
Merits Tree
植德律师事务所
植德观点
数据合规
Data Compliance

目录

系列一：透视 GDPR

作者：朱宣烨 王伟 王啸 贾莉莉

不久之后，欧盟《一般数据保护条例》（General Data Protection Regulation，下称 GDPR）将正式生效。几乎“全网”覆盖的适用范围、宽泛的个人数据保护义务以及可达全球营业额 4%的超高额的处罚金额，使得每个中国企业都有必要思考如下问题：一、GDPR 是否会对企业的业务造成影响；二、影响的程度有多大；三、企业应该如何应对。

就此，植德律师事务所与欧洲合作律所组织了在数据合规方面经验丰富的律师一道进行了相关的研究，并将在随后通过一系列专题进行就 GDPR 以及中国法下的数据合规问题进行解读。

一、GPDR 的前生今世

广受热议的 GDPR 并非横空出世。早在 1995 年 10 月 24 日，欧洲议会与欧盟理事会即颁布了《关于涉及个人数据处理的个人保护以及此类数据自由流动的第 95/46/EC 号指令》(以下简称“数据保护指令”)，以协调与统一成员国数据保护法，促进个人数据在成员国之间自由流动，但是数据保护指令的规定仍需各成员转化为国内法后实施。此后欧盟陆续又出台了一系列规范对个人数据保护进行规定。随着科技的迅速发展和全球化进程，数据保护指令难以实现平衡个人信息保护和促进个人信息流动的立法宗旨。因此，2012 年 1 月 25 日欧盟委员会公布 GDPR 草案; 2014 年 3 月 12 日欧洲议会通过了 GDPR 的首次审读; 2015 年 6 月 15 日欧盟理事会通过首次审读的版本。并最终于 2016 年 4 月 8 日和 4 月 16 日由欧盟理事会和欧洲议会通过，替代了数据保护指令。

GDPR 延续了数据保护指令的保护个人信息和促进个人数据流动的二元化的立法宗旨，但是对内容进行了扩充和调整，GDPR 的正文部分涉及的法律条款从数据保护指令的 7 章共 34 条增加到目前的十一章共 99 条，而且序言部分附有长达 173 条的鉴于条款用以辅助对 GDPR 的理解适用。

二、史上最严格的规范内容

（一）适用范围广

1、地域范围：宽泛的域外效力。

有业务机构设在欧盟境内，并从事个人数据处理的组织受 GDPR 管辖自不待言。但是 GDPR 已经将自身的适用范围扩展到欧盟境外，规定了多个连接点，具体而言：

如果非欧盟成员国企业（下称“数据控制者或数据处理者”）在欧盟境内未设立业务机构，但却处理欧盟境内的个人数据，为欧盟境内的数据主体提供货物或服务，无论数据主体是否被要求付费，应适用 GDPR。根据 GDPR 相关规定，要确定数据控制者或处理者是否向欧盟主体提供货物或服务，主要是确定数据控制者或处理者是否存在明显想要为欧盟一个或多个成员国的数据主体提供货物或服务的意图。如果仅可访问数据控制者或处理者等在欧盟的网站、电子邮件地址或其他联系方式，或使用数据控制者所在国通常使用的语言，并不足以确定存在提供货物或服务的意图；但如果使用一种或多种欧盟成员国通用的语言或货币，且可以使得数据主体根据该等语言订购商品和服务，或提及位于欧盟的客户或使用者，实质上可能属于存在向欧盟的数据主体提供商品或服务的意图。[1]

如果非欧盟成员国企业对数据主体在欧盟境内的行为进行监控的，应适用 GDPR。根据 GDPR 相关规定，这里的“监控”等同于“用户分析”：即在互联网上跟踪个人数据，用类似于“画像”的数据处理技术，“描绘”个人信息，分析预测个人偏好、行为模式或个人态度。所以，如果非欧盟成员国企业如果采用 cookies 等方式“监控”欧盟居民或在欧盟境内发生的个人行为，处理个人监控数据，该企业也适用 GDPR 规定并受监管。[2]

根据国际公法的规定，指向将 GDPR 作为准据法的。

2、主体范围：直接适用于数据控制者和数据处理者。

数据保护指令仅适用于数据控制者[3]（Data Controller,决定数据加工目的和途径的机构）。GDPR 规定其适用于数据控制者或者数据处理者（Data Processor，代表数据控制机构处理数据的实体）对个人数据的处理[4]。也就是说数据处理者在一些数据处理的核心环节受到监管，GDPR 针对数据处理者规定了诸如信息安全措施、未经许可不能转委托、记录保存、协助义务等一系列义务。而且，GDPR 明确规定信息处理者如违反数据保护的义务则可能受到行政处罚[5]或承担民事责任[6]。

（二）对数据处理的要求更严格

1、对取得数据主体的有效同意提出了详细的要求[7]。

同意必须清楚、有别于其他事项，并以清晰易懂的形式提供，使用清晰明了的语言。也即公司不能继续使用含混不清的术语和法律术语堆砌的条件，同意的要求必须清晰易懂，必须说明数据处理的目的。
同意必须很容易撤回，如同提供“同意”操作一样方便。
同意应当基于数据主体自由意志做出，且同意处理的数据范围没有超过必要的限度。

2、提出了记录数据处理的要求[8]

GDPR 要求数据控制者和处理者必须记录数据处理活动的过程、相关人员和数据接收者。这一规定不适用于员工数量低于 250 人以下的企业或机构，除非上述企业或机构处理数据方式可能给数据主体带来高风险，威胁他们的权利和自由。

3、提出数据保护影响评估[9]和事先咨询制度[10]

如数据处理行为的性质、范围、内容和目的可能对自然人的权利和自由产生高风险时，数据控制者在进行数据处理之前应当进行影响评估（并做记录）以此替代将数据处理活动（以及类似于国际数据传输等活动）通告数据保护主管机构的一般性责任。一次评估可能解决一系列带来类似高风险的信息处理操作。风险仍然较高的领域，仍需咨询监管机构。

4、要求设立数据保护官（DPO）[11]

GDPR 规定，在符合特定条件的情况下，必须任命 DPO，该等条件包括控制者和处理者需要经常系统地监控数据主体，而且监控的规模较大、数据种类特殊或涉及到刑事定罪以及违法行为。

（三）新增多项数据主体权利

1、信息泄露通知[12]

GDPR 规定，如果发生数据泄露事件，泄露通知必须在知晓数据泄露事件发生后的 72 个小时内向主管监管机构报告。数据处理者还需要在第一时间通知用户和数据控制者。

2、访问权[13]

GDPR 强调数据透明化，数据主体有权从数据控制者那里获取信息，以确认数据控制者是否要对与他们相关的个人数据进行处理、处理地点、处理目的。此外，控制者应以电子格式免费提供一份个人数据的副本。

3、被遗忘权[14]

被遗忘权赋予数据主体权利，让其可以要求数据控制者清除他/她的个人数据，停止进一步传播数据，并尽可能使第三方停止处理数据。GDPR 第 17 条中概述了数据删除条件，包括拟删除的数据与原数据处理目的不再相关或数据主体撤销同意。

4、可携带权[15]

GDPR 个人数据的可携带权，赋予数据主体接收与自己相关的数据，并有权将这些数据发送给另一个数据控制者。

5、隐私保护设计[16]

GDPR 要求控制者应以有效的方式实施适当的技术和组织措施，满足本条例的要求，保护数据主体的权利。即在系统设计起步就纳入数据保护，而不是系统开发完成后再增加保护。

（四）严厉的法律责任

1、行政处罚：

GDPR 的行政处罚金额极具视觉冲击力。罚金仅仅区分为两档，既适用于数据控制者又适用于数据处理者，分别针对不同的违法行为：

处以 1000 万欧元或者上一年度全球营业收入的 2%，二者取额度高者；其主要针对：违反隐私保护设计，以及默认隐私保护，没有实施充分的 IT 安全保障措施、违反数据泄露通知要求等等[17]；

处以 2000 万欧元或者企业上一年度全球营业收入的 4%，二者取额度高者。其主要针对：违反数据处理原则，

数据处理没有合法基础，违法同意要求，侵害数据主体的合法权利等[18]。

2、民事责任：

民事责任中，为了确保数据主体利益的实现，确立“连带责任＋过错推定”的模式。

就对外（数据主体）责任的承担上，为了确保数据主体获得有效赔偿，GDPR 规定数据控制者和数据处理者就信息主体的全部损失承担连带责任[19]。

就内部的责任分配上，数据控制者就其违反 GDPR 规定的数据处理行为担责；数据处理者只对其未遵守 GDPR 规定的特别是针对数据处理者的义务或者其超过数据控制者的合法指示的行为造成的损失担责[20]。

三、“它亦温柔”

需要注意的是，GDPR 亦并非一味地关注数据主体的绝对权利，而是强调应当根据比例原则，平衡数据权利和其他根本性权利或利益。[21]典型的表现有：

（一）制度本身体现了利益的平衡和促进流通的价值选择

1、跨境数据流动

发生在欧盟内的数据跨境流动是被允许的，但是对于向第三国或者国际组织进行数据转移须符合一定的情形，而 GDPR 对于跨境数据流动较之数据保护指令，提出了多条更加可行的、有效的途径：

欧盟委员会通过检查确定该第三国、第三国的特定区域或者国际组织是否不再具有充分决定保护水平[22]。

有约束力的公司规则[23]：经审核批准有约束的公司规则(Binding Corporate Rules, BCR)，以事业群或从事联合经济活动的集团企业在集团内部实现数据的跨境转移。该机制最早由欧盟第 29 条工作组发展而来，是欧盟委员会提出的标准化格式合同的一个替代选择。

标准合同条款[24]：欧盟委员会或者监管部门根据 GDPR 程序批准的数据保护条款。

其他：数据主体被告知可能的风险后明确表示同意、执行合同所必要、为了公共利益等[25]。

2、行政处罚

行政罚款数额的确定应当考虑行为的性质、主观状态、为减少数据主体损失而采取的措施、责任的轻重程度、是否存在违法行为等等 11 项综合考虑因素，来确定罚金金额[26]。

GDPR 背景引言中也强调了比例原则，主张根据案件具体情况的考虑，做出适当的罚款金额[27]。 并明确，如果“如果违法行为不会对有关数据主体的权利构成重大风险，在这种情况下，可以用警告（warning）代替罚款。

（二）通篇的例外条款

根据笔者的统计，GDPR 中涉及例外或者克减的条款达 38 条。几乎贯穿条例始终，体现了平衡的思想。

数据处理的豁免条款[28]。

数据主体具体权利的限制条款：引发热议的数据访问权、被遗忘权、数据可携权等条款均有限定条件，远非其定义中的那么绝对。

给予中小企业多种豁免，比如：规模在 250 人以下的中小企业可以豁免数据处理记录义务。

行为准则和认证机制成为数据控制者和数据处理者遵守条例的重要证据，降低举证的成本。

设有“有关特殊数据处理情形的规定”一章，将与表达自由、雇佣关系、宗教等七个事项交由成员国在给定框架内自行制定具体规则。

特此申明：以上分析，仅系我们根据现行法律法规、监管政策及相关案例所做的分析和探讨，并不作为我们对相关事项的法律结论意见。

注：

1 GDPR 序言第 23 条

2 GDPR 序言第 24 条

3 数据控制者(Data Controller)指能单独或联合决定个人数据的处理目的和方式的自然人、法人、公共机构、行政机关或其他非法人组织。其中个人数据处理的目的和方式，以及控制者或控制者资格的具体标准由欧盟或其成员国的法律予以规定。数据处理者(Data Processor)是指为控制者处理个人数据的自然人、法人、公共机构、行政机关或其他非法人组织。

4 GDPR 正文第 3 条

5 GDPR 正文第 83 条

6 GDPR 正文第 82 条

7 GDPR 正文第 7 条

8 GDPR 正文第 30 条

9 GDPR 正文第 35 条

10 GDPR 正文第 36 条

11 GDPR 正文第 37 条

12 GDPR 正文第 33、34 条

13 GDPR 正文第 15 条

14 GDPR 正文第 17 条

15 GDPR 正文第 20 条

16 GDPR 正文第 25 条

17 GDPR 正文第 83 条第 4 款

18 GDPR 正文第 83 条第 5 款

19 GDPR 正文第 82 条

20 GDPR 正文第 82 条第 2 款

21 GDPR 序言第 4 条

22 GDPR 正文第 45 条

23 GDPR 正文第 47 条

24 GDPR 正文第 45 条第 3 款

25 GDPR 正文第 49 条

26 GDPR 正文第 83 条

27 GDPR 序言第 150、151 条

28 GDPR 正文第 2 条

作者简介

朱宣烨　合伙人

业务领域：争议解决、知识产权、大数据
电　　话：010-56500912
邮　　箱：xuanye.zhu@meritsandtree.com

王　伟　合伙人

业务领域：私募基金设立、基金投资、并购、跨境投资、境外发债、区块链
电　　话：010-56500983
邮　　箱：wei.wang@meritsandtree.com

系列二：从个人信息涉诉案件情况看企业数据合规注意要点

作者：朱宣烨 王伟 高阳 王明志

2018 年 5 月 25 日生效的欧盟《通用数据保护条例》（简称 GDPR）因其泛化的管辖权和高额的行政罚款引起了世界范围的关注。对于处于数字化转型的中国企业而言，当务之急是如何建立一套行之有效的大数据合规制度，就此，我们从专业数据库上筛选了 2015 年 5 月 1 日至 2018 年 3 月 1 日期间涉及“个人信息”的民事案例（以下简称案件，或统计案件）并进行统计分析，以期对企业的数据合规有所裨益。

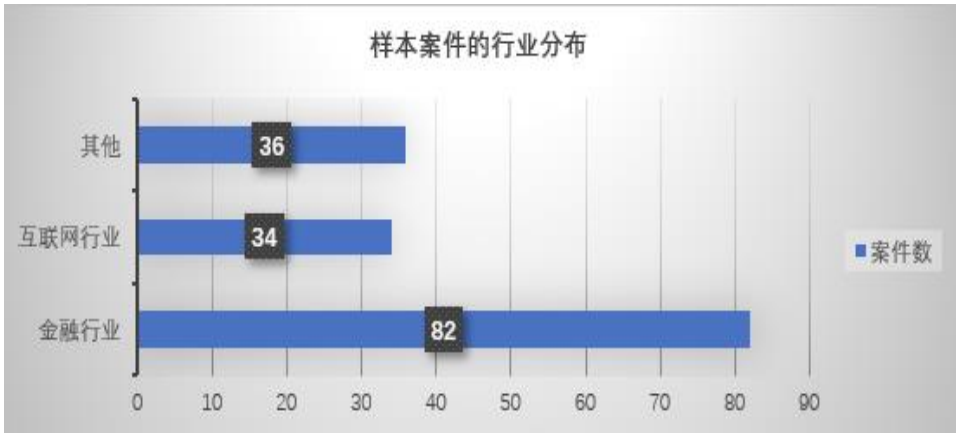
一、样本数据分析概况

（一）涉个人信息的民事案件数量有限

我们系统研究了 146 件涉及个人信息的民事案件，其中侵权纠纷案件 139 件（其中包含 1 件企业间的不正当竞争案件[1]和 1 件企业间的经营秘密纠纷案件[2]），合同纠纷案件共计 7 件。除 2 件案件为企业间纠纷外，其余均为个人与企业之间发生的纠纷。

（二）涉案主体的特点

1、 涉案主体的行业分布集中于金融行业和互联网行业



案件主要集中在对个人信息收集量大、使用比较频繁的领域，其中典型的如金融行业、互联网行业等。

2、涉案主体绝大为数据控制者，但是案件开始关切数据处理者的作用

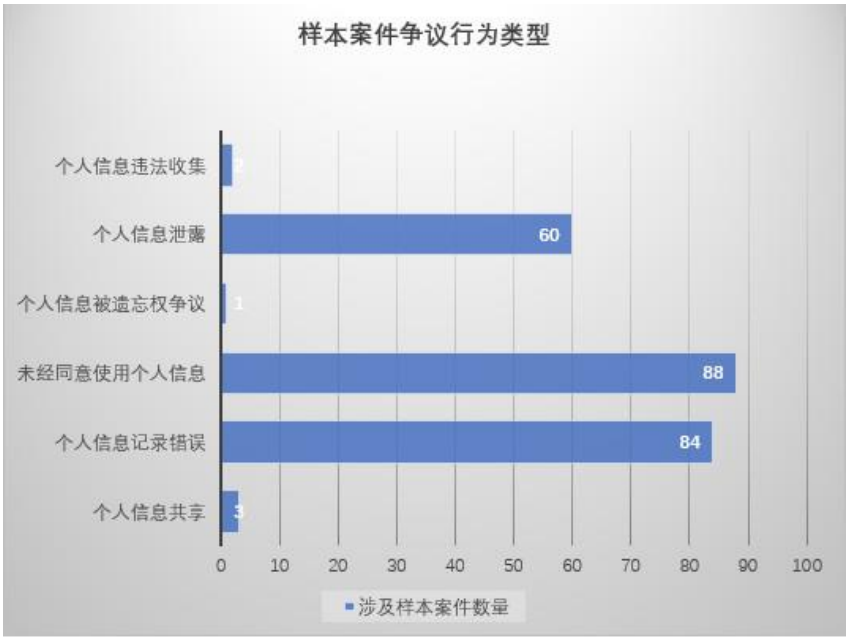
数据控制者和数据处理者是个人信息处理关系中涉及的两个重要主体，不同司法区域的法律对于两者权利义务的边界规定并不完全相同。简单而言，两者的核心区别在于为自己还是为他人目的处理数据，为他人处理数据的一方就是数据处理者。现有案件主体均有数据控制者，仅有两件案件中数据处理者作为共同被告出现。但是很多案件在被告的抗辩意见中开始提及数据处理者，更有案例对于数据控制者和数据处理者的民事责任分担阐述。比如庞理鹏诉去哪儿网、东航的案件中，法院裁判东航作为数据控制者应当对数据处理者中航信的行为担责，同时认定存在信息共享关系的去哪儿网和东航均需对原告个人信息泄露情况担责。

因此，这对于中国企业的合规提出了更高的要求，如何科学、合理的设计合规制度需要每个企业根据自己的行业特点以及业务情况而具体研判。

（三）争议行为

1、争议行为类型集中

现有案件中“个人信息记录错误”以及“未经同意使用个人信息”“个人信息泄露”三类行为涉案数量最多。我们也注意到，涉及个人信息违法收集、信息共享、遗忘权的案件也开始出现。



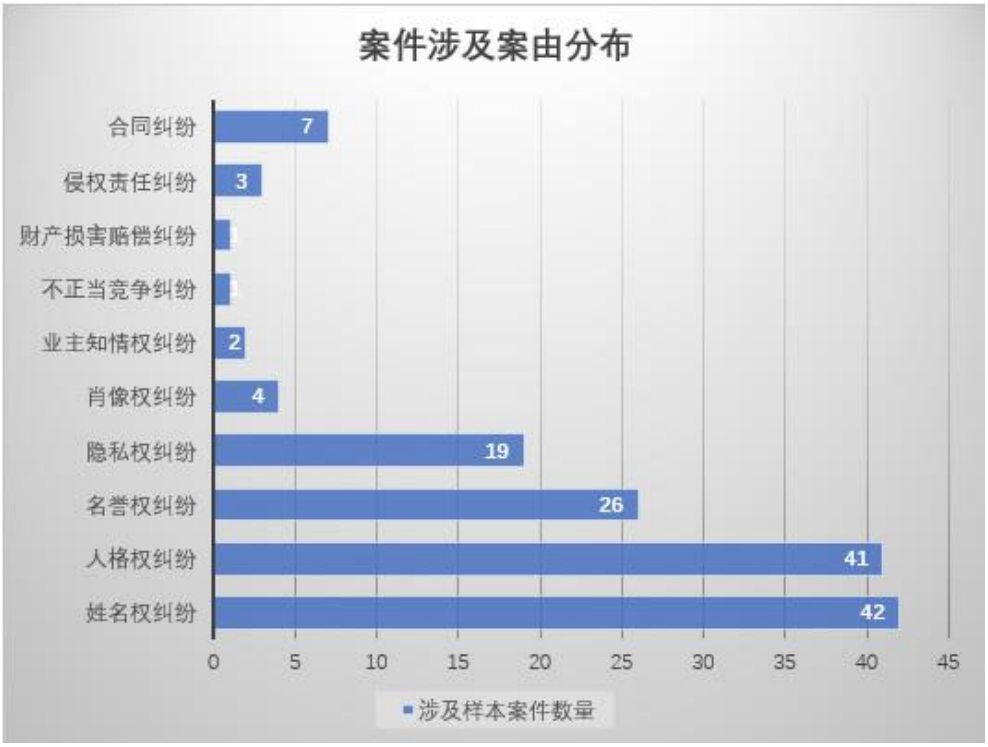
2、典型争议行为类型多样

涉案争议行为具体类型十分丰富，涵盖了个人信息收集、保存、使用等生命周期的全流程。不少案件对于涉案行为的争议背后反映是对个人信息收集使用的商业模式的争议，典型的如朱烨诉百度收集 cookie[3]侵犯隐私权的案件。就此，我们简单梳理了典型案件的争议行为类型以及争议行为表现，以期对正在进行数字化转型的企业有所启发。

序号	争议行为所在环节	争议行为类型	具体的争议行为表现（典型案例）
1	收集	是否是合法收集个人信息	1. 搜索引擎网站利用cookie技术记录和跟踪了搜索过的关键词进行广告投放的行为。[4] 2. 未经同意，擅自使用应用软件筛选、调查数据主体的个人信息的行为。[5]
2	保存	个人信息遭遇泄露	1. 机票信息、酒店信息泄露等等。[6] 2. 网站系统漏洞导致原告信息泄漏。[7]
		遗忘权	百度“相关搜索”显示出的原告曾经的职业经历对原告不利。[8]
3	使用	盗用身份信息开立账户	银行及其工作人员利用数据主体的身份开立账户的行为。[9]
		征信信息错误	数据主体与银行之间没有借款合同关系，但在征信中心却存有数据主体该笔借款的信用不良记录。[10]
		未经同意发送信息，侵犯生活安宁	电商服务平台利用用户在购物时留存的手机信息，给用户手机发送商业短信。[11]
			因银行录入电话号码错误，向与借款无关的原告发送催促还款短信。[12]
			银行通过格式条款约定可以向用户发送与信用卡相关信息并实际发送。[13]
			快递经营者向快递服务过程中收集到的手机号码发送自身电商业务信息。[14]
4	委托处理，共享，转让、公开披露	违法查询，违法披露个人信息	违规或未经同意查询数据主体的个人信息，并且披露给第三方。[15]
		征信信息虽属真实，但是违反依法披露的规定	在中国人民银行征信中心公开原告具有不良信用记录。[16]

（四）适用案由多元

由于我国尚没有独立的侵犯个人信息的民事案件案由，所以涉及个人信息的民事纠纷多取道姓名权、隐私权、名誉权和人格权等其他案由进行诉讼。姓名权纠纷占比高是由于有一个系列案件[17]，有其偶然性。隐私权纠纷仍然是目前与个人信息保护最为密切的案由。《民法总则》颁布之后，人格权纠纷作为兜底的案由，解决了案由的制定晚于个人信息保护需求的实际情况，也反映出个人信息独立于隐私权等既有权利的特殊性。



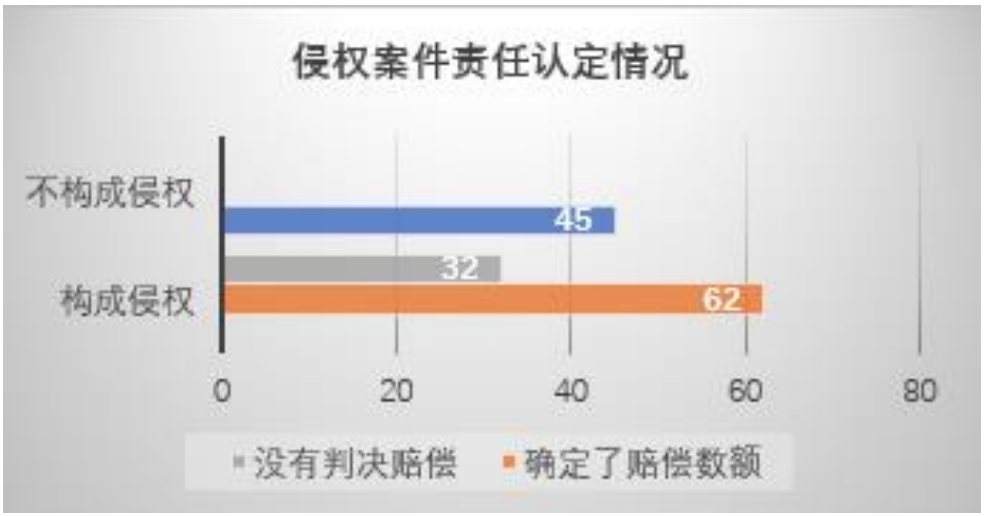
（五）责任认定情况

1、举证责任多由原告方承担

案件显示，事实认定过程中遇到的最大的问题仍是证明的问题。尤其是信息主体，处于信息不对称的弱势地位，举证能力较弱。但目前我国法律没有就涉及个人信息的案件规定专门的举证责任倒置制度，案件事实仍由原告方承担举证责任。上述案件中，仅有 3 件案件中法庭判令由被告承担举证责任。其余 143 件为原告承担举证责任。

2、 认定责任事实的比例分析

统计案件中，侵权类案件 139 件，被认定存在侵权事实的案件数为 94 件。



3、信息共享者共同担责，数据控制者对数据处理者的行为担责或成为趋势

随着各方对个人信息案件特点认识的深入，司法领域的态度发生转变，比如庞理鹏诉去哪儿网、东航的案件中，法院认为东航作为数据控制者应当对数据处理者中航信的行为担责，同时认定存在信息共享关系的去哪儿网和东航均需对原告个人信息泄露情况担责。该案件的判决得到了北京市法院系统的认可和支持。

二、合规提示

我们注意到很多案件的裁判结论直接关系到商业模式的运行。根据对于相关判例的研究我们总结了如下几点作为合规提示。

（一）重视安全合规

从样本案例可知，涉及信息安全问题案件比例达到了样本统计案件数的三分之一。

企业遇到的数据安全问题主要有以下三种情况：

1 由于软硬件设施故障或操作失误造成的数据丢失或者泄露，比如最近的腾讯云故障造成创业公司巨大损失的事件[18]；

2 黑客袭击、病毒入侵导致数据丢失或泄露，比如去年 WannaCry 勒索病毒肆虐事件[19]；

3 内部工作人员恶意泄露或者破坏数据，比如今年 6 月发生的特斯拉员工开发恶意软件进入特斯拉内部生产操作系统，偷取大量数据给第三方[20]。

为应对安全问题，企业应当按照《网络安全法》等法律规范和标准的要求进行安全合规，主要措施有：

1 依据国家标准和安全等级制定企业自身的处理数据操作规范、数据保存规定；
2 对于个人敏感信息，严格控制可接触该信息的人群和流程，对企业内部工作人员管理权限进行分级；
3 确立定期数据安全审计和数据安全风险培训的制度；
4 确立数据安全日常监控制度和应急处理制度，进行符合自身业务类型的数据安全异常点检测，并在出现疑似数据安全问题时及时保留相关证据。

（二）界定好与外包服务提供者、数据共享者权责范围

正如统计案件体现的，外包服务提供者和数据共享者在提高企业商业化使用个人信息效率的同时，也增加了企业自身因个人信息受到侵害而担责的风险。

为此，企业应当注意：

1. 进行数据共享和寻求外包服务时，注重相对方的数据合规情况和资质；
2. 通过合同准确界定各自在参与个人信息处理活动中的作用和主体性质，明确各方具体权责义务；
3. 以及约定对第三方造成损害时的责任承担，内部追偿的范围等。

（三）关注隐私协议的格式合同性质

《合同法》的规定，提供格式条款的一方应当遵循公平原则确定当事人之间的权利和义务，并采取合理的方式提请对方注意免除或者限制其责任的条款，按照对方的要求，对该条款予以说明。提供格式条款一方免除其责任、加重对方责任、排除对方主要权利的条款也会被认定无效。隐私协议属于格式合同，所以隐私协议的条款内容和展现形式可能因其格式条款的性质而被质疑。

朱烨诉百度案的一审判决即认为百度公司细小字体的《使用百度前必读》无法保障用户知情权与选择权。虽然该案的二审判决改变了这种看法，但是随着我国个人信息保护规则的逐步明晰，《信息安全技术个人信息安全规范》等配套标准的逐步出台，对于隐私协议的要求必然日趋严格，所以应引起企业的重视。而比较有效的方

案是参照国家发布的诸如《信息安全技术 个人信息安全规范》等规范标准结合自身行业特点进行制作，对于重要条款和内容利用加粗或加下划线等方式进行提示，对可能限制数据主体权益的条款仔细斟酌。

特此申明：以上分析，仅系我们根据现行法律法规、监管政策及相关案例所做的分析和探讨，并不作为我们对相关事项的法律结论意见。

[1] 北京淘友天下技术有限公司等与北京微梦创科网络技术有限公司不正当竞争纠纷一案（北京知识产权法院（2016）京 73 民终 588 号民事判决书）。

[2] 桂林市培正文化语言培训学校与桂林市斯坦教育咨询有限公司、李立飞侵害经营秘密纠纷一案（参见广西壮族自治区桂林市叠彩区人民法院（2015）叠民初字第 605 号民事判决书）。

[3] Cookie 技术可以被网站应用于跟踪统计用户访问该网站的习惯，例如访问网站的用户名和计算机名、使用的浏览器、访问时间、访问的具体页面、浏览停留的时间。

[4] 北京百度网讯科技有限公司与朱烨隐私权纠纷一案（江苏省南京市中级人民法院（2014）宁民终字第 5028 号民事判决书）

[5] 比如，孙旭东与平安银行股份有限公司深圳市鑫富源投资咨询有限公司隐私权纠纷一案（广东省深圳市福田区人民法院（2016）粤 0304 民初 24741 号民事判决书）。

[6] 比如，林念平与四川航空股份有限公司侵权责任纠纷一案，四川省成都市中级人民法院(2015)成民终字第 1634 号；傅艳与盐城市宇晔酒店管理有限公司隐私权纠纷一案（江苏省东台市人民法院(2015)东民初字第 1887 号民事判决书）

[7] 周新营与上诉人中国保险监督管理委员会、北京中科汇联科技股份有限公司网络侵权责任纠纷一案（海南省三亚市中级人民法院（2016）琼 02 民终 375 号民事判决书）

[8] 原告任甲玉诉被告北京百度网讯科技有限公司（以下简称百度公司）侵犯名誉权、姓名权、一般人格权纠纷一案（北京市海淀区人民法院（2015）海民初字第 17417 号民事判决书）

[9] 马×与盛京银行股份有限公司北京五棵松支行等隐私权纠纷（北京市海淀区人民法院（2016）京 0108 民初 8187 号民事判决书）

[10] 原告李进旺诉被告大同县农村信用合作联社名誉权纠纷案件（山西省大同县人民法院（2016）晋 0227 民初 63 号民事判决书）

[11] 赵炜与纽海电子商务（上海）有限公司（1 号店）其他侵权责任纠纷案（上海市浦东新区人民法院 （2016）沪 0115 民初 2998 号民事判决书）

[12] 如杨南光与中国农业银行股份有限公司钦州明珠支行、中国农业银行股份有限公司钦州分行一般人格权纠纷一案（广西壮族自治区钦州市中级人民法院（2015)钦北民初字第 1883 号判决书）

[13] 刘春泉、中国工商银行股份有限公司上海市分行因侵权责任纠纷（上海市第一中级人民法院（2015）沪一中民六(商)终字第 107 号民事判决书）

[14] 李枚加与顺丰速递有限公司侵权责任纠纷案（四川省乐山市市中区人民法院（2015）乐中民初字第 3090 号民事判决书）

[15] 杨劲秋与中国邮政储蓄银行深圳分行隐私权纠纷一案（广东省深圳市福田区人民法院（2015）深福法民一初字第 4278 号民事判决书）

[16] 肖根与中国农业银行股份有限公司安远县支行（以下简称安远支行）名誉权纠纷案件（江西省安远县人民法院（2015）安民

一初字第 177 号民事判决书）

[17] 某几家金融机构违法违规操作造成的同类案件。

[18] http://tech.hexun.com/2018-08-10/193739278.html，最后访问时间：2018 年 8 月 10 日。

[19] http://www.pcwenti.com/bk/12761.html，最后访问时间：2018 年 8 月 10 日。

[20] http://www.heibai.org/post/436.html，最后访问时间：2018 年 8 月 10 日。

作者简介

朱宣烨　合伙人

业务领域：知识产权、争议解决、大数据
电　　话：010-56500912
邮　　箱：xuanye.zhu@meritsandtree.com

王 伟　合伙人

业务领域：私募基金设立、基金投资、并购、跨境投资、境外发债、区块链
电　　话：010—56500983
邮　　箱：wei.wang.@meritsandtree.com

系列三：企业数字化转型过程中的刑事风险之侵犯公民个人信息犯罪

作者：王伟 朱宣烨 高阳 王明志

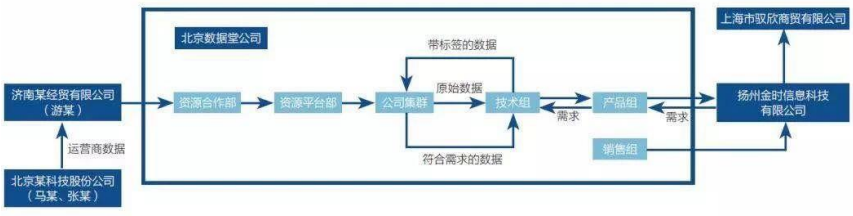
防范刑事风险是企业数据管理合规中的筑底部分的内容，侵犯个人信息犯罪则是企业数据管理过程中可能遇到的一个重要罪名。本文希望通过介绍这一罪名，一方面帮助企业了解如何防止触犯这一罪名，另一方面使企业了解如何预防个人信息遭遇犯罪行为侵害，以及在掌握的个人信息遭遇侵害时可选择的一条救济途径。

一、新三板公司数据堂涉案——侵犯公民个人信息成为企业数据管理的重要风险

企业在收集使用个人信息这一最具价值的数据类型的过程中，极易触发该项罪名，同时也可能遭受这类犯罪行为的侵害。2018 年 7 月，公安部、最高人民检察院督办特大侵犯个人信息专案顺利破获，该案牵涉 11 家公司（其中三家公司涉嫌单位犯罪），57 名犯罪嫌疑人。其中更为抓睛的是，“大数据第一股”的新三板上市公司数据堂也牵涉其中，多名数据堂股东都曾接受过调查，最终包括首席运营官、平台资源部总监等在内的 6 名员工被诉。数据堂公司本身虽然尚未被诉（对数据堂公司本身是否涉嫌单位犯罪仍存争议），但自 2017 年 8 月 14 日起已经停牌，至今仍未复牌，公司的产品营销线和金融征信线已被关停。

该案中，涉案信息的源头为联通一家合作商的两名“内鬼”员工，将涉及全国 15 个省份联通机主的上网数据和偏好，包括手机号、姓名、上网数据、浏览网址等（均为原始未脱敏数据，平均正确率为 99.99%）出售给济南北商经贸有限公司，数据堂人员再从济南北商经贸有限公司购入涉案数据。此后数据堂公司有关人员，将经过清洗和处理的数据卖给扬州金时公司（主要内容为手机号、地区和偏好，如房地产相关等），扬州金时公司再转手将数据卖给上海驭欣公司。具体的个人信息的流经途径见下图。

图 1:“数据堂”案中公民个人信息数据流向图



资料来源：《财经》记者根据采访和司法资料整理　　制图：颜斌

二、侵犯个人信息犯罪的几个要点

据《刑法》第 253 条之一第 1 款，侵犯个人信息犯罪是指违反国家有关规定，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，该罪最高刑罚七年。第 3 款规定，窃取或者以其他方式非法获取公民个人信息的，依照第一款的规定处罚。

关于侵犯个人信息犯罪，我们简单分析如下：

2.1. 公民个人信息范围远远不止身份识别信息

根据《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》（下称“《解释》”）可知，公民个人信息是指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身份或者反映特定自然人活动情况的各种信息，具体而言，姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等都属于个人信息。

此外，根据我们对现有司法判例的研究，我们注意到涉及到的个人信息包括行踪信息、护照信息、驾照信息、车辆信息、手机通讯录、短信、航班信息、住宿信息、通话位置、公司客户信息、出入境信息、支付宝、淘宝账户及密码、游戏账户及密码、购物订单信息、股民信息、劳动合同信息、贷款人信息、婴幼儿个人信息、学生家长姓名电话等等都也都被认定为个人信息。

为方便理解，我们将个人信息范围的要点总结如下：
1 经过匿名化处理，不能关联到具体个人的信息不属于刑法规制的个人信息。
2 公开渠道能够查询到的个人信息，一般不认为是受刑法保护的个人信息。深圳市中级人民法院就认为，企业根据法律法规规定或为经营所需而公开的企业信息，即使包含了个人姓名、联系方式，亦不属于刑法意义上的公民个人信息。
3IP 地址、设备 ID 号和 cookie 信息是否属于个人信息，目前没有案例确定，需根据具体的案件情况判断。

2.2. 单位、个人均可能构成本罪

刑法规定，侵犯公民个人信息罪这个罪名可以构成单位犯罪。认定单位犯罪和个人犯罪的区别在于是否是受单位意思支配，并为单位利益从事犯罪行为。一旦企业被认定构成单位犯罪，绝非仅是罚金损失，而是可能丧失一些领域的投标资质和市场准入的条件，直接影响到业绩指标考核，股价表现。

2.3. 非法获取、非法出售或提供个人信息的行为表现多样，犯罪行为可能发生于个人信息生命全过程。

违反国家规定，通过窃取、购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中获取公民个人信息均可认为是 “非法获取公民个人信息”。

实践中，内部人员窃取、通过业务合作进行交换、通过 qq 群购买、跟踪偷拍、黑客攻击、使用木马病毒获取、通过伪基站非法获取个人信息等都是常见的形式。

非法公开发布公民个人信息也是“提供”的一种表现形式。

实践中，案例主要为利用 qq 群等网络社群进行发布公开。

侵犯公民个人信息的犯罪行为遍布于个人信息流转的各个环节。例如数据堂案件中，电信运营商、电信运维服务企业，到大数据分析、加工企业，再到精准营销公司、数据流通各环节均涉及其中，涵盖数据安全、采购、使用等数据行业领域。

2.4. 只要非法获取或者出售提供的数据达到一定数量就构成犯罪，不以有损害后果为前提，非法获取数据用于合法经营也可构成犯罪。

对于侵犯公民个人信息犯罪的入罪标准——“情节严重”，《解释》根据公民个人信息敏感程度的级别不同分别设置了“五十条以上”、“五百条以上”、“五千条以上”的涉案个人信息数量标准，除此以外，还对违法所得数额、信息用途进行规定。但该罪的构成并不要求造成损害结果，损害结果被规定在“情节特别严重”的情形当中，用以作为加重刑罚的标准。

尤其值得注意的是，非法获取的数据用于合法经营也可构成犯罪。

2.5. 对批量公民个人信息的条数,根据查获的数量直接认定,但是有证据证明信息不真实或者重复的除外。

涉案公民个人信息的数量对于侵犯公民个人信息罪定罪量刑具有重要作用。对批量公民个人信息的条数，根据现有司法解释规定，如果犯罪嫌疑人或者刑事案件被告对根据查获的个人信息数量有异议的，认为信息不真实或者重复的，应当予以证明。

三、合规建议

企业在数字化过程中，既要着重防止踩踏侵犯公民个人信息犯罪的雷区，也应当采取措施防止自身受相关犯罪行为侵害。

3.1. 数据获取环节

企业应当把控数据源头的安全，避免涉嫌“非法获取”公民个人信息。

对于直接向用户进行的收集行为，要根据《网络安全法》等法律法规、参照有关国家标准通过完善的隐私协议获得用户明示的同意，保证数据来源合法；

对于从第三方购买或受让数据的，在接受数据之前，企业应对数据供应商就获得数据而签订的授权书进行审查；企业要重视与数据供应商的协议，要求数据供应商做出如下承诺与保证：（1）供应商保证其采集数据或者获得数据的行为合法；（2）供应商保证已经获得了所有必要的个人授权；或者（3）供应商保证其已经做了数据的脱敏，经处理后无法识别特定个人且不能复原；

对于在公开网络上数据抓取[i]的，注意避免抓取 Robots 协议[ii]明确禁止的内容；

对于通过 API 或 SDK 接入的方式从第三方获取数据的，企业应该严格遵守“用户授权”+“平台授权”+“用户授权”的三重授权原则[iii]。

3.2. 数据提供环节

保证数据权属清晰，核查企业自身是否与相关个人签订授权协议并且检查相关内容；
将所有拟出售的数据进行严格脱敏，即处理之后无法识别特定个人且不能复原；
在与购买者签订协议中要求购买者不能采用任何手段识别特定个人身份；
做好尽职调查，审查购买方对数据的用途；
如有理由确定个体可能暴露身份的时候，应该立即暂时取消或者终止数据流动的发生。

3.3. 人员管理方面

在员工劳动合同中，对数据安全及保密相关的义务和责任进行规定。

对员工处理信息权限分级管理，对录入权限、访问权限及维护权限进行区别，与数据分级相匹配，对数据访问采用身份验证。
对员工进行规范化培训，制定和完善数据处理操作流程。
对员工进行数据安全警示教育，谨防刑事风险发生。
对数据处理工作留痕，对数据处理建立运行日志管理，严格监控操作过程；
对发现的数据安全问题，要及时处理和上报，建立责任追究制度。

3.4. 数据分级管理

数据分级对于数据安全而言不可或缺,我们建议企业均应该建立内部的数据分级机制,严格区分高度敏感信息、敏感信息以及一般的个人信息，分别对各等级信息设置配套的安全措施，并且严格按照数据分级情况进行数据共享或授权使用。明确负责的部门及个人，保障数据安全。

特此申明：以上分析，仅系我们根据现行法律法规、监管政策及相关案例所做的分析和探讨，并不作为我们对相关事项的法律结论意见。

[i]“数据抓取”是指搜索引擎未经数据方授权，通过爬虫（spider）程序进行的，需要自行分析网页上的非结构化数据，并会在数据方的网页服务器的相关日志中体现访问记录的互联网技术行为。

[ii] Robots 协议（也称为爬虫协议、机器人协议等）的全称是“网络爬虫排除标准”（RobotsExclusion Protocol），网站通过 Robots 协议告诉搜索引擎哪些页面可以抓取，哪些页面不能抓取。

[iii] 新浪微博诉脉脉案确立的在 OpenAPI 开发合作模式中，第三方通过 OpenAPI 获取用户信息时应坚持原则。

作者简介

王 伟　　合伙人

业务领域：私募基金设立、基金投资、并购、跨境投资、境外发债、区块链
电　　话：010-56500983
邮　　箱：wei.wang@meritsandtree.com

朱宣烨　　合伙人

业务领域：争议解决、大数据
电　　话：010-56500912
邮　　箱：xuanye.zhu@meritsandtree.com

系列四：企业数字化过程中的刑事风险之非法获取计算机信息系统数据罪

作者：朱宣烨 王伟

不久前，警方破获了一起史上最大的数据窃取案，在本案中 30 亿用户数据被窃。新三板公司北京瑞智华胜科技股份有限公司（以下简称“瑞智华胜”）通过与覆盖十余省市的运营商签订营销广告系统服务合同，在提供软件服务的过程中违反国家规定，利用获得的运营商服务器的远程登录权限将自主编写的恶意程序放在运营商内部的服务器上，从中清洗、采集出用户 cookie、访问记录等关键数据，再通过恶意程序将所有数据导出并存放在瑞智华胜境内外的多个服务器上。这导致了百度、腾讯、阿里、今日头条等国内核心互联网公司的用户数据被获取。目前瑞智华胜被停牌，公司监事黄某、梁某、员工王某、石某已于 8 月 9 日被批捕，原法定代表人、董事周某取保候审。本案值得关注的一点是，虽然瑞智华胜窃取的数据涉及大量的个人信息，但是该案件是以非法获取计算机信息系统数据罪侦查立案。

一、关于非法获取计算机信息系统数据罪的几个特点

根据刑法第 285 条的规定，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域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，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。对于这一罪名适用的理解，应当关注以下几个特点：

1.1 个人、单位皆可构成本罪

随着数据日益成为公司发展的重要资源，甚至关系商业模式的创新，越来越多的单位成为了获取数据甚至非法获取计算机数据的重要主体。非法获取计算机信息系统数据罪的犯罪主体经历了从自然人到自然人和单位均可构成犯罪的发展过程。刑法规定，非法获取计算机信息系统数据罪这个罪名可以由单位构成。也即如果在公司意思支配下，并为公司利益非法获取计算机信息系统数据的，不仅直接负责的主管人员和直接责任人员会被追究刑事责任，公司本身也会被追究刑事责任以及民事责任，这将直接影响公司的融资和生产经营。

例如，上海某网络科技有限公司等非法获取计算机信息系统数据一案中，上海某网络科技有限公司系有限责任公司，经营计算机网络科技领域内的技术开发、技术服务、电子商务、电子产品等业务。张某某系该网络科技有限公司法定代表人兼 CEO，负责公司整体运行；被告人宋某担任联席 CEO，系产品负责人；被告人侯某某担任公司 CTO，系技术负责人；被告人郭某系该网络科技有限公司职员。张某某、宋某、侯某某经共谋，于 2016 年至 2017 年间采用技术手段抓取被害单位北京某网络技术有限公司服务器中存储的视频数据，并由侯某某指使被告人郭某破解北京某网络技术有限公司的防抓取措施，使用“tt_spider”文件实施视频数据抓取行为，造成被害单位损失技术服务费人民币 2 万元。

1.2 什么样的数据受到非法获取计算机信息系统数据罪的保护

计算机信息系统数据是指在计算机信息系统中存储、处理、传输的数据。但并不是所有计算机信息系统的数据都能成为本罪的保护对象。

1.2.1 实践中计算机信息系统数据的类型多样。例如：商业秘密、游戏账号及密码、企业客户信息、游戏源代码、WiFi 热点及对应密码、个人资格信息等都属于计算机信息系统数据。

1.2.2 独立于计算机信息系统外的其他载体，如 U 盘、移动硬盘中所存储的数据并不是本罪的保护对象。当然，如果 U 盘、移动硬盘连接在电脑上，自然属于计算机系统的一部分。

1.2.3 已经公开的数据且数据所有人或控制人没有不允许获取的数据不是本罪的保护对象。最常见的情况是，使用正常的爬虫技术获取数据并不涉及刑事犯罪。

1.2.4 承载了犯罪内容的计算机数据不会成为刑法的保护对象。

1.3 常见的涉及这个罪名的行为有哪些

根据刑法的规定，在司法实践中，下列获取数据的行为可能构成本罪：

（1）利用网络爬虫软件获取数据。并不是所有的爬虫技术都构成违法，还需要看两个内容，第一，爬取的数据性质。例如，涉及个人信息的，没有合法依据不得爬取的；第二，爬取行为是否为数据权利方所禁止。例如在数据权利方已经采取反爬虫措施的情况下，通过模拟数据权利方客户的请求的方式来获取数据的，则属非法。此外，需要指出的是，在采用大量爬虫高频次访问要获取数据的服务器但是导致服务器瘫痪的情形下，也可能构成破坏计算机信息系统罪，加之破坏计算机信息系统罪犯罪构成更加明晰且刑法更重，所以这种情况下，多

依据破坏计算机信息系统罪追究刑事责任。

（2）通过利用企业员工的账号、密码、Token（令牌）或者工号权限，获取计算机信息系统中储存的电子数据。

（3）植入钓鱼链接及利用钓鱼网站获取数据。

（4）未经允许安装域名解析软件（用于显示计算机地址，例如“花生壳”）、多用户系统软件（远程控制计算机）、键盘记录软件（用于盗取账号和密码，例如“灰鸽子”）并利用其获取数据。

（5）通过其他各种木马程序非法获取数据。

（6）行为人获取计算机信息系统数据时，如果对系统内的数据进行了增加、删除、修改等操作，干扰了信息系统的正常运行，行为人通常会被依据破坏计算机信息系统罪追究刑事责任。

1.4 “情节严重”怎么理解?

根据《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第一条的规定，（第一款）下列情形应该认定为“情节严重”： （一）获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；（二）获取第（一）项以外的身份认证信息五百组以上的；（三）非法控制计算机信息系统二十台以上的；（四）违法所得五千元以上或者造成经济损失一万元以上的；（五）其他情节严重的情形。（第二款） 实施前款规定行为，具有下列情形之一的，应当认定为刑法第二百八十五条第二款规定的“情节特别严重”：（一）数量或者数额达到前款第（一）项至第（四）项规定标准五倍以上的（二）其他情节特别严重的情形。（第三款）明知是他人非法控制的计算机信息系统，而对该计算机信息系统的控制权加以利用的，依照前两款的规定定罪处罚。

司法实践中认定“情节严重”、“情节特别严重”的案例有很多。例如，唐某等利用钓鱼网站盗取他人 QQ 号码非法获取计算机信息系统数据案【(2012)通刑初字第 0425 号】，在本案当中，被告人周某某以每 3000 个邮箱 100 元的价格获利 5995 元，被认定为“情节严重”。郭某、刘某非法获取计算机信息系统数据案【案号为(2016)沪 0105 刑初 1027 号】，在本案当中，被告人被认定非法获取被害人公司的热点密码数据达到 241 万余组，被认定为“情节特别严重”。

1.5 本罪与侵犯公民个人信息罪的区别和联系

伴随着我国互联网的高速发展，越来越多的个人信息以数据的形式存储在计算机系统当中。所以非法获取计算机系统数据罪和侵犯公民个人信息罪存在着千丝万缕的联系。

对比事项	侵犯公民个人信息罪	非法获取计算机信息系统数据罪
定义	违反国家规定，向他人出售、提供或者非法获取公民个人信息，情节严重的行为。	使用不法侵入的手段，获取计算机信息系统的数据，情节严重的行为。
对象	本罪对象是“公民个人信息”，《严惩侵害公民信息通知》（2013）指出，“公民个人信息包括公民的姓名、年龄、有效证件号码、婚姻状况、工作单位、学历、履历、家庭住址、电话号码等能够识别公民个人身份或者涉及公民个人隐私的信息、数据资料。”只要与公民个人相关，公民不想公开，而且与公共利益无关的信息，都可以纳入“公民个人信息”的范围，例如个人日常行踪等活动记录。	计算机信息系统中存储、处理或者传输的数据。
行为	违反国家有关规定，向他人出售、提供“公民个人信息”或者非法获取公民个人信息。“国家有关规定”，指有关公民个人信息管理、保护的国家规定，如商业银行法、居民身份证法、护照法、消费者权益保护法、旅游法、社会保险法、统计法等法律中关于保护公民个人信息的规定。违规出售、提供的公民个人信息的来源在所不问。“非法获取”指窃取或者其他方法未经公民或法律授权获取公民个人信息。	非法侵入且非法获取他人计算机信息系统中的数据；“侵入”的实质含义是指：行为人在没有得到许可时，违背计算机信息系统控制人或者权利人的意愿，进入其无权进入的计算机信息系统中。可分为两类：一是非法用户（无权访问特定信息系统的用户）侵入信息系统，如冒充合法用户、破解密码、盗取密码等；二是合法用户（有权访问特定信息系统的用户）的越权访问，如未经批准、授权或者未办理相关手续而擅自访问该信息系统或者调取系统内部数据资源。
罪量	情节严重。根据《严惩侵害公民个人信息通知》（2013），侵害公民个人信息有下列情形的应当追究刑事责任：1.被他人用以实施犯罪，造成受害人人身伤害或者死亡 2.造成重大经济损失、恶劣社会影响的；3.被侵害公民个人信息数量较大的；4.违法所得数额较大的；5.造成其他严重后果的。 有关指导案例裁判要旨指出：	“情节严重”根据《办理计算机刑案解释》（2001）第一条第一款，非法获取计算机信息系统数据或者非法控计算机信息系统，具有下列情形之一的，应认定为“情节严重”：1.获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；2.获取第（一）项以外的身份认证信息五百组以上的；3.非法控制

	判断非法获取公民个人信息的行为是否达到“情节严重”，可以从一下四个方面综合考量：1.用途上，非法获取的信息是否被用于犯罪活动；2.结果上，该信息是否严重影响被害人的生活，或者给被害人带来较大的经济损失；3.行为方式上，采取的手段、方法是否恶劣，是否适用违禁工具等；4.信息数量、获利数额、行为持续时间上，非法获取公民个人信息的数量、次数较多，行为人获利数额较大，以及非法获取行为持续时间较长的，一般都可以认定为“情节严重”。综合以上因素考虑，对于没有使用违禁的密拍设备、窃听窃照器材，跟踪时间较短，没有非法获利的普通跟踪行为，一般不宜作为犯罪处理。	计算机信息系统二十台以上的；4.违法所得五千元以上或者造成经济损失一万元以上的；5.其他情节严重的情形。这里的“其他严重情形”至少包括获取信息的数量、次数、手段、潜在的危险性等，应从实质上判断其行为的法益侵害性和有责性否到达需要刑罚处罚的程度。
量刑	将在履行职责或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，从重处罚。要依法加大对财产刑的适用力度，剥夺犯罪分子非法获利和再次犯罪的资本。	【加重犯】“情节特别严重”，根据《办理计算机刑案解释》（2011）第 1 条第 2 款，指犯罪数额达到“情节严重”标准 5 倍以上或者其他情节特别严重的情形。

二、关于数据相关业务合规的建议

数据是企业重要的竞争力，对于需要数据的公司而言，应当取之有道，否则会遭遇刑事处罚的风险；对于掌握数据的公司，应当采取措施保护自身数据安全和竞争力。

2.1 对于获取计算机数据的企业

2.1.1 获取数据之前应当明确行为的风险等级，具体考虑的因素有：

（1）进入的计算机系统的性质。虽然非法获取计算机系统数据罪针对的是国家安全、国防安全及尖端科技领域的计算机系统以外的计算机系统中的数据，但是举轻以明重，事实上，上述系统数据更是碰不得。只要侵入上述系统即构成犯罪，而不是像非法获取计算机信息系统数据罪那样，“情节严重”的才构成犯罪。

（2）获取数据的性质。虽然数据的性质对于本案的犯罪事实的认定没有影响，但是同样的数据获取行为，不同的数据性质可能有不同的结果。比如，一般的爬虫技术不认为非法获取数据，即便是对于某些设定了一定反爬虫技术的网站，是否构成犯罪也存有争议，但是如果爬取的是个人信息，那很可能构成非法获取公民个人信息罪。

（3）就具体行为而言，直接的爬取风险小于模拟请求绕过密钥，模拟请求绕过密钥风险相对小于采取木马、钓鱼网站。

2.1.2 在进行数据合作、数据交流和提供外包服务的过程中，获取数据的范围超过权利方的授权范围，或者超过权限获取数据。

2.1.3 做好管理人员和员工的风险教育工作。通过入职培训、风险提示等方式，防止公司有关人员从事非法获取计算机数据的行为，确保公司已经尽到必要的管理责任，且明确进行非法行为不是公司意思，减少企业的运行风险。

2.2 对于掌握计算机数据的公司

2.2.1 根据自身业务特点加大对数据异常情况的关注。例如，请求中的 IP 地址出现异常等。设置必要的反爬措施，并对数据的权属进行声明。

2.2.2 如需数据共享和数据合作，除了应当形成有效的协议，写明获取数据的单位和进入其系统的权限，还应当采取技术措施，实现有限、分级开放，尽量避免出现实际开放的权限远大于合同中约定的权限的情况，减少由于双方的主观判断失误而引发的分歧。

2.2.3 加强员工及其账号、权限的管理。明确其在单位中的工作内容、职务权限等。同时，通过工作责任书、岗位职责、劳动合同、保密协议、与授权有关的通知、公告、管理制度等方式进行确认。此外，还要向员工强调账户保密、禁止外泄的重要性。

三、结语

在计算机犯罪日益多发的今天，无论是对掌握数据的企业还是获取数据的企业而言，明确法律禁止的边界都是极为重要的，这既有利于防患于未然，又有利于及时化解企业危机，只有在法律的框架下行事，企业才能行稳致远！

特此申明：以上分析，仅系我们根据现行法律法规、监管政策及相关案例所做的分析和探讨，并不作为我们对相关事项的法律结论意见。

[1] 上海某网络科技有限公司等非法获取计算机信息系统数据案，（2017)京0108刑初2384号。

[2] 白某某等非法获取计算机信息系统数据案，（2017）粤0113刑初字2047号。

[3] 谢某某等非法获取计算机信息系统数据、提供侵入、非法控制计算机信息系统程序、工具案，(2017)苏04刑终160号。

[4] 卫某等非法获取计算机信息系统数据案，(2017)京0108刑初392号。

[5] 邵某等非法获取计算机信息系统数据案，(2016)粤03刑终1168号。

[6] 黄某等非法获取计算机信息系统数据案，(2014)浦刑初字第4938号。

[7] 王某非法获取计算机信息系统数据案，(2014)浙杭刑终字第97号。

[8] 卫某、龚某、薛某非法获取计算机信息系统数据案，（2013）武侯刑初字第691号。

[9] 海珠法院公布网络犯罪六大典型案例之五：林某春等非法获取计算机信息系统数据案——盗取微信公众号推送微商产品和广告非法牟利，广东高院发布2017年度涉互联网十大案例之五：肖某非法获取计算机信息系统数据案——以黑客手段窃取苹果手机ID密码如何定性。

[10] 罗甲、罗乙、柯某分非法获取计算机信息系统数据案。

[11] 董某、李某某非法获取计算机信息系统数据案，杨锋非法获取计算机信息系统数据、盗窃案。

作者简介

朱宣烨　合伙人

业务领域：争议解决 知识产权
电　　话：010-56500912
邮　　箱：xuanye.zhu@meritsandtree.com

王　伟　合伙人

业务领域：私募基金设立、基金投资、并购、跨境投资、境外发债、区块链
电　　话：010-56500983
邮　　箱：wei.wang@meritsandtree.com

系列五：数据领域投资人也会有刑事风险？

作者：朱宣烨 王伟 高阳 孙鑫婧

数字经济时代，数字化或者数字化转型已经成为越来越多企业的选择。数据产业或者附带有数据概念的企业也成为了投资人关注的一个重要领域，投资人也成为数据产业发展重要的推动力量。

随着数据安全日益受到重视，网络安全的监管制度日益完善，各个企业对数据的保护意识日益增强，政府针数据相关的违法犯罪行为的打击力度也逐步加大。投资人在推动数据产业发展，推动企业数字化进程的同时，如果处理不当也会面临着不容忽视的刑事法律风险。本文针对实践中一些典型的不正确的看法，结合案例作出提示。

一、与数据相关的刑法罪名并不少

相较于非法吸收公众存款、虚开增值税专用发票、合同诈骗等企业经营中经常遇到的罪名，涉及数据的罪名并没有经常地出现在大家的视野中。但是，实际上与数据相关的刑法罪名并不少，而且随着数据的价值日益得到重视，这类案件也日益增加。具体而言，企业可能涉及的与数据相关的刑法罪名主要有以下两大类：

1.1 计算机系统安全类罪名

具体包括非法侵入计算机信息系统罪，破坏计算机信息系统罪，非法获取计算机信息系统数据罪，非法控制计算机信息系统罪和提供侵入、非法控制计算机信息系统程序、工具罪。这类罪名较为常见，主要是数字化发展的结果，尤其是大数据时代，数据的存储、处理、应用离不开计算机系统构成的网络环境，要从事与数据相关的刑事犯罪行为，首先就是要破坏或侵入数据所在的计算机系统，对该计算机系统的安全造成损害。例如，盗窃代币（token），盗窃游戏币等行为，其表现为采用技术手段，获取计算机系统中存储的数据，所以即使这一行为不能构成盗窃罪，也有可能涉嫌构成非法获取计算机信息系统数据罪。

1.2 其他犯罪

根据被侵害的数据的具体属性，可能构成其他犯罪。

1.2.1 侵犯公民个人信息犯罪

个人信息也是大数据时代企业的重要资源，但是由于个人信息的特殊性，我国刑法对于侵犯公民个人信息的行为进行了专门规定，该罪名并不必然要求行为人的行为对计算机系统安全构成破坏。例如，非法获取打印在纸上的或者存储在接入计算机系统的 u 盘里的个人信息的行为都可能触犯这一罪名。

1.2.2 盗窃罪

如果侵害的是有财产价值的数据，或者通过数据的修改增加了自身的财产，则可能构成盗窃罪。如直接修改的是银行存款信息，使自己财富增加的，则可能构成盗窃罪。

1.2.3 侵犯著作权罪

如果侵犯的他人服务器中的数据表达为作品的，则可能构成侵犯著作权罪。

需要注意的是，所涉及的罪名之间也可能存在吸收或竞合的关系，本文不再展开。

二、投资人不会必然排除涉刑风险

无论是根据对被投资企业的业务参与度不同，分为的战略投资人、财务投资人以及实业投资人；还是根据投资时企业的发展阶段不同，划分的天使投资人、VC 或是 PE，在被投企业涉及到数据刑事犯罪时，各类投资人虽然没有直接实施犯罪的行为，但是当被投企业涉嫌刑事犯罪时，并没有哪类投资人能必然排除在刑事风险之外。投资人是否涉刑关键在于看其是否有符合刑法规定的罪名的构成要件。根据既往的案例，在被投企业涉刑时，既有投资人作为主要直接主管人员因公司单位犯罪而被处以刑罚，也有投资人与公司其他人员直接构成共犯而被处以刑罚。

以财务投资人为例，财务投资人是参与公司直接经营程度比较低的投资人类型，其更看重短期回报，关心盈利状况以及盈利能力。虽然在很多情况下，财务投资人不直接参与公司的经营管理，因公司的违法犯罪行为受到牵连的情况相对小。但是“财务投资”如果处理不当，仍有受到刑事处罚的风险。

例如，在李某等 18 人合同诈骗罪一案中，李某等人成立某信息公司，并利用该信息公司从事售卖网络域名的合同诈骗活动。被告人张某，在该信息公司成立之后，通过受让股权的方式入股该公司，同时兼任该公司的财务总监。张某抗辩称，其仅为财务投资，并不参与公司管理，仅为该公司财务工作提供策划和咨询，不了解公

司的实际业务模式。但是法院最终认为，张某在入股某公司后，得知该公司从事合同诈骗行为，仍然从事上述相关工作。据此认为，张某构成合同诈骗罪。

三、后期投资也能构成犯罪

很多投资人在公司成立之后，通过增资或者股权转让的方式成为股东。但是即便如此，投资人并不能以在投资前不知道被投公司存在犯罪行为为由，主张对投资后公司的涉刑行为完全免责。认定犯罪嫌疑人是否存在犯罪故意与其介入犯罪过程的时间早晚并没有必然联系。

例如，在上述李某等 18 人合同诈骗罪一案中，被告人张某辩解称，其在入股前对公司销售人员的诈骗行为并不知情，在其得知公司存在的一些违规营销行为后，曾经表示反对并要求退股。据此，其认为自己不具有合同诈骗罪的故意。但是法院判决认为，根据证人证言，被告人张某在得知公司存在合同诈骗的行为之后，仍然帮助公司从事财务管理的相关工作，所以其存在犯罪故意，构成合同诈骗罪。

四、授意和帮助亦有可能构成犯罪

直接实行犯罪行为构成犯罪并无争议，但教唆或帮助他人从事犯罪行为也能构成犯罪的相关法律规定较易被忽视。在涉及数据犯罪的司法实践中，就有股东因为向公司员工提出技术要求，并放纵公司员工使用违法方式实现而被追究刑事责任的情形。

在某技术有限公司于某犯侵犯著作权一案中，某技术有限公司经营的网站设有小说、新闻、美图等多个频道，通过在网页植入广告收取广告收益分成。被告人于某系该公司股东，负责技术工作，并担任法定代表人。2012 年，为提高该网站的用户数量，于某提出开发触屏版小说产品，将 HTML 格式的小说网页转码成 WAP 格式的网页供移动用户阅读。在未获受害公司许可的情况下，擅自使用软件，复制、下载受害公司发行于其网站上的文字作品，存储在某技术公司的服务器内，供移动电话用户在小说频道内免费阅读，再通过在“易查网”内植入广告，使用易查公司的银行账户收取广告收益分成。在本案中，被告人于某抗辩，其仅提出了技术要求，对具体落实情况并不知情，但是法院认为，被告于某既然直接提出该产品的技术需求，则在具体开发中，尤其是产品上线前，其应跟踪了解该产品的技术实现方式，以确保不侵犯他人合法权益。于某自认其并未完全了解该技术的具体实现方式，也未就开发中的具体技术问题进行后续跟踪，其主观上至少存在放任的间接故意。因此，于某作为易查公司的直接负责和主管人员也应该对侵犯著作权罪承担刑事责任。

五、建议

虽然判断是否存在与数据相关的刑事风险比较复杂和专业，不似非法吸收公共存款、合同诈骗等常规的刑事案件那样为普通大众所熟知，但是投资人仍可以从以下几个方面加以把握，提高警惕，降低刑事风险。

5.1 树立数据有价、尊重隐私的观念

虽然与数据相关的刑事犯罪罪名多样，加之很多行为的罪与非罪的边界处于正在逐渐明晰的过程中，作为投资人可能不能详尽准确地了解所有的刑法罪名以及对应的犯罪行为方式。但是刑法中设立的罪名是基于基本的价值判断，所以投资人树立基本的价值判断理念，就足以在对具体被投企业做出具体行为时保有足够的警惕意识。数据尤其是存在于计算机系统中的数据受到法律的特别保护，在获取或对其进行处理时应当考虑方式是否合法；个人信息无论其是否存在于计算机系统中，都受到法律的特别保护，如果获取或处理的数据涉及个人信息，亦需要引起特别的注意。

5.2 不能以经验判断代替法律判断

在互联网和数据行业的发展初期，由于立法的滞后性和执法人员需要有了解、学习的过程，且数据的经济价值并未那么凸显，此类案件并不多见，所以容易造成某些已经触犯刑法的行为并不构成犯罪的“实践经验”。所以不能用经验判断代替法律判断，否则会像下面的案例一样即使是行业老将也难免折戟。在上海某公司及其大股东（兼法定代表人）、CEO、CTO 以及某员工等非法获取计算机信息系统数据罪一案中，公司的大股东（兼法定代表人，以下简称该股东）在行业内“摸爬滚打”十余年，行业经验丰富。为了获取被害公司的数据，上海某公司采用技术手段破解受害公司的防抓取措施，使用“tt_spider”文件抓取被害公司服务器中存储的视频数据。最终，上海某公司的行为被认为构成非法获取计算机信息系统数据罪，大股东（兼法定代表人）、CEO、CTO 作为直接负责的主管人员，某员工作为其他直接责任人员，均被判处刑罚，尤以大股东的刑期最长。

5.3 不要把行业习惯当作免责理由

身为投资人不能持有行业惯例不属违法行为或者即使违法也因为“法不责众”而不会被追责的侥幸心理。行业习惯向来就不是法定免责理由，法律不会因为涉案行为是行业惯常的行为就免除处罚。在某信息公司及李某波等侵犯著作权一案中，被告人李某波系某信息公司的大股东，自 2014 年起，被告人李某波为提高该软件的知名度和点击下载量，在未获被害公司等许可的情况下，擅自通过“快读免费小说”软件复制、转载被害公司等发行于其网站上的多部文字作品，存储在服务器内，供 Android 移动电话用户下载该软件后免费阅读上述文字作品。法院经审理认为，该信息公司行为已构成侵犯著作权罪，依法应当判处罚金。李某波是直接主管人员，和其他主管人员及直接责任人员同样被以侵犯著作权罪追究刑事责任。本案中，被告人李某波辩解称，类似网

站的创业初期均无法承担巨额的版权购买费，均是逐步有序走向正版化，但正版化需要过程及财力支撑。该种辩解理由显然是模糊了行业习惯和法律的界限，被告人想把行业习惯作为自己不构成刑事犯罪的辩解理由，是不能够成立的。

5.4 加强对拟投及被投企业数据合规方面的调查和辅导

近年来，国家在网络安全、数据保护方面颁布了一系列法律制度规范和国家标准，投资人在投资尽职调查过程中和在投资后的管理过程中，应当依照相应的规定、参考推荐性的国家标准，加强对拟投资企业及被投企业在数据合规方面的调查和辅导，降低涉及数据的刑事风险。如果发现拟投资企业或者被投企业存在违法行为，应当及时停止对其投资以及提供其他方面的业务支持。另外，投资人拟对被投企业与数据相关的具体业务提出需求时，亦应谨慎考察该具体业务的需求本身是否能够通过合法且现实的手段实现；如果投资人所提要求难以通过合法且现实的方式实现，则不应要求被投企业实施。

特此申明：以上分析，仅系我们根据现行法律法规、监管政策及相关案例所做的分析和探讨，并不作为我们对相关事项的法律结论意见。

[1]可能由于代币、游戏币是否能够确定经济价值尚存不同看法，上述窃取行为是否可以认定构成盗窃犯罪司法实践也不相同。

作者简介

朱宣烨　合伙人

业务领域：争议解决 知识产权
电　　话：010-56500912
邮　　箱：xuanye.zhu@meritsandtree.com

王　伟　合伙人

业务领域：私募基金设立、基金投资、并购、跨境投资、境外发债、区块链
电　　话：010-56500983
邮　　箱：wei.wang@meritsandtree.com