汉坤法律评述

2021 年 8 月 21 日

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

北京 | 上海 | 深圳 | 香港

聚光灯下的新篇章 — 简评《个人信息保护法》

作者：段志超 | 蔡克蒙 | 王雨婷 | 胡敏喆

2021 年 8 月 20 日，万众瞩目的《个人信息保护法》正式发布，并将于 11 月 1 日生效。《个人信息保护法》将成为我国首部专门针对个人信息保护的系统性、综合性法律。

《个人信息保护法》最终稿（“**最终稿**”）在草案二次审议稿（“**二审稿**”）的基础上进一步强化了个人信息保护要求，完善了个人信息处理的合法基础，并在规制确保平台经济有序发展的大背景下，突出了针对“大数据杀熟”和“数据可携权”的规定，进一步加强了对个人信息主体权利和公共利益的保障。此外，在行政监管以外，最终稿也对个人诉权和公益诉讼的规定做出了进一步的强化，个人信息主体多元化的维权途径将进一步增强《个人信息保护法》的威慑。

但与此同时，最终稿也考虑了法规的可操作性和落地性，将人力资源管理纳入合法性基础的范围，增加了诸如“小型个人信息处理者”的概念，适度放宽了对公开个人信息的处理的限制，并在部分法规细节上结合具体场景进行了优化。

如果说《网络安全法》揭开了我国个人信息保护工作的大幕，《个人信息保护法》则将个人信息保护工作带入了一个新纪元，其基础性的制度构建以及广泛的适用范围将对包括网络零售、人工智能、自动驾驶、医疗健康、物联网在内的数字社会带来深远的影响。

下文我们将结合最终稿的主要变化，对《个人信息保护法》的内容进行分析与解读。

一、最终稿对二审稿的核心修订

《个人信息保护法》最终稿对二审稿的核心修订包括：

- 完善个人信息处理的合法基础，将人力资源管理所必需纳入合法性基础的范围，并进一步明确了处理公开信息这一合法性基础的适用范围；
- 点名“大数据杀熟”，强化对自动化决策的监管，保障个人获得公平交易条件的权利；
- 进一步将敏感个人信息的处理范围限定在“只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下”；
- 创设性新增个人信息“可携带权”，强化个人对其个人信息的控制权，保障个人信息在不同平台之间的自由流动；

- 强化移动应用程序监管；
- 首次提出了“小型个人信息处理者”的概念，为未来豁免小型企业特定个人信息保护义务奠定了规范基础；
- 保障个人诉权，明确处理者拒绝个人行使个人信息权利请求的可诉性；将消费者组织纳入公益诉讼体系。

二、人力资源和公开信息处理：个人信息处理的多元合法基础的进一步调整

《个人信息保护法》突破《网络安全法》将授权同意作为唯一合法基础的立法体例，新增若干处理个人信息的合法基础，包括“为履行个人作为一方当事人的合同所必需”、“为履行法定职责法定义务所必需”等，为处理个人信息提供更为多元的合法性基础。值得注意的是，多元合法性基础在缓解“知情同意”原则的僵化运用的同时，实质上提高了“知情同意”的要求，只有个人信息主体能够作出真实、有效选择时方可视为满足“同意”要求。

最终稿在二审稿的基础上，新增人力资源管理作为个人信息处理的合法基础，同时优化公开信息个人信息处理规则。

（一）人力资源管理

《个人信息保护法》对各类个人信息处理活动的普适性将此前《网络安全法》、《消费者权益保护法》等难以涵盖且在实践中未受到重视的员工个人信息纳入保护范围。最终稿第 13 条第 2 款则进一步明确将“人力资源管理”作为个人信息处理的合法性基础。但这一合法性基础受到严格限制，需为“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人力资源管理所必需”。

强调“按照依法制定的劳动规章制度和依法签订的集体合同”，一方面体现了立法者考虑到劳资关系中天然的不平等现状，试图严格限制员工个人信息的处理范围，防止企业以“人力资源管理”所需为由过度收集员工个人信息；另一方面，这一规定也为企业合规处理员工个人信息指明了方向，如果企业依据《劳动合同法》第 4 条经过必要民主程序制定内部劳动规章制度，根据规章制度收集必要的个人信息，则无需征得个人同意。

随着《个人信息保护法》的出台，未来企业需要像此前对待用户个人信息一样，重视员工个人信息保护。我们建议企业抓紧完善内部劳动规章制度，增加员工个人信息保护相关内容。企业还应重视完善员工的个人信息权利行使机制，因为《个人信息保护法》赋予个人信息主体广泛的权利未来或许将成为劳动纠纷之中员工手中的一把“利器”。

（二）处理公开的个人信息的规则

《个人信息保护法》最终稿第 27 条允许个人信息处理者“在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意”。修订后的本条表述与《民法典》第 1036 条第 2 款[1]更为一致。据此，企业如希望使用从公开渠道收集的个人信息，应注意选择个人信息主体自行公开或其他合法公开的信息来源（例如各类政府网站依法公开的相关信息、公开新闻报道中的信息）。

[1] 第一千零三十六条处理个人信息，有下列情形之一的，行为人不承担民事责任……（二）合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外。

此外，对于处理已经公开的个人信息的方式，最终稿第 27 条大幅简化了此前审议稿中规定的“判断公开时的用途”或者“在用途不明确时，合理、谨慎地处理个人信息”的内容和要求。但处理已公开个人信息仍需以“合理”为限，在判断“合理”范围时，应考虑个人信息被公开时的用途、个人的隐私期待、使用公开信息对个人权益的影响等因素，具体标准仍有待监管执法与司法裁判所明确[2]。

三、大数据杀熟和个性化营销：自动化决策的规范和限制

根据《个人信息保护法》第 73 条，自动化决策是指“通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动”。自动化决策常用于信息推送、商业营销、资信评审、求职者适格性评估、员工绩效考核评估等。对于自动化决策，《个人信息保护法》第 24 条要求：

(1) 应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

(2) 通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供**便捷**的拒绝方式。

(3) 通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

（一）大数据杀熟

前述第（1）款主要针对广受非议的“大数据杀熟”。“大数据杀熟”一般指平台针对具有购买记录的“熟客”、通过大数据分析判定为价格不敏感的用户、以及其他特定人群，采取不同定价策略的行为，且往往导致“熟客”的价格比“新客”更高。

在《个人信息保护法》最终稿颁布前不久，国家市场监督管理总局先后出台了《价格违法行为行政处罚规定（修订征求意见稿）》[3]、《禁止网络不正当竞争行为规定（公开征求意见稿）》[4]等规章，分别从价格歧视、网络不正当竞争等角度，试图针对类似侵犯消费者知情权、公平交易权的行为进行规制。《个人信息保护法》更是从法律的层面对使用用户个人信息进行差异化定价作出规制。

值得注意的是，我们认为第 24 条并非绝对禁止企业利用用户画像进行差异化定价（例如对一些新客、不活跃客户提供更便宜价格或作出优惠补贴），而是强调该等技术的应用不应导致不公平的结果。但差异化的销售策略与侵害个人权益的“大数据杀熟”二者之间的界限究竟在哪里，这一问题值得行

---

[2] 例如，在 2019 年北京互联网法院审理的一起人格权纠纷案件中，原告发布在校内社群社交网站的证件照被置顶在头部搜索引擎的图片搜索结果中。法院以信息发布平台的性质作为判断标准，认为原告在社交网站内发布信息的目的在于特定人群范围内的社交，而非发布全网公开信息。在另一起案件中，原告主张网站转发裁判文书网公开的判决书，侵犯其个人隐私等权益。在这一案件中，法院平衡了公共利益和社会经济利益与个人利益之间的关系，从公开信息利用形式、目的等角度进行判断，认为被告网站并未对裁判文书网公开的判决书内容进行不当篡改，亦未以收集自然人征信、窥探个人隐私等不当目的进行数据匹配和信息处理。网站转载目的不违背司法公开的目的，最终没有支持原告的诉讼请求。而在杭州某公司侵害消费者依法得到保护的个人信息权利案件中，执法机关认为当事人利用从企查查、企信宝等 APP 收集的个人信息资料开展营销活动未经本人同意，侵害消费者依法得到保护的个人信息权利。

[3] 《价格违法行为行政处罚规定（修订征求意见稿）》第 13 条（一）电子商务平台经营者利用大数据分析、算法等技术手段，根据消费者或者其他经营者的偏好、交易习惯等特征，基于成本或正当营销策略之外的因素，对同一商品或服务在同等交易条件下设置不同价格的。

[4] 《禁止网络不正当竞争行为规定（公开征求意见稿）》第二十一条规定，经营者不得利用数据、算法等技术手段，通过收集、分析交易相对方的交易信息、浏览内容及次数、交易时使用的终端设备的品牌及价值等方式，对交易条件相同的交易相对方不合理地提供不同的交易信息，侵害交易相对方的知情权、选择权、公平交易权等，扰乱市场公平交易秩序。交易信息包括交易历史、支付意愿、消费习惯、个体偏好、支付能力、依赖程度、信用状况等。

业进一步探讨。

（二）个性化营销

前述第（2）款主要适用于“信息推送”（例如各类视频、文章等内容产品推送）和“商业营销”。过去一年多来，“定向推送”、“个性化展示”已经逐步成为监管机构执法重点，关注要点由是否向用户提供不针对个人特征的选项或是否提供关闭或拒绝机制，逐步深入到关闭、拒绝机制的真实有效性[5]。企业在利用用户个人信息开展个性化展示、定向推送时，应注意尊重个人信息主体知情权（例如在隐私政策中告知、明显标识区分个性化与非个性化内容）和选择权（确保用户可以拒绝个性化内容）。

（三）对个人权益有重大影响的决定

前述第（3）款的适用强调“对个人权益有重大影响的决定”，从欧盟的立法与执法经验来看，对个人权益有重大影响包括造成对个人的歧视待遇、拒绝交易或雇佣机会、作出奖惩决定甚至作出有法律影响的决定[6]。对于此类自动化决策，个人享有“绝对的知情权”，即有权要求个人信息处理者予以说明，和“相对的拒绝权”，即仅在相关决定仅依据自动化决策作出，无人工干预的情况下，个人有权拒绝该等决定。“绝对的知情权”带来的问题是“要求个人信息处理者予以说明”和第 48 条的“解释权”之间的关系应作何理解，以及个人信息处理者需说明的范围。后者可能进一步涉及到算法解释的范围（例如是否涵盖基本原理解释、责任解释、数据解释、公平性解释、安全和性能解释、影响解释等维度）、如何确保解释的可理解性等更为复杂的问题。

四、敏感个人信息处理：单独同意是否是唯一合法基础？

《个人信息保护法》最终稿第 28 条重申了《GB/T 35273 信息安全技术 个人信息安全规范》的分类，认定不满 14 周岁未成年人的个人信息属于敏感个人信息，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

值得注意的是，最终稿第 29 条删除了“基于个人同意处理敏感信息”相关表述，仅约定“处理敏感个人信息应当取得个人的**单独同意**，法律、行政法规规定处理敏感个人信息应当取得**书面同意**的，从其规定。”

对于这一修订，可能存在两种解读。一方面，可以解读为“单独同意”是处理敏感个人信息的唯一合法基础。另一方面，处理敏感个人信息仍可视情况适用第 13 条规定的不同合法基础（但需要满足具有特定的目的和充分的必要性，并采取严格保护措施的条件），仅在基于同意处理敏感个人信息时，“同意”的形式应符合更高的要求。

我们倾向于认为后一种解读更为合理。这主要是考虑到我国数据法体系下敏感个人信息相对宽泛的定义以及《个人信息保护法》的整体立法思路。具体而言，《个人信息保护法》第 14 条、第 15 条统一约定了基于个人同意处理个人信息时的特别要求，例如同意的标准（自愿、明确、知情）、基于同意处理个人信息时的专门权利（撤回权），而全文其他提及“同意”的条款则不再专门说明“基于个人同意”的处理。

这里另一个值得探讨的是何为“单独同意”。这个问题自《个人信息保护法》一审稿以来一直未得到澄清。从域外经验来看，《欧盟通用数据保护条例》（GDPR）同样区分“普通”的授权同意与“明确同意”（explicit consent）。GDPR 项下的同意，应满足“自愿”（freely given）、“特定”（specific）、“知情”

[5] 近期，定向推送时提供虚假关闭按钮也已被纳入工信部互联网行业专项整治行动的范围“工信部启动互联网行业专项整治活动”，访问地址：https://mp.weixin.qq.com/s/GZkFr4DVxPPRvp0_RP8mAQ。

[6] 例如在美国日益广泛应用的利用算法辅助法官作出假释决策及提供量刑参考的实践。

（informed）、“明确”（unambiguous）四个条件[7]，强调同意针对特定数据处理行为，而非与能否使用产品或服务相绑定。对于处理个人敏感信息之一的“明确同意”，需在满足这四个条件的基础上，强调数据主体作出同意的方式必须是“明确”的[8]。《个人信息保护法》生效后，企业可以借鉴 GDPR 的经验完善相关的“单独同意”机制。

五、可携带权：有待本地化的他山之石

《个人信息保护法》第四章规定个人享有知情权、决定权、限制或拒绝权、查阅复制权、更正补充权、删除权、解释权。《个人信息保护法》最终稿在二审稿基础上创设性新增：“个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。”这一权利借鉴了欧盟 GDPR 所创设的著名的数据可携带权，旨在解决用户与大平台“绑定”的问题，增加用户在同类产品不同平台之间的流动性，在保护用户选择权的同时有效促进市场竞争。

可携带权在后续规章制定中如何细化，企业应如何应对新增的“可携带权”，GDPR 的经验无疑可资借鉴。GDPR 第 20 条赋予了数据主体数据携带权（right to data portability），在特定情形下，数据主体有权获得或指示控制者向另一控制者转移其提供的相关个人数据，该等个人数据应是经过结构化的、普遍使用的和机器可读的。根据 GDPR 的规定及相关指引[9]：

- **权利行使是有前提条件的：**即数据处理是通过自动化方式实现的，并且是基于数据主体授权同意或履行合同目的而作出的。换言之，基于其他合法基础处理的数据（例如为履行法定职责或者法定义务所必需），控制者无义务响应数据携带权的行权请求。
- **行权范围是有限的：**GDPR 项下可携带权的范围限定为“提供”的数据。但欧盟监管机构倾向于广泛解释“提供”的范围，包括控制者观察用户行为获得的个人数据，如活动日志、网站浏览记录，但不包括数据控制者通过后续分析用户数据或用户行为而创造的数据，例如用户画像。
- **数据格式的要求：**GDPR 强调，数据控制者提供的数据应是结构化的、普遍使用的和机器可读的。如果行业没有通用格式，指引鼓励数据控制者应使用常用的开放格式，如 XML、JSON、CSV，且使用合适的元数据。
- **是否可以收费：**原则上不允许收费，但当数据主体的请求没有正当理由或超出合理限度（unfounded or excessive），可以收取合理费用，但应立即告知数据主体费用收取事项。
- **是否可以拒绝：**原则上，控制者不能以技术或成本障碍为理由拒绝响应数据主体的行权请求。仅因为响应成本过高，很难认定为数据主体的行权请求是超过合理限度的。此外。由于目前行业内多以自动化方式处理数据，技术障碍恐怕也很难成为拒绝的数据主体的理由。

目前，《个人信息保护法》最终稿并未明晰“可携带权”的行使条件，而是交由网信部门制定相关规则。我们认为，是否可以在商业实践中真正落实、以及如何落实“可携带权”，一方面取决于顶层制度设计，另

[7] GDPR 前言 32，“Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement。”

[8] EDPB《关于 GDPR 下同意的解释指南》（Guidelines 05/2020 on consent under Regulation 2016/679）。

[9] 第 29 工作组《关于 GDPR 下数据可携带权的解释指南》（Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01）。

一方面也依赖于企业的有益探索。只有制度设计与产业实践相结合，才可以同时兼顾个人信息主体的权利与企业的经营成本。

六、应用程序相关责任和小型个人处理者：个人信息保护监管执法的“一增一减”

最终稿第 61 条、第 62 条分别对履行个人信息保护职责部门的个人信息保护职责做出了“一增一减”的规定，即强化移动应用程序监管，同时试图为小型企业减轻合规义务。

（一）“一增”：第 61 条、第 66 条新增应用程序测评作为个人信息保护部门的工作职责，并匹配罚则

《个人信息保护法》最终稿第 61 条将“组织对应用程序等个人信息保护情况进行测评，并公布测评结果”纳入个人信息保护部门的工作职责。相应地，第 66 条特别规定，“违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，**对违法处理个人信息的应用程序，责令暂停或者终止提供服务……**”。

上述规定为监管机构近两年多的 APP 监管执法提供了更为明确的上位法依据，也将为此前已经发布征求意见稿的《移动互联网应用程序个人信息保护管理暂行规定》的最终落地奠定基础。不可忽视的是，测评已逐渐成为 APP 监管的重要手段之一。

值得探讨的是，APP 测评规则是否可以代替法律适用、测评结果是否可以代替法律判断？我们认为，APP 测评是一项高效、便捷的合规工具，为近年来个人信息保护水平提升贡献显著，但同时我们也呼吁避免僵化使用 APP 测评工具，而是应结合具体场景具体判断 APP 收集、使用个人信息的合理性。

（二）“一减”：第 62 条规定小型个人信息处理者将适用专门的个人信息保护政策

《个人信息保护法》二审稿规定，国家网信部门将针对处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准。最终稿在此基础上新增“小型个人信息处理者[10]”。

如何避免个人信息保护立法对小型企业造成过于严苛的合规负担，不合理的增加其运行成本，避免遏制创新，一直是许多域外立法所关注的重点。而最终稿令人欣喜地对此问题做出了回应。我们预计，未来监管机构或将制定后续规章豁免一些个人信息保护规定对小型企业的适用。

这一规定在域外法中也有迹可循。例如：美国《加州消费者隐私法案》（CCPA）从营收额、收入来源、个人信息数量等方面明确了 CCPA 规制的企业范围，只有那些年营收额达到 2,500 万美元、或者处理个人信息达到 5 万条、或者出售个人信息带来 50%年营收额的公司才受到 CCPA 的管辖。而 GDPR 第 30 条则原则上豁免了雇员少于 250 人的企业或组织记录个人信息处理活动的义务。

七、个人诉权和公益诉讼：个人信息相关诉讼的应对

最终稿第 50 条在二审稿基础上增加了“个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼”。这一规定明确了个人对个人信息处理者拒绝个人信息主体行使其根据《个人信息保护

[10] 《个人信息保护法》第 62 条：国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作……（二）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准。

法》所享有的知情权、决定权、限制拒绝权、查阅复制权、可携带权、更正权、删除权、解释权等一系列权利的诉权，将丰富侵犯个人信息权利相关民事诉讼的类型。

此外，最终稿第 70 条亦将法律规定的消费者组织增加为可以依法就个人信息相关违法事项提起公益诉讼的组织。

上述和诉权相关的规定无疑将和《电商法》以及《消费者权益保护法》一起，为个人信息侵权相关的诉讼提供更多的途径。企业未来在应对监管执法的同时，将可预期地面临陡增的来自个人及国家机关、消费者保护组织等个人信息保护诉讼方面压力，如何就此进行应对将是对相关企业的现实挑战。

八、总结及展望

尽管监管机构在近两年明显加强了个人信息保护的监管执法力度，个人信息相关诉讼也日趋频繁，但在《个人信息保护法》出台之前，个人信息保护因法律基础不足而受到较大限制。这体现在：

- 个人信息保护领域受限，此前以《网络安全法》、《消费者权益保护法》为主的个人信息保护立法，主要针对网络服务、消费者保护场景，无法涵盖线下个人信息收集、特别是员工个人信息保护场景；
- 执法力度偏弱，执法活动虽然频繁，但大多以公告、警告或小额罚款为主；
- 个人权利有限，个人信息主体的权利主要集中在知情、查阅、更正、删除等领域，其他个人信息主体权利缺乏上位法依据，个人诉权保护不足。

《个人信息保护法》的规定则解决了上述问题，对所有个人信息全生命周期的合规要求、个人信息主体权利、监管机构的分工与合作、个人诉权与公益诉讼、域外适用效力与个人信息跨境传输等做出了系统性规定，并大幅提升了执法处罚的力度。此后，个人信息保护工作的复杂程度、执法力度和诉讼频度无疑将显著增加。

值得注意的是，《个人信息保护法》从公布到生效仅预留了两个多月时间，这反映了立法者对这部法律早日投入使用的迫切期盼，但这么短的准备时间对企业及行业从业者而言无疑是巨大挑战。就此，我们建议各行业企业均应高度重视个人信息保护工作，全面梳理本企业个人信息处理情况，建立健全个人权利保护机制，以避免出现重大合规风险问题；同时我们也期望监管机构能够循序渐进的推进个人信息保护执法工作，为企业和从业人员提供一定学习、适应新法的时间，以达到个人信息保护、产业良好发展和市场稳定运行之间的有机平衡。

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