数据生死簿

——大数据企业及高管的刑事法律风险可控吗？

作者：肖波、荣埚　昌言（上海）律师事务所

【作者简介】

肖波 昌言上海办公室　执行主任
邮箱：xiaobo@changyanfirm.com

肖波律师获得中国人民公安大学硕士和复旦大学刑诉法学博士学位，之前曾在上海市浦东新区法院工作 13 年多，审理过 1000 多件案件。后又作为合伙人加盟中伦律师事务所，积累了大量的刑事案件和危机处理经验。肖律师业务聚焦于金融、互联网及经济领域犯罪、白领犯罪的刑事辩护、反商业贿赂、企业危机处理、民商事争议解决等。肖律师在刑事犯罪领域发表了大量的专业论文。

荣埚 昌言上海办公室　律师（实习期）
邮箱：rongguo@changyanfirm.com

荣埚律师获得中山大学法学硕士学位和南开大学法学学士学位，具有六年以上法律工作经验，曾在网易集团、合景泰富集团从事法务工作，主要专业领域在于互联网、电商物流、房地产行业法律服务及争议解决业务。

引言

最近，数家知名大数据企业的高管陆续被带走调查的消息在朋友圈里刷屏，来自大数据企业、特别是金融数据科技服务业企业高管的刑事法律风险咨询需求陡然增多，行业内一片生死关头的战战兢兢。其实不止这两周的雷霆行动，近几年来国家对大数据行业违法犯罪行为的清理整顿从未停歇过。

从这些大数据企业涉刑情况来看，其刑事法律风险既涉及到企业，又关乎企业中的高管、直接责任人员等个人；从其业务范围上来看，更是贯穿从数据获取/采集到数据应用、流出/交易等的全过程。9 月 6 日先后卷入调查的新颜科技和摩羯科技，是通过爬虫技术获取数据并向互联网金融行业客户提供风险管理服务的数据公司；而 9 月 12 日多名高管被带走调查的天翼征信，作为运营商旗下企业，其数据源主要来自于“通讯+支付+第三方数据”

[1]，即既包括了自有的用户数据积累，又包含从上家获取的二手数据，并通过对数据的整合应用提供企业征信服务；更早一点，去年 11 月失联的有脉金控和今年 8 月份被爆调查的阿尔法象，则是现金贷系统供应商，部分业务涵盖从数据获取到风控管理、甚至直接介入催收的应用阶段；而去年 7 月震惊业内的新三板公司数据堂部分高管、员工涉刑一案[2]则涉及到从上游非法获取数据、经过精准化处理后向下游贩卖数据的行为。

正是因为刑事法律风险已渗透到大数据行业的方方面面，有人说“整个行业都快抓没了”[3]也是可以理解的。但大数据企业、以及企业高管们的刑事法律风险真的完全不可控吗？显然不是。对此，本所拟结合法律规定、实务经验，对大数据企业面临的种种刑事法律风险和风险防控措施进行探讨。作为开题第一篇，本文将概述大数据企业数据经营的各阶段中常见的企业和高管的刑事法律风险，以及一般性的风险防控措施。

一、获取数据阶段的刑事风险

无论是前端还是后端的大数据企业，都必然会涉及到获取数据的过程。常见的几种数据获取方式包括：自行收集、积累用户数据；通过爬虫技术获取数据；通过购买、收受、交换等方式从他人处取得二手数据。这几种模式下都存在一些刑事风险，简述如下。

1. 自行收集用户数据的刑事风险

有一些大数据企业在经营过程中会自行收集用户的个人数据，这一模式下最常见的罪名是侵犯公民个人信息罪。根据《刑法》第二百五十三条之一第一款、第三款[4]，以及《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（法释[2017]10 号）（下称“《侵犯公民个人信息案件司法解释》”）第四条[5]的规定，违反国家有关规定，在履行职责、提供服务过程中非法收集、获取公民个人信息的，构成侵犯公民个人信息罪。这里的“违反国家有关规定”，根据《侵犯公民个人信息案件司法解释》

[1] 肖信仔：《中国电信的征信之旅》，来源《东方财经》，访问地址：https://m.hexun.com/tech/2015-12-16/181226620.html，访问时间：2019 年 9 月 18 日 14:26。
[2] 何渊等：《大数据战争——人工智能时代不能不说的事》，北京大学出版社 2019 年 6 月第 1 版，第 5-12 页。
[3] 米格 本妹：《大量数据公司被抓，几十家被列入调查名单：“这只是前戏”》，来源一本财经公众号，访问地址：https://mp.weixin.qq.com/s/cfLrpEO1SyJf5nDuz7760w，访问时间：2019 年 9 月 18 日 14:55。
[4] 第二百五十三条之一【侵犯公民个人信息罪】违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。
[5] 第四条 违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

第二条[6]的规定，应理解为包括法律、行政法规、部门规章有关公民个人信息保护的规定。这些规定散见于各层级各部法条中，有综合性的如《网络安全法》，有针对特定经营领域的如《电子商务法》，有针对特定对象的如《儿童个人信息网络保护规定》，不一而足。考虑到大数据与网络的不可分性，《网络安全法》中对收集公民信息的要求在此具有较高的适用性和适用上的一般性。其要求主要包括：

（1）网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。（第二十二条第三款）

（2）网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。（第四十一条第一款）

（3）网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息。（第四十一条第二款）

如果违反上述要求及其他法律、法规、规章中有关收集个人信息的限制收集公民个人信息，即属违法，达到一定的量则构成刑事犯罪。

2.通过爬虫技术获取数据的刑事风险

网络爬虫，是一种“按照一定的规则，自动地抓取万维网信息的处程序或者脚本。”[7]作为一种技术手段，其本身是中立的，并不存在刑事上的违法性。而且对于处在产业链上游的大数据公司来说，网络爬虫技术是获取数据非常常见的一种手段。但本轮打击风暴中，爬虫企业占了大头，那么，大数据企业运用爬虫技术获取数据在什么情况下触刑？

在这里，我们讨论的是爬取网页上公开信息的爬虫技术，而非突破他人服务器、取得后台数据的黑客技术。后者具有明显的刑事违法性，而前者往往让人迷惑，既然是网页上的公开信息，爬虫行为还可能会具有刑事法律风险吗？答案是肯定的。从目前涉刑的案例和业内讨论来看，运用爬虫技术获取数据可能触犯的罪名主要有三类：第一类，危害计算机信息系

[6] 第二条 违反法律、行政法规、部门规章有关公民个人信息保护的规定的，应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。
[7] 游涛、计莉卉：《使用网络爬虫获取数据行为的刑事责任认定——以“晟品公司”非法获取计算机信息系统数据罪为视角》，载《法律适用》2019 年第 10 期，第 5 页。

统类犯罪，主要是非法获取计算机信息系统数据罪[8]、破坏计算机信息系统罪[9]；第二类，侵犯公民个人信息罪；第三类，侵犯商业秘密、侵犯著作权罪等其他罪名。

第一类罪名中的“非法获取计算机信息系统数据罪”是爬虫技术有关的刑事案件中最常出现的罪名。对于这一罪名的判断逻辑，可以参考“晟品公司非法获取计算机信息系统数据案”中主审法官游涛的观点：[10]第一步，评判网络爬虫程序的爬取行为是否获得合法授权，这里主要考虑的是被爬的网站对爬虫技术是否进行授权以及授权的范围，需关注反爬虫技术手段及设定爬虫规则的 robots 协议，而网站所包含的用户信息中用户的授权/同意与否以及范围，笔者理解其意为隐含在网站的保护范围之中，由网站的授权及范围间接体现出来[11]。第二步，评判网络爬取行为是否属于非法获取计算机信息系统数据罪的侵入行为，判断标准包括直接的采取技术手段进入他人计算机信息系统，也包括更宽泛的未征得他人同意或者授权、即违背他人意愿进入他人计算机信息系统。第三步，评判爬取的内容是否属于刑法进行保护的对象，具体到“晟品公司案”中，即需要考察“公开信息”（APP 上用户可以自由观看的视频）是否属于“共享数据”，这也是该案件宣判后受到较大关注的主要原因之一。

同时，如果采用爬虫技术造成了他人计算机信息系统不能正常运行的后果，且严重程度达到法定标准，还可能构成破坏计算机信息系统罪。例如，前面提到的公信宝，其旗下产品可以爬取用户央行的征信数据，曾因此导致央行征信系统卡顿，这样的行为就可能会涉及到破坏计算机信息系统罪。

[8] 《刑法》第二百八十五条第二款：【非法获取计算机信息系统数据、非法控制计算机信息系统罪】违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。第四款：单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

[9] 《刑法》第二百八十六条：【破坏计算机信息系统罪】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

[10] 参考游涛、计莉卉：《使用网络爬虫获取数据行为的刑事责任认定——以“晟品公司”非法获取计算机信息系统数据罪为视角》，载《法律适用》2019 年第 10 期。其中，作者游涛系该案主审法官，由于该案适用了认罪认罚程序，从判决书来看，辩护中并未提出太多针对实体犯罪构成问题的意见，所以判决书本身对爬虫技术构成该罪的法律问题没有进行一般性的、体系化的说理。后在这篇文章中，游涛法官对该案进行了点评，对相关法律问题进行了梳理，从了解裁判观点的角度来看，具有较强的参考价值。

[11] 对该理解，前引文第 5 页称：“但是，从尊重信息提供者的意愿，并维护其隐私权以及数据资源保护等目的出发，网站有义务也有权利保护其数据资源以及使用者的个人信息和隐私不被侵犯。”之后便谈及网站上应用的反爬虫技术，笔者基于该行文逻辑，作此理解。

第二类罪名侵犯公民个人信息罪，评判标准仍然与第 1 点“自行收集用户数据的刑事风险”中所述一致，在爬取网页公开信息的爬虫技术语境下，多指用户是否主动公开其信息的问题，不再赘述。

第三类罪名与爬虫技术本身的关联度没有那么直接，爬虫技术只是犯罪手段之一，爬取数据的主观目的、方式、内容和后续行为是被关注的重点。

3. 取得二手数据的刑事风险

产业链中下游的大数据企业常常需要从其他握有一手数据的数据公司处取得数据，也就是取得二手数据。根据目前案例来看，这一过程中最常涉及的刑事罪名仍然是侵犯公民个人信息罪。

根据《刑法》第二百五十三条之一第三款和《侵犯公民个人信息案件司法解释》第四条的规定，窃取或者违反国家有关规定通过购买、收受、交换等方式获取公民个人信息的，构成侵犯公民个人信息罪。购买、收受、交换是实践中比较常见的非法获取公民个人信息的方式[12]。在前面提到的数据堂一案中，涉案人员便是通过购买的方式从上游非法取得公民个人信息，进行提纯后销售给他人，从而具有两个阶段的违法性。

在这次大数据行业整治潮开始后，很多获取二手数据的大数据企业纷纷通过要求上游数据提供商签订“合法保证书”、“合法承诺书”等文件的形式企图规避风险。那么这种方式是否有效？这延伸出两个问题：第一，合规审查的必要性和深度；第二，信息权利人“知情同意”的刑事违法阻却效力。

对第一个问题，因为购买、收受、交换这类行为与窃取不同，本身是中性的，并不直接具有明显的违法性，特别是如果取得二手数据后用于合法经营活动（例如经同意的信息推送和广告营销），或者仅对获取数据这一阶段进行评价，其刑事违法性就更难判断。一般认为，侵犯公民个人信息罪要求主观方面具有故意，不要求特定的目的和动机，如果上游出售、提供数据的一方确实是非法收集、获取的数据、中下游大数据企业又确实获得了这样侵犯公民个人信息的二手数据，该取得二手数据的一方是否有侵犯公民个人信息的主观故意就成为是否具有刑事违法性的主要因素，需结合实际情况综合判断。目前并无法律法规或司法解释对此进行明确细致的规定，也未见公开裁判文书中确立的受到广泛认可的细节标准，仅

[12] 相关案例可参考喻海松：《网络犯罪二十讲》，法律出版社 2018 年 5 月第 1 版，第 219 页脚注②、③。

能根据案情具体问题具体分析。可以想象的是，数据获取方是否为整个数据链条犯罪的一环并具有全过程的共谋、从获取的二手数据中是否能明显看出初始收集、获取数据的不正当性而多次交易的、提供方具有明显可疑身份且结合其他情况应当能判断数据来源不合法的（例如上游以其具有电信运营商员工身份为宣传点）等等这些情形都会成为考量的重点。反过来，对于一家确实合法合规的获取二手数据的企业来说，需要考量的问题是，如何避免商业风险变成刑事法律风险。“合法保证书”、“合法承诺书”显然是为了避免这种风险的方式之一，但在很多情况下并不足以达到目的。这里的目的至少有两方面，一方面是案发后作为隔离刑事责任的有效辩护依据；另一方面是实质上预防获取非法的数据，而为后者采取的努力能够有助于前者的实现。要实质上预防获取非法的数据，有赖于建立获取数据环节的合规审查机制。这一机制所含措施包括不限于从合作初期起对合作方资质、能力、工作机制、合规机制、违法犯罪背景等的考察，合作时对对方收集数据合法性、合规性的要求及书面确立、定期检查，获取数据时对数据来源的抽查、对数据形式的审查等等。特别在目前行业大清洗的背景下，我们认为建立合规审查机制是有必要的。接下来的问题自然就是，合规审查要去到什么样的深度？比如作为接受数据的一方，要求提供数据一方必须取得数据权利人的明确、真实同意，这是数据合规的题中之意。但对于接受数据一方来说，提出要求并签在合约里、甚至要求对方出具承诺书是否已经足够？还是需要对方提供数据权利人明确同意的证明材料？如果需要，证明材料要提供到什么程度？等等。这一问题目前尚不明确，日后如有相应合规方面的行业标准出台，可能可以成为重要的参考。

第二个问题是第一个问题的必然延伸。获取二手数据的合规审查，必然涉及到源头数据获得者是否取得了数据权利人同意的问题。这一问题之前常在这样的语境下出现：不法分子专门向老人、受教育程度比较低、收入低的人群购买他们的个人信息用以开设网店，并要求出卖人签订相应授权文件，之后用这些网店进一步售假、诈骗等。在这种情况下，不考虑想象竞合等问题，不法分子已经取得了数据权利人的同意，是否还构成侵犯公民个人信息罪呢？这个问题目前尚未见到公开裁判文书作出明确解答，学术界中更多认为同意并不一定都能完全阻却刑事违法性，还需结合整体行为的实质评价、社会公共利益问题、获取书面同意的形式合法合规性、获取信息是否符合合法、正当、必要等行政法律法规要求等等综合判断，[13]情形较为复杂，在此不做展开。

[13] 可参考高艳东：《经同意买卖个人信息也属违法犯罪》，载《检察日报》，2018 年 8 月 15 日号。

二、使用数据阶段的刑事风险

无论采取什么方式获得数据，以及数据经过多少重的流转，最终都会落地到终端使用者手中。那么，在使用数据过程中，又是否会涉及刑事风险呢？

根据法律法规和司法解释的规定，在侵犯公民个人信息罪中是没有包含非法使用数据问题的，也就是说，如果在获取和对外提供数据阶段合法合规，纯粹的非法使用数据，并不构成侵犯公民个人信息罪。例如，一个第三方支付机构，基于国家法律法规的要求对注册用户进行实名核验，之后自行利用实名核验中取得的个人信息进行诈骗，具有明显的刑事违法性，但按现行法律法规很难用侵犯公民个人信息罪来评价。据了解，在《刑法修正案（九）》的立法过程中，曾有专家学者建议将非法使用公民个人信息罪入刑，但最终未被采纳；[14]《刑法修正案（九）》公布后，这一点也受到一些诟病。[15]

虽然非法使用数据的行为本身不能以侵犯公民个人信息罪来规制，但该行为仍然可以通过其他罪名进行刑事规制，例如前面说到的例子，可以诈骗罪进行论处；再如合法取得受害人家庭、车辆安保信息并利用来行窃的信息公司，可以盗窃罪来论处。

总的来说，非法使用数据而引发刑事风险的行为往往有很明显的刑事违法性，对于一般合法经营的大数据企业来说，这方面的刑事风险一般较小。

三、数据流出阶段的刑事风险

既然有获取二手数据的一方，自然有提供这些数据的一方。这些数据的流出包括主动对外提供数据，例如通过出售、交换、供给方式向他人提供数据，也包括被动地向外流出数据，例如常见的被黑客、内部员工盗窃数据放暗网上卖。这一过程可能遭遇的刑事风险也是大数据企业比较关心的问题。

1. 主动的数据流出

（1）非法提供公民个人信息

根据《刑法》第二百五十三条之一以及《侵犯公民个人信息案件司法解释》有关规定，违反国家规定，向他人出售或者提供公民个人信息，情节严重的，以及在履行职责或者提供

[14] 喻海松：《网络犯罪二十讲》，法律出版社 2018 年 5 月第 1 版，第 233 页脚注②。
[15] 庄绪龙：《侵犯公民个人信息罪的基本问题——以“两高”最新颁布的司法解释为视角展开》，载《法律适用》，2018 年 07 期。

服务过程中获得的公民个人信息出售或提供给他人的，构成侵犯公民个人信息罪。这里的提供既包括向特定人提供公民个人信息，也包括通过信息网络或者其他途径发布公民个人信息，即向不特定公众提供公民个人信息。这里的“违反国家规定”与第一部分所述一样，仍包含国家层面的法律、行政法规、部门规章。在有关法律法规司法解释中，对对外提供公民个人信息的最主要要求就是“经被收集者同意”，或者对外提供的是经过处理无法识别特定个人且不能复原的信息，也即不能识别到特定个人的信息不属于刑法保护的公民个人信息范畴。

目前出现了一种新的规避风险手法，大数据公司对外提供数据时，将涉及公民隐私的数据拆分成不同部分，每段均无法识别到个人，获取信息的一方再自行整合起来，形成完整的公民个人信息数据。[16]这样的拆分信息因为能够复原为完整信息，本质上仍然具有侵犯公民个人信息违法犯罪的特性，故并不能阻断由此产生的刑事风险。

（2）为合法经营活动提供经匿名化的公民个人信息

如前一部分所述，因提供“经过处理无法识别特定个人且不能复原”的信息不在刑事打击的范畴中，对于为合法经营活动的下家提供经过处理的个人信息成为很多大数据公司维系经营的主要方式。

“经过处理无法识别特定个人”与欧盟《数据保护通用条例》（GDPR）中匿名化（Anonymization）的含义基本类似，都是将收集、利用、存储和与其他组织实体共享的数据中的个人信息移除的工具。这在多国法律中都被视为公民个人信息保护的一种例外。[17]我国法律条文中的“识别”应包括直接识别和间接识别，对间接识别的要求即为“不能复原”。但技术上来说，如果对间接识别的深度不做限制，那么即使是经过匿名化处理的信息，只要有足够多的的信息互相结合后，都有可能对特定个人具有比较强的识别性，而这“既未反映企业的实际商业实践，也不利于平衡个人权利保护和商业模式发展”，从而导致“高昂的社会成本”。[18]因此，对这种匿名化的要求的边界到底去到哪里，也就是说“不能复原”的标准到底有多高，是大数据企业非常关心的问题。

[16] 何渊等：《大数据战争——人工智能时代不能不说的事》，北京大学出版社 2019 年 6 月第 1 版，第 12 页。
[17] 张晨原：《数据匿名化处理的法律规制》，载《重庆邮电大学学报（社会科学版）》，2017 年 06 期。
[18] 何渊等：《大数据战争——人工智能时代不能不说的事》，北京大学出版社 2019 年 6 月第 1 版，第 39-40 页。

目前，我国法律法规尚未对这块进行明确的规定，在各大大数据交易所中，虽有意识到这一问题重要性的，但对“匿名化数据处理却缺少具体的描述”。[19]而欧盟和其他信息保护领域立法相对成熟的国家和地区，常常采用匿名化风险分级、“蓄意侵入者”检验等方式来规范匿名化的标准和要求。对我国大数据企业而言，要在目前法律规定比较原则性的情况下规避自身的刑事风险，有必要建立相应的风险防控机制，包括可以自设匿名化处理风险分级机制并设定对应的交易对象，平衡技术、成本与风险之间的关系；另外针对交易对象进行合理的事前调查和事中检查，并在双方的合作协议及其他文件中提出相应的反再识别要求[20]等。

2. 被动的数据流出

对于很多合法掌握大量公民个人信息数据的企业来说，内鬼泄露和黑客攻击是令他们十分头疼的问题，也是被动的数据流出的主要渠道。在这种情况下，作为本身并无意于违法提供数据的公司来说，是否还要因为这些情况而承担刑事责任，以及如何规避可能存在的刑事风险是他们比较关心的问题。

（1）拒不履行信息网络安全管理义务罪

《网络安全法》第四十条[21]和四十二条[22]规定网络运营者应当建立健全用户信息保护制度，采取技术措施和其他必要措施，来确保个人信息安全，防止信息泄露等。但如果这些公司本身并无泄漏公民个人信息数据的故意（包括直接故意和间接故意）及行为，即使是由于过失未能充分履行信息网络安全管理的义务，导致了公民个人信息泄露，仍然不会构成侵犯公民个人信息罪。但根据《侵犯公民个人信息案件司法解释》第九条的规定：“网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一的规定，以拒不履行信息网络安全管理义务罪定罪处罚。”即可能处 3 年以下有期徒刑、拘役或者管制，并处或者单处罚金。这一刑事法律风险相对是好防范的，它具有几重门槛，首先需要具有行政上的违法性，其次要经监管部门责令采取改正措施而拒不改正，并且

[19] 张晨原：《数据匿名化处理的法律规制》，载《重庆邮电大学学报（社会科学版）》，2017 年 06 期。
[20] 小法：《匿名化：数据交易的合规基石》，载“互联网法务那些事”微信公众号，3 月 17 日发。
[21] 第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。
[22] 第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。
网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

还要造成严重后果，因此，对于合法、谨慎经营的大数据企业来说，遵纪守法，接受监管部门的整改要求，能在很大程度上防范该风险。

（2）良好的合规体系有助于隔离员工犯罪与单位责任

除了拒不履行信息网络安全管理义务罪以外，大数据企业往往更为关心另一个问题：我的员工中出了内鬼，擅自把未脱敏的公民个人信息数据卖给了第三人，公司是否因此而面临刑事法律风险？

我们认为，刑事法律风险不仅仅是最终获刑的风险，被卷入刑事案件程序本身就是一种风险，有的时候甚至会严重影响到企业的正常经营。因此，为了有效防范由于员工泄密导致的刑事风险，有必要建立完善的内部合规体系。这一方面可以从源头上截断员工窃取信息并外传的可能性，从而从根本上防范企业的刑事风险，另一方面可在企业万一被卷入刑事案件后，能够充分自证企业本身并不存在违法犯罪行为。合规体系包括技术和法律两方面，并涵盖公司制度、系统建设、员工教育、监督检查等企业运营的各方面，需要不断发展完善。

四、如何有效防范企业和高管的刑事风险

1.单位犯罪与高管责任的问题

最近经常听到大数据公司管理人员问的一个问题是：如果我公司的员工犯罪了，我们公司要承担责任吗？以及进一步的，如果我们公司构成刑事犯罪了，我作为公司的法定代表人/CEO/业务经理等等需要承担责任吗？这个问题其实不独存在于大数据行业，所有可能触犯刑法中规定有单位犯罪罪名的企业都可能遇到。

简单来说，单位犯罪需要具有两个条件：第一是以单位名义实施犯罪，第二是违法所得归单位所得。这里的单位，也包括了单位的分支结构或者内设机构、部门。[23]因此，盗用单位名义实施犯罪，违法所得由实施犯罪的个人私分的，不构成单位犯罪。[24]所以数据堂案件中，最终没有对单位进行定罪。另外，个人为进行违法犯罪活动而设立的公司、企业、事业单位实施犯罪的，或者单位设立后，以实施犯罪为主要活动的，不以单位犯罪论处。[25]本文中提及到的绝大部分罪名（除了盗窃罪、诈骗罪这类与大数据犯罪本身并不直接相关的罪

[23] 参见最高人民法院《全国法院审理金融犯罪案件工作座谈会纪要》（2001 年 1 月 21 日）。
[24] 参见最高人民法院《关于审理单位犯罪案件具体应用法律有关问题的解释》（1999 年 7 月 3 日 法释[1999]14 号）第三条。
[25] 同上，第二条。

名）在刑法中都规定了单位犯罪，因此，如果符合单位犯罪的条件，单位可能会因此承担刑事责任。

单位犯罪中同时涉及到“直接负责的主管人员和其他直接责任人员”也将承担刑事法律责任的问题。“直接负责的主管人员”，是在单位实施的犯罪中起“决定、批准、授意、纵容、指挥”等作用的人员，一般是单位的主管负责人，包括法定代表人。“其他直接责任人员”，是在单位犯罪中“具体实施犯罪并起较大作用”的人员，既可以是单位的经营管理人员，也可以是单位的职工，包括聘任、雇佣的人员。[26]由此可知，具体的头衔名称并不能实质性决定单位中的高管是否将在单位犯罪中承担刑事责任，其在单位犯罪中的地位、作用和实际实施的犯罪情节才是判断是否将承担个人责任的关键。

2. 建立完善的合规体系以防范刑事风险

在前面的内容中我们也多次提到，靠让上家签署《合法承诺书》等文件，或者将涉及公民个人信息的数据拆分后卖出去，这些投机取巧的办法并不足以防范大数据企业的刑事风险。在大数据企业确实打算进行合法合规经营的前提下，建立完善的合规体系有助于防范大数据企业直接承担刑事责任和避免卷入刑事程序的风险。合规体系是技术与法律相结合的综合合规体系，并需根据法律法规、行业标准、技术进步不停地发展完善，同时应当涵盖大数据运营的全流程。

3. 外部团队的合规审查

由于目前大数据领域的法律法规和行业标准尚未形成具体、完备的体系，而大数据行业的业务范围又不断推陈出新，几乎很难立即有一个全行业公认的合规体系可以涵盖各方各面的刑事风险。而一些企业内部人员的思维还停留在利润丰厚、自以为法不责众的灰色地带，这些都反过来体现了外部合规团队的重要性。聘请有经验的外部团队（应包含技术专家团队和法律团队）进行合规审查，一方面有助于整合行业经验和外国立法及行业标准方面的经验，帮助建立尽量完善、贴合的合规体系；另一方面可以充分发挥其中立性，不受干扰地对企业刑事合规状况进行评估，在需要的时候甚至可以介入调查，也可以在企业万一卷入刑事案件中时提供专业上的帮助。此外，外部合规审查本身也是欧美等在该领域具有较先进合规经验国家和地区中企业合规制度的重要组成部分。

[26] 参见最高人民法院《全国法院审理金融犯罪案件工作座谈会纪要》（2001 年 1 月 21 日）。