《个人信息保护法(草案)》的明惑之思

作者：潘永建 | 朱晓阳 | 邓梓珊 | 王雪莹

【本文为通力合规团队对《个人信息保护法(草案)》解读系列文章第一篇，后续将推出更多系列精彩解读。】

聚焦世界范围的个人信息保护立法，欧盟的《通用数据保护条例》(General Data Protection Regulation，以下简称“GDPR”)于 2018 年 5 月 25 日正式生效，被称为“史上最严格”数据安全管理规定；美国最具有典型意义的州隐私立法《加利福利亚消费者隐私法案》(CCPA)也于年初生效，被称作美国“最严厉、最全面的个人隐私保护法案”。不胜枚举，世界各国均着力于制定个人信息相关法律，据联合国贸易和发展会议(UNCTAD)截至今年 4 月 20 日的统计，世界 194 个国家中已有 132 个拥有个人信息保护立法。[1]

我国自 2009 年刑法修正案(七)将非法出售个人信息的行为纳入规制开始，陆续已颁布《电信和互联网用户个人信息保护规定》《网络安全法》《信息安全技术 个人信息安全规范》(以下简称“《个人信息国标》”)《儿童个人信息网络保护规定》等，从法律、部委规章、国家标准等多个维度对个人信息权益进行保护。尽管如此，个人信息领域缺少一部专门的立法。近日，千呼万唤之中，《个人信息保护法(草案)》(以下简称“草案”)提请十三届全国人大常委会第二十二次会议审议，将全貌展现在公众眼前。本文将从草案的“**明**”(已解决的议题)和“**惑**”(正式稿有待解决的议题)两方面浅析草案。

一. 草案之“明”

1. 个人信息：采用“关联”(relating to)标准，外延有所限缩

《民法典》《网络安全法》《个人信息国标》等与个人信息相关的多部法律和政策对个人信息做出较为一致的

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

[1] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

定义，即“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特定自然人的各种信息”，而对于个人信息的列举多参考《个人信息国标》的附录 A。草案作为个人信息的专门法对个人信息亦作出定义：“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”。

对比可知，草案对于个人信息的描述与先前不同，草案的定义方式与欧盟 GDPR 中对于个人数据(personal data)的定义极为相似[2]。**参考欧盟法律的解读，我们认为相较于此前的定义，草案中个人信息的外延有所限缩。**根据英国数据保护监管机构信息专员办公室(Information Commissioner's Office, ICO)对于 GDPR 下个人数据的定义进行拆解，个人数据仅包括下述与自然人有关的信息: 1)从该等信息中能够直接识别出自然人或者仅凭该等信息自然人是可识别的；或 2)该信息与其他信息结合能够间接识别出自然人。[3]“与自然人有关”的表述要求个人数据不仅仅能识别自然人，更重要的是，它必须在某种程度上与自然人相关联，换言之，能够指向可识别自然人的数据可能不是该自然人的“个人数据”，因为该等数据不与自然人相关联。[4]

就现行个人信息的定义而言，由于法律法规未对“与其他信息结合”的程度作出规定，在现实操作中判断是否“能够与其他信息结合识别特定自然人”时往往须参考司法实践。**根据相关司法实践，我们理解法院对于“与其他信息结合”的程度的解释未超过我们对个人信息范围的合理期待。**例如在“陈明侵犯公民个人信息罪二审刑事判决书”中，苏州市中级人民法院将“邮箱账号密码”认定为“能够与其他信息结合进而识别特定自然人身份或者特定自然人活动情况”；类似地，温岭市人民法院将“号码归属地、号码持有人商业需求等信息”，昆山市人民法院将“以电话号码等方式显示的皮肤、妇产科等健康生理信息”认定为个人信息；相反地，“安徽美景信息科技有限公司、淘宝(中国)软件有限公司不正当竞争纠纷”中，浙江省高级人民法院对于“数据产品所涉及的网络用户行为痕迹信息，以及由行为痕迹信息推测所得出的标签信息”，均不认为具备能够单独或者与其他信息结合识别自然人个人身份的可能性。

基于此，我们认为草案关于个人信息的定义有所限缩，或许由此为企业自由收集使用与个人无关联的非个人信息提供了便利。当然，这仍有待于未来行政执法与司法判决的验证。我们建议企业如果在个人信息的识别中遇到模棱两可之处，还需保持审慎，确保在处理该等信息时具备合法性基础。

2. 长臂管辖：首次将效力延伸至境外主体在境外的活动

草案第三条首次将个人信息保护法律的效力延伸至境外主体在境外的行为，明确我国“长臂管辖”的适用情形。草案第三条规定，组织、个人在中国境内处理自然人个人信息的活动适用本法，在境外处理境内自然人个人信息的活动，有下述情形之一的，亦适用本法：

[2] GDPR:‘personal data’ means any information relating to an identified or identifiable natural person.

[3] Personal data only includes information relating to natural persons who:
- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

1) 以向境内自然人提供产品或者服务为目的;
2) 为分析、评估境内自然人的行为;
3) 法律、行政法规规定的其他情形。

根据《关于<中华人民共和国个人信息保护法(草案)>的说明》，草案在赋予个人信息保护法域外适用效力时，“借鉴有关国家和地区的做法”。欧盟无疑在该等“有关国家和地区”之列。根据欧盟数据保护委员会(European Data Protection Board，以下简称“EDPB”)的指南，判断 GDPR 的适用范围主要有两个标准：设立地标准(establishment criterion)以及“目标”标准(targeting criterion)。就“目标”标准而言，如果非欧盟实体的个人信息处理与“向欧盟境内的主体提供商品或服务”或“监控欧盟境内主体以及行为”相关的，那么 GDPR 便适用于该非欧盟实体的个人信息处理活动。

在草案上述条款的具体适用方面，《信息安全技术 数据出境安全评估指南(征求意见稿)》提出在判断网络运营者是否在中华人民共和国境内开展业务，或向中华人民共和境内提供产品或服务时，可参考是否使用中文、是否以人民币作为结算货币、是否向中国境内配送物流等因素。基于我国域外效力规定与欧盟“目标”标准的相似性，我们在此补充 EDPB 指南中列出的考量因素，供企业参考。满足越多下述所列的因素，GDPR 适用的可能性便越高。

1) 商品或服务提及欧盟或成员国;
2) 数据控制者向搜索引擎运营商付费以提升其商品或服务在欧盟境内的搜索效果，或者在欧盟境内进行市场推广或广告活动;
3) 相关活动的国际化属性;
4) 提及欧盟国家内的地址或电话;
5) 使用欧盟或其成员国后缀的顶级域名;
6) 提供从欧盟成员国到商品或服务提供地的路线信息;
7) 提及由住所地位于欧盟成员国的顾客组成的客户;
8) 使用一个或多个欧盟成员国的语言或货币;
9) 数据控制者提供向欧盟运送商品的服务。

3. 数据出境：建立分类分级个人信息跨境提供规则

数据出境制度一直是企业的合规关注重点。较之以往法规及其征求意见稿“雾里看花”似的规定，草案第三十八条和第四十条较为清晰地提出**分类分级制的个人信息跨境提供规则**:

1) 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处理者向境外提供个人信息的，应当通过国家网信部门组织的安全评估;(关于“国家网信部门规定数量”，预计国家网信部门后续会出台更为细致的规定，现阶段可参考《个人信息和重要数据出境安全评估办法(征求意见稿)》提出的“含有或累计含有 50 万人以上的个人信息”或“数据量超过 1000GB”)

2) 其他个人信息处理者向境外提供个人信息的，可选择由专业机构进行个人信息保护认证，或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规定的个人信息保护标准等。

除数据出境安全评估义务外，草案提出较现行法规更为严格的要求：个人信息处理者对于待出境个人信息的主体须履行告知并征得单独同意的义务；对因国际司法协助或者行政执法协助，需要向境外提供个人信息的，还须依法申请有关主管部门批准。基于此条的规定，企业在《个人信息保护法》出台后可能需要对个人信息保护政策(隐私政策)作出相应的修改，另外，**企业在未来还应关注国家网信部门发布的“限制或者禁止个人信息提供清单”以及我国采取反制措施的国家或地区**，如交易相对方被列入上述负面清单，或属于反制国家或地区内的企业或个人，企业向其传输个人信息的行为会受到一定程度的限制，甚至禁止。

4. 处理规则：知情同意不再是个人信息处理唯一合法性基础

值得一提的是，考虑到经济社会生活的复杂性和个人信息处理的不同情况，草案对基于个人同意以外合法处理个人信息的情形作出如下规定，这意味着知情同意不再是处理个人信息的唯一合法基础。

1) 为订立或者履行个人作为一方当事人的合同所必需；
2) 为履行法定职责或者法定义务所必需；
3) 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；
4) 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；
5) 法律、行政法规规定的其他情形。

以知情同意作为唯一的合法性基础存在很多缺陷，亦不是国际社会的通行做法。以 GDPR 为例，“为履行约定义务所必需”“为履行法定义务所必需”“为保护生命安全所必需”“为维护公共利益或行使公权力所必需”“为实现数据控制者或第三方的合法权益所必需”，与知情同意并列，均为处理个人信息的合法基础。

将知情同意作为个人信息处理必要条件的不足之处主要体现在两方面。[5]

1) 首先，这种机制可能导致个人信息所载社会价值的失衡。对数据处理者而言，绝对的知情同意会产生不合理的运营负担，而低成本的“默示同意”和格式合同又会让知情同意沦为形式。因性质的特殊，个人信息具有多重维度的价值，于个人信息主体而言，个人信息意味着人格尊严与自由；于数据处理者而言，个人信息可以带来经济与效率价值；于公共利益而言，个人信息的处理有益于公共利益及公共管理。基于此，以知情同意为唯一法律基础无疑忽视了个人信息于数据处理者和公共利益的意义，尤其在科学研究领域，知情同意原则可能会成为增进全民福祉的障碍。

[5]高富平：《个人信息使用的合法性基础—数据上利益分析视角》，《比较法研究》2019 年第 2 期

2) 另一方面，知情同意看似以个人信息主体的权益为核心考量，实际难以实现有效的保护。在很多生活场景中，个人信息主体由于处于弱势地位，无法出于自由意志给出同意的表示，例如 GDPR 便认为在雇员雇主关系中，雇员通常无法自由地作出“同意/不同意”的表示，因为他们会忧虑雇佣关系下，自己“不同意”的表示会带来不良的影响。此外，在需要高频次征得知情同意的情况下，个人信息主体可能不会对每一次请求仔细审查，这可能使得知情同意的效果大大折扣。

5. 个人生物识别信息：“为维护公共安全所必需”是公共场所合法采集的前提

因“未经同意强制收集个人生物识别信息”问题，2019 年底浙江理工大学特聘副教授郭兵作为消费者将杭州野生动物世界告上法庭，据悉，杭州野生动物世界系为了有效提高入园效率需要，将原指纹识别机器改为使用人脸识别。该案被称为“国内人脸识别第一案”，已于 2020 年 6 月开庭审理，目前尚未取得最终判决。

草案第二十七条对于人脸信息的采集和使用问题作出回应：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。所收集的个人图像、个人身份特征信息只能用于维护公共安全的目的,不得公开或者向他人提供;取得个人单独同意或者法律、行政法规另有规定的除外。草案的出台可能会对法院裁判该案起到指导性作用。

我国目前对包括人脸信息在内的个人生物识别信息的特别保护呈现出软法先行的特点。[6]《个人信息国标》提出收集个人生物识别信息前应单独告知并征得个人信息主体的明示同意；个人生物识别信息应与个人身份信息分开存储；原则上不应共享、转让等。金融领域技术标准《个人金融信息保护技术规范》将用户鉴别的个人生物识别信息列为敏感程度最高的 C3 类信息，在数据处理全生命周期以及网络安全方面采取更高标准的保护，例如金融业机构不应委托或授权无金融业相关资质的机构收集、不应委托第三方机构处理等。除此之外，个人生物识别信息的保护有赖于互联网公司的行业倡议和自律。软法不是终点，对个人生物识别信息的特别保护终究离不开硬法的托底，草案第二十七条即是个人生物识别信息保护在法律层面的萌芽。

二. 草案之“惑”

1. 同意标准：“默示同意”的实践是否符合知情同意的要求尚无定论

《网络安全法》要求网络运营者收集、使用个人信息应当经过被收集者同意，但并未规定该等“同意”的具体形式。草案规定个人信息处理者取得个人的“同意”则可以处理个人信息，但依然未对实践中采取何种“同意”形式方能符合法律的要求提供指引。

在法律缺位的情况下，国家标准层面《个人信息国标》对该问题尝试作出解答。《个人信息国标》第 5.4.a)条规定了收集个人信息需获得个人信息主体的“授权同意”；第 5.4.b)条规定，收集个

[6] 邢会强：《人脸识别的法律规制》，《比较法研究》2020 年第 5 期

人敏感信息前应征得个人信息主体的“明示同意”；定义部分明确提出，授权同意包括通过积极的行为作出授权(“明示同意”)以及通过消极的不作为而作出授权(如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域，意即实践中常见的“默示同意”)。由于《个人信息国标》的法律位阶不高，属于推荐性国标，我们认为，同意标准这类重要议题有必要通过法律条文加以明确。

2. 已公开的个人信息：“已公开”的判断标准有待商议

草案第二十八条对于处理已公开的个人信息的特殊场景作出单独的规定：个人信息处理者处理已公开的个人信息,应当符合该个人信息被公开时的用途；超出与该用途相关的合理范围的,应当依照本法规定向个人告知并取得其同意。个人信息被公开时的用途不明确的,个人信息处理者应当合理、谨慎地处理已公开的个人信息;利用已公开的个人信息从事对个人有重大影响的活动,应当依照本法规定向个人告知并取得其同意。

关于“已公开”这一条件的判断标准，草案留有讨论空间：“已公开的个人信息”是否要求该个人信息已被社会公众知悉，或已落入公有领域？受到侵害发生泄露的个人信息是否属于“已公开的个人信息”？是否默认某些个人信息属于“已公开的个人信息”？在没有明确说明“被公开时的用途”的情况下，该等用途又该如何认定？这些问题都有待正式法律的进一步明确。

3. 个人信息职责部门：专门个人信息保护机构尚未组建

草案第五十六条延续现有的机构设置，由国家网信部门负责个人信息保护工作和相关监督管理工作的统筹协调，由国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作。但草案并未借鉴欧盟立法，设立专门的个人信息保护机构。

就个人信息保护职责部门的执法现状，著名学者周汉华曾评论道，个人信息保护领域的行政执法呈现一种“九龙治水”的分散执法体制——网信、市场监管、工信、公安等相关领域的管理部门都负有相应的管理责任，这一管理格局的弊端在于执法的责任边界不明确，可能出现相互推诿的不良结果。此外，我们认为这种执法机制还可能带来执法尺度不一，不便于群众举报等问题。草案的前述规定，是否能够改变执法中的该等困境，还有待实践的检验。

4. 法律责任：“情节严重”的认定依据和罚款的裁量标准尚不明确

违法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法律责任规定在草案第六十二条至第六十三条(如下)。个人信息处理者和直接责任人员均需对个人信息违法行为负责。

1) 责令改正，没收违法所得，给予警告；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；

2) (对于已规定的情节严重的违法行为)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、吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他责任人员处十万元以上一百万元以下罚款)。
3) 记入信用档案，并予以公示。

关于法律责任，我们提示企业关注加重的违法后果。草案发布之前，有关个人信息保护的违法行为主要由《网络安全法》规制：违法处理个人信息的行为适用《网络安全法》第六十四条的行政处罚，处理个人信息未按照规定采取必要的安全保护措施的行为可能借由《网络安全法》第五十九条违反网络安全保护义务的条文进行惩处。**相较而言，草案大幅提高对情节严重者的罚款标准，承继了“严厉惩罚个人信息违法行为”的国际通行做法。**

尽管草案提出了高额的行政罚款，但具体何种违法行为将落入“情节严重”的范围，进而可能受到惩罚还未可知，草案没有作出明确的界定，而且被认定为“情节严重”之后，处以“五千万元以下”罚款抑或是“上一年度营业额百分之五以下”罚款两种罚款选择是否由执法机关自由裁量？“上一年度营业额”是以何种法律实体为基准进行计算？可以预见，立法机关还将出台更为细致的规定指导行政裁量。我们总结 GDPR 在决定是否施加行政罚款以及施加多少数额的行政罚款时的考量因素如下：

1) 侵权行为的性质，严重性和持续时间(综合考虑个人信息处理的性质范围或目的，以及受影响的个人信息主体的数量和遭到破坏的程度)；
2) 侵权行为系故意还是过失；
3) 数据控制者(data controller)和数据处理者(data processor)为减轻个人信息主体受到的损害而采取的任何措施；
4) 数据控制者和数据处理者实施的安全技术措施和行政措施的可靠程度；
5) 数据控制者和数据处理者此前的任何相关侵权行为；
6) 与监管部门的配合程度，以纠正侵权行为并减轻不利影响；
7) 受侵权行为影响的个人信息类型；
8) 监管部门知晓侵权行为的方式，特别是个人信息处理者是否以及在何种程度上通报侵权行为；
9) 是否遵守此前就同一事项向个人信息处理者下达的指令；
10) 是否遵守行业行为准则或认证机制；
11) 其他加重或减轻因素(例如直接或间接因侵权行为获得的经济利益或避免的损失)。

三. 结语

著名学者程啸总结“个人信息保护法本身并非单纯的民事特别法，而是一部运用民事、行政等综合性手段对于个人信息加以保护，对于自然人个人信息权益、信息自由、公共利益等多重利益关系加以协调的法律。” 协调多重利益关系绝非易事，草案有“拨云见日”之明，亦有“疑团莫释”之惑，实属

正常。**通过枚举辨析若干“明”“惑”，作者希望能对企业有所启发，共同献言进策，对草案进行完善。**

此外需要注意的是，草案中的一些术语可能使熟悉域外个人信息保护法律的读者产生误解，比如草案规定的“个人信息处理者”是指自主决定处理目的、处理方式等个人信息处理事项的组织、个人，不能直接对应 GDPR 语境下的数据处理者，就其对个人信息处理的主导地位和承担的个人信息保护义务而言，“个人信息处理者”更贴近 GDPR 下的数据控制者。在华经营的跨国公司在与其境外总部沟通时，应充分释明这一差异。

《个人信息保护法》对于我国个人信息保护领域的重要意义无法尽述，本文是通力合规团队关于《个人信息保护法》解读系列文章的第一篇，敬请期待我们后续发布的焦点评述。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 16/19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环皇后大道中 5 号 衡怡大厦 27 楼 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野