法治日报

专刊

2021年9月29日
星期三

法学院

LEGAL DAILY

专刊主编：蒋安杰
见习编辑：刘秀宇
美编：李晓军
责校：邓春兰
电子信箱：angelar1102@163.com

合规不是做一套书面的计划 也不是做一套纸面的规章制度

数据合规高端论坛在京举行

前沿聚焦

□ 本报记者 蒋安杰

近年来，随着大数据、云计算、移动互联网的不断发展，特别是大数据与5G、人工智能、区块链等新一代信息技术的融合发展日益紧密，数据种类日益增多，数据规模急剧增长，数据合规越来越受到社会各界的普遍关注和立法部门的普遍重视。9月25日，由中国人民大学刑事法律科学研究中心、北京市东卫律师事务所共同举办的“数据合规高端论坛”在京举行，来自学术界、实务界近60位代表与会。全国人大法工委经济法室林一英，最高检第四检察厅俞启泳，北京大学法学院教授陈瑞华，中国人民大学法学院教授张新宝、刘品新，北京师范大学法学院教授张远煌等分别作主题演讲。

中国人民大学刑事法律科学研究中心主任时延安和北京市东卫律师事务所主任郝春莉分别代表主办方致辞。时延安表示，对数据安全的维护，首先就要认识到数据对于当前政治、经济、社会的重要意义。对数据重要性的理解，可以从两方面来认识：一是，数据的生产资料化；二是，数据的资产化。围绕数据的享有、处理形成了一个综合法益，其中包括安全、社会秩序以及个人利益。因而，对数据安全的维护，也必须依靠多个法律来实现，包括数据安全法、个人信息保护法、网络安全法，也包括民法、刑法，乃至宪法。从企业经营来讲，维护数据安全就要大大加强合规建设，而且要形成一个综合性、结构化的体系，不能仅向数据安全法看齐，而是要向多个法律看齐。在合规计划制定上，不仅要考虑和用户的关系，更要将政治安全、经济安全、社会安全等因素考虑进去，尤其是网络服务提供者，要切实充分考虑数据安全所具有的多面性、多层性，要充分考虑到数据处理当中的各种风险，进而通过合规建设防范风险于未然。

郝春莉表示，继民法典、网络安全法、电子商务法颁布以来，今年6月10日、8月20日又相继通过了数据安全法、个人信息保护法，下一步还会有更多数据合规的法律法规陆续出台。与当前日益趋紧的措施和法律法规不相适应的是，目前国内一些企业在收集和使用用户个人信息方面，还存在着惯性的商业逻辑和商业思维，很多做法与现在的法律法规相违背。数字经济时代在智能+的产业数字化转型中，数据合规势必成为维护产业平稳健康发展，保障公司商业利益和正常运营的重要基石。我们举办数据合规高端论坛，就是为了凝聚包括立法、司法、理论、企业、律师等社会各界力量，强化数据合规理论与实务研究，完善数据合规的建设以及开拓数据合规法律研究和法律服务的新蓝海。

数据合规治理的重要性

林一英从立法背景和意义、法律定位以及涉及合规要点的主要制度介绍了个人信息保护法（以下简称《个保法》）的基本情况。在数字经济背景下，《个保法》的出台不但有利于促进数据经济健康持续的发展，维护人民群众在网络空间的合法权益，还标志着我国法律制度逐步走向体系化、专门化和系统化，并为国际数字治理贡献出“中国方案”。她认为，《个保法》对规范个人信息的处理行为不同于民法的人格权保护制度，其主要采取了公法与私法兼顾的综合性保护手段，而且主要进行事前预防的保护。因此，《个保法》是我国在网络空间和数字经济领域重要的一个综合性法律。

张新宝从数据合规的角度介绍了数据合规治理的重要性、完善个人信息权益保护的措施及加强企业合规治理的内部建设等内容。

张新宝认为，数据合规包括数据安全、数据监管、数据存储等物理层面的安全问题，也包括个人信息处理的各个环节。因此，在现有的数据合规法律基本框架下，如何落实和实施法律法规，是未来数据合规治理的努力方向。个人信息保护合规是数据合规治理的重要组成部分，对个人信息保护合规应当进一步加强制度规范供给。例如，对个人信息实行分类合规治理，将个人信息分为一般、敏感以及私密三个等级，并强化对敏感信息和私密信息的保护。同时，对个人信息处理者进行分类施策。

张新宝以超大网络平台个人信息合规为例，结合《个保法》第五十八条规定，提出了几点思考：一是如何鉴定大型平台；二是关于“成立主要由外部成员组成的独立机构”的问题；三是如何明确平台规则的制定标准；四是适用停止服务的问题。

张新宝建议，企业内应当设立专人进行数据合规工作，对企业法务部门的职能进行调整，还要建立相关的规章制度，制定处理个人信息的规则。数据合规作为法律服务的一个新领域，还应加强律师的合规培训，学界也应加强相关研究。

数据合规研究需要注意的四个问题

陈瑞华指出，在研究数据合规时，有四个问题应当重点关注：第一，企业数据合规的价值。为企业在市场竞争中提供诚信度背书；将企业责任与员工责任、上下游企业责任进行有效切割；最大限度预防行政违规与刑事犯罪危险。第二，网络安全法、数据安全法、个人信息保护法中包含的合规义务。他认为，重要数据处理者应当定期进行风险评估；个人信息处理者应当定期对处理的个人信息遵守法律、行政法规的情况进行合规审计；企业应当在发生网络、数据、个人信息安全事件时，立即采取补救措施，并通知有关行政部门和可能受影响的个人。第三，数据合规的两种模式。危机发生前的日常性合规体系，即数据风险评估与预防；危机发生后的合规整改体系，即通过合规整改换取宽大处理。第四，合规与危机处理的关系。陈瑞华认为，企业面临的最严重的危机是行政处罚和刑事追责；合规整改方案是要解决问题，纠正错误，填补制度漏洞，完善治理结构，改变经营模式；合规整改方案的本质就是防止再次发生类似的行政违法行为和刑事犯罪行为。

陈瑞华表示，不管是日常合规管理体系，还是合规整改体系，根本目的是要预防违规、预防再次发生违规和违法犯罪活动，合规不是做一套书面的计划，也不是做一套纸面的规章制度，而是要把合规的管理模式、体系、整改方案有效运行起来，有效地识别违规行为，预防数据领域的违法行为，监控整个公司的运营情况，一旦发生危机能进行自我处理和有效的监管。

张远煌指出，合规的本质是防控违法犯罪风险。企业合规需要打破传统部门法之间的界限，形成从违规、违法到犯罪预防的整体性合规思维。张远煌着重从犯罪预防角度分析了数据合规对企业的影响以及企业如何做到有效合规。

他说，当前数据合规的外部规制主要体现在三个方面：一是非刑事领域出台了网络安全法、数据安全法以及个人信息保护法等专门立法；二是刑事领域原本就有关于个人信息和网络信息保护的规定；三是最高人民检察院开始启动具有刑事司法性质的企业合规改革试点，意味着作为企业合规高端形态的刑事合规已经现实呈现，对企业合规提出了更高要求。当前，数据安全问题不仅涉及公民个人的基本权利，更关系到数字经济的健康发展，也涉及国家的整体安全。为此，数据合规正在经历重要转型：一方面，在规制体系上，对企业的外部管理要向企业内部的自我监督转移，使国家外部监督与企业自我监管形成合力；另一方面，在规制力度上，企业合规要从民事、行政规制向刑事规则升级发展，制度化、机制化地贯彻“惩罚并举，预防为主”方针，实现企业违法犯罪的源头治理。

张远煌认为，有效合规是当前最紧迫的问题。他提出了评价企业有效合规的三条实质性标准建议：一是企业制定的合规计划应当具有特定的针对性。合规计划必须是基于企业的规模和实际面临的合规风险建立起来的，而不是照搬法律规定或通用合规指南；二是企业内部的合规监管机构应当具有独立性与充分的资源配置；三是对发现的违法违规行为及时妥当地处置。企业要用证据和实际行动表明，只要企业成员在企业运行过程中实施了违规行为，不论其层级如何，都予以了一视同仁的处理。这是判断企业是否在着力倡导合规文化的重要标志。

数据刑事合规方案应当采取“三线”标准

刘品新认为，数据刑事合规的研究既有理论问题，也有实务问题。为什么要进行数据合规？在刘品新看来，不仅因为我们正处在大数据时代，数据合规与个人信息保护、国家安全紧密相关，还因为在涉数据犯罪案件中，如果提出数据合规整改，就可能形成一个真正意义上的“认罪”，可能会争取到刑法上的缓刑或者其他的从宽效果。

数据刑事合规是什么？简单来讲，数据刑事合规与行政合规、民事合规最明显的区别在于它会产生刑事责任减免的效果，是“皇冠”意义上的数据合规。

数据刑事合规应采取怎样的标准？刘品新认为，检察机关验收数据刑事合规整改应当采取相对主义的标准：一是对象相对，合规的对象不是一个罪名，也不是全部罪名，而是数据具体业态涉及一系列关联罪名；二是合规结果相对，不要简单地追求合规后绝对不再犯罪，而是要审查有关平台进行数据刑事合规整改力度是否足以预见其涉嫌犯罪的罪量、可能性等现有风险。

第三方组织等主体提出数据刑事合规方案应当采取反向标准：作为第三方组织或者律师介入数据合规时，不能告知当事人这样做可以不犯罪，而要告知其某种做法可能触犯哪几个罪名及构罪的可能性。

数据平台等主体制定数据刑事合规方案应当采取“三线”标准。第一是以刑法、司法解释等规范中刑事责任条款为红线，梳理具体业务涉及哪些罪名，做重点防范；第二是以触犯数据安全法三大法律、行政处罚条款或者其他的行政法规为黄线，梳理可能因情节严重便构成犯罪的数据违规情节，谨慎避免；第三是绿线，是指民事法规、技术规范或者行业标准里面完全允许的数据行为。

这个“三线”标准是动态标准。考虑到我国这方面的法律、技术、规范在不断演变，建议至少每年要对有关标准进行一次更新。

俞启泳介绍，数据安全问题日益凸显，严重影响着数字经济发展和个人信息保护。特别是互联网垄断和不正当竞争问题日益突出，数字经济发展面临新风险。检察办案环节反映出，近年来，数字经济竞争愈发激烈，网络制假售假、虚假广告、流量劫持、刷单炒信、大数据杀熟、“二选一”等新型违法犯罪大量滋生，平台内部贪腐案件多发，严重影响行业生态，侵蚀公众数据安全，成为平台治理新问题。在数据垄断方面，平台企业独占海量数据，其中，不仅有合法取得的商业数据，也有处于灰色地带的越界索权、过度收集信息，涉及侵犯公民个人信息问题，成为平台垄断的重要根源。在算法垄断上，平台确立以企业利益为中心的算法规则，由于这些规则不透明不公开且技术性强，形成“算法黑箱”，对其监管和违法调查存在困境。在资本垄断上，头部企业规模过大、横纵跨越、树立壁垒，已引起社会对资本无序扩张的关注。

俞启泳表示，2020年11月，最高检向工信部制发“六号检察建议”，围绕网络黑灰产业链条整治、App违法违规收集个人信息、未成年人网络保护等问题提出治理建议。当前，涉案企业合规改革试点还处在起步期、培育期，需要我们勇于尝试、大胆创新，推动建立现代企业规制司法制度的“中国方案”。

据悉，论坛上，围绕着“数据安全风险的一般问题”“数据处理中的风险点”“数据安全犯罪问题”“数据安全合规领域的主要问题”为内容的圆桌研讨同时进行。

“刑民（行）关系与犯罪认定”之二十二

个人信息公开目的对于定罪的实质影响

刑法光圈

□ 周光权（清华大学法学院教授）

在《获取已公开个人信息并出售牟利的定罪争议》（《法治日报》2021年9月22日9版）一文中，笔者指出，对于行为人在公开的网络上（包括企业征信网、“企查查”“天眼查”等企业信息查询网站、裁判文书网站等）爬取已公开的企业登记信息，从中获取个人信息，再对这些已公开的个人信息进行有偿转让、出售的，实务中基本都按侵犯个人信息罪予以定罪处罚。但是，这一做法是值得商榷的。对此，需要关注民法典及个人信息保护法的相关规定。

民法典第一千零三十六条强调，如果行为系对已公开人的个人信息进行不合理处理的，仍然应当承担侵权责任。换言之，并不是所有对已公开人的个人信息的处理行为都合法，法律对于“不合理地处理”已公开的个人信息的行为仍然持反对态度。对于已公开的个人信息必须合理处理的进路，在个人信息保护法中得到了坚持。该法第六条第1款规定，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。第十三条第6项规定，“依照本法规定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”的，个人信息处理者可以处理个人信息，不需要取得个人同意。本条也特别强调仅在“合理的范围内”对于个人信息的获取、提供行为，不需要取得个人同意。第十四条第2款规定，个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。第二十七条规定，个人信息处理者可以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。

必须承认，个人公开其信息的目的以及信息的用途属于侵犯公民个人信息罪保护法益的一部分，而非法益之外的东西。虽然企业法人的信息属于企业应当对社会公众公开的登记或企业运行信息，对于其中所涉及的已公开个人信息，他人可以通过工商登记网站对此类信息进行查询，但是，个人选择在企业公开的信息中，对于自己的姓名、通讯方式等予以公开有特定目的：使自己所在的企业的设立和运行符合国家行政主管机关的要求，为企业合法获取商业利益创造机会。因此，已公开的个人信息中，信息的内容成为刑法保护的对象，基于特定目的对信息的处分自由（对信息的最终决定权）也是法益的一部分。那么，对于处理已公开的个人信息且未偏离该信息公开的目的，没有改变其用途的行为，没有侵害法益主体的法益处分自由，对于这种尊重信息公开目的前提下的对个人信息的合理处理，民法典、网络安全法、个人信息保护法等部门法均不反对，该个人信息是权利主体自愿放弃保护的财物，且处分行为没有违背其处分财物的意思，不属于刑法所保护的行为对象。

按照民法典、个人信息保护法的相关规定，处理已公开的个人信息，仅在合理利用该信息的限度内不需要得到信息主体的同意，如果处理该信息侵害其重大利益的，就应当得到或重新取得个人的同意。“在有的情况下，自然人的个人信息虽然是自己主动公开或者是通过其他合法方式公开的，但若处理这些个人信息的行为损害该自然人重大利益的，行为人仍不能免除责任。例如，某人对外公开了自己的电话号码，但行为人却利用这些电话号码频频向某人发送垃圾短信或者拨打电话，严重滋扰了某人的生活安宁，此时，行为人仍应承担民事责任”（参见黄薇主编：《中华人民共和国民法典释义及适用指南（下册）》，中国民主法制出版社2020年版，第1551页）。因此，处理个人信息明显违背个人公开其信息的目的，改变已公开信息的用途的，都有可能构成本罪。例如，互联网公司工作人员将其在工作中获取的个人已公开信息出售给体检机构，以便于后者拓展客源的，显然改变了个人公开其信息的目的和用途，可以构成本罪；再比如，通过公开征信系统获得他人手机号码之后对个人进行追踪定位的，使他人的生命、身体陷入危险，也违背了他人公开其信息的目的和用途，该信息仍然属于本罪对象。

考虑到信息公开目的对于定罪的实质影响，笔者认为，对于处理个人已公开的信息有以下情形的，不宜定罪：（1）针对已公开的个人信息仅实施单纯获取或爬取、持有等行为的。由于行为人还没有将该信息予以批量出售、提供的，很难判断他人后来对于该信息的使用目的是否与个人公开其信息时相同，也无法确定信息的用途是否被改变，难以得出行为人侵害被害人法益处分自由的唯一结论。（2）获取、提供他人已公开的个人信息的目的是帮助行为人拓展业务的情形。企业注册登记或者将其信息在征信系统中收录，其目的是为了企业自身发展。行为人处理企业公开信息中包含的个人信息，如果与该企业的经营发展目的相一致的，应当认定该处理信息行为具有合理性。例如，某些特定行业的从业人员为扩展业务范围、推销产品、开展市场营销，大量收集或向他人购买特定行业的企业注册登记信息（包括企业法定代表人的姓名、工作单位、手机号码等），或者与他人交换上述信息的，实务上倾向于认为个人信息被侵犯。此外，实务上将为了寻找潜在客户而获取、提供公开的个人信息的行为认定为犯罪的情形为数不少。但是，在上述案件中，行为人为了企业利益获取他人信息，但已公开信息所在企业也是为了开展市场营销等经济活动而存在的，因此，行为人获取、使用个人信息的行为与信息主体的目的之间具有大致相同性，其对信息的处理相对具有合理性。因此，不宜将为了扩展业务范围、推销产品、开展市场营销寻找潜在客户而获取、提供公开的个人信息的行为认定为犯罪。（3）获取、提供他人已公开的个人信息的目的是为企业发展提供贷款等金融支撑的情形。企业的发展需要使用支付、结算器械，向企业推销此类产品不违背企业设立的目的。例如，对于为了推销POS机业务而接受罗某发送的邮件，其中包含公民个人征信信息共计456条的，法院认定被告人构成本罪。但是，这一定罪结论是否妥当还需要推敲。企业存在的目的是开展市场交易活动，为此，需要金融结算工具的支持。行为人获取企业登记信息然后向其推销POS机，不宜认定为违背企业公开其个人信息的经营目的，并未侵害个人的信息自主权。

归结起来讲，对于获取企业注册登记信息、征信信息等公开信息中的个人信息，然后将其提供、交换给他人的，仅将信息数量作为区分罪与非罪标准的思考方法过于简单化。获取、提供、交换、出售已公开的个人信息，明显违背信息公开目的，或者明显改变已公开个人信息的用途以及利用已公开个人信息实施可能危及公民人身或财产安全的违法犯罪行为的，才有可能构成侵犯公民个人信息罪。

（“刑民（行）关系与犯罪认定”之二十一详见于《法治日报》2021年9月22日9版）