欧盟《通用数据保护条例》之中国效应及应对

胡文华 孔华锋
(公安部第三研究所 上海 201204)

摘 要 为建立数字单一市场、刺激数字经济发展,以及重建欧洲民众对数字经济的信任,欧盟于2016 年 4 月 14 日通过了《通用数据保护条例》。2018 年 5 月 25 日该条例开始正式实施。该条例通过建立完善的数据权利体系、义务履行机制、数据跨境传输机制以及监管机制,建立了高标准的个人数据保护机制。鉴于《通用数据保护条例》的域外效力,其落地实施也将对我国带来巨大冲击。我国国家、行业、企业等须共同着力,有效应对《通用数据保护条例》对我国带来的影响。

关键词 欧盟 《通用数据保护条例》 中国效应 应对

中图分类号 TP309.2 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2018.11.052

THE IMPACT OF EU GENERAL DATA PROTECTION REGULATION ON CHINA AND ITS RESPONSE

Hu Wenhua Kong Huafeng
(*Third Research Institute of Ministry of Public Security, Shanghai 201204, China*)

Abstract In order to establish a single digital market, stimulate the development of the digital economy, and rebuild the trust of the European people in the digital economy, the EU adopted the General Data Protection Regulation in April 14, 2016. It was formally implemented in May 25, 2018. The regulation established a high standard personal data protection mechanism through the establishment of a perfect data rights system, compulsory implementation mechanism, data cross-border transmission mechanism and regulatory mechanism. In view of the extraterritorial effect of the General Data Protection Regulation, its implementation also brings great impact to our country. Our country, industry and enterprises must work together to effectively cope with the impact of it on China.

Keywords European Union General Data Protection Regulation Impact on China Response

0 引 言

2016 年 4 月 14 日,欧洲议会通过了《通用数据保护条例》(General Data Protection Regulation),以下简称“GDPR”,2018 年 5 月 25 日该条例开始正式实施。作为欧盟 1995 年颁布《欧洲议会和欧盟理事会关于保护涉及个人数据处理与数据自由流动的 95/46/EC 号指令》(以下简称“95 指令”)后,隐私与数据保护领域 20 年来最引人瞩目的立法变革,GDPR 旨在赋予数据主体以个人数据控制力,在欧盟境内建立一个高水平的、统一的、适应数字时代的个人数据保护框架。

值得注意的是,GDPR 采用属地加长臂管辖原则,不再以“营业机构所在地”作为地域管辖的依据,而是以“数据”是否为欧盟境内产生作为管辖权重要依据,将适用范围扩展至了“未在欧盟境内设立营业地,但向欧盟提供商品或服务”涉及到个人数据处理的机构。鉴于 GDPR 所确立的域外效力,GDPR 的落地实施将对我国带来诸多影响。我国应如何应对上述影响亟需研究。

收稿日期:2018-06-21。国家社会科学基金重大项目(15ZDA047);上海市 2017 年度“科技创新行动计划”高新技术领域项目(17DZ1101004);公安理论及软科学研究计划项目(2016LLYJGASS020)。**胡文华**,研究实习员,主研领域:网络安全法律政策。**孔华锋**,研究员。

1 GDPR 的颁布背景

任何立法的背后都有经济价值和社会效应的考量,欧盟 GDPR 的出台也不例外。在数字经济高速发展的背景下,数据尤其是个人数据成为经济增长和社会进步的重要资源。欧盟统计,2015 年欧盟数据经济的价值超过 2 850 亿欧元,占欧盟 GDP 的 1.94% 以上。2016 年这一数字增加到 3 000 亿欧元,占 2016 年欧盟 GDP 的 1.99%。欧盟认为如果及时制定有利的政策和立法,到 2020 年欧洲数据经济的价值可能会增加到 7 390 亿欧元,占欧盟 整体国内生产总值的 4%[1]。但与此同时,隐私保护、数据泄露、数据歧视等问题不断涌现,给数据产业的发展以及个人数据保护带来了诸多新挑战。

1.1 建立数字单一市场,刺激数字经济发展

为迎接数字革命为欧洲带来的机遇,2015 年 5 月 6 日,欧盟提出了"数字单一市场"的详细规划,以保障欧洲民众和企业能够无障碍地、公平地访问在线商品和服务。同时打破监管壁垒,将 28 个成员国市场转化为单一的欧盟市场,以促进欧洲数字经济增长潜力的最大化[2]。

在建立欧洲数字单一市场的目标下,欧盟亟需一个统一的、适用于全部成员国的数据保护框架。但 95 指令并不能实现该目标。首先,从法律效力来看,95 指令并不属于"条例",不具有强制性,不能直接适用于成员国,而需要成员国将其转化为国内法方可落实。其次,从 95 指令的实施情况来看,欧盟各国对于数据保护保护水平参差不齐,甚至存在冲突的情况。这一方面,加大了企业的合规成本,也不利于欧洲民众的个人数据保护。在此背景下,GDPR 作为欧盟推进数字单一市场、刺激欧洲数字经济发展的重大举措应运而生。

1.2 重建欧洲民众对数字经济的信任

与早期的互联网时代相比,大数据背景下,个人数据化现象更加普遍,数据收集和共享的规模也不断扩大。经自然人之手, 越来越多的个人信息被公诸于众。个人对其数据的控制力进一步弱化,数据处理者的数据处理能力进一步加强[3]。与此相应地,间谍、数据泄露等传统风险不断加大,数据歧视、人格物化等新型问题不断凸显。

在此背景下,产生于互联网早期的 95 指令已不能为个人数据提供充分保护,欧洲民众对于数字经济的信任逐渐降低。欧盟表示 92% 的欧洲人担心手机应用程序在未经他们同意的情况下收集他们的数据。89% 的人表示他们想知道智能手机上的数据何时与第三方共享[4]。欧盟亟需通过数据保护改革,加强个人数据保护水平,重建欧洲民众对数字经济的信任。

2 GDPR 的主要内容

GDPR 建立了完善的数据权利体系、义务履行机制、数据跨境传输机制、监管机制以及法律责任机制。

2.1 权利机制

本次欧盟个人信息保护法改革,力图通过完善和细化个人信息权利,从而实现全面保障个人对其信息的控制权[5]。GDPR 框架下,数据主体享有访问权、更正权、反对权、限制处理权、被遗忘权、数据可携权,以及限制自动化决策等诸多权利。其中,被遗忘权赋予了数据主体在撤回同意、数据不再必要、数据处理行为违法或违规,或涉及儿童的个人数据等情形下删除个人数据的权利。数据可携权赋予了数据主体从数据控制者处获取、转移其个人数据的权利。在技术可行的情况下,依据数据可携权,数据主体还有权直接将个人数据转移至另一控制者处,数据控制者应当提供技术支持。此外,限制自动化决策权赋予了数据主体在特定情形下,不受自动化决策制约,要求数据控制者提供相关人为干预机制的权利。

2.2 义务机制

基于风险管理理论,GDPR 建立了以"数据控制者"为核心的问责制。数据控制者对 GDPR 的遵从负责,数据处理者的责任则原则上交由合同调整(除安全保障、设置数据保护官义务外)。GDPR 框架下,数据控制者应当履行的义务可分为一般义务和特殊义务。前者是所有数据控制者均须遵守的义务,后者则是满足相关条件的数据控制者才须遵守的义务。一般义务包括隐私设计、数据处理记录、数据泄露通知和安全保障。特殊义务则包括设置数据保护官、数据保护影响评估。GDPR 首次引入了"隐私设计理念"。通过设计保护隐私旨意于从产品的设计之初融入隐私保护的理念,在数据的全生命周期中均提供保护[6]。数据泄露通知义务对数据控制者的内部监测和反应机制提出了较高的要求,明确数据控制者原则上应当在发现数据泄漏事件 72 小时内,通知监管机构。数据泄露会对个人的权利和自由带来较高风险的还须通知个人。

2.3 数据跨境传输机制

针对数据向欧盟境外的传输,GDPR 建立了三种机制。第一种也是最主要的一种,目标国的个人数据

保护水平被欧盟认定为达到“充分保护水平”。此外,采用欧盟制定的标准合同条款或满足欧洲数据保护机构批准的有约束力的公司规则的要求,也是有效的数据传输机制。截至目前,欧盟委员会认定的满足为个人数据提供充分保护的国家或地区为安道尔、阿根廷、加拿大、法罗群岛、格恩西岛、以色列、马恩岛、泽西岛、新西兰、瑞士、乌拉圭和美国。我国尚不属欧盟认定的满足“充分保护水平”的国家。

2.4　监管机制

为促进个人数据保护规则的落实,GDPR 建立了完善的个人数据保护监管机制。其中在公权力监管机构方面,GDPR 规定,成员国应当设立一个或一个以上独立的监管机构来处理个人数据保护问题,监管机构的主要职责在于监督和促进 GDPR 的实施[7]。目前,欧盟成员国基本都设立了本国的个人数据保护机构,例如:法国的国家数据保护委员会、芬兰的数据保护办公室、德国的联邦数据保护与信息自由保护专员等。在监管机构的权力设置方面,GDPR 授予了监管机构调查权、矫正权、授权与建议权、司法参与权等诸多权力。

2.5　法律责任机制

在 GDPR 框架下,数据控制者或处理者违反个人数据保护规定的责任包括民事责任和行政责任。其中:民事责任部分,以损失存在为前提,GDPR 赋予了数据主体以损害赔偿请求权。行政责任部分,GDPR 设置了高昂的罚款数额。根据数据控制者或处理者违反的规则不同,GDPR 设定了两档罚则:(1) 对于违反默认隐私保护设计、数据安全保障、数据泄露通知、数据影响评估等义务的行为,处 1 000 万欧元或上一年度全球营业额 2% 的罚款(取高者罚)。(2) 对于违反数据处理原则、违反同意规则的要求、损害数据主体的合法权利等行为,处2 000万欧元或者上一年度全球营业额 4% 的罚款(取高者罚)。

3　GDPR 的中国效应

作为数字经济治理的集大成者,同时也是个人数据保护的重要依据,GDPR 既是我国企业走出去的合规参照,也是我国数据治理的借鉴对象[8]。与此同时也应注意,GDPR 的落地实施将对我国带来诸多影响。

3.1　国家层面:冲击我国执法机构的执法效力

GDPR 通过适用长臂管辖原则将诸多中国企业纳入其管辖范畴,又通过设置高水平的保护规则导致中国企业面临巨大合规风险。最终通过完善的监管机制,保障落实其监管权限。三大举措相辅相成,极有力地促进了欧盟监管机构对中国企业的监管实质影响的扩大。这直接导致的后果为:欧盟的监管机构将有权依据 GDPR 对中国企业,即使未在欧盟境内设立机构的企业行使其监管权。其中,依据调查权,欧盟的数据监管机构有权要求该企业提供其履行职责所需的所有信息,甚至包括依据欧盟方面的程序法,进入在华企业的经营场所、相关设备或工具进行个人数据保护事件调查的权力。

欧盟调查权的落实将直接冲击我国网安法第 37 条个人数据和重要数据出境制度的实施,同时也对我国数据主权带来潜在的威胁。可以预见的场景是:一方面,欧盟基于调查权要求获取在华企业的数据或进入其设备系统的访问权限;另一方面,我国依据网安法确立的数据出境评估制度而要求数据不予出境,或基于捍卫数据主权的考量要求企业对于欧盟调查权的行使要求不予执行。该法律冲突的产生,将导致企业需在 GDPR 的遵从和网安法的遵从之间做出选择,鉴于 GDPR 高额的罚款机制,企业极可能选择遵守GDPR的规定,进而降低我国执法机构的执法效力。

3.2　企业层面:增加我国企业的合规成本

作为欧盟乃至全球范围内个人数据水平最高的立法,GDPR 通过强化知情同意规则的要求、新增被遗忘权、数据可携权等新权利,增设数据泄露通知、数据影响风险评估、数据保护专员等义务,加大违规处罚力度,全面提升了个人数据保护水平。对于企业而言,小至隐私政策、业务流程,大到信息技术系统、战略布局,无一不需要重新审视规划[9]。

鉴于 GDPR 所确立的域外效力,GDPR 的落地实施将对我国境内航空、金融等传统领域,以及通信、互联网等新兴领域的企业对欧业务的开展带来冲击。部分在华企业将须同时满足 GDPR 与网安法两部法律的合规要求。为遵守 GDPR 的规定,企业的合规成本将大幅度增加。

(1) 作为欧盟层面通用型的规定,GDPR 从 95 指令的 34 个条款发展为如今的 99 个条款,且创设了大量的新概念、新权利、新义务,内容本身复杂且相对抽象。虽然目前欧盟已经出台了一些适用指南以对具体规范加以细化,但对于 GDPR 的释明仍然任重道远。

(2) 在大数据背景下,GDPR 设置的诸多机制实难达到。例如,严苛的知情同意如何落实、被遗忘权、数据可携权如何实现等。同时,GDPR 目前的诸多规则的不明确性导致合规工作的不确定性,也给予了欧盟监管当局大量的可解释和可裁量空间。

(3) 鉴于我国长久以来在个人数据保护方面比较薄弱,受 GDPR 冲击的中国企业基本都面临违规的现实风险。

因此,无论是从 GDPR 规范本身的不明确性,还是从技术的不可行性,抑或中国企业的合规能力角度出发,GDPR 给中国企业带来的违规风险是现实的,且远超欧盟以往颁布的任何一部个人数据保护规范。

3.3 行业层面:冲击现行商业模式

GDPR 新增的数据权利将对现行互联网商业模式带来巨大冲击。尤其从国内互联网企业的实际情况来看,在掌握大量用户的个人信息之后,通过对用户行为的分析提供的收益,这是目前互联网企业主流的盈利模式。但根据 GDPR 的规定,对于个人数据收集的知情同意要求更为严格,使得大量的用户数据难以被收集。另一方面,GDPR 对自动化决策行为也做出了限制,明确用户可以拒绝该自动化决策。在此规定下,以往简单的,通过获取用户个人信息并进行数据分析进而提供精准服务的模式将面临极大的合规成本。而该合规成本最终可能转嫁至用户,进而也将导致现行互联网服务以免费模式为主走向付费模式。现行商业模式的改变可能会对现行的整个互联网市场带来巨大的冲击。

4 GDPR 的中国应对

面对 GDPR 的落地实施,我们既要学习其个人数据保护方面的先进理念,为我国个人数据保护立法提供借鉴。也要注意立足本国国情理性谨慎对待从而达到有效应对 GDPR 带来的全方位的冲击和挑战。

4.1 国家层面:批判借鉴

1) 完善数据出境评估制度。GDPR 带来的国家安全风险主要来源于欧盟监管机构对中国企业的监管权限。在 GDPR 监管机制下,尤其需要注意的是欧盟监管机构的调查权。一旦欧盟方面行使调查权,作为被调查对象的中国企业将需要提交诸多信息,包括所有涉事的个人数据,以及欧盟监管机构认为需要提交的其他数据。这极有可能产生的风险在于:中国企业迫于欧盟的监管压力,向欧盟监管机构传输相关个人数据和其他数据,进而给中国带来国家安全隐患。鉴于此,我国亟需完善数据出境评估制度。

2) 尽快出台专门的个人信息保护法。近年来,我国通过《网络安全法》《民法总则》等一系列的法律提升个人信息保护水平。但整体来看,目前我国尚未出台专门的个人信息保护法,相关规定较为分散、缺乏体系化和系统性。随着我国数据产业的发展,我国也亟需一部统一的、专门的个人信息保护法。但同时也需注意,GDPR 诸多规定尚不明确,需要进一步的细化,其具体的落地实施情况仍待观察。另一方面,鉴于我国个人数据保护水平的现状以及数据产业发展情况,采用 GDPR 如此高的个人数据保护标准是否适宜,也需要审慎考量。

3) 在数据立法部分考虑使用长臂管辖原则,扩大本国立法的域外效力。无论是欧盟的 GDPR 还是美国 2018 年通过的《合法使用境外数据明确法》(Clarify Lawful Overseas Use of Data Act)均将属地管辖扩展至长臂管辖原则,扩大其法律的域外效力。随着数据在全球范围内的自由流动,对于数据的监管突破原有的属地管辖已成国际立法趋势。国际空间围绕数据主权的争夺态势日益严峻,我国也亟需对此作出立法上的应对,以争取我国在国际博弈中的主动性。

4.2 企业层面:提升合规能力

从现状来看,我国境内有诸多企业与欧洲有业务往来,包括银行、电子商务、互联网等诸多涉及个人数据处理的业务,这意味着我国诸多企业也将成为GDPR 规制的对象。此类企业需高度重视开展 GDPR 的合规工作,提升自身的合规能力,以免承担高额的违规成本。具体而言,企业应当:

1) 梳理业务情况,确定合规对象。在华企业准确定位自己是否属于 GDPR 框架下的合规义务主体是开展合规工作的首要环节。企业应当首先全面梳理其业务开展情况,了解各业务处理的个人数据的来源、类型、存储位置、用途、访问权限、共享和披露情况、安全保障措施等信息,确定合规对象。

2) 区分数据来源,针对性合规。鉴于 GDPR 与网安法规范的诸多差异,对于企业合规而言,做好来源于欧盟境内的数据和其他数据来源的区分,有利于后续针对性合规业务的开展。在系统数据难以区分的情况下,为降低企业合规风险,建议从严落实。再者,完善内控机制,加强合规记录。在 GDPR 框架下,传统的个人数据管理机制已不能满足要求。企业应当重新规划、建设自身的个人数据管理内控机制。通过默认隐私保护、数据保护专员、数据影响评估、数据泄露通知等机制建立一套从产品设计到应用、从管理到流程、从规范到技术的最佳实践,以最大限度地降低合规风险。此外,合规文档记录对于企业内部的风险评估以及应对外部合规审查均非常重要。无论是 GDPR 还是网安法下的合规工作,均应当加强合规文档记录,包括隐私政策、数据传输协议、与第三方合作协议、人员培

训计划等。

3）放眼全球,整体布局。鉴于 GDPR 与网安法可能带来的数据出境合规困境。企业应当以全球化视野重新考虑数据中心或服务器在全球的战略布局,尤其是面向欧盟服务相对应的服务器或数据中心的位置设计,以应对数据跨境传输限制及国际法律冲突难题。此外,随着数据经济在全球范围内发展,全球范围内的数据合规审查将成为必然趋势。无论是为 GDPR 还是其他未来立法带来的合规冲击,企业均应及时跟进全球立法动态,以全球化的视野为企业的发展战略和合规工作做好预判。

4.3　行业层面:发挥协调指导作用

GDPR 实施后,全国信息安全标准技术委员会发布了《网络安全实践指南—欧盟 GDPR 关注点》为我国企业的 GDPR 合规工作提供了有益的指引。但鉴于 GDPR 的复杂性,仅仅依靠该文件并不能满足企业合规的需求。未来,行业层面仍需继续推进 GDPR 的合规指引工作。

再者,随着 GDPR 的实施,欧盟必将以此为抓手向全球扩张其影响力,并为世界个人信息保护法树立新的标准。虽然 GDPR 通过欧盟自身市场的吸引性配之以严苛的罚则,使之具有一定的域外威慑力。但欧盟方面要进一步扩大其域外执行力仍面临诸多挑战。可以预见,欧盟可能会通过一系列双边协议或谈判,巩固其制度优势。基于此,行业层面,应当积极加强与中欧监管机构的沟通协调,及时掌握中欧相关监管机构的最新动向,为企业 GDPR 合规争取有利形势。

此外,鉴于 GDPR 可能会对现行的商业模式造成冲击,行业层面,相关机构应当及时对后 GDPR 时代的互联网发展模式进行积极研判,推进整个行业的进一步发展。

5　结　语

作为数字经济治理的集大成者,GDPR 通过强化知情同意规则的要求、新增被遗忘权、数据可携权等新权利,增设数据泄露通知、数据影响风险评估、数据保护专员等义务,加大违规处罚力度,设立“一站式”投诉服务,全面提升了个人数据保护水平。

鉴于 GDPR 的域外效力,其落地实施对我国将带来了巨大冲击,体现在:国家层面,冲击我国执法机构的执法效力;企业层面,增加我国企业的合规成本;行业层面,冲击现行商业模式。为应对 GDPR 的冲击,我国应当积极采取措施。国家层面,完善数据出境评估制度,尽快出台个人信息保护法,但也需注意结合本国国情,切忌原搬照抄。企业层面,企业应在全面梳理其业务开展情况的前提下,确定合规对象;区分数据来源,开展针对性合规;完善内控机制,加强合规记录;以全球化视野制定合规策略。行业层面,应充分发挥协调指导作用,及时对后 GDPR 时代的互联网发展模式进行积极研判,推进行业的进一步发展。

参　考　文　献

[1] European Commission. Building a European data economy [EB/OL]. [2017-1-10] https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

[2] European Commission. Shaping the Digital Single Market [EB/OL]. [2015-3-25] https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.

[3] 郭瑜. 个人数据保护法研究[M]. 北京:北京大学出版社,2012.

[4] European Commission. The right to be forgotten and the EU data protection reform: Why we must see through a distorted debate and adopt strong new rules soon [EB/OL]. [2015-3-25] http://europa.eu/rapid/press-release_SPEECH-14-568_en.htm.

[5] 刘云. 欧洲个人信息保护法的发展历程及其改革创新[J]. 暨南学报(哲学社会科学版),2017,39(2):72-84.

[6] 李维扬. 通过设计保护隐私[J]. 信息安全与通信保密,2018(1):32-42.

[7] 高富平. 个人数据保护和利用国际规则:源流与趋势[M]. 北京:法律出版社,2016.

[8] 桂畅旋. 欧盟通用数据保护法案的影响与对策[J]. 中国信息安全,2017(7):90-93.

[9] 王融. 欧盟数据保护通用条例[J]. 中国征信,2016,2(4):93-101.

(上接第 258 页)

[13] ARM Ltd. The Architecture for the Digital World[EB/OL]. [2018-03-02]. https://silver.arm.com/download/ARM_and_AMBA_Architecture/AR100-DA-70501-r0p0-00eac5/ARMv8_ISA_PRD03-GENC-010197-30-0.pdf.

[14] ARM Ltd. The Architecture for the Digital World[EB/OL]. [2018-03-02]. https://silver.arm.com/download/ARM_and_AMBA_Architecture/AR100-DA-70501-r0p0-00eac5/ DDI0487A_a_armv8_arm_errata.pdf.

[15] Checkoway S, Davi L, Dmitrienko A, et al. Return-oriented programming without returns[C]// ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, Usa, October. DBLP, 2010:559-572.

[16] Linaro. Linaro ARMv8 Project[EB/OL]. [2018-03-02]. http://www Linaro.org/ projects/armv8/.