从 GDPR 看我国《数据安全法》的立法方向

□徐 漪 沈建峰

【内容摘要】欧盟 GDPR 的制定和实施，对个人数据的保护和数字经济的发展，产生了深刻而广泛的影响，其立法背景、渊源、动机、目标，以及实施的机制与效应，具有理论和现实的参考价值和借鉴意义。我国应当从平衡个人信息安全与数字经济发展的关系、合理制定个人信息保护的管辖范围和力度、努力突破数字经济发展的壁垒等三个方向推动相关立法的进程。

【关键词】GDPR; 个人数据; 数据安全; 数字经济

【作者单位】徐漪，上海社会科学院信息研究所

【通讯作者】沈建峰，国家无线电监测中心

被称为“史上最严数据保护法”的欧盟《通用数据保护条例》(General Data Protection Regulation，简称“GDPR”) 已经实施半年，从其效果看，世界各大互联网企业都已表示服从该法监管，并已经开始调整各自的隐私和数据保护政策，最新判例也已出炉。GDPR 的影响恐怕也才刚刚开始。事实上，作为超国家联盟的欧盟，能通过立法并获得各成员国议会批准，本身必然是各方利益妥协的结果。仔细研读《GDPR》可以看出，在业界关注的广泛义务和高额罚款背后，GDPR 在数据主体权利，数据控制或处理者的正当利益、经济发展、社会公共利益等各方之间的努力寻求着动态平衡，以风险管理为基础，提供多种风险规制路径，将平衡的立法思路贯彻到具体的制度设计之中。通常欧盟立法文本中习惯采用“个人数据”(personal data) 的表达，我国习惯采用个人信息的表述，二者内涵差别不大，本文原则上不加区分，视作同一概念直接采用。

一、GDPR 历史渊源及背景

(一) 立法渊源。欧盟关于网络安全法律的规定始自 1992 年的《信息安全框架决议(92/242/EEC)》，内容涉及信息安全需求、战略框架、规范和标准、操作和功能等。随后欧盟又出台了几个个比较重要的法律文件，如：1995 年 10 月颁布的《关于涉及个人数据处理的个人保护以及此类数据自由流通的指令(95/46/EC)》(以下称“95 指令”)、1999 年 1 月的《关于打击互联网上非法和有害内容以促进更安全使用互联网的若干年度共同体行动计划(276/1999/EC)》和 1999 年 5 月的《关于打击计算机犯罪协议的共同宣言(1999/364/JHA)》。其中 95 指令是全球较早涉及个人隐私与数据保护领域的法律，亦是 GDPR 最直接的源头。

进入 21 世纪，欧盟掀起了一个信息安全立法的高潮，如 2005 年 2 月通过的《关于打击信息系统犯罪的欧盟委员会框架决议》，2003 年 2 月的《关于建立欧洲网络信息安全文化》，2004 年 3 月的《建立欧洲网络和信息安全机构的规则》，2007 年 3 月 2 的《关于建立欧洲信息安全社会战略的决议》等，欧盟区域的信息安全上升到社会安全的高度，但涉及个人数据保护的法令并没有重大变化，依然是“95 指令”。

(二) 欧盟个人数据安全立法基础。欧盟针对个人数据的保护源于人的基本权利或人权保护，从欧洲普遍接受的人权观念来看，每个人都是独立的个体，而个人数据由人的活动所产生，因此可以看作个人的“延伸”，所以个人数据应当归属于个人这一数据主体，所有涉及个人数据的处理必须以体现和尊重其个人意志为基本前提。《GDPR》立法的基本宗旨，就是保障数据主体对个人数据的处理事务的自主、自治、自决。

具体来看，欧盟及其成员国的个人数据保护立法旨在落实欧洲委员会 1981 年通过的《个人数据自动化处理中的个人保护公约》，该《公约》的基础是《欧洲人权公约》中个人应当享有的 17 项基本权利和自由，其中的第 8 条特别规定，尊重私人和家庭生活的权利。因此，“95 指令”中，赋予个人数据主体很多权利，以保障数据主体知晓有关他的何种数据被谁用于何种用途，并能够及时更正错误、删除或拒绝处理，体现对个人的尊重。在这个基础上，2000 年《欧盟基本人权宪章》明确将个人数据保护作为一项独立的基本权利加以规定。

(三) GDPR 的数字经济背景。早在 1993 年欧盟成立之初，欧盟就发布了《增长、竞争、就业——迈向 21 世纪的挑战和道路》白皮书，明确了发展数字经济的重要性，并提出了“创建欧洲信息社会、迎接 21 世纪挑战”战略。1996 年 3 月，欧盟理事会签署《关于数据库的法律保护的指令(Directive 96/9/EC)》，其目的就是激励数据产业的发展。到 2010 年，欧盟发布《2010 倡议——为了促进增长和就业的欧洲信息社会》，提出发展数字经济三大支柱：第一，建立市场导向的数字经济规则体系；第二，推动与私营部门合作，提高欧盟的创新和技术领导力；第三，提供高效、便利的公共服务，建立包

容性的欧洲信息社会，作为建立数字经济规则体系的重要步骤，2012 年 1 月欧洲议会公布了 GDPR 草案。

2014 年 7 月，欧盟委员会主席容克对新一届欧洲议会发表政策讲话，提出欧洲“数字一体化市场”战略，旨在为个人和企业提供更好的数字产品和服务，创造有利于数字经济发展的环境，最大化地实现数字经济的增长潜力。欧盟相信，“数字一体化市场”能激励个人和企业公平的无缝访问和在线活动，从而促进欧盟数字经济发展，确保欧洲在全球数字经济中的地位。这一战略极大地推进了 GDPR 的制定。由此可见，GDPR 并不仅仅是在信息科技迅速发展情况下，欧盟对欧洲公民人格尊严和人格自由的重申，而是结合了经济价值和社会效应，综合个人数据保护与促进数字经济发展等多重因素考量的成果。

二、GDPR 主要内容

作为欧洲议会通过的法律，GDPR 的法律位阶比 95 指令高出许多，95 指令不具有强制性，不能直接适用于各成员国，而需要各国经过国内立法才能实际落实，而 GDPR 则属于欧盟立法，欧盟各国必须遵守，从而统一了欧盟内部个人数据保护标准，为创造欧盟数字一体化市场奠定了基础。

GDPR 正文共 11 章，99 条，建立了完善的数据管理体系，针对数据主体权利、数据控制与处理机构义务、数据跨境传输、独立监管以及责任与处罚等多项严格规定，多处具有创新。

（一）数据主体权利。GDPR 全面完善和细化了个人信息权利，数据主体享有访问权、更正权、反对权、删除权、数据可携权以及限制自动化决策等权利。其中，删除权、数据可携带权、限制自动化决策权是全新设置：删除权赋予了数据主体撤回同意使用或删除个人数据的权利；数据可携权赋予了数据主体转移其个人数据的权利，在技术许可的条件下，数据主体有权直接将个人数据转移至他处，而数据控制者应当提供必要的支持；免受自动化决策权是指在特定情形下，数据主体不受数据自动化处理规则制约等。

（二）数据控制者义务。GDPR 将数据操作分为控制与处理两个部分，以“数据控制者”为核心，规定数据控制者的必须履行一定的义务，从而将数据保护的责任落实。而数据处理者的责任则原则上通过合同进行具体规定。控制者的义务分为一般义务和特殊义务两部分，所有数据控制者均须遵守一般义务，如隐私设计、数据处理记录、安全保障措施和数据泄露通知等。其中数据泄露通知义务明确要求，发现数据泄漏事件 72 小时内，数据控制者原则上应当报告监管机构，如果数据泄露会对个人带来较高风险时，必须通知个人。特殊义务则是符合某些条件的数据控制者才须遵守的义务，如设置数据保护官和数据保护影响评估等。

（三）数据跨境传输限制。与欧盟内部数据自由流通不同，对于数据向欧盟境外的传输，GDPR 做出了严格规定：对于数据向域外国家和组织的数据传输，采用类似白名单制度的“充分性认定”机制，以数据的适足、充分保护为首要参考，划分了三个层次：第一层次，目标国的个人数据保护水平达到了欧盟认定的“充分保护水平”，则数据流动没有限制；第二层，如果目标国没有获得充分性认定，则企业应对输入的数据提供一定的保护策略，诸如有约束力的公司规则、商业合同、第三方认证等；如果上述条件都达不到，则适用第三层，可以采取列举有限数据传输减损清单的方式，如数据主体同意的转移、为了数据主体利益实行的必要转移以及公共利益等。

（四）监管机制。GDPR 建立了完善的个人数据保护监管机制，授予成员国监管机构以调查权、矫正权、授权与建议权、司法参与权等诸多权力。同时，由于欧盟及各成员国内部的法律规定，不同的数据监管机构有所分工，数据处理过程中存在跨境转移、数据处理等较为复杂的情形，经常出现一个数据监管机构难以完成对整个数据处理过程的监管的现象。因此，GDPR 中对监管机构的联合行动也做出了相应规定，以期通过不同区域、不同层级之间数据监管机构的相互配合，达到对数据处理过程的全方位监管，减少数据处理活动中的违规行为，避免数据主体的合法权益受到侵犯。

（五）法律责任。GDPR 对数据控制者或处理者违反规定设置了民事责任和行政责任。GDPR 规定，数据主体可依据所遭受的实际损失提请赔偿，但这仅仅是数据处理者面对的民事赔偿责任，其行政责任则要面临更大的处罚。根据违反规则的程度不同，GDPR 规定了两档罚则：第一，数据控制者违反默认隐私保护设计、数据安全保障、数据泄露通知、数据影响评估等行为，处 1,000 万欧元或上一年度全球营业额 2% 的罚款。第二，数据控制者违反数据处理原则、同意规则，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。

三、GDPR 对我国的借鉴意义

进入 21 世纪以来，信息技术的发展已经催生出了一种新的经济形态，诸如信息经济、网络经济、数字经济、分享经济或共享经济、知识经济等，尽管目前对此还尚未达成称谓上的共识，但其内涵基本一致，都是指以数字化的知识和信息为关键要素，以信息网络为基础，依靠信息技术提高经济效率，优化经济结构的经济活动的集合。

进入 21 世纪，我国的数字经济发展迅猛，但是与数字经济密切相关的个人信息保护方面，相比欧盟，存在着明星差距。过去几年层出不穷的电信诈骗、网络诈骗等犯罪活动，严重影响了我国在个人信息保护方面的声誉，我国涉及个人信息保护的立法非常分散，相关规定零星分布在不同层阶的法律、法规、部门规章中。针对已经纳入立法计划的我国《数据安全法》，欧盟 ODPR 具有较大的借鉴意义。

（一）平衡个人信息安全与数字经济发展的关系。GDPR 在序言中指出 “个人数据的处理应当坚持以为人类服务为导向。个人数据保护并非绝对权利，必须根据比例原则考虑其在社会中的作用，并与其他基本权利相平衡。”这种动态利益平衡的理念，在 GDPR 的第 6 条“数据处理的合法性基础”中再次得到体现，GDPR 为数据控制者和处理者提供了数据处理的多种合法性基础，除了数据主体同意外，还包括了履

行合同、履行法律义务、重大利益平衡、公共利益平衡、正当利益平衡等多重路径，均可作为数据处理合法性的充分非必要条件，由数据控制者和处理者选择。一方面是考虑到特定情况下无法也无需征得数据主体同意的情况（如控制者在履行法定义务时）；另一方面也避免了如果将“主体同意”作为唯一性合法依据，很有可能在事实上架空了这一制度的设定初衷，增加数据主体负担，降低其行使数据权利的实效性。

GDPR 以“识别性”作为核心，对个人数据进行了不同层次的界定，从而为其设定了不同的保护程度，实现了数据保护义务与流通处理之间的平衡。识别性概念是一个从人群中把个人“挑选”出来的过程，根据数据对主体的识别精度差异，而设置不同的风险评估结果，并设置不同的保护规则。根据可识别程度，GDPR 大致将数据划分为五个层次，其处理风险和相对应的义务从高到低依次递减。

1. 已识别的个人数据。这类数据通常可以将个人轻易地识别出来，如身份识别号码、生物识别数据等。这类数据被 GDPR 给予了最强保护，例如基因数据、生物识别数据等是禁止被处理的。

2. 可识别的个人数据。这类数据一般需要跟其他数据结合后才能识别到个人，例如位置数据、浏览记录等。

3. 假名化数据。一般指经过技术化处理之后的个人数据，在不使用附加信息的情况下不能与特定主体产生关联。例如使用技术手段处理的手机号码：138＊＊＊＊2345，这种假名化处理可以大幅降低风险。

4. 无需再恢复识别的数据。当后续的数据处理已经无需再识别到个人时，一些用来恢复原始数据的附加信息就无需保留。相应地，数据主体更正、删除等权利也就不能行使。

5. 匿名化数据。匿名化数据指已经无法与任何已识别或可识别的主体相关联的数据，多见于统计数据形式。这种数据无需适用 GDPR。

（二）合理制定个人信息保护的管辖范围和力度。互联网的高度发展，尤其是个人信息的低成本（或零成本）、零时间跨境流动，对主权国家的管辖和监管带来了新的挑战。应对突破这一难题，GDPR 摒弃了传统的“属地管辖”原则，采取的了“保护性管辖”这一新方式，拓展了欧盟的管辖范围，即不论数据控制者、处理者是否在欧盟地域上，或其处理行为是否发生在欧盟之内，均适用于 GDPR。这一长臂猿管辖原则和“一站式”执法，也为数据保护管辖在法律上提供了新思路，值得借鉴。

GDPR 对违规的处罚力度可谓空前，设置了令企业望而生畏的高额罚金。一方面是由于目前互联网巨头大多全球布局，而且其中没有欧盟企业的身影；另一方面是由于这些企业财大气粗，对一般性的罚款无动于衷，不足以令它们自觉遵守法规。虽然这大大抬高了小企业合规成本，但 GDPR 也充分关注了数据控制者为控制和管理风险所做出过的努力，对企业数据保护设置了多重问责，希望数据控制者必须采取“足够的措施”来确保其数据安全。这也意味着，数据控制者的数据保护努力永远不会被忽视，在数据安全影响评估和问责机制中会得到相应的回报。数据控制者的保护程度包括以下几类。

1. 数据保护官制度。企业设立具有数据保护专业知识的独立数据保护官，直接向高层管理汇报，向监管机构报备，其联系方式必须公开。

2. 文档化管理制度。数据控制者必须建立相应文档，记载其数据处理活动，如数据处理的目的、类型、安全保障措施以及数据转移的接收者等。

3. 数据泄露报告。一旦发生数据泄露事故，数据控制者必须在事发 72 小时内，将事件报告给指定的监管机构。

（三）努力突破数字经济发展的壁垒。在数字经济高速发展的背景下，数据尤其是个人数据已经成为人们改变市场、创造价值和获得知识的新源泉和新动能，是经济增长的重要资源。如何化解数据保护与数据跨境流动之间的冲突，是普通货物贸易关税之后，数字经济时代国际社会必须要解决的重要问题。同时，数据跨境流动也会造成国家安全、公共道德和个人数据泄露等隐患，GDPR 将个人信息保护程度作为处理数字经济时代国际经济和政治关系的关键因素，在同一内部各成员国法规政策的同时，对数据跨境输出做出了明确限制，只有获得欧盟“充分性认定”的国家，遵从欧盟批准的企业级数据保护策略的企业，才能进入欧盟单一市场，这一限制，无疑形成了新的数字经济壁垒。

相比而言，我国在个人信息保护方面，还有较大差距。我国应充分借鉴 GDPR 经验，加速《数据安全法》立法，通过立法过程，宣传、普及个人信息保护意识，提高个人信息保护水平，不仅是满足国内日益高涨的个人信息保护要求的切实措施，更是促进我国数字经济发展，消除经济壁垒的一条捷径。

【参考文献】

[1] 李维扬. 通过设计保护隐私 [J]. 信息安全与通信保密，2018，1

[2] 吴沈括. 欧盟《一般数据保护条例》（GDPR）与中国应对 [J]. 信息安全与通信保密，2018（06）

[3] 罗斯. 欧盟数据隐私新规或制造贸易壁垒 [EB/OL]. http://www.ftchinese.com/story/001077857? archive last visited on Jan 17，2019

[4] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data（CETS No. 108，Strasbourg，28/01/1981）

[5] Summary report of the public consultation on the evaluation of Directive 9 6/9/EC on the legal protection of databases [EB/OL]. https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-legal-protection-databases last visited on Jan. 15 2019

[6] President Junckers Political Guidelines. A New Start for Europe: My Agenda for Jobs，Growth，Fairness and Democratic Change [EB/OL]. https://ec.europa.eu/commission/publications/president-junckers-political-guidelines_en last visited on Jan. 15 2019