

数据出境安全评估的申报义务与责任分配

以义务主体的识别、评估标准的适用与违法出境的责任构造为中心

赵跃

(安徽国运律师事务所, 安徽 合肥 230000)

摘要: 数据出境的安全评估, 是我国数据跨境流动管理的基础制度。数据处理者向境外提供重要数据或者达到规定数量的个人信息, 应当申报评估, 未经评估不得出境。制度的运行暴露出三个问题: 义务主体的识别标准不清, 评估的内容与标准缺乏可操作性, 违法出境的责任构造不完整。本文认为, 申报义务的主体应当以数据处理者为核心, 同时区分委托处理、共同处理与境外接收方的责任层次, 不能将义务不加区分地加于所有参与主体。评估的标准应当从形式审查转向实质判断, 重点考察出境的目的、数量、敏感程度与接收方的保护能力, 形成可量化的判断框架。未申报的法律后果, 应当包括行政责任与民事责任两个方面。行政责任以责令改正、罚款、暂停业务为主; 民事责任的构造, 则须解决权益侵害的认定、因果关系的证明与赔偿范围的计算三个难题。在责任的分配上, 应当区分处理者的组织责任与接收方的直接责任, 避免责任的虚置或者过度集中。

关键词: 数据出境; 安全评估; 申报义务; 责任分配; 个人信息保护

中图分类号: D922.17 **文献标识码:** A **文稿编号:** WJLT(2021)06-0025-12

Reporting Obligations and Allocation of Liability in Security Assessment of Outbound Data Transfers

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: Security assessment is the foundation of China's regulation of cross-border data flows. A data processor transferring important data or personal information above the prescribed threshold abroad must file for assessment before transfer. Three problems have emerged: unclear tests for identifying the obligated subject, inoperable assessment standards, and an incomplete structure of liability for unlawful transfer. This article argues that the obligated subject should center on the data processor, with liability layered among entrusted processing, joint processing and overseas recipients rather than imposed indiscriminately. Assessment should move from formal review to substantive judgment, examining purpose, volume, sensitivity and the protection capacity of the recipient in a quantifiable framework. Consequences of failure to file include both administrative and civil liability; the latter must resolve the recognition of infringement, proof of causation and calculation of damages. Liability should be allocated between the organizational responsibility of the processor and the direct responsibility of the recipient.

Key words: outbound data transfer; security assessment; reporting obligation; allocation of liability; personal information protection

说明: (本文为作者个人研究观点, 不代表所在单位意见)

作者简介: 赵跃, 安徽国运律师事务所执业律师, 主要研究数据权益保护与网络治理的裁判规则。

一、问题的提出

数据跨境流动, 是数字经济的常态。企业开展跨国经营、使用境外云服务、与境外关联方共享信息, 都会涉及数据的出境。数据的流动带来效率, 也带来风险。

风险的核心, 是个人信息的保护与国家安全。数据出境后, 我国的法律难以直接适用, 接收方的保护水平可能低于我国, 数据可能被境外执法机构调取, 也可能被滥用或者泄露。

为应对风险, 我国建立了数据出境的三条路径: 安全评估、标准合同、个人信息保护

认证。三条路径适用于不同的情形，其中安全评估的门槛最高、审查最严。

安全评估的规范依据，主要是网络安全法、数据安全法、个人信息保护法，以及国家网信部门制定的评估办法。规范明确了申报的情形、评估的流程、未申报的后果。

但规范的运行，暴露出一系列问题。第一，义务主体如何识别？委托处理、共同处理、境外接收方，谁负有申报义务？集团内部的数据共享，是否构成出境？

第二，评估的标准如何适用？评估办法列举了评估的重点，但多为原则性表述，缺乏可量化的指标。评估机构如何判断，企业如何预期，都存在不确定性。

第三，未申报的后果如何落实？行政责任相对明确，但民事责任的构造模糊。个人信息被境外接收方泄露，个人可以向谁主张，依据什么请求权基础，赔偿如何计算？

三个问题相互关联。义务主体不清，评估无从谈起；标准不明，评估流于形式；责任不实，义务缺乏约束。三者构成制度运行的关键节点。

实务中的处理并不统一。有的企业将数据出境等同于服务器出境，认为只要服务器在境内即不构成出境；有的企业将集团内部共享视为内部事务，不履行申报义务；有的企业则过度申报，增加了合规成本。

监管的尺度也在变化。早期以整改为主，处罚较少；近期处罚增多，罚款金额提高，暂停业务、下架应用的案例出现。企业的不确定性增加，合规的紧迫性上升。

本文即以这三个问题为线索，讨论义务主体的识别、评估标准的构造、责任的分配。目的在于为制度的完善提供参考，也为企业的合规提供指引。

讨论的立场是，安全与流动应当平衡。过严的管制会阻碍数字经济的发展，过松的管制会使个人信息与国家安全的保护落空。平衡的支点，在于精准的义务设定与合理的责任分配。

评估与许可的区别，也值得辨析。行政许可须由法律设定，评估的依据是部门规章与规范性文件。从性质上看，评估更接近于事前的行政确认，而非典型的许可。

这一性质，影响到救济的途径。评估不通过的，企业可以申请复核，也可以提起行政复议或者行政诉讼。诉讼的审查范围，应当是评估的程序与依据，而非评估机构的专业判断。

评估的时限，规范未作强制规定。实践中，评估的周期较长，可能影响企业的业务开展。建议明确时限，规定受理、审查、决定的最长期限，提高可预期性。

二、三条路径与评估的定位

三条路径并非并列的选择，而是有层次的安排。安全评估是基础路径，适用于风险较高的情形；标准合同与认证是替代路径，适用于风险较低的情形。

安全评估的适用情形，包括三类：向境外提供重要数据；关键信息基础设施运营者向境外提供个人信息；向境外提供个人信息达到规定数量。三类情形，风险依次递减，但仍

属较高。

重要数据的界定，是适用的前提。重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。具体的目录，由各地区、各部门制定。

目录的制定，仍不完善。多数行业尚未发布目录，企业难以判断其数据是否属于重要数据。此时应当结合数据的性质、规模、敏感情形综合判断，不能以无目录为由免除义务。

关键信息基础设施的认定，由保护工作部门确定。被认定的运营者，其向境外提供个人信息，无论数量多少，均须申报评估。这一规定，体现了对关键领域的从严管理。

数量门槛，是实践中最常适用的标准。累计向境外提供一百万人以上个人信息，或者一万人以上敏感个人信息的，须申报评估。数量的计算，以自然人为单位，不以条数为单位。

数量的累计，应当有合理的期间。规范未明确期间，实践中一般按年度累计。企业应当建立台账，记录出境的规模，避免因累计超限而未申报。

标准合同的适用，限于未达到评估门槛的情形。企业须与境外接收方签订国家网信部门制定的标准合同，并向所在地省级网信部门备案。备案不是审批，但备案后发现问题的，可以责令改正。

个人信息保护认证的适用，同样限于未达到门槛的情形。企业须经专业机构认证，证明其数据处理活动符合保护标准。认证的自愿性，使其适用范围有限。

三条路径的关系，可以理解为风险分级的管理。风险高的，事前评估；风险中等的，合同加备案；风险较低的，认证。分级管理，既保障了安全，也便利了流动。

自由贸易试验区可以制定负面清单，清单外的数据出境，免于申报。这一安排，是制度创新的尝试，目的是在特定区域先行先试，积累经验。

评估的定位，是事前的行政许可性质的审查。未经评估或者评估未通过的，不得出境。违反的，构成违法出境，须承担相应的责任。

评估的有效期，一般为两年。有效期届满，需要继续出境的，应当重新申报。情形发生变化的，例如接收方变更、出境目的变更，也应当重新申报。

三条路径的适用条件与相互关系，可参见数据出境的合规底线：条例第35条给了八条路一文对路径选择所作的梳理，本文不再重复其适用条件的列举，只就评估环节的义务主体、判断标准与责任后果展开。

对于境外主体直接在境内收集数据的情形，是否适用评估？本文认为适用。境外主体在境内开展业务、收集个人信息，属于在境内的处理活动，其将数据传输至境外，构成出境。

对于跨境电商、跨境物流、跨境支付等业态，数据的出境是业务的内在环节。此类情

形，不能以业务需要为由免除申报，而应当审查其出境的必要性与保护措施的有效性。

对于学术研究、国际合作中的数据共享，是否适用评估？若涉及个人信息或者重要数据，同样适用。学术目的不是豁免的理由，但可以作为必要性的考量因素。

对于境外上市、跨境诉讼等情形提供的证据材料，涉及数据出境的，应当履行相应手续。此类提供往往具有被动性，可以作为从宽的考量，但不能免除义务。

对于数据的共享，还应当区分单向与双向。单向共享是提供，构成出境；双向交换是互惠，同样构成出境。双方均应履行各自的义务，不能以对方未申报为由免除自己的责任。

对于数据本地化存储的要求，与出境评估的关系应当厘清。本地化是前置的义务，评估是出境的前提。同时违反的，应当分别处理，不能以评估通过为由免除本地化的义务。

三、申报义务的主体与触发

申报义务的主体，是数据处理者。数据处理者是指自主决定处理目的、处理方式的组织或者个人。这一界定，强调了自主决定，而非单纯的技术操作。

委托处理的情形，义务主体如何确定？委托人自主决定处理目的与方式，受托人仅按指示处理。此时申报义务应当由委托人承担，受托人负有协助义务。

但受托人将数据再转移至境外的，是否构成独立的出境？本文认为构成。再转移是新的出境行为，受托人应当就此取得委托人的同意，并履行相应的申报义务。

共同处理的情形，义务主体如何确定？两个以上的处理者共同决定处理目的与方式的，为共同处理。共同处理者应当约定各自的义务，但对外承担连带责任。

连带责任的正当性，在于保护个人的救济。个人难以判断哪一个处理者实际控制了数据，若要求其分别主张，将增加救济的难度。连带责任，简化了救济的路径。

集团内部的数据共享，是否构成出境？若境外的关联方自主决定处理目的与方式，则构成独立的处理者，共享即为出境；若境外关联方仅按境内母公司的指示处理，则可能构成委托处理。

实务中，集团往往以内部管理为由，主张不构成出境。这一主张难以成立。数据的物理位置在境外，境外主体可以实际访问，风险已经发生，不能以股权关系否定出境的事实。

境外接收方的地位，也值得讨论。接收方不是申报义务的主体，但其负有保护义务。接收方违反保护义务，造成个人损害的，应当承担相应的责任。

接收方的责任基础，可以是合同，也可以是侵权。以合同为基础，个人不是合同当事人，难以直接主张；以侵权为基础，个人可以主张，但须证明过错与因果关系。

本文主张，接收方的责任应当以侵权为基础，并适用过错推定。接收方掌握数据的处理过程，个人难以证明其过错，由接收方证明自己无过错，更为公平。

申报义务的触发，以出境行为的发生为准。出境行为包括传输、存储、提供、公开等方式。仅在境外访问但未传输的，是否构成出境？本文认为，可以访问即构成风险，应当认定为出境。

对于过境数据，即仅在境内中转、目的地为境外第三国的数据，是否构成出境？本文认为不构成。过境数据未在境内落地使用，风险未在我国境内发生，不宜纳入管制。

对于数据的境外备份，是否构成出境？本文认为构成。备份数据可以被境外主体访问，风险与直接传输无异，应当履行申报义务。

评估的核心，是风险与措施的比例。风险越高，措施应当越严；措施的成本，应当与风险的规模相适应。比例失衡的，评估难以通过。

对于去标识化、匿名化的数据，评估的标准可以放宽。匿名化后的数据不属于个人信息，不受出境限制；去标识化后的数据仍属个人信息，须履行义务，但保护措施可以适当简化。

匿名化的认定，应当严格。仅删除姓名、身份证号，仍可通过其他信息重新识别的，不构成匿名化。企业主张匿名化的，应当承担举证责任。

对于数据汇聚的风险，应当特别关注。单条数据无害，大量汇聚后可能形成画像、揭示敏感信息。评估时应当审查汇聚后的风险，而非仅看单条数据。

评估应当动态进行。出境的目的、规模、接收方的环境发生变化，风险也随之变化。企业应当建立监测机制，定期复评，不能一次评估、长期适用。

评估报告的保存，也是义务的一部分。企业应当保存自评估报告、官方评估决定、整改记录，保存期限不少于三年。未保存的，发生争议时难以证明合规。

四、评估的内容与标准

评估的内容，规范列举了五项：出境的目的、范围、方式是否合法、正当、必要；境外接收方的保护能力；数据的规模、类型、敏感程度；风险的大小；保护措施是否有效。

五项内容，可以归纳为三个维度：目的正当性、风险可控性、保护有效性。三个维度，构成了评估的基本框架，也是企业自查的指引。

目的正当性，要求出境具有合法的业务需要，且不能通过其他方式实现。例如，跨国企业的人力资源管理需要将员工信息传至总部，属于正当目的；为规避境内监管而转移数据，则不正当。

必要性的判断，要求出境的范围与目的相匹配。仅需传输姓名的，不得传输身份证号；仅需传输汇总数据的，不得传输明细数据。最小必要，是判断的核心。

风险可控性，要求接收方的保护水平达到我国法律的要求。判断的要素包括：接收方所在国的法律环境、接收方的技术措施、接收方的管理制度的健全程度。

所在国的法律环境，是重要的考量。若该国法律允许政府广泛调取企业数据，且缺乏

救济途径，则保护水平不足。此时应当采取补充措施，例如加密、去标识化。

技术措施的有效性，应当实质判断。仅签订保密协议，不足以证明保护有效；应当审查加密的强度、访问控制的设计、日志审计的完整。形式合规而实质不足的，评估不通过。

保护有效性，还要求建立事后的监督机制。企业应当定期检查接收方的保护情况，发现问题的，应当要求整改；整改不力的，应当停止传输。

评估的标准，应当量化。规范的原则性表述，需要通过指南、问答、案例逐步具体化。国家网信部门发布的多份问答，已经在做这样的工作，但仍不够。

量化的尝试，可以参考国际经验。例如，欧盟的充分性认定，列出了判断的要素与权重；亚太经合组织的跨境隐私规则，规定了认证的指标。我国可以借鉴，但须结合本国实际。

评估的方法，应当区分自评估与官方评估。自评估由企业自行开展，形成报告；官方评估由网信部门或者其委托的机构开展，作出决定。二者衔接，自评估是基础，官方评估是确认。

自评估的质量，直接影响到官方评估的效率。企业应当建立数据映射，梳理数据的流向、类型、数量；应当开展风险评估，识别威胁与脆弱性；应当制定保护措施，落实整改。

官方评估的重点，是审查自评估的真实性与充分性。发现自评估虚假、遗漏重要事项的，应当不予通过，并可以追究企业的责任。

评估的结论，可以是通过、不通过、附条件通过。附条件通过的，企业应当在期限内完成整改，整改后再次提交。未完成整改的，视为不通过。

对于未申报的认定，应当区分未申报与申报未通过。前者是程序上的不作为，后者是实体上的不合格。二者的责任程度不同，处理也应当有所区别。

对于主动补报的情形，可以从轻或者减轻处罚。主动补报表明企业有改正的意愿，处罚的目的已经部分实现。但对于造成严重后果的，从宽的幅度应当有限。

对于因标准不明而未申报的情形，应当给予合理的过渡期。规则不清晰导致的不合规，不宜一概重罚，应当以指导、整改为主，逐步提高要求。

对于持续性的违法出境，处罚的时效如何计算？本文认为，应当自违法行为终了之日起计算。持续出境期间，时效不开始计算，避免企业以持续违法规避处罚。

对于责令改正的决定，企业应当按期履行。逾期不履行的，可以按日连续处罚，直至改正为止。按日计罚的引入，解决了长期违法成本过低的问题。

五、未申报的法律后果

未申报的后果，首先是行政责任。网络安全法、数据安全法、个人信息保护法均规定

了处罚，包括责令改正、警告、罚款、暂停相关业务、停业整顿、吊销许可证。

罚款的幅度，视情节而定。一般情形，罚款金额较低；情节严重的，罚款金额可以提高至五千万元或者上一年度营业额的百分之五。这一幅度，具有相当的威慑力。

情节严重的情形，包括：造成大量个人信息泄露；被境外机构获取重要数据；拒不改正；曾因同类行为受过处罚。认定的标准，应当结合后果与主观恶性。

对于直接负责的主管人员与其他直接责任人员，也可以处罚款。这一规定，将责任落实到个人，避免了企业以罚代管、个人免责的局面。

行政责任之外，还有信用惩戒。违法出境的企业，可以被列入失信名单，影响其融资、投标、评优。信用惩戒的威力，往往超过罚款。

民事责任的构造，是本文的重点。个人因数据出境受到损害，可以向处理者主张，也可以向接收方主张。请求权的基础，可以是个人信息保护法，也可以是民法典。

个人信息保护法规定，处理个人信息侵害个人信息权益造成损害，处理者不能证明自己没有过错的，应当承担赔偿责任。这一规定，确立了过错推定责任。

过错推定的适用，减轻了个人的举证负担。个人只需证明损害的发生与处理行为的存在，处理者须证明自己无过错。这一分配，符合双方的举证能力。

但因果关系仍需个人证明。数据出境与损害之间的因果关系，往往难以证明。例如，个人信息被诈骗分子利用，诈骗分子如何获得信息，个人难以查证。

本文主张，在因果关系上可以适用推定的方法。若处理者违法出境，且损害的类型与泄露的信息具有对应关系，可以推定因果关系成立，由处理者反证。

推定的正当性，在于风险的控制。处理者违法出境，制造了法所不容许的风险；损害的发生，正是该风险的实现。由制造风险者承担举证不能的后果，符合公平。

赔偿的范围，包括财产损失与精神损害。财产损失，按实际损失计算；难以确定的，可以按处理者获得的利益计算。精神损害，视情节酌定。

对于大规模泄露，个人诉讼的成本高、收益低，可以适用公益诉讼。人民检察院、消费者组织、网信部门确定的组织，可以提起公益诉讼。

公益诉讼的功能，不仅是赔偿，更是制止与预防。诉讼请求可以包括停止侵害、消除危险、赔礼道歉、修复信用，这些请求对个人的救济更为实际。

对于损害的认定，还应当注意机会损失。因信息泄露导致个人失去商业机会、就业机会的，属于可得利益损失，可以主张，但须证明机会的现实性与损失的确定性。

对于因果关系的证明，可以借助专家的意见。数据泄露的路径、损害的发生机制，往往需要技术判断。法院可以委托鉴定，也可以采纳专家辅助人的意见。

对于多数人侵权，可以适用份额的推定。多个处理者共同造成损害的，难以确定各自份额的，平均承担。这一规则，简化了认定，也促使各方相互监督。

对于责任的保险，应当完善。网络安全的保险产品尚不成熟，承保范围、保费定价、

理赔标准都缺乏规范。建议监管部门引导开发，为企业的风险转移提供工具。

对于举证妨碍，可以适用不利推定。处理者无正当理由拒不提供数据流向记录的，可以推定其存在过错，或者推定出境规模达到门槛。这一规则，缓解了个人与监管机关的举证困难。

对于赔偿数额的确定，可以适用酌定。损失的范围难以精确计算，法院可以根据信息的类型、数量、泄露的情节、企业的过错程度酌定，避免因举证不能而使个人得不到救济。

六、民事责任的构造

民事责任的构造，须解决三个问题：责任的主体、归责的原则、责任的范围。三个问题相互关联，共同决定了救济的效果。

责任的主体，包括处理者与接收方。处理者是出境的决定者，接收方是数据的实际控制者。二者可能承担连带责任，也可能承担按份责任。

本文主张，处理者与接收方原则上承担连带责任，但接收方能够证明其已按约定采取保护措施、损害完全由处理者的指示造成的，可以减轻或者免除责任。

连带责任的正当性，在于保护个人。个人难以判断损害由哪一方造成，若要求其分别主张，将增加救济的难度。连带责任，使个人可以向任何一方主张全部赔偿。

但连带责任可能过重。接收方仅按指示处理，对出境的决定没有影响力，令其承担全部责任，有失公平。故应当允许其通过证明免责或者减责。

归责的原则，应当区分情形。处理者违法出境，适用过错推定；接收方违反保护义务，同样适用过错推定；双方均无过错但损害发生的，可以适用公平责任。

公平责任的适用，应当严格。仅在双方均无过错、损害严重、不补偿显失公平的情形下适用，且补偿的数额应当合理，不能变成无过错的赔偿责任。

责任的范围，应当包括直接损失与间接损失。直接损失，例如因信息泄露导致的账户被盗、财产被划转；间接损失，例如因信用受损导致的贷款被拒、就业受阻。

间接损失的认定，应当谨慎。须证明损失与泄露之间具有相当因果关系，且损失是确定的、可计算的。纯粹的担忧、不安，不构成可赔偿的损失。

对于精神损害，应当区别对待。敏感个人信息泄露，例如生物识别、医疗健康、金融账户，容易引发歧视、骚扰，可以支持精神损害赔偿；一般信息泄露，原则上不支持。

对于惩罚性赔偿，现行法未明确规定。本文认为，对于恶意出境、造成严重后果的情形，可以探索适用惩罚性赔偿，以发挥惩戒与威慑的功能。

惩罚性赔偿的适用，应当限于故意或者重大过失，且须有法律的明确规定。在解释论上，可以参照消费者权益保护法的规定，但不宜类推过度。

责任的分担，还应当考虑保险的作用。企业可以投保网络安全责任险，将赔偿的风险

转移。保险的存在，不减轻企业的责任，但可以保障个人的受偿。

对于单位犯罪，应当追究直接负责的主管人员与其他直接责任人员的责任。企业的合规体系健全、已尽合理努力的，可以作为从宽的情节。

对于跨境数据的刑事管辖，存在争议。行为地在境内、结果地在境外的，可以适用我国刑法；行为地与结果地均在境外的，管辖的依据不足，需要通过国际合作解决。

对于行政处罚与民事赔偿的关系，应当区分。行政处罚上缴国库，民事赔偿归个人，二者不冲突。企业不能以已受处罚为由拒绝赔偿。

七、行政与刑事的衔接

数据出境的违法行为，可能同时构成犯罪。刑法规定了侵犯公民个人信息罪、拒不履行信息网络安全管理义务罪、非法获取计算机信息系统数据罪等，可以适用。

侵犯公民个人信息罪，适用于非法出售或者提供公民个人信息的情形。违法出境是否构成本罪，取决于是否违反国家规定、情节是否严重。

情节严重，一般以信息的条数、违法所得、造成的后果为标准。违法出境的数量达到一定标准，可以认定为情节严重；造成被害人死亡、重伤、重大财产损失的，属于情节特别严重。

拒不履行信息网络安全管理义务罪，适用于网络服务提供者不履行法律规定的义务，经监管部门责令改正而拒不改正的情形。违法出境，可能构成本罪。

本罪的适用，须具备三个条件：主体是网络服务提供者；不履行安全管理义务；经责令改正而拒不改正。三个条件缺一不可，不能仅以未申报为由入罪。

行政与刑事的衔接，应当遵循一事不再罚的原则。行政处罚与刑罚的性质不同，可以并处，但罚款与罚金应当折抵，拘留与徒刑应当折抵。

对于涉嫌犯罪的案件，行政机关应当移送司法机关。不移送、以罚代刑的，可能构成渎职。移送的标准，应当明确，避免选择性执法。

对于刑事追诉的标准，应当统一。同样的违法出境行为，有的地方立案，有的地方不立案，损害了法律的统一性。最高司法机关可以通过案例、解释予以明确。

对于跨境取证的难题，应当通过司法协助解决。数据在境外，证据难以获取，可以请求境外司法机关协助，也可以通过网络服务提供者调取。

对于境外接收方的追责，存在管辖的障碍。境外主体不在我国境内，难以对其行政处罚或者刑事追诉。可以通过冻结资产、限制交易等措施，间接施加压力。

国际合作的路径，包括双边条约、多边公约、执法互助。我国已加入多个相关公约，可以据此请求协助。合作的深度，取决于国际关系的大环境。

对于行政案件，审查的重点是程序的合法性与裁量的合理性。处罚的幅度是否与情节相当，是否考虑了从轻、减轻的情节，都是审查的内容。

对于民事案件，审查的重点是责任的构成与赔偿的范围。过错的推定、因果关系的判断、损失的计算，都需要精细的说理，避免简单化处理。

对于刑民交叉的案件，应当遵循先刑后民或者刑民并行的规则。刑事程序未终结的，民事案件可以中止；不依赖刑事认定的，可以继续审理。

对于案例的指导，应当加强。数据出境的案件类型新、争议大，通过发布典型案例，可以统一裁判尺度，也可以为企业提供行为的指引。

对于合规不起诉的探索，可以在数据领域试点。企业建立有效的合规体系、主动整改的，可以不起诉或者从宽处理，实现特殊预防与一般预防的结合。

对于涉外因素，应当注意法律适用。境外接收方的责任，可能适用其所在国的法律。我国法院审理的，应当依涉外民事关系法律适用法确定准据法，不能一概适用我国法律。

对于判决的承认与执行，跨境执行存在障碍。可以借助互惠原则、国际公约，请求境外法院承认执行。现实中的成功率不高，需要长期的双边合作积累互信。

八、裁判方法与规则完善

基于上述分析，本文提出裁判的三步法。第一步，认定出境行为是否存在，确定义务的主体与触发条件；第二步，审查评估的履行情况，判断是否违法出境。

第三步，处理责任的分配，包括行政责任、民事责任与刑事责任的衔接。三步依次进行，任何一步的缺失都会导致结论的不完整。

第一步的重点，是出境行为的实质认定。不能仅以数据的物理位置判断，而应当看境外主体是否可以实际访问、是否实际使用了数据。可以访问，即构成风险。

第二步的重点，是评估的实质性。企业提交了评估报告，但报告虚假、遗漏重要事项的，仍属未履行义务。形式合规不能替代实质合规。

第三步的重点，是责任的均衡。行政责任重在纠正，民事责任重在填补，刑事责任重在惩戒。三者的功能不同，不能相互替代。

在举证责任上，本文主张：监管机关须证明出境行为的存在与规模；企业须证明其已履行申报义务，或者属于免于申报的情形；个人主张赔偿的，须证明损害的存在。

对于规模的证明，监管机关可以要求企业提供台账、日志、合同。企业不能提供的，可以推定其出境规模达到门槛，由其反证。这一分配，促使企业建立合规记录。

在规则完善上，本文提出四点建议。其一，加快重要数据目录的制定，明确各类数据的分类分级，减少企业的不确定性。

其二，细化评估的标准，制定量化的指标与操作指南，使企业能够自查，使评估机构能够统一尺度。

其三，明确民事责任的构造，规定连带责任的适用与免责事由，规定因果关系的推定规则，为个人救济提供明确的依据。

其四，建立跨境监管的合作机制，通过双边协议、多边框架，解决境外取证与境外追责的难题。

除规则之外，还应当重视企业的合规建设。企业应当设立数据保护负责人，建立数据映射与风险评估机制，定期开展培训与审计。合规的成本，远低于违法的代价。

对于中小微企业，应当给予适当的支持。合规的成本对小企业而言负担较重，可以通过提供模板、简化流程、减免费用等方式，降低合规的门槛。

数据治理的难点，在于平衡。安全与流动、保护与利用、监管与自治，三对关系贯穿始终。任何一端的过度，都会损害制度的整体效果。

规则的完善，需要时间。技术的迭代快于立法的更新，这是数字时代的常态。在规则尚未完备时，司法的审慎与行政机关的指导，显得尤为重要。

企业应当认识到，合规不是一次性的投入，而是持续的过程。建立机制、培养人才、完善流程，才能在监管的变化中保持主动。

从更宏观的视角看，数据出境制度是我国参与全球数字治理的制度表达。规则的合理性与可预期性，直接影响我国在全球数据流动格局中的地位。

数据是新的生产要素，其价值的释放有赖于流动，其风险的防控有赖于规则。二者并非零和，好的规则能够让流动更安全，让安全更便利。这是制度设计的智慧所在。

九、结语

数据出境的管理，是数字时代的新课题。它涉及个人权益、企业发展与国家安全三重价值，任何一重都不能偏废。制度的设计，须在三者之间寻求平衡。

本文的分析表明，平衡的支点在于精准。精准的义务设定，避免一刀切；精准的评估标准，避免形式化；精准的责任分配，避免虚置或者过度。

精准的前提，是清晰。义务主体清晰，企业才知道做什么；标准清晰，企业才知道怎么做；责任清晰，企业才知道不做的后果。清晰，是制度有效运行的基础。

当然，清晰不等于僵化。技术在发展，业态在变化，规则也应当随之调整。动态的调整，需要在稳定与灵活之间取得平衡。

对于司法而言，其角色是适用规则、解释规则、发展规则。通过个案裁判，将抽象的原则转化为具体的标准，为制度的完善积累经验。

对于企业而言，合规不是负担，而是竞争力。在数据监管趋严的背景下，合规的企业更容易获得信任，更容易开展跨境业务。

对于个人而言，权利的实现需要制度的支撑。完善的救济渠道、合理的举证规则、有效的公益诉讼，是个人信息保护的最后防线。

数据流动不可逆转，规则建设仍在路上。愿本文的讨论，能为这条路上的行者提供一点参考。

参考文献

- [1] 张新宝：《个人信息保护法释义》，中国人民大学出版社2021年版。
- [2] 周汉华：《数据安全法释义》，法律出版社2021年版。
- [3] 程啸：《个人信息保护法理解与适用》，中国法制出版社2021年版。
- [4] 洪延青：《数据出境安全评估的制度逻辑》，载《中国法律评论》2022年第3期。
- [5] 丁晓东：《数据跨境流动的规制路径》，载《法学研究》2022年第5期。
- [6] 许可：《数据出境的三种路径及其适用》，载《政法论坛》2023年第1期。
- [7] 王锡锌：《数据治理的国家逻辑》，载《中外法学》2021年第6期。
- [8] 刘金瑞：《重要数据的界定与保护》，载《环球法律评论》2022年第4期。
- [9] 国家互联网信息办公室：《数据出境安全评估办法释义》，2022年版。
- [10] 何渊：《数据法学》，北京大学出版社2023年版。