个人信息保护法落地在即，被互联网“脱下”的个人信息外衣，将由法律重新穿上

当大数据遇上个人隐私

去年12月，一位“头盔哥”在网上一夜爆红——为避免自己被售楼处的人脸识别系统采集到、受到电话推销的“轰炸”，他索性戴上头盔，把脸挡个严严实实。

现实中，让人无奈的却是，即便用头盔把脸挡住，却依旧挡不住个人信息被手机里无数个App厂商自在地采集和流通，在数字经济大潮下，许多人都在被迫“裸泳”。

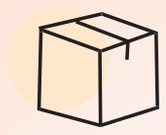
为保护个人信息安全，8月20日，全国人大常委会会议表决通过了《中华人民共和国个人信息保护法》，该法将于今年11月1日起正式实施。这部维护个人信息安全的专门法律，明确了“不得过度收集个人信息”“禁止大数据杀熟”“保护人脸信息等敏感个人信息”等内容，为个人信息罩上了“金钟罩”。

而对于快消、零售、医疗健康、金融、互联网、物流等处理大量个人信息的行业而言，当“隐私”遇上“大数据”，如何平衡商业利益和用户隐私保护的关系，成为企业亟须解决的问题

■本报记者 张天弛

数字合规不含糊

怎样勾选用户协议才有效



当下，手机App过度收集个人信息使用似乎已成了一种“常态”。工信部一则公开数据显示，今年上半年，工信部审查了76万款手机App，其中，通报批评748款、下架245款，预计今年将完成180万款App的合规检查目标。

对违规违法的企业，《个人信息保护法》也明确规定了其法律责任：第一次责令整改；拒不改正的，并处一百万元以下罚款；再不整改的，情节严重者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，甚至可吊销营业执照。

这一前所未有的高额罚款力度，对企业威慑力巨大，有力地推动企业加速数字合规转型。

什么是数字合规？数字合规是企业合规治理的一部分。在安永网络安全与隐私保护团队高级经理王伯铮看来，手机App在个人信息保护的合规风险点主要出现在以下四方面：一是违规处理用户个人信息；二是频繁、过度骚扰用户，获取过多的用户信息；三是欺骗诱导用户下载或获取信息；四是应用分发平台责任落实不到位，没有对App获取用户个人信息进行明确的提示。

那么，企业如何收集和使用用户个人信息才合规呢？王伯铮认为：“企业必须公开、明示收集和使用个人信息的目的、方式和使用范围，并且不过度收集信息。”

他进一步解释道，首先，一款App应该在官网、应用商店和App内展示其隐私政策，告诉用户其收集个人信息的目的、方式和使用范围。他举例说道，此前某快递App在收集用户的电话和邮箱信息时，只附上一行小字“若订单出现问题，我们将通过手机或邮箱方式联络您”，“这就是典型的违反个人信息保护法的行为”，王伯铮表示，这行提示小字不能替代隐私政策存在。还有一点需要注意的是，现在绝大多数App都会使用SDK（第三方软件开发工具包），App内要将SDK对用户信息的收集和使用情况引渡至App的隐私政策里公示出来，否则也是不合规的。“例如，某App为用户提供的服务并不需要访问用户的手机相册，但其SDK需要相册信息，最终该App因未在隐私政策中提及需访问用户手机相册信息而被处罚。”

提起“勾选用户使用协议”，市民萧先生就满腹牢骚，“有的协议用词太专业拗口，一般人如果不是静下心来一字一句抠，很难理解；有的协议则是冗长繁琐，根本没有耐心读完，但不勾选同意就不能下载或继续使用App。”不少专业机构的调查也显示，大部分用户在下载App时，都没有真正阅读用户协议并理解协议内容是什么。王伯铮提醒，在申请收集个人信息权限时，App要以明显、清晰、突出的显示方式提示给用户，“不能缩小字体，用与底色相近的字体颜色，或用遮盖、调整透明度等方式，去模糊隐私政策。”他还特别指出，一些App登录默认勾选隐私政策的方式，也是违反规定的。

《个人信息保护法》还规定了处理个人信息时，要遵守个人权益影响最小原则。这也意味着，企业不能过度收集用户信息，收集的信息必须与业务直接相关。王伯铮举了一款输入法的例子，“这款输入法要求访问用户的手机通讯录，声称这样当用户输入熟人姓名的汉语拼音首字母或简称时，输入法就可以弹出相关人姓名的词条。”他说，但实际上，收集个人通讯录超出了输入法的必要信息收集范围，同时，被收集到App后台的联系人和电话号码也存在泄露的风险，因此，该款App已经被工信部公示处罚。

彻底叫停“大数据杀熟”

放进“笼子”里的自动化决策

今年7月，浙江一起针对“大数据杀熟”的判决在网上掀起了一场舆情。某旅游服务平台给其一名“钻石级VIP”用户提供的酒店价格，比普通用户贵一倍还多，这名用户以“大数据杀熟”为由将该平台告上法庭，最终法院判决该平台“退一赔三”。

《个人信息保护法》第二十四条规定，个人信息处理者利用个人信息进行自动化决策时，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。安永网络安全与隐私保护团队高级经理梁卓毅指出：“如果大数据算法设计本身和训练数据集有偏差，就会导致带有歧视的算法。”这就意味着，企业在业务运营中，应当对大数据处理和自动化决策进行人工干预，并对自动化决策结果进行人工复核，把自动化决策放进“笼子”里。

不仅如此，梁卓毅介绍，对自动化决策应有一套完整的监管体系——在决策处理前，应由人工对该决策可能会对用户产生的影响程度进行评估，决定是否采用自动化决策。并且，在使用自动化决策的过程中，要定期或至少每年一次，进行自动化决策的影响评估。“此外，企业还要建立透明的反馈机制，为用户提供查询、咨询和投诉的便利渠道，并能提供停止自动化决策的服务方式。”梁卓毅表示。

“个保法”落地

拒绝“打补丁”式合规，企业要有合规治理体系

《个人信息保护法》出台后，企业亟须出台完整的数字合规治理体系。

安永网络安全与隐私保护咨询服务团队总监朱汉乐将互联网企业的发展分为三个时期：“蛮荒时代”“网络安全法时代”和“个人信息保护法时代”。他解释道，“蛮荒时代”是指在网络安全法出台之前，缺少个人信息保护机制的时期，企业野蛮生长；“网络安全法时代”，则代表着个人信息保护受法律保障，也出现了一些监管行为，企业的应对方式是开始关注个人隐私问题，并开始了打补丁式的合规补救；而在《个人信息保护法》出台之后，互联网进入了“个人信息保护法时代”，这时，企业如果还想继续生存，就需要将个人信息保护融入企业的业务全流程之中，将个人信息保护视为企业竞争力之一，“也就是说，企业要建立和实施个人信息保护合规治理体系，系统全面保护信息安全。

“治理体系因企业自身发展情况而异，”朱汉乐说，但一些关键治理元素是不变的，例如人员组织。他说，数据和隐私保护不是靠几个人就能完成的，它需要客户支持、法律、运营、IT等多个职能人员的跨职能协作，“明确的问责制也是必不可少的”。同时，与其他风险管控一样，数字合规体系也需要建立起至少三道防线，他进一步解释说，第一道防线是在业务条线中，培训员工合规操作；第二道防线是公司的风险管理和内控制度，定期披露风险管理报告，并对正在执行的流程进行合规抽查和监控；最后的第三道防线，则包含问责制度和内审流程。

而在数字合规治理体系中，数据分类分级工作是其基础和核心。朱汉乐解释道，企业每天要面对浩繁庞杂的海量数据，但这些数据的敏感度和关键性是有差别的，因此，要按照其重要性进行数据的分级和分类，这有助于企业内部管理和建立问责制，以满足监管和合规要求。他表示，企业可以给数据打上不同的敏感星级和标签，如“公开”“内部”“机密”“绝密”等，需要使用时，一目了然就知道哪些数据可以使用、哪些不可以使用。

防不胜防的泄密

企业如何保障数字资产安全

近年来，国内外企业数据泄露事件时有发生：雅诗兰黛被发现泄露4.4亿条邮箱记录；河北省某物流公司员工账号泄露大量客户信息；某招聘网站贩卖求职者简历……这些防不胜防的个人信息泄密，不仅损害了用户的个人信息安全，还会对企业的利益和名誉造成巨大影响，更令人无法接受的是，这些泄密事件，有不少还是企业的“内鬼”所为。

朱汉乐建议，为了更有效地保护企业机密数据，企业应定期对员工进行培训，如机密文件决不允许通过电子邮件发送，打印、传真或复印不应留下文档，对于存储机密文件的硬件设施和软件设备，只能由有授权的员工进行操作等。

有信息安全专家表示，以目前的通用技术手段，很难查到员工在电脑上进行的各种恶意违规操作，如离职员工用还未更改的账号信息窃取机密文件，或在职员工恶意进行泄露。针对这种情况，有不少软件企业开始研发推广针对信息安全的应用和服务，如微软最新开发的Microsoft365软件，就能有效保护企业的数据资产安全。据相关负责人介绍，这款软件可在多种场景下识别敏感信息，并自动加密，切断敏感数据向外传输的途径，如拦截邮件发送、内网敏感信息无法复制、文件不能被拖拽至第三方平台、打印敏感文件被阻止等；同时，该软件还可以识别员工的异常操作并即时“报警”，在员工批量下载内部资料，越权访问敏感信息，恶意篡改机密信息时，软件会实时将这些异常操作上传到后台管理员端，有效保护企业数据资产安全。

相关链接

■《个人信息保护法》保护哪些信息

以电子或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，但不包括匿名化处理后的信息；个人信息处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

■禁止“大数据杀熟”

《个保法》第二十四条规定，个人信息处理者利用个人信息进行自动化决策，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。

■规范使用人脸识别

《个保法》第二十六条规定，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。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

专家视角

网络安全立法日趋完善

■本报记者 徐晶卉

今年8月，酝酿多年的《中华人民共和国个人信息保护法》表决通过，并将于11月1日正式实施。这是我国首部个人信息保护领域的专门立法，根据个人信息保护法的相关规定，大数据、算法等技术将被关在“笼子”里，“大数据杀熟”等以科技、便捷为名对个人信息的侵害，将受到法律的严格监管。长期关注网络空间安全立法的华东政法大学数字法治研究院院长马长山教授认为，《中华人民共和国个人信息保护法》即将实施，是我国在网络安全立法领域的一大重要成果，配合此前已经实施的《中华人民共和国数据安全法》《中华人民共和国网络安全法》以及更高层级的《中华人民共和国国家安全法》，我国涉及网络空间安全的立法步伐不断加快，体系日趋完善。

记者：您提出网络空间安全立法，既具有维护自身安全的目的性，又出于大国竞争博弈的需要。如何理解网络空间安全的这一“双重属性”？

马长山：网络空间安全首先是要保障安全。国家安全法第二条规定，国家安全是指即国家政权、主权统一和领土完整，以及其他重大利益没有危险，或者不受内外威胁的状态。网络安全法、数据安全法也有相应的规定，以保护公民和其他法人合法利益，维护公共利益、网络安全和秩序。第三条也做了类似的规定。这是网络空间安全立法最重要的出发点。

另一方面，在当今数字化时代，网络空间安全立法也是大国博弈的法律工具和策略。在网络兴起之初，网络自由主义曾盛行一时，可以称其为“网络无政府时代”。但随后的发展表明，网络并非法外之地，也出现了好多问题，比如说民粹主义、数据“黑灰产”、犯罪活动等等，这些无疑打破了网络自由主义的梦想，各国的国家权力纷纷开始介入，这样，不仅是那种扁平化、匿名化、无国界的网络空间观念被颠覆了，网络越来越演变成大国竞争的政策工具。特别是在近几年，某些国家泛化国家安全观念，运用诸如网络安全、空间安全这样的法律工具，力图在世界大国的博弈中占据有利地位。

对于中国而言，采取的策略是从立法上确认和界定“网络空间主权”，网络安全法第一条就完成了这一法律确认，这在世界上也是一个重要创新。当然，确认网络安全主权，也曾引起了一些争议，认为网络空间是没有边界的，怎么会有主权？或者它是虚拟的，怎么会有主权？然而，我国立法并没有从“范围”或者“地域上”对网络安全主权进行界定，而是从行为上作出界定，即一切在我国网络空间领域内非法入侵窃取破坏计算机，以及其他服务设备提供相关的行为，都被视为侵害我国国家主权的行为。这就明确指出了什么样的行为是侵犯网络空间主权的行为，进而通过控制行为来维护国家的网络空间主权。

记者：中国对网络空间主权的立法构建，主要有哪些原则？

马长山：具体而言，我国对网络空间主权进行了价值设定。国家安全法、网络安全法、数据安全法的相关条款明确规定，要保护公民的权利自由、尊重和保障人权、保障公民的生命财产、保障使用网络的权利、保障信息自由流动、促进公共数据的资源开放等原则。

有了上述价值设定之后，就应对网络空间主权提出疆域主张。尽管我们的立法是通过行为来保护网络空间主权的，但疆域主张还是必要的，即我们的网络空间主权应该在哪里。从网络安全法来讲，对内我们要独立自主，管理本国事务；对外要防止对我们的入侵，这是对网络安全的基本理解。

记者：如何理解“网络空间疆域”这一全新概念？

马长山：网络空间疆域这一概念的提出，一是依据属地原则，二是依据效果原则。

就属地原则而言，相关法律规定得十分清楚：在中国境内建设运营维护使用网络以及管理，要适用网络安全法；在中国境内开展数据处理活动，安全监管要适应数据安全法。这就是属地原则。

就效果原则而言，不管在境内还是在境外，只要对我国产生社会后果，那就要纳入我们的法律管辖，因为网络本身就是虚拟的，没有边界，至少是超越了物理边界。因此，境外的机构、组织或者个人从事攻击、侵入、干扰、破坏我国的信息基础设施，造成一定社会后果的，我们应当追究其法律责任。数据安全法第二条规定，在中国境外开展数据处理活动，损害中国国家安全、公共利益或公民、组织合法权益的，依法追究法律责任。刚刚通过的个人信息保护法第三条规定，在境外处理我国境内自然人个人信息的活动，以向境内自然人提供产品或者服务为目的；分析、评估境内自然人的行为；以及法律、行政法规规定的其他情形，要适用个人信息保护法。

本版图片 视觉中国