州法律与联邦法律产生冲突的情况下，联邦法律将优先适用；没有联邦法律时，州法律可以适用。在各州陆续颁布数据泄露通知法案的情况下，一旦联邦出台统一的国家标准，必然对州立法的法律效力和执法权限构成冲击，因此其对于联邦统一立法的态度并不积极。2015 年田纳西州共和党众议员 Marsha Blackburn 和佛蒙特州民主党众议员 Peter Welch 曾共同发起了一项“数据安全和泄露通知法”（Data Security and Breach Notification Act）提案，并获得了一定范围的支持。但来自 47 个州的检察长联名致信国会领导人反对该项提案，批评它削弱了州法律对消费者的现有保护，认为国会不应该阻止任何一个州在其境内制定更严格的法律，也不应该限制州检察长对违法者的追诉权。[1] 正如学者所言，在联邦法律对州隐私法的优先性等问题上，只要这些利益相关方“还守在自己的角落里，更广泛的隐私辩论就会冻结，联邦立法也会停滞不前。”[11]

二是两党之间的相互掣肘。美国是典型的两党制国家，民主和共和两党通过竞选轮流执政，掌握国家政权。两党的斗争和内耗贯穿在政治活动的各个环节，很多时候并非为了科学决策和维护选民利益，而是党派斗争的需要，两党在党派议案等方面长期地明争暗斗、相互否决。[12] 数据泄露通知法案迟迟无法出台，背后同样有两党斗争的因素。同样以 2015 年的“数据安全和泄露通知法”提案为例，尽管该法案在众议院能源和商务委员会获得了通过，但投票结果却呈现出明显的党派分歧：共和党 29 票，民主党 20 票。就连该法案最初的共同作者、民主党众议员 Peter Welch 最终也和其他民主党人一起对他自己的法案投了反对票。[1]

（二）特定行业领域的单行立法有其必要性

在美国联邦数据泄露通知立法陷入泥沼的同时，各州却在以近乎狂热的速度颁布相关法律规范。到 2018 年，随着南达科他州州长 Dennis Daugaard 和阿拉巴马州州长 Kay Ivey 分别签署 SB 62 号和 SB 318 号法案，美国 50 个州实现了数据泄露通知立法的全覆盖。较早制定法律的州，也在不断开展修法工作。

单独来看，每个州的行动都是为了维护其居民的合法利益，但这种不断变化的“大杂烩”式立法格局也为企业带来巨大困难。特别是对于跨州经营的大公司而言，要准确了解每个州的数据泄露通知规则并非易事。如此一来，各州非但没有为消费者提供更有效的保护，反而制造了一个法律泥潭，妨碍了企业有效应对数据泄露的能力。在综合性立法缺位的情况下，在个别行业领域内制定单行法规就成为一项次优选择，既可在一定程度上维护联邦的权威性，也可为州级立法提供制度样本和指引。从实际执行效果来看，尽管联邦法律并不必然能够取代州级数据泄露通知法，但许多州的确将企业按照 HIPAA、GLBA 等联邦规范采取通知行动视为满足了州法律中的数据泄露通知要求。

况且，目前已颁布联邦数据泄露通知规范的领域均有其特殊必要性。联邦政府部门基于公共管理职能掌握大量的

公民个人信息数据，能否做好保护工作，在数据泄露后作出及时应对，对于获得民众支持信任、维护政府形象至关重要。医疗健康领域的个人信息既包含公民的一般个人信息，更关联公民的生理特征、检验结果、既往病史等高度私密信息，一旦遭到泄露后果极其严重。银行等金融机构与公民的日常生活息息相关，掌握着海量的、有价值的个人信息数据，并且其数字化转型为网络攻击者访问这些数据创造了更多机会，从而使得金融部门成为网络犯罪分子的第二优选目标，仅次于医疗健康领域。[13]

（三）个人信息泄露通知规则较为合理

在保护个人信息和数据权利方面，美国起步较早、经验较为丰富。综观美国联邦领域的数据泄露通知立法，尽管囿于政治体制等问题，迟迟没能制定一部综合性法律，但其在金融等领域的单行立法同样值得称道。总体而言，至少有以下三点值得借鉴。

其一，遵循利益平衡的价值理念。人类的思想是不断丰富的，价值目标的多元状态是在人类社会的进步发展中形成的[14]588，法的制定或修改，是协调多方利益、平衡多种价值的复杂过程。[15]数据泄露对公民个人利益、企业经营管理、社会秩序稳定构成了多重危害。窃取个人信息的犯罪行为，首要侵害的是普通公民的财产、隐私等合法权益，同时也会对信息控制主体的经营管理以及社会秩序的稳定构成损害。个人信息泄露通知制度的目的，是通过课予个人信息处理者一定的通知义务，保护公民的信息权益和社会秩序稳定。但是，如果将通知义务不当扩大、启动条件过度放宽，就会使个人信息处理者承担过重的人力、物力、财力成本，有违公平原则，还有可能造成公民和监管机构被大量泄露通知“淹没”，最终不利于减少数据泄露造成的损失。综观美国联邦医疗健康、金融等领域的泄露通知规范，可以清晰地发现其遵循以保护公民权益为首要目标、兼及企业经营和监管需要的价值理念。为保护公民利益，法规对个人信息处理者的迅速通知义务、有效通知方式、简明通知内容等作出了硬性规定；为维护个人信息处理者利益，允许其在通知前进行风险评估，在通知人数过多时选择替代通知方式等；为保障监管需要，对个人信息处理者向监管机构报告数据泄露事件的义务设置了明确要求。

其二，根据社会发展不断调整完善。法律是调整社会关系的规范，由于社会关系总是处于变动和发展中，而且“社会变化，从典型意义上讲，要比法律变化快”[16]20，这就要求立法者不断通过修法来保持法律的生命力。综观美国联邦数据泄露通知立法，鲜明地体现出与时俱进、不断发展的特征。如在医疗健康领域，自 1996 年 HIPAA 法案公布后，相关的适用规范不断颁布实施，最终才在 2013 年形成较为完善的健康信息泄露通知规则。针对金融服务领域的个人信息保护，从 2001 年联邦机构联合出台指南要求金融机构制定信息安全计划，到 2005 年发布明确的数据泄露响应机制指南，同样是根据数据泄露形势变化作出的适时完善。

其三，个人信息泄露通知规则较完备。既然法律将数据泄露后的通知作为一项积极义务，那么需要明确的问题至少包括履行义务的主体、条件、时间、方式、对象以及未履行义务的后果。考察美国联邦系统个人信息泄露通知规范，无论是公共部门还是私营领域，均包含有基本定义、风险评估、通知内容、通知方式、通知时间、违规处罚等模块，为个人信息处理者提供了清晰明确的指引。另外，每一项规则在出台之前均经过广泛征求意见，反复调整修改，最终通过的规则在保证实现立法目的的前提下，能够保证现实可操作性。

六、美国联邦个人信息泄露通知制度对我国的借鉴意义

通过对美国联邦层面数据泄露通知立法的考察，可以为我国的法律建设提供一定的借鉴和参考。

（一）重视个人信息泄露通知的综合性立法工作

我国的个人信息保护和数据安全立法起步虽晚，却不存在美国式的体制性困境，因此个人信息（数据）泄露通知制度在近年来颁布的《民法典》《网络安全法》《数据安全法》《个人信息保护法》等综合性法律中得到了明确规定。但从实践层面来讲，由于法律条文数量稀少、规范内容原则含糊，诸如如何通知、何时通知等问题缺乏操作规程，实际上还是存在无法可依的问题。一旦出现大量数据泄露事故，各地为了实现治理法治化，就会选择出台地方性法规或条例，如此就陷入了美国式的困局，各地自行其是，企业莫衷一是。为此，国家应当提高对个人信息泄露通知制度综合性立法的重视程度，在《网络安全法》《个人信息保护法》等法律的解释文件中进一步细化数据泄露通知规则，或者出台专门的数据泄露通知法，确保实务操作有法可依。

（二）允许特定行业制定个人信息泄露通知规范

与美国情况相类似，在统一的个人信息泄露法律出台之前，我国一些掌握大量公民个人信息的行业已自行颁布了相关规范，以应对不断出现的信息泄露事件和日益严峻的数据安全形势。例如，中国人民银行 2011 年发布的《关于银行业金融机构做好个人金融信息保护工作的通知》提出，银行业金融机构发生个人金融信息泄露事件的，应当在事件发生之日起 7 个工作日内将相关情况及初步处理意见报告中国人民银行当地分支机构。[17]2013 年工业和信息化部

《电信和互联网用户个人信息保护管理规定》第14条要求，电信业务经营者、互联网信息服务提供者保管的用户个人信息发生或者可能发生泄露的，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向电信管理机构报告。[18]

在《个人信息保护法》《数据安全法》等综合性法律已经颁布的情况下，这些单行法规或部门规章是否还有保留的正当性和必要性？笔者认为答案是肯定的。一是因为《个人信息保护法》等法律中关于数据泄露通知的内容尚显粗疏，无法为金融机构、电信业务经营者等主体提供明确的操作指引，这一点与美国金融服务等行业立法的背景类似。再者，即便将来通过立法或司法解释的方式制定了统一的数据泄露通知规则，也不意味着行业立法就失了根基，毕竟虽然同为个人信息集中的领域，但金融、电信、医疗健康、保险等行业各有其特殊性，在信息类型、涵盖主体、处罚机制等方面难免有所不同。事实上，已经有部门在此方面采取了行动。例如，2020年9月中国人民银行发布了修订后的《中国人民银行金融消费者权益保护实施办法》，于第34条第2款增加了关于泄露通知的规定，要求银行以及支付机构应当在确认信息泄露可能危及金融消费者人身、财产安全时，立即向住所地的中国人民银行分支机构报告并告知金融消费者，可能造成其他不利影响的应在72小时以内报告中国人民银行分支机构。[19]

（三）构建系统明晰个人信息泄露通知规则体系

与美国联邦个人信息泄露通知规范相比，我国相关立法在结构完整性、语言明确性、立法统一性等方面存在不足。多部综合性立法往往只有关于信息处理者或网络运营者应当即时报告的原则性规定，除《个人信息保护法》中规定了通知内容、《数据安全法》中规定了通知方式外，诸如通知的触发条件、通知的时间、未及时通知的法律后果等内容均付之阙如。在具体行业领域，仅中国人民银行通过的《关于银行业金融机构做好个人金融信息保护工作的通知》《金融消费者权益保护实施办法》等规范性文件中，就使用过“客户信息”“个人金融信息”“消费者金融信息”等名称，其内容与国家市场监督管理总局、国家标准化管理委员会发布的《信息安全技术个人信息安全规范》中对金融信息保护对象的规定也不一致。

立法的粗疏和混乱可能使得信息控制者在遭遇网络安全事件后无所适从，不知如何通知受侵害的个体、通知哪些事项以及通知不到位可能面临何种处罚等。如此，既可能使涉事企业或机构承担了过大的成本，也可能为其怠于履责提供了借口，最终使消费者权益和国家利益遭受不必要的损失。参考美国立法，笔者认为首先应当坚定以保护信息主体利益为主、兼顾信息控制者利益的指导思想，在法律文本中对于个人信息、通知主体、通知对象等作出界定，明确通知义务的触发条件和风险评估标准，在通知较为困难或成本过高时允许信息控制者采取替代通知方式，对于怠于通知或拒不通知的应当明确法律后果，包括民事罚款甚至刑事追责等。

参考文献：

[1] Mark L. Krotoski, Lucy Wang, Jennifer S. Rosen. The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze [EB/OL]. https://www.morganlewis.com/-/media/files/publication/outside-publication/article/bna-need-to-repair-data-breach-notification-maze-08feb16.pdf, 2022-01-23.

[2] Chlotia Garrison & Clovia Hamilton. A Comparative Analysis of the EU GDPR to the US's Breach Notifications [J]. Information & Communications Technology Law, 2019, (1).

[3] Alicia Gilleskie. What Obama's Proposed Anti-Hacking Legislation Means for Entrepreneurs [EB/OL]. https://www.entrepreneur.com/article/242099, 2022-01-23.

[4] The President's Identity Theft Task Force. Combating Identity Theft: A Strategic Plan [EB/OL]. https://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf, 2022-01-15.

[5] Safeguarding Against and Responding to the Breach of Personally Identifiable Information [EB/OL]. https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-16.pdf, 2021-11-25.

[6] Health Insurance Portability and Accountability Act of 1996 [EB/OL]. https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996, 2021-12-05

[7] Carols Leyva. HIPAA Omnibus Rule Summary [EB/OL]. http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php, 2022-02-03.

[8] $475,000 Settlement for Delayed HIPAA Breach Notification [EB/OL]. https://www.hipaajournal.com/475000-settlement-delayed-hipaa-breach-notification-8640, 2022-02-18.

[9] Interagency Guidelines Establishing Information Security Standards [EB/OL]. https://www.federalregister.gov/docu-

ments/2001/02/01/01 - 1114/interagency - guidelines - establishing - standards - for - safeguarding - customer - information - and - rescission，2021 - 12 - 18.

[10] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice [EB/OL]. https://www.federalregister.gov/documents/2005/03/29/05 - 5980/interagency - guidance - on - response - programs - for - unauthorized - access - to - customer - information - and#footnote - 1 - p15736，2022 - 02 - 03.

[11] Cameron F. Kerry，etc. Bring the Gaps：A Path Forward to Federal Privacy Legislation [EB/OL]. https://www.brookings.edu/wp - content/uploads/2020/06/Bridging - the - gaps - a - path - forward - to - federal - privacylegislation.pdf，2021 - 12 - 18.

[12] 何旗. 论中国新型政党制度的优势与自信——基于美国政党政治的比较分析 [J]. 科学社会主义，2019，(1).

[13] Nine Biggest Data Breaches in Financial Services [EB/OL]. https://www.upguard.com/blog/biggest - data - breaches - financial - services，2022 - 02 - 15.

[14] 卓泽渊. 法的价值论 [M]. 北京：法律出版社，2006.

[15] 莫湘益. 法的价值表达与语言优化——以刑事诉讼法为域 [J]. 海峡法学，2011，(2).

[16] [美] E·博登海默. 法理学：法律哲学与法律方法 [M]. 邓正来译. 北京：中国政法大学出版社，2004.

[17] 人民银行关于银行业金融机构做好个人金融信息保护工作的通知 [EB/OL]. http://www.gov.cn/gongbao/content/2011/content_1918924.htm，2022 - 02 - 22.

[18] 电信和互联网用户个人信息保护规定 [EB/OL]. http://www.cac.gov.cn/2012 - 07/29/c_133142088.htm，2022 - 02 - 22.

[19] 中国人民银行金融消费者权益保护实施办法 [EB/OL]. http://www.pbc.gov.cn/tiaofasi/144941/144957/4099060/index.html，2022 - 02 - 22.

责任编辑：南　岭