从网络安全视野探讨数据跨境转移管理体系构建

■ 刘敏玲

摘　要　大数据、物联网、云计算及信息通讯技术等广泛应用，使数据处理和传输变得越来越便捷，然而也增加了监管的难度，尤其当商务交易变得越来越国际化及区域化，个人数据跨境传输日趋频繁，使数据自由流动和数据安全问题与国家利益、国家安全、网络安全、隐私保护紧密关连。随着粤港澳大湾区建设不断推进，大湾区城市将进一步融合发展，数据跨境流动的安全问题成为各地方政府在网络空间治理中的重要课题，有必要分类逐步完善关于数据跨境转移的法律制度体系。

关键词　数据跨境转移　网络安全　数据安全　隐私保护　个人数据合理流动

一、引言

在数字经济日益蓬勃发展下，人的流动与企业的跨境经营，使个人数据跨平台、跨地域的收集、存储、处理、使用和转移逐渐成为常态。近年来，以数字技术为代表的前沿科技飞速发展，也为粤港澳大湾区城市的协同发展创造出便利条件，例如电子商务为大湾区城市经济发展创造了新空间；智慧交通拉近了城市间的距离、人员流动更频繁、货物运输更高效。然而，在大湾区城市协同推进从民生到经济的多维度数字技术应用探索时，数据出境引发的流动性安全问题，不仅带来对数据跨境传输中的个人数据保护问题，同时也成为影响网络安全乃至整体国家安全的核心内容。

目前，粤港澳涉及网络安全和隐私保护等法律制度各异，如何在大数据、云计算等新技术背景下促进个人数据的跨境流动并确保安全，有效协调数据保护法制的差异性，是一个亟待解决的问题。因此，本文从网络安全的角度探讨构建数据跨境转移管理体系的可行性，从而更好地应对数字经济时代网

作者：澳门司法警察局副督察，暨南大学法学院知识产权学院民商法专业博士研究生

本文为第十六届海峡两岸暨香港澳门警学研讨论文。

络安全和隐私保护带来的新挑战。

二、数据跨境转移立法政策概述

（一）数据跨境转移的含义

1968 年联合国在《世界人权宣言》发布 20 周年的“国际人权会议”上，首次提出了“数据保护”（data protection）的概念。而最早出现“数据跨境流动”这词语的，是在 20 世纪 70 年代经济合作暨发展组织 OECD 科学技术政策委员会（CSTP）下设的计算机应用工作组（CUG）提出。OECD 于 1980 年发布《关于隐私保护与个人数据跨境流动的指南》的第一部分第一条第三款将“个人数据跨境流动”定义为“跨越国境的个人数据移动”，第一条第二款将“个人数据”定义为“任何与已被识别或可识别的个人（数据主体）有关的信息”。

“数据跨境转移”一词又称“数据跨境流动”“数据跨境传输”“数据跨境流通”等，是指通过各种技术与方法实现数据跨越一个国家的国境或一个地区的地域的流动；而使用“转移”的称谓，主要是考虑数据流动过程中涉及两个不同法域的不同主体。在数据跨境转移问题上，最重要和最具争议的是个人数据跨境流动，目前绝大部分文献都以“数据跨境流动”代指“个人数据跨境流动”。许多国家的数据保护法都包含跨境数据流动条款，这本身就属于单边跨境数据流动规制。从国际层面，跨境数据流动的规制与数据保护法之间的关系比较复杂，两者规制的目标存在差别，数据保护法的规制目标主要是保护个人隐私，跨境数据流动规制目标却同时包括保护个人隐私和确保合理的数据流动。二者不仅有紧密的历史渊源，而且在内容上相互影响，在功能上也存在补充。

（二）国外跨境数据转移的法律框架

限制数据跨境转移的假设性前提都是基于认为第三国的个人数据保护水平不及本国的同等水平。然而，在跨境数据流动创造的巨大商业利益驱使下，企业进行数据跨境转移成为国际贸易的必然需要，下文将分别阐述全球不同国家共同建设的跨境数据传输的法律框架。

1．经济合作与发展组织 OECD—《OECD1980 年指南》

经济合作暨发展组织（OECD）成立于 1961 年，是全球 37 个市场经济国家组成的政府间国际组织。早在 1980 年 OECD 便制定《关于隐私保护和个人数据跨境流动指南》（以下简称《OECD1980 年指南》），其后在《OECD1980 年指南》的基础上，分别于 2007 年及 2013 年通过《OECD2007 年建议》及《OECD2013 年指南》。

在最初的《OECD1980 年指南》要求各国对成员国之间的个人数据跨境流通限制采取克制态度，在后期的修改中则要求进一步放宽限制，但同时也要求数据控制者对于数据的管理保护责任，并确立了数据跨境流通的限制与风险成比例原则。

2．亚太经济合作组织 APEC—跨境隐私规则 CBPR

APEC 隐私权保护框架，以下称《APEC 隐私框架》于 2004 年获得 APEC 部长会议认可，成为亚太地区第一份关于跨境数据流动保护的最高指导纲领。APEC 于 2007 年提出“开路者”倡议，并决定建构跨境隐私规则，并于 2012 年正式启动。《APEC 隐私框架》由九项指导原则和实施指南组成，以协助亚太经合组织经济体制定一致的内部办法，以保护个人隐私信息权。同时，制定区域办法，为成员经济体之间彼此权责明确的

数据跨境传输和隐私保护奠定基础。

3．美国—隐私盾协议 Privacy Shield 与 CLOUD 法案

欧美在跨境数据流动创造的商业利益驱使下，于 2016 年 7 月 12 日达成《欧美隐私盾协定》，成为规制双方数据流动的新妥协方案。《隐私盾协议》（Privacy Shield）的核心是对大西洋两岸跨境转移个人数据的隐私保护进行规制，为大西洋两岸的欧洲和美国企业从欧盟向美国传输个人数据过程中提供欧盟数据保护规定的合规机制，并支持跨大西洋商业合作的发展。根据《隐私盾协议》用于商业目的的个人数据从欧洲传输到美国，享有与在欧盟境内同样的数据保护标准。美国承诺将严格履行《隐私盾协议》中的要求，保证国家安全部门不会对这些个人数据采取任意监控或大规模监控措施。然而，欧盟最高法院出于对欧盟公民数据隐私安全的考虑，于2020年7月宣布废除《隐私盾协议》。

2018 年美国议会通过《澄清境外数据的合法使用法案》（CLOUD），通过适用“控制者原则”，CLOUD 法案明确赋予美国执法机构跨境调取数据的权力，美国可以出于公共安全等目的对境外存储的数据进行调取。此外，美国允许“适格外国政府”（qualifying foreign government）执法机构调取美国存储的数据。对“适格外国政府”的认定，要求外国政府的国内立法，包括对其国内法的执行，是否提供了对隐私和公民权利足够的实质和程序上的保护。

4．欧盟—《一般数据保护条例 GDPR》

欧盟于 2016 年制定及通过《一般数据保护条例》（GDPR），并于 2018 年 5 月 25 日正式生效。GDPR 不仅在所有成员国范围内直接具有法律约束力，而且谋求更大的域外效力，明确规定条例对在欧盟境外处理个人数据的行为也具有适用效力。

由此可见，欧盟的数据跨境转移政策主要体现在个人数据保护制度中，其实机制也相应地依附于个人数据保护执法体系中。当数据控制者实施个人数据跨境流动时，有三种合法方式：第一、数据传输至“充分性认定”地区；第二、例外情况，包括用户同意，或者执行合同需要等；第三、充分保障措施，制定“充分性认定机制”和“充分保障措施”。所谓“充分性认定机制”是指欧盟委员会负责根据第三国的个人数据保护立法状况、执法能力，以及是否存在有效的救济机制等因素，做出综合评估。而“充分保障措施”主要体现为“标准合同文本”机制（SCC）和“有约束力公司规则”机制（BCR）。对于“标准合同文本”机制，目前欧盟委员会已经形成了三个合同模板，此类合同模板通过规定数据输出方和数据接收方基于合同的资料保护责任，来间接提供对个人的保护机制。对于“有约束力的公司规则”则是集团型跨国企业可优先考虑的机制，集团遵循一套完整的、经个人数据监管机构认可的数据处理机制，使该集团内部整体成为“安全港”，个人数据可以从集团内的一个成员合法传输给另一个成员。

（三）内地、香港与澳门对保护数据跨境转移的立法现状

1．内地

内地的《个人信息保护法》自 2021 年 11 月 1 日起施行。内地自 2017 年起，已就个人信息的定义及个人信息出境安全方面制定了一系列的规范。目前，内地已确立了数据出境安全管理的基本框架。对于数据跨境传输的限制性规定，分散于各类法律法规、部门规章之中。

2017 年 6 月 1 日起施行的《网络安全法》

是内地首部针对网络隐私和网络空间安全管理而制定的综合性监管法案，着重于在境内所生成信息的流动性。该法第三十七条规定关键信息基础设施的运营者在境内运营时所收集和产生的个人信息和重要数据必须存储在境内，并对数据出境提出了安全评估的要求，规范了安全评估的责任主体、管理对象、管理要求等内容。国家网信办分别于 2017 年发布了《个人信息和重要数据出境安全评估办法》(征求意见稿) 及 2019 年《个人信息出境安全评估办法》（征求意见稿），提出了建立“主管部门评估——网络运营者自评估”两级评估机制。其中 2019 年版的（征求意见稿）第二条更明确规定，经安全评估认定个人信息出境可能影响国家安全、损害公共利益，或者难以有效保障个人信息安全的，不得出境。

此外，于 2021 年 9 月 1 日起施行的《数据安全法》明确规定国家积极开展数据安全治理、数据开发利用等领域的国际交流合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全和自由流动；建立数据分类分级保护制度、建立数据安全应急处理机制和审查制度，并加强风险监测及风险评估。

至于非法进行数据跨境转移的处罚，根据《网络安全法》第六十六条规定，关键信息基础设施的运营者没有按该法第三十七条进行安全评估的规定，而在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处 5 万至 50 万元罚款，并责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人处 1 万至 10 万元罚款。

《数据安全法》第四十六条规定，违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，并处 10 万元以上 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处 1 万元以上 10 万元以下罚款；情节严重的，处 100 万元以上 1,000 万元以下罚款，并责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处 10 万元以上 100 万元以下罚款。

2．香港特别行政区

香港政府基于便利营商环境、维持香港的金融和贸易中心地位，以及保障个人隐私的目的，参考《OECD1980 年指南》及 1995 年欧盟《第 95/46/EC 号数据保护指令》，于 1995 年通过及于 1996 年 12 月正式生效的《个人资料（私隐）条例》(以下简称《条例》)，并设立个人资料私隐专员公署，该《条例》是亚洲最早全面保障个人资料私隐的法例之一。其后《条例》先后进行了多次修订，并于 2021 年 7 月 21 日通过《2021 年个人资料（私隐）（修订）条例草案》。

根据香港《条例》第 6 部第三十三条的规定，禁止除在指明情况外将个人资料移转至香港以外地方，除非符合《条例》第三十三（2）条列明的例外情况：

（a）个人资料私隐专员藉宪报公告，指明该地方有与《条例》大体上相似或达致与《条例》相同目的之法律正在生效；

（b）该使用者有合理理由相信在该地方有与本条例大体上相似或达致与本条例的目的相同之法律正在生效；

（c）获得有关资料当事人书面同意该项转移；

（d）该使用者有合理理由相信该项转移是为避免针对资料当事人的不利行动或减轻该等行动的影响而作出的；获取资料当事人

对该项转移的书面同意不是切实可行的；及如获取书面同意是切实可行的，则资料当事人是会给予上述同意的；

（e）该资料凭借条例第 8 部的豁免而不受保障资料第 3 原则所管限；

（f）凡假使该资料在香港以某方式收集、持有、处理或使用，便会属违反条例下的规定，该使用者已采取所有合理的预防措施及已作出所有应作出的努力，以确保该资料不会在该地方以该方式收集、持有、处理或使用。

另外，根据《条例》第六十四 A 条，资料使用者没有合理辩解而违反第三十三条，即属犯罪，最高可被判处罚款港币 10,000 元。虽然《条例》第三十三条早已于 2012 年法律公告第二条及 2013 年第一号编辑修订记录中制定了条文及违反规定，然而，《条例》第三十三条仍处于尚未实施阶段。

3．澳门特别行政区

《澳门民法典》由 1999 年 8 月 3 日公布的第 39/99/M 号法令核准，并于同年 11 月 1 日起开始生效。该法典第七十九条已就个人资料之保护作出了规定，当收集个人资料以便作信息化处理时，应严格依照收集该等资料之目的而进行收集，并应让当事人知悉该等目的；以及为知悉第三人之个人资料而查阅或连接信息化数据库及记录时，必须就每一个案获负责监察个人资料之收集、贮存及使用之公共当局之许可。然而，《澳门民法典》并未就何谓“个人资料”及“个人资料跨境转移”作出定义。其后，随着澳门社会发展，澳门特区政府参考欧洲理事会《第 108 号公约》、欧盟第 95/46/EC 号指令等国际组织、日本、泰国、台湾地区和香港特区的相关立法经验，于 2005 年 8 月 22 日公布第 8/2005 号法律《个人资料保护法》。该法对个人资料转移到境外的原则性规定采用第三方适当性评估的立法模式，但也有排除适用的例外规定。在一般原则性规定上，采用“第三方适当性评估”模式，要求接收转移资料的法律体系确保适当的保护程度的情况下，方可将个人资料转移到澳门特区以外的地方。

而在下列三种例外情况下，排除适用“适当性评估”的原则性规定：

第一种例外情况，获数据主体（即资料当事人）同意。根据澳门特区第 8/2005 号法律《个人资料保护法》第二十条规定，当资料当事人明确同意转移或转移符合下列情况时，经对个人资料保护办公室作出通知后，将个人资料转移到一个法律体系不能确保该法第十九条第二款规定的适当保护程度的地方：一、转移是执行资料当事人和负责处理个人资料的实体间的合同所必需，或是应资料当事人要求执行签订合同的预先措施所必需者；二、转移是执行或签订合同所必需，而该合同是为了资料当事人的利益由负责处理资料实体和第三人之间所订立或将要订立者；三、转移是保护重要的公共利益，或是司法诉讼中宣告、行使或维护权利和所必需的或法律所要求者；四、转移是保护资料当事人的重大利益所必需者；五、转移自作出公开登记后进行。根据法律或行政法规，该登记是为公众信息和可供一般公众或证明有正当利益的人公开查询之用者，只要能遵守上述法律或行政法规制定的查询条件。

第二种例外情况，是由数据控制者作出担保，即负责处理资料的实体能确保有足够的保障他人的私人生活、基本权利和自由的机制，尤其通过适当的合同条款确保这些权利的行使。在数据控制者能作出担保的情况下，个人资料保护办公室许可将个人资料转

移到一个法律体系不能确保适当保护程度的国家或地区。

第三种例外情况，是当个人资料的转移成为维护公共安全、预防犯罪、刑事侦查和制止刑事违法行为以及保障公共卫生所必须的措施时，个人资料的转移由专门法律或适用于特区的国际法文书以及区际协定规范。

由此可见，澳门在个人资料跨境转移的处理上同时采用了“第三方适当性评估”、“数据主体同意”及“数据控制者担保”的模式进行相关立法规定。对某一法律体系是否能确保符合适当保护程度，必须经由澳门个人资料保护办公室进行审议及作出决定，而不管是否已获数据主体同意，或是否已有数据控制者担保，当把个人资料境外转移时，均必须通知个人资料保护办公室，并获得该办公室的许可，才可以排除适用“第三方适当性评估”。

虽然《澳门网络安全法》已于 2019 年 12 月 21 日生效，对“关键基础设施”、“关键基础设施营运者”及“网络营运者”作出了具体定义。然而，对数据境外传输如何进行“适当性评估”没有作出具体规范，亦没有立法规范安全评估的责任主体、管理对象、管理要求等，而是否符合“适当的保护程度”，则由个人资料保护办公室根据转移的所有情况或转移资料的整体进行审议及作出决定，尤其应考虑资料的性质、处理资料的目的、期间或处理计划、资料来源地和最终目的地，以及有关法律体系现行的一般或特定的法律规则及所遵守的专业规则和安全措施。

至于非法进行数据跨境转移的处罚，根据第 8/2005 号法律《个人资料保护法》第三十三条第二款的规定，如违反该法第十九条（原则）及第二十条（排除适用）规定将个人资料转移到澳门特区以外的地方，属于行政违法行为，可被处澳门币 8,000 至 80,000 元罚款。

三、构建数据跨境传输管理体系的必要性

（一）网络及数据安全是数字经济发展的前提

当今全球数字经济正蓬勃发展，已成为推动各国经济高质量增长的重要动能。而数字经济的发展是以信息技术和数据资源作为关键要素，加强数字治理，为建设数字经济强国提供制度保障是国家立法的当务之急。习近平总书记曾指出：“要制定数据资源确权、开放、流通、交易相关制度，完善数据产权保护制度。”因此，数据已成为重要的生产要素和企业的核心资产，而在粤港澳三地各领域发展越趋紧密合作的态势下，数据的共享、整合、流通将成为大势所趋，保障数据安全，促进数据开发利用已成为各地方政府工作的首要任务。

（二）政策支撑经济多元发展，数据跨境传输需求不断增加

粤港澳大湾区着力建设国际科技创新中心，发展成以创新为主要动力和支撑的经济体系，以电子商贸、健康科技、机器人、金融科技和生物科技企业为主。根据 2020 年全球创新指数（Global Innovation Index）显示，由香港、深圳及广州的创新及科技业组成的广深港科技集群位居世界第二大科技集群，仅次于东京－横滨科技集群。香港与深圳政府正共同建设由港深科创园和深圳科创园区组成的深港科技创新合作区，实现“一国两制”下的“一区两园”，预计港深科创园第一批发展可于 2024 年起分阶段落成。

在澳门方面，为了把握《粤港澳大湾区发展规划纲要》赋予横琴推进珠海横琴粤港澳深度合作示范的重大机遇，深化琴澳合作，支援澳门融入国家发展大局，2020 年 9 月 11 日，珠海市政府制定《横琴新区发展规划（2021-2035 年）》（下简称《规划》），内容主要以“战略 + 空间 + 功能 + 政策”等四位一体，丰富横琴与澳门的合作内涵，与澳门共同推进特色金融、医疗健康、科技创新、会展旅游、文化创意等产业发展；并着力在经济管理、营商环境、市场监管等方面构建与港澳趋同、与国际更高标准的投资贸易规则相适应的政策环境。《规划》亦从技术层面搭建横琴空间信息数据库，开展多源大数据分析，对横琴层面的大数据分析，包括基于网络爬虫的 POI 自动抓取技术，对高德、百度地图和大众点评网等兴趣点进行智能获取；通过遥感技术对横琴的建设用地进行了遥感自动解译等。而对澳门层面的大数据分析，则包括利用政务数据对社会经济情况进行了横向和纵向对比分析；利用人口热力图对口岸通关情况进行分析；利用专利联系度分析澳门与粤港澳大湾区各城市的创新合作情况等。

一系列的政策陆续出台，使粤港澳的资源互补，大大促进三地间的经济多元发展。由于三地人员不断交往，数据跨境传输也将不断增加，有必要为三地构建数据跨境传输管理体系，从而确保数据流通的安全性。

（三）数据保护标准不一，增加数据跨境流通风险

在数据跨境流通不断增加的态势下，数据安全面临更为复杂的威胁。一方面是各国数据保护标准不统一，数据从高水平保护国家流入低水平保护国家，使流出国使用者的权利在数据跨境转移后难以得到保障，执法和救济存在障碍；另一方面，各国关键信息基础设施和重要机构承载的庞大数据信息具有重大的国家安全战略价值，例如由信息网络系统所控制的石油和天然气管道、水、电力、交通、银行、金融、军事等领域的大数据安全，已经上升为国家安全的关键组成部分。这些领域的大量敏感性数据在跨境传输中存在不可控的风险，需要国家层面加强数据安全能力和监管能力。

在促进经济发展的同时，各项政策制度的制定更应符合国家数据跨境流通的统一技术标准，才能更好地维护网络安全。

四、构建数据跨境传输管理体系的困难与挑战

（一）法律制度的冲突

由于历史原因，在“一国两制”下，粤港澳地区形成不同的社会及法律制度，法制的差异性也使数据跨境流通中难免出现制度方面的冲突。内地的《网络安全法》《个人信息出境安全评估办法》与香港的《个人资料（私隐）条例》及澳门的《个人资料保护法》分别规定了不同的个人信息监管机构，同时对数据和隐私的界定及适用范围均有区别。

内地的《个人信息保护法》第三章规定了个人信息跨境提供的规则，其他数据跨境流通管理的限制性规定分散于各类法律法规和部门规章中，关键信息基础设施的数据出台提出了安全评估的要求，提出了建立“主管部门评估 -- 网络运营者自我评估”的两级评估机制。

虽然香港的《个人资料（私隐）条例》早已于 1995 年制定，多年来进行了多次修订，然而《条例》的部分条文是分阶段实施的，正如前述，《条例》第三十三条至今仍

处于尚未实施阶段，换言之，香港对于数据跨境转移的限制性规定只有条文规定却未能落实执行。

至于澳门，对于涉及个人资料数据的境外传输，根据第 8/2005 号法律《个人资料保护法》第二十条第三款规定：“当将个人资料转移到澳门特区以外的地方，且该资料的转移成为维护公共安全、预防犯罪、刑事侦查和制止刑事违法行为以及保障公共卫生所必需的措施时，这种资料转移就由专门法律规定或适用澳门特区的国际法文书以及区际协定规范。”然而至目前为止，澳门特区仍未就数据转移而制定专门法律。此外，由于澳门《个人资料保护法》是参考欧盟的相关法律制度而制定，因此，澳门在个人信息跨境转移的处理上一直遵循“严格限制”的立场，必须由个人资料保护办公室根据数据转移的所有情况或信息转移的整体情况进行审议的基础上作出是否适当的判断。然而，国际上的惯例做法，在对于接收转移信息地是否具备个人保护适当程度作出判断，会把已经达到充分保护的国家或地区名单（俗称“白名单”）列出并公布，而澳门尚未公布任何一个国家或地区具有适当保护程度，亦没有制定数据安全评估机制及指引。

（二）司法体系相对独立，处罚金额差距甚大

从《网络安全法》第六十六条与新通过的《数据安全法》第四十六条的规定可见，对违反这两条法律规定而进行数据跨境转移的处罚金额有着明显的差距，前者的最高罚款金额仅为人民币 50 万元，而后者的最高罚款金额为人民币 1,000 万元，两部法律的处罚金额存有明显的不协调性；而相对澳门而言，澳门地区的最高罚款金额则仅仅是 8 万澳门元，两地的处罚金额差距甚大；至于香港，由于《条例》第三十三条尚未实施，有关规定根本无从执行。

除此之外，内地与港澳的司法体系相对独立，对证据和搜证方式等的要求也不同，有必要加强三地间跨境司法合作和交流。

（三）技术标准和人才的差距

在涉及数据跨境流通的技术层面，内地与港澳地区缺乏统一的技术标准，例如底层算法代码的差异、API 数据接口、数据跨境合规审查规定、数据标准等均存有差异。此外，不同机构在数据传输流通的过程中，能从中挖掘分析到的结果和准确性亦存有差异，在技术人才供不应求的情况下，对构建粤港澳大湾区数据跨境传输管理体系带来一定的阻碍。

五、对构建数据跨境传输管理体系的建议

（一）从国家层面协调制定粤港澳大湾区内数据安全保护机制

要求数据合规跨境流通的前提，是要构建一套健全的数据规则，包括数据使用权、收益权的归属、数据定价和交易规则、数据流通中的权利义务和侵权责任等。《数据安全法》已于 2021 年 6 月 10 日通过，并于同年 9 月 1 日起施行。根据《数据安全法》第五条规定，国家安全机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。本文建议从国家层面更好地协调粤港澳三地的数据安全保护的统一指挥及战略部署，统筹协调包括港澳两个特别行政区在内的数据安全的重大事项和工作，加强数据跨境传输的合

规性，引导数据产业链的平衡发展。

（二）建立适用于粤港澳大湾区的数据安全流通评估机制

随着电子商贸发展不断深入，数据跨境流通的水平不断提升。由于香港、澳门特区仍未就跨境数据流通制定安全评估机制，建议参照内地的两级评估机制，按照《信息安全技术数据出境安全评估指南》综合考虑安全与发展两方面的情况，从而制定适用于粤港澳大湾区的跨境数据传输管理体系的统一标准及评估机制，梳理数据跨境流通机制，减少本地化的数据跨境流通阻碍，从而达到维护国家数据主权和促进跨境数据自由流动的平衡。

（三）确立不同性质的数据分类及保护制度

内地与港澳地区对个人数据的界定及适用范围的不同，使跨境数据流通难免面对法律冲突，有必要对不同性质的数据进行分类管理，从而把个人信息中的一般数据、重要数据、机密数据区分开，而不是把所有涉及个人信息的数据均视作隐私权的保护对象，这不仅阻碍大湾区内数据的自由流通，还不利于大湾区城市的共同发展。因此，建议确立不同性质的数据分类及保护制度，在健全的法律体制下，才能更大程度地使隐私权得到保障。

（四）制定指引性的数据跨境流通协议模板

借鉴欧盟、OECD 等国际组织的经验制定“白名单”，根据个人信息保护状况及对等措施，将部份地区纳入数据可自由流通的国家和地区，并制定数据跨境流通协议模板，类似欧盟标准的合同模板，指引企业通过合同法律机制来管控数据出境风险。

六、结语

数据出境引发的流动性安全问题，不仅带出对数据跨境传输中的个人数据保护问题，同时也成为影响网络安全乃至整体国家安全的核心内容。各国和地区限制数据跨境转移的假设性前提都是基于认为第三国或地区的个人数据保护水平不及本国或本地区的同等水平。然而，在跨境数据流动创造的巨大商业利益驱使下，企业进行数据跨境转移成为国际贸易的必然需要。

在“一国两制”的背景下，各国和地区限制数据跨境转移的同时，必须综合考量安全与发展的平衡，制定内地与港澳地区的跨境数据传输管理体系的统一标准及评估机制，梳理数据跨境流通机制，减少本地化的数据跨境流通阻碍，从国家层面更好地协调粤港澳三地的数据安全保护的统一指挥及战略部署，统筹协调包括港澳两个特别行政区在内的数据安全的重大事项和工作，加强数据跨境传输的合规性，引导数据产业链的平衡发展，从而达到维护国家数据主权和数据安全与促进跨境数据自由流动的平衡。

参考文献：

[1]杨崇尉、廖志汉、廖志聪．澳门个人资料保护制度 [M]．澳门基金会社会科学文献出版社．2015

[2]黄宁、李杨．“三难选择”下跨境数据流动规则的演进与成因 [J]．清华大学学报（哲学社会学版）．2017．5

[3]张金平．跨境数据转移的国际规制及中国法律的应对——兼评我国网络安全法上的跨境数据转移限制 [J]．政治与法律．2016．12

[4]蔡静怡．大数据时代下的 APEC跨境隐私保护规则 [J]．中华台北 APEC研究中心．2014．10

[5]刘敏玲．构建警务云区际信息共享平台的设想．第五届澳门珠海警务论坛交流论文集．2016．6

责任编辑 尚钰涛