**造谣引流案例**

•山东枣庄某传媒公司为吸粉引流，买大量实名自媒体账号，用人工智能编造谣言，发视频、图文300余万条，87名嫌疑人落网，查获近10万个违法违规账号。

•广东广州叶某某等人为赚流量收益，招兼职注册账号，用人工智能改写文章发50余万篇虚假信息，6名嫌疑人被抓。

•温州许某某等人设公司，组洗稿团队，用人工智能翻炒旧闻，非法获利200余万元，17名嫌疑人被抓获。

**网络敲诈勒索案例**

•江西抚州邹某某等人成立传媒公司，搜集企业负面信息发近万篇帖文，敲诈100余家企业，获利1000余万元，11名嫌疑人被抓。

•河南南阳宋某某等人冒充记者，编造2000余条负面帖文及视频敲诈企事业单位，12人被抓，查获3000余份虚假新闻手稿。

**刷量控评案例**

•浙江台州范某等人搭建刷单平台，为3万余家商户提供刷单服务，刷单1000余万条，26名嫌疑人落网。

•江苏宿迁宗某等人成立工作室，用“群控”软件操控账号，为直播、“饭圈”提供刷量控评服务，获利数千万元，7名嫌疑人被抓。

•四川内江赵某某等人以“躺赚”诱网民入会，组织10万余人在直播间互动及虚假购物好评，23名嫌疑人被抓获。

**有偿删帖案例**

•江苏镇江肖某等人组建群组，买账号，为文娱、电商人员有偿删帖1万余条，获利200余万元，10名嫌疑人被抓。

•辽宁锦州西某等人招募300余人，在汽车测评平台发40余万条虚假评论，删1000余条负面评论，3名嫌疑人落网。

**软暴力案情分析**

**案情概述**

根据江门市新会区人民法院发布消息，某犯罪团伙6人通过网络软暴力手段催收债务，包括电话轰炸、短信威胁、PS侮辱性图片、骚扰亲友等行为，形成恶势力组织，最终被法院以寻衅滋事罪、侵犯公民个人信息罪等罪名判刑（主犯获刑五年三个月）。该案是打击网络软暴力催收的典型案例，涉及对新型网络犯罪行为的法律定性。

**案件详情**

为牟取不法利益，肖某、杨某经密谋，按6:4出资比例成立某公司，专门接受金融机构委托对信贷逾期债务人及相关关系人进行催收。

该公司人员组织架构完备、层级分明，由肖某担任法定代表人、执行董事，负责对外接洽业务、对外转包业务；杨某担任监事，负责公司人事、业务管理、员工培训等。涂某等人先后入职该公司，先后担任催收员、催收组长。

催收员根据金融贷款公司提供的联系方式或者从肖某购买的公民个人信息，有组织地采取骚扰电话、高频电话呼叫、短信轰炸、PS抖音图片、叫外卖服务上门等“软暴力”手段，骚扰、威胁、辱骂、恐吓债务人及其亲属、其他社会关系人、债务人及其亲属所在工作单位，从而逼迫债务人还款，影响他人正常工作、生活、生产、经营，严重破坏社会秩序，形成以肖某、杨某为首要分子，涂某等四人为成员的恶势力犯罪集团。

2023年6月至10月期间，上述恶势力犯罪集团为牟取不法利益，对涉及全国部分省市的32名债务人实施了上述“软暴力”催收行为，造成二十多家单位及工作人员无法正常经营、工作，30余名被害人因此产生恐惧、恐慌心理，导致家庭矛盾，两名被害人因此被辞退、离职。各被告人的行为影响他人正常工作、生活、生产、经营，严重破坏社会秩序。

法院审理认为，本案被告人使用从网贷公司或非法渠道处获取的债务人及其他关系人信息，滋扰、纠缠、辱骂债务人及其他关系人，破坏他人生活安宁和工作秩序，实施时间长、次数多、被害人人数多，其中导致部分被害人离职、停职，行为程度达到情节恶劣，严重影响他人的工作、生活的程度，构成寻衅滋事罪。

涉案被告人有组织地实施的或者足以使他人认为暴力、威胁具有现实可能性的软暴力催收行为，使他人产生恐惧、形成心理强制。尤其是各被告人恶意滋扰与债务无关的其他人员、单位，严重破坏社会秩序，具有为非作恶，欺压百姓的特征，产生较为恶劣的社会影响，应认定为恶势力犯罪集团。

被告人肖某、杨某在该恶势力犯罪集团纠集开始时就起组织、策划、指挥作用，客观上反映其处于核心地位，所起作用重要，应认定为恶势力犯罪集团的首要分子，按照集团所犯的全部罪行处罚。被告人涂某等四人多次参与恶势力犯罪集团的违法犯罪活动，是固定的组成人员，但被告人涂某、谢某、陈某、黄某被动参与共同犯罪，均起次要所用，是从犯，应当从轻处罚。

被告人肖某犯寻衅滋事罪、侵犯公民个人信息罪被数罪并罚，判处有期徒刑五年三个月，并处罚金6万元，被告人杨某犯寻衅滋事罪，被判处有期徒刑五年，并处罚金5万元，其余四名被告人被判处一年六个月至一年不等有期徒刑。

新会法院综合各被告人的犯罪情节、所起作用，遂作出上述判决。被告人肖某、杨某不服，提出上诉。江门中院经二审维持原判。

公安部近日公布了2024年依法打击网络黑客犯罪8起典型案例。

2024年，按照公安部统一部署，全国公安机关网安部门聚焦危害系统数据安全、社会公共秩序、生产交通安全、市场税收秩序、生态环境安全等突出黑客犯罪活动，全力推进打击网络黑客犯罪专项工作。全年，共侦破相关案件1600余起，抓获犯罪嫌疑人4900余名，有力震慑网络黑客犯罪活动，切实维护网络安全和数据安全。

**案情梳理**

**1、浙江杭州公安机关侦破祁某等人非法获取计算机信息系统数据、非法控制计算机信息系统案。**2023年8月以来，以祁某为首的黑客团伙开发勒索病毒程序，对杭州某医药公司等实施渗透入侵、植入病毒、敲诈勒索等违法犯罪活动，导致受害企业因系统瘫痪无法正常经营，造成严重损失。2024年1月，浙江杭州公安机关抓获祁某等4名犯罪嫌疑人。公安部网安局在本案基础上，及时对存在网络安全风险隐患的600余家企业进行通报预警，指导开展漏洞修复等工作。

**2、黑龙江大庆公安机关侦破张某等人非法控制计算机信息系统案。**2023年4月以来，犯罪嫌疑人张某雇佣黑客编写“木马”病毒，组织“投毒手”在互联网电商平台寻找并添加特定行业商户客服微信，以下单、询价等理由，发送伪装成订单明细、采购计划的“木马”病毒，诱骗受害人点击后实施非法控制，进而实施精准诈骗等犯罪活动。2024年9月，黑龙江大庆公安机关抓获张某以及黑客、“投毒手”共18人，查明被控电脑1100余台。公安部网安局在本案基础上部署全国网安部门开展集群打击，共打掉黑客等犯罪团伙80余个，抓获犯罪嫌疑人270余人。

**3、安徽合肥公安机关侦破李某某等人提供侵入、非法控制计算机信息系统程序、工具案。**2023年9月以来，犯罪嫌疑人黄某某等人建立窝点，并雇佣李某某等人研发“木马”病毒，通过非法侵入、控制部分公司财务人员电脑，窃取相关数据后，再冒充公司老板，针对公司财务人员实施精准诈骗。2024年5月，安徽合肥公安机关抓获黄某某、李某某等犯罪嫌疑人17名，及时预警劝阻全国7200余家感染该“木马”病毒的公司，止损资金2.65亿元。

**4、四川成都公安机关侦破某三甲医院专家号被“抢号”案。**2023年1月以来，多个犯罪团伙在社交平台发布代抢某三甲医院专家号源的广告。经查，相关团伙通过制作抢号外挂程序，绕过医院网络挂号系统安全验证、风控机制进行抢挂号，并收取“代抢”费。2024年7月，四川成都公安机关抓获犯罪嫌疑人54名，查明涉案金额700余万元。

**5、广东东莞公安机关侦破某机动车驾驶培训机构作弊案。**2023年5月以来，犯罪嫌疑人吴某联合部分驾校，通过替学员代刷学时设备生成虚假学时数据，让学员在未完成规定培训学时的情况下获得机动车驾驶证，严重扰乱驾驶培训行业经营秩序，威胁道路交通安全。2024年1月，广东东莞公安机关抓获犯罪嫌疑人87名，查处驾校62家。

**6、浙江绍兴公安机关侦破莫某等人涉嫌破坏计算机信息系统案。**2024年1月以来，以莫某为首的黑客团伙勾连电子秤系统芯片生产厂家工作人员，制作可修改电子秤系统数据的作弊芯片，将正常的电子秤非法改装成可用指令调控重量及显示数值的的“鬼秤”并进行兜售牟利。2024年11月，浙江绍兴公安机关抓获犯罪嫌疑人21名，涉案金额达上亿元。

**7、河南安阳公安机关侦破某公司篡改、伪造监测数据污染环境案。**2022年3月以来，河南安阳某第三方环境检测机构为使合作企业排污数据达标，通过向监测系统植入“木马”病毒等方式篡改排放数据，致使监测数据长期失真。2024年3月，河南安阳公安机关抓获犯罪嫌疑人25名，查明涉案资金1200余万元。

**8、湖南长沙公安机关侦破某工程机械企业计算机系统被破坏案。**2024年3月以来，犯罪嫌疑人郭某某等人通过对塔式起重机等重型工程机械控制器加装相关“控制器”，破坏企业计算机信息系统对工程机械的远程锁机和监测维护功能，并以此逃避偿付租赁费用，甚至将工程机械进行转卖。2024年9月，湖南长沙公安机关抓获犯罪嫌疑人3名，查明被破坏的工程机械70余台，为相关企业挽回损失3000余万元。

**例1：祁某等人非法获取计算机信息系统数据、非法控制计算机信息系统案**

**涉及罪名**

1.**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**（《刑法》第285条）

￮行为：开发勒索病毒程序，渗透入侵企业系统。

￮司法解释：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》（以下简称《解释》）第1条，非法获取支付结算、证券交易等系统数据，或控制20台以上计算机系统的，属“情节严重”。本案涉及企业系统瘫痪，损失重大，应认定为“情节特别严重”。

2.**敲诈勒索罪**（《刑法》第274条）

￮行为：植入病毒后勒索财物。

￮量刑：根据勒索金额及造成损失，可能处3年以上有期徒刑，最高可判无期徒刑。

**数罪并罚**

祁某团伙同时触犯两罪，应数罪并罚。

**案例2：张某等人非法控制计算机信息系统案**

**涉及罪名**

1.**非法控制计算机信息系统罪**（《刑法》第285条）

￮行为：通过木马病毒控制1100余台电脑。

￮司法解释：控制100台以上计算机系统属“情节特别严重”，法定刑为3-7年有期徒刑。

2.**诈骗罪**（《刑法》第266条）

￮行为：利用被控电脑实施精准诈骗。

￮量刑：根据诈骗金额（本案未明确）及团伙规模（18人），主犯可能处10年以上有期徒刑或无期徒刑。

**案例3：李某某等人提供侵入、非法控制计算机信息系统程序、工具案**

**涉及罪名**

1.**提供侵入、非法控制计算机信息系统程序、工具罪**（《刑法》第285条第三款）

￮行为：研发木马病毒并提供给他人使用。

￮司法解释：提供专门用于非法控制的程序且违法所得5000元以上，即构成犯罪。本案涉案金额2.65亿元，属“情节特别严重”。

2.**诈骗罪**（《刑法》第266条）

￮行为：冒充公司老板骗取财务人员资金。

￮量刑：金额特别巨大（超50万元），主犯可处10年以上有期徒刑或无期徒刑。

**牵连关系**

提供工具行为与诈骗行为存在牵连，择一重罪（诈骗罪）或数罪并罚。

**案例4：医院专家号“抢号”案**

**涉及罪名**

1.**破坏计算机信息系统罪**（《刑法》第286条）

￮行为：制作外挂程序绕过医院挂号系统安全机制。

￮司法解释：对系统功能造成干扰且违法所得2.5万元以上，属“后果严重”，本案涉案700万元，属“后果特别严重”，法定刑5年以上有期徒刑。

2.**非法经营罪**（《刑法》第225条）

￮行为：通过代抢号牟利，扰乱医疗秩序。

￮量刑：非法经营数额超30万元，属“情节严重”，处5年以下有期徒刑。

**竞合处理**

外挂程序破坏系统功能与非法经营行为竞合，择一重罪（破坏计算机信息系统罪）定罪。

**案例5：驾校学时作弊案**

**涉及罪名**

1.**破坏计算机信息系统罪**（《刑法》第286条）

￮行为：篡改学时数据生成虚假记录。

￮司法解释：干扰系统数据造成严重后果（威胁道路交通安全），处5年以下有期徒刑。

2.**伪造、变造国家机关证件罪**（《刑法》第280条）

￮行为：虚假学时数据用于申领驾驶证，可能构成伪造国家机关证件罪。

**数罪并罚**

同时触犯两罪，应数罪并罚。

**案例6：电子秤“鬼秤”作弊案**

**涉及罪名**

1.**破坏计算机信息系统罪**（《刑法》第286条）

￮行为：篡改电子秤系统数据。

￮司法解释：违法所得2.5万元以上或造成经济损失5万元以上即构罪，本案涉案上亿元，属“后果特别严重”。

2.**生产、销售伪劣产品罪**（《刑法》第140条）

￮行为：销售非法改装的“鬼秤”，可能构成此罪。

**择一重罪**

以破坏计算机信息系统罪（最高15年）定罪，因其社会危害性更显著。

**案例7：篡改环境监测数据案**

**涉及罪名**

1.**破坏计算机信息系统罪**（《刑法》第286条）

￮行为：植入木马篡改监测数据。

2.**污染环境罪**（《刑法》第338条）

￮行为：通过篡改数据掩盖排污超标，造成环境污染。

￮司法解释：篡改监测数据属“严重污染环境”情形（《关于办理环境污染刑事案件适用法律若干问题的解释》第1条），可处3-7年有期徒刑。

**数罪并罚**

同时触犯两罪，应数罪并罚。

**案例8：破坏工程机械系统案**

**涉及罪名**

1.**破坏计算机信息系统罪**（《刑法》第286条）

￮行为：破坏远程锁机和监测功能。

￮司法解释：破坏70余台设备，造成损失3000万元，属“后果特别严重”。

2.**盗窃罪或合同诈骗罪**（《刑法》第264条、第224条）

￮行为：逃避租赁费用并转卖设备，可能构成合同诈骗罪。

**数罪并罚**

破坏系统与诈骗行为独立，应数罪并罚。

**注**：前述分析仅作可能性分析，相关案件是否构成犯罪，需要根据案件事实与证据进行判定，具体量刑需结合犯罪情节、主从犯地位、悔罪表现等综合判定。

在首例游戏外挂非法经营案中，被告人谈某某、刘某某、沈某某未经授权，擅自研发、销售游戏外挂软件，经营额高达人民币 280 余万元。此案中，涉案外挂软件不仅突破游戏技术保护措施、修改数据，侵犯著作权人的合法权益，还破坏了游戏的公平环境，给运营商造成经济损失。经审理，被告人的行为构成非法经营罪。

作为被害人代理人，滕立章律师凭借专业的法律知识和丰富的经验，代为提起控告、参加庭审，为维护被害人的合法权益发挥了重要作用。这一案例再次彰显了法律对非法经营行为的严厉打击，也体现了法律在维护互联网游戏出版经营正常秩序方面的重要作用。

北京市第一中级人民法院

刑事判决书（2007）一中刑终字第1277号

抗诉机关北京市海淀区人民检察院。

原审被告人谈某某，男，35岁（1971年10月21日出生）汉族，出生地贵州省贵阳市，大学文化程度，北京市通广恒泰商贸有限公司法定代表人，暂住(略)（户籍所在地：(略)）。因涉嫌犯非法经营罪，于2005年9月7日被羁押，同年10月11日被逮捕。现羁押于北京市海淀区看守所。

原审被告人刘某某，女，36岁（1970年11月6日出生），汉族，出生地贵州省贵阳市，大学文化程度，北京市通广恒泰商贸有限公司经理，暂住(略)（户籍所在地：(略)）。因涉嫌犯非法经营罪，于2005年9月7日被羁押，同年9月8日被取保候审。

原审被告人沈某某，男，36岁（1971年6月14日出生），汉族，出生地湖北省宜昌市，硕士研究生文化程度，无业，户籍所在地：(略)。因涉嫌犯非法经营罪，于2005年9月7日被羁押，同年10月11日被逮捕。2007年3月6日刑满释放。

原审被害人：广州光通通信发展有限公司

被害人代理人：滕立章 北京XX律师事务所律师

北京市海淀区人民法院审理北京市海淀区人民检察院指控被告人谈某某、刘某某、沈某某犯非法经营一案，于二00七年二月九日作出（2006）海法刑初字第1750号刑事判决。北京市海淀区人民检察院以京海检抗字[2007]第1号抗诉书向本院提出抗诉。本院依法组成合议庭，公开开庭审理了本案。北京市人民检察院第一分院指派检察员朱琏出庭执行职务，原审被告人谈某某及其辩护人王某某、原审被告人刘某某、沈某某到庭参加诉讼。现已审理终结。

北京市海淀区人民法院判决认定：《恶魔的幻影》（又名《传奇三代》，又称传奇3G或传奇3）是经新闻出版总署审查批准引进，由中国大百科全书出版社出版，中国广州光通通信发展有限公司(以下简称光通公司)运营的网络游戏出版物。光通公司是中国大陆地区《恶魔的幻影》游戏的唯一合法运营商。《恶魔的幻影》软件由服务器端程序和客户端程序组成，其软件部分和动画形象部分分别属于我国《著作权法》所保护的计算机软件作品和美术作品。2004年6月起，被告人谈某某未经授权或许可，组织他人与其共同使用跟踪软件动态跟踪《恶魔的幻影》客户端运行，又用IDA软件静态分析该客户端，最终用反汇编语言将客户端程序全部反汇编，从而获悉《恶魔的幻影》软件的数据结构，在破译《恶魔的幻影》游戏服务器端与客户端之间经过加密的用于通讯和交换数据的特定通讯协议的基础上，研发出“007传奇3外挂”计算机软件（以下简称007外挂软件）。后被告人谈某某等人设立“007智能外挂网”网站（www.wg1818.com）和“闪电外挂门户”网站（www.wgdoor.com），上载007外挂软件和《恶魔的幻影》动画形象，向游戏消费者进行宣传并提供下载服务，并向游戏消费者零售和向零售商批发销售007外挂软件点卡。游戏消费者及零售商向其网站上公布的在本市海淀区、昌平区等银行开设的名为“王亿梅”的账户汇入相应价款后，即可获得点卡。被告人刘某某负责外挂软件销售，被告人沈某某负责网站日常维护。2005年1月，北京市版权局强行关闭上述网站并将网络服务器查扣之后，被告人谈某某、刘某某、沈某某另行租用网络服务器，在恢复开通“闪电外挂门户”网站的基础上，先后设立“零零发：传奇3智能外挂”网站（www.wg0008.com）和“超人外挂”网站（www.wg8888.com），继续宣传其陆续研发的“008传奇3外挂”计算机软件（以下简称008外挂软件）、“超人传奇3外挂”计算机软件（以下简称超人外挂软件），提供上述软件的下载服务，并使用恢复开通的“闪电外挂门户”网站销售上述两种外挂软件的点卡，销售收入仍汇入名为“王亿梅”的账户。至2005年9月，被告人谈某某、刘某某、沈某某通过信息网络等方式经营上述外挂软件的金额达人民币2 817 187.5元。

网络游戏消费者要使用《恶魔的幻影》，在正常情况下，只需通过下载客户端程序后，在互联网上与服务器端连接即可运行游戏；若使用007外挂软件、008外挂软件，则不仅要下载《恶魔的幻影》软件客户端程序，而且要输入《恶魔的幻影》和007外挂软件、008外挂软件所要求的用户名和密码，这样才能最终与《恶魔的幻影》服务器端连接；而若使用超人外挂软件，则无需下载《恶魔的幻影》网络游戏软件客户端程序，就能直接与《恶魔的幻影》服务器端连接，但也必须输入《恶魔的幻影》和超人外挂软件所要求的用户名和密码。使用涉案外挂软件运行《恶魔的幻影》的消费者，要同时向运营商光通公司和外挂经营者谈某某等人付费。

涉案上述系列外挂软件使用了《恶魔的幻影》的地图场景名称等名词；超人外挂程序目录中存在一个与《恶魔的幻影》软件目录相同反映服务器端IP地址的配置文件。《恶魔的幻影》客户端程序在内存中的动态表现形式只有以非加密的形式存在，才能被执行。涉案007外挂软件、008外挂软件在运行时，利用上述条件，能绕过客户端程序经加密的静态文件，直接对《恶魔的幻影》客户端程序在内存中的动态表现形式进行修改，并调用《恶魔的幻影》所使用的大量函数，使007外挂软件、008外挂软件功能能添加到《恶魔的幻影》运行过程之中。加载了007或008外挂软件的《恶魔的幻影》客户端，所发送的对原游戏功能作出修改的数据也可被《恶魔的幻影》服务器端接收和反馈。而使用超人外挂软件的游戏消费者在启动《恶魔的幻影》网络游戏软件后，即使消费者不再亲自操控游戏，该外挂软件也能使处于在线状态的游戏一直进行下去。上述外挂软件的运行，改变了《恶魔的幻影》网络游戏软件设定的游戏规则，使用外挂软件的消费者较之未使用外挂软件的消费者在游戏能力上取得了明显的优势地位，通过外挂软件设置的功能可以更容易和更快地升级或过关，从而造成游戏消费者之间游戏能力明显不平等的局面。

2005年9月7日，被告人谈某某、刘某某、沈某某被抓获归案。作案工具亦被起获，涉案27个银行账号已被冻结，赃款人民币51 700元扣押在案。

上述事实，有经一审法院庭审举证、质证的被告人谈某某、刘某某、沈某某的供述、证人俞XXXXXXXXXXX的证言、电子数据司法鉴定结论、物证检验报告、笔记鉴定书、北京市版权局著作权鉴定书、北京市版权局《007外挂举证报告》及附件、新闻出版总署的批复、案件函、搜查笔录、扣押物品清单、到案经过、光通公司举报材料、照片、数额认定说明、认定王亿梅的身份证号码的真实身份的书证、冻结及余额查询手续、北京市版权局出具的关于007外挂非法收入的计算方法的补充说明等证据予以证实。

**孙某媛制造、散播网络谣言敲诈勒索案**：孙某媛因自认为侯某与主播关系暧昧，辱骂侯某并向其家人宣称婚内出轨，索要100万被拒后，散布侯某多种虚假信息，还向相关部门举报，导致侯某轻生获救后仍继续索要钱财，后被抓获。

•**赵某杰利用网络敲诈勒索未成年人案**：赵某杰用QQ添加未成年女性为好友，以到学校和家中持刀捅人相威胁，向4名未成年人索要共计18964元，案发后退赔并取得谅解。

•**相某漫编造事由向网络平台商家恶意索赔敲诈勒索案**：相某漫在多个线上外卖平台购买食品投放异物，以不赔偿就投诉相威胁，向4家餐饮店铺索要共计3169元。

•**罗某甲等人制造、散播负面信息并以有偿删帖方式敲诈勒索案**：罗某甲等人作为新闻媒体从业人员，注册公司和账号，发布企业负面消息，以不支付“商务合作”费用就不删帖相要挟，向6家互联网企业索要29.6万元。

•**李某等人以“裸聊”为诱饵敲诈勒索案**：李某与他人共谋，偷渡到缅甸，通过“客服”引诱被害人“裸聊”录制不雅视频、植入病毒读取通讯录，“枪手”以散布不雅视频相要挟索要钱款，从30余名被害人处索要70余万元。

•**贺某武为网络敲诈勒索犯罪分子提供技术支持案**：贺某武与龙某鹏共谋，为缅甸“裸聊”敲诈勒索犯罪窝点搭建跨境网络专线并维护，获利857万余元，导致学生吴某明被敲诈勒索34.4万元，贺某武被抓获后主动上交违法所得并返还部分损失获得谅解。

**孙某媛案**：孙某媛构成敲诈勒索罪，虽系犯罪未遂，但犯罪情节恶劣，依法予以从严惩处，判处有期徒刑八年七个月，并处罚金人民币十万元。

•**赵某杰案**：赵某杰构成敲诈勒索罪，对多名未成年人实施敲诈勒索应从重处罚，到案后如实供述、自愿认罪认罚、积极退赔并取得谅解可从轻处罚，判处拘役六个月，并处罚金人民币二万元。

•**相某漫案**：相某漫构成敲诈勒索罪，到案后如实供述、自愿认罪认罚可从轻从宽处理，判处有期徒刑七个月，并处罚金人民币四千元，并责令退赔违法所得。

•**罗某甲等人案**：罗某甲等人构成敲诈勒索罪，罗某甲是主犯，其余为从犯，部分人有自首、坦白情节，均认罪认罚可从轻从宽处理，罗某甲判处有期徒刑三年十个月，并处罚金人民币五万元；其余五人分别判处有期徒刑并适用缓刑，并处罚金；追缴违法所得。

•**李某等人案**：李某等人构成敲诈勒索罪，李某系主犯，依法按全部犯罪处罚，王某佳、谷某、钟某龙系从犯从轻或减轻处罚，李某判处有期徒刑十二年，并处罚金人民币十万元，与前罪并罚决定执行有期徒刑十二年六个月，并处罚金人民币十万五千元；王某佳、谷某、钟某龙判处九年至六年不等有期徒刑，并处罚金；共同退赔被害人财产损失。

•**贺某武案**：贺某武构成敲诈勒索罪，有坦白情节、认罪认罚、退缴违法所得、退赔部分损失并取得谅解可从宽处罚，判处有期徒刑四年五个月，并处罚金人民币五万元

。

**孙某媛案**：孙某媛构成敲诈勒索罪，虽系犯罪未遂，但犯罪情节恶劣，依法予以从严惩处，判处有期徒刑八年七个月，并处罚金人民币十万元。

•**赵某杰案**：赵某杰构成敲诈勒索罪，对多名未成年人实施敲诈勒索应从重处罚，到案后如实供述、自愿认罪认罚、积极退赔并取得谅解可从轻处罚，判处拘役六个月，并处罚金人民币二万元。

•**相某漫案**：相某漫构成敲诈勒索罪，到案后如实供述、自愿认罪认罚可从轻从宽处理，判处有期徒刑七个月，并处罚金人民币四千元，并责令退赔违法所得。

•**罗某甲等人案**：罗某甲等人构成敲诈勒索罪，罗某甲是主犯，其余为从犯，部分人有自首、坦白情节，均认罪认罚可从轻从宽处理，罗某甲判处有期徒刑三年十个月，并处罚金人民币五万元；其余五人分别判处有期徒刑并适用缓刑，并处罚金；追缴违法所得。

•**李某等人案**：李某等人构成敲诈勒索罪，李某系主犯，依法按全部犯罪处罚，王某佳、谷某、钟某龙系从犯从轻或减轻处罚，李某判处有期徒刑十二年，并处罚金人民币十万元，与前罪并罚决定执行有期徒刑十二年六个月，并处罚金人民币十万五千元；王某佳、谷某、钟某龙判处九年至六年不等有期徒刑，并处罚金；共同退赔被害人财产损失。

•**贺某武案**：贺某武构成敲诈勒索罪，有坦白情节、认罪认罚、退缴违法所得、退赔部分损失并取得谅解可从宽处罚，判处有期徒刑四年五个月，并处罚金人民币五万元。

最高法发布惩治网络敲诈勒索犯罪典型案例

最高人民法院

随着信息网络与社会生活的深度融合，违法犯罪行为也正在向网络空间扩散。近年来，利用网络制造散播谣言、负面信息进行敲诈勒索的案件时有发生，严重损害人民群众和企事业单位的名誉权、财产权等合法权益，危害网络安全、社会稳定和经济发展。党和国家高度重视防范和惩治网络敲诈勒索等违法犯罪工作。为充分发挥典型案例的震慑、警示、教育作用，标明网络行为红线，指明依法维权路径，最高人民法院发布6件依法惩治利用网络敲诈勒索犯罪典型案例。本次发布的典型案例，具有以下三个方面的特点：

**一是彰显依法严厉惩处的态度。**一些不法分子利用网络传播门槛低、速度快、影响大的特点，在网络空间肆意制造、散播谣言和负面信息非法敛财，社会危害严重，人民群众反映强烈。此次公布的典型案例涉及网络造谣、恶意索赔、曝光企业“黑料”后寻求“商务合作”、借“裸聊”实施威胁等多种敲诈勒索新型犯罪手段。虽然手段升级，但本质上仍是以非法占有为目的，采取威胁、要挟手段迫使他人基于心理强制交付财物，对于依照刑法第二百七十四条规定构成敲诈勒索罪的，人民法院坚决依法从严惩处。

**二是坚持全链条打击的举措。**近年来，跨境“裸聊”等网络敲诈勒索犯罪呈现出团伙化、链条化、国际化的特征，一些不法分子明知他人利用信息网络实施敲诈勒索犯罪仍为其提供资金、场所、技术等方面的帮助，促使此类犯罪滋生蔓延，必须坚持全链条打击、全方位惩处。人民法院审理此类案件时坚持全面准确贯彻宽严相济的刑事政策。一方面,重点惩处团伙犯罪中的组织者、策划者、指挥者和骨干成员，该判处重刑的，坚决依法重判。另一方面，对具有从犯、自首、坦白、立功等从轻、减轻处罚情节的，依法予以从宽处理。

**三是倡导被害人积极寻求法律保护。**审判过程中发现，有的敲诈勒索被害人因为害怕隐私暴露不敢报警，有的被害单位因自身存在问题怕被追责或影响生产经营不愿报警，导致一些犯罪行为没有被及时制止和打击。通过此次公布典型案例，告诫不法分子网络虽是虚拟空间，但绝非法外之地，违法犯罪必然要付出沉重的代价。同时，也鼓励网络犯罪被害人在自身合法权益受到侵害时及时报案寻求公安、司法机关的帮助，勇于拿起法律武器与违法犯罪作斗争。

以人民为中心是新时代坚持和发展中国特色社会主义的根本立场。依法惩治网络敲诈勒索犯罪，切实维护人民群众的人身和财产安全，事关家庭幸福安宁，事关社会和谐稳定，事关国家长治久安。人民法院通过案件办理对犯罪分子形成有效震慑，积极促进形成良好的网络氛围和公正的社会环境，确保互联网始终在法治轨道上健康运行。同时，呼吁社会各界自觉遵守互联网秩序，依法上网、文明上网，理性表达、有序参与，共同营造清朗的网络环境。

**依法惩治利用网络敲诈勒索犯罪典型案例**

一、孙某媛制造、散播网络谣言敲诈勒索案

二、赵某杰利用网络敲诈勒索未成年人案

三、相某漫编造事由向网络平台商家恶意索赔敲诈勒索案

四、罗某甲等人制造、散播负面信息并以有偿删帖方式敲诈勒索案

五、李某等人以“裸聊”为诱饵敲诈勒索案

六、贺某武为网络敲诈勒索犯罪分子提供技术支持案

**案例一**

**孙某媛敲诈勒索案**

——制造、散播网络谣言敲诈勒索

**（一）基本案情**

被告人孙某媛系某网络主播的“粉丝”，被害人侯某经营的培训机构与该主播有业务合作。2022年6月，孙某媛自认为侯某与主播关系暧昧，遂在网络直播间辱骂侯某，并通过自媒体平台找到侯某家人联系方式，借用他人电话向侯某家人宣称侯某婚内出轨。侯某要求孙某媛停止人身攻击，孙某媛索要人民币100万元，被侯某拒绝后，孙某媛给侯某的培训机构员工、学员家属打电话、发短信，散布侯某婚内出轨、偷税漏税、猥亵儿童等虚假信息。孙某媛还匿名拨打电话向相关政府部门、公安机关举报侯某的培训机构存在没有办学资质、偷税漏税等违法行为，并在多个知名网站论坛发布涉及前述虚假内容的帖子。侯某不堪其扰轻生自杀，幸被人发现获救，孙某媛又发布侯某“畏罪自杀”的帖子，并继续向侯某索要钱财。侯某向公安机关报案，孙某媛被抓获。

**（二）裁判结果**

法院审理认为，被告人孙某媛以非法占有为目的，采取威胁、要挟手段索要他人数额特别巨大的财物，其行为已构成敲诈勒索罪。孙某媛未能取得财物，系犯罪未遂，可以比照既遂犯从轻或者减轻处罚。孙某媛捏造多条虚假负面信息，匿名向被害人亲属、同事、客户以及社会公众散布，多次威胁、要挟被害人给付巨额钱财，并在被害人有自杀举动后继续人身攻击、索要钱财，犯罪情节恶劣，依法予以从严惩处。据此，对孙某媛以敲诈勒索罪判处有期徒刑八年七个月，并处罚金人民币十万元。

**（三）典型意义**

在网上炮制、散布谣言进而威胁他人交付财物，与在线下实施的敲诈勒索犯罪相比，危害更加严重。本案中，被告人孙某媛制造的谣言涉及背叛婚姻、性侵儿童、违法经营等多个方面，严重损害他人人格和名誉。孙某媛为达到非法占有的目的，采取网上发帖、拨打电话、向有关部门举报等多种方式散播谣言向被害人施压，导致被害人不堪其扰轻生自杀，虽然获救但身心已受到严重伤害。最终被害人报案，避免了更大损失。审理法院根据此案的犯罪性质、情节、后果，综合考虑从重、从轻处罚情节，对孙某媛依法从严惩处，做到了罚当其罪。本案提醒网络犯罪的受害者，在自身合法权益受到侵害时要及时报案寻求公安、司法机关的帮助，勇于拿起法律武器与违法犯罪作斗争，让网络犯罪无处遁逃。

**案例二**

**赵某杰敲诈勒索案**

——利用网络敲诈勒索未成年人

**（一）基本案情**

2020年7月至8月期间，被告人赵某杰用QQ添加14至18周岁未成年女性40余人为好友。在聊天过程中，赵某杰故意找茬称对方把自己气病，以到被害人学校和家中持刀捅人相威胁，要求被害人“拿钱治病”，先后向4名被害人（13至16周岁）索要共计人民币18 964元。案发后，赵某杰向被害人退赔违法所得并取得了谅解。

**（二）裁判结果**

法院审理认为，被告人赵某杰以非法占有为目的，采取以暴力相威胁的手段索要他人数额较大的财物，其行为已构成敲诈勒索罪。赵某杰对多名未成年人实施敲诈勒索，依法应当从重处罚；其到案后如实供述罪行，自愿认罪认罚，积极退赔并取得被害人谅解，依法可以从轻处罚。据此，对赵某杰以敲诈勒索罪判处拘役六个月，并处罚金人民币二万元。

**（三）典型意义**

网络世界对未成年人有限开放，法治社会对未成年人无限关怀。人民法院始终坚持对未成年人特殊、优先、全面保护的司法理念，依法严厉惩处针对未成年人的违法犯罪行为。在认定敲诈勒索入罪门槛及确定量刑幅度时，《最高人民法院 最高人民检察院关于办理敲诈勒索刑事案件适用法律若干问题的解释》第二条、第四条规定，对以未成年人为犯罪对象的，降低适用标准，以“数额较大”标准的50%定罪，以“数额巨大”“数额特别巨大”标准的80%提档升刑。本案中，被告人赵某杰在网络上选择多名未成年女性为作案对象，以将暴力诉诸于现实相威胁勒索财物，其行为极易对被害人形成心理强制，具有严重的社会危害性。人民法院依法对利用网络侵犯未成年人合法权益的被告人定罪处罚，为呵护未成年人身心健康提供坚强有力的司法保障。

**案例三**

**相某漫敲诈勒索案**

——编造事由向网络平台商家恶意索赔敲诈勒索

**（一）基本案情**

2021年1月至2023年4月期间，被告人相某漫在多个线上外卖平台购买食品并投放异物,随后拍照反馈给平台和商家,以不赔偿就投诉相威胁先后向4家餐饮店铺索要共计人民币3 169元。

**（二）裁判结果**

法院审理认为，被告人相某漫以非法占有为目的，以投诉相威胁勒索多家被害单位钱款，数额较大，其行为已构成敲诈勒索罪。相某漫到案后如实供述罪行，依法可以从轻处罚;其自愿认罪认罚，依法可以从宽处理。据此，对相某漫以敲诈勒索罪判处有期徒刑七个月，并处罚金人民币四千元，并责令其退赔违法所得。

**（三）典型意义**

消费者的评价和投诉对入驻电商平台商家的口碑及后续经营有着重要影响。合理差评和正当投诉有利于维护消费者的合法权益，提高商家的服务水平和竞争力。然而，一些不法分子盯上了投诉维权渠道，通过伪造有关食品安全的事实，以投诉、举报相要挟向经营者勒索钱财，利用线上平台商家重视评价、害怕影响生产经营等心理实施敲诈勒索犯罪。利用线上平台恶意“索赔”，不仅严重侵害了经营者的财产利益，也扰乱了正常的市场秩序。人民法院依法予以打击，有利于遏制恶意差评的蔓延，避免消费者被误导，维护企业合法权益，营造良好的营商环境。

**案例四**

**罗某甲等人敲诈勒索案**

——制造、散播负面信息并以有偿删帖方式敲诈勒索

**（一）基本案情**

被告人罗某甲、徐某、聂某某、杨某均系新闻媒体从业人员。2019年11月至2022年2月期间，罗某甲注册成立公司，并与徐某、聂某某、杨某以及被告人罗某乙、罗某丙等人共谋通过自媒体发布企业负面消息进而勒索财物。受罗某甲安排，罗某乙注册微信公众号“××经”并在多家知名网络平台注册第三方账号。罗某甲、杨某负责收集企业负面信息并撰写帖文，徐某负责审核，聂某某、罗某乙、罗某丙负责在微信公众号和第三方媒体账号发布、删除帖文。罗某甲还负责与被害单位谈判，罗某乙负责收款。2022年3月至7月期间，罗某甲等人利用“××经”微信公众号及相关网络平台账号发布6家互联网企业的负面帖文，迫使上述企业联系罗某甲等人，罗某甲等人以不支付“商务合作”费用就不删帖相要挟，索要被害单位钱款人民币29.6万元。

**（二）裁判结果**

法院审理认为，被告人罗某甲、罗某乙、徐某、罗某丙、聂某某、杨某以非法占有为目的，在网上发布企业负面信息，以有偿删帖的方式多次勒索他人财物，数额巨大，其行为均已构成敲诈勒索罪。在共同犯罪中，罗某甲是主犯，罗某乙、徐某、罗某丙、聂某某、杨某是从犯。罗某甲、徐某、罗某丙、聂某某、杨某有自首情节，罗某乙有坦白情节，依法可以从轻处罚。各被告人均认罪认罚，依法可以从宽处理。据此，对罗某甲以敲诈勒索罪判处有期徒刑三年十个月，并处罚金人民币五万元；对罗某乙等五人分别判处有期徒刑并适用缓刑，并处罚金；对违法所得予以追缴。

**（三）典型意义**

新闻媒体监督是发现社会问题，及时纠正违法行为的有效手段。但是，一些不法人员利用或者冒充新闻工作者的身份，专门寻找企业经营中存在的问题，打着舆论监督的旗号以发布、不删除负面帖文相要挟，直接向企业经营者索要财物或者通过所谓“合作”的方式索要财物。此类犯罪行为是以监督之名行敲诈勒索之实，既侵害了企业经营者的合法权益，又损害了新闻媒体监督的权威性，应当从严惩处。本案中，被告人罗某甲等人利用媒体从业者的身份积极挖掘企业“黑料”，利用企业经营者害怕被追责、处罚或者影响企业形象、经营业绩的心理不断发布负面消息向对方施压，并明示或者暗示企业与其“商务合作”，迫使对方交付财物，罗某甲等人的行为已构成敲诈勒索罪。该案提醒广大群众，要提高辨别真伪的本领，正常的新闻媒体监督是合法合规的，不能以揭发隐私、不法行为相威胁索要财物。个人或者企事业单位在遇到此类违法犯罪时要及时报案，避免自身合法权益受到侵害。同时警示不法分子，以谋取非法利益为目的恶意发布信息损害他人或者企事业单位的人格尊严、商业信誉、商品声誉的，必将受到法律严惩。

**案例五**

**李某等人敲诈勒索案**

——以“裸聊”为诱饵敲诈勒索

**（一）基本案情**

2020年7月至9月，被告人李某与胡某（另案处理）共谋以“裸聊”方式敲诈勒索，分别提供场地、设备、技术、支付结算账户，并通过层层联系招募“客服”“枪手”，纠集了被告人王某佳、谷某、钟某龙及谢某雄、谢某军、谢某勇（均另案处理）等人先后偷渡到缅甸。同年9月中旬至11月底，在李某指使下，“客服”谢某雄、谢某军、谢某勇等人使用王某佳收购的网络社交账号，冒充女性引诱被害人进行“裸聊”，并趁机录制不雅视频，向被害人手机植入病毒，读取手机内的通讯录信息，之后将不雅视频、手机通讯录交由“枪手”李某、梁某祥、梁某浩（另案处理）等人，再由李某等人以散布不雅视频相要挟索要钱款，先后从30余名被害人处索要人民币70余万元。所得钱款由李某进行分赃。

**（二）裁判结果**

法院审理认为，被告人李某、王某佳、谷某、钟某龙结伙以散布“裸聊”视频相要挟，向多名被害人勒索财物，数额特别巨大，其行为均已构成敲诈勒索罪。在共同犯罪中，李某负责策划、组织、指挥，提供场地、设备、技术，分配犯罪所得钱款等，起主要作用，系主犯，依法应当按照其组织、指挥及参与的全部犯罪处罚；王某佳、谷某、钟某龙起次要作用，系从犯，依法应当从轻或者减轻处罚。根据本案的犯罪事实、性质、情节、对社会的危害程度以及各被告人在共同犯罪中的地位、作用，对李某以敲诈勒索罪判处有期徒刑十二年，并处罚金人民币十万元，与尚未执行完毕的前罪掩饰、隐瞒犯罪所得罪判处的刑罚并罚，决定执行有期徒刑十二年六个月，并处罚金人民币十万五千元；对王某佳、谷某、钟某龙以敲诈勒索罪判处九年至六年不等的有期徒刑，并处罚金；共同退赔被害人财产损失。

**（三）典型意义**

近年来，通过“裸聊”实施的跨境电信网络敲诈勒索犯罪大幅增长，并呈现出团伙化、链条化、国际化的特征，严重破坏公序良俗，影响社会稳定。该类犯罪一般涉案人员较多，人民法院审理时坚持依法认定、精准打击，全面准确贯彻宽严相济的刑事政策，做到当严则严、该宽则宽，宽严相济、罚当其罪。本案中，审理法院根据被告人李某及其他被告人在共同犯罪中具体实施的行为、所起作用和主观恶性等因素判处不同刑罚，体现了区别对待的态度，对共同犯罪中的组织者、策划者、指挥者和骨干成员重点惩处，对具有从犯、自首、坦白、立功等从轻情节的低层级人员依法从宽处理。该案也警醒广大网民要增强防范意识，远离网络不良诱惑和违法行为，避免落入圈套、掉进陷阱。

**案例六**

**贺某武敲诈勒索案**

——为网络敲诈勒索犯罪分子提供技术支持

**（一）基本案情**

2022年5月，被告人贺某武与通过聊天软件结识的龙某鹏（在逃）共谋后，向网络资源商蔡某智（另案处理）购买IP地址非法搭建跨境网络专线，出售给缅甸某专门从事“裸聊”敲诈勒索犯罪的窝点，并雇佣技术人员对跨境网络专线进行维护。为规避打击，龙某鹏用泰达币及现金泰铢与上述犯罪窝点结算、与贺某武分成。至2023年2月，贺某武、龙某鹏获利共计人民币857万余元。2023年2月，某学院学生吴某明（被害人）被“裸聊”敲诈勒索人民币34.4万元。同年7月贺某武被抓获，之后贺某武主动上交违法所得，并返还了被害人吴某明的部分损失，获得吴某明的谅解。

**（二）裁判结果**

法院审理认为，被告人贺某武明知他人利用信息网络实施敲诈勒索犯罪，仍为他人提供技术支持，致使被害人吴某明被敲诈勒索数额巨大的财物，其行为已构成敲诈勒索罪。贺某武有坦白情节，认罪认罚，退缴违法所得，退赔被害人部分损失并取得谅解，依法可以从宽处罚。据此，对贺某武以敲诈勒索罪判处有期徒刑四年五个月，并处罚金人民币五万元。

**（三）典型意义**

明知他人利用信息网络实施敲诈勒索犯罪活动，仍为其提供资金、场所、技术等方面的帮助，助长了敲诈勒索犯罪的气焰，必须坚持全链条打击、全方位惩处。本案中，被告人贺某武明知境外窝点利用网络对境内人员实施“裸聊”式敲诈勒索犯罪，仍为其搭建跨境网络专线并积极提供维护服务，致使被害人损失数额巨大的财产，依法构成敲诈勒索罪的共犯。审理法院综合考虑贺某武的犯罪性质、情节、后果以及法定、酌定从宽处罚情节，在量刑上对其适当从轻，做到罪责刑相适应。该案警示广大互联网从业人员要培育正确的职业道德规范，自觉守住法律底线，为互联网在法治轨道上健康运行承担应有的社会责任。

近期，个别网民为博取眼球，继续以“转发一次得到200元红包为噱头”在社交群组内传播，造成虚假信息扩散，产生社会恐慌，公安机关网安部门迅速开展核查。

经查，网民潘某某、高某某、李某某为博取眼球，通过社交群组大量传播扩散该谣言。根据《中华人民共和国治安管理处罚法》等法律规定，属地公安机关依法对潘某某、高某某、李某某给予行政处罚。

属地公安机关依法传唤视频发布者乔某某进行调查。经查，乔某某上网时看见一条视频下方有网民评论称“盐津县水田坝放烟花炸死五六个人”，乔某某为博人眼球，吸引关注，在上述评论基础上编辑发布了上述视频。

警方随后也将在评论下散布虚假信息的杜某某查获。

严惩发布涉四川宜宾山体滑坡网络谣言违法行为 公安机关网安部门公布2起典型案例

[公安部网安局](javascript:void(0);)

 2025年02月13日 21:22 北京



2月8日11时50分许，四川省宜宾市筠连县沐爱镇金坪村2组突发山体滑坡。灾害发生后，各项工作紧张有序开展，消防员、武警官兵和民兵等各种救援力量千方百计搜救失联人员，切实保障人民群众生命财产安全。广大人民群众都希望这片土地早日恢复生机，希望所有的受灾群众尽快迎来新生活。然而，个别网民却为博取关注、吸引流量,借机编造发布涉灾害等公共安全类谣言,引发群众焦虑恐慌,造成不良社会影响，给灾害救援带来阻碍。公安机关网安部门依法严厉打击，现公布部分典型案例：

**一、造谣未受灾地区发生山体滑坡灾害。**2025年2月12日，网民秦某齐（男，48岁）为博取关注、吸引流量，冒用某自媒体公司名义，在某短视频平台发布筠连县山体滑坡视频，并谣称：“重庆特大事故，八家人全部被埋”，造成该不实信息传播扩散，产生不良社会影响。

**二、造谣救灾及民众伤亡情况。**2025年2月11日，网民吴某洪（男，30岁）在筠连县山体滑坡灾害的相关视频评论区发布捏造的救灾情况及民众伤亡人数，谣称“找到8个，有2个活的”，以此博取关注。

目前，相关属地公安机关已对秦某齐、吴某洪依法查处。

**网  警**丨**提  示**

**网络不是法外之地**

**广大网民在网上发布信息、言论**

**应遵守法律法规**

**共建清朗网络空间**

**—欢迎关注—**

冬季行动73

信息安全123

公安机关查处网络谣言218

网络谣言打击整治专项行动418

净网专项行动375

冬季行动 · 目录

上一篇十五的月亮十六圆！昨天的灯谜你答对了吗？下一篇拒绝“魔丸”谣言，守护清朗网络空间

阅读 7.0万

​网络水军行为，越来越多地受到刑事责任追究。针对网络水军行为，司法实践中会有多种不同罪名认定。常见的如将组织刷单的平台经营者认定为非法经营罪或者虚假广告罪；将网店经营者雇用刷客对同行商家进行恶评刷单的行为认定为损害商业信誉、商品声誉罪；将网店经营者雇用刷单人对自己经营的商品进行好评刷单的行为认定为虚假广告罪等等。

针对删帖、刷单等网络水军行为的定性，从目前司法实践看，并没有太大争议。但对于“转评赞”方式进行的网络水军行为，比如针对娱乐圈相关主体进行虚假“转赞评”，以提升明星、节目等的热度，吸引更多关注。其行为定性则存在一定争议。有的认定刑事犯罪，有的则认定民事侵权行为。

首先，从《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》制定背景看，并未明确涵盖“刷单炒信”行为，该司法解释的制定背景是：一些“网络公关公司”、“营销公司”通过在信息网络上进行信息炒作、发布不实信息等方式，吸引公众关注，进而牟取非法利益。这种以营利为目的，通过信息网络向他人有偿提供删除信息服务，或者明知是虚假信息，通过信息网络有偿提供发布信息等服务的行为，实际上是为诽谤、敲诈勒索、寻衅滋事等违法犯罪提供了传播虚假信息的手段、平台，扩大了信息网络上虚假信息的影响范围。不仅扰乱网络秩序，而且破坏了市场管理秩序，是当前信息网络上种种乱象的重要推手，具有较大的社会危害性，应当以非法经营罪定罪处罚。

由此可以看出，该司法解释规制的主要是为诽谤、敲诈勒索、寻衅滋事等违法犯罪目的的发布虚假信息或有偿删帖等行为。

其次，组织“转评赞”是否需要获得互联网信息服务经营许可证（ICP）？司法实践中，很多判决对这个问题都忽略了，有的认为只要是收费了，在他人电商平台上留下的购物记录及评价信息，就属于从事经营性互联网信息服务，有的认为经营者有自己的小程序或者APP，就属于从事经营性互联网信息服务，控辩双方也都很少关注这个问题。

互联网信息服务（ICP）按照《电信业务分类目录》是有明确限定的，主要包括信息发布平台和递送服务、信息搜索查询服务、信息社区平台服务、信息即时交互服务、信息保护和处理服务等。信息发布平台和递送服务是指建立信息平台，为其他单位或个人用户发布文本、图片、音视频、应用软件等信息提供平台的服务。平台提供者可根据单位或个人用户需要向用户指定的终端、电子邮箱等递送、分发文本、图片、音视频、应用软件等信息。信息搜索查询服务是指通过公用通信网或互联网，采取信息收集与检索、数据组织与存储、分类索引、整理排序等方式，为用户提供网页信息、文本、图片、音视频等信息检索查询服务。信息社区平台服务是指在公用通信网或互联网上建立具有社会化特征的网络活动平台，可供注册或群聚用户同步或异步进行在线文本、图片、音视频交流的信息交互平台。信息即时交互服务指利用公用通信网或互联网，并通过运行在计算机、智能终端等的客户端软件、浏览器等，为用户提供即时发送和接收消息（包括文本、图片、音视频）、文件等信息的服务。信息即时交互服务包括即时通信、交互式语音服务（IVR），以及基于互联网的端到端双向实时话音业务（含视频话音业务）。信息保护和处理服务指利用公用通信网或互联网，通过建设公共服务平台以及运行在计算机、智能终端等的客户端软件，面向用户提供终端病毒查询、删除，终端信息内容保护、加工处理以及垃圾信息拦截、免打扰等服务。

事实上，很多情况下并不需要办理互联网信息服务经营许可证（ICP），比如：企业利用自身网站、APP并以自营方式直接销售自身或其它企业的商品或服务，无其它单位或个人以自身名义入驻该网站、APP实施销售行为的，或者企业利用自身网站、APP自行发布信息，并非为其他单位或个人用户发布信息提供平台服务的，或者企业依托微信、支付宝等互联网平台的小程序、公众号、视频号、H5网站、线上店铺等形式经营业务，且无其他独立运营平台的，无需取得互联网信息服务经营许可证（ICP）。

组织“转评赞”，很多时候可能并不需要获得互联网信息服务经营许可证（ICP），当然需要具体情况具体分析。

最后，《全国人民代表大会常务委员会关于维护互联网安全的决定》也没有针对“对商品、服务作虚假宣传”的表现形式及罪名进行明确。需要说明的是，《最高人民法院关于准确理解和适用刑法中“国家规定”的有关问题的通知》指出，对于行为是否属于刑法第二百二十五条第（四）项的规定，有关司法解释未作明确规定的，应当作为法律适用问题，逐级向最高人民法院请示。

值得注意的是，在人民法院案例库中最新入库的“杭州市滨江区人民检察院诉杨某鹏等网络侵权责任纠纷案（入库编号：2024-18-2-369-003）”中，认定：被告杨某鹏利用其注册的多家公司研发的平台，招募数量庞大的兼职人员充当“网络水军”，并通过组织、操纵“网络水军”“养号”等方式，开展有偿“转评赞”等业务。杭州互联网法院认为，该行为扰乱了网络舆论环境和互联网信用管理秩序，损害了公共利益，应当承担民事侵权责任。

“转评赞”如何定性，可能需要结合案件中行为人的具体行为事实，进行综合评判，不能一概而论。

四川达州石某某侵犯公民个人信息案

（2017）鲁1311刑初332号

一、基本案情

四川省达州市通川区人民检察院以通川检公诉刑诉（2018）186号起诉书指控被告人石某某犯侵犯公民个人信息罪，于2018年8月9日向本院提起公诉。本院受理后，依法组成合议庭，适用普通程序公开开庭审理了本案。四川省达州市通川区人民检察院指派检察员王跃平、徐亮、吕德胜出庭支持公诉。被告人石某某及其辩护人张绍旺到庭参加诉讼。现已审理终结。

**1、公诉机关指控：**

四川省达州市通川区人民检察院指控，2016年底，被告人石某某通过互联网以1000元的价格购买了一个包含个人姓名、身份证号码等公民个人信息的压缩包，压缩包内共计公民个人信息1300余万条，然后被告人石某某以这些公民个人信息为基础，在家申请制作12306铁路购票实名账号，并将每个12306账号的用户名、密码以及所对应账号的个人姓名、身份证号码，以2元至7元不等的价格在互联网上出售，目前已出售12306实名账号20余万条，非法获利20余万元。其中被告人石某某以2元至4元一条不等的价格向在达州市通川区西外火车站倒卖火车票的冯某出售含有公民个人信息的12306账号7000余条用于网络倒票。被告人石某某于2018年4月4日被抓获归案。

为指控上述犯罪事实，公诉机关当庭举证了相关证据。据此认为，被告人石某某违反国家有关规定，非法获取、出售公民个人信息，情节特别严重，其行为应构成侵犯公民个人信息罪。提请本院依法判处。

**2、被告人及辩护人意见：**

被告人石某某辩解其虽购买了1300余万条个人信息，但没有核实个人信息的真实性，不是侵犯。其辩护人的主要辩护意见是：被告人石某某的行为不属于“情节特别严重”；其购买的1300余万条个人信息属于非法持有，而不是侵犯；其出售的个人信息是7000余条；其如实交代自己的犯罪行为，其亲属代为退清违法所得，没有前科，请求从轻处罚。其当庭举证了被告人石某某所在村民委员会出具的证明、被告人石某某的诊断报告及四川省政府非税收入一般缴款书。

**3、法院审理查明：**

经审理查明，2016年底，被告人石某某从他人处购买了1300余万条公民个人信息，包含个人姓名、身份证号码等信息。然后，被告人石某某以此为基础，在家制作12306铁路购票实名账号，并通过网络将其制作的账号及对应的公民个人信息对外出售。其中，被告人石某某先后向冯某（已判刑）出售了7000余条个人信息用于网络倒票，收取款项共计20868元。2018年4月4日，被告人石某某被民警抓获归案。案发后，从被告人石某某处扣押了手机、笔记本电脑、记事本、银行卡等物品。

二、诉讼结果

法院认为，被告人石某某违反国家有关规定，非法获取、出售公民个人信息，情节特别严重，其行为已构成侵犯公民个人信息罪。公诉机关指控的罪名成立。被告人石某某归案后尚能如实供述主要犯罪事实，可以从轻处罚；其亲属代为退清违法所得，可以酌情从轻处罚。对被告人石某某的辩护人提出的相关辩护意见，予以采纳。对于被告人石某某及其辩护人提出的其购买公民个人信息不属于侵犯公民个人信息范畴，其行为不属于“情节特别严重”的意见，与法相悖，本院不予采纳。根据被告人石某某的犯罪事实、犯罪性质、情节和对于社会的危害程度，依照《中华人民共和国刑法》第二百五十三条之一第一、三款、第六十七条第三款、第六十四条和《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》第一条、第四条、第五条第二款（三）项、第十二条之规定，判决如下：被告人石某某犯侵犯公民个人信息罪，判处有期徒刑四年，并处罚金人民币9万元；；对扣押的物品，由扣押机关依法处理。

五）案例

四川自贡畅网汽车服务有限公司、钟郑涛、刘僖非法侵入

计算机信息系统案

**一、基本案情**

被告单位四川畅网汽车服务有限公司成立于2013年5月16日，住所地自贡市贡井区贡舒路2163号，法定代表人黄茂兰，经营范围为代办车辆上户、过户、年审；代办驾驶证年审、换证、补证服务；代办车证服务、租车、二手车交易；代办车辆违章缴费服务等，被告人钟郑涛为公司总经理、实际经营者。2016年5月至2017年1月期间，被告人钟郑涛为方便公司业务的开展，利用获取到的自贡市公安局交通警察支队沿滩区大队民警黄某管理的安装有四川省公安交警警务云平台的康佳手机及其账号和密码，多次登录四川省公安交警警务云平台，查询车辆和驾驶人违章等信息。2016年12月，时任自贡市公安局交通警察支队自流井区大队舒坪中队辅警的被告人刘僖，在被告人钟郑涛的请求下，将其管理的安装有四川省公安交警警务云平台的康佳手机借给钟郑涛使用，钟郑涛则用该部手机和刘僖账号和密码以及民警卢平、黄某的账号和密码，多次登录四川省公安交警警务云平台，查询车辆和驾驶人违章等信息。经依法认定，四川省公安交警警务云平台属于国家事务类计算机信息系统。

**二、诉讼结果**

被告单位四川畅网汽车服务有限公司违反国家规定，侵入国家事务领域的计算机信息系统；被告人钟郑涛系公司的实际经营者且系公司非法侵入国家事务领域计算机信息系统直接责任人；被告人刘僖明知钟郑涛有可能登录四川省公安交警警务云平台，仍然将其管理的安装有该平台的手机借给被告人钟郑涛使用，导致被告人钟郑涛用该部手机多次登录四川省公安交警警务云平台。故，被告单位四川畅网汽车服务有限公司、被告人钟郑涛、被告人刘僖的行为均已构成非法侵入计算机信息系统罪。

**四）案例**

案例一：四川成都黄辉军、钱贵峰非法获取计算机信息

系统数据案

**一、基本案情**

2016年12月底开始，被告人黄辉军在深圳市龙岗区坪地圩老屋村二巷×号×室其暂住屋，通过在网上认识的YY昵称“赶回途中”（姓名不详、另案处理）制作含有能够盗取账户和密码的木马程序，并通过360推广，而后通过YY昵称“bbg2017”的人（姓名不详、另案处理）制作接受盗取账户和密码的“箱子”，并将箱子出售给被告人钱贵峰，非法获取深圳维京人网络科技有限公司“亲朋棋牌”游戏玩家的账户和密码超过9000条。在获取信息的同时，黄辉军将时时传输至“箱子”内的有用信息5627条（账户和密码正确）以每个14元人民币的价格卖给钱贵峰。被告人钱贵峰于2017年4月13日在南京市玄武区汇贤路兴贤家园29栋1201室被挡获。被告人黄辉军于2017年4月28日于深圳市龙岗区坪地圩老屋村二巷×号×室被挡获。

**二、诉讼结果**

被告人黄辉军、钱贵峰违反国家规定，非法获取计算机系统中储存、处理或者传输的数据，情节特别严重，其行为已构成非法获取计算机信息系统数据罪。

**三、案例简析**

1、非法获取计算机信息系统数据的方法包括入侵或者诸如“钓鱼网站”等其他技术手段。

2、非法获取计算机信息系统数据要求必须是“情节严重”。

3、对于非法获取不能识别个人身份信息的数据、账号等，可以利用非法获取计算机信息系统罪打击处理。

案例二：广东深圳刘某非法控制计算机信息系统案

**一、基本案情**

2016年10月份左右，被告人刘某以每月1600元人民币（以下币种相同）的费用向他人租用“limit”木马程序的使用权限，通过“limit”木马程序生成绑定木马的图片，自己以及雇佣其表弟钟某（分案处理）用QQ等通讯工具将绑定木马的图片发送到他人计算机，待对方点击图片后实现对对方计算机的控制并获取对方的键盘记录。对方计算机被控制后，刘某远程控制对方的计算机，在“地下城与勇士”游戏内强制与对方玩家进行游戏装备交易，然后在5173游戏平台上变卖获得的游戏装备提现。刘某与钟某作案至今共发送木马程序非法控制他人计算机约150台，刘某通过非法控制他人计算机作案获利53863.69元，钟某收取刘某支付的劳务费15000元。

**二、诉讼结果**

被告人刘某无视国法，对他人计算机系统实施非法控制，情节特别严重。其行为已经构成非法控制计算机信息系统罪，依法应予惩处。

**上海胡某拒不履行信息网络安全管理义务罪**

**（2018）沪0115刑初2974号**

一、基本案情

上海市浦东新区人民检察院以沪浦检金融刑诉〔2018〕3088号起诉书指控被告人胡某犯拒不履行信息网络安全管理义务罪，于2018年8月1日向本院提起公诉。本院于同日立案，依法组成合议庭，公开开庭审理了本案。上海市浦东新区人民检察院指派检察员吴某某出庭支持公诉，被告人胡某及辩护人马朗到庭参加诉讼。现已审理终结。

**上海市浦东新区人民检察院指控：**2015年7月至2016年12月30日间，被告人胡某为非法牟利，租用国内、国外服务器，自行制作并出租“土行孙”、“四十二”翻墙软件，为境内2000余名网络用户非法提供境外互联网接入服务。2016年3月、2016年6月上海市公安局浦东分局先后两次约谈被告人胡某，并要求其停止联网服务。2016年10月20日，上海市公安局浦东分局对被告人胡某利用上海丝洱网络科技有限公司擅自建立其他信道进行国际联网的行为，作出责令停止联网、警告、并处罚款人民币15,000元，没收违法所得人民币40,445.06元的行政处罚。被告人胡某拒不改正，于2016年10月至2016年12月30日，继续出租“土行孙”翻墙软件，违法所得共计人民币236,167元。经鉴定，“土行孙”翻墙软件采用了gotunnel程序，可以实现代理功能，适用本地计算机通过境外代理服务器访问境外网站。为证实上述指控，公诉机关当庭宣读并出示相关工作情况、行政处罚决定书、鉴定意见等证据，据此认为应当以拒不履行信息网络安全管理义务罪追究被告人胡某的刑事责任，被告人有自首情节，提请法庭依法判处。

庭审中，被告人胡某及辩护人对起诉书指控的基本犯罪事实和罪名均无意见。

**法院审理查明：**2015年7月至2016年12月30日间，被告人胡某为非法牟利，租用国内、国外服务器，自行制作并出租“土行孙”、“四十二”翻墙软件，为境内2000余名网络用户非法提供境外互联网接入服务。2016年3月、2016年6月上海市公安局浦东分局先后两次约谈被告人胡某，并要求其停止联网服务。2016年10月20日，上海市公安局浦东分局对被告人胡某利用上海丝洱网络科技有限公司擅自建立其他信道进行国际联网的行为，作出责令停止联网、警告、并处罚款人民币15,000元，没收违法所得人民币40,445.06元的行政处罚。被告人胡某拒不改正，于2016年10月至2016年12月30日，继续出租“土行孙”翻墙软件，违法所得共计人民币236,167元。经鉴定，“土行孙”翻墙软件采用了gotunnel程序，可以实现代理功能，适用本地计算机通过境外代理服务器访问境外网站。

二、诉讼结果

被告人胡某非法提供国际联网代理服务，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后拒不改正，情节严重，其行为已构成拒不履行信息网络安全管理义务罪，判处拘役六个月，缓刑六个月，罚金人民币三万元。

四川成都杨远高、苏敏非法利用信息网络案

（2019）川0108刑初489号

一、基本案情

成都市成华区人民检察院以成华检公诉刑诉[2019]466号起诉书指控被告人杨远高、苏敏犯非法利用信息网络罪一案，于2019年7月9日向本院提起公诉。本院受理后，依法适用普通程序，组成合议庭，于2019年7月29日公开开庭审理本案。成都市成华区人民检察院指派检察员黄通治出庭支持公诉，前述被告人及辩护人到庭参加了诉讼。本案现已审理终结。

**1、成都市成华区人民检察院指控**

2015年至今，被告人杨远高和苏敏共谋在成都市温江区，由被告人杨远高购买域名，由被告人苏敏提供技术支持，编写代码，共同制作非法网站（四川逍遥网、成都耍耍网等），通过在该网站上发布卖淫招嫖广告违法犯罪信息进行盈利，共计非法获利数十万。

自2016年下半年以来，曾某（已起诉至成华区人民法院）在成都市成华区“某某某小区”暂住地内，通过被告人杨远高、苏敏的网站，在网上发布招嫖信息，并多次通过微信、ＱＱ等方式介绍卖淫。

公诉机关认为，被告人杨远高、苏敏利用信息网络，为他人实施介绍卖淫的犯罪活动发布信息，其行为已触犯《中华人民共和国刑法》第二百八十七条之一的规定，应当以非法利用信息网络罪追究其刑事责任。被告人杨远高、苏敏均无犯罪前科，到案后如实供述犯罪事实，案发后积极退赔，认罪认罚，可从轻处罚。

**2、被告人及辩护人意见**

被告人杨远高对公诉机关指控的犯罪事实和罪名没有异议。辩护人提出以下辩护意见：获利金额应认定为杨远高的转账记录3万余元；被告人非法获利较少，情节轻微，具有坦白情节，认罪认罚，此前无犯罪前科，被告人家属主动退赃，杨远高为家庭经济支柱，当地社区矫正机构愿意接受杨远高社区矫正。请求法院从轻量刑并适用缓刑。

被告人苏敏对公诉机关指控的犯罪事实和罪名没有异议。辩护人提出以下辩护意见：苏敏不是网站的管理者和使用者，是从犯，本人也没有刊登过违法犯罪信息，通过建设网站获利只有一万多元，请求对其适用缓刑。

**3、法院审理查明**

法院审理查明，2015年至今，被告人杨远高和苏敏共谋在成都市温江区，先后建立四川逍遥网、四川耍耍网、成都耍耍网三个非法网站，在网站上为他人发布卖淫招嫖广告。杨远高主要负责购买域名以及网站的日常运营、管理；苏敏负责编写四川逍遥网代码、参与四川逍遥网网站前期经营，并为杨远高建立、运营四川耍耍网、成都耍耍网提供技术支持。杨远高、苏敏通过在前述网站发布卖淫招嫖广告，收取信息费用30100元，杨远高向苏敏转款6400元。经远程勘验，成都耍耍网（××）主页显示总帖数137139、会员总数103842。

另查明，自2016年下半年以来，曾某（已判决）在成都市成华区“某某某小区”暂住地内，通过四川逍遥网、四川耍耍网等网站发布招嫖信息广告，并多次通过微信、ＱＱ介绍卖淫。2018年7月，成都市公安局成华区分局治安大队在办理曾某涉嫌介绍卖淫一案时，根据曾某交代线索展开侦查，于2019年2月28日在成都市温江区内将杨远高、苏敏挡获，自杨远高处查获并扣押其使用的黑色小米手机一部，在二被告人位于成都市温江区的住所查获并扣押运营网站使用的黑色ａｃｅｒ牌笔记本电脑一台、苏敏使用的黑色苹果牌ＸＳＭＡＸ手机一部。此外，公安机关还查获并扣押玫瑰金苹果7Ｐｌｕｓ手机、玫瑰金ＯＰＰＯＲ9手机、红色无品牌手机各一部以及电脑硬盘三个。

二、诉讼结果

法院认为，被告人杨远高、苏敏为牟取非法利益，设立网站为他人实施介绍卖淫的犯罪活动发布招嫖信息，情节严重，其行为符合《中华人民共和国刑法》第二百八十七条之一的规定，构成非法利用信息网络罪，成都市成华区人民检察院起诉指控被告人所犯罪行事实清楚，罪名正确，本院予以支持。公诉机关指控被告人杨远高、苏敏非法获利数十万，仅有被告人杨远高的供述，本院不予支持，但杨远高指认其通过微信收取信息发布费用30100元，本院确认该金额为被告人获利数额，对相应辩护意见予以采纳。

本案系共同犯罪，被告人杨远高与苏敏共谋通过设立网站为他人介绍卖淫发布信息以谋取非法利益，被告人杨远高购买域名、负责网站日常运营、管理，被告人苏敏提供网站建设、维护的技术支持，二被告人不宜区分主从，本院在量刑时根据二被告人的具体犯罪作用予以量刑。对被告人苏敏的辩护人所提苏敏系从犯的辩护意见，本院不予采纳。被告人杨远高、苏敏到案后如实供述犯罪事实、认罪认罚，依法可以从轻处罚。被告人杨远高、苏敏无犯罪前科，且已退缴大部分违法所得，可酌定从轻处罚。

关于辩护人建议适用缓刑的辩护意见，本院认为，被告人杨远高、苏敏建立运营数个网站为他人违法犯罪活动发布信息，严重扰乱社会公共管理秩序，不宜适用缓刑，本院对相应辩护意见不予采纳。

综上，为了维护公共网络通讯的正常秩序，保障公众的合法权益，惩罚犯罪，判决如下：被告人杨远高犯非法利用信息网络罪，判处有期徒刑九个月，并处罚金人民币二万元；被告人苏敏犯非法利用信息网络罪，判处有期徒刑八个月，并处罚金人民币二万元。

四川资阳徐溧、许晓虹、李强帮助信息网络犯罪活动案

（2019）川2002刑初186号

一、基本案情

四川省资阳市雁江区人民检察院以雁检公检刑诉（2019）1139号起诉书指控被告人徐溧、许晓虹犯非国家工作人员受贿罪、被告人李强、张舒犯对非国家工作人员行贿罪、被告人吴政领、彭跃犯帮助信息网络犯罪活动罪，于2019年5月17日向本院提起公诉。本院审查后于同月20日立案，依法适用简易程序，实行独任审判，公开开庭审理了本案。四川省资阳市雁江区人民检察院指派检察员马晨涛出庭支持公诉。上列被告人及其辩护人到庭参加了诉讼。现已审理终结。

四川省资阳市雁江区人民检察院指控，被告人徐溧、许晓虹、李强为中国电信公司资阳分公司员工，徐溧从事岗位为网络运营部云网维护支撑，许晓虹从事岗位为雁江网络运营分局现场维护，李强从事岗位为政企客户部金融客户经理。

2015年5月至2018年5日，被告人吴政领使用他人身份信息注册zya26826810、zya226115077等多个宽带账号。因需要租赁IP并获取利益，吴政领向李强提出希望其帮助开通IP“多拨”功能。因不具备修改权限，李强向徐溧提出更改连接数要求，并承诺给予好处费，后徐溧利用职务便利为李强提供的账号开通IP“多拨”。吴政领将IP资源租赁给被告人彭跃，彭跃又租赁给“掘金网”工作人员蒋某，蒋某租赁与其他人员使用。2017年，因福建省福州市、河南省安阳市等地发生诈骗案件，警方经侦查锁定诈骗使用IP系吴政领实际使用。警方在侦查过程中，徐溧、李强、吴政领、彭跃明知其违法开通并租赁的IP“多拨”可能被人用于违法犯罪仍然从事上述行为。李强通过徐溧在为吴政领开通的同时，还通过徐溧帮助董某某、李某某、曾某某从事IP资源多拨开通和租赁。通过上述行为，李强共获得违法所得257938元，徐溧获取违法所得85300元，彭跃获取违法所得10680元。

被告人徐溧在为李强提供的账号开通IP资源多拨的同时，还伙同被告人许晓虹为被告人张舒账号提供上述服务。张舒将开通多拨的IP资源租赁给邱某、李某某、王某。通过上述行为，徐溧获取违法所得86838元，许晓虹获取违法所得88627元，张舒获取违法所得136239元。

案发后，被告人吴政领、彭跃、李强、徐溧、张舒先后被警方抓获。2018年7月30日，经民警电话通知，被告人许晓虹主动到案。六名被告人到案后如实供述了犯罪事实。徐溧退缴违法所得172138元、许晓虹退缴违法所得10万元、李强退缴违法所得25万元、张舒退缴违法所得的13万元、彭跃退缴违法所得1万元。

二、诉讼结果

被告人徐溧、许晓虹身为公司、企业人员，利用职权便利为他人谋取利益，收受他人财物，数额较大，其行为已触犯了刑律，构成非国家工作人员受贿罪，且在为张舒谋取利益部分构成共同犯罪。被告人李强、张舒为谋取不正当利益，给予公司、企业人员财物，数额较大，其行为触犯刑律，构成对非国家工作人员行贿罪。被告人吴政领、彭跃明知他人利用信息网络实施犯罪，为其提供技术支持，其行为触犯刑律，构成帮助信息网络犯罪活动罪。

三）案例

# 练某某编造、故意传播虚假信息

（2017）粤0306刑初2760号

一、基本案情

2016年底，被告人练某某入职位于深圳市龙华区大浪街道的深圳市某网络科技有限公司，其工作职责是通过该公司的微信公众号发布贴文吸引粉丝，从而推广销售陈某某的成功学课程演讲会门票。2017年2月9日下午14时许，被告人练某某在西瓜助手（一种APP，专门搜索网络上的文章，上面有显示阅读量）上发现了标题为“今天凌晨，胶济铁路动车相撞，这么大的事故竟然报道伤亡不详，又要掩埋事实吗？转发曝光”的一篇违规文章，因该文章的点击量很高，被告人练某某为了推广其微信号“吸引粉丝，在明知该文章是违规虚假的情况下，通过公司微信公众号编辑发布了该文章。之后，被告人练某某还通过朋友圈和微信群对该文章进行传播。截至2017年2月10日该文章的点击量已超过10万人次。同日，网络民警在网上发现了该虚假信息已对社会秩序造成了不良影响，便通过对发布该信息的账号定位，然后在上述公司内将被告人练某某抓获归案。

二、诉讼结果

被告人练某某无视国家法律，故意编造虚假信息，在信息网络上传播，其行为构成编造、故意传播虚假信息罪，判处拘役五个月。

三、案例剖析

截至2019年，中国裁判文书网中仅收录了四川1份生效裁判案例，全国共计30余起。编造传播虚假信息罪暂无司法解释，适用的行为包括编造虚假信息和故意传播虚假信息。本罪适用的虚假信息仅针对险情、疫情、灾情、警情四种。本罪是结果犯，需要达到严重扰乱社会秩序的严重程度，关于严重扰乱社会秩序的认定，可参见《编造、故意传播恐怖信息案件司法解释》。