# 网络数据安全的司法实践

浙江高院 陈为

2021/12/10

# 浙江法院涉数字经济案件的审理情况

重点调研课题：《关于数据权益知识产权保护的调研》

民事

1.近五年来，从中国裁判文书网能够检索到的相关裁判文书有150余份，2018年以来案件数量逐年快速递增，截至2021年6月，涉及数据的2021年的诉讼案件已经超过2020年全年的总和。从地域上看，案件主要集中于北、上、广、浙、苏等经济较为发达的地区。2016年至2021年上半年，浙江法院共受理涉数据权益知识产权民事一审案件20件，其中2016年至2019年分别为2件、2件、2件、1件，2020年增幅明显，共受理8件，2021年上半年受理5件。

2.数据权益各方主体仍处于商业模式的创新阶段，对数据利用行为是否侵害他人权益没有明确预期，案件主要集中在大型互联网平台因他人获取、使用其数据的行为提起的诉讼。

# 浙江法院涉数字经济案件的审理情况

刑事

1.近五年来，浙江法院审理的涉数据权益刑事案件的裁判文书共708份，其中非法侵入计算机信息系统罪8份，非法获取计算机信息系统数据罪137份，破坏计算机信息系统罪87份，侵犯公民个人信息罪464件，侵犯著作权罪8份，侵犯商业秘密罪4份，侵犯知识产权罪的裁判文书仅占比1.69%。

2.海淀检察院刚发布了《网络安全保护检察白皮书（2016-2021）》，五年来，该院共办理网络科技犯罪案件1484件3127人，其中纯正网络科技犯罪共计271件，其中帮助信息网络犯罪活动罪181件，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40件，破坏计算机信息系统罪34件、非法利用信息网络罪15件，拒不履行信息网络安全管理义务罪1件。

3.涉企数据安全犯罪危害性增强，企业核心数据易灭失、易删改、易泄露，企业内部人员作案现象突出，第三方外包服务引发数据安全新风险，数据勒索对数据权利人造成二次伤害。

# 浙江法院涉数字经济案件的审理情况

特点：

1.民事案件案由主要为不正当竞争纠纷和著作权侵权纠纷。“在涉及大数据的相关典型案件中，不正当竞争纠纷案件占比达46.20%，著作权纠纷达23%”。浙江法院受理的数据权益知识产权民事案件案由均为不正当竞争纠纷。被诉不正当竞争行为主要表现为以下两种类型：一是数据污染，如通过刷单炒信等方式虚构交易记录、用户评价等数据，扰乱正常的市场竞争秩序，本次调研不涉及此类纠纷；二是数据爬取，即互联网企业利用网络数据爬虫等技术手段获取其他企业收集积累的数据资源用于自身经营。

2.原告多为大型互联网公司。数据是互联网与科技发展的自然产物，并逐渐成为基本生产要素，掌握海量的大型互联网平台更易成为其他互联网企业数据抓取的对象，进而引发数据权益的争夺。近年来典型的数据权益知识产权案例中，如奇虎诉百度robots协议案、新浪微博诉脉脉案、新浪微博诉超级星饭团案、大众点评诉百度地图案、酷米客诉车来了案、淘宝诉美景案、同花顺诉灯塔案、蚂蚁金服诉朗动案，国内知名的大型互联网公司基本都提起过数据权益保护诉讼。

3.主要以判决方式结案，案件调撤率较低。从结案方式来看，浙江省在近五年审结的14件数据权益知识产权案件中，判决结案10件，占比71.43%，其中判决认定构成不正当竞争的9件，胜诉率90%；调解结案1件，撤诉及按撤诉处理方式结案3件，调撤率28.57%，远低于其他知识产权民事案件。

# 浙江法院涉数字经济案件的审理情况

存在问题：

1.数据权益归属主体错综复杂。数据权益的归属问题既关乎诉讼中原告的适格性认定，也关乎行为正当性判断时所涉及的主体范围。尤其是涉及个人信息集合的数据权益归属问题在学理上最具争议。

2.数据权益难以通过知识产权专门法获得充分保护。数据权益与知识产权专门法的客体具有相通之处，都需要一定的劳动或者创新投入，都具有可复制性和非竞争性。但是，受知识产权专门法保护的客体十分有限，仅有部分数据符合受保护的要件，大量数据无法作为知识产权专门法的客体受到保护。

3.涉数据行为安全、流通、公开等价值判断因素互相交织，导致对行为的不正当性判定标准不一。企业更多地是以反不正当竞争法作为主要救济手段，在数据不正当竞争案件中需要判断数据抓取、使用行为是否正当性，但针对不同的案情，不同案例在从不同角度论述正当性标准的同时，也产生了各标准之间的冲突。

4.审判机制协调性仍需加强。三合一审判发挥了重大的作用，但涉及数据案件的法律行为多样，如刑事案件中，大量涉数据案件均非知识产权犯罪，各审判庭之间的裁判标准的统一仍需加强。

# 典型案例一

1数据贩卖。“大数据时代，如果你没有为某个产品会费，那你自己本身就是产品。”2020年11月，圆通速递被爆出有多位内鬼有偿租借员工账号，导致40万条公民个人信息被泄露事件。今年的315晚会中，也披露了多地商家装有具有人脸识别的摄像头，在客户毫无知觉的情况下，偷偷收集海量顾客人脸信息，涉及万店掌、悠络客、雅量科技、瑞为等公司；智联招聘、前程无忧、猎聘网等多个招聘平台存在泄露求职者简历并被贩卖的现象。

2.数据垄断。2019年，德国联邦卡特尔局对Facebook涉嫌滥用市场支配地位行为做出处罚，认为其通过用户协议条款，迫使用户同意公司收集和使用在其他平台的数据，构成垄断行为。德国最高法院作出裁定，支持了FCO对Facebook滥用市场支配地位的认定及限制其对个人数据进行处理的相关决定。二选一、大数据杀熟。数据垄断将会间接引起数字权利滥用的问题，或将威胁到国家安全。

3.数据窃取。2018年，浙江绍兴侦破一起特大流量劫持案，涉案的新三板挂牌公司北京瑞智华胜科技股份有限公司，涉嫌非法窃取用户个人信息30亿条，涉及百度、腾讯、阿里、京东等全国96家互联网公司产品。法院判决7名被告人分别判处3年6个月到对 2年不等的刑期，并处罚金。涉爬虫的不正当竞争案件就更多了。

4.数据泄露。滴滴上市事件，4.93亿活跃用户，1500万活跃司机，纽交所退市，港交所上市准备工作。2020年3月19日，有用户发现5.38亿条微博用户信息在暗网出售，其中1.72亿条有账户基本信息。Facebook被罚50亿美元。

# 典型案例二

杭州某网络科技公司和汪某侵害商业秘密纠纷一案

简要案情：网络公司与主播签约，用户通过注册以现金充值方式获得代币，以代币向主播打赏，主播按约定比例以代币向公司兑换收益。为鼓励用户注册并使用代币，科技公司在用户充值环节设置中奖程序，后台将当日注册用户消费额90%的代币进入奖池，用户有机会获得其打赏金额的10倍、100倍的代币。汪某为科技公司前管理人员，其在任职期间，利用其管理员的职务便利，以管理员账号登陆、查看后台中奖数据进程，根据奖池代币金额、是否已被他人中奖等其他用户无法获取的数据，择时充值、打赏，中奖后将代币再以打赏方式转移至事先约定的主播，并与主播私下分成。在离职期间，入股另一家直播公司，与科技公司管理人员串通，继续用上述手段获取代币，共获利260万元。科技公司向公安举报内部人员受贿一案中，汪某在询问笔录中承认了上述事实，该刑事案件被撤销后，科技公司向法院起诉汪某侵害商业秘密，要求适用惩罚性赔偿390万元。

# 典型案例一

杭州某网络科技公司和汪某侵害商业秘密纠纷一案

法院认定:
1.科技公司主张打赏中奖的实时数据和通过中奖数据分析推算的中奖概率等经营数据属于反法保护的商业秘密。
2.汪某的行为构成对科技公司商业秘密的侵害。
3.汪某的行为符合故意和情节严重的要件，可以适用惩罚性赔偿，根据其侵权获利的1.5倍计算，支持科技公司300万的赔偿数额。

# 典型案例一

杭州某网络科技公司和汪某侵害商业秘密纠纷一案

典型意义：
经营性数据符合商业秘密中商业价值的认定。
1.科技公司的相应经营性数据既是影响平台正常经营的安全风险所在，亦是平台累积的数据资源优势所在，能为经营者带来商业利益。
2.科技公司的经营数据蕴含着用户的打赏习惯和消费水平等深层次信息，体现用户的交易内容和偏好，帮助经营者提高用户粘性，获取持续的交易关系和稳定的流量。
3.科技公司的经营数据中包含的中奖分配和相关排列组合信息，体现了经营者特定经营策略，是企业重要的经营利益之所在。

# 从典型案例看司法实践对数据安全的考量

数据安全与数据价值紧密相关

1.数据产生、流通与应用是大数据生态中完整的产业链，而数据流通是关键节点，其中涉及的数据生产者、所有者、使用者、管理者等在数据流通中承担了多种角色，如何充分识别各种角色，如何精准地为每种角色分配应有的权限，如何保障流通中的安全，这些问题直接影响了数据流通乃至价值。

2.数据安全与数据信任精密相关，可以说数据安全是数字经济的底座与基石，数字经济需要使一切链入或映射到数字空间的网络实体在以数字身份信任和可信数字流通为两大核心建设的信任支撑体系下，通过制度、管理、技术等一系列组合方式减少数字空间安全风险，并形成数字社会安全交互、高效运行的机制，更好地实现数据价值。

3.数据安全是数据价值的“新风口”，滴滴事件折射出包括数据跨境审查在内的数据安全合规问题引起了各方重视，《数据安全法》的施行使数据安全领域有法可依，《数安条例》更是为网络数据安全领域各方主体的行为提出了明确的行为准则。同样，也为数据价值的实现扫除了障碍。

# 从典型案例看司法实践对数据安全的考量

司法实践尚无明确的规则

1.数据权属界定不清晰。

2.数据分类模糊。

3.数据行为纷繁复杂。

4.数据法律更新快，且有冲突之处。

# 《网络数据安全管理条例（征求意见稿）》

1.地位：《网络安全法》《数据安全法》《个人信息保护法》的实施条例。

2.框架

第一章 总则
第二章 一般规定
第三章 个人信息保护
第四章 重要数据安全
第五章 数据跨境安全管理
第六章 互联网平台运营者义务
第七章 监督管理
第八章 法律责任
第九章 附则

# 《网络数据安全管理条例（征求意见稿）》

1.地位：《网络安全法》《数据安全法》《个人信息保护法》的实施条例。

2.沿袭、细化、完善方面：
（1）数据分类分级保护制度：明确数据分级（一般数据、重要数据、核心数据），细化分级分类的要求（重要数据重点保护，核心数据严格保护），专章规定重点保护的细化要求，明确保护方式——制定目录和报备
（2）数据安全风险管理制度：强化评估报告（赴境外上市的数据处理者）、明确行业评估监管、加强个人信息保护风险监测义务。
（3）数据安全应急处理机制：主管部门、行业管理者、数据处理者，明确数据应急机制、数据应急预案、数据应急处置。
（4）数据安全审查制度：明确数据安全审查适用条件、数据安全审查流程
（5）数据出口管制和反制机制：将出口管制数据明确列为重要数据之一。
（6）数据交易管理制度：明确强调了数据交易机构的整入管理。

3.创新
（1）数据安全审计制度：自主审计和检查审计
（2）网络身份认证基础设施：建立类似于公安机关的网络身份认证公共服务基础设施避免运营者对个人信息的直接收集。

# 《网络数据安全管理条例（征求意见稿）》意见建议

第六章 互联网平台运营者义务

1.73条九、十：互联网平台经营者和大型互联网平台经营者，主要问题在于大型互联网平台经营者中关于顿号之间的关系，“大量”“强大”“市场支配地位”等用语或不确定、或证明难度大、或不是法律用语。

2.43条：（1）算法策略的披露与责任的协调，上位法中未见算法策略的强制披露义务，《条例》也未对算法策略作相应解释，可能造成与平台商业秘密之间的冲突，建议对算法策略进行细化。（2）如何判断对用户权益有重大影响的判定建议明确。（3）日活用户用语欠妥当，不是一个法律用语，界定较难。

3.44条：平台先行赔偿制度。（1）前后条款衔接问题。此处的第三方产品和服务造成损害概念太大，从前款来看应当限于涉及第三方数据处理者提供产品或服务，但易解读成所有的产品或服务；（2）上位法依据问题。民法典、网络安全法、数据安全法、个人信息保护法均未规定否定避风港制度的无过错责任，在《条例》中予以规定是否合法？（3）平台与第三方涉及多种数据处理关系，委托处理、共同控制数据、既不属于委托也不属于共同控制，不同平台对第三方的控制能力也不同，如严格要求平台先行赔付，虽加强监管，平台也往往进行转嫁，最终影响的是用户的利益。

# 《网络数据安全管理条例（征求意见稿）》意见建议

第六章 互联网平台运营者义务

4.45条：条款用语为国家鼓励，但设置了相应法律责任条款，违反该条的情形如何界定？没有区分个人通信和非个人通信信息？还是针对个人通信没有按照个人信息保护要求严格保护的行为？

5.46条：（1）大数据杀熟，具有市场支配地位的平台经济领域经营者，利用对个人偏好数据掌控的优势，通过推荐定向广告、营销网页等来固化交易相对人对差异定价的认知，向已经形成消费依赖的客户群体收取高价格，同时以低价格吸引潜在客户群体。通过对交易相对人进行用户画像，对同一商品进行精准的差异化标准、规则或算法定价，实施“大数据杀熟”。但《条例》的规定大大拓宽了对于大数据杀熟的内涵和外延，既缺少市场支配地位的条件，也没有排除、限制市场竞争的结果要件，容易对平台正常竞争带来影响。
（2）对于最低价销售是促进竞争还是损害竞争，是个非常复杂的话题，可能会限制商业模式的创新。
（3）平台数据的限制利用。中小企业如何界定？非平台用户的权益如何保护？纵观数据抓取案例中，大互联网平台均赢得胜利，但实践中也出现平台利用数据优势，在商业模式上对经营者进行反向模仿，再打击竞争者获得胜诉的案件也曾出现。可能会成为平台限制向平台外企业开放数据的合理化条款。

# 谢谢聆听