

欧盟数据保护立法改革之发展趋势分析

张敏, 马民虎

(西安交通大学法学院, 陕西 西安 710049)

摘要: 欧盟数据保护立法改革是世界各国关注的焦点。阐述了欧盟数据保护立法改革致力于提升数据保护立法的统一性与执法的一致性、高效性, 强化对个人数据权利的保护力度, 加强欧—美个人数据保护的双边合作, 重建数据流通信任机制。提出了中国应关注与思考欧盟数据保护立法改革之发展趋势带来的深远影响。

关键词: 数据保护; 立法; 执法; 数据权利; 数据流通信任机制

中图分类号: D922.16

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00030

Analysis on the development trend of EU data protection legislation reform

ZHANG Min, MA Min-hu

(Law School, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: EU data protection legislation reforming has become the attention by countries in the world. That EU data protection legislation reforming concentrated on promoting the unity of legislation and the consistency and efficiency of law enforcement and reinforcing the protection of personal data rights, enhancing EU-US bilateral cooperation in the protection of personal data, rebuilding the trust mechanism of data flow was stated. That China should focus on the profound influence power by the development trend of EU data protection legislation reform was proposed.

Key words: data protection, legislation, law enforcement, data right, trust mechanism of data flow

1 引言

近年来, 欧盟数据保护立法改革的持续推进成为信息时代的一大盛事, 牵动着全世界的目光。欧盟数据保护立法改革是内忧和外患共同作用的结果。大数据、云计算以及数据挖掘与分析技术的快速发展使制定于 20 年前的《1995 年 10 月 24 日欧洲议会与欧盟理事会关于个人数据处理中个

人权利保护及促进数据自由流通的第 95/46/EC 号指令》(以下简称《指令》) 难以有力应对个人数据被非法窃取、破坏和监控的难题。《指令》在法律规则的设计上多具有开放性且统一解释机制匮乏, 各成员国在实施中享有较大的自由裁量权, 再加上成员国数据监管机构的权力差异大、缺乏有效合作以及监管权弱化, 导致《指令》在实施中的不确定 (uncertainty) 以及不一致性执行

收稿日期: 2016-01-20; 修回日期: 2016-02-01。通信作者: 张敏, fish_law@163.com

基金项目: 2015 年国家社科基金资助项目 (No.15BFX050); 信息网络安全公安部重点实验室开放课题基金资助项目 (No.C13604)

Foundation Items: 2015 National Social Science Foundation (No.15BFX050), Ministry of Public Security's Information Network Security Key Laboratory Item Foundation (No.C13604)

(inconsistent enforcement) 尤为突出^[1]。云环境下, 数据跨境流动已成为常态, 而《指令》对数据跨境流动的充分性(adequacy)保护标准严苛而繁琐, 减损了欧盟对于企业投资的吸引力。除商业领域外, 刑事与司法合作领域内的个人数据收集与使用也因缺乏透明度而保护乏力。

为解决内忧, 2012年, 欧盟委员会提出“一揽子”改革方案, 主要包含2项立法建议: 一项是《欧洲议会和欧盟理事会关于个人数据处理中个人权利保护及促进个人数据自由流通条例提案》(简称《条例提案》); 另一项是《欧洲议会和欧盟理事会针对主管当局为预防、调查、侦查和起诉刑事犯罪或执行刑事处罚的目的而进行的个人数据处理进行保护以及强化该数据的自由流动指令提案》(简称《指令提案》)。2014年, 欧洲议会和欧盟理事会已分别对《条例提案》完成了一轮审议, 《条例提案》的基本原则已被欧洲议会和欧盟理事会所认可。但因政治立场的差异以及企业的频繁游说, 2015年欧盟三方机构还未对《条例提案》的某些条款达成一致意见, 其最终立法文本的确定还需欧盟三方机构的磋商与妥协。

“棱镜门”丑闻使欧—美在数据跨境流动与数据保护双边合作中的信任降至冰点。为应对外患, 欧盟加速推进数据保护立法改革的步伐, 积极与美国展开磋商与合作, 以期重建欧—美数据流通的信任机制。本文试图在分析与评述欧盟数据保护立法改革基本内容及最新动向的基础上, 对欧盟数据保护立法改革的三大发展趋势作出分析。

2 提升立法的统一性与执法的一致性、高效性

为改善和消除《指令》在实施中的不确定性与不一致性, 欧盟从数据保护立法与执法的2个主要环节入手, 旨在通过改革既有规则和创设新规则, 提升数据保护立法的统一性与执法的一致性、高效性。

2.1 从指令到条例

根据《欧洲联盟运作条约》第288条的规定, 指令针对每个成员国而不是当事人, 成员国有权选择具体的形式、方法制定国内法以执行指令,

而条例生效即成为国内法的一部分, 无论对于成员国还是当事人都具有广泛的约束力。欧盟将个人数据保护立法从指令提升至条例, 以确保“一个欧洲一部数据保护法”, 这一改革事项在欧洲议会与欧盟理事会层面取得基本共识。较之《指令》, 《条例提案》在生效后将带来更高度上的统一适用, 特别是一些成员国分歧较大的核心的法律概念与规则的统一定义将有效降低法律不确定的负面影响。然而, “一个欧洲一部数据保护法”将会产生新的问题: 如何有效平衡法律的确信性与灵活性以及基线保护与行业特殊保护之间的关系? 《条例提案》赋予了欧盟委员会一项权力——当某些特殊条款需要一致性执行或非重要的条款需要被补充修正时, 欧盟委员会可采用实施法案(implementing act)与授权法案(delegated act)。第86条限定了欧盟委员会采用授权法案的26种具体情形, 欧洲议会或欧盟理事会也可随时撤销欧盟委员会的授权权力。为限制欧盟委员会权力的膨胀化, 欧洲议会和欧盟理事会在修正案中极大缩减了欧盟委员会可采用授权法案的范围。

2.2 在执法中建立“一站式”服务机制

为解决《指令》在成员国的不一致性执行这一棘手问题, 欧盟委员会在《条例提案》中提出“一站式(one-stop-shop)”服务机制这一关注度极高的改革事项。“一站式”服务机制主要依赖于以下3个组成要素。一是数据控制者与处理者的主营业机构(main establishment)决定主数据保护机构(main data protection agency)。《条例提案》第51条规定, 数据控制者与处理者在欧盟境内多个成员国设有分支机构, 则其数据处理行为可选择由主营业机构所在地的成员国的数据保护机构统一行使管辖权。二是“一站式”服务中不同成员国数据保护机构与主数据保护机构之间的协作机制。第55条、第66条规定了“一站式”服务中不同成员国数据保护机构与主数据保护机构之间的协作机制。三是成员国数据保护机构对于条例进行解释与实施时的一致性确保机制(consistency mechanism)。根据第57条至第63条, 成员国数据保护机构的实施旨在产生法律效力, 并在影响一个以上成员国的相关决策前, 应将决策的内容告知欧盟委员会和欧盟数据保护理

事会 (EU Data Protection Board), 并应将两者所发表的意见予以参考。第 60 条规定, 当欧盟委员会怀疑成员国数据保护机构不能保证对条例的一致性进行执行时, 可以以合理理由要求成员国数据保护机构在一定期限内中止执行。

在立法审议中, “一站式”服务机制引起了欧盟委员会、欧洲议会、欧盟理事会这三方政治团体极高的关注与争论。欧盟委员会是“一站式”服务机制的倡导者——欧盟委员会副主席 Viviane Reding 认为: “一站式”服务是取得个人、企业、数据保护机构‘三赢’局面的唯一路径^[2]。在“一站式”服务模式, 在欧盟多成员国设置分级机构的跨国企业只需要与一个成员国数据保护机构打交道, 而无需耗费精力应对多个成员国的法规遵从难题, 商业决策效率因此而大大提升; 欧盟境内的居民遭遇权利侵害时可直接向居住地数据保护机构投诉, 极大方便了跨国诉讼与维权; 在处理跨境纠纷时, 为确保本国数据保护机构所做出的处理决定被其他国家的数据保护机构予以认可和执行, 成员国数据保护机构的沟通与合作将更为紧密, 有利于提升调查与决策效率。

但欧洲议会、欧盟理事会及某些成员国对“一站式”服务机制却持有不同的声音。欧洲议会担心“一站式”争议解决机制会导致更多的腐败问题, 损害消费者的权利^[3]。顾及到少数成员国对“一站式”服务的反对以及欧盟委员会逐渐膨胀的权力, 欧盟理事会认为, “一站式”机制应仅适用于至关重要的跨境案件, 主数据保护机构应定位为协调者而非决策者, 若主数据保护机构未与其他利益相关的数据保护机构达成合意, 应将最终的决定权交予欧盟数据保护理事会^[4]。随后, 欧盟理事会的意见遭到质疑与批评: 企业认为新的数据保护法并未给其带来多少“胡萝卜”, 而欧盟理事会对“一站式”机制的修订意见将剥夺企业最大的一根“胡萝卜”^[5]。欧盟委员会副主席 Vivian Red 认为理事会的修订意见将使“一站式”机制变为空壳, 企业和公民将是直接的受害者^[6]。欧盟成员国提出了对“一站式”机制的完善意见, 爱尔兰政府部长 Dara Murphy 呼吁在条例中引入审查条款 (review clause) 以确保“一站

式”机制的有效执行, 英国司法大臣 Lord Faulks 认同其观点, 并进一步指出, 应对欧盟数据保护理事会接手的案件进行定量过滤 (quantitative filter), 以提高决策的效率^[7]。综上, 尽管“一站式”服务机制的具体制度模型还未敲定, 但可以预测的是该制度将在欧盟委员会、欧洲议会、欧盟理事会三方的争议、磋商与妥协中逐渐清晰与完善, 通过变革现有立法规则, 提升欧盟数据保护执法的一致性、高效性与协调性将是众望所归。

2.3 优化数据保护机构的权力配置, 加强有效合作

为提升法律实施高的有效性与协调性, 《条例提案》优化了数据保护机构的权力配置。在欧盟层面, 欧盟数据保护理事会取代第 29 条工作组 (Article 29 Data Protection Working Party), 成为重要的欧盟数据保护监管机构。《条例提案》第 65 条至第 68 条明确了欧盟数据保护理事会的独立地位以及角色定位与职责等。欧洲议会在修正案中对欧盟数据保护理事会的基本职责做了更多扩充性规定, 例如, 可对欧盟委员会实施授权法案与实施法案及数据保护行为准则 (code of conduct) 与认证机制 (certification mechanism) 的标准制定提供建议等^[3]。此外, 与《指令》相比, 《条例提案》第 71 条的变化在于规定了欧盟数据保护理事会的秘书处的设置权由欧盟委员会的司法、自由和安全总司转移到欧盟数据保护专员 (EU data protection board supervisor), 这种关系调整进一步强化了欧盟数据保护专员的权力, 权利的释放也使欧盟委员节约资源以专注解决其他问题。

在成员国层面, 《条例提案》第 46 条第 1 款增加了成员国数据保护监管机构与欧盟数据保护理事会及其他监管机构之间的合作义务, 第 47 条增加了对各数据保护监管机构的独立性的规定, 第 53 条增加了各数据保护机构对行政违法行为的处罚权, 处罚的重点对象为第 79 条第 4 款、第 5 款、第 6 款所规定的行政违法行为。欧洲议会在立法修正案中对上述条款予以认可。行政处罚权使成员国数据保护机构拥有了执法的“牙齿”, 企业将更重视个人数据保护这一企业合规问题。

2.4 明晰、简化数据跨境流通规则，促进数据自由流动

云环境下数据跨境流动将成为常态，促进数据自由流通是欧盟数据保护立法的基本价值取向之一。《指令》第25条规定，在不违反各成员国根据指令所制定的国内法的情况下，以数据处理为目的向第三国转移数据时，成员应当确保第三国达到了充分性保护水平。与之相比，《条例提案》不仅规定了充分性保护标准，又增加了数据控制者和处理者采取个人数据保护的适当保护措施（appropriate safeguard）作为数据跨境流通的基本条件。第42条对适当保护措施的内容作了明确规定，主要包括具有约束力的公司规则、欧盟委员会制定的标准合同条款、成员国数据保护机构制定的标准合同条款、成员国数据保护机构特别批准的标准合同条款。欧洲议会和欧盟理事会在立法修正案中进一步扩展了适当保护措施的范围，欧洲议会在修正案中引入欧洲数据保护印章（European data protection seal）制度，而欧盟理事会倾向于引入经认证的行为准则与认证机制作为补充^[3]。总之，适当保护措施多元化无疑为数据跨境流通打开了另一条主要通道。

3 强化个人数据权利的保护力度

保护个人数据权利在欧盟被视为公民的一项宪法性权利。新技术带来的挑战使欧盟认识到个人数据保护的紧迫性。欧盟将强化数据主体的权利保护作为数据保护立法改革最重要的政策目标之一，其实现方式具体如下。

3.1 深化个人数据保护的透明度原则

透明度原则是欧盟数据保护立法的基本原则。提升个人数据保护的透明度是增强数据主体个人数据控制力，保护个人数据权利的基本途径之一。《条例提案》进一步深化了该原则。第14条规定，当数据主体的个人数据被收集时，至少应告诉数据主体数据控制者的身份、联系方式、代理人及数据保护专员，数据的处理目的，存储期限。数据主体享有访问、更改、删除或拒绝处理的权利以及向监管机构提起申诉的权利等。欧洲议会在修正案中进一步深化了数据保护的透明度原则：一是增加标准化信息政策（standardised

information policy），即数据主体在履行《条例提案》第14条规定的告知义务前，应告知数据主体其个人数据被收集时是否超过最小必要限度及特定目的、是否散布给商业化的第三方机构、是否被出售或出租、是否以加密形式存留等；二是扩大了数据控制者在收集个人数据时应履行的告知义务，例如，当数据控制者采用数据分析（profiling）技术采集个人数据时，应告知数据主体数据分析技术的方法及预期的实施效果以及个人数据是否在连续的12个月内被提供给公共机构^[3]。透明度原则的深化使数据主体清楚地判断所做出的积极同意是否是有必要，这种有效性判断可防止数据控制者依据个人数据而产生用户歧视，并促进个人数据在保存与使用中的问责机制的建立^[8]。

3.2 提升对数据主体的赋权的力度

一是引入数据主体的积极同意规则，以强化数据主体对个人数据的控制能力。《指令》并未明确个人同意是积极同意还是消极同意，而欧盟委员会在《条例提案》中引入了积极同意（explicit consent）规则。第4条规定，数据主体同意是指数据主体自愿给出的具体的、有根据的、详细的表明其意愿的说明，该说明可以通过声明或明确肯定的行动表示。第7条规定，数据主体还有权在任何时候撤回同意。欧洲议会和欧盟理事会在修正案中对积极同意规则做出进一步补充，欧洲议会认为同意需由数据主体自由（freely）做出，且应像做出同意般易于撤回。当数据主体基于特定目的做出同意时，若特定目的不存在或不符合数据收集的目的，则该同意无效，欧盟理事会认为，数据控制者证实数据主体做出的同意是积极同意。相对消极同意，积极同意无疑是更为严格的权利保护措施；二是增加数据遗忘权与删除权（right to be forgotten and right to erasure）与数据携带权（data portability）两大创新性权利。《条例提案》第17条规定了数据遗忘权，即在法律限定条件下，数据主体有权要求数据控制者立即删除其直接控制的个人数据。当被要求删除的个人数据已经被数据控制者公开，则数据主体有权要求数据控制者采取一切合理措施（包括技术措施），通知处理个人数据的第三方按照数据主体的要求

删除个人数据的连接、副本或复印件。欧洲议会在修正案中将数据遗忘权与删除权改为数据删除权,增加规定数据删除权的行使应基于法庭或监管机构的最终裁定^[9]。随后,在欧盟理事会还未就此达成一致意见时,欧盟最高法院已在谷歌西班牙案中通过不可上诉判决的形式对数据遗忘权加以确认。被遗忘权的提出增加了数据主体对个人数据的控制能力,也吻合了大数据时代人们对个人隐私保护的强烈需求。但数据遗忘权的提出在欧盟引发了巨大争议,言论自由、数字经济发展、科研进步与国家安全成为反对者对该权利攻击的矛头。第18条规定数据携带权指数据主体可从数据控制者处获取个人电子化数据并将其转移到其他数据控制者的服务系统的权利。这一规定在欧洲议会法案审议中被删除,但被欧盟理事会予以保留。

3.3 强化企业的信息安全治理义务

强化企业信息安全治理义务,提升社会整体的个人数据权利保护力度是欧盟数据保护立法改革的一个重要议题。在企业管理架构中增设数据保护专员(DPO, data protection officer),明确其法律责任是企业信息安全治理的路径之一。尽管欧盟委员会、欧洲议会及欧盟理事会已就增设数据保护专员达成了一致意见,但对具体的制度设计仍有不同意见。欧盟委员会在《条例提案》中规定雇员人数超过250人的数据控制者应在内部指定数据保护专员。这一规定在欧盟成员国引起了较大争议,给企业带来较大的行政与财务负担成为最主要的攻击矛头。随后,欧洲议会在法案审议中进一步提升了企业任命DPO的门槛:任何数据控制者若在连续12个月内涉及处理超过5000名数据主体的个人数据都应任命为企业数据保护专员^[3]。这一变化使企业数据保护专员的任命门槛从企业规模转向企业数据处理行为产生的影响,这也意味着不是所有的大公司都需履行这一法定义务,而一些中小型的大数据公司也需履行这一义务。欧盟委员会、欧洲议会及欧盟理事会均一致认可企业数据保护官应具有独立的地位,对内监督及记录数据控制者与处理者对条例的实施与应用情况,对外回应数据主体的请求或与数据监管部门开展合作。

其次,在技术与管理层面,欧盟委员会将数据控制者与处理者的设计隐私(privacy by design)与数据保护影响评估(impact assessment)义务纳入立法。《条例提案》第23条规定隐私设计保护指数据控制者在支付合理的实施成本下,采用适当的技术措施、组织措施及程序,使数据处理行为符合《条例提案》规定的标准及对数据主体权利的保护要求。欧洲议会在修正案中进一步倡导设计隐私的标准化,并将该义务主体扩大至数据处理者。而欧盟理事会则进一步规定了设计隐私的认证机制,并将匿名化(pseudonymisation)个人数据纳入设计隐私的保护范畴^[3]。设计隐私的价值在于将企业信息安全治理义务渗透至技术和产品的设计开发阶段,有利于企业对条例的遵从与个人权利的保护。第33条、第34条规定了数据保护影响评估,即数据控制者、数据处理者应对拟建数据处理系统进行评估,以识别系统对数据保护可能产生的特定风险,评估的内容至少应包括对拟进行的数据处理活动的描述、对数据主体权利造成的风险以及应对风险的措施。欧洲议会在修正案中进一步明确了数据保护影响评估所针对的特定风险应涉及从数据收集、处理到销毁的全生命周期管理,而欧盟理事会认为当采用新技术时,数据安全风险评估尤其应考虑到数据处理行为的性质、范围、目的等因素^[3]。数据影响评估可作为有效的法律遵从工具,提前预测到数据处理活动是否对个人数据权利产生影响以及影响的程度并给出规避风险的实际建议,还可有助于数据控制者或处理者将隐私影响评估与风险管理标准化相衔接^[10]。

3.4 增加对数据侵权行为的惩罚力度与对数据主体的有效救济

增加对侵权主体的惩罚力度与对数据主体的有效救济是强化个人权利保护的有力武器。遗憾的是《指令》并未明确规定对侵犯个人数据权利的惩罚措施与对数据主体的救济方式。《条例提案》第79条详细规定了对不同数据违法行为的各种严厉处罚,对自然人最高可施行25万欧元至100万欧元的罚款,对企业最高可处罚其全球年收入的0.5%~2%,对无商业利益的个人、雇员在250人以下的非以数据处理为主业的企业可免除上述

行政处罚。尽管欧盟委员会所设定的处罚标准已经非常严厉，欧洲议会在修正案中将对企业罚款的最高金额提升至1亿欧元或全球年收入的5%^[3]，这将是《条例提案》处罚标准的2倍。可以预见，如此大金额的行政处罚将迫使数据控制者与处理者重视个人数据保护的法规遵从与个人数据保护。

此外，《条例提案》还详细规定了对受害数据主体的救济方式。《条例提案》第73条至第75条规定了任何自然人和法人都有权要求成员国的数据保护机构对数据违法行为进行调查处理，有权将数据控制者、数据处理者以及数据保护机构起诉至法院，以获得司法救济。第77条、第78条规定了数据主体有权从数据控制者（包括其代表人）与处理者处获得赔偿。值得注意的是第77条规定，一项数据侵权行为涉及多个数据控制者与处理者，则每一个控制者和处理者负有连带责任，若数据控制者和处理者可以证明自己不对该损失负责，则可以全部或部分免除责任。欧洲议会在修正案中补充，数据主体可获得赔偿的损失不限于物质损失^[3]。立法对连带责任与举证责任倒置规则的明确将使数据主体获得更为有效的救济。

3.5 提升警察和司法合作领域内个人数据的保护力度

刑事领域的警察和司法合作中的个人数据是欧盟数据保护立法改革中的特殊问题。欧盟并未在《指令》中对这一问题作出明确规定，而是通过制定《欧盟理事会2008/977/JHA号框架决定》（简称“框架决定”）为其提供法律依据。但“框架决定”适用范围有限，只适用于跨境数据处理，而不适用于成员国内部的刑事和司法（如自由、安全与司法领域）行为。“框架决定”通过例外性规定几乎排除了所有数据保护原则的适用，且未明文规定任何监管机构^[11]，在实践中，不同当事人（如犯罪嫌疑人和犯罪分子）的权利并未予以区分保护，这导致警察和司法合作领域出现了个人数据权利保护的灰色地带。

为回应和解决以上问题，欧盟委员会在此次改革中，适时地提出了《指令提案》作为个人数

据保护“一揽子”计划的重要组成部分。《指令提案》有3个方面引人关注：第一，在确保刑事领域的警察和司法合作的特殊性之前提下，将一般性数据保护原则（特别是透明度与数据最小必要原则）适用于该领域的个人数据保护工作；第二，欧盟数据保护机构有权对成员国警察以及司法机构的数据处理行为进行监督；第三，对特殊执法行动制定特别的规范，比如区分对待犯罪嫌疑人、犯罪分子或证人的数据权利保护问题。尽管《指令提案》的关注度逊色于《条例提案》，但2015年1月法国恐怖袭击的发生又一次激化了隐私与安全之间的矛盾，欧洲议会和欧盟理事会将加速对《指令提案》的审议。

4 重建欧—美数据跨境流动的信任机制

“斯诺登”事件使得大规模的数据监控危机凸显，再加上其往往与国家安全问题交织在一起，因此很难被有效遏制。为应对以上难题，重建欧美数据流通和共享中的信任机制，欧盟委员会呼吁“国家安全应作为例外而非规则^[12]”，并制定若干行动计划。具体而言，欧盟重建数据流通信信任机制将主要围绕以下方面展开。

4.1 持续推进数据保护立法改革

“棱镜门”丑闻成为欧盟数据保护立法改革全面提速的助推器。《条例提案》第3条进一步扩大了《指令》的效力范围，将数据控制者不在欧盟境内，但其处理活动涉及“向欧盟境内的数据主体提供产品或服务”与“监控其行为”的情况也纳入了立法的规制范围。这也意味着提案生效后，除非符合欧盟法或相关国际条约协定有除外规定，否则欧盟数据保护执法机关有权对企业涉及收集、处理欧洲居民数据的行为予以干预和管辖，其中包括类似“棱镜门”事件的监听计划。欧洲议会在修正案中将数据处理者也纳入第3条的监管范围，同时补充规定，数据控制者和处理者“向欧盟境内的数据主体提供产品或服务”也包括免费的产品或服务^[13]。欧盟通过扩大数据保护立法之域外效力，强制向世界推行数据保护的欧洲标准；通过施压于企业，抑制以国家安全之名的数据监控行为。

4.2 废除欧—美安全港协议，达成数据保护新框架协议

“棱镜门”之后，欧盟对美国企业隐私保护水平和政府监管力度颇为不满。随后，欧盟委员会于2013年提出了旨在完善安全港（safe harbour）协议之功能的13项具体建议，并要求美国当局基于该建议于2014年夏确立安全港协议的改进计划^[14]。目前，尽管这13项建议的大部分已经取得了实质性进展，然而美国并未就该13项建议所涉及的“限制以国家安全目的而获取安全港中的数据”这一核心政治问题提出解决方案^[15]，这也是完善安全港协议框架有待解决的关键性问题。然而，随着欧美数据流通中信任危机的进一步加剧，欧美2000年制定的安全港协议走向终结：欧盟最高法院于2015年10月6日作出判决并在裁定书中指出，欧盟的数据保护法规定，欧盟公民的个人数据不能传输至非欧盟国家，除非该非欧盟国家能为这些数据提供有效保护。鉴于美国未能达到上述要求，欧美之间签订的安全港协议无效。欧盟法院的最新裁决进一步推动了双方重新建立数据流通的新框架协议，该新协将议于2016年2月达成。新框架协议主要体现在以下几方面。第一，处理欧盟个人数据的公司需履行更为严格的数据保护义务并予以稳健的实施。美国商务部将对企业自行发布并由联邦贸易委员会按照美国法律予以执行的承诺书予以监督。第二，进一步明确美国政府机构获取个人数据的透明度与安全防护义务。欧美委员会和美国商务部将对协议的履行，包括国家安全准入问题进行年度审查。美国国家情报部门专家及欧盟数据保护机构将受邀参与审查。第三，欧洲居民的权利将会有受到救济的可能性。欧洲数据保护机构可向美国商务部及联邦贸易委员会投诉，同时，替代性纠纷解决机制是免费的。新的监察员将被设立以监督针对国家情报部门的投诉。该新协议在最终实施前还需要欧美双方的最终确认和准备。

4.3 推进欧美在警察及司法合作领域有关数据保护的框架性协定——雨伞协定谈判

欧美雨伞协定（data protection umbrella agreement）谈判始于2011年，至今已有20余轮谈判，已到最终阶段。目前，双方已就协定的范

围、目的、实质性规则以及实施与监管机制达成初步协定。雨伞协定旨在提高因预防、调查、侦查和起诉刑事犯罪（包括打击恐怖主义）而在欧美间跨境流动的个人数据的保护水平，加强双方合作。根据该协定，跨境传输的相关数据在处理时应遵守非歧视性原则，确保数据质量、完整性与安全性。在特定情形下，公民有权获取并更正个人数据。监管机构应该独立地行使职权，包括接受投诉与行使调查权^[16]。雨伞协定的最大亮点在于赋予了欧洲公民与美国本土居民同等、有效的司法救济权。这也意味着，欧洲公民将可以在美国提起相关司法诉讼并获取司法救济。为确保欧盟公民享有的司法救济权具有强制执行的效力，美国承诺将采取有效的解决方式，比如通过提议国会立法予以兑现^[17]。在雨伞协定的基础上，欧美双方在法律实施与司法合作方面的其他数据共享协议，例如，乘客姓名记录（passenger name records）和恐怖分子财务跟踪项目（terrorist finance tracking programme）的谈判将变得更顺利。

5 结束语

有美国学者认为，随着全球化进程的加快，欧盟数据保护立法在世界范围内将引起棘轮效应（ratcheting-up effect）^[18]，《条例提案》生效后可能会成为国际数据隐私保护标准，甚至是未来主导世界数据隐私保护的治理模式之一^[19]。这一现象值得中国关注与思考：其一，中国的跨国IT企业将成为欧盟数据保护立法潮流最直接的冲击对象，如何通过有效的公司信息安全治理应对隐私法规遵从的挑战是不得不考虑的问题；其二，目前，中国还不是欧盟认为可对个人数据提供充分性保护的国家，中欧间的数据跨境流动一直出现单向流动的尴尬局面，个人数据被喻为信息时代的生产要素，个人数据安全与网络安全、经济安全乃至国家安全有着密切的关系，我国应正确看待欧盟立法发展趋势带来的深刻影响，积极规划与实施适合我国国情的对内、对外的立法进路；其三，在新的技术背景下，我国也是以国家安全之名的情报收集与数据监控行为的受害者，应积极参与到个人数据保护的国家合作中，积极争取个人数据保护规则拟定中的话语权。

参考文献：

- [1] European Commission. Commission staff working paper[R/OL]. http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.
- [2] European Commission: vice-president reding's intervention at the justice council on the data protection reform and the one-stop shop principle[EB/OL]. http://europa.eu/rapid/press-release_SPEECH-13-788_en.htm.
- [3] PANICHI J. Ministers sign up for controversial one-stop-shop for data protection[R/OL]. <http://www.politico.eu/article/ministers-sign-up-for-one-stop-shop-for-data-protection/>.
- [4] European Commission: data protection: council agrees on general principles and the "one stop shop" mechanism[EB/OL]. <http://www.consilium.europa.eu/en/press/press-releases/2015/03/13-data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism/>.
- [5] FOSTER S L. One less carrot for business: council of european union limits the "one-stop shop" mechanism in the draft data protection regulation[N/OL]. Mondaq Business Briefing, <http://www.highbeam.com/doc/1G1-405868619.html>.
- [6] European Commission: justice council: we need a simple solution for citizens and business on data protection[EB/OL]. http://europa.eu/rapid/press-release_SPEECH-13-1029_de.htm.
- [7] Bureaucracy will prevail in 'one stop shop' data protection regime, UK and Ireland warn[EB/OL]. <http://www.out-law.com/en/articles/2015/march/bureaucracy-will-prevail-in-one-stop-shop-data-protection-regime-uk-and-ireland-warn/>.
- [8] RALLO A. International standardson the protection of personal data and privacy: the madridre solution[EB/OL]. http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf.
- [9] Looking at European Union data protection law reform through a different prism: the proposed EU general data protection regulation two years later[J]. Journal of Internet Law, 2014, 17(1):12-24.
- [10] Big data, big protection[R/OL]. https://www.google.com/url?q=http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/big-data-and-data-protection.pdf.
- [11] HERT P D. The police and criminal justice data protection directive: comment and analysis[J]. Computers & Law Magazine of SCL, 2012,22(6):1-4.
- [12] European Commission: protecting EU citizens' data from mass surveillance[EB/OL]. http://europa.eu/rapid/press-release_SPEECH-14-209_en.htm.
- [13] Comparison of the parliament and council text on the general data protection regulation[EB/OL]. https://edri.org/files/EP_Council_Comparison.pdf.
- [14] European Commission: data protection day 2014: full speed on EU data protection reform[EB/OL]. http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.
- [15] European Commission: e fact sheet U-U.S. negotiations on data protection[EB/OL].http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf.
- [16] Council of the European Union: EU-US data protection "umbrella agreement"-commission services non-paper on state of play of negotiations[EB/OL].<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%208761%202014%20EXT%201>.
- [17] European Commission: a data protection compact for europe[EB/OL]. http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm.
- [18] ROTENBERG M, JACOBS D. Updating the law of information privacy: the new framework of the european union[J]. Harvard Journal of Law & Public Policy, 2013(36):607-631.
- [19] HERT P D, PAPAKONSTANTINOV V. Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency[J]. Journal of Law and Policy for the Information Society, 2013,9(2):272-324.

作者简介：



张敏（1986-），女，陕西西安人，西安交通大学博士生，主要研究方向为信息安全法。

马民虎（1958-），男，陕西周至人，西安交通大学教授、博士生导师，主要研究方向为民商法、信息安全法。