LeeZhao
www.leezhao.com

里兆律师事务所 Leezhao Law Office
中国上海市陆家嘴环路 1000 号恒生银行大厦 29 层
29F, Hang Seng Bank Tower, 1000 Lujiazui Ring Road, Shanghai, China
Tel (86-21) 68411098 Fax (86-21) 68411099 Postal Code 200120

数据跨境传输新规实施 将对企业在华经营产生影响

■ 背景

2016 年底公布的《中华人民共和国网络安全法》（简称 “《网络安全法》”）已于 2017 年 06 月 01 日起正式施行。该法第三十七条针对数据跨境传输作出了如下规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”

基于《网络安全法》的上述规定，国家互联网信息办公室（简称 “网信办”）于 2017 年 04 月 11 日公布了《个人信息和重要数据出境安全评估办法（征求意见稿）》（简称 “《办法草案》”），并向社会公开征求意见。《办法草案》就应当进行安全评估的个人信息与重要数据的范围、评估的具体要求和程序、主管部门等做了细化规定。作为对《网络安全法》有关数据跨境传输规定的细化，《办法草案》一旦正式公布实施，数据跨境传输的管理即具有了具体可执行的依据，这必将对外商投资企业与境外关联企业之间的信息共享产生实际而重要的影响，需予以密切关注。

■ 哪些企业将受到影响

根据《网络安全法》第三十七条，受到数据跨境传输限制的主体为 “关键信息基础设施的运营者”。根据该法第三十一条，“关键信息基础设施的运营者” 主要是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施的运营者。**对企业而言，若其为上述关键信息基础设施领域内相关网络的所有者、管理者和网络服务提供者，则确定会受到数据跨境传输的限制。**

需要注意的是，根据《办法草案》第二条的规定，“网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法

国境を越えて行われるデータ伝送に関する新規定が 企業において中国での経営に与える影響

■ 背景

2016 年末に公表された「中華人民共和国サイバーセキュリティ法」（以下「『サイバーセキュリティ法』」という）が 2017 年 6 月 1 日から正式に施行された。同法の第三十七条は、国境を越えて行われるデータ伝送について、以下の通り規定している。「重要情報インフラの運営者が中華人民共和国国内での運営過程で収集し、発生する個人情報及び重要データは、国内で保存しなければならない。業務上の必要から、国外への提供がどうしても必要である場合、国家インターネット情報部門が国務院の関係部門と共同で制定した弁法に従って、セキュリティ評価を行わなければならない。法律、行政法規に特段の規定がある場合、その規定に従う。」

「サイバーセキュリティ法」の上述規定に基づき、国家インターネット情報弁公室（以下「インターネット情報弁公室」という）は 2017 年 4 月 11 日に「個人情報及び重要データの国外持ち出しに係るセキュリティ評価弁法（意見募集案）」（以下「『弁法草案』」という）を公表し、社会に向けてパブリックコメントを募集した。「弁法草案」では、セキュリティ評価を行うべき個人情報及び重要データの対象範囲、評価の具体的要求・手続き、主管部門などについて、詳細化した規定を行っている。「サイバーセキュリティ法」での国境を越えるデータ伝送に関する規定を詳細化したものとして、「弁法草案」が正式に公表、実施された後は、データの国境を越える伝送行為への管理が具体的且つ実施可能な根拠をもつことになり、そうなると、外商投資企業と国外の関連企業との情報共有に対し現実的で重大な影響をもたらすのは必至であり、細心の注意を払う必要がある。

■ どのような企業が影響を受けるのか

「サイバーセキュリティ法」第三十七条によると、国境を越えるデータ伝送において制限を受ける主体は「重要情報インフラの運営者」である。同法の第三十一条によると、「重要情報インフラの運営者」とは、主に公共通信・情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政府などの重要な業界及び分野、並びに機能の破壊、喪失又はデータの漏えいに遭遇した場合、国の安全、国の経済と人々の暮らし、公共の利益に重大な危害を与えうるその他重要情報インフラの運営者を指すとしている。**企業が上記重要情報インフラ分野に係るインターネット所有者、管理者及びインターネットサービス提供者である場合、国境を越えるデータ伝送が制限を受けることは明らかである。**

なお、「弁法草案」第二条では、「インターネット運営者が中華人民共和国国内での運営過程で収集し発生する個人情報及び重要データは、国内で保存しなければならない。業務上の必要から、国外への提供がどうして

进行安全评估。”据此理解，《办法草案》将适用的主体扩大到了所有的网络经营者，而不仅仅限于关键信息基础设施的运营者。**如果《办法草案》不作修改而全文予以通过并公布实施，则受到数据跨境传输限制的，将可能涉及到所有在华企业。**

■ **哪些经营活动将受到影响**

根据《网络安全法》第三十七条以及《办法草案》第二条等规定，企业在中国境内运营中收集和产生的个人信息和重要数据的存储与出境活动会受到限制。对此，律师解读如下：

1. *何谓“在中国境内运营中收集和产生的个人信息与重要数据”？*

- **个人信息。**根据《网络安全法》与《办法草案》对个人信息的解释，个人信息是指以电子或者其他方式记录的、能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。除此之外，结合《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第一条对于个人信息范围的规定，个人信息还应当包括账号密码、财产状况、行踪轨迹等信息。

- **重要数据。**《网络安全法》对此未作规定，《办法草案》虽进行了解释，但内容相对模糊。根据《办法草案》中的相关解释，重要数据是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。目前，该规定可操作性不强，有待中国有关部门出台相关的标准或者识别指南进一步细化。

- **中国境内运营中收集和产生。**《网络安全法》和《办法草案》对此都未予以明确。按照通常理解，只要是因在中国境内的经营活动而产生的个人信息和重要数据，都应作为限制出境的对象，既包括企业在中国境内运营获取的上述数据，也包括企业从事跨境经营获取的上述数据。

2. *何谓“数据出境”？*

- **数据出境是指企业向位于境外的机构、组**

も必要である場合、本弁法に従いセキュリティ評価を行わなければならない」と規定している。この文言によると、適用される主体は、重要情報インフラの運営者だけでなく、すべてのインターネット事業者に拡大された。**「弁法草案」が修正されないままで可決され、公表、実施された場合、国境を越えるデータ伝送において制限が課される主体は、中国に進出している全ての企業となる可能性がある。**

■ **どのような経営活動が影響を受けるのか**

「サイバーセキュリティ法」第三十七条及び「弁法草案」第二条などの規定によると、企業が中国国内での運営過程で収集し発生する個人情報及び重要データの保存、国外への持ち出しが制限される。これについて、筆者は以下の通り解釈する。

1. *「中国国内での運営過程で収集し発生する個人情報及び重要データ」とは何か？*

- **個人情報**。「サイバーセキュリティ法」及び「弁法草案」における個人情報の解釈によると、個人情報とは、デジタル又はその他方式により記録され、自然人の個人の身元を単独で又はその他の情報を踏まえた上で識別できる各種の情報を指し、自然人の氏名、生年月日、本人証明書番号、個人生体認証情報、住所、電話番号などを含むがこれらに限らない。また、「公民個人情報侵害刑事案件を取り扱う際の法律適用に係る若干の問題に関する最高人民裁判所、最高人民検察院による解釈」第一条にいう個人情報の範囲についての規定によれば、個人情報には、ID・パスワード、財産状況、足取りなどの情報が含まれる。

- **重要データ**。「サイバーセキュリティ法」では規定しておらず、「弁法草案」では解釈はあるが、その内容はかなり曖昧である。「弁法草案」の係る解釈によると、重要データとは、国の安全、経済の発展、及び社会公共の利益と密接に関係するデータをいい、具体的な範囲は国の係る基準及び重要データ判別ガイドラインを参照すること、とされている。現在、当該規定は操作性に欠けており、中国の関係部門による基準の公表又は判別ガイドラインの更なる詳細化が必要とされる。

- **中国国内での運営過程での収集及び発生**。「サイバーセキュリティ法」及び「弁法草案」のいずれも、これを明確にしていない。通常の理解によるならば、中国国内での経営活動により発生した個人情報及び重要データであれば、いずれも国外持ち出しの制限対象とするはずであり、また企業が中国国内での運営過程で獲得した上述のデータが含まれるだけでなく、企業が国境を越えるオペレーション行為により入手した上述データも含まれる。

2. *「データの国外持ち出し」とは？*

- **データの国外持ち出しとは、国外にある機構、組**

织、个人提供数据的行为。《网络安全法》以及《办法草案》仅限制的是通过网络向境外提供数据的行为，通过其他物理载体（如服务器、硬盘、U 盘和纸质材料等）等方式进行的数据跨境转移行为应不在上述法规的限制范围内。[1]

- **不符合如下要求的信息，明确不得出境。**一类为未经个人信息主体同意或可能侵害个人利益的个人信息（需要注意的是，个人通过拨打国际电话、发送国际电子邮件、互联网跨境购物以及其他个人主动行为提供信息的，视为个人信息主体已经同意）；另一类是出境会给中国政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益的数据。

織、個人に対し、企業がデータを提供する行為を言う。「サイバーセキュリティ法」及び「弁法草案」によると、ネットワークを通じて国外にデータを提供する行為だけが制限をかけられ、その他の物理的記憶媒体など（例えば、サーバ、ハードディスクドライブ、USB メモリや紙面の資料など）の方式により国境を越えてデータ伝送を行う行為は、上述法規に制限される範囲に含まれない。[1]

- **次の要件に該当する情報は、国外に持ち出してはならないことは明白である。**一つは、個人情報の持ち主の同意を得ていない、又は個人の利益を侵害するおそれのある個人情報（なお、個人が国際電話での通話、国際電子メールの送信、国境を越えたネットショッピング及びその他個人での自発的な行為を通じて情報提供する場合は、個人情報の持ち主がすでに同意したものとみなす）であり、もう一つは、国外に持ち出すことで、中国の政治、経済、科学技術、国防などの安全にリスクをもたらし、国の安全に影響を及ぼし、社会公共の利益を損害するおそれのあるデータである。

■ 如何进行数据的存储与出境？

1. 境内存储。

根据规定，企业在中国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。按照通常理解，此规定要求经营者将前述个人信息与重要数据存储在位于中国境内的服务器上。对于采取云存储的企业，应当选择服务器位于中国境内的云服务供应商。

2. 安全评估。

根据规定，企业因业务需要，确需向位于境外的机构、组织、个人提供个人信息和重要数据的，应当进行安全评估。参考《办法草案》，不同类型的数据由不同的主体进行安全评估，适用不同的程序。在此简要介绍如下：

- 针对一般的数据出境，企业只需要自行组织安全评估，并对评估结果负责。
- 对于符合《办法草案》第九条规定的各类数据，例如，含有或累计含有 50 万人以上的个人信息、超过 1000GB 数据量的数据、

■ データの保存及び国外への持ち出しはどのように行うべきか？

1. 国内で保存。

規定によれば、企業が中国国内での運営過程で収集し、発生した個人情報及び重要データは、国内で保存しなければならない。通常の理解によれば、同規定は、事業者に対し前述の個人情報及び重要データを中国国内にあるサーバに保存するよう求めている。クラウドストレージを採用する企業は、中国国内にサーバを構えるクラウドサービス提供者を選定しなければならない。

2. セキュリティ評価。

規定によると、企業が業務上の必要から、国外にある機構、組織、個人に個人情報及び重要データを提供する必要がどうしてもある場合、セキュリティ評価を行わなければならないとされている。「弁法草案」を参照する場合、データのタイプ別に異なる主体がセキュリティ評価を行い、異なる手続きが適用される。本稿では、以下の通り簡潔に紹介する。

- 一般的なデータの国外持ち出しであれば、企業は自らセキュリティ評価を手配し、評価結果について責任を負うだけでよい。
- 「弁法草案」第九条の規定に合致する各種のデータ（例えば、50 万人以上又は累計して 50 万人以上の個人情報を含むもの、データ量が

[1] 但通过前述其他物理载体的方式向境外转移个人信息等数据时，根据《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第三条之规定，“未经被收集者同意，将合法收集的公民个人信息向他人提供的”的行为可能涉嫌构成《刑法》第二百五十三条之一所规定的侵犯个人信息罪，也应当予以留意。

[1] ただし、前述したその他の物理的記憶媒体を通じて、個人情報などのデータを国外に伝送する場合、「公民個人情報侵害刑事案件を取り扱う際の法律適用に係る若干の問題に関する最高人民裁判所、最高人民検察院による解釈」第三条の規定によると、「情報を収集される者の同意を得ずして、適法に収集した公民の個人情報を他人に提供する」行為は、「刑法」第二百五十三条の一に規定される個人情報侵害罪を構成する可能性があり、この点についても注意が必要である。

包含关键信息基础设施的系统漏洞、安全防护等网络安全信息等，则需要企业报请行业主管或监管部门组织安全评估。

- 当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，企业应及时重新进行安全评估。

- 涉及到数据出境的企业应根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估，同时要及时将评估情况报行业主管或监管部门。

1,000GB を超えるもの、重要情報インフラの脆弱性、セキュリティ保護などのネットワーク・セキュリティ情報が含まれるものなど）は、企業が業界主管部門又は監督管理部門に報告し、セキュリティ評価の手配を申請する必要がある。

- データの受け手が変更され、データを国外に持ち出す目的、範囲、数量、型などにやや大きな変化が生じ、データの受け手又は国外に持ち出すデータに重大なセキュリティ事件が発生した場合、企業はセキュリティ評価を速やかに改めて実施しなければならない。

- データの国外持ち出しの必要性がある企業は、業務の発展及びネットワークの運営状況を踏まえ、データの国外持ち出しについて、毎年、少なくとも 1 回はセキュリティ評価を行わなければならず、またそれと同時に、評価状況を速やかに業界主管部門又は監督管理部門に報告する必要がある。

■ 建议采取的措施

1. 将经营过程中收集到的数据进行本地化存储处理

上述规定的实施会对企业开展经营活动带来影响，尤其对于外商投资企业而言，因其经常需要其将在中国境内收集到的数据传输给位于境外的关联企业，今后该类企业应注意将经营中收集的个人信息和重要数据储存在位于中国境内的服务器上，同时要尽量与位于其境外服务器进行一定的隔离，避免产生不必要的麻烦。

2. 向境外提供个人信息时应当取得个人信息主体的同意并进行处理

新规定实施后，企业向境外提供个人信息时，须取得个人信息主体或其监护人的同意，若企业违反上述规定，则可能会因违反《网络安全法》而承担相应的行政责任。同时建议企业在经个人信息主体同意后向境外传输个人信息时提高防范意识，尽可能对个人信息进行脱敏处理，保障个人信息安全。

3. 加强对于员工的内部监管

企业因违法向境外传输数据将会面临主管部门警告、罚款、停业整顿、吊销营业执照等处罚，为避免因员工私自违法向境外提供数据给企业带来不利影响，有关企业应当对数据进行分类管理，确立不同的管理权限，针对员工在履行职责或者提供服务过程中如何依法获取、使用、存储、向境外传输个人信息或者其他重要数据制定具体可行的操作指引与内控制度，并加强员工的相关培训和教育，防患于未然。

■ 推奨される措置

1. 経営過程にて収集したデータを現地で保存する

上述規定の実施により、企業による経営活動の展開に影響が生じることが予想され、とりわけ外商投資企業にとってみれば、中国国内で収集したデータを日常的に国外の関連企業に伝送する必要があり、今後、このような企業は経営過程で収集した個人情報及び重要データを中国国内にあるサーバで保管するようにし、なるべく国外のサーバから隔てて取り扱い、余計な面倒が生じてしまうことがないように気をつけなければならない。

2. 国外に個人情報を提供する場合、個人情報の持ち主の同意を得た上で行われなければならない

新規定が実施された後、企業が海外に個人情報を提供する際には、必ず個人情報の持ち主又はその後見人の同意を得なければならず、企業が上述規定に違反した場合、「サイバーセキュリティ法」違反により、係る行政責任を負うことになるおそれがある。また、企業が国外へ個人情報を伝送する際には、リスクマネジメントの意識を高め、個人情報に対しては、マスキング処理を極力行い、個人情報の安全が保障されるようにしておくことが望ましい。

3. 従業員に対する内部監督管理を強化する

企業は、データを違法に国外へ伝送することにより、主管機関から警告、過料、営業停止・整頓、営業許可証の取り上げなどの処罰を受けるおそれがあり、従業員がデータを無断で違法に国外へ伝送するなどして、企業に悪影響がもたらされないよう、企業は、データの分類管理を実施し、それぞれ管理権限を設定し、従業員の職務履行、又はサービスの提供にあたり、法に依拠して個人情報又はその他重要データの獲得、利用、保存、国外への伝送方法について、具体的で実行可能な運用ガイドライン及び内部統制制度を制定し、従業員への研修や教育を強化し、不祥事を未然に防ぐようにしなければ

■ 结语

《网络安全法》确立了数据存储和跨境传输的基本原则，其具体实施需要《办法草案》等细化规定的配合。目前对外公开征求意见的《办法草案》，其相关规定较《网络安全法》更为严格。甚至在一定程度上突破了《网络安全法》设定的基本原则，存在“违反上位法”之嫌。举例如下：

- 《网络安全法》第三十七条仅针对“关键信息基础设施的运营者”作出跨境数据传输限制，并未针对所有网络运营者。此外，从立法体系看，《网络安全法》第三十七条被放在了第三章网络运行安全下关键信息基础设施的运行安全一节中，也表明规制的主体限于关键信息基础设施的运营者。但是，《办法草案》将其扩大为所有网络运营者，扩大了上位法对于适用主体范围的限制。

- 《办法草案》第九条列举了需要进行安全评估的跨境数据，但该条规定所列举的数据类型可能已经超出了《网络安全法》所限定的范围。例如“含有或累计含有 50 万人以上的个人信息”或“超过 1000GB 数据量的数据”就不一定能与《网络安全法》所提及的“重要数据”等同。

综上，在有关数据跨境传输的配套规定尚未出台之前，《网络安全法》第三十七条对企业在华经营的影响程度如何，存在一定的不确定性。但是，律师推测，正式出台的配套规定，应当不会比《办法草案》更加严厉。因此，目前情况下，相关企业参照《办法草案》进行提前规划，应当是合适的。

（里兆律师事务所 2017 年 07 月 07 日编写）

■ まとめ

「サイバーセキュリティ法」は、データ保存及び国境を越えるデータ伝送の基本的原則を確立するものであるが、具体的に実施するためには、「弁法草案」などの詳細化した規定が必要である。先頃パブリックコメントを募集していた「弁法草案」は、その規定が「サイバーセキュリティ法」よりも厳しく、ひいては、「サイバーセキュリティ法」で確立された基本的原則の枠をやや超えており、「上位の法に反する」疑いがあると言える。例えば、以下の通りである。

- 「サイバーセキュリティ法」第三十七条によれば、「重要情報インフラの運営者」が行う国境を越えたデータ伝送だけを制限しており、すべてのインターネット運営者を制限対象としているわけではない。また、立法体系の観点からみると、「サイバーセキュリティ法」第三十七条を第三章「ネットワーク運用におけるセキュリティ」の「重要情報インフラの運行の安全」にもってきていることも、規制される主体が重要情報インフラの運営者に限られることを意味している。しかしながら、「弁法草案」では、対象を全てのインターネット運営者にまで拡大し、上位法の適用主体の範囲に対する制限を拡大した。

- 「弁法草案」第九条では、セキュリティ評価を行う必要のある国境を越えて伝送されるデータを列挙しているが、同条規定に列挙されるデータの型は「サイバーセキュリティ法」で限定している範囲を逸脱してしまっているおそれがある。例えば、「50 万人以上又は累計して 50 万人以上の個人情報を含むもの」又は「データ量が 1,000GB を超えるもの」は、必ずしも「サイバーセキュリティ法」にいう「重要データ」と同様に扱うことができるとは限らない。

以上から、国境を越えるデータ伝送に関する関係規定が公表されるまでは、「サイバーセキュリティ法」第三十七条が企業において中国での経営にどこまで影響をもたらすのか、一定の不確実性がある。なお、筆者の推測では、正式に公布される関係規定は「弁法草案」よりも厳しい内容になることはないであろうと思われる。従って現時点では、企業は「弁法草案」を参考にしながら、予め長期的な計画を立てておくのがよいであろう。

（里兆法律事務所が 2017 年 7 月 7 日付で作成）