·《数据安全法》专题·

欧盟《通用数据保护条例》对我国数据安全立法的启示

张利国

(西华大学知识产权学院/法学院 四川成都 610039)

2018年5月欧盟《通用数据保护条例》(General Data Protection Regulation, 简称GDPR)[1]正式生效,对世界很多国家的数据保护都产生了非常重要的影响,但经过两年多的运行也暴露了一些问题。本文分析欧盟《通用数据保护条例》中与数据安全保护有关的主要内容,以及出台、运行两年多来发现的主要问题,从比较法的视角提出了对我国数据安全立法的启示。

欧盟GDPR是一个比较全面的数据保护立法,并不仅限于数据安全保护,其中涉及到数据安全保护的内容主要包括两方面的内容。

首先,欧盟GDPR中规定了涉及到数据安全的四项基础原则。第一,合法性、合理性和透明性原则,这个原则要求对个人数据应当以合法、合理和透明的方式来进行处理;第二,目的限制原则,要求数据的收集应当具有具体、清晰和正当的目的,对数据的处理不应当违反初始的目的;第三,数据最小化原则,要求数据的处理应当是为了实现数据处理目的而适当的、相关的和必要的;第四,数据的完整性与保密性原则,要求数据处理过程中应确保个人数据的安全,采取合理的技术手段、组织措施,避免数据未经授权即被处理或遭到非法处理,避免数据发生意外毁损或灭失。GDPR要求数据控制者有义务证明其遵守了上述各项原则。

其次,基于上述原则,GDPR规定了数据控制者和处理者的具体义务。这些义务主要包括:第一,通过设计以默认方式保护数据的义务,数据控制者在确定处理方式时,应当采取合适的技术与组织措施,并且在处理中整合必要的保障措施;第二,记录处理活动的义务,数据控制者和处理者都应当保持其处理活动的记录;第三,与监管部门合作的义务,在监管机构的要求下,数据控制者和处理者应当配合监管机构的工作;第四,安全处理数据的义务,数据控制者和处理者应当采取适当技术与组织措施,以便保证和风险相称的安全水平;第五,数据泄露通知义务,发生数据泄露后,数据控制者在知悉后应当在72小时内告知监管机构,数据处理者在获知个人数据泄露后,应当及时告知控制者;第六,开展数据保护影响评估的义务,当处理个人数据采用新技术,企业在开展个人数据处理之前,应当先行对新技术可能给个人数据保护带来的影响进行评估;第七,设立数据保护官的义务,要求数据控制者和处理者应当委任数据保护官。此外,GDPR对于违反上述义务的行为规定了巨额的行政罚款。

GDPR在生效执行两年多以来,在实践中产生了很多问题,这些问题对于我国制定数据安全法具有参考意义。

第一个问题是各国执法标准和力度不统一。由于欧盟特殊的体制,以及GDPR规定的内容本身比较原则和灵活,这给执法机构解释和适用条例提供了很大的空间,结果是GDPR在有的国家执行宽松,处罚力度小,有的国家执行严格,处罚力度大。这对我国数据安全立法中执法标准的一致性和执法主体的统一提供了启示。

基金项目: 国家社科基金项目"知识产权投机性牟利行为的法律控制研究"。
作者简介: 张利国,男,博士,主要研究方向为国际知识产权法、知识产权与反垄断、技术标准与知识产权、法律经济学、比较法理论。

第二个问题是 GDPR 给中小企业带来了很高的合规成本和不确定性。因为 GDPR 涉及了很多严格的程序、要求、义务和处罚规定,违反这些义务会导致巨额罚款,谷歌、Facebook 等大型的企业可以投资几百万美元使企业的运行达到合规,但是中小企业往往没有这样的资本和能力来确保合规,导致很多中小企业面临法律风险,经营活动受到很大限制。我国数据安全立法中要考虑合规和执法对相关中小企业的经营所带来的潜在影响。

第三个问题是数据安全保护和新技术开发和利用之间的矛盾。数据处理技术发展的如此之快,一些新技术的应用会不可避免的和条例中规定的义务产生冲突。如区块链要求所有的信息数据要进行记录,这就与 GDPR 的数据最小化等条款产生了矛盾[2]。GDPR 对数据安全保护的高标准要求,往往限制了企业对新技术的开发利用,也直接冲击了以免费服务获取顾客个人数据推送精准广告的互联网商业模式,直接影响了欧盟境内的互联网业务经营。GDPR 也对严重依赖大规模数据资源的大数据和人工智能技术的发展产生了一定的约束[3]。

第四个问题是对国际合作和跨境数据流动的阻碍。在 GDPR 的框架下,欧盟与中国、美国、日本等国的数据跨境合作交流都在执行层面存在一定的障碍。

欧盟 GDPR 执行过程中出现的上述问题对我国数据安全立法具有重要的启示作用。第一,要高度关注数据安全监管的执法统一和标准统一问题。我国近期面向公众征求意见的《中华人民共和国数据安全法(草案)》(以下简称《数据安全法(草案)》)第七条规定多个部门分工负责的监管规则,有可能导致各个部门执行标准不一致、不统一的风险,不同的部门监管的行业存在交叉和重叠,如果实施不一致的标准和细则会增加被监管对象的负担,影响监管的效率。《数据安全法(草案)》第七条规定的数据安全监管主体,需要增加一个机制以避免形成多头管理、互相推诿、互相掣肘的局面。此外,《数据安全法(草案)》不仅要考虑到部门之间的协调,还要考虑到各个地区之间的协调问题,因为数据的收集、存储、处理和流动以及利用是可能分散在全国各地的,具体的数据安全监管问题由哪个地区的机构来进行管辖有可能会存在着冲突和重叠的问题。

第二,数据安全保护措施要为新技术的应用预留政策空间,尽量避免给前沿技术的发展和应用造成不必要的障碍。因此《数据安全法(草案)》可以对前沿技术的应用规定安全影响评估程序和豁免机制。

第三,数据安全立法设定的保护措施和具体义务要考虑中小微企业的负担。法律中规定的看起来微不足道的义务在实践中有可能会给中小微企业造成比较大的负担。例如《数据安全法(草案)》第三十一条规定数据处理服务的经营者应当依法取得经营业务的许可和备案,这和我国当前发展营商环境的要求实际上是不相协调的,会给中小微企业进入增加一个门槛,要考虑许可和备案的目的是什么,这样的程序是不是必要的,要同发展良好营商环境的整体要求衔接,此外还要考量第四十四条对数据处理行业发展的影响。

第四,在数据安全事件的报告义务方面,《数据安全法(草案)》第二十七条只规定了数据安全事件的报告义务,但是没有规定具体的报告时限。我国可以借鉴 GDPR 的经验,设定一个明确的报告时限,在发生数据安全事件后,要在规定的时限内进行报告,避免隐瞒和拖延,有利于及时对事件进行处理。

第五,要考虑到我国企业走出去在海外经营过程中,遵守不同国家和地区的数据管理法规同我国数据安全法中规定的义务相冲突和衔接问题。

参考文献:

[1] EUR-LEX. Regulation(EU)2016/679 of the European parliament and of the council of 27 April 2016. [EB/OL]. (2016-04-27)[2020-01-10].https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[2] JESSIE P. The GDPR: The biggest threat to the implementation of blockchain technology in global supply chains. UMKC Law Review[EB/OL].[2017-07-06]. https://umkclawreview.org/2018/12/27/fall-2018-student-comment-selection.

[3] MATTHEW R A H. The GDPR and the consequences of big regulation. Pepperdine Law Review[EB/OL].[2020-05-01]. http://lawcomm.pepperdine.edu/blogs/review/the-gdpr-and-the-consequences-of-big-regulation.