论大数据时代企业数据权益的法律保护

◆闫　东

（沈阳城市学院，辽宁 沈阳 110112）

【摘要】数据是最重要的资源，企业是数字经济中最为活跃的主体，在数据利用过程中发挥着重大的作用，数据资源正成为不同企业之间竞争的核心要素，因此，企业数据保护是当下亟待解决的问题。本文分析了企业数据的属性，阐述了企业数据的商业秘密保护法制现状，梳理了企业数据商业秘密保护中存在企业商业秘密泄露防范措施不足、商业秘密认定困难、商业秘密侵权举证难的问题，提出了加强企业商业秘密防范措施、明确企业数据构成商业秘密的标准、完善商业秘密侵权举证责任的完善措施。

【关键词】企业数据；商业秘密；不正当竞争；一般性条款

人工智能、区块链、5G、量子计算、大数据等新一代信息技术的快速发展，已将使得数字经济成为推动经济社会变革、促进经济高质量发展的重要动能。 数字经济条件下，数据日益成为重要的市场要素，并成为企业重要的商业资源和竞争优势。 当数据价值释放愈发依赖于个人信息的“喂养”，个人信息安全也成为阻碍数据价值开发的“羁绊”。数据流通利用与个人信息保护之间存在着天然的矛盾。 当前，《中华人民共和国民法典》《网络安全法》《数据安全法》以及《个人信息保护法》等一系列法律法规，都对现实中的个人信息保护问题予以了回应。 与之相对应的是，企业数据保护还缺乏相应法律规范。 当数字经济已经成为经济发展的常态，数据保护理应顺应数字经济发展的规律，应在个人信息安全与企业数据保护之间寻求平衡，在加强个人信息保护的同时，也要重视对企业数据权益的保护。 我国目前还没有直接针对企业数据保护的法律规定，因此，仍需从既有法律体系中寻求制度供给空间。

一、企业数据属性的法律界定

企业数据，指由企业通过大量人力、物力和财力的投入，通过收集、存取、基础架构、分析处理等数据技术，对原始数据进行开发整合所得到营销策略、用户名单、产品开发等具有经济价值的数据。 企业数据的财产性贯穿于其获取、形成、控制、支配和转移的全过程，企业获取并整合这些数据的过程中会产生成本，最终通过其技术手段形成的大数据产品又会服务于企业的运营，为其创造价值。 根据企业数据是否公开，实践中通常会将企业数据分类为“公开数据”与“非公开数据”，或者“原始数据”与“衍生数据”。企业数据法律本质的认定在学术界存在不同观点。 有的从物权体系出发，认为企业数据是一种新型财产，建议以数据财产权保护；有的从知识产权的角度出发，将企业数据视为企业的作品或数据库，甚至是新形态的知识产权客体，但司法实践中法院已经开拓性地将企业数据定性为《反不正当竞争法》中的竞争性利益来保护。 企业将其合法获取的数据汇总后进行脱敏处理，已不再具有个体识别性，不违反《网络安全法》及《个人信息保护法》的规定，在此基础上，企业数据存在企业的创作和劳动，并服务于企业的经营，属于企业的合法利益。 企业数据的利益应归属于生产数据产品的企业，而非原始数据的个人数据主体，虽然个人数据在数据产品中存在经济价值，但这部分价值应当在企业获取数据时支付，个人主体不再对数据产品重复享受利益。

二、企业数据的商业秘密保护法制现状

当下，企业数据保护有民法保护、刑法保护、竞争法保护等。 民法中，《民法典》第 127 条明确了数据、虚拟财产属于受法律保护的财产权客体，在没有规定具体的保护模式，因此，企业数据在私法上的保护措施仍存在一定困境。刑法中，《刑法》第 285 条第 2 款规定了非法获取计算机信息系统数据罪，该罪名自成立以来已经被实践所采纳，司法案例中已经开始以此罪名定罪，一些案例都涉及对个人信息的滥用，比如，盗用他人的身份信息、账号密码等，也包括滥用知识产权等，都涉及企业数据的保护。 竞争法保护即《反不正当竞争法》一般条款的保护，这是数据权益最重要的保护路径，也是比较常见的保护方式。 实际上，商业秘密保护是企业数据最常见的做法。 在司法实践中，法院往往会将企业数据分类为“公开数据”与“非公开数据”，或者“原始数据”与“衍生数据”。 对于企业拥有的一些公开数据，可以适用《反不正当竞争法》的一般条款进行保护，我国尚未就商业秘密保护进行专门立法，商业秘密保护制度作为《反不正当竞争法》的一部分，其解释规则应当符合《反不正当竞争法》的立法意旨，如果一味地为了保护数据持有企业所拥有的公开数据，而将商业秘密的范围扩大，会使商业秘密的秘密性要件在此类案件中被架空，从而导致商

业秘密认定标准门槛较低，这种局面可能不利于司法的一致性，也有可能限制市场的自由竞争并且阻碍数据相关技术的发展。因此，商业秘密制度更适合用于保护企业的非公开数据。非公开企业数据更符合商业秘密保护所要求的秘密性、价值性、保密性。2019年修订的《反不正当竞争法》在一定程度上体现了对商业秘密保护的政策性倾向，通过适用商业秘密条款来保护企业数据愈发具备可行性。

三、企业数据的商业秘密保护现实困境

（一）企业商业秘密泄露防范措施不完善

企业经营中不可避免地存在制度不完善的问题，企业对数据保护没有给予重视，保护力度小，保护水平低。即使有的企业重视商业秘密，也只是停留在某些技术信息、经营信息上。部分企业高级管理人员法律意识不高，对企业的制定措施不具体，因而无法落到实处。另外，在企业发展中，在职员工对于企业数据可能签署过保密协议，但仍不能避免商业秘密泄露的风险，尤其是技术型企业，在技术背后蕴含的是经济利益，因员工离职而产生的侵权纠纷较常见。

（二）商业秘密认定难

从商业秘密司法实践来看，原告起诉被告商业秘密侵权胜诉的案件较少，这是因为案件标的没能被认定为商业秘密。商业秘密认定一直都并非易事，传统商业秘密认定较难，企业数据商业秘密认定则更难。一方面，企业数据的秘密性认定存在不确定性。在商业秘密构成要件中，秘密性要件处于重要地位，而司法解释仅从反面规定了不构成不为公众所知悉的六种情形，秘密性的具体内涵和判断标准却难以获知。企业拥有多种多样的数据，其中，对于研究数据、技术信息等非公开的企业数据，不难认定其秘密性，但更多的数据是源自于企业对用户的个人信息、行为偏好等数据的收集、处理和分析，这些企业从公有领域获取的数据是否构成商业秘密尚有争议，无论是理论界抑或是司法实践中，对于这类数据是否符合秘密性要件还存在着疑虑。另一方面，保密性的认定也并非全无疑惑，对企业数据采取何种保护措施才能达到法律规定的合理程度，法律也没有予以明确，商业秘密认定困难导致企业数据发生侵权行为时维权困难。

（三）商业秘密侵权举证难

和其他不正当竞争行为相比，商业秘密侵害行为本就具有隐蔽性特点，商业秘密权利人往往难以证明侵权人所实施的不正当竞争行为。而数据与商业秘密的结合使得商业秘密侵害行为更具隐蔽性，企业数据的商业秘密保护面临着挑战与阻碍。2019年修正的《反不正当竞争法》第32条减轻了商业秘密权利人在民事诉讼中的举证责任，商业秘密权利人仅需提供初步证据，合理表明其商业秘密被侵害，但不可否认的是，技术的更新迭代无疑会加剧商业秘密侵害行为的隐蔽性，从而增加权利人的维权难度。在大数据时代，侵权行为人运用计算机技术，使得权利人无法识别到权利被侵犯，被侵害者甚至无法察觉自己的数据已经被窃取。商业秘密侵害行为的隐蔽性和侵害结果的隐蔽性，无疑会加重企业的举证责任。

四、企业数据的商业秘密保护实施路径

（一）制定企业商业秘密防范措施

第一，企业在经营中对不同的商业信息进行不同等级的划分，在员工入职时就对员工进行商业秘密专门培训，使员工明确哪些数据属于商业秘密，哪些数据受到法律保护，避免将商业秘密当作普通信息对待。员工需要对企业数据提高警惕，才能防范数据被泄露。第二，由于企业中信息会逐级传递、储存，对于企业数据可以根据员工的身份进行限制，例如，限制不同职位员工的访问权限，设定相关的内部制度，规范不同级别员工所能接触到的不同级别数据。企业高级管理人员接触的商业秘密必然高于普通员工，所以对企业高级管理人员必须做出更高的限制，例如，签署竞业限制协议等。对不同员工进行秘密等级防范，也能有效避免商业秘密二次泄露。目前，传统的商业秘密防范手段已经不能防范高科技侵权行为，因此，应全面升级企业数据保护措施，设置多重生物识别程序，实时监控员工是否有侵权行为，及时阻断侵权行为的发生。

（二）明确企业数据构成商业秘密的标准

实践中，企业援引商业秘密制度保护企业数据较为常见。然而，商业秘密认定难是商业秘密权利人维权的最大阻碍，尤其是秘密性要件的认定。企业数据要想通过商业秘密途径获得有力保护，就要明确商业秘密构成要件的认定标准。鉴于实践中企业希望通过商业秘密保护企业数据的现实需要，有必要在立法层面对数据的商业秘密认定问题作出回应。在商业秘密构成要件标准仍然较模糊的情形下，可以通过司法解释对秘密性和保密性的内涵作出进一步解释。同时，对秘密性和保密性的认定标准也不宜过于严格。尽管目前还存在着争议，但针对企业从公有领域获取、汇聚的数据，只要相关信息的收集、加工、筛选和组合的结构本身是无法获得的，即可以认为具有未公开性，而不论数据的来源是否发端于公开信息。同时，《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》第4条第2款也印证了这一点。而在保密性的认定上，只要企业通过采取合理的保密措施，使得商业秘密置于其控制下，即可认定为符合商业秘密构成要件的保密性要求。这也与《反不正当竞争法》修订稿将原法条中的“采取保密措施”修改为“采取相应保密措施”的立法意图相契合。

（三）完善商业秘密侵权举证责任

当下企业商业秘密侵权的举证责任尚未明确，举证标准

也需要进一步地细化和调整。根据我国《民事诉讼法》及相关司法解释的规定，一般侵权行为的举证责任的方式是“谁主张、谁举证”。但是由于一些案件自身具有的特殊性质，所以为了司法公正的需要，可以将一部分举证责任分配给被告一方。对于商业秘密侵权案件而言，借助企业数据本身具有的复杂性和隐蔽性，原告是很难明确知晓侵权行为的发生地点和具体侵权程度的，这种举证规则对互联网环境下企业商业秘密的所有者而言是不公平的。因为在复杂多变的互联网环境下，商业秘密所有人很难证明被告在主观上有过错。这样的情况下，在具体司法实践过程中，审判机构经常采取“举证责任倾向”的方式，以更好地契合互联网环境下对企业商业秘密保护的新要求，采取“实质相似＋接触”的举证责任标准。按照“实质相似＋接触”的举证原则，原告需要提供证据以证明侵权内容与自己所有的商业秘密的内容在实质上是较为相似的，并且被告是存在接触到自己商业秘密的可能性的，被告负责证明除此之外的其他证据内容。如果被告证明自身是通过反向工程等合法获得相应内容，则侵权行为不成立。总之，在企业商业秘密的侵权纠纷中，应该适当调整举证标准来合理分配举证责任，更加公平地制定举证责任标准。

五、结束语

随着数据相关技术愈发成熟及从业者的逐渐增多，数据作为一种企业获得利益的重要因素，逐渐变为公司之间相互角逐的“主角”。数据正在悄然改变着传统商业模式与竞争格局，并对现行法律制度提出了挑战。当企业间的数据竞争已无法避免，如何在既有法律体系中寻求企业数据保护的制度空间，则成为当下亟待解决的难题。

参考文献：

[1]彭诚信.“《民法典》出台背景下个人信息的保护和利用”专题研究[J].河南社会科学,2020,28(11):1.

[2]龙卫球.再论企业数据保护的财产权化路径[J].东方法学,2018(03):50-63.

[3]李扬,李晓宇.大数据时代企业数据边界的界定与澄清——兼谈不同类型数据之间的分野与勾连[J].福建论坛(人文社会科学版),2019(11):35-45.

[4]聂洪涛,李宁.大数据下金融交易商业秘密的保护:困境与对策[J].科技与法律,2020(01):31-37.

[5]许可.数据保护的三重进路——评新浪微博诉脉脉不正当竞争案[J].上海大学学报(社会科学版),2017,34(06):15-27.

作者简介：

闫东(1989－),男,汉族,辽宁沈阳人,硕士,研究方向:知识产权、网络法。