信息权益保护、处理行为规范与信息合理利用

“三轮驱动”下的《个人信息保护法（草案）》

张继红

- 《个人信息保护法（草案）》构建了差异化、有重点、分层次的个人信息保护机制；聚焦个人信息处理者的行为及义务规范，补强个人信息权益保护，建构双向互动的信息保护屏障；完善个人信息处理的合法性事由；建立了个人信息跨境提供制度。
- 针对信息业的复杂环境，在十八周岁以内普遍予以特殊保护的同时，应当根据不同的应用场景进行精细化立法，采用年龄分段并结合个人信息的类型，区别设计不同年龄阶段的保护制度，对低龄未成年人严格保护，对高龄未成年人则在最大限度内给予其自主决定权。
- 对于图像、身份识别信息采集等设备的安装应当确立严格明确的程序，通过相应的必要性审查。同时，也应注意到，如果存在的维护公共安全的必要性事由消失，应当确立拆除或停用相关设备的“退出机制”，以保护个人隐私和信息安全。

2020年10月21日，《个人信息保护法（草案）》（简称“《草案》”）由十三届全国人大常委会第二十二次会议审议后公布并向社会公开征求意见。根据各方提出的意见，2021年4月《草案》二次审议稿做了部分调整和修改。从内容上看，《草案》系我国首次对个人信息进行的专项立法，全面、系统梳理了《民法典》《网络安全法》《消费者权益保护法》等已有法律规范的相关规定，设定了个人信息保护所应遵循的基本原则及标准，明确了个人信息处理者的行为规范、义务及法律责任，赋予了个人在信息处理活动中的权利，厘清个人信息保护部门的监管职责和权限，推动形成政府、企业、行业组织、社会公众共同参与的个人信息保护体系。

《草案》的体例和特点

从体例结构上看，《草案》包括总则、个人信息处理规则、个人信息跨境提供、个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门、法律责任、附则共八章，对于当下民众所关切的突出问题，如个人信息的过度采集及滥用、公共场所人脸识别技术的应用、敏感个人信息的处理、个人信息跨境传输等都作出了及时回应。

第一，构建差异化、有重点、分层次的个人信息保护机制。

《草案》针对不同主体、不同的信息类别制定了不同的处理规则，充分考虑了不同场景下个人信息处理的特殊性，突出了敏感个人信息、国家机关以及互联网头部企业的处理规则及义务，旨在构建差异化、有重点、分层次的个人信息保护体制。

在个人信息的类别上，区分了一般个人信息与敏感个人信息。设立专节规定敏感个人信息的处理规则，对敏感个人信息的处理设立更严格的标准和要求，不仅界定了哪些个人信息属于“敏感个人信息”，还强调个人信息处理者仅在“具有特定的目的和充分的必要性”前提下方可处理敏感个人信息，基于同意处理敏感个人信息应当取得个人的单独同意或者书面同意。

在个人信息的处理主体方面，对国家机关的处理行为进行了特别规定。国家机关处理个人信息具有公益性、职权性等特点，与其他法人及非法人组织处理个人信息的商业性、自治性存在显著差异。鉴于此，《草案》设立专节规定了国家机关处理个人信息规则。其中，第35条强调了国家机关履行法定职责处理个人信息，通常情形下遵循“告知同意”规则，但法律、行政法规规定应当保密，或者告知同意将妨碍履行法定职责的除外。

同时，《草案》要求国家机关处理的个人信息应当在境内存储，确需向境外提供的应当进行风险评估。值得注意的是，《草案》强调了国家机关履行法定职责处理个人信息，应依据法定权限、程序，不得超出履行法定职责之所必需的范围和限度。该项内容切实回应了公众对公权力机关滥用其职权获取个人信息的担忧和焦虑。

不同于一般企业，处理海量用户信息的互联网头部企业实际控制甚至垄断了技术资源、技术环境和运营环境，理应承担更重的个人信息保护义务。《草案》不仅要求“达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人”，二审稿还特别增加了“提供基础性互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”，应当成立独立的个人信息处理活动的监督机构，及时下架平台内严重违法处理个人信息的产品或服务，并定期发布个人信息保护社会责任报告，接受社会监督。对拥有技术垄断优势的信息处理者施以特别义务，将监管机构的部分监管职责前置于头部企业，由此增设以互联网头部企业为核心的个人信息保护安全网。

第二，聚焦个人信息处理者的行为及义务规范，补强个人信息权益保护，建构双向互动的信息保护屏障。

从整个《草案》的构架来看，重点聚焦个人信息处理的行为及义务规范，同时确立了个人信息权益的赋权性安排，正是对现实生活中个人信息处理者（企业）与个人（用户）在个人信息控制和管理过程中技术、资金、人员等力量悬殊的矫正。用户虽然是个人信息所关联或标识的主体，数量众多，但其本身并无有效控制、管理及监督能力。基于此，《草案》不仅重点规范了个人信息处理行为，明确了信息处理者的告知义务、特殊情形下的单独取得个人同意情形（如敏感个人信息、个人信息的公开）、安全保障义务、事先的风险评估义务、个人信息泄露的补救义务等，还在《民法典》1037条基础上确立了知情权、决定权、限制及拒绝权、查询复制权、更正补充权以及删除权等，建构了“义务+权利”的双重保护屏障。

此外，二审稿还特别增加死者个人信息的保护，对于留存于个人信息处理者手中的“个人数字遗产”如何处理、由谁来行使权利进行了及时回应。需注意，欧盟GDPR并不适用于已故人士，但其成员国可以对死者个人数据的处理进行相应的规定。

第三，完善个人信息处理的合法性事由，为个人信息的合理利用预留空间。

应该说，个人信息上不仅附着了个体的人格尊严和自由，还承载着个人信息处理者的合法利益以及公共利益。具体而言，个人信息保护制度不仅仅是保护个人信息权益，也要促进个人信息的合理利用和流通。企业、政府及其他组织都有权基于法律规定或约定收集、处理个人信息。当公共利益的实现和维护需要使用个人信息时，如疫情下对确诊或疑似患者行踪轨迹信息的采集，获取为刑事侦查、起诉或审判所需的个人信息等，也可以不经同意直接使用。这不仅仅保护了社会其他主体的合法权益及公共利益之所需，还有利于直接或间接增进社会福祉。

《草案》第13条规定了个人信息处理的合法性事由，在强调取得个人同意的基础上，并未将其作为处理个人信息的唯一合法基础，而是采用列举方式规定了除同意之外的其他个人信息处理的其他合法性事由，即“为订立或者履行个人作为一方当事人的合同所必需；为履行法定职责或者法定义务所必需；为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；为公共利益实施新闻报道、舆论监督等行为在合理的范围内处理个人信息”。同时，为了衔接《民法典》第1036条个人信息免责条款的规定，二审稿还特别增加了“在合理范围内处理已公开的个人信息”这一项内容。应该说，《草案》在很大程度上放宽了个人信息处理的限制，为个人信息的合理使用提供了法律依据，进一步丰富了个人信息处理的合法性基础，一定程度上突破了“告知同意”为核心的个人信息处理规则，有利于促进个人信息保护与信息合理使用之间的平衡。

第四，建立了个人信息跨境提供制度，促进个人信息的有序跨境流动。

《草案》从法律层面对我国个人信息出境制度作出明确规定，解决了目前个人信息跨境传输规则的立法缺位问题。第38条规定了个人信息出境的四种法定情形：国家网信部门组织的安全评估；经专业机构进行个人信息保护认证；与境外接收方订立合同，约定双方的权利和义务，并监督其个人信息处理活动达到法律规定的保护标准；法律、行政法规或者国家网信部门规定的其他条件。对个人信息处理者的告知义务也作了详细规定，并要求取得个人单独同意。境外提供个人信息也属于必须进行事先风险评估的法定事项。同时，要求关键信息基础设施运营者、处理个人信息达到网信部门规定数量的个人信息处理者，应当本地化存储。由此可见，《草案》通过传输路径、义务性规范两个方面构建我国个人信息出境的基本规则，并未采用欧盟《通用数据保护条例》（GDPR）的“充分性保护”标准而对个人信息出境设置更高的流通壁垒，而是在严格规范信息跨境提供者义务的基础上，更加注重个人信息跨境传输路径上认证、合同等市场自治工具的使用，完全契合国际社会所遵循的促进个人数据跨境流动的立法主旨。

第五，设置了严格的行政、民事责任，形成个人、政府、社会多元救济机制。

面对新技术背景下个人信息保护面临的新问题、新形势，《草案》综合运用公力救济、私力救济、社会救济等多种手段以实现对个人信息的周延保护。

与欧盟GDPR相类似，《草案》根据情节轻重分两档规定了违法处理个人信息的行政责任：一般违法，处以责令改正、警告、没收违法所得，拒不改正的并处一百万元以下罚款；严重违法，处以责令改正、没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照等。同时，适用“双罚制”，不仅对违法处理个人信息的单位施以行政处罚，还对直接负责的主管人员和其他直接责任人员处以相应的罚款。

在民事责任方面，正是因为个人信息处理者与用户之间双方力量对比差异性明显，让个人举证证明信息处理者存在过错实在是勉为其难，《草案》开创性地引入了“过错推定责任”，将主要举证责任转移至个人信息处理者一方，即因个人信息处理活动侵害个人信息权益的，个人信息处理者如果不能证明自己没过错的，就应当承担损害赔偿责任，更加便利了个人诉权的实现。

与此同时，由于个体在自身维权能力及维权意识上的限制，其个人信息权益一旦遭到侵害难以实现有效救济，为此《草案》还专门引入“公益诉讼”制度，当个人信息处理者违法处理个人信息，侵害众多个人权益的情形下，人民检察院、履行个人信息保护职责的部门和国家网信部门确定的组织都可以依法向人民法院提起诉讼。该条明确了提起公益诉讼的主体以及适用条件，充分发挥司法机关、行政机关以及相关社会组织在个人信息保护上的积极作用，给予个人信息更加完备的救济保护。我国司法实践中已经出现了个人信息保护公益诉讼的相关案例。2021年4月，最高人民检察院发布“检察机关个人信息保护公益诉讼典型案例”，涉及互联网企业违法违规收集个人信息并进行消费欺诈等11个案件，有效监督了个人信息保护领域严重损害个人信息权益的活动，推动落实企业的主体责任，为个人信息保护的公益诉讼作出了有益探索。

《草案》的完善建议

虽然《草案》构建了我国个人信息保护的基本框架，但在具体细节上的规则设计还存在些许不足，主要表现在：

第一，个别原则过于泛化，并不能真正反映出个人信息保护制度的立法主旨，如公开、透明原则。从基本原则的本身涵义来看，是贯彻个人信息保护全过程的基本精神和准绳，对全局起到统帅引领的关键性作用。基本原则不应局限于个别领域或某个方面，有可能会以偏概全。公开、透明原则，又称为政策透明原则，将其作为基本原则的国家及地区并不多见，仅有我国澳门特区《个人资料保护法》专门规定了透明原则。但该原则与澳门信息监管制度中的“通知与许可”制度紧密联系，便于社会大众以及监管当局对于负责处理个人资料的实体的资料处理行为进行有效的监督和管理，也有利于当事人了解资料处理相关情况，及时行权。应该说，该项原则的引入有其特殊的应用场景，但并不能因此作为一项具有普遍性效力的基本原则。而且，对于处理规则的公开透明要求，在个人信息处理者的告知义务及个人信息权益中已有明确规定，即“处理规则应当公开，而且便于查阅和保存”“个人有权要求个人信息处理者对其个人信息处理规则进行解释说明”，不宜再做重复规定。

第二，未成年个人信息的保护规定过于简单、原则，并未与已有法律进行内容上的协调，无法满足现阶段对未成年人个人信息保护的实际需要。《草案》仅规定个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得其监护人的同意，并未考虑到不同年龄阶段未成年人的差异性要求，欠缺更为宏观、体系化的未成年人信息保护规则的构建。同时，本条内容应该注意与《未成年人保护法》相关规定的衔接。刚刚修订的《未成年人保护法》第76条规定，为年满十六周岁的未成年人提供网络直播发布者账号注册服务时，应当对其身份信息进行认证，并征得其父母或者其他监护人同意。也就是说，针对信息业的复杂环境，在十八周岁以内普遍予以特殊保护的同时，应当根据不同的应用场景进行精细化立法，采用年龄分段并结合个人信息的类型，区别设计不同年龄阶段的保护制度，对低龄未成年人严格保护，对高龄未成年人则在最大限度内给予其自主决定权。

第三，对于公共场所安装图像采集、个人身份识别设备等的限制性要求过于模糊，影响实际的执行效果。《草案》规定，在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。这里，“维护公共安全所必需”的认定标准和程序并不明确，极易出现实际操作中的滥用问题，直接侵害公民隐私权和信息权益，毕竟人脸识别信息属于敏感度较高的个人信息，需要设置更严格的保护要求。应该说，监控设备的推广普及，虽然在一定程度上对行政执法效率的提高、刑事案件的侦破以及居民的安全感的获得发挥着重要的促进作用，但这并不意味着其所保护的价值利益绝对优于隐私及个人信息。因此，对于图像、身份识别信息采集等设备的安装应当确立严格明确的程序，通过相应的必要性审查。同时，也应注意到，如果存在的维护公共安全的必要性事由消失，应当确立拆除或停用相关设备的“退出机制”，以保护个人隐私和信息安全。

（作者系上海政法学院教授）