财经法学 No. 5，2024
pp. 23 - 40

数据跨境双轨制下
个人信息出境监管豁免制度的适用与完善

刘金瑞*

内容提要：数据跨境新规确立了个人信息出境监管豁免制度，既豁免了申报数据出境安全评估，也豁免了订立个人信息出境标准合同、通过个人信息保护认证。但从我国数据跨境管理双轨制体系来看，这些豁免规则在理解适用上仍存在一系列困惑：符合场景豁免的个人信息是否必然豁免安全评估，一定数量个人信息为何可以豁免同等保护要求出境，过境个人信息豁免、负面清单外豁免的合理限度何在，实践需要与安全关切双重压力下应如何完善豁免。破解这些困惑，就应该明确特定豁免只是豁免保护个人权益的监管机制，厘清个人信息与重要数据关系以明确豁免边界，系统把握过境个人信息豁免和负面清单外豁免，增强数据跨境制度协同性以缓解豁免规则压力。

关键词：个人信息　出境监管豁免　数据跨境双轨制　重要数据　国家安全

2024 年 3 月 22 日，《促进和规范数据跨境流动规定》（以下简称《规定》）正式公布施行。该规定优化调整了数据出境管理规则，通过提高监管门槛、增设豁免制度等适当放松了事前监管，转而强调构建事前事中事后全链条监管，这有利于促进数据依法有序跨境流动，降低跨境数字贸易合规成本，充分释放数据要素价值，扩大高水平对外开放，切实推动我国乃至全球数字经济发展。其中最重要的制度设计是规定了免予“申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证”，〔1〕即本文所称的“事前监管”的条件。对于个人信息跨境流动而言，就是确立了个人信息出境免予事前监管的规则，本文将这种免予事前监管的规则称为“个人信息出境监管豁免制度”。

在《规定》出台之前，我国通过制定《中华人民共和国网络安全法》（以下简称《网络安全

* 刘金瑞，中国法学会法治研究所研究员。

〔1〕 为行文简洁，下文将这三种事前监管机制分别简称为“申报安全评估”“订立标准合同”“通过保护认证”。

法》）、《中华人民共和国数据安全法》（以下简称《数据安全法》）、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）及相关配套规定，相继建立了旨在维护国家安全、公共利益的重要数据出境安全管理制度和旨在保护个人权益的个人信息跨境提供制度，〔2〕这两种侧重事前监管的并行制度形成了我国数据跨境管理的“双轨制”体系。从这种双轨制体系来看，上述个人信息出境监管豁免制度的理解适用存在不少困惑，例如：符合场景豁免条件的个人信息是否必然豁免数据出境安全评估，该制度的规范逻辑和体系定位何在。再加上近年来域外国家也日益重视基于国家安全管控个人信息跨境流动，甚至出现了以“国家安全”为由无端阻止个人信息流向我国的乱象，例如美国拜登政府 2024 年 2 月签发《防止受关注国家访问美国人的大量敏感个人数据和美国政府相关数据》行政命令（以下简称《敏感个人数据行政命令》），〔3〕如何在保障国家数据安全的前提下澄清困惑，妥当平衡保护个人信息权益和促进数据跨境流动，成为个人信息出境监管豁免制度实施面临的重大难题。

本文就是在此背景下，在体系化理解个人信息出境监管豁免制度的基础上，针对数据跨境双轨制下该制度适用面临的实践困惑，从解释论出发就如何妥当适用和完善个人信息出境监管豁免制度提出建议，以期能够对我国数据跨境流动法治提供有益参考。

一、数据跨境双轨制体系中的个人信息出境监管豁免制度

《规定》根据当前经济社会发展需要，确立了个人信息出境监管豁免的一系列规则，对这些规则需要在我国现有数据跨境双轨制体系中予以系统把握才能准确理解。

（一）跨境新规确立的个人信息出境监管豁免制度

《规定》贯彻中央促进和便利跨境数据流动的要求，〔4〕考虑个人信息出境场景、出境个人信息敏感性、个人信息入境处理、自贸试验区探索等因素，规定了六种豁免个人信息出境事前监管的情形。从信息出境场景和出境信息敏感性出发，第 5 条规定了四种豁免情形。前三种情形是豁免了个人主动发起和为了个人重大利益的特定场景：为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；〔5〕按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供个人信息；紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息。第四种情形是豁免了向境外提供低敏感性个人信息集合的处理者，其中从输出主体、信息类型和所涉人数等方面限定了出境个人信息集合的敏感性，即关键信息基础设施

〔2〕 长期以来，域外关注的数据跨境流动主要是指个人信息跨境流动。See Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013. 而我国还针对高风险的重要数据出境建立了专门的管控制度。

〔3〕 See Executive Order 14117: *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, Federal Register, Vol. 89, No. 42, March 1, 2024, pp. 15421 - 15430.

〔4〕 2022 年 12 月印发的《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》要求“构建数据安全合规有序跨境流通机制”；2023 年 8 月发布的《国务院关于进一步优化外商投资环境 加大吸引外商投资力度的意见》要求“探索便利化的数据跨境流动安全管理机制”；2024 年 3 月，国务院办公厅发布《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》，要求“支持外商投资企业与总部数据流动”“健全数据跨境流动规则”。

〔5〕 该情形列举了个人主动发起的场景，包括跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等。

运营者以外的数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）（以下简称“一般个人信息”）。

此外，为了鼓励个人信息入境处理，第4条豁免了某些过境个人信息，即在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据。为了自贸试验区的探索需要，第6条豁免了自贸试验区内数据处理者向境外提供该试验区负面清单外的数据包括个人信息，这里将数据纳入事前监管的负面清单，需要在国家数据分类分级保护制度框架下，经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。需要指出的是，国家网信办在《〈促进和规范数据跨境流动规定〉答记者问》〔6〕（以下简称《答记者问》）中还认为第2条是一种豁免，即对国际贸易等活动中不涉及个人信息或重要数据的出境数据免予事前监管，但笔者认为该条只是重申了上位法建立的数据出境管理范围只限于重要数据和个人信息，重申“未纳入监管”并不是创设监管豁免。

第5条前三种场景豁免情形是参照了《个人信息保护法》第13条规定的同意以外合法处理个人信息的情形，表述与该条第2项和第4项基本一致。笔者认为，如此参照规定的原因在于：在这些个人主动发起和为了个人重大利益的场景中，处理个人信息的必要性较为充分，〔7〕而且个人信息处理目的主要是为了保护个人信息主体自身的合法权益，这种必要性和目的性能证成这些场景本身就可以作为同意以外处理个人信息的合法基础，在便利数据跨境流动的立场下，同样能用来证成这些场景可以豁免旨在保护个人权益的事前监管。由于表述基本一致，对这些豁免情形的理解可以参照对《个人信息保护法》相关规定的理解。例如订立、履行合同的“确需”可以参照上位法“必需”的理解：是指“客观上的必要”，处理个人信息“应符合合同相对人、社会公众的合理期待或者行业惯例”，必要性的判断要“兼顾实现合同目的和保护个人信息权益的比例性原则”〔8〕。

第5条第四种处理者豁免情形，本身也属于未达到第7条安全评估申报数量门槛的情形，〔9〕其免予申报安全评估的上位法依据主要是《个人信息保护法》第40条。该条在《网络安全法》的基础上，在“关键信息基础设施运营者”之外增加规定“处理个人信息达到国家网信部门规定数量的个人信息处理者”，也应当将在我国境内收集和产生的个人信息存储在境内，确需向境外提供的应当通过安全评估，但法律、行政法规和国家网信部门可以规定不进行安全评估的情形。如此规定主要是考虑到这种个人信息处理者处理的个人信息数量大，不仅涉及众多个人的权益，还关系公共利益甚至是国家安全。〔10〕此豁免情形即是国家网信办根据上位法授权从反面规定了免于安全评估的监管门槛。值得注意的是，这里的豁免不仅豁免了安全评估，还豁免了订立标准合同、通过保护认证，相较于之前根据《个人信息出境标准合同办法》（以下简称《标准合同办

〔6〕 参见《〈促进和规范数据跨境流动规定〉答记者问》，载 https://www.cac.gov.cn/2024-03/22/c_1712776611649184.htm，最后访问时间：2024年7月25日。

〔7〕 参见周汉华主编：《〈个人信息保护法〉条文精解与适用指引》，法律出版社2022年版，第104-107页。

〔8〕 杨合庆主编：《中华人民共和国个人信息保护法释义》，法律出版社2022年版，第46页。

〔9〕 根据《规定》第7条，关键信息基础设施运营者以外的数据处理者申报安全评估的条件为：向境外提供重要数据，或者自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息。

〔10〕 参见杨合庆主编：《中华人民共和国个人信息保护法释义》，法律出版社2022年版，第105-106页。

法》）此时有可能需要事前订立标准合同，〔11〕该豁免规定进一步提高了监管门槛。

相对于第 5 条四种特定的豁免情形，第 4 条规定的过境个人信息豁免情形和第 6 条规定的自贸试验区负面清单外豁免情形，都是在《个人信息保护法》之外新创设的较为不特定的豁免规则。前者是一种相对普遍的豁免，只要个人信息在过境过程中“没有引入境内个人信息或者重要数据”就得以豁免；后者是确立了一种豁免机制，没有纳入自贸试验区事前监管负面清单的数据就可以豁免，当然前提是负面清单应符合国家数据分类分级保护制度框架并履行报批报备手续以确保法制的统一性。

（二）双轨制下豁免个人信息出境事前监管的理解

总结来看，《规定》综合考虑多种因素，对特定的个人信息出境较低风险情形豁免了申报安全评估、订立标准合同、通过保护认证等三种事前监管机制，适当放宽了个人信息跨境流动条件。对这种事前监管豁免制度的理解，需要在我国数据跨境管理双轨制体系中予以系统把握。我国从数据跨境流动的不同关切入手，以“重要数据”和“个人信息”为抓手建立了两种不同的数据跨境管理制度：一是旨在维护国家安全、公共利益的重要数据出境安全管理制度，主要规定在《数据安全法》和《网络安全法》中；二是旨在保护个人权益的个人信息跨境提供制度，主要规定在《个人信息保护法》中。这两种制度在目标定位、适用范围、监管机制上均存在显著区别，再加上区分了重要数据处理者、处理个人信息达到规定数量的处理者等主体，还规定了司法执法跨境调取等不同场景规则，形成了“双轨并行、多层规制”的制度体系。〔12〕

从该制度体系来看，《规定》确立的个人信息出境豁免制度只是豁免了上述三种事前监管机制，《个人信息保护法》第三章“个人信息跨境提供的规则”规定的其他监管要求仍然适用。〔13〕例如该章第 41 条基于主权管辖〔14〕规定了司法执法跨境调取数据规则：我国主管机关根据有关法律和我国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内的个人信息的请求；非经过我国主管机关批准，个人信息处理者原则上不得向外国司法或者执法机构提供存储于我国境内的个人信息。因此，当外国司法或执法机构要求个人信息处理者提供存储于境内的个人信息时，上述豁免情形不能作为向外国司法或者执法机构跨境提供个人信息的合法基础。

在双轨制体系中，订立标准合同、通过保护认证是旨在保护个人权益的事前监管机制。从《个人信息保护法》第 38 条、第 56 条以及相关配套规定〔15〕来看，二者目的都在于保障境外接收方处理个人信息的活动达到我国《个人信息保护法》规定的个人信息保护标准，〔16〕二者都需要在事前进行个人信息保护影响评估，而评估的重点在于“对个人权益的影响及安全风险”。因此，

〔11〕 该办法第 4 条规定，适用订立标准合同需要满足的情形之一就是自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人。

〔12〕 参见刘金瑞：《迈向数据跨境流动的全球规制：基本关切与中国方案》，载《行政法学研究》2022 年第 4 期。

〔13〕 参见胡啸：《中国数据跨境流动安全管理制度设计》，载《中国网信》2024 年第 5 期。

〔14〕 参见吴玄：《数据主权视野下个人信息跨境规则的建构》，载《清华法学》2021 年第 3 期。

〔15〕 包括《个人信息出境标准合同办法》《个人信息出境标准合同备案指南》《关于实施个人信息保护认证的公告》等。

〔16〕 参见金晶：《作为个人信息跨境传输监管工具的标准合同条款》，载《法学研究》2022 年第 5 期；邢会强、李泽荟：《我国个人数据跨境流动认证制度及其完善》，载《郑州大学学报（哲学社会科学版）》2023 年第 6 期。

豁免订立标准合同、通过保护认证的实质就是豁免旨在保护个人权益的事前监管机制。由此也可看出，在订立标准合同、通过保护认证等保障措施下向境外提供个人信息，与根据上述豁免制度向境外提供个人信息，二者存在根本区别：前者是通过采取保障措施，确保个人信息即使流向境外也能得到相当于我国法规定水准的同等保护；后者是在没有保障措施确保达到我国法规定水准保护的情况下，仍然允许个人信息向境外提供。从保障个人信息传输至我国境外后也能得到同等保护这一原则来看，豁免订立标准合同、通过保护认证的事前监管构成了例外，应该严格解释。

而申报安全评估是旨在维护国家安全、公共利益的事前监管机制。这对于根据《网络安全法》第37条、《数据安全法》第31条以及相关配套规定，〔17〕关键信息基础设施运营者向境外提供个人信息或重要数据、其他数据处理者向境外提供重要数据应当申报安全评估来说，比较容易理解，因为关键信息基础设施和重要数据本身就涉及国家安全、公共利益。对于根据《个人信息保护法》第40条及相关配套规定，个人信息向境外提供应当通过安全评估的情形，虽然文义上没那么明显，但也应作如此理解。如前所述，第40条涉及的大量个人信息已经关系到公共利益甚至国家安全，而且将处理个人信息达到规定数量的个人信息处理者与关键信息基础设施运营者并列，也暗含了二者具有同等的重要性；处理者需要在申报前开展数据出境风险自评估，重点是评估个人信息出境活动可能“对国家安全、公共利益、个人或者组织合法权益带来的风险”，此时相较于个人信息主体的个人权益，对国家安全、公共利益带来的风险显然才是主要评估因素。〔18〕因此，豁免申报安全评估的实质就是豁免旨在维护国家安全、公共利益的事前监管机制。

由此，《规定》第5条的四种豁免情形同时豁免申报安全评估、订立标准合同、通过保护认证等三种事前监管，就是既豁免了旨在保护个人权益的事前监管机制，也豁免了旨在维护国家安全、公共利益的事前监管机制。但从上述对这四种豁免情形由来的分析看，在便利数据跨境流动的立场下，前三种场景豁免的主要考虑在于保护个人信息主体的个人权益且风险较低，第四种处理者豁免的主要考虑在于向境外提供的个人信息集合不至于影响国家安全、公共利益。这样来看，第5条的规定实际对基于个人权益考虑的前三种场景豁免同时豁免了旨在维护国家安全、公共利益的安全评估，对基于国家安全、公共利益考虑的第四种处理者豁免同时豁免了旨在保护个人权益的订立标准合同、通过保护认证。这是否意味着对于前三种场景豁免可以不再考虑大量个人信息出境对国家安全、公共利益的风险？如何理解第四种处理者豁免允许一定数量的个人信息在没有同等保护保障措施的情况下传输至境外？属于前三种场景豁免的，所涉及的个人信息是否计入第四种处理者豁免的累计数量？可以发现，在数据跨境管理双轨制下，对某些特定情形同时豁免目标定位不同的监管机制，会不可避免地产生理解与适用的困惑。

当然，在《规定》起草过程中，已经认识到需要在数据跨境管理双轨制体系中设计个人信息出境监管豁免制度。相较于《规范和促进数据跨境流动规定（征求意见稿）》，《规定》新增了多处有关“重要数据”的规定，以重申同时并行的旨在维护国家安全、公共利益的事前管理制度，例如第5条明确其四种豁免情形中“向境外提供的个人信息，不包括重要数据”，第2条强调

〔17〕 包括《数据出境安全评估办法》《数据出境安全评估申报指南》等。

〔18〕 参见程啸：《个人信息保护法理解与适用》，中国法制出版社2021年版，第319页；丁晓东：《数据跨境流动的法理反思与制度重构——兼评〈数据出境安全评估办法〉》，载《行政法学研究》2023年第1期。

“数据处理者应当按照相关规定识别、申报重要数据”。虽然“重要数据”概念的引入有利于明确豁免的边界，但鉴于重要数据和达到规定处理数量的个人信息之间的关系并不明确，重要数据认定制度仍在探索之中，〔19〕这些新增规定显然并没有解决上述困惑。

除了《规定》第 5 条规定的四种豁免外，第 4 条规定的过境个人信息豁免、第 6 条规定的自贸试验区负面清单外豁免，也都是同时豁免了申报安全评估、订立标准合同、通过保护认证等三种事前监管，这两种完全在上位法之外创设的豁免从文义上看可以涵盖的范围较广，在数据跨境管理双轨制体系下同样可能产生适用上的困惑。而理清和破解上述这些困惑就是实施个人信息出境监管豁免制度的关键所在。

二、数据跨境双轨制下个人信息出境监管豁免的适用困惑

上述豁免规则对特定情形既豁免了旨在维护国家安全、公共利益的安全评估机制，也豁免了旨在保护个人权益的订立标准合同、通过保护认证机制，但从数据跨境管理双轨制规范体系来看，这些豁免规则在理解与适用上仍存在一些亟待澄清的困惑。

（一）符合场景豁免的个人信息是否必然豁免安全评估

根据《规定》第 5 条，为订立履行合同所确需、为依法管理人力资源所确需、为保护信息主体切身利益所确需等三种场景豁免，不仅豁免了订立标准合同、通过保护认证，还豁免了申报安全评估。从文义上看，这三种场景豁免情形下所涉及的个人信息，无论数量多少，都豁免了申报安全评估。国家网信办《答记者问》就明确指出，属于这三种场景豁免情形的，不计入第 7 条作为安全评估申报判定条件之一的当年出境个人信息累计数量。按照这一解释逻辑，属于这三种场景豁免的，所涉个人信息也不应计入第 5 条第四种处理者豁免情形的累计数量。

但从《个人信息保护法》第 40 条规定来看，超过规定数量的大量个人信息不仅涉及众多个人的权益，还事关国家安全、公共利益。这背后的原因在于，一定规模的个人信息集合通过搜索、比对、关联等聚合分析，就可能会挖掘出信息集合背后蕴含的敏感信息甚至国家秘密。例如有研究者结合相关信息就从健身应用程序 Strava 公布的用户运动轨迹数据集中分析出了美国在阿富汗等地的军事基地位置。〔20〕鉴于此，该条才规定超过一定数量门槛的个人信息出境应当通过旨在维护国家安全、公共利益的事前安全评估机制。如果按照上述逻辑，将三种场景豁免下的个人信息都不计入作为安全评估申报门槛的当年出境个人信息累计数量，通过这三种场景豁免出境的个人信息即使超过《规定》第 7 条所设定的 100 万人一般个人信息或 1 万人敏感个人信息的申报门槛，也不需要事前申报安全评估，那此时如何管控这种大量信息集合出境可能引发的国家安全、公共利益风险？大量信息集合一旦出境往往更难管控，将此时的风险应对完全寄希望于事中事后监管是否妥当？如何落实第 40 条从出境个人信息数量维度管控风险的规范意旨？

需要指出的是，评估个人信息集合引发的国家安全、公共利益风险，除了数量这一定量维度

〔19〕 参见郭德香：《我国数据出境安全治理的多重困境与路径革新》，载《法学评论》2024 年第 3 期。

〔20〕 参见《跑步 APP 泄露美军事基地位置？五角大楼着手调查》，载 http://www.xinhuanet.com/world/2018-01/31/c_129802139.htm，最后访问时间：2024 年 6 月 10 日。

外，还要考虑敏感性这一定性维度，第 7 条区分一般个人信息和敏感个人信息已经意识到这一点。从定性维度看，即使达不到 1 万人敏感个人信息的安全评估申报门槛，对于关系国家安全、公共安全的敏感岗位人员例如军事人员，其特定的敏感个人信息就可能足以影响国家安全、公共利益。例如掌握某些关键岗位人员的医疗健康、金融支付等敏感个人信息，通过分析挖掘可以获知其健康、财务状况，以此可以威胁、利诱这些人员实施危害国家安全、公共利益的行为。〔21〕在这种情况下，即使符合上述前三种场景豁免和第四种处理者豁免，是否就必然不用考虑这些信息出境对国家安全、公共利益的可能影响而予以豁免安全评估？

虽然《规定》第 5 条明确其四种豁免情形中“向境外提供的个人信息，不包括重要数据”，可是重要数据与达到一定数量门槛的个人信息集合、敏感岗位人员特定敏感个人信息之间是何种关系并不明确，因此这种将重要数据排除适用豁免的规定，并不能解决上述适用困惑。而破解这些困惑，就亟须在数据跨境双轨制体系下厘清个人信息与重要数据、个人信息出境监管豁免制度与重要数据出境安全管理制度的关系。

（二）一定量个人信息为何可以豁免同等保护要求出境

《规定》第 5 条确立的第四种处理者豁免，对不涉及关键信息基础设施、当年累计不满 10 万人的一般个人信息出境，不仅豁免了申报安全评估，还豁免了订立标准合同、通过保护认证。其实该情形本身就未达到第 7 条规定的安全评估申报门槛，既然本来就未纳入安全评估范围，笔者认为该规定并不是创设安全评估的豁免，只是重申此时不需要申报安全评估。因此该规定只是创设了订立标准合同、通过保护认证的豁免。而如前所述，订立标准合同、通过保护认证是确保个人信息即使流向境外也能得到相当于我国法规定水准同等保护的保障措施，豁免这两种旨在确保同等保护的事前监管机制，就是允许个人信息在得不到同等保护的情况下仍然向境外提供，如此根据这一豁免将个人信息传输至境外显然会使信息主体的个人权益面临更大的风险。考虑到这种风险，是否还应该认为三种场景豁免下的个人信息都不计入此豁免下当年出境一般个人信息累计数量？

还需要指出的是，《个人信息保护》第 38 条规定的订立标准合同、通过保护认证等事前监管机制，是借鉴了欧盟《一般数据保护条例》（以下简称 GDPR）〔22〕的规定，但 GDPR 并没有类似上述第四种处理者豁免的规定。自 1995 年《个人数据保护指令》以来，欧盟一直坚持其境内的个人数据只能流向其认定提供同等的“充分水平保护”的国家。〔23〕GDPR 延续了这一规定，并明确将欧盟境内个人数据传输到未获充分性认定的国家或地区只能通过两种方式：一是具备适当的保障措施，包括具有约束力的公司规则、欧盟委员会批准的标准合同条款以及欧盟批准的认证机制等；二是符合特定情形下的克减规则，包括数据主体知悉风险后的明确同意、数据传输对于履行合同或法律请求是必要的、保护法律认可的公共利益、为了个人信息主体的重要利益等，

〔21〕 参见刘金瑞：《数据安全范式革新及其立法展开》，载《环球法律评论》2021 年第 1 期。

〔22〕 See *Regulation* (*EU*) 2016/679 *of the European Parliament and of the Council of* 27 *April* 2016 *on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data*, *and Repealing Directive* 95/46/*EC* (*General Data Protection Regulation*), Official Journal of the European Union, L 119, 4.5.2016, pp.1-88.

〔23〕 See *Directive* 95/46/*EC of the European Parliament and of the Council of* 24 *October* 1995 *on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data*, Official Journal of the European Communities, L 281, 23.11.95, Art.25, pp.31-50.

而且 GDPR 序言指出为合同或法律请求所必要的克减情形仅限于“临时性”的传输。〔24〕

比较而言，从制度功能上看，《规定》确立的“豁免规则”类似于欧盟的“克减规则”。不过从具体表述上看，二者存在较大差异：欧盟的“克减规则”规定了更多的例外情形，强调针对特定情形下的传输而不是经常性的，并且只有在穷尽所有可能确保同等保护水平的保障措施如标准合同、认证之后才能援引；〔25〕《规定》虽然确立了与 GDPR 部分克减情形类似的三种场景豁免，但还豁免了一定限量内成规模的一般个人信息出境，而 GDPR 显然并不支持为合同履行所必要等例外可以作为大量个人信息出境的合法基础，《规定》确立的豁免规则直接免除了订立标准合同、通过保护认证，并没有强调在穷尽标准合同、认证等措施保障同等保护的情况下才得以援引。

总结来看，《规定》第 5 条确立的第四种豁免情形允许当年累计不满 10 万人的一般个人信息在没有同等保护保障措施的情况下传输至境外，而这本属于《标准合同办法》明确要求事前订立标准合同的范围，这种新增豁免会使据此传输至境外的个人信息面临更大的风险，再加上上位法所借鉴的 GDPR 并未规定甚至隐含反对这种例外，如何在现有规范体系下妥当解释和适用这一豁免成为亟待解决的问题。

（三）符合豁免条件的过境个人信息是否必然豁免监管

《规定》第 4 条确立的过境个人信息豁免，对境内处理过程中“没有引入境内个人信息或者重要数据”的过境个人信息，既豁免了旨在维护国家安全、公共利益的申报安全评估，也豁免了旨在保护个人权益的订立标准合同、通过保护认证。需要指出的是，这里的过境个人信息并非一定是未经处理的单纯过境，但如果经处理则需符合上述限定条件，因而其不同于新加坡《个人数据保护法》豁免的“数据过境”情形，即个人数据经由新加坡中转至其他地区，且中转期间未被传输组织以外的主体访问、使用或向任何组织披露。〔26〕该豁免旨在鼓励个人信息入境处理，有利于我国跨境数据处理外包（“来数加工”）〔27〕和国际数据中心产业的发展，〔28〕值得高度肯定。但从上位法规定的属地管辖、域外管辖以及该条的文义涵盖范围来看，该豁免仍然存在一定的适用困惑。

《个人信息保护法》《数据安全法》都规定了属地管辖、域外管辖。前者第 3 条第 1 款明确规定在我国境内处理自然人个人信息的活动适用该法，而不论收集和产生个人信息是在境内还是境外，也不论自然人是中国公民还外国人；后者第 4 条第 2 款明确规定即使在我国境外开展数据处理活动，损害我国国家安全、公共利益或者公民、组织合法权益的，也应当依法追究法律责任。虽然可以认为该豁免是在便利数据跨境流动的立场下，根据《个人信息保护法》第 38 条授权条款“国家网信部门规定的其他条件”作出的例外规定，但这里豁免的只是个人信息跨境三种事前

〔24〕 See General Data Protection Regulation, Art. 46, Art. 47, Art. 49, Recital 111.

〔25〕 参见〔波兰〕马里厄斯·克里奇斯托弗克：《欧盟个人数据保护制度：〈一般数据保护条例〉》，张韬略译，商务印书馆 2023 年版，第 349 页。

〔26〕 See Personal Data Protection Act 2012, Art. 26; Personal Data Protection Regulations 2021, Art. 9, Art. 10.

〔27〕 “数字保税”（来数加工）是指在特定区域内，为产生于境外的数据要素提供收集、存储、加工、治理、交易等增值服务，服务产品用于境外市场或经审批后用于境内市场的商业模式。参见《海南儋州洋浦建成中国首个“数字保税”区》，载 https://www.chinanews.com.cn/cj/2024/02-27/10170910.shtml，最后访问时间：2024 年 6 月 10 日。

〔28〕 参见洪延青：《中国数据出境安全管理制度的“再平衡”——基于国家间数据竞争战略的视角》，载《中国法律评论》2024 年第 3 期。

监管机制，这些过境个人信息在我国境内的处理，按照属地管辖仍然要遵守上位法规定的其他处理义务和要求。既然《数据安全法》第2条第2款强调即使在我国境外开展数据处理活动损害我国国家安全、公共利益、私人合法权益都应当依法追责，那么在境外收集和产生的个人信息传输至我国境内处理，如果其处理损害我国国家安全、公共利益、私人合法权益，更应当依法追责。

那么有疑问的是，如果这些过境个人信息的境内处理，虽然符合处理过程中没有引入境内个人信息或者重要数据，但却发现违反上位法的规定，处理结果会损害个人信息主体（无论该主体是中国公民还是外国人）的个人权益，甚至是我国公共利益、国家安全，此时是否还应该允许这些处理后的个人信息出境呢？比如，境外收集的大量敏感个人信息（无论是否涉及中国公民）传输至我国境内进行分析，意图用于歧视性对待甚至电信诈骗等违法目的，此时是否还应允许其出境回传？再比如，假设某国机构在境外收集了曾在该国居住的我国特定人群的敏感个人信息，传输至我国境内进行某些行为习惯的分析，这些分析可能会影响我国国家安全，此时是否还应允许这些信息出境？

这些疑问说明《规定》确立的过境个人信息豁免，在表述上可能较为绝对、涵盖较广，应该在现有规范体系中予以准确理解和适当限缩。

（四）自贸试验区负面清单可否与现有豁免规则不一致

《规定》第6条确立的自贸试验区负面清单外豁免，是确立了一种豁免机制，自贸试验区可以按要求自行制定需要纳入事前监管的数据清单即负面清单，自贸试验区内数据处理者向境外提供负面清单外的个人信息，可以同时豁免申报安全评估、订立标准合同、通过保护认证等事前监管。这一负面清单外豁免规则，既有利于自贸试验区根据自身产业特点积极探索试验区内安全便捷的数据跨境流动，也有利于在实践基础上推动我国数据跨境管理制度创新。

在该规定出台之前，北京、天津、上海等地的自贸试验区已经开始积极探索跨境数据清单管理，2024年以来相关制度成果不断推出。1月初，据报道北京大兴国际机场临空经济区正在编制大兴自贸区数据跨境便利化管理办法以及相关数据清单。〔29〕2月7日，天津自贸试验区印发《中国（天津）自由贸易试验区企业数据分类分级标准规范》（以下简称《天津规范》），将企业数据分成13大类40子类，从高到低分为核心、重要、一般三个级别，明确了重要数据的识别标准。2月8日，上海自贸试验区印发《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》（以下简称《上海办法》），将跨境数据从高到低分为核心数据、重要数据、一般数据三个级别，其第9条规定既要制定重要数据目录，又要制定数据出境负面清单。据官方披露，该试验区正在加快编制跨境数据的一般数据清单和重要数据目录，截至2月底已基本编制完成智能网联汽车、公募基金、生物医药等领域的跨境流动分级分类的首批清单目录。〔30〕《规定》出台后，天津自贸试验区延续《天津规范》数据分类分级和重要数据识别的思路于5月8日印发了全国首个“数据出境管理清单（负面清单）”；上海自贸试验区于5月16日印发了涵盖

〔29〕 参见骆倩雯：《助力数字经济高质量发展 北京率先实现数据跨境安全便捷流动》，载《北京日报》2024年1月9日，第2版。

〔30〕 参见《对境内外媒体开放！上海团代表今天回答了这些热点问题》，载 https://mp.weixin.qq.com/s/E8aIKLrOh9q69tCdpQ5rDQ，最后访问时间：2024年6月10日。

智能网联汽车、公募基金、生物医药等三个领域的首批一般数据清单。

有疑问的是，自贸试验区设立的负面清单外豁免，可否与《规定》确立的豁免规则不一致，可否比现有豁免规则更为宽松或更加严格。例如，《天津规范》在“互联网服务和电子商务类”数据下，将“在提供互联网服务过程中产生的可用来实施社会动员的数据，相关退伍人员等敏感人群数字画像数据，对军工、政府类客户记录和跟踪的数据”认定为重要数据，如果将退伍人员等敏感群体的数据纳入负面清单，会不会与《规定》的场景豁免或处理者豁免发生冲突，如果冲突应如何处理？此外，负面清单和重要数据目录是何种关系？从目前地方探索来看，《上海办法》仅提出同时规定，尚未涉及二者的关系；《天津规范》虽只提出制定重要数据目录，但上述天津负面清单明确规定“国家行业主管部门或本市认定的重要数据纳入本清单管理”。

虽然为了法制统一，《规定》要求在国家数据分类分级保护制度框架下制定负面清单并履行报批报备手续，但显然这些规定并不能解决上述困惑。解答这些困惑，就需要在现有规范体系下准确把握负面清单外豁免的实质并予以妥当适用。

（五）实践需要与安全关切双重压力下应如何完善豁免

《规定》在便利数据跨境流动的立场下，就个人信息跨境提供而言，确立了个人主动发起和为了个人重大利益的特定场景豁免、向境外提供低敏感性个人信息集合的处理者豁免、过境个人信息豁免和自贸试验区负面清单外豁免，这些豁免规则降低了相关企业开展跨境业务和运营的合规成本，受到各方广泛肯定。但企业跨境数字贸易和跨境运营的实践场景丰富多样，这些豁免规则显然并不能完全覆盖实践需要。

例如，跨国企业往往会在全球分支机构统一部署跨境协同办公系统如远程会议系统，并将办公系统的服务器部署在总部所在国，其中国分支机构的员工使用该系统时，该员工的个人信息必然会出境，而且根据业务需要也会向境外提供相关客户或供应商的个人信息。这种跨国公司常见运营场景下的个人信息出境，就无法被《规定》确立的豁免规则所涵盖。相较之下，欧盟 GPPR 确立的克减规则能够提供更多的豁免选择。在上述例子中，如果只是涉及个别客户或供应商的个人信息出境，可以按照“数据主体知悉风险后明确同意”的克减规则向境外提供。〔31〕

虽然从实践看增设一些必要豁免规则是合理的，但笔者认为并非所有实践需要都适合创设豁免规则。欧盟克减规则的制度定位和适用顺位提醒我们：个人信息出境监管豁免规则是保障个人信息传输至境外后也能得到同等保护这一原则的例外，根据此豁免将个人信息传输至境外显然会使个人信息权益面临更大的风险，因此这种例外的豁免不应成为个人信息大规模出境的一般合法基础。换言之，《规定》确立的豁免规则，本身就是个人信息跨境流动的例外规则，其制度定位不是为了解决经常性、成规模的个人信息跨境，这就是 GDPR 克减规则只针对“特定情形”的原因所在。〔32〕申言之，很多日常的个人信息跨境流动的实践需要，是豁免制度不能承受之重，并

〔31〕 当然欧盟的规定和实践，并不支持以克减规则下的“同意”作为个人信息大规模跨境传输的合法基础，而且 GPPR 的克减规则必须在穷尽所有可能确保同等保护水平的保障措施如标准合同、认证之后才能援引。

〔32〕 See European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, p. 4, available at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf, last visited on Jun. 10, 2024.

不能通过豁免规则来实现。

需要指出的是，无论是免除个人信息出境事前监管的豁免规则，还是确保个人信息出境后得到同等保护的保障措施，都是促进个人信息跨境流动和利用的制度设计，相较于欧盟 GDPR 等国外个人信息保护法的相关规定，我国这两方面的制度规定都相对较少，导致我国个人信息跨境流动制度被扣上了“严苛”的帽子。笔者认为规定较为有限的原因很大程度上在于国家安全的关切，担忧大量个人信息等数据出境后可能引发国家安全风险。〔33〕在便利数据跨境流动的立场下，这种囿于安全忧虑的数据跨境管理制度，结合域外法可资借鉴的规则来看，仍有一定的完善空间。

面对数据跨境流动迫切的实践需求，随着我国数据跨境双轨制体系下维护国家安全、公共利益的数据出境安全管理制度的不断完善，笔者认为在保障国家数据安全的前提下，可以对个人信息出境监管豁免制度予以进一步的完善。

三、数据跨境双轨制下个人信息出境监管豁免的规则完善

上述数据跨境双轨制下的适用困惑，凸显了个人信息出境监管豁免制度完善的规则需求：制度定位亟需更加明确，规则适用边界有待厘清，豁免限度需要系统把握，规则运行需要制度协同。以下就从这四方面入手，就数据跨境管理双轨制体系下如何妥当适用个人信息出境监管豁免制度提出完善建议。

（一）明确特定豁免只是豁免保护个人权益监管机制

我国法律目前确立的数据跨境管理制度是双轨并行的：一是旨在维护国家安全、公共利益的重要数据出境安全管理制度，监管机制是事前申报安全评估；二是旨在保护个人权益的个人信息跨境提供制度，监管机制是事前订立标准合同或通过保护认证。对于个人信息出境监管豁免制度而言，首先就要明确其豁免的是“哪一轨”的事前监管，这涉及其本质上的制度定位。虽然从目前《规定》的表述看，第 5 条的四种特定豁免情形都同时豁免了申报安全评估、订立标准合同、通过保护认证，但从前文分析来看，同时豁免目标定位分属双轨的监管机制是产生适用困惑的主要原因。

实际上，对于个人信息而言，一般情况下只涉及信息主体的个人权益，例外情况下才会涉及国家安全、公共利益，这被《个人信息保护法》从定量维度规定为“达到规定数量”，即超过一定数量门槛成规模的个人信息集合通过聚合分析可能影响国家安全、公共利益，《规定》第 7 条将数量门槛设定为当年出境个人信息累计达到 100 万人一般个人信息或 1 万人敏感个人信息。因而，对于一般情况下达不到数量门槛的个人信息出境而言，豁免的只能是旨在保护个人权益的事前监管机制，在我国就是订立标准合同或通过保护认证。从前述豁免由来分析看，第 5 条前三种场景豁免就属于这种一般情况。对于这三种场景豁免，由于未达到安全评估申报门槛，因而不需要申报安全评估，《规定》对此表述为“免予”申报，但笔者认为这里的“免予”申报不应认为是创设了一种豁免，应监管而免予监管才可谓“豁免”，未监管而称“免予”监管只能算是一种

〔33〕 参见许可：《自由与安全：数据跨境流动的中国方案》，载《环球法律评论》2021 年第 1 期；赵海乐：《数据主权视角下的个人信息保护国际法治冲突与对策》，载《当代法学》2022 年第 4 期。

重申。前三种场景豁免实质上豁免的只是旨在保护个人权益的订立标准合同或通过保护认证。

第 5 条第四种处理者豁免，其本身也未达到安全评估申报门槛，同样也不能认为是规定了申报安全评估的豁免，而只能是创设了订立标准合同、通过保护认证的豁免。豁免这两种事前监管机制，就是豁免了保障个人信息传输至我国境外后也能得到同等保护的基本要求，如此该豁免就是允许当年累计不满 10 万人的一般个人信息可以在没有同等保护保障措施的情况下传输出境，那么为何允许一定规模的个人信息豁免同等保护要求出境呢？从《个人信息保护法》的规定来看，明确涉及出境个人信息数量的第 40 条只是授权法律、行政法规和国家网信部门可以豁免出境安全评估，第 38 条授权条款“国家网信部门规定的其他条件”本身不足以解释豁免个人信息出境同等保护要求的正当性。笔者认为，该豁免的上位法依据除了《个人信息保护法》第 38 条外，还应当包括该法第 62 条中授权国家网信部门针对小型个人信息处理者〔34〕制定专门个人信息保护规则的规定，如此第四种处理者豁免可以理解为：基于便利数据跨境流动的立场，在未达到安全评估申报数量门槛即不至于影响国家安全、公共利益的情况下，为适当减轻小型个人信息处理者数据跨境合规成本，对限定规模的一般个人信息集合出境豁免了出境后也需得到相当于我国法规定水准的同等保护的要求。

有疑问的是，《规定》第 5 条前三种场景豁免情形下的个人信息，是否计入该条第四种处理者豁免情形、第 7 条应申报安全评估情形、第 8 条应订立标准合同或通过保护认证情形下的当年出境个人信息累计数量。国家网信办《答记者问》的观点是不计入。但如果认为不计入累计数量，则通过这三种场景豁免出境的所有个人信息，包括敏感个人信息或一般个人信息，不论数量规模有多大，例如超过 100 万人一般个人信息或 1 万人敏感个人信息，既不会受到旨在保护个人权益的订立标准合同或通过保护认证机制的监管，也不会受到旨在维护国家安全、公共利益的申报安全评估机制的监管。

从保护个人权益来看，基于场景豁免向境外提供信息，本身就属于我国法上保障个人信息传输至境外后也能得到同等保护这一原则的例外，会使出境个人信息面临较大风险，如果此时出境个人信息规模不受任何限制，则同等保护的例外情形就会成为普遍现象，没有同等保护措施保障的大量出境个人信息只能陷入风险之中，大规模个人信息出境也不能以“小型个人信息处理者”证成正当性，那么上位法同等保护出境个人信息的规范目的就可能落空。从维护国家安全、公共利益来看，基于场景豁免向境外提供信息，虽然一般情形下不涉及国家安全、公共利益，但按照《个人信息保护法》第 40 条的规范意旨，达到规定数量门槛的大规模个人信息集合出境就可能影响国家安全、公共利益，这也是规定此时应如同重要数据一样通过安全评估的原因所在，如果不管控通过这些场景豁免出境的个人信息，那么上位法从出境个人信息数量维度管控国家安全、公共利益风险的规范目的就可能落空。因此，基于体系解释和目的解释，笔者认为第 5 条前三种场景豁免情形下的个人信息，应该计入上述情形下的当年出境个人信息累计数量。

总而言之，个人信息出境监管豁免制度实际上豁免的只是旨在保护个人权益的事前监管机制即

〔34〕 对于小型个人信息处理者目前尚未有明确界定，主要是指处理个人信息数量较少且自身规模也很小的个人信息处理者。参见程啸：《个人信息保护法理解与适用》，中国法制出版社 2021 年版，第 470 页。

订立标准合同、通过保护认证。如果一定数量的个人信息集合，无论是通过《规定》第5条前三种场景豁免还是第四种处理者豁免出境，尚未达到旨在维护国家安全、公共利益的事前监管机制即安全评估的申报门槛，则本身不属于安全评估的适用范围，此时谓之“免予申报”只是重申和强调未纳入监管，不存在豁免申报安全评估的问题。前三种场景豁免情形下的个人信息，限于个人发起或为了个人利益的场景往往数量较少，虽然在特定场景之下豁免了旨在保护个人权益的订立标准合同、通过保护认证，但应该计入当年出境个人信息累计数量，如果累计达到了第8条的监管门槛，则应按规定订立标准合同或通过保护认证，如果累计达到了第7条安全评估的申报门槛，则应依法申报安全评估。因此，笔者认为对第5条“免予申报安全评估”应当予以限缩解释：特定场景或处理者所处理的个人信息，在累计数量未达到安全评估申报数量门槛的情况下，不需要申报安全评估。《规定》第7条第2款中“属于第五条规定情形的，从其规定”，也应该在这个意义上予以理解。如此解释，才符合我国数据跨境管理双轨制度相互独立、并行不悖的体系架构。申言之，无论是为了个人信息主体的场景豁免，还是为了个人信息处理者的豁免，都是为了私人利益的豁免，为了私人利益针对特定情形的监管豁免不等于就可以同时豁免为了国家安全、公共利益的监管。

（二）厘清个人信息与重要数据关系以明确豁免边界

虽然《规定》第5条第2款明确其四种豁免情形中“向境外提供的个人信息，不包括重要数据”，但这种排除规定并不能消除对于豁免制度适用边界的困惑，原因就在于个人信息和重要数据的关系并不明确：个人信息和重要数据是否为简单包含关系，《规定》第7条达到一定数量门槛的个人信息集合是否属于重要数据，达不到数量门槛的个人信息集合是否就一定不属于重要数据。面对这些困惑，根据《规定》第2条负有重要数据识别申报义务的数据处理者仍然面临较大的合规压力，因为其不可能仅以“未被告知或公布为重要数据”为由就主张尽到了该义务，如果对于未被告知或公布为重要数据但可能影响国家安全、公共利益的数据〔35〕视而不见，数据处理者仍要承担相应法律责任。厘清个人信息与重要数据关系，成为明确个人信息出境监管豁免制度适用边界的关键所在。

对于重要数据，法律并未给出明确定义，2022年7月发布的《数据出境安全评估办法》将其界定为“一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据”。〔36〕对于个人信息和重要数据的关系，2021年8月发布的《汽车数据安全管理若干规定（试行）》第3条规定“涉及个人信息主体超过10万人的个人信息”属于“重要数据”，2021年11月发布的《网络数据安全管理条例（征求意见稿）》[以下简称《条例（征求意见稿）》]第26条把“100万人以上个人信息”视为“重要数据”来管理，而根据《规定》第7条与“重要数据”一样需要申报数据出境安全评估的情形为当年累计向境外提供100万人以上一般个人信息或者1万人以上敏感个人信息，这些不同规定说明目前对二者的关系尚未达成共识。

〔35〕 对于这些可能纳入重要数据范围的数据，数据处理者负有主动申报义务。从重要数据识别认定程序来看，先由数据处理者按照有关标准梳理识别自身可能的重要数据，向相关主管部门申报，然后由主管部门予以审核认定。

〔36〕 国家标准《数据安全技术 数据分类分级规则》（GB/T 43697—2024）将其界定为“特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据”。

从个人信息和重要数据的定义来看，前者的核心在于“个人”，即“与已识别或者可识别的自然人有关”，后者的核心在于“重要”，即事关国家安全、公共利益，因此仅涉及私主体权益的数据包括个人信息在内，一般不会构成重要数据。〔37〕但如前所述，达到一定规模的个人信息集合通过聚合分析，可能会挖掘出影响国家安全、公共利益的敏感信息，笔者认为这种个人信息集合应该纳入重要数据的范围。《条例（征求意见稿）》将“100 万人以上个人信息”视为“重要数据”来管理，就是考虑了数据集合的风险。但对于界定个人信息集合引发的国家安全、公共利益风险，笔者认为仅从数量这一定量维度出发是不充分的，还应考虑敏感性这一定性维度。美国近年来出于国家安全考虑，将敏感个人数据纳入外资安全审查，〔38〕签发《敏感个人数据行政命令》等，对个人数据集合引发国家安全风险的“敏感性”进行了专门界定，值得借鉴。

以《敏感个人数据行政命令》为例，其识别了六种可能被利用于危害美国国家安全的“敏感个人数据”，包括个人标识符、地理位置和相关传感器数据、生物特征标识符、人体组学数据、个人健康数据以及个人财务数据，又根据这些数据引发国家安全风险的不同分为“美国人大量敏感个人数据”和“美国政府相关数据”两类。按照美国司法部近期就该行政命令发布的拟议规则，〔39〕前者是指达到规定数量门槛的美国人敏感个人数据集合，拟议规则以过去 12 个月为期限对每类敏感个人数据设定了可能影响国家安全的不同数量门槛，例如：对于个人健康数据和个人财务数据来说，涉及超过 100 万美国人是高风险；对于生物特征标识符来说，涉及超过 1 万美国人是高风险。后者是指与美国政府敏感人员或地点相关联或可关联的敏感个人数据，而无论其数量如何，其中敏感人员主要涉及联邦政府（包括军队）现任或近期离任的雇员、承包商或者前任高级官员，敏感地点主要涉及地理围栏区域内的某些敏感地点。可以发现，该行政命令在界定国家安全“敏感性”上不仅考虑了定量维度，还考虑了个人信息本身涉及的敏感领域、敏感人员或地点等定性维度，对于敏感人员或地点而言，并未规定数量门槛。

笔者认为，界定因聚合挖掘可能影响国家安全、公共利益而构成重要数据的个人信息集合，除了考虑数量规模这一定量维度外，还应当从定性维度界定个人信息集合对国家安全、公共利益的高风险性。这种高风险性界定可以从个人信息本身涉及的敏感领域、敏感人员或地点入手：对于所涉领域这种敏感“面”的界定，为防止泛化可以列明具体领域并辅以数量门槛予以限定，例如当年累计出境 1 万人以上个人生物识别信息；对于所涉人员或地点这种敏感“点”的界定，因为风险足够特定则不需要规定数量门槛，例如涉及关系国家安全、公共安全的特定人员或地点的个人信息。从这个角度看，不宜将《规定》第 7 条规定的需要申报安全评估的当年累计出境 100 万人以上一般个人信息或者 1 万人以上敏感个人信息直接理解为“重要数据”：100 万人以上一般个人信息，仅有定量维度而未考虑定性因素，显然无法充分界定对国家安全、公共利益的高风险性；而 1 万人以上敏感个人信息，虽然区分了一般领域与敏感领域的个人信息，但这里的“敏

〔37〕 国家标准《数据安全技术 数据分类分级规则》（GB/T 43697—2024）指出仅影响公民个体的数据一般不作为重要数据。

〔38〕 See *Foreign Investment Risk Review Modernization Act of* 2018（FIRRMA），Pub. L. No. 115－232，132 Stat. 2173；*Provisions Pertaining to Certain Investments in the United States By Foreign Persons*，31 C. F. R. Part 800.

〔39〕 See Department of Justice：*National Security Division*：*Provisions Regarding Access to Americans’ Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern*，*Federal Register*，Vol. 89，No. 44，March 5，2024，pp. 15780－15802.

感”主要是考虑了个人信息对信息主体权益保护的重要性，〔40〕考虑到个人信息集合因所涉领域、人员或地点的不同而对国家安全、公共利益有不同程度的风险性，笼统而未区分具体领域的敏感个人信息以及1万人以上的统一数量门槛仍不足以界定这种风险差异性。

因此，除了累计达到《规定》第7条和第8条设定的数量门槛之外，个人信息或个人信息集合还可能因为构成重要数据而排除适用个人信息出境监管豁免制度。为了减轻个人信息处理者识别重要数据的合规压力，应该尽快在重要数据认定规则中厘清个人信息与重要数据的关系。虽然考虑到不同领域的差异性和复杂性，重要数据认定规则需要按行业或领域单独制定，〔41〕但笔者认为《网络数据安全管理条例（草案）》等配套立法应当规定重要数据认定的基本条件、基本程序等共通规则，形成相对统一的认定指引，这种共通规则就应当包括界定个人信息或个人信息集合因引发国家安全、公共利益风险而构成重要数据的规则，而根据上述分析就需要以定性与定量相结合的方式，明确可能对国家安全、公共利益构成高风险的敏感个人信息的特定种类，以及这些敏感个人信息所涉及的敏感人员或地点的范围，或者这些不同种类敏感个人信息集合需要达到的数量门槛。

（三）系统把握过境个人信息豁免和负面清单外豁免

相较于《规定》第5条的四种特定豁免情形，第4条规定的过境个人信息豁免情形和第6条规定的自贸试验区负面清单外豁免情形，由于文义涵盖范围较广，都是创设了相对不特定的豁免规则。由于这两种情形是就相对不特定范围同时豁免了申报安全评估、订立标准合同、通过保护认证等事前监管，为了避免这种不特定豁免造成负面影响，就需要在数据跨境管理双轨制体系下系统把握这两种豁免规则适用的合理限度。

如前所述，《规定》确立的过境个人信息豁免，其中的过境个人信息既涵盖未经处理的单纯过境个人信息，也涵盖经过处理的过境个人信息，只要后者符合境内处理“没有引入境内个人信息或者重要数据”的限定条件。但这一限定条件是否足以承载《个人信息保护法》《数据安全法》对个人信息主体权益以及我国国家安全、公共利益的保护？符合这一简单限定条件是否就可以不受任何监管而自由出境？从前文所举的例子看，回答都应该是否定的。笔者认为，《规定》第4条确立的过境个人信息豁免，仅是豁免了个人信息出境的三种事前监管机制，过境个人信息在我国境内的处理，按照上位法确立的管辖制度仍要遵守上位法规定的其他义务和监管要求；如果过境个人信息的境内处理会损害个人信息主体（无论是否为中国公民）的个人权益或者我国国家安全、公共利益，则经过处理的过境个人信息及其处理结果也不应允许出境。因此，准确理解《规定》第4条就应该按照体系解释对该条增加必要的限制，即过境个人信息境内处理没有引入境内个人信息或者重要数据的，免于申报安全评估、订立标准合同、通过保护认证，但“损害我国国家安全、公共利益或者自然人个人信息权益的除外”。

《规定》确立的自贸试验区负面清单外豁免，依托于自贸试验区的负面清单制度，目前较为困惑的是自贸试验区自行设立的负面清单外豁免可否与《规定》确立的豁免规则不一致，负面清单与重要数据目录到底是何种关系。所谓的负面清单，即要纳入申报安全评估、订立标准合同、通过保

〔40〕 参见张继红、蔡雨倩：《敏感个人信息跨境流动的国际规制》，载《广西社会科学》2023年第7期。

〔41〕 参见国家标准《数据安全技术 数据分类分级规则》（GB/T 43697—2024）附录G“重要数据识别指南”；周亚超、左晓栋：《我国重要数据识别方法研究》，载《网络信息法学研究》2020年第2期。

护认证等三种事前监管的数据清单，负面清单的反面就是负面清单外豁免的范围。如果允许自贸试验区负面清单外豁免与《规定》的豁免规则不一致，实际就是允许自贸试验区规定的上述三种事前监管范围比《规定》更加严格或更加宽松，而无论是更加严格或更加宽松显然都是改变了目前《规定》较为统一的监管水平。笔者认为对于包括个人信息在内的数据来说，其属性不会因地域不同而发生改变，对于全国性规定确立的统一监管要求，如果没有充分正当的理由不宜轻易调整其在某个地域的适用。从目前自贸试验区的定位和探索来看，并不存在因地域性差异而调整《规定》数据出境事前监管要求的空间，《规定》也明确要求负面清单应在国家数据分类分级保护制度框架下制定。因此，笔者认为原则上自贸试验区负面清单外豁免应该与《规定》确立的豁免规则保持一致。

那么为何还要设立自贸试验区负面清单外豁免呢？笔者认为原因在于：目前国家数据分类分级保护制度仍在不断发展健全中，这也是《规定》称之为“制度框架”的原因所在，尤其是重要数据认定制度正在按行业或领域逐步探索健全中，〔42〕在某些行业或领域尚未制定重要数据认定规则，而自贸试验区因自身产业发展又在这些行业或领域如生物医药、智能网联汽车等存在数据跨境迫切需要的情况下，赋予自贸试验区探索负面清单的空间，允许负面清单外数据豁免出境事前监管，既有利于便利自贸试验区数据跨境流动，避免因规则不确定性阻碍相关产业发展，也有利于在自贸试验区探索基础上，推动各行业各领域加快形成和健全重要数据认定规则。因此，笔者认为自贸试验区负面清单机制实质上是通过业务场景触发推动相关行业或领域加快形成重要数据认定规则的有力举措，自贸试验区负面清单的主要内容最终要被纳入国家重要数据目录之中。正是因为自贸试验区负面清单涉及重要数据目录的制定，尽管国家网信办已会同国家数据局明确了此种负面清单备案工作机制和流程，〔43〕但目前《规定》确立的负面清单报批报备手续仍有完善的空间。根据《数据安全法》第 21 条的规定，在重要数据认定方面，国家数据安全工作协调机制负责统筹协调有关部门制定重要数据目录，各地区、各部门负责确定本地区、本部门以及相关行业、领域的重要数据具体目录。笔者认为，为了贯彻这一规定并维护重要数据认定制度的统一性，自贸试验区自行制定的负面清单，经省级网络安全和信息化委员会批准后，应当报国家数据安全工作协调机制办公室备案。〔44〕

（四）增强数据跨境制度协同性以缓解豁免规则压力

面对日益增长的跨境数字贸易和跨境业务运营的需要，我国适时增设个人信息出境监管豁免制度，及时回应了数据跨境流动的实践需求，但有观点认为目前的豁免规则仍不能满足实践需要，应该扩大豁免规则的覆盖范围。〔45〕与此同时，我国面临的数据安全形势依然严峻，再加上域外国家不断出台基于国家安全关切管控个人信息跨境流动的举措，〔46〕有的国家甚至泛化国家

〔42〕 参见刘金瑞：《我国重要数据认定制度的探索与完善》，载《中国应用法学》2024 年第 1 期。

〔43〕 参见胡啸：《中国数据跨境流动安全管理制度设计》，载《中国网信》2024 年第 5 期。

〔44〕 经国家数据安全工作协调机制批准发布的《天津规范》就明确指出，天津自贸试验区企业重要数据目录，应当按程序报送国家数据安全工作协调机制办公室。

〔45〕 有学者指出从国际经贸协定看《规定》存在“缺失”，一些正常经贸活动所涉业务模式未被豁免。参见洪延青：《中国数据出境安全管理制度的“再平衡”——基于国家间数据竞争战略的视角》，载《中国法律评论》2024 年第 3 期。

〔46〕 See World Economic Forum, *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*, p. 16, available at http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf, last visited on Jun. 10, 2024.

安全概念毫无根据地阻止个人数据流向我国，例如美国颁行的《敏感个人数据行政命令》，凸显了豁免规则的适用必须以保障国家数据安全为前提。面对实践需要与安全关切的双重压力，如何妥当适用和完善豁免规则就更加棘手。

解决此棘手问题，离不开对个人信息出境监管豁免制度体系定位的准确把握。总结前文所述，在数据跨境管理双轨制体系中，个人信息出境监管豁免制度属于个人信息跨境提供制度的一部分，其豁免的只是旨在保护个人权益的事前监管机制即订立标准合同、通过保护认证，其无法豁免旨在维护国家安全、公共利益的事前监管机制即申报安全评估，如此才符合我国数据跨境管理双轨制度独立并行的应有之义。这种理解的关键在于将《规定》第 5 条前三种场景豁免情形下的个人信息，认为仅是在特定场景之下豁免了旨在保护个人权益的订立标准合同、通过保护认证，但应该计入当年出境个人信息累计数量，如果累计达到了安全评估的申报门槛，就应当依法申报安全评估。如此才能贯彻《个人信息保护法》第 40 条从出境个人信息数量维度管控国家安全、公共利益风险的规范目的，避免出现基于特定场景豁免向境外提供大量信息引发国家安全、公共利益风险而不受管控的问题。这说明只要准确适用数据跨境管理双轨制，就可以在保障国家数据安全的前提下适用豁免规则，国家安全关切就会得到充分重视和妥善解决。

在个人信息跨境提供制度中，我国《个人信息保护法》确立了保障个人信息传输至境外后也能得到同等水平保护的基本要求，订立标准合同、通过保护认证就是确保这种境外同等水平保护的保障措施，而个人信息出境监管豁免制度正是豁免了这两种旨在确保同等保护的事前监管措施，就是允许个人信息在得不到同等保护的情况下仍然向境外提供，显然根据豁免规则出境的个人信息会面临较大风险。从体系解释来看，为了贯彻同等保护出境个人信息的规范目的，订立标准合同、通过保护认证才应当是个人信息出境的一般合法基础，作为同等保护原则例外的豁免规则，应当严格限于特定情形适用，其制度定位不是为了解决经常性、成规模的个人信息跨境流动。因此，面对很多经常性的个人信息跨境流动实践需要，应当在坚持同等保护出境个人信息的原则下，探索设立新的个人信息跨境流动合法途径，而非寄希望于不断增设更多的豁免规则。

需要指出的是，即使面对实践迫切需要的压力，也应该恪守制度体系的规范性、系统性，不能让豁免规则的适用变形和异化，从而影响整个数据跨境管理制度体系的规范意旨。上文提到的认为《规定》第 5 条前三种特定场景豁免下的个人信息不计入当年出境个人信息累计数量的观点，虽然出发点是为了便利数据跨境流动，但这种理解会使基于场景豁免出境的大量个人信息不受任何管控，如此既可能使上位法从出境个人信息数量维度管控国家安全、公共利益风险的规范目的落空，也可能使上位法同等保护出境个人信息的规范目的落空，从而影响整个数据跨境管理双轨制体系的运行。这也说明豁免制度只能在其制度定位范围内便利数据跨境流动，不能让其承受不能承受之重。

当然在数据跨境管理双轨制体系下，基于便利数据跨境流动的立场，贯彻构建事前事中事后全链条监管的要求，结合域外法治经验来看，个人信息出境监管豁免制度及其与相关个人信息跨境提供制度的协同性仍有完善空间。具体而言，一是考虑增设一些必要的豁免规则。考虑到常见的实践场景，借鉴 GDPR 等规定，可以考虑增设个人信息主体知悉风险后的明确同意、保护法律认可的公共利益等豁免规则。二是可以增加个人信息跨境流动的合法基础。对于确保出境个人信

息得到同等水平保护的保障机制，除了目前的订立标准合同、通过保护认证，可以考虑增加允许跨国公司内部转移个人信息的具有约束力的公司规则。〔47〕还可以考虑根据对等原则，通过双边或者多边谈判在相关国家之间建立个人信息跨境流动“白名单”制度〔48〕以及健全境外个人信息处理者问责制度。〔49〕通过完善个人信息跨境提供制度，增强不同制度规则促进个人信息跨境流动和利用的协同性，可以有效缓解豁免规则面临的实践压力。

Abstract: The new regulations for cross-border data establish an exemption system from supervision on outbound transfer of personal information, which provides exemptions from the requirements to apply for the outbound data transfer security assessment, to conclude a standard contract for the outbound transfer of personal information, and to obtain the personal information protection certification. However, from the perspective of the dual-track management system for cross-border data in China, these exemption rules still face a series of application confusions: whether personal information that meets the scenario exemption is necessarily exempted from security assessment, why a certain amount of personal information transfer abroad can be exempted from the same protection requirements, what are the reasonable limits of exemptions of personal information in transit and data outside the negative list, and how to improve exemptions under the dual pressure of practical needs and safety concerns. To resolve these confusions, we should make it clear that specific exemptions are only exemptions from the regulatory mechanism to protect personal rights and interests, clarify the relationship between personal information and important data to clarify the boundaries of exemptions, systematically grasp exemptions of personal information in transit and data outside the negative list, and enhance the synergy of systems for cross-border data flows to ease pressure on exemption rules.

Key Words: personal information, exemption from supervision on outbound transfer, dual-track system for cross-border data, important data, national security

（责任编辑：张金平）

〔47〕 See European Data Protection Board, *Recommendations 1/2022 on the Application for Approval and on the Elements and Principles to be Found in Controller Binding Corporate Rules* (*Art. 47 GDPR*), available at https://www.edpb.europa.eu/system/files/2023-06/edpb_recommendations_20221_bcr-c_v2_en.pdf, last visited on Jun. 10, 2024.

〔48〕 参见何波：《中国参与数据跨境流动国际规则的挑战与因应》，载《行政法学研究》2022 年第 4 期。

〔49〕 事后问责制度的典型代表是亚太经济合作组织的跨境隐私规则体系（CBPR System）。See APEC, *APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines*, available at http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf, last visited on Jun. 10, 2024.