立方律師
NEWSLETTER
LIFANG & PARTNERS 立方观评
No.266
2021.09

目录
Contents

中国化学医药领域专利补充数据的最新标准

王颖、李春晅 立方律师事务所

多年来，国家知识产权局和法院在申请程序、无效宣告程序和行政诉讼程序中对补交数据有比较严格的限制，这种的做法饱受质疑。因为这导致专利申请容易被驳回，或者导致专利被宣告无效的几率变高。但是，最新司法解释以及最高人民法院（以下简称“最高院”）和国家知识产权局的相关案例改变了此前的标准，放宽接收补充数据的标准，这将加强化学医药领域专利权的稳定性，并且，将极大地提升化学医药领域专利的价值，进而促进化学医药领域的创新。

一、最新规定：放宽对化学医药领域补充数据的接收要求

由于在接收化学医药领域专利补充数据方面，国家知识产权局比美国和欧洲专利局的要求更为严格，所以，在2020年1月15日签署的《中美经济贸易协定》（以下简称“协定”）中，关于补充数据是一项关键问题。协定的第1.10条对补充数据作出如下规定：“中国应允许药品专利申请人在专利审查程序、专利复审程序和司法程序中，依靠补充数据来满足可专利性的相关要求，包括对公开充分和创造性的要求。”我国为了履行该协定，在2020年的相关法律文件对补充数据的条款进行了修订。

首先，自2020年9月12日起施行的司法解释，即**《最高人民法院关于审理专利授权确权行政案件适用法律若干问题的规定（一）》**（以下简称《若干问题的规定》），该规定第十条与《协定》第1.10条相对应，即“药品专利申请人在申请日以后提交补充实验数据，主张依赖该数据证明专利申请符合专利法第二十二条第三款、第二十六条第三款等规定的，人民法院应予审查。”但该条仅规定了法院对补充的实验数据应予审查，并未明确法院对于补充实验数据应采取何种标准。

随后，国家知识产权局新修改的**《专利审查指南》**（以下简称《指南》）已于2021年1月15日起施行，对于化学医药领域的专利补充数据的接收，规定了更为明确的标准。《指南》第二部分第十章第3.5节明确规定，对于申请日之后申请人为满足专利法第二十二条第三款（创造性）、第二十六条第三款（公开不充分）等要求补交的实验数据，审查员应当予以审查。补交实验数据所证明的技术效果应当是所属技术领域的技术人员能够从专利申请公开的内容中得到的。并且

《指南》中给出了涉及药品专利申请的审查示例：

例1：权利要求请求保护化合物A，说明书记载了化合物A的制备实施例、降血压作用及测定降血压活性的实验方法，但未记载实验结果数据。为证明说明书充分公开，申请人补交了化合物A的降血压效果数据。该补交实验数据在审查创造性时也应当予以审查。因为，对于所属技术领域的技术人员来说，根据原始申请文件的记载，化合物A的降血压作用已经公开，补交实验数据所要证明的技术效果能够从专利申请文件公开的内容中得到。

例2：化合物 A和其他化合物在通式下的抗肿瘤作用已经在说明书中的实验数据中进行了举例说明，申请人补交了对比实验数据，通过比较化合物A的抗肿瘤作用和对比文件中的抗肿瘤作用，以证明权利要求具备创造性，此时，补充试验数据应当予以审查。

然而，通过对《指南》的理解，仍无法确定在专利授权确权程序中，是否允许申请人在申请日后提交补充数据，以证明其主张的技术效果，即在说明书中描述了某一技术效果，但是缺乏数据支撑时能否通过补充数据证明技术效果。在以往司法实践中，不允许申请人在申请日后提交补充试验数据用以证明说明书中未经确认的技术效果。例如阿斯利康(瑞典)有限公司诉国家知识产权局一案（(2018)京行终6345号）、贝林格尔英格海姆法玛两合公司与国家知识产权局一案（(2017)京行终2470号）。

二、案例：明确申请日后补充实验数据的接收条件

在相关案例中，对于专利权人或专利申请人申请日后提交的实验数据可以接收的标准以及可以解决的问题，最高院和国家知识产权局作出了进一步的明确。

（一）申请日后补充试验数据可以证明专利的创造性

阿斯利康无效行政诉讼案（“替格瑞洛”案）【案号：(2019)最高法知行终33号】，该案涉及的是专利号为200610002509.5、名称为“三唑并[4,5-D]嘧啶化合物的新晶形和非晶形”的发明专利，专利权人为阿斯利康，该专利因缺乏创造性而被宣告无效。在专利无效宣告行政程序中，专利权人提交了其员工所做的代谢稳定性和生物可利用率的补充试验数据，以证明说明书中记载的“令人惊讶的高代谢稳定性和生物利用率”技术效果。但是，专利复审

委员会对该等数据不予考虑，因为专利复审委员会的专家认为：1. 关于药物的代谢稳定性和生物可利用率，本专利说明书并未提供任何实验数据以证实上述技术效果的存在；2. 补充数据是在优先权日之后形成的，专利权人的员工所作出的结果不可避免地带有主观性。因此，专利复审委员会作出决定，在未考虑补充数据的情况下，以缺乏创造性为由宣告涉案专利无效。北京知识产权法院对该决定予以确认。

虽然，最高院在二审判决中维持了北京知识产权法院的判决，但是，最高院对于是否接收补充实验数据持有不同的处理意见。最高院依据《若干问题的规定》第十条，厘清了关于接收补充实验数据的标准：首先，如果补充实验数据拟直接证明的待证事实为原专利申请文件明确记载或者隐含公开，即可认定申请人完成了相关研究，有关补充实验数据的接受不违反先申请原则；其次，补充实验数据通常应当通过证明原专利申请文件明确记载或者隐含公开的待证事实具备真实性，进而对申请人或者专利权人最终要证明的法律要件事实起到补充证明作用，而非独立证明原专利申请文件中未予公开的内容，进而克服原专利申请文件自身公开不充分等内在缺陷。

本案中，因为药物的代谢稳定性和生物可利用率在专利文件已明确记载，并且提供补充数据用以证明前述技术效果真实存在，所以，最高院对权利人提交的补充数据进行了审查。因本案中补充数据不足以证明涉案专利具有本领域技术人员预料不到的药物效果，最高院最终维持了一审判决，但是，本案仍是适用《若干问题规定》第十条的首例案例，对于申请日后补充数据的接收条件设定了标准，具有指导意义。

此后，在京新药业无效吉瑞工厂的专利无效案件中，国家知识产权局于2020年11月27日作出的第47087号无效决定，基于专利权人提交的补充数据维持了该专利。国家知识产权局在接收补充数据时也基本上沿袭了与“替格瑞洛”案中设定的标准。

（二）申请日后补充数据可以克服公开不充分的问题

在国家知识产权局、北京嘉林药业股份有限公司诉沃尼尔·朗伯有限责任公司专利权无效行政纠纷一案中（“立普妥”案）【案号：(2014)行提字第8号】，最高法确认了公开不充分的情况下，补充数据的接收标准：在专利申请日后提交的用于证明说明书充分公开的实验性证据，如果可以证明以本领域技术人员在申请日前的知识水平和认知

能力，通过说明书公开的内容可以实现该发明，那么该实验性证据应当予以考虑，不宜仅仅因为该证据是申请日后提交而不予接受。在考虑实验性证据是否采纳的时候应严格审查时间和主体两个条件。首先，实验性证据涉及的实验条件、方法等在时间上应该是申请日或优先权日前本领域技术人员通过阅读说明书直接得到或容易想到的；其次，在主体上，应立足于本领域技术人员的知识水平和认知能力。但是我们仍需要通过更多案件了解国家知识产权局和法院在公开不充分问题上，对补充实验数据的把握尺度。

结论

“立普妥”案与“替格瑞洛”案中设定的标准十分相近，即补充数据所体现的技术效果或者技术方案，应是基于申请日或优先权日前所属领域的技术人员的认知水平，可以通过原始专利申请文件中直接获得的。这两项标准均符合在先申请原则。

国家知识产权局和法院放宽了以往接收补充数据的标准，设立了新的标准，即仅在说明书中载明技术效果，但没有具体的实施方式或者支撑数据，可以通过补充数据来证明，在现行标准下相关专利相对于现有技术具有创造性，或用以克服公开不充分的缺陷。但是需要注意的是，专利文件中需要记载技术效果，以便补充数据加以证明。

最高法颁布的《若干问题规定》以及相关案例确定的补充数据的接收标准，这不仅可以提高专利申请的授权率，而且增强了专利的稳定性，降低专利被宣告无效的风险。此外，明确补充试验数据的接收标准，是对蓬勃发展的制药行业期待已久的回应，既可以鼓励创新，亦可以提高化学医药专利的价值。

王颖

立方律师事务所合伙人

执业领域：知识产权

yingwang@lifanglaw.com

李春晅

立方律师事务所合伙人

执业领域：知识产权

chunxuanli@lifanglaw.com

Latest Developments on Data Supplementation for Chemical or Pharmaceutical Patents in China

WANG Ying & LI Chunxuan, Lifang & Partners

CNIPA (China National Intellectual Property Administration) and the Chinese courts have been challenged for years for their strict practices on accepting post-filing data during prosecution, invalidation, and administrative litigation proceedings. Such practices render patent applications with broad scopes less likely to succeed or much more likely to be revoked during invalidation procedures. However, the Supreme People's Court's latest judicial interpretation and precedents set by the courts and CNIPA create new practices that give chemical and pharmaceutical patent holders better prospects of acquiring stable patent rights. Moreover, new practices on accepting post-filing data will add more value to chemical and pharmaceutical patents and further boost innovation in the chemical and pharmaceutical industries.

Latest Policy and Law Updates on Data Supplementation

A. China-US Economic and Trade Agreement

Data supplementation was one of the key issues in the China-US Economic and Trade Agreement ("*Agreement*") executed on January 15, 2020, because CNIPA had narrower criteria for accepting post-filing data for chemical and pharmaceutical patents than the US and the European Patent Office.

Article. 1.10 of the Agreement, which relates to Data Supplementation, states that "*China shall permit pharmaceutical patent applicants to rely on supplemental data to satisfy relevant requirements for patentability, including the sufficiency of disclosure and inventive step, during patent examination proceedings, patent review proceedings, and judicial proceedings*". Accordingly, Chinese legislators took steps in 2020 to implement the *Agreement*.

B. Provisions of the Supreme People's Court on Several Issues concerning the Adjudication of Administrative Cases on Granting and Affirming Patent Rights

To echo Article 1.10 of the *Agreement*, the Supreme People's Court promulgated *Provisions of the Supreme Court on Several Issues concerning the Adjudication of Administrative Cases on Granting and Affirming Patent Rights* ("*Provisions*"), which took effect on September 12, 2020. Article 10 of the Provisions specifically relates to data supplementation. Article 10 of the Provisions states that:

Where a drug patent applicant submits supplementary experimental data after the date of application and claims that the patent application should be proved as conforming to Article 22.3, Article 26.3 and other provisions of the Patent Law by relying on such data, the People's Court shall examine such data.

However, Article 10 of the Provisions only specifies that the court shall examine supplementary experimental data. However, the standards for

accepting supplementary data remain unclear.

C. Chinese Patent Examination Guideline

Later, on January 15, 2021, the amended Chinese Patent Examination Guidelines ("Guidelines") introduced seemingly clearer standards for accepting supplementary data for chemical and pharmaceutical patents.

The Guidelines specify that: (1) the examiner shall examine experimental data submitted by an applicant after the application date regarding Articles 22.3 (inventive step) and 26.3 (insufficient disclosure) of the Patent Law; and (2) the technical effect proved by supplementary experimental data must be obtainable by one skilled in the art based on disclosures in the patent application.

The Guidelines also give two examples to demonstrate the standards for post-filing data acceptance. One example concerns a patent application claiming to protect compound A with a specification that discloses the experimental method of measuring the activity of lowering blood pressure without disclosing experimental results. In such situations, post-filing data submitted by an applicant on the blood pressure lowering effects of compound A to overcome objections of insufficient disclosure are acceptable since such data is obtainable from the method disclosed in the specification. In the other example, the anti-tumor effects of Compound A and other compounds under the general formula are exemplified with solid data in the specification. The data supplemented by the applicant to show the inventive step of the patent by comparing the anti-tumor effect of Compound A with that in the prior art is acceptable.

However, there remains uncertainty on whether a court or CNIPA would allow an applicant or patentee to submit post-filing data to prove an asserted technical effect, which is merely mentioned but lacking data to confirm the effect in the specification. In many previous cases, supplemental data submitted after the filing date to prove such unconfirmed technical effects in the patent document was rejected. Such cases include AstraZeneca v. PRB, (2018) Jing Xing Zhong No. 6345 and Boehringer Ingelheim v. PRB, (2017) Jing Xing Zhong 2470 decided by Beijing High People's Court, and other cases.

The most recent cases decided by the Supreme People's Court and CNIPA present clearer standards on the acceptance of supplemental data filed by the patentee to prove such unconfirmed technical effects in patent documents.

Data Supplementation to Overcome Lack of Inventive Step Objections

AstraZeneca's ZL200610002509.5 patent, which concerned a crystalline form of a triazolo (4,5-d) pyrimidine compound known as "Ticagrelor", was invalidated for lacking an inventive step. During invalidation proceedings, the patentee submitted data showing metabolic stability and bioavailability prepared by the patentee's employee to show the surprising effects of the Ticagrelor. However, that data was not considered by the Patent Reexamination Board (PRB), which took the position that: (i) surprisingly high metabolic stability and bioavailability effects were merely asserted in the background of the patent without any data in the original patent document to prove these effects; and (ii) supple-

mental data was submitted after the priority date, and the results made by the patentee's employees were inevitably subjective. Therefore, the patent was invalidated for lacking an inventive step by the PRB, without considering the supplemental data. The Beijing Intellectual Property Court confirmed the PRB's decision.

Although the Beijing Intellectual Property Court's decision was upheld in the second instance in Supreme People's Court case (2019) Zhi Xing Zhong No. 33 in October 2020, the Supreme People's Court took a different view towards the acceptance of post-filing data. By referring to Article 10 of the *Provisions* as its legal basis, the Supreme People's Court clarified the standards for post-filing data acceptance as: (i) if the facts to be proved by the post-filing data are clearly recorded or implicitly made public in the specification, the applicant can be considered to have completed relevant research, and so, acceptance of the data would not violate the first to file principle; and (ii) supplementary data shows that the facts to be proved in the specification are true.

By adopting the above standards, the Supreme People's Court could consider the supplemental data submitted by the patentee because the metabolic stability and bioavailability effects had been recorded in the patent and later proved by the supplemental data. Although the Supreme People's Court upheld the decision of the first instance court because the supplemental data was not convincing enough to manifest surprising effects compared with those in the prior art, this was the first case to apply Article 10 of the *Provisions* and set a clear standard for post-filing data acceptance to be followed in similar future cases.

In a later invalidation case, Jingxin Pharmaceutical v. Richter Gedeon NYRT (Invalidation Decision No. 47087), decided by CNIPA in November 2020, the validity of the subject patent was upheld based on post-filing data submitted by the patentee. CNIPA's attitude of accepting post-filing data to prove the asserted technical effect followed the standards that applied in the above Ticagrelor case.

Data Supplementation to Overcome Insufficient Disclosure Objections

According to the *Guidelines*, a chemical product invention must be sufficiently disclosed by identifying the chemical product, at least one method of preparing the product, and proof supporting its anticipated uses or technical effects. Very few post-filing data submissions were accepted in the past due to insufficient disclosure of the preparation method or technical effects.

In administrative litigation (2014) Xing Ti Zi Ti No. 8, which concerned Pfizer's product Lipitor and was heard by the Supreme People's Court in 2015, the patentee submitted experimental reports during litigation to demonstrate that the Type I crystals for atorvastatin calcium trihydrate could be produced by one skilled in the art. The court intended to set a tone or establish a practical rule for accepting post-filing data under insufficient disclosure. That is, regarding the post-filing data for manifesting insufficient disclosure, if it can be proved that the invention can

be realized through the content disclosed in the specification with the knowledge and cognitive ability of one skilled in the art before the filing date, the supplemental data should be considered and should not be rejected simply because the data was submitted after the filing date. Moreover, when considering the acceptance of experimental evidence: (i) the experimental conditions and methods used in collecting the experimental evidence must be directly obtainable or easily thought of by one skilled in the art who reads the instructions before the filing date or the priority date; and (ii) matters must be considered based on the knowledge and cognitive ability of one skilled in the art.

In recent years, CNIPA examiners have become more prone to raising lack of inventive step objections instead of insufficient disclosure objections during the prosecution of inventions without substantial data to manifest their technical effects. In (2018) Jing 73 Xing Chu No. 2626, a case heard by the Beijing IP court in November 2020, the applicant submitted its prior application, filed before the filing date but published after the filing date of the patent application-in-suit, as evidence that the same chemical as that found in the patent application-in-suit had an SGLT2 inhibition effect. Therefore, the crystal form of the chemical, as claimed in the patent application-in-suit, obviously had such an effect. Such evidence was rejected by CNIPA but accepted by the Beijing IP Court because: (1) the evidence showed that the technical effect described in the patent application-in-suit is a technical contribution made before the filing date; and (2) the public could identify such an effect at the time when the patent application-in-suit was published. Therefore, accepting such experimental data would neither give the applicant protection beyond his technical contribution nor affect the public interest.

In summary, the standards set in the above cases are quite similar in that the technical effect or technical solution manifested by the supplemental data was obtainable from the original patent application by the patentee before the filing date, without contravening the first to file principle, and the acceptance of such data did not affect public interests.

Conclusion

It is good to see that CNIPA and courts no longer adhere to very stringent standards for accepting supplemental data. For technical effects merely asserted in the specification without any specific embodiment, supplementary data can be used to manifest the inventive step over the prior art using current standards. It should, however, be noted that the effects need to be recorded in the patent document so that data supplementation can prove such effects.

Although data can be supplemented to overcome insufficient disclosure objections when certain rules are met, we strongly recommend that applicants, insofar as is possible, fully disclose experimental data related to an invention, such as the technical effect and preparation process, in the original patent document.

The *Provisions* and cases decided by the courts have clarified standards for accepting post-filing data to a large degree. Acceptance of post-filing data during prosecution or invalidation proceed-

ings for chemical or pharmaceutical patents can also improve patent application grant rates and patent stability, which will reduce the risk of patents being invalidated. Clarifying the standards for accepting supplementary experimental data is a measure taken to support a long-awaited and expected boom in the pharmaceutical industry. Moreover, it will encourage innovation and significantly improve the transaction value of chemical and pharmaceutical patents.

WANG Ying
Partner of Lifang & partners
Practice Areas:
Intellectual Property
yingwang@lifanglaw.com

LI Chunxuan
Partner of Lifang & partners
Practice Areas:
Intellectual Property
chunxuanli@lifanglaw.com

《个人信息保护法》下跨国公司个人信息跨境传输规则解读

秦英、肖莆羚令 立方律师事务所

2021年8月20日，《个人信息保护法》（以下简称为“《个保法》”）经全国人大常委会表决正式通过。作为个人信息保护领域的基本法，其无论是对于个人信息保护还是企业合规经营都具有重要法律意义。

个人信息保护的重要性在于其“可识别”的认定标准和具有私主体性质的信息主体，一旦信息遭遇不当处理，可能会给个人的财产和人身安全带来极大风险，甚至影响企业和社会的信用体系和经济安全。

与此同时，商品和经济全球化推动着跨国公司的发展壮大与个人信息跨境流动。如此一来，如何保障国民个人信息的境外保护、协调各司法辖区的规则冲突，把握个人信息跨境的尺度与边界等问题逐渐凸显。

本文旨在以《个保法》为基点，结合其他相关数据或个人信息保护法律规范，探究跨国企业在个人信息跨境传输场景中面临的监管措施和相应责任，以求为跨国公司在实务中提供一些参考和支持。

一、跨国公司集团内部的个人信息跨境传输明确受《个保法》的规制

《个保法》第四条

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

根据《个保法》第四条，传输行为属于信息处理的一种，受到《个保法》的约束。然而，对于跨国公司内部个人信息的流通，《个保法》并未明确其是否属于受监管的“传输”行为。《个保法》第三章“个人信息跨境提供规则”更侧重于境内信息处理者在跨境传输中应承担的提供者义务。对此，《信息安全技术 数据出境安全评估指南》（“《数据出境指南》”）3.7注2（c）规定，网络运营者集团内部数据由境内转移至境外，涉及其在境的内运营中收集和产生的个人信息和重要数据的，属于数据出境。虽然《数据出境指南》不具有强制执行力，但其明确了一个基础问题：集团内个人信息由境内转移至境外属于跨境传输。结合《个保法》第四条和《数据出境指南》的规定，跨国公司内部的个人信息跨境传输行为显然应

当受到《个保法》的约束。

实践中，位于境内的个人信息处理者将个人信息传输至境外集团内部公司的方式主要表现为两种：

- 一是前者通过外包协议将其收集的个人信息直接传输至境外服务器并交由其他境外集团公司处理的行为；
- 二是前者将在我国境内收集的个人信息传输至境外母公司数据中心服务器或者是通过母子公司之间共享的计算机系统来实现数据传输的行为。

此两种行为均属于信息跨境传输行为。我们认为，所谓数据跨境并非仅仅局限于数据物理空间的转移，即便上述场景中中心服务器设置在中国境内，如果境外公司对其可以接触（access）或拥有控制权，例如后台修改个人信息或为了维护系统而接触个人信息，该行为仍有较大可能被认定为数据出境。此外，由于《个保法》第四条关于“处理”行为的规定是不完全列举，因此，该等“可以接触”或“有控制权”的状态也很可能属于“处理”行为。可见，无论从“传输”还是“处理”的角度看，跨国公司集团内部的个人信息跨境传输都将受《个保法》的规制。

二、《个保法》的域外管辖效力

《个保法》第三条

在中华人民共和国境内处理自然人个人信息的活动，适用本法。

2. 在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

（一）以向境内自然人提供产品或者服务为目的；

（二）分析、评估境内自然人的行为；

（三）法律、行政法规规定的其他情形。

关于《个保法》的适用范围，立法者采用了**属地管辖+保护管辖**相结合的思路。关于属地原则，《个保法》规定的连接点是“行为所在地”，即处理活动发生在境内的企业均受到《个保法》的约束，而无论处理活动的主体是否为中国境内企业。

若处理活动发生在境外，则需要满足《个保法》第三条第二款的条件，判断该境外公司是否符合两项具体情形，而具体情形既包括目的又包括实在行为，所囊括范围广阔。在跨国公司个人信息跨境传输的情景中，境内企业由于实施了“传输”动作，必然受制于《个保法》的管辖；而境外公司往往是为境内公司提供研发技术支持，或者作为信息枢纽统筹协调集团内的数据处理活

动，其很有可能落入“以向境内自然人提供产品或者服务为目的”或“分析、评估境内自然人的行为”的范围。

即便境外公司有充分理由证明不属于上述两项情形，该条第二款第三项作为兜底条款，为立法者和执法者在实践中留下了较大的自由裁量空间。

需要指出的是，我国的《个保法》在内容和框架的构建都借鉴了欧盟的《通用数据保护条例》（“GDPR”）第三条[1]的规定。虽然在管辖范围上GDPR采用的是属地管辖+属人管辖+保护管辖+国际公法管辖相结合的思路，但通过保护管辖原则，在实践中《个保法》和GDPR法律对个人信息保护的范围都达到对域外的个人信息处理行为进行管辖的效果。

三、境内外企业的具体义务

1、跨境传输需遵守《个保法》对个人信息处理活动的普遍要求

首先，跨境传输作为个人信息处理活动的一种类型，应当遵循处理《个保法》的一般规定，包括但不限于：（1）向个人告知个人信息处理者的身份和联系方式，个人信息的处理目的、处理方式，处理的个人信息种类和保存期限；（2）取得数据主体的单独同意；以及（3）跨境传输前后个人信息的保存期限应当为实现处理目的所必要的最短时间等。

其次，如果跨境传输的信息属于敏感个人信息[2]，还应参照适用第二章第二节的特殊规定规定。

2、《个保法》对个人信息跨境传输活动的特殊要求

（1）境外传输的个人信息的性质和数量的特殊要求

> **《个保法》第四十条**
>
> 关键信息基础设施运营者和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，应当将在中华人民共和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，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

如《个保法》第四十条所言，对于（1）关键信息基础设施运营者收集和产生的个人信息，以及（2）达到一定数量的个人信息的跨境传输活动，《个保法》规定应以本地化存储为原则。确需向境外提供的，应通过国家网信部门组织的安全评估。

- **关键信息基础设施：**是指涉及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、丧失功能或者个人信息泄露，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。对关键信息基础设施所搜集和产生的个人信息本地化要求是为了保障个人信息内容的安全性。有关关键信息基础设施的认定，可参考《网络安全审查办法》和今年9月1日生效的《关键信息基础设施安全保护条例》。

- **达到国家网信部门规定数量的个人信息：**目前，网信部门尚未对此数量作出明确界定。作为参考，网信办在2017年公布的《个人信息和重要数据出境安全评估办法（征求意见稿）》和今年7月公布的《网络安全审查办法（修订草案征求意见稿）》中，要求对超过一定数量的个人信息运营者进行安全评估。

相关规定	监管对象	监管要求
《个人信息和重要数据出境安全评估办法（征求意见稿）》（2017）第九条	含有或累计含有50万人以上的个人信息；	出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估
《网络安全审查办法（修订草案征求意见稿）》第六条	超过100万用户的个人信息	运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查

虽然以上两条规定暂未生效，但不难理解，国家对于达到一定规模的个人信息出境具有高度敏感性且积极适用本地化原则。因此在实践中，拟进行信息跨境传输的境内运营者，若掌握超过50万以上用户的个人信息或数据规模超过1000GB，很有可能受到“个人信息本地化”的限制。

目前，针对个人信息跨境传输，2019年网信办曾发布《个人信息出境安全评估办法（征求意见稿）》，但此后并未正式出台任何强制性法律文件。该征求意见稿第四条要求，网络运营者申报个人信息出境安全评估应当提供（1）申报书；（2）网络运营者与接收者签订的合同；（3）个人信息出境安全风险及安全保障措施分析报告；以及（4）国家网信部门要求提供的其他材料。经营企业虽然被鼓励参照适用相关法规和指南以求最大程度地降低监管风险，但在具体行为和程序中，他们仍然面临“无法可依”的窘境。考虑到个人信息保护的立法势头发展迅速及其之于国家安全的重要性，在缺少明确指导的情况下，建议跨国公司在进行个人信息跨境传输前内部进行风险及安全措施评估分析报告并留存。

（2）个人信息跨境传输活动的前置条件

由于个人信息流通不可逆性，《个保法》对于个人信息跨境传输活动采用事前监管的方式。《个保法》第三十八条规定，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当至少具备下列一项条件：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

安全评估或个人信息保护认证均需由国家网信部门进行组织安排。如上所述，目前安全评估的相关规则还处于征求意见阶段，关于专业机构的个人信息保护认证更是没有任何参考指南，可能有待后续网信部门的进一步立法加以明确。因此，“与境外接受方订立合同”是相对切实且容易满足的条件。跨国企业在进行个人信息跨境传输时，应要求其境内外公司签订合同，约定双方关于个人信息处理和保护的权利和义务。

3、个人信息跨境传输活动的其他要求

《个保法》第四十三条还规定了信息跨境传输的“对等原则”，如果信息接收国家和地区在个人信息保护方面对我国采取歧视性的禁止、限制或者其他类似措施，中国可以根据实际情况对该国家或者地区对等采取措施，因此对该国的个人信息跨境传输很有可能受到限制。

此外，本次《个保法》三审稿进一步完善了个人信息跨境提供规则，中国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。同时，《个保法》要求个人信息处理者采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。我们理解，该条规定解决了不同司法辖区就个人信息跨境传输程序上的冲突规定，但同时通过将《个保法》下跨境传输的实质义务施加到境内的个人信息处理者，间接实现了个人信息跨境传输活动中《个保法》的域外效力。

注释：

[1]GDPR第三条：

1. 本法适用于设立在欧盟内的控制者或处理者对个人数据的处理，无论其处理行为是否发生在欧盟

内。

2. 本法适用于对欧盟内的数据主体的个人数据处理，即使控制者和处理者没有设立在欧盟内，其处理行为：

a) 发生在向欧盟内的数据主体提供商品或服务的过程中，无论此项商品或服务是否需要数据主体支付对价；或

b) 是对数据主体发生在欧盟内的行为进行的监控的。

3. 本法适用于设立在欧盟之外，但依据国际公法欧盟成员国法律可适用地的控制者对个人数据的处理。

[2]敏感个人信息是一旦泄露或者非法使用，可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息，包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

秦英

立方律师事务所 合伙人

执业领域：反垄断、合规

yingqin@lifanglaw.com

肖莆羚令

立方律师事务所 律师

执业领域：反垄断、合规

pulinglingxiao@lifanglaw.com

Review of the Rules on PI Cross-border Transmission by Multi-national Corporations under the PIPL

QIN Ying & XIAO Pulingling, Lifang & Partners

On August 20, 2021, the Personal Information Protection Law of the People's Republic of China ("PIPL") was formally passed by the Standing Committee of the National People's Congress. As a fundamental law in the field of personal information ("PI") protection, it is of great legal significance both for individuals' information protection and for the compliance activities of corporate.

The significance of PI protection lies in its "identifiable" criteria and the nature of private subjects for the PI subjects. Improper processing of PI may bring great risks to personal property and personal safety, and even affect the credit system and economic security of companies and society.

Meanwhile, the globalization of commodities and economy drives the development of multinational corporations and the cross-border flow of PI. As a result, questions such as how to achieve overseas protection of PI, coordinate the conflict of different jurisdictions, and manage the extent and boundaries of PI cross-border transmission have become increasingly important.

This article would discuss the regulatory measures and corresponding responsibilities of multinational corporations in the context of PI cross-border transmission under the PIPL and other relevant laws and regulations governing data or PI protection, to provide some practical reference and support for multinational corporations.

I. The PI Cross-border Transmission Within Multinational Corporations is Clearly Subject to PIPL

Article 4 of the PIPL.

PI refers to any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded excluding information that has been anonymized.

Processing of PI includes the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information.

According to Article 4 of the PIPL, the act of transmission is a form of information processing, and is subject to the PIPL. However, the PIPL does not clarify whether the internal circulation of PI of multinational corporations falls within the scope of the targeted "transmission" activity. The Rules on the Cross-border Provision of PI under Chapter 3 of the PIPL focuses on the obligations of domestic data processors who act as PI providers in PI cross-border transmission. Note 2 (c) of Article 3.7 of the Information Security Technology - Guidelines for Data Cross-border transmission Security Assessment (the "Guidelines for Data Cross-border Transmission") provides that where the internal data of a network operator group is transmitting from onshore to offshore, it shall be deemed as data cross-border transmission if such transmission

involves PI and important data collected and generated during its onshore operation. Although the Guidelines for Data Cross-border Transmission is not an enforceable law but only a national standard, it clarifies a fundamental issue: the transmission of PI within a group from onshore to offshore shall be deemed as cross-border transmission. Based on the provisions of Article 4 of the PIPL and the Guidelines for Data Cross-border Transmission, it is obvious that the PI cross-border transmission within the group of multinational corporations shall be subject to the PIPL.

In practice, there are mainly two methods by which an onshore PI processor transmits PI to an overseas company within the same group:

- First, the onshore PI processor transmits the PI to an overseas server for processing directly with a data agreement;
- Second, the onshore PI processor stores the PI collected to the server of the data center of its overseas parent company or through the shared computer system between the parent company and its subsidiaries.

Both of the above two scenario will constitute PI cross-border transmission. We believe that PI cross-border transmission is not limited to the change of its physical location of the PI. Even if the central server in the above second scenario is located in China, if the overseas company has access to or control over the PI, such as modifying PI in the background or accessing PI for the purpose of maintaining the system, such behavior is likely to be considered as cross-border transmission. In addition, because the activities of “processing” is defined non-exhaustively in Article 4 of the PIPL, such state of "access" or "control" are also likely to be regarded as a form of "processing". Therefore, no matter from the perspective of "transmission" or "processing", the PI cross-border transmission by multinational corporations will be subject to the PIPL.

II. Extraterritorial Effect of the PIPL

Article 3 of the PIPL

This Law shall apply to any activity of processing of personal information of a natural person that is carried out within the territory of the People's Republic of China

This Law shall also apply to any activity of processing of personal information of any natural person located within the territory of the People's Republic of China that is carried out outside the territory of the People's Republic of China under any of the following circumstances:

(I) The purpose is to provide domestic natural persons with products or services;

(II) Analyzing and evaluating the behaviors of domestic natural persons;

(III) Other circumstances stipulated by laws and administrative regulations.

As for the applicable scope of the PIPL, legislators have adopted the approach of **combining territorial jurisdiction and protective jurisdiction**. As for the principle of territorial jurisdiction, the connecting point adopted by the PIPL is the "place where the behavior is conducted", that is, an entity that process PI within China shall be governed by the PIPL, no matter whether the said entity are domestic enterprises or not.

If the processing activity is conducted outside

the territory of China, the overseas entity shall assess whether it falls into the circumstances stipulated in Article 3.2 of the PIPL. The situations include both purposes criteria and act criteria, covering a wide range. Under the scenario of PI cross-border transmission of multinational corporations, the domestic enterprises will inevitably be subject to the PIPL due to their behavior of "transmission". The overseas entities usually provide domestic companies with R&D technical support, or act as information hubs to coordinate the data processing activities within the group, so they are likely to fall into the circumstances of "Where the purpose of the activity is to provide a product or service to that natural person located within China;" or " Where the purpose of the activity is to analyze or assess the behavior of that natural person located within China".

Even if the overseas entities have sufficient reasons to prove that it does not fall within the above two circumstances, the third circumstance of Article 3(2) acts as a miscellaneous provision, providing the authority more than enough discretion in practice.

It should be noted that the content and framework of PIPL have drawn lessons from Article 3 of the General Data Protection Regulation of EU ("GDPR")[1]. Although GDPR adopted the approach of combining territorial jurisdiction, personal jurisdiction, protective jurisdiction and public international law jurisdiction, through the principle of protective jurisdiction, in practice, both PIPL and GDPR has reached the extraterritorial effect of PI processing activities.

III. Specific Obligations of the Domestic and Overseas Entity

1. PI Cross-border Transmission Shall Complies with the General Requirements of the PIPL for PI Processing Activities.

First of all, as a type of PI processing activities, PI cross-border transmission should follow the general provisions of the PIPL, including but not limited to: (1) informing individuals of the identity and contact information of the personal information processor, the purpose and method of processing PI, and the types and retention period of the processed PI; (2) obtaining the individual consent of the data subject; and (3) before and following the transmission, the retention period of PI shall be the minimum period necessary for achieving the purpose of processing, etc.

Second, if the PI to be transmitted is classified as sensitive PI[2], the special provisions of Section II of Chapter II shall also apply.

Article 40 of the PIPL

Critical information infrastructure operators, or personal information processors whose processing of personal information reaches the threshold amount prescribed by the national cyberspace authority, shall store within the territory of the People's Republic of China the personal information collected or generated by them within the territory of the People's Republic of China. Where it is necessary to provide such information to an overseas recipient, a security assessment organized by the national cyberspace authority shall be passed; if a security assessment is not re-

quired as provided by law, administrative regulations or the national cyberspace authority, such provision shall prevail.

2. Special Requirements for PI Cross-border Transmission under the PIPL

2.1 Special requirements on the Nature and Quantity of PI Transmitted aboard

As stated in Article 40 of the PIPL, with respect to the (1) PI collected and generated by critical information infrastructure operators, and (2) PI cross-border transmission activities up to a certain amount, the PIPL stipulates that the principle of localized storage shall be applied. If it is necessary to transmit such data and PI aboard, it shall be subject to the security assessment organized by the Cyberspace Administration of China ("CAC").

- **Critical information infrastructure** refers to critical information infrastructure involving public communications and information services, energy, transportation, water conservancy, finance, public services, e-government and other important industries and fields, as well as other critical information infrastructure that may seriously endanger national security, national economy, people's livelihood, and public interests in the event of damage, malfunction, or leakage of PI. The requirement of localization of PI collected and generated by critical information infrastructure is to protect the security of PI. The Cybersecurity Review Measures and the Regulations on the Protection of the Security of Critical Information Infrastructure, which just came into effect on September 1, may apply as a reference to the determination of critical information infrastructure. The Lifang Team also summarized the criteria in the article *Review of Regulations on the Protection of the Security of Critical Information Infrastructure.*
- **PI up to the amount specified by CAC**: Currently, CAC has not yet defined this amount. As a reference, the Measures on the Security Assessment of PI and Important Data to be Transmitted Abroad (Exposure Draft) and the Cybersecurity Review Measures (Revised Draft for Comments) by the CAC require security assessment for the PI up to a certain amount.

Relevant Provisions	Thresholds for Security Assessment	Regulatory Requirements
Article 9 of the Measures on the Security Assessment of PI and Important Data to be Transmitted Abroad (Exposure Draft) (2017)	It contains or contains in aggregate the PI of more than 500,000 users; The data volume exceeds 1,000 GB	Network operators shall report to the competent authority or regulator of the industry to organize a security assessment if the data to be transmitted abroad
Article 6 of the Measures on the Cybersecurity Review (Revised Draft for Comments)	The PI of more than 1 million users	Operators who intend to go public abroad must apply to the Cybersecurity Review Office for cybersecurity review.

Although the above two provisions have not come into effect yet, it is understandable that the Although the above two provisions have not come into effect yet, it is understandable that the State is highly sensitive to the transmission of PI up to a certain scale and actively applies the localization principle. Therefore, in practice, if an inshore entity intending to transmit aboard the PI

of more than 500,000 users or whose size exceeds 1,000 GB, it is likely to be subject to the localization restriction.

In 2019, CAC issued the Measures for the Security Assessment of PI cross-border transmission (Exposure Draft) ("Measures"), but the Measures has not been formally published yet. Article 4 of the Measures requires network operators to submit: (1) an application form; (2) the contract signed by and between the network operator and the receiver; (3) an assessment report on the security risks for PI cross-border transmission and the relevant security measures; and (4) other materials required by CAC. Although operators are encouraged to refer to relevant regulations and guidelines in order to minimize regulatory risks, they still face the problem that no rules to follow in terms of specific obligations and procedures. Considering the rapid development of legislation on PI protection and its importance to national security, in the absence of clear guidance, it is advisable for multinational company to conduct the assessment of security risks for PI cross-border transmission and the relevant security measures before the cross-border transmission of PI, and keep the report of such assessment.

2.2 Preconditions for PI Cross-border Transmission

Due to the irreversibility of the flow of PI, the PIPL adopts a pre-supervision approach for the cross-border transmission of PI. Article 38 of the PIPL provides that where it is necessary for personal information to be provided by a personal information processor to a recipient outside the territory of the People's Republic of China due to any business need or any other need, at least one of the following conditions shall be met:

i. Where a security assessment organized by the national cyberspace authority has been passed in accordance with Article 40 of this Law;
ii. Where a certification of personal information protection has been given by a professional institution in accordance with the regulations of the national cyberspace authority;
iii. Where a contract in compliance with the standard contract provided by the national cyberspace authority has been concluded with the overseas recipient, establishing the rights and obligations of both parties; or
iv. Where any other condition prescribed by law, administrative regulations or the national cyberspace authority is met.

Security assessment or certification of PI protection shall be organized and arranged by the national cyberspace administration. As mentioned above, the relevant rules of security assessment are still in the consultation stage, and there is no reference to the certification of PI protection by professional institutions, which may be further clarified by CAC. Therefore, "enter into a contract with the overseas receiver" is a condition which is relatively practical and easy to satisfy. When conducting PI cross-border transmission, a multinational company shall require its domestic and overseas companies to enter into a contract to stipulate the rights and obligations of both parties with respect to PI processing and protection.

3. Other Requirements for PI Cross-border Transmission

Article 43 of the PIPL also stipulates the "principle of reciprocity" in PI cross-border

transmission. Any country or region that takes any discriminatory prohibition, restriction, or any other such measure against China in respect of personal information protection may be subject to reciprocal measures taken by China depending on the actual situation. Therefore, the PI cross-border transmission to such countries is likely to be restricted.

In addition, the formally passed PIPL has further improved the rules for PI cross-border transmission. Where there is any stipulation on the condition or any other stipulation for the provision of personal information to a recipient outside the territory of China in any international treaty or agreement concluded or acceded by China, such stipulation may apply. Meanwhile, the PIPL requires PI processors to take any necessary measure to ensure that the activities of the processing of the personal information provided by them carried out by overseas recipients meet the standards of personal information protection provided in this Law. We understand that such provision resolves the conflicting provisions in different jurisdictions regarding the cross-border transmission of PI, but at the same time, it impose the substantial obligation of cross-border transmission on domestic PI processors, which indirectly achieves the extraterritorial effect of the PIPL.

Annotation

[1]Article 3 of GDPR:

This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

[2]Sensitive personal information refers to personal information that, once leaked or illegally used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a natural person, including biometric recognition, religious belief, specific identity, medical and health, financial account, personal whereabouts, and other information of a natural person, as well as any personal information of a minor under the age of 14.

QIN Ying
Partner of Lifang & partners
Practice Areas:
Compliance
yingqin@lifanglaw.com

XIAO Pulingling
Associate of Lifang & partners
Practice Areas:
Antitrust and Unfair Competition
pulinglingxiao@lifanglaw.com

Subscribe to our WeChat community

扫码关注公众号“立方律师事务所”和“竞争法视界”

北京 | 上海 | 武汉 | 广州 | 深圳 | 韩国

Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Korea

www.lifanglaw.com
Tel：+8610 64096099
Email：info@lifanglaw.com
Fax：+8610 64096260/64096261