汉坤法律评述

2021 年 4 月 30 日

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

千呼万唤始出来：简评《个人信息保护法（草案）》与《数据安全法（草案）》二次审议稿

作者：段志超 | 蔡克蒙 | 王雨婷 | 胡敏喆[1]

2021 年 4 月 30 日，十三届人大常委会在万众瞩目下公布了《个人信息保护法（草案二次审议稿）》与《数据安全法（草案二次审议稿）》。本文将简要评述这两部重要法律二审稿中的变化。总体而言，两部二审稿均沿用了一审稿中的整体框架和大部分规则（我们关于一审稿的解读文章详见《似曾相识-<个人信息保护法（草案）>浅析》、《简评<数据安全法>草案》），仅在具体规则上作出补充和优化。由此可见，立法者已对这两部立法的基本制度和大部分规则形成了广泛共识，其最终出台指日可待。

一、个人信息保护法二审草案

《个人信息保护法（草案二次审议稿）》（在本文第一部分，**“二审稿”**指《个人信息保护法（草案二次审议稿）》）所规定的个人信息处理原则与规则与 2020 年 10 月公布的一审稿（在本文第一部分，**“一审稿”**指《个人信息保护法（草案一次审议稿）》）基本保持一致，并在一审稿基础上强化了个人信息处理者在人脸识别、委托处理、责任推定等方面的义务与责任，优化并完善了在个人信息处理法律基础、自动化决策和个性推送等方面的法律规则。二审稿还在一审稿基础上创造性地提出了死者个人信息权利行权、超级互联网平台监管等规定。此外，在广受跨国企业关注的数据跨境传输方面，二审稿基本沿用了一审稿确立的数据跨境传输多元监管路径，保障了企业跨境数据传输的便利。

（一）优化并完善个人信息处理原则与规则

二审稿第一章节与第二章节规定了个人信息处理应遵循的原则与规则，对处理者开展个人信息处理活动起到了提纲挈领的作用。二审稿基本保留了一审稿中的核心内容，并针对实践中个人信息收集环节不透明、过度收集与滥用、数据质量层次不齐等乱象，结合既往立法与执法实践，对个人信息处理原则进行了优化，具体而言：

- 明确不得通过误导、胁迫等方式处理个人信息（第 5 条）；
- 细化最小必要原则，要求采取对个人权益影响最小的方式处理个人信息（第 6 条）；
- 补充要求处理者公示处理的目的、方式和范围（第 7 条）；

[1] 实习生蔡诗萌对本文的写作亦有贡献。

- 数据“准确及时”要求提升为“保证数据质量”，明确应避免因个人信息不准确、不完整对个人权益造成不利影响（第 8 条）。

同时，草案第二稿进一步完善了个人信息处理规则，具体包括：

- 与《民法典》第 1036 条相衔接，增加合理范围内处理已公开的个人信息作为个人信息处理的合法性基础（第 13 条）；
- 与《个人信息安全规范》相衔接，增加规定，要求提供便捷的撤回同意方式且撤回同意不影响撤回前授权同意的效力（第 16 条）、要求针对自动化决策商业推送提供非针对个人特征的选项或拒绝的方式（第 25 条）；
- 公开个人信息（第 26 条）、基于非公共安全目的公开或共享公共场所收集的个人图像（第 27 条）等敏感场景必须获得个人单独同意，法律、行政法规的规定不再作为例外。

（二）个人信息跨境提供的规则基本保持不变

一审稿基于个人信息跨境风险差异的考量建立了多元的个人信息跨境传输机制。借鉴域外立法经验，二审稿就其中涉及的跨境传输协议提出了规范性要求，即跨境传输数据提供方应“按照国家网信部门制定的标准合同”签署跨境传输协议（第 38 条）。

统一的标准合同模板将进一步降低企业跨境传输个人信息的合规成本。根据目前二审稿的规定，对于非关键信息基础设施运营者且处理个人信息未达到法定数量的运营者，最为便捷的个人信息出境流程系在完成高风险个人信息处理活动事先内部风险评估[2]、获得个人单独同意、并签署标准合同后，向境外提供个人信息。

第 40 条项下规定的“达到一定数量”是非关键信息基础设施运营者是否需要履行更严格的数据跨境传输合规义务的分界线。这一条款自一审稿颁布以来一直广受热议。目前，二审稿条款与相关的审议情况说明均未对此类运营者的具体数量标准和认定规则作出进一步解释。我们期待监管机构在后续法规或标准中对此作出细化，为数据提供方提供更为明确的合规指引。

（三）创造性提出死者个人信息权利由其近亲属行使

根据二审稿第 49 条规定，自然人死亡后，其在个人信息处理活动中的权利（即知情、决定、查阅、复制、更正、删除等权利）由其近亲属行使。

该条款与《民法典》第 994 条相衔接，旨在允许死者近亲属在死者姓名、肖像、名誉、隐私等受到侵害时，要求个人信息处理者履行义务、承担责任。目前，学界尚未就死者继承人是否针对死者个人信息享有继承权达成共识。在此背景下，第 49 条的规定实属超前。诚然，该条规定可以在一定程度上协助死者近亲属捍卫死者的合法权益，但不区具体场景而允许死者近亲属行使个人信息访问权是否会引发额外的隐私问题值得进一步探讨。此外，该场景下的行权主体、行权方式也有待在实践中进一步明确。

（四）创设超级互联网平台外部监督机制

二审稿第 57 条针对超级互联网平台的个人信息处理义务提出了特殊规定。针对提供基础性互联网

[2] 第 54 条，个人信息处理者应当对下列个人信息处理活动在事前进行风险评估，并对处理情况进行记录……（四）向境外提供个人信息……

平台服务、用户数量巨大、业务类型复杂的个人信息处理者，其应按照二审稿要求：

- 成立主要由外部成员组成的独立机构，对其个人信息处理活动进行监督；
- 针对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；
- 定期发布个人信息保护社会责任报告，接收社会监督。

目前，超级互联网平台因其庞大的业务规模掌握海量的用户数据，其合规经营关系到广大社会的公共利益，二审稿第 57 条一方面要求平台对平台内产品和服务提供者的个人信息保护承担起“守门人”责任（例如近期公布的《移动互联网应用程序个人信息保护暂行规定》草案征求意见稿对 APP 分发平台、移动智能终端生产企业个人信息治理责任的规定即体现这一思路，参见*《移动互联网应用程序个人信息保护暂行规定》（征求意见稿）*），另一方面通过外部监督机制保障并增强超级平台的个人信息处理合规水平。同时，数据垄断与数据滥用也是平台反垄断治理的重点与难点，二审稿这一规定亦可被视为数据监管领域针对平台反垄断治理作出的回应。

（五）明确个人信息受托处理者的合规义务

二审稿保留了一审稿中“个人信息处理者”这一概念，并未区分个人信息控制者与处理者。针对因此造成的义务界限模糊，二审稿第 58 条明确了个人信息委托处理受托方的义务。

接受委托处理个人信息的受托方，应当履行二审稿第五章项下的个人信息处理者义务，具体包括：

- 采取内部安全管理措施（第 51 条）；
- 完善个人信息保护组织架构，包括指定个人信息保护负责人并公布其联系方式（第 52 条），设置境内专门机构或指定代表（第 53 条，针对境外处理者）；
- 定期针对个人信息处理活动进行合规审计（第 54 条）；
- 针对特定处理活动开展事前风险评估（第 55 条）；
- 妥善处理个人信息安全事件并依法履行上报义务（第 56 条）。

值得注意的是，二审稿并未明确要求受托处理者履行“第二章 个人信息处理规则”或“第四章 个人在个人信息处理活动中的权利”项下的个人信息处理者义务。我们认为，这一条款可以解释为，取得个人的同意（第 23 条）、公布个人信息处理规则（第 18 条）、个人信息共同处理者承担连带责任（第 21 条）、处理个人行权申请（第 50 条）等《个人信息安全规范》项下个人信息控制者应承担的合规义务将不适用于受托处理者。

（六）连带责任与过错推定责任原则将增加个人信息处理者的民事责任风险

二审稿第 21 条将“个人信息共同处理者侵害个人信息权益的，‘依法’承担连带责任”修订为“应当”承担连带责任，这一文字调整将个人信息共同处理者牢牢绑定在一起。在互联网业务模式日趋复杂的大背景下，单一业务场景或数据处理活动可能涉及多个个人信息处理者。未来，开展合作的个人信息处理者之间，不仅应通过数据处理协议就其内部权责划分进行划定，更应采取审计等管控措施，就对方的个人信息保护措施进行实质性监督。

二审稿第 68 条规定，处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。考虑到个人信息处理者一般为企业，相对于个人而言具备显著的技术与信息优势，这一规定将缓解个人信息主体

因举证困难而无法主张侵权责任救济的困境，存在合理性。早在 2017 年庞某某与某网络订票平台、航空公司等隐私权纠纷上诉案等一系列案例中，法院已经已采取类似裁判规则。但不可否认，客观上该规定将增加企业承担民事责任的风险。个人信息处理者应在日常经营过程中注意留存操作记录与必要数据，以避免在民事诉讼中承担不利后果。

二、数据安全法二审草案

《数据安全法（草案二次审议稿）》（就本文第二部分而言，**“二审稿”**指《数据安全法（草案二次审议稿）》）同样沿用了 2020 年 7 月公布的《数据安全法（草案一次审议稿）》（就本文第二部分而言，**“一审稿”**指《数据安全法（草案一次审议稿）》）的规定，但强化了在数据分级分类、重要数据监管、数据跨境流动方面的监管。二审稿值得关注的主要要点如下。

（一）国家建立数据分级分类制度

二审稿第 20 条规定国家建立数据分类分级保护制度，分级分类的标准仍是“数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度”。此处重点强调分级分类制度的主体是国家，而非像此前《网络安全法》第 21 条[3]和《科学数据管理办法》、《证券基金经营机构信息技术管理办法》等行业领域法规要求网络运营者自行对数据进行分级分类管理。这意味着数据分级分类保护制度可能被上升到国家数据保护基本制度的高度，类似于“网络安全等级保护制度”在网络安全保护领域的制度地位[4]。各地区、各部门亦将以此为依据，全面开展本地区、本部门及相关行业或领域数据分级分类保护工作。

（二）重要数据及其出境管理制度

除数据分级分类保护制度外，二审稿第 20 条还新增规定国家将确定重要数据目录。各地区、各部门亦将依据数据分级分类保护制度确定本地区、本部门及相关行业或领域重要数据目录，对列入目录的数据进行重点保护。重点保护沿用了一审稿所规定的义务，包括，重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任（第 26 条）；并按规定对其数据处理活动定期开展风险评估，向有关主管部门报送风险评估报告（第 29 条）。此外，对于受到广泛关注的重要数据出境方面，二审稿第 30 条新增规定关键信息基础设施运营者之外的其他数据处理者将境内重要数据传输出境，应当适用国家网信部门会同国务院有关部门制定的管理办法。这一规定将填补非关键信息基础设施运营者向境外提供重要数据监管审查方面的制度空白。

（三）境外机构数据调取

此前一审稿规定，境外执法机构要求调取存储于中国境内数据的，原则上需经中国主管机关批准后方可提供。二审稿第 35 条在此基础上增加境外司法机构调取境内数据，同样需要经过中国主管机关批准，否则不得提供。这一规定与《国际刑事司法协助法》第 4 条[5]及《民事诉讼法》第 277 条相衔接[6]，

[3] 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：……（四）采取数据分类、重要数据备份和加密等措施……

[4] 参见“网安寻路人”公众号，洪延青，《理解<数据安全法><个人信息保护法>二审稿的实质性修改内容（一）》。

[5] 非经中华人民共和国主管机关同意，外国机构、组织和个人不得在中华人民共和国境内进行本法规定的刑事诉讼活动，中华人民共和国境内的机构、组织和个人不得向外国提供证据材料和本法规定的协助。

[6] 未经中华人民共和国主管机关准许，任何外国机关或者个人不得在中华人民共和国领域内送达文书、调查取证。

填补了一审稿仅限制境外执法机构调取数据所可能带来的歧义和空白。更为重要的是，二审稿新增第46 条明确规定境内组织、个人违反规定未经主管机关批准提供向境外执法机构、司法机构提供境内数据，可能被责令整改、警告并处 10 万元以上 100 万元以下罚款，直接负责主管人员和其他直接责任人员可能被处以 2 万元以上 20 万元以下罚款。填补了此前《国际刑事司法协助法》、《民事诉讼法》、《证券法》[7]等未明确规定违规向境外执法或司法机构提供数据的法律责任的漏洞，为有关组织、个人拒绝外国不合理要求提供更为充分的法律依据。

（四）法律责任强化

二审稿还从以下方面进一步强化了数据处理者的法律责任：

- 新增规定我国境内的组织和个人在境外开展数据处理活动，如侵犯国家安全、公共利益或者公民、组织合法权益的，同样依法追究法律责任（第 2 条）；
- 明确规定组织和个人拒不配合公安机关、国家安全机关的数据调取，除由有关部门责令整改外，还可能面临警告并处 5 万元以上 50 万元以下罚款，并可对直接负责主管人员和其他直接责任人员可能被处以 1 万元以上 10 万元以下罚款（第 46 条）；
- 违反数据安全管理制度、数据安全风险监测与应急处置制度、重要数据处理风险评估制度、重要数据出境限制制度，拒不改正或造成大量数据泄露等严重后果的，处罚上限由原来的 100 万元提高至 500 万元（第 44 条）。

[7] 境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动。未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动有关的文件和资料。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com