

· 信息技术 ·

# 中外个人数据安全风险比较 ——基于金融交易情景的个人数据保护分析

杨光<sup>1</sup> 宋婧<sup>2</sup>

(1. 山西大学 图书馆, 山西 太原 030006; 2. 山西大学 经济与管理学院, 山西 太原 030006)

**摘要:** 信息时代改变了早期复杂繁琐的工作方式, 创新出更多便捷的个性化服务。但暴露于危险系数极高的互联网环境下的个人数据有着令人堪忧的安全隐患。其中, 最为关键的是金融个人数据, 它涉及个人的财务和资产分布情况, 如果泄露将给个人造成难以估量的损失。本文采取文献调研法和比较研究法从适用范围、个人数据获取及数据保护官等视角对美国、日本、欧盟针对个人数据保护的相关法律法规进行比较分析。发现我国在金融交易情景下的个人数据保护存在相关立法起步晚、内容过于笼统并且数据主体的自我保护意识比较单薄等问题。我国应在完善相关立法的同时加强数据主体的自我保护意识。

**关键词:** 数据安全; 个人数据; 数据交易

中图分类号: G203; D91

文献标识码: A

文章编号: 1004 - 1680(2020)05 - 0008 - 09

## 1 背景及相关概念

互联网的出现更新了金融机构的交易支付方式, 金融机构利用网络技术摆脱了地理空间的阻碍, 实现了没有地域限制的线上交易。近年来, 随着淘宝和苏宁易购等电商平台的崛起, 人们可以通过线上商店购买相对满意的商品, 这极大地促进了金融业的线上发展。线上金融在与人方便的同时, 安全隐患也随之而来。

### 1.1 相关定义

#### 1.1.1 个人数据

目前, 对于个人数据并没有统一的定义, 多数是引用相关法律法规中的定义。虽然表述不同, 但学者们普遍认为个人数据相比其他数据最大的区别是可以通过个人数据精准定位到某个人, 从而将其从人群中识别出来<sup>[1]</sup>。因此, 综合国内外研究可以将个人数据定义为: 可以识别出数据主体本人的数据。这种“识别说”也符合多国对个人数据的界定思路<sup>[2]</sup>。

#### 1.1.2 金融数据

金融数据指在各项金融活动中产生的数据, 它除了拥有一般数据的特点之外, 还具有真实性、可靠性、广泛性和综合性的特点。将其按照业务活动可分为银行业务数据、证券业务数据、保险业务数据和信托咨询等业务数据。从数据的来源和内容上则将其划分为来自市场的数据和来自全社会的数据<sup>[3]</sup>。

#### 1.1.3 金融交易

金融交易是在机构单位中金融资产所有权变化的所有交易。金融交易的本质就是资金流的交换<sup>[4]</sup>。

## 1.2 金融交易中的个人数据安全隐患

由于个人金融数据涉及个人财务情况, 如果处理不当, 将会给个人隐私和数据安全造成不堪设想的后果。个人金融数据涉及的数据主体、金融机构和整个交易环节都处于具有安全隐患的环境中。

### 1.2.1 数据主体的安全意识淡薄

数据主体对于个人数据的安全防范意识不强,

收稿日期: 2020 - 02 - 24

作者简介: 杨光(1977 -), 女, 博士, 山西大学图书馆研究馆员, 研究方向为信息法律与知识管理。E-mail: sunnysxu@126.com

通讯作者: 宋婧(1992 -), 女, 山西大学经济与管理学院图书馆学在读研究生, 研究方向为信息法律与知识管理。E-mail: 535502907@qq.com

引文格式: 杨光, 宋婧. 中外个人数据安全风险比较——基于金融交易情景的个人数据保护分析[J]. 晋图学刊, 2020(5): 8 - 16.

导致金融机构超出其使用目的地收集相关个人数据,还令窃取个人数据的不法分子有机可趁,例如:数据主体在网络活动中无意留下的姓名、职业、手机联系方式等一系列个人数据都会埋下被盗取、篡改的安全隐患;在使用各类APP时,用户只有同意APP获取用户的位置、相册、通讯录等数据才可以继续使用。多数用户在使用应用软件时,对APP访问个人数据并不在意,同样为个人数据泄露造成风险。只有数据主体重视对其数据的保护,才能守好保护个人数据安全的第一道防线。

### 1.2.2 金融机构缺乏严格管理和有效的保护技术

我国银行、保险、证券等金融行业遵守各自的行业规范,缺乏统一的管理规范<sup>[5]</sup>,需完善针对个人金融数据的监管机制与法律制度建设。更值得关注的是金融机构为了营销和市场竞争而超出其数据使用目的的过度数据收集,造成数据主体的隐私泄露。例如:一些手机银行软件会获取用户的定位和语音权限以监听用户。其次,由于金融机构内部管理不严格,个别金融机构的工作人员,以工作之便为一己私利在未经客户授权或未告知客户情况下,将用户的个人数据非法售卖给第三方,造成数据泄露。生活中可以见到这样的情况:当消费者购买汽车后,随之而来的是一系列汽车保险公司的推销电话和广告信息。最后,由于整个金融业的数据安全保护技术不高,黑客等不法分子能够轻易窃取用户账号密码,篡改用户交易数据进行网络诈骗<sup>[6]</sup>。

### 1.2.3 网络攻击

个人数据在传播过程中也存在风险。由于数据传输主要通过HTTP等协议来实现,不法分子会利用这些协议编码共同存在的不可避免的安全漏洞破坏和篡改数据或者利用各种欺诈手段,截获或盗取金融交易中的数据造成用户财产损失<sup>[7]</sup>。此外,网络购物盛行,使得个人的购买偏好、财务情况和信用状况都会在互联网环境中留下印记,可能被未知的第三方所获取,对用户的个人数据和财产安全构成威胁。

总体看来,网络诈骗行为与传统的诈骗相比,具有技术水平高、匿名性强和防御难度高的特点<sup>[8]</sup>。

## 2 各国对于个人金融数据的保护现状及其必要性

### 2.1 各国对于个人金融数据的保护现状

在美国,有两部针对金融领域的专门法《公平信用报告法》(1970年版,下文采用相同版本)和

《金融服务现代化法》(1999年版,下文采用相同版本)。《公平信用报告法》旨在规范信用机构在收集和获取个人信用数据并生成信用报告时,遵循公平、准确并保护个人隐私的原则。为防止消费者因不真实的信用报告而遭受损失,该报告规定了报告使用人的义务、报告使用条件与范围以及信用报告机构的权利义务。《金融服务现代化法》的立法理念除了在于加强金融业良性竞争外,也强调保护个人非公开信息的重要性<sup>[5]</sup>。我国和日本规范金融机构收集、处理和运用个人数据的法律可以分别参见我国的《网络安全法》(2017年版,下文采用相同版本)和《信息安全技术个人信息安全规范》(2017年版,下文采用相同版本),以及日本的《个人信息保护法》(2017年版,下文采用相同版本)。日本《个人信息保护法》是目前日本政府针对个人信息处理的主要法案<sup>[9]</sup>。

此外,欧盟于2018年5月25日为保护个人数据出台的《通用数据保护条例》(即《GDPR》)更加详尽,可操作性更强。

### 2.2 金融个人数据保护的必要性

数据可以产生巨大商业价值,它和金融业的融合产生了新型的线上金融服务形式。由于金融个人数据具有财产属性,电子银行和移动支付等在线虚拟交易更容易造成数据篡改、交易信息泄露和网络支付安全等问题<sup>[10]</sup>。金融交易中,金融消费者相比金融机构而言对日益复杂的金融产品所掌握的信息不够全面而处于弱势地位,其个人数据更易受到泄露、滥用的威胁<sup>[11]</sup>。最后,由于金融业与网络的融合使得消费者的个人数据在互联网上更容易被不法分子盗取,严重危及金融消费者的财产安全。互联网时代,金融消费者的个人数据正面临着前所未有的威胁。我国现行的数据保护法律法规还不完善,给一些数据控制者和处理者以可乘之机<sup>[12]</sup>。因此必须采取立法等措施保护金融消费者的数据安全。

## 3 各国金融数据相关法律对个人数据保护的对比分析

数据利用以获取为前提,作为数据主体是否知晓自己的数据被收集,而数据的收集者是否要在经过数据主体同意情况下才能利用其数据;当数据委托给第三方时,委托者和被委托者的工作也不同;专业的数据保护人员应该具备哪些基本素养,等等,都是需要探讨和分析的问题。本章将从个人数据的获

取方、数据委托的情况、数据保护专业人员、数据控制者和数据监管等角度进行对比分析。

### 3.1 适用范围

不同法律适用的范围不同。如前所述,《公平信用报告法》和《金融服务现代化法》是规范金融行业的专门法。《隐私权法》和《个人信息保护法》则重在规范政府行政部门行为。欧盟的《GDPR》则是规范整个欧盟成员国的个人数据安全的法律。本节将从法律规范所涉及的不同范围进行比较。

#### 3.1.1 行业适用范围

《公平信用报告法》主要针对信用报告机构进行行为规范,还适用于对出售、借贷和租赁历史记录的银行、信用合作社和代理机构进行行为规范,以及对任何基于信用报告信息进行招聘的企业进行行为规范。主要体现了信用信息公开、负面信息修复和个人隐私权的保护的思想。目的是维护消费者权益和金融市场公平竞争,为征信行业的规范操作提供法律依据。《金融服务现代化法》涉及了银行、证券和保险三大金融行业,并对其具体的运作流程做了具有可行性的规定和指导。旨在促进银行、证券和保险等行业之间联合经营,加强金融机构的竞争力<sup>[13]</sup>。其中,第五章明确规定了一种强制性和持续性的义务:金融机构必须谨慎处理个人非公开信息,尊重顾客的隐私权。

#### 3.1.2 政府适用范围

《隐私权法》是美国用以规范行政部门、军事部门等联邦政府机构收集、使用和公开个人数据的法律,还对个人数据的保密问题做了详细规定。

日本的《个人信息保护法》总体包含六章,前三章于 2003 年颁布实施,规定了国家及地方公共团体的义务等,属于基本法部分。2015 年,日本《个人信息保护法》修正案增加了第五章“个人信息保护委

员会”,新增章节规定了个人信息保护委员会的设置、所属、任务、管辖事务、委员身份保障或任期、义务等事项。此外,在适用中并没有包含媒体、宗教团体、政治团体和研究教育机构等,但也要求其制定自律性规定<sup>[14]</sup>。

我国《网络安全法》第八条规定:我国的网络安全工作及其相关监督管理是由国家网信部门负责的。县级以上人民政府有关部门的网络安全保护和监督管理职责,按照国家有关规定确定。

#### 3.1.3 地域适用范围

首先,经合组织和欧盟的成员国,都分别适用《关于隐私保护与个人资料跨国流通的指针的建议》(以下简称《建议》)和《GDPR》这两部法律规范。并且经合组织的《建议》适用于规范公共领域和私人领域的个人数据保护行为<sup>[15]</sup>。

其次,欧盟的《GDPR》的适用范围广泛。在欧盟内设立的控制者或处理者在处理个人数据时,无论其处理行为是否发生在欧盟境内都适用《GDPR》。即使处理者或控制者没有设立在欧盟境内,但其处理的数据主体在欧盟境内,也适用《GDPR》<sup>[16]</sup>。总之,与数据处理相关的数据主体、控制者或处理者只要有一类归属欧盟境内都适用《GDPR》。

我国《网络安全法》和日本的《个人信息保护法》都适用于各自国家境内,没有强调与境外衔接的部分。

#### 3.1.4 公共适用范围

日本的《个人信息保护法》后三章于 2005 年实施,是对企业法人等民间部门中的个人信息获得者的义务的规定,属于一般法部分<sup>[14]</sup>。我国《信息安全技术个人信息安全规范》指明:对个人信息和个人数据处理活动的监督、管理和评估不仅适用于各类组织,也适用于各监督部门和第三方评估机构。

对各国法律是否涉及以上范围总结如表 1 所示。

表 1 各国金融数据相关法律适用范围

Table 1 Application scope of financial data laws in various countries

法律	是否针对金融行业	是否涉及政府部门等	地域适用范围	是否涉及公共领域
《网络安全法》	否	是	中国	否
《信息安全技术个人信息安全规范》	否	否	中国	是
《公平信用报告法》	是	否	美国	否
《金融服务现代化法》	是	否	美国	否
《个人信息保护法》	否	是	日本	是
《GDPR》	否	否	欧盟成员国	否

### 3.2 个人数据获取及知悉情况

#### 3.2.1 个人数据获取

绝大部分个人数据保护相关法律在个人数据收集和使用环节中都赋予数据主体“同意权”。各国的法律法规各有特色。日本于2017年施行了新版的《个人信息保护法》,采用了“选择进入”(opt-in)和“选择退出”(opt-out)两个规则<sup>[17]</sup>。“选择进入”指数据的持有者需要取得数据主体同意后才能向第三方传输个人数据,并且数据主体有权拒绝。“选择退出”则相反,持有数据者默认数据主体同意其获得数据,不需要征得数据主体同意便可以向第三方传输个人数据,但数据主体有权要求停止这一操作。在本文提到的其他法律法规中,多数遵循“选择退出”的原则。《GDPR》的“同意权”不同于其他法律中“不反对即为同意”的条款规定,这里的“同意”是指数据主体自愿做出的具体、清晰、明确地对其相关的个人数据处理的意思表示。同样,我国《网络安全法》规定网络运营者收集用户数据时应当向用户明示并取得同意。日本《个人信息保护法》只规定“需注意的个人数据”必须事先取得用户同意,对于一般的个人数据则限制滥用,本质上属于默认同意的范畴。

对于个人数据的收集,各国安全规范都要求遵循目的明确和数据最小化原则,即:收集前要有明确的目的,且收集的个人信息范围不能超出初始使用目的或不能利用个人信息获得其他利益。此外,还要将利用目的及其收集的数据类型和内容告知数据主体,并采取适当合理的措施保护其收集到的个人信息。

美国《公平信用报告法》规定:除了数据主体和列入可许可访问名单上的机构外,其他人没有法律授权不可获得数据主体的信用报告。报告使用者要证明自己的身份以及所采取的合理合法程序来确保数据的收集和使用目的合法。若使用者无法提供上述证明,征信机构有权拒绝向使用者提供数据。信用报告影响着一个人信用业务的办理,征信机构仅仅收集制作信用报告并不协助报告使用者对消费者信用业务做出决定<sup>[18]</sup>。《公平信用报告法》规定报告中若含有不利于消费者行为的信息时,报告使用者应将做出的不利行为告知消费者,并告知提供该报告的机构名称、地址和电话。同时告知消费者这一不利行为并不是报告机构做出的,消费者有权提出异议。该法律既要维护征信行业公平有序,又要尊重数据主体的数据安全。相比之下,数据安全的

重视度较低,因为该法律没有对敏感数据进行界定,也没有设置禁止收集和使用敏感数据的相关条款。但对于信用报告的使用者的义务做了详细的规定。

不同于其他安全规范,我国《信息安全技术个人信息安全规范》对“收集频率”做出规定:为了实现产品或服务的业务功能,所收集的必需的个人的数据的频率应是最低频率。此外,当个人数据控制者目的达成后,应根据约定删除个人数据。

当数据的获取不是直接来自数据主体时,我国《信息安全技术个人信息安全规范》规定间接获取个人信息数量应是实现其使用目的所必需的最少数量,并且对被授权访问个人信息的内部数据操作人员,应按照最小授权的原则。被授权访问的数据操作人员所访问到的数据范围仅限于完成其职责所必需的最小范围。类似地,《GDPR》第4条规定:当控制者从第三方获得数据主体的个人数据时,应当向数据主体说明获得其数据的具体类型与内容。第9条和第10条又进一步对特殊种类个人数据的处理和有关刑事犯罪的罪犯的个人数据如何处理做了规定<sup>[19]</sup>。《公平信用报告法》提到报告的使用者是基于从征信机构以外的第三方得到的信用报告之外的(信用地位和一般声誉等)信息而否定了数据主体信用业务申请决定时,应清晰准确地告知当事人该信息的性质<sup>[20]</sup>。《金融服务现代化法》也对第三方的转送做了规定,一个公司向非分支机构第三方传送数据后,第三方不得将该数据转给他人<sup>[21]</sup>。这一规定有效地遏制了数据的转移,使按照规定不直接获取数据的公司也不能通过第三方间接获取。该法律的缺陷在于,仅仅监管向第三方的数据转送,并没有规制关联机构之间数据的转送行为。

对于儿童数据的收集,《GDPR》和我国《信息安全技术个人信息安全规范》分别对未满16周岁和未满14周岁的儿童数据的获取同意做了类似规定,即:都要征得其父母或监护人的明示同意才能获取。

#### 3.2.2 知悉情况

虽然各国法律规范都规定数据主体有权知道自己数据的被利用情况,例如:具体的数据类型、被利用的目的和范围等,但是美国对于这种知悉情况做了更详细的规定。

美国的三部法律都详细规定数据主体有权得到其数据记录的复制品。其中《公平信用报告法》和《金融服务现代化法》都对时间范围的知悉情况做了详细规定。《公平信用报告法》第604节指出,数据主体有权凭借身份证明免费获得其信用报告的副

本,并对报告内的错误数据提出异议。消费者还有权知道其信用报告在上一年度被哪些机构申请或申请了哪些数据等申请情况。

因为通知义务不同,《金融服务现代化法》还对客户和消费者作了区分<sup>[22]</sup>。要求金融机构在披露消费者的个人非公开数据前,要向个人发出“选择退出”和隐私政策等初始通知。一旦消费者经过交易成为客户后,金融机构必须每年提供其隐私政策的年度书面通知。初始通知的时间比较有弹性,凡在金融机构建立客户关系后的合理时间段内皆可,

并且同一客户持续取得金融服务时,除非隐私政策有变,否则不用重复通知。而年度通知则规定金融机构在客户关系存续期间,每年都要告知客户隐私政策及其执行情况。对于告知的内容,必须是可以合理理解和足以引起客户注意的信息。

《隐私权法》第四部分除了指出数据主体有权向行政机关得到其数据记录的复制品,还规定政府在收集数据和建立数据库时要发布公告。关于个人数据获取整理如表 2 所示。

表 2 个人数据获取  
Table 2 Personal data access

法律	个人数据获取	是否对儿童数据获取做出规定
《网络安全法》	需取得数据主体同意	否
《信息安全技术个人信息安全规范》	不反对即同意	是
《公平信用报告法》	不反对即同意	否
《金融服务现代化法》	不反对即同意	否
《个人信息保护法》	特殊数据须征得数据主体同意	否
《GDPR》	需获得数据主体明确同意	是

### 3.3 数据委托

数据委托是指个人数据获得者把个人数据的全部或部分委托给委托方。当数据被委托处理时,我国、日本和欧盟都做了详细规定。我国《信息安全技术个人信息安全规范》规定:委托处理个人信息时,个人信息控制者不得超出信息主体授权同意的范围,为保证受委托者具有足够的能力处理和保护数据,要对委托行为进行评估。当然,受委托者也要严格按照个人信息控制者的要求处理个人信息。

日本《个人信息保护法》第 22 条规定:当个人

信息获得者实行委托行为时,要安全管理委托出去的个人信息并对委托方进行监督。当个人信息获得者是从其他的信息获得者那继承实业而获得个人信息时,在事先没有取得本人同意情况下,超过了在继承前达成取得该个人信息必要范围的,不能取得该个人信息<sup>[14]</sup>。

《GDPR》第 27 条规定:当数据处理者没有设立在欧盟境内,处理者应当以书面形式在欧盟内指定其代理人。并且代理人应被控制者、监管机构和数据主体授权来处理所有相关问题。

各国法律的数据委托情况如表 3 所示。

表 3 数据委托  
Table 3 Data commission

法律	是否对数据委托情况做出规定
《网络安全法》	否
《信息安全技术个人信息安全规范》	是
《公平信用报告法》	否
《金融服务现代化法》	否
《个人信息保护法》	是
《GDPR》	是

### 3.4 数据保护人员的设立

在不同国家的安全规范中对数据保护人员的称呼不同,但就其职责来说,都是为了保护个人数据隐私,且有着举足轻重的地位。

《GDPR》对数据保护官(DPO)做了规定,在第 37 条、第 38 条和第 39 条中不仅规定了需要指派数据保护人员的情况还指明数据保护人员的地位和任务。并根据 DPO 是否属于数据控制者的员工将其分为内部 DPO 和外部 DPO<sup>[23]</sup>。内部 DPO 是数据控制者的员工,对数据控制者内部的基本操作比较熟悉,但数据保护的知识和经验不足。外部 DPO 专业性强,基于合同向数据控制者履行职责。GDPR 第 37 条规定,DPO 不仅要掌握《GDPR》,还要掌握其他与数据保护相关的欧盟法规和成员国法律。此外,DPO 作为数据控制者与数据主体、数据保护监管机构的沟通媒介也要具备强大的语言表达能力和人际交往能力<sup>[24]</sup>。

日本于 2015 年颁布实施《个人信息保护法》修正案,增加了第五章《个人信息保护委员会》。增加的第五章规定了个人信息保护委员会的设置、所属、任务、管辖事务、委员身份保障或任期、义务等内容。

2016 年,日本设立了个人信息保护委员会,该委员会是为确保个人信息有用性、妥善处理个人信息而设立的具有高度独立性的机关,并且该委员会直属日本内阁总理大臣管辖,独立行使职权,地位相当高<sup>[8]</sup>。

我国《信息安全技术个人信息安全规范》指出:对个人信息安全负全面领导责任的保护人员的职责包括为个人信息安全工作提供人力、财力和物力保障等。应任命个人信息保护的专门负责人和个人信息保护的专门工作机构。同样也对设立专职的个人信息保护负责人的情况做了描述。类似地,《网络安全法》中的安全管理负责人也有类似职能。该法指出关键信息基础设施的运营者还应当履行下列安全保护义务:设置专门安全管理机构和安全管理负责人,并确保管理负责人的背景审查达到标准;定期对从业人员进行相关技术培训和技能考核;对重要系统和数据库进行备份;为抵御突发网络安全事件制定网络安全事件应急预案。美国的两部法律具有较强针对性,对数据保护人员的规定并未在这两部法律中提及,所以本文不用以与其他国法律对比。

关于数据保护人员的设立,总结如表 4 所示。

表 4 数据保护官

Table 4 Data protection officer

法律	数据保护相关人员名称	备 注
《网络安全法》	安全管理负责人	会定期接受技术培训和考核,工作中须备份数据以防突发事件。
《信息安全技术个人信息安全规范》	数据保护人员	为个人信息安全工作提供人力、财力和物力保障。
《个人信息保护法》	个人信息保护委员会	直属日本内阁总理大臣管辖,独立行使职权,是一个高度独立的机关。
《GDPR》	数据保护官(DPO)	须掌握《GDPR》及数据保护的相关法律法规,具备语言表达和人际交往能力。

### 3.5 数据控制者的基本义务

数据控制者确定个人数据处理的方式和目的,包括收集什么数据、谁可以收集、以及数据保存时间等<sup>[25]</sup>。采取适当合理的措施保护个人数据是各数据控制者的基本义务,但在细节上略有不同。美国的征信机构负责控制信用报告管理,防止被滥用。《公平信用报告法》规定:所有征信机构在为用户制作信用报告前,要尽力证实自身身份及说明数据使用目的,并将使用人的名称、使用时间和使用目的等信息记录在报告中<sup>[20]</sup>。《隐私权法》要求行政机关必须在《联邦登记》上公布其建立或修改的个人数

据系统的名称和存放地点,以及收集了哪些数据主体的信息、数据主体的哪类信息和使用目的等。行政机关所保有的个人数据只限于完成其必要的职责所需的范围。并且,所保有个人数据应该是实时、准确和完整的。日本《个人信息保护法》第 21 条规定:个人数据获得者在允许相关从业者获取个人数据时,为了实现对该个人数据的安全管理,应该对该从业者进行合适且必要的监督<sup>[14]</sup>。

我国的《网络安全法》除了要求网络运营者采取安全措施外,第 21 条(三)中还规定了以下义务:采取监测、记录网络运行状态、网络安全事件的技术

措施,并按照规定留存相关的网络日志不少于 6 个月。第 25 条规定:网络运营者应当制定网络安全事件应急预案,及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。第 34 条的规定,关键信息基础设施的运营者还要设置专门安全管理机构和安全管理负责人。定期对负责人和关键岗位的人员进行技术培训和考核。

我国《信息安全技术个人信息安全规范》要求个人数据控制者制订隐私政策,并要求将隐私政策一一投递给个人信息主体。

《GDPR》中强调数据控制者同时决定数据处理目的和方式。数据控制者不需要决定数据处理活动的每一个环节<sup>[22]</sup>。如果数据控制者不在欧盟境内,而数据主体在欧盟境内,该数据控制者应以书面形

式在欧盟境内指定代理人来处理境内数据主体的数据。数据控制者还要指定数据保护官,公开其联系方式并确保数据保护官可以及时充分地参与数据保护事务。

《GDPR》和我国《信息安全技术个人信息安全规范》都提到了不止一个控制者的情况。在《GDPR》中称之为联合控制者,《信息安全技术个人信息安全规范》称为共同信息控制者。两部法律都规定,当出现不止一个控制者时,要明确区分出各自的责任和义务。信息安全技术个人信息安全规范》还规定要将这种具体分工告知信息主体。

总结来说,关于数据控制者的基本义务如表 5 所示。

表 5 数据控制者的基本义务  
Table 5 Basic obligations of data controllers

法律	数据控制者基本义务
《网络安全法》	记录网络运行状态和事件,对突发事件要制定应急预案并上报。
《信息安全技术个人信息安全规范》	需制定隐私政策并投递给数据主体。
《公平信用报告法》	需证实自己身份及数据使用目的。
《GDPR》	需指定数据保护官,境外的数据控制者须制定一个境内代理人。

### 3.6 数据监管

《GDPR》规定了欧盟内各成员国要至少设立一个独立的用以监控本法案施行的机构。如果有成员国设立多个机构的情况,需指定其中一个监督机构人员作为代表参加理事会<sup>[25]</sup>。同时,被委任的机构人员要具备所需的经验和技能等职业资格,并对自己的工作绝对保密。各监督机构按规定执行任务时,应完全独立行动且不受任何外来影响和指示。美国的《公平信用报告法》本就是对征信业务的监管,包括信用信息公开、负面信息修复与个人隐私报告的合理生成与管理。所监管的对象是消费者信用报告机构和报告使用者<sup>[18]</sup>。《金融服务现代化法》则对监管部门提出要求:要制定技术和物理上的保护措施以消除可能存在的风险,防止任何人未经授权而窃取客户的金融数据而导致客户受到损害。各监管机构还须制定相应的行政规章使得本法案能够具体落实。

为了顺利实施《个人信息保护法案》,日本在监督机制上设有主务大臣一职。主务大臣是由内阁总理大臣从国家公安委员会中选定的。主务大臣有权要求经营者在允许的范围内向其报告个人数据的使

用情况并给予必要的建议。如果经营者违反本法案,主务大臣可给予经营者改正、中止该违法行为并采取相应措施的劝告。如果数据主体的权益受到迫害,主务大臣可命令该经营者采取解决措施。主务大臣还可以要求相关法人处理经营者依法提出的投诉,为其提供便利以确保其恰当利用个人数据。目前中国没有另外设立专门的监督机构。其中,《网络安全法》规定:国家网络部门应对关键信息基础设施的安全风险进行抽查,定期组织网络安全应急演练。网络关键设备和网络安全专用产品须满足国家标准的强制性要求,由具备资格的机构安全认证或安全检测,符合要求方可提供服务。

是否对数据监管做出规范的总结如表 6 所示。

## 4 不足与建议

### 4.1 不足

相比美国,我国目前尚未制定完整的金融个人数据保护的专门法。虽然我国《网络安全法》对信息安全和个人信息保护表现出极高的关注,《信息安全技术个人信息安全规范》也对数据控制者行为

表 6 数据监管  
Table 6 Data curation

国家	是否设有监管部门	法律	是否对数据监管做出规定
中国	否	《网络安全法》	是
		《信息安全技术个人信息安全规范》	是
美国	是	《公平信用报告法》	是
		《金融服务现代化法》	是
日本	是	《个人信息保护法》	是
欧盟	是	《GDPR》	是

做了规范,《刑法修正案(九)》对侵犯个人信息犯罪做了惩戒规定。但其适用范围相对狭窄,对于金融领域来说不能完全适用,缺乏可操作性<sup>[26]</sup>。此外,关于个人数据保护的法律法规也比较分散,没有形成完整的体系。

数据主体也缺乏数据保护意识。在我国,很多数据主体在没有造成一定程度的损失时,不太在意数据泄露情况。例如支付宝的“年度账单”活动吸引了广大用户参与。“年度账单”的生成需要访问个人消费数据,当用户不假思索地点击“同意”时就赋予了支付宝 APP 访问个人金融数据的权限。可见,我国公民在互联网上留下的足迹积少成多就有可能泄露个人隐私,给自己带来危害。

## 4.2 建议

### 4.2.1 立法的加强及监管机构的设立

金融个人数据的保护除了要有针对性地加强立法外,还应该强调金融机构、金融监管机构和技术服务机构保护金融消费者个人数据的义务。

首先,金融机构要严格规范和管理金融消费者个人数据的收集、处理和使用行为。同时加强对金融机构内部工作人员的管理,明确不同部门不同及级别的职责和任务,并对工作人员进行专业培训以提高员工的责任意识和保密意识。

其次,金融监管机构应为金融消费者创造一个安全的金融交易环境,定期对金融机构进行检查,加强对金融机构的监督管理。此外,相关的技术服务机构也有保护金融消费者个人数据的义务。监管机构也应对技术服务机构进行监管,令技术服务机构制定明确的技术水平标准,签订技术服务保密协议,防止技术操作过程中对金融个人数据的安全造成威胁<sup>[27]</sup>。

### 4.2.2 提高金融消费者自我保护意识

作为数据主体的金融消费者在金融交易中是基

础而重要的环节。尽管互联网的发展给人们的生活带来了便利,但在互联网上的一个无意的行为就可能造成个人数据泄露的情况。因此,在信息时代下,提高公民自我保护意识是最基本的保护措施。同时,公民的个人数据保护意识也应随着瞬息万变的信息时代而不断变化。

### 参考文献:

- [1] 黄国彬,张莎莎,闫鑫.个人数据的概念范畴与基本类型研究[J].图书情报工作,2017(5):41-49.
- [2] 方禹.日本个人信息保护法(2017)解读[J].中国信息安全,2019(5):81-83.
- [3] 王希龙.金融数据采集与分析系统设计研究[J].数字通信世界,2018(9):142.
- [4] 姜瑜.人工智能在金融交易中的作用及未来的发展方向[J].农村经济与科技,2019(14):278-279.
- [5] 王军强.大数据金融:现状、问题与对策[J].经济师,2018(12):144-145.
- [6] 莫小春.大数据时代金融消费者个人信息保护现状及对策[J].企业科技与发展,2016(5):219-221.
- [7] 杨秀莲.探析大数据环境如何维护个人数据安全[J].才智,2017(23):268-270.
- [8] 唐正伟.互联网金融风险影响因素及其防范机制研究[D].杭州:浙江财经大学,2015.
- [9] 内阁秘书处.个人信息保护法案[EB/OL].(2016-02-20)[2019-12-19].<http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>.
- [10] 江小慧.大数据背景下金融消费者信息权益保护浅析[J].福建金融,2016(1):49-52.
- [11] 王佳惠.金融隐私权国际化保护法律问题研究[D].大连:大连海事大学,2012.
- [12] 高红静.欧盟个人数据保护的做法及启示[J].保密科学技术,2018(9):53-59.
- [13] 张乐俊.金融隐私权法律保护问题研究[D].上海:华东政法大学,2012.
- [14] 黄晨.日本《个人信息保护法》立法问题研究[D].重庆:重庆大学,2014.



- [15] 刘小燕,贾森,齐爱民. OECD《关于隐私保护与个人资料跨国流通的指针的建议》[J]. 广西政法管理干部学院学报 2005(1): 51-52.
- [16] 王翔. 欧盟《通用数据保护条例》(GDPR) 解读[J]. 法制博览 2018(34): 195.
- [17] 吕梦达. 日本个人信息保护法修改案例研究[J]. 时代金融 2019(9): 95-96.
- [18] 李贞彩. 大数据征信的监管思路: 来自《公平信用报告法》的启示[J]. 征信 2016(11): 32-37.
- [19] 杨延超. 《欧盟通用数据保护条例》解读与启示[N]. 经济参考报 2018-06-13(008).
- [20] 人民银行哈尔滨中心支行课题组. 美国《公平信用报告法》对我国信用信息使用人行为规范的启示[J]. 黑龙江金融 2007(11): 8-10.
- [21] Kyle Thomas Sammin, 梁志坚, 张义东. 安全港:《格朗-利奇金融服务现代化法案》及金融服务的隐私问题[J]. 经济资料译丛 2011(3): 82-93.
- [22] 廖昱荣. 论金融隐私权保护之法律问题[D]. 上海: 上海交通大学 2008.
- [23] PAUL L. The Data Protection Officer: Profession, Rules, and Role[M]. New York: Auerbach Publication 2016.
- [24] MIGUEL R. Data Protection Officer: the Key Figure to Ensure Data Protection and Accountability[J]. European Data Protection Law Review 2017 3(1): 114-118.
- [25] IT Governance Privacy Team 2016. EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide[M]. Cambridgeshire: IT Governance Publishing, 2016.
- [26] 李春华,冯中威. 欧盟与美国个人数据保护模式之比较及其启示[J]. 社科纵横 2017(8): 89-92.
- [27] 吴振华. 大数据背景下金融消费者个人信息的保护和利用[J]. 金融科技时代 2018(12): 53-56.

## Comparison of Chinese and Foreign Personal Data Security Norms

——Based on the Personal Data Protection Analysis of Financial Transaction Scenarios

YANG Guang<sup>1</sup>, SONG Jing<sup>2</sup>

(1. Shanxi University Library, Shanxi University, Taiyuan 030006, China;

2. Department of Economic and Management, Shanxi University, Taiyuan 030006, China)

**Abstract:** The information age has changed the complicated and tedious way of work in the early stage and created more convenient and personalized services. However, it is hazardous that personal data expose to the Internet, which causes worrying data security. Among them, personal financial data is most critical. Financial data involve individual finance and asset distribution. Data leakage will cause unimaginable loss to individual. This paper adopts the method of literature research and comparative study to compare the relevant laws and regulations on personal data protection in the United States, Japan and the European Union from the perspectives of scope of application, personal data access and data protection officers. It is found that China's relevant legislation started late, the content is not detailed and lacks self-protection awareness. We should improve relevant legislation and strengthen the consciousness.

**Key words:** data security; personal data; data trading