

DOI:10.12154/j.qbzlgz.2021.05.008

日本开放政府数据中的隐私风险控制研究*

陈 美 (中南财经政法大学公共管理学院 武汉 430073)

梁乙凯 (山东财经大学管理科学与工程学院 济南 250014)

摘 要: [目的/意义]从隐私风险评估与防控的角度,调查日本政府开放数据的隐私保护实践,为我国政府开放数据和隐私保护提供参考。[方法/过程]利用文献调研和案例分析的研究方法,以日本为例,通过对文献资料和网站内容的调查,获取一手资料阐述日本政府开放数据中隐私风险控制的经验,对日本个人隐私保护法律体系、政府开放数据中个人隐私的评判标准、隐私风险应对的匿名化技术、隐私风险应对的机构与救济制度、隐私风险应对的安全控制措施与认证机制进行分析和概况。[结果/结论]制定统一的《个人信息保护法》,就个人隐私范围、保障措施等进行规范。在开放政府数据时,任命熟悉个人隐私保护的专家担任开放数据政策执行的管理者,以便于在各个阶段能针对隐私保护具有周全的考虑。另外,在开放数据前,应当先去除数据的可识别性,将相关数据匿名化,以避免对个人隐私的侵害。

关键词: 政府开放数据 隐私风险 日本

Research on Privacy Risk Control of Open Government Data in Japan

Chen Mei (School of Public Administration, Zhongnan University of Economics and Law, Wuhan, 430073)

Liang Yikai (School of Management Science and Engineering, Shandong University of Finance and Economics, Ji'nan, 250014)

Abstract: [Purpose/significance] From the perspective of privacy risk assessment and prevention control, this paper investigates the privacy protection practices of government open data in Japan, in order to provide a reference for the development of policy of open data in China. [Method/process] Using the research methods of literature review and case analysis, this paper takes Japan as an example, accesses to the first-hand materials from literature and discusses the experience of government open data privacy risk assessment and prevention in Japan, analyzes and summarizes the legal system of personal privacy protection in Japan, the judgment criteria of personal privacy in government open data, anonymization technology which respond to privacy risk and related posts, institutions that address and relief system which respond to privacy risk, security and control measures and authentication mechanism which respond to privacy risk. [Results/conclusion] This paper put forward to formulate a unified personal information protection law to regulate the scope of personal privacy and safeguard measures. When opening government data, experts familiar with personal privacy protection should be appointed as managers of the implementation of the open data policy so as to have comprehensive consideration on privacy protection at all stages. In addition, before opening data, the identifications of data should be removed and related data should be anonymized to avoid the infringement of personal privacy.

Keywords: government open data privacy risk Japan

*本文系国家自然科学基金“面向用户的开放政府数据使用行为机理及隐私风险控制研究”(批准号:72004056)的研究成果之一。

通过对开放数据进行利用,能够产生公共价值,但开放数据也意味着对个人隐私和自由产生新危险。通过国外对开放数据过程中公民基本权利保护的政策研究不难看出,作为公民基本人身权利的隐私权在数据开放过程中受到很大关注^[1]。从国内研究情况来看,有研究阐述日本开放政府数据的内容,并在此基础上总结日本开放政府数据的特点^[2],但尚无对日本开放政府数据中个人隐私保护进行研究。之所以选择日本作为案例研究,原因在于:一方面,日本的开放政府数据实践相对较好;另一方面,尽管有研究对美国、英国、法国等国的开放政府数据隐私保护进行分析,但较少对日本的开放政府数据隐私风险控制进行系统研究。因此,本文对日本个人隐私保护法律体系、日本政府数据开放中个人隐私的评判标准、隐私风险应对的匿名化技术、隐私风险应对的机构与救济制度、隐私风险应对的安全控制措施与认证机制来梳理理论和实践经验,旨在为我国政府开放数据和个人隐私保护提供借鉴。

1 日本个人隐私保护法律体系

在日本,个人隐私保护的主要制度是《个人信息保护法》(Act on the Protection of Personal Information, APPI)。《个人信息保护法》(2003第57号)^[3]最初在2003年完成,并于2005年4月开始执行。2015年,日本国会通过《个人信息保护法》的第一个修正案。从法律的具体文本来看,《个人信息保护法》主要内容如下:第I章为总则(第1至3条);第II章为国家及地方政府的责任义务等(第4至6条);第III章为个人信息保护的相关措施等(第7至14条);第IV章为个人信息处理运营者的义务等(第15至58条);第V章为个人信息保护委员会(Information Protection Commission)(第59至74条);第VI章为其它规定(第75至81条);第VII章为罚款规定(第82至88条)^[4]。在完成这个法律后,日本将《行政机构个人信息保护法》修订为《行政机构所持有个人信息保护法》(2003第58号)^[5],而且重新制定《独立行政机构等持有个人信息保

护法》(2003第59号)^[6]。2013年5月26日,日本通过《行政程序中为识别特定个人的编号利用法》(My Number Law, 2013年第27号法)^[7],并于2015年10月正式生效。这些法律构成日本个人信息保护法律体系(见图1)。“#1”为《个人信息保护法》,其第1章至第3章涉及国家及地方公共团体的义务、政策基本方针的制定等;第4章至第6章涉及个人信息处理业务运营者的义务。“#2”为《行政机构所持有个人信息保护法》,其规制对象为国家行政机关。“#3”为《独立行政机构等持有个人信息保护法》,其规制对象为独立行政机构等。“#4”为各地方公共团体的个人信息保护条例,针对地方公共团体等进行规制。

除上述个人隐私保护法律以外,日本还存在一些针对特定行业的特别隐私保护规范。在通信隐私方面,根据《电信业务法》(Telecommunications Business Act)第4条,任何人不得违反电信运营商所处理的通信的隐私;从事电信业务的人会在办公室内针对电信运营商处理的通信而获得隐私信息,但这些人不得对这些隐私进行披露,而且即使这些人离开办公室,也应适用同样的规定^[9]。在电子邮件方面,《特定电子邮件传输规范法》在2008年12月1日生效,通过电子邮件规范未经请求的营销。根据该法第2条,发送营销电子邮件的条件包括:得到收件人请求或同意;收件人是从事与其广告有关的销售活动有业务关系的人^[10]。在商业交易方面,《特定商业交易法》^[11]通过电子邮件规定了包括

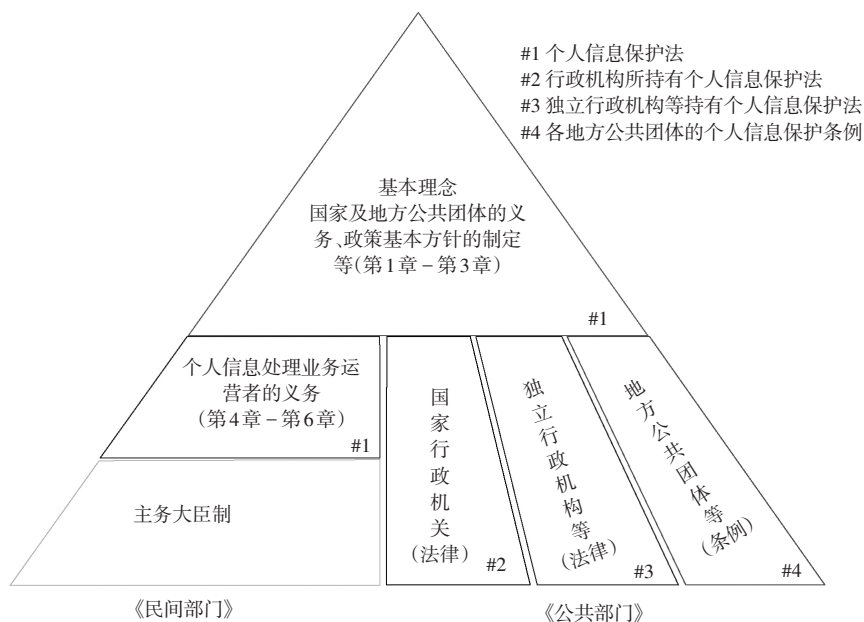


图1 日本个人信息保护法律体系^[8]

主动营销在内的其它形式未经请求的营销,而且需要得到营销对象的同意。

2 日本政府数据开放中个人隐私的评判标准

2.1 个人隐私界定

2.1.1 个人信息的定义

在个人隐私的具体保护范围上,大多数国家对于个人隐私的界定与保护都十分宽泛,在法律中仅以“个人敏感数据”或“个人信息”一言以蔽之,而少数国家,例如挪威、希腊和乌克兰等国则对所纳入保护的个人信息有较明确的定义^[12]。就日本而言,根据《个人信息保护法》第2条,“个人信息”是关于活着个体的信息,可以通过包含在这一信息中的姓名、出生日期或其它方式识别特定的个体;个人信息包括那些“容易参考其它信息”而能识别特定个人的信息。根据个人信息保护委员会发布的指南《在促进个人数据利用与消费者信任之间进行平衡》^[13]，“容易参考其它信息”是指业务运营者可以通过在正常运营过程中采用的方法,容易地参考其它信息。如果一个运营者需要向另一个运营者查询以获取“其它信息”,而且对运营者来说,这样做很困难,那么这种情况不会被视作“容易参考其它信息”。

从以上界定可知,个人信息包括任何“个人识别码”。根据《个人信息保护法》第2条第1款,个人识别码是《个人信息保护法》所涉及的相关内阁命令中所指的特定数据类型,包括那些可识别特定个人的生物特征数据,或以唯一分配给个人的特定代码的形式存在的数据。这类代码的典型例子是护照号码或驾驶执照。根据2017年5月30日生效的《为执行<个人信息保护法>而进行的内阁法令修订》(Amendment to the Cabinet Order to Enforce the Act on the Protection of Personal Information),“个人识别码”包括代码、字符、字母、符号,包括两种代码类型:(1)能够识别一个特定个体的身体特征的代码被转变至数据中,这一数据被计算机提供而得到利用,包括DNA序列数据、脸部识别数据、虹膜图数据、声纹数据、步态图案数据、手掌/手指静脉模式数据和指纹/掌纹数据;(2)代码被分配给正在得到使用的服务当中,而这一服务提供给个人或卖给个人的商品,或这些都在发给个体的文件中得以说明,以便能够识别特定用户或购买者,如护照号码、基本养老金编号、司机的许可证号码、个人号码和国家健康保险号码^[14]。

2.1.2 敏感个人信息的定义

尽管《个人信息保护法》没有“敏感个人信息”这一

名称,但包含“特别照料的个人信息”(Special Care-Required Personal Information),符合“敏感个人信息”的概念。根据《个人信息保护法》第2条第3款,“特别照料的个人信息”包括关于一个人的种族、信仰、社会地位、病史、犯罪记录、因相关罪行而受到伤害的事实,以及可能导致该人受到歧视的任何其它信息;这些信息需要特别照料,以防止引起不公平的歧视、偏见或对当事人产生其它不利条件。此外,根据《为执行<个人信息保护法>而进行的内阁法令修订》第2条,“特别照料的个人信息”包括:肢体残疾、智力残疾、精神障碍、医学检查结果、特定健康指南、医疗护理、医药处方、刑事诉讼^[15]。在敏感个人信息的获取与传输方面,根据《个人信息保护法》第17条第2款,业务运营者需要得到数据主体的同意后,才能获得敏感信息;根据该法第23条第2款,不能基于“选择退出”选项来将敏感信息传输给第三方,而是需要获得数据主体的事先同意,才能将敏感信息传输给第三方。

2.2 开放数据政策中个人隐私保护

日本IT战略本部(IT Strategic Headquarters)于2012年7月发布《开放数据战略》(Open Government Data Strategy),在“III.基本指导”的“1.基本原则”中指出,开放数据的基本原则包括:(1)政府应积极释放公共数据;(2)公共数据应以机器可读的格式进行发布;(3)鼓励以商业目的或非商业目的来使用公共信息;(4)采取特定措施来促进及时发布公共数据,而且稳定积累结果。当根据这些基本原则来采取措施时,需要处理机密信息或个人信息^[16]。2016年12月,日本在通过的《促进对公共部门数据和私营部门数据进行利用的基本法》第11条规定,国家和地方公共实体应对其自身所拥有的公共和私营部门数据采取必要措施,使公民能够通过互联网或任何其它先进的信息和电信网络轻松使用这些数据,同时确保个人和公司的权益、国家安全等不受损害^[16]。在日本开放数据网站data.go.jp上,存在一个网站栏目“关于使用可用数据的通知说明”,其中第三条内容为:根据《行政机关持有的信息获取法》(1999年第42号法)和《行政机关所持有个人信息保护法》(2003年第58号法),本平台将妥善处理您输入的用于通知使用现有数据的电子邮件地址和其他信息^[17]。data.go.jp平台的隐私政策内容包括:基本立场、收集的信息范围、使用目的、限制使用和提供、安防措施、披露用户信息、适用范围、其它^[18]。

3 隐私风险应对的匿名化技术

3.1 匿名信息的定义及其认定标准

根据《个人信息保护法》第2条第9款,“匿名信息”涉及与个人相关的任何信息,而且这一个人的所有个人信息(即可以识别特定个人的信息,包括任何敏感信息)已被删除,而且不能通过采取相关执行规则和个人信息保护委员会发布的相关指南中规定的适当措施来恢复信息。这意味着,由于个人信息包括个人识别码,因而在考虑对信息进行匿名化之前,必须考虑移除这些个人识别码。2013年6月25日,日本发布的《个人数据利用与流通的研究会报告书》指出,匿名信息要满足三个原则,包括:(1)对该数据已采取适当的去识别化措施;(2)已对外声称,该去识别化的信息将不再会被重新识别;(3)向第三方提供匿名化信息时,以契约形式来禁止获取这个匿名化信息的获取方对该信息进行重新识别^[19]。

3.2 匿名处理信息生成方法

根据《个人信息保护法》第2条第9款,匿名处理信息是采取相关行动来对个人信息进行处理后,所得的无法识别特定个人且无法恢复个人信息的信息。为了应对隐私风险,需要对个人信息进行匿名处理,但基于利用目的限制原则,《个人信息保护法》第16条第1款规定:如果没有事先得到当事人同意,就不得超越达成特定利用目的的必要范围来进行个人信息处理。为了针对各个领域提供可参考的匿名处理方法,《个人信息保护法》第36条第1款规定,个人信息处理业务者在生成匿名处理信息时,应依照特定方法来进行个人信息的处理:为了让个人信息无法识别特定个人,而且无法对进行处理制作时所使用的个人信息进行恢复,以及达到个人信息保护规则规定的标准;《个人信息保护法》第53条规定,各个领域的匿名处理方法,可以针对民间认可的个人信息保护组织制定的《个人信息保护指南》来制定相应的指南。为了方便参考具体标准来进行操作,个人信息委员会在2016年10月发布的《个人信息保护相关法律指南(匿名处理信息篇)》的第19条指出,匿名处理信息生成方法的标准包括五个方面:(1)删除能识别特定个人的全部或部分描述(例如,姓名、住所等);删除将识别个人的全部符号(包括护照号码、健保号码等);(3)删除个人信息与其它个人信息链接的符号(例如,存有个人信息压缩文件的密码等);(4)删除特殊的描述(例如,年龄为116岁);(5)考虑到个人信息库中个

人信息与其它个人信息之间存在差异,因而可以采取适当措施(例如,为了不显示小学生的身高是170,用“身高为150以上”来模糊显示身高)^[20]。

3.3 匿名处理信息生成所承担的义务

在生成匿名处理信息时,匿名信息业务运营者以及获取匿名处理信息的运营者都要承担相应的义务。

(1)禁止识别义务。根据《个人信息保护法》第38条“禁止识别行为”,当匿名处理信息业务运营者在处理“匿名处理信息”时,不得为了识别特定个人而获取从个人信息中被删除的描述、个人识别码或关于处理方法的信息。根据《个人信息保护法》第36条第5款,个人信息处理业务运营者在创建匿名处理信息并由自身来处理这些匿名处理信息时,不得为识别出这些匿名处理信息的当事人而将这些匿名处理信息与其它信息进行组合和对比。

(2)公开匿名处理信息的义务。对于匿名处理信息处理业务者而言,根据《个人信息保护法》第36条第3款,个人信息处理业务运营者在制作匿名处理信息时,应根据个人信息保护委员会所发布的规则,向公众披露匿名处理信息中包含与个人有关的信息;根据《个人信息保护法》第36条第4款,个人信息处理业务经营者在制作匿名处理信息以及向第三方提供匿名处理信息时,应依据个人信息保护委员会所制定的规则,提前披露匿名处理信息中个人信息类别、提供方法以及对第三方明确所提供的信息是匿名处理信息。同样地,根据《个人信息保护法》第37条,获取匿名处理信息的运营者也承担相同的义务。

(3)安全维护义务。根据《个人信息保护法》第36条第6款,个人信息处理运营者在制作匿名处理信息时,不仅需要努力为匿名处理信息采取适当的安全控制行动,而且需要采取必要的行动来确保在处理匿名处理信息的投诉时得到适当处理,力求向公众披露这些措施的内容。同样地,根据《个人信息保护法》第39条,获取匿名处理信息的运营者也同样承担安全维护义务。

4 隐私风险应对的机构与救济制度

4.1 隐私风险应对的机构

如前所述,根据日本国会在2015年通过《个人信息保护法》的第一个修正案,一个新政府机构被创建,即个人信息保护委员会,其任务见下页图2。以下将就其设置理念、组成、职责、权限进行阐述。

4.1.1 机构设置理念

2019年2月5日,个人信息保护委员会发布的《设置个人信息保护委员会的设置理念》指出,个人信息保护委员会的设置理念包括:(1)对个人数据周围情况变化进行适当地反应;(2)能够准确掌握个人信息处理情况并进行监督,并且进行灵活应对;(3)促进形成安全、自由的个人数据流通的全球倡议;(4)努力确保特定个人信息的安全性;(5)向各种主体发送容易理解的信息;(6)完善体系,从而可以更灵活地应对尖端技术和国际协作^[22]。

4.1.2 机构组成

根据《个人信息保护法》第63条,个人信息保护委员会由1名委员长及7名委员组成;其中4人为兼任委员;委员及委员长需要得到日本参议院和众议院同意后,由日本首相任命。在委员组成方面,应当具有如下成员:对个人信息保护及个人信息利用具有学术经历者;对消费者保护具有充分知识和经验者;对信息处理技术具有学术经历者;对公共行政领域利用特定个人信息具有学术经历者;对民间企业实践具有充足知识和经历者;联合组织(为《地方自治法》第263-3条第1款所称的联合组织)所推荐者。

4.1.3 机构职责

依《个人信息保护法》第61条,个人信息保护委员会所负责的事项包括:(1)基本政策的制定与推进的相关事务;(2)个人信息及匿名处理信息处理的监督,对提出的申诉进行必要的调解,以及与业务运营者进行合作;(3)与民间认可的个人信息保护组织的相关事项;(4)针对特定个人信息处理进行监视和监督,以及对当事人所提出的申诉进行必要的调解,并为业务运营者提供合作;(5)特定个人信息保护评估相关的事务;(6)针对个人信息的适当、有效应用以及个人信息保护开展启蒙教育;(7)对实施如前所述的六项事务进行必要的调查及研究;(8)与所管辖事务的国际合作有关的事项;(9)除前述事项外的其它依法属于个人信息保护委员会的事务。

4.1.4 机构权限

第一,提交报告以及检查。根据《个人数据保护法》第40条第1款,个人信息保护委员会在前二节及本节规定执行的必要范围内,就个人信息处理业务者或匿名处理信息处理业务者在关于个人信息或匿名处理信息的处理事宜,应当要求提出必要的报告或提供相关数据,或使其职员进入该个人信息处理业务者或其它的处所,质问有关个人信息等处理事宜,或检查账本、书类、文件

《行政程序中为识别特定个人的编号利用法》
《行政程序中为识别特定个人的编号利用法》为内阁所管

【《个人信息保护法》】
《个人信息保护法》为个人信息保护委员会所管

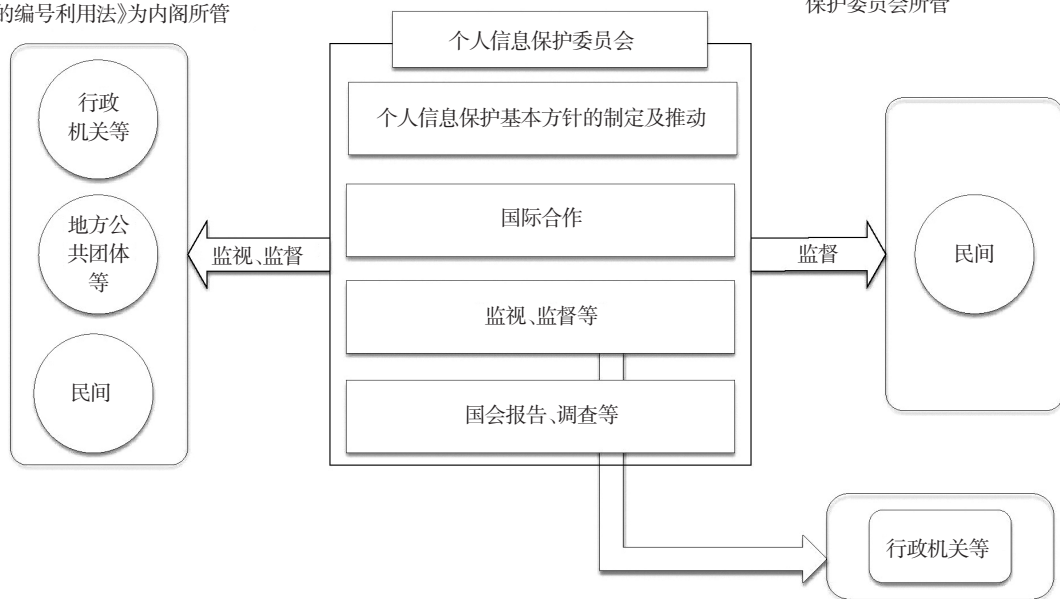


图2 个人信息保护委员会的任务^[21]

及其它对象;上述检查行为并非犯罪调查。

第二,指导或建议。根据《个人信息保护法》第41条,个人信息保护委员可以为个人信息处理业务者或匿名处理信息处理业务者就个人信息处理事项提供指导及建议。

第三,劝告及命令。根据《个人信息保护法》第42条第1款,当信息处理业务者存在违反本法第16条至18条、第20条至第22条、第23条(不含第4款)、第24条至第26条(不含第2款)、第27条、第28条(不含第1款)、第29条第2款或第3款、第30条第2款、第4款或第5款、第33条第2款;或匿名处理信息处理业务者违反第32条第2款、第36条(不含第6款)、第37条、第38条时,如果个人信息保护委员会认为有必要保护个人权力和利益,那么个人信息保护委员会可以劝告其采取改正或中止该当违法行为的必要措施。根据第42条第2款,如果依照前述规定的接受劝告者没有正当理由而没有采取关于其劝告措施,而且被认为对个人重大权益有紧迫侵害时,那么个人信息保护委员会要命令其采取有关劝告的措施。根据《个人信息保护法》第42条第3款,如果个人信息处理业务者或匿名处理信息处理业务者违反本法第16条、17条、第20条至22条、第23条第1款、第24条、第36条第1款、第2款或第5款、第38条,而且被认为存在侵害个人重大权益的事实,如果有必要采取紧急措施,应直接命令这个个人信息处理业务者采取中止或改正违法行为的必要措施。如果违反这条命令,会依照第84条进行惩罚。依据《个人信息保护法》第84条,如果业务运营商处理个人信息时,

不符合个人信息保护委员会的命令,将被处以最多6个月的监禁或罚款最高30万日元;根据《个人信息保护法》第85条,如果处理个人信息的业务运营商未提交报告,或属于虚假报告或提供虚假信息,将被处以最高30万日元的罚款。根据《个人信息保护法》第83条,为了谋求自身或任何第三方利益而未经授权披露个人信息,那么将受到最高1年监禁或最高50万日元罚款。针对这一条款中的罚款问题,第《个人信息保护法》87条规定,如果披露方是一个实体,那么受此处罚的各方将是相关官员、代表或负责披露的管理人员以及被审计单位,而且应缴纳上述罚款。

4.2 隐私风险应对的救济制度

日本具有完善的救济制度来应对隐私风险(见图3):一方面,如果出现不正当的个人信息处理及利用,应当向“个人信息处理业务运营者”或“个人信息保护团体”或“地方公共团体的国民生活中心”来进行申诉;另一方面,作为独立的监督机关,个人信息保护委员会具有报告、劝告、命令等权限。

在这个救济程序中,个人信息保护委员会是中立和独立的,它有能力执行《个人信息保护法》。但是,它只有权执行审计并发布停止和停止命令,但无权征收行政罚款。

5 隐私风险应对的安全控制措施与认证机制

5.1 隐私风险应对的安全控制措施

《个人信息保护法》没有条款规定是否任命隐私保护官或数据保护官,但第20条规定,个人信息处理业务

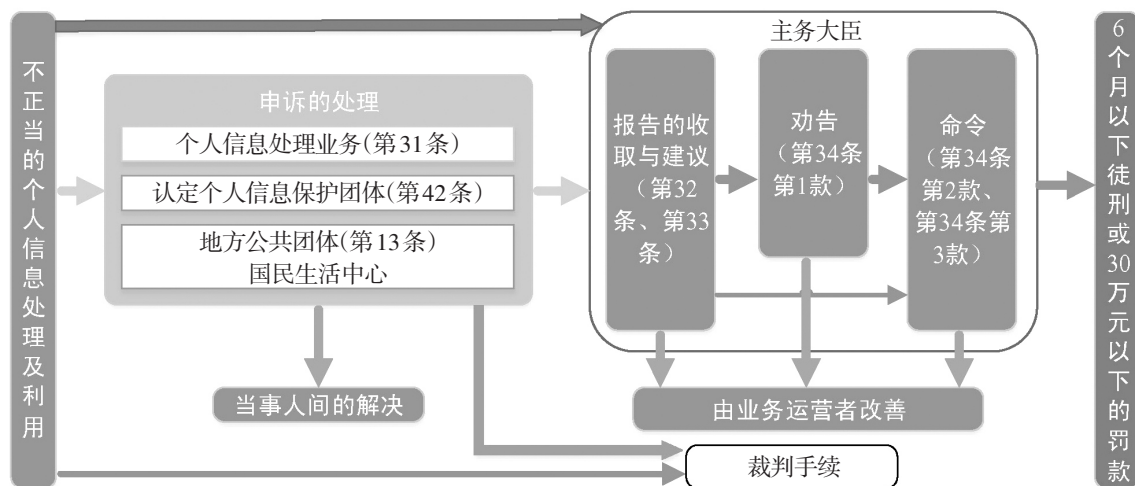


图3 日本个人信息保护的救济程序^[8]

运营者应当采取必要和适当的措施来对个人数据进行安全控制,防止其处理的个人数据中出现个人信息泄露、丢失或毁损。尽管《个人数据保护法》没有规定必须采取的具体步骤,但根据个人信息保护委员会发布的《金融领域个人信息保护指南》的第10条“安全控制措施”^[23]指出,本条与《个人信息保护法》第20条相关,建议业务运营商应采取所建议的步骤,以确保个人数据安全,这些必要和适当的措施通常包括:系统安全控制措施、人身安全控制措施、物理安全措施和技术安全控制措施。从具体内容来看,《金融领域个人信息保护指南》包含一些具体步骤或示例,受该指南所约束的实体必须针对每个安全控制措施来进行参考,如制定与安全措施有关的内部指南、与那些能获取个人数据的雇员签订非披露协议、保护机器和设备、制定能够应对数据泄露的框架。

5.2 隐私风险应对的认证机制

在日本,运营者可以使用“隐私标章”(privacy mark)来表明其符合相关法律和日本工业标准(JIS Q 15001:2006)。JIS Q 15001:2006^[24]包括两个部分内容。第一部分为《個人情報保護マネジメントシステム作成指針》,对个人信息保护管理体系构建指南进行规范。第二部分为《個人情報保護マネジメントシステム一要求事項》,又分为:(1)适用范围;(2)术语和定义;(3)要求。它规定,拥有个人信息的企业必须安全地管理个人信息,并采取措施避免损坏、破坏、篡改和泄漏等个人信息,并且不会对此造成任何不利影响。JIS Q 15001:2006以PDCA循环为基础,构建技术与组织维度的必要措施。总体来看,与个人信息保护法相关的标准有BS 10012、TPIPAS、JIS-Q-15001:2006等,但日本的JIS-Q-15001:2006规范相对比较严谨。JIS-Q-15001:2006由日本信息处理发展中心设立,虽然它不是法律,但它在某些方面比日本《个人信息保护法》提供了更高水平的标准。

6 总结与借鉴

为了更能顺畅的推动开放数据,日本很重视个人隐私保护问题。特别是在美国的影响下,日本将信息安全,特别是网络安全提升至国家战略高度^[25]。它的主要经验包括:积极制定与修订《个人信息保护法》;在政策方面,日本开放数据政策要求政府部门根据开放数据基本原则来进行开放数据的同时,强调处理机密信息与隐私信息问题;在匿名化方面,明确匿名处理信息

生成、利用时应遵守的义务,建议采用数据集匿名的方式,将可识别的个人数据模糊化或分离;明确设置个人数据保护委员会,负责去识别化数据的监管及配套措施的制定和执行;在救济方面,如果个人信息保护委员会发现任何违反或可能违反《个人信息保护法》的行为,可以要求业务运营商提交报告、进行现场检查以及要求或质问有关个人数据,或命令处理信息的人员采取补救措施;在机制方面,通过认证机制来让企业进行审查,通过给予认证的隐私标章来减缓用户对于开放数据应用的障碍。

政府数据中包含公民的个人数据,在执行开放数据政策的过程中,不可避免地涉及个人隐私保护问题。为了降低这个障碍,日本通过提供操作指南、改善法律与匿名化技术、隐私保护认证的方式,从而降低负面影响。就我国而言,2017年5月27日,在国家发改委、工信部、国家互联网信息办公室、贵州省人民政府共同主办的2017中国国际大数据产业博览会上,“数据开放与隐私保护”高峰论坛得到举行,旨在探讨面临数据开放的挑战,如何探隐私风险,究法治路径^[26];2019年5月26日至29日,2019中国国际大数据产业博览会举办了49场论坛,围绕“数字经济、技术创新、融合发展、数据安全、合作交流”五大版块设置不同主题^[27]。然而,我国当前并没有针对个人隐私的一部完整法律,而是分散于各个法律当中。因此,可以借鉴日本的做法,在如下方面进行完善:(1)在法律层面,制定专门的《个人信息保护法》,就个人隐私范围、保障措施等进行规范。例如,建立数据隐私与信用等级联动制度,一旦发现组织或个人存在恶意泄露数据隐私的行为就降低其信用等级,并在全中国信用公示系统里予以公示,从而使信用等级可以真正发挥遏制泄露隐私数据行为的作用^[28]。(2)在匿名化层面,在开放数据前,应当先去除数据的可识别性,将相关数据匿名化,以避免对个人隐私的侵害。(3)在救济层面,我国并没有《宪法》上权利的救济途径,但可以让数据主体向相应组织咨询有关开放政府数据中侵犯个人信息的损害赔偿。同时,如果因开放政府数据负责人的数据处置或遗漏而要求信息主体更正、删除、暂停处理数据等,则按照相应规定要求进行行政处罚。在开放政府数据时,任命熟悉个人隐私保护的专家担任开放数据政策执行的管理者,以便于在各个阶段能针对隐私保护具有周全的考虑。(4)在认证机制层面,加大开放政府数据网站的认证,如美国开放政府数据网站Data.gov已获得美国总务管理局

(GSA)所颁发的认证(C&A)。政府数据开放平台运营者可以使用类似日本的“隐私标章”(privacy mark)来表明其政府数据开放符合相关法律法规和个人信息保护行业标准,从而能对开放政府数据进行隐私安全审查。

参考文献

- [1] 马海群, 蒲攀. 国内外开放数据政策研究现状分析及我国研究动向研判[J]. 中国图书馆学报, 2015(5):76-86.
- [2] 陈美. 日本开放政府数据分析及对我国的启示[J]. 图书馆, 2018(6):8-14.
- [3] Act on the Protection of Personal Information Act No. 57 of (2003) [EB/OL].[2019-05-21].<http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>.
- [4] Amended Act on the Protection of Personal Information[EB/OL].[2019-05-24].https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.
- [5] Act on the Protection of Personal Information Held by Administrative Organs (Act No. 58 of 2003) [EB/OL].[2019-05-25].<http://www.cas.go.jp/jp/seisaku/hourei/data/APPIHAO.pdf>.
- [6] Act on the Protection of Personal Information Held by Incorporated Administrative Agencies[EB/OL].[2019-05-27].http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&ia=03&vm=02&id=3264.
- [7] Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures[EB/OL].[2019-06-11].http://www.japaneselawtranslation.go.jp/law/detail_main?re=2&vm=02&id=2755.
- [8] よくわかる個人情報保護のしくみ?改訂版? 消費者庁 - 日本病院会[EB/OL].[2019-06-11].https://www.hospital.or.jp/pdf/01_20130301_01.pdf.
- [9] Telecommunications Business Act[EB/OL].[2019-09-11].http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=02&id=2859.
- [10] Act on Regulation of Transmission of Specified Electronic Mail [EB/OL].[2019-06-18].<http://www.cas.go.jp/jp/seisaku/hourei/data/ACPT.pdf>.
- [11] Act on Specified Commercial Transactions[EB/OL].[2019-08-21].http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&ia=03&vm=02&id=2065.
- [12] 周庆山, 蒋天骥. 欧洲各国政府信息公开法中的豁免公开范围比较分析[J]. 现代情报, 2017(12):10-18.
- [13] パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて[EB/OL].[2019-12-01].https://www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf.
- [14] Amendment to the Cabinet Order to Enforce the Act on the Protection of Personal Information[EB/OL].[2019-07-11].http://www.ppc.go.jp/files/pdf/Cabinet_Order.pdf.
- [15] Open Government Data Strategy[EB/OL].[2019-11-21].<http://japan.kantei.go.jp/policy/it/20120704/text.pdf>.
- [16] 官民データ活用推進基本法[EB/OL].[2019-09-21].http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&vm=04&id=2975.
- [17] 掲載データ利用の御連絡にあたっての留意事項[EB/OL].[2019-12-02].<https://www.data.go.jp/attention-for-use/?lang=japanese>.
- [18] プライバシーポリシーについて[EB/OL].[2019-10-02].<https://www.data.go.jp/privacy-policy/?lang=japanese>.
- [19] パーソナルデータの利用?流通に関する研究会報告書[EB/OL].[2019-08-02].http://www.soumu.go.jp/main_content/000231357.pdf.
- [20] 個人情報の保護に関する法律についてのガイドライン(匿名処理情報編)[EB/OL].[2019-08-08].<https://www.ppc.go.jp/files/pdf/guidelines04.pdf>.
- [21] 個人情報保護委員会について[EB/OL].[2019-08-08].<http://www.ppc.go.jp/aboutus/commission/>.
- [22] 個人情報保護委員会の組織理念~個人情報を取り巻く環境変化に機敏に対応~[EB/OL].[2019-08-08].<https://www.ppc.go.jp/files/pdf/soshikirinen.pdf>.
- [23] Guidelines for Personal Information Protection in the Financial Field[EB/OL].[2020-04-18].https://www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf.
- [24] JIS Q 15001:2006をベースにした個人情報保護... - プライバシーマーク[EB/OL].[2019-08-18].https://privacymark.jp/system/guideline/pdf/guideline_V2_180410.pdf.
- [25] 相丽玲, 陈梦婕. 试析中外信息安全保障体系的演化路径[J]. 中国图书馆学报, 2018(2):113-131.
- [26] 聚焦·大数据 | 专家学者共话“数据开放与隐私保护”[EB/OL].[2020-05-02].http://mp.weixin.qq.com/s?__biz=MjM5MDMyMjEyMQ==&mid=2652295991&idx=1&sn=fccae304ab70ccdc4280d6577215cc8&chksm=bd2ef9918a597087f7031f4ed8b9882923b79ce22803bf2016d819fa1ed325922fcee0355e48&mpshare=1&scene=23&srcid=0612gWXyoV6CsqzImnxTDGHQ#rd.
- [27] 2019中国国际大数据产业博览会5月26日至29日在贵阳举行[EB/OL].[2020-03-18].http://www.gywb.cn/content/2019-02/26/content_6027289.htm.
- [28] 朱晓峰, 黄晓婷, 吴志祥. 基于种群演化的政府数据开放实证研究[J]. 情报科学, 2020(7):123-131.

【作者简介】陈美,男,1987年生,中南财经政法大学公共管理学院副教授。

梁乙凯,男,1986年生,山东财经大学管理科学与工程学院副教授。

收稿日期:2021-04-29