

The Impact of the Implementation of China's Personal Information Protection Law on Sino-Korean Enterprises

Zhiyuan Tang^a

^aLaw School Law Major, Panzhihua University, China

Received 20 October 2023, Revised 16 January 2024, Accepted 1 April 2024

Abstract

Purpose –China has established a unified personal information protection law, aligned with cybersecurity laws and criminal laws. This year, China officially implemented the Personal Information Protection Law (PIPL), which was passed in October 2020. After a year of preparations, the law took effect on November 1, 2021. This article discusses the significance of the PIPL and its implications for legislation in China, analyzes its legal framework, and examines its impact on Chinese and Korean enterprises.

Design/Methodology/Approach – The study reviews the legislative process of the PIPL, examining expert opinions and media coverage in China and globally. It also investigates the PIPL's influence on personal information security, considering the views of both Chinese lawmakers and international observers.

Findings – The PIPL has established a legal framework for personal information security and significantly influenced related laws. However, its implementation has posed challenges, particularly in balancing legal provisions with practical application. Therefore, it is necessary to refine relevant laws and ensure their effective enforcement to protect personal information in both Chinese and Korean enterprises.

Research Implications – This article provides an overview of the key actions and principles underlying China's personal information protection legislation and the PIPL. It also discusses the impacts on Chinese and Korean enterprises, offering theoretical and practical insights to improve personal information protection and compliance with legal standards.

Keywords: China's Personal Information Protection Law, Personal Information Processing Principles, Personal Information Security, Personal Information Processing Activities

JEL Classifications: K23,K20,L86,F15,O34,L51

Lecturer, Panzhihua College

^a First Author, E-mail: tangzhiyuan0215@qq.com

© 2023 The NLBA Eurasian Institute Limited. All rights reserved.

I . 引言

2021 年之前, 与经济规模、网络利用率等相比, 中国的个人信息保护相关法律相对不完善。殷妮赵东济(2020)认为 2020 年的中国缺乏独立的个人信息保护法, 只在民法、网络安全法、刑法等多种法律中制定了相关条款, 也制定了一些个人信息保护政策和相关运营制度。中国负责个人信息管理的部门是国家互联网信息办公室(Cyberspace Administration of China), 负责网络使用的实名制、网络内容审查制等, 与强调独立性的普通个人信息监督机构性质是不同的。另外, 中国不是个人信息监督机构的国际协议体 GPA(Global Privacy Assembly)、APPA(Asia Pacific Privacy Authorities)的成员, 也不会作为观察员出席。同时随着智能手机的普及、ICT 技术的发展, 中国互联网用户已达到 9 亿、网站多达 400 万个、应用程序超过 300 万个等, 取得了相当大的发展, 但随之因个人信息泄露而出现的电信诈骗等案件也在剧增。中国国内也认识到了个人信息保护的重要性, 对加强相关法制的要求也越来越高。金钟宇(2019)指出, 中国在 2017 年制定并施行了《网络安全法》, 该法整体结构与《韩国信息通信网法》相似。虽然存在部分个人信息保护相关条款, 但大部分是有关网络安全的内容。目前, 世界主要国家和地区都认识到了个人信息的重要性, 纷纷制定并实施相关保护法律。欧盟在 2018 年施行了 GDPR(General Data Protection Regulation), 俄罗斯、越南等国也制定了相关信息保护法, 均旨在加强包括数据区域化(data localization)在内的个人信息保护相关规制。中国也在 2020 年 10 月第 13 届全国人民代表大会常务委员会第 22 次会议上公开了个人信息保护法草案, 并收集意见。从这一趋势来看, 中国对于完善个人信息保护法, 保护本国国民的个人信息, 限制个人信息向国外转移的决心很坚决。

2004 年 11 月 18 日, 中国亚太经合组织(Asia-Pacific Economic Cooperation, APEC)部长级会议通过了《亚太经合组织隐私框架协议》(APEC Privacy Framework), 会上正式对中国国内制定个人信息保护法的必要性进行了讨论。但实际制定工作没有取得大的成效。因此, 在此次 2020 年版个人信息保护法草案公布之前, 中国并没有存在旨在保护个人信息的统一、专门的法规, 而是在诉讼法, 刑法, 商法等各领域都散落着相关个人信息保护相关的法令和内容。在这样的背景下, 一些法学家认为, 中国国内个人信息的概念和范围都不够明确和广泛。例如, 2016 年 11 月 7 日制定并实施的《中华人民共和国网络安全法》, 以及《全国人民代表大会常务委员会关于加强网络信息保护的決定》, 《信息安全技术公共及商用服务信息系统个人信息保护指南》, 《电信和互联网用户个人信息保护规定》等政府机关正式公布的信息保护相关文件里, 对在中国使用的个人信息的概念和保护范围侧重点各不相同, 因而比较片面(徐宜景, 2017)。所以, 2021 年 11 月 1 日正式颁布和施行的《中国个人信息保护法》应运而生, 势在必行。

本文将 2021 年 11 月正式执行的个人信息保护法为基础, 与韩国个人情报保护法进行比较研究, 通过介绍该法的主要内容, 以及对今后个人信息保护法发展趋势的相关预测, 来分析现今及今后中国个人信息保护法体系对中国及韩国企业产生的影响。

II . 中国个人信息保护法立法过程及必要性

2020 年 10 月, 中国召开第 13 届全国人民代表大会审议并公布了 2020 年版《中华人民共和国个人信息保护法》草案。该草案从 10 月 22 日开始在全国人民代表大会官方网站公开, 并于 11 月 19 日前实施意见征集程序(public comment)。该草案作为中国首个个人信息保护专门立法, 受到了全世界的关注。中国个人信息保护法草案共由 8 章 70 个条款构成, 着眼于当前网络中发生的个人信息滥用等突出问题, 以严格的制度、严格的标准和严格的责任为基础, 以保护信息主体个人信息为宗旨, 进而提高对违法行为的惩罚力度。该草案中个人信息处理规则更加明确, 个人信息处理者想要处理个人信息时, 必须明确了其责任和权利、义务, 该草案也公示了履行个人信息保护职责的政府部门名称(朴容淑,

2021)。2021年8月20日该法经全国人大常委会审核通过并于2021年11月1日正式颁布和施行。

2019年2月,美国联邦交易委员会(FTC)以中国视频平台TikTok非法收集儿童个人信息为由,对其处以570万美元罚款。另外,TikTok违反谷歌个人信息保护政策偷偷收集用户信息的情况被确认,特朗普政府甚至宣布全面禁止TikTok在美国的使用。不仅如此,印度在2020年6月对TikTok、微信等中国59个应用程序以“侵犯了主权、防卫、安保等公共秩序”的可笑理由,采取了禁止运营措施。尹贤硕(2021)研究表明,2019年在韩国有367万名用户的TikTok,在未经法定代理人同意的情况下,不仅收集了韩国14岁儿童及青少年的个人信息,还将这些用户的个人信息保管在美国、新加坡等地的云计算处理器里,但并没有告知韩国用户这一事实。因此,韩国广播通信委员会认为,该行为违反了促进信息通信网使用及信息保护等相关法律规定,决定对其处以罚款。这一事例虽因中美之间的贸易战而引发,但也让人们认识到了个人信息保护的重要性。此前,脸书、Instagram、谷歌等众多IT企业收集并利用用户信息的事实,说明这不仅仅是TikTok的问题。认识到了个人信息,即数据已被少数IT企业垄断这一问题的国家纷纷着手制定个人信息保护相关法律。欧盟(EU)从2018年5月开始实行《一般个人信息保护法》(General Data Protection Regulations, GDPR),韩国也受欧盟GDPR的影响,于2020年2月和2021年两次修订了韩国的个人信息保护法,即《韩国个人情报保护法》(涂萌,金正镇,2017)。

王晓红认为,个人信息保护的法治化是为了确保第四次产业革命时代的必要数据,即个人信息的安全。另外,中国出现了本国企业擅自利用用户个人信息的事例,也发生了个人信息泄露和私生活受侵害的案件。中国虽然也在用民法、刑法、电子商务相关法律等对个人信息的侵害行为进行法律对抗。但是,在个人信息,即数据越来越重要的时代,这些法律作用显然有限。而且,像TikTok的事件一样,随着各国数据向国外转移的问题日益突出,中国在保护本国人民个人信息的同时,也对采取有悖于中国立场的歧视性措施的国家或地区采取了对等反制措施,《中国个人信息保护法》立法势在必行。与此同时,中国希望通过2017年网络安全法、2020年数据安全法和个人信息保护法的立法,完成个人信息,即数据保护相关的完整的法律体系的整合(姜达千,2021)。本文也以第四次产业革命背景下的基础数据处理,中国国内对个人信息的立法主旨,以中国个人信息保护法中的个人信息的范围、个人信息处理及法律责任等内容为中心,与韩国的个人情报保护法进行了一系列比较研究,以更好把握中国今后数据保护法律体系的完善方向。

III. 中国个人信息保护法内容解析

1. 个人信息及个人信息保护法的定义

中国个人信息保护法第4条第1项规定了以下个人信息:个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。这里的匿名化意味着进行个人信息处理时,不能识别特定个人,不能用现有信息复原个人信息。个人信息处理方面,个人信息保护法第4条第2项规定如下:个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。另外,关于个人信息处理者,个人信息保护法第69条第1项规定如下:处理个人信息侵害个人信息权益造成损害,个人信息处理者不能证明自己没有过错的,应当承担损害赔偿等侵权责任。对于敏感个人信息,个人信息保护法第29条第2项规定如下:处理敏感个人信息应当取得个人的单独同意;法律、行政法规规定处理敏感个人信息应当取得书面同意的,从其规定。同时,个人信息保护法第52条规定如下:处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人,负责对个人信息处理活动以及采取的保护措施等进行监督。这一条款对境外适用的外

国个人信息处理者也赋予了指定负责人的义务。该条款类似于韩国《个人情报保护法》第 39 条第 11 项，欧盟 GDPR 第 27 条规定的不设境内据点管理者或处理者的“指定代理人义务”（尹贤硕，2021）。另外，考虑到对境外企业直接处罚等存在一定程度的障碍，规定如下（中国个人信息保护法第 42 条）：境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。同时，对违反事项等的改善劝告、改正措施命令、罚款等相关结果的公告，尹贤硕（2021）指出，在韩国个人情报保护法第 66 条中也有类似规定，与 2020 年 6 月 5 日修正的日本《个人信息保护相关法律》第 42 条第 4 款第 24 项中追加的内容也类似。

2. 信息主体的权利保障

可以说，中国个人信息保护法的特点是，与欧盟 GDPR 类似，为保护信息主体的权利，对个人信息处理者等进行了严格的限制。个人信息保护法第 5 条—10 条关于信息处理，明确规定了合法性、正当性、信义性原则（第 5 条）、影响最小使用原则（第 6 条）、公开透明性原则（第 7 条）、准确性原则（第 8 条）、确保责任性、安全性的原则（第 9 条）及遵守法律、国家安全、公共利益保护原则（第 10 条）等。这样的个人信息处理基本原则与 GDPR 第 5 条规定的原则相似，体现了符合国际标准、通过信任实现自由信息移动（DFFT: Data Free Flow with Trust）的中国个人信息保护相关政策的方向性，同时可以理解为强调国家安全的中国数据主权独立性的特点（姜达千，2021）。

中国个人信息保护法第 13 条规定，符合下列情形时：取得个人的同意；为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；为履行法定职责或者法定义务所必需；为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；法律、行政法规规定的其他情形。个人信息处理者可以处理个人信息。涂萌和金正镇（2017）认为，像这样限定个人信息处理者可以处理信息主体个人信息的情况进行列举的方式与 GDPR 规定的方式相同，在内容上也大同小异。但是，由于没有规定像 GDPR 第 6 条第 1 款（f）号一样，存在“正当利益”的情况，因此也不能排除比 GDPR 更严格适用的可能性。以同意为依据处理个人信息时，个人信息主体本人可以撤回该同意。而且不能以撤回同意为由拒绝提供商品或服务。例如，同意用于营销目的的用户撤回其同意时，运营商不得终止其服务提供。也就是说，在提供服务的同时，不能将个人信息用于营销目的。但是，根据但书条款中规定的“必要时”范围的解释，在实务上继续利用同意体系（scheme）的可能性仍然存在。

对于向第三方提供个人信息，个人信息保护法第 23 条规定如下：个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。该条款要求个别同意，换句话说，为了向第三方提供个人信息，不是不可以，而是需要信息主体对第三方提供的事项进行个别同意。这一结构与韩国《个人情报保护法》第 17 条（提供个人信息）类似。个人信息保护法第 24 条规定了自动化决策等相关事项。涂萌和金正镇（2017）指出，这一条款与 GDPR 第 22 条第 1 项 29 号内容相似，可以评价为体现应对 AI 时代意志的条款。个人信息保护法第 24 条第 2 项规定了以自动化决策的方法实施商业营销及信息提供时，应同时提供不以其个人特征为依据的选项。另外，个人信息保护法第 44 条的规定，还保障了信息主体知情，决定，拒绝等权利。

3. 个人信息的国内保存义务及域外转移

刘中恺（2018）研究发现，中国从2017年6月1日开始实行的《网络安全法》第37条中规定了数据的国内保存义务，个人信息保护法中也规定了相同的内容。即，核心信息基础设施（Critical Information Infrastructure, CII）运营者，以及处理个人信息达到网络信息部门规定数量的个人信息处理者，在国内保存义务及域外转移方面要求安全评估必须合格。但是，对于不要求国家网络信息当局进行安全评估的个人信息处理者，仅限于规定情况，可以将个人信息转移到域外（中国个人信息保护法第38条）。此外，将个人信息转移至域外时，应告知信息主体对个人信息接收人的身份、联系方式、信息处理目的、处理方法、处理的个人信息种类及信息主体对个人信息接收人行使本法规定的自身权利的方法等事项，并事先应获得同意（中国个人信息保护法第39条）。即，一般个人信息处理者与域外转移处（个人信息接收人）签订个人信息处理合同，对个人信息处理人赋予个人信息处理活动达到本法规定的个人信息保护标准的义务时，根据中国个人信息保护法第38条第3号，可以将中国国内的个人信息转移到域外。但是，根据第39条，需要对信息主体进行详细说明和取得个别同意。尹贤硕（2021）指出，该条款与韩国《个人情报保护法》第17条第3项规定的对国外迁移的内容如出一辙。同时，第四十三条规定：任何国家和地区在个人信息保护方面，对中国抱有偏见，采取禁止、限制或其他类似措施的，中国可以根据实际情况，对有关国家或地区采取相应措施。有学者推测，这一规定可能反映了美国和中国最近因TikTok等问题产生的矛盾，因此，韩国也应该注意，这是一条有可能对个人信息转移产生影响的条文。

4. 个人信息处理者的义务

李尚禹（2021）指出，个人信息处理者须综合考虑信息处理的目的、处理方法、处理个人信息的种类及可能导致的结果以及可能发生风险的程度等，同时履行实施保护措施的义务，以免发生个人信息被擅自阅览、泄露、窃取、变更、删除等安全问题。处理特定信息时，有义务进行风险评价的个人信息处理者要对以下个人信息处理活动进行事前风险评价，并记录处理情况。（中国个人信息保护法第55条）风险评价内容应包括以下内容：信息的处理目的、处理方式等是否合法、正当、必要。另外，还有这些相关内容：对个人权益的影响及安全风险；所采取的保护措施是否合法、有效并与风险程度相适应。而且相关风险评价报告书及处理情况记录至少要保存3年。（中国个人信息保护法第56条）个人信息处理者如果得知个人信息泄露的事实，应立即采取救济措施，并通知个人信息保护专门当局及信息主体以下事项（中国个人信息保护法第57条）。这些条款都很适用并且有针对性。最后，个人信息处理者为了防止个人信息泄露而采取的侵害措施，可以避免因信息泄露而造成的损失时，个人信息处理者可以不通知信息主体。但是，如果个人信息保护部门认定个人信息泄露有可能对信息主体造成损失的，可以利用职权下达相应通知。（中国个人信息保护法第57条）尹贤硕（2021）认为，这一条款与2020年2月修正的韩国个人情报保护法第39条及GDPR第33条第1项和第36条第1项相似。但是，与韩国规定的24小时以内、72小时以内通知和申报的时效不同，中国虽没规定时效，但普遍理解为即时通知。

5. 处罚事项

违反本法规定处理个人信息时，未采取规定的必要安全措施、保护措施、救济措施的，不服从个人信息保护部门的纠正命令或警告的，可以没收违法所得或处以罚款（中国个人信息保护法第66条）。该条款与韩国2021年修正的《个人情报保护法》第39条的条款相似。此外，如有违反本法规定的行为，

将根据相关法律、行政法规的规定，记载并公布相关法人或个人的信用记录（中国个人信息保护法第 67 条）。另外，在处理个人信息的过程中侵害信息主体的权利时，作为信息主体而遭受的实际损失或个人信息处理者承担相应利益的赔偿责任，很难计算出实际损失额或利润额时，法院可以利用职权确定赔偿额（中国个人信息保护法第 69 条）。另外，个人信息处理者违反本法规定，侵害多名信息主体权益时，检察机关、消费者组织、个人信息保护部门及国家网络信息部门可以根据本法提出团体诉讼（中国个人信息保护法第 66 条）。这些处罚事项都比较严格和有效，对数据滥用等违法行为能起到有效的威慑作用和对受害人能给予一定的救济（李尚禹，2021）。

IV. 中国个人信息保护法对中国及韩国企业的影响

对于中国自身企业以及在中国设立营业点的众多韩国企业，还有通过网络对中国提供商品和服务的韩国企业来说，中国个人信息保护法的实施是必须关注和重视的事情。接下来，本文将以制定和实施的个人信息保护法对中国及韩国企业产生的影响为中心，讨论相关问题。

1. 今后的立法动向

根据郑泰仁和郑秀妍、尹在锡（2021）的研究表明，中国个人情报保护法为保护个人信息，在最初建议案里有限制国内个人信息迁移到国外、并引进黑名单制度、指定代理人等等条文，可能会给企业带来相当大的负担。因此，在这种情况下，正式颁布的中国个人信息保护法对这些建议条款预做了修改或给予缓期时间。随着市场国际化和第 4 次产业革命的进程，这部法律也会不断完善和修正，并和相关法律一起构建起中国信息保护法律的完整体系，对中国和韩国等企业的日常数据运营管理将产生更大的影响。

2. 新设主管部门

朴容淑（2021）认为，虽然本法没有明确规定负责部门，但根据法条里所提，国家网络信息办公室和工业和信息化部主管的国家网信部门应该将会成为负责部门。但是，国家网络信息办公室作为专门负责对网络内容进行审查的部门，在负责个人信息保护方面存在很大的利害冲突。因此，如果在中国运营个人信息保护制度的意志坚定，将来很有可能新设独立的委员会组织。尹贤硕（2021）指出，韩国已成立并运营着专门负责个人信息保护业务的个人信息保护委员会，英国等许多国家也都有设立相关委员会，这些委员会的目的是更好地保障独立的个人信息保护活动的执行。

3. 域外适用

卢恩英和鞠情勋（2021）认为，与 GDPR 类似，本法规定了域外适用于包括韩国在内的中国以外的个人信息处理者的法律。不仅适用于在本国经营的企业，还适用于在海外经营的企业，如果违反，将禁止提供个人信息 或予以处罚，因此预计将有些争议。但是 GDPR 首先采用了域外适用，所以争议会比较小。也可以想象得到，今后很多国家会以这样的先例为依据，在本国法律中明确域外适用情况，这从一定意义上可以说是本国法律向国际区域履行合理管辖权的一大进步。

4. 数据局部化

核心信息基础设施运营者、个人信息处理规模达到特定标准的个人信息处理者必须在中国国内义务性地保管个人信息，只有通过安全评价才能转移到国外。由于这两个对象均可由中国政府制定标准，因此进入中国的韩国企业也可能成为对象。据推测，此举是为了强化中国将个人信息视为重要资源并保存在本国境内，保护相关产业，限制进入中国的跨国企业将收集到的个人信息转移回本国。俄罗斯、越南也在法律上规定了数据局部化并义务化的相关条款（金钟宇，2019）。

5. 个人信息提供限制

中国个人信息保护法第四十二条：境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。即，禁止目录主管部门认为，境外机关、个人侵害中国公民个人信息权益或威胁国家安全、公共利益的，可以将其纳入限制提供个人信息、禁止目录，限制或禁止提供个人信息。而中国《网络安全法》第四十七条也规定，网络运营商必须切断和报告非法信息，同时，第六十八条规定，违反时罚款 500,000 元以下，停止营业，关闭网站，吊销审批。因此，在中国运营的韩国企业很有可能要接受中国政府根据相关条款切断内容这一要求（卢恩英，鞠情勋，2021）。

6. 代理人制度

金钟宇（2019）研究指出，除中国企业外，个人信息处理者在中国境内设立专门机构或指定代表负责个人信息保护工作，相关机构的名称、代表声明、联系方式等要上报主管部门。代理人制度在 GDPR、韩国个人情报保护法中均被采用。但是韩国只适用于用户数、销售额等符合标准的企业，中国并不存在这种标准，而是要求所有企业报告相关内容。不仅仅是中国企业，这对韩国企业来说也是需要注意的事项，要遵从中国法律依法进行业务处理。

7. 个人信息泄露通知

个人信息处理人发现有个人信息泄漏情况的，应立即采取救济措施，并通知主管部门及个人。涂萌和金正镇（2017）指出，该制度在 GDPR、韩国个人情报保护法中也同样存在，但是规定了例外事项。韩国泄露一千人以上个人信息时需通知，GDPR 则规定了，应通知因个人信息泄露，给个人权利和自由带来危险的事实。中国没有规定这些例外事项，因此发生泄漏事故时必须通知主管部门。但是通过个人信息处理者采取的措施，可以有效地避免个人信息泄露的损失时，可以不通知个人。这些特定事项，都是中国和韩国企业在今后日常业务处理当中必须严格遵守的。

8. 违反时所受处罚

与网络安全法相比，中国个人信息保护法的法律责任已经被大大强化了。违反法律时，由主管部门责令改正，不遵从法令者将被罚款。罚款视情况而定，严重违规时，处以最高 5000 万元或上年度销售额的 5% 以下的处罚。另外，不仅罚款，还可以暂停业务、停止营业、吊销营业执照，整体处罚力度高于韩国。韩国仅征收相关销售额的 3% 或 1 亿韩元以下的罚款。另外，因个人信息处理行为侵犯个

人信息权益的赔偿诉讼，应根据个人损失或个人信息处理者获得的收益来承担赔偿责任。但对详细的处理程序和最大赔偿额都没有规定。韩国也规定了类似的损害赔偿。如果个人信息处理者违反法律处理个人信息，多数权益会受到侵害，检察机关、相关部门可以依法向法院提起诉讼。韩国的情况，如果集体纠纷调解被拒绝，消费者团体等可以据此提出集体诉讼（尹贤硕，2021）。因而，不仅仅是中国企业，韩国企业也要积极避免违反相关中国个人信息保护法事项，避免巨额处罚和诉讼的发生。

V. 结论

郑泰仁和郑秀妍、尹在锡（2021）研究表明，中国通过2017年网络安全法的制定、2020年草案公布，数据安全法以及2021年个人信息保护法的最终立法，积极地完善了个人信息，即数据保护相关的法律体系的建设。特别是中国《个人信息保护法》的实施，有效地保护了中国国内互联网用户的个人信息。同时，也希望依靠此法的法律依据，能对中国执行歧视措施的国家或地区采取相关有效的反制措施。中国的个人信息保护相关立法详细规定了个人信息的定义。殷妮和赵东济（2020）认为，虽然个别法，例如民法、网络安全法、个人信息保护法等都规定了类似个人信息的法律定义，但是这些定义的实质内容的解释和独立完整的中国个人信息保护法上的定义解释有很多的不同。中国政府也注意到了，根据相关个别法上的适用，个人信息的收集范围也是不同的。另外，姜达千（2021）也指出了一些需要注意的事项；例如，中国《个人信息保护法》第43条规定，任何国家及地区，在个人信息保护方面，对中国持有偏见，采取禁止、限制或其他类似措施时，都应采取相应的应对措施，这一法条也是中国维护国家本国人民信息处理主权和人民信息利益自主保护的象征。另外，我们也能感受到，网络安全法和个人信息保护法实施后，中国国内的企业如果非法将个人信息及数据转移到中国以外的相关处罚内容上，很明显，中国的处罚水平是大大高于韩国的。中国《个人信息保护法》中规定没收非法所得，并处以5000万元人民币或上一年度销售额5%以下的罚款的处罚内容比韩国规定的销售额3%的罚款要重的多（尹贤硕，2021）。李尚禹（2021）也认为，从总体来看，中国个人信息保护相关立法体系的不断完善，也体现在了个人信息在中国国内保管及国外转移等相关规定及调整的具体内容方面。因此，中国企业，在中国甚至中国境外的外国企业，包括韩国企业在内，在今后的各项业务中，要收集中国国内个人信息，必须仔细分析中国个人信息相关保护法的内容和今后完善方向，并需要制定相应的应对政策以适应中国信息保护相关法律的发展。这样才能在中国市场合法有效地获取更大利润。才能让企业在中国有更长远的发展。

参考文献

- 刘中恺（2018），“大数据时代个人信息保护问题研究”，载《网络空间安全》9卷4期，中国，28-29。
- 王晓红（2017），“互联网金融消费者个人信息安全权法律保护问题探讨”，载《北方金融》2017.02，中国，63-66。
- 金钟宇（2019），“在大数据时代中国个人信息保护法律制度现状以及立法课题研究”，载《情报法学》23卷2号，韩国，252-290。
- 涂萌（著）/金正镇（译）（2017），“欧盟的《情报保护指南》和《一般情报保护规定》的研究及对中国立法的启示”，载《中国法研究》30卷，韩国，49-71。
- 殷妮 赵东济（2020），“中国民法典中对个人信息合理使用制度的思考”，《民事法的理论和实务》

2020.12, 韩国, 119-149.

李尚禹(2021),“关于中国个人信息保护体系的研究—新个人信息保护法的主要内容—”,《中国法研究》45卷,韩国,333-361.

尹贤硕(2021),“中国个人信息保护相关法制的动向—与韩国的个人情报保护法相比较—”,《法与政策研究》21卷1号,韩国,351-380.

郑泰仁 郑秀妍 尹在锡(2021),“中国个人信息保护法制定动向”,载《信息保护学会刊》31卷1号,韩国,65-73.

徐宜景(2017),“中国个人信息保护立法研究—网络安全法为中心”,载《中国研究》72卷,韩国,133-155.

朴容淑(2021),“对中国个人信息保护的重新审视—以2020年版个人信息保护法草案为中心—”,载《人权法评论》26号,韩国,3-35.

姜达千(2021),“关于中国数据保护立法动向和数据主权的考察”,载《中央法学》23卷2号,韩国,24-45.

卢恩英 鞠情勋(2021),“中国网络平台的限制研究—以个人信息保护为中心—”,载《中国法研究》45卷,韩国,363-398.