网络犯罪法律法规及案例汇编

（2022 年 3 月）

广州市律师协会

普通犯罪刑事法律专业委员会　编制

目 录

第一编 扰乱公共秩序罪范畴之网络犯罪

第三编 观点文章

第一编 扰乱公共秩序罪范畴之网络犯罪

一、《刑法》第六章　妨害社会管理秩序罪　第一节　扰乱公共秩序罪

第二百八十五条　【非法侵入计算机信息系统罪】违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

【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。

【提供侵入、非法控制计算机信息系统程序、工具罪】提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

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。

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。

第二百八十六条之一　【拒不履行信息网络安全管理义务罪】网络服务提供者不履行法律、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，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：

（一）致使违法信息大量传播的；

（二）致使用户信息泄露，造成严重后果的；

（三）致使刑事案件证据灭失，情节严重的；

（四）有其他严重情节的。

单位犯前款罪的，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，依照前款的规定处罚。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

第二百八十七条　【利用计算机实施犯罪的提示性规定】利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

第二百八十七条之一　【非法利用信息网络罪】利用信息网络实施下列行为之一，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：

（一）设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；

（二）发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违

法犯罪信息的；

（三）为实施诈骗等违法犯罪活动发布信息的。

单位犯前款罪的，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。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

第二百八十七条之二　【帮助信息网络犯罪活动罪】明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，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。

单位犯前款罪的，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。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

第二百九十一条之一　【编造、故意传播虚假信息罪】编造虚假的险情、疫情、灾情、警情，在信息网络或者其他媒体上传播，或者明知是上述虚假信息，故意在信息网络或者其他媒体上传播，严重扰乱社会秩序的，处三年以下有期徒刑、拘役或者管制；造成严重后果的，处三年以上七年以下有期徒刑。

第二百九十三条　【寻衅滋事罪】有下列寻衅滋事行为之一，破坏社会秩序的，处五年以下有期徒刑、拘役或者管制：

（一）随意殴打他人，情节恶劣的；

（二）追逐、拦截、辱骂、恐吓他人，情节恶劣的；

（三）强拿硬要或者任意损毁、占用公私财物，情节严重的；

（四）在公共场所起哄闹事，造成公共场所秩序严重混乱的。

纠集他人多次实施前款行为，严重破坏社会秩序的，处五年以上十年以下有期徒刑，可以并处罚金。

第二百九十三条之一　有下列情形之一，催收高利放贷等产生的非法债务，情节严重的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：

（一）使用暴力、胁迫方法的；

（二）限制他人人身自由或者侵入他人住宅的；

（三）恐吓、跟踪、骚扰他人的。

第二百九十四条　【组织、领导、参加黑社会性质组织罪】组织、领导黑社会性质的组织的，处七年以上有期徒刑，并处没收财产；积极参加的，处三年以上七年以下有期徒刑，可以并处罚金或者没收财产；其他参加的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利，可以并处罚金。

黑社会性质的组织应当同时具备以下特征：

（一）形成较稳定的犯罪组织，人数较多，有明确的组织者、领导者，骨干成员基本固定；

（二）有组织地通过违法犯罪活动或者其他手段获取经济利益，具有一定的经济实力，以支持该组织的活动；

（三）以暴力、威胁或者其他手段，有组织地多次进行违法犯罪活动，为非作恶，欺压、残害群众；

（四）通过实施违法犯罪活动，或者利用国家工作人员的包庇或者纵容，称霸一方，在

一定区域或者行业内，形成非法控制或者重大影响，严重破坏经济、社会生活秩序。

第三百零三条　【赌博罪】以营利为目的，聚众赌博或者以赌博为业的，处三年以下有期徒刑、拘役或者管制，并处罚金。

【开设赌场罪】开设赌场的，处五年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处五年以上十年以下有期徒刑，并处罚金。

组织中华人民共和国公民参与国（境）外赌博，数额巨大或者有其他严重情节的，依照前款的规定处罚。

二、相关规定

（一）上述罪名相关规定

1.《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》

（2011 年 6 月 20 日最高人民法院审判委员会第 1524 次会议、2011 年 7 月 11 日最高人民检察院第十一届检察委员会第 63 次会议通过 ）

法释〔2011〕19 号

为依法惩治危害计算机信息系统安全的犯罪活动，根据《中华人民共和国刑法》、《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》的规定，现就办理这类刑事案件应用法律的若干问题解释如下：

第一条　非法获取计算机信息系统数据或者非法控制计算机信息系统，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。

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。

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。

第二条　具有下列情形之一的程序、工具，应当认定为刑法第二百八十五条第三款规定的“专门用于侵入、非法控制计算机信息系统的程序、工具”：

（一）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权获取计算机信息系统数据的功能的；

（二）具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权对计算机信息系统实施控制的功能的；

（三）其他专门设计用于侵入、非法控制计算机信息系统、非法获取计算机信息系统数据的程序、工具。

第三条　提供侵入、非法控制计算机信息系统的程序、工具，具有下列情形之一的，应当认定为刑法第二百八十五条第三款规定的“情节严重”：

（一）提供能够用于非法获取支付结算、证券交易、期货交易等网络金融服务身份认证

信息的专门性程序、工具五人次以上的；

（二）提供第（一）项以外的专门用于侵入、非法控制计算机信息系统的程序、工具二十人次以上的；

（三）明知他人实施非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的违法犯罪行为而为其提供程序、工具五人次以上的；

（四）明知他人实施第（三）项以外的侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具二十人次以上的；

（五）违法所得五千元以上或者造成经济损失一万元以上的；

（六）其他情节严重的情形。

实施前款规定行为，具有下列情形之一的，应当认定为提供侵入、非法控制计算机信息系统的程序、工具“情节特别严重”：

（一）数量或者数额达到前款第（一）项至第（五）项规定标准五倍以上的；

（二）其他情节特别严重的情形。

第四条　破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”：

（一）造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的；

（二）对二十台以上计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加操作的；

（三）违法所得五千元以上或者造成经济损失一万元以上的；

（四）造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

（五）造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

（一）数量或者数额达到前款第（一）项至第（三）项规定标准五倍以上的；

（二）造成为五百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

（三）破坏国家机关或者金融、电信、交通、教育、医疗、能源等领域提供公共服务的计算机信息系统的功能、数据或者应用程序，致使生产、生活受到严重影响或者造成恶劣社会影响的；

（四）造成其他特别严重后果的。

第五条　具有下列情形之一的程序，应当认定为刑法第二百八十六条第三款规定的“计算机病毒等破坏性程序”：

（一）能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的；

（二）能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的；

（三）其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序。

第六条　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，具有下列情形之一的，应当认定为刑法第二百八十六条第三款规定的“后果严重”：

（一）制作、提供、传输第五条第（一）项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播的；

（二）造成二十台以上计算机系统被植入第五条第（二）、（三）项规定的程序的；

（三）提供计算机病毒等破坏性程序十人次以上的；

（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）造成其他严重后果的。

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

（一）制作、提供、传输第五条第（一）项规定的程序，导致该程序通过网络、存储介质、文件等媒介传播，致使生产、生活受到严重影响或者造成恶劣社会影响的；

（二）数量或者数额达到前款第（二）项至第（四）项规定标准五倍以上的；

（三）造成其他特别严重后果的。

第七条　明知是非法获取计算机信息系统数据犯罪所获取的数据、非法控制计算机信息系统犯罪所获取的计算机信息系统控制权，而予以转移、收购、代为销售或者以其他方法掩饰、隐瞒，违法所得五千元以上的，应当依照刑法第三百一十二条第一款的规定，以掩饰、隐瞒犯罪所得罪定罪处罚。

实施前款规定行为，违法所得五万元以上的，应当认定为刑法第三百一十二条第一款规定的“情节严重”。

单位实施第一款规定行为的，定罪量刑标准依照第一款、第二款的规定执行。

第八条　以单位名义或者单位形式实施危害计算机信息系统安全犯罪，达到本解释规定的定罪量刑标准的，应当依照刑法第二百八十五条、第二百八十六条的规定追究直接负责的主管人员和其他直接责任人员的刑事责任。

第九条　明知他人实施刑法第二百八十五条、第二百八十六条规定的行为，具有下列情形之一的，应当认定为共同犯罪，依照刑法第二百八十五条、第二百八十六条的规定处罚：

（一）为其提供用于破坏计算机信息系统功能、数据或者应用程序的程序、工具，违法所得五千元以上或者提供十人次以上的；

（二）为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、费用结算、交易服务、广告服务、技术培训、技术支持等帮助，违法所得五千元以上的；

（三）通过委托推广软件、投放广告等方式向其提供资金五千元以上的。

实施前款规定行为，数量或者数额达到前款规定标准五倍以上的，应当认定为刑法第二百八十五条、第二百八十六条规定的“情节特别严重”或者“后果特别严重”。

第十条　对于是否属于刑法第二百八十五条、第二百八十六条规定的“国家事务、国防建设、尖端科学技术领域的计算机信息系统”、“专门用于侵入、非法控制计算机信息系统的程序、工具”、“计算机病毒等破坏性程序”难以确定的，应当委托省级以上负责计算机信息系统安全保护管理工作的部门检验。司法机关根据检验结论，并结合案件具体情况认定。

第十一条　本解释所称“计算机信息系统”和“计算机系统”，是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。

本解释所称“身份认证信息”，是指用于确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书等。

本解释所称“经济损失”，包括危害计算机信息系统犯罪行为给用户直接造成的经济损失，以及用户为恢复数据、功能而支出的必要费用。

2. 《最高人民法院　最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》

（2019 年 6 月 3 日最高人民法院审判委员会第 1771 次会议、2019 年 9 月 4 日最高人民检察院第十三届检察委员会第二十三次会议通过，自 2019 年 11 月 1 日起施行）

为依法惩治拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活

动等犯罪，维护正常网络秩序，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》的规定，现就办理此类刑事案件适用法律的若干问题解释如下：

第一条　提供下列服务的单位和个人，应当认定为刑法第二百八十六条之一第一款规定的“网络服务提供者”：

（一）网络接入、域名注册解析等信息网络接入、计算、存储、传输服务；

（二）信息发布、搜索引擎、即时通讯、网络支付、网络预约、网络购物、网络游戏、网络直播、网站建设、安全防护、广告推广、应用商店等信息网络应用服务；

（三）利用信息网络提供的电子政务、通信、能源、交通、水利、金融、教育、医疗等公共服务。

第二条　刑法第二百八十六条之一第一款规定的“监管部门责令采取改正措施”，是指网信、电信、公安等依照法律、行政法规的规定承担信息网络安全监管职责的部门，以责令整改通知书或者其他文书形式，责令网络服务提供者采取改正措施。

认定“经监管部门责令采取改正措施而拒不改正”，应当综合考虑监管部门责令改正是否具有法律、行政法规依据，改正措施及期限要求是否明确、合理，网络服务提供者是否具有按照要求采取改正措施的能力等因素进行判断。

第三条　拒不履行信息网络安全管理义务，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第一项规定的“致使违法信息大量传播”：

（一）致使传播违法视频文件二百个以上的；

（二）致使传播违法视频文件以外的其他违法信息二千个以上的；

（三）致使传播违法信息，数量虽未达到第一项、第二项规定标准，但是按相应比例折算合计达到有关数量标准的；

（四）致使向二千个以上用户账号传播违法信息的；

（五）致使利用群组成员账号数累计三千以上的通讯群组或者关注人员账号数累计三万以上的社交网络传播违法信息的；

（六）致使违法信息实际被点击数达到五万以上的；

（七）其他致使违法信息大量传播的情形。

第四条　拒不履行信息网络安全管理义务，致使用户信息泄露，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第二项规定的“造成严重后果”：

（一）致使泄露行踪轨迹信息、通信内容、征信信息、财产信息五百条以上的；

（二）致使泄露住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的用户信息五千条以上的；

（三）致使泄露第一项、第二项规定以外的用户信息五万条以上的；

（四）数量虽未达到第一项至第三项规定标准，但是按相应比例折算合计达到有关数量标准的；

（五）造成他人死亡、重伤、精神失常或者被绑架等严重后果的；

（六）造成重大经济损失的；

（七）严重扰乱社会秩序的；

（八）造成其他严重后果的。

第五条　拒不履行信息网络安全管理义务，致使影响定罪量刑的刑事案件证据灭失，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第三项规定的“情节严重”：

（一）造成危害国家安全犯罪、恐怖活动犯罪、黑社会性质组织犯罪、贪污贿赂犯罪案件的证据灭失的；

（二）造成可能判处五年有期徒刑以上刑罚犯罪案件的证据灭失的；

（三）多次造成刑事案件证据灭失的；

（四）致使刑事诉讼程序受到严重影响的；

（五）其他情节严重的情形。

第六条　拒不履行信息网络安全管理义务，具有下列情形之一的，应当认定为刑法第二百八十六条之一第一款第四项规定的“有其他严重情节”：

（一）对绝大多数用户日志未留存或者未落实真实身份信息认证义务的；

（二）二年内经多次责令改正拒不改正的；

（三）致使信息网络服务被主要用于违法犯罪的；

（四）致使信息网络服务、网络设施被用于实施网络攻击，严重影响生产、生活的；

（五）致使信息网络服务被用于实施危害国家安全犯罪、恐怖活动犯罪、黑社会性质组织犯罪、贪污贿赂犯罪或者其他重大犯罪的；

（六）致使国家机关或者通信、能源、交通、水利、金融、教育、医疗等领域提供公共服务的信息网络受到破坏，严重影响生产、生活的；

（七）其他严重违反信息网络安全管理义务的情形。

第七条　刑法第二百八十七条之一规定的“违法犯罪”，包括犯罪行为和属于刑法分则规定的行为类型但尚未构成犯罪的违法行为。

第八条　以实施违法犯罪活动为目的而设立或者设立后主要用于实施违法犯罪活动的网站、通讯群组，应当认定为刑法第二百八十七条之一第一款第一项规定的“用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组”。

第九条　利用信息网络提供信息的链接、截屏、二维码、访问账号密码及其他指引访问服务的，应当认定为刑法第二百八十七条之一第一款第二项、第三项规定的“发布信息”。

第十条　非法利用信息网络，具有下列情形之一的，应当认定为刑法第二百八十七条之一第一款规定的“情节严重”：

（一）假冒国家机关、金融机构名义，设立用于实施违法犯罪活动的网站的；

（二）设立用于实施违法犯罪活动的网站，数量达到三个以上或者注册账号数累计达到二千以上的；

（三）设立用于实施违法犯罪活动的通讯群组，数量达到五个以上或者群组成员账号数累计达到一千以上的；

（四）发布有关违法犯罪的信息或者为实施违法犯罪活动发布信息，具有下列情形之一的：

1.在网站上发布有关信息一百条以上的；

2.向二千个以上用户账号发送有关信息的；

3.向群组成员数累计达到三千以上的通讯群组发送有关信息的；

4.利用关注人员账号数累计达到三万以上的社交网络传播有关信息的；

（五）违法所得一万元以上的；

（六）二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又非法利用信息网络的；

（七）其他情节严重的情形。

第十一条　为他人实施犯罪提供技术支持或者帮助，具有下列情形之一的，可以认定行为人明知他人利用信息网络实施犯罪，但是有相反证据的除外：

（一）经监管部门告知后仍然实施有关行为的；

（二）接到举报后不履行法定管理职责的；

（三）交易价格或者方式明显异常的；

（四）提供专门用于违法犯罪的程序、工具或者其他技术支持、帮助的；

（五）频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份，逃避监管或

者规避调查的；

（六）为他人逃避监管或者规避调查提供技术支持、帮助的；

（七）其他足以认定行为人明知的情形。

第十二条　明知他人利用信息网络实施犯罪，为其犯罪提供帮助，具有下列情形之一的，应当认定为刑法第二百八十七条之二第一款规定的“情节严重”：

（一）为三个以上对象提供帮助的；

（二）支付结算金额二十万元以上的；

（三）以投放广告等方式提供资金五万元以上的；

（四）违法所得一万元以上的；

（五）二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又帮助信息网络犯罪活动的；

（六）被帮助对象实施的犯罪造成严重后果的；

（七）其他情节严重的情形。

实施前款规定的行为，确因客观条件限制无法查证被帮助对象是否达到犯罪的程度，但相关数额总计达到前款第二项至第四项规定标准五倍以上，或者造成特别严重后果的，应当以帮助信息网络犯罪活动罪追究行为人的刑事责任。

第十三条　被帮助对象实施的犯罪行为可以确认，但尚未到案、尚未依法裁判或者因未达到刑事责任年龄等原因依法未予追究刑事责任的，不影响帮助信息网络犯罪活动罪的认定。

第十四条　单位实施本解释规定的犯罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

第十五条　综合考虑社会危害程度、认罪悔罪态度等情节，认为犯罪情节轻微的，可以不起诉或者免予刑事处罚；情节显著轻微危害不大的，不以犯罪论处。

第十六条　多次拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动构成犯罪，依法应当追诉的，或者二年内多次实施前述行为未经处理的，数量或者数额累计计算。

第十七条　对于实施本解释规定的犯罪被判处刑罚的，可以根据犯罪情况和预防再犯罪的需要，依法宣告职业禁止；被判处管制、宣告缓刑的，可以根据犯罪情况，依法宣告禁止令。

第十八条　对于实施本解释规定的犯罪的，应当综合考虑犯罪的危害程度、违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金。

第十九条　本解释自 2019 年 11 月 1 日起施行。

3. 《最高人民法院、最高人民检察院、公安部关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》

（公通字〔2014〕10 号 2014 年 5 月 4 日）

各省、自治区、直辖市高级人民法院，人民检察院，公安厅、局，新疆维吾尔自治区高级人民法院生产建设兵团分院，新疆生产建设兵团人民检察院、公安局：

为解决近年来公安机关、人民检察院、人民法院在办理网络犯罪案件中遇到的新情况、新问题，依法惩治网络犯罪活动，根据《中华人民共和国刑法》、《中华人民共和国刑事诉讼法》及有关司法解释的规定，结合侦查、起诉、审判实践，现就办理网络犯罪案件适用刑事诉讼程序问题提出以下意见：

一、关于网络犯罪案件的范围

1、本意见所称网络犯罪案件包括：

（1）危害计算机信息系统安全犯罪案件；

（2）通过危害计算机信息系统安全实施的盗窃、诈骗、敲诈勒索等犯罪案件；

（3）在网络上发布信息或者设立主要用于实施犯罪活动的网站、通讯群组，针对或者组织、教唆、帮助不特定多数人实施的犯罪案件；

（4）主要犯罪行为在网络上实施的其他案件。

二、关于网络犯罪案件的管辖

2、网络犯罪案件由犯罪地公安机关立案侦查。必要时，可以由犯罪嫌疑人居住地公安机关立案侦查。

网络犯罪案件的犯罪地包括用于实施犯罪行为的网站服务器所在地，网络接入地，网站建立者、管理者所在地，被侵害的计算机信息系统或其管理者所在地，犯罪嫌疑人、被害人使用的计算机信息系统所在地，被害人被侵害时所在地，以及被害人财产遭受损失地等。

涉及多个环节的网络犯罪案件，犯罪嫌疑人为网络犯罪提供帮助的，其犯罪地或者居住地公安机关可以立案侦查。

3、有多个犯罪地的网络犯罪案件，由最初受理的公安机关或者主要犯罪地公安机关立案侦查。有争议的，按照有利于查清犯罪事实、有利于诉讼的原则，由共同上级公安机关指定有关公安机关立案侦查。需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的人民检察院、人民法院受理。

4、具有下列情形之一的，有关公安机关可以在其职责范围内并案侦查，需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的人民检察院、人民法院受理：

（1）一人犯数罪的；

（2）共同犯罪的；

（3）共同犯罪的犯罪嫌疑人、被告人还实施其他犯罪的；

（4）多个犯罪嫌疑人、被告人实施的犯罪存在关联，并案处理有利于查明案件事实的。

5、对因网络交易、技术支持、资金支付结算等关系形成多层级链条、跨区域的网络犯罪案件，共同上级公安机关可以按照有利于查清犯罪事实、有利于诉讼的原则，指定有关公安机关一并立案侦查，需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的人民检察院、人民法院受理。

6、具有特殊情况，由异地公安机关立案侦查更有利于查清犯罪事实、保证案件公正处理的跨省（自治区、直辖市）重大网络犯罪案件，可以由公安部商最高人民检察院和最高人民法院指定管辖。

7、人民检察院对于公安机关移送审查起诉的网络犯罪案件，发现犯罪嫌疑人还有犯罪被其他公安机关立案侦查的，应当通知移送审查起诉的公安机关。

人民法院受理案件后，发现被告人还有犯罪被其他公安机关立案侦查的，可以建议人民检察院补充侦查。人民检察院经审查，认为需要补充侦查的，应当通知移送审查起诉的公安机关。

经人民检察院通知，有关公安机关根据案件具体情况，可以对犯罪嫌疑人所犯其他犯罪并案侦查。

8、为保证及时结案，避免超期羁押，人民检察院对于公安机关提请批准逮捕、移送审查起诉的网络犯罪案件，第一审人民法院对于已经受理的网络犯罪案件，经审查发现没有管辖权的，可以依法报请共同上级人民检察院、人民法院指定管辖。

9、部分犯罪嫌疑人在逃，但不影响对已到案共同犯罪嫌疑人、被告人的犯罪事实认定的网络犯罪案件，可以依法先行追究已到案共同犯罪嫌疑人、被告人的刑事责任。在逃的共同犯罪嫌疑人、被告人归案后，可以由原公安机关、人民检察院、人民法院管辖其所涉及的案件。

三、关于网络犯罪案件的初查

10、对接受的案件或者发现的犯罪线索，在审查中发现案件事实或者线索不明，需要经过调查才能够确认是否达到犯罪追诉标准的，经办案部门负责人批准，可以进行初查。

初查过程中，可以采取询问、查询、勘验、检查、鉴定、调取证据材料等不限制初查对象人身、财产权利的措施，但不得对初查对象采取强制措施和查封、扣押、冻结财产。

四、关于网络犯罪案件的跨地域取证

11、公安机关跨地域调查取证的，可以将办案协作函和相关法律文书及凭证电传或者通过公安机关信息化系统传输至协作地公安机关。协作地公安机关经审查确认，在传来的法律文书上加盖本地公安机关印章后，可以代为调查取证。

12、询（讯）问异地证人、被害人以及与案件有关联的犯罪嫌疑人的，可以由办案地公安机关通过远程网络视频等方式进行询（讯）问并制作笔录。

远程询（讯）问的，应当由协作地公安机关事先核实被询（讯）问人的身份。办案地公安机关应当将询（讯）问笔录传输至协作地公安机关。询（讯）问笔录经被询（讯）问人确认并逐页签名、捺指印后，由协作地公安机关协作人员签名或者盖章，并将原件提供给办案地公安机关。询（讯）问人员收到笔录后，应当在首页右上方写明“于某年某月某日收到”，并签名或者盖章。

远程询（讯）问的，应当对询（讯）问过程进行录音录像，并随案移送。

异地证人、被害人以及与案件有关联的犯罪嫌疑人亲笔书写证词、供词的，参照本条第二款规定执行。

五、关于电子数据的取证与审查

13、收集、提取电子数据，应当由二名以上具备相关专业知识的侦查人员进行。取证设备和过程应当符合相关技术标准，并保证所收集、提取的电子数据的完整性、客观性。

14、收集、提取电子数据，能够获取原始存储介质的，应当封存原始存储介质，并制作笔录，记录原始存储介质的封存状态，由侦查人员、原始存储介质持有人签名或者盖章；持有人无法签名或者拒绝签名的，应当在笔录中注明，由见证人签名或者盖章。有条件的，侦查人员应当对相关活动进行录像。

15、具有下列情形之一，无法获取原始存储介质的，可以提取电子数据，但应当在笔录中注明不能获取原始存储介质的原因、原始存储介质的存放地点等情况，并由侦查人员、电子数据持有人、提供人签名或者盖章；持有人、提供人无法签名或者拒绝签名的，应当在笔录中注明，由见证人签名或者盖章；有条件的，侦查人员应当对相关活动进行录像：

（1）原始存储介质不便封存的；

（2）提取计算机内存存储的数据、网络传输的数据等不是存储在存储介质上的电子数据的；

（3）原始存储介质位于境外的；

（4）其他无法获取原始存储介质的情形。

16、收集、提取电子数据应当制作笔录，记录案由、对象、内容，收集、提取电子数据的时间、地点、方法、过程，电子数据的清单、规格、类别、文件格式、完整性校验值等，并由收集、提取电子数据的侦查人员签名或者盖章。远程提取电子数据的，应当说明原因，有条件的，应当对相关活动进行录像。通过数据恢复、破解等方式获取被删除、隐藏或者加密的电子数据的，应当对恢复、破解过程和方法作出说明。

17、收集、提取的原始存储介质或者电子数据，应当以封存状态随案移送，并制作电子数据的复制件一并移送。

对文档、图片、网页等可以直接展示的电子数据，可以不随案移送电子数据打印件，但应当附有展示方法说明和展示工具；人民法院、人民检察院因设备等条件限制无法直接展示

电子数据的，公安机关应当随案移送打印件。

对侵入、非法控制计算机信息系统的程序、工具以及计算机病毒等无法直接展示的电子数据，应当附有电子数据属性、功能等情况的说明。

对数据统计数量、数据同一性等问题，公安机关应当出具说明。

18、对电子数据涉及的专门性问题难以确定的，由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具检验报告。

六、关于网络犯罪案件的其他问题

19、采取技术侦查措施收集的材料作为证据使用的，应当随案移送批准采取技术侦查措施的法律文书和所收集的证据材料。使用有关证据材料可能危及有关人员的人身安全，或者可能产生其他严重后果的，应当采取不暴露有关人员身份、技术方法等保护措施，必要时，可以由审判人员在庭外进行核实。

20、对针对或者组织、教唆、帮助不特定多数人实施的网络犯罪案件，确因客观条件限制无法逐一收集相关言词证据的，可以根据记录被害人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实的电子数据、书证等证据材料，在慎重审查被告人及其辩护人所提辩解、辩护意见的基础上，综合全案证据材料，对相关犯罪事实作出认定。

4.《最高人民法院关于审理危害军事通信刑事案件具体应用法律若干问题的解释》

第六条第三款，违反国家规定，侵入国防建设、尖端科学技术领域的军事通信计算机信息系统，尚未对军事通信造成破坏的，依照刑法第二百八十五条的规定定罪处罚；对军事通信造成破坏，同时构成刑法第二百八十五条、第二百八十六条、第三百六十九条第一款规定的犯罪的，依照处罚较重的规定定罪处罚。

5.《公安部关于对破坏未联网的微型计算机信息系统是否适用《刑法》第２８６条的请示的批复》（１９９８年１１月２５日　公复字〔１９９８〕７号）

吉林省公安厅：

你厅《关于“破坏未联网计算机财务系统程序和数据的行为是否适用〈刑法〉第２８６条故意破坏计算机信息系统数据应有程序罪”的请示》收悉，现批复如下：

《刑法》第２８６条中的“违反国家规定”是指包括《中华人民共和国计算机信息系统安全保护条例》（以下简称《条例》）在内的有关行政法规、部门规章的规定。《条例》第５条第２款规定的“未联网的微型计算机的安全保护办法，另行规定”，主要是考虑到未联入网络的单台微型计算机系统所处环境和使用情况比较复杂，且基本无安全功能，需针对这些特点另外制定相应的安全管理措施。然而，未联网的计算机信息系统也属计算机信息系统，《条例》第２、３、７条的安全保护原则、规定，对未联网的微型计算机系统完全适用。因此破坏未联网的微型计算机信息系统适用《刑法》第２８６条。

此复。

6.《最高人民法院、最高人民检察院关于办理环境污染刑事案件适用法律若干问题的解释》

第十条　违反国家规定，针对环境质量监测系统实施下列行为，或者强令、指使、授意他人实施下列行为的，应当依照刑法第二百八十六条的规定，以破坏计算机信息系统罪论处：

（一）修改参数或者监测数据的；

（二）干扰采样，致使监测数据严重失真的；

（三）其他破坏环境质量监测系统的行为。

重点排污单位篡改、伪造自动监测数据或者干扰自动监测设施，排放化学需氧量、氨氮、二氧化硫、氮氧化物等污染物，同时构成污染环境罪和破坏计算机信息系统罪的，依照处罚

较重的规定定罪处罚。

从事环境监测设施维护、运营的人员实施或者参与实施篡改、伪造自动监测数据、干扰自动监测设施、破坏环境质量监测系统等行为的，应当从重处罚。

7.《最高人民法院关于审理毒品犯罪案件适用法律若干问题的解释》

第十四条　利用信息网络，设立用于实施传授制造毒品、非法生产制毒物品的方法，贩卖毒品，非法买卖制毒物品或者组织他人吸食、注射毒品等违法犯罪活动的网站、通讯群组，或者发布实施前述违法犯罪活动的信息，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚。

实施刑法第二百八十七条之一、第二百八十七条之二规定的行为，同时构成贩卖毒品罪、非法买卖制毒物品罪、传授犯罪方法罪等犯罪的，依照处罚较重的规定定罪处罚。

8.《最高人民法院、最高人民检察院关于办理组织、强迫、引诱、容留、介绍卖淫刑事案件适用法律若干问题的解释》

第八条第二款 利用信息网络发布招嫖违法信息，情节严重的，依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚。同时构成介绍卖淫罪的，依照处罚较重的规定定罪处罚。

9.《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》

第八条 设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。

第九条 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。

10.《最高人民法院、最高人民检察院、公安部、司法部关于依法惩治妨害新型冠状病毒感染肺炎疫情防控违法犯罪的意见》

（六）依法严惩造谣传谣犯罪。编造虚假的疫情信息，在信息网络或者其他媒体上传播，或者明知是虚假疫情信息，故意在信息网络或者其他媒体上传播，严重扰乱社会秩序的，依照刑法第二百九十一条之一第二款的规定，以编造、故意传播虚假信息罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第四项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第四项的规定，以寻衅滋事罪定罪处罚。

利用新型冠状病毒感染肺炎疫情，制造、传播谣言，煽动分裂国家、破坏国家统一，或者煽动颠覆国家政权、推翻社会主义制度的，依照刑法第一百零三条第二款、第一百零五条第二款的规定，以煽动分裂国家罪或者煽动颠覆国家政权罪定罪处罚。

网络服务提供者不履行法律、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，致使虚假疫情信息或者其他违法信息大量传播的，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。

11.《最高人民法院、最高人民检察院、公安部、司法部关于办理利用信息网络实施黑恶势力犯罪刑事案件若干问题的意见》

为认真贯彻中央关于开展扫黑除恶专项斗争的部署要求，正确理解和适用最高人民法院、最高人民检察院、公安部、司法部《关于办理黑恶势力犯罪案件若干问题的指导意见》（法发〔2018〕1号，以下简称《指导意见》），根据刑法、刑事诉讼法、网络安全法及有关司法解释、规范性文件的规定，现对办理利用信息网络实施黑恶势力犯罪案件若干问题提出以下意见：

一、总体要求

1. 各级人民法院、人民检察院、公安机关及司法行政机关应当统一执法思想、提高执法效能，坚持“打早打小”，坚决依法严厉惩处利用信息网络实施的黑恶势力犯罪，有效维护网络安全和经济、社会生活秩序。

2. 各级人民法院、人民检察院、公安机关及司法行政机关应当正确运用法律，严格依法办案，坚持“打准打实”，认真贯彻落实宽严相济刑事政策，切实做到宽严有据、罚当其罪，实现政治效果、法律效果和社会效果的统一。

3. 各级人民法院、人民检察院、公安机关及司法行政机关应当分工负责，互相配合、互相制约，切实加强与相关行政管理部门的协作，健全完善风险防控机制，积极营造线上线下社会综合治理新格局。

二、依法严惩利用信息网络实施的黑恶势力犯罪

4. 对通过发布、删除负面或虚假信息，发送侮辱性信息、图片，以及利用信息、电话骚扰等方式，威胁、要挟、恐吓、滋扰他人，实施黑恶势力违法犯罪的，应当准确认定，依法严惩。

5. 利用信息网络威胁他人，强迫交易，情节严重的，依照刑法第二百二十六条的规定，以强迫交易罪定罪处罚。

6. 利用信息网络威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

7. 利用信息网络辱骂、恐吓他人，情节恶劣，破坏社会秩序的，依照刑法第二百九十三条第一款第二项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第四项的规定，以寻衅滋事罪定罪处罚。

8. 侦办利用信息网络实施的强迫交易、敲诈勒索等非法敛财类案件，确因被害人人数众多等客观条件的限制，无法逐一收集被害人陈述的，可以结合已收集的被害人陈述，以及经查证属实的银行账户交易记录、第三方支付结算账户交易记录、通话记录、电子数据等证据，综合认定被害人人数以及涉案资金数额等。

三、准确认定利用信息网络实施犯罪的黑恶势力

9. 利用信息网络实施违法犯罪活动，符合刑法、《指导意见》以及最高人民法院、最高人民检察院、公安部、司法部《关于办理恶势力刑事案件若干问题的意见》等规定的恶势力、恶势力犯罪集团、黑社会性质组织特征和认定标准的，应当依法认定为恶势力、恶势力犯罪集团、黑社会性质组织。

认定利用信息网络实施违法犯罪活动的黑社会性质组织时，应当依照刑法第二百九十四条第五款规定的“四个特征”进行综合审查判断，分析“四个特征”相互间的内在联系，根据在网络空间和现实社会中实施违法犯罪活动对公民人身、财产、民主权利和经济、社会生活秩序所造成的危害，准确评价，依法予以认定。

10. 认定利用信息网络实施违法犯罪的黑恶势力组织特征，要从违法犯罪的起因、目的，以及组织、策划、指挥、参与人员是否相对固定，组织形成后是否持续进行犯罪活动、是否有明确的职责分工、行为规范、利益分配机制等方面综合判断。利用信息网络实施违法犯罪的黑恶势力组织成员之间一般通过即时通讯工具、通讯群组、电子邮件、网盘等信息网络方式联络，对部分组织成员通过信息网络方式联络实施黑恶势力违法犯罪活动，即使相互未见面、彼此不熟识，不影响对组织特征的认定。

11. 利用信息网络有组织地通过实施违法犯罪活动或者其他手段获取一定数量的经济利益，用于违法犯罪活动或者支持该组织生存、发展的，应当认定为符合刑法第二百九十四条第五款第二项规定的黑社会性质组织经济特征。

12. 通过线上线下相结合的方式，有组织地多次利用信息网络实施违法犯罪活动，侵犯不特定多人的人身权利、民主权利、财产权利，破坏经济秩序、社会秩序的，应当认定为符合刑法第二百九十四条第五款第三项规定的黑社会性质组织行为特征。单纯通过线上方式实施的违法犯罪活动，且不具有为非作恶、欺压残害群众特征的，一般不应作为黑社会性质组织行为特征的认定依据。

13. 对利用信息网络实施黑恶势力犯罪非法控制和影响的“一定区域或者行业”，应当结合危害行为发生地或者危害行业的相对集中程度，以及犯罪嫌疑人、被告人在网络空间和现实社会中的控制和影响程度综合判断。虽然危害行为发生地、危害的行业比较分散，但涉案犯罪组织利用信息网络多次实施强迫交易、寻衅滋事、敲诈勒索等违法犯罪活动，在网络空间和现实社会造成重大影响，严重破坏经济、社会生活秩序的，应当认定为“在一定区域或者行业内，形成非法控制或者重大影响”。

四、利用信息网络实施黑恶势力犯罪案件管辖

14. 利用信息网络实施的黑恶势力犯罪案件管辖依照《关于办理黑社会性质组织犯罪案件若干问题的规定》和《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》的有关规定确定，坚持以犯罪地管辖为主、被告人居住地管辖为辅的原则。

15. 公安机关可以依法对利用信息网络实施的黑恶势力犯罪相关案件并案侦查或者指定下级公安机关管辖，并案侦查或者由上级公安机关指定管辖的公安机关应当全面调查收集能够证明黑恶势力犯罪事实的证据，各涉案地公安机关应当积极配合。并案侦查或者由上级公安机关指定管辖的案件，需要提请批准逮捕、移送审查起诉、提起公诉的，由立案侦查的公安机关所在地的人民检察院、人民法院受理。

16. 人民检察院对于公安机关提请批准逮捕、移送审查起诉的利用信息网络实施的黑恶势力犯罪案件，人民法院对于已进入审判程序的利用信息网络实施的黑恶势力犯罪案件，被告人及其辩护人提出的管辖异议成立，或者办案单位发现没有管辖权的，受案人民检察院、人民法院经审查，可以依法报请与有管辖权的人民检察院、人民法院共同的上级人民检察院、人民法院指定管辖，不再自行移交。对于在审查批准逮捕阶段，上级检察机关已经指定管辖的案件，审查起诉工作由同一人民检察院受理。人民检察院、人民法院认为应当分案起诉、审理的，可以依法分案处理。

17. 公安机关指定下级公安机关办理利用信息网络实施的黑恶势力犯罪案件的，应当同时抄送同级人民检察院、人民法院。人民检察院认为需要依法指定审判管辖的，应当协商同级人民法院办理指定管辖有关事宜。

12.《最高人民法院、最高人民检察院关于办理赌博刑事案件具体应用法律若干问题的解释》法释[2005]3 号

为依法惩治赌博犯罪活动，根据刑法的有关规定，现就办理赌博刑事案件具体应用法律的若干问题解释如下：

第一条　以营利为目的，有下列情形之一的，属于刑法第三百零三条规定的“聚众赌博”：

（一）组织 3 人以上赌博，抽头渔利数额累计达到 5000 元以上的；

（二）组织 3 人以上赌博，赌资数额累计达到 5 万元以上的；

（三）组织 3 人以上赌博，参赌人数累计达到 20 人以上的；

（四）组织中华人民共和国公民 10 人以上赴境外赌博，从中收取回扣、介绍费的。

第二条　以营利为目的，在计算机网络上建立赌博网站，或者为赌博网站担任代理，接受投注的，属于刑法第三百零三条规定的“开设赌场”。释义引用统计

第三条　中华人民共和国公民在我国领域外周边地区聚众赌博、开设赌场，以吸引中华人民共和国公民为主要客源，构成赌博罪的，可以依照刑法规定追究刑事责任。释义引用统计

第四条　明知他人实施赌博犯罪活动，而为其提供资金、计算机网络、通讯、费用结算等直接帮助的，以赌博罪的共犯论处。释义引用统计

第五条　实施赌博犯罪，有下列情形之一的，依照刑法第三百零三条的规定从重处罚：

（一）具有国家工作人员身份的；

（二）组织国家工作人员赴境外赌博的；

（三）组织未成年人参与赌博，或者开设赌场吸引未成年人参与赌博的。

第六条　未经国家批准擅自发行、销售彩票，构成犯罪的，依照刑法第二百二十五条第（四）项的规定，以非法经营罪定罪处罚。释义引用统计

第七条　通过赌博或者为国家工作人员赌博提供资金的形式实施行贿、受贿行为，构成犯罪的，依照刑法关于贿赂犯罪的规定定罪处罚。释义引用统计

第八条　赌博犯罪中用作赌注的款物、换取筹码的款物和通过赌博赢取的款物属于赌资。通过计算机网络实施赌博犯罪的，赌资数额可以按照在计算机网络上投注或者赢取的点数乘以每一点实际代表的金额认定。

赌资应当依法予以追缴；赌博用具、赌博违法所得以及赌博犯罪分子所有的专门用于赌博的资金、交通工具、通讯工具等，应当依法予以没收。释义引用统计

第九条　不以营利为目的，进行带有少量财物输赢的娱乐活动，以及提供棋牌室等娱乐场所只收取正常的场所和服务费用的经营行为等，不以赌博论处。

13.《最高人民法院、最高人民检察院、公安部关于办理网络赌博犯罪案件适用法律若干问题的意见》

（公通字[2010]40 号）

各省、自治区、直辖市高级人民法院、人民检察院、公安厅、局，新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局：

为依法惩治网络赌博犯罪活动，根据《中华人民共和国刑法》、《中华人民共和国刑事诉讼法》和最高人民法院、最高人民检察院《关于办理赌博刑事案件具体应用法律若干问题的解释》等有关规定，结合司法实践，现就办理网络赌博犯罪案件适用法律的若干问题，提出如下意见：

一、关于网上开设赌场犯罪的定罪量刑标准

利用互联网、移动通讯终端等传输赌博视频、数据，组织赌博活动，具有下列情形之一的，属于刑法第三百零三条第二款规定的“开设赌场”行为：

（一）建立赌博网站并接受投注的；

（二）建立赌博网站并提供给他人组织赌博的；

（三）为赌博网站担任代理并接受投注的；

（四）参与赌博网站利润分成的。

实施前款规定的行为，具有下列情形之一的，应当认定为刑法第三百零三条第二款规定的“情节严重”：

（一）抽头渔利数额累计达到 3 万元以上的；

（二）赌资数额累计达到 30 万元以上的；

（三）参赌人数累计达到 120 人以上的；

（四）建立赌博网站后通过提供给他人组织赌博，违法所得数额在 3 万元以上的；

（五）参与赌博网站利润分成，违法所得数额在 3 万元以上的；

（六）为赌博网站招募下级代理，由下级代理接受投注的；

（七）招揽未成年人参与网络赌博的；

（八）其他情节严重的情形。

二、关于网上开设赌场共同犯罪的认定和处罚

明知是赌博网站，而为其提供下列服务或者帮助的，属于开设赌场罪的共同犯罪，依照刑法第三百零三条第二款的规定处罚：

（一）为赌博网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道、投放广告、发展会员、软件开发、技术支持等服务，收取服务费数额在 2 万元以上的；

（二）为赌博网站提供资金支付结算服务，收取服务费数额在 1 万元以上或者帮助收取赌资 20 万元以上的；

（三）为 10 个以上赌博网站投放与网址、赔率等信息有关的广告或者为赌博网站投放广告累计 100 条以上的。

实施前款规定的行为，数量或者数额达到前款规定标准 5 倍以上的，应当认定为刑法第三百零三条第二款规定的“情节严重”。

实施本条第一款规定的行为，具有下列情形之一的，应当认定行为人“明知”，但是有证据证明确实不知道的除外：

（一）收到行政主管机关书面等方式的告知后，仍然实施上述行为的；

（二）为赌博网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道、投放广告、软件开发、技术支持、资金支付结算等服务，收取服务费明显异常的；

（三）在执法人员调查时，通过销毁、修改数据、账本等方式故意规避调查或者向犯罪嫌疑人通风报信的；

（四）其他有证据证明行为人明知的。

如果有开设赌场的犯罪嫌疑人尚未到案，但是不影响对已到案共同犯罪嫌疑人、被告人的犯罪事实认定的，可以依法对已到案者定罪处罚。

三、关于网络赌博犯罪的参赌人数、赌资数额和网站代理的认定

赌博网站的会员账号数可以认定为参赌人数，如果查实一个账号多人使用或者多个账号一人使用的，应当按照实际使用的人数计算参赌人数。

赌资数额可以按照在网络上投注或者赢取的点数乘以每一点实际代表的金额认定。

对于将资金直接或间接兑换为虚拟货币、游戏道具等虚拟物品，并用其作为筹码投注的，赌资数额按照购买该虚拟物品所需资金数额或者实际支付资金数额认定。

对于开设赌场犯罪中用于接收、流转赌资的银行账户内的资金，犯罪嫌疑人、被告人不能说明合法来源的，可以认定为赌资。向该银行账户转入、转出资金的银行账户数量可以认定为参赌人数。如果查实一个账户多人使用或多个账户一人使用的，应当按照实际使用的人数计算参赌人数。

有证据证明犯罪嫌疑人在赌博网站上的账号设置有下级账号的，应当认定其为赌博网站的代理。

四、关于网络赌博犯罪案件的管辖

网络赌博犯罪案件的地域管辖，应当坚持以犯罪地管辖为主、被告人居住地管辖为辅的原则。“犯罪地”包括赌博网站服务器所在地、网络接入地，赌博网站建立者、管理者所在地，以及赌博网站代理人、参赌人实施网络赌博行为地等。

公安机关对侦办跨区域网络赌博犯罪案件的管辖权有争议的，应本着有利于查清犯罪事实、有利于诉讼的原则，认真协商解决。经协商无法达成一致的，报共同的上级公安机关指定管辖。对即将侦查终结的跨省（自治区、直辖市）重大网络赌博案件，必要时可由公安部商最高人民法院和最高人民检察院指定管辖。

为保证及时结案，避免超期羁押，人民检察院对于公安机关提请审查逮捕、移送审查起诉的案件，人民法院对于已进入审判程序的案件，犯罪嫌疑人、被告人及其辩护人提出管辖异议或者办案单位发现没有管辖权的，受案人民检察院、人民法院经审查可以依法报请上级人民检察院、人民法院指定管辖，不再自行移送有管辖权的人民检察院、人民法院。

五、关于电子证据的收集与保全

侦查机关对于能够证明赌博犯罪案件真实情况的网站页面、上网记录、电子邮件、电子合同、电子交易记录、电子账册等电子数据，应当作为刑事证据予以提取、复制、固定。

侦查人员应当对提取、复制、固定电子数据的过程制作相关文字说明，记录案由、对象、内容以及提取、复制、固定的时间、地点、方法，电子数据的规格、类别、文件格式等，并由提取、复制、固定电子数据的制作人、电子数据的持有人签名或者盖章，附所提取、复制、固定的电子数据一并随案移送。

对于电子数据存储在境外的计算机上的，或者侦查机关从赌博网站提取电子数据时犯罪嫌疑人未到案的，或者电子数据的持有人无法签字或者拒绝签字的，应当由能够证明提取、复制、固定过程的见证人签名或者盖章，记明有关情况。必要时，可对提取、复制、固定有关电子数据的过程拍照或者录像。

14.最高人民法院、最高人民检察院、公安部关于印发《办理跨境赌博犯罪案件若干问题的意见》的通知（公通字〔2020〕14 号）

各省、自治区、直辖市高级人民法院，人民检察院，公安厅、局，解放军军事法院、军事检察院，新疆维吾尔自治区高级人 民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局：

为依法惩治跨境赌博等犯罪活动，维护我国经济安全、社会稳定，根据有关法律、司法解释的规定，结合司法实践，最高人民法院、最高人民检察院、公安部联合制定了《办理跨境 赌博犯罪案件若干问题的意见》。现予以印发，请结合实际认真 贯彻执行。在执行中遇到的新情况、新问题，请及时分别报告最高人民法院、最高人民检察院、公安部。

最高人民法院 最高人民检察院 公安部

2020 年 10 月 16 日

办理跨境赌博犯罪案件若干问题的意见

为依法惩治跨境赌博等犯罪活动，维护我国经济安全、社会稳定，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》 和《最高人民法院、最高人民检察院关于办理赌博刑事案件具体应用法律若干问题的解释》等有关规定，结合司法实践，制定本意见。

一、总体要求

近年来，境外赌场和网络赌博集团对我国公民招赌吸赌问题日益突出，跨境赌博违法犯罪活动日益猖獗，严重妨碍社会管理秩序，引发多种犯罪，严重危害我国经济安全和社会稳定。与此同时，互联网领域黑灰产业助推传统赌博和跨境赌博犯罪向互联网迁移，跨境网络赌博违法犯罪活动呈高发态势，严重威胁人民群众人身财产安全和社会公共安全。人民法院、

人民检察院、公安机关要针对跨境赌博犯罪特点，充分发挥职能作用，贯彻宽严相济刑事政策，准确认定赌博犯罪行为，严格依法办案，依法从严从快惩处，坚决有效遏制跨境赌博犯罪活动，努力实现政治效果、法律效果、社会效果的高度统一。

二、关于跨境赌博犯罪的认定

（一）以营利为目的，有下列情形之一的，属于刑法第三百 零三条第二款规定的“开设赌场”:

1. 境外赌场经营人、实际控制人、投资人，组织、招揽中华人民共和国公民赴境外赌博的；

2. 境外赌场管理人员，组织、招揽中华人民共和国公民赴境外赌博的；

3. 受境外赌场指派、雇佣，组织、招揽中华人民共和国公民赴境外赌博，或者组织、招揽中华人民共和国公民赴境外赌博， 从赌场获取费用、其他利益的；

4. 在境外赌场包租赌厅、赌台，组织、招揽中华人民共和国公民赴境外赌博的；

5. 其他在境外以提供赌博场所、提供赌资、设定赌博方式等， 组织、招揽中华人民共和国公民赴境外赌博的。

在境外赌场通过开设账户、洗码等方式，为中华人民共和国公民赴境外赌博提供资金担保服务的，以“开设赌场"论处。

（二）以营利为目的，利用信息网络、通讯终端等传输赌博 视频、数据，组织中华人民共和国公民跨境赌博活动，有下列情形之一的，属于刑法第三百零三条第二款规定的“开设赌场”：

1. 建立赌博网站、应用程序并接受投注的；

2. 建立赌博网站、应用程序并提供给他人组织赌博的；

3. 购买或者租用赌博网站、应用程序，组织他人赌博的；

4. 参与赌博网站、应用程序利润分成的；

5. 担任赌博网站、应用程序代理并接受投注的；

6. 其他利用信息网络、通讯终端等传输赌博视频、数据，组织跨境赌博活动的。

（三） 组织、招揽中华人民共和国公民赴境外赌博，从参赌 人员中获取费用或者其他利益的，属于刑法第三百零三条第一款 规定的“聚众赌博”。

（四） 跨境开设赌场犯罪定罪处罚的数量或者数额标准，参 照适用《关于办理赌博刑事案件具体应用法律若干问题的解释》《关于办理利用赌博机开设赌场案件适用法律若干问题的意见》 和《关于办理网络赌博犯罪案件适用法律若干问题的意见》的有 关规定。

三、关于跨境赌博共同犯罪的认定

（一） 三人以上为实施开设赌场犯罪而组成的较为固定的犯 罪组织，应当依法认定为赌博犯罪集团。对组织、领导犯罪集团的首要分子，按照集团所犯的全部罪行处罚。对犯罪集团中组织、 指挥、策划者和骨干分子，应当依法从严惩处。

（二）明知他人实施开设赌场犯罪，为其提供场地、技术支 持、资金、资金结算等服务的，以开设赌场罪的共犯论处。

（三）明知是赌博网站、应用程序，有下列情形之一的，以 开设赌场罪的共犯论处：

1. 为赌博网站、应用程序提供软件开发、技术支持、互联 网接入、服务器托管、网络存储空间、通讯传输通道、广告投放、 会员发展、资金支付结算等服务的；

2. 为赌博网站、应用程序担任代理并发展玩家、会员、下线的。

为同一赌博网站、应用程序担任代理，既无上下级关系，又 无犯意联络的，不构成共同犯罪。

（四）对受雇佣为赌场从事接送参赌人员、望风看场、发牌 坐庄、兑换筹码、发送宣传广告等活动的人员及赌博网站、应用 程序中与组织赌博活动无直接关联的一般工作人员，

除参与赌场、 赌博网站、应用程序利润分成或者领取高额固定工资的外，可以 不追究刑事责任，由公安机关依法给予治安管理处罚。

四、关于跨境赌博关联犯罪的认定

（一）使用专门工具、设备或者其他手段诱使他人参赌，人为控制赌局输赢，构成犯罪的，依照刑法关于诈骗犯罪的规定定 罪处罚。

网上开设赌场，人为控制赌局输赢，或者无法实现提现，构成犯罪的，依照刑法关于诈骗犯罪的规定定罪处罚。部分参赌者 赢利、提现不影响诈骗犯罪的认定。

（二）通过开设赌场或者为国家工作人员参与赌博提供资金的形式实施行贿、受贿行为，构成犯罪的，依照刑法关于贿赂犯罪的规定定罪处罚。同时构成赌博犯罪的，应当依法与贿赂犯罪 数罪并罚。

（三）实施跨境赌博犯罪，同时构成组织他人偷越国（边） 境、运送他人偷越国（边）境、偷越国（边）境罪等罪的，应当 依法数罪并罚。

（四） 实施赌博犯罪，为强行索要赌债，实施故意杀人、故 意伤害、非法拘禁、故意毁坏财物、寻衅滋事等行为，构成犯罪 的，应当依法数罪并罚。

（五） 为赌博犯罪提供资金、信用卡、资金结算等服务，构 成赌博犯罪共犯，同时构成非法经营罪、妨害信用卡管理罪、窃 取、收买、非法提供信用卡信息罪、掩饰、隐瞒犯罪所得、犯罪 收益罪等罪的，依照处罚较重的规定定罪处罚。

为网络赌博犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，构成赌博犯罪共犯，同时构成非法利用信息网络罪、帮助信息网络犯罪活动罪等罪的，依照处罚较重的规定定罪处罚。

为实施赌博犯罪，非法获取公民个人信息，或者向实施赌博犯罪者出售、提供公民个人信息，构成赌博犯罪共犯，同时构成侵犯公民个人信息罪的，依照处罚较重的规定定罪处罚。

五、关于跨境赌博犯罪赌资数额的认定及处理

赌博犯罪中用作赌注的款物、换取筹码的款物和通过赌博赢 取的款物属于赌资。

通过网络实施开设赌场犯罪的，赌资数额可以依照开设赌场行为人在其实际控制账户内的投注金额，结合其他证据认定；如无法统计，可以按照查证属实的参赌人员实际参赌的资金额认定。

对于将资金直接或者间接兑换为虚拟货币、游戏道具等虚拟 物品，并用其作为筹码投注的，赌资数额按照购买该虚拟物品所需资金数额或者实际支付资金数额认定。

对于开设赌场犯罪中主要用于接收、流转赌资的银行账户内的资金，犯罪嫌疑人、被告人不能说明合法来源的，可以认定为赌资。

公安机关、人民检察院已查封、扣押、冻结的赌资、赌博用具等涉案财物及孳息，应当制作清单。人民法院对随案移送的涉 案财物，依法予以处理。赌资应当依法予以追缴。赌博违法所得、 赌博用具以及赌博犯罪分子所有的专门用于赌博的财物等，应当 依法予以追缴、没收。

六、关于跨境赌博犯罪案件的管辖

（一） 跨境赌博犯罪案件一般由犯罪地公安机关立案侦查， 由犯罪嫌疑人居住地公安机关立案侦查更为适宜的，可以由犯罪 嫌疑人居住地公安机关立案侦查。犯罪地包括犯罪行为发生地和 犯罪结果发生地。

跨境网络赌博犯罪地包括用于实施赌博犯罪行为的网络服务使用的服务器所在地，网络服务提供者所在地，犯罪嫌疑人、参赌人员使用的网络信息系统所在地，犯罪嫌疑人为网络赌博犯罪 提供帮助的犯罪地等。

（二） 多个公安机关都有权立案侦查的跨境赌博犯罪案件，由最初受理的公安机关或者主要犯罪地公安机关立案侦查。有争 议的，应当按照有利于查清犯罪事实、有利于诉讼

的原则，协商解决。经协商无法达成一致的，由共同上级公安机关指定有关公安机关立案侦查。

在境外实施的跨境赌博犯罪案件，由公安部商最高人民检察 院和最高人民法院指定管辖。

（三）具有下列情形之一的，有关公安机关可以在其职责范围 内并案侦查：

1. 一人犯数罪的；

2. 共同犯罪的；

3. 共同犯罪的犯罪嫌疑人实施其他犯罪的；

4. 多个犯罪嫌疑人实施的犯罪存在直接关联，并案处理有利 于查明案件事实的。

（四）部分犯罪嫌疑人在逃，但不影响对已到案共同犯罪嫌疑人、被告人的犯罪事实认定的，可以依法先行追究已到案共同 犯罪嫌疑人、被告人的刑事责任。

已确定管辖的跨境赌博共同犯罪案件，在逃的犯罪嫌疑人、 被告人归案后，一般由原管辖的公安机关、人民检察院、人民法院管辖。

七、关于跨境赌博犯罪案件证据的收集和审查判断

（一）公安机关、人民检察院、人民法院在办理跨境赌博犯 罪案件中应当注意对电子证据的收集、审查判断。公安机关应当 遵守法定程序，遵循有关技术标准，全面、客观、及时收集、提取电子证据；人民检察院、人民法院应当围绕真实性、合法性、关联性审查判断电子证据。

公安机关、人民检察院、人民法院收集、提取、固定、移送、展示、审查、判断电子证据应当严格依照《最高人民法院、最高 人民检察院、公安部关于办理刑事案件收集提取和审查判断电子 数据若干问题的规定》《最高人民法院、最高人民检察院、公安部 关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》的规定进行。

（二） 公安机关采取技术侦查措施收集的证据材料，能够证 明案件事实的，应当随案移送，并移送批准采取技术侦查措施的 法律文书。

（三） 依照国际条约、刑事司法协助、互助协议或者平等互 助原则，请求证据材料所在地司法机关收集，或者通过国际警务 合作机制、国际刑警组织启动合作取证程序收集的境外证据材料，公安机关应当对其来源、提取人、提取时间或者提供人、提供时间以及保管移交的过程等作出说明。

当事人及其辩护人、诉讼代理人提供的来自境外的证据材料，该证据材料应当经所在国公证机关证明，所在国中央外交主管机 关或者其授权机关认证，并经我国驻该国使、领馆认证。未经证明、认证的，不能作为证据使用。

来自境外的证据材料，能够证明案件事实且符合刑事诉讼法 及相关规定的，经查证属实，可以作为定案的根据。

八、关于跨境赌博犯罪案件宽严相济刑事政策的运用

人民法院、人民检察院、公安机关要深刻认识跨境赌博犯罪的严重社会危害性，正确贯彻宽严相济刑事政策，运用认罪认罚 从宽制度，充分发挥刑罚的惩治和预防功能。对实施跨境赌博犯 罪活动的被告人，应当在全面把握犯罪事实和量刑情节的基础上，依法从严惩处，并注重适用财产刑和追缴、没收等财产处置手段， 最大限度剥夺被告人再犯的能力。

（一） 实施跨境赌博犯罪，有下列情形之一的，酌情从重处罚：

1. 具有国家工作人员身份的；

2. 组织国家工作人员赴境外赌博的；

3. 组织、胁迫、引诱、教唆、容留未成年人参与赌博的；

4. 组织、招揽、雇佣未成年人参与实施跨境赌博犯罪的；

5. 采用限制人身自由等手段强迫他人赌博或者结算赌资，尚 不构成其他犯罪的；

6. 因赌博活动致 1 人以上死亡、重伤或者 3 人以上轻伤，或 者引发其他严重后果，尚不构成其他犯罪的；

7. 组织、招揽中华人民共和国公民赴境外多个国家、地区赌博的；

8. 因赌博、开设赌场曾被追究刑事责任或者二年内曾被行政处罚的。

（二） 对于具有赌资数额大、共同犯罪的主犯、曾因赌博犯 罪行为被追究刑事责任、悔罪表现不好等情形的犯罪嫌疑人、被告人，一般不适用不起诉、免予刑事处罚、缓刑。

（三） 对实施赌博犯罪的被告人，应当加大财产刑的适用。对被告人并处罚金时，应当根据其在赌博犯罪中的地位作用、赌资、违法所得数额等情节决定罚金数额。

（四） 犯罪嫌疑人、被告人提供重要证据，对侦破、查明重大跨境赌博犯罪案件起关键作用，经查证属实的，可以根据案件具体情况，依法从宽处理。

（二）其他关联规定

1. 最高人民法院、最高人民检察院、公安部印发《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》的通知（法发〔2016〕22 号）

各省、自治区、直辖市高级人民法院、人民检察院、公安厅（局），解放军军事法院、军事检察院，新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局：

为规范电子数据的收集提取和审查判断，提高刑事案件办理质量，最高人民法院、最高人民检察院、公安部制定了《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》。现印发给你们，请认真贯彻执行。执行中遇到的问题，请及时分别层报最高人民法院、最高人民检察院、公安部。

最高人民法院
最高人民检察院
公安部
2016 年 9 月 9 日

最高人民法院 最高人民检察院 公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定

为规范电子数据的收集提取和审查判断，提高刑事案件办理质量，根据《中华人民共和国刑事诉讼法》等有关法律规定，结合司法实际，制定本规定。

一、一般规定

第一条 电子数据是案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。

电子数据包括但不限于下列信息、电子文件：

（一）网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息；

（二）手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息；

（三）用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息；

（四）文档、图片、音视频、数字证书、计算机程序等电子文件。

以数字化形式记载的证人证言、被害人陈述以及犯罪嫌疑人、被告人供述和辩解等证据，不属于电子数据。确有必要的，对相关证据的收集、提取、移送、审查，可以参照适用本规定。

第二条　侦查机关应当遵守法定程序，遵循有关技术标准，全面、客观、及时地收集、提取电子数据；人民检察院、人民法院应当围绕真实性、合法性、关联性审查判断电子数据。

第三条　人民法院、人民检察院和公安机关有权依法向有关单位和个人收集、调取电子数据。有关单位和个人应当如实提供。

第四条　电子数据涉及国家秘密、商业秘密、个人隐私的，应当保密。

第五条　对作为证据使用的电子数据，应当采取以下一种或者几种方法保护电子数据的完整性：

（一）扣押、封存电子数据原始存储介质；

（二）计算电子数据完整性校验值；

（三）制作、封存电子数据备份；

（四）冻结电子数据；

（五）对收集、提取电子数据的相关活动进行录像；

（六）其他保护电子数据完整性的方法。

第六条　初查过程中收集、提取的电子数据，以及通过网络在线提取的电子数据，可以作为证据使用。

二、电子数据的收集与提取

第七条　收集、提取电子数据，应当由二名以上侦查人员进行。取证方法应当符合相关技术标准。

第八条　收集、提取电子数据，能够扣押电子数据原始存储介质的，应当扣押、封存原始存储介质，并制作笔录，记录原始存储介质的封存状态。

封存电子数据原始存储介质，应当保证在不解除封存状态的情况下，无法增加、删除、修改电子数据。封存前后应当拍摄被封存原始存储介质的照片，清晰反映封口或者张贴封条处的状况。

封存手机等具有无线通信功能的存储介质，应当采取信号屏蔽、信号阻断或者切断电源等措施。

第九条　具有下列情形之一，无法扣押原始存储介质的，可以提取电子数据，但应当在笔录中注明不能扣押原始存储介质的原因、原始存储介质的存放地点或者电子数据的来源等情况，并计算电子数据的完整性校验值：

（一）原始存储介质不便封存的；

（二）提取计算机内存数据、网络传输数据等不是存储在存储介质上的电子数据的；

（三）原始存储介质位于境外的；

（四）其他无法扣押原始存储介质的情形。

对于原始存储介质位于境外或者远程计算机信息系统上的电子数据，可以通过网络在线提取。

为进一步查明有关情况，必要时，可以对远程计算机信息系统进行网络远程勘验。进行网络远程勘验，需要采取技术侦查措施的，应当依法经过严格的批准手续。

第十条　由于客观原因无法或者不宜依据第八条、第九条的规定收集、提取电子数据的，可以采取打印、拍照或者录像等方式固定相关证据，并在笔录中说明原因。

第十一条　具有下列情形之一的，经县级以上公安机关负责人或者检察长批准，可以对电子数据进行冻结：

（一）数据量大，无法或者不便提取的；

（二）提取时间长，可能造成电子数据被篡改或者灭失的；

（三）通过网络应用可以更为直观地展示电子数据的；

（四）其他需要冻结的情形。

第十二条　冻结电子数据，应当制作协助冻结通知书，注明冻结电子数据的网络应用账号等信息，送交电子数据持有人、网络服务提供者或者有关部门协助办理。解除冻结的，应当在三日内制作协助解除冻结通知书，送交电子数据持有人、网络服务提供者或者有关部门协助办理。

冻结电子数据，应当采取以下一种或者几种方法：

（一）计算电子数据的完整性校验值；

（二）锁定网络应用账号；

（三）其他防止增加、删除、修改电子数据的措施。

第十三条　调取电子数据，应当制作调取证据通知书，注明需要调取电子数据的相关信息，通知电子数据持有人、网络服务提供者或者有关部门执行。

第十四条　收集、提取电子数据，应当制作笔录，记录案由、对象、内容、收集、提取电子数据的时间、地点、方法、过程，并附电子数据清单，注明类别、文件格式、完整性校验值等，由侦查人员、电子数据持有人（提供人）签名或者盖章；电子数据持有人（提供人）无法签名或者拒绝签名的，应当在笔录中注明，由见证人签名或者盖章。有条件的，应当对相关活动进行录像。

第十五条　收集、提取电子数据，应当根据刑事诉讼法的规定，由符合条件的人员担任见证人。由于客观原因无法由符合条件的人员担任见证人的，应当在笔录中注明情况，并对相关活动进行录像。

针对同一现场多个计算机信息系统收集、提取电子数据的，可以由一名见证人见证。

第十六条　对扣押的原始存储介质或者提取的电子数据，可以通过恢复、破解、统计、关联、比对等方式进行检查。必要时，可以进行侦查实验。

电子数据检查，应当对电子数据存储介质拆封过程进行录像，并将电子数据存储介质通过写保护设备接入到检查设备进行检查；有条件的，应当制作电子数据备份，对备份进行检查；无法使用写保护设备且无法制作备份的，应当注明原因，并对相关活动进行录像。

电子数据检查应当制作笔录，注明检查方法、过程和结果，由有关人员签名或者盖章。进行侦查实验的，应当制作侦查实验笔录，注明侦查实验的条件、经过和结果，由参加实验的人员签名或者盖章。

第十七条　对电子数据涉及的专门性问题难以确定的，由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具报告。对于人民检察院直接受理的案件，也可以由最高人民检察院指定的机构出具报告。

具体办法由公安部、最高人民检察院分别制定。

三、电子数据的移送与展示

第十八条　收集、提取的原始存储介质或者电子数据，应当以封存状态随案移送，并制作电子数据的备份一并移送。

对网页、文档、图片等可以直接展示的电子数据，可以不随案移送打印件；人民法院、人民检察院因设备等条件限制无法直接展示电子数据的，侦查机关应当随案移送打印件，或者附展示工具和展示方法说明。

对冻结的电子数据，应当移送被冻结电子数据的清单，注明类别、文件格式、冻结主体、证据要点、相关网络应用账号，并附查看工具和方法的说明。

第十九条　对侵入、非法控制计算机信息系统的程序、工具以及计算机病毒等无法直接展示的电子数据，应当附电子数据属性、功能等情况的说明。

对数据统计量、数据同一性等问题，侦查机关应当出具说明。

第二十条　公安机关报请人民检察院审查批准逮捕犯罪嫌疑人，或者对侦查终结的案件移送人民检察院审查起诉的，应当将电子数据等证据一并移送人民检察院。人民检察院在审查批准逮捕和审查起诉过程中发现应当移送的电子数据没有移送或者移送的电子数据不符合相关要求的，应当通知公安机关补充移送或者进行补正。

对于提起公诉的案件，人民法院发现应当移送的电子数据没有移送或者移送的电子数据不符合相关要求的，应当通知人民检察院。

公安机关、人民检察院应当自收到通知后三日内移送电子数据或者补充有关材料。

第二十一条　控辩双方向法庭提交的电子数据需要展示的，可以根据电子数据的具体类型，借助多媒体设备出示、播放或者演示。必要时，可以聘请具有专门知识的人进行操作，并就相关技术问题作出说明。

四、电子数据的审查与判断

第二十二条　对电子数据是否真实，应当着重审查以下内容：

（一）是否移送原始存储介质；在原始存储介质无法封存、不便移动时，有无说明原因，并注明收集、提取过程及原始存储介质的存放地点或者电子数据的来源等情况；

（二）电子数据是否具有数字签名、数字证书等特殊标识；

（三）电子数据的收集、提取过程是否可以重现；

（四）电子数据如有增加、删除、修改等情形的，是否附有说明；

（五）电子数据的完整性是否可以保证。

第二十三条　对电子数据是否完整，应当根据保护电子数据完整性的相应方法进行验证：

（一）审查原始存储介质的扣押、封存状态；

（二）审查电子数据的收集、提取过程，查看录像；

（三）比对电子数据完整性校验值；

（四）与备份的电子数据进行比较；

（五）审查冻结后的访问操作日志；

（六）其他方法。

第二十四条　对收集、提取电子数据是否合法，应当着重审查以下内容：

（一）收集、提取电子数据是否由二名以上侦查人员进行，取证方法是否符合相关技术标准；

（二）收集、提取电子数据，是否附有笔录、清单，并经侦查人员、电子数据持有人（提供人）、见证人签名或者盖章；没有持有人（提供人）签名或者盖章的，是否注明原因；对电子数据的类别、文件格式等是否注明清楚；

（三）是否依照有关规定由符合条件的人员担任见证人，是否对相关活动进行录像；

（四）电子数据检查是否将电子数据存储介质通过写保护设备接入到检查设备；有条件的，是否制作电子数据备份，并对备份进行检查；无法制作备份且无法使用写保护设备的，是否附有录像。

第二十五条　认定犯罪嫌疑人、被告人的网络身份与现实身份的同一性，可以通过核查相关 IP 地址、网络活动记录、上网终端归属、相关证人证言以及犯罪嫌疑人、被告人供述和辩解等进行综合判断。

认定犯罪嫌疑人、被告人与存储介质的关联性，可以通过核查相关证人证言以及犯罪嫌疑人、被告人供述和辩解等进行综合判断。

第二十六条　公诉人、当事人或者辩护人、诉讼代理人对电子数据鉴定意见有异议，可以申请人民法院通知鉴定人出庭作证。人民法院认为鉴定人有必要出庭的，鉴定人应当出庭作证。

经人民法院通知，鉴定人拒不出庭作证的，鉴定意见不得作为定案的根据。对没有正当理由拒不出庭作证的鉴定人，人民法院应当通报司法行政机关或者有关部门。

公诉人、当事人或者辩护人、诉讼代理人可以申请法庭通知有专门知识的人出庭，就鉴定意见提出意见。

对电子数据涉及的专门性问题的报告，参照适用前三款规定。

第二十七条　电子数据的收集、提取程序有下列瑕疵，经补正或者作出合理解释的，可以采用；不能补正或者作出合理解释的，不得作为定案的根据：

（一）未以封存状态移送的；

（二）笔录或者清单上没有侦查人员、电子数据持有人（提供人）、见证人签名或者盖章的；

（三）对电子数据的名称、类别、格式等注明不清的；

（四）有其他瑕疵的。

第二十八条　电子数据具有下列情形之一的，不得作为定案的根据：

（一）电子数据系篡改、伪造或者无法确定真伪的；

（二）电子数据有增加、删除、修改等情形，影响电子数据真实性的；

（三）其他无法保证电子数据真实性的情形。

五、附则

第二十九条　本规定中下列用语的含义：

（一）存储介质，是指具备数据信息存储功能的电子设备、硬盘、光盘、优盘、记忆棒、存储卡、存储芯片等载体。

（二）完整性校验值，是指为防止电子数据被篡改或者破坏，使用散列算法等特定算法对电子数据进行计算，得出的用于校验数据完整性的数据值。

（三）网络远程勘验，是指通过网络对远程计算机信息系统实施勘验，发现、提取与犯罪有关的电子数据，记录计算机信息系统状态，判断案件性质，分析犯罪过程，确定侦查方向和范围，为侦查破案、刑事诉讼提供线索和证据的侦查活动。

（四）数字签名，是指利用特定算法对电子数据进行计算，得出的用于验证电子数据来源和完整性的数据值。

（五）数字证书，是指包含数字签名并对电子数据来源、完整性进行认证的电子文件。

（六）访问操作日志，是指为审查电子数据是否被增加、删除或者修改，由计算机信息系统自动生成的对电子数据访问、操作情况的详细记录。

第三十条　本规定自 2016 年 10 月 1 日起施行。之前发布的规范性文件与本规定不一致的，以本规定为准。

2.《网络安全法》（2017.06.01）

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日通过，现予公布，自 2017 年 6 月 1 日起施行。

中华人民共和国主席 习近平

2016 年 11 月 7 日

中华人民共和国网络安全法

（2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过）

目录

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对

网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条　网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条　国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条　国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条　任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章　网络安全支持与促进

第十五条　国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条　国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条　国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条　国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条　各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条　国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章　网络运行安全

第一节　一般规定

第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十二条　网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，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。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

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。

第二十三条　网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条　网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条　网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条　开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条　任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条　网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条　国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条　网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节　关键信息基础设施的运行安全

第三十一条　国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条　按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条　建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条　除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第三十五条　关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条　关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条　关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十八条　关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条　国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章　网络信息安全

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。

第四十一条　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。

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，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

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。

第四十三条　个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条　依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条　任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条　网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条　任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条　网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条　国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章　监测预警与应急处置

第五十一条　国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条　负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条　国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条　网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条　发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条　省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条　因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条　因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章　法律责任

第五十九条　网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条　违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条　网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条　违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条　违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条　网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条　关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条　关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十七条　违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条　网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条　网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条　发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输

的信息的，依照有关法律、行政法规的规定处罚。

第七十一条　有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条　国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十三条　网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十四条　违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条　境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章　附 则

第七十六条　本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条　存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条　军事网络的安全保护，由中央军事委员会另行规定。

第七十九条　本法自 2017 年 6 月 1 日起施行。

3.《互联网直播服务管理规定》（国家互联网信息办公室 2016 年 11 月 4 日发布）

第一条　为加强对互联网直播服务的管理，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》《互联网信息服务管理办法》和《互联网新闻信息服务管理规定》，制定本规定。

第二条　在中华人民共和国境内提供、使用互联网直播服务，应当遵守本规定。

本规定所称互联网直播，是指基于互联网，以视频、音频、图文等形式向公众持续发布实时信息的活动；本规定所称互联网直播服务提供者，是指提供互联网直播平台服务的主体；本规定所称互联网直播服务使用者，包括互联网直播发布者和用户。

第三条　提供互联网直播服务，应当遵守法律法规，坚持正确导向，大力弘扬社会主义核心价值观，培育积极健康、向上向善的网络文化，维护良好网络生态，维护国家利益和公

共利益，为广大网民特别是青少年成长营造风清气正的网络空间。

第四条　国家互联网信息办公室负责全国互联网直播服务信息内容的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内的互联网直播服务信息内容的监督管理执法工作。国务院相关管理部门依据职责对互联网直播服务实施相应监督管理。

各级互联网信息办公室应当建立日常监督检查和定期检查相结合的监督管理制度，指导督促互联网直播服务提供者依据法律法规和服务协议规范互联网直播服务行为。

第五条　互联网直播服务提供者提供互联网新闻信息服务的，应当依法取得互联网新闻信息服务资质，并在许可范围内开展互联网新闻信息服务。

开展互联网新闻信息服务的互联网直播发布者，应当依法取得互联网新闻信息服务资质并在许可范围内提供服务。

第六条　通过网络表演、网络视听节目等提供互联网直播服务的，还应当依法取得法律法规规定的相关资质。

第七条　互联网直播服务提供者应当落实主体责任，配备与服务规模相适应的专业人员，健全信息审核、信息安全管理、值班巡查、应急处置、技术保障等制度。提供互联网新闻信息直播服务的，应当设立总编辑。

互联网直播服务提供者应当建立直播内容审核平台，根据互联网直播的内容类别、用户规模等实施分级分类管理，对图文、视频、音频等直播内容加注或播报平台标识信息，对互联网新闻信息直播及其互动内容实施先审后发管理。

第八条　互联网直播服务提供者应当具备与其服务相适应的技术条件，应当具备即时阻断互联网直播的技术能力，技术方案应符合国家相关标准。

第九条　互联网直播服务提供者以及互联网直播服务使用者不得利用互联网直播服务从事危害国家安全、破坏社会稳定、扰乱社会秩序、侵犯他人合法权益、传播淫秽色情等法律法规禁止的活动，不得利用互联网直播服务制作、复制、发布、传播法律法规禁止的信息内容。

第十条　互联网直播发布者发布新闻信息，应当真实准确、客观公正。转载新闻信息应当完整准确，不得歪曲新闻信息内容，并在显著位置注明来源，保证新闻信息来源可追溯。

第十一条　互联网直播服务提供者应当加强对评论、弹幕等直播互动环节的实时管理，配备相应管理人员。

互联网直播发布者在进行直播时，应当提供符合法律法规要求的直播内容，自觉维护直播活动秩序。

用户在参与直播互动时，应当遵守法律法规，文明互动，理性表达。

第十二条　互联网直播服务提供者应当按照“后台实名、前台自愿”的原则，对互联网直播用户进行基于移动电话号码等方式的真实身份信息认证，对互联网直播发布者进行基于身份证件、营业执照、组织机构代码证等的认证登记。互联网直播服务提供者应当对互联网直播发布者的真实身份信息进行审核，向所在地省、自治区、直辖市互联网信息办公室分类备案，并在相关执法部门依法查询时予以提供。

互联网直播服务提供者应当保护互联网直播服务使用者身份信息和隐私，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

第十三条　互联网直播服务提供者应当与互联网直播服务使用者签订服务协议，明确双方权利义务，要求其承诺遵守法律法规和平台公约。

互联网直播服务协议和平台公约的必备条款由互联网直播服务提供者所在地省、自治区、直辖市互联网信息办公室指导制定。

第十四条　互联网直播服务提供者应当对违反法律法规和服务协议的互联网直播服务使用者，视情采取警示、暂停发布、关闭账号等处置措施，及时消除违法违规直播信息内容，

保存记录并向有关主管部门报告。

第十五条　互联网直播服务提供者应当建立互联网直播发布者信用等级管理体系，提供与信用等级挂钩的管理和服务。

互联网直播服务提供者应当建立黑名单管理制度，对纳入黑名单的互联网直播服务使用者禁止重新注册账号，并及时向所在地省、自治区、直辖市互联网信息办公室报告。

省、自治区、直辖市互联网信息办公室应当建立黑名单通报制度，并向国家互联网信息办公室报告。

第十六条　互联网直播服务提供者应当记录互联网直播服务使用者发布内容和日志信息，保存六十日。

互联网直播服务提供者应当配合有关部门依法进行的监督检查，并提供必要的文件、资料和数据。

第十七条　互联网直播服务提供者和互联网直播发布者未经许可或者超出许可范围提供互联网新闻信息服务的，由国家和省、自治区、直辖市互联网信息办公室依据《互联网新闻信息服务管理规定》予以处罚。

对于违反本规定的其他违法行为，由国家和地方互联网信息办公室依据职责，依法予以处罚；构成犯罪的，依法追究刑事责任。通过网络表演、网络视听节目等提供网络直播服务，违反有关法律法规的，由相关部门依法予以处罚。

第十八条　鼓励支持相关行业组织制定行业公约，加强行业自律，建立健全行业信用评价体系和服务评议制度，促进行业规范发展。

第十九条　互联网直播服务提供者应当自觉接受社会监督，健全社会投诉举报渠道，设置便捷的投诉举报入口，及时处理公众投诉举报。

第二十条　本规定自 2016 年 12 月 1 日起施行。

4. 文化部关于印发《网络表演经营活动管理办法》的通知（文市发〔2016〕33 号）

各省、自治区、直辖市文化厅（局），新疆生产建设兵团文化广播电视局，西藏自治区、北京市、天津市、上海市、重庆市文化市场（综合）行政执法总队：

为切实加强网络表演经营活动管理，规范市场秩序，推动网络表演行业健康有序发展，根据《互联网信息服务管理办法》、《互联网文化管理暂行规定》等有关法律法规，文化部制定了《网络表演经营活动管理办法》，现予印发，请认真贯彻执行。

网络表演是网络文化的重要组成部分。各级文化行政部门和文化市场综合执法机构要加强对网络表演市场的管理和规范，主动引导网络文化经营单位依法依规开展经营活动，自觉提供内容健康、向上向善，有益于弘扬社会主义核心价值观的优秀网络表演，促进我国网络文化繁荣发展。

特此通知。

文　化　部

2016 年 12 月 2 日

网络表演经营活动管理办法

第一条　为切实加强网络表演经营活动管理，规范网络表演市场秩序，促进行业健康有序发展，根据《互联网信息服务管理办法》、《互联网文化管理暂行规定》等有关法律法规，制定本办法。

第二条　本办法所称网络表演是指以现场进行的文艺表演活动等为主要内容，通过互联网、移动通讯网、移动互联网等信息网络，实时传播或者以音视频形式上载传播而形成的互联网文化产品。

网络表演经营活动是指通过用户收费、电子商务、广告、赞助等方式获取利益，向公众提供网络表演产品及服务的行为。

将网络游戏技法展示或解说的内容，通过互联网、移动通讯网、移动互联网等信息网络，实时传播或者以音视频形式上载传播的经营活动，参照本办法进行管理。

第三条　从事网络表演经营活动，应当遵守宪法和有关法律法规，坚持为人民服务、为社会主义服务的方向，坚持社会主义先进文化的前进方向，自觉弘扬社会主义核心价值观。

第四条　从事网络表演经营活动的网络表演经营单位，应当根据《互联网文化管理暂行规定》，向省级文化行政部门申请取得《网络文化经营许可证》，许可证的经营范围应当明确包括网络表演。网络表演经营单位应当在其网站主页的显著位置标明《网络文化经营许可证》编号。

第五条　网络表演经营单位对本单位开展的网络表演经营活动承担主体责任，应当按照《互联网文化管理暂行规定》和《网络文化经营单位内容自审管理办法》的有关要求，建立健全内容审核管理制度，配备满足自审需要并取得相应资质的审核人员，建立适应内容管理需要的技术监管措施。

不具备内容自审及实时监管能力的网络表演经营单位，不得开通表演频道。未采取监管措施或未通过内容自审的网络表演产品，不得向公众提供。

第六条　网络表演不得含有以下内容：

（一）含有《互联网文化管理暂行规定》第十六条规定的禁止内容的；

（二）表演方式恐怖、残忍、暴力、低俗，摧残表演者身心健康的；

（三）利用人体缺陷或者以展示人体变异等方式招徕用户的；

（四）以偷拍偷录等方式，侵害他人合法权益的；

（五）以虐待动物等方式进行表演的；

（六）使用未取得文化行政部门内容审查批准文号或备案编号的网络游戏产品，进行网络游戏技法展示或解说的。

第七条　网络表演经营单位应当加强对未成年人的保护，不得损害未成年人身心健康。有未成年人参与的网络表演，不得侵犯未成年人权益。

第八条　网络表演经营单位要加强对表演者的管理。为表演者开通表演频道的，应与表演者签订协议，约定双方权利义务，要求其承诺遵守法律法规和相关管理规定。

第九条　网络表演经营单位应当要求表演者使用有效身份证件进行实名注册，并采取面谈、录制通话视频等有效方式进行核实。网络表演经营单位应当依法保护表演者的身份信息。

第十条　网络表演经营单位为外国或者香港特别行政区、澳门特别行政区、台湾地区的表演者（以下简称境外表演者）开通表演频道并向公众提供网络表演产品的，应当于开通网络表演频道前，向文化部提出申请。未经批准，不得为境外表演者开通表演频道。为境内表演者开通表演频道的，应当于表演者开展表演活动之日起 10 日内，将表演频道信息向文化部备案。

第十一条　网络表演经营单位应当在表演频道内及表演音视频上，标注经营单位标识等信息。网络表演经营单位应当根据表演者信用等级、所提供的表演内容类型等，对表演频道采取针对性管理措施。

第十二条　网络表演经营单位应当完善用户注册系统，保存用户注册信息，积极采取措施保护用户信息安全。要依照法律法规规定或者服务协议，加强对用户行为的监督和约束，发现用户发布违法信息的，应当立即停止为其提供服务，保存有关记录并向有关部门报告。

第十三条　网络表演经营单位应当建立内部巡查监督管理制度，对网络表演进行实时监管。网络表演经营单位应当记录全部网络表演视频资料并妥善保存，资料保存时间不得少于 60 日，并在有关部门依法查询时予以提供。

网络表演经营单位向公众提供的非实时的网络表演音视频（包括用户上传的），应当严格实行先自审后上线。

第十四条　网络表演经营单位应当建立突发事件应急处置机制。发现本单位所提供的网络表演含有违法违规内容时，应当立即停止提供服务，保存有关记录，并立即向本单位注册地或者实际经营地省级文化行政部门或文化市场综合执法机构报告。

第十五条　网络表演经营单位应当在每季度第一个月月底前将本单位上季度的自审信息（包括实时监运情况、发现问题处置情况和提供违法违规内容的表演者信息等）报送文化部。

第十六条　网络表演经营单位应当建立健全举报系统，主动接受网民和社会监督。要配备专职人员负责举报受理，建立有效处理举报问题的内部联动机制。要在其网站主页及表演者表演频道页面的显著位置，设置“12318”全国文化市场举报网站链接按钮。

第十七条　文化部负责全国网络表演市场的监督管理，建立统一的网络表演警示名单、黑名单等信用监管制度，制定并发布网络表演审核工作指引等标准规范，组织实施全国网络表演市场随机抽查工作，对网络表演内容合法性进行最终认定。

第十八条　各级文化行政部门和文化市场综合执法机构要加强对网络表演市场的事中事后监管，重点实施“双随机一公开”。要充分利用网络文化市场执法协作机制，加强对辖区内网络表演经营单位的指导、服务和日常监管，制定随机抽查工作实施方案和随机抽查事项清单。县级以上文化行政部门或文化市场综合执法机构，根据查处情况，实施警示名单和黑名单等信用管理制度。及时公布查处结果，主动接受社会监督。

第十九条　网络表演行业的协会、自律组织等要主动加强行业自律，制定行业标准和经营规范，开展行业培训，推动企业守法经营。

第二十条　网络表演经营单位违反本办法第四条有关规定，从事网络表演经营活动未申请许可证的，由县级以上文化行政部门或者文化市场综合执法机构按照《互联网文化管理暂行规定》第二十一条予以查处；未按照许可证业务范围从事网络表演活动的，按照《互联网文化管理暂行规定》第二十四条予以查处。

第二十一条　网络表演经营单位提供的表演内容违反本办法第六条有关规定的，由县级以上文化行政部门或者文化市场综合执法机构按照《互联网文化管理暂行规定》第二十八条予以查处。

第二十二条　网络表演经营单位违反本办法第十条有关规定，为未经批准的表演者开通表演频道的，由县级以上文化行政部门或者文化市场综合执法机构按照《互联网文化管理暂行规定》第二十八条予以查处；逾期未备案的，按照《互联网文化管理暂行规定》第二十七条予以查处。

网络表演经营单位自 2017 年 3 月 15 日起，按照本办法第十条有关规定，通过全国文化市场技术监管与服务平台向文化部提交申请或备案。

第二十三条　网络表演经营单位违反本办法第十三条有关规定，未按规定保存网络表演视频资料的，按照《互联网文化管理暂行规定》第三十一条予以查处。

第二十四条　网络表演经营单位违反本办法第十四条有关规定的，由县级以上文化行政部门或者文化市场综合执法机构按照《互联网文化管理暂行规定》第三十条予以查处。

第二十五条　网络表演经营单位违反本办法第五条、第八条、第九条、第十一条、第十二条、第十三条、第十五条有关规定，未能完全履行自审责任的，由县级以上文化行政部门或者文化市场综合执法机构按照《互联网文化管理暂行规定》第二十九条予以查处。

第二十六条　通过信息网络实时在线传播营业性演出活动的，应当遵守《互联网文化管理暂行规定》、《营业性演出管理条例》及《营业性演出管理条例实施细则》的有关规定。

第二十七条　本办法自 2017 年 1 月 1 日起施行。

6. 关于印发《人民检察院办理网络犯罪案件规定》的通知(最高人民检察院 2021 年 1 月 22 日发布)

各级人民检察院：

《人民检察院办理网络犯罪案件规定》已经 2020 年 12 月 14 日最高人民检察院第十三届检察委员会第五十七次会议通过，现印发你们，请结合实际，认真贯彻落实。

最高人民检察院

2021 年 1 月 22 日

人民检察院办理网络犯罪案件规定

第一章 一般规定

第一条 为规范人民检察院办理网络犯罪案件，维护国家安全、网络安全、社会公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国刑事诉讼法》《人民检察院刑事诉讼规则》等规定，结合司法实践，制定本规定。

第二条 本规定所称网络犯罪是指针对信息网络实施的犯罪，利用信息网络实施的犯罪，以及其他上下游关联犯罪。

第三条 人民检察院办理网络犯罪案件应当加强全链条惩治，注重审查和发现上下游关联犯罪线索。对涉嫌犯罪，公安机关未立案侦查、应当提请批准逮捕而未提请批准逮捕或者应当移送起诉而未移送起诉的，依法进行监督。

第四条 人民检察院办理网络犯罪案件应当坚持惩治犯罪与预防犯罪并举，建立捕、诉、监、防一体的办案机制，加强以案释法，发挥检察建议的作用，促进有关部门、行业组织、企业等加强网络犯罪预防和治理，净化网络空间。

第五条 网络犯罪案件的管辖适用刑事诉讼法及其他相关规定。

有多个犯罪地的，按照有利于查清犯罪事实、有利于保护被害人合法权益、保证案件公正处理的原则确定管辖。

因跨区域犯罪、共同犯罪、关联犯罪等原因存在管辖争议的，由争议的人民检察院协商解决，协商不成的，报请共同的上级人民检察院指定管辖。

第六条 人民检察院办理网络犯罪案件应当发挥检察一体化优势，加强跨区域协作办案，强化信息互通、证据移交、技术协作，增强惩治网络犯罪的合力。

第七条 人民检察院办理网络犯罪案件应当加强对电子数据收集、提取、保全、固定等的审查，充分运用同一电子数据往往具有的多元关联证明作用，综合运用电子数据与其他证据，准确认定案件事实。

第八条 建立检察技术人员、其他有专门知识的人参与网络犯罪案件办理制度。根据案件办理需要，吸收检察技术人员加入办案组辅助案件办理。积极探索运用大数据、云计算、人工智能等信息技术辅助办案，提高网络犯罪案件办理的专业化水平。

第九条 人民检察院办理网络犯罪案件，对集团犯罪或者涉案人数众多的，根据行为人的客观行为、主观恶性、犯罪情节及地位、作用等综合判断责任轻重和刑事追究的必要性，按照区别对待原则分类处理，依法追诉。

第十条 人民检察院办理网络犯罪案件应当把追赃挽损贯穿始终，主动加强与有关机关协作，保证及时查封、扣押、冻结涉案财物，阻断涉案财物移转链条，督促涉案人员退赃退赔。

第二章 引导取证和案件审查

第十一条 人民检察院办理网络犯罪案件应当重点围绕主体身份同一性、技术手段违法性、上下游行为关联性等方面全面审查案件事实和证据，注重电子数据与其他证据之间的相

互印证，构建完整的证据体系。

第十二条 经公安机关商请，根据追诉犯罪的需要，人民检察院可以派员适时介入重大、疑难、复杂网络犯罪案件的侦查活动，并对以下事项提出引导取证意见：

（一）案件的侦查方向及可能适用的罪名；

（二）证据的收集、提取、保全、固定、检验、分析等；

（三）关联犯罪线索；

（四）追赃挽损工作；

（五）其他需要提出意见的事项。

人民检察院开展引导取证活动时，涉及专业性问题的，可以指派检察技术人员共同参与。

第十三条 人民检察院可以通过以下方式了解案件办理情况：

（一）查阅案件材料；

（二）参加公安机关对案件的讨论；

（三）了解讯（询）问犯罪嫌疑人、被害人、证人的情况；

（四）了解、参与电子数据的收集、提取；

（五）其他方式。

第十四条 人民检察院介入网络犯罪案件侦查活动，发现关联犯罪或其他新的犯罪线索，应当建议公安机关依法立案或移送相关部门；对于犯罪嫌疑人不构成犯罪的，依法监督公安机关撤销案件。

第十五条 人民检察院可以根据案件侦查情况，向公安机关提出以下取证意见：

（一）能够扣押、封存原始存储介质的，及时扣押、封存；

（二）扣押可联网设备时，及时采取信号屏蔽、信号阻断或者切断电源等方式，防止电子数据被远程破坏；

（三）及时提取账户密码及相应数据，如电子设备、网络账户、应用软件等的账户密码，以及存储于其中的聊天记录、电子邮件、交易记录等；

（四）及时提取动态数据，如内存数据、缓存数据、网络连接数据等；

（五）及时提取依赖于特定网络环境的数据，如点对点网络传输数据、虚拟专线网络中的数据等；

（六）及时提取书证、物证等客观证据，注意与电子数据相互印证。

第十六条 对于批准逮捕后要求公安机关继续侦查、不批准逮捕后要求公安机关补充侦查或者审查起诉退回公安机关补充侦查的网络犯罪案件，人民检察院应当重点围绕本规定第十二条第一款规定的事项，有针对性地制作继续侦查提纲或者补充侦查提纲。对于专业性问题，应当听取检察技术人员或者其他有专门知识的人的意见。

人民检察院应当及时了解案件继续侦查或者补充侦查的情况。

第十七条 认定网络犯罪的犯罪嫌疑人，应当结合全案证据，围绕犯罪嫌疑人与原始存储介质、电子数据的关联性、犯罪嫌疑人网络身份与现实身份的同一性，注重审查以下内容：

（一）扣押、封存的原始存储介质是否为犯罪嫌疑人所有、持有或者使用；

（二）社交、支付结算、网络游戏、电子商务、物流等平台的账户信息、身份认证信息、数字签名、生物识别信息等是否与犯罪嫌疑人身份关联；

（三）通话记录、短信、聊天信息、文档、图片、语音、视频等文件内容是否能够反映犯罪嫌疑人的身份；

（四）域名、IP 地址、终端 MAC 地址、通信基站信息等是否能够反映电子设备为犯罪嫌疑人所使用；

（五）其他能够反映犯罪嫌疑人主体身份的内容。

第十八条 认定犯罪嫌疑人的客观行为，应当结合全案证据，围绕其利用的程序工具、

技术手段的功能及其实现方式、犯罪行为和结果之间的关联性，注重审查以下内容：

（一）设备信息、软件程序代码等作案工具；

（二）系统日志、域名、IP 地址、WiFi 信息、地理位置信息等是否能够反映犯罪嫌疑人的行为轨迹；

（三）操作记录、网络浏览记录、物流信息、交易结算记录、即时通信信息等是否能够反映犯罪嫌疑人的行为内容；

（四）其他能够反映犯罪嫌疑人客观行为的内容。

第十九条 认定犯罪嫌疑人的主观方面，应当结合犯罪嫌疑人的认知能力、专业水平、既往经历、人员关系、行为次数、获利情况等综合认定，注重审查以下内容：

（一）反映犯罪嫌疑人主观故意的聊天记录、发布内容、浏览记录等；

（二）犯罪嫌疑人行为是否明显违背系统提示要求、正常操作流程；

（三）犯罪嫌疑人制作、使用或者向他人提供的软件程序是否主要用于违法犯罪活动；

（四）犯罪嫌疑人支付结算的对象、频次、数额等是否明显违反正常交易习惯；

（五）犯罪嫌疑人是否频繁采用隐蔽上网、加密通信、销毁数据等措施或者使用虚假身份；

（六）其他能够反映犯罪嫌疑人主观方面的内容。

第二十条 认定犯罪行为的情节和后果，应当结合网络空间、网络行为的特性，从违法所得、经济损失、信息系统的破坏、网络秩序的危害程度以及对被害人的侵害程度等综合判断，注重审查以下内容：

（一）聊天记录、交易记录、音视频文件、数据库信息等能够反映犯罪嫌疑人违法所得、获取和传播数据及文件的性质、数量的内容；

（二）账号数量、信息被点击次数、浏览次数、被转发次数等能够反映犯罪行为对网络空间秩序产生影响的内容；

（三）受影响的计算机信息系统数量、服务器日志信息等能够反映犯罪行为对信息网络运行造成影响程度的内容；

（四）被害人数量、财产损失数额、名誉侵害的影响范围等能够反映犯罪行为对被害人的人身、财产等造成侵害的内容；

（五）其他能够反映犯罪行为情节、后果的内容。

第二十一条 人民检察院办理网络犯罪案件，确因客观条件限制无法逐一收集相关言词证据的，可以根据记录被害人人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实的电子数据、书证等证据材料，在审查被告人及其辩护人所提辩解、辩护意见的基础上，综合全案证据材料，对相关犯罪事实作出认定。

第二十二条 对于数量众多的同类证据材料，在证明是否具有同样的性质、特征或者功能时，因客观条件限制不能全部验证的，可以进行抽样验证。

第二十三条 对鉴定意见、电子数据等技术性证据材料，需要进行专门审查的，应当指派检察技术人员或者聘请其他有专门知识的人进行审查并提出意见。

第二十四条 人民检察院在审查起诉过程中，具有下列情形之一的，可以依法自行侦查：

（一）公安机关未能收集的证据，特别是存在灭失、增加、删除、修改风险的电子数据，需要及时收集和固定的；

（二）经退回补充侦查未达到补充侦查要求的；

（三）其他需要自行侦查的情形。

第二十五条 自行侦查由检察官组织实施，开展自行侦查的检察人员不得少于二人。需要技术支持和安全保障的，由人民检察院技术部门和警务部门派员协助。必要时，可以要求公安机关予以配合。

第二十六条 人民检察院办理网络犯罪案件的部门，发现或者收到侵害国家利益、社会公共利益的公益诉讼案件线索的，应当及时移送负责公益诉讼的部门处理。

第三章 电子数据的审查

第二十七条 电子数据是以数字化形式存储、处理、传输的，能够证明案件事实的数据，主要包括以下形式：

（一）网页、社交平台、论坛等网络平台发布的信息；

（二）手机短信、电子邮件、即时通信、通讯群组等网络通讯信息；

（三）用户注册信息、身份认证信息、数字签名、生物识别信息等用户身份信息；

（四）电子交易记录、通信记录、浏览记录、操作记录、程序安装、运行、删除记录等用户行为信息；

（五）恶意程序、工具软件、网站源代码、运行脚本等行为工具信息；

（六）系统日志、应用程序日志、安全日志、数据库日志等系统运行信息；

（七）文档、图片、音频、视频、数字证书、数据库文件等电子文件及其创建时间、访问时间、修改时间、大小等文件附属信息。

第二十八条 电子数据取证主要包括以下方式：收集、提取电子数据；电子数据检查和侦查实验；电子数据检验和鉴定。

收集、提取电子数据可以采取以下方式：

（一）扣押、封存原始存储介质；

（二）现场提取电子数据；

（三）在线提取电子数据；

（四）冻结电子数据；

（五）调取电子数据。

第二十九条 人民检察院办理网络犯罪案件，应当围绕客观性、合法性、关联性的要求对电子数据进行全面审查。注重审查电子数据与案件事实之间的多元关联，加强综合分析，充分发挥电子数据的证明作用。 ?

第三十条 对电子数据是否客观、真实，注重审查以下内容：

（一）是否移送原始存储介质，在原始存储介质无法封存、不便移动时，是否说明原因，并注明相关情况；

（二）电子数据是否有数字签名、数字证书等特殊标识；

（三）电子数据的收集、提取过程及结果是否可以重现；

（四）电子数据有增加、删除、修改等情形的，是否附有说明；

（五）电子数据的完整性是否可以保证。

第三十一条 对电子数据是否完整，注重审查以下内容：

（一）原始存储介质的扣押、封存状态是否完好；

（二）比对电子数据完整性校验值是否发生变化；

（三）电子数据的原件与备份是否相同；

（四）冻结后的电子数据是否生成新的操作日志。

第三十二条 对电子数据的合法性，注重审查以下内容：

（一）电子数据的收集、提取、保管的方法和过程是否规范；

（二）查询、勘验、扣押、调取、冻结等的法律手续是否齐全；

（三）勘验笔录、搜查笔录、提取笔录等取证记录是否完备；

（四）是否由符合法律规定的取证人员、见证人、持有人（提供人）等参与，因客观原因没有见证人、持有人（提供人）签名或者盖章的，是否说明原因；

（五）是否按照有关规定进行同步录音录像；

（六）对于收集、提取的境外电子数据是否符合国（区）际司法协作及相关法律规定的要求。 ？

第三十三条 对电子数据的关联性，注重审查以下内容：

（一）电子数据与案件事实之间的关联性；

（二）电子数据及其存储介质与案件当事人之间的关联性。

第三十四条 原始存储介质被扣押封存的，注重从以下方面审查扣押封存过程是否规范：

（一）是否记录原始存储介质的品牌、型号、容量、序列号、识别码、用户标识等外观信息，是否与实物一一对应；

（二)是否封存或者计算完整性校验值,封存前后是否拍摄被封存原始存储介质的照片，照片是否清晰反映封口或者张贴封条处的状况；

（三）是否由取证人员、见证人、持有人（提供人）签名或者盖章。

第三十五条 对原始存储介质制作数据镜像予以提取固定的，注重审查以下内容：

（一）是否记录原始存储介质的品牌、型号、容量、序列号、识别码、用户标识等外观信息，是否记录原始存储介质的存放位置、使用人、保管人；

（二）是否附有制作数据镜像的工具、方法、过程等必要信息；

（三）是否计算完整性校验值；

（四）是否由取证人员、见证人、持有人（提供人）签名或者盖章。

第三十六条 提取原始存储介质中的数据内容并予以固定的，注重审查以下内容：

（一）是否记录原始存储介质的品牌、型号、容量、序列号、识别码、用户标识等外观信息，是否记录原始存储介质的存放位置、使用人、保管人；

（二）所提取数据内容的原始存储路径，提取的工具、方法、过程等信息，是否一并提取相关的附属信息、关联痕迹、系统环境等信息；

（三）是否计算完整性校验值；

（四）是否由取证人员、见证人、持有人（提供人）签名或者盖章。

第三十七条 对于在线提取的电子数据，注重审查以下内容：

（一)是否记录反映电子数据来源的网络地址、存储路径或者数据提取时的进入步骤等；

（二）是否记录远程计算机信息系统的访问方式、电子数据的提取日期和时间、提取的工具、方法等信息，是否一并提取相关的附属信息、关联痕迹、系统环境等信息；

（三）是否计算完整性校验值；

（四）是否由取证人员、见证人、持有人（提供人）签名或者盖章。

对可能无法重复提取或者可能出现变化的电子数据，是否随案移送反映提取过程的拍照、录像、截屏等材料。

第三十八条 对冻结的电子数据，注重审查以下内容：

（一）冻结手续是否符合规定；

（二）冻结的电子数据是否与案件事实相关；

（三）冻结期限是否即将到期、有无必要继续冻结或者解除；

（四）冻结期间电子数据是否被增加、删除、修改等。

第三十九条 对调取的电子数据，注重审查以下内容：

（一）调取证据通知书是否注明所调取的电子数据的相关信息；

（二）被调取单位、个人是否在通知书回执上签名或者盖章；

（三）被调取单位、个人拒绝签名、盖章的，是否予以说明；

（四）是否计算完整性校验值或者以其他方法保证电子数据的完整性。

第四十条　对电子数据进行检查、侦查实验，注重审查以下内容：

（一）是否记录检查过程、检查结果和其他需要记录的内容，并由检查人员签名或者盖章；

（二）是否记录侦查实验的条件、过程和结果，并由参加侦查实验的人员签名或者盖章；

（三）检查、侦查实验使用的电子设备、网络环境等是否与发案现场一致或者基本一致；

（四）是否使用拍照、录像、录音、通信数据采集等一种或者多种方式客观记录检查、侦查实验过程。

第四十一条　对电子数据进行检验、鉴定，注重审查以下内容：

（一）鉴定主体的合法性。包括审查司法鉴定机构、司法鉴定人员的资质，委托鉴定事项是否符合司法鉴定机构的业务范围，鉴定人员是否存在回避等情形；

（二）鉴定材料的客观性。包括鉴定材料是否真实、完整、充分，取得方式是否合法，是否与原始电子数据一致；

（三）鉴定方法的科学性。包括鉴定方法是否符合国家标准、行业标准，方法标准的选用是否符合相关规定；

（四）鉴定意见的完整性。是否包含委托人、委托时间、检材信息、鉴定或者分析论证过程、鉴定结果以及鉴定人签名、日期等内容；

（五）鉴定意见与其他在案证据能否相互印证。

对于鉴定机构以外的机构出具的检验、检测报告，可以参照本条规定进行审查。

第四十二条　行政机关在行政执法和查办案件过程中依法收集、提取的电子数据，人民检察院经审查符合法定要求的，可以作为刑事案件的证据使用。

第四十三条　电子数据的收集、提取程序有下列瑕疵，经补正或者作出合理解释的，可以采用；不能补正或者作出合理解释的，不得作为定案的根据：

（一）未以封存状态移送的；

（二）笔录或者清单上没有取证人员、见证人、持有人（提供人）签名或者盖章的；

（三）对电子数据的名称、类别、格式等注明不清的；

（四）有其他瑕疵的。

第四十四条　电子数据系篡改、伪造、无法确定真伪的，或者有其他无法保证电子数据客观、真实情形的，不得作为定案的根据。

电子数据有增加、删除、修改等情形，但经司法鉴定、当事人确认等方式确定与案件相关的重要数据未发生变化，或者能够还原电子数据原始状态、查清变化过程的，可以作为定案的根据。

第四十五条　对于无法直接展示的电子数据，人民检察院可以要求公安机关提供电子数据的内容、存储位置、附属信息、功能作用等情况的说明，随案移送人民法院。

第四章 出庭支持公诉

第四十六条　人民检察院依法提起公诉的网络犯罪案件，具有下列情形之一的，可以建议人民法院召开庭前会议：

（一）案情疑难复杂的；

（二）跨国（边）境、跨区域案件社会影响重大的；

（三）犯罪嫌疑人、被害人等人数众多、证据材料较多的；

（四）控辩双方对电子数据合法性存在较大争议的；

（五）案件涉及技术手段专业性强，需要控辩双方提前交换意见的；

（六）其他有必要召开庭前会议的情形。

必要时，人民检察院可以向法庭申请指派检察技术人员或者聘请其他有专门知识的人参

加庭前会议。

第四十七条　人民法院开庭审理网络犯罪案件，公诉人出示证据可以借助多媒体示证、动态演示等方式进行。必要时，可以向法庭申请指派检察技术人员或者聘请其他有专门知识的人进行相关技术操作，并就专门性问题发表意见。

公诉人在出示电子数据时，应当从以下方面进行说明：

（一）电子数据的来源、形成过程；

（二）电子数据所反映的犯罪手段、人员关系、资金流向、行为轨迹等案件事实；

（三）电子数据与被告人供述、被害人陈述、证人证言、物证、书证等的相互印证情况；

（四）其他应当说明的内容。

第四十八条　在法庭审理过程中，被告人及其辩护人针对电子数据的客观性、合法性、关联性提出辩解或者辩护意见的，公诉人可以围绕争议点从证据来源是否合法，提取、复制、制作过程是否规范，内容是否真实完整，与案件事实有无关联等方面，有针对性地予以答辩。

第四十九条　支持、推动人民法院开庭审判网络犯罪案件全程录音录像。对庭审全程录音录像资料，必要时人民检察院可以商请人民法院复制，并将存储介质附检察卷宗保存。

第五章 跨区域协作办案

第五十条　对跨区域网络犯罪案件，上级人民检察院应当加强统一指挥和统筹协调，相关人民检察院应当加强办案协作。

第五十一条　上级人民检察院根据办案需要，可以统一调用辖区内的检察人员参与办理网络犯罪案件。

第五十二条　办理关联网络犯罪案件的人民检察院可以相互申请查阅卷宗材料、法律文书，了解案件情况，被申请的人民检察院应当予以协助。

第五十三条　承办案件的人民检察院需要向办理关联网络犯罪案件的人民检察院调取证据材料的，可以持相关法律文书和证明文件申请调取在案证据材料，被申请的人民检察院应当配合。

第五十四条　承办案件的人民检察院需要异地调查取证的，可以将相关法律文书及证明文件传输至证据所在地的人民检察院，请其代为调查取证。相关法律文书应当注明具体的取证对象、方式、内容和期限等。

被请求协助的人民检察院应当予以协助，及时将取证结果送达承办案件的人民检察院；无法及时调取的，应当作出说明。被请求协助的人民检察院有异议的，可以与承办案件的人民检察院进行协商；无法解决的，由承办案件的人民检察院报请共同的上级人民检察院决定。

第五十五条　承办案件的人民检察院需要询问异地证人、被害人的，可以通过远程视频系统进行询问，证人、被害人所在地的人民检察院应当予以协助。远程询问的，应当对询问过程进行同步录音录像。

第六章　跨国（边）境司法协作

第五十六条　办理跨国网络犯罪案件应当依照《中华人民共和国国际刑事司法协助法》及我国批准加入的有关刑事司法协助条约，加强国际司法协作，维护我国主权、安全和社会公共利益，尊重协作国司法主权、坚持平等互惠原则，提升跨国司法协作质效。

第五十七条　地方人民检察院在案件办理中需要向外国请求刑事司法协助的，应当制作刑事司法协助请求书并附相关材料，经报最高人民检察院批准后，由我国与被请求国间司法协助条约规定的对外联系机关向外国提出申请。没有刑事司法协助条约的，通过外交途径联系。

第五十八条　人民检察院参加现场移交境外证据的检察人员不少于二人，外方有特殊要

求的除外。

移交、开箱、封存、登记的情况应当制作笔录，由最高人民检察院或者承办案件的人民检察院代表、外方移交人员签名或者盖章，一般应当全程录音录像。有其他见证人的，在笔录中注明。

第五十九条　人民检察院对境外收集的证据，应当审查证据来源是否合法、手续是否齐备以及证据的移交、保管、转换等程序是否连续、规范。

第六十条　人民检察院办理涉香港特别行政区、澳门特别行政区、台湾地区的网络犯罪案件，需要当地有关部门协助的，可以参照本规定及其他相关规定执行。

第七章　附则

第六十一条　人民检察院办理网络犯罪案件适用本规定，本规定没有规定的，适用其他相关规定。

第六十二条　本规定中下列用语的含义：

（一）信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及局域网络；

（二）存储介质，是指具备数据存储功能的电子设备、硬盘、光盘、优盘、记忆棒、存储芯片等载体；

（三）完整性校验值，是指为防止电子数据被篡改或者破坏，使用散列算法等特定算法对电子数据进行计算，得出的用于校验数据完整性的数据值；

（四）数字签名，是指利用特定算法对电子数据进行计算，得出的用于验证电子数据来源和完整性的数据值；

（五）数字证书，是指包含数字签名并对电子数据来源、完整性进行认证的电子文件；

（六）生物识别信息，是指计算机利用人体所固有的生理特征（包括人脸、指纹、声纹、虹膜、DNA 等）或者行为特征（步态、击键习惯等）来进行个人身份识别的信息；

（七）运行脚本，是指使用一种特定的计算机编程语言，依据符合语法要求编写的执行指定操作的可执行文件；

（八）数据镜像，是指二进制（0101 排序的数据码流）相同的数据复制件，与原件的内容无差别；

（九）MAC 地址，是指计算机设备中网卡的唯一标识，每个网卡有且只有一个 MAC 地址。

第六十三条　人民检察院办理国家安全机关、海警机关、监狱等移送的网络犯罪案件，适用本规定和其他相关规定。

第六十四条　本规定由最高人民检察院负责解释。

第六十五条　本规定自发布之日起施行。

6.**《中华人民共和国个人信息保护法》** 主席令第九十一号

《中华人民共和国个人信息保护法》已由中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议于 2021 年 8 月 20 日通过，现予公布，自 2021 年 11 月 1 日起施行。

中华人民共和国主席 习近平

2021 年 8 月 20 日

中华人民共和国个人信息保护法

（2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过）

第一章 总 则

第一条　为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根

据宪法，制定本法。

第二条 自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第三条 在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

（一）以向境内自然人提供产品或者服务为目的；

（二）分析、评估境内自然人的行为；

（三）法律、行政法规规定的其他情形。

第四条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

第五条 处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

第七条 处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条 个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

第二章 个人信息处理规则

第一节 一般规定

第十三条 符合下列情形之一的，个人信息处理者方可处理个人信息：

（一）取得个人的同意；

（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；

（三）为履行法定职责或者法定义务所必需；

（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；

（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

（七）法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项

规定情形的，不需取得个人同意。

第十四条　基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

第十五条　基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条　个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

第十七条　个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

（一）个人信息处理者的名称或者姓名和联系方式；

（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

（三）个人行使本法规定权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第十八条　个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

第十九条　除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

第二十条　两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

第二十一条　个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

第二十二条　个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十三条　个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取

得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十四条 个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十五条 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第二十六条 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

第二十七条 个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

第二节 敏感个人信息的处理规则

第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

第二十九条 处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第三十条 个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

第三十一条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

第三节 国家机关处理个人信息的特别规定

第三十三条 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。

第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。

第三十七条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章 个人信息跨境提供的规则

第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

第四十二条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

第四十三条 任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 个人在个人信息处理活动中的权利

第四十四条 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十五条 个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第四十六条 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

第四十七条 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；

（三）个人撤回同意；

（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

（五）法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第四十八条 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

第五十条 个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章 个人信息处理者的义务

第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

（一）制定内部管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

（五）制定并组织实施个人信息安全事件应急预案；

（六）法律、行政法规规定的其他措施。

第五十二条 处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十三条 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第五十五条 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

（一）处理敏感个人信息；

（二）利用个人信息进行自动化决策；

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

（四）向境外提供个人信息；

（五）其他对个人权益有重大影响的个人信息处理活动。

第五十六条 个人信息保护影响评估应当包括下列内容：

（一）个人信息的处理目的、处理方式等是否合法、正当、必要；

（二）对个人权益的影响及安全风险；

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；

（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

第五十八条 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：

（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；

（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；

（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；

（四）定期发布个人信息保护社会责任报告，接受社会监督。

第五十九条 接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

第六章 履行个人信息保护职责的部门

第六十条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条 履行个人信息保护职责的部门履行下列个人信息保护职责：

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

（二）接受、处理与个人信息保护有关的投诉、举报；

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

（四）调查、处理违法个人信息处理活动；

（五）法律、行政法规规定的其他职责。

第六十二条 国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

（一）制定个人信息保护具体规则、标准；

（二）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；

（三）支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设；

（四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务；

（五）完善个人信息保护投诉、举报工作机制。

第六十三条 履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

（一）询问有关当事人，调查与个人信息处理活动有关的情况;

（二）查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料;

（三）实施现场检查，对涉嫌违法的个人信息处理活动进行调查;

（四）检查与个人信息处理活动有关的设备、物品;对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十四条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第六十五条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章 法律责任

第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第六十七条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第六十八条 国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正;对直接负责的主管人员和其他直接责任人员依法给予处分。

履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六十九条 处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定;个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

第七十条 个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十一条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第八章 附 则

第七十二条 自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

第七十三条 本法下列用语的含义：

（一）个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

（二）自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

（四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

第七十四条 本法自 2021 年 11 月 1 日起施行。

7.《中华人民共和国数据安全法》（主席令第八十四号，2021.09.01）

《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于 2021 年 6 月 10 日通过，现予公布，自 2021 年 9 月 1 日起施行。

中华人民共和国主席 习近平

2021 年 6 月 10 日

中华人民共和国数据安全法

（2021 年 6 月 10 日第十三届全国人民代表大会常务委员会第二十九次会议通过）

第一章 总 则

第一条为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

第七条国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

第八条开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第九条国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第二章 数据安全与发展

第十三条国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

第十六条国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

第十八条国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

第二十三条国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法作出的安全审查决定为最终决定。

第二十五条国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 数据安全保护义务

第二十七条开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第二十八条开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

第三十一条关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第三十二条任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

第三十三条从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

第三十四条法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

第三十五条公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

第三十六条中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第五章 政务数据安全与开放

第三十七条国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。

第三十八条国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第四十条国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

第四十二条国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

第四十三条法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第四十七条从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五

百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第四十九条国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第五十条履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第五十二条违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第五十三条开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条本法自 2021 年 9 月 1 日起施行。

7. **《关键信息基础设施安全保护条例》**（国务院令第 745 号，2021.09.01）

《关键信息基础设施安全保护条例》已经 2021 年 4 月 27 日国务院第 133 次常务会议通过，现予公布，自 2021 年 9 月 1 日起施行。

总理　　李克强

2021 年 7 月 30 日

关键信息基础设施安全保护条例

第一章 总 则

第一条为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。

第二条本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

第三条在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。

省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

第四条关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者（以下简称运营者）主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。

第五条国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。

任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。

第六条运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第七条对在关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照国家有关规定给予表彰。

第二章 关键信息基础设施认定

第八条本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。

第九条保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

（一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

（三）对其他行业和领域的关联性影响。

第十条保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

第十一条关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起 3 个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。

第三章 运营者责任义务

第十二条安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

第十三条运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

第十四条运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。

第十五条专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：

（一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；

（二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

（三）按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；

（四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

（五）组织网络安全教育、培训；

（六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；

（七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；

（八）按照规定报告网络安全事件和重要事项。

第十六条运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

第十七条运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

第十八条关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。

发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

第十九条运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第二十条运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第二十一条运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

第四章 保障和促进

第二十二条保护工作部门应当制定本行业、本领域关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。

第二十三条国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。

第二十四条保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

第二十五条保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

第二十六条保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

第二十七条国家网信部门统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。

有关部门在开展关键信息基础设施网络安全检查时，应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

第二十八条运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。

第二十九条在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要，及时提供技术支持和协助。

第三十条网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。

第三十一条未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。

第三十二条国家采取措施，优先保障能源、电信等关键信息基础设施安全运行。

能源、电信行业应当采取措施，为其他行业和领域的关键信息基础设施安全运行提供重点保障。

第三十三条公安机关、国家安全机关依据各自职责依法加强关键信息基础设施安全保卫，防范打击针对和利用关键信息基础设施实施的违法犯罪活动。

第三十四条国家制定和完善关键信息基础设施安全标准，指导、规范关键信息基础设施安全保护工作。

第三十五条国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。

第三十六条国家支持关键信息基础设施安全防护技术创新和产业发展，组织力量实施关键信息基础设施安全技术攻关。

第三十七条国家加强网络安全服务机构建设和管理，制定管理要求并加强监督指导，不断提升服务机构能力水平，充分发挥其在关键信息基础设施安全保护中的作用。

第三十八条国家加强网络安全军民融合，军地协同保护关键信息基础设施安全。

第五章 法律责任

第三十九条运营者有下列情形之一的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款：

（一）在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工作部门的；

（二）安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的；

（三）未建立健全网络安全保护制度和责任制的；

（四）未设置专门安全管理机构的；

（五）未对专门安全管理机构负责人和关键岗位人员进行安全背景审查的；

（六）开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的；

（七）专门安全管理机构未履行本条例第十五条规定的职责的；

（八）未对关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的；

（九）采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的；

（十）发生合并、分立、解散等情况，未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的。

第四十条运营者在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款。

第四十一条运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额 1 倍以上 10 倍以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

第四十二条运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；情节严重的，依法追究相应法律责任。

第四十三条实施非法侵入、干扰、破坏关键信息基础设施，危害其安全的活动尚不构成犯罪的，依照《中华人民共和国网络安全法》有关规定，由公安机关没收违法所得，处 5 日以下拘留，可以并处 5 万元以上 50 万元以下罚款；情节较重的，处 5 日以上 15 日以下拘留，可以并处 10 万元以上 100 万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处 10 万元以上 100 万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本条例第五条第二款和第三十一条规定，受到治安管理处罚的人员，5 年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第四十四条网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十五条公安机关、保护工作部门和其他有关部门在开展关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的，由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十六条网信部门、公安机关、保护工作部门等有关部门、网络安全服务机构及其工作人员将在关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十七条关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

第四十八条电子政务关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，依照《中华人民共和国网络安全法》有关规定予以处理。

第四十九条违反本条例规定，给他人造成损害的，依法承担民事责任。

违反本条例规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第六章 附 则

第五十条存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。

第五十一条本条例自 2021 年 9 月 1 日起施行。

三、指导案例、典型案例

（一）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；提供侵入、非法控制计算机信息系统程序罪

1.最高人民检察院关于印发最高人民检察院第十八批指导性案例的通知（高检发办字[2020]21 号）

各级人民检察院：

经 2020 年 1 月 3 日最高人民检察院第十三届检察委员会第三十一次会议通过，现将张凯闵等 52 人电信网络诈骗案等三件指导性案例（检例第 67－69 号）作为第十八批指导性案例发布，供参照适用。

最高人民检察院

2020 年 3 月 28

检例第 68 号：叶源星、张剑秋提供侵入计算机信息系统程序、谭房妹非法获取计算机信息系统数据案

【关键词】

专门用于侵入计算机信息系统的程序 非法获取计算机信息系统数据 撞库 打码

【要旨】

对有证据证明用途单一，只能用于侵入计算机信息系统的程序，司法机关可依法认定为“专门用于侵入计算机信息系统的程序”；难以确定的，应当委托专门部门或司法鉴定机构作出检验或鉴定。

【基本案情】

叶源星，男，1977 年 3 月 10 日出生，超市网络维护员。

张剑秋，男，1972 年 8 月 14 日出生，小学教师。

谭房妹，男，1993 年 4 月 5 日出生，农民。

2015 年 1 月，被告人叶源星编写了用于批量登录某电商平台账户的“小黄伞”撞库软件（“撞库”是指黑客通过收集已泄露的用户信息，利用账户使用者相同的注册习惯，如相同的用户名和密码，尝试批量登陆其他网站，从而非法获取可登录用户信息的行为）供他人免费使用。“小黄伞”撞库软件运行时，配合使用叶源星编写的打码软件（“打码”是指利用人工大量输入验证码的行为）可以完成撞库过程中对大量验证码的识别。叶源星通过网络向他人有偿提供打码软件的验证码识别服务，同时将其中的人工输入验证码任务交由被告人张剑秋完成，并向其支付费用。

2015 年 1 月至 9 月，被告人谭房妹通过下载使用“小黄伞”撞库软件，向叶源星购买打码服务，获取到某电商平台用户信息 2.2 万余组。

被告人叶源星、张剑秋通过实施上述行为，从被告人谭房妹处获取违法所得共计人民币

4 万余元。谭房妹通过向他人出售电商平台用户信息，获取违法所得共计人民币 25 万余元。法院审理期间，叶源星、张剑秋、谭房妹退缴了全部违法所得。

【指控与证明犯罪】

（一）审查起诉

2016 年 10 月 10 日，浙江省杭州市公安局余杭区分局以犯罪嫌疑人叶源星、张剑秋、谭房妹涉嫌非法获取计算机信息系统数据罪移送杭州市余杭区人民检察院审查起诉。期间，叶源星、张剑秋的辩护人向检察机关提出二名犯罪嫌疑人无罪的意见。叶源星的辩护人认为，叶源星利用“小黄伞”软件批量验证已泄露信息的行为，不构成非法获取计算机信息系统数据罪。张剑秋的辩护人认为，张剑秋不清楚组织打码是为了非法获取某电商平台的用户信息。张剑秋与叶源星没有共同犯罪故意，不构成非法获取计算机信息系统数据罪。

杭州市余杭区人民检察院经审查认为，犯罪嫌疑人叶源星编制“小黄伞”撞库软件供他人使用，犯罪嫌疑人张剑秋组织码工打码，犯罪嫌疑人谭房妹非法获取网络用户信息并出售牟利的基本事实清楚，但需要进一步补强证据。2016 年 11 月 25 日、2017 年 2 月 7 日，检察机关二次将案件退回公安机关补充侦查，明确提出需要补查的内容、目的和要求。一是完善“小黄伞”软件的编制过程、运作原理、功能等方面的证据，以便明确“小黄伞”软件是否具有避开或突破某电商平台服务器的安全保护措施，非法获取计算机信息系统数据的功能。二是对扣押的张剑秋电脑进行补充勘验，以便确定张剑秋主观上是否明知其组织打码行为是为他人非法获取某电商平台用户信息提供帮助；调取张剑秋与叶源星的 QQ 聊天记录，以便查明二人是否有犯意联络。三是提取叶源星被扣押电脑的 MAC 地址（又叫网卡地址，由 12 个 16 进制数组成，是上网设备在网络中的唯一标识），分析“小黄伞”软件源代码中是否含有叶源星电脑的 MAC 地址，以便查明某电商平台被非法登陆过的账号与叶源星编制的“小黄伞”撞库软件之间是否存在关联性。四是对被扣押的谭房妹电脑和 U 盘进行补充勘验，调取其中含有账号、密码的文件，查明文件的生成时间和特征，以便确定被查获的存储介质中的某电商平台用户信息是否系谭房妹使用“小黄伞”软件获取。

公安机关按照检察机关的要求，对证据作了进一步补充完善。同时，检察机关就“小黄伞”软件的运行原理等问题，听取了技术专家意见。结合公安机关两次退查后补充的证据，案件证据中存在的问题已经得到解决：

一是明确了“小黄伞”软件具有以下功能特征：（1）“小黄伞”软件用途单一，仅针对某电商平台账号进行撞库和接入打码平台，这种非法侵入计算机信息系统获取用户数据的程序没有合法用途。（2）“小黄伞”软件具有避开或突破计算机信息系统安全保护措施的功能。在实施撞库过程中，一个 IP 地址需要多次登录大量账号，为防止被某电商平台识别为非法登陆，导致 IP 地址被封锁，“小黄伞”软件被编入自动拨号功能，在批量登陆几组账号后，会自动切换新的 IP 地址，从而达到避开该电商平台安全防护的目的。（3）“小黄伞”软件具有绕过验证码识别防护措施的功能。在他人利用非法获取的该电商平台账号登录时，需要输入验证码。“小黄伞”软件会自动抓取验证码图片发送到打码平台，由张剑秋组织的码工对验证码进行识别。（4）“小黄伞”软件具有非法获取计算机信息系统数据的功能。“小黄伞”软件对登陆成功的某电商平台账号，在未经授权的情况下，会自动抓取账号对应的昵称、注册时间、账号等级等信息数据。根据以上特征，可以认定“小黄伞”软件属于刑法规定的“专门用于侵入计算机信息系统的程序”。

二是从张剑秋和叶源星电脑中补充勘查到的QQ聊天记录等电子数据证实，叶源星与张剑秋聊天过程中曾提及“扫平台”、“改一下平台程序”、“那些人都是出码的”；通过补充讯问张剑秋和叶源星，明确了张剑秋明知其帮叶源星打验证码可能被用于非法目的，仍然帮叶源星做打码代理。上述证据证实张剑秋与叶源星之间已经形成犯意联络，具有共同犯罪故意。

三是通过进一步补充证据，证实了使用撞库软件的终端设备的MAC地址与叶源星电脑的MAC地址、小黄伞软件的源代码里包含的MAC地址一致。上述证据证实叶源星就是“小黄伞”软件的编制者。

四是通过对谭房妹所有包含某电商平台用户账号和密码的文件进行比对，查明了谭房妹利用“小黄伞”撞库软件非法获取的某电商平台用户信息文件不仅包含账号、密码，还包含了注册时间、账号等级、是否验证等信息，而谭房妹从其他渠道非法获取的账号信息文件并不包含这些信息。通过对谭房妹电脑的进一步勘查和对谭房妹的进一步讯问，确定了谭房妹利用“小黄伞”软件登陆某电商平台用户账号的过程和具体时间，该登录时间与部分账号信息文件的生成时间均能一一对应。根据上述证据，最终确定谭房妹利用“小黄伞”撞库所得的网络用户信息为2.2万余组。

综上，检察机关认为案件事实已查清，但公安机关对犯罪嫌疑人叶源星、张剑秋移送起诉适用的罪名不准确。叶源星、张剑秋共同为他人提供专门用于侵入计算机信息系统的程序，均已涉嫌提供侵入计算机信息系统程序罪；犯罪嫌疑人谭房妹的行为已涉嫌非法获取计算机信息系统数据罪。

（二）出庭指控犯罪

2017年6月20日，杭州市余杭区人民检察院以被告人叶源星、张剑秋构成提供侵入计算机信息系统程序罪，被告人谭房妹构成非法获取计算机信息系统数据罪，向杭州市余杭区人民法院提起公诉。11月17日，法院公开开庭审理了本案。

庭审中，3名被告人对检察机关的指控均无异议。谭房妹的辩护人提出，谭房妹系初犯，归案后能如实供述罪行，自愿认罪，请求法庭从轻处罚。叶源星和张剑秋的辩护人提出以下辩护意见：一是检察机关未提供省级以上有资质机构的检验结论，现有证据不足以认定“小黄伞”软件是“专门用于侵入计算机信息系统的程序”。二是张剑秋与叶源星间没有共同犯罪的主观故意。三是叶源星和张剑秋的违法所得金额应扣除支付给码工的钱款。

针对上述辩护意见，公诉人答辩如下：一是在案电子数据、勘验笔录、技术人员的证言、被告人供述等证据相互印证，足以证实“小黄伞”软件具有避开和突破计算机信息系统安全保护措施，未经授权获取计算机信息系统数据的功能，属于法律规定的“专门用于侵入计算机信息系统的程序”。二是被告人叶源星与张剑秋具有共同犯罪的故意。QQ聊天记录反映两人曾提及非法获取某电商平台用户信息的内容，能证实张剑秋主观明知其组织他人打码系用于批量登录该电商平台账号。张剑秋组织他人帮助打码的行为和叶源星提供撞库软件的行为相互配合，相互补充，系共同犯罪。三是被告人叶源星、张剑秋的违法所得应以其出售验证码服务的金额认定，给码工等相关支出均属于犯罪成本，不应扣除。二人系共同犯罪，应

当对全部犯罪数额承担责任。四是3名被告人在庭审中认罪态度较好且上交了全部违法所得，建议从轻处罚。

（三）处理结果

浙江省杭州市余杭区人民法院采纳了检察机关的指控意见，判决认定被告人叶源星、张剑秋的行为已构成提供侵入计算机信息系统程序罪，且系共同犯罪；被告人谭房妹的行为已构成非法获取计算机信息系统数据罪。鉴于3名被告人均自愿认罪，并退出违法所得，对3名被告人判处三年有期徒刑，适用缓刑，并处罚金。宣判后，3名被告人均未提出上诉，判决已生效。

【指导意义】

审查认定“专门用于侵入计算机信息系统的程序”，一般应要求公安机关提供以下证据：一是从被扣押、封存的涉案电脑、U盘等原始存储介质中收集、提取相关的电子数据。二是对涉案程序、被侵入的计算机信息系统及电子数据进行勘验、检查后制作的笔录。三是能够证实涉案程序的技术原理、制作目的、功能用途和运行效果的书证材料。四是涉案程序的制作人、提供人、使用人对该程序的技术原理、制作目的、功能用途和运行效果进行阐述的言词证据，或能够展示涉案程序功能的视听资料。五是能够证实被侵入计算机信息系统安全保护措施的技术原理、功能以及被侵入后果的专业人员的证言等证据。六是对有运行条件的，应要求公安机关进行侦查实验。对有充分证据证明涉案程序是专门设计用于侵入计算机信息系统、非法获取计算机信息系统数据的，可直接认定为“专门用于侵入计算机信息系统的程序”。

证据审查中，可从以下方面对涉案程序是否属于“专门用于侵入计算机信息系统的程序”进行判断：一是结合被侵入的计算机信息系统的安全保护措施，分析涉案程序是否具有侵入的目的，是否具有避开或者突破计算机信息系统安全保护措施的功能。二是结合计算机信息系统被侵入的具体情形，查明涉案程序是否在未经授权或超越授权的情况下，获取计算机信息系统数据。三是分析涉案程序是否属于“专门”用于侵入计算机信息系统的程序。

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》第十条和《最高人民法院、最高人民检察院、公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第十七条的规定，对是否属于“专门用于侵入计算机信息系统的程序”难以确定的，一般应当委托省级以上负责计算机信息系统安全保护管理工作的部门检验，也可由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具报告。实践中，应重点审查检验报告、鉴定意见对程序运行过程和运行结果的判断，结合案件具体情况，认定涉案程序是否具有突破或避开计算机信息系统安全保护措施，未经授权或超越授权获取计算机信息系统数据的功能。

【相关规定】

《中华人民共和国刑法》第二百八十五条、第二十五条

《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、第二条、第三条、第十条、第十一条

《最高人民法院、最高人民检察院、公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第十七条

2.最高人民检察院关于印发最高人民检察院第九批指导性案例的通知（高检发研字[2017]10号）

各省、自治区、直辖市人民检察院，解放军军事检察院，新疆生产建设兵团人民检察院：

经2017年10月10日最高人民检察院第十二届检察委员会第七十次会议决定，现将李丙龙破坏计算机信息系统案等六件指导性案例（检例第33－38号）作为第九批指导性案例发布，供参照适用。

最高人民检察院

2017年10月12日

检例第36号：卫梦龙、龚旭、薛东东非法获取计算机信息系统数据案

【关键词】

非法获取计算机信息系统数据　超出授权范围登录　侵入计算机信息系统

【基本案情】

被告人卫梦龙，男，1987年10月生，原系北京某公司经理。

被告人龚旭，女，1983年9月生，原系北京某大型网络公司运营规划管理部员工。

被告人薛东东，男，1989年12月生，无固定职业。

被告人卫梦龙曾于2012年至2014年在北京某大型网络公司工作，被告人龚旭供职于该大型网络公司运营规划管理部，两人原系同事。被告人薛东东系卫梦龙商业合作伙伴。

因工作需要，龚旭拥有登录该大型网络公司内部管理开发系统的账号、密码、Token令牌（计算机身份认证令牌），具有查看工作范围内相关数据信息的权限。但该大型网络公司禁止员工私自在内部管理开发系统查看、下载非工作范围内的电子数据信息。

2016年6月至9月，经事先合谋，龚旭向卫梦龙提供自己所掌握的该大型网络公司内部管理开发系统账号、密码、Token令牌。卫梦龙利用龚旭提供的账号、密码、Token令牌，违反规定多次在异地登录该大型网络公司内部管理开发系统，查询、下载该计算机信息系统中储存的电子数据。后卫梦龙将非法获取的电子数据交由薛东东通过互联网出售牟利，违法所得共计37000元。

【诉讼过程和结果】

本案由北京市海淀区人民检察院于2017年2月9日以被告人卫梦龙、龚旭、薛东东犯非法获取计算机信息系统数据罪，向北京市海淀区人民法院提起公诉。6月6日，北京市海淀区人民法院作出判决，认定被告人卫梦龙、龚旭、薛东东的行为构成非法获取计算机信息系统数据罪，情节特别严重。判处卫梦龙有期徒刑四年，并处罚金人民币四万元；判处龚旭有期徒刑三年九个月，并处罚金人民币四万元；判处薛东东有期徒刑四年，并处罚金人民币四万元。一审宣判后，三被告人未上诉，判决已生效。

【要旨】

超出授权范围使用账号、密码登录计算机信息系统，属于侵入计算机信息系统的行为；侵入计算机信息系统后下载其储存的数据，可以认定为非法获取计算机信息系统数据。

【指导意义】

非法获取计算机信息系统数据罪中的“侵入”，是指违背被害人意愿、非法进入计算机信息系统的行为。其表现形式既包括采用技术手段破坏系统防护进入计算机信息系统，也包括未取得被害人授权擅自进入计算机信息系统，还包括超出被害人授权范围进入计算机信息系统。

本案中，被告人龚旭将自己因工作需要掌握的本公司账号、密码、Token 令牌等交由卫梦龙登录该公司管理开发系统获取数据，虽不属于通过技术手段侵入计算机信息系统，但内外勾结擅自登录公司内部管理开发系统下载数据，明显超出正常授权范围。超出授权范围使用账号、密码、Token 令牌登录系统，也属于侵入计算机信息系统的行为。行为人违反《计算机信息系统安全保护条例》第七条、《计算机信息网络国际联网安全保护管理办法》第六条第一项等国家规定，实施了非法侵入并下载获取计算机信息系统中存储的数据的行为，构成非法获取计算机信息系统数据罪。按照 2011 年《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》规定，构成犯罪，违法所得二万五千元以上，应当认定为“情节特别严重”，处三年以上七年以下有期徒刑，并处罚金。

【相关法律规定】

《中华人民共和国刑法》

第二百八十五条　违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

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。

《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　非法获取计算机信息系统数据或者非法控制计算机信息系统，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“情节严重”：

……

（四）违法所得五千元以上或者造成经济损失一万元以上的；

……

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；

……

《中华人民共和国计算机信息系统安全保护条例》

第七条　任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

《计算机信息网络国际联网安全保护管理办法》

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

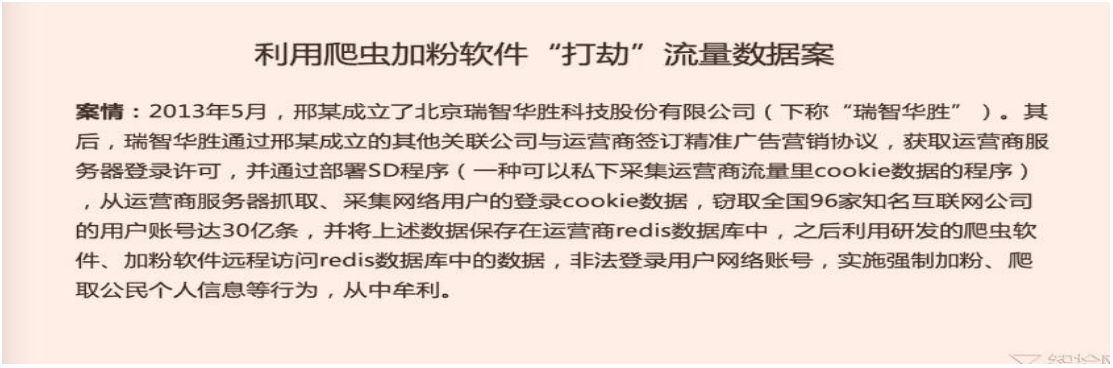
（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

3.2019 年度浙江省互联网十大检察案例之一：利用爬虫加粉软件“打劫”流量数据案-周嘉林等非法获取计算机信息系统数据案



2019 年 10 月，由绍兴市越城区人民检察院提起公诉的“史上最大规模数据窃取案”宣判。被告单位利用爬虫、加粉等恶意软件，规避或突破计算机保护措施，疯狂窃取网络流量中的 cookie 数据，窃取全国 96 家知名互联网公司的用户账号达 30 亿条，并进行爬取订单、强制加粉、推广等行为，从中牟取巨额利益。本案是一起利用爬虫技术窃取网络数据的典型案例，犯罪手法极其专业，检察机关通过细致审查，准确把握 cookie 数据与公民个人信息的区别，厘清非法获取计算机信息系统数据罪与其他关联犯罪的界限，严厉打击了信息系统数据黑灰产业链。本案的成功办理，也给网络运营商敲响了警钟，查补数据安全漏洞，被包括央视新闻、新华网等各大媒体报道。

附：北京瑞智华胜科技股份有限公司、周嘉林、黄健等违法运用资金罪一审刑事判决书

浙江省绍兴市越城区人民法院

刑 事 判 决 书

（2019）浙0602刑初636号

公诉机关绍兴市越城区人民检察院。

被告单位北京瑞智华胜科技股份有限公司，住所地北京市海淀区西四环北路******9D。

法定代表人周嘉林，男，1980年11月1日出生于，汉族，本科文化，系北京瑞智华胜科技股份有限公司股东，住广东省广州市越秀区。

诉讼代表人王晓月，女，1995年7月11日出生于河北省青龙满族自治县，满族，系北京瑞智华胜科技股份有限公司人事行政专员，住河北省青龙满族自治县。

被告人周嘉林，男，1980年11月1日出生于，汉族，本科文化，系北京瑞智华胜科技股份有限公司法定代表人、股东，住广东省广州市越秀区。因涉嫌犯侵犯公民个人信息罪于2018年7月3日被绍兴市公安局越城区分局刑事拘留，同月13日变更为取保候审。2019年7月15日，被本院取保候审。2019年10月28日，本院决定对其逮捕。

辩护人游志雄，北京市逸峰律师事务所律师。

被告人黄健，男，1980年11月2日出生于北京市海淀区，回族，本科文化，系北京瑞智华胜科技股份有限公司部门经理、股东，住北京市海淀区。因涉嫌犯侵犯公民个人信息罪于2018年7月3日被绍兴市公安局越城区刑事拘留，同年8月9日被逮捕，2019年7月3日变更为取保候审。2019年10月28日，本院决定对其逮捕。

辩护人季慧娈，浙江大公律师事务所律师。

被告人梁修军，曾用名梁贝贝，男，1991年9月15日出生于河南省淮阳县，汉族，本科文化，系北京瑞智华胜科技股份有限公司运维部员工，住河南省淮阳县。因涉嫌犯侵犯公民个人信息罪于2018年7月3日被绍兴市公安局越城区分局刑事拘留，同年8月9日被逮捕，2019年7月3日变更为取保候审。2019年10月28日，本院决定对其逮捕。

辩护人张丽英，浙江浙杭（绍兴）律师事务所律师。

被告人石炳瑞，男，1990年5月21日出生于山西省阳泉市，汉族，本科文化，系北京瑞智华胜科技股份有限公司研发部员工，住山西省阳泉市。因涉嫌犯侵犯公民个人信息罪于2018年7月3日被绍兴市公安局越城区分局刑事拘留，同年8月9日被逮捕，2019年7月3日变更为取保候审。2019年10月28日，本院决定对其逮捕。

辩护人陈芳斌、沈亚婷，浙江大公律师事务所律师。

被告人裘庚，男，1989年8月16日出生于山东省济南市，汉族，研究生文化，系北京瑞智华胜科技股份有限公司技术总监、股东，住山东省济南市槐荫区。因涉嫌犯侵犯公民个人信息罪于2018年9月11日被绍兴市公安局越城区分局刑事拘留，同年10月18日变更为取保候审。2019年10月18日，本院决定对其取保候审。现取保候审于居住地。

辩护人陈泽玮，浙江大公律师事务所律师。

被告人王岳，男，1991年6月25日出生于北京市海淀区，汉族，本科文化，系北京瑞智华胜科技股份有限公司研发部员工，户籍地北京市海淀区，住北京市海淀区。因涉嫌犯侵犯公民个人信息罪于2018年7月3日被绍兴市公安局越城区分局刑事拘留，同年8月9日被逮捕，同年11月30日变更为取保候审。现取保候审于居住地。

辩护人俞华南，浙江大公律师事务所律师。

被告人王鹏，曾用名王朋，男，1992年12月23日出生于河北省邯郸市，汉族，本科文化，系北京瑞智华胜科技股份有限公司研发部员工，住河北省邯郸市邯山区。因涉嫌犯侵犯公民个人信息罪于2018年7月3日被绍兴市公安局越城区分局刑事拘留，同年8月9日

被逮捕，同年 11 月 30 日变更为取保候审。现取保候审于居住地。

辩护人谌波平，浙江大公律师事务所律师。

绍兴市越城区人民检察院以越检公诉刑诉〔2019〕641 号起诉书指控被告单位北京瑞智华胜科技股份有限公司（以下简称“瑞智公司”）及被告人周嘉林、黄健、梁修军、石炳瑞、裘庚、王岳、王鹏犯非法获取计算机信息系统数据罪，于 2019 年 7 月 12 日向本院提起公诉。本院于同月 15 日立案受理，并依法组成合议庭，适用简易程序审理。因在审理中发现本案具有不宜适用简易程序审理的情形，遂依法转为普通程序，并公开开庭进行了审理。绍兴市越城区人民检察院指派检察员施某出庭支持公诉，被告单位瑞智公司诉讼代表人王晓月、被告人周嘉林、黄健、梁修军、石炳瑞、裘庚、王岳、王鹏及各被告人的辩护人均到庭参加了诉讼。现已审理终结。

绍兴市越城区人民检察院指控：

2013 年 5 月，邢某（另案处理）在北京成立被告单位瑞智公司。瑞智公司通过邢某成立的其他关联公司与运营商签订精准广告营销协议，获取运营商服务器登录许可，并通过部署 SD 程序，从运营商服务器抓取采集网络用户的登录×××数据，并将上述数据保存在运营商 redis 数据库中，利用研发的爬虫软件、加粉软件，远程访问 redis 数据库中的数据，非法登录网络用户的淘宝、微博等账号，进行强制加粉、订单爬取等行为，从中牟利。案发前，瑞智公司发现浙江淘宝网络有限公司在调查订单被爬的情况，遂将服务器数据删除。经鉴定，SD 程序运行后可以实现对指定网卡网络传输流量数据包进行获取并解析的功能；淘宝爬虫程序运行后可以绕过系统保护措施，提取出淘宝订单信息；淘宝加粉程序运行后可以实现绕过系统保护措施获取用户信息，并对指定淘宝账号添加好友。

被告人周嘉林系瑞智公司的法定代表人，负责公司运维部的各项工作；被告人黄健系瑞智公司股东，负责关联公司与运营商签订营销协议，获取运营商登录权限；被告人梁修军、石炳瑞系瑞智公司运维部员工，主要负责 SD 程序、爬虫程序、加粉程序的部署；被告人裘庚、王岳、王鹏系瑞智公司研发部员工，被告人裘庚负责淘宝加粉程序的研发、维护，被告人王岳负责 SD 程序的研发、维护，被告人王鹏负责爬虫程序的维护、优化更新。

经查，2018 年 4 月 17 日至 18 日期间，瑞智公司通过被告人黄健租用的 116.63 段 IP 地址，爬取包括居住绍兴市越城区的被害人李某 1 在内的淘宝订单共计 220552 条（浙江淘宝网络有限公司实际输出 10000 条）。瑞智公司向指定加粉淘宝账号恶意加淘好友共计 137093 个（浙江淘宝网络有限公司实际输出 20000 个）。

2018 年 7 月 2 日，被告人周嘉林、黄健、梁修军、石炳瑞、王岳、王鹏在北京市海淀区被警察抓获归案；同年 9 月 10 日，被告人裘庚在北京市海淀区西三环车公庄西路 35 号院 5 号楼 5 单元 402 室被警察抓获归案。2018 年 10 月 26 日，被告人周嘉林向浙江省湖州市公安局吴兴区分局检举揭发他人的犯罪行为，且已查证属实。

为证明上述事实，公诉人当庭宣读和出示了相关证据。

公诉机关认为，被告单位瑞智公司违反国家规定，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，获取该计算机信息系统中存储、处理或者传输的数据，情节特别严重，被告人周嘉林、黄健、梁修军、石炳瑞、裘庚、王岳、王鹏系直接负责的主管人员与其他直接责任人员，且系共同犯罪，被告单位及被告人的行为触犯了《中华人民共和国刑法》第二百八十五条第二款、第三十条、第三十一条、第二十五条第一款之规定，均应当以非法获取计算机信息系统数据罪追究刑事责任。被告人周嘉林、黄健在共同犯罪中起主要作用，均属主犯；被告人梁修军、石炳瑞、裘庚、王岳、王鹏在共同犯罪中起次要作用，均属从犯。被告人周嘉林揭发他人犯罪行为，查证属实，属立功。被告人周嘉林、黄健、梁修军、石炳瑞、王岳、王鹏、裘庚能够自愿认罪，可酌情从轻处罚。公诉机关在庭审中追加认定被告人黄健具有立功情节。遂根据《中华人民共和国刑法》第二十六条第一款、第二十

七条、第六十七条第三款、第六十八条、第七十二条之规定，建议判处被告人黄健有期徒刑三年至四年，并处罚金人民币八万元至十万元；判处被告人梁修军、石炳瑞有期徒刑二年至三年，并处罚金人民币四万元至六万元；判处被告人裘庚有期徒刑二年至三年，适用缓刑，并处罚金人民币四万元至六万元；判处被告人王岳、王鹏有期徒刑一年六个月至二年六个月，适用缓刑，并处罚金人民币四万元至六万元。

被告单位瑞智公司对起诉指控的事实及罪名均无异议。

被告人周嘉林对起诉指控的事实及罪名均无异议，并表示认罪认罚。

被告人周嘉林的辩护人主要提出以下意见：1.对公诉机关指控的罪名及爬取数据的基本犯罪事实无异议，但就涉案具体事实而言可分为获取运营商数据以及获取淘宝数据两部分内容，其中（1）涉及获取、使用运营商数据的部分不构成非法入侵并获取计算机信息系统数据，该行为具有合同依据，获得了运营商许可，即便后期使用不当也仅构成违约，不具备刑事上的可罚性。此外，被告单位获取的运营商数据已不复存在，因此对相关行为不宜作为犯罪评价。（2）对于指控的淘宝数据而言，对淘宝公司实际输出的数据数量认定无异议，但起诉指控爬取的淘宝订单数据数量为 22 万余条，加好友数据数量为 13 万余条的证据不足。2.基于上述对本案事实认定的意见，现有证据不足以认定被告人的行为已达到情节特别恶劣程度。3.关于对被告人周嘉林的量刑，（1）本案系单位犯罪，被告人周嘉林虽名为公司法定代表人，但实质上其仅仅系公司运营部负责人，持股较少。（2）被告人周嘉林具有立功情节，所举报对象可能判处刑期在十年以上甚至无期。（3）被告人周嘉林系初犯，自始认罪态度良好，且自身身体健康状况不佳。综上，请求对被告人周嘉林在三年以下判处刑罚并适用缓刑。

被告人黄健对起诉指控事实、罪名及量刑建议均无异议，且签字具结，认罪认罚，并请求认定其立功情节，对其适用缓刑。

被告人黄健的辩护人主要提出以下意见：1.对起诉指控的罪名无异议。2.被告人黄健在本案中主要负责与运营商签订营销协议以获取登录权限，该行为对本案危害后果的发生仅起到辅助作用。被告人黄健在行为过程中未组织、策划、指挥涉案人员爬取订单数据，不是犯意的发起者，也不是数据获取的直接实施者，因此应认定其在共同犯罪中为从犯。3.被告人黄健已在庭前签字具结，自愿认罪认罚。4.被告人黄健具有立功表现。5.被告人黄健系初犯、偶犯。综上，请求结合被告人黄健的家庭情况对其从轻处罚，并结合庭审中追加认定的立功情节对其适用缓刑。

被告人梁修军对起诉指控事实、罪名及量刑建议均无异议，且签字具结，认罪认罚。

被告人梁修军的辩护人主要提出以下意见：1.对起诉指控的罪名无异议。2.本案系单位犯罪，被告人梁修军的涉案行为属于履行工作职责，非积极主动参与实施犯罪行为。3.被告人梁修军在行为过程中系听从安排实施相关行为，对本案的发生仅起到辅助作用，应认定为共同犯罪中的从犯。4.被告人梁修军到案后如实供述案件事实，已在庭前签字具结，自愿认罪认罚。5.被告人梁修军系初犯、偶犯，系因法律意识淡薄而走上犯罪道路，主观恶性不深，再犯可能性极小。综上，请求对被告人梁修军在量刑时从轻处罚。

被告人石炳瑞对起诉指控事实、罪名及量刑建议均无异议，且签字具结，认罪认罚。

被告人石炳瑞的辩护人主要提出以下意见：1.对起诉指控的罪名无异议。2.被告人石炳瑞参与作案时间较短，工作内容受人指派，获利仅为基本工资，在共同犯罪中起次要作用，属从犯。3.被告人石炳瑞归案后如实供述案件事实，已在庭前签字具结，认罪认罚。4.本案系单位犯罪，被告人石炳瑞系初犯、偶犯，主观恶性较小，不具有再犯的危险。综上，请求对被告人石炳瑞从轻处罚。

被告人裘庚对起诉指控事实、罪名及量刑建议均无异议，且签字具结，认罪认罚。

被告人裘庚的辩护人主要提出以下意见：1.对起诉指控的罪名无异议。2.被告人裘庚在

单位中属底层员工，仅获取固定工资，其职责仅涉及单位的部分犯罪行为，因此在共同犯罪中属从犯。3.被告人袭庚具有坦白情节，已签字具结，认罪认罚。4.被告人袭庚系初犯、偶犯，对其适用缓刑不至于再发生社会危害。综上，请求对被告人袭庚从轻处罚并适用缓刑。

被告人王岳对起诉指控事实、罪名及量刑建议均无异议，且签字具结，认罪认罚。

被告人王岳的辩护人主要提出以下意见：1.对起诉指控的罪名无异议。2.被告人王岳的涉案行为属职务行为，在公司属于底层员工，在单位犯罪中仅起到次要作用，属于从犯。3.被告人王岳归案后如实供述了案件事实，自愿认罪认罚。4.被告人王岳系初犯、偶犯。综上，请求结合被告人王岳的家庭情况对其从轻处罚并适用缓刑。

被告人王鹏对起诉指控事实、罪名及量刑建议均无异议，且签字具结，认罪认罚。

被告人王鹏的辩护人主要提出以下意见：1.对起诉指控的罪名无异议。2.被告人王鹏的涉案行为系职务行为，非蓄意实施犯罪，工作内容受人支配，所起作用较小，应认定为从犯。3.被告人王鹏具有坦白情节，已签字具结，认罪认罚。4.被告人王鹏系初犯，一贯表现良好。综上，请求对被告人王鹏从轻处罚并适用缓刑。

经审理查明：

被告单位瑞智公司于2013年5月在北京注册成立，案发时邢某（另案处理）系公司实际控制人。被告人周嘉林系公司法定代表人，负责公司运维部各项工作。被告人周嘉林、黄健、袭庚均系公司股东，被告人梁修军、石炳瑞、王岳、王鹏均系公司员工，被告人黄健主要负责与运营商签订服务、合作协议，被告人梁修军、石炳瑞主要负责公司研发应用程序的部署、运行，被告人袭庚、王岳、王鹏主要负责公司应用程序的研发、维护。被告单位瑞智公司在经营过程中，联合关联公司北京中科云某信息技术有限公司（以下简称“云某公司”）、北京点智互动信息技术有限公司（以下简称“点智公司”），通过与运营商签订服务、合作协议的方式获取运营商服务器的登录许可，后恶意部署计算机应用程序采集并保存运营商服务器中的用户登录×××数据等信息，后又利用公司研发的爬虫程序调用数据库中保存的×××数据等信息，并服务于公司研发的QQ、淘宝、微博、抖音等加粉程序，据此开展公司的精准广告营销业务。在业务开展过程中，被告单位瑞智公司的行为涉及通过×××数据非法登录用户账号，爬取用户订单信息、强制添加好友、强行推送广告等操作。

案发前，被告单位瑞智公司在获悉公司采集用户数据信息的行为正在被调查的消息后，随即删除了服务器数据库中保存的数据信息。经浙江淘宝网络有限公司排查，被告单位瑞智公司通过被告人黄健租用的IP地址，仅在2018年4月16-18日期间，即爬取了淘宝用户（部分系绍兴市越城区居民）的订单信息共计22万余条次，为淘宝用户恶意添加好友13万余个次。被告单位瑞智公司及其关联公司通过上述业务非法获利数额特别巨大。

2018年7月2日，被告人周嘉林、黄健、梁修军、石炳瑞、王岳、王鹏被警察抓获归案；同年9月10日，被告人袭庚被民警抓获归案。案发后，被告人周嘉林向公安机关检举揭发了他人的犯罪行为，经查证属实；经被告人黄健规劝，非同案共犯王某2一已投案自首。

上述事实，由公诉机关及被告单位提交，并经庭审质证的下列证据予以证实：

1.被告人周嘉林的供述、辨认笔录及照片主要证明：其是瑞智公司的法定代表人兼股东，瑞智公司与云某公司、点智公司是并列公司，相互配合开展公司业务。其对公司人员的职责分工、公司开展的业务、公司业务开展流程有明确的供述。其负责公司的网络推广业务，主要就是为客户公司进行网络推广，包括但不限于为客户公司的账号添加好友。运营商不知其公司在劫持服务器数据，公司于2017年年初至2018年4月18日劫持的数据已经根据邢某的指示进行了删除，原因是收到了公司行为在被调查的消息。公司劫持的数据包含用户的登录×××信息，据此可以获得账号的登录权限。案发近几天每天劫持的数据在一到二万条。公司的推广业务每月至少获利100万元。2017年年初至案发，其的个人获利至少15万元。拦截并保存运营商数据的SD程序由王岳编写，爬取数据的爬虫程序以及加粉程序由王鹏编

写，部署、操作 SD 程序、爬虫程序的是梁修军和石炳瑞，裘庚是技术部负责人。公司的加粉情况由石炳瑞统计。被告人周嘉林对邢某的身份进行了辨认。

2.被告人黄健的供述主要证明：其是瑞智公司的股东、监事，瑞智公司、点智公司、云某公司是并列公司，三家公司是一套人马三块牌子，公司大老板邢某。云某公司负责与运营商签订合同，获取流量镜像使用权限。点智公司负责广告营销业务。瑞智公司负责数据获取。其对公司业务以及业务的具体开展流程有明确的供述。其的工作是与运营商对接、签订合同，获取数据流量权限，为获取用户×××数据提供条件。其和周嘉林都有对公司运维部进行管理，运维组长是梁修军，具体运维业务由梁修军负责。获取×××数据的程序从 2016 年开始研发，由梁修军、石炳瑞具体操作，数据获取也由他们具体实施。公司加粉数量由梁修军、石炳瑞统计。其的工资大概每月 2 万元，公司的自媒体业务每月获利至少 100 万元。因为获悉公司获取数据的行为被调查，因此 2018 年 4 月公司对获取的数据进行了删除。在与运营商的合同中明确约定不允许滥用数据，运营商数据仅限于合作范围内的广告投放。公司业务开展使用的部分 IP 地址由其向黎某租用。

3.被告人梁修军的供述主要证明：其对瑞智公司的人员结构以及瑞智、云某、点智等公司的关系、公司开展业务的流程有明确的供述，公司法定代表人是周嘉林，研发部人员有王鹏、王岳、裘庚等，运维部负责人是黄健，员工有其和石炳瑞等人。公司的运营是窃取运营商流量上的公民个人数据，并利用这些数据开展广告业务。公司的加粉业绩情况有进行过统计，由黄健指派其和石炳瑞完成。公司的 SD 程序由王岳编写，由其指派石炳瑞等人部署在运营商服务器，通过这个程序可以获取运营商流量上的用户×××数据，并存入 redis 数据库，保存在运营商的服务器上。公司爬虫程序由王鹏、王岳、裘庚等人编写，用于采集用户×××数据，为加粉等业务开展服务，加粉程序研发部的人都有参与编写。裘庚是技术总监，负责加粉业务，加粉规则由裘庚提供。2018 年 4 月有根据老板指示对公司获取的数据进行删除，具体操作由石炳瑞完成。其的月收入 2 万元，年收入大约 29 万元。

4.被告人石炳瑞的供述主要证明：其对瑞智公司的人员结构、公司的业务、业务开展流程有明确的供述。公司先是与运营商签订合作协议，获取流量镜像权限，然后通过公司的 SD 程序采集运营商流量中的×××等数据，并保存在 redis 数据库中，然后通过爬虫程序对淘宝订单等数据进行爬取，用于公司的加粉等业务开展。只要是 SD 程序采集的数据，在加粉业务开展时都会被加粉程序调用。与运营商签订合同由黄健完成。SD 程序由王岳编写，是其放到采集机上的，是根据周嘉林、黄健、梁修军的指示完成数据采集。加粉程序由研发部制作完成，裘庚有参与，其有根据指示执行过加粉工作，并对加粉情况进行统计。2018 年 4 月 18 日，其根据指示将服务器上采集的数据进行了删除操作。其在瑞智公司工作一年半，总共获利 20 万元左右。其被抓获以后，有配合公安机关对相关数据进行提取，包括一小时内提取的抖音×××数据量 1.4 万余条，百度百家二三天的×××数据量 600 多条，一小时内提取的微博×××数据量 2000 多条，百度搜词几个小时的×××数据量 4000 多条等。公司通过 SD 程序采集数据最多的时候涉及 20 多家运营商。

5.被告人裘庚的供述主要证明：其的涉案行为是负责程序研发，其参与研发的程序包括爬虫程序、加粉程序、数据监控程序等，其是公司的技术总监，持有公司 2%的股份。瑞智公司、云某公司、点智公司实际上是一套人马，相同办公地点。其在公司中是根据邢某的安排完成工作任务，其对公司的人员结构有明确的供述。王鹏、王某 2 一有编写部分加粉程序。加粉程序具体是运维部在使用，是梁修军、石炳瑞在操作。加粉是通过程序调用 redis 数据库中的×××数据完成。

6.被告人王岳的供述主要证明：其的涉案行为是根据指示编写、更新了 SD 采集程序，该程序的功能是采集运营商流量中的用户×××等数据，并进行自动保存。程序编写完成后其和梁修军进行测试，之后交给石炳瑞使用，使用的方法是其教给梁修军和石炳瑞的。SD

程序安装到运营商服务器需要运营商的登录用户名和密码。数据采集用途是为了公司的广告投放以及加粉等业务开展。公司研发部的人员有袭庚、王鹏、王某 2 一等人，袭庚是根据邢某的想法研发产品，袭庚、王鹏有参与编写加粉程序，主要是袭庚研发，王鹏跟进。其的获利大概是税后年收入 25 万元。

7.被告人王鹏的供述主要证明：其在公司隶属于研发部，做技术研发工作，公司实际分为瑞智、点智、云某三家公司。其根据指示制作、研发了公司的爬虫程序，在程序出现问题时进行维护，爬虫程序的功能就是通过×××数据爬取流量中的订单信息等内容。×××数据通过清洗运营商流量获得，并保存在 redis 数据库中，爬虫程序就是爬取 redis 数据库中的数据，从流量中清洗×××数据通过 SD 程序完成，SD 程序由王岳编写。爬虫程序的使用者是运维部，负责人是梁修军。公司研发部还根据需要研发了针对不同账号类型的加粉程序，其中抖音、微博、印某、百家号的加粉程序是其编写的，QQ、QQ 部落加粉程序其有进行维护。淘宝加粉程序是袭庚、王某 2 一研发完成，印某加粉程序的破解工作是袭庚做的。通过×××数据完成加粉，账号权利人是不知情的。袭庚是研发部的负责人。其在公司的获利大概是税前年收入 20 万元。

8.非同案犯王某 2 一的供述主要证明：其对瑞智公司、点智公司、云某公司的关系有明确的供述，其参与过公司爬虫程序、加粉程序、破解程序以及监控程序的编写，袭庚、王鹏也有编写加粉程序，加粉通过获取用户的×××数据完成。

9.证人沈某的证言主要证明：其是瑞智公司的财务主管，具体的财务包括瑞智、点智、云某三家公司，公司做自媒体广告业务。

10.证人田某的证言主要证明：其是点智公司员工，点智公司是做精准广告投放的，投放对象是运营商下面的用户，其负责运营商拓展，上级是黄健。

11.证人洪某的证言主要证明：其是点智公司员工，从事运营商拓展项目，上级是黄健。点智公司的业务是做精准广告投放。

12.证人高某的证言主要证明：其是瑞智公司员工，负责对外广告业务接洽，公司业务就是做广告营销。

13.证人黎某的证言主要证明：其有向黄健出租 IP 地址，数量前后共有 1 个 B 段、64 个 C 段，时间是 2017 年 4 月至 2018 年 4 月。2018 年 4 月 18 日，阿某的人在调查其出租的 IP 地址使用情况，其就给黄健报了信，给黄健说了 IP 地址出事的情况，让他赶紧处理。邢某的公司是通过加粉做广告赚钱的，租用大量 IP 地址就是防止同一地址大量登录被封号。黎某与梁修军、黄健、阿某工作人员等人的聊天记录印证了黎某陈述的内容。

14.证人张某 1 的证言主要证明：其在公司经营过程中与邢某的公司存在合作，合作内容一是 QQ 加群，即其公司负责建群，邢某的公司负责加好友，目的是为在群内发淘宝广告，合作 QQ 群数量有 161 个，至 2017 年 9 月 28 日人数添加至 14.7 万余人，中途有衰减（账号权利人发现加入的群在发布广告后退出 QQ 群）后再另行添加的情况，通过添加 QQ 群其支付给邢某公司的利润有 34 万余元（2017 年 5 月至 2018 年 2 月）。二是淘宝加好友，其总共提供了 95 个淘宝号让邢某的公司添加好友，每个账号要求是添加 1000-2000 个好友，这一块邢某公司负责操作的人是梁修军。三是抖音加粉，其是跟周嘉林联系的，其提供了 8 个抖音账号，一个账号加粉一万到十几万不等。张某 1 提供的 QQ 群主账号、QQ 群列表、抖音号列表、淘宝账号列表、合同文本、邮件截图印证了其证言陈述的内容，合同与点智公司签订。

15.证人鹿明的证言主要证明：其是中国联合网络通信有限公司河南省分公司大数据运营中心的产品经理，点智公司与其所在公司曾经有过精准广告投放的合作。

16.证人蒋某的证言主要证明：其是中国电信股份有限公司浙江号百信息分公司信息传媒室的部门经理。云某公司与其所在公司存在合作，合作项目是精准广告投放。根据双方的

协议，云某公司不应该有其所在公司的服务器管理权限。根据双方的保密协议，云某公司不得将数据向第三方或存储介质输出，不得向第三方提供接口。在合作过程中，云某公司不能获取其所在公司的流量信息，数据不能出平台，不能作其他使用。中国电信股份有限公司浙江分公司与云某公司签订的合同文本、保密协议印证了蒋某陈述的事实，云某公司无权下载、留存平台的信息数据，无权将数据作合作项目外的其他用途。

17.证人毋某的证言主要证明：其是号百信息服务有限公司河南省分公司的主管，负责互联网广告业务。点智公司曾经通过北京智云在线科技有限公司、北京中云科创技术有限公司与其所在公司存在合作，项目是互联网广告营销。北京智云在线科技有限公司、北京中云科创技术有限公司使用公司的流量数据仅限于营销平台操作，不能作他用，不能再授权给点智公司使用。毋某提供的合同文本印证了其所在公司与北京中云科创技术有限公司、北京智云在线科技有限公司合作的情况，合同约定北京中云科创技术有限公司、北京智云在线科技有限公司在合作中从号百信息服务有限公司河南省分公司获取的信息不能向第三方披露，不得将信息用于合同约定事项以外的用途，不能对保密信息进行存留。

18.证人陈某的证言主要证明：其是中国电信公司海南分公司创新产品运营中心总经理助理，云某公司跟其公司集团的号百有过业务合作，合作项目就是精准广告投放，合作中云某公司是做平台的软、硬件支撑。合作合同中有明确海南电信服务器上的用户流量不得擅自使用，不得向第三方披露，并采取保密措施。

19.被害人李某 1、王某 1、伍某、董某 1、董某 2 的陈述及淘宝账号信息截图主要证明：几人均居住于绍兴市越城区，其几人的淘宝账号均莫名被添加了好友，部分人员还收到了广告推送。

20.合同文本主要证明：点智公司、瑞智公司、云某公司与运营商签订合作协议、与广告商签订广告发布协议的情况。合同文本中有对信息数据使用权限的约定。点智公司、瑞智公司、云某公司系关联公司，云某公司为瑞智公司提供数据服务，完成数据采集及清洗，每天提供数据量不得少于 10W 条，数据延时不得超过 10 分钟。

21.供应商、运营商列表主要证明：与点智公司、瑞智公司、云某公司存在业务合作的运营商、供应商情况，数量巨大。列表资料由公司财务主管沈某提供。

22.聊天记录主要证明：周嘉林、裘庚与公司员工张某 2 妮的 QQ 聊天记录反映了公司的加粉业务。

23.扣押决定书、扣押清单主要证明公安民警在案件调查中从黄健处扣押了手机 2 部、电脑主机 1 台，从周嘉林处扣押了手机 6 部、电脑硬盘 2 个、U 盘 1 个、电脑主机 1 台，从梁修军处扣押了手机 1 部、电脑 1 台，从王鹏处扣押了手机 1 部、电脑 1 台，从石炳瑞处扣押了手机 1 部、电脑 1 台，从王岳处扣押了手机 1 部、电脑 1 台，从田某处扣押了电脑 1 台，从黎某处扣押了手机 1 部、电脑 1 台，从沈某处扣押了瑞智公司签订的合同文本 40 份、点智公司签订的合同文本 10 份、云某公司签订的合同文本 4 份。

24.电子证据检查笔录、现场勘验检查笔录主要证明：公安民警对涉案周嘉林、石炳瑞、梁修军、王岳、王鹏的电脑进行检查的情况，周嘉林电脑中保存的电子邮件记载的内容、聊天记录、加粉数据统计、公司业绩月报表明细等能够印证审理查明的事实。

25.司法鉴定意见书主要证明：公安机关在案件侦查中委托福建中证司法鉴定中心对从王鹏电脑中提取的程序进行了功能鉴定。通过安装 setup.py、setup_conf.py 文件可以实现对指定网卡网络传输流量进行监控，并保存网络传输流量数据包和日志文件；sd 文件运行后可以实现对指定网卡网络传输流量数据包进行获取并解析的功能；tshark_fields.py 文件运行后可以从指定网卡网络传输流量数据包中筛选出需要的数据包；JDColl.py、TaoColl.py 文件运行后可以绕过系统保护措施，通过匹配×××信息从筛选后的数据包中分别提取出京东、淘宝用户信息、订单信息等数据；douyin.py 文件运行后会调用 test 函数，之后通过调用

douyin_addfans、douyin_like 函数实现绕过系统保护措施获取用户信息，并对指定的“抖音”账号进行粉丝添加及点赞操作；baijia_addfans.py 文件运行后会调用 baijia_addfans 函数实现绕过系统保护措施获取用户信息，并对指定“百家号”账号进行添加粉丝操作；server.py 文件运行后会调用 GET、POST 函数监听 app 发起的 http 请求，prepare.py 文件运行后会调用 fill_data 等函数获取数据并整理请求数据，send.py 文件运行后会将请求数据进行发送从而实现绕过系统保护措施获取用户信息，并对指定淘宝账号添加好友的操作；qq_fans_public_new.py 文件运行后会调用 qq_add_fans 函数实现绕过系统保护措施获取用户信息，并对指定 QQ 账号进行好友添加的操作。

26.公司业绩月报表明细、费用结算清单主要证明：经被告人周嘉林签字确认，瑞智公司 2017 年 1 月收入 1694668 元，2 月收入 2911603 元，3 月收入 3262059 元，4 月收入 2387492 元，5 月收入 2060552 元，6 月收入 1645449 元，7 月收入 1678695 元，8 月收入 1942627 元，9 月收入 1865450 元，10 月收入 1295426 元，11 月收入 2592503 元，12 月收入 2097139 元。其中 2017 年 10 月至 2018 年 1 月的微信小号广告净获利超过 170 万元。上述数据保存于周嘉林被扣押的电脑中。瑞智公司与云某公司之间在 2016 年 1-10 月的业务结算金额为 300 余万元。

27.微博加粉数据统计表主要证明经被告人周嘉林签字确认，被告人石炳瑞统计的 2018 年 1 月的微博加粉数量远超 700 万条。该数据保存于周嘉林被扣押的电脑中。

28.情况说明、订单数据说明及电子信息数据主要证明：经浙江淘宝网络有限公司排查，2018 年 4 月 17 日李某 1 账号被多个 IP 地址爬取多条订单信息，订单信息内容包括商品名称、价格、金额、收货地址、收货人姓名、手机号码等。公安机关提供的 IP 地址号段爬取订单信息的最晚时间为 2018 年 4 月 18 日，2018 年 4 月 17 日之前的流量已过期，通过技术手段已找到 2018 年 4 月 17-18 日两天的数据，2018 年 4 月 16-18 日共计爬取淘宝订单信息 220552 条，浙江淘宝网络有限公司实际输出数据明细 10000 条。公安机关提供的淘宝账号共计恶意添加好友 137096 条，浙江淘宝网络有限公司实际输出数据明细 20000 条。

29.情况说明、询问笔录、立案决定书、拘留证、起诉意见书主要证明：被告人周嘉林在案发后揭发检举他人容留吸毒犯罪事实的立功表现情况，其对贩毒事实提供的线索极其有限。

30.讯问笔录、到案经过、电话录音、聊天记录主要证明：被告人黄健规劝非同案犯王某 2 一投案自首的情况。

31.抓获经过证实了各被告人的到案情况。

32.营业执照、授权委托书、身份证复印件、户籍证明证实了被告单位的基本信息及被告人、诉讼代表人的身份情况。

本院认为，被告单位北京瑞智华胜科技股份有限公司违反国家规定，采用技术手段获取国家事务、国防建设、尖端科学技术领域以外的计算机信息系统中存储、传输、处理的数据，情节特别严重，被告人周嘉林、黄健、梁修军、石炳瑞、裘庚、王岳、王鹏系被告单位直接负责上述行为的主管人员或直接责任人员，其行为均已构成非法获取计算机信息系统数据罪，且系共同犯罪。公诉机关指控的罪名成立，本院予以支持。在本案事实中，被告单位及其关联公司对数据的采集、保存、调取、使用系一个完成的犯罪行为链，数据的采集、保存行为系超越授权的操作，且直接服务于后续的数据非法使用，应认定为具有刑事违法性，被告人周嘉林的辩护人就此提出的否定意见，本院不予采纳。综合被告单位经营的时间、行为的影响范围及恶劣程度、已查证获取的身份认证信息的数量、数据的违法使用情况以及非法获利情况，足以认定被告单位及被告人的行为已达到“情节特别严重”程度，被告人周嘉林的辩护人就此提出的否定意见，本院不予采纳。被告人周嘉林、黄健在共同犯罪中起主要作用，依法以主犯对二被告人予以量刑处罚。被告人梁修军、石炳瑞、裘庚、王岳、王鹏在共

同犯罪中起次要、辅助作用，依法以从犯对五被告人减轻处罚。被告人周嘉林在案发后揭发检举他人的一般犯罪行为，经查证属实；被告人黄健规劝非同案犯投案自首，均可依法认定为立功表现，据此对二被告人予以从轻处罚。被告人黄健、梁修军、石炳瑞、裘庚、王岳、王鹏在审查起诉阶段已签字具结、认罪认罚，被告人周嘉林在庭审中对起诉指控事实供认不讳，亦表示认罪认罚，各被告人均系初犯，据此依法对各被告人予以从轻处罚。各被告人及辩护人根据被告人具有的上述从轻处罚情节，分别请求从轻处罚的意见，本院均视情予以采纳。辩护人提出认定被告人黄健在共同犯罪中属从犯的意见与被告人黄健的股东身份、在被告单位承担的管理职责以及获取运营商服务器登录权限对涉案行为危害后果产生的作用不相适应，本院不予采纳。根据被告人裘庚、王岳、王鹏的犯罪情节及悔罪表现，本院依法对三被告人适用缓刑。公诉机关提出的量刑建议适当，本院予以采纳。被告人黄健及被告人周嘉林、黄健的辩护人请求适用缓刑的意见与二被告人的犯罪情节不符，本院均不予采纳。依照《中华人民共和国刑法》第二百八十五条第二、四款、第三十条、第三十一条、第二十五条第一款、第二十六条第一、四款、第二十七条、第六十七条第三款、第六十八条、第七十二条第一、三款、第六十四条，《中华人民共和国刑事诉讼法》第十五条、第二百零一条之规定，判决如下：

一、被告单位北京瑞智华胜科技股份有限公司犯非法获取计算机信息系统数据罪，判处罚金人民币一千万元（罚金在本判决生效后三十日内缴纳）；

二、被告人周嘉林犯非法获取计算机信息系统数据罪，判处有期徒刑三年六个月，并处罚金人民币十万元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日。罚金在本判决生效后十日内缴纳）；

三、被告人黄健犯非法获取计算机信息系统数据罪，判处有期徒刑三年二个月，并处罚金人民币十万元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日。罚金在本判决生效后即时缴纳）；

四、被告人梁修军犯非法获取计算机信息系统数据罪，判处有期徒刑二年八个月，并处罚金人民币六万元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日。罚金在本判决生效后即时缴纳）；

五、被告人石炳瑞犯非法获取计算机信息系统数据罪，判处有期徒刑二年六个月，并处罚金人民币六万元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日。罚金在本判决生效后即时缴纳）；

六、被告人裘庚犯非法获取计算机信息系统数据罪，判处有期徒刑二年四个月，缓刑三年，并处罚金人民币六万元（缓刑考验期从判决确定之日起计算；罚金在本判决生效后即时缴纳）；

七、被告人王岳犯非法获取计算机信息系统数据罪，判处有期徒刑二年，缓刑二年六个月，并处罚金人民币六万元（缓刑考验期从判决确定之日起计算；罚金在本判决生效后即时缴纳）；

八、被告人王鹏犯非法获取计算机信息系统数据罪，判处有期徒刑二年，缓刑二年六个月，并处罚金人民币六万元（缓刑考验期从判决确定之日起计算；罚金在本判决生效后即时缴纳）；

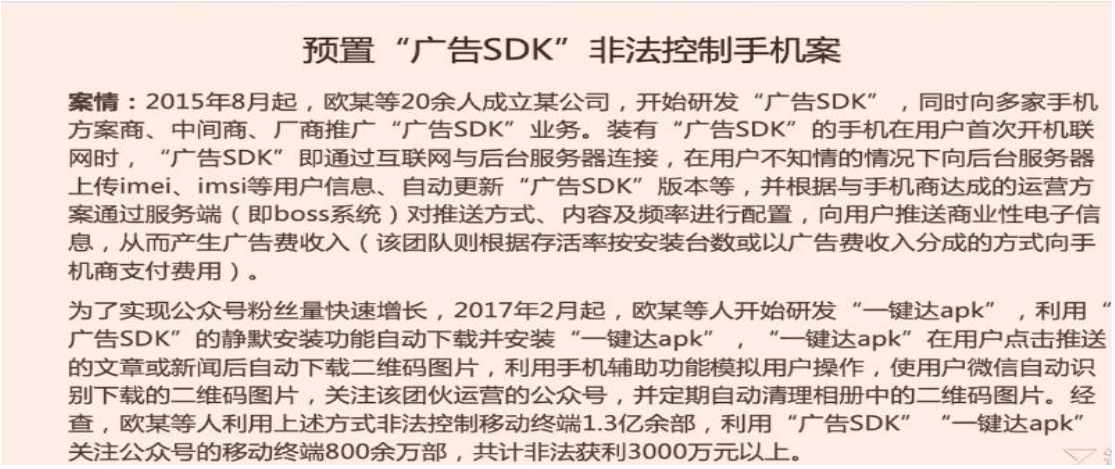
九、从本案被告人处扣押的手机、电脑、电脑硬盘、电脑主机、U盘（均暂存于绍兴市公安局越城区分局）均予以没收，从非本案被告人处扣押的电脑、手机由扣押机关依法处理；非法获利继续予以追缴。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向浙江省绍兴市中级人民法院提出上诉，书面上诉的，应当提交上诉状正本一份，副本二份。

审　判　长　　张　毅

人民陪审员　　章定安
人民陪审员　　周红英
二〇一九年十月二十八日
书　记　员　　陈雨燕

4.2019 年度浙江省互联网十大检察案例之一：预置“广告 SDK”非法控制手机案--欧建宏等人非法控制计算机信息系统案（平湖市人民检察院）



2019 年 1 月，平湖市人民法院对我省首例预置“广告 SDK”非法弹送广告案进行了判决。28 名被告人组成的团伙通过与手机方案商、手机厂商相互勾结，在销售手机内预置“广告 SDK”，在未经用户允许情况下，向用户推送信息并静默下载“一键达 apk”,模拟用户操作关注微信公众号，共计非法控制用户手机上亿台、违法所得 3000 万。本案系新型计算机领域案件，检察机关特邀网安业务骨干分析研判案情，并申请专家证人出庭作证，通过多媒体直观展现“弹送广告”的危害性，成功指控犯罪。此案明确了预装方式下“非法控制”的法律定性，对非法弹送广告、静默下载等互联网黑灰产业链予以打击，对今后该领域案件的处理具有指导意义，同时促进行业整改、净化行业领域，社会效果良好。

附：欧建宏、陈言敏、宋瑞等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一审刑事判决书

浙江省平湖市人民法院
刑 事 判 决 书
（2018）浙 0482 刑初 574 号

公诉机关平湖市人民检察院。

被告人欧建宏，曾用名徐建鸿，男，1981 年 7 月 2 日生，汉族，出生地湖南省衡阳市，硕士研究生，原系上海朗趣软件科技有限公司（以下简称朗趣公司）COO（运营总监），户籍地北京市朝阳区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕。现羁押于平湖市看守所。

辩护人楼伯坤，北京大成（杭州）律师事务所律师。

辩护人李彤，北京德和衡律师事务所律师。

被告人陈言敏，男，1982 年 9 月 15 日生，汉族，出生地浙江省瑞安市，硕士研究生，原系朗趣公司研发部负责人，户籍地北京市朝阳区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕。现羁押于平湖市看守所。

辩护人刘玲，北京德和衡律师事务所律师。

被告人宋瑞，男，1983 年 12 月 28 日生，汉族，出生地北京市通县，大学文化，原系朗趣公司项目部负责人，户籍地北京市通州区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕。现羁押于平湖市看守所。

辩护人杨琢孔，北京德和衡律师事务所律师。

被告人孟宪巍，男，1983 年 8 月 18 日生，汉族，出生地辽宁省朝阳市，硕士研究生，原系朗趣公司员工，户籍地北京市朝阳区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕。现羁押于平湖市看守所。

辩护人戚海燕，浙江天卓律师事务所律师。

被告人任友松，男，1974 年 8 月 18 日生，汉族，出生地安徽省无为县，大学文化，原系朗趣公司员工，户籍地安徽省芜湖市无为县。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕。现羁押于平湖市看守所。

辩护人张曙、王剑洪，浙江靖霖律师事务所律师。

被告人周飞，男，1985 年 1 月 23 日生，汉族，出生地北京市朝阳区，大学文化，原系朗趣公司员工，户籍地北京市朝阳区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕。现羁押于平湖市看守所。

辩护人夏建，浙江平行律师事务所律师。

被告人邹琪，男，1992 年 9 月 20 日生，汉族，出生地湖南省新化县，大学文化，原系朗趣公司员工，户籍地湖南省新化县。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕。现羁押于平湖市看守所。

辩护人史明生、肖锦辉，上海明生律师事务所律师。

被告人吕涛，男，1978 年 11 月 2 日生，汉族，出生地辽宁省兴城市，大学文化，原系朗趣公司产品运营部负责人，户籍地辽宁省兴城市,暂住北京市海淀区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同月 30 日转取保候审。经本院决定，于 2018 年 9 月 29 日取保候审。

指定辩护人沈婷婷，浙江平行律师事务所律师。

被告人刘鹏，男，1982 年 4 月 22 日生，汉族，出生地山东省齐河县，大学文化，原系朗趣公司商务部负责人，户籍地北京市大兴区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 28 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人罗丹，浙江浙平律师事务所律师。

被告人颜琦，男，1986 年 9 月 23 日生，汉族，出生地陕西省富平县，大学文化，原系北京瑞徕科技有限公司（以下简称瑞徕公司）新媒体部负责人，户籍地陕西省富平县，暂住北京市丰台区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 7 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人付德欢，北京德和衡律师事务所律师。

被告人赖宜练，男，1983 年 7 月 27 日生，汉族，出生地广东省连平县，大学文化，原系深圳市鼎勤通讯有限公司（以下简称鼎勤公司）软件经理，户籍地广东省深圳市南山区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 29 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人金耀，浙江浙平律师事务所律师。

被告人罗轶先，男，1979 年 2 月 10 日生，汉族，出生地湖南省茶陵县，硕士研究生，原系深圳智汇云商科技有限公司（以下简称智汇云商公司）副总经理，户籍地上海市闵行区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 29 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人田芳，北京盈科（上海）律师事务所律师。

被告人李铭岳，男，1981 年 4 月 3 日生，汉族，出生地山东省泰安市，大学文化，原系智汇云商公司软件工程师，户籍地上海市闵行区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 29 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人陈晓薇，北京盈科（上海）律师事务所律师。

被告人张振兴，男，1984 年 3 月 17 日生，汉族，出生地湖南省平江县，大学文化，原系朗趣公司员工，户籍地广东省深圳市龙华新区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 21 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人江文峰，北京市盈科（深圳）律师事务所律师。

辩护人沈潮赟，浙江广诚律师事务所律师。

被告人刘小军，男，1984 年 5 月 18 日生，汉族，出生地江西省南丰县，大专文化，原系朗趣公司员工，户籍地江西省南丰县，暂住广东省深圳市宝安区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 20 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人顾海峰，浙江子城律师事务所律师。

被告人李仁平，曾用名李任平，男，1987 年 9 月 4 日生，汉族，出生地四川省阆中市，大专文化，原系朗趣公司员工，户籍地四川省阆中市，暂住广东省深圳市龙岗区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 19 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人钱益波、赵全，浙江子城律师事务所律师。

被告人张刚，男，1978 年 10 月 29 日生，汉族，出生地上海市南汇区，大学文化，原系朗趣公司员工，户籍地上海市浦东新区。因本案，于 2017 年 10 月 1 日被平湖市公安局刑事拘留，同年 11 月 4 日转取保候审。经本院决定，于 2018 年 11 月 3 日取保候审。

被告人廖天一，男，1992 年 3 月 4 日生，汉族，出生地湖南省宁乡县，大学文化，原系朗趣公司员工，户籍地湖南省宁乡县，暂住北京市昌平区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 28 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人杨晓雷，浙江天卓律师事务所律师。

被告人刘寸霞，女，1983 年 6 月 1 日生，汉族，出生地河北省高邑县，大学文化，原系朗趣公司员工，户籍地河北省石家庄市高邑县。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 7 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人林红依，浙江泽大（平湖）律师事务所律师。

被告人周雷，男，1990 年 8 月 2 日生，汉族，出生地山东省济阳县，大学文化，原系朗趣公司员工，户籍地山东省济阳县。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日转取保候审。经本院决定，于 2018 年 11 月 3 日取保候审。

辩护人戴锦跃，浙江浙平律师事务所律师。

被告人兰雪玲，女，1985 年 10 月 15 日生，汉族，出生地湖北省郧县，大学文化，原系朗趣公司员工，户籍地天津市津**，暂住北京市昌平区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 7 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人张荣发，浙江天鸿律师事务所律师。

被告人张明伟，男，1993 年 1 月 14 日生，汉族，出生地河北省迁安市，大学文化，原系朗趣公司员工，户籍地河北省迁安市。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日转取保候审。经本院决定，于 2018 年 11 月 3 日取保候审。

辩护人贾致瑜，北京安理（天津）律师事务所律师。

被告人蔡鹏，男，1991 年 12 月 3 日生，汉族，出生地山东省乐陵市，大学文化，原系朗趣公司员工，户籍地山东省德州市乐陵市。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 28 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人邱香珠，浙江东港律师事务所律师。

被告人李晓蒙，女，1990 年 4 月 24 日生，汉族，出生地河北省清河县，大学文化，原系朗趣公司员工，户籍地河北省邢台市清河县，暂住北京市朝阳区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日转取保候审。经本院决定，于 2018 年 11 月 3 日取保候审。

辩护人李越明，浙江天鸿律师事务所律师。

被告人何娟凤，女，1990 年 12 月 2 日生，汉族，出生地江西省贵溪市，大学文化，原系朗趣公司员工，户籍地江西省贵溪市。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 9 月 30 日转取保候审。经本院决定，于 2018 年 9 月 29 日取保候审。

被告人张皓然，男，1994 年 10 月 26 日生，汉族，出生地江西省丰城市，大学文化，原系朗趣公司员工，户籍地广东省深圳市南山区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 21 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人袁昕炜，浙江金道律师事务所律师。

被告人白雪卿，男，1990 年 8 月 6 日生，汉族，出生地河北省河间市，大专文化，原系朗趣公司员工，户籍地湖南省冷水江市。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 19 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

辩护人冯王，浙江泽大（平湖）律师事务所律师。

被告人韩明明，男，1996 年 7 月 8 日生，汉族，出生地安徽省临泉县，大学文化，原系朗趣公司员工，户籍地安徽省临泉县，暂住北京市昌平区。因本案，于 2017 年 9 月 28 日被平湖市公安局刑事拘留，同年 11 月 4 日被依法逮捕，同年 12 月 20 日转取保候审。经本院决定，于 2018 年 11 月 27 日取保候审。

平湖市人民检察院以平检公诉刑诉[2017]572 号起诉书指控被告人欧建宏、陈言敏、宋瑞、孟宪巍、任友松、周飞、邹琪、吕涛、刘鹏、颜琦、赖宜练、罗轶先、李铭岳、张振兴、刘小军、李仁平、张刚、廖天一、刘寸霞、周雷、兰雪玲、张明伟、蔡鹏、李晓蒙、何娟凤、张皓然、白雪卿、韩明明犯非法控制计算机信息系统罪，于 2018 年 7 月 31 日向本院提起公诉。本院于同日受理，依法适用普通程序，组成合议庭，公开开庭审理了本案。在审理期间，公诉机关以补充侦查为由，建议我院延期审理，本院于 2018 年 10 月 29 日决定延期审理，并于同年 11 月 20 日恢复审理。平湖市人民检察院指派检察员向鸣霞出庭支持公诉，被告人欧建宏、陈言敏、宋瑞、孟宪巍、任友松、周飞、邹琪、吕涛、刘鹏、颜琦、赖宜练、罗轶先、李铭岳、张振兴、刘小军、李仁平、张刚、廖天一、刘寸霞、周雷、兰雪玲、张明伟、蔡鹏、李晓蒙、何娟凤、张皓然、白雪卿、韩明明，辩护人楼伯坤、李彤、刘玲、杨琢孔、戚海燕、张曙、王剑洪、夏建、史明生、肖锦辉、沈婷婷、罗丹、付德欢、金耀、田芳、陈晓薇、江文峰、沈潮赟、顾海峰、钱益波、赵全、杨晓雷、林红依、戴锦跃、张荣发、贾致瑜、邱香珠、李越明、袁昕炜、冯王以及证人陈某、梁某，鉴定人员陆某到庭参加诉讼。

现已审理终结。

平湖市人民检察院指控：被告人欧建宏、陈言敏、宋瑞、孟宪巍、任友松、周飞、邹琪、吕涛、刘鹏、颜琦、赖宜练、罗轶先、李铭岳、张振兴、刘小军、李仁平、张刚、廖天一、刘寸霞、周雷、兰雪玲、张明伟、蔡鹏、李晓蒙、何娟凤、张皓然、白雪卿、韩明明违反国家规定，采用技术手段，非法控制计算机信息系统，属情节特别严重，应当以非法控制计算机信息系统罪共同犯罪追究刑事责任。在共同犯罪中，被告人欧建宏起主要作用，系主犯；其余被告人起次要作用，系从犯，依法应当从轻或减轻处罚。为证实指控的犯罪事实，公诉机关当庭提供了受案登记表、被害人陈述、证人证言、辨认笔录、搜查笔录、扣押笔录、扣押清单及照片、司法鉴定意见书、现场勘验检查笔录，远程勘验工作记录、网络在线提取工作记录、电子证据远程勘察、检查笔录等电子数据，银行查询信息、工商查询信息、协助冻结通知书回执、情况说明、违法犯罪经历查询证明、身份证明等证据，诉请本院予以惩处。

被告人欧建宏辩称：1、对起诉书指控的犯罪事实有异议，认为起诉书上关于其及团队加入朗趣公司的时间、广告 SDK 的研发时间、2017 年 8 月集体从朗趣公司离职加入瑞徕公司以及有关一键达 apk 的指控均与事实不符。2、对指控其利用广告 SDK 非法控制他人手机有异议，原因如下：（1）并非没有授权或超越授权，广告 SDK 是桌面功能，不是独立的产品，不能独立运行，是手机厂商集成到桌面应用程序里去的，已通过手机商的购机协议以及用户使用时的许可协议完成了对用户的告知，朗趣公司作为工具提供方与手机厂商签订了合同，获得了手机厂商的授权，推送广告之前，也获得了厂商确认和允许；（2）广告 SDK 不控制桌面本身，广告可以不运营，可以关闭；（3）静默安装不代表用户不知情，是用户看到广告点击后发起的安装，手机厂商授予了广告 SDK 静默安装权限，但用得很少；（4）自动更新数据、替换数据是应用软件的基本功能，是桌面内部数据更新，不属于控制行为，且有升级提示，需要用户确认；（5）一键达 apk 是由用户自主安装，使用该软件时用户同意授予辅助功能才会行使之后的自动关注功能。3、对指控的各项数据及金额有异议，广告 SDK 的获利金额未扣除合法收入的金额，控制手机的数量没有区分桌面业务的用户、白名单、没存活以及双卡双待重复计算的数量，关注公众号的移动终端数与广告 SDK 用户是重合的，且没有扣除倍儿赚的用户数和主动关注的用户数。4、本案系单位行为，是公司的业务决策，其不是主犯，广告 SDK 业务由公司董事、CEO 决策，其只负责落实，与鼎勤、智汇云商前期谈合作的部分其未参与。5、朗趣公司有 1 个多亿的用户数，广告 SDK 业务只占朗趣公司业务的一小部分，广告 SDK 业务的用户数只占其中一小部分；朗趣公司与手机厂商并非合谋，而是业务合作。

被告人欧建宏的辩护人提出本案事实不清、证据不足、定性不当，现有证据不能证明被告人欧建宏的行为构成非法控制计算机信息系统罪，起诉书指控被告人欧建宏的罪名不能成立。理由如下：1、本案起诉书依赖的事实形成过程不符合法律规定，本案两次立案违反刑事诉讼法的规定，无侦查权的嘉兴市公安局港区分局获取的证据材料不能作为定案依据；司法鉴定意见书因委托机关无侦查权、鉴定主体不适格、结论不明确、鉴定结论不客观、结论与鉴定过程中检材文件的分析和提取内容不符、资料来源不可靠、检材不具有代表性等原因不能作为本案证据。2、本案认定事实错误：（1）起诉书叙述的部分事实有误，混淆了行为人行为之间的逻辑关系。指控被告人欧建宏等人于 2015 年 8 月加入朗趣公司，成立北京团队后开始研发并推广广告 SDK 与事实不符，广告 SDK 是朗趣公司原先广告项目的延续；广告 SDK 不是独立的手机应用程序，不能独立运行，由手机方案商修改自身的桌面 APP 将广告 SDK 集成进去，成为具有广告推送功能的桌面 APP，集成以及后续的手机生产、销售、推广均由手机厂商完成，取得用户的允许是手机方案商的义务；朗趣公司是被动地基于手机方案商的要求和技术方案提供半成品代码、测试服务及按要求进行配置，整个过程方案商是主导；关于一键达 apk 的指控与事实不符。（2）起诉书对数据统计的依据与事实不符，远

勘报告没有区分产品、业务、双卡双待、白名单等情况，只汇总了总数，新媒体业务中没有区别主动关注的部分。3、对被告人欧建宏行为的性质认定错误，不构成非法控制计算机信息系统罪：（1）本案没有《刑法》第十三条规定的社会危害性情形；（2）被告人欧建宏的行为不符合指控罪名的构成要件：没有违反国家规定，主观上也没有犯罪故意，没有对用户手机造成“非法控制”，本罪保护的客体，即“计算机信息系统”没有受到侵犯。4、本案是朗趣公司的单位行为，不是共同犯罪行为，在当前没有足够证据证明相关单位构成犯罪的情况下，被告人欧建宏应当被宣告无罪；在确定相关单位构成犯罪的情况下，应当由公诉机关查明情况后补充起诉，若公诉机关不增加起诉，根据法律规定追究直接负责的主管人员和其他直接责任人员的刑事责任，且应在朗趣公司、鼎勤公司、智汇云商公司之间以对用户手机控制的作用和行为来区分主从犯。5、被告人欧建宏对一键达 apk 的研发不知情，且微信调用辅助功能的技术不是非法控制，对一键达 apk 功能的指控缺乏证据，没有被害人指控，没有实际关注行为的记录，属证据不足。6、被告人欧建宏系初犯、偶犯，到案后如实供述，属于有坦白情节，且其具有自愿认罪认罚的从轻量刑情节。

被告人陈言敏对起诉书指控的犯罪事实基本无异议，愿意认罪服法，辩称其是技术人员，服从公司的工作安排，广告 SDK 的预装、控制手机的数量、广告是否运营、运营方式及频率其均不清楚，技术人员不应当承担主要责任，手机商责任更大，请求法院考虑其在全案中的地位、作用、决策权大小、获利大小；其还提出司法鉴定意见书缺乏合法性、专业性，没有结论，具有很强的倾向性、诱导性，应不予采纳；用户许可桌面联网即许可广告 SDK 联网，手机商已通过用户协议告知用户，故广告 SDK 不属于没有授权或超越授权。

被告人陈言敏的辩护人认为本案事实不清，证据不足，不应以犯罪论处。理由如下：1、指控的行为不属于控制；2、计算机信息系统应当指是操作系统，广告 SDK 是一个应用软件，不属于计算机信息系统；广告展示功能没有突破或避开手机安全系统，不需要授权，手机用户在购买手机、开机同意使用协议时就已经同意授予广告 SDK 联网和读取手机信息的权限，且广告 SDK 行使的是程序运行权，而不是系统控制权，不符合司法解释对控制的定义；3、利用广告 SDK 推送广告不具有非法性，预装软件是手机厂商的权限，广告 SDK 并没有非法侵入手机的行为，没有获取用户敏感信息，弹出的广告也符合广告法的要求；4、司法鉴定意见书不能作为本案的定案依据；5、本案若构成犯罪，应当认定为单位犯罪，其中朗趣公司起次要作用，应当按利润分成比例区分主从犯；6、若被告人陈言敏罪名成立，鉴于其所起的作用和在本案中的地位，以及其主观上没有犯罪故意，没有直接的、重大的社会危害后果，有坦白情节，又系初犯、偶犯等情况，建议对其从轻或减轻处罚并适用缓刑。

被告人宋瑞辩称其是履行职务，人事关系被北京网秦天下科技有限公司（以下简称网秦公司）强制转到朗趣公司，又服从安排转入瑞徕公司；不清楚广告 SDK 研发时间，其接触到广告 SDK 是 2016 年下半年，之前一直负责桌面和主题商店；其无主观恶意，行业竞争大，无明确行业规则，网秦公司是上市公司，使其无法预见其行为的犯罪可能性；其实质上属于客服人员，无技术能力和决策权力，对起诉书指控其是项目部负责人有异议，其属于商务部中负责项目的人员。

被告人宋瑞的辩护人认为被告人宋瑞不构成犯罪，广告 SDK 虽给用户带来不良体验，但区别于木马病毒、黑客，不具有明显的社会危害性和刑事违法性；并提出鉴定机构不具备鉴定资质，委托事项超出了鉴定机构的鉴定能力和业务范围，具有引导性和暗示性，司法鉴定意见书不能成为本案定案依据，工信部回函能证明广告 SDK 不是恶意程序；使用白名单、静默期和静默安装不是规避行为，而是为了减少用户的不良体验，不能以此认定被告人的主观故意；对起诉书指控被告人宋瑞系项目部负责人有异议，与事实不符，被告人宋瑞参与程度小，其工作相当于客服人员，无技术含量和商业贡献；本案系单位行为，若认定为犯罪，朗趣公司作用、地位较轻，系从犯；被告人宋瑞有坦白情节。综上，请求认定被告人宋瑞无

罪，若认定有罪，对其免予处罚或减轻处罚并适用缓刑。

被告人孟宪巍对起诉书指控的部分事实有异议，其并不是与欧建宏等人一起加入的朗趣公司；加入瑞徕公司是被捕前一个月左右，被捕前的主要工作是与网秦公司做交接，离职还没有实际完成；其不是服务端的负责人，是服务端统计组的组长；对指控的 imei 数、imsi 数及 9 月 26 日当日的数据均有异议；对指控的收入金额有异议，有部分收入与广告 SDK 无关，可能包含其他产品的收入；广告 SDK 上传用户信息目的是用于统计，无主观恶意。

被告人孟宪巍的辩护人认为本案事实不清、证据不足，统计数据有误，没有区分合法和非法，司法鉴定意见书不能作为定案依据；被告人孟宪巍在本案中是履职行为，不是服务端负责人，没有非法获利，无主观犯罪故意；获利方是公司，应当属于单位犯罪，被告人孟宪巍的作用较小，建议对其免予刑事处罚。

被告人任友松辩称研发广告 SDK 的时间是 2015 年年底；其负责广告 SDK 的主线研发、维护、升级，是从 2017 年 5 月份才开始的，时间比较短；广告 SDK 联网后用户信息的交换、自动更新不属于控制，均是软件的基本功能；其工作是公司安排的，网秦公司也有责任；其没有意识到是犯罪，其工作的部分不涉及控制；其是初犯。

被告人任友松的辩护人提出：首先，涉案的广告 SDK 未侵犯到信息网络安全的法益，并非属于非法控制行为，被告人不应承担本罪的法律后果；其次，本案若认定犯罪，应当是单位犯罪，且朗趣公司应当为从犯，被告人任友松不是直接负责的主管人员或其他直接责任人员，不应承担刑事责任；第三，对指控的控制手机数量、犯罪金额均有异议，证据不足，计算方法存疑，没有区分双卡双待、海外业务及其他合法业务；第四，被告人任友松对一键达 apk 不知情；最后，被告人任友松在开发广告 SDK 过程中起辅助作用，其设计的开屏广告对于控制行为没有决定性作用，系初犯，有坦白情节。综上，请求对被告人任友松减轻处罚并适用缓刑。

被告人周飞对起诉书指控的罪名无异议，辩称北京团队在网秦公司早已存在，主要做桌面、主题商店；广告 SDK 是在 2016 年上半年才陆续开始研发测试，其工作从 2016 年下半年才开始往广告 SDK 上转移，其只是测试人员；被告人张皓然不是测试组的人员，主要服务于项目组，被告人张皓然现场测试时其只是技术辅助；广告 SDK 需要集成，不能独立运行，手机商有集成权和运营权，告知用户是软件制造商的责任；其测试过程中要关注安装了广告 SDK 后手机的功能、稳定性是否受影响，目的是为了确保手机能正常运行；手机商不止集成一种广告 SDK，手机用户体验差并不是朗趣公司导致的；弹广告是行业内常见的现象；其通过正规途径应聘入职，履行公司指令。

被告人周飞的辩护人对起诉书指控的罪名无异议，提出本案系单位犯罪，广告 SDK 是公司高层决策，建议法庭对被告人周飞的量刑与其他被告人一致；被告人周飞系从犯，应当减轻处罚，其不负责主线测试，不是测试组负责人；其情节较轻，主观恶性小，社会危害性不大，本案不同于木马病毒、黑客类的犯罪；被告人周飞有坦白情节，系初犯、偶犯，建议判处一年半以下有期徒刑并适用缓刑。

被告人邹琪对起诉书指控的犯罪事实及罪名均无异议，辩称其根据公司指令工作，使用的是常规技术手段，广告 SDK 没有超越安卓系统权限，其作为技术人员不知用户是否明知，其是普通员工，地位、作用小；其未参与新媒体业务；广告 SDK 上传用户信息是用于标记用户。

被告人邹琪的辩护人认为被告人邹琪不构成犯罪，即使本案构成犯罪，也属于单位犯罪，被告人邹琪属于底层员工，对其应与其他被告一视同仁，适用刑罚一致；司法鉴定意见书无效，不能作为定案依据；本案主客观不统一，被告人邹琪无主观犯罪故意；被告人邹琪系从犯、初犯、偶犯，情节较轻，无严重后果，社会影响不大，请求对其免予刑事处罚或判处缓刑。

被告人吕涛对起诉书指控的犯罪事实及罪名均无异议，辩称其行为是职务行为，广告SDK是公司高层决策，通过手机商授权；其是产品经理，对产品负责，后期加入了运营工作，不分配研发和测试任务，产品不涉及广告SDK，广告SDK等待被激活，广告策略与桌面业务没区别；司法鉴定意见书无定性结论，恶意软件无行业标准，工信部未检测被害人手机是否有广告SDK；渠道号是公开的，网秦是上市大公司，其信任网秦公司造成认识偏差。

被告人吕涛的辩护人提出本案系单位犯罪，获利金额是否包含合法收入，获取的imei、imsi数是否包含双卡双待及主题商店的数据都存疑；被告人吕涛主观犯罪意图不明，恶性较小，在本案中起次要作用，系从犯，应当从轻或减轻处罚；其有坦白情节，主动认罪，有悔罪表现，系初犯、偶犯，请求对其从轻、减轻处罚并适用缓刑。

被告人刘鹏对起诉书指控的犯罪事实及罪名均无异议，辩称与手机厂商合作系公司决策，商务流程通过公司审批；其入职时间短，因专业限制对广告SDK不了解；其主要工作是维护客户关系，管理商务团队，对一键达apk不知情；从市场和行业环境看，广告SDK业务很常见，其拿固定工资，没有提成，属于打工者。

被告人刘鹏的辩护人提出本案系单位犯罪，被告人刘鹏主要负责管理商务人员和拜访客户，入职晚，工作时间短，不应当作为主管及其他直接责任人员处罚；若认定自然人犯罪，被告人刘鹏系从犯，主观恶性小，犯罪情节较轻，系初犯、偶犯，具有坦白情节，建议免予刑事处罚或从轻处罚并适用缓刑。

被告人颜琦对起诉书指控的犯罪事实及罪名均无异议，辩称其主观上没有犯罪故意。

被告人颜琦的辩护人提出鉴定意见不具代表性，对司法鉴定意见书与待证事项的关联性、客观性有异议，鉴定意见未对鉴定事项给予肯定或明确的回复，一键达apk对手机恶意控制程度未进行单独鉴定；被告人颜琦从事的工作是履行岗位职责，主观恶性小，行为危害性小，系从犯，有坦白情节，系初犯、偶犯，请求从轻或减轻处罚；被告人颜琦身体原因亦不适于羁押，请求对其适用缓刑。

被告人赖宜练自愿认罪，但对起诉书指控的事实有异议，辩称其是鼎勤公司员工，广告SDK业务是两个公司的合作，其是按照公司的要求去跟进、调试，对公司的做法不清楚，广告SDK的权限是桌面给的。

被告人赖宜练的辩护人提出被告人赖宜练是按公司指使履行职务，本案系单位犯罪，被告人赖宜练是普通员工，无决策权，在整个合作过程中只负责技术层面，不负责量产、运营、销售等其他环节；在共同犯罪中，鼎勤公司起次要作用，系从犯；被告人赖宜练主观恶性小，起辅助作用，系从犯，社会危害性小，有坦白情节，系初犯、偶犯，请求对其从轻或减轻处罚并适用缓刑。

被告人罗轶先对起诉书指控的罪名无异议，对指控的犯罪事实部分有异议，一是金额，智汇云商公司跟朗趣公司的合作其中有部分是桌面业务，相关金额应予以扣除，桌面业务虽然停止，但收入存在滞后性；不存在与朗趣公司合谋，只是帮朗趣公司推广产品，2014年有桌面业务，广告SDK的合作时间在2015年8月份之前，8月份已经有预装出货，因此已经有广告SDK的结算，广告SDK是桌面业务的延续，故其对广告SDK认识不清；智汇云商公司是软件代理商，没有硬件的生产和制造，方案商是智汇云商公司的客户，智汇云商公司因广告SDK产生的利润在40—50万元；其对微信业务不知情。

被告人罗轶先的辩护人认为被告人罗轶先所涉行为情节轻微，不构成犯罪，即便本案认定为犯罪，也应当系单位犯罪，并非自然人犯罪，理由如下：1、被告人罗轶先涉案相关情况未达到非法控制计算机信息系统的刑事立案标准，广告SDK未脱离用户控制，未达到非法控制的程度，获取的数据也非用户重要信息，未造成严重后果，不应当认定为犯罪；2、智汇云商公司属于渠道商，在整个案件过程中所起的作用十分有限，公司获利较少，被告人罗轶先未获利；3、本案应当认定为单位犯罪，并非被告人罗轶先个人犯罪，且智汇云商公

司不是主犯，是朗趣公司向智汇云商公司寻求合作；4、被告人罗轶先无主观故意；5、即便本案构成犯罪，被告人罗轶先的情节轻微，起次要作用，系从犯，积极配合公安机关调查，经传唤跟随公安机关至平湖，应依法认定为自首或坦白，其一贯表现良好，无前科。综上，请求对其免予刑事处罚或判处缓刑。

被告人李铭岳对起诉书指控的犯罪事实及罪名均无异议，辩称其无主观恶意，对广告SDK认识较少，无辨别能力；其系普通员工，广告SDK业务系公司决策；其在公司内还有其他工作，在本案中作用较小。

被告人李铭岳的辩护人提出：1、起诉书认定的金额错误，应扣除桌面业务收入以及支付给深圳市沃特沃德股份有限公司（以下简称沃特沃德公司）的金额；2、本案系单位犯罪，被告人李铭岳作为普通员工，不应被追究刑事责任；3、即便被告人李铭岳被认定为犯罪，其作用地位较小，系从犯，情节轻微，没有获利，又有坦白情节，请求对其免予刑事处罚或免予罚金处罚。

被告人张振兴对起诉书指控的犯罪事实及罪名均无异议，辩称其系商务代表，对朗趣公司具体情况不了解，市场上广告SDK很常见，其无辨识力，无法预见是犯罪。

被告人张振兴的辩护人对本案罪名有异议，认为指控被告人张振兴罪名不成立，首先，本案应当为单位犯罪，被告人张振兴不属于直接负责的主管人员和其他直接责任人员；其次，公诉机关对“非法控制”认定事实不清，非法控制计算机信息系统罪必须有非法的目的性，必须采取“侵入”手段，“控制”应达到排除他人的控制；第三、指控被告人张振兴的犯罪事实及罪名证据不足，司法鉴定意见书缺乏独立性，不能作为定案依据；最后，被告人张振兴有坦白情节，系从犯，无前科，本案没有严重后果，在被告人张振兴作用下没有植入广告SDK的手机流入市场。综上，若认定其有罪，请求对其免予刑事处罚或减轻处罚并适用缓刑。

被告人刘小军对起诉书指控的犯罪事实及罪名均无异议，其自我辩解与被告人张振兴一致。

被告人刘小军的辩护人提出本案系单位犯罪，即使认定为个人犯罪，被告人刘小军系从犯，应当从轻或减轻处罚；鼎勤公司的业务不是被告人刘小军促成的，其是后期接手并进行维护管理；其是初犯、偶犯，请求对其免予刑事处罚或判处缓刑。

被告人李仁平对起诉书指控的犯罪事实及罪名均无异议，其自我辩解与被告人张振兴一致，并提出其认罪态度较好，请求对其从轻处罚。

被告人李仁平的辩护人提出本案系单位犯罪，被告人李仁平主观上无犯罪故意；本案无侵入行为，未实施控制；被告人李仁平系从犯、初犯、偶犯，请求对其免予刑事处罚或判处缓刑。

被告人张刚对起诉书指控的犯罪事实及罪名均无异议，辩称其从事商务工作，主观恶性较小，在本案中所起作用较小，情节轻微，不明知广告SDK对用户手机进行控制，对微信业务不知情；其工作期间无运营成功的客户，无社会危害；商务行为经公司层层审批；其有自首情节，请求减轻或免除处罚。

被告人廖天一对起诉书指控的犯罪事实及罪名均无异议，辩称一键达apk是经用户允许并安装的，请求对其从轻处罚。

被告人廖天一的辩护人对被告人廖天一在本案中的客观行为无异议，同意其他辩护人关于单位犯罪、从犯等方面的辩护意见，建议对大部分被告人定罪免罚或对全部被告人判处缓刑。

被告人刘寸霞对起诉书指控的犯罪事实没有异议，辩称因网秦公司的背景原因，且其不是技术人员，没有意识到广告SDK触犯法律，其在朗趣公司负责项目协调，2016年开始接触广告SDK业务，但其工作内容涉及广告SDK的部分较少，且大部分最终没有运营，即使运营也不涉及静默安装，弹送的广告都是百度、阿里、腾讯等大公司的广告，没有意识到

是犯罪。

被告人刘寸霞的辩护人提出本案构成单位犯罪，被告人刘寸霞不是直接负责人员，属于普通员工，负责少量广告 SDK 工作，未参与新媒体业务；若认定为个人犯罪，被告人刘寸霞工作性质类似于客服人员，参与度小，无决策力，岗位可替代性强，系从犯；其无主观故意，有坦白情节，系初犯，请求对其免予刑事处罚或从轻、减轻处罚并适用缓刑。

被告人周雷对起诉书指控的犯罪事实无异议，辩称不知道其行为构成犯罪，其无主观恶意，只负责数据统计，不了解广告 SDK。

被告人周雷的辩护人认为本案不构成犯罪，广告 SDK 是内置于程序内的广告开发工具包，用户有选择广告的权利，只要不点击或选择关闭，都是能关闭广告窗口的，并没有控制移动终端。还提出本案系单位犯罪，被告人周雷的行为不构成犯罪，其不属于单位主要负责人，主观上无犯罪的故意，指控其有主观故意的证据不足，凭聊天记录认定主观故意不妥，且应当采信其后期的供述；其数据统计的行为未侵犯法益，综上，指控被告人周雷构成非法控制计算机信息系统罪的证据不足，若认定其构成本罪，请求考虑其从犯、初犯等情节对其从轻、减轻处罚。

被告人兰雪玲对起诉书指控的犯罪事实无异议，辩称不知道其行为构成犯罪，其是应网秦公司要求转入朗趣公司，转入朗趣公司后，前期依旧是做桌面业务的测试，后期才开始做广告 SDK 的研发工作，以学习为主，主观上无犯罪意图，请求从轻处罚。

被告人兰雪玲的辩护人提出本案系单位犯罪；被告人兰雪玲系从犯，依法应当从轻或减轻处罚；其能如实供述所犯罪行，悔罪态度较好；其系初犯、偶犯，有坦白情节，请求对其适用缓刑。

被告人张明伟对起诉书指控的犯罪事实无异议，不认为其行为构成犯罪，愿意认罪伏法，辩称一键达 apk 需要用户同意才能安装并关注公众号，并且可以取消，其编写的内容是服务行为，有用户授权，其未参与广告 SDK 的研发。

被告人张明伟的辩护人提出被告人张明伟主观上没有犯罪故意，客观上其工作内容不具备犯罪行为，本案即使构成犯罪，也应当是单位犯罪；一键达 apk 不具备非法控制行为，不存在违法性；其电脑中的文档是交接文档，不是其实际工作内容；综上，请求认定其无罪。

被告人蔡鹏对起诉书指控的犯罪事实及罪名均无异议，辩称其于 2017 年 3 月经过正常招聘程序入职朗趣公司，刚大学毕业，法律意识淡薄，广告 SDK 是其工作的一小部分，请求法庭考虑其认罪态度较好对其从轻处罚。

被告人蔡鹏的辩护人提出本案系单位犯罪，被告人蔡鹏不是主要负责人或其他直接责任人，不应追究其刑事责任；其主观上无犯罪故意，入职时间短，客观上没有社会危害后果，工作不涉及一键达 apk，指控的获利及控制数量不应算在被告人蔡鹏名下；其系从犯，依法应当从轻或减轻处罚；其自愿认罪，系初犯、偶犯；综上，请求对其免予刑事处罚。

被告人李晓蒙对起诉书指控的犯罪事实及罪名均无异议，辩称其入职晚，接触广告 SDK 时间短，刚开始做广告 SDK 的简单修复，对公司不了解，没有主观恶意和犯罪意识，只拿基本工资，没有非法收入，请求对其从轻处罚。

被告人李晓蒙的辩护人对起诉书指控的犯罪事实及罪名均无异议，提出被告人李晓蒙系从犯，依法可以从轻或减轻处罚；其系初犯、偶犯，主观恶性较小，如实供述，当庭认罪，请求对其减轻处罚并适用缓刑。

被告人何娟凤对起诉书指控的犯罪事实及罪名均无异议，辩称其无主观恶意，因网秦公司的上市背景以及公司内部正规的业务流程，使其对广告 SDK 没有正确的主观认知；其行为属于履职行为，拿基本工资，入职时间短，负责公司老客户，所起作用小，系从犯，对新媒体业务不知情，有坦白情节，系初犯，情节轻微，请求对其减轻或免除处罚。

被告人张皓然对起诉书指控的犯罪事实及罪名均无异议，辩称其在朗趣公司的主要工

作是主题商店部分，现场测试的时间很少；广告 SDK 弹送广告的次数应当以测试清单上要求的次数为准，朗趣公司不允许乱弹广告；其不了解一键达 apk 的情况，不知道有一键达 apk 的安装；获取用户信息是为了标识用户，没有不法目的，安卓系统也没有进行限制；在其之前有其他人从事该工作，有入职时间比其长的，都没有被追究。

被告人张皓然的辩护人对被告人张皓然从事现场测试的事实不持异议，认为本案不构成犯罪，恶意程序不等同于非法控制，广告 SDK 只推送广告，没有控制手机，广告 SDK 的源代码可能具备的功能不代表可以使用或已经实现；若本案构成犯罪，应考虑上述因素在量刑时考虑整体从轻；本案系单位犯罪，被告人张皓然作为底层员工，可以不追究刑事责任；若认定个人犯罪，被告人张皓然在本案中的犯罪情节轻微，有从犯、初犯、坦白等情节，同时鉴于被告人张皓然所在岗位的前任工作人员未被追究，请求对其免予刑事处罚或判处缓刑。

被告人白雪卿对起诉书指控的犯罪事实及罪名均无异议，辩称其初入互联网行业，在工作中以学习为主，接触广告 SDK 业务时间短，主要负责测试广告能否正常弹送，请求对其从轻处罚。

被告人白雪卿的辩护人提出起诉书指控的犯罪事实和证据不明确、充分、清楚，被告人白雪卿于 2017 年 3 月入职，在此之前的获利、激活数量等均与其无关，司法鉴定意见书没有明确的结论，不应作为本案的证据；被告人白雪卿系从犯，有坦白情节，认罪态度较好，请求对其从轻处罚。

被告人韩明明对起诉书指控的犯罪事实及罪名均无异议，辩称其只负责初级测试工作，请求对其从轻处罚。

经审理查明：

2015 年 8 月，被告人欧建宏、陈言敏、宋瑞、孟宪巍、任友松、周飞、邹琪、吕涛、张振兴、刘小军、廖天一、刘寸霞、兰雪玲等人的人事关系从网秦公司转入朗趣公司，成为朗趣公司北京团队，直至案发期间陆续有被告人刘鹏、李仁平、张刚、周雷、张明伟、蔡鹏、李晓蒙、何娟凤、张皓然、白雪卿、韩明明等人加入。朗趣公司北京团队成立后，继续与原朗趣公司团队（又称上海团队）合作原有业务，并开始研发只保留广告功能的 SDK，即广告 SDK，同时向被告人赖宜练所在的鼎勤公司，被告人罗轶先、李铭岳所在的智汇云商公司以及深圳语信时代通信设备有限公司、上海耘棋信息技术有限公司、深圳云逗科技有限公司等手机方案商、中间商、厂商（以下统称为手机商）推广广告 SDK 业务。经协商，由北京团队提供广告 SDK 工具包，手机商将广告 SDK 工具包预装到智能手机系统（以下简称手机）中，并使广告 SDK 获取系统权限，北京团队则根据存活率按安装台数或以广告费收入分成的方式向手机商支付费用。

装有广告 SDK 的手机在用户首次开机联网时，广告 SDK 即通过互联网与后台服务器连接，在用户不知情的情况下向后台服务器上传 imei、imsi 等用户信息、自动更新广告 SDK 版本等，并根据与手机商达成的运营方案通过服务端（即 BOSS 系统）对推送方式、内容及频率等进行配置，向用户推送商业性电子信息，从而产生广告费收入。

朗趣公司北京团队按工作内容可分为研发、项目、运营、商务等部门，也可分为主线和项目两条线。

研发部负责广告 SDK 的研发、维护、测试、服务器搭建及管理，可分为客户端组、服务端组和测试组。被告人陈言敏系负责人；客户端组中被告人任友松、邹琪、李晓蒙负责广告 SDK 的主线研发、维护和升级，被告人蔡鹏负责集成支持（对接项目）；服务端组中被告人孟宪巍系服务端组负责人，负责服务器运维，并与被告人周雷一起负责统计及提供数据，被告人兰雪玲负责服务器接口的修改、维护等；测试组中被告人周飞系负责人，与被告人白雪卿负责项目测试，被告人韩明明、张皓然分别负责主线测试和现场测试。

项目部负责对接手机商、研发部人员，促使广告 SDK 顺利集成及运营，被告人宋瑞系负责人，对接智汇云商公司，此外还负责数据结算；被告人刘寸霞负责对接语信、凡卓、鼎智等公司；被告人何娟凤负责对接鼎勤等公司。

产品运营部负责产品需求及 BOSS 系统的运营配置，被告人吕涛系负责人。

商务部负责向手机商推广广告 SDK，被告人刘鹏系负责人，对商务人员进行管理，同时维护客户关系；被告人张刚系上海商务代表，负责联系智汇云商、凡卓、禾苗等公司；被告人张振兴系深圳商务代表，负责联系语信、鼎智等公司；被告人李仁平系深圳商务代表，负责联系云逗、赛特尔等公司；被告人刘小军系深圳商务代表，负责联系鼎勤、云中酷等公司。

2015 年下半年起，朗趣公司原本的桌面业务因市场原因萎缩，负责桌面业务的原朗趣公司团队于 2016 年 11 月左右解散，北京团队的广告 SDK 业务成为朗趣公司的主要业务，2016 年底起，朗趣公司的绝大部分收入来源于广告 SDK 产生的收入。

2016 年，被告人欧建宏使用他人身份信息陆续注册成立北京瑞徕科技有限公司、北京徕乾科技有限公司、新疆港乾信息技术有限公司、北京泰安瑞达科技有限公司等用于收取广告收入。

2016 年 8 月，被告人欧建宏招募被告人颜琦进入瑞徕公司作为新媒体部负责人，于 2017 年 2 月开始微信公众号推广业务，为了实现公众号粉丝量快速增长，经被告人欧建宏、颜琦商议，由被告人欧建宏调拨被告人廖天一、张明伟到瑞徕公司新媒体部研发“一键达 apk”，利用广告 SDK 的静默安装功能自动下载并安装“一键达 apk”，“一键达 apk”在用户点击推送的文章或新闻后自动下载公众号二维码图片，利用手机辅助功能模拟用户操作，使用户微信自动识别下载的二维码图片，关注瑞徕公司运营的公众号，并定期自动清理相册中的二维码图片。

2017 年 8 月，被告人欧建宏带领北京团队人员集体离开朗趣公司，入驻瑞徕公司办公地点。

经上海弘连网络科技有限公司计算机司法鉴定所鉴定，在检材镜像文件的程序“com.aliyun.homeshell”中含有解密文件“f9ed53b467ab67.jar”（即广告 SDK），在手机系统主界面程序“com.aliyun.homeshell”启动时会自动执行，解密后的程序文件“f9ed53b467ab67.jar”具有自动更新功能、监听 home 键按键事件并显示广告窗口的功能、下载程序文件并静默安装执行的功能等;该镜像文件中已下载安装程序包“com.touchscreen”,该程序具有接受“f9ed53b467ab67.jar”发送的指令并静默安装对应程序的功能；“com.touchscreen”的 apk 文件中含有“mm.ceb”，具有解密该文件并执行解密后的程序文件“55291.apk”（即一键达 apk）的功能；解密后的程序文件“55291.apk”具有自动更新功能，并具有自动下载二维码图片并控制“微信”程序识别图片中的二维码、关注对应公众号的功能。检材手机中同样存在“f9ed53b467ab67.jar”文件，与检材镜像文件中的“f9ed53b467ab67.jar”文件功能相同；“f9ed53b467ab67.jar”对应的 SharedPreference 文件“AdSDKSettings.xml”中记录的已下载程序“mm_apk_pkg”的包名为“com.proxyserver”,数据目录中存在 6 张微信公众号二维码图片，目录中有一张图片文件已被删除无法恢复；打开检材手机中任一应用，再按 home 键返回后，手机主界面弹出广告窗口，广告窗口资源属于包“com.aliyun.homeshell”，即“f9ed53b467ab67.jar”中的资源。

经查，朗趣公司自 2015 年 10 月 21 日起至案发，收到深圳腾讯科技有限公司（以下简称腾讯公司）打款共计 36122708.36 元，其中 2017 年收到的 14493171.03 元均系广告 SDK 的违法所得；自 2016 年 7 月起至案发，徕乾公司收到腾讯公司打款共计 20211758.27 元，其中包含广告 SDK 的违法所得；自 2017 年 6 月起至案发，瑞徕公司收到腾讯公司打款共计 9673163.13 元，均系广告 SDK 的违法所得；鼎勤公司自 2016 年 1 月 27 日起至案发，以深

圳市鼎科创达科技有限公司的名义收到朗趣公司打款共计 4755745.25 元，均系广告 SDK 的违法所得；智汇云商公司自 2015 年 8 月 3 日起至案发，收到朗趣公司打款共计 3916164.28 元，其中 130 余万元系广告 SDK 的违法所得。

经勘查，北京团队使用的线上服务器数据库（内网 IP 地址 10.0.1.87，互联网 IP 地址 54.223.55.234）内 mobileNumber、userResourceAssoc 中发现大量手机号、imsi 号、imei 号，对 userResourceAssoc 内数据进行去重，去重后 imei 号共计 21712194 个，去重后 imsi 号共计 23911294 个；newuserResourceAssoc 总记录条数为 131507300 条。

新媒体统计数据库下内网服务器 mkmoney 中 mmUserInfo 中含有大量用户微信信息，数据库字段有微信号、性别、名字、区域、微信状态等，User 集合含有生日、好友数量、国家、职业、用户手机号、微信昵称、性别、imsi 号、imei 号、mac 地址等信息。mmUserInfo 集合共有 2569222 条记录，去重后的微信号总数为 1303469 个，user 集合共有 11892848 条记录，去重后 imei 号共计 8200909 个。

另查明，公安机关从被害人朱某等 20 人处调取涉案手机 20 部；从北京市朝阳区北美国际商务中心 B 座底楼查获并扣押笔记本电脑 2 台、苹果手机 2 部、硬盘 4 个；北京市朝阳区北美国际商务中心 B 座 1 楼查获并扣押章 24 个、文件若干、U 盘 2 个、电子密码器 1 个；从被告人欧建宏位于北京朝阳区世华泊郡**楼****住所查获并扣押笔记本电脑 2 台；从深圳市南山区黑海街道科苑南路海阔天空雅居 C 栋 17A 查获并扣押联想笔记本电脑 1 台、苹果手机 1 部、三星手机 1 部、笔记本 1 本、其他手机 6 部、戴某笔记本电脑 3 台；从深圳市南山区西丽街道崇文华源 17 栋 2712 被告人李仁平处查获并扣押手机 3 部、苹果 6plus 手机 1 部、联想笔记本电脑 1 台；从被告人赖宜练处查获并扣押电脑主机 2 台、苹果 6SPLUS 手机 1 部，苹果 5 手机 1 部；从被告人陈言敏处查获并扣押移动硬盘 1 个、电脑 2 台、手机 1 部；从被告人宋瑞处查获并扣押联想电脑 1 台、手机 2 部；从被告人邹琪处查获并扣押笔记本电脑 1 台，手机 3 部；从被告人任友松处查获并扣押笔记本电脑 1 台、手机 1 部；从被告人周飞处查获并扣押笔记本电脑 1 台；从被告人吕涛处查获并扣押笔记本电脑 1 台、手机 1 部；从刘鹏处查获并扣押手机 1 部；从被告人颜琦处查获并扣押笔记本电脑 1 台、手机 2 部；从被告人罗轶先处查获扣押手机 1 部、电脑主机 1 台、手机软件推广框架合作协议 1 份、业务代理合作协议 1 份、智汇云商软件推广合作协议书 1 份；从被告人李铭岳处查获并扣押笔记本电脑 1 台、台式主机 1 台、手机 1 部、测试手机 21 台；从被告人刘小军处查获并扣押笔记本电脑 1 台、笔记本 1 本、手机 2 部；从被告人廖天一处查获并扣押电脑 1 台、手机 2 部；从被告人刘寸霞处查获并扣押笔记本电脑 1 台、手机 2 部；从被告人周雷处查获并扣押电脑 1 台、手机 1 部；从被告人兰雪玲处查获并扣押电脑 1 台、移动硬盘 1 只、手机 1 部；从被告人张明伟处查获并扣押白色戴某电脑 1 台、手机 2 部；从被告人蔡鹏处查获并扣押笔记本电脑 1 台、手机 4 部；从被告人李晓蒙处查获并扣押笔记本电脑 1 台、手机 2 部；从被告人孟宪巍处扣押电脑 1 台、手机 1 部；从被告人张刚处扣押手机 1 部；从被告人何娟凤处查获并扣押联想 1 台，手机 2 部；从被告人张皓然处查获并扣押手机 7 部、笔记本电脑 1 台、笔记本 3 本；从被告人白雪卿处查获并扣押电脑 1 台、手机 1 部；从被告人韩明明处查获并扣押电脑一台。公安机关于 2017 年 9 月 29 日冻结北京瑞徕科技有限公司银行账户资金 4394581 元；于同年 12 月 27 日冻结智汇云商公司银行账户资金 3397928.02 元，冻结深圳市鼎科创达科技有限公司银行账户资金 47380.77 元。

上述事实，有受案登记表、被告人供述、被害人陈述、证人证言、搜查笔录、调取证据清单、扣押决定书、扣押清单及照片、辨认笔录、域名注册信息、域名关联的控制台账号注册信息（光盘 1 张）、服务器数据（硬盘 5 个）、服务器账号注册信息、工业和信息化部电信设备认证中心查询去函及复函、现场勘查资料及视频、业务代理合作协议、补充协议、采购合同、销售合同、被害人手机检查笔录、电子证据远程勘察工作记录、司法鉴定意见书、

电子证据检查笔录及电子数据勘验移动硬盘、银行查询信息、工商查询信息、协助冻结财产通知书（回执）、抓获经过、到案经过、情况说明、违法犯罪经历查询证明、身份证明等证据予以证实。

被告人宋瑞、孟宪巍及其辩护人对起诉书指控二人在朗趣公司内担任的职务有异议，经查，朗趣公司内部系扁平化管理，没有明确的部门划分和人员任职文书，但各被告人供述可证实各被告人根据各自的分工及工作内容，对公司内设机构及相应负责人有较为统一的认知，据此，本院结合各被告人供述及被告人宋瑞、孟宪巍的工作内容分别认定被告人宋瑞为项目部负责人、被告人孟宪巍为研发部服务端组负责人，对被告人宋瑞、孟宪巍及其辩护人提出的相应辩护意见不予采纳。

本院认为，本案主要的争议焦点如下：1、司法鉴定意见书是否应当予以排除；2、广告 SDK 及一键达 apk 的安装、运行是否构成非法控制计算机信息系统；3、本案非法控制的手机数量以及违法所得的金额问题；4、本案是否为单位犯罪；5、各被告人的主观故意问题。

1、司法鉴定意见书是否应当予以排除。

首先，被告人欧建宏的辩护人提出嘉兴市公安局港区分局所调取的证据因其无管辖权，调查取证的行为属于程序违法，故包括司法鉴定意见书在内的相关证据均应当予以排除，对此本院认为，本案部分被害人的工作地点在嘉兴市港区，嘉兴市公安局港区分局在案件移送前具有管辖权，况且在本院组织的庭前会议中，各被告人及辩护人均未提出非法证据排除申请，故对被告人欧建宏的辩护人提出的该辩护意见不予采纳。

其次，对于有被告人及辩护人提出本案应当委托省级以上负责计算机信息系统安全保护管理工作的部门进行鉴定，上海弘连网络科技有限公司计算机司法鉴定所及其鉴定人员没有鉴定资质，司法鉴定程序违法，弘连司鉴[2017]计鉴字第 309 号司法鉴定意见书应当予以排除的意见，本院认为，本案不属于《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》第十条规定的需要由省级以上负责计算机信息系统安全保护管理工作的部门检验的情形，即不属于对专门用于侵入、非法控制计算机信息系统的程序、工具难以确定的情形，本案的鉴定机关及鉴定人员均具备计算机司法鉴定资质，鉴定事项符合其业务范围，鉴定过程符合法定程序，且各被告人及辩护人在庭前会议中未提出非法证据排除申请，故对上述意见本院不予采纳。

此外，各被告人及辩护人对于鉴定意见提出异议，认为鉴定意见不客观，结论不明确，具有倾向性、诱导性，经审查，该份司法鉴定意见书的检材是被害人手机提取的镜像文件以及另一部被害人手机，鉴定过程是对两份检材进行的实际检测和操作，从中找到了被害人手机弹送广告的程序源头，即广告 SDK，还发现了一键达 apk 的程序文件，并对两份检材中检测到的广告 SDK、一键达 apk 所具备的功能、行为进行了对比，最后进行了客观描述。鉴定意见中广告 SDK 和一键达 apk 的相关功能、行为以及发现的域名指向等均能与被害人陈述、证人证言、被害人手机检查笔录、各被告人供述以及其他客观性证据相互印证，虽然不是结论性意见，但属客观真实，本院予以采纳，各被告人及辩护人对鉴定意见提出的相关意见本院亦不予采纳。

2、广告 SDK 及一键达 apk 的安装、运行是否构成非法控制计算机信息系统。

首先，非法控制的本质在于非法性，即违反国家规定；其次，控制行为的本质在于非用户本人操作。本案大部分被告人及辩护人认为广告 SDK 的预装及运行不属于非法控制计算机信息系统，一是广告 SDK 是合法的，预装行为不属于侵入或其他技术手段，没有违反国家规定；二是广告 SDK 获取用户信息、向用户手机弹送广告不属于控制行为；三是广告 SDK 行使的是程序运行权，而非系统控制权，本案中计算机信息系统没有被侵害。

（1）是否违反国家规定的问题。

有多名被告人供述证实手机用户对广告 SDK 的预装及运行并不知情，且有如下客观

事实予以印证：广告 SDK 是预装在手机中的，弹送广告与用户操作手机的行为目的无因果关系，而广告 SDK 的预装及运营有诸多规避行为，例如设置白名单（不运营的用户）、区域性运营（避开百度、阿某、腾讯三大公司所在地）、设置静默期（激活后一段时间内不运营）、不在桌面上显示广告 SDK 的图标、规避操作系统提供方的检测获取签名、进网样机中未植入广告 SDK 等；在弹送广告的方式上具有伪装性，例如在用户点击某个应用程序的前后弹送广告，使用户误以为是打开的应用程序所弹的广告等。此外，被害人陈述亦证实对所使用的手机装有广告 SDK 并不知情，所弹广告未经允许，故有被告人及辩护人提出广告 SDK 的预装、运行已告知手机用户并获得许可的辩解及辩护意见与事实不符，本院不予采信和采纳。基于广告 SDK 的预装及运行均未经用户允许，其获取用户信息、自动更新、静默安装等在其他经用户允许的应用程序中同样具备的功能，均属于未经用户授权。

一键达 apk 是利用广告 SDK 的静默安装功能经 BOSS 系统打开放量后未经用户允许进行安装，上述事实有被告人颜琦、廖天一、张明伟、吕涛等人的供述及司法鉴定意见书予以证实；被告人欧建宏当庭辩称只有同时开启静默安装权限、辅助功能权限并且点击查看推送的用户才会自动下载、安装并运行一键达 apk，实现自动关注微信公众号，被告人廖天一当庭辩称用户点击推送的文章或新闻，即表示喜欢该公众号，一键达 apk 则给用户提供自动关注公众号的服务，被告人张明伟当庭辩称一键达 apk 经用户同意后安装并关注公众号，其功能是服务行为，对此本院认为，手机用户开启静默安装权限、辅助功能权限目的是为了获得合法的服务，而一键达 apk 的目的是为了实现微信公众号粉丝量快速增长，从而利用大量的粉丝资源谋取利益，没有任何服务性质的功能，且所谓的用户点击查看即表示同意关注微信公众号的理解，是将程序开发者的主观意志强加于用户的行为之上，曲解用户点击阅读的行为目的。综上，被告人欧建宏、廖天一、张明伟就一键达 apk 提出的辩解与事实不符，本院不予采信，对辩护人提出的相应辩护意见不予采纳。

可见，广告 SDK 及一键达 apk 的预装和安装未经用户允许，二者的运行亦未取得用户授权，违反了《中华人民共和国计算机信息系统安全保护条例》及《全国人大常委会关于加强网络信息保护的决定》的相关规定，属于违反国家规定。

（2）关于控制行为的问题。

本院认为，广告 SDK 及一键达 apk 运行的一系列行为均属于控制行为。控制行为的本质是非用户本人操作，后果是使计算机信息系统执行特定操作，不限于行为人直接行使了控制权，也可以是通过计算机程序等媒介使用了控制权，且控制行为不必然具有排他性，包括完全控制，也包括部分控制，只要是计算机信息系统执行其发出的指令即可。本案便是利用广告 SDK 和一键达 apk 等程序使用户手机执行了一系列操作：获取用户信息，自动上传、下载、删除数据，弹出广告、调用手机辅助功能自动模拟用户操作等等，而二者的运行及运行后果能否被手机用户中止、改变不影响行为性质的认定，故对各被告人及辩护人相应的辩解和辩护意见均不予采纳。

（3）计算机信息系统的问题。

所谓计算机信息系统是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等，指的是设备整体，并非仅指其中的操作系统，被告人欧建宏、陈言敏的辩护人提出广告 SDK 行使的是程序的运行权，而非系统的控制权，计算机信息系统没有受到侵犯的意见本院不予采纳。

综上，广告 SDK 及一键达 apk 的安装、运行构成非法控制计算机信息系统。

3、本案非法控制的手机数量以及违法所得的金额问题。

（1）广告 SDK 控制手机的总数问题。

各被告人及辩护人均对控制手机的数量及违法所得金额有异议，经查，朗趣公司原本的桌面及主题商店变现业务与广告 SDK 业务使用同一个服务器，二者的数据有所混同，单

从数据上确实难以进行区分。但结合被告人兰雪玲的供述可知，其负责服务器接口工作，2016年年初参与研发了uid，是给用户生成一个唯一的身份标识存在数据库内，提高用户激活的效率，也便于统计。uid存放在数据库内的userResourceAssoc表（以下简称旧表），表内存放的是早期桌面用户和一部分广告SDK用户，后来启用了newuserResourceAssoc新表（以下简称新表），表内都是广告SDK用户，uid在表里显示的是_id，旧表和新表有一小部分重叠。关于uid，被告人陈言敏、孟宪巍、张皓然、白雪卿有相关供述，能印证uid是对用户的唯一标识。据此，新表内uid是用户身份的唯一标识，从2016年以后启用，既排除了双卡双待的问题，又排除了与桌面用户混同的问题，故以新表内的数据认定控制数量较为妥当，公诉机关以旧表内去重后的imei号数量进行指控，不符合客观事实。但新表内uid数量远远大于旧表内去重后imei号的数量，在公诉机关未增加指控的情况下，本院基于查清的事实，对于相关数据在事实部分进行客观描述，不以控制手机的总数作为本案定罪量刑的依据。

（2）广告SDK违法所得的金额问题。

经查，广告SDK从2015年下半年开始研发并投入运行，该事实有被告人供述、证人陈某的证言予以证实；被告人欧建宏供述证实从2016年10月开始，广告SDK成为朗趣的主要业务和获利点；2016年朗趣公司原来桌面业务产生的广告收入，加上刚起来的广告SDK业务的收入，有部分打到了徕乾公司的账户上，都是腾讯打过去的；从2016年年底开始，绝大部分的收入是广告SDK的收入；2017年朗趣公司广告SDK业务的收入有部分打到了瑞徕公司的账户上，都是腾讯打过去的。据此，至少2016年开始广告SDK已产生违法所得，且2017年朗趣公司、瑞徕公司从腾讯公司获得的收入均是广告SDK的违法所得，虽然2017年以前桌面业务的收入与广告SDK的违法所得无法进行区分，但2017年朗趣公司、瑞徕公司的违法所得达2400余万元，该部分金额已属情节特别严重。

鼎勤公司因没有桌面业务，故其从朗趣公司处获得的均是广告SDK产生的违法所得，共计470余万元。

被告人罗轶先、李铭岳的供述及证人陈某的证言能证实智汇云商公司与朗趣公司有桌面业务，鉴于桌面业务收入与广告SDK产生的违法所得无法区分，根据被告人罗轶先的供述，智汇云商因广告SDK业务从朗趣公司获得100万至200万元，70—80%的款项打给了沃特沃德公司，智汇云商互利40万至50万元，本院据此就低认定智汇云商公司违法所得130余万元，支付给沃特沃德公司的款项属于对违法所得的分配，不予扣除。

（3）一键达apk非法控制手机的数量问题。

认定一键达apk控制手机数量时同样存在双卡双待、与其他业务用户数量混同等问题，但一键达apk没有实际获取违法所得的证据，鉴于一键达apk存在控制手机的客观事实，故结合新媒体数据库中相关集合内去重后的微信号总数和imei数，以及被告人颜琦的供述、证人王某的证言，本院认为一键达apk控制手机的数量已远远超过属情节特别严重的100台，将结合相关被告人关于控制数量的辩解酌情予以量刑。

4、本案是否构成单位犯罪的问题。

被告人赖宜练、罗轶先、李铭岳的辩护人均提出本案应当认定为鼎勤公司和智汇云商公司的单位犯罪行为，对此本院认为，上述三被告人的行为并非是单位意志的体现，鼎勤公司、智汇云商公司与朗趣公司签订的业务代理合作协议中有关于合作业务合法性的约定，可见鼎勤公司和智汇云商公司主观上没有犯罪故意，但作为具体实施的个人，被告人赖宜练、罗轶先、李铭岳对广告SDK的功能和原理以及实施过程中的规避行为均是明知的，具有非法控制计算机信息系统的主观故意，因此，虽然被告人赖宜练、罗轶先、李铭岳的行为从表现上是代表公司履行职务，收入亦归单位所有，但不宜认定为单位犯罪，对上述三被告人的辩护人就单位犯罪提出的辩护意见不予采纳。

本案其他被告人及辩护人亦提出本案应当属于朗趣公司单位犯罪，经查，2016年7

月朗趣公司 CEO 变更为曹锡宇，2016 年 11 月原朗趣公司团队解散后，仅剩被告人欧建宏的北京团队，主要业务为广告 SDK，公司收入主要来源于广告 SDK 的收入，虽然还有一部分主题商店业务，但属于给客户提供的免费服务，仅有个别人员从事相关工作，其他人员的工作内容均为广告 SDK，上述客观事实有各被告人的供述、证人证言予以证实，由此可见朗趣公司以广告 SDK 业务为主要活动，属于单位设立后以犯罪行为为主要活动，不应认定为单位犯罪。此外，2016 年以后，被告人欧建宏以他人身份成立多个公司，利用这些公司名义推广广告 SDK 业务并收取广告费，在瑞徕公司成立新媒体部主要运营一键达 apk，并带领整个团队于 2017 年 8 月集体跳槽，上述事实亦有各被告人供述、证人证言、银行流水明细等证据予以证实，亦可证明被告人欧建宏等人的行为并非代表朗趣公司的意志，收入也并非全部归朗趣公司所有，不应认定为单位犯罪。故对各被告人及辩护人提出本案属于朗趣公司单位犯罪的辩解及辩护意见均不予采纳。

5、各被告人的主观故意问题。

各被告人的供述及电子证据检查笔录能证实各被告人对于广告 SDK 的功能、原理及运营中的规避行为是明知的，结合客观事实可以认定各被告人具备非法控制计算机信息系统的主观故意，各被告人对各自行为的违法可能性缺乏认知，不影响对其行为性质的认定；被告人欧建宏、颜琦是一键达 apk 的决策者，被告人廖天一、张明伟是研发者，四被告人对一键达 apk 的研发目的、功能应当明知，故对各被告人提出没有非法控制计算机信息系统的主观故意的辩解均不予采信，辩护人的相应辩护意见不予采纳。

综上，本案事实清楚，证据确实、充分，足以认定。

本院认为，被告人欧建宏、陈言敏、宋瑞、孟宪巍、任友松、周飞、邹琪、吕涛、刘鹏、颜琦、赖宜练、罗轶先、李铭岳、张振兴、刘小军、李仁平、张刚、廖天一、刘寸霞、周雷、兰雪玲、张明伟、蔡鹏、李晓蒙、何娟凤、张皓然、白雪卿、韩明明以牟利为目的，违反国家规定，采用技术手段非法控制他人计算机信息系统，属情节特别严重，其行为均已构成非法控制计算机信息系统罪，系共同犯罪。公诉机关指控的罪名成立，应予支持。在共同犯罪中，被告人欧建宏起主要作用，系主犯，应当按照其所参与的全部犯罪处罚，对被告人欧建宏提出其系从犯的自我辩护意见不予采纳；被告人陈言敏、宋瑞、孟宪巍、任友松、周飞、邹琪、吕涛、刘鹏、颜琦、赖宜练、罗轶先、李铭岳、张振兴、刘小军、李仁平、张刚、廖天一、刘寸霞、周雷、兰雪玲、张明伟、蔡鹏、李晓蒙、何娟凤、张皓然、白雪卿、韩明明起辅助作用，系从犯，对于从犯，依法应当从轻或减轻处罚，对上述被告人及辩护人就从犯提出的辩护意见本院予以采纳。被告人张刚提出其有自首情节，经查，被告人张刚的归案并非是其主动投案，亦没有证据证实其被抓获时是正在去投案途中，故不属于自动投案，不构成自首；被告人罗轶先的辩护人提出被告人罗轶先有自首情节，经查，公安机关传唤被告人罗轶先时已掌握了本案的相关证据，其如实供述不属于自首，故对被告人张刚、被告人罗轶先的辩护人就自首提出的辩护意见不予采纳。各被告人归案后均能如实供述本案的主要犯罪事实，属坦白，依法均可以从轻处罚；鉴于各被告人系初犯，均可酌情对从轻处罚，对于各辩护人就坦白、初犯提出的辩护意见予以采纳。综上，可依法对被告人欧建宏从轻处罚，对其余被告人减轻处罚，对各辩护人提出的从轻、减轻处罚的辩护意见予以采纳；本案犯罪情节属特别严重，不宜免予刑事处罚，被告人欧建宏作为主犯，被告人陈言敏、宋瑞、孟宪巍、任友松、周飞、邹琪作为重要部门负责人或主线研发人员，均不宜适用缓刑，对辩护人提出的免予刑事处罚及对被告人欧建宏、陈言敏、宋瑞、孟宪巍、任友松、周飞、邹琪适用缓刑的辩护意见均不予采纳；依法对其余被告人适用缓刑，对其余辩护人就缓刑提出的辩护意见予以采纳。据此，为惩治犯罪，根据本案的犯罪事实及各被告人在共同犯罪中的地位、作用、参与程度，依照《中华人民共和国刑法》第二百八十五条第二款、第二十五条第一款，第二十六条第一、四款，第二十七条、第六十七条第三款，第七十二条第一、三款，第六十

四条及《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》第一条第二款第（一）项、第十一条第一款之规定，判决如下：

一、被告人欧建宏犯非法控制计算机信息系统罪，判处有期徒刑四年六个月，并处罚金三十万元（即自2017年9月28日起至2022年3月27日止）；

二、被告人陈言敏犯非法控制计算机信息系统罪，判处有期徒刑二年八个月，并处罚金十四万元（即自2017年9月28日起至2020年5月27日止）；

三、被告人宋瑞犯非法控制计算机信息系统罪，判处有期徒刑二年六个月，并处罚金十二万元（即自2017年9月28日起至2020年3月27日止）；

四、被告人吕涛犯非法控制计算机信息系统罪，判处有期徒刑二年四个月，缓刑二年十个月，并处罚金十万元；

五、被告人孟宪巍犯非法控制计算机信息系统罪，判处有期徒刑二年，并处罚金八万元（即自2017年9月28日起至2019年9月27日止）；

六、被告人刘鹏犯非法控制计算机信息系统罪，判处有期徒刑二年，缓刑二年六个月，并处罚金八万元；

七、被告人颜琦犯非法控制计算机信息系统罪，判处有期徒刑二年，缓刑二年六个月，并处罚金八万元；

八、被告人任友松犯非法控制计算机信息系统罪，判处有期徒刑一年十个月，并处罚金七万元（即自2017年9月28日起至2019年7月27日止）；

九、被告人周飞犯非法控制计算机信息系统罪，判处有期徒刑一年十个月，并处罚金七万元（即自2017年9月28日起至2019年7月27日止）；

十、被告人赖宜练犯非法控制计算机信息系统罪，判处有期徒刑一年十个月，缓刑二年四个月，并处罚金七万元；

十一、被告人罗轶先犯非法控制计算机信息系统罪，判处有期徒刑一年八个月，缓刑二年二个月，并处罚金六万元；

十二、被告人邹琪犯非法控制计算机信息系统罪，判处有期徒刑一年四个月，并处罚金四万元（即自2017年9月28日起至2019年1月27日止）；

十三、被告人李铭岳犯非法控制计算机信息系统罪，判处有期徒刑一年四个月，缓刑一年十个月，并处罚金四万元；

十四、被告人张振兴犯非法控制计算机信息系统罪，判处有期徒刑一年四个月，缓刑一年十个月，并处罚金四万元；

十五、被告人刘寸霞犯非法控制计算机信息系统罪，判处有期徒刑一年四个月，缓刑一年十个月，并处罚金四万元；

十六、被告人兰雪玲犯非法控制计算机信息系统罪，判处有期徒刑一年四个月，缓刑一年十个月，并处罚金四万元；

十七、被告人刘小军犯非法控制计算机信息系统罪，判处有期徒刑一年四个月，缓刑一年十个月，并处罚金四万元；

十八、被告人廖天一犯非法控制计算机信息系统罪，判处有期徒刑一年四个月，缓刑一年十个月，并处罚金四万元；

十九、被告人周雷犯非法控制计算机信息系统罪，判处有期徒刑一年四个月，缓刑一年十个月，并处罚金四万元；

二十、被告人李仁平犯非法控制计算机信息系统罪，判处有期徒刑一年，缓刑一年六个月，并处罚金二万元；

二十一、被告人张刚犯非法控制计算机信息系统罪，判处有期徒刑一年，缓刑一年六个月，并处罚金二万元；

二十二、被告人张明伟犯非法控制计算机信息系统罪，判处有期徒刑一年，缓刑一年六个月，并处罚金二万元；

二十三、被告人蔡鹏犯非法控制计算机信息系统罪，判处有期徒刑一年，缓刑一年六个月，并处罚金二万元；

二十四、被告人李晓蒙犯非法控制计算机信息系统罪，判处有期徒刑一年，缓刑一年六个月，并处罚金二万元；

二十五、被告人张皓然犯非法控制计算机信息系统罪，判处有期徒刑一年，缓刑一年六个月，并处罚金二万元；

二十六、被告人何娟凤犯非法控制计算机信息系统罪，判处有期徒刑十个月，缓刑一年四个月，并处罚金一万元；

二十七、被告人白雪卿犯非法控制计算机信息系统罪，判处有期徒刑十个月，缓刑一年四个月，并处罚金一万元；

二十八、被告人韩明明犯非法控制计算机信息系统罪，判处有期徒刑十个月，缓刑一年四个月，并处罚金一万元；

上述刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日；缓刑考验期限从判决确定之日起计算；罚金款限本判决生效后十日内缴纳。

二十九、扣押的与本案有关的作案工具由扣押机关依法予以没收，冻结的违法所得依法予以没收并上交国库，其余违法所得依法予以追缴。

被告人吕涛、刘鹏、颜琦、赖宜练、罗轶先、李铭岳、张振兴、刘小军、李仁平、张刚、廖天一、刘寸霞、周雷、兰雪玲、张明伟、蔡鹏、李晓蒙、何娟凤、张皓然、白雪卿、韩明明回到社会后，应当遵守法律、法规，服从监督管理，接受教育，完成公益劳动，做一名有益社会的公民。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向浙江省嘉兴市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审　判　长　　吴竹琴

人民陪审员　　金　兰

人民陪审员　　蒋锡麟

二〇一九年一月二十五日

书　记　员　　林媛媛

5.典型案例：杨小慧等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

案例要旨

被告人未经用户同意，向用户手机中预置具有获取用户手机位置、网络状态、安装其他应用程序以及上传手机收发短信、通话信息、通信录、GPS 定位信息等功能的软件，并通过操控后台服务器的方式，在用户不知情的情况下向用户推送软件、广告等商业性电子信息，达到“情节严重”标准的，构成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。

关键词：手机 计算机信息系统 非法获取 非法控制 商业性电子信息

【相关法条】

《中华人民共和国刑法》第二百八十五条第二款违反国家规定，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。

【案件索引】

一审：北京市朝阳区人民法院（2014）朝刑初字第01743号（2015年1月29日）

二审：北京市第三中级人民法院（2015）三中刑终字第00288号（2015年6月19日）

【基本案情】

法院经审理查明：2010年7月，被告人杨小慧、陈新、罗真运、张炳等人在广东省深圳市成立深圳市安丰易联信息技术有限公司（以下简称安丰公司，住所位于广东省深圳市福田区，法定代表人陈新）；后杨小慧、罗真运等人又成立深圳市万丰博通信息技术有限公司（以下简称万丰公司，住所位于广东省深圳市福田区，法定代表人罗真运）；2011年5月，杨小慧在北京市成立北京麦德联合信息技术有限公司（以下简称麦德公司，住所位于北京市朝阳区望京新兴产业区利泽中园二区208号3号楼3509A室）。上述三家公司的经营范围包括计算机软件开发、网络技术开发、手机软硬件开发等。被告人马庆沐于2011年底在安丰公司任技术员，后于2012年底到麦德公司任技术员；被告人林伟东于2011年1月至2012年2月在安丰公司任技术员；被告人吴浩于2011年6月至2013年2月在麦德公司任技术员；被告人黄光侠于2012年9月至2013年8月在麦德公司任副总经理。

自2011年底起，被告人杨小慧、陈新、罗真运、张炳经商议后，授意被告人马庆沐、林伟东、吴浩、黄光侠研发“静默插件”，将该插件通过刷机的方式植入大量移动终端；杨小慧、张炳等人安排被告人祝春娟、杜雪梅通过后台服务端操控的方式向植入“静默插件”的移动终端推送软件、广告等商业性电子信息。经鉴定：涉案的“静默插件”具有在用户不知情的情况下，获取用户手机位置、用户手机网络状态、更改用户网络状态、删除用户手机内安装的应用程序、安装其他应用程序、通过手机网络访问互联网、强制关闭用户手机内正在运行的应用程序、获取当前用户手机内运行的应用列表、唤醒用户手机、读写用户存储卡等信息的功能；以及在用户不知情时，上传手机收发短信、通话信息、通信录、GPS定位信息的功能。经对涉案公司网站数据库进行勘查：被告人杨小慧等所经营的公司服务器内含有大量用户移动终端内的信息，其中被获取imsi（即国际移动用户识别码）的移动终端有206806部，被获取手机型号的移动终端有265970部，被获取手机号码的移动终端有44564部，被获取地址信息的移动终端有132168部，被获取软件安装列表的移动终端有196733部，被获取imei（即国际移动设备识别码）的移动终端有265991部，被获取通讯录的移动终端有102368部，被获取的通讯录共19426523条。

【裁判结果】

北京市朝阳区人民法院于2015年1月29日作出（2014）朝刑初字第01743号刑事判决：被告人杨小慧犯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，判处有期徒刑三年六个月，罚金人民币5万元；判处被告人陈新、罗真运、张炳有期徒刑三年，罚金人民币3万元；判处被告人马庆沐有期徒刑二年，罚金人民币3万元；判处被告人黄光侠、吴浩有期徒刑一年六个月，罚金人民币2万元；判处被告人林伟东有期徒刑一年五个月，罚金人民币2万；判处被告人祝春娟、杜雪梅有期徒刑一年五个月，罚金人民币1万元。

一审宣判后，被告人杨小慧、陈新、张炳、罗真运、黄光侠均提出上诉，北京市第三中级人民法院于2015年6月19日作出（2015）三中刑终字第00288号刑事裁定：驳回杨小慧等5人的上诉，维持原判。

【裁判理由】

法院生效裁判认为：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是指行为人违反国家规定，实施了侵入普通计算机信息系统或采用其他技术手段，获取计算机信息系统数据，或者对计算机信息系统实施非法控制，达到情节严重的行为。本案中，被告人杨小慧、陈新、罗真运、张炳，以营利为目的，授意技术人员马庆沐、林伟东、吴浩、黄光侠研发、升级“静默插件”，安排祝春娟、杜雪梅通过后台服务端操控的方式向植入“静默插件”

的移动终端推送软件、广告等商业性电子信息，从而非法获取计算机信息系统数据，实现对计算机信息系统的非法控制。上述10被告人的行为均已构成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。

关于被告人杨小慧及其辩护人、被告人陈新、张炳的辩护人所提本案被告人安装“静默插件”的行为没有违反国家规定，杨小慧、陈新、张炳的行为不构成犯罪的辩护意见。经查：根据《计算机信息系统安全保护条例》（以下简称《计算机保护条例》）的规定，任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。违反本条例的规定……构成犯罪的，依法追究刑事责任。根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》（以下简称《加强网络信息保护决定》）的规定，任何组织和个人未经电子信息接收者同意或者请求，或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。对有违反本决定行为的……构成犯罪的，依法追究刑事责任。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《办理危害计算机系统安全刑事案件的解释》）的规定，“计算机信息系统”是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。本案中，被告人杨小慧、陈新、张炳等人以营利为目的，共同商量决定研发“静默插件”，未经手机用户的同意，通过向用户手机（通信设备）预置“静默插件”的方式侵入计算机信息系统，非法获取身份认证信息，并在手机用户不知情的情况下向用户推送软件、广告等商业性电子信息，其行为已违反国家规定，构成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。故该辩护意见不予采纳。

关于被告人吴浩的辩护人所提公诉机关指控其所犯罪行“情节特别严重”不能成立，本案应认定为“情节严重”的辩护意见。经查：根据《办理危害计算机系统安全刑事案件的解释》第一条规定，获取网络金融服务以外的身份认证信息五百组以上或非法控制计算机信息系统二十台以上的，应认定为《刑法》第二百八十五第二款规定的“情节严重”；数量达到上述标准五倍以上的，应认定为“情节特别严重”。根据对涉案公司网站数据库进行远程勘验，综合全案证据，能够认定本案非法获取的计算机信息系统数据、非法控制的计算信息系统的数量，已远超出上述“情节特别严重”的标准，本案应认定为“情节特别严重”。故该辩护意见不予采纳。

关于被告人祝春娟的辩护人、被告人杜雪梅及其辩护人所提二被告人的行为不属于非法获取计算机信息系统数据的辩护意见。经查：被告人祝春娟、杜雪梅身为麦德公司的员工，知晓“静默插件”的运营模式，其中祝春娟负责市场推广，杜雪梅负责后台推送，二被告人的行为系整个犯罪活动的重要组成部分，非法获取计算机信息系统数据并不违背二被告人的主观意志，其与非法控制计算机信息系统紧密关联，不可分割。故该辩护意见不予采纳。

关于各被告人在共同犯罪中的地位和作用。本案中，被告人杨小慧等10人的行为属于一个完整的犯罪活动。被告人杨小慧、陈新、罗真运、张炳等四人作为决策者，在共同犯罪中起组织、领导作用，均系主犯，应当对全部犯罪活动承担刑事责任；其中杨小慧作用较大，其余三被告人作用相当。被告人马庆沐、黄光侠、吴浩、林伟东等四人作为技术人员，在杨小慧等人的授意下，参与研发升级“静默插件”，在共同犯罪中处于从属地位，均系从犯；其中马庆沐始终参与犯罪活动，作用较大；黄光侠、吴浩、林伟东在不同时间段参与犯罪活动，三被告人应对各自参与的部分承担刑事责任。被告人祝春娟、杜雪梅在张炳等人的安排下，负责市场推广，进行后台操控，在共同犯罪中起帮助作用，均系从犯。被告人杨小慧、陈新、罗真运、张炳、马庆沐、吴浩、祝春娟、杜雪梅归案后如实供述犯罪事实，其中被告人罗真运、张炳、马庆沐、吴浩、祝春娟、杜雪梅当庭自愿认罪，十被告人均系初犯，综合上述量刑情节，对被告人杨小慧、陈新、罗真运、张炳所犯罪行依法予以从轻处罚；对被告人马庆

沐、黄光侠、吴浩、林伟东、祝春娟、杜雪梅所犯罪行依法予以减轻处罚，故作出上述判决。
法院评论

本案涉及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的司法认定。根据《刑法》第二百八十五条第二款（系《刑法修正案（七）第九条新增规定》）之规定，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是指违反国家规定，侵入国家事务、国防科技、尖端科学技术领域以外的计算机信息系统或采用其他技术手段，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，达到情节严重的行为。2011 年 9 月 1 日施行的《办理危害计算机系统安全刑事案件的解释》明确了“计算机信息系统”“身份认证信息”的内涵和外延，对“情节严重”“情节特别严重”、单位犯罪及共同犯罪作了明确规定。但是关于行为人侵入、控制计算机信息系统，以及获取计算机信息系统数据的具体行为方式，立法和司法解释并未明确列举释明，尤其是随着近年来随着互联网信息技术的快速发展，侵入用户手机等通讯设备进而获取相关手机数据，推送软件、广告等电子信息的行为时有发生，对这类案件的定性日益成为争议焦点和审判难点，亟需在司法实践中加以解决。本案系涉通讯设备终端的新类型网络犯罪案件，具有较强的典型性和指导性。本案重点探讨以下几个问题：

一、用户手机是否属于计算机信息系统

随着信息技术的发展，各类内置有可以编程、安装程序的操作操作系统的数字化设备广泛应用于各个领域，其本质与传统的计算机信息系统和计算机系统已无差别。任何内置有操作系统的具备自动处理数据功能的设备都可能成为侵入、破坏和传播计算机病毒的对象，有必要将这些设备的安全纳入刑法保护范畴。《办理危害计算机系统安全刑事案件的解释》采用概括加列举的方式，将“计算机信息系统”“计算机系统”界定为具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等，其中网络设备是指路由器、交换机等组成的用于连接网络的设备；通信设备包括手机、通信基站等用于提供通信服务的设备；自动化控制设备是指在工业中用于实施自动化控制的设备，如电力系统中的检测设备、制造业中的流水线控制设备等。当前，智能手机已成为手机市场的主流，使用日益广泛。智能手机具有独立的操作系统，独立的运行空间，可由用户自行安装软件、游戏、导航等第三方服务商提供的程序，并可以通过移动通讯网络来实现无线网络接入，它具有 PDA 的功能，具有开放性的操作系统，运行速度快，兼具人性化与个性化特点。从功能来看，智能手机与个人计算机已无本质差别，故用户手机属于计算机信息系统。

二、向用户手机预置静默插件的行为是否违反国家规定

根据《刑法》第九十六条的规定，《刑法》所称的违反国家规定，是指违反全国人民代表大会及其常务委员会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令。根据《计算机保护条例》的规定，任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。违反本条例的规定……构成犯罪的，依法追究刑事责任。根据《加强网络信息保护决定》的规定，任何组织和个人未经电子信息接收者同意或者请求，或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。对有违反本决定行为的……构成犯罪的，依法追究刑事责任。根据上述法律、行政法规的规定，获取手机用户信息或者向手机用户推送商业性电子信息应当以向用户明示为原则，且必须征得用户的同意方可进行。

本案中的“静默插件”，是指在用户不知情的情况下，具备获取用户手机位置、用户手机网络状态、更改用户网络状态、删除用户手机内安装的应用程序、安装其他应用程序、通过手机网络访问互联网、强制关闭用户手机内正在运行的应用程序、获取当前用户手机内运行的应用列表、唤醒用户手机、读写用户存储卡等信息的功能的软件安装包。“静默插件”是在

用户不知情的情况下植入的，它不可能满足用户事先同意的条件，因此，安装、使用“静默插件”的行为违反了上述国家规定。

三、向尚未出售的手机预置静默插件的行为能否认定为非法侵入计算机信息系统

根据《刑法》第二百八十五条第二款的规定，构成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的要件是行为人违反国家规定，侵入计算机信息系统或采用其他技术手段，获取该计算机信息系统中的数据，或对该计算机信息系统实施非法控制。非法侵入的常见方式是利用他人网上认证信息进入计算机信息系统，或者在计算机信息系统中植入木马后门程序，获取该计算机信息系统中存储、处理或者传输的信息数据。本案中，杨小慧等人通过“刷机”的方式，即通过一定的方式更改或替换手机中原本存在的一些语言、图片、铃声、软件或操作系统（通俗地讲即给手机重装系统）将自己研发的静默插件植入尚未出售的手机，这一行为能否认定为非法侵入计算机信息系统。手机作为最常用的通讯设备，属于计算机信息系统的范围，本案的特殊之处在于，“静默插件”的植入对象为尚未出售、使用的手机，这是否属于司法解释中规定的“通讯设备”。笔者认为，尚未出售的手机已经完全具备了自动处理数据功能的系统，且随时可以投入使用，并连通互联网，其与正在使用中的手机没有本质区别，属于司法解释中规定的“通讯设备”的范围。就本案而言，被告人事先向用户手机预置“静默插件”的行为是整个犯罪活动不可或缺的一个环节，不应将其限定在某一时段内孤立看待，而应视为非法获取手机数据、非法控制手机的准备行为，能够认定为非法侵入计算机信息系统。

四、涉案手机 imei 号码、用户通讯录、地理位置等信息是否属于非法获取计算机信息系统数据罪中的“数据”

本案被告人通过静默插件获取了用户手机 imei 号码（即国际移动设备标识，手机串号，是手机的唯一识别号码）、激活时间、用户所安装的软件数量、插件版本号、手机系统版本号、手机型号、用户通讯录、手机位置信息等数据，那么这些数据是否属于《刑法》第二百八十五条第二款所规定的“计算机信息系统数据”与计算机信息系统安全相关的数据中最为重要的是用于认证用户身份的身份认证信息（如口令、证书等），此类数据通常是网络安全的第一道防线，也是网络盗窃的最主要对象，特别是非法获取电子银行、证券交易、期货交易等网络金融服务的账号、口令等身份认证信息的活动非常猖獗，故应对身份认证信息予以重点保护。为此，《办理危害计算机系统安全刑事案件的解释》界定了“身份认证信息”，是指确认用户在计算机信息系统上操作权限的数据，包括账号、口令、密码、数字证书。从实践来看，数字签名、生物特征等都属于身份认证信息。基于保障计算机信息系统安全之考量，应对“数据”的范围进行当然性解释。具体就本案所涉手机数据来看，用户手机激活时间、用户安装的软件数量、插件版本号、手机系统版本号、手机型号等信息均属于计算机存储、处理的数据，反映了用户的个性化特征，具有一定的统计分析和商业价值，当然属于“数据”的范围。imei 号码是手机的唯一识别号码，具有识别确定手机使用人的功能；手机通讯录和地理位置信息则属于公民个人信息的范畴，涉及用户隐私，事关用户安全，更应受法律严格保护。

五、通过“静默插件”向手机用户推送软件、广告等商业性电子信息的行为能否认定为非法控制计算机信息系统

本案被告人预置“静默插件”的目的是为了向手机用户推送软件、广告等商业性电子信息，进而从网络运营商处谋取利益。那么，该行为能否认定为非法控制计算机信息系统呢？所谓非法控制，比较常见的是行为人利用网站漏洞将木马植入到网站上，在用户访问网站时利用客户端漏洞将木马移植到用户计算机上，或在互联网上传播捆绑有木马的程序或文件，当用户连接到互联网时，这个程序会通知黑客，来报告 IP 地址以及预先设定的端口。黑客在收到这些信息后，利用这个潜伏在其中的程序，可以任意地修改计算机的参数设定、复制

视频、窥视整个硬盘中的内容等，从而达到控制计算机的目的。从“静默插件”的功能来看，其具有更改用户网络状态、删除用户手机内安装的应用程序、安装其他应用程序、通过手机网络访问互联网、强制关闭用户手机内正在运行的应用程序、唤醒用户手机等功能。这意味着在用户完全不知情的情况下，被告人可以通过后台服务器远程遥控用户手机自动下载相关软件。这一行为已实质上侵犯了用户对手机完整的支配权利，属于未经授权即对计算机信息系统实施控制的情形。因此，在未获允许的情况下，通过“静默插件”向手机用户推送软件、广告等商业性电子信息的行为，应当认定为非法控制计算机信息系统。

六、本案能否认定为犯罪“情节特别严重”

根据《办理危害计算机系统安全刑事案件的解释》第一条的规定，非法获取计算机信息系统数据或者非法控制计算机信息系统，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（1）项以外的身份认证信息 500 组以上的；（3）非法控制计算机信息系统 20 台以上的；（4）违法所得 5000 元以上或者造成经济损失 1 万元以上的……数量或者数额达到上述第（1）项至第（4）项规定标准五倍以上的，应当认定为“情节特别严重”。

本案中，远程勘验结果显示涉案公司服务器内含有大量用户移动终端内的信息，其中被获取 imsi（即国际移动用户识别码）的移动终端有 206806 部，被获取手机型号的移动终端有 265970 部，被获取手机号码的移动终端有 44564 部，被获取地址信息的移动终端有 132168 部，被获取软件安装列表的移动终端有 196733 部，被获取 imei（即国际移动设备识别码）的移动终端有 265991 部，被获取通讯录的移动终端有 102368 部，被获取的通讯录共 19426523 条，从以上数据可以看出被告人非法控制计算机信息系统数量之大，远远超出了“情节特别严重”所要求的 100 台的规定。从案发经过和社会危害来看：在整个作案过程中，手机用户均处于不知情的状态，如果不是警方主动介入，用户不会发现自己的手机被控制；杨小慧等人所获取的手机信息涉及个人隐私等公民个人信息，侵犯用户手机的数量达到数十万之众，危害范围广，社会影响大。综合全案证据，本案非法获取的计算机信息系统数据、非法控制的计算信息系统的数量，已远远超出上述“情节特别严重”的标准，故应认定为“情节特别严重”。

随着互联网信息行业的快速发展，涉及手机等移动通讯终端的网络犯罪案件日渐增多。在专业技术壁垒的掩护下，该类犯罪表现出极强的隐蔽性和专业性，往往犯罪行为已持续很久，但手机用户却毫不知情。鉴于这一新型网络犯罪的专业性和隐蔽性，我国亟需出台专门针对手机等通讯设备的网络犯罪立法或司法解释，对该类犯罪的行为模式、认定标准以及处罚方式作出明确的规定，以便于统一该类案件在审判实践中的裁判尺度，有利于规范相关从业者的市场行为，促进我国手机互联网行业的健康发展。

6.充分发挥检察职能 推进网络空间治理典型案例之六：吴某等 19 人非法控制计算机信息系统、侵犯公民个人信息案 （2020）浙 0624 刑初 235 号

一、基本案情

2017 年 11 月至 2019 年 8 月底，深圳云某科技有限公司（以下简称云某公司）实际控制人吴某等人在与多家手机主板生产商合作过程中，将木马程序植入手机主板内。装有上述主板的手机出售后，吴某等人通过之前植入的木马程序控制手机回传短信，获取手机号码、验证码等信息，并传至公司后台数据库，后由该公司商务组人员联系李某理（在逃）、管某辉等人非法出售手机号码和对应的验证码。期间，云某公司以此作为公司主要获利方式，通过非法控制 330 余万部手机并获取相关手机号码及验证码数据 500 余万条，出售这些数据后获利人民币 790 余万元。

其中，李某理等人向云某公司购买非法获取的手机号码和验证码后，利用自行开发的“番薯”平台软件贩卖给陈某峰等人。陈某峰等人将从李某理处非法购买的个人信息用于平台用户注册、“拉新”、“刷粉”、积分返现等，非法获利人民币 80 余万元。管某辉从云某公司购买手机号码和对应的验证码后，也用于上述用途，非法获利人民币 3 万余元。

二、诉讼过程

2019 年 12 月 31 日，浙江省绍兴市新昌县公安局将本案移送新昌县人民检察院审查起诉。2020 年 6 月 19 日，新昌县人民检察院对吴某等 5 人以非法控制计算机信息系统罪，对陈某峰、管某辉等 14 人以侵犯公民个人信息罪提起公诉。2020 年 11 月 18 日，新昌县人民法院以非法控制计算机信息系统罪分别判处吴某等 5 名被告人有期徒刑二年至四年六个月不等，并处罚金；以侵犯公民个人信息罪分别判处陈某峰、管某辉等 14 名被告人有期徒刑六个月至三年六个月不等，并处罚金。

三、典型意义

（一）利用公民个人信息实施网络犯罪日益高发，获取信息方式日趋隐蔽。当前，非法获取公民个人信息的现象屡见不鲜，手段花样翻新，往往成为网络犯罪的必备前置程序。违法犯罪分子有的通过手机 APP、电脑软件，有的通过搭建钓鱼网站、发送木马链接，有的则在手机、智能手表、路由器等硬件设备的生产环节植入病毒程序，非法获取公民个人信息。这些行为侵害了公民个人隐私和人身、财产权利，滋生大量网络违法犯罪，社会危害巨大。

（二）依法严厉打击侵犯公民个人信息犯罪。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》，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,包括姓名、身份证件号码、通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。随着网络技术发展，逐步扩展到人脸、虹膜等生物识别信息，以及网络支付账户信息等，而且其范围仍在逐步扩展。违反国家规定，非法获取、出售或提供上述公民个人信息，情节严重的，构成侵犯公民个人信息罪，应当依法严厉打击。

（三）提高个人防范意识，规范企业行业数据收集使用。社会公众要提高对个人信息的保护意识，不轻易点击、下载来源不明的链接和程序，务必在正规商店购买正规厂家生产的电子设备，不轻易向外透露个人信息。相关部门要加强监管，从网络硬件的生产、流通、使用各环节规范数据收集，规范网络平台、APP 软件等收集、使用公民个人信息的行为，监督相关企业建立数据合规制度。

7.广东高院发布 2017 年度涉互联网十大案例之五：以黑客手段窃取苹果手机 ID 密码如何定性 （2017）粤 20 刑终 258 号

基本案情

2015 年 5 月起，肖某通过网络发布破解苹果手机账号密码广告，先后接受 12 名客户的订单，在没有获得手机绑定 ID 用户的同意下，肖某本人或者委托他人利用网上租用的“钓鱼网站”和“XSS”方式非法获取进入苹果官方服务器的 ID 密码，对手机与 ID 进行解除绑定的操作，从中收取费用。截至 2016 年 6 月，肖某采用上述手段共破解 174 台苹果手机 ID，违法所得人民币 4 万余元。

裁判结果

法院生效裁判认为，肖某无视国家法律，结伙违反国家规定，采用技术手段，非法获取计算机信息系统中存储的数据，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，应依法惩处。判处有期徒刑三年，并处罚金三万元。

典型意义

随着智能终端设备的广泛普及，非法使用苹果用户 ID 密码锁定设备，以解锁为由索要

财物的案件屡见报端。苹果手机 ID 密码可以在任何计算机终端使用，是用于确认用户在计算机信息系统操作权限的数据，属于计算机信息系统数据。本案例对于打击类似犯罪，保护智能终端用户的合法权益具有积极的意义。

8.最高人民法院发布第 26 批指导性案例之二：张竣杰等非法控制计算机信息系统案

(2019)苏 01 刑终 768 号

裁判要点

1.通过植入木马程序的方式，非法获取网站服务器的控制权限，进而通过修改、增加计算机信息系统数据，向相关计算机信息系统上传网页链接代码的，应当认定为刑法第二百八十五条第二款“采用其他技术手段”非法控制计算机信息系统的行为。

2.通过修改、增加计算机信息系统数据，对该计算机信息系统实施非法控制，但未造成系统功能实质性破坏或者不能正常运行的，不应当认定为破坏计算机信息系统罪，符合刑法第二百八十五条第二款规定的，应当认定为非法控制计算机信息系统罪。

相关法条

《中华人民共和国刑法》第 285 条第 1 款、第 2 款

基本案情

自 2017 年 7 月开始，被告人张竣杰、彭玲珑、祝东、姜宇豪经事先共谋，为赚取赌博网站广告费用，在马来西亚吉隆坡市租住的 Trillion 公寓 B 幢 902 室内，相互配合，对存在防护漏洞的目标服务器进行检索、筛查后，向目标服务器植入木马程序（后门程序）进行控制，再使用“菜刀”等软件链接该木马程序，获取目标服务器后台浏览、增加、删除、修改等操作权限，将添加了赌博关键字并设置自动跳转功能的静态网页，上传至目标服务器，提高赌博网站广告被搜索引擎命中几率。截止 2017 年 9 月底，被告人张竣杰、彭玲珑、祝东、姜宇豪链接被植入木马程序的目标服务器共计 113 台，其中部分网站服务器还被植入了含有赌博关键词的广告网页。后公安机关将被告人张竣杰、彭玲珑、祝东、姜宇豪抓获到案。公诉机关以破坏计算机信息系统罪对四人提起公诉。被告人张竣杰、彭玲珑、祝东、姜宇豪及其辩护人在庭审中均对指控的主要事实予以承认；被告人张竣杰、彭玲珑、祝东及其辩护人提出，各被告人的行为仅是对目标服务器的侵入或非法控制，非破坏，应定性为非法侵入计算机信息系统罪或非法控制计算机信息系统罪，不构成破坏计算机信息系统罪。

裁判结果

江苏省南京市鼓楼区人民法院于 2019 年 7 月 29 日作出（2018）苏 0106 刑初 487 号刑事判决：一、被告人张竣杰犯非法控制计算机信息系统罪，判处有期徒刑五年六个月，罚金人民币五万元。二、被告人彭玲珑犯非法控制计算机信息系统罪，判处有期徒刑五年三个月，罚金人民币五万元。三、被告人祝东犯非法控制计算机信息系统罪，判处有期徒刑五年，罚金人民币四万元。四、被告人姜宇豪犯非法控制计算机信息系统罪，判处有期徒刑二年六个月，罚金人民币二万元。一审宣判后，被告人姜宇豪以一审量刑过重为由提出上诉，其辩护人请求对被告人姜宇豪宣告缓刑。江苏省南京市中级人民法院于 2019 年 9 月 16 日作出（2019）苏 01 刑终 768 号裁定：驳回上诉，维持原判。

裁判理由

法院生效裁判认为，被告人张竣杰、彭玲珑、祝东、姜宇豪共同违反国家规定，对我国境内计算机信息系统实施非法控制，情节特别严重,其行为均已构成非法控制计算机信息系统罪，且系共同犯罪。南京市鼓楼区人民检察院指控被告人张竣杰、彭玲珑、祝东、姜宇豪实施侵犯计算机信息系统犯罪的事实清楚，证据确实、充分，但以破坏计算机信息系统罪予以指控不当。经查，被告人张竣杰、彭玲珑、祝东、姜宇豪虽对目标服务器的数据实施了修改、增加的侵犯行为，但未造成该信息系统功能实质性的破坏，或不能正常运行，也未对该信息系统内有价值的数据进行增加、删改，其行为不属于破坏计算机信息系统犯罪中的对计算机信息系统中存储、处理或者传输的数据进行删除、修改、增加的行为，应认定为非法控制计算机信息系统罪。部分被告人及辩护人提出相同定性的辩解、辩护意见，予以采纳。关于上诉人姜宇豪提出“量刑过重”的上诉理由及辩护人提出宣告缓刑的辩护意见，经查，该上诉人及其他被告人链接被植入木马程序的目标服务器共计 113 台，属于情节特别严重。一审法院依据本案的犯罪事实和上诉人的犯罪情节，对上诉人减轻处罚，量刑适当且与其他被告人的刑期均衡。综合上诉人犯罪行为的性质、所造成的后果及其社会危害性，不宜对上诉人适用缓刑。故对上诉理由及辩护意见，不予采纳。

（二）破坏计算机信息系统罪

1.最高人民检察院关于印发最高人民检察院第十八批指导性案例的通知（高检发办字[2020]21 号）

各级人民检察院：

经 2020 年 1 月 3 日最高人民检察院第十三届检察委员会第三十一次会议通过，现将张凯闵等 52 人电信网络诈骗案等三件指导性案例（检例第 67－69 号）作为第十八批指导性案例发布，供参照适用。

最高人民检察院

2020 年 3 月 28

检例第 69 号：姚晓杰等 11 人破坏计算机信息系统案

【关键词】

破坏计算机信息系统　网络攻击 引导取证 损失认定

【要旨】

为有效打击网络攻击犯罪，检察机关应加强与公安机关的配合，及时介入侦查引导取证，结合案件特点提出明确具体的补充侦查意见。对被害互联网企业提供的证据和技术支持意见，应当结合其他证据进行审查认定，客观全面准确认定破坏计算机信息系统罪的危害后果。

【基本案情】

被告人姚晓杰，男，1983 年 3 月 27 日出生，无固定职业。

被告人丁虎子，男，1998 年 2 月 7 日出生，无固定职业。

其他 9 名被告人基本情况略。

2017 年初，被告人姚晓杰等人接受王某某（另案处理）雇佣，招募多名网络技术人员，在境外成立“暗夜小组”黑客组织。“暗夜小组”从被告人丁虎子等 3 人处购买大量服务器

资源，再利用木马软件操控控制端服务器实施 DDoS 攻击（指黑客通过远程控制服务器或计算机等资源，对目标发动高频服务请求，使目标服务器因来不及处理海量请求而瘫痪）。2017 年 2-3 月间，“暗夜小组”成员三次利用 14 台控制端服务器下的计算机，持续对某互联网公司云服务器上运营的三家游戏公司的客户端 IP 进行 DDoS 攻击。攻击导致三家游戏公司的 IP 被封堵，出现游戏无法登录、用户频繁掉线、游戏无法正常运行等问题。为恢复云服务器的正常运营，某互联网公司组织人员对服务器进行了抢修并为此支付 4 万余元。

【指控与证明犯罪】

（一）介入侦查引导取证

2017 年初，某互联网公司网络安全团队在日常工作中监测到多起针对该公司云服务器的大流量高峰值 DDoS 攻击，攻击源 IP 地址来源不明，该公司随即报案。公安机关立案后，同步邀请广东省深圳市人民检察院介入侦查、引导取证。

针对案件专业性、技术性强的特点，深圳市人民检察院会同公安机关多次召开案件讨论会，就被害单位云服务器受到的 DDoS 攻击的特点和取证策略进行研究，建议公安机关及时将被害单位报案提供的电子数据送国家计算机网络应急技术处理协调中心广东分中心进行分析，确定主要攻击源的 IP 地址。

2017 年 6-9 月间，公安机关陆续将 11 名犯罪嫌疑人抓获。侦查发现，“暗夜小组”成员为逃避打击，在作案后已串供并将手机、笔记本电脑等作案工具销毁或者进行了加密处理。“暗夜小组”成员到案后大多作无罪辩解。有证据证实丁虎子等人实施了远程控制大量计算机的行为，但证明其将控制权出售给“暗夜小组”用于 DDoS 网络攻击的证据薄弱。

鉴于此，深圳市检察机关与公安机关多次会商研究“暗夜小组”团伙内部结构、犯罪行为和技术特点等问题，建议公安机关重点做好以下三方面工作：一是查明导致云服务器不能正常运行的原因与“暗夜小组”攻击行为间的关系。具体包括：对被害单位提供的受攻击 IP 和近 20 万个攻击源 IP 作进一步筛查分析，找出主要攻击源的 IP 地址，并与丁虎子等人出售的控制端服务器 IP 地址进行比对；查清主要攻击源的波形特征和网络协议，并和丁虎子等人控制的攻击服务器特征进行比对，以确定主要攻击是否来自于该控制端服务器；查清攻击时间和云服务器因被攻击无法为三家游戏公司提供正常服务的时间；查清攻击的规模；调取“暗夜小组”实施攻击后给三家游戏公司发的邮件。二是做好犯罪嫌疑人线上身份和线下身份同一性的认定工作，并查清“暗夜小组”各成员在犯罪中的分工、地位和作用。三是查清犯罪行为造成的危害后果。

（二）审查起诉

2017 年 9 月 19 日，公安机关将案件移送广东省深圳市南山区人民检察院审查起诉。鉴于在案证据已基本厘清“暗夜小组”实施犯罪的脉络，“暗夜小组”成员的认罪态度开始有了转变。经审查，全案基本事实已经查清，基本证据已经调取，能够认定姚晓杰等人的行为已涉嫌破坏计算机信息系统罪：一是可以认定系“暗夜小组”对某互联网公司云服务器实施了大流量攻击。国家计算机网络应急技术处理协调中心广东分中心出具的报告证实，筛选出的大流量攻击源 IP 中有 198 个 IP 为僵尸网络中的被控主机，这些主机由 14 个控制端服务器控制。通过比对丁虎子等人电脑中的电子数据，证实丁虎子等人控制的服务器就是对三家

游戏公司客户端实施网络攻击的服务器。分析报告还明确了云服务器受到的攻击类型和攻击采用的网络协议、波形特征，这些证据与“暗夜小组”成员供述的攻击资源特征一致。网络聊天内容和银行交易流水等证据证实“暗夜小组”向丁虎子等三人购买上述 14 个控制端服务器控制权的事实。电子邮件等证据进一步印证了“暗夜小组”实施攻击的事实。二是通过进一步提取犯罪嫌疑人网络活动记录、犯罪嫌疑人之间的通讯信息、资金往来等证据，结合对电子数据的分析，查清了“暗夜小组”成员虚拟身份与真实身份的对应关系，查明了小组成员在招募人员、日常管理、购买控制端服务器、实施攻击和后勤等各个环节中的分工负责情况。

审查中，检察机关发现，攻击行为造成的损失仍未查清：部分犯罪嫌疑人实施犯罪的次数，上下游间交易的证据仍欠缺。针对存在的问题，深圳市南山区人民检察院与公安机关进行了积极沟通，于 2017 年 11 月 2 日和 2018 年 1 月 16 日两次将案件退回公安机关补充侦查。一是鉴于证实受影响计算机信息系统和用户数量的证据已无法调取，本案只能以造成的经济损失认定危害后果。因此要求公安机关补充调取能够证实某互联网公司直接经济损失或为恢复网络正常运行支出的必要费用等证据，并交专门机构作出评估。二是进一步补充证实“暗夜小组”成员参与每次网络攻击具体情况以及攻击服务器控制权在“暗夜小组”与丁虎子等人间流转情况的证据。三是对丁虎子等人向“暗夜小组”提供攻击服务器控制权的主观明知证据作进一步补强。

公安机关按要求对证据作了补强和完善，全案事实已查清，案件证据确实充分，已经形成了完整的证据链条。

（三）出庭指控犯罪

2018 年 3 月 6 日，深圳市南山区人民检察院以被告人姚晓杰等 11 人构成破坏计算机信息系统罪向深圳市南山区人民法院提起公诉。4 月 27 日，法院公开开庭审理了本案。

庭审中，11 名被告人对检察机关的指控均表示无异议。部分辩护人提出以下辩护意见：一是网络攻击无处不在，现有证据不能认定三家网络游戏公司受到的攻击均是“暗夜小组”发动的，不能排除攻击来自其他方面。二是即便认定“暗夜小组”参与对三家网络游戏公司的攻击，也不能将某互联网公司支付给抢修系统数据的员工工资认定为本案的经济损失。

针对辩护意见，公诉人答辩如下：一是案发时并不存在其他大规模网络攻击，在案证据足以证实只有“暗夜小组”针对云服务器进行了 DDoS 高流量攻击，每次的攻击时间和被攻击的时间完全吻合，攻击手法、流量波形、攻击源 IP 和攻击路径与被告人供述及其他证据相互印证，现有证据足以证明三家网络游戏公司客户端不能正常运行系受“暗夜小组”攻击导致。二是根据法律规定，“经济损失”包括危害计算机信息系统犯罪行为给用户直接造成的经济损失以及用户为恢复数据、功能而支出的必要费用。某互联网公司为修复系统数据、功能而支出的员工工资系因犯罪产生的必要费用，应当认定为本案的经济损失。

（四）处理结果

2018 年 6 月 8 日，广东省深圳市南山区人民法院判决认定被告人姚晓杰等 11 人犯破坏计算机信息系统罪；鉴于各被告人均表示认罪悔罪，部分被告人具有自首等法定从轻、减轻

处罚情节，对 11 名被告人分别判处有期徒刑一年至二年不等。宣判后，11 名被告人均未提出上诉，判决已生效。

【指导意义】

（一）立足网络攻击犯罪案件特点引导公安机关收集调取证据。对重大、疑难、复杂的网络攻击类犯罪案件，检察机关可以适时介入侦查引导取证，会同公安机关研究侦查方向，在收集、固定证据等方面提出法律意见。一是引导公安机关及时调取证明网络攻击犯罪发生、证明危害后果达到追诉标准的证据。委托专业技术人员对收集提取到的电子数据等进行检验、鉴定，结合在案其他证据，明确网络攻击类型、攻击特点和攻击后果。二是引导公安机关调取证明网络攻击是犯罪嫌疑人实施的证据。借助专门技术对攻击源进行分析，溯源网络犯罪路径。审查认定犯罪嫌疑人网络身份与现实身份的同一性时，可通过核查 IP 地址、网络活动记录、上网终端归属，以及证实犯罪嫌疑人与网络终端、存储介质间的关联性综合判断。犯罪嫌疑人在实施网络攻击后，威胁被害人的证据可作为认定攻击事实和因果关系的证据。有证据证明犯罪嫌疑人实施了攻击行为，网络攻击类型和特点与犯罪嫌疑人实施的攻击一致，攻击时间和被攻击时间吻合的，可以认定网络攻击系犯罪嫌疑人实施。三是网络攻击类犯罪多为共同犯罪，应重点审查各犯罪嫌疑人的供述和辩解、手机通信记录等，通过审查自供和互证的情况以及与其他证据间的印证情况，查明各犯罪嫌疑人间的犯意联络、分工和作用，准确认定主、从犯。四是对需要通过退回补充侦查进一步完善上述证据的，在提出补充侦查意见时，应明确列出每一项证据的补侦目的，以及为了达到目的需要开展的工作。在补充侦查过程中，要适时与公安机关面对面会商，了解和掌握补充侦查工作的进展，共同研究分析补充到的证据是否符合起诉和审判的标准和要求，为补充侦查工作提供必要的引导和指导。

（二）对被害单位提供的证据和技术支持意见需结合其他在案证据作出准确认定。网络攻击类犯罪案件的被害人多为大型互联网企业。在打击该类犯罪的过程中，司法机关往往会借助被攻击的互联网企业在网络技术、网络资源和大数据等方面的优势，进行溯源分析或对攻击造成的危害进行评估。由于互联网企业既是受害方，有时也是技术支持协助方，为确保被害单位提供的证据客观真实，必须特别注意审查取证过程的规范性；有条件的，应当聘请专门机构对证据的完整性进行鉴定。如条件不具备，应当要求提供证据的被害单位对证据作出说明。同时要充分运用印证分析审查思路，将被害单位提供的证据与在案其他证据，如从犯罪嫌疑人处提取的电子数据、社交软件聊天记录、银行流水、第三方机构出具的鉴定意见、证人证言、犯罪嫌疑人供述等证据作对照分析，确保不存在人为改变案件事实或改变案件危害后果的情形。

（三）对破坏计算机信息系统的危害后果应作客观全面准确认定。实践中，往往倾向于依据犯罪违法所得数额或造成的经济损失认定破坏计算机信息系统罪的危害后果。但是在一些案件中，违法所得或经济损失并不能全面、准确反映出犯罪行为所造成的危害。有的案件违法所得或者经济损失的数额并不大，但网络攻击行为导致受影响的用户数量特别大，有的导致用户满意度降低或用户流失，有的造成了恶劣社会影响。对这类案件，如果仅根据违法所得或经济损失数额来评估危害后果，可能会导致罪刑不相适应。因此，在办理破坏计算机信息系统犯罪案件时，检察机关应发挥好介入侦查引导取证的作用，及时引导公安机关按照法律规定，从扰乱公共秩序的角度，收集、固定能够证实受影响的计算机信息系统数量或用户数量、受影响或被攻击的计算机信息系统不能正常运行的累计时间、对被害企业造成的影响等证据，对危害后果作出客观、全面、准确认定，做到罪责相当、罚当其罪，使被告人受

到应有惩处。

【相关规定】

《中华人民共和国刑法》第二百八十六条

《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》第四条、第六条、第十一条

2.最高人民法院关于发布第 20 批指导性案例的通知（法〔2018〕347 号）

各省、自治区、直辖市高级人民法院，解放军军事法院，新疆维吾尔自治区高级人民法院生产建设兵团分院：

经最高人民法院审判委员会讨论决定，现将付宣豪、黄子超破坏计算机信息系统案等五个案例（指导案例 102-106 号），作为第 20 批指导性案例发布，供在审判类似案件时参照。

最高人民法院

2018 年 12 月 25 日

指导案例 102 号：付宣豪、黄子超破坏计算机信息系统案

（最高人民法院审判委员会讨论通过 2018 年 12 月 25 日发布）

关键词　刑事/破坏计算机信息系统罪/DNS 劫持/后果严重/后果特别严重

裁判要点

1.通过修改路由器、浏览器设置、锁定主页或者弹出新窗口等技术手段，强制网络用户访问指定网站的“DNS 劫持”行为，属于破坏计算机信息系统，后果严重的，构成破坏计算机信息系统罪。

2.对于“DNS 劫持”，应当根据造成不能正常运行的计算机信息系统数量、相关计算机信息系统不能正常运行的时间，以及所造成的损失或者影响等，认定其是“后果严重”还是“后果特别严重”。

相关法条

《中华人民共和国刑法》第 286 条

基本案情

2013 年底至 2014 年 10 月，被告人付宣豪、黄子超等人租赁多台服务器，使用恶意代码修改互联网用户路由器的 DNS 设置，进而使用户登录“2345.com”等导航网站时跳转至其设置的“5w.com”导航网站，被告人付宣豪、黄子超等人再将获取的互联网用户流量出售给杭州久尚科技有限公司（系“5w.com”导航网站所有者），违法所得合计人民币 754，762.34 元。

2014 年 11 月 17 日，被告人付宣豪接民警电话通知后自动至公安机关，被告人黄子超主动投案，二被告人到案后均如实供述了上述犯罪事实。

被告人及辩护人对罪名及事实均无异议。

裁判结果

上海市浦东新区人民法院于 2015 年 5 月 20 日作出（2015）浦刑初字第 1460 号刑事判决：一、被告人付宣豪犯破坏计算机信息系统罪，判处有期徒刑三年，缓刑三年。二、被告人黄子超犯破坏计算机信息系统罪，判处有期徒刑三年，缓刑三年。三、扣押在案的作案工具以及退缴在案的违法所得予以没收，上缴国库。一审宣判后，二被告人均未上诉，公诉机关未抗诉，判决已发生法律效力。

裁判理由

法院生效裁判认为，根据《中华人民共和国刑法》第二百八十六条的规定，对计算机信息系统功能进行破坏，造成计算机信息系统不能正常运行，后果严重的，构成破坏计算机信息系统罪。本案中，被告人付宣豪、黄子超实施的是流量劫持中的“DNS 劫持”。DNS 是域名系统的英文首字母缩写，作用是提供域名解析服务。“DNS 劫持”通过修改域名解析，使对特定域名的访问由原 IP 地址转入到篡改后的指定 IP 地址，导致用户无法访问原 IP 地址对应的网站或者访问虚假网站，从而实现窃取资料或者破坏网站原有正常服务的目的。二被告人使用恶意代码修改互联网用户路由器的 DNS 设置，将用户访问“2345.com”等导航网站的流量劫持到其设置的“5w.com”导航网站，并将获取的互联网用户流量出售，显然是对网络用户的计算机信息系统功能进行破坏，造成计算机信息系统不能正常运行，符合破坏计算机信息系统罪的客观行为要件。

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》，破坏计算机信息系统，违法所得人民币二万五千元以上或者造成经济损失人民币五万元以上的，应当认定为“后果特别严重”。本案中，二被告人的违法所得达人民币 754，762.34 元，属于“后果特别严重”。

综上，被告人付宣豪、黄子超实施的“DNS 劫持”行为系违反国家规定，对计算机信息系统中存储的数据进行修改，后果特别严重，依法应处五年以上有期徒刑。鉴于二被告人在家属的帮助下退缴全部违法所得，未获取、泄露公民个人信息，且均具有自首情节，无前科劣迹，故依法对其减轻处罚并适用缓刑。

（生效裁判审判人员：李俊、白艳利、朱根初）

指导案例 103 号：徐强破坏计算机信息系统案

（最高人民法院审判委员会讨论通过 2018 年 12 月 25 日发布）

关键词　刑事/破坏计算机信息系统罪/机械远程监控系统

裁判要点

企业的机械远程监控系统属于计算机信息系统。违反国家规定，对企业的机械远程监控系统功能进行破坏，造成计算机信息系统不能正常运行，后果严重的，构成破坏计算机信息系统罪。

相关法条

《中华人民共和国刑法》第 286 条第 1 款、第 2 款

基本案情

为了加强对分期付款的工程机械设备的管理，中联重科股份有限公司（以下简称中联重科）投入使用了中联重科物联网 GPS 信息服务系统，该套计算机信息系统由中联重科物联网远程监控平台、GPS 终端、控制器和显示器等构成，该系统具备自动采集、处理、存储、回传、显示数据和自动控制设备的功能，其中，控制器、GPS 终端和显示器由中联重科在工程机械设备的生产制造过程中安装到每台设备上。

中联重科对“按揭销售”的泵车设备均安装了中联重科物联网 GPS 信息服务系统，并在产品买卖合同中明确约定“如买受人出现违反合同约定的行为，出卖人有权采取停机、锁机等措施”以及“在买受人付清全部货款前，产品所有权归出卖人所有。即使在买受人已经获得机动车辆登记文件的情况下，买受人未付清全部货款前，产品所有权仍归出卖人所有”的条款。然后由中联重科总部的远程监控维护平台对泵车进行监控，如发现客户有拖欠、赖账等情况，就会通过远程监控系统进行“锁机”，泵车接收到“锁机”指令后依然能发动，但不能作业。

2014 年 5 月间，被告人徐强使用“GPS 干扰器”先后为钟某某、龚某某、张某某名下

或管理的五台中联重科泵车解除锁定。具体事实如下：

1.2014 年 4 月初，钟某某发现其购得的牌号为贵 A77462 的泵车即将被中联重科锁机后，安排徐关伦帮忙打听解锁人。徐某某遂联系龚某某告知钟某某泵车需解锁一事。龚某某表示同意后，即通过电话联系被告人徐强给泵车解锁。2014 年 5 月 18 日，被告人徐强携带“GPS 干扰器”与龚某某一起来到贵阳市清镇市，由被告人徐强将“GPS 干扰器”上的信号线连接到泵车右侧电控柜，再将“GPS 干扰器”通电后使用干扰器成功为牌号为贵 A77462 的泵车解锁。事后，钟某某向龚某某支付了解锁费用人民币 40000 元，龚某某亦按约定将其中人民币 9600 元支付给徐某某作为介绍费。当日及次日，龚某某还带着被告人徐强为其管理的其妹夫黄某从中联重科及长沙中联重科二手设备销售有限公司以分期付款方式购得的牌号分别为湘 AB0375、湘 AA6985、湘 AA6987 的三台泵车进行永久解锁。事后，龚某某向被告人徐强支付四台泵车的解锁费用共计人民币 30000 元。

2.2014 年 5 月间，张某某从中联重科以按揭贷款的方式购买泵车一台，因拖欠货款被中联重科使用物联网系统将泵车锁定，无法正常作业。张某某遂通过电话联系到被告人徐强为其泵车解锁。2014 年 5 月 17 日，被告人徐强携带“GPS 干扰器”来到湖北襄阳市，采用上述同样的方式为张某某名下牌号为鄂 FE7721 的泵车解锁。事后，张某某向被告人徐强支付解锁费用人民币 15000 元。

经鉴定，中联重科的上述牌号为贵 A77462、湘 AB0375、湘 AA6985、湘 AA6987 泵车 GPS 终端被拆除及控制程序被修改后，中联重科物联网 GPS 信息服务系统无法对泵车进行实时监控和远程锁车。

2014 年 11 月 7 日，被告人徐强主动到公安机关投案。在本院审理过程中，被告人徐强退缴了违法所得人民币 45000 元。

裁判结果

湖南省长沙市岳麓区人民法院于 2015 年 12 月 17 日作出（2015）岳刑初字第 652 号刑事判决：一、被告人徐强犯破坏计算机信息系统罪，判处有期徒刑二年六个月。二、追缴被告人徐强的违法所得人民币四万五千元，上缴国库。被告人徐强不服，提出上诉。湖南省长沙市中级人民法院于 2016 年 8 月 9 日作出（2016）湘 01 刑终 58 号刑事裁定：驳回上诉，维持原判。该裁定已发生法律效力。

裁判理由

法院生效裁判认为，《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》第十一条规定，“计算机信息系统”和“计算机系统”，是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。本案中，中联重科物联网 GPS 信息服务系统由中联重科物联网远程监控平台、GPS 终端、控制器和显示器等构成，具备自动采集、处理、存储、回传、显示数据和自动控制设备的功能。该系统属于具备自动处理数据功能的通信设备与自动化控制设备，属于刑法意义上的计算机信息系统。被告人徐强利用“GPS 干扰器”对中联重科物联网 GPS 信息服务系统进行修改、干扰，造成该系统无法对案涉泵车进行实时监控和远程锁车，是对计算机信息系统功能进行破坏，造成计算机信息系统不能正常运行的行为，且后果特别严重。根据刑法第二百八十六条的规定，被告人徐强构成破坏计算机信息系统罪。徐强犯罪以后自动投案，如实供述了自己的罪行，系自首，依法可减轻处罚。徐强退缴全部违法所得，有悔罪表现，可酌情从轻处罚。针对徐强及辩护人提出“自己系自首，且全部退缴违法所得，一审量刑过重”的上诉意见与辩护意见，经查，徐强破坏计算机信息系统，违法所得 45000 元，后果特别严重，应当判处五年以上有期徒刑，一审判决综合考虑其自首、退缴全部违法所得等情节，对其减轻处罚，判处有期徒刑二年六个月，量刑适当。该上诉意见、辩护意见，不予采纳。原审判决认定事实清楚，证据确实充分，适用法律正确，量刑适当，审判程序合法。

（生效裁判审判人员：黎璠、刘刚、何琳）

指导案例 104 号：李森、何利民、张锋勃等人破坏计算机信息系统案

（最高人民法院审判委员会讨论通过 2018 年 12 月 25 日发布）

关键词　刑事/破坏计算机信息系统罪/干扰环境质量监测

采样/数据失真/后果严重

裁判要点

环境质量监测系统属于计算机信息系统。用棉纱等物品堵塞环境质量监测采样设备，干扰采样，致使监测数据严重失真的，构成破坏计算机信息系统罪。

相关法条

《中华人民共和国刑法》第 286 条第 1 款

基本案情

西安市长安区环境空气自动监测站（以下简称长安子站）系国家环境保护部（以下简称环保部）确定的西安市 13 个国控空气站点之一，通过环境空气质量自动监测系统采集、处理监测数据，并将数据每小时传输发送至中国环境监测总站（以下简称监测总站），一方面通过网站实时向社会公布，一方面用于编制全国环境空气质量状况月报、季报和年报，向全国发布。长安子站为全市两个国家直管监测子站之一，由监测总站委托武汉宇虹环保产业股份有限公司进行运行维护，不经允许，非运维方工作人员不得擅自进入。

2016 年 2 月 4 日，长安子站回迁至西安市长安区西安邮电大学南区动力大楼房顶。被告人李森利用协助子站搬迁之机私自截留子站钥匙并偷记子站监控电脑密码，此后至 2016 年 3 月 6 日间，被告人李森、张锋勃多次进入长安子站内，用棉纱堵塞采样器的方法，干扰子站内环境空气质量自动监测系统的数据采集功能。被告人何利民明知李森等人的行为而没有阻止，只是要求李森把空气污染数值降下来。被告人李森还多次指使被告人张楠、张肖采用上述方法对子站自动监测系统进行干扰，造成该站自动监测数据多次出现异常，多个时间段内监测数据严重失真，影响了国家环境空气质量自动监测系统正常运行。为防止罪行败露，2016 年 3 月 7 日、3 月 9 日，在被告人李森的指使下，被告人张楠、张肖两次进入长安子站将监控视频删除。2016 年 2、3 月间，长安子站每小时的监测数据已实时传输发送至监测总站，通过网站向社会公布，并用于环保部编制 2016 年 2 月、3 月和第一季度全国 74 个城市空气质量状况评价、排名。2016 年 3 月 5 日，监测总站在例行数据审核时发现长安子站数据明显偏低，检查时发现了长安子站监测数据弄虚作假问题，后公安机关将五被告人李森、何利民、张楠、张肖、张锋勃抓获到案。被告人李森、被告人张锋勃、被告人张楠、被告人张肖在庭审中均承认指控属实，被告人何利民在庭审中辩解称其对李森堵塞采样器的行为仅是默许、放任，请求宣告其无罪。

裁判结果

陕西省西安市中级人民法院于 2017 年 6 月 15 日作出（2016）陕 01 刑初 233 号刑事判决：一、被告人李森犯破坏计算机信息系统罪，判处有期徒刑一年十个月。二、被告人何利民犯破坏计算机信息系统罪，判处有期徒刑一年七个月。三、被告人张锋勃犯破坏计算机信息系统罪，判处有期徒刑一年四个月。四、被告人张楠犯破坏计算机信息系统罪，判处有期徒刑一年三个月。五、被告人张肖犯破坏计算机信息系统罪，判处有期徒刑一年三个月。宣判后，各被告人均未上诉，判决已发生法律效力。

裁判理由

法院生效裁判认为，五被告人的行为违反了国家规定。《中华人民共和国环境保护法》第六十八条规定禁止篡改、伪造或者指使篡改、伪造监测数据，《中华人民共和国环境大气

污染防治法》第一百二十六条规定禁止对大气环境保护监督管理工作弄虚作假，《中华人民共和国环境计算机信息系统安全保护条例》第七条规定不得危害计算机信息系统的安全。本案五被告人采取堵塞采样器的方法伪造或者指使伪造监测数据，弄虚作假，违反了上述国家规定。

五被告人的行为破坏了计算机信息系统。《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》第十一条规定，计算机信息系统和计算机系统，是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。根据《最高人民法院、最高人民检察院关于办理环境污染刑事案件适用法律若干问题的解释》第十条第一款的规定，干扰环境质量监测系统的采样，致使监测数据严重失真的行为，属于破坏计算机信息系统。长安子站系国控环境空气质量自动监测站点，产生的监测数据经过系统软件直接传输至监测总站，通过环保部和监测总站的政府网站实时向社会公布，参与计算环境空气质量指数并实时发布。空气采样器是环境空气质量监测系统的重要组成部分。PM10、PM2.5 监测数据作为环境空气综合污染指数评估中的最重要两项指标，被告人用棉纱堵塞采样器的采样孔或拆卸采样器的行为，必然造成采样器内部气流场的改变，造成监测数据失真，影响对环境空气质量的正确评估，属于对计算机信息系统功能进行干扰，造成计算机信息系统不能正常运行的行为。

五被告人的行为造成了严重后果。（1）被告人李森、张锋勃、张楠、张肖均多次堵塞、拆卸采样器干扰采样，被告人何利民明知李森等人的行为而没有阻止，只是要求李森把空气污染数值降下来。（2）被告人的干扰行为造成了监测数据的显著异常。2016 年 2 至 3 月间，长安子站颗粒物监测数据多次出现与周边子站变化趋势不符的现象。长安子站 PM2.5 数据分别在 2 月 24 日 18 时至 25 日 16 时、3 月 3 日 4 时至 6 日 19 时两个时段内异常，PM10 数据分别在 2 月 18 日 18 时至 19 日 8 时、2 月 25 日 20 时至 21 日 8 时、3 月 5 日 19 时至 6 日 23 时三个时段内异常。其中，长安子站的 PM10 数据在 2016 年 3 月 5 日 19 时至 22 时由 361 下降至 213，下降了 41%，其他周边子站均值升高了 14%（由 316 上升至 361），6 日 16 时至 17 时长安子站监测数值由 188 上升至 426，升高了 127%，其他子站均值变化不大（由 318 降至 310），6 日 17 时至 19 时长安子站数值由 426 下降至 309，下降了 27%，其他子站均值变化不大（由 310 降至 304）。可见，被告人堵塞采样器的行为足以造成监测数据的严重失真。上述数据的严重失真，与监测总站在例行数据审核时发现长安子站 PM10 数据明显偏低可以印证。（3）失真的监测数据已实时发送至监测总站，并向社会公布。长安子站空气质量监测的小时浓度均值数据已经通过互联网实时发布。（4）失真的监测数据已被用于编制环境评价的月报、季报。环保部在 2016 年二、三月及第一季度的全国 74 个重点城市空气质量排名工作中已采信上述虚假数据，已向社会公布并上报国务院，影响了全国大气环境治理情况评估，损害了政府公信力，误导了环境决策。据此，五被告人干扰采样的行为造成了严重后果，符合刑法第二百八十六条规定的“后果严重”要件。

综上，五被告人均已构成破坏计算机信息系统罪。鉴于五被告人到案后均能坦白认罪，有悔罪表现，依法可以从轻处罚。

（生效裁判审判人员：张燕萍、骆成兴、袁兵）

3.最高人民检察院关于印发最高人民检察院第九批指导性案例的通知（高检发研字[2017]10号）

各省、自治区、直辖市人民检察院，解放军军事检察院，新疆生产建设兵团人民检察院：

经 2017 年 10 月 10 日最高人民检察院第十二届检察委员会第七十次会议决定，现将李丙龙破坏计算机信息系统案等六件指导性案例（检例第 33－38 号）作为第九批指导性案例发布，供参照适用。

最高人民检察院
2017 年 10 月 12 日

检例第 33 号：李丙龙破坏计算机信息系统案

【关键词】

破坏计算机信息系统　劫持域名

【基本案情】

被告人李丙龙，男，1991 年 8 月生，个体工商户。

被告人李丙龙为牟取非法利益，预谋以修改大型互联网网站域名解析指向的方法，劫持互联网流量访问相关赌博网站，获取境外赌博网站广告推广流量提成。2014 年 10 月 20 日，李丙龙冒充某知名网站工作人员，采取伪造该网站公司营业执照等方式，骗取该网站注册服务提供商信任，获取网站域名解析服务管理权限。10 月 21 日，李丙龙通过其在域名解析服务网站平台注册的账号，利用该平台相关功能自动生成了该知名网站二级子域名部分 DNS（域名系统）解析列表，修改该网站子域名的 IP 指向，使其连接至自己租用境外虚拟服务器建立的赌博网站广告发布页面。当日 19 时许，李丙龙对该网站域名解析服务器指向的修改生效，致使该网站不能正常运行。23 时许，该知名网站经技术排查恢复了网站正常运行。11 月 25 日，李丙龙被公安机关抓获。至案发时，李丙龙未及获利。

经司法鉴定，该知名网站共有 559 万有效用户，其中邮箱系统有 36 万有效用户。按日均电脑客户端访问量计算，10 月 7 日至 10 月 20 日邮箱系统日均访问量达 12.3 万。李丙龙的行为造成该知名网站 10 月 21 日 19 时至 23 时长达四小时左右无法正常发挥其服务功能，案发当日仅邮件系统电脑客户端访问量就从 12.3 万减少至 4.43 万。

【诉讼过程和结果】

本案由上海市徐汇区人民检察院于 2015 年 4 月 9 日以被告人李丙龙犯破坏计算机信息系统罪向上海市徐汇区人民法院提起公诉。11 月 4 日，徐汇区人民法院作出判决，认定李丙龙的行为构成破坏计算机信息系统罪。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》第四条规定，李丙龙的行为符合“造成为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上”“后果特别严重”的情形。结合量刑情节，判处李丙龙有期徒刑五年。一审宣判后，被告人李丙龙提出上诉，经上海市第一中级人民法院终审裁定，维持原判。

【要旨】

以修改域名解析服务器指向的方式劫持域名，造成计算机信息系统不能正常运行，是破坏计算机信息系统的行为。

【指导意义】

修改域名解析服务器指向，强制用户偏离目标网站或网页进入指定网站或网页，是典型的域名劫持行为。行为人使用恶意代码修改目标网站域名解析服务器，目标网站域名被恶意解析到其他 IP 地址，无法正常发挥网站服务功能，这种行为实质是对计算机信息系统功能的修改、干扰，符合刑法第二百八十六条第一款“对计算机信息系统功能进行删除、修改、增加、干扰”的规定。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》第四条的规定，造成为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的，属于“后果严重”，应以破坏计算机信息系统罪论处；造成为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的，属于“后果特别严重”。

认定遭受破坏的计算机信息系统服务用户数，可以根据计算机信息系统的功能和使用特点，结合网站注册用户、浏览用户等具体情况，作出客观判断。

【相关法律规定】
《中华人民共和国刑法》

第二百八十六条　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。

《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》

第四条　破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”：

……

（四）造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

……

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

……

（二）造成为五百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；

检例第 34 号：李骏杰等破坏计算机信息系统案

【关键词】
破坏计算机信息系统　删改购物评价　购物网站评价系统

【基本案情】
被告人李骏杰，男，1985 年 7 月生，原系浙江杭州某网络公司员工。

被告人胡榕，男，1975 年 1 月生，原系江西省九江市公安局民警。

被告人黄福权，男，1987 年 9 月生，务工。

被告人董伟，男，1983 年 5 月生，无业。

被告人王凤昭，女，1988 年 11 月生，务工。

2011 年 5 月至 2012 年 12 月，被告人李骏杰在工作单位及自己家中，单独或伙同他人通过聊天软件联系需要修改中差评的某购物网站卖家，并从被告人黄福权等处购买发表中差评的该购物网站买家信息 300 余条。李骏杰冒用买家身份，骗取客服审核通过后重置账号密码，登录该购物网站内部评价系统，删改买家的中差评 347 个，获利 9 万余元。

经查：被告人胡榕利用职务之便，将获取的公民个人信息分别出售给被告人黄福权、董伟、王凤昭。

2012 年 12 月 11 日，被告人李骏杰被公安机关抓获归案。此后，因涉嫌出售公民个人信息、非法获取公民个人信息，被告人胡榕、黄福权、董伟、王凤昭等人也被公安机关先后抓获。

【诉讼过程和结果】

本案由浙江省杭州市滨江区人民检察院于 2014 年 3 月 24 日以被告人李骏杰犯破坏计算机信息系统罪、被告人胡榕犯出售公民个人信息罪、被告人黄福权等人犯非法获取公民个人信息罪，向浙江省杭州市滨江区人民法院提起公诉。2015 年 1 月 12 日，杭州市滨江区人民法院作出判决，认定被告人李骏杰的行为构成破坏计算机信息系统罪，判处有期徒刑五年；被告人胡榕的行为构成出售公民个人信息罪，判处有期徒刑十个月，并处罚金人民币二万元；被告人黄福权、董伟、王凤昭的行为构成非法获取公民个人信息罪，分别判处有期徒刑、拘役，并处罚金。一审宣判后，被告人董伟提出上诉。杭州市中级人民法院二审裁定驳回上诉，维持原判。判决已生效。

【要旨】

冒用购物网站买家身份进入网站内部评价系统删改购物评价，属于对计算机信息系统内存储数据进行修改操作，应当认定为破坏计算机信息系统的行为。

【指导意义】

购物网站评价系统是对店铺销量、买家评价等多方面因素进行综合计算分值的系统，其内部储存的数据直接影响到搜索流量分配、推荐排名、营销活动报名资格、同类商品在消费者购买比较时的公平性等。买家在购买商品后，根据用户体验对所购商品分别给出好评、中评、差评三种不同评价。所有的评价都是以数据形式存储于买家评价系统之中，成为整个购物网站计算机信息系统整体数据的重要组成部分。

侵入评价系统删改购物评价，其实质是对计算机信息系统内存储的数据进行删除、修改操作的行为。这种行为危害到计算机信息系统数据采集和流量分配体系运行，使网站注册商户及其商品、服务的搜索受到影响，导致网站商品、服务评价功能无法正常运作，侵害了购物网站所属公司的信息系统安全和消费者的知情权。行为人因删除、修改某购物网站中差评

数据违法所得

25000 元以上，构成破坏计算机信息系统罪，属于“后果特别严重”的情形，应当依法判处五年以上有期徒刑。

【相关法律规定】
《中华人民共和国刑法》

第二百八十六条　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。

《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》

第四条　破坏计算机信息系统功能、数据或者应用程序，具有下列情形之一的，应当认定为刑法第二百八十六条第一款和第二款规定的“后果严重”：

……

（三）违法所得五千元以上或者造成经济损失一万元以上的；

……

实施前款规定行为，具有下列情形之一的，应当认定为破坏计算机信息系统“后果特别严重”：

（一）数量或者数额达到前款第（一）项至第（三）项规定标准五倍以上的；

……

《计算机信息网络国际联网安全保护管理办法》

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

检例第 35 号：曾兴亮、王玉生破坏计算机信息系统案

【关键词】

破坏计算机信息系统　智能手机终端　远程锁定

【基本案情】

被告人曾兴亮，男，1997 年 8 月生，农民。

被告人王玉生，男，1992 年 2 月生，农民。

2016 年 10 月至 11 月，被告人曾兴亮与王玉生结伙或者单独使用聊天社交软件，冒充年轻女性与被害人聊天，谎称自己的苹果手机因故障无法登录“iCloud”（云存储），请被害人代为登录，诱骗被害人先注销其苹果手机上原有的 ID，再使用被告人提供的 ID 及密码登录。随后，曾、王二人立即在电脑上使用新的 ID 及密码登录苹果官方网站，利用苹果手机相关功能将被害人的手机设置修改，并使用“密码保护问题”修改该 ID 的密码，从而远程锁定被害人的苹果手机。曾、王二人再在其个人电脑上，用网络聊天软件与被害人联系，以解锁为条件索要钱财。采用这种方式，曾兴亮单独或合伙作案共 21 起，涉及苹果手机 22 部，锁定苹果手机 21 部，索得人民币合计 7290 元；王玉生参与作案 12 起，涉及苹果手机 12 部，锁定苹果手机 11 部，索得人民币合计 4750 元。2016 年 11 月 24 日，二人被公安机关抓获。

【诉讼过程和结果】

本案由江苏省海安县人民检察院于 2016 年 12 月 23 日以被告人曾兴亮、王玉生犯破坏计算机信息系统罪向海安县人民法院提起公诉。2017 年 1 月 20 日，海安县人民法院作出判决，认定被告人曾兴亮、王玉生的行为构成破坏计算机信息系统罪，分别判处有期徒刑一年三个月、有期徒刑六个月。一审宣判后，二被告人未上诉，判决已生效。

【要旨】

智能手机终端，应当认定为刑法保护的计算机信息系统。锁定智能手机导致不能使用的行为，可认定为破坏计算机信息系统。

【指导意义】

计算机信息系统包括计算机、网络设备、通信设备、自动化控制设备等。智能手机和计算机一样，使用独立的操作系统、独立的运行空间，可以由用户自行安装软件等程序，并可以通过移动通讯网络实现无线网络接入，应当认定为刑法上的“计算机信息系统”。

行为人通过修改被害人手机的登录密码，远程锁定被害人的智能手机设备，使之成为无法开机的“僵尸机”，属于对计算机信息系统功能进行修改、干扰的行为。造成 10 台以上智能手机系统不能正常运行，符合刑法第二百八十六条破坏计算机信息系统罪构成要件中“对计算机信息系统功能进行修改、干扰”“后果严重”的情形，构成破坏计算机信息系统

罪。

行为人采用非法手段锁定手机后以解锁为条件，索要钱财，在数额较大或多次敲诈的情况下，其目的行为又构成敲诈勒索罪。在这类犯罪案件中，手段行为构成的破坏计算机信息系统罪与目的行为构成的敲诈勒索罪之间成立牵连犯。牵连犯应当从一重罪处断。破坏计算机信息系统罪后果严重的情况下，法定刑为五年以下有期徒刑或者拘役；敲诈勒索罪在数额较大的情况下，法定刑为三年以下有期徒刑、拘役或管制，并处或者单处罚金。本案应以重罪即破坏计算机信息系统罪论处。

【相关法律规定】
《中华人民共和国刑法》

第二百八十六条　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。

第二百七十四条　敲诈勒索公私财物，数额较大或者多次敲诈勒索的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑，并处罚金。

《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》

第十一条　本解释所称“计算机信息系统”和“计算机系统”，是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。

……

《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》

第一条　敲诈勒索公私财物价值二千元至五千元以上、三万元至十万元以上、三十万元至五十万元以上的，应当分别认定为刑法第二百七十四条规定的“数额较大”、“数额巨大”、“数额特别巨大”。

各省、自治区、直辖市高级人民法院、人民检察院可以根据本地区经济发展状况和社会治安状况，在前款规定的数额幅度

内，共同研究确定本地区执行的具体数额标准，报最高人民法院、最高人民检察院批准。

《江苏省高级人民法院、江苏省人民检察院、江苏省公安厅关于我省执行敲诈勒索公私财物“数额较大”、“数额巨大”、“数额特别巨大”标准的意见》

根据《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》的规定，结合我省经济发展和社会治安实际状况，确定我省执行刑法第第二百七十四条规定的敲诈勒索公私财物“数额较大”、“数额巨大”、“数额特别巨大”标准如下：

一、敲诈勒索公私财物价值人民币四千元以上的，为“数额较大”；

二、敲诈勒索公私财物价值人民币六万元以上的，为“数额巨大”；

……

4.2019 年度浙江省互联网十大检察案例之一：全国首例技术修改抖音靓号案--构成破坏计算机信息系统罪。（义乌市人民检察院）

2019 年 5 月，义乌市人民检察院对全国首例技术修改抖音靓号案提起公诉，法院依法判决被告人构成破坏计算机信息系统罪。被告人利用 DY190 易语言程序编写软件，通过破坏抖音系统后台数据的方式非法获取技术靓号 700 余个并出售给他人，部分技术靓号经修改后单价高达 1.5 万元。检察机关准确区分修改抖音号不同技术手段的罪与非罪界限，精准打击新型互联网犯罪，从源头上铲除了非法获取抖音技术靓号再进行层层销售的黑灰产业链。同时检察机关积极履行服务民营经济的职责使命，主动对接互联网企业，提示微播公司技术漏洞的风险，提高防范意识，被检察日报、今日头条等媒体广泛宣传报道。

（三）非法利用信息网络罪、帮助信息网络犯罪活动罪

1.最高人民法院发布 4 起非法利用信息网络罪、帮助信息网络犯罪活动罪典型案例（2019 年 10 月 25 日）

目录

一、黄杰明、陶胜新等非法利用信息网络案

发布有关销售管制物品的信息，情节严重的，构成非法利用信息网络罪

（一）基本案情

2017 年 7 月至 2019 年 2 月，被告人黄杰明使用昵称为“刀剑阁”的微信，在朋友圈发布其拍摄的管制刀具图片、视频和文字信息合计 12322 条，用以销售管制刀具，并从中非法获利。被告人陶胜新、李孔祥、陶霖、曾俊杰在微信朋友圈发布从他人的微信朋友圈转载的管制刀具图片、视频和文字信息，数量分别为 6677 条、16540 条、15210 条、5316 条，用以销售管制刀具，并从中非法获利。

2018 年 5 月至 7 月，宋雨林（已判刑）先后三次通过微信联系陶胜新，购买管制刀具。陶胜新通过微信与黄杰明联系，由黄杰明直接发货给宋雨林，被告人陶胜新从中赚取差价。宋雨林购得刀具后实施了故意伤害致人死亡的犯罪行为。黄杰明违法所得人民币 329 元，陶胜新违法所得人民币 858 元。

（二）裁判结果

江苏省盐城市滨海县人民法院判决认为：被告人黄杰明、陶胜新、李孔祥、曾俊杰、陶霖利用信息网络，发布有关销售管制物品的违法犯罪信息，其行为已构成非法利用信息网络罪。被告人黄杰明、陶胜新归案后，如实供述自己的犯罪事实，构成坦白，且认罪认罚，依法可以从轻处罚。被告人李孔祥、曾俊杰、陶霖自动投案，如实供述自己的犯罪事实，构成自首，且认罪认罚，依法可以从轻处罚。以非法利用信息网络罪分别判处被告人黄杰明、陶胜新有期徒刑八个月，并处罚金人民币一万元；被告人李孔祥、曾俊杰、陶霖有期徒刑七个月，缓刑一年，并处罚金人民币一万元。同时，禁止被告人李孔祥、曾俊杰、陶霖在缓刑考验期内从事网络销售及相关活动。该判决已发生法律效力。

二、谭张羽、张源等非法利用信息网络案

为实施诈骗活动发布信息，情节严重的，构成非法利用信息网络罪

（一）基本案情

2016 年 12 月，为获取非法利益，被告人谭张羽、张源商定在网络上从事为他人发送“刷单获取佣金”的诈骗信息业务，即通过“阿里旺旺”向不特定的淘宝用户发送信息，信息内容大致为“亲，我是×××，最近库存压力比较大，请你来刷单，一单能赚 10-30 元，一天能赚几百元，详情加 QQ×××，阿里旺旺不回复”。通常每 100 个人添加上述信息里的 QQ 号，谭张羽、张源即可从让其发送信息的上家处获取平均约 5000 元的费用。谭张羽、张源雇佣被告人秦秋发等具体负责发送诈骗信息。张源主要负责购买“阿里旺旺”账号、软件、租赁电脑服务器等；秦秋发主要负责招揽、联系有发送诈骗信息需求的上家、接收上家支付的费用及带领其他人发送诈骗信息。

2016 年 12 月至 2017 年 3 月，谭张羽、张源通过上述方式共非法获利约人民币 80 余万元，秦秋发在此期间以“工资”的形式非法获利人民币约 2 万元。被害人王某甲、洪某因添加谭张羽、张源等人组织发送的诈骗信息中的 QQ 号，后分别被骗 31000 元和 30049 元。

（二）裁判结果

江苏省宿迁市沭阳县人民法院一审判决、宿迁市中级人民法院二审判决认为：被告人谭张羽、张源、秦秋发以非法获利为目的，通过信息网络发送刷单诈骗信息，其行为本质上属于诈骗犯罪预备，构成非法利用信息网络罪。虽然本案中并无证据证实具体实施诈骗的行为人归案并受到刑事追究，但不影响非法利用信息网络罪的成立。谭张羽、张源、秦秋发共同实施故意犯罪，系共同犯罪。在共同犯罪中，谭张羽、张源起主要作用，均系主犯；秦秋发起次要作用，属从犯，依法予以从轻处罚。综合考虑各被告人归案后如实供述罪行以及谭张羽、张源赔偿部分受害人经济损失的情节，以非法利用信息网络罪判处被告人张源有期徒刑二年一个月，并处罚金人民币十万元；被告人谭张羽有期徒刑一年十个月，并处罚金人民币八万元；被告人秦秋发有期徒刑一年四个月，并处罚金人民币三万元。

附：张源、谭张羽等非法利用信息网络罪二审刑事判决书

宿迁市中级人民法院
刑事判决书

（2018）苏13刑终203号

原公诉机关沭阳县人民检察院。

上诉人（原审被告人）张源，男，1995年10月22日出生，汉族，学生，住广西。因涉嫌犯诈骗罪，于2017年3月18日被临时羁押于桂林市第二看守所，同月20日被刑事拘留，同年4月24日被取保候审，2018年4月8日被逮捕。现羁押于沭阳县看守所。

辩护人王建明，江苏正伍律师事务所律师。

上诉人（原审被告人）谭张羽，男，1990年11月1日出生，汉族，无业，住广西壮族自治区桂林市临桂区。曾因犯危险驾驶罪，于2012年4月25日被广西壮族自治区桂林市叠彩区人民法院判处拘役一个月，并处罚金人民币一千元。现因涉嫌犯诈骗罪，于2017年4月7日被广西柳州铁路公安处刑警支队抓获并临时羁押于广西柳州市第一看守所，同月14日被刑事拘留，同年4月24日被取保候审，2018年4月8日被逮捕。现羁押于沭阳县看守所。

辩护人仲跻文，江苏通达声远律师事务所律师。

原审被告人秦秋发，男，1987年6月25日出生，汉族，无业。曾因犯贩卖毒品罪，于2011年1月10日被广西壮族自治区桂林市七星区，并处罚金2000元。因涉嫌犯诈骗罪，于2017年3月18日被临时羁押于桂林市第二看守所，同月20日被刑事拘留，同年4月24日被取保候审，2018年4月8日被逮捕。现羁押于沭阳县看守所。

沭阳县人民法院审理沭阳县人民检察院指控原审被告人张源、谭张羽、秦秋发犯非法利用信息网络罪一案，于2018年5月9日作出2017苏1322刑初1327号刑事判决。原审被告人张源、谭张羽不服，提出上诉。本院受理后，依法组成合议庭，公开开庭审理了本案。在本院审理过程中，检察机关分别于2018年9月5日、11月28日提出延期审理建议，本院分别决定延期审理。现已审理终结。

原审法院认定，2016年10月25日，被告人谭张羽、张源共同出资注册“广西羽源信息咨询有限公司”（现已注销，以下简称羽源公司），登记业务为信息咨询（证券、期货咨询除外）、网络信息咨询、商品信息咨询；网络维护；活动策划；（依法需经批准的项目，经相关部门批准后方可开展经营活动）。

2016年12月份，因羽源公司所从事的微盘业务亏损，被告人谭张羽、张源共同商议决定并购买阿里旺旺账号、租赁电脑服务器、购买软件等，被告人秦秋发负责招揽有刷单需求的上家（即广告主），后又雇佣周遵超、王志成、唐柏芳钰进行具体测试、发送虚假广告，开始为他人从事发送“刷单获取佣金”诈骗信息的业务，即向不特定的淘宝用户发送“刷单获取佣金”的信息，信息内容大致为“你好，我是***，最近库存压力比较大，代理不给力，请你来刷单，一单能赚10-15块，一天能赚一两百，详情加QQ**×××**，阿里旺旺不回复。”每有一个人添加上述信息里的QQ号为好友，被告人谭张羽、张源就可以从找其发送

信息的上家处得到30至70元不等的报酬。

被告人谭张羽、张源、秦秋发在明知上述刷单广告不可能存在真实刷单事实，而系上家用于诈骗（刷单后不发还本金）的情况下，仍然帮助他人发布上述诈骗广告。2016年12月至2017年3月，被告人谭张羽、张源、秦秋发通过上述方式共非法获利约人民币80万元。被告人秦秋发在此期间以“工资”的形式非法获利人民币2万元,其他员工以“工资”从中获利人民币1.2万元。其中已查清因接收被告人谭张羽、张源、秦秋发发送的诈骗广告而被骗的事实分述如下：

1.2017年1月13日，王某甲（江苏沭阳人）在收到被告人谭张羽、张源、秦秋发所发送的“刷单”信息后添加其中的QQ为好友。后王某甲根据对方的要求，通过扫描二维码方式支付31000元货款进行刷单，被对方骗取应按约返还的刷单货款31000元，也未得到任何佣金。

2.2017年2月23日，洪某（安徽弋阳县人）在收到被告人谭张羽、张源、秦秋发所发送的“刷单”信息后添加其中的QQ为好友。后洪某根据对方的要求，通过扫描二维码方式支付30049元货款进行刷单，被对方骗取应按约返还的刷单货款30049元，也未得到任何佣金。

3.2017年3月7日至9日，王某乙（江苏南通人）在收到被告人谭张羽、张源、秦秋发所发送的“刷单”信息后添加其中的QQ为好友。后王某乙根据对方的要求，通过扫描二维码方式支付16480元货款进行刷单，被对方骗取应按约返还的刷单货款16480元，也未得到任何佣金。

案发后，被告人谭张羽、张源、秦秋发均被抓获归案，归案后如实供述了自己的罪行。

原审判决认定上述事实的证据，有被告人谭张羽、张源、秦秋发的供述与辩解，同案关系人周遵超、王志成、唐柏芳钰的供述，被害人王某甲、洪某、王某乙的陈述，沭阳县公安局搜查笔录、扣押清单、照片，电子数据检查工作记录，视听资料，银行卡交易明细清单、对账单，羽源公司的营业执照,发破案经过，抓获经过、归案情况说明，刑事拘留证、释放证明等。

原审法院认为，被告人谭张羽、张源、秦秋发以非法获利为目的，明知他人利用信息网络实施犯罪，仍为其犯罪提供广告推广帮助，情节严重，侵犯了国家对正常信息网络环境的管理秩序，其行为均已构成帮助信息网络犯罪活动罪。被告人谭张羽、张源、秦秋发共同实施故意犯罪，系共同犯罪。在共同犯罪中，被告人谭张羽、张源起主要作用，均系主犯，应按照其参与的或组织、指挥的全部犯罪处罚。在共同犯罪中，被告人秦秋发处于受指挥、受支配的员工地位，起次要作用，属从犯，依法予以从轻处罚。被告人谭张羽、张源、秦秋发归案后均能如实供述其罪行，依法予以从轻处罚。被告人谭张羽、张源归案后能赔偿部分受害人经济损失，酌情予以从轻处罚。据此，依照《中华人民共和国刑法》第二百八十七条之二第一款、第二十五条第一款、第二十六条第一款、第四款、第二十七条、第六十七条第

三款、第六十四条之规定，判决：一、被告人张源犯帮助信息网络犯罪活动罪，判处有期徒刑二年一个月，并处罚金人民币十万元；被告人谭张羽犯帮助信息网络犯罪活动罪，判处有期徒刑一年十个月，并处罚金人民币八万元；被告人秦秋发犯帮助信息网络犯罪活动罪，判处有期徒刑一年四个月，并处罚金人民币三万元。二、追缴被告人谭张羽、张源违法所得人民币七十三万七千元、被告人秦秋发违法所得人民币二万元。

上诉人张源上诉称：1.其曾受到侦查人员刑讯逼供。2.其不明知所发送的“刷单”信息是诈骗信息。3.一审判决认定违法所得为80余万元，证据不足。4.其不是主犯，一审判决对其量刑过重。

上诉人张源的辩护人提出：1.上诉人张源曾受到侦查人员刑讯逼供，其以往在侦查阶段的供述应作为非法证据予以排除。2.认定洪某及王某乙系由张源等人所发送“刷单”信息被骗的证据不充分。3.本案所涉罪名是帮助犯，只有在被帮助行为构成犯罪的前提下才能成立，但并无证据证明张源等人所帮助的行为被确定为犯罪。4.一审判决认定的违法所得存在重复计算情况，认定违法所得为80余万元不当。5.一审判决对上诉人张源的量刑过重。

上诉人谭张羽上诉称：1.认定被害人洪某及王某乙是因其与张源等人所发“刷单”信息被骗的证据不充分。2.一审判决认定的违法所得没有扣除发送“刷单”信息的成本。

上诉人谭张羽的辩护人提出：1.现有证据无法证明洪某、王某乙的被骗是由于上诉人谭张羽等人发送“刷单”信息造成的。2.一审判决对上诉人谭张羽的量刑过重。

江苏省宿迁市人民检察院出庭履行职务的检察员提出：一审判决认定的事实清楚，证据确实、充分，适用法律正确，量刑适当，建议驳回上诉，维持原判。

经审理查明，2016年10月份，上诉人谭张羽、张源共同出资注册“广西羽源信息咨询有限公司”（已注销，以下简称羽源公司）。2016年12月份，为获取非法利益，上诉人谭张羽、张源商定在网络上从事为他人发送“刷单获取佣金”的诈骗信息业务，即通过“阿里旺旺”向不特定的淘宝用户发送信息，信息内容大致为“亲，我是***，最近库存压力比较大，请你来刷单，一单能赚10-30元，一天能赚几百元，详情加QQ**×××**”。通常每100个人添加上述信息里的QQ号，上诉人谭张羽、张源即可从要其发送诈骗信息的上家处获取平均约5000元的费用。上诉人谭张羽、张源雇佣原审被告人秦秋发及周遵超、王志成、唐柏芳钰等人具体负责发送诈骗信息。上诉人张源主要负责购买阿里旺旺账号、软件、租赁电脑服务器等，并经常到羽源公司处理事务；原审被告人秦秋发主要负责招揽、联系有发送诈骗信息需求的上家、接收上家支付的费用及带领周遵超、王志成、唐柏芳钰等人发送诈骗信息。2016年12月至2017年3月，上诉人谭张羽、张源通过上述方式共非法获利约人民币80余万元，原审被告人秦秋发在此期间以“工资”的形式非法获利人民币约2万元。被害人王某甲、洪某因添加上诉人谭张羽、张源等人组织发送的诈骗信息中的QQ号,后分别被骗31000元和30049元。案发后，上诉人谭张羽、张源及原审被告人秦秋发均被抓获归案，归案后如实供述了自己的主要犯罪事实。

另查明，上诉人张源曾因另案发送诈骗信息涉嫌诈骗罪（未遂），于2016年5月27日被桂林市公安局象山公安分局刑事拘留，后因检察机关未批准逮捕，于2016年7月2日被释放。

认定上述事实的证据有：

1.上诉人谭张羽供述，证明自己租了一处住所，与张源共同出资成立了羽源公司，自己任总经理，张源任副总经理，但自己很少去公司，由张源负责公司的日常管理。为了赚取非法利润，自己和张源商定为他人发送刷单诈骗信息，后雇佣秦秋发、周遵超、王志成、唐柏芳钰等人从2016年12月初开始为他人群发刷单信息，信息内容大概为“亲，你好，有空吗？帮我做兼职刷单，一单给5-20元，详情加QQ**×××**”。一般每有100个人添加信息中的QQ，一单任务就算完成了，上家会支付5000元费用。自己经营过淘宝店铺，也找过人刷单，知道正常刷单所需的费用，而上家给予自己的报酬加上刷单费用等成本高于正常刷单成本十倍多，所以不可能是真实刷单，而应该是诈骗信息。为上家发送诈骗信息，估计非法获利50多万元，由自己和张源平分，进入涉案银行卡中的钱都是给上家发送信息得来的。秦秋发是自己找来的，周遵超、王志成、唐柏芳钰是张源找来的，自己和张源各自负责上述人等的电脑配备及工资发放。为了规避公安机关查处，自己和张源、秦秋发商量买了他人的银行卡用于接收上家支付的报酬，还在电脑上安装了“影子”软件以自动删除电脑里的信息。阿里旺旺号和软件是张源买的，秦秋发负责和上家联系。

2.上诉人张源供述，证明自己与谭张羽共同出资成立了羽源公司，为了赚取非法利润，自己和谭张羽商定为他人发送刷单诈骗信息，后雇佣秦秋发、周遵超、王志成、唐柏芳钰等人从2016年12月初开始为他人群发刷单信息，信息内容大概为“兼职刷单，一单10-30元，每天可以赚几百元，需要请联系QQ**×××**”。一般每有100个人添加信息中的QQ，一单任务就算完成了，上家会支付5000元左右费用。谭张羽负责公司全面事务，自己负责购买阿里旺旺账号和采集、群发信息的软件，有时也会对外发送诈骗信息，秦秋发负责联系上家及接收上家支付的费用。秦秋发将钱取出后交给自己，自己再给谭张羽。周遵超、王志成、唐柏芳钰是自己找来的，工资由自己发放。发送信息的电脑上安装了“影子”软件，关机后查不到记录。

3.原审被告人秦秋发供述，证明从2016年12月份开始，自己在谭张羽、张源的羽源公司发送诈骗信息。谭张羽租了办公住所，但他不负责具体事务，很少去公司，张源经常去公司，并负责租服务器、买阿里旺旺账号和采集、群发信息软件用于发送诈骗信息，自己负责联系上家及接收上家支付的费用，并带周遵超、王志成、唐柏芳钰发送诈骗信息。涉案户名为“莫平”的中国银行卡、户名为“熊炳翔”、“陈信有”的浦发银行卡均是用于接收上家支付的费用，别无他途，户名为“张荣任”的浦发银行卡用于取款。自己把上家支付的费用取出来后都交给了张源，由其统一分配，自己每个月能分到五六千元。每有一个人加所发送信息里的QQ，上家就给50元，上家还要给刷单人10-20元钱，价格明显异常，自己开始

时就怀疑所发送的信息是诈骗信息，后来上家跟自己 QQ 聊天时也说根本就没有刷单这回事，就是诈骗用的。用来发送信息的电脑文件中的 TXT 文档是以发送诈骗信息的当天日期命名的，里面是用来登录并发送信息的阿里旺旺账号和密码。为了逃避公安机关查处，电脑上还安装了“影子”软件以清除相关信息。

4.同案关系人周遵超、王志成、唐柏芳钰供述，证明三人在谭张羽和张源的的公司具体负责发送刷单的诈骗信息，信息内容大概为“亲，我是***，最近库存压力比较大，请你来刷单，一单能赚 10-30 元，一天能赚几百元，详情加 QQ**×××**”。三人开始不知道所发送的是诈骗信息，后来通过秦秋发跟上家 QQ 的语音聊天及与自己的交谈或上家支付的费用明显异常等情况，得知所发送的信息是诈骗信息。谭张羽很少到公司，张源、秦秋发负责购买、提供阿里旺旺账号，秦秋发还负责联系上家、收取费用及带领三人发送诈骗信息，周遵超和张源也负责测试信息发送情况。为了逃避公安机关查处，发送信息的电脑上还安装了“影子”软件以清除相关信息。

5.被害人王某甲陈述，证明 2017 年 1 月 13 日，自己在阿里旺旺中被“有古文 d”推送的刷单信息诱骗而添加 QQ 刷单，后被骗 31000 元的经过。同时，被害人王某甲还提供了其被骗过程的聊天记录、支付记录等证据。

6.被害人洪某陈述，证明 2017 年 2 月 23 日，自己在阿里旺旺中被“1i471861320”推送的刷单广告诱骗而添加 QQ 刷单，后被骗 30049 元的经过。同时，被害人洪某还提供了其被骗过程的聊天记录、支付记录等证据。

7.沭阳县公安局搜查笔录、扣押清单、照片证明对秦秋发所使用的联想 L430 笔记本电脑一台及电脑硬盘两个、周遵超所使用的联想 9580 型笔记本一台及硬盘一个、唐柏芳钰所使用的东芝 R840 笔记本电脑一台、王志成所使用的惠普笔记本电脑一台、总经理办公室电脑硬盘一个依法扣押并提取其电子数据。

秦秋发所使用的联想 L430 笔记本电脑中桌面“号实名”文件夹内的“10 号.TXT”文件中检查出向王某甲发送诈骗信息 x i a ×××@126. c o m Ilixf6149I130684198701307028Iqqq123I1314001 有古文 d 的阿里旺旺号注册信息及密码。

秦秋发所使用的联想 L430 笔记本电脑中桌面“号实名”文件夹内的“东哥 23.TXT”文件中检查出向洪某发送诈骗信息的“1i471861320”的阿里旺旺号及其注册信息及密码。

8.沭阳县公安局调取的秦秋发所使用的账户名为“莫平”（卡号 62×××51）的中国银行银行卡的交易明细清单，其中 2016 年 12 月 5 日至 2017 年 1 月 11 日通过银行网银支付清算方式转入的资金约为人民币 26 万元。

沭阳县公安局调取的秦秋发所使用的账户名为“熊炳翔”（卡号 62×××21）的浦发银行银行卡的对账单，其中 2017 年 2 月 6 日至 2017 年 3 月 8 日通过互联网汇入方式转入的资金约为人民币 48 万元。其中转入账户名“张荣任”的浦发银行卡约人民币 34.6 万元，其中转入账户名“陈信有”的浦发银行卡人民币 14999 元，从 ATM 机取现金约人民币 80000

元。

沭阳县公安局调取的秦秋发所使用的账户名为“陈信有”（卡号62×××54）的浦发银行银行卡的对账单，其中2017年3月6日至2017年3月9日通过互联网汇入方式转入的资金为人民币9.7万元。其中从ATM机取现金约87000元，卡内余额为11968元。

沭阳县公安局调取的秦秋发所使用的账户名为“张荣任”（卡号62×××47）的浦发银行银行卡的对账单，其中2017年2月6日至2017年3月10日从熊炳翔的浦发银行卡中转入的资金为人民币34.6万余元，其中从ATM机取现金约32万元，卡内余额为26096元。

9.沭阳县公安局从中国银行桂林分行、上海浦发银行桂林支行分别调取了取款录像，显示秦秋发于2017年3月7日在中国银行桂林分行ATM机、2017年3日7日在上海浦发银行桂林分行ATM机取款，上述取款时间、地点与银行卡交易明细及对账单均相符。

10.羽源公司的营业执照，证明了羽源公司的相关情况。

11.谭张羽亲属及张源的辩护人提交的赔偿协议书、谅解书、收条，证明谭张羽、张源赔偿了被害人王某甲经济损失，谭张羽、张源得到了对方的谅解。

12.沭阳县公安局出具的有无前科劣迹证明、刑事判决书、刑事拘留证、释放证明书，证明谭张羽、张源及秦秋发的前科劣迹情况，张源曾因发送诈骗信息涉嫌诈骗罪（未遂），于2016年5月27日被桂林市公安局象山公安分局采取刑事强制措施。

13.常住人口基本信息，证明上诉人谭张羽、张源及原审被告人秦秋发作案时达到刑事责任年龄。

14.沭阳县公安局出具的发破案经过、抓获经过、归案情况说明，证明本案的案发及谭张羽、张源、秦秋发的归案情况。

上述证据经一、二审庭审质证，均来源合法，与案件相关联，且证据间相互印证，本院予以确认。

关于上诉人张源以往在侦查阶段的供述是否应作为非法证据予以排除的问题。经查，入所体检表证明上诉人张源入所检查时身体无异常情况；侦查人员出具的情况说明证明对上诉人张源无刑讯逼供行为；上诉人张源在一审庭审中对侦查机关取证的合法性没有提出异议，并供认在侦查机关所作出的供述属实，二审中其未提供受到刑讯逼供的证据材料；从讯问笔录内容来看，上诉人张源不仅在公安机关办案中心作出过有罪供述，在看守所也作出过有罪供述，其供述与同案犯的供述亦能够相互印证。综上，上诉人张源以往在侦查阶段所作的供述可以作为证据使用。故对上诉人张源及其辩护人所提上诉人张源曾受到刑讯逼供，其以往在侦查阶段的供述应作为非法证据予以排除的意见，本院不予采纳。

关于一审判决认定被害人洪某及王某乙被骗与上诉人谭张羽、张源等人的行为存在因果关系的证据是否充分的问题。经查，1.被害人洪某陈述2017年2月23日，自己被名为“1i471861320”的阿里旺旺账号推送的刷单广告吸引，而添加其中的QQ刷单，后被骗30049元，被害人洪某并提供了其被骗过程的聊天记录、支付记录等证据。而原审被告人秦秋发所

使用的联想 L430 笔记本电脑中桌面“号实名”文件夹内的“东哥 23.TXT”文件中检查出“1i471861320”的阿里旺旺账号及其注册信息、密码。原审被告人秦秋发供述，其电脑中 TXT 文档是以发送诈骗信息的日期命名。被害人洪某陈述的被骗过程与上诉人谭张羽、张源及原审被告人秦秋发等人供述的犯罪行为实施过程相印证，并得到电子数据勘验情况的佐证，上述证据足以证实被害人洪某被骗与上诉人谭张羽、张源等人的行为存在因果关系。2.被害人王某乙陈述 2017 年 3 月 7 日，骗其钱财的一方使用 QQ 号主动加其 QQ 号，而后发给其刷单的流程链接，其陈述与上诉人谭张羽、张源及原审被告人秦秋发等人供述的通过阿里旺旺发送含有 QQ 号的刷单信息，而后由被害人添加所发送信息里的 QQ 号的情况不符。虽然根据电子数据检查，同案关系人唐柏芳钰所使用的东芝 R840 笔记本电脑中“在线名单.txt”文件和“2 月数据.txt”文件中、王志成所使用的惠普笔记本电脑回收站文件、原审被告人秦秋发所使用的联想 L430 笔记本电脑回收站文件中均检查出“51303019880521 王某乙”内容，与被害人王某乙的姓名、身份证号相符，但现有证据之间的矛盾无法排除，不足以认定被害人王某乙被骗与上诉人谭张羽、张源等人的行为存在因果关系。故对上诉人谭张羽及其辩护人以及上诉人张源的辩护人提出认定被害人洪某及王某乙系由张源等人所发送的信息被骗的证据不充分的意见，本院对其中涉及王某乙的部分，予以采纳。

关于一审判决认定上诉人谭张羽、张源的违法所得为 80 余万元是否正确的问题。经查，根据上诉人谭张羽、张源及原审被告人秦秋发的供述，秦秋发负责使用银行卡接收上家支付的发送诈骗信息报酬，一审法院根据秦秋发使用四张银行卡的时间、交易明细清单、对账单，在排除重复计算的基础上，并结合原审被告人秦秋发供述的银行卡的用途、资金往来数额，得出其违法所得约为 83.7 万元，并无不当。二审中上诉人张源的辩护人提交了莫平的书面证言及银行交易流水明细清单各一份，以证明涉案莫平的中国银行卡中有两笔共计 1.5 万元是他人借款，而非上家支付的发送诈骗信息费用。虽然根据现有证据，无法排除该 1.5 万元是他人借款，从有利于被告人的角度，本院可对该 1.5 万元从上诉人张源、谭张羽的违法所得数额中予以扣除，但即便二审对该 1.5 万元予以扣除，认定其违法所得仍为 80 余万元亦无不当。另，上诉人谭张羽、张源购买阿里旺旺账号、租用服务器、支付涉案人员“工资”等支出系为了实施违法犯罪，依附于其犯罪行为，具有非法性，在计算违法所得时对于该犯罪成本，不应予以扣除。故对上诉人谭张羽、张源及其辩护人提出一审判决认定上诉人谭张羽、张源的违法所得为 80 余万元不当的意见，本院不予采纳。

本院认为，上诉人谭张羽、张源及原审被告人秦秋发为他人实施诈骗等违法犯罪活动发布信息，情节严重，其行为均已构成非法利用信息网络罪。上诉人谭张羽、张源及原审被告人秦秋发共同实施故意犯罪，系共同犯罪。在共同犯罪中，上诉人谭张羽、张源起主要作用，系主犯，应按照其参与的或组织、指挥的全部犯罪处罚；原审被告人秦秋发处于受指挥、支配的地位，起次要作用，属从犯，依法予以从轻处罚。上诉人谭张羽、张源及原审被告人秦秋发归案后能如实供述其主要犯罪事实，依法予以从轻处罚。上诉人谭张羽、张源归案后

能赔偿部分受害人经济损失并取得其谅解，酌情予以从轻处罚。

关于本案的定性问题。经查：1.非法利用信息网络罪与帮助信息网络犯罪活动罪的界分。根据法律规定，非法利用信息网络罪，是指利用信息网络设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，或者发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息，或者为实施诈骗等违法犯罪活动发布信息，情节严重的行为。帮助信息网络犯罪活动罪，是指明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的行为。非法利用信息网络罪是对网络犯罪预备行为独立入罪，实现网络犯罪预备行为的实行化，帮助信息网络犯罪活动罪是对网络犯罪的帮助行为独立入罪，实现网络犯罪帮助行为正犯化。非法利用信息网络罪只要求行为人实施了法律规定的相应行为，即所设立的网站、群组用于实施违法犯罪活动，或者所发布的信息内容有关违法犯罪或者为实施诈骗等违法犯罪活动，并不要求客观上实施了相应的违法犯罪活动，而帮助信息网络犯罪活动罪通常须以帮助对象的行为构成犯罪为前提，该罪中的“广告推广”一般是指为推广网站扩大犯罪活动范围所需的投放广告行为。为他人实施诈骗等违法犯罪活动发布信息，虽然也属于帮助信息网络犯罪活动的情形，但其本质上还是一种非法利用信息网络。2.本案罪名的确定。具体到本案中，首先，上诉人谭张羽、张源等人的行为属于为实施诈骗等违法犯罪活动发布信息。根据其所发送的信息内容、收取费用明显异常，购买他人银行卡用于接收上家支付的费用及在电脑里安装“影子”软件清除使用痕迹以规避调查，有证据证实存在现实的诈骗犯罪行为，上诉人张源之前曾因发送诈骗信息被刑事拘留，上诉人谭张羽、张源及原审被告人秦秋发等人以往均供述明知所发送的信息是诈骗信息等情况，足以认定上诉人谭张羽、张源等人明知自己为上家发布的信息是为了实施诈骗违法犯罪活动。上诉人谭张羽等人发送刷单诈骗信息的行为并非是帮助信息网络犯罪活动罪中所意指的“广告推广”。故而，应认定上诉人谭张羽、张源等人的行为符合非法利用信息网络罪的客观表现。其次，上诉人谭张羽、张源等人通过发送含有QQ号的刷单诈骗信息，目的是诱骗他人添加该QQ号，每达100人添加，其即向上家移交该QQ号，由于此时诈骗犯罪尚未着手实施，其行为在实质上属于诈骗犯罪预备，将其行为评价为非法利用信息网络性质也契合非法利用信息网络罪将网络犯罪预备行为独立入罪的情形。再者，本案不管是从违法所得数额、可计算的QQ成员数，还是从造成被害人实际被骗的数额，均应认定达到法律规定的“情节严重”的程度。最后，虽然本案中并无证据证实具体实施诈骗的行为人归案并受到刑事追究，但相关人员客观上是否实施了相应违法犯罪活动，不影响非法利用信息网络罪的成立。而且，有证据证实诈骗行为客观存在，并且达到构成犯罪的程度。综上，本院认为，上诉人谭张羽、张源及原审被告人的行为已构成非法利用信息网络罪。

关于一审判决对二上诉人的量刑是否适当问题。经查，一审判决根据本案的犯罪事实、性质、情节及社会危害后果，对上诉人谭张羽和张源所作出的量刑并无不当。虽然上诉人谭

张羽和张源共同商定从事本案犯罪活动，共同出资并均分违法所得，但上诉人张源负责涉案信息发送的具体事务，购买阿里旺旺账号和相关软件，并雇佣王志成、周遵超、唐柏芳钰发送信息，而上诉人谭张羽去公司的次数相对较少，一审判决根据上诉人张源和谭张羽在犯罪具体实施过程中作用的不同，对其二人予以区别量刑，并无不当。故对上诉人谭张羽的辩护人以及上诉人张源及其辩护人提出一审判决量刑过重的意见，本院不予采纳。

综上，一审判决认定的主要事实清楚，证据确实、充分，但认定上诉人谭张羽、张源及原审被告人秦秋发的行为构成帮助信息网络犯罪活动罪，定性不准确，应依法予以改判。对出庭检察员建议驳回上诉、维持原判的意见，不予采纳。据此，依照《中华人民共和国刑法》第二百八十七条之一第一款，第二十五条第一款，第二十六条第一款、第四款，第二十七条，第六十七条第三款，第六十四条之规定，《中华人民共和国刑事诉讼法》第二百三十六条第一款第一项、第二项之规定，判决如下：

一、维持沭阳县人民法院（2017）苏 1322 刑初 1327 号刑事判决第二项；

二、撤销沭阳县人民法院（2017）苏 1322 刑初 1327 号刑事判决第一项；

三、上诉人张源犯非法利用信息网络罪，判处有期徒刑二年一个月，并处罚金人民币十万元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自二〇一八年四月八日起至二〇二〇年三月三十一日止；所处罚金应在判决生效后十日内缴纳完毕。）

上诉人谭张羽犯非法利用信息网络罪，判处有期徒刑一年十个月，并处罚金人民币八万元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自二〇一八年四月八日起至二〇二〇年一月二十日止；所处罚金应在判决生效后十日内缴纳完毕。）

原审被告人秦秋发犯非法利用信息网络罪，判处有期徒刑一年四个月，并处罚金人民币三万元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自二〇一八年四月八日起至二〇一九年六月三十日止；所处罚金应在判决生效后十日内缴纳完毕。）

本判决为终审判决。

审判长　戴建军

审判员　张成飞

审判员　高峰

二〇一九年二月十二日

书记员　蒋芹

三、赵瑞帮助信息网络犯罪活动案

为他人实施信息网络犯罪提供支付结算帮助，情节严重的，构成帮助信息网络犯罪活动罪

（一）基本案情

被告人赵瑞经营的网络科技有限公司的主营业务为第三方支付公司网络支付接口代理。赵瑞在明知申请支付接口需要提供商户营业执照、法人身份证等五证信息和网络商城备案域名，且明知非法代理的网络支付接口可能被用于犯罪资金走账和洗钱的情况下，仍通过事先购买的企业五证信息和假域名备案在第三方公司申请支付账号，以每个账号收取2000至3500元不等的接口费将账号卖给他人，并收取该账号入金金额千分之三左右的分润。

2016年11月17日，被害人赵某被骗600万元。其中，被骗资金50万元经他人账户后转入在第三方某股份有限公司开户的某贸易有限公司商户账号内流转，该商户账号由赵瑞通过上述方式代理。

（二）裁判结果

浙江省义乌市人民法院判决认为：被告人赵瑞明知他人利用信息网络实施犯罪，为其犯罪提供支付结算的帮助，其行为已构成帮助信息网络犯罪活动罪。被告人赵瑞到案后如实供述自己的罪行，依法可以从轻处罚。以帮助信息网络犯罪活动罪判处被告人赵瑞有期徒刑七个月，并处罚金人民币三千元。该判决已发生法律效力。

附：赵瑞帮助信息网络犯罪活动罪一案一审刑事判决书

义乌市人民法院

刑事判决书

（2017）浙0782刑初1563号

公诉机关义乌市人民检察院。

被告人赵瑞，男，1987年6月21日出生于山东省单县，汉族，高中文化，家住山东省单县。因涉嫌犯帮助信息网络犯罪活动罪于2016年12月29日被义乌市公安局刑事拘留，2017年1月27日被依法逮捕。现押于义乌市看守所。

辩护人余文峰，浙江义元律师事务所律师。

辩护人王雷，山东盛雅律师事务所律师。

义乌市人民检察院以义检刑诉[2017]1539号起诉书指控被告人赵瑞犯帮助信息网络犯罪活动罪，于2017年6月29日向本院提起公诉。本院依法适用简易程序，实行独任审判，公开开庭审理了本案。义乌市人民检察院指派检察员林华出庭支持公诉，被告人赵瑞及辩护人余文峰、王雷到庭参加诉讼。现已审理终结。

经审理查明：2015年12月，被告人赵瑞所经营的某网络科技有限公司，主营业务为第三方支付公司网络支付接口代理。被告人赵瑞在明知申请支付接口需要提供商户营业执

照、法人身份证等五证信息和网络商城备案域名，且明知非法代理的网络支付接口可能被用于犯罪资金走账和洗钱的情况下，仍通过事先购买的企业五证信息和假域名备案在第三方公司申请支付账号，以每个账号收取 2000 至 3500 元不等的接口费将账号卖给他人，并收取该账号入金金额千分之三左右的分润。2016 年 11 月 17 日，被害人赵某在我市被人通过以冒充公检法，称其涉嫌犯罪的方式被骗人民币 600 万元。经查，被害人赵某 600 万元被骗资金中 50 万元经宋彦顺(账号 62×××70）和某（账号 62×××70）账户后转入在第三方某股份有限公司开户的某贸易有限公司商户账号内流转，该商户账号由被告人赵瑞通过上述方式代理。

上述事实，被告人赵瑞在庭审过程中亦无异议，且有被害人赵某的陈述，扣押决定书，扣押清单，易宝支付合作协议，易宝支付有限公司代理权利义务转让协议，某在线代理合作协议，某 2 在线商务合作协议，易宝支付服务协议，笔记本复印件，银行卡交易记录，网银收款流水，某股份有限公司互联网业务联合拓展协议，某股份有限公司在线支付业务服务合同，某服务股份有限公司代收付业务服务合同，营业执照，开户许可证，搜查笔录，到案经过，被告人赵瑞的供述及身份证明等证据证实，足以认定。

本院认为，被告人赵瑞明知他人利用信息网络实施犯罪，为其犯罪提供支付结算的帮助，其行为已构成帮助信息网络犯罪活动罪。公诉机关指控成立，应予支持。被告人赵瑞到案后如实供述自己的罪行，依法可以从轻处罚。辩护人余文峰提出被告人赵瑞认罪态度好、系初犯，请求对其从轻处罚的辩护意见有理，予以采纳。依照《中华人民共和国刑法》第二百八十七条之二第一款、第六十七条第三款、第五十二条、第五十三条之规定，判决如下：

被告人赵瑞犯帮助信息网络犯罪活动罪，判处有期徒刑七个月，并处罚金人民币三千元（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2016 年 12 月 29 日起至 2017 年 7 月 28 日止。罚金限判决生效后一个月内缴纳）。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向浙江省金华市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审判员　王清

二Ｏ一七年七月十二日

书记员　员吴菁

四、侯博元、刘昱祈等帮助信息网络犯罪活动案

为他人实施信息网络犯罪提供开办银行卡帮助，情节严重的，构成帮助信息网络犯罪活动罪

（一）基本案情

2018 年 5 月 28 日，被告人侯博元、刘昱祈在台湾地区受人指派，带领被告人刘育民、

蔡宇彦等进入大陆到银行办理银行卡，用于电信网络诈骗等违法犯罪活动。刘育民、蔡宇彦明知开办的银行卡可能用于电信网络诈骗等犯罪活动，但为了高额回报，依然积极参加。当日下午，抵达杭州机场，后乘坐高铁来到金华市区并入住酒店。当晚，侯博元、刘昱祈告知其他人办理银行卡时谎称系来大陆投资，并交代了注意事项及具体操作细节。5 月 29 日上午，在金华多家银行网点共开办了 12 张银行卡，并开通网银功能。

另，2018 年 5 月 14 日至 18 日，被告人侯博元、刘昱祈以同样的方式在金华市区义乌两地办理银行卡，并带回台湾地区。

（二）裁判结果

浙江省金华市婺城区人民法院判决认为：被告人侯博元、刘昱祈、蔡宇彦、刘育民明知开办的银行卡可能用于实施电信网络诈骗等犯罪行为，仍帮助到大陆开办银行卡，情节严重，其行为均已构成帮助信息网络犯罪活动罪。以帮助信息网络犯罪活动罪判处被告人侯博元、刘昱祈有期徒刑一年二个月，并处罚金人民币一万元；被告人蔡宇彦、刘育民有期徒刑九个月，并处罚金人民币五千元。该判决已发生法律效力。

附：侯博元、刘昱祈、蔡宇彦等帮助信息网络犯罪活动罪一审刑事判决书

金华市婺城区人民法院

刑事判决书

（2018）浙 0702 刑初 915 号

公诉机关金华市婺城区人民检察院。

被告人侯博元，男，1996 年 6 月 23 日出生于台湾地区嘉义县，汉族，初中文化，务农，家住台湾地区嘉义县。因本案于 2018 年 5 月 30 日被金华市公安局江南分局刑事拘留，同年 7 月 6 日被依法逮捕。现羁押于金华市看守所。

辩护人诸葛莹，浙江一剑律师事务所律师。

被告人刘昱祈，男，1996 年 4 月 29 日出生于台湾地区，汉族，大学文化，无业，家住台湾地区。因本案于 2018 年 5 月 30 日被金华市公安局江南分局刑事拘留，同年 7 月 6 日被依法逮捕。现羁押于金华市看守所。

辩护人盛清华，浙江十全律师事务所律师。

被告人蔡宇彦，男，2000 年 3 月 10 日出生于台湾地区嘉义县，汉族，高中文化，务农，家住台湾地区嘉义县。因本案于 2018 年 5 月 30 日被金华市公安局江南分局刑事拘留，同年 7 月 6 日被依法逮捕。现羁押于金华市看守所。

辩护人徐旻，浙江振进律师事务所律师。

被告人刘育民，男，2000 年 2 月 8 日出生于台湾地区嘉义县，汉族，初中文化，务农，家住台湾地区嘉义县。因本案于 2018 年 5 月 30 日被金华市公安局江南分局刑事拘留，同年 7 月 6 日被依法逮捕。现羁押于金华市看守所。

辩护人龚志坚，浙江民宜律师事务所律师。

金华市婺城区人民检察院以婺检公诉刑诉〔2018〕909号起诉书指控被告人侯博元、刘昱祈、蔡宇彦、刘育民、林某犯帮助信息网络犯罪活动罪，于2018年10月18日向本院提起公诉。被告人林某在审理过程中死亡，本院已于2018年11月26日裁定对其终止审理。本院依法组成合议庭，公开开庭审理了本案。金华市婺城区人民检察院指派检察员万斌出庭支持公诉，被告人侯博元及其辩护人诸葛莹、被告人刘昱祈及其辩护人盛清华、被告人蔡宇彦及其辩护人徐旻、被告人刘育民及其辩护人龚志坚到庭参加诉讼。现已审理终结。

金华市婺城区人民检察院指控，2018年5月28日，宋某让被告人侯博元、刘昱祈带领被告人刘育民、蔡宇彦、林某从台湾到大陆办理银行卡，用于违法犯罪活动。刘育民、蔡宇彦等人明知开的银行卡可能用于犯罪活动，但为了高额回报，依然积极参加。当日下午，五人抵达金华市区并入住酒店。当晚，侯博元、刘昱祈告知其他三人办理银行卡的时候谎称系来大陆投资，并交代了注意事项及具体操作细节。5月29日上午，五人在金华各银行网点共开办了12张银行卡，并开通网银功能。另查明，2018年5月14日至18日，侯博元、刘昱祈与宋瑞景以同样方式在金华市区义乌两地办理银行卡并带回台湾。

公诉机关认为，被告人侯博元、刘昱祈、蔡宇彦、刘育民的行为均已构成帮助信息网络犯罪活动罪，系共同犯罪。针对上述指控，公诉机关提供了相关证据予以证实，提请本院依法判处。

被告人侯博元、刘昱祈、蔡宇彦、刘育民在庭审中均辩解称不知道所办银行卡可能用于违法犯罪活动。

辩护人诸葛莹辩护提出：一、对公诉机关指控的罪名和犯罪事实没有异议。二、被告人侯博元有从轻处罚情节：其只是听从公司安排带人到大陆办卡，相关办卡人员的召集也由公司安排，其收入仅仅是普通员工工资，办卡人员可能造成的危害后果要比其严重，各被告人的地位和作用基本相当，量刑时不应区别对待；系初犯、主观恶性较小，其认为自己不参与犯罪活动，其所带人员提供的身份信息真实，公司也没有告知所办银行卡用于犯罪活动，其参与的环节没有任何虚假及违法行为存在，就不会构成犯罪，同时对带队办卡行为是否一定会造成后续的现实危害也是持放任心态；社会危害性不大，办卡人员均是自愿参与，所办银行卡已全部被查获，没有用于违法犯罪活动，没有发生现实危害后果；归案后如实交代自己的犯罪行为，具有坦白情节，自愿认罪，具有悔罪表现。综上，请法庭对其从轻处罚。

辩护人盛清华辩护提出：首先，同意公诉机关和第一被告人辩护人的意见。其次，被告人刘昱祈主观恶性小。其是在公安机关提审时才知道这个事情有可能构成犯罪，且办卡的收入少。综上，请法庭对其从轻处罚。

辩护人徐旻辩护提出：首先，被告人蔡宇彦只是一个普通参与者，只开办了4张银行卡，应认定为从犯。其次，我国台湾地区没有帮助信息网络犯罪活动罪这一罪名，且公司跟他们讲过来办卡不会有什么问题，故被告人蔡宇彦的主观恶性小。最后，被告人蔡宇彦在归案后如实供述，自愿认罪，具有明显的悔罪表现，且涉案银行卡立即被公安机关查获，没有

造成任何危害后果。综上，请法庭对其从轻处罚。

辩护人龚志坚辩护提出：首先，同意前面辩护人的辩护意见。其次，被告人刘育民之前没有任何违法犯罪记录，此次犯罪是由于不了解大陆法律，想赚钱，未认识到赚钱的方式是否恰当或者违法。最后，被告人刘育民在归案后如实供述自己的犯罪事实，所办银行卡没有流入犯罪分子手中，没有造成其他社会危害。综上，请法庭对其从轻处罚。

经审理查明：

2018 年 5 月 28 日，宋某（另案处理）在台湾指派被告人侯博元、刘昱祈，让两人带领被告人刘育民、蔡宇彦、林某进入中国大陆到银行办理银行卡，用于电信网络诈骗等违法犯罪活动。刘育民、蔡宇彦、林某明知开办的银行卡可能用于电信网络诈骗等犯罪活动，但为了高额回报，依然积极参加。当日下午，五人抵达杭州机场，后乘坐高铁来到金华市区并入住酒店。当晚，侯博元、刘昱祈告知其他三人办理银行卡时谎称系来大陆投资，并交代了注意事项及具体操作细节。5 月 29 日上午，五人在金华多家银行网点共开办了 12 张银行卡，并开通网银功能。当日晚，被告人侯博元、刘昱祈、刘育民、蔡宇彦、林某等五人在酒店被公安机关抓获归案，现场缴获银行卡、手机和电脑。

另查明，2018 年 5 月 14 日至 18 日，被告人侯博元、刘昱祈跟着宋某以同样的方式在金华市区义乌两地办理银行卡，并带回台湾。

上述事实，有公诉机关提供并经法庭质证、认证的下列证据予以证实：被告人侯博元、刘昱祈、蔡宇彦、刘育民等人的供述与辩解，搜查证、搜查笔录及照片，扣押决定书、清单及照片，辨认笔录，回复查询出入境情况表，资金流向表，案件关联表，护照、台湾居民来往大陆通行证复印件，抓获经过等。上述证据符合证据的客观性、关联性、合法性要件，且证据之间能够相互印证，本院依法予以确认。

本院认为，被告人侯博元、刘昱祈、蔡宇彦、刘育民明知开办的银行卡可能用于实施电信网络诈骗等犯罪行为，仍为犯罪分子到大陆开办银行卡，情节严重，其行为均已构成帮助信息网络犯罪活动罪。系共同犯罪。公诉机关的指控成立，予以支持。

针对各被告人所提不知道所办银行卡可能用于违法犯罪活动的辩解意见。经查，第一，侯博元等人所在的公司每隔一段时间会叫不同的人专程从台湾来大陆开卡。侯博元在公司的主要工作就是带人到大陆开卡。此次有 5 人来开卡，且一天就开了 10 余张卡。第二，公司对开卡有特定要求。一定要申请 U 盾开通网上转账功能，汇款额度越高越好，统一设置银行卡和 U 盾的密码，且向银行工作人员谎称办卡是用于在大陆开店做生意周转资金，办卡时登记的手机号是来金华后临时办理的，登记的地址是随意填写的，还要测试 U 盾能否汇款以及登记开卡信息。第三，公司支付高额费用收卡。此次从台湾到大陆来开卡共 5 天时间，开卡的人均有 2 万新台币的报酬，且交通、吃住等开支均由公司支付。第四，实际上，侯博元在大陆取钱使用的银行卡关联到被电信诈骗的款项。第五，各被告人对各种异常情况没有作出合理解释，而且在归案后均供述称开办的银行卡用于汇不正当的钱，比如网络诈骗等，但为

了赚钱还是做了这个事情。综上，被告人侯博元、刘昱祈、蔡宇彦、刘育民应当知道开办的银行卡可能会被用于网络诈骗等违法犯罪行为。故不采纳各被告人对主观明知所提的辩解意见。

被告人侯博元、刘昱祈、蔡宇彦、刘育民在庭审中未如实供述犯罪事实，不构成坦白。故不采纳各辩护人分别所提坦白的辩护意见。被告人蔡宇彦开办了4张银行卡，行为积极，不宜认定为从犯，其与同伙的具体作用在量刑时酌情予以考虑。故不采纳辩护人所提被告人蔡宇彦系从犯的辩护意见。综上，依照《中华人民共和国刑法》第二百八十七条之二、第二十五条第一款、第五十二条、第五十三条、第六十四条之规定，判决如下：

一、被告人侯博元犯帮助信息网络犯罪活动罪，判处有期徒刑一年二个月，并处罚金人民币一万元。罚金限于本判决生效后十日内缴纳。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年5月30日起至2019年7月29日止）。

二、被告人刘昱祈犯帮助信息网络犯罪活动罪，判处有期徒刑一年二个月，并处罚金人民币一万元。罚金限于本判决生效后十日内缴纳。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年5月30日起至2019年7月29日止）。

三、被告人蔡宇彦犯帮助信息网络犯罪活动罪，判处有期徒刑九个月，并处罚金人民币五千元。罚金限于本判决生效后十日内缴纳。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年5月30日起至2019年2月28日止）。

四、被告人刘育民犯帮助信息网络犯罪活动罪，判处有期徒刑九个月，并处罚金人民币五千元。罚金限于本判决生效后十日内缴纳。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年5月30日起至2019年2月28日止）。

五、已被扣押的银行卡予以没收，其余物品由扣押机关金华市公安局江南分局依法处理。

如不服本判决，可在接到判决书第二日起十日内通过本院或者直接向浙江省金华市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审判长　王娜

人民陪审员　龙霞

人民陪审员　俞旦星

二〇一八年十二月二十六日

书记员　ＸＸ真

2.2019 年度浙江省互联网十大检察案例之一：全国首例全链条打击制贩大麻网站案--非法利用信息网络案

（诸暨市人民检察院）

2019 年 10 月，诸暨市人民检察院提起公诉的全国首例全链条打击制贩大麻“园丁丁”网站案宣判。“园丁丁”论坛是近几年国内规模较大的大麻论坛，内容从大麻种植知识分享到种子、种植用具、吸食工具、成品大麻买卖，为国内大麻吸食人群提供种植、交易渠道，逐渐成为制贩大麻的源头组织。该案因类型新颖、涉案人员广，被公安部列为互联网涉毒目标案件。此前互联网涉毒案件，仅对贩毒行为作刑事打击，对上游网站最多作关停处理，本案系国内将大麻交流网站以“非法利用信息网络罪”定罪处罚的第一案，为打击无法查实贩毒事实但利用互联网发布涉毒信息行为提供了解决方案。本案的成功办理摧毁了利用互联网制贩大麻黑色产业链，为遏制互联网涉毒犯罪提供了范本。

3. 典型案例：王某帮助信息网络犯罪活动案

案例要旨

行为人为非法获利，为多个赌博网站提供域名跳转等技术支持，帮助其逃避网络监管部门监管，使参赌人员得以顺利访问赌博网站，助长赌博犯罪，情节严重的，构成帮助信息网络犯罪活动罪。

案例正文

王某帮助信息网络犯罪活动案

基本案情

2019 年 4 月至 2019 年 6 月间，被告人王某租用免备案的服务器，明知“金沙娱乐场”、“银河娱乐城”等系以营利为目的的赌博、博彩网站，仍接受委托，在计算机上通过“宝塔面板”控制端多次为赌博、博彩等违法网站进行 301 跳转，以逃避网络监管部门拦截，使上述相关违法网站得以继续访问。经勘验，被告人王某先后为多家赌博网站的 143 个域名进行了跳转并从中获利 3 万余元。

裁判结果

根据刑法及有关司法解释规定，明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、通讯传输等技术支持，违法所得一万元以上的，构成帮助信息网络犯罪活动罪，处三年以下有期徒刑或者拘役，并处或者单处罚金。扬州经济技术开发区人民法院经审理认定，被告人王某构成帮助信息网络犯罪活动罪，判处有期徒刑一年六个月，缓刑二年，并处罚金人民币一万元；被告人王某退出的赃款人民币四万元，依法予以没收，上缴国库。

法院评论

当前，网络赌博等非法网站为获取巨额非法利益，犯罪手法不断翻新、技术手段不断升级，以此逃避网络监管和打击，由此衍生出为此类网站提供技术服务，帮助其规避网络监管措施的黑色产业链条，具有很大社会危害性。本案中，被告人王某为非法获利，为多个赌博网站提供域名跳转等技术支持，帮助其逃避网络监管部门监管，使参赌人员得以顺利访问赌博网站，助长了赌博犯罪，应受到刑罚处罚。

4.在校学生涉“两卡”犯罪典型案例之一：涂某通、万某玲帮助信息网络犯罪活动案

(2020)川 0781 刑初 373 号

一、基本案情

涂某通，1998 年 8 月出生，系某大学在校学生。

万某玲，1998 年 9 月出生，作案时系某职业技术学校在校学生，案发时系某医院员工。

2018 年起，涂某通明知他人利用信息网络实施犯罪，为牟取非法利益，长期收购银行卡提供给他人使用。2018 年，涂某通与万某玲通过兼职认识后，涂某通先后收购了万某玲的 3 套银行卡（含银行卡、U 盾/K 宝、身份证照片、手机卡），并让万某玲帮助其收购银行卡。2019 年 3 月至 2020 年 1 月，万某玲为牟利，在明知银行卡被用于信息网络犯罪的情况下，以亲属开淘宝店需要用卡等理由，从 4 名同学处收购 8 套新注册的银行卡提供给涂某通，涂某通将银行卡出售给他人，被用于实施电信网络诈骗等违法犯罪活动。经查，共有 21 名电信网络诈骗被害人向万某玲出售的上述银行卡内转入人民币 207 万余元。

二、诉讼过程

2020 年 11 月 3 日，四川省江油市公安局以涂某通、万某玲涉嫌帮助信息网络犯罪活动罪移送起诉。同年 12 月 3 日，江油市人民检察院以帮助信息网络犯罪活动罪对涂某通、万某玲提起公诉。鉴于万某玲犯罪时系在校大学生，因找兼职误入歧途而收购、贩卖银行卡，主动认罪认罚，江油市人民检察院对其提出从轻处罚的量刑建议。涂某通在审查起诉阶段不认罪，也不供述银行卡销售去向、获利数额等情况。2020 年 12 月 31 日，江油市人民法院作出一审判决，以帮助信息网络犯罪活动罪判处涂某通有期徒刑一年四个月，并处罚金人民币一万元；判处万某玲有期徒刑十个月，并处罚金人民币五千元。涂某通、万某玲未上诉，判决已生效。

三、教育治理

针对在校大学生违法收购、贩卖银行卡被用于网络犯罪的情况，江油市人民检察院会同学校所在地检察院，向涉案学生所在高校制发检察建议，提示在校学生涉“两卡”违法犯罪风险。相关学校积极开展法治宣传，通过以案释法，加强对全校学生的教育引导。江油市人民检察院还会同本辖区内学校开展“断卡”宣传进校园活动，将包括本案在内的多个真实案例纳入宣讲；制作“断卡”普法小漫画进行推送宣传，着力提高在校学生学法懂法、遵法守法的意识。

四、典型意义

从近年来的办案情况看，手机卡、银行卡（以下简称“两卡”）已经成为电信网络诈骗犯罪分子实施诈骗、转移赃款的重要工具。为依法严厉打击非法出租、出售“两卡”违法犯罪活动，2020 年 10 月起，最高人民法院、最高人民检察院、公安部、工业和信息化部、中国人民银行等五部门联合部署开展“断卡”行动，以斩断电信网络诈骗违法犯罪的信息流和资金链。

工作中发现，部分在校学生由于社会阅历不足、法治观念淡薄，已成为非法买卖“两卡”的重要群体之一。在利益诱惑面前，有的学生迷失方向，一步步陷入违法犯罪泥潭，从办卡、卖卡发展到组织收卡、贩卡，成为潜伏在校园中的“卡商”。本案被告人即是这样的“卡商”，他们不仅出售自己的银行卡，还在学校里招揽同学出售银行卡。这些银行卡经过层层周转，落入到诈骗人员等犯罪分子手中，用于流转非法资金，危害不容小觑。对于从“工具人”转变为“卡商”的在校学生，应当综合其犯罪事实、情节和认罪态度，依法追究刑事责任。

对于办案中发现的在校学生涉电信网络诈骗以及“两卡”犯罪风险点，检察机关和教育部门要加强以案释法，深入校园开展形式多样的法治宣传教育活动。特别是对于案件相对多发的学校，要共同研究加强教育管理的意见，提升在校学生的风险意识和防范能力，避免成为犯罪“工具人”。办案地和学校所在地检察机关要加强沟通衔接，及时通报情况，积极提供协助，共同推动做好社会治理工作。

（四）开设赌场罪

1.最高人民法院关于发布第 20 批指导性案例的通知（法〔2018〕347 号）

各省、自治区、直辖市高级人民法院，解放军军事法院，新疆维吾尔自治区高级人民法院生产建设兵团分院：

经最高人民法院审判委员会讨论决定，现将付宣豪、黄子超破坏计算机信息系统案等五个案例（指导案例 102-106 号），作为第 20 批指导性案例发布，供在审判类似案件时参照。

最高人民法院

2018 年 12 月 25 日

案例一、指导案例 105 号：洪小强、洪礼沃、洪清泉、李志荣开设赌场案

（最高人民法院审判委员会讨论通过 2018 年 12 月 25 日发布）

关键词　刑事/开设赌场罪/网络赌博/微信群

裁判要点

以营利为目的，通过邀请人员加入微信群的方式招揽赌客，根据竞猜游戏网站的开奖结果等方式进行赌博，设定赌博规则，利用微信群进行控制管理，在一段时间内持续组织网络赌博活动的，属于刑法第三百零三条第二款规定的“开设赌场”。

相关法条

《中华人民共和国刑法》第 303 条第 2 款

基本案情

2016 年 2 月 14 日，被告人李志荣、洪礼沃、洪清泉伙同洪某 1、洪某 2（均在逃）以福建省南安市英都镇阀门基地旁一出租房为据点（后搬至福建省南安市英都镇环江路大众电器城五楼的套房），雇佣洪某 3 等人，运用智能手机、电脑等设备建立微信群（群昵称为“寻龙诀”，经多次更名后为“（新）九八届同学聊天”）拉拢赌客进行网络赌博。洪某 1、洪某 2 作为发起人和出资人，负责幕后管理整个团伙；被告人李志荣主要负责财务、维护赌博软件；被告人洪礼沃主要负责后勤；被告人洪清泉主要负责处理与赌客的纠纷；被告人洪小强为出资人，并介绍了陈某某等赌客加入微信群进行赌博。该微信赌博群将启动资金人民币 300000 元分成 100 份资金股，并另设 10 份技术股。其中，被告人洪小强占资金股 6 股，被告人洪礼沃、洪清泉各占技术股 4 股，被告人李志荣占技术股 2 股。

参赌人员加入微信群，通过微信或支付宝将赌资转至庄家（昵称为“白龙账房”、“青龙账房”）的微信或者支付宝账号计入分值（一元相当于一分）后，根据“PC 蛋蛋”等竞

猜游戏网站的开奖结果，以押大小、单双等方式在群内投注赌博。该赌博群 24 小时运转，每局参赌人员数十人，每日赌注累计达数十万元。截至案发时，该团伙共接受赌资累计达 3237300 元。赌博群运行期间共分红 2 次，其中被告人洪小强分得人民币 36000 元，被告人李志荣分得人民币 6000 元，被告人洪礼沃分得人民币 12000 元，被告人洪清泉分得人民币 12000 元。

裁判结果

江西省赣州市章贡区人民法院于 2017 年 3 月 27 日作出（2016）赣 0702 刑初 367 号刑事判决：一、被告人洪小强犯开设赌场罪，判处有期徒刑四年，并处罚金人民币五万元。二、被告人洪礼沃犯开设赌场罪，判处有期徒刑四年，并处罚金人民币五万元。三、被告人洪清泉犯开设赌场罪，判处有期徒刑四年，并处罚金人民币五万元。四、被告人李志荣犯开设赌场罪，判处有期徒刑四年，并处罚金人民币五万元。五、将四被告人所退缴的违法所得共计人民币 66000 元以及随案移送的 6 部手机、1 台笔记本电脑、3 台台式电脑主机等供犯罪所用的物品，依法予以没收，上缴国库。宣判后，四被告人均未提出上诉，判决已发生法律效力。

裁判理由

法院生效裁判认为，被告人洪小强、洪礼沃、洪清泉、李志荣以营利为目的，通过邀请人员加入微信群的方式招揽赌客，根据竞猜游戏网站的开奖结果，以押大小、单双等方式进行赌博，并利用微信群进行控制管理，在一段时间内持续组织网络赌博活动的行为，属于刑法第三百零三条第二款规定的“开设赌场”。被告人洪小强、洪礼沃、洪清泉、李志荣开设和经营赌场，共接受赌资累计达 3237300 元，应认定为刑法第三百零三条第二款规定的“情节严重”，其行为均已构成开设赌场罪。

（生效裁判审判人员：杨菲、宋征鑫、蔡慧）

案例二、指导案例 106 号：谢检军、高垒、高尔樵、杨泽彬开设赌场案

（最高人民法院审判委员会讨论通过 2018 年 12 月 25 日发布）

关键词　刑事/开设赌场罪/网络赌博/微信群/微信群抢红包

裁判要点

以营利为目的，通过邀请人员加入微信群，利用微信群进行控制管理，以抢红包方式进行赌博，在一段时间内持续组织赌博活动的行为，属于刑法第三百零三条第二款规定的“开设赌场”。

相关法条

《中华人民共和国刑法》第 303 条第 2 款

基本案情

2015 年 9 月至 2015 年 11 月，向某（已判决）在杭州市萧山区活动期间，分别伙同被

告人谢检军、高垒、高尔樵、杨泽彬等人，以营利为目的，邀请他人加入其建立的微信群，组织他人在微信群里采用抢红包的方式进行赌博。期间，被告人谢检军、高垒、高尔樵、杨泽彬分别帮助向某在赌博红包群内代发红包，并根据发出赌博红包的个数，从抽头款中分得好处费。

裁判结果

浙江省杭州市萧山区人民法院于2016年11月9日作出（2016）浙0109刑初1736号刑事判决：一、被告人谢检军犯开设赌场罪，判处有期徒刑三年六个月，并处罚金人民币25000元。二、被告人高垒犯开设赌场罪，判处有期徒刑三年三个月，并处罚金人民币20000元。三、被告人高尔樵犯开设赌场罪，判处有期徒刑三年三个月，并处罚金人民币15000元。四、被告人杨泽彬犯开设赌场罪，判处有期徒刑三年，并处罚金人民币10000元。五、随案移送的四被告人犯罪所用工具手机6只予以没收，上缴国库；尚未追回的四被告人犯罪所得赃款，继续予以追缴。宣判后，谢检军、高尔樵、杨泽彬不服，分别向浙江省杭州市中级人民法院提出上诉。浙江省杭州市中级人民法院于2016年12月29日作出（2016）浙01刑终1143号刑事判决：一、维持杭州市萧山区人民法院（2016）浙0109刑初1736号刑事判决第一项、第二项、第三项、第四项的定罪部分及第五项没收犯罪工具、追缴赃款部分。二、撤销杭州市萧山区人民法院（2016）浙0109刑初1736号刑事判决第一项、第二项、第三项、第四项的量刑部分。三、上诉人（原审被告人）谢检军犯开设赌场罪，判处有期徒刑三年，并处罚金人民币25000元。四、原审被告人高垒犯开设赌场罪，判处有期徒刑二年六个月，并处罚金人民币20000元。五、上诉人（原审被告人）高尔樵犯开设赌场罪，判处有期徒刑二年六个月，并处罚金人民币15000元。六、上诉人（原审被告人）杨泽彬犯开设赌场罪，判处有期徒刑一年六个月，并处罚金人民币10000元。

裁判理由

法院生效裁判认为，以营利为目的，通过邀请人员加入微信群，利用微信群进行控制管理，以抢红包方式进行赌博，设定赌博规则，在一段时间内持续组织赌博活动的行为，属于刑法第三百零三条第二款规定的“开设赌场”。谢检军、高垒、高尔樵、杨泽彬伙同他人开设赌场，均已构成开设赌场罪，且系情节严重。谢检军、高垒、高尔樵、杨泽彬在共同犯罪中地位和作用较轻，均系从犯，原判未认定从犯不当，依法予以纠正，并对谢检军予以从轻处罚，对高尔樵、杨泽彬、高垒均予以减轻处罚。杨泽彬犯罪后自动投案，并如实供述自己的罪行，系自首，依法予以从轻处罚。谢检军、高尔樵、高垒到案后如实供述犯罪事实，依法予以从轻处罚。谢检军、高尔樵、杨泽彬、高垒案发后退赃，二审审理期间杨泽彬的家人又代为退赃，均酌情予以从轻处罚。

（生效裁判审判人员：钱安定、胡荣、张茂鑫）

2.典型案例：开设网络平台利用彩票开奖信息进行竞猜赌博的，应当认定为开设赌场罪--颜

植毅、黄吉兴等开设赌场、诈骗，梁锦辉开设赌场案

案例要旨

在网络上开设平台，利用“重庆时时彩”的投注规则、开奖时间及开奖号码作为输赢标准，在平台与投注之间进行对赌的行为，应当认定为开设赌场罪。

案例正文

颜植毅、黄吉兴等开设赌场、诈骗，梁锦辉开设赌场案

【相关法条】

《中华人民共和国刑法》第三百零三条第二款开设赌场的，处三年以下有期徒刑、拘役或者管制，并处罚金;情节严重的，处三年以上十年以下有期徒刑，并处罚金。

第二百二十五条违反国家规定，有下列非法经营行为之一，扰乱市场秩序，情节严重的，处五年以下有期徒刑或者拘役，并处或者单处违法所得一倍以上五倍以下罚金；情节特别严重的，处五年以上有期徒刑，并处违法所得一倍以上五倍以下罚金或者没收财产：

（一）未经许可经营法律、行政法规规定的专营、专卖物品或者其他限制买卖的物品的；

（二）买卖进出口许可证、进出口原产地证明以及其他法律、行政法规规定的经营许可证或者批准文件的；

（三）未经国家有关主管部门批准非法经营证券、期货、保险业务的，或者非法从事资金支付结算业务的；

（四）其他严重扰乱市场秩序的非法经营行为。

第二百六十六条诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

【案件索引】

一审：浙江省杭州市萧山区人民法院（2016）浙 0109 刑初第 2025 号（2017 年 6 月 8 日）

二审：浙江省杭州市中级人民法院（2017）浙 01 刑终 599 号（2017 年 11 月 30 日）

【基本案情】

被告人颜植毅，男，1975 年 3 月 16 日出生于福建省安溪县，汉族，大专文化，无业，户籍地安溪县凤城镇新安西路南侧 2 号 1 梯×××室;因本案于 2016 年 4 月 20 日被刑事拘留，同年 5 月 26 日被逮捕，现羁押于杭州市萧山区看守所。

被告人黄吉兴，别名黄建兴，男，1984 年 10 月 11 日出生于福建省安溪县，汉族，初中文化，个体投资公司经营者，户籍地安溪县魁斗镇镇西村湖内××号；因本案于 2016 年 4 月 20 日被刑事拘留，同年 5 月 26 日被逮捕，现羁押于杭州市萧山区看守所。

被告人陈界龙，男，1980 年 6 月 5 日出生于福建省南安市，汉族，初中文化，无业，

户籍地南安市金淘镇水阁村大路××号；因本案于2016年4月20日被刑事拘留，同年5月26日被逮捕，现羁押于杭州市萧山区看守所。

被告人梁锦辉，男，1984年12月27日出生于福建省南安市，汉族，中专文化，无业，户籍地南安市诗山镇凤坡村瑞莲×××号；因本案于2016年4月20日被刑事拘留，同年5月26日被取保候审，2017年5月25日继续被取保候审。

浙江省杭州市萧山区人民法院经审理查明：

一、开设赌场事实

1.2015年6月份左右，被告人颜植毅、黄吉兴、陈界龙经事先商量后，通过购买网络平台的方式在福建省厦门市翔鹭花城小区房间内开设“中金国际”网络平台，组织他人利用“重庆时时彩”的中奖号码，私设赔率进行竞猜赌博。期间，被告人颜植毅负责日常管理，被告人陈界龙负责平台操作，被告人黄吉兴还聘用被告人梁锦辉等人通过QQ聊天方式招揽客户投注。2015年8月至2016年2月，共接受在该赌博网络平台的充值赌资5208278　91元。

2.2016年3月，被告人颜植毅、黄吉兴结伙，通过购买网络平台的方式在福建省宁德市盈丰佳园小区房间内开设“将军娱乐”网络平台，组织他人利用“重庆时时彩”的中奖号码，私设赔率进行竞猜赌博。期间，被告人颜植毅负责日常管理，被告人黄吉兴聘请被告人梁锦辉等人通过QQ聊天招揽客户投注。至2016年4月20日，共接受在该赌博网络平台的充值赌资54322　75元。

二、诈骗事实

2015年6月至2016年2月，被告人颜植毅、黄吉兴、陈界龙在福建省厦门市翔鹭花城小区房间内开设“中金国际”网络平台组织他人进行赌博竞猜，期间因投注人员中奖金额较大，造成了经营亏损，被告人颜植毅、黄吉兴、陈界龙决定以开展充值优惠活动诱骗客户充值，在活动结束后将平台关闭。2016年2月3日，被告人颜植毅等人在平台上发布充值送百分之五十的优惠活动，骗取充值金额共计3530266元。

杭州市萧山区人民检察院指控被告人颜植毅、黄吉兴、陈界龙犯非法经营罪、诈骗罪、被告人梁锦辉犯非法经营罪，向杭州市萧山区人民法院提起公诉。

被告人颜植毅对起诉书指控其等人开设网络平台招募人员充值投注的主要事实无异议，但辩称其没有销售彩票，只是利用了“重庆时时彩”的中奖号码与网络会员对赌，其行为应认定为赌博罪；对起诉书指控的诈骗事实及罪名均提出异议，辩称自己没有诈骗他人钱财，其行为不构成犯罪。

其辩护人对起诉书指控被告人颜植毅犯诈骗罪的事实及罪名无异议，但对起诉书指控被告人颜植毅犯非法经营罪提出异议，其认为应以赌博罪定罪为宜。量刑方面，其提出被告人颜植毅如实供述了赌博事实，且在赌博过程中基本无获利，建议对被告人颜植毅酌情从轻处罚。

被告人黄吉兴对起诉书指控的事实及罪名均无异议，并当庭表示自愿认罪。

被告人陈界龙对起诉书指控其等人开设网络平台招募人员下注的主要事实无异议，但辩称其等人开设的是赌博网络平台，没有销售彩票，具体罪名由法院依法认定；对起诉书指控其犯诈骗罪的事实及罪名均提出异议，辩称其仅听从安排取钱，并不知道颜植毅等人要关闭网络平台，其没有诈骗故意。

其辩护人对起诉书指控被告人陈界龙犯非法经营罪提出异议，认为应以赌博罪认定为妥；对起诉书指控被告人陈界龙犯诈骗罪的事实及罪名均提出异议，其提出陈界龙对颜植毅等人搞充值送活动的目的及关闭网络平台的事实并不知晓，无共同犯罪故意，其行为不构成诈骗罪。量刑方面，其提出被告人陈界龙有坦白情节，且系初犯，建议对被告人陈界龙从轻处罚。

被告人梁锦辉对起诉书指控的事实及罪名均无异议，并当庭表示自愿认罪。

【裁判结果】

浙江省杭州市萧山区人民法院于 2017 年 6 月 8 日作出浙江省杭州市萧山区人民法院（2016）浙 0109 刑初 2025 号刑事判决：一、被告人颜植毅犯开设赌场罪，判处有期徒刑六年，并处罚金 30 万元；犯诈骗罪，判处有期徒刑八年六个月，并处罚金 1 万元。两罪并罚，决定执行有期徒刑十三年六个月，并处罚金 31 万元。二、被告人黄吉兴犯开设赌场罪，判处有期徒刑六年，并处罚金 30 万元；犯诈骗罪，判处有期徒刑七年六个月，并处罚金 1 万元。两罪并罚，决定执行有期徒刑十二年六个月，并处罚金 31 万元。三、被告人陈界龙犯开设赌场罪，判处有期徒刑五年六个月，并处罚金 25 万元；犯诈骗罪，判处有期徒刑八年，并处罚金 1 万元。两罪并罚，决定执行有期徒刑十二年六个月，并处罚金 26 万元。四、被告人梁锦辉犯开设赌场罪，判处有期徒刑三年，缓刑四年，并处罚金 3 万元。五、公安机关冻结的赃款 246744　44 元按比例发还各被害人；扣押在本院的被告人梁锦辉退出的赃款人民币 18000 元予以没收，上缴国库；尚未追回的被告人颜植毅、黄吉兴、陈界龙犯罪所得赃款，继续予以追缴；随案移送的犯罪工具笔记本电脑 9 台予以没收，上缴国库。

宣判后，浙江省杭州市萧山区人民检察院认为被告人颜植毅等人属于非法发行、销售彩票，其行为应构成非法经营罪，故依法提起抗诉。被告人颜植毅、黄吉兴、陈界龙因事实或罪名有异议均向浙江省杭州市中级人民法院提起上诉。浙江省杭州市中级人民法院于 2017 年 11 月 30 日作出浙江省杭州市中级人民法院（2017）浙 01 刑终 599 号刑事判决：一、驳回抗诉机关（原公诉机关）杭州市萧山区人民检察院之抗诉。二、驳回上诉人（原审被告人）颜植毅、黄吉兴、陈界龙之上诉。三、撤销浙江省杭州市萧山区人民法院（2016）浙 0109 刑初第 2025 号刑事判决第五项中对公安机关冻结的赃款的处理情况的判决；维持判决的其余部分。四、公安机关冻结的赃款人民币 24674444 元全部予以没收并上缴国库。

【裁判理由】

法院生效判决认为：关于抗诉机关提出本案第一起事实应当认定为非法经营罪的抗诉意

见以及上诉人颜植毅提出第一起事实应当定赌博罪的上诉理由。经查：（1）上诉人颜植毅等人设立该网络平台的主观故意是与人在网上对赌，只是利用了“重庆时时彩”这种彩票的投注规则、开奖时间和将开奖号码作为确定输赢的标准，客观上也是由上诉人颜植毅等人以网络平台的形式自己坐庄与参赌人员进行赌输赢，而参赌人员则需要先在该网络平台注册、登录并向账户内充值以获取积分，再以积分下注猜号码。（2）上诉人颜植毅等人的利益来源全部是参赌人员的对赌赌资，且是以庄家的身份和参赌人员结算的方式获取非法利益，并不具有非法发行、销售等经营行为的特点。（3）官方“重庆时时彩”发行的范围仅限于重庆地区，且在此之前就已停止网上销售的方式，因此上诉人颜植毅等人的行为不会干扰到官方“重庆时时彩”的正常经营和国家彩票市场管理交易秩序。（4）上诉人颜植毅等人以营利为目的，在计算机网络上开设赌博网站，接受不特定参赌人员充值投注，参赌人员人数众多且流动性大，社会公众认知度广，涉及赌资金额大，符合开设赌场罪的构成要件。综上，原判认定第一起事实构成开设赌场罪正确，因此，抗诉机关提出的该抗诉意见、上诉人颜植毅提出的该上诉理由均不能成立，二审法院不予采纳。

法院评论

【案例注解】

在审理过程中，对于各被告人在网络上开设平台，利用“重庆时时彩”的投注规则、开奖时间及开奖号码作为输赢标准，在平台与投注之间进行对赌的行为的定性，有三种不同的意见：第一种观点认为各被告人的行为构成非法经营罪；第二种观点认为各被告人的行为构成赌博罪；第三种观点认为各被告人的行为构成开设赌场罪。笔者认为各被告人通过网络，以彩票中奖号码组织他人对赌的行为构成开设赌场罪。

一、被告人的行为不构成非法经营罪

（一）被告人的行为不属于非法发行、销售彩票行为

根据《最高人民法院、最高人民检察院关于办理赌博刑事案件具体应用法律若干问题的解释》第六条的规定，未经国家批准擅自发行、销售彩票，构成犯罪的，以非法经营罪定罪处罚。彩票是指国家为筹集社会公益资金，促进社会公益事业发展而特许发行、依法销售，按照特定规则获得中奖机会的凭证。彩票销售金额的50%左右用于返奖，其余35%左右是政府收入，用于社会公益事业，余者是发行费用。本案中各被告人的利益来源全部是参赌人员的对赌赌资，且是以庄家身份和参赌人员结算的方式获取非法利益。因此，其行为不具有非法发行、销售等经营行为的特点。

（二）被告人的行为没有侵犯市场交易管理秩序

非法经营罪，是指自然人或者单位，违反国家规定，故意从事非法经营活动，扰乱市场秩序，情节严重的行为。非法经营罪侵犯的客体是国家的市场交易管理秩序，涉及彩票的，则为国家的彩票市场管理交易秩序。彩票的发行涉及面广、数额巨大，且其也属于射幸合同，其与赌博在很大程度上具有相似性，但适度的规范彩票市场又是一种有利于社会的再分配。

因此，在我国内地，国家将发行、销售彩票纳入专营范围，进行规范管理，未经审批擅自发行、销售彩票的行为，必然扰乱国家对彩票发行、销售的正常管理秩序。但并非所有利用彩票信息的行为均应当以非法经营罪进行定罪处罚，还要看行为人的行为结果与彩票经营机构有无关联。如果与彩票经营机构没有关联，即使有“重庆时时彩”的外衣，也不应当将其定性为非法经营罪，而应当以赌博罪或者开设赌场罪进行定性。根据在案证据，“重庆时时彩”在2015年2月就已不允许网上销售，且被告人与相应的彩票经营机构之间也没有任何的关联，其只是利用了相应的彩票开奖信息进行对赌，故被告人在网上销售“重庆时时彩”的行为并未扰乱“重庆时时彩”的正常市场交易管理秩序，主要侵害的法益是良好的社会风尚和正常的社会管理秩序。

（三）不以非法经营罪定罪处罚更加符合民众对赌博行为的理解

自彩票不允许网上进行销售之后，一般民众对于网络上还存在的大量的所谓的彩票网站平台，实际上知道该彩票平台不是真正的彩票，其只是利用了彩票的外衣而进行所谓的赌博行为。因此，本案被告人在网络上建立相关平台，让参与人员在该平台上进行注册、登记并向账户内充值获取积分，再以积分下注猜号码比输赢，将参与人员的行为认定为赌博，更加符合民众长期以来对于赌博行为的理解。

二、本案被告人的行为应认定为开设赌场罪

开设赌场罪原是赌博罪的罪状之一，但由于开设赌场参赌人数多，赌资数额大，行为人从中不法获利更多，与一般的聚众赌博相比而言社会危害性更大，因此，《刑法修正案（六）》将其从赌博罪中分立了出来单独进行规定。聚众赌博与开设赌场均有为赌博提供场所、赌具等物质便利条件的行为。但实践中赌博罪与开设赌场罪的主要区别在于赌博犯罪活动的组织性、开放性和经营性。如果被告人对赌场的管理、控制及规模是有严格组织的，且赌博时间、地点相对固定，参赌人员流动性较大的话，就符合开设赌场罪的构罪要件。《最高人民法院、最高人民检察院关于办理网络赌博犯罪案件适用法律若干问题的意见》（以下简称《意见》）明确规定：“利用互联网、移动通讯终端等传输赌博视频、数据，组织赌博活动，具有下列情形之一的，属于刑法第三百零三条第二款规定的‘开设赌场’行为：（一）建立赌博网站并接受投注的；（二）建立赌博网站并提供给他人组织赌博的；（三）为赌博网站担任代理并接受投注的；（四）参与赌博网站利润分成的。”该《意见》明确规定，建立赌博网站并接受投注的属于开设赌场。虽然网络聚众赌博与网络开设赌场在表面行为上有相似之处，但二者不论在主观目的上，还是在客观行为方式上，均有所不同：首先，聚众者的目的仅限于组织他人参赌，以此营利；而赌场的开设者和管理者对整个赌博活动有详细的规划和管理，并通过多种方式吸引更多的人参与赌博活动，维系赌场运行，经营性特征明显，其营利的目的具有更大的全局性和长远性。其次，开设赌场即使是帮助犯，也具有相对的稳定性、连贯性，行为者必然与该赌博网站有某种固定联系，如为赌博网站负责推广、招募会员等，其行为对象面向不特定的社会公众。而聚众赌博则稳定性较弱，对每次赌博的时间与地点的控制

性较弱，行为对象也往往仅局限于其人际关系网。因此，我们在判断区分的时候不能单纯、割裂地从某一招引行为去判断，而更应该根据行为者的主观目的、一贯行为状态以及与赌博网站、赌客之间的关系等因素综合判断。

本案被告人颜植毅、黄吉兴、陈界龙经事先商量后，通过先后开设“中金国际”网络平台、“将军娱乐”网络平台，组织他人利用“重庆时时彩”的中奖号码，私设赔率进行竞猜赌博。期间，被告人颜值毅负责日常管理，被告人陈界龙负责平台操作，被告人黄吉兴还聘用被告人梁锦辉等人通过 QQ 聊天方式招揽客户投注。可见本案被告人的目的是建立一个拥有众多会员的赌博网站，该赌博平台有一套严密的组织体系和工作制度，组织者对赌博平台管理较为严格，人员分工明确，其经营性特征明显。且被告人梁锦辉被招聘进网络平台工作，其所负责的就是向不特定社会公众推广该赌博网站，招揽客户，让客户注册网站会员，从而让客户在该网站上进行赌博。且实际上该赌博网站也拥有一大批会员，规模较大，社会公众的认知度较高。因此，纵观本案情况，各被告人各司其职，分工明确，赌博时间、地点相对固定，赌场规模较大，参赌人员人数众多且流动性大，社会公众认知度广，涉及赌资金额大，可以认定本案被告人的行为属于建立赌博网站并接受投注，应以开设赌场罪进行定罪。

3.典型案例：以营利为目的，利用赌博网站账号开设赌场，并接受他人投注，构成开设赌场罪--谢某某、侯某某开设赌场案

案例要旨

行为人以营利为目的，利用赌博网站账号开设赌场，并接受他人投注的，应按照开设赌场罪追究刑事责任。其中，赌资数额累计达到 30 万元以上的，属于“情节严重”。

案例正文

谢某某、侯某某开设赌场案

【基本案情】

公诉机关：上海市长宁区人民检察院

被告人：谢某某、侯某某

公诉机关指控称：被告人谢某某、侯某某犯开设赌场罪，提请法院依法惩处。

被告人谢某某、侯某某对公诉机关指控的事实、证据和罪名均无异议。

辩护人辩称：对公诉人指控的罪名没有异议，但提出本案不应认定情节严重，同时被告人到案后如实供述自己的犯罪行为，希望对被告人予以从轻处罚。

经审理查明：2015 年 7 月起，被告人谢某某伙同被告人侯某某在其租住的本市长宁路 476 弄小区内，利用申博赌博网站账号开设赌场，以百家乐网络赌博的形式接受赌客投注，并根据投注金额按比例从中牟利。同年 9 月 21 日至 9 月 29 日，该账户的累计投注金额为人民币 670 649 元。

2015 年 9 月 30 日，公安机关在该处抓获两名被告人及纪某某、徐某某等 9 名参赌人员，查获赌资人民币 8300 余元。

【裁判结果】

上海市长宁区人民法院于2016年1月29日作出（2016）沪0105刑初108号刑事判决：

一、被告人谢某某犯开设赌场罪，判处有期徒刑三年六个月，并处罚金人民币一万元。

二、被告人侯某某犯开设赌场罪，判处有期徒刑三年六个月，并处罚金人民币一万元。

三、责令被告人退缴违法所得后予以没收。

【裁判理由】

上海市长宁区人民法院认为：被告人谢某某、侯某某以营利为目的，利用赌博网站组织赌博活动，抽头渔利，其行为均已构成开设赌场罪，且情节严重，依法应予惩处。公诉机关的指控，事实清楚，定性正确。根据查明的事实、情节、后果，公诉机关认定本案情节严重符合相关的法律规定，辩护人关于本案不应认定情节严重的意见，本院不予采纳。被告人谢某某、侯某某到案后能够如实供述自己的罪行，依法可从轻处罚。辩护人与此相关的辩护意见，本院予以采纳。

法院评论

【案例评析】

伴随网络技术的发展与普遍应用，传统的开设赌场犯罪在犯罪手段和表现形式上出现了新的变化，从线下有形场所、面对面的真实庄家转变为线上投注、非可见的虚拟庄家的犯罪形式。这些变化使得该类犯罪呈现出形式更隐蔽、跨域性更广、技术程度更高、组织结构更严密、资金转移更快捷等特点，不仅使得该类犯罪的社会危害性急剧扩大，侦破难度也成倍增加。

本罪的客观方面表现为开设赌博场所的行为。传统意义上的开设赌场行为包括两种情形：一是行为人开设赌场并以自己为庄家，接受参赌者投注，通过获胜机率上的差异而赢取多数参赌人员的财物，实现其营利的犯罪目的。如老虎机、轮盘机、赌球、“百家乐”、赛马等赌博属于此类。二是行为人只提供场所与服务，通过抽头、收取佣金或收取高额的场地费、设备使用费来实现其营利目的。如具有赌博性质的麻将馆、棋牌馆属于此类。

对于利用网络开设赌场的行为，2010年最高人民法院、最高人民检察院、公安部出台的《关于办理网络赌博犯罪案件适用法律若干问题的意见》将其界定为：利用互联网、移动通讯终端等传输赌博视频、数据，组织赌博活动，具有下列情形之一的，属于《刑法》第303条第2款规定的“开设赌场”行为：（1）建立赌博网站并接受投注的；（2）建立赌博网站并提供给他人组织赌博的；（3）为赌博网站担任代理并接受投注的；（4）参与赌博网站利润分成的。可见利用互联网络技术开设赌场主要表现为在计算机网络上建立赌博网站，或者为赌博网站担任代理，接受他人投注。

网络形态的开设赌场有别于传统的开设赌场在于：赌博场所虚拟化，不再是有形的、固定的场所，而是在虚拟的互联网空间进行；赌博投注数字化，不再是真金白银的现金式投注，演变为网上转账、移动支付的数字化投注；庄家非可视化，不再是与庄家面对面交流，而是

通过互联网络联系；赌具电子化，不再是传统有形的机械式赌具，而是通过计算机软件和程序代替；赌博流程即时可视化，使得过去像赛马、赌球等非即时即开性赌博也可以通过网络技术全程可视、即时开奖，便于扩大玩家参与范围。

本罪的主观方面除要求故意之外，还需以营利为目的。即行为人开设赌场是为了获取钱财，而不是为了单纯地消遣、娱乐。

结合本案来看，根据被告人的供述和辩护人的意见，在评价被告人谢某某、侯某某的行为时应当注意两点：一是该行为是否属于司法解释明文规定的利用互联网开设赌场的行为；二是二被告人的犯罪行为是否属于情节严重：

1.被告人的行为是否属于开设赌场行为。被告人谢某某与侯某某利用申博赌博网站账号开设赌场，以百家乐网络赌博的形式接受赌客投注，该行为符合前述司法解释中“为赌博网站担任代理并接受投注的”的客观特征，同时二被告人根据投注金额按比例从中抽头牟利，印证了其主观上具有营利的目的，因此二被告人的行为属于《刑法》第303条第2款规定的“开设赌场”行为。

2.本案是否属于“情节严重”。辩护人提出，本案被告人的行为不应认定为情节严重。根据《最高人民法院、最高人民检察院、公安部关于办理网络赌博犯罪案件适用法律若干问题的意见》的规定，实施前款规定的行为，具有下列情形之一的，应当认定为《刑法》第303条第2款规定的“情节严重”：（1）抽头渔利数额累计达到3万元以上的；（2）赌资数额累计达到30万元以上的；（3）参赌人数累计达到120人以上的；（4）建立赌博网站后通过提供给他人组织赌博，违法所得数额在3万元以上的；（5）参与赌博网站利润分成，违法所得数额在3万元以上的；（6）为赌博网站招募下级代理，由下级代理接受投注的；（7）招揽未成年人参与网络赌博的；（8）其他情节严重的情形。本案中，二被告人接受赌资投注的账户据查累计投注金额为人民币670 649元，符合该司法解释中关于“（2）赌资数额累计达到30万元以上的”构成情节严重的规定，因此法院认定被告人的犯罪行为属于“情节严重”于法有据。

综上所述，本案判决罪名认定和情节认定正确，同时量刑时综合考虑了行为的社会危害性，以及被告人坦白的从轻情节，做到了宽严相济、量刑适当。

利用网络开设赌场犯罪不仅侵犯了社会主义社会风尚，同时也对网络领域的公共秩序和社会主义核心价值观造成了侵害，赌博犯罪往往也是盗窃、抢劫、故意伤害等侵财和暴力犯罪的重要诱因。打击互联网领域的开设赌场犯罪势在必行、刻不容缓。这其中需要注意的是，刑法虽然是打击犯罪的重要手段，但刑罚固有的惩罚性和威吓性属于社会治理模式中的末端治理，无法从源头堵截赌博犯罪的发生和扩大。因此网络空间的社会治理和风气净化需要创新社会治理模式，建立齐抓共治、多元参与的网络综合治理体系，方能营造清朗有序的网络空间。

4.最高人民法院发布第 26 批指导性案例之三：陈庆豪、陈淑娟、赵延海开设赌场案

（2019）赣刑终 93 号

裁判要点

以“二元期权”交易的名义，在法定期货交易场所之外利用互联网招揽“投资者”，以未来某段时间外汇品种的价格走势为交易对象，按照“买涨”“买跌”确定盈亏，买对涨跌方向的“投资者”得利，买错的本金归网站（庄家）所有，盈亏结果不与价格实际涨跌幅度挂钩的，本质是“押大小、赌输赢”，是披着期权交易外衣的赌博行为。对相关网站应当认定为赌博网站。

相关法条

《中华人民共和国刑法》第 303 条

基本案情

2016 年 6 月，北京龙汇联创教育科技有限公司（以下简称“龙汇公司”）设立，负责为龙汇网站的经营提供客户培训、客户维护、客户发展服务，幕后实际控制人周熙坤。周熙坤利用上海麦曦商务咨询有限公司聘请讲师、经理、客服等工作人员，并假冒上海哲荔网络科技有限公司等在智付电子支付有限公司的支付账户，接收全国各地会员注册交易资金

龙汇网站以经营“二元期权”交易为业，通过招揽会员以“买涨”或“买跌”的方式参与赌博。会员在龙汇网站注册充值后，下载安装市场行情接收软件和龙汇网站自制插件，选择某一外汇交易品种，并选择 1M（分钟）到 60M 不等的到期时间，下单交易金额，并点击“买涨”或“买跌”按钮完成交易。买定离手之后，不可更改交易内容，不能止损止盈，若买对涨跌方向即可盈利交易金额的 76%-78%，若买错涨跌方向则本金全亏，盈亏情况不与外汇实际涨跌幅度挂钩。龙汇网站建立了等级经纪人制度及对应的佣金制度，等级经纪人包括 SB 银级至 PB 铂金三星级六个等级。截止案发，龙汇网站在全国约有 10 万会员。

2017 年 1 月，陈庆豪受周熙坤聘请为顾问、市场总监，从事日常事务协调管理，维系龙汇网站与高级经纪人之间的关系，出席“培训会”“说明会”并进行宣传，发展会员，拓展市场。2016 年 1 月，陈淑娟在龙汇网站注册账号，通过发展会员一度成为 PB 铂金一星级经纪人，下有 17000 余个会员账号。2016 年 2 月，赵延海在龙汇网站注册账号，通过发展会员一度成为 PB 铂金级经纪人，下有 8000 余个会员账号。经江西大众司法鉴定中心司法会计鉴定，2017 年 1 月 1 日至 2017 年 7 月 5 日，陈淑娟从龙汇网站提款 180 975.04 美元，赵延海从龙汇网站提款 11598.11 美元。2017 年 7 月 5 日，陈庆豪、陈淑娟和赵延海被抓获归案。陈庆豪归案后，于 2017 年 8 月 8 日退缴 35 万元违法所得。

裁判结果

江西省吉安市中级人民法院于 2019 年 3 月 22 日作出（2018）赣 08 刑初 21 号刑事判决，以被告人陈庆豪犯开设赌场罪，判处有期徒刑三年，并处罚金人民币五十万元，驱逐出境；被告人陈淑娟犯赌博罪，判处有期徒刑二年，并处罚金人民币三十万元；被告人赵延海犯赌博罪，判处有期徒刑一年十个月，并处罚金人民币二十万元；继续追缴被告人陈淑娟和赵延海的违法所得。宣判后，陈庆豪、陈淑娟提出上诉。江西省高级人民法院于 2019 年 9 月 26 日作出（2019）赣刑终 93 号刑事判决，以上诉人陈庆豪犯开设赌场罪，改判有期徒刑二年六个月，并处罚金人民币五十万元，驱逐出境；上诉人陈淑娟犯开设赌场罪，判处有期徒刑二年，并处罚金人民币三十万元；被告人赵延海犯开设赌场罪，判处有期徒刑一年十个月，并处罚金人民币二十万元；继续追缴陈淑娟和赵延海的违法所得。

裁判理由

法院生效裁判认为，根据国务院 2017 年修订的《期货交易管理条例》第一条、第四条、第六条规定，期权合约是指期货交易场所统一制定的、规定买方有权在将来某一时间以特定价格买入或者卖出约定标的物的标准化合约。期货交易应当在期货交易所等法定期货交易场所进行，禁止期货交易场所之外进行期货交易。未经国务院或者国务院期货监督管理机构批准，任何单位或者个人不得以任何形式组织期货交易。简言之，期权是一种以股票、期货等品种的价格为标的，在法定期货交易场所进行交易的金融产品，在交易过程中需完成买卖双方权利的转移，具有规避价格风险、服务实体经济的功能。

龙汇“二元期权”的交易方法是下载市场行情接收软件和龙汇网站自制插件，会员选择外汇品种和时间段，点击“买涨”或“买跌”按钮完成交易，买对涨跌方向即可盈利交易金额的 76%-78%，买错涨跌方向则本金即归网站（庄家）所有，盈亏结果与外汇交易品种涨跌幅度无关，实则是以未来某段时间外汇、股票等品种的价格走势为交易对象，以标的价格走势的涨跌决定交易者的财产损益，交易价格与盈亏幅度事前确定，盈亏结果与价格实际涨跌幅度不挂钩，交易者没有权利行使和转移环节，交易结果具有偶然性、投机性和射幸性。因此，龙汇“二元期权”与“押大小、赌输赢”的赌博行为本质相同，实为网络平台与投资者之间的对赌，是披着期权外衣的赌博行为。

被告人陈庆豪在龙汇公司担任中国区域市场总监，从事日常事务协调管理，维护公司与经纪人关系，参加各地说明会、培训会并宣传龙汇“二元期权”，发展新会员和开拓新市场，符合《最高人民法院最高人民检察院公安部关于办理网络赌博犯罪案件适用法律若干问题的意见》（以下简称《意见》）第二条规定的明知是赌博网站，而为其提供投放广告、发展会员等服务的行为，构成开设赌场罪，其非法所得已达到《意见》第二条规定的“收取服务费数额在 2 万元以上的”5 倍以上，应认定为开设赌场“情节严重”。但考虑到其犯罪事实、行为性质、在共同犯罪中的地位作用和从轻量刑情节，对其有期徒刑刑期予以酌减，对罚金刑依法予以维持。陈淑娟、赵延海面向社会公众招揽赌客参加赌博，属于为赌博网站担任代理并接受投注行为，且行为具有组织性、持续性、开放性，构成开设赌场罪，并达到“情节严重”。原判认定陈淑娟、赵延海的罪名不当，二审依法改变其罪名，但根据上诉不加刑原则，维持一审对其量刑。

5.检察机关依法惩治开设赌场犯罪典型案例

发布时间：2021 年 11 月 29 日

11 月 29 日，最高人民检察院召开以“依法履行检察职能，从严惩治开设赌场犯罪”为主题的新闻发布会，发布检察机关依法惩治开设赌场犯罪典型案例。

案例一、刘某某、曾某某等 11 人开设赌场案

【基本案情】

2018 年，被告人刘某某、曾某某等人经商议后，将原先各自建在国内运营的“极速”、“鼎鑫”两个网络赌盘的软件服务器移设至某国合并运营，并招纳人员出境负责赌场的运营管理。赌场开设“北京赛车”“重庆时时彩”“幸运飞艇”等赌博项目，通过电信网络发布信息等方式，在网络上组织招揽包括福建、湖南、江西等十余省的 9242 人为会员进行赌博，并以给会员“返水”、客服人员提成、发展代理的方式逐渐做大并陆续新增多个赌盘。截至 2019 年 11 月案发，涉案赌资流水达 24 亿余元，该犯罪团伙非法获利 2400 多万元。

福建省连城县人民法院于2021年3月2日以开设赌场罪分别判处刘某某、曾某某等11名被告人七年至一年不等的有期徒刑，并处最高55万元的罚金。该案经二审审理，判决已生效。

【办案经过】

福建省连城县人民检察院对该案提前介入，引导公安机关通过技术手段调取相关证据，依法认定该案的涉案赌资及相关人员的非法获利；针对33名涉案人员仅到案11人，大部分涉案人员尤其是负责赌场财务管理的核心人员滞留境外未归案的情况，检察机关积极履行法律监督职责，与公安机关共同通过加强政策法律宣讲，督促在案人员及其家属动员同案人投案。后部分涉案人员主动从境外回国投案。

【典型意义】

1.该案社会危害性大。网络赌博这种新型开设赌场犯罪，严重危害了人民群众财产安全和合法权益，损害了社会诚信和社会秩序，导致受害者深陷泥潭。本案涉及地域广、人员多，涉案金额大，侦查机关调查取证的16名参赌人员，总计输了500多万元，无一人获利。其中有的参赌人员短短半个月内就输了110多万元，倾家荡产，导致生产经营项目资金链断裂；有的参赌人员经微信好友推荐参与赌博后，从小赌到大赌，整天沉迷于网络赌博，玩物丧志；有的参赌人员是父子，输了数十万元，因债务导致父子反目成仇。

2.检察机关在办案中坚持贯彻宽严相济刑事政策。为依法严惩该犯罪，检察机关在依法提出的量刑建议中，综合考虑该案社会危害性，对于所有的被告人建议不适用缓刑，并根据各被告人在犯罪中的地位作用以及查明的非法获利数额，建议对各被告人并处相应的罚金刑，以剥夺其再犯的能力。同时，对于认罪悔罪，成功规劝同案人投案的被告人，依法认定为立功，建议对其减轻处罚。法院采纳了检察机关的相关意见。

案例二、吴某等63人开设赌场系列案

【基本案情】

1999年至2020年8月期间，吴某、邓某某等人与许某（另案处理）相互纠合，依托某国外赌场，以开展高尔夫球运动等“商务活动”为名，采取游、住、赌一体化的经营模式，组织我国公民入住位于该赌场所在的酒店并到赌场参与赌博活动。2020年后，该犯罪组织为牟取更多的非法利益，依托该实体赌场发展面向中国公民的网上赌博业务，并将实体赌场的中国籍“洗码”人员发展为赌博网站股东代理，再通过股东代理发展下级代理及会员。股东代理与下级代理利用微信、支付宝、银行卡转账等方式收取赌资，通过与赌博网站五五分成和抽取赌客投注金额0.8%提成的方式获取非法利益。该犯罪组织共发展中国籍股东代理与下级代理51名，发展中国籍赌博会员数百名，涉案赌资达2.5亿元。

【办案经过】

该案由广东省广州市公安机关立案侦查，广州市从化区人民检察院通过提前介入，引导侦查取证，在案件定性、事实认定、证据收集等方面提出引导侦查意见，全面完善案件证据体系。因该案具有主要犯罪行为在国外实施、涉案人员多、陆续到案等特点，检察机关对于

在案人员，分案处理，目前已对该系列案全部案件依法提起公诉，对组织中国公民出境赌博、招揽中国公民参与网络赌博人员中的11名赌场高管、骨干成员依法从严惩处，提出有期徒刑六年至三年不等的量刑建议，法院采纳了检察机关的量刑建议并已宣判。

【典型意义】

1.一些民营企业主成为境外赌博犯罪集团重点“围猎”的目标。在该案中，犯罪分子以较有经济实力的民营企业主为重点目标群体，利用与“商务公司”合作组织出国或者与旅行社合作吸引高尔夫球客户的名义，组织我国境内民营企业主出国入住赌场所在的酒店，参与赌博，有的参赌人员还被一步步引诱发展为代理，继续组织其他人员出国赌博，实施开设赌场犯罪。该案中的被告人文某某、王某等人原是民营企业主，先是成为赌博会员，后注册成为代理以求快速“翻盘”，最终深陷泥潭，走上犯罪的道路，而自己经营的企业也因群龙无首，面临破产。

2.部分赴境外务工人员法律意识淡薄，为赚取“快钱”走上犯罪的道路。因疫情原因，境外实施开设赌场犯罪的团伙为继续牟取非法利益，多开始向网络赌场转型。该系列案中的邓某某等人原是赌场的厨房员工，后兼职“洗码”，从中赚取“快钱”，并注册成为该赌场网站股东代理，招揽中国公民参与网络赌博。牟某某为该赌场人事部主管，明知该犯罪团伙大肆组织我国公民出境赌博并招揽我国境内公民参与网上赌博，仍负责招聘、培训“荷官”（在赌场内负责发牌等事项的人），成为开设赌场犯罪的帮助者。该二人原本都是普通的出国务工人员，但因法律意识淡薄，一直误以为自己在国外从事的是合法工作，最终成为了犯罪集团的成员，走上了犯罪的道路。

案例三、宋某某等11人开设赌场案

【基本案情】

马来西亚居民熊某某（原中国籍，在逃）为牟取非法利益，自2017年10月至2019年8月，实施网络开设赌场犯罪。为方便与境内参赌人员收付结算赌资，被告人宋某某、家某某、卫某某等人与在国外的熊某某合谋，雇用被告人万某等人，在山西省运城市、长治市等地开设“网络工作室”，为熊某某的网络赌博平台发送赌博广告信息，提供赌博平台链接，并大量收购银行卡、身份证、网银U盾、支付宝（俗称“四件套”），用于为网络赌博平台收取赌资。通过网上银行向境外进行赌资结算，或直接提现，偷越国境将赌资运往境外，涉案资金高达3亿余元。另查明，该团伙部分成员还实施了非法拘禁，盗窃，掩饰、隐瞒犯罪所得，贷款诈骗等犯罪。

山西省运城市盐湖区人民法院于2021年6月29日作出一审判决，以开设赌场罪、非法拘禁罪、偷越国境罪分别判处被告人宋某某等11人八年六个月至二年六个月不等的有期徒刑，并判处相应的罚金。该判决已生效。

【办案过程】

山西省运城市检察机关在办理该案中，准确认定事实，精准适用法律。检察机关认为，网络赌博网站结算赌资过程中收购使用“四件套”，其是为网络赌博结算赌资而实施的，是开设赌场犯罪行为的一部分，应当评价为开设赌场犯罪。

【典型意义】

借助互联网的便利性，新型赌博犯罪中，赌资收付、变现作为开设赌场犯罪牟取暴利的重要组成部分，已成为一个独立实施的环节。该案中，宋某某等人并没有直接实施开设赌场的行为，但其与组织实施网络赌博的人员事前共谋，代为收付结算赌资并变现，与直接实施开设赌场犯罪的熊某某构成共同犯罪，应当按照开设赌场罪对其进行评价。同时，在新型开设赌场犯罪中，因为犯罪分工更加细化，犯罪链条长，参与人员多，也易衍生、伴生多种犯罪，该案中，涉案人员在实施开设赌场犯罪过程中，该团伙部分成员还实施了非法拘禁、偷越国境等其他犯罪，社会危害性大。

案例四、唐某某等 9 人开设赌场案

【基本案情】

“德扑圈”APP 是一款网络德州扑克软件。2018 年 3 月，被告人唐某某、王某某在“德扑圈”APP 内通过平台的分组功能建立了“云巅俱乐部”，招揽赌客利用该款软件在俱乐部内以德州扑克的形式进行赌博。赌客可以与其他赌客对赌，也可以与系统对赌，唐某某等人用联盟币（该应用软件中的“虚拟币”）为赌客结算，1 个联盟币对应 1 元人民币，赌客充值到客服提供的微信或支付宝，客服就会在赌客俱乐部账户内增加相应的联盟币数量。赌博结束后赌客可以找客服提现，把联盟币转化成真实钱款。2019 年 6 月至 2020 年 5 月，“云巅俱乐部”共接受赌客赌资 697 万余元，唐某某等 9 人非法获利 300 万余元。

江苏省常州市天宁区人民法院于 2021 年 6 月 21 日对该案作出一审判决，以开设赌场罪分别判处唐某某等 9 人四年六个月至十个月不等的有期徒刑，并判处相应的罚金。该案经二审审理，判决已生效。

【办案过程】

江苏省常州市天宁区人民检察院在办理该案过程中，先后列出多条补充侦查提纲，引导侦查机关调查赃款去向、厘清款项性质，查封房产 2 套、扣押汽车 1 辆、冻结银行账户资金 50 余万元，积极敦促被告人退赃。同时检察机关积极释法说理，其中 8 名被告人自愿认罪认罚。

【典型意义】

近年来，网络赌博犯罪多发、手段花样翻新，犯罪分子通过搭建网络赌博平台，打着网络游戏、虚拟币等“幌子”接受投注，吸引群众参与赌博。该案中，被告人利用网络棋牌游戏应用，通过线下兑换虚拟币，实施开设赌场犯罪，对于该种行为，要透过现象看实质，从游戏过程中是否有资金、实物兑换，是否有抽头渔利行为等来准确认定是娱乐还是赌博。对于以游戏为名，通过缴纳报名费或者现金换取筹码参加游戏的形式，赢取筹码后能够兑换现金、有价证券或者其他财物的，其实质是赌博违法犯罪，也必将被法律所严惩。

案例五、陈某某等 14 人开设赌场案

【基本案情】

2018 年 10 月至 2020 年 8 月期间，陈某某伙同他人雇佣朱某某、丁某某等人在某国建立工作室，形成较为固定的赌博犯罪集团，下设值班财务、主持、推码手、代理等岗位。该犯罪集团通过国内的即时通信应用软件建立网络赌博平台，组织我国公民在境内通过直播网站观看境外赌博实况视频并接受投注，以赌场洗码返水的方式获利。其中由值班财务负责为赌客提供赌资充值、提现等资金结算服务，并发送赌场直播网站网址和桌位号；由主持负责接受赌博群内赌客下注，统计下注情况和发布输赢结果；由推码手负责赌场的现场下注。其间，该犯罪集团经手转账赌资达 8746 万元以上。

浙江省平阳县人民法院于 2021 年 6 月 25 日作出一审判决，以开设赌场罪判处被告人陈某某五年有期徒刑，并处罚金，该判决已生效。其余同案人员尚在审查起诉阶段。

【办案经过】

浙江省温州市平阳县人民检察院在办理该案过程中，准确认定犯罪集团成员架构，审慎采取强制措施，坚持分层处理、区分罪责的原则，对该犯罪集团的 6 名一般参加者不予批准逮捕；针对侦查机关移送起诉时涉案赌资仅为 34 万元，赌资认定存在难点等问题，通过自行补充侦查，以用于支付结算的黑灰产业链为切入点，倒查赌资结算路径，排查犯罪集团相关人员及亲属的支付结算账号的大额、异常流水，明确涉赌支付结算账户以及赌资数额认定规则，将原认定的赌资由人民币 34 万元增至 8746 万元。

【典型意义】

近年来，跨境赌博犯罪活动向互联网迁移，其中赌资数额的认定，常常需要通过电子证据证实，认定困难。而准确认定该事实，既有利于依法打击赌博犯罪，斩断犯罪分子通过违法犯罪获利的利益链，也有助于摧毁该类犯罪的经济基础，最大限度剥夺犯罪分子再犯能力。该案中检察机关充分发挥检察职能，通过自行补充侦查，准确认定开设赌场犯罪赌资数额，依法严厉打击此类犯罪，同时积极贯彻少捕慎押的刑事司法政策，实现办案“三个效果”统一。

（五）编造、故意传播虚假信息罪

【法律要旨】在疫情防控期间，编造虚假的疫情信息，在信息网络或者其他媒体上传播，或者明知是虚假疫情信息，故意在信息网络上或者其他媒体上传播，严重扰乱社会秩序的，依照刑法第二百九十一条之一第二款的规定，以编造、故意传播虚假信息罪定罪处罚。编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第四项的规定，以寻衅滋事罪定罪处罚。

最高检跟踪发布 5 件全国检察机关依法惩治妨害疫情防控秩序犯罪典型案例之五：辽宁省鞍山市赵某某编造、故意传播虚假信息案：

被告人赵某某系无业人员，自 2018 年开始购置警用装备，并多次在社交平台发布其穿戴警用装备的视频冒充警察。2020 年 1 月 26 日，赵某某为满足虚荣心，扩大网络影响力，将自己身着警服的照片设为微信头像，同时将微信昵称设为“鞍山交警小龙”，并在微信朋友圈发布信息称：“鞍山交警小龙温馨提示大家！今天鞍山市城市公交车！全部停运！从明天开始长途客运站停止营运所有长途汽车！今晚我值班由我带队出去执勤！今晚从半夜 12 点开始！由我带队在鞍山所有的高速公路口全城封闭！所有的车辆不准进入我们鞍山！”“鞍山市今晚全城开始封路！请广大司机朋友们！没事请不要出门了”，并配发多张警察执勤图

片。该条信息发布后，被多名网友转发至朋友圈和微信群，大量市民向相关部门电话咨询，鞍山市交通管理局接听 95 人次，鞍山市 8890 民生服务平台接听 24 人次，110 接警中心接听 78 人次，引发不良影响，影响疫情防控工作的正常秩序。案发后，鞍山市铁西区人民检察院第一时间启动重大敏感案件快速反应工作机制，掌握案件进展与取证情况，就证据调取、适用法律问题与公安机关充分交换意见。2020 年 2 月 10 日，铁西区人民检察院对赵某某以编造、故意传播虚假信息罪批准逮捕。2 月 17 日，铁西区人民检察院对赵某某以编造、故意传播虚假信息案提起公诉。2 月 21 日，鞍山市铁西区人民法院适用速裁程序审理该案并当庭宣判，全部采纳检察机关量刑建议，以编造、故意传播虚假信息罪判处赵某某有期徒刑一年六个月。赵某某未上诉，判决生效。

四、普通案例

（一）非法侵入计算机信息系统罪

案例一、李文环、王硕、卢晓燕等非法侵入计算机信息系统案

李文环、王硕、卢晓燕等非法侵入计算机信息系统罪一审刑事判决书

(2018)川 3424 刑初 169 号

公诉机关四川省德昌县人民检察院。

被告人李文环,男,1986 年 3 月 22 日出生,汉族,大学本科文化,居民,户籍所在地浙江省杭州市余杭区,住浙江省杭州市余杭区。因涉嫌犯非法获取计算机信息系统数据罪,于 2017 年 12 月 8 日被德昌县公安局刑事拘留,同年 12 月 28 日经德昌县人民检察院以非法侵入计算机信息系统罪批准逮捕,次日被德昌县公安局执行逮捕。现羁押于德昌县看守所。

被告人王硕,男,1985 年 9 月 24 日出生,汉族,大学本科文化,居民,户籍所在地上海市闵行区,住上海市闵行区。因涉嫌犯非法获取计算机信息系统数据罪,于 2017 年 12 月 5 日被德昌县公安局刑事拘留,同年 12 月 28 日经德昌县人民检察院以非法侵入计算机信息系统罪批准逮捕,次日被德昌县公安局执行逮捕。2018 年 10 月 12 日,因存疑不诉被释放。本院于 2018 年 12 月 19 日依法对其决定予以逮捕,2019 年 1 月 18 日德昌县公安局对其执行逮捕。现羁押于德昌县看守所。

被告人卢晓燕,女,1988 年 5 月 29 日出生,汉族,硕士研究生文化,居民,户籍所在地上海市浦东新区,住上海市浦东区。因涉嫌犯非法获取计算机信息系统数据罪,于 2017 年 12 月 5 日被德昌县公安局刑事拘留,同年 12 月 28 日经德昌县人民检察院以非法侵入计算机信息系统罪批准逮捕,次日被德昌县公安局执行逮捕。2018 年 10 月 12 日,因存疑不诉被释放。本院于 2018 年 12 月 19 日依法对其决定予以逮捕,2019 年 1 月 24 日德昌县公安局对其执行逮捕。现羁押于德昌县看守所。

被告人栾东超,男,1982 年 8 月 19 日出生,汉族,大专文化,居民,户籍所在地山东省聊城市茌平县,住山东省聊城市茌平县。因涉嫌犯非法获取计算机信息系统数据罪,于 2017 年 11 月

26 日被德昌县公安局刑事拘留,同年 12 月 28 日经德昌县人民检察院以非法侵入计算机信息系统罪批准逮捕,次日被德昌县公安局执行逮捕。2018 年 10 月 12 日,因存疑不诉被释放。本院于 2018 年 12 月 19 日依法对其决定予以逮捕,2019 年 1 月 19 日德昌县公安局对其执行逮捕。现羁押于德昌县看守所。

被告人徐明,男,1989 年 8 月 24 日出生,汉族,大专文化,居民,户籍所在地山东省聊城市东昌府区,住山东省聊城市东昌府区。因涉嫌犯非法获取计算机信息系统数据罪,于 2017 年 11 月 23 日被德昌县公安局刑事拘留,同年 12 月 28 日经德昌县人民检察院以非法侵入计算机信息系统罪批准逮捕,次日被德昌县公安局执行逮捕。2018 年 10 月 12 日,因存疑不诉被释放。本院于 2018 年 12 月 19 日依法对其决定予以逮捕,2019 年 1 月 19 日德昌县公安局对其执行逮捕。现羁押于德昌县看守所。

被告人吴杰,男,1983 年 5 月 1 日出生,汉族,中专文化,居民,户籍所在地四川省阿坝藏族羌族自治州,住四川省成都市郫都区。因涉嫌犯非法获取计算机信息系统数据罪,于 2017 年 11 月 25 日被德昌县公安局刑事拘留,同年 12 月 28 日经德昌县人民检察院以非法侵入计算机信息系统罪批准逮捕,次日被德昌县公安局执行逮捕。2018 年 3 月 27 日被德昌县公安局取保候审,2018 年 9 月 12 日德昌县人民检察院决定对其取保候审,同日由德昌县公安局执行。2018 年 10 月 12 日,德昌县人民检察院对其作出存疑不起诉。本院于 2018 年 12 月 19 日依法对其决定予以逮捕,2019 年 1 月 18 日德昌县公安局对其执行逮捕。现羁押于德昌县看守所。

四川省德昌县人民检察院于 2018 年 12 月 10 日以德检公诉刑诉〔2018〕149 号起诉书指控被告人李文环、王硕、卢晓燕、栾东超、徐明、吴杰犯非法侵入计算机信息系统罪向本院提起公诉。本院受理后,在本案审理期间,德昌县人民检察院于 2019 年 3 月 7 日建议本院延期审理,本院于次日决定延期审理本案。2019 年 4 月 4 日德昌县人民检察院补充侦查完毕,建议本院恢复审理,本院于同日恢复本案的审理。本院依法组成合议庭,并召开了庭前会议,公开开庭审理了本案。德昌县人民检察院指派检察员鞠勇、李必洁出庭支持公诉,被告人李文环、王硕、卢晓燕、栾东超、徐明、吴杰,以及李文环的辩护人罗伟军、苏小平,王硕的辩护人陈立英,吴杰的辩护人谢春到庭参加了诉讼。本案现已审理终结。

鉴于本案案情复杂,证据较多,本院依职权于 2019 年 6 月 17 日召开了庭前会议,承办法官就控辩双方在管辖、回避等方面的程序性事项了解情况,听取意见。控辩双方在庭前会议中就程序性事项已达成一致意见,并予以确认。庭前会议形成了会议报告,并提交合议庭。

四川省德昌县人民检察院起诉书指控: 2014 年至今,被告人李文环使用“爬虫”软件,大量爬取全国各地及凉山州公安局
交警支队车管所公告的车牌放号信息,之后使用软件采用多线程提交、批量刷单、验证码自动识别等方式,突破系统安全保护措施,将爬取的车牌号提交至“交通安全服务管理平台”车辆报废查询系统,进行对比,并根据反馈情况自动记录未注册车牌号,建立全国未注册车牌号

数据库。李文环之后编写客户端查询软件,由李文环通过 QQ、淘宝、微信等方式,以 300-3000 元每月的价格,分省市贩卖数据库查阅权限。其中将软件卖给李某 2(微信名为“嗨亲爱的”),非法选取凉山州车牌三个(WQQ777、WQJ777、WQX999);将软件卖给李某 1(微信名为“成都车森林”),非法选取凉山州车牌 1 个(WQD777)。被告人吴杰明知李文环使用非法手段获取未注册车牌信息,而购买抢号软件、查库软件,非法选取四个成都市车牌号码(A5432F、A6543J、A4777、DAS456)。2016 年 6 月至今,被告人王硕编写使用软件登录“交通安全服务管理平台”,大量爬取全国各地及凉山州公安局交警支队车管所公告的车牌放号信息,使用软件突破系统安全保护措施,将爬取的车牌号提交至“交通安全服务管理平台”车辆违章查询系统,进行对比,并根据反馈情况自动记录未注册车牌号,建立全国未注册车牌号数据库。王硕编写客户端查询软件,由卢晓燕通过淘宝、微信等方式,以 20 元每 48 小时的价格,分省市贩卖数据库查阅权限。王硕、栾东超、卢晓燕在全国范围内招募徐明、吴杰等各省选车牌号下线代理人,并招揽客户,提供身份证号码、车架号等信息,比对未注册车牌号数据库使用抢号软件采用多线程登录,编辑“按键精灵”类软件模拟人工操作,编辑验证码自动识别输入,实现快速抢号,之后选取车牌贩卖。

被告人徐明、吴杰明知栾东超、王硕等人采用软件等非法手段获取未注册车牌数据库,而向栾东超提供由蒋某、唐某、曹某、韦某提供给的凉山州车主身份证号码、车架号,栾东超又将信息提交给王硕以选取车牌(WPX999、WQC888、WQE666、WQK777、WPQ888、WQK888、WPF888)。

被告人吴杰在案发后提供线索揭发他人犯罪行为,经查证属实。被告人卢晓燕在案发后协助公安机关成功抓捕同案其他被告人。被告人栾东超在案发后主动到公安机关投案自首,并如实供述自己的犯罪事实。

公诉机关认为,被告人李文环、王硕、卢晓燕、栾东超、徐明、吴杰为牟取私利,违法国家规定,侵入国家事务领域的计算机信息系统,其行为均已触犯《中华人民共和国刑法》第二百八十五条第一款之规定,应当以非法侵入计算机信息系统罪追究其刑事责任。被告人王硕、卢晓燕、栾东超、徐明、吴杰的行为同时适用《中华人民共和国刑法》第二十五条第一款关于共同犯罪的规定。被告人吴杰、卢晓燕的行为适用《中华人民共和国刑法》第六十八条关于立功的规定。被告人栾东超的行为适用《中华人民共和国刑法》第六十七条关于自首的规定。在开庭审理前,公诉机关向本院提交了本案不宜区分主从的补充说明。对指控的事实,公诉机关当庭出示了相关证据予以证实。

被告人李文环、王硕、卢晓燕、栾东超、徐明、吴杰,以及李文环、王硕、吴杰的辩护人对起诉书指控的罪名和事实、当庭出示的证据均无异议,且在法庭上均无证据出示。六被告人当庭自愿认罪认罚,被告人及其辩护人均请求对被告人从轻处罚。本院审理查明的事实

与起诉书指控六被告人的上述事实相符。另查明,被告人吴杰已代被告人王硕、卢晓燕、栾东超、徐明退清了本案的涉案赃款。

上述事实,被告人李文环、王硕、卢晓燕、栾东超、徐明、吴杰在开庭审理过程中亦无异议,并有受案登记表、立案决定书、户籍信息、抓获经过、扣押决定书、扣押清单、指定管辖决定书、情况说明、银行交易明细、号牌投放记录、操作日志、上海弘连网络科技有限公司计算机司法鉴定所司法鉴定意见书、提取笔录、搜查笔录、侦查实验笔录、证人张某、羊某、刘某1、刘某2、罗某、周某、邓某、李某1、李某2等人的证言、光盘、拷贝数据移动硬盘、被告人李文环、王硕、卢晓燕、栾东超、徐明、吴杰的供述等证据予以证实,足以认定。

本院认为,被告人李文环、王硕、卢晓燕、栾东超、徐明、吴杰为牟取私利,违法国家规定,侵入国家事务领域的计算机信息系统,六被告人的行为均已构成非法侵入计算机信息系统罪。德昌县人民检察院指控六被告人的罪名成立,本院予以支持。在案的证据证实,被告人吴杰在案发后提供线索揭发他人犯罪行为,并经查证属实;被告人卢晓燕在案发后协助公安机关成功抓捕同案其他被告人。二被告人的行为均属立功,依法可对其从轻处罚。被告人栾东超在案发后主动到公安机关投案,并如实供述其犯罪事实,其行为属自首,依法可对其从轻处罚。被告人王硕、卢晓燕、栾东超、徐明、吴杰属共同犯罪。对公安机关依法扣押本案的涉案财物,应依法予以没收。案发后,被告人李文环已退缴了违法所得,被告人吴杰已退缴了自己的违法所得,并代被告人王硕、卢晓燕、栾东超、徐明退缴了本案的涉案赃款,可对被告人酌情从轻处罚。被告人李文环、王硕、卢晓燕、栾东超、徐明、吴杰当庭自愿认罪认罚,均可对其从轻处罚。

在对六被告人量刑时,将根据各被告人的犯罪事实、性质、情节及对社会的危害程度,依法对其进行处罚。公诉机关对六被告人提出的量刑建议与其所犯罪行的事实、情节相适应,本院予以采纳。为此,依照《中华人民共和国刑法》第二百八十五条第一款、第二十五条第一款、第六十八条、第六十七条第一款、第三款、第六十四条、第四十七条之规定,判决如下:

一、被告人李文环犯非法侵入计算机信息系统罪,判处有期徒刑一年零七个月。(刑期从判决执行之日起计算。判决执行以前先行羁押的,羁押一日折抵刑期一日,即自二0一七年十二月八日起至二0一九年七月七日止。)

二、被告人王硕犯非法侵入计算机信息系统罪,判处有期徒刑一年四个月零十五日。(刑期从判决执行之日起计算。判决执行以前先行羁押的,羁押一日折抵刑期一日,即自二0一九年一月十八日起至二0一九年七月二十四日止。先行羁押天数已折抵。)

三、被告人卢晓燕犯非法侵入计算机信息系统罪,判处有期徒刑一年四个月零五日。(刑期从判决执行之日起计算。判决执行以前先行羁押的,羁押一日折抵刑期一日,即自二 0 一九年一月二十四日起至二 0 一九年七月十九日止。先行羁押天数已折抵。)

四、被告人栾东超犯非法侵入计算机信息系统罪,判处有期徒刑一年四个月零五日。(刑期从判决执行之日起计算。判决执行以前先行羁押的,羁押一日折抵刑期一日,即自二 0 一九年一月十九日起至二 0 一九年七月五日止。先行羁押天数已折抵。)

五、被告人徐明犯非法侵入计算机信息系统罪,判处有期徒刑一年四个月零十五日。(刑期从判决执行之日起计算。判决执行以前先行羁押的,羁押一日折抵刑期一日,即自二 0 一九年一月十九日起至二 0 一九年七月十三日止。先行羁押天数已折抵。)

六、被告人吴杰犯非法侵入计算机信息系统罪,判处有期徒刑十个月。 (刑期从判决执行之日起计算。判决执行以前先行羁押的,羁押一日折抵刑期一日
,即自二 0 一九年一月十八日起至二 0 一九年七月十五日止。先行羁押天数已折抵。)

七、对公安机关依法扣押供被告人犯罪所用的涉案财物:李文环的 ASUS 牌笔记本电脑一台;王硕的东芝牌笔记本电脑一台、苹果牌手机一部;徐明的 iphone 手机一部;吴杰的 iphone 手机一部、三星牌笔记本电脑一台应依法予以没收,上缴国库。被告人李文环退缴的违法所得 8800 元、吴杰退缴的违法所得以及吴杰代被告人王硕、卢晓燕、栾东超、徐明退缴的违法所得共 43800 元,依法应当予以追缴,上缴国库。

如不服本判决,可在接到判决书的第二日起十日内通过本院或者直接向凉山彝族自治州中级人民法院提出上诉,书面上诉的应交上诉状正本一份,副本三份。

审判长 蒋丽萍

审判员 卢泰铭

人民陪审员 崔光涛

二〇一九年六月二十一日

法官助理吴盛书

记员何未

（二）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

案例一、孟陈林、刘铸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

审理法院： 浙江省温州市中级人民法院

案 号： （2019）浙 03 刑终 1117 号

案 由： 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

裁判日期： 2019 年 11 月 15 日

浙江省温州市中级人民法院

刑事裁定书

（2019）浙03刑终1117号

抗诉机关浙江省温州市瓯海区人民检察院。

抗诉机关浙江省温州市瓯海区人民检察院。

上诉人（原审被告人）孟陈林，男，1996年11月5日出生于贵州省毕节市，汉族，大专文化，在校学生，户籍地毕节市七星关区。因本案于2018年5月23日被刑事拘留，同年6月15日被取保候审，2019年4月15日被逮捕。现羁押于温州市瓯海区看守所。

辩护人孟天明，贵州威迪律师事务所律师。

上诉人（原审被告人）刘铸，男，1998年5月20日出生于贵州省毕节市，汉族，高中文化，无业，户籍地毕节市七星关区。因本案于2018年5月23日被刑事拘留，同年6月15日被取保候审，2019年4月15日被逮捕。现羁押于温州市瓯海区看守所。

辩护人吴祖兴，湖南远达律师事务所律师。

辩护人杨振中，湖南择流律师事务所律师。

浙江省温州市瓯海区人民法院审理温州市瓯海区人民检察院指控原审被告人孟陈林、刘铸犯非法获取计算机信息系统数据罪一案，于2019年6月4日作出（2019）浙0304刑初229号刑事判决。原公诉机关浙江省温州市瓯海区人民检察院提出抗诉。原审被告人孟陈林、刘铸均不服，分别提出上诉。本院依法组成合议庭，于2019年9月25日公开开庭审理了本案，温州市人民检察院指派检察员吴晓节出庭履行职务，孟陈林、刘铸及其辩护人孟天明、吴祖兴、杨振中到庭参加诉讼。本案经浙江省高级人民法院批准，延长审限二个月。现已审理终结。

原判认定，被告人刘铸、孟陈林创建“BTCETH担保交易群”微信群，以对以太坊虚拟币（以下简称以太币）提供交易担保的名义发展成员。2017年12月30日，被害人朱某在该微信群里发布出售以太币的信息，刘铸、孟陈林经合谋后由刘铸通过微信联系朱某并谎称以每个以太币5000多元的价格收购朱某50个以太币。当日15时许，朱某将50个以太币转到刘铸指定的以太坊钱包后，刘铸、孟陈林即将朱某的微信“拉黑”并“踢出”微信群。同日，刘铸、孟陈林以同样手段获取被害人倪某（网友“夜”）10个以太币。此后，孟陈林将获取的60个以太币等虚拟货币出售套现30余万元并与刘铸予以瓜分。

原审法院根据上述事实及相关法律规定，以非法获取计算机信息系统数据罪判处被告人孟陈林、刘铸各有期徒刑三年十个月，并处罚金4万元；责令被告人孟陈林、刘铸退赔违法所得分别返还被害人朱某、倪某。

抗诉机关温州市瓯海区人民检察院抗诉称：（1）涉案以太币具有财产属性，属于侵财犯罪侵害对象，本案应定诈骗罪。理由如下：首先，虚拟财产已纳入我国民法总则调整和保护范围，而2017年七部委公告仅否定代币、虚拟币的法定货币属性，并禁止代币、虚拟币

发行融资活动，但并未否定私人间持有、流转虚拟币的合法性，更未否定虚拟币的财产属性，且七部委公告前后，多地法院将虚拟币作为侵财犯罪对象予以认定，故涉案以太币属于我国刑法第92条第四项规定的依法归个人所有的其他财产。其次，根据被害人、证人、被告人的言词证据及相关书证，本案能证实涉案以太币收购、销赃交易单价均为5000余元（符合交易行情），故可以明确涉案60个以太币价值30万元以上。再次，被告人通过其他技术手段获取他人计算机信息系统数据（以太币）的行为是犯罪手段，其犯罪目的是骗取他人财物。依据我国刑法犯罪目的和手段牵连，择一重罪处罚的基本原则，结合犯罪情节，相较诈骗罪与非法获取计算机信息系统罪量刑幅度，本案应以处罚较重的诈骗罪认定。（2）本案两被告人的行为应定性为诈骗罪，涉案60个以太币价值在30万元以上，诈骗公私财物价值10万元至50万元的，属于数额巨大，因此判处被告人有期徒刑四年至六年的量刑建议并无不当，原判以非法获取计算机信息系统数据罪仅判处两被告人有期徒刑三年十个月，量刑畸轻。综上，原审判决适用法律不当，定性错误，量刑畸轻。

温州市人民检察院支持抗诉意见，出庭检察员认为：（1）一审判决适用法律不当，定性错误。首先，被告人孟陈林、刘铸通过微信聊天使被害人朱某、倪某陷入错误认识，让被害人主动将以太币转入二人指定的以太坊钱包，从而获取二被害人购买的60个以太币，随后予以出售，获利30余万元人民币。孟陈林、刘铸其主观目的是非法占有被害人的以太币，非法获取计算机信息系统数据只是二被告人为了实现非法目的而采取的犯罪手段，本质上属于以非法占有为目的骗取他人财物的诈骗行为。其次，虽然2017年9月中国人民银行等七部委联合发布公告，禁止中间交易平台从事“比特币”等虚拟货币的平台兑换、买卖业务，但并未否认虚拟货币的经济价值，像数字货币这样仅被禁止作为货币流通的有“虚拟商品属性”的财产，应当作为犯罪对象。再次，被害人朱某等人付出人民币对价后得到以太币，不仅是一种特定的虚拟商品，也代表着被害人在现实生活中实际享有的财产，其损失的财产应受刑法保护。孟陈林、刘铸取得被害人的以太币后出售获利，获取人民币对价，与被害人的财产损失存在因果关系。不能因为数字货币具有计算机信息系统数据的性质，就将诈骗数字货币的行为认定为非法获取计算机信息系统数据罪。最后，根据被告人、被害人、证人的言辞证据及相关书证，能证实本案涉案以太币收购、销赃案发时交易单价为5000余元人民币，故可以明确涉案60个以太币共价值30余万元人民币。（2）本案两被告人的行为应定性为诈骗罪。原审判决适用法律不当、定性错误、量刑畸轻，建议二审法院依法改判。

原审被告人孟陈林上诉及辩护人提出：（1）朱某、倪某主动出售以太币，孟陈林、刘铸与对方达成交易约定，朱某、倪某未收到约定的钱款是民事交易违约或民事欺诈，属于民事案件，而非刑事案件。（2）涉案的以太币不属于我国现行法律规定的公私财物的范畴，不属于法律保护的财产利益，孟陈林不构成诈骗罪。（3）以太币存在于类似微信钱包等电子钱包中，而非存储在计算机中的数据；60个以太币系被害人主动、自愿提供给被告人的，

“拉黑”、“踢出”微信群的方式并不属于采用其他技术手段非法获取他人计算机系统中存储的数据，被告人不构成非法获取计算机信息系统数据罪。（4）虽有60个以太币转至境外平台销售，但在该平台兑换的数量仅为52个以太币，原判认定孟陈林获利30余万元主要来源于涉案60个以太币系事实不清。（5）孟陈林家属愿意代为退出一半违法所得。综上，请求改判孟陈林无罪或宣告缓刑。

原审被告人刘铸上诉及辩护人提出：（1）涉案的以太币交易活动不合法，不受法律保护。（2）以太币不属于刑法意义上的公私财物，刘铸不构成诈骗罪。（3）刘铸、孟陈林先前就有投资虚拟币，此次销售的虚拟币包括先前投资的虚拟币，原判未明确60个以太币的价值；因以太币的价格非常不稳定，故无法认定刘铸、孟陈林二人的具体违法所得数额。（4）本案所有网页、电子邮件、电子交易记录、图片等电子证据取证程序不合法。（5）原判对刘铸、孟陈林如何取得被害人的以太币没有调查清楚；原判将微信聊天行为认定为刑法第285条中的“采用其他技术手段”，明显突破罪刑法定原则而对被告人进行定罪量刑。综上，请求二审法院改判刘铸无罪。

经二审审理查明，孟陈林将获取的60个以太币出售套现人民币386266.2元的事实清楚。除了上述事实以外，原判认定的其他事实，有被害人朱某、倪某的陈述，被告人孟陈林、刘铸的供述，微信聊天记录、手机取证分析报告、情况说明，以太币交易平台流转记录及情况说明、Gate.io平台客服技术部回复邮件、虚拟货币平台交易记录、银行交易记录，证人柳某、叶某的证言，扣押决定书、扣押清单，抓获经过及情况说明，身份情况等证据予以证实，本院予以确认。本案事实清楚，证据确实、充分。

二审审理期间，孟陈林家属提供了陈光芬的银行账户明细等证据材料。经审查，上述材料所反映内容，和本案事实之间没有关联性，上述材料不属于对孟陈林定罪量刑有影响的新证据。

关于上诉理由、辩护意见及抗诉理由。本院综合评析如下：

1、关于本案所有网页、电子邮件、电子交易记录、图片等电子证据取证程序是否合法的问题。

本案中，侦查机关采取拍照方式固定电子数据等证据，且能够清晰反映相关内容，被告人孟陈林、刘铸等相关人员对此亦予认可并签名、按指印确认，此举符合收集提取电子数据的有关规定，故关于本案相关电子证据取证程序不合法的上诉意见于法无据，不予采纳。

2、关于以太币是否属于刑法保护对象的问题。

本院认为，以太币作为一种特定的虚拟商品，与金钱财物等有形财产、电力燃气等无形财产存在明显差别，将其解释为刑法意义上的“公私财物”，超出了司法解释的权限，将诈骗以太币认定为诈骗罪有违罪刑法定原则。

七部委公告仅否定以太币等“虚拟货币”的货币属性并禁止代币发行融资活动，并未否定私人持有以太币的合法性，也未禁止其成为私人间交付或流转的客体；我国民法总则第127条有关“法律对数据、网络虚拟财产的保护有规定的，依照其规定”等内容标志数据、网络虚拟财产正式进入民法调整和保护的范围，以太币是依据特定的算法通过大量的计算产生，实质上是动态的数据组合，其法律属性是计算机信息系统数据，依法属于刑法“非法获取计算机信息系统数据罪”所保护的对象。故关于以太币并非存储在计算机中的数据的上诉、辩护意见及以太币属于侵财犯罪侵害对象的抗诉意见，均不予支持。

3、关于被告人孟陈林、刘铸获取被害人以太币的手段是否属于刑法第285条规定的“采用其他技术手段”的问题。

经查，我国刑法规定的非法获取计算机信息系统数据罪是指非法获取他人计算机信息系统中存储、处理或者传输的数据的行为，“获取”包括从他人计算机信息系统中窃取，如直接侵入他人计算机信息系统中，秘密窃取他人存储的数据，也包括从他人计算机信息系统中骗取，如采用建立假冒网站、发送钓鱼链接等其他技术手段，在受骗者登录时，要求用户输入数据信息等；其中的“其他技术手段”是指“侵入”之外的其他犯罪手段，具有兜底性，囊括其他与前述情况相仿可采用的技术手段。在本案中，被告人通过微信发出其收购以太币的虚假信息而取得被害人的信任，被害人因此将以太币转入其指定的以太坊钱包，但被告人随即通过将被害人微信拉黑并踢出微信群等手段，导致被害人无法即时对其进行追踪，该手段行为利用了微信作为即时通讯应用程序所具有的远程性、非接触性等技术特点，来实现其既能非法获取以太币又能“隐身”的目的，此效果类似于以上所述的“从他人计算机信息系统中骗取”，属于非法获取计算机信息系统数据罪的“其他技术手段”范畴。故上诉人、辩护人关于被告人的犯罪手段不属于“采用其他技术手段”的上诉、辩护意见，不予采纳。

4、关于本案违法所得金额认定的问题。

被害人朱某、倪某的陈述和被告人孟陈林、刘铸的供述及微信聊天记录、手机取证分析报告、情况说明等证据相互印证，证实朱某、倪某二人共将60个以太币转到刘铸指定的以太坊钱包。孟陈林、刘铸的供述及以太币交易平台流转记录及情况说明、Gate.io平台客服技术部回复邮件、虚拟货币平台交易记录相互印证，证实孟陈林、刘铸已实际获取涉案60个以太币，并将此60个以太币转至境外平台出售套现38余万元。孟陈林、刘铸的供述及银行交易记录相互印证，证实孟陈林、刘铸将60个以太币套现后，对获利款386266.2元予以了瓜分。在案证据无法证明孟陈林、刘铸在销售60个以太币时，其账户内还有其他虚拟货币，且孟陈林、刘铸及辩护人均未能提供孟陈林在将二被害人60个以太币出售时，孟陈林账户内有无其他币以及其他虚拟币数量的相关证据。故关于销赃金额38万余元不是60个以太币的对价的相关上诉、辩护意见，均不予采纳。

本院认为，上诉人孟陈林、刘铸结伙采用其他技术手段，非法获取他人计算机系统中存储的数据，情节特别严重，其行为均已构成非法获取计算机信息系统数据罪。上诉人及辩护人要求改判二被告人无罪的意见，于法不符，不予采纳。抗诉机关提出孟陈林、刘铸构成诈骗罪的意见，不予支持。原判鉴于孟陈林、刘铸在侦查阶段如实供述孟陈林的罪行后翻供，但当庭能够如实供述本案主要犯罪事实，已予从轻处罚。原判定罪准确，量刑适当，审判程序合法。依法追缴被告人孟陈林、刘铸的全部违法所得386266.2元，其中应退赔被害人朱某265500元，退赔被害人倪某53300元，其余款项67466.2元应予以追缴，上缴国库。据此，依照《中华人民共和国刑法》第二百八十五条第二款、第二十五条第一款、第六十七条第三款、第六十四条和《中华人民共和国刑事诉讼法》第二百三十六条第一款第（一）项之规定，裁定如下：

驳回抗诉及上诉，维持原判。

本裁定为终审裁定。

审 判 长　韦 娜

审 判 员　孙彭聃

审 判 员　林方芳

二〇一九年十一月十五日

法官助理刘晓艳

代书记员　龙 梦

案例二、张丰、王泽文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

审理法院：　宜兴市人民法院

案　　号：　（2018）苏0282刑初1332号

案　　由：　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

裁判日期：　2019年03月25日

宜兴市人民法院

刑事判决书

（2018）苏0282刑初1332号

公诉机关宜兴市人民检察院。

公诉机关宜兴市人民检察院。

被告人张丰，男，1986年12月27日出生于河南省**门峡市湖滨区，汉族，大专文化，个体经营，住河南省**门峡市湖滨区。因本案于2018年6月29日被抓获，6月30日被刑事拘留，8月1日被宜兴市公安局决定取保候审，同年9月20日被宜兴市人民检察院决定

取保候审，2019 年 3 月 21 日被本院决定逮捕，同年 3 月 25 日由宜兴市公安局执行逮捕。现羁押于宜兴市看守所。

辩护人吴文艳，江苏鼎一律师事务所律师。

被告人王泽文，男，1996 年 5 月 30 出生于黑龙江省齐齐哈尔市，，汉族，初中文化，无，住内蒙古自治区呼伦贝尔市牙克石市名生**区区，户籍地黑龙江省齐齐哈尔市龙江县。因本案于 2018 年 6 月 29 日被刑事拘留，8 月 1 日被宜兴市公安局决定取保候审，同年 9 月 20 日被宜兴市人民检察院决定取保候审，2019 年 3 月 21 日被本院决定逮捕，同年 3 月 25 日由宜兴市公安局执行逮捕。现羁押于宜兴市看守所。

辩护人邵君，江苏太滆律师事务所律师。

宜兴市人民检察院以宜检诉刑诉（2018）1377 号起诉书指控被告人张丰、王泽文犯提供非法控制计算机信息系统的程序、工具罪，于 2018 年 11 月 12 日以简易程序向本院提起公诉，本院于同日受理后，认为本案不宜适用简易程序审理，于同年 12 月 27 日变更为普通程序审理，依法组成合议庭，于 2019 年 3 月 1 日公开开庭审理了本案。宜兴市人民检察院指派检察员蒋奇飚出庭支持公诉，被告人张丰及其辩护人吴文艳、被告人王泽文及其辩护人邵君到庭参加诉讼。现已审理终结。

经审理查明：2018 年 4 月至 6 月期间，被告人张丰单独或伙同王泽文，利用张丰自行编写的外挂软件，对腾讯游戏《绝地求生:刺激战场》进行控制，从而改变游戏中人物、场景的数值，达到作弊的效果。后被告人张丰单独或伙同王泽文通过 QQ、易卡、左发卡平台、微信、支付宝等销售渠道向他人销售该外挂软件，其中被告人张丰销售得款人民币 37324.26 元、被告人王泽文销售得款人民币 24732.66 元。具体事实如下：

1、2018 年 4 月，被告人张丰未经腾讯公司授权自行编写可对腾讯游戏《绝地求生:刺激战场》进行控制、影响的外挂软件，通过修改游戏的参数，从而对该游戏客户端的上色、加速、自动瞄准、除草、人物放大、天线等功能，绕过了游戏的保护措施，继而破坏游戏的平衡性，对该游戏的正常操作流程和运行方式造成了干扰和控制。

2018 年 4 月至 6 月期间，被告人张丰通过 QQ、易卡，左发卡平台、微信、支付宝等销售渠道向他人销售腾讯游戏《绝地求生：刺激战场》的外挂软件，共计得款人民币 12591.6 元。

2、2018 年 4 月，被告人王泽文通过 QQ 得知被告人张丰销售的腾讯游戏《绝地求生：刺激战场》外挂软件有利可图，遂与张丰协商，由被告人王泽文作为该款外挂软件的销售代理，获利后按 3:7 分成（王泽文得 3,张丰得 7)，被告人张丰表示同意。同年 5 月至 6 月期间，被告人王泽文通过 QQ、微信、支付宝、易卡平台等销售渠道向他人销售该外挂软件，共计得款人民币 24732.66 元。

2018 年 6 月 29 日，被告人张丰、王泽文被公安机关抓获，归案后如实供述了上述事实。

案发后，被告人张丰退出现金人民币35000元、被告人王泽文退出现金人民币6000元，现暂扣于公安机关。

上述事实，被告人张丰、王泽文在庭审中均未提出异议，并有证人冷某、郑某、江某、赵某、冯某的证言笔录，公安机关对相关人员手机内提取电子数据时制作的提取笔录、微信聊天记录、转账记录截图，两被告人通过左发卡、易卡、微信、QQ、支付宝向他人销售外挂软件的收入清单，被告人王泽文通过微信向被告人张丰外挂软件的交易情况及其利用冷某支付宝收取易卡平台提现款项记录，宜兴市公安局网络安全保卫大队出具的网络在线提取工作记录、电子证据检查工作记录，北京网络行业协会电子数据司法鉴定中心出具的司法鉴定意见书，腾讯科技（深圳）有限公司授权书，侦查人员出具的刑事案件侦破经过、抓获经过说明材料等证据证实，并有被告人张丰、王泽文的供述及相关户籍摘录予以佐证，足以认定。

被告人张丰的辩护人提出：1、被告人张丰系初犯，且无前科劣迹，归案后能如实供述自己的犯罪事实，认罪态度较好，可以从轻处罚。2、案发后，被告人张丰能够积极退赃，亦可对其酌情从轻处罚。综上，建议法庭对其适用缓刑。

被告人王泽文的辩护人提出：1、被告人王泽文无前科、此次犯罪属于初犯，归案后能如实供述自己的犯罪事实，可以从轻处罚。2、案发后，被告人王泽文能够积极退赃，亦可对其酌情从轻处罚。综上，建议法庭对其适用缓刑。

本院认为，被告人张丰单独或伙同王泽文向他人提供专门用于非法控制计算机信息系统的程序、工具，其中被告人张丰属于情节特别严重，被告人王泽文情节严重，其行为均已构成提供非法控制计算机信息系统的程序、工具罪，均应予惩处。且系共同犯罪。归案后，被告人张丰、王泽文均能如实供述自己的犯罪事实，且在庭审中能够自愿认罪，均可予以从轻处罚。案发后，两被告人均予以了退赃，有一定的悔罪表现，予以从轻处罚。公诉机关指控的罪名成立，应予采纳。关于两辩护人提出建议对两被告人适用缓刑的辩护意见，因本案属于利用网络犯罪，涉及面广，社会危害性大，故对两被告人不适宜宣告缓刑，对两被告人的辩护人提出的该辩护意见，不予采纳。对两辩护人提出的与上述相同的辩护意见，予以采纳。据此，依照《中华人民共和国刑法》第二百八十五条第三款、第二款，第二十五条第一款，第六十七条第三款，第六十四条之规定，判决如下：

一、被告人张丰犯提供非法控制计算机信息系统的程序、工具罪，判处有期徒刑三年三个月（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2019年3月25日起至2022年5月21日止），并处罚金人民币二万元（罚金于本判决发生法律效力第二日起三十日内缴纳）。

二、被告人王泽文犯提供非法控制计算机信息系统的程序、工具罪，判处有期徒刑二年三个月（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，

即自 2019 年 3 月 25 日起至 2021 年 5 月 21 日止），并处罚金人民币一万元（罚金于本判决发生法律效力第二日起三十日内缴纳）。

三、扣押在案的违法所得，予以没收，上缴国库。

如不服本判决，可在接到本判决书的第二日起十日内，通过本院或者直接向江苏省无锡市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本两份。

审 判 长　王兴鹤

审 判 员　王爱芳

人民陪审员　　郑一平

二〇一九年三月二十五日

法官 助理　徐 英

书 记 员　钟依依

（三）提供侵入、非法控制计算机信息系统程序、工具罪

案例一、赵某某 1、朱某某 1 提供侵入、非法控制计算机信息系统程序、工具案

审理法院：　湖南省张家界市中级人民法院

案　号：　（2020）湘 08 刑终 30 号

案　由：　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

裁判日期：　2020 年 03 月 05 日

湖南省张家界市中级人民法院刑事裁定书

（2020）湘 08 刑终 30 号

原公诉机关湖南省张家界市永定区人民检察院。

上诉人（原审被告人）赵某某 1，曾用名“赵纯元”，女，1969 年 11 月 21 日出生，汉族， 初中文化，户籍所在地湖南省益阳市南县，住上海市宝山区。因涉嫌非法控制计算机信息系统犯罪，2019 年 3 月 6 日被张家界市公安局永定分局刑事拘留，同年 3 月 8 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。辩护人陶宽、何承宸，北京市京师律师事务所律师。

原审被告人朱某某 1，男，1979 年 8 月 1 日出生，汉族，大学文化，深圳市辉创软件技术有限公司法定代表人，户籍所在地广东省深圳市南山区，住广东省深圳市南山区。因涉嫌提供非法控制计算机信息系统程序、工具犯罪，2019 年 3 月 15 日被珠海横琴出入境边防检查站抓获，同年 3 月 21 日被张家界市公安局永定分局逮捕，同年 7 月 25 日被张家界市公安局永定分局取保候审，同年 8 月 23 日被张家界市永定区人民检察院决定取保

候审。2019 年 11 月 28 日，被张家界市永定区人民法院决定逮捕，同日由张家界市公安局永定分局执行逮捕。2019 年 12 月 27 日被张家界市永定区人民法院决定取保候审。

原审被告人叶某某 1，男，1985 年 6 月 4 日出生，汉族，大专文化，深圳市天微云控科技有限公司法定代表人，户籍所在地湖南省岳阳市湘阴县，住广东省东莞市。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 26 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕。2019 年 5 月 24 日，被张家界市永定区人民检察院决定取保候审。2019 年 11 月 28 日，被张家界市永定区人民法院决定逮捕，同日由张家界市公安局永定分局执行逮捕。2019 年 12 月 4 日，被张家界市永定区人民法院决定取保候审。

原审被告人杨某 1，男，1981 年 2 月 14 日出生，汉族，小学文化，微云时代传媒科技（深圳）有限公司法定代表人，户籍所在地湖南省郴州市嘉禾县，住广东省深圳市罗湖区。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕，同年 4 月 3 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

原审被告人叶某 1，男，1991 年 3 月 25 日出生，汉族，初中文化，长沙市墨尘网络科技有限公司法定代表人，户籍所在地湖南省岳阳市湘阴县，住湖南省湘阴县。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕，同年 3 月 9 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

原审被告人戴某某 1，绰号“小戴”，男，1989 年 6 月 24 日出生，汉族，高中文化，公司职员，户籍所在地湖南省常德市桃源县，住湖南省常德市桃源县。因涉嫌提供非法控制计算机信息系统程序、工具犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕，同年 4 月 1 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

原审被告人黎某 1，男，1989 年 1 月 16 日出生，汉族，初中文化，长沙市微远网络科技有限公司法定代表人，户籍所在地湖南省岳阳市湘阴县，住长沙市天心区。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕，2019 年 3 月 5 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

原审被告人王某某 1，男，1993 年 12 月 28 日出生，汉族，大专文化，户籍所在地湖南省益阳市赫山区，住岳阳市经济开发区。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 2 月 20 日被张家界市公安局永定分局决定取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

原审被告人曾某某 1，男，1989 年 1 月 3 日出生，汉族，初中文化，经商，户籍所在地湖南省益阳市南县，住广东省东莞市。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 23 日被张家界市公安局永定分局刑事拘留，同年 2 月 20 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

原审被告人于某 1，男，1974 年 7 月 6 日出生，汉族，大学文化，微云时代传媒科技（深圳）有限公司股东，户籍所在地广东省广州市天河区，住广东省深圳市罗湖区。因涉嫌非法控制计算机信息系统犯罪，2019 年 4 月 3 日被张家界市公安局永定分局刑事拘留，同年 4 月 10 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

原审被告人周某 1，绰号“强别”，男，1988 年 10 月 15 日出生，汉族，高中文化，长沙市微远网络科技有限公司监事，户籍所在地湖南省岳阳市湘阴县，住湖南省长沙市开福区。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕。2019 年 6 月 4 日被张家界市公安局永定分局决定取保候审。

原审被告人黄某某 1，男，1991 年 3 月 27 日出生，回族，高中文化，公司职员，户籍所在地湖南省常德市武陵区，现住广东省深圳市南山区。2018 年 9 月 30 日，因赌博被常德市鼎城区公安局决定行政拘留十日，并处罚款一千元。因涉嫌提供非法控制计算机信息系统程序、工具犯罪，2019 年 6 月 4 日被张家界市公安局永定分局刑事拘留，同日被张家界市公安局永定分局取保候审，同年 7 月 2 日被张家界市永定区人民检察院决定取保候审。

原审被告人苏某某 1，男，1992 年 8 月 12 日出生，汉族，大学文化，公司职员，户籍所在地广东省深圳市罗湖区，住广东省深圳市罗湖区。因涉嫌提供非法控制计算机信息系统程序、工具犯罪，2019 年 2 月 19 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

原审被告人肖某某 1，曾用名“肖红叶”，女，1987 年 6 月 13 日出生，汉族，初中文化， 户籍所在地广东省深圳市福田区，住广东省东莞市。因涉嫌非法控制计算机信息系统罪，2019 年 1 月 23 日被张家界市公安局永定分局刑事拘留，同年 2 月 2 日被张家界市公安局永定分局取保候审，同年 3 月 28 日被张家界市永定区人民检察院决定取保候审。

原审被告人温某某 1，曾用名“温昕烨”，男，1993 年 3 月 15 日出生，汉族，初中文化， 公司职员，户籍所在地广东省揭西县，住广东省揭西县。因涉嫌非法控制计算机信息系统犯罪， 2019 年 3 月 11 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

湖南省张家界市永定区人民法院审理湖南省张家界市永定区人民检察院指控原审被告人朱某某 1、戴某某 1、苏某某 1、黄某某 1 犯提供非法控制计算机信息系统程序、工具罪，被告人叶某某 1、肖某某 1、温某某 1、杨某 1、于某 1、叶某 1、黎某 1、周某 1、曾某某 1、王某某 1、赵某某 1 犯非法控制计算机信息系统罪一案，于 2019 年 12 月 27 日作出[2019]湘 08**刑初 402 号刑事判决。原审被告人赵某某 1 不服，提起上诉。本院受理后，依法组成合议庭， 经过阅卷，讯问上诉人和原审被告人，听取辩护人的意见，认为事实清楚，决定不开庭审理， 现已审理终结。

原审判决认定：

一、提供非法控制计算机信息系统程序、工具罪

2016 年 3 月，被告人朱某某 1 安排被告人戴某某 1、苏某某 1 负责研发一款依托腾讯公司微信系统，实现微信不具有的自动化操作功能，达到批量控制微信的目的的软件。戴某某 1、苏某某 1 分别负责研发该软件手机端 App 和网页端，2016 年 6 月，包含手机端和网页端的移动营销助手云控系统研发成功，该软件被命名为“移动营销助手”，由被告人黄某某 1 负责软件销售和售后服务工作。“云控移动营销平台”通过对安装有“移动营销助手”以及 Xposed 框架模块“wx_release.apk”插件的智能手机来获取微信数据，实现微信不具有的自动化操作功能，从而达到批量控制微信的目的。“天微云控”、“AKA”、“微云时代”等 3 款手机 App 具有以下功能性：1、通过实验环境的搭建，实现了检材手机端与“云控移动营销平台”（包含天微云控、AKA、微云时代等 3 款手机 App）Web 服务端连接的建立。2、通过对安装了“天微云控”、“AKA”、“微云时代”App 的手机进行联网测试，发现在“云端移动营销平台”Web 端控制下，安装了“微云时代”、“天微云控”、“AKA”等 App 的手机能够实现接收 Web 服务端发送的任务指令，实现自动完成“朋友圈”、“好友消息”、“添加好友”、“编辑统计”、“群功能”等 5 个模块中的“朋友圈点赞”、“朋友圈评论”、“好友群发消息”、“修改头像”、“扔捡漂流瓶”、“修改个性签名”等功能。软件使用者在招徕到广告、点赞、小说推广等业务后，可以批量向自己控制的微信朋友圈内批量转发广告、小说点赞等，事后按微信朋友圈内好友的点击量、充值款向需求者收取费用牟利。被告人朱某某 1 获利 535 万元，被告人戴某某 1 获利 60 余万元，被告人苏某某 1 获利 2 万余元，被告人黄某某 1 获利 47 万元。

另查明，2019 年 3 月 15 日，被告人朱某某 1 自动到中华人民共和国横琴出入境边防检查站投案，并如实供述自己罪行。2019 年 2 月 19 日，被告人苏某某 1 自动到张家界市公安局永定分局投案，并如实供述自己的罪行。2019 年 6 月 4 日，被告人黄某某 1 自动到张家界市公安局永定分局投案，并如实供述自己的罪行。

再查明，案发后，被告人朱某某 1 已退赃人民币 535 万元，被告人戴某某 1 已退赃人民币 60 万元，被告人苏某某 1 已退赃人民币 2 万元，被告人黄某某 1 已退赃人民币 47 万元。

上述事实，被告人朱某某 1、戴某某 1、苏某某 1、黄某某 1 在法庭审理过程中均无异议， 且有证人舒某、赵某 1、叶某、罗某、莫某、杨某的证言，专家证人刘某 1 的证言，线索来源及抓获经过，深圳市辉创软件技术有限公司工商登记信息、营销报表情况、财务资料，程序代码资料，小说推广页面截图、上海铜爵网络科技有限公司营业执照，阿里云计算有限公司客户租用服务器情况，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，扣押决定书，扣押物品、文件清单，发还物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，辨认笔录，搜查笔录，封存、拆封提取笔录，电子数据，行政处罚决定书，视频资料，户籍资料等证据证明，足以认定。

二、非法控制计算机信息系统罪

（一）2016 年 6、7 月份，被告人叶某某 1 从朱某某 1 处知晓移动营销助手软件功能后， 获得该软件授权。2017 年 1 月，叶某某 1 成立了天微云控科技有限公司，将移动营销助手软件更名为“天微云控”。该公司通过销售天微云控软件及利用该软件控制 2000 余台手机微信， 通过微信朋友圈推广广告等方式牟利，并向他人或公司介绍小说推广业务，从中赚取差价。被告人肖某某 1 为客户提供软件和授权，进行售后服务及购买微信号等工作，并提供银行卡用于公司转账，核对公司账目。被告人温某某 1 负责微信养号及操作天微云控后台。叶某某 1 获利 500 万余元。

另查明，2019 年 3 月 11 日，被告人温某某 1 主动到张家界市公安局永定分局投案，并如实供述自己的罪行。

再查明，案发后，被告人叶某某 1 已退赃人民币 500 万元。

上述事实，被告人叶某某 1、肖某某 1、温某某 1 在法庭审理过程中均无异议，且有证人张某、叶某、罗某、琚某、涂某、莫某、杨某的证言，线索来源及抓获经过，深圳市天微云控科技有限公司工商登记信息资料，银行交易明细及流水，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，扣押决定书，扣押物品、文件清单，发还物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，搜查笔录及现场照片，电子数据，户籍资料等证据证明，足以认定。

（二）2016 年 5 月，被告人杨某 1 从朱某某 1 处获得移动营销助手软件代理权，成立了微云时代传媒科技（深圳）有限公司，将移动营销助手软件更名为“微云时代”。2017 年 3 月， 被告人于某 1 了解该软件盈利模式后入股该公司。该公司通过销售“微云时代”软件及使用该软件控制手机微信推广广告等方式牟利。杨某 1 获利 315 万余元，于某 1 获利 64 万余元。

另查明，案发后，被告人杨某 1 已退赃人民币 315 万元，被告人于某 1 已退赃人民币 64 万元。

上述事实，被告人杨某 1、于某 1 在法庭审理过程中均无异议，且有证人黄某、曾某 1、莫某、杨某的证言，线索来源及抓获经过，深圳市微云时代传媒科技（深圳）有限公司工商登记信息资料，银行交易明细、流水及对账单，授权书资料，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，扣押决定书，扣押物品、文件清单，发还物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，搜查笔录及现场照片，辨认笔录，提取笔录，电子数据， 户籍资料等证据证明，足以认定。

（三）2017 年 6 月，叶某某 1、叶某 1 与被告人黎某 1、周某 1 等人合伙成立长沙微远网络科技有限公司，黎某 1 负责公司整体运行，周某 1 负责财务，潘某（另案处理）负责员工管理和联系业务。黎某 1 陆续从天微云控公司购买安装了“天微云控”软件的手机 5000 台，利用控制的手机微信为需求者推广小说等方式牟利。黎某 1 获利 50 余万元，周某 1 获利 31 万余元。

另查明，被告人黎某 1 已退赃人民币 50 万元，被告人周某 1 已退赃人民币 9 万元。

上述事实，被告人黎某 1、周某 1 在法庭审理过程中均无异议，且有证人胡某 1、田某、胡某 2、潘某的证言，线索来源及抓获经过，长沙微远网络科技有限公司工商登记信息资料，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，银行交易流水及对账单，扣押决定书，扣押物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，搜查笔录，电子数据， 户籍资料等证据证明，足以认定。

（四）2018 年 1 月，被告人叶某 1 从叶某某 1 处购买“天微云控”软件，叶某某 1 以 3000 余台手机入股与其合伙经营，叶某 1 通过使用“天微云控”软件实现对微信的自动化群控，以此在微信朋友圈推广广告牟利。为便于招揽客户，2018 年 9 月，叶某 1 成立了长沙墨尘网络有限公司，叶某 1 负责公司的运营管理，肖某某 1 为公司财务，宋某 2（另案处理）负责微信养号、操作软件在微信朋友圈推广广告等工作。叶某 1 获利人民币 56 万元。

另查明，案发后，被告人叶某 1 已退赃人民币 56 万元。

上述事实，被告人叶某 1 在法庭审理过程中均无异议，且有证人宋某 1、吴某、彭某、宋某 2 的证言，线索来源及抓获经过，长沙墨尘网络科技有限公司工商登记信息资料、养号步骤、后台工作分配情况，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，银行交易流水及对账单，扣押决定书，扣押物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书， 搜查笔录，电子数据，户籍资料等证据证明，足以认定。

（五）2018 年 4 月，被告人曾某某 1、王某某 1 了解到“天微云控”软件盈利模式后，从叶某某 1 处购买了 1000 台手机和天微云控软件。为便于招徕业务，曾某某 1、王某某 1 等人合伙成立了微音科技有限公司，曾某某 1 负责联系业务，王某某 1 负责软件操作等工作，通过利用软件控制微信为广告商推广小说等方式牟利。曾某某 1 获利 30 余万元，王某某 1 获利 50 余万元。

另查明，被告人曾某某 1 已退赃人民币 30 万元，被告人王某某 1 已退赃人民币 50 万元。上述事实，被告人曾某某 1、王某某 1 在法庭审理过程中均无异议，且有证人曾某 2、刘某 2 的证言，线索来源及抓获经过，腾讯科技（深圳）有限公司报案书及法人授权委托证明书， 银行交易流水及对账单，扣押决定书，扣押物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，搜查笔录，电子数据，户籍资料等证据证明，足以认定。

（六）2018 年 5 月，被告人赵某某 1 了解到“天微云控”软件的盈利模式后，从叶某某 1 处购买了 1000 台手机及“天微云控”软件并出资成立了星微工作室，安排赵某 2（另案处理） 负责日常经营管理，该工作室通过该软件控制手机中的微信为广告商推广小说等方式牟利。

上述事实，被告人赵某某 1 在法庭审理过程中均无异议，且证人有张某、叶某、罗某、赵某 2 的证言，线索来源及抓获经过，腾讯科技（深圳）有限公司报案书及法人授权委托证明书， 扣押决定书，扣押物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，辨认笔录， 搜查笔录，电子数据，户籍资料等证据证明，足以认定。

原审法院认为，被告人朱某某 1、戴某某 1、苏某某 1、黄某某 1 违反国家规定，提供专门用于侵入、非法控制计算机信息系统的程序、工具，情节特别严重，四名被告人的行为均构成提供非法控制计算机信息系统程序、工具罪；被告人叶某某 1、肖某某 1、温某某 1、杨某 1、于某 1、叶某 1、黎某 1、周某 1、曾某某 1、王某某 1、赵某某 1 违反国家规定，对计算机信息系统实施非法控制，情节特别严重，十一名被告人的行为均构成非法控制计算机信息系统罪。

在提供非法控制计算机信息系统程序、工具罪共同犯罪中，被告人朱某某 1、戴某某 1 起主要作用，均系主犯，应当按照所参与的全部犯罪处罚，被告人苏某某 1、黄某某 1 起次要作用，系从犯，依法应当减轻处罚。在非法控制计算机信息系统罪共同犯罪中，被告人叶某某 1、杨某 1、于某 1、黎某 1、周某 1、叶某 1、曾某某 1、王某某 1、赵某某 1 均起主要作用，系主犯，应当按照所参与的全部犯罪处罚，被告人肖某某 1、温某某 1 起次要作用，系从犯，依法应当减轻处罚。被告人朱某某 1、苏某某 1、黄某某 1、温某某 1 犯罪后自动投案，如实供述自己的罪行，是自首，依法可以从轻处罚。被告人朱某某 1、苏某某 1、黄某某 1、温某某 1、叶某某 1、戴某某 1、肖某某 1、杨某 1、于某 1、叶某 1、黎某 1、周某 1、曾某某 1、王某某 1、赵某某 1 归案后，自愿如实供述自己的罪行，承

认指控的犯罪事实，愿意接受处罚，依法可以从宽处罚。被告人朱某某 1、苏某某 1、黄某某 1、叶某某 1、戴某某 1、杨某 1、于某 1、叶某 1、黎某 1、周某 1、曾某某 1、王某某 1 积极退赃，依法可酌定从轻处罚。

被告人朱某某 1、苏某某 1、黄某某 1、温某某 1、叶某某 1、戴某某 1、肖某某 1、杨某 1、于某 1、叶某 1、黎某 1、周某 1、曾某某 1、王某某 1、赵某某 1 犯罪后有悔罪表现，没有再犯罪的危险，宣告缓刑对所居住的社区没有重大不良影响，可对其宣告缓刑，依照《中华人民共和国刑法》第二百八十五条第二、三款，第二十五条第一款，第二十六条第一、四款，第二十七条，第六十七条第一、三款，第六十四条，第五十二条，第七十二条第二款、第七十三条第二、三款，《中华人民共和国刑事诉讼法》第十五条之规定，经审判委员会讨论决定，判决被告人朱某某 1 犯提供非法控制计算机信息系统程序、工具罪，判处有期徒刑三年，缓刑四年，并处罚金人民币五十万元。被告人叶某某 1 犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑四年，并处罚金人民币三十八万元。被告人杨某 1 犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币四十万元。被告人叶某 1 犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十九万元。被告人戴某某 1 犯提供非法控制计算机信息系统程序、工具罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十五万元。被告人黎某 1 犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十二万元。被告人王某某 1 犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十二万元。被告人曾某某 1 犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十二万元。被告人于某 1 犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十万元。被告人周某 1 犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十万元。被告人赵某某 1 犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币四万元。被告人黄某某 1 犯提供非法控制计算机信息系统程序、工具罪，判处有期徒刑二年六个月，缓刑三年，并处罚金人民币十万元。被告人苏某某 1 犯提供非法控制计算机信息系统程序、工具罪，判处有期徒刑二年六个月，缓刑三年，并处罚金人民币八万元。被告人肖某某 1 犯非法控制计算机信息系统罪，判处有期徒刑二年六个月，缓刑三年，并处罚金人民币十万元。被告人温某某 1 犯非法控制计算机信息系统罪，判处有期徒刑一年，缓刑一年，并处罚金人民币一万五千元。对扣押机关扣押的供本案犯罪所用的财物， 由扣押机关依法处置。对被告人朱某某 1 违法所得人民币 5350000 元、被告人叶某某 1 违法所得人民币 5000000 元、被告人杨某 1 违法所得人民币 3150000 元、被告人叶某 1 违法所得人民币 560000 元、被告人戴某某 1 违法所得人民币 600000 元、被告人黎某 1 违法所得人民币 500000 元、被告人王某某 1 违法所得人民币 500000 元、被告人曾某某 1

违法所得人民币 300000 元、被告人于某 1 违法所得人民币 640000 元、被告人周某 1 违法所得人民币 310000 元、被告人黄某某 1 违法所得人民币 470000 元、被告人苏某某 1 违法所得人民币 20000 元予以追缴。

赵某某 1 上诉称：本案没有被控制的对象，不存在非法控制的问题；上诉人没有违法所得，认定上诉人构成犯罪没有事实依据；本案四份《鉴定意见书》，存在检材来源不合法、超出鉴定范围、鉴定主体不合法等原因，不能依法作为本案定案依据，不能证明涉案软件具有非法控制计算机信息系统的功能；原审错误地适用法律，将涉案软件认定为“专门用于侵入、非法控制计算机信息系统的程序、工具。”

其辩护人提出：赵某某 1 控制的是“手机”，绝非“微信系统”，一审判决认定事实错误、证据不足；涉案软件的功能是“模拟人工点击”，不改变、干扰或增加微信功能，并非“避开或突破微信系统安全保护措施”的控制软件；涉案软件系通过“批量控制手机”，达到“微信批量操作”的效果，并非对微信系统进行控制；涉案软件只能在“经过 ROOT 后取得最高权限”的“安卓”手机上使用，未 ROOT 或 IOS 手机则无法使用；涉案软件的源代码仅作用于手机系统，并未修改微信系统源代码；赵某某 1 控制自己所有的手机显然是合法控制，绝非“非法控制”；最高人民法院研究室认为，对此类案件应慎用刑事制裁手段；本案四份《鉴定意见书》不能证明涉案软件对微信系统进行了控制，一审判决证据不足；赵某某 1 的行为并未违反国家规定，且无任何违法所得，赵某某 1 虽购买涉案软件，但并未成功使用、运营，属于犯罪预备；赵某某 1 并无非法控制计算机信息系统的犯罪故意；犯罪情节比赵某某 1 严重的多个案例，检察机关作出不起诉的决定；新证据证实赵某某 1 并非星微工作室的实际控制人，甚至不是股权最大的合伙人，一审判决认定事实错误；赵某某 1 积极参与公益、捐献器官，对社会作出积极贡献，无社会危害性；赵某某 1 身患癌症，急需国外就医。故请求二审对赵某某 1 予以改判。经审理查明，原审判决认定事实清楚，证据确实、充分，本院予以确认。

本院认为，原审被告人朱某某 1、戴某某 1、苏某某 1、黄某某 1 违反国家规定，提供专门用于侵入、非法控制计算机信息系统的程序、工具，情节特别严重，其行为均构成提供非法控制计算机信息系统程序、工具罪；原审被告人叶某某 1、肖某某 1、温某某 1、杨某 1、于某 1、叶某 1、黎某 1、周某 1、曾某某 1、王某某 1、上诉人赵某某 1 违反国家规定，对计算机信息系统实施非法控制，情节特别严重，其行为均构成非法控制计算机信息系统罪。

在提供非法控制计算机信息系统程序、工具罪共同犯罪中，朱某某 1、戴某某 1 起主要作用，均系主犯，应当按照所参与的全部犯罪处罚，苏某某 1、黄某某 1 起次要作用，系从犯， 依法应当减轻处罚。在非法控制计算机信息系统罪第 1 起共同犯罪中，叶某某 1 起主要作用， 系主犯，应当按照所参与的全部犯罪处罚，肖某某 1、温某某 1 起次要作用，

系从犯，依法应当减轻处罚。在非法控制计算机信息系统罪第 2 起共同犯罪中，杨某 1、于某 1 起主要作用，均系主犯，应当按照所参与的全部犯罪处罚。在非法控制计算机信息系统罪第 3 起共同犯罪中，黎某 1、周某 1 起主要作用，均系主犯，应当按照所参与的全部犯罪处罚。在非法控制计算机信息系统罪第 4 起共同犯罪中，叶某 1 起主要作用，系主犯，应当按照所参与的全部犯罪处罚。在非法控制计算机信息系统罪第 5 起共同犯罪中，曾某某 1、王某某 1 起主要作用，均系主犯，应当按照所参与的全部犯罪处罚。在非法控制计算机信息系统罪第 6 起共同犯罪中，赵某某 1 起主要作用，系主犯，应当按照所参与的全部犯罪处罚。

原审被告人朱某某 1、苏某某 1、黄某某 1、温某某 1 犯罪后自动投案，如实供述自己的罪行，是自首，依法可以从轻处罚。原审被告人叶某某 1、戴某某 1、肖某某 1、杨某 1、于某 1、叶某 1、黎某 1、周某 1、曾某某 1、王某某 1、上诉人赵某某 1 归案后，自愿如实供述自己的罪行，承认指控的犯罪事实，愿意接受处罚，依法可以从宽处罚。朱某某 1、苏某某 1、黄某某 1、叶某某 1、戴某某 1、杨某 1、于某 1、叶某 1、黎某 1、周某 1、曾某某 1、王某某 1 积极退缴违法所得，依法可酌定从轻处罚。

原审被告人朱某某 1、苏某某 1、黄某某 1、温某某 1、叶某某 1、戴某某 1、肖某某 1、杨某 1、于某 1、叶某 1、黎某 1、周某 1、曾某某 1、王某某 1、上诉人赵某某 1 犯罪后有悔罪表现，没有再犯罪的危险，宣告缓刑对所居住的社区没有重大不良影响，可对其依法宣告缓刑。

对于上诉人及其辩护人提出本案四份《鉴定意见书》存在检材来源不合法、超出鉴定范围、鉴定主体不合法等问题，不能依法作为本案定案依据，不能证明涉案软件具有非法控制计算机信息系统的功能的意见。经查，该四份鉴定意见使用的检材系侦查机关依法提取并移送，鉴定机构具有法定资质，鉴定程序合法，鉴定事项未超出业务范围，可作为定案依据使用。对该意见不予采纳。

对于上诉人及其辩护人提出赵某某 1 的行为不构成非法控制计算机信息系统罪的意见。经查，1.微信程序属于计算机信息系统。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》的规定，解释中的“计算机信息系统”和“计算机系统”，是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。《中华人民共和国计算机系统安全保护条例》第二条规定，计算机信息系统是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。腾讯公司微信程序由服务程序（安装在服务器上）、客户端程序（安装在用户手机上）组成，需要智能手机、计算机服务器、网络通讯设备等硬件支撑，具备自动采集、处理、存储、回传、显示数据等功能，属于计算机信息系统；2.涉案软件属于非法控制微信程序的程序、工具。微

信作为腾讯公司向用户提供的跨平台的通讯工具，支持单人、多人参与，其定位于自然人操作使用。本案中涉案软件“移动营销助手”接受用户在“云控移动营销平台”下发的指令，通过查询微信的版本号调用该版本的微信脚本文件中的具体方法来调用微信“微信好友逐个发消息”等具体功能，实现微信自身不具有的自动化操作功能，从而达到批量控制微信的目的，侵犯了微信系统的功能运行和管理程序，属于非法控制。3.赵某某 1 的行为构成非法控制计算机信息系统罪。赵某某 1 的供述、证人赵某 2、罗某等人的证言及搜查笔录、扣押决定书等书证能够证明赵某某 1 从叶某某 1 处购买 1000 台手机及具有非法控制微信功能的“天微云控”软件并安排赵某 2 负责操控的事实。原审判决虽未认定赵某某 1 的违法所得，但赵某某 1 购入 1000 台手机安装涉案软件后安排他人使用，根据两高司法解释“非法控制计算信息系统数量 100 台以上应认定情节特别严重”的规定，其行为已构成非法控制计算机信息系统罪，且属情节特别严重情形。故对该意见不予采纳。

对于上诉人的辩护人提出新证据证实赵某某 1 并非星微工作室的实际控制人，甚至不是股权最大的合伙人，一审判决认定事实错误的意见。经查，在卷证据能够证明赵某某 1 的行为已构成犯罪，赵某某 1 是否是星微工作室的实际控制人及股权最大的合伙人均不影响对其犯罪事实和量刑情节的认定。对该意见不予采纳。

对于上诉人的辩护人提出赵某某 1 积极参与公益、捐献器官，对社会作出积极贡献，无社会危害性；赵某某 1 身患癌症，急需国外就医，请求二审改判的意见。本院认为，人民法院在对被告人定罪量刑时应该且只能考虑定罪事实和量刑情节，否则有违法治的基本原则。对该意见不予采纳。

综上，原审判决认定事实清楚，证据确实、充分，适用法律正确，量刑适当，审判程序合法。依照《中华人民共和国刑事诉讼法》第二百三十六条第一款第（一）项之规定，裁定如下：

驳回上诉，维持原判。

本裁定为终审裁定。

审 判 长 刘 华

审判员　涂明珠

审 判 员 张 晓

二〇二〇年三月五日

法官助理 巩守信

书记员　甄婕琳

案例二、朱晓辉、叶丹墨提供侵入、非法控制计算机信息系统程序、工具案

审理法院：　张家界市永定区人民法院

案　号：　（2019）湘 0802 刑初 402 号

案　由：　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

裁判日期：　2019 年 12 月 27 日

张家界市永定区人民法院刑事判决书

（2019）湘 0802 刑初 402 号

公诉机关湖南省张家界市永定区人民检察院。公诉机关湖南省张家界市永定区人民检察院。

被告人朱晓辉，男，1979 年 8 月 1 日出生，汉族，大学文化，深圳市辉创软件技术有限公司法定代表人，户籍所在地广东省深圳市南山区，住广东省深圳市南山区。因涉嫌提供非法控制计算机信息系统程序、工具犯罪，2019 年 3 月 15 日被珠海横琴出入境边防检查站抓获，同年 3 月 21 日被张家界市公安局永定分局逮捕，同年 7 月 25 日被张家界市公安局永定分局取保候审，同年 8 月 23 日被张家界市永定区人民检察院决定取保候审。2019 年 11 月 28 日，被本院决定逮捕，同日由张家界市公安局永定分局执行逮捕。2019 年 12 月 27 日被本院决定取保候审。

辩护人张建春，湖南澧滨律师事务所律师。

被告人叶丹墨，男，1985 年 6 月 4 日出生，汉族，大专文化，深圳市天微云控科技有限公司法定代表人，户籍所在地湖南省岳阳市湘阴县，住广东省东莞市。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 26 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕。2019 年 5 月 24 日，被张家界市永定区人民检察院决定取保候审。2019 年 11 月 28 日，被本院决定逮捕，同日由张家界市公安局永定分局执行逮捕。2019 年 12 月 4 日，被本院决定取保候审。

辩护人欧阳显南，湖南高新律师事务所律师。

被告人杨军，男，1981 年 2 月 14 日出生，汉族，小学文化，微云时代传媒科技（深圳） 有限公司法定代表人，户籍所在地湖南省郴州市嘉禾县，住广东省深圳市罗湖区。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕，同年 4 月 3 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

辩护人黄璜，北京德和衡（长沙）律师事务所律师。辩护人李滨，湖南风云律师事务所律师。

被告人叶佳，男，1991 年 3 月 25 日出生，汉族，初中文化，长沙市墨尘网络科技有限公司法定代表人，户籍所在地湖南省岳阳市湘阴县，住湖南省湘阴县。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 3 月

1 日被逮捕，同年 3 月 9 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

辩护人徐卓，湖南高新律师事务所律师。

被告人戴登科，绰号“小戴”，男，1989 年 6 月 24 日出生，汉族，高中文化，公司职员， 户籍所在地湖南省常德市桃源县，住湖南省常德市桃源县。因涉嫌提供非法控制计算机信息系统程序、工具犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕，同年 4 月 1 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

辩护人邹立洪，广东普多米修斯（龙华）律师事务所律师。

被告人黎威，男，1989 年 1 月 16 日出生，汉族，初中文化，长沙市微远网络科技有限公司法定代表人，户籍所在地湖南省岳阳市湘阴县，住长沙市天心区。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 3 月 1 日被逮捕，2019 年 3 月 5 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

指定辩护人屈煜，湖南天门律师事务所律师。

被告人王志文，男，1993 年 12 月 28 日出生，汉族，大专文化，户籍所在地湖南省益阳市赫山区，住岳阳市经济开发区。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘留，同年 2 月 20 日被张家界市公安局永定分局决定取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

指定辩护人罗忠娟，湖南人和人（张家界）律师事务所律师。

被告人曾山峰，男，1989 年 1 月 3 日出生，汉族，初中文化，经商，户籍所在地湖南省益阳市南县，住广东省东莞市。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 23 日被张家界市公安局永定分局刑事拘留，同年 2 月 20 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。指定辩护人陶胜军,湖南天门律师事务所律师。

被告人于强，男，1974 年 7 月 6 日出生，汉族，大学文化，微云时代传媒科技（深圳）有限公司股东，户籍所在地广东省广州市天河区，住广东省深圳市罗湖区。因涉嫌非法控制计算机信息系统犯罪，2019 年 4 月 3 日被张家界市公安局永定分局刑事拘留，同年 4 月 10 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。指定辩护人陆清江，湖南大好律师事务所律师。

被告人**，绰号“强别”，男，1988 年 10 月 15 日出生，汉族，高中文化，长沙市微远网络科技有限公司监事，户籍所在地湖南省岳阳市湘阴县，住湖南省长沙市开福区。因涉嫌非法控制计算机信息系统犯罪，2019 年 1 月 22 日被张家界市公安局永定分局刑事拘

留，同年 3 月 1 日被逮捕。2019 年 6 月 4 日被张家界市公安局永定分局决定取保候审。指定辩护人龚媚丹，湖南人和人（张家界）律师事务所律师。

被告人赵元纯，曾用名“赵纯元”，女，1969 年 11 月 21 日出生，汉族，初中文化，户籍所在地湖南省益阳市南县，住上海市宝山区。因涉嫌非法控制计算机信息系统犯罪，2019 年 3 月 6 日被张家界市公安局永定分局刑事拘留，同年 3 月 8 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

辩护人安吉彪，湖南金旅事务所律师。

被告人黄侣霆，男，1991 年 3 月 27 日出生，回族，高中文化，公司职员，户籍所在地湖南省常德市武陵区，现住广东省深圳市南山区。2018 年 9 月 30 日，因赌博被常德市鼎城区公安局决定行政拘留十日，并处罚款一千元。因涉嫌提供非法控制计算机信息系统程序、工具犯罪，2019 年 6 月 4 日被张家界市公安局永定分局拘留，同日被张家界市公安局永定分局取保候审，同年 7 月 2 日被张家界市永定区人民检察院决定取保候审。

指定辩护人秦昌猛，湖南天门律师事务所律师。

被告人苏少涛，男，1992 年 8 月 12 日出生，汉族，大学文化，公司职员，户籍所在地广东省深圳市罗湖区，住广东省深圳市罗湖区。因涉嫌提供非法控制计算机信息系统程序、工具犯罪，2019 年 2 月 19 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

指定辩护人王祥政，湖南古庸律师事务所律师。

被告人肖桂珍，曾用名“肖红叶”，女，1987 年 6 月 13 日出生，汉族，初中文化，户籍所在地广东省深圳市福田区，住广东省东莞市。因涉嫌非法控制计算机信息系统罪，2019 年 1 月 23 日被张家界市公安局永定分局刑事拘留，同年 2 月 2 日被张家界市公安局永定分局取保候审，同年 3 月 28 日被张家界市永定区人民检察院决定取保候审。辩护人舒媛，湖南高新律师事务所律师。

辩护人王添，湖南高新律师事务所律师。

被告人温智烨，曾用名“温昕烨”，男，1993 年 3 月 15 日出生，汉族，初中文化，公司职员，户籍所在地广东省揭西县，住广东省揭西县。因涉嫌非法控制计算机信息系统犯罪，2019 年 3 月 11 日被张家界市公安局永定分局取保候审，同年 4 月 28 日被张家界市永定区人民检察院决定取保候审。

指定辩护人刘文娟，湖南人和人（张家界）律师事务所律师。

张家界市永定区人民检察院以张定检公诉刑诉〔2019〕377 号起诉书指控被告人朱晓辉、戴登科、苏少涛、黄侣霆涉嫌犯提供非法控制计算机信息系统程序、工具罪，被告人叶丹墨、肖桂珍、温智烨、杨军、于强、叶佳、黎威、**、曾山峰、王志文、赵元纯涉嫌犯非法控制计算机信息系统罪，于 2019 年 11 月 25 日向本院提起公诉。本院于同日受理后，依法组

成合议庭，于 2019 年 12 月 18 日公开开庭进行了审理。张家界市永定区人民检察院指派检察员谷淑云出庭支持公诉，被告人朱晓辉及其辩护人张建春，被告人叶丹墨及其辩护人欧阳显南，被告人杨军及其辩护人黄璜、李滨，被告人戴登科及其辩护人邹立洪，被告人苏少涛及其指定辩护人王祥政，被告人黄侣霆及其指定辩护人秦昌猛，被告人于强及其指定辩护人陆清江，被告人叶佳及其辩护人徐卓，被告人黎威及其指定辩护人屈煜，被告人**及其指定辩护人龚媚丹，被告人曾山峰及其指定辩护人陶胜军，被告人王志文及其指定辩护人罗忠娟，被告人赵元纯及其辩护人安吉彪，被告人肖桂珍及其辩护人舒媛、王添，被告人温智烨及其指定辩护人刘文娟均到庭参加诉讼。现已审理终结。经审理查明：

一、提供非法控制计算机信息系统程序、工具罪

2016 年 3 月，被告人朱晓辉安排被告人戴登科、苏少涛负责研发一款依托腾讯公司微信系统，实现微信不具有的自动化操作功能，达到批量控制微信的目的的软件。戴登科、苏少涛分别负责研发该软件手机端 App 和网页端，2016 年 6 月，包含手机端和网页端的移动营销助手云控系统研发成功，该软件被命名为“移动营销助手”，由被告人黄侣霆负责软件销售和售后服务工作。“云控移动营销平台”通过对安装有“移动营销助手”以及 Xposed 框架模块“wx_release.apk”插件的智能手机来获取微信数据，实现微信不具有的自动化操作功能，从而达到批量控制微信的目的。“天微云控”、“AKA”、“微云时代”等 3 款手机 App 具有以下功能性：1、通过实验环境的搭建，实现了检材手机端与“云控移动营销平台”（包含天微云控、AKA、微云时代等 3 款手机 App）Web 服务端连接的建立。2、通过对安装了“天微云控”、“AKA”、“微云时代”APP 的手机进行联网测试，发现在“云端移动营销平台”Web 端控制下，安装了“微云时代”、“天微云控”、“AKA”等 APP 的手机能够实现接收 Web 服务端发送的任务指令，实现自动完成“朋友圈”、“好友消息”、“添加好友”、“编辑统计”、“群功能”等 5 个模块中的“朋友圈点赞”、“朋友圈评论”、“好友群发消息”、“修改头像”、“扔捡漂流瓶”、“修改个性签名”等功能。软件使用者在招徕到广告、点赞、小说推广等业务后，可以批量向自己控制的微信朋友圈内批量转发广告、小说点赞等，事后按微信朋友圈内好友的点击量、充值款向需求者收取费用牟利。被告人朱晓辉获利 535 万元，被告人戴登科获利 60 余万元，被告人苏少涛获利 2 万余元，被告人黄侣霆获利 47 万元。

另查明，2019 年 3 月 15 日，被告人朱晓辉自动到中华人民共和国横琴出入境边防检查站投案，并如实供述自己罪行。2019 年 2 月 19 日，被告人苏少涛自动到张家界市公安局永定分局投案，并如实供述自己的罪行。2019 年 6 月 4 日，被告人黄侣霆自动到张家界市公安局永定分局投案，并如实供述自己的罪行。

再查明，案发后，被告人朱晓辉已退赃人民币 535 万元，被告人戴登科已退赃人民币 60 万元，被告人苏少涛已退赃人民币 2 万元，被告人黄侣霆已退赃人民币 47 万元。

上述事实，被告人朱晓辉、戴登科、苏少涛、黄侣霆在法庭审理过程中均无异议，且证人舒某、赵某 1、叶某、罗某、莫某、杨某的证言，专家证人刘某 1 的证言，线索来源及抓获经过，深圳市辉创软件技术有限公司工商登记信息、营销报表情况、财务资料，程序代码资料， 小说推广页面截图、上海铜爵网络科技有限公司营业执照，阿里云计算有限公司客户租用服务器情况，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，扣押决定书，扣押物品、文件清单，发还物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，辨认笔录，搜查笔录，封存、拆封提取笔录，电子数据，行政处罚决定书，视频资料，户籍资料等证据证明， 足以认定。

二、非法控制计算机信息系统罪

（一）2016 年 6、7 月份，被告人叶丹墨从朱晓辉处知晓移动营销助手软件功能后，获得该软件授权。2017 年 1 月，叶丹墨成立了天微云控科技有限公司，将移动营销助手软件更名为“天微云控”。该公司通过销售天微云控软件及利用该软件控制 2000 余台手机微信，通过微信朋友圈推广广告等方式牟利，并向他人或公司介绍小说推广业务，从中赚取差价。被告人肖桂珍为客户提供软件和授权，进行售后服务及购买微信号等工作，并提供银行卡用于公司转账，核对公司账目。被告人温智烨负责微信养号及操作天微云控后台。叶丹墨获利 500 万余元。

另查明，2019 年 3 月 11 日，被告人温智烨主动到张家界市公安局永定分局投案，并如实供述自己的罪行。

再查明，案发后，被告人叶丹墨已退赃人民币 500 万元。

上述事实，被告人叶丹墨、肖桂珍、温智烨在法庭审理过程中均无异议，且证人张某、叶某、罗某、琚某、涂某、莫某、杨某的证言，线索来源及抓获经过，深圳市天微云控科技有限公司工商登记信息资料，银行交易明细及流水，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，扣押决定书，扣押物品、文件清单，发还物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，搜查笔录及现场照片，电子数据，户籍资料等证据证明，足以认定。

（二）2016 年 5 月，被告人杨军从朱晓辉处获得移动营销助手软件代理权，成立了微云时代传媒科技（深圳）有限公司，将移动营销助手软件更名为“微云时代”。2017 年 3 月，被告人于强了解该软件盈利模式后入股该公司。该公司通过销售“微云时代”软件及使用该软件

控制手机微信推广广告等方式牟利。杨军获利 315 万余元，于强获利 64 万余元。

另查明，案发后，被告人杨军已退赃人民币 315 万元，被告人于强已退赃人民币 64 万元。上述事实，被告人杨军、于强在法庭审理过程中均无异议，且证人黄某、曾某 1、莫某、

杨某的证言，线索来源及抓获经过，深圳市微云时代传媒科技（深圳）有限公司工商登记信息资料，银行交易明细、流水及对账单，授权书资料，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，扣押决定书，扣押物品、文件清单，发还物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，搜查笔录及现场照片，辨认笔录，提取笔录，电子数据，户籍资料等证据证明，足以认定。

（三）2017 年 6 月，叶丹墨、叶佳与被告人黎威、**等人合伙成立长沙微远网络科技有限公司，黎威负责公司整体运行，**负责财务，潘某（另案处理）负责员工管理和联系业务。黎威陆续从天微云控公司购买安装了“天微云控”软件的手机 5000 台，利用控制的手机微信

为需求者推广小说等方式牟利。黎威获利 50 余万元，**获利 31 万余元。

另查明，被告人黎威已退赃人民币 50 万元，被告人**已退赃人民币 9 万元。

上述事实，被告人黎威、**在法庭审理过程中均无异议，且证人胡某 1、田某、胡某 2、潘某的证言，线索来源及抓获经过，长沙微远网络科技有限公司工商登记信息资料，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，银行交易流水及对账单，扣押决定书，扣押物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，搜查笔录，电子数据，户籍资料等证据证明，足以认定。

（四）2018 年 1 月，被告人叶佳从叶丹墨处购买“天微云控”软件，叶丹墨以 3000 余台手机入股与其合伙经营，叶佳通过使用“天微云控”软件实现对微信的自动化群控，以此在微信朋友圈推广广告牟利。为便于招揽客户，2018 年 9 月，叶佳成立了长沙墨尘网络有限公司， 叶佳负责公司的运营管理，肖桂珍为公司财务，宋某 2（另案处理）负责微信养号、操作软件在微信朋友圈推广广告等工作。叶佳获利人民币 56 万元。另查明，案发后，被告人叶佳已退赃人民币 56 万元。

上述事实，被告人叶佳在法庭审理过程中均无异议，且证人宋某 1、吴某、彭某、宋某 2 的证言，线索来源及抓获经过，长沙墨尘网络科技有限公司工商登记信息资料、养号步骤、后台工作分配情况，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，银行交易流水及对账单，扣押决定书，扣押物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，搜查笔录，电子数据，户籍资料等证据证明，足以认定。

（五）2018 年 4 月，被告人曾山峰、王志文了解到“天微云控”软件盈利模式后，从叶丹墨处购买了 1000 台手机和天微云控软件。为便于招徕业务，曾山峰、王志文等人合伙成立了微音科技有限公司，曾山峰负责联系业务，王志文负责软件操作等工作，通过利用软件控制微信为广告商推广小说等方式牟利。曾山峰获利 30 余万元，王志文获利 50 余万元。

另查明，被告人曾山峰已退赃人民币 30 万元，被告人王志文已退赃人民币 50 万元。

上述事实，被告人叶佳在法庭审理过程中均无异议，且证人曾某 2、刘某 2 的证言，线索来源及抓获经过，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，银行交易流水及对账单，扣押决定书，扣押物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，搜查笔录，电子数据，户籍资料等证据证明，足以认定。

（六）2018 年 5 月，被告人赵元纯了解到“天微云控”软件的盈利模式后，从叶丹墨处购买了 1000 台手机及“天微云控”软件并出资成立了星微工作室，安排赵某 2（另案处理）负责日常经营管理，该工作室通过该软件控制手机中的微信为广告商推广小说等方式牟利。

上述事实，被告人赵元纯在法庭审理过程中均无异议，且证人张某、叶某、罗某、赵某 2 的证言，线索来源及抓获经过，腾讯科技（深圳）有限公司报案书及法人授权委托证明书，扣押决定书，扣押物品、文件清单，湖南非税收入一般缴款书，司法鉴定意见书，辨认笔录，搜查笔录，电子数据，户籍资料等证据证明，足以认定。

本院认为，被告人朱晓辉、戴登科、苏少涛、黄侣霆违反国家规定，提供专门用于侵入、非法控制计算机信息系统的程序、工具，情节特别严重，四名被告人的行为均构成提供非法控制计算机信息系统程序、工具罪；被告人叶丹墨、肖桂珍、温智烨、杨军、于强、叶佳、黎威、**、曾山峰、王志文、赵元纯违反国家规定，对计算机信息系统实施非法控制，情节特别严重， 十一名被告人的行为均构成非法控制计算机信息系统罪，公诉机关指控的犯罪事实及罪名成立， 本院予以确认。

关于被告人戴登科的辩护人提出“对本案事实无异议，但对定性有异议，被告人戴登科构成犯罪证据不足”的意见，经查，腾讯公司微信程序属于计算机信息系统范围，戴登科明知其研发的“移动营销助手”软件未获腾讯公司授权也非腾讯公司研发，“云控移动营销平台”通过对安装有“移动营销助手”以及 Xposed 框架模块“wx_release.apk”插件的智能手机来获取微信数据，实现微信不具有的自动化操作功能，从而达到批量控制微信的目的。安装了“移动营销助手”的手机接受“云控移动营销平台”下发的指令，在微信系统里自动完成微信系统的“向好友发送消息”、“统计好友数量”等功能，该自动群发消息、统计好友数量、好友数据回传等功能是微信系统自身不具有的功能。戴登科研发、提供“移动营销助手”软件，其行为构成提供非法控制计算机信息系统程序、工具罪。该事实有证人证言、被告人的供述、司法鉴定意见书等证据相互印证，故对该意见，本院不予采纳。

关于被告人戴登科的辩护人提出“本案司法鉴定意见不合法”的意见，经查，湖南迪安司法鉴定中心作出的湘迪安司鉴中心[2019]电鉴字第 18-1、18-2、18-3、18-4 司法鉴定意见书，鉴定机构具有法定资质，鉴定程序合法，鉴定事项未超出业务范围，可作为证据使用，故对该意见，本院不予采纳。

在提供非法控制计算机信息系统程序、工具罪共同犯罪中，被告人朱晓辉、戴登科起主要作用，均系主犯，应当按照所参与的全部犯罪处罚，被告人苏少涛、黄侣霆起次要作用，

系从犯，依法应当减轻处罚。在非法控制计算机信息系统罪第 1 起共同犯罪中，被告人叶丹墨起主要作用，系主犯，应当按照所参与的全部犯罪处罚，被告人肖桂珍、温智烨起次要作用，系从犯，依法应当减轻处罚。在非法控制计算机信息系统罪第 2 起共同犯罪中，被告人杨军、于强起主要作用，均系主犯，应当按照所参与的全部犯罪处罚。在非法控制计算机信息系统罪第 3 起共同犯罪中，被告人黎威、**起主要作用，均系主犯，应当按照所参与的全部犯罪处罚。在非法控制计算机信息系统罪第 4 起共同犯罪中，被告人叶佳起主要作用，系主犯，应当按照所参与的全部犯罪处罚。在非法控制计算机信息系统罪第 5 起共同犯罪中，被告人曾山峰、王志文起主要作用，均系主犯，应当按照所参与的全部犯罪处罚。在非法控制计算机信息系统罪第 6 起共同犯罪中，被告人赵元纯起主要作用，系主犯，应当按照所参与的全部犯罪处罚。被告人朱晓辉、苏少涛、黄侣霆、温智烨犯罪后自动投案，如实供述自己的罪行，是自首，依法可以从轻处罚。被告人朱晓辉、苏少涛、黄侣霆、温智烨、叶丹墨、戴登科、肖桂珍、杨军、于强、叶佳、黎威、**、曾山峰、王志文、赵元纯归案后，自愿如实供述自己的罪行，承认指控的犯罪事实，愿意接受处罚，依法可以从宽处罚。被告人朱晓辉、苏少涛、黄侣霆、叶丹墨、戴登科、杨军、于强、叶佳、黎威、**、曾山峰、王志文积极退赃，依法可酌定从轻处罚。

综上，被告人朱晓辉、苏少涛、黄侣霆、温智烨、叶丹墨、戴登科、肖桂珍、杨军、于强、叶佳、黎威、**、曾山峰、王志文、赵元纯犯罪后有悔罪表现，没有再犯罪的危险，宣告缓刑对所居住的社区没有重大不良影响，可对朱晓辉、苏少涛、黄侣霆、温智烨、叶丹墨、戴登科、肖桂珍、杨军、于强、叶佳、黎威、**、曾山峰、王志文、赵元纯宣告缓刑，依照《中华人民共和国刑法》第二百八十五条第二、三款，第二十五条第一款，第二十六条第一、四款，第二十七条，第六十七条第一、三款，第六十四条，第五十二条，第七十二条第二款、第七十三条第二、三款，《中华人民共和国刑事诉讼法》第十五条之规定，经本院审判委员会讨论决定， 判决如下：

一、被告人朱晓辉犯提供非法控制计算机信息系统程序、工具罪，判处有期徒刑三年，缓刑四年，并处罚金人民币五十万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

二、被告人叶丹墨犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑四年，并处罚金人民币三十八万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

三、被告人杨军犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币四十万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

四、被告人叶佳犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十九万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

五、被告人戴登科犯提供非法控制计算机信息系统程序、工具罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十五万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

六、被告人黎威犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十二万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

七、被告人王志文犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十二万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

八、被告人曾山峰犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十二万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

九、被告人于强犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

十、被告人**犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币十万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

十一、被告人赵元纯犯非法控制计算机信息系统罪，判处有期徒刑三年，缓刑三年六个月， 并处罚金人民币四万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

十二、被告人黄侶霆犯提供非法控制计算机信息系统程序、工具罪，判处有期徒刑二年六个月，缓刑三年，并处罚金人民币十万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

十三、被告人苏少涛犯提供非法控制计算机信息系统程序、工具罪，判处有期徒刑二年六个月，缓刑三年，并处罚金人民币八万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

十四、被告人肖桂珍犯非法控制计算机信息系统罪，判处有期徒刑二年六个月，缓刑三年， 并处罚金人民币十万元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

十五、被告人温智烨犯非法控制计算机信息系统罪，判处有期徒刑一年，缓刑一年，并处罚金人民币一万五千元。（缓刑考验期限，从判决确定之日起计算）

（罚金限本判决生效后十日内缴纳）。

十六、对扣押机关扣押的供本案犯罪所用的财物，由扣押机关依法处置。（附扣押财物清单）

十七、对被告人朱晓辉违法所得人民币 5350000 元、被告人叶丹墨违法所得人民币 5000000 元、被告人杨军违法所得人民币 3150000 元、被告人叶佳违法所得人民币 560000 元、被告人戴登科违法所得人民币 600000 元、被告人黎威违法所得人民币 500000 元、被告人王志文违法所得人民币 500000 元、被告人曾山峰违法所得人民币 300000 元、被告人于强违法所得人民币 640000 元、被告人**违法所得人民币 310000 元、被告人黄侣霆违法所得人民币 470000 元、被告人苏少涛违法所得人民币 20000 元予以追缴。

如不服本判决，可在接到判决书的第二日起十日内通过本院或直接向湖南省张家界市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本十八份。

审 判 长　　王红英

人民陪审员　耿 莉

人民陪审员　张爱平

二〇一九年十二月二十七日

法官助理　　朱润杰

书记员　宋黄静

案例三、北京博捷微客科技有限公司、李某甲等提供侵入计算机信息系统的程序、工具案

审理法院：　南通市通州区人民法院

案　　号：　（2018）苏 0612 刑初 700 号

案　　由：　提供侵入、非法控制计算机信息系统程序、工具罪

裁判日期：　2019 年 04 月 11 日

南通市通州区人民法院

刑事判决书

（2018）苏 0612 刑初 700 号

公诉机关南通市通州区人民检察院。

被告人李某甲，男，1993 年 1 月 6 日生，北京 xx**科技有限公司法定代表人，住吉林省前郭尔罗斯蒙古族自治县。因涉嫌提供侵入计算机信息系统工具罪，于 2018 年 2 月 8 日被南通市通州区公安局刑事拘留，同年 3 月 16 日被逮捕。现羁押于南通市通州区看守所。

辩护人陈俊杰，执业证号13206201110623661，北京市炜衡（南通）律师事务所律师。

辩护人何维，执业证号13206200810404979，北京市炜衡（南通）律师事务所律师。

被告人张某甲，男，1985年5月28日生，北京xx**科技有限公司员工，住黑龙江省大兴安岭地区。因涉嫌提供侵入计算机信息系统工具罪，于2018年2月8日被南通市通州区公安局刑事拘留，同年3月16日被逮捕。现羁押于南通市通州区看守所。

辩护人张锦云，执业证号13206199211944300，江苏维业律师事务所律师。

被告人王某甲，男，1988年5月5日生，北京xx**科技有限公司员工，住内蒙古自治区通辽市科尔沁区。因涉嫌提供侵入计算机信息系统工具罪，于2018年2月8日被南通市通州区公安局刑事拘留，同年3月16日被逮捕。现羁押于南通市通州区看守所。

辩护人季栋栋，执业证号13206201210581003，江苏维业律师事务所律师。

被告人张某乙，男，1988年9月3日生，北京xx**科技有限公司员工，住河南省栾川县。因涉嫌提供侵入计算机信息系统工具罪，于2018年2月8日被南通市通州区公安局刑事拘留，同年3月16日被逮捕。现羁押于如东县看守所。

辩护人单敏，执业证号13206201411969218，北京市大成（南通）律师事务所律师。

辩护人冯薇雅，执业证号13206200911572347，北京大成（南通）律师事务所律师。

被告人王某乙，男，1989年10月16日生，北京xx**科技有限公司员工，住陕西省西安市阎良区。因涉嫌提供侵入计算机信息系统工具罪，于2018年2月8日被南通市通州区公安局刑事拘留，同年3月16日被逮捕。现羁押于如东县看守所。

辩护人熊军，执业证号13206200410728258，江苏维业律师事务所律师。

被告人魏某甲，女，1994年1月4日生，北京xx**科技有限公司员工，住河北省保定市满城区。因涉嫌提供侵入计算机信息系统工具罪，于2018年2月8日被南通市通州区公安局刑事拘留，同年3月16日被逮捕。现羁押于南通市看守所。

辩护人ＸＸ义，执业证号11101199810783087，北京市当代律师事务所律师。

被告人刘某甲，男，1986年2月15日生，个体经营手机维修，住北京市海淀区。因涉嫌提供侵入计算机信息系统工具罪，于2018年2月14日被南通市通州区公安局刑事拘留，同年3月16日被逮捕。现羁押于南通市通州区看守所。

辩护人王边国，执业证号13101200310838790，上海申浩律师事务所律师。

被告人李某乙，男，1990年2月8日生，个体经营手机维修，住北京市昌平区。因涉嫌提供侵入计算机信息系统工具罪，于2018年2月8日被南通市通州区公安局刑事拘留，同年3月16日被逮捕。现羁押于南通市通州区看守所。

辩护人王引，执业证号13206199410727924，江苏清心律师事务所律师。

被告人张某丁，男，1972年9月7日生，个体销售，住广东省广州市白云区。曾因犯销售伪劣产品罪，于2012年7月30日被广东省深圳市宝安区人民法院判处有期徒刑一年，

并处罚金人民币五万元，2013 年 3 月 26 日刑满释放。因涉嫌提供侵入计算机信息系统工具罪，于 2018 年 3 月 13 日被南通市通州区公安局刑事拘留，同年 4 月 19 日被逮捕。现羁押于南通市通州区看守所。

辩护人曹巧玲，执业证号 14403201711495718，广东守静律师事务所律师；

辩护人王允庆，执业证号 14403200510442692，广东海埠律师事务所律师。

被告人刘某乙，男，1993 年 4 月 1 日生，北京 xx**科技有限公司员工，住吉林省公主岭市。因涉嫌提供侵入计算机信息系统工具罪，于 2018 年 2 月 8 日被南通市通州区公安局刑事拘留，同年 3 月 16 日被取保候审；同年 5 月 16 日经南通市通州区人民检察院决定取保候审，同日由南通市通州区公安局执行。

被告人郑某，男，1989 年 12 月 28 日生，买卖网络程序，住广西壮族自治区崇左市宁明县。因涉嫌提供侵入计算机信息系统工具罪，于 2018 年 4 月 27 日被南通市通州区公安局刑事拘留，同年 5 月 16 日被取保候审；同日经南通市通州区人民检察院决定取保候审，同日由南通市通州区公安局执行。

辩护人廖蔚，执业证号 14514201110279453，广西大腾律师事务所律师。

被告人张某丙，男，1988 年 6 月 24 日生，郑州 xxx 通讯有限公司经营者，住河南省沈丘县。因涉嫌提供侵入计算机信息系统工具罪，于 2018 年 4 月 7 日被南通市通州区公安局刑事拘留，同年 5 月 4 日被取保候审；同年 5 月 16 日经南通市通州区人民检察院决定取保候审，同日由南通市通州区公安局执行。

辩护人李玥赟，执业证号 13201201411907042，江苏海越律师事务所律师。

被告人汪某，女，1992 年 1 月 8 日生，微商，住湖北省蕲春县。因涉嫌提供侵入计算机信息系统工具罪，于 2018 年 3 月 7 日被南通市通州区公安局刑事拘留，同年 4 月 3 日被取保候审；同年 5 月 16 日经南通市通州区人民检察院决定取保候审，同日由南通市通州区公安局执行。

辩护人代承，执业证号 14201201520523882，北京盈科（武汉）律师事务所律师。

南通市通州区人民检察院以通检诉刑诉〔2018〕701 号起诉书、通检诉刑变诉〔2019〕5 号变更起诉决定书指控被告单位北京 xx**科技有限公司（以下简称 xx 公司）、被告人李某甲、张某甲、王某甲、张某乙、王某乙、魏某甲、刘某甲、李某乙、张某丁、刘某乙、郑某、张某丙、汪某犯提供侵入计算机信息系统的程序、工具罪，于 2019 年 1 月 2 日向本院提起公诉，后又于 2019 年 2 月 20 日变更起诉。本院依法组成合议庭，于 2019 年 3 月 12 日、13 日、4 月 11 日公开开庭审理了本案。南通市通州区人民检察院指派检察员曹雪芳出庭支持公诉，被告单位诉讼代表人李某丙、被告人李某甲、张某甲、王某甲、张某乙、王某乙、魏某甲、刘某甲、李某乙、张某丁、刘某乙、郑某、张某丙、汪某及其各自的辩护人均到庭参加了诉讼。现已审理终结。

南通市通州区人民检察院指控，2017 年 10 月至 2018 年 1 月期间，被告单位 xx 公司、被告人李某甲、张某甲、王某甲、张某乙、王某乙、魏某甲、刘某甲、李某乙、张某丁、刘某乙、郑某、张某丙、汪某为牟取非法利益，开发、销售具有突破腾讯视频等视频播放平台安全防护机制，在未取得腾讯视频等视频平台 V**会员权限的情况下，对视频平台的完整视频内容进行播放功能的手机 APP“酷视界”、“橙子视频”、“乐尚视界”、“爱尚”，并制作实体卡进行销售。经统计，登陆使用“酷视界”APP 平台的用户有 50900 人，登陆使用“橙子视频”APP 平台的用户有 470075 人，登陆使用“乐尚视界”APP 平台的用户有 3163834 人，xx 公司获相关广告收益人民币 60 万余元（以下币种均为人民币）。其中，被告人郑某提供“17 云解析”等解析地址为软件开发提供帮助，xx 公司给付其 2 万余元;被告人刘某甲、李某乙将“橙子视频”、“乐尚视界”、“爱尚”视频 APP 软件的部分电子卡密提供给被告人张某丁，张某丁付款给被告人李某乙、刘某甲 300000 万元；被告人刘某甲、李某乙将“橙子视频”、“乐尚视界”电子卡密制作成实体卡销售给涂某、徐某和齐某等人（均另处），非法获利 135748.88 元；被告人张某丁将“橙子视频”、“乐尚视界”电子卡密制作成实体卡，销售给被告人张某丙、李某丁（另处），非法获利 188500 元；被告人张某丙销售给被告人汪某“橙子视频”、“乐尚视界”的视频卡，非法获利 6 万余元；被告人汪某将所购的“橙子视频”、“乐尚视界”视频卡销售给何某（另处）等人，非法获利 102370 元。

为证明上述指控，公诉机关提供了下列证据：1.南通市通州区公安局查扣的相关视频卡、电脑、手机等物证；2.银行往来明细及支付宝记录、张某丁的微信“夏尚”财付通记录、微信转账记录截屏等书证；3.证人冯某、王某丙、李某丙等人的证言；3.国家林业局森林公安司法鉴定中心物证检验报告、福建中证司法鉴定中心司法鉴定意见；4.被告人李某甲等十三名被告人的供述和辩解等。

公诉机关认为，被告单位 xx 公司、被告人李某甲、张某甲、王某甲、张某乙、王某乙、魏某甲、刘某甲、李某乙、张某丁、刘某乙、郑某、张某丙、汪某，开发或销售具有突破计算机信息系统安全保护措施、未经授权获取计算机信息系统数据的功能的程序、工具，情节特别严重，其行为均已触犯《中华人民共和国刑法》第二百八十五条第三款、第四款的规定，应当以提供侵入计算机信息系统的程序、工具罪追究被告单位及各被告人的刑事责任。被告单位 xx 公司、李某甲、张某甲、王某甲、张某乙、王某乙、魏某甲、刘某甲、李某乙、张某丁、刘某乙、郑某、张某丙、汪某共同实施全部或部分犯罪，系共同犯罪，其中，被告单位 xx 公司、被告人李某甲、刘某甲、李某乙、张某丁起主要作用，是主犯；被告人王某乙、郑某、张某丙、汪某起次要作用，是从犯，提请本院依法分别判处。

被告单位 xx 公司、被告人李某甲对起诉书指控的犯罪事实及罪名均不持异议，并自愿认罪。被告人李某甲的辩护人提出如下辩护意见：1.本案鉴定单位福建中证司法鉴定中心的鉴定资质缺少省级公安机关授权的证据；2.被告人李某甲并非是制作“橙子视频”、“乐尚视界”

手机 APP 软件犯意的提议者，其所在公司被告单位 xx 公司也并未实际获利；3.被告人李某甲是初犯、偶犯，犯罪手段一般，社会危害性小，且具有自首情节，认罪认罚，建议法院对其依法从轻或减轻处罚。

被告人张某甲对起诉书指控的犯罪事实及罪名不持异议，并自愿认罪。其辩护人对指控罪名亦无异议，但提出指控被告单位 xx 公司获相关广告收益 60 余万元不实，xx 公司并未实际获得该广告收益；同时提出被告人张某甲是从犯，有自首情节，且是初犯，其本人并未获利，建议对其从轻或减轻处罚的辩护意见。

被告人王某甲对起诉书指控的犯罪事实及罪名不持异议，并自愿认罪。其辩护人提出被告人王某甲在共同犯罪中作用较小，是从犯，有自首情节，且无前科劣迹，属初犯、偶犯，建议对其从轻处罚的辩护意见。

被告人张某乙对起诉书指控的犯罪事实及罪名不持异议，并自愿认罪。其辩护人提出如下意见：1.本案中的鉴定报告存在问题，首先，福建中证司法鉴定中心的鉴定主体资格不符合两高司法解释的要求；其次，缺乏提取物证、委托过程，以及涉案软件入侵报案人腾讯公司计算机信息系统的证据；2.被告人张某乙在整个案件中所起作用较小，并不是直接责任人，其仅是参与了涉案软件的开发，并未参与销售；3.被告人张某乙是因为对本案侵犯客体的认知存在错误才导致犯罪，主观恶性不大，且具有自首、认罪情节，建议对其从轻处罚。

被告人王某乙对起诉书指控的犯罪事实及罪名不持异议，且自愿认罪。其辩护人提出如下意见：1.被告人王某乙只是负责技术工作，并未从中获利，在共同犯罪中所起作用较小，是从犯；2.被告人王某乙是初犯、偶犯，有自首情节，建议对其从轻处罚。

被告人魏某甲对起诉书指控的犯罪事实及罪名不持异议，且自愿认罪。其辩护人提出如下辩护意见：1.被告人魏某甲主要从事技术工作，对涉案事件的性质认识不明确，因此，主观恶性不深，应是从犯；2.被告人魏某甲没有前科劣迹，属于初犯、偶犯，并认罪悔罪，建议对其从轻处罚。

被告人刘某甲对起诉书指控的罪名不持异议，且自愿认罪，但对获利金额提出异议，同时辩解自己仅是对涉案手机 APP 软件做推广和销售，应是从犯。其辩护人提出如下意见：1.起诉书指控被告人刘某甲是主犯不正确。被告人刘某甲并未参与涉案手机 APP 软件的设计、开发，其仅是推广、销售实体卡，未向被告单位提出开发涉案 APP 软件的技术要求，仅提出对软件程序界面外观的要求；2.起诉书指控被告人刘某甲和李某乙销售实体卡的数量及获利不确切。被告人张某丁支付的 300000 元中有两笔共计 50000 元，是张某丁之前所欠的“看易看”视频卡的款项；3.被告人刘某甲无前科、劣迹，主观恶性不深，案发后如实供述，认罪、悔罪，建议对被告人刘某甲从轻处罚。

被告人李某乙对起诉书指控的罪名不持异议，且自愿认罪，但对获利金额提出异议，同时辩解自己和被告人刘某甲并没有与被告单位 xx 公司共同开发。其辩护人提出如下辩护意

见：1.被告人李某乙、刘某甲与被告人李某甲等人并不属于共同犯罪，亦不起主要作用；2.鉴定意见中未载明涉案手机 APP 软件侵入了腾讯的服务器还是第三方服务器取得片源；3.起诉书认定被告人李某乙销售金额不实；4.被告人李某乙归案后认罪态度较好，自愿认罪，建议对其从轻处罚。

被告人张某丁对起诉书指控的犯罪事实及罪名不持异议，且自愿认罪。其辩护人对犯罪事实及罪名亦无异议，对量刑情节提出如下意见：1.被告人张某丁不是犯意的提起者，且仅是销售者，不起主要作用，应是从犯；2.公诉机关指控罪名的法定刑应为三年以下有期徒刑或拘役；3.被告人张某丁在到案前已经主动停止并要求他人停止售卖行为，其社会危害性较小；4.被告人张某丁归案后如实供述，当庭认罪、认罚，并愿意退出全部违法所得；5.被告人张某丁检举他人违法犯罪线索，属有立功表现。综合上述情节，建议对被告人张某丁从轻或减轻处罚。

被告人刘某乙对起诉书指控的犯罪事实及罪名不持异议，且自愿认罪。

被告人郑某对起诉书指控的犯罪事实及罪名不持异议，且自愿认罪。其辩护人提出被告人郑某是从犯，归案后已退出犯罪所得，当庭认罪、认罚，且是初犯、偶犯，建议对其从轻处罚的辩护意见。

被告人张某丙对起诉书指控的犯罪事实及罪名不持异议，且自愿认罪。其辩护人提出被告人张某丙主观恶性较小，是从犯，有自首情节，归案后已退出犯罪所得，当庭认罪、认罚，且是初犯、偶犯，建议对其从轻处罚的辩护意见。

被告人汪某对起诉书指控的犯罪事实及罪名不持异议，且自愿认罪。其辩护人提出被告人汪某是从犯，归案后如实供述自己的犯罪事实，并已退出违法所得，建议对其单处罚金的辩护意见。

经审理查明，被告单位 xx 公司于 2016 年 12 月在北京注册成立，经营范围为技术开发、技术推广、技术转让、技术咨询、技术服务等经营活动，法定代表人为被告人李某甲。xx 公司先后聘用被告人张某甲、王某甲、张某乙、魏某甲、刘某乙等人为公司员工，被告人王某乙由上海 xxxx 科技有限公司北京分公司借调至 xx 公司工作。

2017 年 10 月，被告单位 xx 公司、被告人李某甲为提升公司知名度，通过非法途径获取广告收益，以牟取非法利益，指使被告人张某甲、张某乙、王某乙、魏某甲等共同参与开发并运营具有突破腾讯视频等视频播放平台安全防护机制，在未取得腾讯视频等视频平台的 VIP 会员权限的情况下，播放视频平台的影视资源功能的手机 APP 软件“酷视界”。被告人李某甲在网上通过百度找视频网站里会员视频的链接，张某甲和王某甲负责测试和维护 APP 后台程序，王某甲还负责联系客户，推送视频软件电子卡密，联系广东专门做会员卡的单位制作实体卡，魏某甲和张某乙负责后台数据的整合、修补，王某乙负责编写手机 APP 软件的程序，刘某乙负责将“酷视界”APP 实体卡通过快递发放给买家。

被告人刘某甲、李某乙合伙做手机维修以及“看易看”视频卡生意。2017 年 12 月，被告人刘某甲、李某乙经人介绍找到被告单位 xx 公司，与被告人李某甲、张某甲、王某甲商议，由 xx 公司向被告人刘某甲、李某乙免费提供“酷视界”手机 APP 视频软件卡密，刘某甲、李某乙为 xx 公司做推广，获得的广告收益五五分成。此后，被告人李某甲根据被告人刘某甲、李某乙的要求，安排张某甲、张某乙、王某乙、魏某甲等人按照“酷视界”的模版，开发制作了与“酷视界”功能类似的手机 APP 软件“橙子视频”。后被告人刘某甲、李某乙又根据被告人张某丁的要求，要求 xx 公司先后制作了可以观看 12 个视频网站的手机 APP 软件“乐尚视界”、“爱尚”。被告人张某丁提出自己独家销售“乐尚视界”手机 APP，被告人李某乙、刘某甲还设立客服，负责手机软件的问题处理，被告人刘某乙注册了相关广告账户。在此期间，被告人李某甲通过 QQ 结识并联系被告人郑某，由被告人郑某为上述软件提供技术支持，被告人郑某后提供了“17 云解析”等解析地址为软件开发提供帮助，xx 公司支付被告人郑某 20000 余元。

2017 年 12 月至 2018 年 1 月期间，被告人王某甲将“橙子视频”、“乐尚视界”、“爱尚”三款手机 APP 软件的电子卡密免费提供给被告人刘某甲、李某乙，刘某甲、李某乙将部分电子卡密销售给被告人张某丁，被告人张某丁支付给被告人李某乙、刘某甲 250000 元；刘某甲、李某乙另将 274851 张“橙子视频”、“乐尚视界”电子卡密制作成实体卡销售给涂某、徐某和齐某等人，得款 135748.88 元。

被告人张某丁将“橙子视频”、“乐尚视界”电子卡密制作成实体卡，将其中的 381500 张销售给被告人张某丙和李某丁，得款 188500 元。

被告人张某丙销售给被告人汪某“橙子视频”实体卡 18500 张、“乐尚视界”实体卡 44700 张，共得款 60000 余元。

被告人汪某销售给何某等人“橙子视频”实体卡 18500 张、“乐尚视界”实体卡 44700 张，共得款 102370 元。

经统计，登陆“酷视界”APP 平台的用户有 50900 人，登陆“橙子视频”APP 平台的用户有 470075 人，登陆“乐尚视界”APP 平台的用户有 3163834 人。经电子数据抽选检验，上述“酷视界”、“橙子视频”、“乐尚视界”等手机 APP 软件能够播放腾讯等视频网站的 VIP 视频，上述软件服务器中的腾讯等视频网站的 VIP 视频数据，来自于腾讯等网站服务器。经鉴定，“酷视界”、“橙子视频”、“乐尚视界”手机 APP 软件是具有突破腾讯视频等视频播放平台安全防护机制，在未取得腾讯视频等视频平台的 VIP 会员权限的情况下，具备对视频平台的完整视频内容进行播放的功能，属于专门用于突破腾讯视频等视频平台视频内容安全防护机制并播放视频平台影视内容的工具软件。

2018 年 1 月 31 日，深圳市腾讯计算机系统有限公司向南通市通州区公安局报案，被告人李某甲、张某甲、王某甲、张某乙、王某乙、魏某甲、刘某乙、李某乙于 2018 年 2 月 7

日在接受公安机关询问时，即如实供述了自己的犯罪事实。被告人刘某甲于2018年2月13日被抓获，被告人汪某于2018年3月6日被抓获，被告人张某丁于2018年3月13日被抓获，被告人张某丙于2018年4月6日被抓获，被告人郑某于2018年4月26日被抓获。被告人张某丁、刘某甲、郑某、张某丙、汪某到案后均如实供述了自己的犯罪事实。

案发后，被告人郑某退出90000元、被告人汪某退出30000元、被告人张某丙退出30000元。

本案审理期间，被告人刘某甲退出违法所得185748.88元，被告人李某乙退出违法所得200000元，被告人张某丁退出违法所得188500元，被告人张某丙退出违法所得30000元，被告人汪某退出违法所得72370元，上述款项均暂存于本院财政专户。

上述事实，有公诉机关当庭提供并经过庭审质证的下列证据予以证明：

1.物证及照片：公安机关分别从被告单位xx公司、被告人李某乙、刘某甲、张某丁、郑某、汪某以及何某、李某丁、徐某、齐某等处查扣的手机、电脑，“酷视界”、“橙子视频”、“乐尚视界”、“爱尚”实体卡。

2.书证：

（1）被告单位xx公司登记注册信息、被告人李某甲、张某甲、王某甲、张某乙、王某乙、魏某甲、刘某甲、李某乙、张某丁、刘某乙、郑某、张某丙、汪某的常住人口基本信息。

（2）夏尚电子发送快递记录截屏、户名为“李某丁”的银行卡以及被告人张某丙的银行卡交易记录、支付宝记录、微信转账记录截屏，被告人张某丁的微信“夏尚”财付通记录，证人李某丁的记事本。

（3）证人朱某、周某、魏某乙提供的手机微信红包、转账记录截屏。

（4）广东省深圳市宝安区人民法院刑事判决书。

3.未到庭证人冯某、王某丙、李某丙、郝某、李某丁、王某丁、杨某甲、朱某、周某、魏某乙、杨某乙等人的证言。

4.被告人李某甲、张某甲、王某甲、张某乙、王某乙、魏某甲、刘某甲、李某乙、张某丁、刘某乙、郑某、张某丙、汪某以及同案行为人何某、李某丁、徐某、齐某、涂某的供述和辩解。

5.南通市通州区公安局网络安全保卫大队制作的视频卡提取笔录、送检电子物证情况说明、电子检查工作记录及提取电子证据清单。

6.鉴定意见：（1）国家林业局森林公安司法鉴定中心物证检验报告；（2）福建中证司法鉴定中心司法鉴定意见书。

7.南通市通州区公安局出具的发破案经过，制作的搜查笔录、扣押笔录、扣押清单，情况说明。

8.其他材料：南通市通州区公安局交通警察大队事故处理中队出具的情况说明，江苏省非税收入一般缴款书。

归纳本案的争议焦点，本院综合评判如下：

1.关于被告单位 xx 公司是否获利。

被告人张某甲的辩护人对公诉机关指控被告单位 xx 公司获广告收益 600000 元提出异议，本院认为，公诉机关未能提供证据证明被告单位 xx 公司已实际获得该广告收益，因此，采纳辩护人的意见，对公诉机关指控的该节事实本院不予支持。

2.关于登录使用“酷视界”、“橙子视频”、“乐尚视界”三款手机 APP 软件用户统计数据是否确切。

被告人张某乙以及部分辩护人在庭审中提出，因有用户拥有几个账户，不一定全部登录使用，本案中用户统计数据不确切。公诉机关庭审中表示就该问题可作为量刑情节。本院认为，案涉三款手机 APP 软件用户数的统计数据是公安机关根据相关电子证据统计的结果，其数量已远远超出两高《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》中关于“情节特别严重”的规定，因此，该统计数据即便存在部分重复也不影响本案量刑情节的认定。

3.关于被告人刘某甲、李某乙的获利情况。

被告人李某乙及其辩护人庭审中提出，公诉机关指控其和被告人刘某甲与被告人张某丁之间的交易金额有误，被告人张某丁支付的 300000 元中有两笔共计 50000 元是之前的往来款，并非本案中“橙子视频”、“乐尚视界”两款手机 APP 软件视频卡的货款。经查，被告人李某乙、刘某甲、张某丁庭审中供述一致，均表示在张某丁与李某乙、刘某甲的交易明细中有两笔款项合计 50000 元是之前销售“看易看”视频卡的货款，本院认为，综合本案相关证据，应从有利于被告人的原则就低认定，故采纳被告人李某乙的辩解意见，从其和被告人刘某甲的违法所得中剔除该 50000 元。

4.关于本案鉴定机构“福建中证司法鉴定中心”的鉴定资格以及委托鉴定程序是否合法的问题。

被告人李某甲、张某乙的辩护人均提出福建中证司法鉴定中心不是公安部指定的鉴定机构，不符合鉴定主体资格。本院认为，根据最高人民法院、最高人民检察院、公安部《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》，对电子数据涉及的专门性问题难以确定的，由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具报告。根据该规定，可以由具备司法鉴定资格的机构出具鉴定意见，也可以由公安部指定的机构出具，是选择性规定。而福建中证司法鉴定中心具有福建省司法厅颁发的司法鉴定许可证，鉴定业务范围为“电子数据司法鉴定”，因此，符合上述规定的要求，属具有司法鉴定资格的鉴定机构，且参与检验鉴定的两名工作人员亦具有电子证据检验鉴定的资格。本案中，侦查机关从各被

告人或相关电子数据持有人处收集、提取电子数据后，根据相关规定和要求，进行了电子证据检查，提取出与案件有关的数据并保存。同时，为准确鉴别案涉数据中的数量，侦查机关将有关数据分别送国家林业局森林公安司法鉴定中心、福建中证司法鉴定中心进行检验鉴定，检验对象与送检材料一致，检验过程符合相关专业操作规范标准。该两鉴定中心作出的物证检验报告，检验程序合法，检验方法科学，检验结论能够证明本案案件事实，可以采信。

5.关于本案主、从犯的认定。

关于公诉机关在起诉书中认定被告单位、被告人李某甲、张某甲、王某甲、张某乙、魏某甲、刘某乙与被告人王某乙、刘某甲、李某乙、张某丁、郑某、张某丙、汪某共同实施全部或部分犯罪，系共同犯罪，其中，被告人李某甲、刘某甲、李某乙、张某丁起主要作用，被告人王某乙、郑某、张某丙、汪某起次要作用。经查，被告人王某乙虽是借调至被告单位工作，但其是在被告单位获取劳动报酬，并接受被告单位管理，应视为被告单位员工，不应将其列为被告单位之外的人员。

本案中，被告单位 xx 公司是单位犯罪，被告人李某甲作为被告单位法定代表人，为了公司获取非法利益，参与并指使公司员工开发用于侵入计算机信息系统的程序、工具，负有直接主管责任，属单位犯罪中的“直接负责的主管人员”，承担主要责任；被告人张某甲、王某甲、张某乙、王某乙、魏某甲、刘某乙在执行单位决定或公司负责人指令实施犯罪，虽然犯罪情节属特别严重，但犯罪地位具有从属性，属单位犯罪中的“其他直接责任人员”，因此，应根据在单位犯罪中各自的职责及所起的作用分别进行处罚，不宜再区分主、从犯。

被告人张某丙、汪某各自独立销售案涉视频卡，与被告单位 xx 公司及被告人刘某甲、李某乙、张某丁主观上并无共同实施犯罪的合谋，客观上亦无犯罪行为的交叉。因此，该两被告人与被告单位及其他各被告人之间不属共同犯罪，不应认定为从犯。

关于被告人李某乙、张某丁的辩护人分别提出该两被告人在共同犯罪中不起主要作用，应认定为从犯的意见。经查，被告人李某乙、刘某甲、张某丁虽未直接参与案涉“橙子视频”、“乐尚视频”手机 APP 软件的技术开发，但该两款视频软件是被告单位 xx 公司根据被告人刘某甲、李某乙、张某丁的要求，在“酷视界”功能的基础上进行的改进，包括视频软件的名称、外观、可观看视频的频道数，且该两款视频软件是由被告单位 xx 公司向被告人刘某甲、李某乙免费提供卡密，由刘某甲、李某乙负责推广，并约定广告收益五五分成。为此，本院认为，被告人刘某甲、李某乙、张某丁在共同犯罪中均起主要作用，均应认定为主犯。

6.关于被告人张某丁的辩护人提出被告人张某丁检举他人违法犯罪线索，有立功表现的辩护意见，经查，南通市通州区公安局交通警察大队根据被告人张某丁提供的线索，对 2017 年 9 月 5 日发生在通州区金沙镇的一起交通肇事逃逸案嫌疑人张某进行了传唤和审查，目前尚未查证属实。因此，被告人张某丁尚不构成立功。

综上，本院认为，被告单位 xx 公司、被告人刘某甲、李某乙、张某丁、张某丙、汪某为了谋取非法利益，开发、销售专门用于突破计算机信息系统安全保护措施、未经授权获取计算机信息系统数据功能的手机 APP 软件，被告人郑某明知他人实施侵入计算机信息系统的违法犯罪行为而提供程序，其行为均已构成提供侵入计算机信息系统的程序、工具罪，属情节特别严重，应予惩处。被告人李某甲作为被告单位 xx 公司直接负责的主管人员，对 xx 公司的行为负有主管责任；被告人张某甲、王某甲、张某乙、王某乙、魏某甲、刘某乙系 xx 公司其他直接责任人员，对该七名被告人的行为均应当按照犯提供侵入计算机信息系统的程序、工具罪且情节特别严重进行刑事处罚。公诉机关指控的主要犯罪事实清楚，证据确凿，罪名成立，本院予以支持。被告单位 xx 公司、被告人刘某甲、李某乙、张某丁、郑某共同实施部分犯罪行为，属共同犯罪，被告人刘某甲、李某乙、张某丁在共同犯罪中均起主要作用，均为主犯，应当按照各自所参与的全部犯罪处罚；被告人郑某起次要作用，是从犯，依法应当从轻或减轻处罚。被告人李某甲、张某甲、王某甲、张某乙、王某乙、魏某甲、刘某乙、李某乙在接受公安机关一般性询问时，即如实供述了自己的主要犯罪事实，均可视为自首，依法可从轻或减轻处罚。被告人刘某甲、郑某、张某丙、汪某归案后如实供述自己的犯罪事实，属坦白，依法可从轻处罚。被告人张某丁在侦查期间认为自己的行为仅侵犯了版权，并不是犯罪，是对其行为性质的辩解，但对犯罪事实仍作了如实供述，亦属坦白，依法可对其从轻处罚。被告人张某丁曾因故意犯罪被判处有期徒刑以上刑罚，刑罚执行完毕以后，在五年以内再犯应当判处有期徒刑以上刑罚之罪，系累犯，依法应当从重处罚。庭审中，被告单位 xx 公司、各被告人均当庭自愿认罪，被告人刘某甲、李某乙、张某丁退出违法所得，均可酌情从轻处罚，其中，被告人刘某乙犯罪情节较轻，被告人郑某、张某丙、汪某已退出违法所得，均可适用缓刑。采纳各辩护人提出的有关各被告人从轻处罚情节的辩护意见。违法所得、作案工具等，均应予没收。为严肃国法，惩罚犯罪，保护他人的计算机信息系统不受侵入，维护社会管理秩序，根据《中华人民共和国刑法》第二百八十五条第三、四款、第三十条、第三十一条、第二十五条第一款、第二十六条第一、四款、第二十七条、第六十七条第一、三款、第六十五条第一款、第七十二条第一、三款、第七十三条第二、三款、第六十四条，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》第三条第二款第（一）项、第九条第二款之规定，判决如下：

一、被告单位北京 xx**科技有限公司犯提供侵入计算机信息系统的程序、工具罪，判处罚金人民币三十万元（罚金已缴纳）；

二、被告人李某甲犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑三年（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 2 月 8 日起至 2021 年 2 月 7 日止）；

三、被告人张某甲犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑二年（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年2月8日起至2020年2月7日止）；

四、被告人王某甲犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑二年（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年2月8日起至2020年2月7日止）；

五、被告人张某乙犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑一年六个月（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年2月8日起至2019年8月7日止）；

六、被告人王某乙犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑一年六个月（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年2月8日起至2019年8月7日止）；

七、被告人魏某甲犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑一年六个月（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年2月8日起至2019年8月7日止）；

八、被告人刘某甲犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑三年，并处罚金人民币十万元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年2月14日起至2021年2月13日止；罚金已缴纳）；

九、被告人李某乙犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑二年九个月，并处罚金人民币十万元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年2月8日起至2020年11月7日止；罚金已缴纳）；

十、被告人张某丁犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑三年六个月，并处罚金人民币八万元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年3月13日起至2021年9月12日止；罚金于判决生效后一个月内缴纳）；

十一、被告人刘某乙犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑一年三个月，缓刑一年六个月（缓刑考验期限，从判决确定之日起计算）；

十二、被告人郑某犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑二年，缓刑三年，并处罚金人民币二万元（缓刑考验期限，从判决确定之日起计算；罚金已缴纳）；

十三、被告人张某丙犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑三年，缓刑四年，并处罚金人民币三万元（缓刑考验期限，从判决确定之日起计算；罚金已缴纳）；

十四、被告人汪某犯提供侵入计算机信息系统的程序、工具罪，判处有期徒刑三年，缓刑四年，并处罚金人民币五万元（缓刑考验期限，从判决确定之日起计算；罚金已缴纳）；

十五、已扣押的作案工具笔记本电脑、硬盘、手机、案涉 APP 视频卡等，均予以没收，由扣押机关依法处理。

被告人刘某甲退出的违法所得 185748.88 元，被告人李某乙退出的违法所得 200000 元、被告人张某丁退出的违法所得 188500 元，被告人郑某退出的违法所得 20000 元、被告人张某丙退出的违法所得 60000 元、被告人汪某退出的违法所得 102370 元，合计人民币 756618.88 元均予以没收，上缴国库。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向江苏省南通市中级人民法院提出上诉，书面上诉的，应提交上诉状正本一份，副本二份。

审判长　殷晓露

人民陪审员　施玉萍

人民陪审员　曹荣芬

二〇一九年四月十一日

书记员　张　洋

吴忧

案例四、李琦、杨克群、周阳等提供侵入、非法控制计算机信息系统程序、工具案

审理法院：　浙江省绍兴市中级人民法院

案　　号：　（2018）浙 06 刑终 742 号

案　　由：　侵犯公民个人信息罪

裁判日期：　2018 年 12 月 28 日

浙江省绍兴市中级人民法院

刑事裁定书

（2018）浙 06 刑终 742 号

原公诉机关绍兴市越城区人民检察院。

上诉人（原审被告人）李琦，男，1983 年 5 月 23 日出生于辽宁省沈阳市，汉族，大专文化，原系沈阳纳信科技有限公司法定代表人，住辽宁省沈阳市大东区。因涉嫌犯诈骗罪于 2017 年 3 月 23 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

辩护人魏力，浙江金道（绍兴）律师事务所律师。

辩护人刘兴，辽宁华建律师事务所律师。

上诉人（原审被告人）杨克群，男，1983 年 8 月 29 日出生于福建省古田县，汉族，大学文化，无业，住福建省厦门市湖里区。因涉嫌犯诈骗罪于 2017 年 3 月 24 日被刑事拘留，同年 4 月 29 日被逮捕。现羁押于绍兴市看守所。

辩护人谌波平，浙江大公律师事务所律师。

辩护人柯松江，国浩律师（福州）事务所律师。

上诉人（原审被告人）郑辉鸿，男，1990 年 10 月 1 日出生于江西省大余县，汉族，高中文化，农民，住江西省大余县。因涉嫌犯诈骗罪于 2017 年 3 月 23 日被刑事拘留，同年 4 月 29 日被逮捕。现羁押于绍兴市看守所。

上诉人（原审被告人）张鑫，男，1985 年 1 月 15 日出生于山西省定襄县，汉族，大学文化，无业，住山西省定襄县。因涉嫌犯诈骗罪于 2017 年 3 月 24 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

上诉人（原审被告人）周阳，曾用名周阳阳，女，1988 年 7 月 1 日于陕西省渭南市，汉族，大专文化，无业，住陕西省渭南市临渭区。因涉嫌犯诈骗罪于 2017 年 3 月 24 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

辩护人俞华南，浙江大公律师事务所律师。

上诉人（原审被告人）李星星，男，1984 年 10 月 7 日出生于湖南省岳阳市，汉族，高中文化，原系岳阳时运公司员工，住湖南省岳阳市岳阳楼区。因涉嫌犯侵犯公民个人信息罪于 2017 年 4 月 1 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

原审被告人曾睿，男，1992 年 10 月 10 日出生于江西省大余县，汉族，大专文化，农民，住江西省大余县。因涉嫌犯

诈骗罪于 2017 年 3 月 23 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

原审被告人林江，男，1983 年 10 月 21 日出生于四川省宜宾县，汉族，大专文化，无业，住四川省成都市天府新区。因涉嫌犯诈骗罪于 2017 年 3 月 24 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

原审被告人陈天明，男，1990 年 10 月 16 日出生于广东省信宜市，汉族，高中文化，无业，住广东省信宜市。因涉嫌犯诈骗罪于 2017 年 3 月 24 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

原审被告人张朝荣，男，1983 年 8 月 4 日出生于四川省宜宾县，汉族，大学文化，无业，住四川省成都市金牛区。因涉嫌犯诈骗罪于 2017 年 3 月 24 日被刑事拘留，同年 4 月 29 日被逮捕。现羁押于绍兴市看守所。

原审被告人朱涛，男，1986 年 8 月 1 日出生于湖北省仙桃市，汉族，初中文化，个体经营，住湖北省仙桃市。2006 年 1 月 23 日因犯抢劫罪被湖北省仙桃市人民法院判处有期徒刑一年六个月，并处罚金人民币一万元。因涉嫌犯诈骗罪于 2017 年 4 月 7 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

原审被告人张明伟，男，1987 年 7 月 23 日出生于广西壮族自治区玉林市，汉族，初中文化，原系出租车司机，住广西壮族自治区玉林市玉州区。因涉嫌犯诈骗罪于 2017 年 3 月 26 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

原审被告人胡义龙，男，1989 年 3 月 14 日出生于安徽省濉溪县，汉族，大专文化，原系合肥领路者网络科技有限公司监理，住安徽省濉溪县。因涉嫌犯诈骗罪于 2017 年 3 月 23 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

原审被告人李路平，男，1988 年 6 月 23 日出生于四川省渠县，汉族，初中文化，农民，住四川省渠县。因涉嫌犯诈骗罪于 2017 年 3 月 24 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

原审被告人陈明，男，1993 年 3 月 15 日出生于湖北省孝感市，汉族，初中文化，农民，住湖北省孝感市孝南区。因涉嫌犯诈骗罪于 2017 年 3 月 24 日被刑事拘留，同年 4 月 28 日被逮捕。现羁押于绍兴市看守所。

原审被告人李杰，男，1985 年 4 月 29 日出生于湖南省娄底市，汉族，大专文化，个体经营，住湖南省娄底市娄星区。因涉嫌犯侵犯公民个人信息罪于 2017 年 3 月 30 日被刑事拘留，同年 4 月 29 日被逮捕。现羁押于绍兴市看守所。

绍兴市越城区人民法院审理绍兴市越城区人民检察院指控原审被告人李琦、杨克群、陈天明、张鑫、林江、张朝荣、朱涛、周阳犯提供侵入计算机信息系统程序、工具罪，原审被告人张明伟、胡义龙、李路平、陈明、李星星、李杰、犯侵犯公民个人信息罪，被告人曾睿、郑辉鸿犯侵犯公民个人信息罪、诈骗罪一案，于 2018 年 9 月 30 日作出（2018）浙 0602 刑初 101 号刑事判决。宣判后，原审被告人李琦、杨克群、郑辉鸿、周阳、张鑫、李星星不服，提出上诉。本院依法组成合议庭，经过阅卷，讯问上诉人，听取辩护人意见，认为本案事实清楚，决定不开庭审理。现已审理终结。

原判认定：

一、提供侵入计算机信息系统程序、工具

2015 年年初开始，被告人李琦创建“快啊答题”平台，后与提供图文验证码识别技术的被告人杨克群合作，合伙有偿为他人提供批量图文验证码识别服务。被告人张鑫、林江、陈天明、张朝荣、朱涛等众多软件开发作者在编译出具有批量登录腾讯 QQ 账号功能的软件后，将软件接入被告人李琦提供的“快啊答题”平台的对外端口。软件通过平台接入的被告人杨克群的图文验证码识别技术，快速、批量实现对腾讯公司服务器下发图文验证码的识别，以顺利完成腾讯 QQ 账密的验证及账号的登录。后众多软件用户以向“快啊答题”平台充值的形式有偿使用上述程序工具，并通过运行上述程序工具侵入腾讯公司服务器，批量验证腾讯 QQ 账密的一致性以及登录账号获取账号内信息。已查清的软件接入平台事实及获利情况为：

1.2015 年下半年开始，被告人张鑫将其编译的软件接入“快啊答题”平台，并将软件上传至网络供他人有偿使用。同时，被告人张鑫还将其编译的类似功能软件出售给他人获利。经查，被告人李琦于 2016 年 6 月 1 日至 2017 年 3 月 23 日通过支付宝向被告人张鑫支付软件使用获利钱款人民币 153 万余元。

2.2016 年上半年开始，被告人林江将其编译的软件接入“快啊答题”平台，并将软件上传至网络供他人有偿使用。经查，被告人李琦于 2016 年 6 月 1 日至 2017 年 3 月 23 日通过支付宝向被告人林江支付软件使用获利钱款人民币 54 万余元。

3.2015 年 5 月开始，被告人陈天明将其编译的软件接入“快啊答题”平台，并将软件上传至网络供他人有偿使用。2016 年 5 月，被告人陈天明将其编译的软件交由被告人周阳推广、销售，获利二人五五分成。2017 年 2 月 8 日，被告人周阳以人民币 30 万元的价格向被告人陈天明购买了上述软件，此后软件获利归被告人周阳一人所有。经查，被告人李琦于 2016 年 6 月 20 日至 2017 年 2 月 9 日通过支付宝向被告人陈天明支付软件使用获利钱款人民币 29 万余元，于 2017 年 2 月 20 日至 3 月 20 日通过支付宝向被告人周阳支付软件使用获利钱款人民币 5.8 万余元。

4.2016 年下半年开始，被告人张朝荣将其编译的软件接入“快啊答题”平台，并将软件上传至网络供他人有偿使用。经查，被告人李琦于 2016 年 7 月 4 日至 2017 年 3 月 21 日通过支付宝向被告人张朝荣支付软件使用获利钱款人民币 22.8 万余元。

5.2016 年 10 月开始，被告人朱涛将其编译的软件接入“快啊答题”平台，并将软件上传至网络供他人有偿使用。经查，被告人李琦于 2016 年 10 月 8 日至 2017 年 3 月 23 日通过支付宝向被告人朱涛支付软件使用获利钱款人民币 22.7 万余元。

6.2016 年 7 月至案发，软件作者从“快啊答题”平台的成功提现金额（作者的软件使用获利）为 320 余万元。2016 年 6 月 1 日至 2017 年 3 月 22 日，被告人李琦通过支付宝支付给被告人杨克群的图文验证码识别技术使用获利为人民币 347 万余元。

二、侵犯公民个人信息

1.2016-2017 年间，被告人李杰通过网络购买等方式获取大量 QQ 账密形式的数据，后加价出售给被告人郑辉鸿、曾睿等人。被告人李杰贩卖数据给被告人郑辉鸿、曾睿的交易金额约 34 万元。被告人郑辉鸿、曾睿利用软件再次对数据进行账密匹配后用于网络推广。案发后，被告人郑辉鸿处尚有 3 万余条 QQ 账密数据被查获。

2.2016-2017 年间，被告人张明伟通过网络购买等方式获取大量 QQ 账密形式的数据，后利用软件进行批量账密匹配并出售获利，其出售金额超过 34 万元。案发后，被告人张明伟处尚有超过 10G 容量的数据被查获。

3.2016-2017 年间，被告人胡义龙通过网络购买等方式获取大量 QQ 账密形式的数据，后利用软件进行批量账密匹配并出售获利，其出售金额超过 28 万元。案发后，被告人胡义龙处尚有超过 3G 容量的数据被查获。

4.2016-2017 年间，被告人李路平通过网络购买等方式获取大量 QQ 账密形式的数据，后利用软件进行批量账密匹配并出售获利，其出售金额超过 22 万元。案发后，被告人李路平处尚有超过 3.5G 容量的数据被查获。

5.2016-2017 年间，被告人陈明通过网络购买等方式获取大量 QQ 账密形式的数据，后利用软件进行批量账密匹配并出售获利，其出售金额超过 26 万元。案发后，被告人李路平处尚有近 4G 容量的数据被查获。

6.2016-2017 年间，被告人李星星通过网络购买等方式获取大量 QQ 账密形式的数据，后利用软件进行批量账密匹配并出售获利，已查清的出售金额有近 4000 元。案发后，被告人李星星处尚有超过 2G 容量的数据被查获。

三、诈骗

2016-2017 年间，被告人曾睿、郑辉鸿经事先合谋，付费委托他人制作能够后台修改中奖号码的博彩网站，并登录购买的 QQ 账号进行网络推广，引诱玩家加入 QQ 群组并至网站下注博彩。被告人曾睿、郑辉鸿同时招募刘某、陈某 1、周某、熊永发（均另案处理）等数十人分组管理博彩 QQ 群组，团伙成员在 QQ 群组中以管理员、技术员、玩家等不同角色通过发布投注计划、虚假中奖结果等方式活跃气氛，引导玩家集中下注“幸运彩”，并通过后台修改开奖结果以“杀大放小”方式占有玩家的下注钱款。经查，被告人曾睿、郑辉鸿通过上述方式占有的玩家的钱款超过 486 万元。

在案件审理过程中，被告人朱涛退缴了人民币 10000 元，被告人周阳退缴了人民币 58308 元，被告人张明伟退缴了人民币 4000 元，被告人胡义龙退缴了人民币 10000 元，被告人李星星退缴了人民币 4000 元，被告人李杰退缴了人民币 5000 元。

2017 年 3 月 23 日，被告人李琦、曾睿、郑辉鸿、周阳、胡义龙、张朝荣被警察抓获归案；同月 24 日，被告人杨克群、张鑫、林江、陈明、陈天明、李路平被警察抓获归案；同月 26 日被告人张明伟被警察抓获归案；同月 30 日，被告人李杰被警察抓获归案；同月 31 日，被告人李星星被警察抓获归案；同年 4 月 7 日，被告人朱涛被警察抓获归案。

为认定上述事实，原判确认了相应证据。

原审认为，被告人李琦、杨克群、张鑫、林江、陈天明、张朝荣、朱涛、周阳的行为均已构成提供侵入计算机信息系统程序、工具罪，且系共同犯罪；被告人曾睿、郑辉鸿、张明伟、胡义龙、李路平、陈明、李星星、李杰的行为均已构成侵犯公民个人信息罪，部分系共同犯罪；被告人曾睿、郑辉鸿的行为均已构成诈骗罪，系共同犯罪。对被告人曾睿、郑辉鸿的行为予以数罪并罚。基于本案及系列案件的恶劣社会影响，酌情对各被告人予以从重处罚。

被告人曾睿、郑辉鸿组织、领导犯罪集团实施犯罪行为，对二被告人予以从重处罚。依照《中华人民共和国刑法》第二百八十五条第三款、第二百五十三条之一第一、三款、第二百六十六条、第二十五条第一款、第二十六条、第六十九条、第六十四条之规定，

判决如下：一、被告人李琦犯提供侵入计算机信息系统程序、工具罪，判处有期徒刑四年二个月，并处罚金人民币五十万元；二、被告人杨克群犯提供侵入计算机信息系统程序、工具罪，判处有期徒刑四年二个月，并处罚金人民币七十万元；三、被告人曾睿犯侵犯公民个人信息罪，判处有期徒刑四年，并处罚金人民币五万元；犯诈骗罪，判处有期徒刑十三年，并处罚金人民币五十万元；决定执行有期徒刑十四年六个月，并处罚金人民币五十五万元；四、被告人郑辉鸿犯侵犯公民个人信息罪，判处有期徒刑四年，并处罚金人民币五万元；犯诈骗罪，判处有期徒刑十三年，并处罚金人民币五十万元；决定执行有期徒刑十四年六个月，并处罚金人民币五十五万元；五、被告人张鑫犯提供侵入计算机信息系统程序、工具罪，判处有期徒刑三年十个月，并处罚金人民币二十万元；六、被告人林江犯提供侵入计算机信息系统程序、工具罪，判处有期徒刑三年四个月，并处罚金人民币十万元；七、被告人陈天明犯提供侵入计算机信息系统程序、工具罪，判处有期徒刑三年四个月，并处罚金人民币十万元；八、被告人张朝荣犯提供侵入计算机信息系统程序、工具罪，判处有期徒刑三年，并处罚金人民币六万元；九、被告人朱涛犯提供侵入计算机信息系统程序、工具罪，判处有期徒刑三年，并处罚金人民币六万元；十、被告人周阳犯提供侵入计算机信息系统程序、工具罪，判处有期徒刑三年，并处罚金人民币三万元；十一、被告人张明伟犯侵犯公民个人信息罪，判处有期徒刑四年六个月，并处罚金人民币六万元；十二、被告人胡义龙犯侵犯公民个人信息罪，判处有期徒刑四年，并处罚金人民币五万元；十三、被告人李路平犯侵犯公民个人信息罪，判处有期徒刑四年，并处罚金人民币五万元；十四、被告人陈明犯侵犯公民个人信息罪，判处有期徒刑四年，并处罚金人民币五万元；十五、被告人李星星犯侵犯公民个人信息罪，判处有期徒刑三年六个月，并处罚金人民币二万元；十六、被告人李杰犯侵犯公民个人信息罪，判处有期徒刑四年，并处罚金人民币五万元；十七、被告人朱涛退缴的人民币 10000 元、被告人周阳退缴的人民币 58308 元、被告人张明伟退缴的人民币 4000 元、被告人胡义龙退缴的人民币 10000 元、被告人李星星退缴的人民币 4000 元、被告人李杰退缴的人民币 5000 元，均系非法获利，予以没收。公安机关在案件侦查中扣押的电脑主机、笔记本电脑、平板电脑、手机、手机卡、银行卡、U 盘、硬盘、印章、服务器、一体机、电源、内存、交换机、路由器、小主机、无线网络信号接收器、网关、U 盾、营业执照、身份证等由扣押机关根据物品属性予以处置，系作案工具的予以没收，与案件无关的发还给所有人。公安机关冻结在案的被告人李琦名下的人民币 10118.31 元（账号 62×××78），被告人曾睿名下的人民币 19735.52 元（账号 62×××38），被告人郑辉鸿名下的人民币 512642.05 元（账号 62×××94）、人民币 67304.77 元（账号 62×××15）、人民币 404597.91 元（账号 62×××27）、人民币 939767.01

元（账号 62×××77）、人民币 422678.41 元（账号 62×××09），被告人张朝荣名下的人民币 101116.09 元（账号 62×××77），被告人陈天明名下的人民币 46936.7 元（账号 62×××86），被告人林江名下的人民币 80656.83 元（账号 62×××84），均作为非法获利予以没收。被告人杨克群名下的人民币 68581.34 元（账号 62×××83）、王丽玉名下的人民币 5115226.92 元（账号 62×××79）、王某 1 名下的人民币 20841.96 元（账号 62×××28），其中人民币 3474000 元作为被告人杨克群的非法获利予以没收，余款中的人民币 700000 元，抵作被告人杨克群的罚金，上述钱款扣缴后，账户予以解冻。其余未追回的非法获利继续予以追缴。

原审被告人李琦上诉及其辩护人辩护意见如下：1.快啊答题平台提供的图文验证码识别服务系通用合法技术，并非专门用于侵入计算机信息系统的程序、工具，无证据证明本案各被告人存在侵入计算机信息系统的行为。2.李琦并不知道平台用户具有侵入计算机信息系统的犯罪行为，也不知道对接平台的软件是专门侵入、非法控制计算机信息系统的软件，与杨克群、张鑫、陈天明等人之间没有共同犯罪的故意，不具有提供侵入、非法控制计算机信息系统程序、工具的主观故意。3.司法鉴定意见书主体不合法、结论不正确，不能作为认定李琦有罪的依据。综上，李琦的行为不构成提供侵入、非法控制计算机系统程序、工具罪。请求给予公正判决。

原审被告人杨克群上诉及其辩护人辩护意见如下：1.图片验证码的智能识别技术不具有侵入计算机信息系统的功能，杨克群并不知道提供的图文识别程序被他人用于非法用途。一审认定杨克群与快啊平台负责人李琦之间系合作关系，二人合伙有偿为他人提供批量图文验证码识别服务，为他人侵入计算机信息系统提供程序、工具帮助，系事实认定错误。2.对 QQ 图片验证码的识别没有法律禁止性规定，不能以大量 QQ 验证码被识别推定杨克群具有为他人侵入计算机信息系统提供帮助的故意。杨克群主观上没有提供侵入、非法控制计算机信息系统程序、工具犯罪的故意，客观上没有与他人实施共同犯罪的合意和行为，一审法院将其的图文识别程序与快啊平台、其他软件作为整体进行评价，认定整体具有侵入计算机信息系统的功能，并以此认定各程序作者构成提供侵入计算机信息系统程序、工具罪，系法律适用错误。3.公安机关提供的司法鉴定意见书鉴定机构不具备鉴定资质，且鉴定结果与杨克群无关，不能作为定案依据。综上，上诉人杨克群不构成犯罪，请求依法改判。

原审被告人郑辉鸿上诉提出：1.其购买的 QQ 信息全部用于其与曾睿运营的赌博网站推广，是为实施诈骗的手段行为，不构成侵犯公民个人信息罪，不应实行数罪并罚。2.其被扣押的银行卡内有部分是其父母所有，不应作为其非法获利予以没收。请求法院依法改判。

原审被告人周阳上诉及其辩护人提出：周阳作为陈天明软件的代理售卖者，对软件技术问题一概不知，相对李琦、杨克群、陈天明等人只是次要主体，在共同犯罪中仅起到辅助作用，应认定为从犯，同时考虑到其犯罪情节较轻，获利较少、积极退赃，有悔罪表现及家庭实际情况，请求对其减轻处罚并适用缓刑。

原审被告人张鑫上诉提出：1.2015 年下半年至 2016 年 6 月份并没有涉案违法软件接入快啊平台或上传网盘公开下载；2016 年 9 月 4 日后，其因得知软件可能被用于违法用途就删除了软件下载源并停用软件，之后并未参与犯罪。故这两个时间段未实施犯罪获利，一审认定其犯罪时间有误。2.并非所有返利都来自涉案几款查询软件，另有部分软件和技术本身是合法的。综上，请求二审重新认定并依法改判。

原审被告人李星星上诉提出：1.一审法院对其犯罪的信息条数认定有误。其存储的 2.22G 数据中，除了 QQ 账密数据之外还有很大一部分 md5 加密数据，此外还有大量重复信息和非公民个人信息；其提取的全部数字数据约为 300 万条，通过筛选后匹配数据中属于公民个人信息的不超过 1.5 万条，远未达到 5 万条标准，不属于“情节特别严重”。2.与同案犯相比量刑过重。综上，请求依法改判。

经审理查明的事实与原判认定的一致，有经一审庭审质证、认证的各原审被告人供述、非同案犯庞峰、陈某 2、邓某、王某 2、刘某、容某、钟喁、熊永发、周某供述、证人王某 1、翁某、张某、朱某、马某、江某 1、委托书、情况说明、现场勘验工作记录、电子证据检查工作记录及电子数据、司法鉴定意见书、聊天记录、平台交易记录、支付宝交易明细、搜查笔录及照片、扣押决定书、扣押清单、扣押物品照片、辨认笔录及照片、书记信息提取结果、数量统计结果、实名验证结果、情况说明、充值记录、远程勘验工作记录、执行、调解款票据、抓获经过、刑事判决书、人员详细信息、户籍证明、常住人口信息等证据予以证实，二审予以确认。

关于上诉和辩护意见，综合评析如下：

一、关于上诉人李琦、杨克群及辩护人提出的相关意见。1.司法鉴定意见书系具有电子数据鉴定资质的机构依照法定程序所作，鉴定意见客观真实，结合腾讯公司安全管理部出具的情况说明、被告人张鑫、林江、陈天明、周阳等人供述，足以证实涉案平台、程序、软件通过各自实现功能绕过 QQ 登陆验证码保护措施，批量验证 QQ 账号密码是否一致的事实。2、上诉人李琦、杨克群均供述，虽然不清楚这些原始数据的来源和用途，但有意识到正常情况下不会有那么多原始数据需要识别，大量使用打码服务的人有可能用于网络违法活动；收集在案的杨克群与平台创建者李琦、软件提供者张鑫等人的聊天记录亦能证实二人应当知晓相关软件接入平台后通过图文识别程序用于批量识别腾讯 QQ 验证码的事实。上述证据足以认定二人主观上明知自己提供的平台、程序可能用于侵入腾讯服务器获取相关信息，即主观上存在提供侵入计算机信息系统的程序、工具的故意。3.原审被告人张鑫、林江、陈天明等人将批量登录腾讯 QQ 账号功能的软件接入上诉人李琦创建的“快啊答题”平台，通过上诉人杨克群提供的图文验证码识别技术快速批量识别验证码筛选出账密一致的 QQ 号码信息，从而达到侵入腾讯服务器获取数据的目的。软件提供者、图文识别技术提供者和平台创建者虽然未经事先商谋，但主观对上述过程均系明知，在此认知下相互配合，共同完成绕过验证

码安全保护措施，筛选账密一致的 QQ 号码，为侵入腾讯服务器获取数据提供了帮助，属共同犯罪，程序或软件本身是否具备侵入计算机信息系统功能或是否合法不影响对上述事实的认定。故上诉人李琦、杨克群提出主观上无犯罪故意，客观上无共同犯罪行为的意见，与事实不符，不予采纳。

二、关于郑辉鸿提出的上诉意见，经查：1.最高人民法院、最高人民检察院、公安部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》规定：“使用非法获取的公民个人信息，实施电信网络诈骗犯罪行为，构成数罪的，应当依法予以并罚”，即使郑辉鸿购买的 QQ 信息全部用于自己实施诈骗的赌博网站推广，其购买 QQ 信息的行为也已构成侵犯公民个人信息罪，应数罪并罚。2.郑辉鸿在实施诈骗犯罪期间无其他合法收入，公安机关冻结其个人名下银行卡内资金作为其非法获利进行追缴并无不当，其辩称卡内资金系其父母所有无证据支持，不予采纳。

三、关于周阳提出系从犯的意见，经查：上诉人周阳前期名义上系陈天明开发软件的代理，但周阳具体负责软件推广，与陈天明互相配合，获利五五分成，后期购买了陈天明的软件进行独立开发，积极主动实施犯罪，在共同犯罪中所起作用较大，不能认定为从犯。

四、关于张鑫提出关于犯罪时间和犯罪数额的意见。经查：上诉人张鑫在庭前多次供述及相关聊天记录证实，其所设计的软件均针对腾讯 QQ 账号并自 2015 年下半年开始接入快啊平台；支付宝交易交易记录证实，从 2016 年 6 月 1 日至 2017 年 3 月 23 日陆续有资金从快啊平台支付宝账户转入张鑫支付宝账户，即 2017 年 9 月份之后仍有软件接入平台获取利润，该事实与上诉人李琦供述张鑫的参与时间能够相互印证。上诉人张鑫称前期无违法软件接入平台及后期未实施犯罪的意见与上述证据相矛盾，不予采信。

五、关于李星星提出信息数量认定有误，认定其为“情节特别严重”不当的意见。经查：经侦查机关统计，从李星星 U 盘中查获的数据信息达 4500 万条以上，经对其中 QQ 数据抽样验证，超过 50%为公民身份证或银行账户等公民个人信息，结合其在“快啊平台”充值消费、出售公民个人信息的销售金额等情况，足以认定其侵犯公民个人信息已达到“情节特别严重”程度。对李星星提出的该上诉意见，不予采纳。

本院认为，上诉人李琦、杨克群、张鑫及原审被告人林江、陈天明、张朝荣、朱涛、周阳违反国家规定，提供专门用于侵入计算机信息系统的程序、工具，情节特别严重，其行为均已构成提供侵入计算机信息系统程序、工具罪，系共同犯罪；上诉人李星星、郑辉鸿及原审被告人曾睿、张明伟、胡义龙、李路平、陈明、李杰违反国家有关规定，以非法方式获取或出售公民个人信息，情节特别严重，其行为均已构成侵犯公民个人信息罪，且部分系共同犯罪；上诉人郑辉鸿及原审被告人曾睿以非法占有为目的，采用虚构事实、隐瞒真相的方法，骗取他人财物，数额特别巨大，其行为均已构成诈骗罪，系共同犯罪。上诉人郑辉鸿及原审被告人曾睿均构成两罪，依法予以并罚。基于本案及系列案件的恶劣社会影响，酌情对各被

告人予以从重处罚。原判定罪和适用法律正确，已结合各原审被告人的犯罪事实、情节、悔罪表现等情况作出适当量刑。审判程序合法。各上诉人提出的上诉意见，不予采纳，要求二审改判，均不予支持。依照《中华人民共和国刑事诉讼法》第二百三十六条第一款第（一）项之规定，裁定如下：

驳回上诉，维持原判。

本裁定为终审裁定。

审判长　祝ＸＸ

审判员　李　莹

审判员　翟金源

二〇一八年十二月二十八日

书记员　傅　莹

（四）破坏计算机信息系统罪

案例一、徐浩、邱鹏破坏计算机信息系统案

审理法院：　盐城市亭湖区人民法院

案　号：　（2018）苏 0902 刑初 437 号

案　由：　破坏计算机信息系统罪

裁判日期：　2018 年 08 月 10 日

盐城市亭湖区人民法院刑事判决书

（2018）苏 0902 刑初 437 号

公诉机关江苏省盐城市亭湖区人民检察院。

被告人徐浩，男，1995 年 1 月 14 日出生，住广东省惠州市惠城区。因涉嫌犯破坏计算机信息系统罪，于 2017 年 10 月 12 日被刑事拘留，同年 11 月 17 日被逮捕。现羁押于盐城市看守所。

辩护人刘卫忠，广东晟晨律师事务所律师。

被告人邱鹏，男，1997 年 1 月 13 日出生，住湖南省益阳市大通湖区。因涉嫌犯破坏计算机信息系统罪，于 2017 年 11 月 27 日被刑事拘留，同年 12 月 21 日被逮捕。现羁押于盐城市看守所。

江苏省盐城市亭湖区人民检察院以亭检诉刑诉［2018］343 号起诉书指控被告人徐浩、邱鹏犯破坏计算机信息系统罪，于 2017 年 7 月 5 日向本院提起公诉。本院审查后，于同日立案， 依法适用简易程序，并组成合议庭，公开开庭进行了审理。江苏省盐城市亭湖区人民检察院指派检察员黄祥坤出庭支持公诉，被告人徐浩及其辩护人刘卫忠、邱鹏到庭参加诉讼。现已审理终结。

江苏省盐城市亭湖区人民检察院指控，2017 年 2 月份以来，赵某（另案处理）在互联网上建立**网站，发布其设计编写“XY 修改器 4.0.apk”程序，提供该软件及使用教程、教学视频等下载服务，在网站页面上设置了“充值”、“代理”页面在互联网上销售该软件，还通过建立 QQ 群进行推广。该软件在客户端安装后为 Xposed 模块“XY 修改器”，该模块通过拦截并修改系统 API 的调用结果实现修改 Android 系统中的 IMEI、MSISDN、IMSI、ICCID、MAC 地址、无线网络 SSID、BSSID、IP 地址等信息的功能。软件购买者在 Xposed 模块“XY 修改器” 软件中运行某某网络科技（上海）有限公司“某某”APP 应用时，该软件可通过拦截并篡改客户端程序与服务器之间的传输数据，骗过某某网络科技（上海）有限公司的首单减免审核机制， 使服务器端程序根据篡改的传输数据，将重复使用该软件注册、不符合新用户标准的用户认定为新用户并支付首单优惠补贴，给某某网络科技（上海）有限公司造成损失。被告人徐浩、邱鹏明知该软件可篡改客户端程序中硬件信息，具有将篡改的信息传输至服务器端程序以实现骗取首单优惠补贴功能，仍然担任赵某的下级代理，从赵某处批量购得该软件使用权后，通过 QQ 群等加价推广销售该软件使用权，给某某网络科技（上海）有限公司造成损失人民币 25020 元。其中，被告人徐浩从赵某处购买“XY 修改器”使用权累计人民币 37048.98 元，通过互联网加价后销售给他人给某某网络科技（上海）有限公司造成损失计人民币 13974 元；被告人邱鹏从赵某处购买“XY 修改器”使用权累计人民币 20862 元，通过互联网加价后销售给他人给某某网络科技（上海）有限公司造成损失计人民币 11046 元。经鉴定，“XY 修改器 4.0.apk”程序符合破坏性程序的定义，可以认为检材程序具有破坏性。具体事实如下：

1.2017 年 2 月至 8 月间，被告人徐浩明知赵某编写发布的“XY 修改器 4.0.apk”软件可篡改客户端程序中硬件信息，具有将篡改的信息传输至服务器端程序以实现骗取首单优惠补贴功能，仍然担任赵某的下级代理，以 2 元/天、15 元/周、50 元/月、180 元/年的价格从赵某处购买该软件使用权，并建立“奥特曼外卖交流一群”、“奥特曼外卖交流二群”、“奥特曼外卖交流三群”等 QQ 群等推广销售该软件使用权，以 4 元/天、20 元/周、70 元/月、240 元/ 年的价格，将软件使用权销售给陈某、何某某、黄某某、支某某等 25 人。陈某、何某某、黄某某、支某某等 25 人使用“XY 修改器”模拟出的客户端硬件信息，在“某某”外卖 APP 上重复注册新用户点餐骗取首单优惠补贴，给某某网络科技（上海）有限公司造成损失共计人民币 13974 元。

2.2017 年 2 月至 9 月间，被告人邱鹏明知赵某编写发布的“XY 修改器 4.0.apk”软件可篡改客户端程序中硬件信息，具有将篡改的信息传输至服务器端程序以实现骗取首单优惠补贴功能，仍然担任赵某的下级代理，以 2 元/天从赵某处购买该软件使用权，并建立“XY 安卓改机①群”、“XY 安卓改机②群”等 QQ 群等推广销售该软件使用权，以 4 元/天、20 元/周、70 元/月的价格，将软件使用权销售给陈某、曾某某、陈某某、林某某等 12 人。

陈某、曾某某、陈某某、林某某等 12 人使用“XY 修改器”模拟出的客户端硬件信息，在“某某”外卖 APP 上重复注册新用户点餐骗取首单优惠补贴，给某某网络科技（上海）有限公司造成损失共计人民币 11046 元。

被告人徐浩被抓获归案后如实供述上述事实。被告人邱鹏犯罪后主动投案并如实供述上述事实。

被告人徐浩及其辩护人刘卫忠、被告人邱鹏对公诉机关指控的犯罪事实和罪名均无异议。被告人徐浩的辩护人刘卫忠还提出以下辩护意见：被告人徐浩相对于赵某来说，作用较小，系从犯；被告人有坦白情节、退赃事实、其母患病、家庭生活困难、平时表现较好，建议从轻处罚，并提供了其母患病的相关的病历、社区表现调查证明等证据予以证明。

上述事实，被告人徐浩及其辩护人刘卫忠、被告人邱鹏在开庭审理过程中均无异议，并有证人赵某、何某某、黄某某、陈某等人的证言，盐城市公安局亭湖分局出具和制作的被告人户籍证明、归案经过、某某网络科技（上海）有限公司营业执照、扣押清，盐城市公安局亭湖分局网络安全保卫大队制作的电子证据检查工作记录、电子证物检查笔录，盐城市公安局亭湖分局收集的电子数据，上海辰星电子数据司法鉴定中心出具的司法鉴定意见、上海弘连网络科技有限公司计算机司法鉴定所计算机司法鉴定意见书等证据予以证实，足以认定。

本院认为，被告人徐浩、邱鹏违反国家规定，故意传播专门设计用于破坏计算机系统数据的破坏性程序，影响计算机系统正常运用，后果严重，其行为构成破坏计算机信息系统罪。被告人徐浩、邱鹏分别与他人共同实施破坏计算机信息系统犯罪，系共同犯罪，应当按照二名被告人在犯罪中所起的作用分别予以处罚。公诉机关指控被告人徐浩、邱鹏犯破坏计算机信息系统罪的事实清楚，证据确实、充分，罪名成立，本院予以支持。关于被告人徐浩的辩护人提出被告人徐浩系从犯的辩护意见，经查，赵某系可篡改客户端程序中硬件信息的开发者，被告人徐浩系购买该软件后向不特定公众销售的实行者，二人的行为均系实行行为，故不宜区分主从犯，上述事实，有被告人徐浩的供述、证人赵某等人的证言、相关的司法鉴定意见书等证据予以证实，故对辩护人的该辩护意见，本院不予采纳。关于被告人徐浩的辩护人提出被告人徐浩系坦白、有退赃表现，建议从轻处罚的辩护意见，经查，该辩护意见符合客观事实，本院予以采纳。被告人徐浩归案后，能如实供述自己的罪行，系坦白，可以从轻处罚。被告人邱鹏犯罪后自动投案并如实供述自己的罪行，系自首，可以从轻或者减轻处罚。案发后，被告人徐浩、邱鹏能退出全部赃款，均可以从轻处罚。为维护国家互联网安全，根据被告人犯罪的事实、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》第二百八十六条第一、二款， 第二十五条第一款，第六十七条第一款、第三款，《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》第四条第一款第（三）项之规定， 判决如下：

一、被告人徐浩犯破坏计算机信息系统罪，判处有期徒刑十个月。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2017 年 10 月 12 日起至 2018 年 8 月 11 日止。）

二、被告人邱鹏犯破坏计算机信息系统罪，判处有期徒刑九个月。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2017 年 11 月 27 日起至 2018 年 8 月 26 日止。）

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向江苏省盐城市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份、副本两份。

审判长　方飞权

人民陪审员　郑锦萍

人民陪审员　周红霞

二〇一八年八月十日

书记员　邵晓晨

案例二、胡凌云破坏计算机信息系案

审理法院：　上海市普陀区人民法院

案　　号：　（2016）沪 0107 刑初 1395 号

案　　由：　破坏计算机信息系统罪

裁判日期：　2016 年 12 月 27 日

上海市普陀区人民法院

刑事判决书

（2016）沪 0107 刑初 1395 号

公诉机关上海市普陀区人民检察院。

公诉机关上海市普陀区人民检察院。

被告人胡凌云，男，1988 年 7 月 23 日生，汉族，户籍地本市虹口区，暂住本市嘉定区。

辩护人傅建平，上海博和律师事务所律师。

上海市普陀区人民检察院以沪普检诉刑诉[2016]1253 号起诉书指控被告人胡凌云犯破坏计算机信息系统罪，于 2016 年 12 月 1 日向本院提起公诉。本院依法组成合议庭，公开开庭审理了本案。上海市普陀区人民检察院指派检察员戈某出庭支持公诉，被告人胡凌云及其辩护人傅建平均到庭参加诉讼。现已审理终结。

上海市普陀区人民检察院指控：2015 年 8 月，被告人胡凌云进入上海波克城市网络科技股份有限公司担任客服人员，其通过破译他人账户密码，以他人名义登陆该公司开发运营的网络游戏“捕鱼达人 3D”的后台系统，通过更改其指定用户游戏系统中的“游戏金币”数量，并在游戏中通过“游戏金币”的操作获取相关游戏装备，后通过网络出售给他人谋利，

截止案发，仅部分销售额达到人民币 38000 余元。

2016 年 8 月 23 日，被告人胡凌云被公安机关抓获归案，其到案后如实供述上述犯罪事实。被告人胡凌云的家属已代为赔偿被害单位的经济损失并取得谅解。

为证实上述指控的事实，公诉机关提供了证人刘某 1、冯某、刘某 2 的证言，搜查笔录、照片、扣押决定书、扣押清单，聊天记录截图，上海波克城市网络科技股份有限公司的报案材料及截图，刑事谅解书以及公安机关出具的工作情况等证据。

据此，公诉机关认为被告人胡凌云以谋利为目的，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修改的操作，后果特别严重，其行为已构成破坏计算机信息系统罪,被告人胡凌云到案后如实供述犯罪事实，提请依照《中华人民共和国刑法》第二百八十六条第一款、第二款、第六十七条第三款之规定，对被告人胡凌云予以处罚。

庭审中，被告人胡凌云对起诉书指控的犯罪事实无异议。

辩护人对犯罪事实无异议，但提出被告人胡凌云的行为应认定为非法获取计算机信息系统数据罪，建议对被告人胡凌云减轻处罚并适用缓刑。

经审理查明，2015 年 8 月，被告人胡凌云进入上海波克城市网络科技股份有限公司(以下简称“波克公司”)担任客服人员，后其通过破译他人账户密码，以他人名义登陆“波克公司”开发运营的网络游戏“捕鱼达人 3D”的后台系统，利用他人修改数据的权限更改其指定用户游戏系统中的“游戏金币”数量,并在游戏中通过“游戏金币”的操作获取相关游戏装备，通过网络出售给他人谋利，截止案发，经查证部分销售额达到人民币 38000 余元。

2016 年 8 月 23 日，被告人胡凌云在“波克公司”被公安机关抓获。

以上事实，有下列证据证实：

1、证人刘某 1 的证言，证明其系“波克公司”的员工，2016 年 7 月 25 日，该公司员工冯某向公司反映自己的游戏管理员账号被人盗用，公司查证后发现，冯某的游戏管理员账号自 2015 年 12 月至 2016 年 7 月共私自充值 130 亿游戏币,分多次打入 10 个普通游戏账户，公司发现冯某的账号多次在胡凌云的电脑上登陆并有修改游戏币的操作记录，10 个普通游戏账户绑定的手机号是胡凌云的手机号。“波克公司”的充值方式是通过人民币购买 Q 币，用 Q 币在游戏内转换成游戏币，130 亿游戏币通过正常渠道充值的话需要约人民币 260 万，胡凌云盗用管理员账户、修改账户资料的行为破坏了游戏的平衡性和玩家的游戏体验，给公司的经济及名誉造成很严重的影响。

2、证人冯某的证言，证明其系“波克公司”的员工，2016 年 7 月，其发现有人盗用其员工 ID 登陆游戏后台后，修改部分用户的游戏金币设置，后又查询到是用胡凌云的电脑登陆的，其遂向公司反映情况。其账号被盗用始于 2015 年 12 月，胡凌云当时是其小组的接待专员，胡没有更改游戏设置的权限，只有其有权限。在“捕鱼达人 3D”游戏中，只有拥有了金币才能玩这个游戏，有了金币更容易打出游戏装备，而有了装备才可以打出更多金币。胡凌云的行为破坏了游戏的平衡性,因为公司是基于玩家的游戏体验以及消费情况进行游戏

研发和升级的，同时游戏环节也有玩家共同完成任务的模式，不正常的用户会破坏这种平衡和公平竞争，破坏整个游戏系统的运行和平衡。

3、证人刘某2的证言，证明其系胡凌云的妻子，胡凌云自2016年2月起陆续从支付宝转账给其20余万元，胡凌云称系打游戏赚的钱，现其已赔偿给“波克公司”30万元，得到了公司的谅解。

4、上海市公安局普陀分局搜查笔录、扣押决定书、扣押清单及现场照片，证明2016年8月23日16时10分许，公安人员至胡凌云暂住地进行搜查，查获作案用电脑并依法扣押。

5、聊天记录截图，证明胡凌云通过网络出售游戏装备并获利，仅部分销售额达到人民币38000余元。

6、“波克公司”的报案材料、截图等，证明“波克公司”发现胡凌云使用自己的工作电脑登陆冯某的账号，通过修改数据为胡本人及其亲友增加游戏金币。

7、刑事谅解书，证明案发后胡凌云的家属对“波克公司”进行了赔偿，获得公司的谅解。

8、公安机关出具的工作情况，证明胡凌云的到案情况。

上述证据均由公诉机关提供，经庭审质证，合法、有效，予以确认。

本院认为，被告人胡凌云违反国家规定，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修改，后果特别严重，其行为已构成破坏计算机信息系统罪，依法应予处罚。上海市普陀区人民检察院指控被告人胡凌云的犯罪事实和罪名成立。经查，被告人胡凌云违反国家有关规定，通过破译他人账户密码进入“捕鱼达人3D”的后台系统，利用他人修改后台数据的权限更改其指定用户游戏系统中的“游戏金币”数量，后又通过后续操作获取游戏装备出售牟利，其行为破坏了整个游戏系统的运行和平衡，对被害单位造成严重影响，符合破坏计算机信息系统罪的犯罪构成要件，对辩护人的相关辩护意见不予采纳。被告人胡凌云到案后能如实供述犯罪事实，依法可从轻处罚。案发后，被告人胡凌云的家属已代为赔偿被害单位的经济损失，并取得被害单位的谅解，可对被告人胡凌云酌情从轻处罚。辩护人提出对被告人胡凌云减轻处罚并适用缓刑的辩护意见，不予采纳。公诉机关当庭提出的量刑建议，可予采纳。根据被告人胡凌云的犯罪事实、性质、情节及对社会的危害程度等，依照《中华人民共和国刑法》第二百八十六条第一款、第二款、第六十七条第三款以及《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》第四条之规定，判决如下：

被告人胡凌云犯破坏计算机信息系统罪，判处有期徒刑五年。

(刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2016年8月23日起至2021年8月22日止)。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向上海市第二中

级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本一份。

审 判 长　谢 燕

审 判 员　谭佳怡

人民陪审员　　成 建

二〇一六年十二月二十七日

书 记 员　俞惠清

案例三、吴凯破坏计算机信息系统案

审理法院：　浙江省杭州市中级人民法院

案　　号：　（2016）浙 01 刑终 40 号

案　　由：　破坏计算机信息系统罪

裁判日期：　2016 年 05 月 24 日

浙江省杭州市中级人民法院

刑事判决书

（2016）浙 01 刑终 40 号

原公诉机关杭州市余杭区人民检察院。

上诉人（原审被告人）吴凯，男，1984 年 3 月 3 日出生，汉族，浙江省乐清市人，大学文化，经商，户籍地乐清市。因本案于 2014 年 11 月 10 日被刑事拘留，同年 12 月 16 日被逮捕。现押于杭州市余杭区看守所。

辩护人李健勇，北京市中银（上海）律师事务所律师。

杭州市余杭区人民法院审理杭州市余杭区人民检察院指控被告人吴凯犯破坏计算机信息系统罪一案，于 2015 年 12 月 10 日作出（2015）杭余刑初字第 754 号刑事判决。被告人吴凯不服，提出上诉。本院依法组成合议庭，公开开庭审理了本案。杭州市人民检察院指派检察员蔡某、代理检察员张某出庭执行职务，被告人吴凯及其辩护人李健勇到庭参加诉讼。本案经杭州市人民检察院建议延期审理一次。现已审理终结。

原判认定，2014 年 10 月，被告人吴凯以非法获利为目的，编写 swf 文件后上传至淘宝店铺等相关页面，当淘宝用户登录访问插入该 swf 文件的网页时，该文件能够自动触发，加载其配置文件中的推送数据并在未经用户确认的情况下实现相应的推送商品、优惠券、添加商品或店铺收藏等功能，并将该 swf 文件插入访问者的店铺，以实现自我复制和传播。同年 10 月底至 11 月初，被告人吴凯以网络营销为名，将上述推送功能出售给多个淘宝卖家，非法获利共计 7 万余元。

案发后，侦查机关从被告人吴凯处查获作案工具苹果牌 MacBook 笔记本电脑一台、iphone 手机一部，并冻结了被告人吴凯存于户主姓名为康某的支付宝账户（账号为 18×××10）内的违法所得人民币 20674.39 元。

以上事实有证人谢某、严某、易某、吴某、赖某、冯某、汪某、念小妹、朱某、田某、梁某、石某、潘某、沈某、胡某、伍某的证言，接受证据清单、商品截图，营业执照，个人网上银行凭证、支付宝交易记录，调取证据通知书、阿某计算机有限公司出具的情况说明、分析说明及光盘，远程勘验笔录及光盘，协助冻结财产通知书，扣押笔录、扣押决定书、扣押清单及照片，账户信息、交易明细，抓获、破案经过，户籍证明和被告人吴凯的供述等证据予以证实。

原审法院以破坏计算机信息系统罪，判处被告人吴凯有期徒刑五年三个月，并处罚金人民币 55000 元;扣押于杭州市公安局余杭区分局未随案移送的被告人吴凯的作案工具苹果牌 MacBook 笔记本电脑一台、iphone 手机一部，均予以没收，由杭州市公安局余杭区分局上缴国库；被告人吴凯存于户主姓名为康某的支付宝账户（账号为 18×××10）内的违法所得人民币 20674.39 元，予以追缴，由杭州市公安局余杭区分局上缴国库。

被告人吴凯上诉提出其行为不符合破坏计算机信息系统罪的规定，应以非法控制计算机系统罪定罪。其辩护人提出，一审错误认定刑法第二百八十六条第二款规定的犯罪属于行为犯，超越了罪刑法定原则；吴凯无破坏计算机信息系统的故意；淘宝对本案的发生有重大过错；从技术角度看，本案的程序更像控制计算机系统的程序，而不是破坏性程序，故一审认定的破坏计算机信息系统罪缺乏主观、客观构成要件，宜按照刑事诉讼法第十五条第一款“情节显著轻微、危害不大，不认为是犯罪的”之规定宣告无罪。

出庭检察员提出，（1）原判认定吴凯的行为构成破坏计算机信息系统罪事实清楚，证据确实、充分，定性准确，判处的有期徒刑量刑适当，审判程序合法，但并处罚金于法无据；（2）吴凯提出其行为符合非法控制计算机系统罪、其编写的程序没有造成破坏性后果等上诉理由缺乏事实和法律依据，不能成立，故建议驳回上诉，维持原判事实、定性及主刑部分，对附加刑部分进行纠正。

经审理查明，原判认定事实清楚，证据确实、充分，本院予以确认。

本院认为，上诉人吴凯违反国家规定，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修改、增加的操作，后果特别严重，其行为已构成破坏计算机信息系统罪。原判定罪正确。关于上诉人吴凯及其辩护人对原判定性所提诉辩意见，经审理认为，（1）根据法律规定，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、增加的操作系破坏计算机信息系统的方式之一。（2）上诉人吴凯上传具有推送功能的 swf 文件，对淘宝网信息系统中的数据进行了修改、增加，并非达到控制淘宝网信息系统的目的。（3）淘宝网的公开接口系用于用户正常使用，而上诉人吴凯上传经伪装后的 swf 文件，已侵害计算机信息系统安全这一客体，淘宝网是否有过错并不影响对其定罪，故上诉人吴凯提出其行为不构成破坏计算机信息系统罪及其辩护人提出应宣告吴凯无罪等相关诉辩意见均不能成立，本院不予采纳。原判根据吴凯的犯罪事实、性质、情节在法定量刑幅度裁量的有期徒刑刑罚适当，但对其并处罚金于法无据，本院予以纠正。出庭检察员关于本案的定性、

上诉人吴凯的上诉理由不能成立、原判并处罚金于法无据等相关出庭意见，本院均予以采纳。原审审判程序合法。据此，依照《中华人民共和国刑法》第二百八十六条第一款、第二款、第五十二条、第五十三条第一款、第六十四条以及《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》第四条第一款第（三）项、第二款第（一）项、《最高人民法院关于适用财产刑若干问题的规定》第一条、第二条第一款和《中华人民共和国刑事诉讼法》第二百二十五条第一款第（二）项之规定，判决如下：

一、维持杭州市余杭区人民法院（2015）杭余刑初字第754号刑事判决中对被告人吴凯犯破坏计算机信息系统罪的定罪部分及第二项没收作案工具、第三项追缴违法所得部分。

二、撤销杭州市余杭区人民法院（2015）杭余刑初字第754号刑事判决中对被告人吴凯犯破坏计算机信息系统罪的量刑部分。

三、上诉人（原审被告人）吴凯犯破坏计算机信息系统罪，判处有期徒刑五年三个月（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日。即自2014年11月10日起至2020年2月9日止）。

本判决为终审判决。

审判长　管　波

审判员　徐　洁

代理审判员　蒋科宇

二〇一六年五月二十四日

书记员　陆勋潮

案例四、马志松等破坏计算机信息系统案

审理法院：　江苏省无锡市中级人民法院

案　　由：　破坏计算机信息系统罪

江苏省无锡市中级人民法院

刑事

公诉机关：江苏省无锡市滨湖区人民检察院。

被告人：马志松，男，29岁，无业，住四川省成都市武侯区少陵路，因本案于2008年2月15日被逮捕。

被告人：彭旭，男，31岁，农民，住四川省双流县彭镇福田村，因本案于2008年2月15日被逮捕。

被告人：马志强，男，26岁，无业，住黑龙江省东宁县东宁镇，因本案于2008年2月15日被逮捕。

被告人：柳绪刚，男，23岁，农民，住黑龙江省东宁县东宁镇宏源社区，因本案于2008年2月15日被逮捕。

被告人：唐嵩钧，男，22岁，学生，住浙江省杭州市江干区2号大街，因本案于2008年2月15日被逮捕。

被告人：补勇（曾用名岘勇），男，26岁，无业，住四川省资阳市安岳县岳阳镇解放街，因本案于2008年2月15日被逮捕。

根据《中华人民共和国刑法》第二百八十六条的规定，违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰或者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、增加的操作或者故意制作、传播计算机病毒等破坏性程序，造成计算机信息系统不能正常运行，后果严重的，构成破坏计算机信息系统罪。

行为人违反国家规定，采用干扰的技术手段攻击劫持互联网运营商的公共域名服务器，在域名服务器中添加指令，在大量个人计算机信息系统中植入木马病毒，造成计算机信息系统不能正常运行，后果严重的，应以破坏计算机信息系统罪定罪处罚。

江苏省无锡市滨湖区人民检察院以被告人马志松、彭旭、唐嵩钧、马志强、柳绪刚、补勇犯破坏计算机信息系统罪，向江苏省无锡市滨湖区人民法院提起公诉。

起诉书指控：2007年9月底至11月中旬，被告人马志松、彭旭、马志强、柳绪刚、唐嵩钧、补勇合谋盗取互联网用户的网络游戏账户信息，其利用域名服务器劫持程序攻击劫持了上海市、重庆市、扬州市等10余个省市共计27台域名服务器，造成互联网用户在访问腾讯公司迷你网主页时，被错误指向到马志松等人事先设置于无锡市的携带17种网络游戏木马的服务器上，从而被感染木马病毒。因马志松等人的攻击劫持行为，腾讯公司被迫暂时关闭其迷你网首页，致使腾讯公司迷你网及QQ客户端的计算机信息系统不能正常运行，由此造成腾讯公司直接经济损失达人民币100800元。马志松等人的行为已经构成破坏计算机信息系统罪，请依法予以惩处。

无锡市滨湖区人民法院一审查明：

互联网运营商的公共域名服务器是我国互联网的重要基础设施。域名服务器的作用是对网站和其对应的IP地址进行解析，使互联网用户通过输入网址访问到相应的网站，即域名服务器的解析是互联网用户访问网站的必要步骤。

2007年7月，被告人马志松获悉可以通过劫持域名服务器的方法盗取他人的网络游戏账号信息并掌握了劫持域名服务器的原理，随后，马志松与被告人彭旭一起研究、学习劫持域名服务器的具体方法。同年8月，彭旭按照马志松的要求和思路编写出域名服务器的劫持程序，马志松遂准备采用劫持域名服务器的方法欺骗互联网用户，使域名服务器错误解析从而指向到其设置的携带多种网络游戏木马（一种远程监控软件，用于搜集用户的上网信息及键盘操作，并进行远程传送）的服务器上，以达到盗取用户网络游戏账号信息的目的。同年9月，马志松将上述意图告知被告人补勇、马志强、柳绪刚等人，并由补勇出资人民币4000元，马志强、柳绪刚各出资人民币18000元，用于租用作案用的出租房、电脑以及服务器等。马志强还通过互联网租用了无锡电信大浮IDC机房8台服务器，用于存放由马志松伪造的腾

讯公司迷你网首页和由马志强、柳绪刚收集到的17种用于盗取国内网络游戏账号的木马。2007年10月初，马志松通过网络联系了被告人唐嵩钧，让唐嵩钧为其编写了收集各地域名服务器地址的程序以及优化修改下载的木马程序和编写网页木马的免杀程序，用于劫持域名服务器。

2007年9月底至11月中旬，被告人马志松等人在成都市使用编译好的劫持程序对上海市、重庆市、扬州市等10余个省市共计27台域名服务器实施攻击劫持，造成互联网用户在访问腾讯公司迷你网主页时，被错误指向到马志松等人事先设置于无锡市的携带17种网络游戏木马的服务器上，从而被感染木马病毒。因马志松等人的攻击劫持行为，腾讯公司被迫暂时关闭其迷你网首页，致使腾讯公司迷你网及QQ客户端的计算机信息系统不能正常运行，由此造成腾讯公司直接经济损失达人民币100800元。

上述事实，被告人马志松、彭旭、马志强、柳绪刚、唐嵩钧、补勇在审理过程中均无异议，另有腾讯公司的报案材料，证人王鸿鹏、丁晓亮、蒋勇、王修军、钟胜、李敬、陈慧、章健的证言，广东安证计算机司法鉴定所出具的粤安计司鉴（2008）第14号司法鉴定检验报告书，江苏省公安厅出具的苏公网鉴字（2008）001号电子数据检验鉴定书，江苏省公安厅出具的苏公网鉴字（2008）002号电子数据检验鉴定书，深圳中勤万信会计师事务所出具的审核报告，无锡市公安局网络警察支队制作的电子证据检查工作记录，无锡市公安局出具的案发经过说明等证据予以证明，足以认定。

本案的争议焦点是：公诉机关对于马志松等六名被告人的指控罪名是否成立。

无锡市滨湖区人民法院一审认为：

根据《中华人民共和国刑法》（以下简称刑法）第二百八十六条的规定，违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰或者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、增加的操作或者故意制作、传播计算机病毒等破坏性程序，造成计算机信息系统不能正常运行，后果严重的，构成破坏计算机信息系统罪。本罪侵犯的客体是计算机信息系统的安全。《中华人民共和国计算机信息系统安全保护条例》第三条规定：“计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。”对行为人违反国家规定而对计算机信息系统功能进行破坏后果严重构成犯罪的，应当依法处罚。本罪的客观方面表现为行为人实施了破坏计算机信息系统功能后果严重的行为。计算机信息系统的功能，是指按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索的功用和能力。本罪的行为具体表现为对计算机信息系统的功能进行删除、修改、增加、干扰或者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、增加的操作或者故意制作、传播计算机病毒等破坏程序，使计算机信息系统的功能不能得到正常发挥，从而导致计算机信息系统不能正常运行。构成本罪还要求后果严重。所谓后果严重，一般是指：破坏国家重要计算机信息系统功能的；给国

家、社会、集体、组织或者个人造成较大经济损失的；造成恶劣社会影响的，等等。本罪的主观方面是故意。行为人明知自己所输入的程序或指令等非法行为会导致计算机信息系统不能正常运行的危害结果，仍希望或者放任此种结果发生。

被告人马志松、彭旭、马志强、柳绪刚、唐嵩钧、补勇在域名服务器中添加指令，利用域名服务器劫持程序，对互联网运营商的公共域名服务器进行攻击劫持，构成对计算机信息系统的解析功能的干扰；马志松等人的劫持干扰行为使互联网用户在访问腾讯公司迷你网主页时被错误指向到携带木马的服务器上，使大量客户端计算机信息系统被植入木马病毒，从而不能正常运行，腾讯公司为保护用户利益被迫暂时关闭了其迷你网首页，由此造成腾讯公司迷你网的计算机信息系统亦不能正常运行，且造成腾讯公司直接经济损失 100800 元，后果严重。

综上，被告人马志松、彭旭、马志强、柳绪刚、唐嵩钧、补勇违反国家规定，采用干扰的技术手段攻击劫持互联网运营商的公共域名服务器，在域名服务器中添加指令，在大量个人计算机信息系统中植入木马，造成计算机信息系统不能正常运行，后果严重，其行为均已构成破坏计算机信息系统罪，且系共同犯罪，依法应处五年以下有期徒刑或者拘役。公诉机关指控马志松等六人犯破坏计算机信息系统罪的事实清楚，证据确实、充分，指控的罪名成立，予以采纳。马志松、彭旭、马志强、柳绪刚、唐嵩钧在共同犯罪中起主要作用，系主犯；补勇在共同犯罪中起次要作用，系从犯，应当从轻处罚。关于唐嵩钧的辩护人提出的唐嵩钧系共同犯罪的从犯的辩护意见，与事实不符，不予采纳，但对辩护人提出的唐嵩钧归案后如实供述自己罪行，认罪态度较好，请求对唐嵩钧予以从轻处罚的辩护意见，予以采纳。

据此，无锡市滨湖区人民法院依据刑法第二百八十六条第一款、第二十五条第一款、第二十六条第一款、第二十七条之规定，于 2008 年 9 月 11 日判决：

一、被告人马志松犯破坏计算机信息系统罪，判处有期徒刑四年；

二、被告人彭旭犯破坏计算机信息系统罪，判处有期徒刑三年；

三、被告人马志强犯破坏计算机信息系统罪，判处有期徒刑二年六个月；

四、被告人柳绪刚犯破坏计算机信息系统罪，判处有期徒刑二年六个月；

五、被告人唐嵩钧犯破坏计算机信息系统罪，判处有期徒刑二年；

六、被告人补勇犯破坏计算机信息系统罪，判处有期徒刑一年。

彭旭、柳绪刚均不服一审判决，向无锡市中级人民法院提起上诉。彭旭的上诉理由是：本人未与原审被告人马志松一起研究劫持程序，本案中攻击域名服务器的行为对腾讯公司没有影响。柳绪刚的上诉理由是：本人在共同犯罪中系从犯，应从轻处罚。请求二审法院依法改判。

无锡市中级人民法院经二审，确认了一审查明的事实。

无锡市中级人民法院二审认为：

上诉人彭旭、柳绪刚及一审被告人马志松、马志强、唐嵩钧、补勇违反国家规定，在域

名服务器中添加指令，在大量个人计算机信息系统中植入木马，采用干扰的技术手段造成计算机信息系统不能正常运行，后果严重，其行为均已构成破坏计算机信息系统罪。在共同犯罪中，彭旭、柳绪刚、马志松、马志强、唐嵩钧系主犯，补勇系从犯。

对于上诉人彭旭提出的上诉理由，二审法院认为：1、对于彭旭与一审被告人马志松一起研究公共域名服务器劫持程序的事实，有彭旭本人及马志松的供述予以证实，彭旭在一审庭审时亦明确予以认可，足以认定。2、彭旭等人虽未直接对腾讯公司的所有服务器进行攻击，但其在对域名服务器的劫持过程中，使用挂有木马病毒的伪造的腾讯公司迷你网主页，造成腾讯公司的大量 QQ 用户的计算机信息系统被添加恶意程序，致使腾讯公司为保护 QQ 用户的利益，关闭了相应功能，间接侵害了腾讯公司的利益。综上，彭旭提出的上诉理由均不能成立，不予采纳。

对于上诉人柳绪刚提出的上诉理由，二审法院认为：柳绪刚在获悉一审被告人马志松等人可以通过劫持域名服务器的方式获取计算机用户的网络游戏账户信息后，纠集一审被告人马志强一同前往成都，并与马志强分别出资 1.8 万元，用于购买劫持公共域名服务器所必需的设备等，使马志松等人攻击劫持域名服务器的一系列犯罪行为得逞。同时，柳绪刚提供给马志松的木马程序直接侵入了大量个人计算机信息系统。据此可以认定柳绪刚在本案共同犯罪中系主犯。综上，柳绪刚提出的上诉理由不能成立，不予采纳。

综上，一审判决认定事实清楚，证据确实、充分，适用法律正确，定罪量刑适当，审判程序合法，应予维持。无锡市中级人民法院依据《中华人民共和国刑事诉讼法》第一百八十九条第（一）项之规定，于 2008 年 10 月 30 日裁定：

驳回上诉，维持原判。

本裁定为终审裁定。

案例五、吕薛文破坏计算机信息系统案

审理法院：　广东省广州市中级人民法院

案　　由：　破坏计算机信息系统罪

广东省广州市中级人民法院

刑事

被告人：吕薛文，男，25 岁，广东省广州市人，高中文化，无业，1998 年 5 月 5 日被逮捕。

辩护人：李智波、廖时飞，广东环宇商务律师事务所律师。

广东省广州市人民检察院以被告人吕薛文犯破坏计算机信息系统罪，向广州市中级人民法院提起公诉。

起诉书指控：被告人吕薛文入侵中国公众多媒体通信网广州主机（以下简称广州主机）和蓝天 BBS 主机，进行修改、增加、删除等一系列非法操作，其行为已触犯《中华人民共和

国刑法》第二百八十六条第一、二款的规定，构成破坏计算机信息系统罪，请依法判处。

被告人吕薛文当庭辩称：我修改广州主机的root（最高权限）密码，是经过该主机的网管员同意的，不是非法修改。我入侵广州主机和蓝天主机，目的是要尝试进入别人主机的方法是否可行，从中学习如何保障网络安全，并非从事破坏活动。

吕薛文的辩护人称：被告人吕薛文没有对计算机信息系统的功能、数据和应用程序进行破坏，其入侵行为没有使计算机信息系统无法正常运行，没有产生严重后果，起诉书指控的罪名不能成立，应当宣告吕薛文无罪。

广州市中级人民法院经审理查明：

1997年4月间，被告人吕薛文加入国内黑客组织。1998年1至2月间，吕薛文使用自己的手提电脑，盗用邹某、王某、何某、朱某的帐号和使用另外两个非法帐号，分别在广东省中山图书馆多媒体阅览室及自己家中登录上网，利用从互联网上获取的方法攻击广州主机。在成功入侵该主机系统并取得最高权限后，吕薛文非法开设了两个具有最高权限的帐号和一个普通用户帐号，以便长期占有该主机系统的控制权。期间，吕薛文于2月2日至27日多次利用gzlittle帐号上网入侵广州主机，对该主机系统的部分文件进行修改、增加、删除等一系列操作，非法开设了gzfifa、gzmicro、gzasia三个帐号送给袁某（另案处理）使用，并非法安装和调试网络安全监测软件，未遂。2月25日、26日，吕薛文先后3次非法修改广州主机系统的root密码，致使该主机系统最高权限密码3次失效，造成该主机系统管理失控约15个小时。当广州主机网管员第一次发现使用自己设置的root密码无法进入主机的超级用户状态对主机进行管理时，吕薛文上网主动要求与网管员对话，询问网管员是否将密码丢失了，声称他能将密码修改回来。当网管员询问其是否将网管员设置的密码修改了时，吕薛文矢口否认。在此情况下，网管员为能进入并操作主机，只得同意吕薛文“帮助”他将密码修改回来。吕薛文随即将root密码已经改为root123密码一事通知了网管员。网管员经试验root123密码可用后，为安全起见，又把root123设置为另一密码。但是网管员随后即发现，他刚改过的这一密码，又被改回为只有吕薛文和网管员知道的root123密码。2月26日下午，广州主机采取了封闭普通用户登录进入该主机的措施后，只有吕薛文仍能以非法手段登录进入，期间该主机的root密码第三次失效，吕薛文再次主动与网管员交谈，虽然仍否认自己修改了主机的密码，但是将能够进入主机的新root密码告诉了网管员。吕薛文实施了入侵行为后，把其使用的帐号记录删除，还将拨号信息文件中的上网电话号码改为12345678或00000000，以掩盖其入侵行为。

此外，1998年2月12日，被告人吕薛文还利用.Lss程序和所获得的密码对蓝天BBS主机进行攻击，在取得该主机的最高权限后提升LP帐号为最高权限用户帐号，以便长期取得该主机的最高权限。

上述事实，有吕薛文的作案工具等物证，作案地点的照片和通信记录、文件记录等书证以及鉴定结论、证人证言等证据证实。

广州市中级人民法院认为：

伴随着计算机信息系统不断深入社会生活的各个领域，针对计算机信息系统的犯罪也逐渐增多，成为社会不安定的一种因素。依法惩治这类犯罪活动，已成为刑法的一项重要任务。

国务院 1994 年 2 月 18 日发布的《中华人民共和国计算机信息系统安全保护条例》第七条规定："任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。"被告人吕薛文违反这一规定，利用其掌握的知识入侵广州主机、蓝天 BBS 主机信息系统，取得控制该系统的最高权限，实施了增设最高权限的帐户和普通帐户，对广州主机存储、处理和传输的数据进行删改、监测，3 次修改广州主机的最高权限密码等 3 种破坏行为。

《中华人民共和国刑法》第二百八十六条第一款规定："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。"第二款规定："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。"计算机信息系统上的帐号和密码，是以数据形式表现出来的计算机信息系统功能的一部分。被告人吕薛文对计算机信息系统上的帐号和密码进行修改、增加，其行为触犯了刑法第二百八十六条第一款的规定。而吕薛文在广州主机系统中安装并调试网络安全监测软件，则是对计算机信息系统中存储、处理或者传输的应用程序进行删除、修改、增加的操作，其行为触犯了第二百八十六条第二款的规定。吕薛文的行为已经危害了计算机信息系统的安全，造成广州主机管理失控、不能正常运行的严重后果，构成破坏计算机信息系统罪，应当依法处以刑罚；对其用于犯罪的本人财物，应当依照刑法第六十四条的规定，予以没收上缴国库。

被告人吕薛文入侵广州主机后，成为该主机除网管员以外唯一获得最高权限的人。尽管吕薛文矢口否认私自修改过广州主机的 root 密码，但是在网管员将吕薛文告诉他的 root123 密码设置为另一密码，而他设置的这一密码随即就被改回为只有他和吕薛文才知道的 root123 密码，这一情节足以证实修改密码的人不能是其他人，只能是吕薛文。

被告人吕薛文掌握并修改了广州主机的密码，致使网管员也不能进入主机系统进行管理工作。在此情况下，吕薛文将自己修改的密码告诉网管员，使网管员能够继续操作主机。这一行为只是减轻了犯罪的危害后果，不能改变行为的犯罪本质，更不是为网管员提供帮助。

无论出于何种目的，非法进入计算机信息系统进行删除、修改等操作，致使计算机信息系统不能正常运行，造成严重后果的，都是刑法规定的犯罪行为。被告人吕薛文及其辩护人关于修改密码是经网管员同意的，进入信息系统是为了学习，且没有破坏该信息系统，行为不构成犯罪的意见，不能成立。

综上，广州市中级人民法院于 1999 年 8 月 19 日判决：

一、被告人吕薛文犯破坏计算机信息系统罪，判处有期徒刑一年六个月；

二、缴获被告人吕薛文作案用的手提电脑1台，予以没收上缴国库。

一审宣判后，被告人吕薛文没有上诉，人民检察院也没有抗诉。

（五）帮助信息网络犯罪活动罪

案例一、周道鹏、宁志杰诈骗罪、王银珍妨害信用卡管理罪、王锋犯帮助信息网络犯罪活动罪、朱曰军、潘锦业、廖正鑫、张宗宏、廖洁犯非法经营案

吉林省四平市铁东区人民法院刑事判决书

案号：（2019）吉0303刑初182号

公诉机关吉林省四平市铁东区人民检察院。

被告人周道鹏，男，1995年1月1日出生，汉族，海南省海口市人，小学文化，无业，户籍所在地海口市琼山区，现住海口市龙华区。因犯贩卖毒品罪于2012年9月26日被海南省定安县人民法院判处拘役5个月，因犯贩卖毒品罪于2013年7月12日被海南省定安县人民法院判处有期徒刑八个月，于2013年12月27日刑满释放。因涉嫌诈骗，于2018年12月1日被四平市公安局铁东区分局刑事拘留。因涉嫌犯诈骗罪，经四平市铁东区人民检察院批准，于2019年1月4日被四平市公安局铁东区分局执行逮捕。现羁押于四平市看守所。

辩护人杨桂清，北京市京师（长春）律师事务所律师。

辩护人盛晓丽，北京市京师（长春）律师事务所实习律师。

被告人宁志杰，男，1987年2月16日出生，汉族，河北省邯郸市人，高中文化，无业，户籍所在地邯郸市大名县，现住河北省石家庄市裕华区。因涉嫌诈骗，于2018年12月25日被四平市公安局铁东区分局刑事拘留。因涉嫌犯诈骗罪，经四平市铁东区人民检察院批准，于2019年1月4日被四平市公安局铁东区分局执行逮捕。现羁押于四平市看守所。

被告人王银珍，女，1973年3月3日出生，汉族，湖北省监利县人，文盲，无业，户籍所在地监利县，现住海南省海口市龙华区。因涉嫌诈骗，于2018年12月1日被四平市公安局铁东区分局刑事拘留。因涉嫌犯妨害信用卡管理罪，经四平市铁东区人民检察院批准，于2019年1月4日被四平市公安局铁东区分局执行逮捕。现羁押于四平市看守所。

被告人王锋，男，1980年10月9日出生，汉族，陕西省合阳县人，高中文化，无业，户籍所在地合阳县，现住陕西省西安市新城区。因涉嫌诈骗，于2018年11月28日被四平市公安局铁东区分局刑事拘留。因涉嫌犯开设赌场罪，经四平市铁东区人民检察院批准，于2019年1月4日被四平市公安局铁东区分局执行逮捕。现羁押于四平市看守所。

辩护人刘彬，吉林睿智律师事务所律师。

被告人朱曰军，男，1991年4月12日出生，汉族，江苏省建湖县人，中专文化，无业，户籍所在地建湖县，现住建湖县。因涉嫌诈骗，于2018年12月1日被四平市公安局铁东区分局刑事拘留。因涉嫌犯开设赌场罪，经四平市铁东区人民检察院批准，于2019年1月4日被四平市公安局铁东区分局执行逮捕。现羁押于四平市看守所。

辩护人李阿凛，吉林辅民律师事务所律师。

被告人潘锦业，男，1989 年 12 月 22 日出生，汉族，上海市杨浦区人，大学文化，无业，户籍所在地上海市杨浦区，现住上海市宝山区。因涉嫌诈骗，于 2018 年 12 月 1 日被四平市公安局铁东区分局刑事拘留。因涉嫌犯开设赌场罪，经四平市铁东区人民检察院批准，于 2019 年 1 月 4 日被四平市公安局铁东区分局执行逮捕。现羁押于四平市看守所。

辩护人周军，吉林东泰律师事务所律师。

被告人廖正鑫，男，1991 年 12 月 17 日出生，汉族，江苏省建湖县人，中专文化，无业，户籍所在地建湖县，现住址同上。因涉嫌诈骗，于 2018 年 12 月 1 日被四平市公安局铁东区分局刑事拘留。因涉嫌犯开设赌场罪，经四平市铁东区人民检察院批准，于 2019 年 1 月 4 日被四平市公安局铁东区分局执行逮捕。现羁押于四平市看守所。

辩护人赵德刚，吉林吉鼎律师事务所律师。

被告人张宗宏，男，1991 年 11 月 21 日出生，汉族，云南省宣威市人，初中文化，无业，户籍所在地宣威市，现住址同上。因涉嫌诈骗，于 2018 年 12 月 1 日被四平市公安局铁东区分局刑事拘留。因涉嫌犯开设赌场罪，经四平市铁东区人民检察院批准，于 2019 年 1 月 4 日被四平市公安局铁东区分局执行逮捕。现羁押于四平市看守所。

辩护人宋春晖，吉林辅民律师事务所律师。

被告人廖洁，男，1989 年 6 月 28 日出生，汉族，江苏省建湖县人，初中文化，无职业，户籍所在地建湖县，现住址同上。因涉嫌诈骗，于 2018 年 12 月 1 日被四平市公安局铁东区分局刑事拘留。因涉嫌犯开设赌场罪，经四平市铁东区人民检察院批准，于 2019 年 1 月 4 日被四平市公安局铁东区分局执行逮捕。现羁押于四平市看守所。

吉林省四平市铁东区人民检察院以四东检刑检刑诉[2019]136 号起诉书指控被告人周道鹏、宁志杰犯诈骗罪、王银珍犯妨害信用卡管理罪、王锋犯帮助信息网络犯罪活动罪、朱曰军、潘锦业、廖正鑫、张宗宏、廖洁犯非法经营罪一案，于 2019 年 9 月 4 日向本院提起公诉。本院受理后，依法组成合议庭，公开开庭审理了本案。

2019 年 11 月 12 日吉林省四平市铁东区人民检察院建议延期审理，本院于 2019 年 12 月 11 日恢复审理。

吉林省四平市铁东区人民检察院指派检察员张树森、刘国宏、赵春出庭支持公诉，被告人周道鹏及其辩护人杨桂清、被告人宁志杰、王银珍、被告人王锋及其辩护人刘彬、被告人朱曰军及其辩护人李阿凛、被告人潘锦业及其辩护人周军、被告人廖正鑫及其辩护人赵德刚、被告人张宗宏及其辩护人宋春晖、被告人廖洁到庭参加诉讼。

本案现已审理终结。

公诉机关指控:被告人王银珍于 2017 年 5 月 23 日，冒用“吴某 1”的身份信息在海南省海口市中国邮政储蓄银行股份有限公司海口市文明东支行骗领邮政储蓄信用卡一张（卡号×××），并连同开卡人“吴某 1”身份证复印件及已办理手机支付宝业务的手机卡（号码

155XXXXXXXX），以人民币 2000 元价格，在海口市南大桥附近，明知被告人周道鹏用于违法犯罪活动而向其售卖。被告人周道鹏于 2018 年年初，通过网络以人民币 2000 元价格购买被告人宁志杰自行搭建的虚假彩票平台。宁志杰明知该平台为无开奖中奖功能，并可进行后台充值数据改写而向周道鹏出售并提供后期技术支持及维护。

被告人周道鹏利用在王银珍处购买的身份信息在“新葡京赌场”网络赌博网站开设账号，取得支付宝二维码，并通过 QQ 号码“×××”、昵称“稳赚计划”在微信群、QQ 群发送零风险、高收益的彩票稳赚广告，吸引他人在虚假的彩票平台上注册账号，通过扫支付宝二维码进行投注，后通过改动账号余额，骗被害人中奖，需解冻再次注入资金的方式于 2018 年 7 月 20 日、21 日骗取被害人杨某人民币 25000 元，周道鹏利用在“新葡京赌场”网络赌博网站开设账号将骗取的钱款提现取出。

被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁等人于 2018 年 6 月至 11 月间，在上海、江苏等地为“新葡京赌场”等网络平台提供非法资金支付结算，通过支付宝非法进行资金流转，并按比例收取提成或领取工资报酬，其操作资金流水量均达到 500 万元以上。

其中朱曰军、潘锦业、廖正鑫为各小组负责人。

经统计:朱曰军非法从事资金支付的数额为人民币 51141903 元，非法获利人民币 4 万元；潘锦业非法从事资金支付的数额为人民币 27810915.17 元，非法获利人民币 12 万元；廖正鑫非法从事资金支付的数额为人民币 17733146.16 元，非法获利人民币 15 万元；张宗宏非法从事资金支付的数额为 10045496.56 元，非法获利人民币 4 万元；廖洁非法从事资金支付的数额为人民币 7978897.74 元，非法获利人民币 27600 元。

被告人王锋于 2018 年 9 月，明知他人利用信息网络实施犯罪，而向其出售 API 接口使用权并提供技术支持，非法获利人民币 100 余万元。

公诉机关指控上述犯罪事实所列举的证据有:被告人周道鹏、宁志杰、王银珍、王锋、朱曰军、潘锦业、廖正鑫、张宗宏、廖洁的供述与辩解;被害人杨某的陈述;证人吴某 1、朱某 1、祁某、陈某 1、戴某 1、戴某 2、徐某、吴某 2、郭某等的证言;发破案经过、抓获经过、到案经过、户籍证明、情况说明、信用卡申请手续、被害人支付宝交易信息情况、赌博网站网络界面截图、聊天记录截图、银行卡交易明细、扣押决定书、扣押清单、寄押凭证、在逃人员登记表、支付宝流水统计、记账本、辩认笔录；电子数据勘验检查笔录、远程数据提取记录；电子数据 U 盘。

公诉机关认为，被告人周道鹏利用电信网络诈骗他人财物，数额较大，其行为触犯了《中华人民共和国刑法》第二百六十六条　之规定，构成诈骗罪。

被告人宁志杰，明知他人实施电信网络诈骗而为其提供技术支持，构成诈骗罪共犯。

被告人王银珍使用虚假的身份证明骗领信用卡，其行为触犯《中华人民共和国刑法》第一百七十七条　之规定，构成妨害信用卡管理罪。

被告人王锋明知他人利用信息网络实施犯罪，为其犯罪提供技术支持，情节严重，其行

为触犯了《中华人民共和国刑法》第二百八十七条　之规定，构成帮助信息网络犯罪活动罪。

被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁未经国家有关部门批准，非法从事资金支付结算业务，情节严重，其行为触犯了《中华人民共和国刑法》第二百二十五条　之规定，构成非法经营罪。

本案犯罪事实清楚，证据确实、充分，应当以诈骗罪追究被告人周道鹏、宁志杰的刑事责任；以妨害信用卡管理罪追究被告人王银珍的刑事责任；以帮助信息网络犯罪活动罪追究被告人王锋的刑事责任；以非法经营罪追究被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁的刑事责任。

被告人周道鹏曾因故意犯罪被判处有期徒刑，刑罚执行完毕后五年内又犯应当判处有期徒刑以上刑罚之罪，系累犯，应依据《中华人民共和国刑法》第六十五条　之规定予以处罚。

被告人周道鹏对公诉机关指控其犯诈骗罪无异议，当庭表示认罪。

被告人周道鹏辩护人的辩护意见是:被告人周道鹏在侦查阶段以及庭审中均表示认罪，并且如实供述自己的罪行，构成坦白。

另被告人周道鹏积极赔偿被害人经济损失 2 万元并取得被害人谅解，其主观恶性以及社会危害性相对较小，建议法庭从轻处罚。

被告人宁志杰对公诉机关指控其是诈骗罪的共犯无异议，当庭表示认罪。

被告人王银珍对公诉机关指控其犯妨害信用卡管理罪无异议，当庭表示认罪。

被告人王锋对公诉机关指控其犯帮助信息网络犯罪活动罪无异议，当庭表示认罪。

被告人王锋辩护人的辩护意见是:在帮助信息网络犯罪活动罪中童镇、周辉、王锋是共同犯罪，在整个犯罪过程中王锋仅起到次要作用，构成从犯；王锋积极退赃，到案后如实供述自己的罪行，且系初犯、偶犯，请求从轻处罚。

被告人朱曰军对公诉机关指控其犯非法经营罪无异议，但认为其流水转账金额应为 2200 万元左右，对获利数额没有异议。

被告人朱曰军辩护人的辩护意见是:朱曰军是陆侃军介绍并为陆侃军工作，受陆侃军指挥和调遣，故构成从犯，应从轻或减轻处罚。

另朱曰军的犯罪数额应以其自认的账本记载的 2200 万元为准，朱曰军主动交代犯罪事实，主观恶性较小，社会危害性不大，建议从轻处罚。

被告人潘锦业对公诉机关指控其犯非法经营罪无异议，但认为其流水转账金额应为 1700 万元左右，获利数额应为 4-5 万元。

被告人潘锦业辩护人的辩护意见是:从现有证据来看，潘锦业的犯罪行为在共同犯罪中应认定为从犯，依法应减轻处罚；潘锦业到案后如实交待自己的行为，当庭自愿认罪，构成坦白，另被告人犯罪时间较短，主观恶性较小，又是初犯，建议法庭从轻处罚。

被告人廖正鑫对公诉机关指控其犯非法经营罪无异议，当庭表示认罪。

被告人廖正鑫辩护人的辩护意见是:被告人廖正鑫在犯罪活动中的作用较小，主观恶性不深，其自愿认罪，建议法庭从轻处罚。

被告人张宗宏对公诉机关指控其犯非法经营罪无异议，但对其流水转账金额有异议，对获利数额无异议。

被告人张宗宏辩护人的辩护意见是:被告人张宗宏自愿认罪，犯罪地位也属于从犯，另其犯罪金额应为500余万元，建议法庭综合被告人的各种量刑情节公平公正处罚。

被告人廖洁对公诉机关指控其犯非法经营罪无异议，当庭表示认罪。

经审理查明，2017年5月23日，被告人王银珍冒用“吴某1”的身份信息在海南省海口市中国邮政储蓄银行股份有限公司海口市文明东支行骗领邮政储蓄信用卡一张（卡号×××），并连同开卡人“吴某1”身份证复印件及已办理手机支付宝业务的手机卡（号码155XXXXXXXX），以人民币2000元价格，在海口市南大桥附近，明知被告人周道鹏用于违法犯罪活动而向其售卖。

2018年年初，被告人周道鹏通过网络以人民币2000元价格购买被告人宁志杰自行搭建的虚假彩票平台。

宁志杰明知该平台为无开奖中奖功能，并可进行后台充值数据改写而向周道鹏出售并提供后期技术支持及维护。

被告人周道鹏利用在王银珍处购买的身份信息在“新葡京赌场”网络赌博网站开设账号，取得支付宝二维码，并通过QQ号码“×××”、昵称“稳赚计划”在微信群、QQ群发送零风险、高收益的彩票稳赚广告，吸引他人在虚假的彩票平台上注册账号，通过扫支付宝二维码进行投注，后通过改动账号余额，骗被害人中奖后需解冻再次注入资金的方式于2018年7月20日、21日骗取被害人杨某人民币25000元。

周道鹏利用在“新葡京赌场”网络赌博网站开设账号将骗取的钱款提现取出。

案发后，被告人周道鹏退赔受害人杨某人民币2万元并取得谅解。

2018年6月至11月，被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁等人在上海、江苏等地为“新葡京赌场”等网络平台提供非法资金支付结算，通过支付宝非法进行资金流转，并按比例收取提成或领取工资报酬，其操作资金流水量均达到500万元以上。

其中朱曰军、潘锦业、廖正鑫为各小组负责人。

经统计:朱曰军非法从事资金支付的数额为人民币51141903元，非法获利人民币4万元；潘锦业非法从事资金支付的数额为人民币27810915.17元，非法获利人民币4万元；廖正鑫非法从事资金支付的数额为人民币17733146.16元，非法获利人民币8万元；张宗宏非法从事资金支付的数额为10045496.56元，非法获利人民币4万元；廖洁非法从事资金支付的数额为人民币7978897.74元，非法获利人民币27600元。

2018年9月，被告人王锋明知他人利用信息网络实施犯罪，而向其出售API接口使用

权并提供技术支持，非法获利人民币100万元。

公安机关在办案过程中扣押的2096320元、冻结的6911625.29元系被告人朱曰军、潘锦业、廖正鑫、张宗宏等人从事资金结算的一部分，均为赌场赌资；扣押的454885元、冻结的242422.68元系被告人王锋的个人违法所得。

上述扣押、冻结的资金总计为9705252.97元。

上述事实，有在开庭审理中举证、质证的下列证据予以证明:

1、户籍信息。

证明:各被告人的姓名、出生日期、身份证号码、民族、户籍地等情况。

2、接警登记表、立案决定书。

证明:公安机关接到杨某报警称被诈骗，公安机关对此案立案侦查，后对廖正鑫等人立案侦查。

3、发破案经过，抓获经过、到案经过。

证明:2018年7月21日，杨某报警称其在网上被骗30900元。

公安机关通过对被骗资金流进行梳理，发现该笔资金流经三方平台进入新葡京赌博网站，并陆续发现周道鹏、宁志杰、王银珍、王锋、朱曰军、潘锦业、廖正鑫、张宗宏、廖洁的各项违法行为。

公安机关通过侦查，于2018年11月22日，在海口市将周道鹏抓获；于2018年12月24日，在河北省将宁志杰抓获；于2018年11月24日，在海口市将王银珍抓获；于2018年11月25日，在西安市将王锋抓获；于2018年11月26日，在江苏省将朱曰军抓获；于2018年11月26日，在上海市将潘锦业抓获；于2018年11月26日，在上海市将廖正鑫抓获；于2018年11月25日，在江苏省将张宗宏抓获；于2018年11月25日，在上海市将廖洁抓获。

4、辨认笔录。

证明:廖正鑫辨认姜基祥、朱曰军辨认陆侃军的经过。

5、在逃人员登记表、情况说明。

证明:姜基祥、陆侃军被公安机关列为网上逃犯。

6、支付宝流水及统计表、账本、银行流水。

证明:各被告人的转账流水记录。

7、情况说明。

证明:潘锦业的流水资金统计包含组员戴某2、戴某1、徐某、张宗宏的；廖正鑫的流水资金统计包含组员姜某1、廖洁的；朱曰军的流水资金统计包含陈某1、祁某、朱某1的。

8、情况说明、开户信息、银行交易明细、聊天记录。

证明:公安机关经调查发现杨某被骗的资金最终进入开户人吴某1的银行账号。

9、微信交易记录、银行流水、支付宝转账信息。

证明:参赌人员廖某、付某、冯某、唐某、夏某、孟某、余某、张某1、郑某1、朱某2、耿某、李某、施某、姚某、姜某2、王某、隋某、于某、郑某2、林某、曹某1、苏某、张某2、蔡某使用支付宝扫码投注赌博网站的情况。

10、扣押决定书、扣押清单。

证明:公安机关依法扣押被告人潘锦业、张宗宏、廖洁的作案工具。

11、情况说明。

证明:公安机关在朱曰军车内搜出8本账本，其中7本为给商户转账金额的账本，另一本为总转账金额的账本，这8本账本记载的数字均是直付平台转账的金额，记录人为朱某1、陈某1、祁某，记账中A代表万，多少A即为多少万，经统计2018年8月11日至20日平台共转账22450121.1元，其中朱某1为平台转账6872210元，陈某1、祁某共为平台转账15577911.1元；

12、情况说明、扣押决定书、扣押清单、扣押财物票据、协助冻结通知书。

证明:公安机关在办案过程中扣押的2096320元、冻结的6911625.29元系被告人朱曰军、潘锦业、廖正鑫、张宗宏等人从事资金结算的一部分，均为赌场赌资；扣押的454885元、冻结的242422.68元系被告人王锋的个人违法所得，扣押、冻结的资金总计为9705252.97元。

其中扣押、冻结的三笔涉案资金2096320元、436601.47元、727745元已上交到四平市财政局。

13、远程数据提取工作记录。

证明:公安机关依法提取涉案网站的相关信息。

14、电子数据勘验检查笔录、U盘。

证明:公安机关依法提取犯罪工具中的电子信息。

15、羁押手续、情况说明。

证明:周道鹏于2018年11月23日被寄押在海口市看守所；被告人王银珍于2018年11月24日被寄押在海口市看守所；王锋于2018年11月25日被寄押在西安市的看守所；朱曰军于2018年11月26日被寄押在建湖县看守所；潘锦业、廖正鑫、张宗宏、廖洁于2018年11月25日被寄押在上海市的看守所。

16、刑事判决书、释放证明。

证明:被告人周道鹏因犯贩卖毒品罪于2012年9月26日被海南省定安县人民法院判处拘役5个月;因犯贩卖毒品罪于2013年7月12日被海南省定安县人民法院判处有期徒刑八个月，并于2013年12月27日刑满释放。

17、情况说明、违法犯罪记录查询单。

证明:被告人周道鹏有违法犯罪记录，其他被告人无违法犯罪记录。

18、谅解书、收条。

证明:2019年11月6日被告人周道鹏退赔被害人杨某人民币2万元并取得被害人谅解。

19、被害人杨某陈述:2018年7月17日，有人在微信上加我说带我赚钱。

7月20日，我按照这个人的指导登录了一个网站并进行注册，充值了5000元并绑定银行卡，之后我看到账户余额为3万元，我准备提现对方又让我交3万元保证金，7月21日早上那个人说他帮我充了1万元保证金，让我再充2万元就行，我就又往这个账号充了2万元保证金，晚上那个人告诉我钱都输没了，我一共被骗2.5万元。

7月21日我又加了一个好友，以同样的方式被骗5900元。

我通过我的支付宝账号×××扫码给对方转了9次钱。

我和对方都是通过qq联系的。

对方发给我的网址是http//dh.ec123.com.cn/,我注册的账户名是guanhua521。

20、证人朱某1证言:2018年7月25日至8月9日，我在朱曰军的直付平台工作。

朱曰军是我们的小组长。

我和朱曰军负责白班，祁某和陈某1负责晚班。

朱曰军给我开了3000多元工资。

我们的交易流水平均每天七八十万元左右。

21、证人戴某1证言:2018年11月1日，我在直付平台工作，干了25天左右。

潘锦业是我们的小组长，他也是从2018年11月1日开始干的。

我和戴某2给潘锦业提供了10多个支付宝账号、银行卡、手机号。

戴某2和徐某负责白班，我和张宗宏负责晚班。

白班交易流水300万元左右，晚班交易流水100万元左右。

22、证人姜某1证言:我在直付平台工作过三次，时间分别是2018年7月30日左右干了15天、10月2日至10月29日、11月13日至11月25日，这三次廖正鑫都是组长，第一次有廖洁等人，第二次有张宗宏等人，第三次是我和廖洁，这三次我都是负责白班，廖正鑫负责处理出现的问题，有时也跟我们一起操作转账业务。

我们的资金交易流水每天从几十万元到几百万元不等。

我一共得到1万多元工资。

23、证人郭某证言:我干直付工作。

各级代理通过skype软件把支付宝账号发给我，我把账号录入到直付平台，之后他们通过支付宝转钱，在平台上我能看到每个代理的转账金额，第二天凌晨我根据代理转账金额扣除1.8%的费用后把钱返给代理，之后总部再按每天流水量的千分之三利润给代理钱。

我每个月挣1万元。

廖正鑫、潘锦业是代理，平台上的商户由廖正鑫负责。

24、证人戴某2证言:2018年11月3日我开始在直付平台工作，干了22天左右。

潘锦业是我们的小组长，开始我和戴某1与潘锦业商量合伙从事直付平台工作，净利润

各分一半。

我和戴某1给潘锦业提供了10多个支付宝账号、银行卡、手机号，张宗宏和潘锦业都是2018年11月3日从事这项工作的。

我们分白晚班干活，我和徐某是白班，戴某1和张宗宏是晚班。

我们的交易流水开始时是几十万元，后期达到400万元左右。

25、证人祁某证言:2018年7月，陈某1介绍我一个平台转账的工作，之后我到朱曰军那，这是朱曰军组织的，他弄来一些支付宝和银行卡，通过转账收取手续费，我猜就是为了把赌博网站的钱给弄出来。

平台每天转账的金额大约150万元左右，我干了20多天，朱曰军欠平台钱就没有给我开工资。

26、证人徐某证言:2018年10月，潘锦业介绍我用个人支付宝给商家提供支付渠道，从中赚手续费。

2018年11月11日我到江苏昆山找潘锦业、张宗宏等人教我操作流程。

潘锦业负责管理我们，我和戴某2负责白班，张宗宏和戴某1负责晚班。

我总共得到1万元左右的工资。

27、证人许某证言:我姨夫王跃民介绍我到潘锦业那工作。

2018年11月24日下午我找到潘锦业，他带我到建行和移动营业厅办理了一张银行卡和手机卡，之后我就把两张卡给他了。

潘锦业带我到出租屋，屋里有四个人，白班、晚班各两人，他们好像是按照聊天内容用支付宝和银行卡提现、转账。

我在现场看到20多部手机、银行卡。

第二天我就被带到派出所了。

28、证人陈某1证言:2018年7月1日至27日，我正式在朱曰军的直付平台工作。

朱曰军是组长，朱曰军和朱某1负责白班工作，我和祁某负责晚班工作。

朱曰军一共给我开了1万多元工资。

我们的资金交易流水每天二、三百万元。

29、证人吴某2证言:2018年6月，郭某给我介绍个工作，就是在网络平台上帮人添加支付宝账号，并在平台添加点数。

我从2018年6月至11月一共获利2.5万元。

30、证人吴某1证言:我没办理过邮政银行卡，办理银行卡的申请手续上的内容不是我签的，2016年我的身份证丢失过，我办理过挂失登记。

31、证人叶某1证言:我的银行卡被公安冻结了。

这张卡以前我在赌博网站充值绑定过。

32、证人廖某、付某、谢某、冯某、唐某、夏某、孟某、余某、张某1、郑某1、朱某

2、耿某、李某、施某、姚某、姜某2、王某、隋某、于某、郑某2、林某、曹某1、苏某、张某2、蔡某的证言:以上证人均用银行卡、手机号绑定支付宝，通过扫码的形式在赌博网站投注、提现参与赌博。

33、证人江某证言:我名下有6张银行卡，2018年7月我办完民生、农业、中国银行卡后就丢失了，没有使用过。

我没有向卡里存过钱，办卡是用来交罚款和发工资的，公安机关冻结这三张卡里的钱不是我存的。

34、证人周某证言:我名下有7张银行卡，其中尾号是0515的建行卡、尾号是0019的工行卡于2018年6月被我卖给QQ好友了，我没有向这两张银行卡存过钱，现在这两张卡里的钱也不是我的。

35、证人毛某证言:2018年3月我办了一张尾号是3962的建行卡，办完后我一次都没用就借给程小军了，现在卡里的钱不是我的。

36、证人陈某2证言:2014年我办理过一张尾号是5956的邮政卡，卡里现在有53174元，是我在赌博网站赢的赌资。

37、证人曹某2证言:我办理过一张尾号是3352的工行卡，办卡后我把卡借给朋友了，当时卡里没有余额，现在卡里的钱不是我的。

38、证人叶某2证言:我名下有4张银行卡，分别是民生银行卡（尾号是6149）、建行卡（尾号是7385）、徽商银行卡（尾号是8723）、邮政卡（尾号是1096），这四张卡一直是我本人使用，没有转借或售卖过，这4张卡我用于开彩票店的交易和帮别人使用POS机套现以及参与赌博网站充值和提现，其中建行卡和邮政卡是用于赌博时充值提现的。

39、被告人周道鹏供述:我在海口市南大桥附近从一个中年妇女手中花2000元买了银行卡（名为“吴某1”）、手机卡（155XXXXXXXX），并用该信息绑定了支付宝，然后我在网上通过昵称为“爱你呦”的qq号买了一个名为“明发娱乐城”的网站，通过支付宝给对方2500元购买网站的费用，后期大约每个月给对方1300元的网站维护费。

之后我在qq里发广告，让受害人往“明发娱乐城”充钱，我带着他们赚钱，等对方把钱充进来，我就修改网站里对方账户的金额让对方以为赚了，当时这个账户的金额只是数字没有钱，对方想提现我就告诉对方账户冻结了，之后我再使用客服身份的qq号让对方再往账户里缴纳保障费，对方把钱充进来后我再带着对方把钱输掉，等对方账户里金额输没后我就把对方删除。

我使用名为“稳赚计划”的qq号诈骗了两次，第一次是2.5万元，第二次是2000元，对方通过支付宝扫码把钱打到我在“新葡京赌场”的账号，我找到“新葡京赌场”把我骗到的钱提现。

40、被告人宁志杰供述:2018年年初，qq上一个昵称为“爱你呦”的人找我搭建网站，当时我以为搭建的是彩票交流网站，后来知道是能充值、投注能提现的虚假赌博网站，网站

里有一项是“余额”，数字可以随意更改，充值的钱会通过对接的三方平台流转到找我搭建平台的人的账户里。

我搭建平台的成本是500元左右，包括租用服务器和域名的费用，别人找我搭建网站我根据关系收费在1700元到2000元不等，后期每个月我还要收对方租用服务器的费用，价格根据关系在600元到1000元不等。

我通过182XXXXXXXX手机号绑定的支付宝结算租用域名的费用，还用这个账号通过支付宝扫码的方式收取搭建域名的费用和后期租用服务器的费用。

我的支付宝昵称是“嘉禾”，qq号是×××，这个号专门用于发送搭建网站的广告消息和联系搭建网站人员使用的，“爱你呦”的支付宝昵称是“*小莉”，他通过支付宝转给我2000元。

41、被告人王银珍供述:我捡了一张名为“吴绮莉”的身份证，我老乡给我一张155XXXXXXXX的手机卡，2017年5月23日我用身份证和手机卡在邮政银行办理了一张银行卡，银行卡申领手续上的字都是我签的。

在南大桥附近，有个20多岁的男的找我买银行卡，我把名为“吴绮莉”的银行卡、身份证还有我老乡给我的手机卡这一套物品以2000元出卖给对方，对方没有告诉我为什么购买这套物品，但是我知道对方肯定是从事违法犯罪活动，要不不能花2000元来买，我当时就是想挣钱所以就卖给他了，办理卡后我没有使用过。

42、被告人王锋供述:2018年9月，童镇找我说他做了一个API接口，它的功能是可以集成到一个网站上面，用户通过支付宝付款，钱就转到指定的支付宝账户。

当时我们约定，他提供技术拿70%的利润，我找用户拿30%的利润。

随后，我在网上发布了支付接口合作的信息，一个叫Eric的人通过skype软件联系我，我们约定按照支付宝进账数额的6‰支付使用费，我把API的使用文档及账号发送给Eric，从Eric使用API接口至今我收了他340多万元，我分得100多万元。

我在skype软件上的名字叫“俊山张”，Eric让我和名字叫“-L”的对接，Eric等代理把我们这个平台叫做“直付平台”，Eric具体干什么的我不知道，但我认为他们干的是违法的事情，类似地下黑彩等，因为他跟我说他们在国外，客户也在国外，但为了赚钱我还是卖给他了。

43、被告人朱曰军供述:我是2018年5、6月份开始在直付平台工作的，一直干到2018年8月20日，我手下雇佣过祁某、朱某1、陈某1。

我负责和上面联系处理问题，朱某1负责白班，祁某、陈某1负责晚班。

我们的交易流水平均每天200万元左右，一共有3000万元左右的流水。

我一共获利4万元。

我们一共有八个账本，七本是对商户进行转账记账的账本，一本是记录总账的账本，从2018年8月11日记到8月20日。

账本上的余额就是每天对商户的资金转账记录，我和朱某1、陈某1、祁某四个人记账，白班是朱某1，晚班是陈某1、祁某。

44、被告人潘锦业供述:我从2018年11月开始在直付平台工作，干了20多天就被抓了。

我手下雇佣了戴某2、戴某1、许某、徐某、张宗宏。

我们一共获利10万元左右，除去各项开支剩下的净利润我分得一半，大约2万元左右，戴某2和戴某1兄弟分一半，我一个月给张宗宏开1万元左右。

我们工作分白、晚班，戴某2和徐某是白班，戴某1和张宗宏是晚班。

每天交易流水平均二、三百万元。

45、被告人廖正鑫供述:2018年8月，姜基祥介绍我到直付平台上班，负责SKYPE群里的事务以及赌博网站的对接，我在SKYPE群里的名字是“直付-L”。

我们就相当于为赌博网站收款，参与赌博人的充值方式必须是支付宝充值，参赌人员通过支付宝扫码，钱进入我们的支付宝，我们按照商户要求进行返钱。

我在昆山一个工作室干了一个多月后，又和张宗宏等人在另一个工作室工作了20多天，因为直付平台暂停服务，我们休了1个月，之后我和张宗宏、廖洁等人又来到之前的工作室。

11月中旬古玉在上海开了一个直付工作室，我将廖洁、姜某1领到古玉这里，我每天得500-1000元的好处费。

平均每个工作室的资金流水是300万元左右，各工作室的工作人员由工作室的负责人开工资。

我是挣工资，总计获利8、9万元。

46、被告人张宗宏供述:2018年7月底至11月25日，我在直付平台工作，中间停过20多天，开始赵军做负责人，带着我和廖洁、廖正鑫干，2018年11月3日开始，潘锦业带着我和廖洁等人一起干。

廖正鑫进行过转账操作。

我们的资金交易流水每天从几十万元到几百万元不等。

我一共获利4万多元。

47、被告人廖洁供述:我在直付平台工作过，日期分别是2018年7月10日后的一个月、9月16日至11月1日、11月3日至11月25日。

开始廖正鑫是组长，我和张宗宏等人负责具体转账操作，廖正鑫也进行过转账操作。

第三次是潘锦业负责，我和张宗宏等人一起干。

我一共得到27600元工资，我们的资金交易流水每天从几十万元到几百万元不等。

综上，经庭审质证、认证，证据来源合法。

被告人周道鹏对公诉机关指控其犯诈骗罪、被告人宁志杰对公诉机关指控其是诈骗罪的共犯均无异议。

被告人周道鹏、宁志杰的供述与被害人杨某的陈述、同案被告人王银珍的供述、证人吴

某1的证言相吻合，并有发破案经过、抓获经过、刑事判决书、释放证明、谅解书、收条、转账记录等证据证实，足以认定被告人周道鹏诈骗犯罪的事实以及被告人宁志杰诈骗共犯的事实成立。

被告人王银珍对公诉机关指控其犯妨害信用卡管理罪无异议，被告人王银珍的供述与被告人周道鹏的供述、证人吴某1的证言相吻合，并有发破案经过、抓获经过、转账记录等证据证实，足以认定被告人王银珍妨害信用卡管理的犯罪事实成立。

被告人王锋对公诉机关指控其犯帮助信息网络犯罪活动罪无异议，被告人王锋的供述与被告人廖正鑫、证人郭某的证言相吻合，并有发破案经过、抓获经过、银行流水、电子数据提取材料等证据证实，足以认定被告人王锋帮助信息网络犯罪活动的犯罪事实成立。

被告人廖正鑫、廖洁对公诉机关指控其犯非法经营罪以及指控的犯罪事实均无异议，被告人朱曰军、潘锦业、张宗宏对公诉机关指控其犯非法经营罪均无异议，虽然被告人朱曰军、潘锦业、张宗宏均对公诉机关指控的非法从事资金支付结算的数额有异议，但庭审中被告人朱曰军、潘锦业对其是小组负责人没有异议，且公诉机关出示的证人戴某2、戴某1、徐某、张宗宏、陈某1、祁某、朱某1的证言可以证明被告人朱曰军、潘锦业系小组负责人，故被告人朱曰军、潘锦业亦应对小组内成员的非法资金支付结算的数额承担责任，银行流水及统计表、账本、情况说明足以证明各被告人非法从事资金支付结算的数额，故被告人朱曰军、潘锦业、张宗宏的辩解不成立。

关于被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁的违法所得数额，其中被告人朱曰军、张宗宏、廖洁的原始供述与庭审中的供述一致，分别为4万元、4万元、27600元，故对此数额予以认定；被告人潘锦业、廖正鑫的原始供述与庭审中的供述不一致，按照有利于被告人的原则，故应认定被告人潘锦业违法所得为4万元、廖正鑫违法所得为8万元。

另被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁的供述与证人戴某2、戴某1、徐某、张宗宏、陈某1、祁某、朱某1、姜某1等人的证言相吻合，并有银行流水、账本扣押决定书、扣押清单、情况说明、协助冻结通知书等证据佐证，足以认定被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁非法经营的犯罪事实成立。

本院认为，被告人周道鹏使用虚假的网站骗取他人财物，数额较大，被告人宁志杰明知他人实施电信网络诈骗而为其提供技术支持，其行为均构成诈骗罪；被告人王银珍使用虚假的身份证明骗领信用卡后又予以出售，其行为构成妨害信用卡管理罪；被告人王锋明知他人利用信息网络实施犯罪而为其提供互联网接入的技术支持，情节严重，其行为构成帮助信息网络犯罪活动罪；被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁未经国家有关主管部门批准，非法从事资金支付结算业务，扰乱市场秩序，情节严重，其行为均构成非法经营罪。

公诉机关指控的犯罪事实清楚，证据确实充分，本院予以支持。

被告人周道鹏因故意犯罪被判处有期徒刑，刑罚执行完毕后五年内又犯应当判处有期徒刑以上刑罚之罪，系累犯，依法应从重处罚。

被告人周道鹏当庭自愿认罪，积极赔偿被害人经济损失并取得谅解，可酌定从轻处罚。

被告人周道鹏与被告人宁志杰共同实施诈骗犯罪行为，被告人周道鹏策划并直接实施诈骗被害人财物的行为，系主犯，被告人宁志杰为周道鹏实施诈骗活动提供技术支持，系从犯，依法可从轻处罚；被告人宁志杰当庭自愿认罪，主动上缴违法所得，可酌定从轻处罚。

被告人王银珍、王锋当庭自愿认罪，可酌定从轻处罚。

被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁均受他人雇佣共同非法从事资金支付结算业务，在共同犯罪中均起次要作用，均系从犯，依法均可从轻或减轻处罚。

另被告人朱曰军、潘锦业、廖正鑫、张宗宏、廖洁当庭自愿认罪，被告人潘锦业、廖正鑫主动上缴违法所得，均可酌定从轻处罚。

对被告人周道鹏辩护人的辩护意见本院予以采纳;对被告人王锋辩护人认为王锋构成从犯的辩护意见不予采纳，对其他辩护意见予以采纳；对被告人朱曰军辩护人认为朱曰军的犯罪数额为2200万元的辩护意见不予采纳，对其他辩护意见予以采纳；对被告人潘锦业辩护人认为潘锦业构成从犯、自愿认罪、可从轻、减轻处罚的辩护意见予以采纳，对其他辩护意见不予采纳；对被告人廖正鑫辩护人认为廖正鑫在共同犯罪活动中的作用小、自愿认罪，可从轻处罚的辩护意见予以采纳;对被告人张宗宏辩护人认为张宗宏犯罪数额为500余万元的辩护意见不予采纳，对其他辩护意见予以采纳。

依照《中华人民共和国刑法》第二百六十六条　（诈骗罪）、第一百七十七条　之一（妨害信用卡管理罪）、第二百八十七条　之二（帮助信息网络犯罪活动罪）、第二百二十五条　（非法经营罪）、第二十五条　（共同犯罪）、第二十六条　（主犯）、第二十七条　（从犯）、第六十五条　第一款　（一般累犯）、第五十二条　（罚金）、第五十三条　（罚金缴纳期限）、第六十四条　（追缴违法所得和没收财物）之规定，判决如下:

一、被告人朱曰军犯非法经营罪，判处有期徒刑五年六个月，并处罚金人民币4万元。

刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年11月26日起至2024年5月25日止。

二、被告人潘锦业犯非法经营罪，判处有期徒刑三年六个月，并处罚金人民币4万元。

刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年11月25日起至2022年5月24日止。

三、被告人廖正鑫犯非法经营罪，判处有期徒刑二年，并处罚金人民币8万元。

刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2018年11月25日起至2020年11月24日止。

四、被告人王锋犯帮助信息网络犯罪活动罪，判处有期徒刑一年九个月，并处罚金人民币30万元。

刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自

2018 年 11 月 25 日起至 2020 年 8 月 24 日止。

五、被告人张宗宏犯非法经营罪，判处有期徒刑一年八个月，并处罚金人民币 4 万元。

刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 11 月 25 日起至 2020 年 7 月 24 日止。

六、被告人周道鹏犯诈骗罪，判处有期徒刑一年七个月，并处罚金人民币 2 万元。

刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 11 月 23 日起至 2020 年 6 月 22 日止。

七、被告人廖洁犯非法经营罪，判处有期徒刑一年六个月，并处罚金人民币 3 万元。

刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 11 月 25 日起至 2020 年 5 月 24 日止。

八、被告人王银珍犯妨害信用卡管理罪，判处有期徒刑一年三个月，并处罚金人民币 1 万元。

刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 11 月 24 日起至 2020 年 2 月 23 日止。

九、被告人宁志杰犯诈骗罪，判处有期徒刑一年一个月，并处罚金人民币 1 万元。

刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 12 月 25 日起至 2020 年 1 月 24 日止。

上列罚金均于本判决发生法律效力后十日内缴纳。

十、责令被告人周道鹏、宁志杰共同退赔杨某 5000 元。

十一、对被告人宁志杰的违法所得 2000 元（已缴纳）、被告人王银珍的违法所得 2000 元、被告人王锋的违法所得 100 万元（已扣押 454885 元、冻结 242422.68 元）、被告人朱曰军的违法所得 4 万元、被告人潘锦业的违法所得 4 万元（已缴纳）、被告人廖正鑫的违法所得 8 万元（已缴纳）、被告人张宗宏的违法所得 4 万元、被告人廖洁的违法所得 27600 元依法追缴，上缴国库。

十二、公安机关扣押、冻结的涉案赌资 9007945.29 元，由扣押的公安机关予以没收，上缴国库（具体明细详见公安机关扣押、冻结清单）。

十三、对被告人潘锦业、张宗宏、廖洁的犯罪工具手机、银行卡、通用 K 宝、笔记本电脑、动态口令，由扣押的公安机关予以没收，上缴国库（具体明细详见公安机关扣押清单）。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向吉林省四平市中级人民法院提出上诉。

书面上诉的，应当提交上诉状正本一份，副本十份。

审判长宋红霞

审判员刘佳

人民陪审员徐桂芳

二〇二〇年一月十七日

书记员齐桐

案例二、王海洋等帮助信息网络犯罪活动案

山东省济南市历城区人民法院刑事判决书

案号：（2019）鲁 0112 刑初 856 号

公诉机关山东省济南市历城区人民检察院。

被告人王海洋，男，1990 年 1 月 1 日出生于吉林省长春市，汉族因涉嫌犯帮助信息网络犯罪活动罪，于 2019 年 7 月 11 日被刑事拘留，同年 8 月 16 日被逮捕，现羁押于济南市第二看守所。

辩护人刘清玉，山东昌平律师事务所律师。

被告人郭锐，男，1981 年 7 月 8 日出生于福建省莆田市，汉族因涉嫌犯帮助信息网络犯罪活动罪，于 2019 年 8 月 2 日被刑事拘留，同年 8 月 22 日被逮捕，现羁押于济南市第二看守所。

辩护人孙福山，山东储誉律师事务所律师。

被告人黄志豪，男，1974 年 9 月 12 日出生于福建省福州市，汉族因涉嫌犯帮助信息网络犯罪活动罪，于 2019 年 7 月 15 日被刑事拘留，同年 8 月 22 日被逮捕，现羁押于济南市第二看守所。

辩护人李晓艳，山东鲁耀律师事务所律师。

被告人刘一波，曾用名刘波，男，1984 年 11 月 30 日出生于吉林省长春市，汉族因涉嫌犯帮助信息网络犯罪活动罪，于 2019 年 8 月 16 日被刑事拘留，同年 9 月 5 日被逮捕。

辩护人朱明明，山东祥泰律师事务所律师。

被告人李新，男，1994 年 12 月 29 日出生于内蒙古自治区鄂尔多斯市因涉嫌犯帮助信息网络犯罪活动罪，于 2019 年 7 月 31 日被刑事拘留，同年 8 月 16 日被取保候审。

被告人吕玥萱，男，1999 年 9 月 21 日出生于吉林省长春市，汉族因涉嫌犯帮助信息网络犯罪活动罪，于 2019 年 7 月 30 日被刑事拘留，同年 8 月 16 日被取保候审。

被告人孟玲斤，男，1987 年 8 月 4 日出生于吉林省长春市，汉族因犯故意毁坏财物罪，于 2007 年 1 月 31 日被判处有期徒刑一年。因涉嫌犯帮助信息网络犯罪活动罪，于 2019 年 10 月 1 日被刑事拘留，同年 11 月 1 日被逮捕。现羁押于济南市第二看守所。

济南市历城区人民检察院以济历城检一部刑诉[2019]808 号起诉书指控被告人王海洋、郭锐、黄志豪、刘一波、李新、吕玥萱、孟玲斤犯帮助信息网络犯罪活动罪一案，于 2019 年 11 月 29 日向本院提起公诉。本院依法组成合议庭，适用简易程序，于 2019 年 12 月 11 日公开开庭进行了审理。济南市历城区人民检察院指派检察员张洁出庭支持公诉，被告人王海洋及其辩护人刘清玉、被告人郭锐及其辩护人孙福山、被告人黄志豪及其辩护人李晓艳、

被告人刘一波及其辩护人朱明明、被告人李新、被告人吕玥萱、被告人孟玲斤均到庭参加诉讼。现已审理终结。

济南市历城区人民检察院指控:

被告人王海洋经营的吉林省十全十美文化发展有限公司主营业务是为上游客户提供网络支付结算服务，即为需要网络支付结算的网站提供支付接口，被害人通过接口支付的钱款先进入该公司指定的企业支付宝账号上，公司扣除一定比例的利润后，将剩余钱款打入上游客户指定的银行卡内。

被告人王海洋、郭锐、黄志豪、林元生（在逃）、刘一波、李新、吕玥萱、孟玲斤、宋大伟（另案处理）在明知上游客户可能从事电信诈骗、网络赌博等犯罪活动的情况下，由被告人郭锐、黄志豪、林元生联系需要支付结算服务的上游客户，被告人王海洋安排被告人刘一波带领被告人孟玲斤、宋大伟注册营业执照和办理企业支付宝账号及银行卡等，被告人李新、吕玥萱负责程序开发和运营，上游客户的犯罪资金首先进入被告人孟玲斤、宋大伟的数个企业支付宝账号内，各方扣除利润后，由被告人刘一波等人根据被告人郭锐等人提供的银行卡号，将剩余资金向下流转。

2019 年 4 月 17 日、4 月 19 日，被害人刘某某在位于济南市历城区桑园路将军花园的家中，被人以网络炒股的名义骗取 399948.33 元.2019 年 4 月 23 日至 5 月 10 日，被害人房某某在位于山东省荣成市港湾街道黄海南路的家中，被人以网络炒股的名义骗取 2779999.81 元，经查，被害人刘某某的全部被骗资金以及被害人房某某被骗资金中的 20 万元均通过上述支付接口进入被告人孟玲斤、宋大伟办理的企业支付宝账号内，后又转账至下游的批量银行卡中。

自 2019 年 4 月 16 日至 5 月 12 日，被告人孟玲斤、宋大伟的其中五个企业支付宝账号收款总金额为 17479575.6 元。

2019 年 6 月中旬，被告人郭锐等人与被告人王海洋预谋在福建省福清市继续为上游客户提供资金支付结算服务。

被告人郭锐、黄志豪、林元生负责租用办公地点、办理营业执照、对公支付宝账号和联系上游客户等，被告人王海洋安排被告人刘一波、李新、吕玥萱提供技术服务和维护。

自 2019 年 7 月 4 日至 7 月 10 日，上述被告人使用的其中九个企业支付宝账号收款总金额为 6134045.67 元。

2019 年 7 月 11 日、15 日、29 日、31 日、8 月 2 日、10 月 1 日，被告人王海洋、黄志豪、吕玥萱、李新、郭锐、孟玲斤先后被公安机关抓获归案，2019 年 8 月 16 日，被告人刘一波自动投案。

案发后，被告人王海洋、刘一波的亲属分别代其二人各赔偿被害人刘某某经济损失 11 万元，被害人刘某某对被告人王海洋、刘一波表示谅解。

另查明，本案审理期间，被告人王海洋退缴违法所得 100000 元，被告人郭锐退缴违法

所得 60000 元，被告人黄志豪退缴违法所得 20000 元，被告人刘一波退缴违法所得 60000 元，被告人李新退缴违法所得 55000 元，被告人吕玥萱退缴违法所得 40000 元，被告人孟玲斤退缴违法所得 12000 元。

扣押于济南市公安局历城区分局的被告人王海洋名下车牌号为吉 AXXXF 雷克萨斯牌白色汽车一辆，根据被告人王海洋的辩护人提交的银行转账回单，证实该车辆的购车款系王海洋之妻单立伟支付。

公诉机关认为被告人王海洋、郭锐、黄志豪、刘一波、李新、吕玥萱、孟玲斤的行为均构成帮助信息网络犯罪活动罪。

被告人王海洋、郭锐、黄志豪、刘一波、李新、吕玥萱、孟玲斤签字具结认罪认罚，被告人刘一波具有自首情节，被告人王海洋、刘一波赔偿被害人部分经济损失，并取得被害人谅解等量刑情节，建议判处被告人王海洋、郭锐二年六个月以下有期徒刑，并处罚金；建议判处被告人黄志豪二年四个月以下有期徒刑，并处罚金；建议判处被告人刘一波二年以下有期徒刑，并处罚金；建议判处被告人李新、吕玥萱、孟玲斤一年六个月以下有期徒刑，并处罚金。

被告人王海洋、郭锐、黄志豪、刘一波、李新、吕玥萱、孟玲斤对起诉指控的犯罪事实、罪名及量刑建议均没有异议，上述七名被告人均已签字具结，并有经庭审举证、质证予以确认的户籍证明，前科情况、归案经过、刑事判决书、扣押物品清单、工商登记信息、被害人聊天记录、银行卡交易明细、支付宝账号及商户信息、交易流水、被告人聊天记录、被害人刘某某、房某某陈述、共同作案人宋大伟的供述、辨认笔录、刑事谅解书、被告人的供述与辩解、认罪认罚具结书、视频资料等证据证实，足以认定。

本院认为，被告人王海洋、郭锐、黄志豪、刘一波、李新、吕玥萱、孟玲斤明知他人利用信息网络实施犯罪，为犯罪提供资金支付结算等帮助，情节严重，其行为均已构成帮助信息网络犯罪活动罪。

被告人王海洋、郭锐、黄志豪、刘一波在共同犯罪中，均起主要作用，均系主犯，依法应从重处罚；被告人李新、吕玥萱、孟玲斤在共同犯罪中，均起次要作用，均系从犯，可依法从轻处罚。

被告人孟玲斤有犯罪前科，依法应从重处罚；被告人刘一波自动投案，归案后能如实供述其犯罪事实，系自首，可依法对其从轻处罚。

被告人王海洋、刘一波案发后积极赔偿被害人刘某某的经济损失，并取得被害人谅解，可酌情从轻处罚。

被告人王海洋、郭锐、黄志豪、刘一波、李新、吕玥萱、孟玲斤均签字具结认罪认罚，主动退缴违法所得并缴纳罚金，可依法从轻处罚。

关于被告人王海洋、郭锐、黄志豪、刘一波的辩护人提出的对被告人适用缓刑的辩护意见，经查，本案各被告人在共同犯罪过程中组织严密，分工细致，与上游犯罪共同组成了一

个完整的“黑色”产业链，被告人的行为社会危害性较大、影响范围较广，根据四被告人的犯罪情节，均不宜适用缓刑。

故，对辩护人提出的适用缓刑的意见，本院均不予采纳。

综上，根据各被告人在共同犯罪中所起的作用、犯罪情节、性质、社会危害程度及认罪、悔罪表现，依照《中华人民共和国刑法》第二百八十七条　之二、第二十五条　第一款　、第二十七条　、第五十二条　、第五十三条　第一款　、第六十四条　、第六十七条　第一款　、第七十二条　第一款　、第七十三条　第二、三款之规定，判决如下:

一、被告人王海洋犯帮助信息网络犯罪活动罪，判处有期徒刑一年三个月，并处罚金人民币二万元。（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 7 月 11 日起至 2020 年 10 月 10 日止。罚金已缴纳。

二、被告人郭锐犯帮助信息网络犯罪活动罪，判处有期徒刑一年三个月，并处罚金人民币二万元（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 8 月 2 日起至 2020 年 11 月 1 日止。罚金已缴纳。

三、被告人黄志豪犯帮助信息网络犯罪活动罪，判处有期徒刑一年，并处罚金人民币一万元。

（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 7 月 15 日起至 2020 年 7 月 14 日止。罚金已缴纳。

四、被告人刘一波犯帮助信息网络犯罪活动罪，判处有期徒刑十个月，并处罚金人民币一万元。（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 8 月 16 日起至 2020 年 6 月 15 日止。罚金已缴纳。

五、被告人李新犯帮助信息网络犯罪活动罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币八千元。（缓刑考验期限从判决确定之日起计算。罚金已缴纳）

六、被告人吕玥萱犯帮助信息网络犯罪活动罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币八千元。（缓刑考验期限从判决确定之日起计算。罚金已缴纳。

七、被告人孟玲斤犯帮助信息网络犯罪活动罪，判处有期徒刑六个月，并处罚金人民币五千元（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 10 月 1 日起至 2020 年 3 月 31 日止。罚金已缴纳）。

八、被告人王海洋退缴违法所得 100000 元，被告人郭锐退缴违法所得 60000 元，被告人黄志豪退缴违法所得 20000 元，被告人刘一波退缴违法所得 60000 元，被告人李新退缴违法所得 55000 元，被告人吕玥萱退缴违法所得 40000 元，被告人孟玲斤退缴违法所得 12000 元，依法上缴国库。

九、扣押于济南市公安局历城区分局车牌号为吉 AXXXF 雷克萨斯牌白色汽车一辆，发还被告人王海洋；扣押于公安机关的手机、银行卡等作案工具依法予以没收。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或直接向山东省济南市中

级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份、副本两份。

审判长丁磊

人民陪审员赵婷

人民陪审员王启玉

二〇一九年十二月十八日

法官助理蔡文

案例三、武汉旭文信息科技有限公司、余西文等帮助信息网络犯罪活动罪魏所勤帮助信息网络犯罪活动罪、诈骗罪杜光远、杨绪磊等诈骗案

江苏省无锡市中级人民法院刑事判决书

案号：（2019）苏 02 刑终 516 号

原公诉机关无锡市锡山区人民检察院。

上诉人杜光远，男，1992 年 7 月 8 日出生于河南省淮滨县，汉族，大学文化，杭州融投泰信息科技有限公司法定代表人、股东，户籍地河南省淮滨县，住浙江省杭州市萧山区。2018 年 1 月 19 日因涉嫌犯诈骗罪被刑事拘留，同年 2 月 24 日被逮捕。现羁押于无锡市第一看守所。

上诉人(原审被告人)杨绪磊（曾用名恩池），男，1990 年 10 月 8 日出生于河南省淮滨县，汉族，大学文化，杭州融投泰信息科技有限公司股东，户籍地河南省淮滨县，住浙江省杭州市萧山区。2018 年 1 月 19 日因涉嫌犯诈骗罪被刑事拘留，同年 2 月 24 日被逮捕。现羁押于无锡市第一看守所。

辩护人顾磊，江苏闳远律师事务所律师。

原审被告单位武汉旭文信息科技有限公司,住所地武汉市洪山区卓刀泉路 238 号三金雄楚天地 1 号 1105 室，法定代表人余西文。

诉讼代表人罗某，女，1991 年 9 月 2 日生，住湖北省武汉市江夏区。

原审被告人余西文，男，1989 年 10 月 11 日出生于湖北省监利县，汉族，硕士文化，武汉旭文信息科技有限公司法定代表人，户籍地湖北省监利县，住湖北省武汉市江夏区。2018 年 1 月 12 日被因涉嫌犯诈骗罪被刑事拘留，同年 2 月 13 日被逮捕。现羁押于无锡市第一看守所。

原审被告人魏所勤（化名张萌、魏峰），男，1994 年 4 月 28 日出生于湖北省武穴市，汉族，大学文化，武汉旭文信息科技有限公司职员，户籍地湖北省武穴市，住湖北省武汉市洪山区。2018 年 1 月 12 日因涉嫌犯诈骗罪被刑事拘留，同年 2 月 13 日被逮捕。现羁押于无锡市第一看守所。

原审被告人赵丹青，女，1994 年 12 月 12 日出生于湖北省宜昌市，汉族，大专文化，武汉旭文信息科技有限公司职员，户籍地湖北省宜昌市夷陵区。

被告人赵丹青因涉嫌犯诈骗罪，于2018年1月13日被无锡市公安局锡山分局刑事拘留，2018年2月6日被取保候审。

原审被告人刘毅（曾用名刘昭成），男，1993年7月18日出生于湖北省麻城市，汉族，大专文化，武汉旭文信息科技有限公司职员，户籍地湖北省麻城市。2018年1月12日因涉嫌犯诈骗罪被刑事拘留，同年2月13日被取保候审。

原审被告人万灿，男，1995年8月16日出生于湖北省鄂州市，汉族，中专文化，武汉旭文信息科技有限公司职员，户籍地湖北省鄂州市鄂城区，住鄂州市鄂城区。2018年1月13日因涉嫌犯诈骗罪被刑事拘留，同年2月13日被取保候审。

原审被告人李文博，男，1998年2月26日出生于湖北省洪湖市，汉族，大专文化，武汉旭文信息科技有限公司职员，户籍地湖北省洪湖市，住湖北省武汉市东湖开发区。2018年1月13日因涉嫌犯诈骗罪被刑事拘留，同年2月13日被取保候审。

原审被告人徐芳（曾用名徐金娥），女，1991年10月2日出生于湖北省郧县，汉族，大学文化，武汉旭文信息科技有限公司职员，户籍地湖北省十堰市郧阳区。2018年1月13日因涉嫌犯诈骗罪被刑事拘留，同年2月13日被取保候审。

原审被告人王龙龙，男，1992年10月1日出生于河南省淮滨县，汉族，大专文化，杭州融投泰信息科技有限公司事业一部经理，户籍地河南省淮滨县，住浙江省杭州市萧山区。2018年1月19日因涉嫌犯诈骗罪被刑事拘留，同年2月24日被逮捕。现羁押于无锡市第一看守所。

原审被告人孙雪发，男，1996年7月26日出生于江西省万年县，汉族，大专文化，杭州融投泰科技有限公司事业三部经理，户籍地江西省上饶市万年县，住浙江省杭州市萧山区。2018年1月19日因涉嫌犯诈骗罪被刑事拘留，同年2月24日被逮捕。现羁押于无锡市第一看守所。

原审被告人夏丽，女，1990年8月6日出生于湖南省溆浦县，汉族，初中文化，杭州融投泰信息科技有限公司股东，户籍地湖南省溆浦县，住浙江省杭州市萧山区。2018年1月19日因涉嫌犯诈骗罪被刑事拘留，同年2月13日被取保候审，2019年8月16日被逮捕。现羁押于无锡市第二看守所。

原审被告人符雪玲，女，1999年7月20日出生于河南省淮滨县，汉族，高中文化，杭州融投泰信息科技有限公司职员，户籍地河南省淮滨县。2018年1月19日因涉嫌犯诈骗罪被刑事拘留，同年2月13日被取保候审。

无锡市锡山区人民法院审理无锡市锡山区人民检察院指控原审被告单位武汉旭文信息科技有限公司（以下简称旭文公司）、原审被告人余西文、魏所勤、赵丹青、刘毅、万灿、李文博、徐芳犯帮助信息网络犯罪活动罪，原审被告人魏所勤、杜光远、杨绪磊、王龙龙、孙雪发、夏丽、符雪玲犯诈骗罪一案，于2019年9月10日作出（2018）苏0205刑初537号刑事判决。

原审被告人杜光远、杨绪磊不服，提出上诉。

本院依法组成合议庭，经过阅卷，讯问上诉人，听取辩护人的辩护意见和江苏省无锡市人民检察院阅卷后的意见，认为事实清楚，决定不开庭审理。

现已审理终结。

原审判决认定:

一、帮助信息网络犯罪活动

（一）被告单位旭文公司成立于2014年12月，经营范围包括计算机软硬件研发、销售、维护等，被告人余西文担任该公司法定代表人。

2017年7月左右，被告人余西文与公司经理被告人魏所勤合谋以旭文公司的名义制作、销售虚假的投资类微盘（手机交易软件），所得利润均分，余西文负责技术及发放工资，魏所勤负责销售。

被告人赵丹青系销售小组长，被告人刘毅、万灿系公司业务员。

余西文、魏所勤组织业务员从事网上发布广告、招揽客户、软件推销和操作指导等工作。

余西文以购得具有后台控制盈亏功能的源代码，根据购买方需求，组织公司技术员即被告人李文博、徐芳从事微盘的制作和运行维护、第三方支付平台的接入等技术工作。

具体事实分述如下:

1.2017年7月，经被告人万灿网上联系、推荐，被告人魏所勤和欲购买虚假投资类软件的被告人杜光远、杨绪磊接洽、商议后，旭文公司以38000元的价格向二人出售具有后台控制盈亏功能的微盘“中汇国际”，并接入“钱通宝”平台作为第三方结算支付平台，于2018年1月收取域名注册费人民币2500元。

在微盘使用、运行等过程中，被告人李文博根据旭文公司安排，参与部分技术工作。

后杜光远、杨绪磊等人利用该微盘实施诈骗，诈骗金额21万余元。

2.2017年10月，经被告人赵丹青通过网络等联系、推荐，被告人魏所勤和欲购买虚假投资类软件的王启明、邱荣浬、张海峰（均另案处理）接洽、商议后，王启明等人以80000元左右的价格向旭文公司购买具有后台控制盈亏功能的微盘“鑫义环球”、“瑞益商品”。

在微盘制作、使用、运行等过程中，被告人李文博、徐芳根据旭文公司安排，参与部分技术等工作。

后王启明等人利用该两套微盘实施诈骗。

3.2017年11月，经被告人刘毅网上联系、推荐，被告人魏所勤和欲购买虚假投资类软件的艾有（另案处理）接洽、商议后，旭文公司以38000元左右的价格向艾有等人出售具有后台控制盈亏功能的微盘“金盛环球”，并接入第三方支付平台。

被告人刘毅通过网络指导艾有操作使用该微盘。

在微盘制作、使用、运行等过程中，被告人徐芳根据旭文公司安排，参与部分技术工作。

后艾有等人利用该微盘实施诈骗活动，诈骗金额65万余元。

4.2017 年 12 月，经被告单位旭文公司业务员网上联系、推荐，被告人魏所勤和欲购买虚假投资类软件的刘洋成（另案处理）接洽、商议后，旭文公司以 40000 元的价格向刘洋成出售虚假投资类微盘“环球国际”。

在微盘制作等过程中，被告人李文博根据公司安排，参与部分技术工作。

（二）2017 年 10 月，经被告人赵丹青联系、推荐，被告人魏所勤和欲购买虚假投资类软件的黄科、丘文润（均另案处理）接洽，旭文公司以 20 万元从他人处外购虚假投资类软件“环球证券”，后以 30 万元的价格转售给黄科、丘文润，从中赚取非法所得 10 万元，并在后续的软件运行过程中提供技术支持、支付结算帮助。

黄科、丘文润等人利用该软件实施网络犯罪。

（三）旭文公司从五次销售软件的过程中共计非法获利 298500 元。

归案后，被告单位旭文公司、被告人余西文、魏所勤、赵丹青、刘毅、万灿、李文博、徐芳如实供述了自己及其单位帮助信息网络犯罪活动的犯罪事实。

公安机关从上述被告人处扣缴电脑主机、笔记本电脑、手机、U 盘等物品。

上述事实，原审判决有经庭审质证的公安机关出具、制作、调取的刑事案件侦破经过、抓获录像、搜查笔录、现场平面图、扣押清单、扣押物品照片、数据侦查实验笔录、远程勘验笔录、检查截图记录表，营业执照、赵丹青手机截图及工作笔记照片，旭文公司合同、余西文招商银行卡交易记录，赵丹青、魏所勤 QQ 聊天记录打印件，深圳市公安局盐田分局起诉意见书复印件，证人许某、钟某、何某、孙某甲、李某甲、成某、廖某、罗某的证言，涉案微信聊天记录，涉案人员郑佳明、李宜芸、吴祥征、艾有、刘洋成、王启明、丘文润、黄科等人的供述及相关辨认笔录，被告人余西文、魏所勤、徐芳、赵丹青、刘毅、万灿、李文博、徐芳、杜光远的供述等证据证明。

二、被告人魏所勤诈骗

2017 年 12 月，被告人魏所勤与王启明一方合谋，由魏所勤提供具有后台控制盈亏功能的虚假投资类微盘及部分客户（被害人）信息，王启明一方负责运营，所得利润按 35%和 65%的比例分配。

王启明伙同邱荣浬、张海峰纠集公司业务员，利用魏所勤提供的部分客户信息，通过打电话、微信交友、发展网络代理商等方式发展客户，引诱客户使用魏所勤提供的“鼎泰云购”软件进行虚假的商品交易。

王启明通过软件后台操控强行造成被害人亏损，控制被害人出金来骗取钱财。

在微盘使用、运行过程中，被告人徐芳根据魏所勤安排，参与部分技术工作。

该诈骗团伙诈骗金额共计 377000 余元，其中魏所勤从中分得 11 万余元。

案破后，王启明、邱荣浬、张海峰家属已分别向被害人退赃 38071 元，共计 114213 元。

本案审理阶段，被告人魏所勤家属代其退赃 110000 元；业务员周锦、黄建锋退赃共计 11000 元，故尚余 141000 余元未退赔。

上述事实，原审判决有经庭审质证的公安机关出具的刑事案件侦破经过，鼎运公司的营业执照、考勤记录表，涉案人员王启明的招商银行卡交易明细，公安机关制作的电子数据侦查实验笔录及相关电子光盘、远程勘验笔录及相关电子光盘、后台数据入金、出金情况统计表，被害人季某、胡某、阴某、孔某、易某、王某甲、韩某、周某、李某乙、王某乙、姚某、刘某甲、陈某甲、李某丙、杨某甲、彭某、刘某乙、卢某等人的陈述、平台交易信息、出金及入金统计表，充某记录，涉案人员王启明、邱荣浬、张海峰、张峻玮的供述，证人廖某的证言，被告人魏所勤的供述等证据证明。

三、被告人杜光远等人诈骗

2016 年 11 月，被告人杜光远、杨绪磊、夏丽共同注册成立杭州融投泰信息科技有限公司（以下简称融投泰公司），杜光远为法定代表人，杜光远、杨绪磊、夏丽为股东，股份比例为杜光远 45%、杨绪磊 45%、夏丽 10%，扣除成本后的非法所得按照 35%、45%、20%分配。

被告人王龙龙为事业一部经理，下有业务员被告人符雪玲、王雪婷（另案处理）；被告人孙雪发为事业三部经理，下有业务员王燕（另案处理）。

2017 年 7 月底，杜光远、杨绪磊至旭文公司，从被告人魏所勤处以 38000 元的价格购买带有后台控制盈亏功能的“中汇国际”软件。

2017 年 8 月至 2018 年 1 月间，杜光远、杨绪磊利用“中汇国际”软件，伙同王龙龙、孙雪发等人，由业务员使用微信号虚拟女性身份，利用“夜神模拟器”软件将使用的微信位置虚假定位至目标城市，以此交友发展客户（被害人），在拉拢被害人的过程中借机推荐“中汇国际”软件，并将被害人拉至融投泰公司的微信群内，杨绪磊伪装成外汇理财分析师“老师”，王龙龙、孙雪发伪装成客服，普通业务员伪装成从“中汇国际”软件盈利的客户，共同欺骗被害人下载“中汇国际”APP 软件注册充某投资。

被害人充某的资金进入“中汇国际”软件的第三方支付平台“钱通宝”后，即转入杨绪磊的工商银行卡内，被害人申请出金受杜光远、杨绪磊的控制，无法自主操控投入的资金。

后由杜光远、杨绪磊通过后台操控，造成被害人账户亏损，控制被害人出金，从而非法占有被害人资金。

其中，杜光远主要负责员工招聘、培训、后台操控等工作；杨绪磊负责冒充“老师”提示下单、后台操控、统计业绩、发放工资等工作；王龙龙、孙雪发作为经理，直接发展客户的同时，对组内的业务员进行指导，冒充客服、客户制造通过平台盈利的假象引诱被害人充某投资；夏丽、符雪玲、王雪婷、王燕作为普通业务员主要负责引诱发展客户，冒充已盈利客户引诱被害人充某投资。

该犯罪团伙采用上述方式，从 20 名被害人处骗取金额共计 215000 余元，具体骗取被害人张某甲 68270 余元、于某 48300 元、王某丙 16500 元、王某丁 8800 余元、杨某乙 10990 元、杨某丙 6190 余元、狄某 6100 元、左某 8880 元、穆某 1500 元、孙某乙 2500 元、陈某乙 1400 元、李某丁 1200 元、毕某 2650 元、谭某 2100 元、黄某 2800 余元、袁某 1750 元、

白某 1100 余元、张某乙 8640 余元、冀某 1510 余元、刘某丙 14300 余元。

其中被告人符雪玲参与骗取金额 48050 余元（从 2017 年 11 月 13 日入职起算）。

归案后，被告人杜光远、杨绪磊、王龙龙、孙雪发、夏丽、符雪玲如实供述了自己参与实施诈骗的事实，并当庭自愿认罪。

公安机关从上述被告人处扣缴电脑、手机、笔记本等物品。

上述事实，原审判决有经庭审质证的公安机关出具、制作、调取的刑事案件侦破经过、银行卡明细、企业档案材料、工资单，转账记录及后台查询记录，扣押笔录、扣押决定书、扣押清单、被骗数额统计表、电子证据检查工作记录、远程勘验工作记录、远程勘验工作视频，证人施某的证言，被害人张某甲、于某、王某丙、王某丁、杨某乙、杨某丙、狄某、左某、穆某、孙某乙、陈某乙、李某丁、毕某、谭某、黄某、袁某、白某、张某乙、冀某、刘某丙的陈述，涉案人员王雪婷、王燕的供述，被告人杜光远、杨绪磊、王龙龙、孙雪发、夏丽、符雪玲、魏所勤、万灿的供述等证据证明，被告人杜光远、杨绪磊、王龙龙、孙雪发、夏丽、符雪玲在开庭审理过程中亦无异议。

一审审理阶段，被告人孙雪发家属代其退赃 4 万元，被告人夏丽退赃 2 万元，被告人符雪玲退赃 1.5 万元。王雪婷、王燕在（2018）苏 0205 刑初 515 号案件中分别退赃 1.7 万元、8000 元。

原审法院认为:被告单位旭文公司明知他人利用信息网络实施犯罪，为犯罪提供技术支持、支付结算帮助，情节严重，其行为已构成帮助信息网络犯罪活动罪。

被告人余西文、魏所勤作为被告单位旭文公司直接负责的主管人员，被告人赵丹青、刘毅、万灿、李文博作为直接责任人员，其行为均已构成帮助信息网络犯罪活动罪。

被告人徐芳为魏所勤、王启明等人诈骗犯罪提供技术支持，其行为亦构成帮助信息网络犯罪活动罪。

在帮助信息网络犯罪活动共同犯罪中，被告人魏所勤、余西文起主要作用，系主犯，应当按照其所参与的全部犯罪处罚；被告人赵丹青、刘毅、万灿、李文博、徐芳起次要和辅助作用，系从犯，应当从轻处罚。

归案后，被告单位旭文公司、被告人余西文、魏所勤、赵丹青、刘毅、万灿、李文博、徐芳均如实供述了自己及其单位帮助信息网络犯罪活动的犯罪事实，依法均可以从轻处罚。

根据被告人赵丹青、刘毅、李文博、徐芳、万灿帮助信息网络犯罪活动的犯罪事实和情节，对其适用缓刑不致再危害社会，可以对其宣告缓刑。

被告人魏所勤以非法占有为目的，与他人合谋实施电信网络诈骗，提供诈骗软件和客户信息，诈骗数额巨大，其行为已构成诈骗罪。

魏所勤在诈骗共同犯罪中系主犯，应当按照其所参与的全部犯罪处罚。

魏所勤归案后未如实供述诈骗事实，但其当庭认罪，并退出 11 万元赃款，可酌情从轻处罚。

被告人魏所勤一人犯两罪，应当数罪并罚。

被告人杜光远、杨绪磊、王龙龙、孙雪发、夏丽、符雪玲以非法占有为目的，利用电信网络技术手段实施诈骗，数额巨大，其行为均已构成诈骗罪。

在诈骗共同犯罪中，杜光远、杨绪磊起主要作用，系主犯，应当按照其所参与的全部犯罪处罚；王龙龙、孙雪发、夏丽、符雪玲起次要作用，系从犯，应当从轻或者减轻处罚。

归案后，杜光远、杨绪磊、王龙龙、孙雪发、夏丽、符雪玲均如实供述自己诈骗的犯罪事实，均可以从轻处罚。

孙雪发、夏丽、符雪玲能退赔部分赃款，均可酌情从轻处罚。

杜光远、杨绪磊组织、指挥电信网络诈骗犯罪团伙对不特定被害人实施诈骗，酌情从重处罚。

决定对王龙龙从轻处罚，对孙雪发、夏丽、符雪玲分别予以减轻处罚，且对符雪玲适用缓刑不致再危害社会，可以对其宣告缓刑。

据此，依照《中华人民共和国刑法》第二百八十七条　之二、第二百六十六条　、第二十五条　第一款　、第二十六条　第一款　及第四款，第二十七条　、第三十条　、第三十一条　、第六十九条　、第六十七条　第三款　、第六十四条　、第七十二条　第一款　、第三款　之规定，以犯帮助信息网络犯罪活动罪，分别判处被告单位武汉旭文信息科技有限公司罚金人民币三十五万元；判处被告人余西文有期徒刑二年七个月，并处罚金人民币六万元；判处被告人赵丹青有期徒刑一年三个月，缓刑一年三个月，并处罚金人民币二万元；判处被告人刘毅有期徒刑十个月，缓刑一年，并处罚金人民币一万五千元；判处被告人李文博有期徒刑十个月，缓刑一年，并处罚金人民币一万五千元；判处被告人徐芳有期徒刑十个月，缓刑一年，并处罚金人民币一万五千元；判处被告人万灿有期徒刑八个月，缓刑一年，并处罚金人民币一万元；以犯帮助信息网络犯罪活动罪，判处被告人魏所勤有期徒刑二年四个月，并处罚金人民币五万元，以犯诈骗罪，判处被告人魏所勤有期徒刑五年，并处罚金人民币五万元，决定执行有期徒刑六年四个月，并处罚金人民币十万元；以犯诈骗罪，分别判处被告人杜光远有期徒刑五年，并处罚金人民币五万元；判处被告人杨绪磊有期徒刑四年十个月，并处罚金人民币五万元；判处被告人王龙龙有期徒刑三年四个月，并处罚金人民币一万六千元；判处被告人孙雪发有期徒刑二年七个月，并处罚金人民币一万三千元；判处被告人夏丽有期徒刑二年，并处罚金人民币一万三千元；判处被告人符雪玲有期徒刑九个月，缓刑一年，并处罚金人民币四千元；公安机关扣缴的作案电脑、手机、U盘等物品，由公安机关予以没收；被告单位武汉旭文信息科技有限公司的非法所得298500元予以追缴，扣缴在案的被告人魏所勤退赔款110000元，发还相关被害人；扣缴在案的被告人孙雪发、夏丽、符雪玲退赔款75000元发还相关被害人；责令被告人魏所勤对其参与的诈骗犯罪尚未追缴的赃款141000元，予以退赔，并发还相关被害人；责令被告人杜光远、杨绪磊、王龙龙、孙雪发、夏丽对本案尚未追缴的赃款115000元，予以退赔，被告人符雪玲对

其中的25400元予以退赔，并发还相关被害人。

上诉人杜光远提出的上诉理由是:1.平台的资金是被害人自主控制的；2.原审判决量刑过重。

上诉人杨绪磊提出的上诉理由是:1.其名为股东，但不参与公司决策，日常工作接受杜光远的领导和安排，不应认定其为主犯；2.原审判决量刑过重。

上诉人杨绪磊的辩护人提出的辩护意见是:1.杜光远也做过“老师”的角色，并非杨绪磊单独扮演；2.被害人可以自主操控投入的资金，且客户的亏损中含有其自行操作造成的亏损，指控本案系诈骗的证据不足，应认定为非法经营罪；3.杜光远的地位、作用高于杨绪磊，应认定杨绪磊为从犯。

江苏省无锡市人民检察院经讯问上诉人杜光远、杨绪磊，并审查全部案件材料后认为:原审判决认定事实清楚，证据确实、充分，定罪准确，量刑适当，审判程序合法。

鉴于二审期间上诉人杨绪磊主动退赃，建议酌情予以从宽处罚。

经审理查明:原审判决认定原审被告单位旭文公司、原审被告人余西文、魏所勤、赵丹青、刘毅、万灿、李文博、徐芳犯帮助信息网络犯罪活动罪，上诉人杜光远、杨绪磊、原审被告人魏所勤、王龙龙、孙雪发、夏丽、符雪玲犯诈骗罪的事实，有原审法院经过当庭质证的证据证实，本院对原审判决认定的事实和相关证据予以确认。

二审另查明，在魏所勤诈骗过程中，原审被告人徐芳在不明知魏所勤诈骗的情况下，在魏所勤安排下参与了部分技术工作。

此部分事实有已经过原审法院当庭质证的相关证据证实。

上诉人杨旭磊在本案二审期间主动退出赃款5万元。

此项事实有收款收据在卷佐证。

关于上诉人杜光远、杨绪磊的上诉理由及辩护人提出的辩护意见，本院综合评判如下:

1.上诉人杜光远、杨绪磊均供述，客户充某的资金进入“中汇国际”软件的第三方支付平台“钱通宝”后，即转入杨绪磊的银行卡内；如果客户盈利，并选择出金，金额少的，杜光远和杨绪磊会在后台看到申请并点击同意，让客户出金，让他们尝到甜头，吸引他们更多的入金；如果客户入金数额大，且还要出金，杜光远和杨绪磊就会后台操作，强制让客户亏损，或者拒绝出金。

原审被告人王龙龙也供称，受害人想提现撤资时，杜光远和杨绪磊就会后台操作强制受害人全部亏损。

张某甲、王某丁、杨某乙、狄某、穆某、陈某乙、李某丁等多名被害人的陈述中也均提到申请提现遭拒的情况。

上述证据能够相互印证，足以证明本案被害人并不能自主操控投入的资金。

2.上诉人杜光远与杨绪磊及原审被告人王龙龙等人以高额投资回报为诱饵，欺骗被害人向其控制的“中汇国际”软件的第三方支付平台“钱通宝”充某，通过软件在后台操控客户

输赢，并控制客户出金，骗取客户钱财的行为，符合诈骗罪的犯罪构成要件，构成为诈骗罪。

杜光远、杨绪磊及其他原审被告人在一审庭审中均对指控其诈骗没有异议，并表示认罪。

辩护人提出应定性为非法经营罪的意见无事实和法律依据，不能成立。

同时，被害人基于上诉人和原审被告人的欺骗注册充某投资后，造成的损失均应计入诈骗金额。

3.虽然原审被告人夏丽、符雪玲、涉案人员王雪婷的供述，均证实杜光远有时候也会冒充“老师”提示下单，但原审判决关于杜光远主要负责员工招聘、培训、后台操控等工作的表述并没有错误。

杨绪磊与杜光远同为公司主要股东，与杜光远一起至旭文公司，从原审被告人魏所勤处购买带有后台控制盈亏功能的“中汇国际”软件，而后在犯罪团伙中主要负责冒充“老师”提示下单、后台操控、统计业绩、发放工资等工作，与杜光远均是犯罪团伙的管理者，在犯罪中起相对主要的作用。

虽然作为公司法定代表人的杜光远在犯罪中的地位、作用稍高于杨绪磊，但根据杨绪磊在犯罪中的地位、作用，不应当认定杨绪磊为从犯。

4.原审法院依据杜光远、杨绪磊的诈骗金额、犯罪情节及悔罪表现，对其量刑符合法律规定，不存在量刑过重的情况。

综上，上诉人及辩护人提出的上诉理由和辩护意见均不能成立，本院不予采纳。

本院认为:原审被告单位旭文公司明知他人利用信息网络实施犯罪，为犯罪提供技术支持、支付结算等帮助，情节严重，其行为已构成帮助信息网络犯罪活动罪。

原审被告人余西文、魏所勤作为旭文公司直接负责的主管人员，原审被告人赵丹青、刘毅、万灿、李文博、徐芳作为直接责任人员，其行为均已构成帮助信息网络犯罪活动罪。

其中，魏所勤、余西文起主要作用，系主犯，应当按照其所参与的全部犯罪处罚；赵丹青、刘毅、万灿、李文博、徐芳起次要和辅助作用，系从犯，应当从轻处罚。

归案后，余西文、魏所勤、赵丹青、刘毅、万灿、李文博、徐芳均如实供述了自己及其单位帮助信息网络犯罪活动的犯罪事实，依法可以从轻处罚。

根据赵丹青、刘毅、李文博、徐芳、万灿帮助信息网络犯罪活动的犯罪事实和情节，对其适用缓刑不致再危害社会，可以对其宣告缓刑。

原审被告人魏所勤还以非法占有为目的，与他人合谋利用电信网络技术手段实施诈骗，数额巨大，其行为已构成诈骗罪。

魏所勤在其参与的诈骗共同犯罪中系主犯，应当按照其所参与的全部犯罪处罚。

魏所勤当庭认罪，并退出赃款 11 万元，可以酌情从轻处罚。

魏所勤一人犯数罪，依法应当数罪并罚。

上诉人杜光远、杨绪磊、原审被告人王龙龙、孙雪发、夏丽、符雪玲以非法占有为目的，利用电信网络技术手段共同实施诈骗，数额巨大，其行为均已构成诈骗罪。

其中，杜光远、杨绪磊起主要作用，系主犯，应当按照其所参与的全部犯罪处罚；王龙龙、孙雪发、夏丽、符雪玲起次要作用，系从犯，应当从轻或者减轻处罚。

归案后，杜光远、杨绪磊、王龙龙、孙雪发、夏丽、符雪玲如实供述自己的犯罪事实，依法可以从轻处罚。

孙雪发、夏丽、符雪玲退赔部分赃款，可以酌情从轻处罚。

杜光远、杨绪磊组织、指挥诈骗犯罪团伙利用电信网络发布虚假信息，对不特定被害人实施诈骗，酌情从重处罚。

综上，决定对王龙龙予以从轻处罚，对孙雪发、夏丽、符雪玲予以减轻处罚。

根据符雪玲的犯罪事实和情节，对其适用缓刑不致再危害社会，可以对其宣告缓刑。

原审判决认定上诉人杜光远、杨绪磊、原审被告人魏所勤、王龙龙、孙雪发、夏丽、符雪玲犯诈骗罪，原审被告单位旭文公司、原审被告人余西文、魏所勤、赵丹青、刘毅、万灿、李文博、徐芳犯帮助信息网络犯罪活动罪的事实和适用法律正确，量刑符合法律规定，诉讼程序合法，应当予以维持。

鉴于上诉人杨绪磊在二审期间主动退出赃款 5 万元的新事实，结合原判量刑，对杨绪磊的量刑可再适当予以从轻处罚。

江苏省无锡市人民检察院的阅卷意见成立，本院予以采纳。

据此，依照《中华人民共和国刑事诉讼法》第二百三十六条　第一款　第三项　，《中华人民共和国刑法》第二百八十七条　之二、第二百六十六条　、第二十五条　第一款　、第二十六条　第一款　及第四款，第二十七条　、第三十条　、第三十一条　、第六十九条　、第六十七条　第三款　、第六十四条　、第七十二条　第一款　、第三款　之规定，判决如下：

一、维持无锡市锡山区人民法院（2018）苏 0205 刑初 537 号刑事判决第一项、第二项、第三项、第四项、第五项，第六项、第七项、第八项、第九项、第十一项、第十二项、第十三项、第十四项、第十五项，以及第十项的定罪部分，即对上诉人杜光远、原审被告单位武汉旭文信息科技有限公司、原审被告人余西文、魏所勤、赵丹青、刘毅、万灿、李文博、徐芳、王龙龙、孙雪发、夏丽、符雪玲的定罪量刑部分和对上诉人杨绪磊的定罪部分；

二、撤销无锡市锡山区人民法院（2018）苏 0205 刑初 537 号刑事判决第十项对杨绪磊的量刑部分和第十六项；

三、上诉人杨绪磊犯诈骗罪，判处有期徒刑四年（刑期自判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 1 月 19 日起至 2022 年 1 月 18 日止），并处罚金人民币三万元（罚金于本判决生效次日起十日内缴纳）；

四、扣押在案的原审被告人魏所勤退赔款人民币 110000 元及原审被告人孙雪发、夏丽、符雪玲的退赔款人民币 75000 元按比例发还相关被害人；继续追缴原审被告单位武汉旭文信息科技有限公司的违法所得人民币 298500 元；责令原审被告人魏所勤与其共同诈骗人员共

同退赔其参与诈骗犯罪尚未追缴的赃款人民币 141000 元；责令上诉人杜光远、杨绪磊、原审被告人王龙龙、孙雪发、夏丽共同退赔尚未追缴的赃款人民币 65000 元，原审被告人符雪玲对其中的人民币 25400 元承担共同退赔责任；上述退赔款项收缴后一并发还相关被害人。

本判决为终审判决。

审判长华栋

审判员蔡连德

审判员周群

二〇一九年十二月六日

书记员程文斌

案例四、赵松明、沙某甲等诈骗罪陈某丁、吴某等帮助信息网络犯罪活动案

启东市人民法院一审刑事判决书

案号：（2018）苏 0681 刑初 292 号

公诉机关江苏省启东市人民检察院。

被告人赵松明，上海兴遥投资管理有限公司负责人。因涉嫌犯诈骗罪，于 2018 年 1 月 17 日被刑事拘留，同年 2 月 13 日被逮捕。现羁押于启东市看守所。

辩护人ＸＸ，江苏东疆律师事务所律师。

被告人沙某甲，个体务工。因涉嫌犯诈骗罪，于 2018 年 1 月 17 日被刑事拘留，同年 2 月 13 日被逮捕。现羁押于启东市看守所。

辩护人盛伟，江苏东晋律师事务所律师。

被告人李某，个体务工。因涉嫌犯诈骗罪，于 2018 年 1 月 17 日被刑事拘留，同年 2 月 13 日被逮捕。现羁押于启东市看守所。

辩护人陈卫东，江苏东疆律师事务所律师。

被告人王某甲，个体务工。因涉嫌犯诈骗罪，于 2018 年 1 月 17 日被刑事拘留，同年 2 月 13 日被逮捕。现羁押于启东市看守所。

辩护人陆浴东，江苏东晋律师事务所律师。

被告人杨某，个体务工。因涉嫌犯诈骗罪，于 2018 年 1 月 17 日被刑事拘留，同年 2 月 13 日被逮捕。现羁押于南通市看守所。

辩护人刘娟，江苏东晋律师事务所律师。

被告人冯某，个体务工。因涉嫌犯诈骗罪，于 2018 年 1 月 17 日被刑事拘留，同年 2 月 13 日变更为取保候审。

被告人潘某，个体务工。因涉嫌犯诈骗罪，于 2018 年 1 月 17 日被取保候审。

被告人周某，个体务工。因涉嫌犯诈骗罪，于 2018 年 1 月 17 日被取保候审。

被告人程某，个体务工。因涉嫌犯诈骗罪，于 2018 年 1 月 17 日被取保候审。

被告人沙某乙，个体务工。因涉嫌犯诈骗罪，于2018年1月17日被取保候审。

被告人龙某，个体务工。因涉嫌犯诈骗罪，于2018年1月17日被取保候审。

被告人陈某甲，个体务工。因涉嫌犯诈骗罪，于2018年1月17日被取保候审。

被告人余某，个体务工。因涉嫌犯诈骗罪，于2018年1月17日被取保候审。

被告人陈某乙，个体务工。因涉嫌犯诈骗罪，于2018年1月17日被取保候审。

被告人陈某丙，个体务工。因涉嫌犯诈骗罪，于2018年1月17日被取保候审。

被告人陈某丁，广州市天河区七锦宫网络科技有限公司经理。因涉嫌犯诈骗罪，于2018年1月25日被刑事拘留，同年3月1日变更为取保候审。

辩护人吴红权，江苏江海明珠律师事务所律师。

被告人吴某，广州市天河区七锦宫网络科技有限公司员工。

被告人吴某因涉嫌诈骗罪，于2018年1月25日被启东市公安局刑事拘留，同年2月24日变更为取保候审。2018年4月16日，本院决定对被告人吴某取保候审。

辩护人汪小建，广东一粤律师事务所律师。

被告人黄某甲，广州市天河区七锦宫网络科技有限公司员工。因涉嫌犯诈骗罪，于2018年1月25日被刑事拘留，同年2月24日变更为取保候审。

辩护人陆波，江苏禾东律师事务所律师。

被告人林某，广州市天河区七锦宫网络科技有限公司员工。因涉嫌犯诈骗罪，于2018年1月25日被刑事拘留，同年2月24日变更为取保候审。

被告人王某乙，广州市天河区七锦宫网络科技有限公司员工。因涉嫌犯诈骗罪，于2018年1月25日被刑事拘[illegible]，同年2月24日变更为取保候审。

江苏省启东市人民检察院以启检诉刑诉〔2018〕289号起诉书指控被告人赵松明、沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙犯诈骗罪，被告人陈某丁、吴某、黄某甲、林某、王某乙犯帮助信息网络犯罪活动罪，于2018年6月19日向本院提起公诉。本院依法组成合议庭，于2018年7月5日公开开庭审理了本案。启东市人民检察院指派检察员陈兵出庭支持公诉。上列被告人及辩护人均到庭参加了诉讼。现已审理终结。

公诉机关指控：

一、诈骗

2017年6月至2018年1月期间，被告人赵松明租用上海市闵行区浦江镇联行路某办公楼设置办公地点，先后招募被告人沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈[illegible]乙、陈某丙等人，以代理、运营嘀嘀商城、哒哒商城、抱抱商城等投资网站为名诱骗他人钱款。

被告人赵松明、沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙明知所代理、运营的投资网站系以赌博的方式进行所谓

的投资，经常更换网站名称、微信公众号，网站所交易的红酒等产品无实际的市场交易，且系未经国家许可的违规网站，先后在微信社交软件上以虚假的身份引诱被害人添加微信好友获取对方信任，诱使对方进入网站内以买涨买跌方式进行所谓投资交易，并以投资专家、投资人的虚假身份在微信聊天群中发言，诱使被害人在网站充值交易，骗取钱款。

2017 年 6 月 23 日至 9 月 2 日，上述十五名被告人以嘀嘀商城、哒哒商城等投资网站为名诱骗被害人黄某乙向网站充值共计人民币 345929 元，期间，被害人黄某某 于 2017 年 6 月 23 日至 8 月 5 日从网站提取人民币 98000 元，至 2017 年 9 月 3 日，黄某乙在网站的账户余额为 12956.93 元。

2018 年 1 月，上述十五名被告人以抱抱商城投资网站为名诱骗被害人陈某戊、王某丙、王某丁、田某等人向抱抱商城充值共计人民币 97518 元，期间，被害人提某共计人民币 51399 元。

上述抱抱商城网站系被告人赵松明指使被告人陈某丁等人制作，该网站的交易后台可以人为控制涨跌。

其中，被告人赵松明、沙某甲、杨某、李某、王某甲、周某、程某、冯某、龙某参与全部犯罪；被告人沙某乙、陈某乙参与诱骗被害人向网站充值共计人民币 108028 元；被告人潘某、陈某丙参与诱骗被害人向网站充值共计人民币 97518 元。

二、帮助信息网络犯罪活动

2017 年 10 月至 12 月，被告人陈某丁经他人介绍结识被告人赵松明，赵向其提出帮忙设计一个能让玩家买涨跌的网络微交易网站，且该交易网站能人为操纵涨跌的数据。

被告人陈某丁即联系被告人吴某、黄某甲、王某乙、林某按被告人赵松明的要求设计上述微交易网站。

被告人陈某丁、吴某、黄某甲、王某乙、林某明知该微交易网站能人为控制涨跌数据，可能被用于犯罪活动，仍由被告人黄某甲编写程序，由被告人吴某购买对应网站的微信公众号，由被告人林某、王某乙完成网站第三方通道对接，共同制作该网站，将该网站命名“抱抱商城”投资网站，并将该网站交给被告人赵松明等人，被用于实施网络诈骗犯罪。

被告人陈某丁事后向被告人赵松明收取了该网站的设计费用人民币 40000 元。

为指控上述事实，公诉机关当庭出示了被告人供述、被害人陈述、证人证言及相关书证等证据。

公诉机关认为，被告人赵松明、沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙以非法占有为目的，骗取他人财物，数额巨大，其行为均应以诈骗罪追究其刑事责任。

被告人陈某丁、吴某、黄某甲、林某、王某乙明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入等技术支持，情节严重，其行为均应以帮助信息网络犯罪活动罪追究刑事责任。

本案系共同犯罪。

被告人赵松明、陈某丁在共同犯罪中均是主犯，应当按照其所参与的全部犯罪处罚。

被告人沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙、吴某、黄某甲、林某、王某乙在共同犯罪中均是从犯，应当从轻或者减轻处罚。

诉请本院依法判处。

被告人赵松明、沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙、陈[illegible]丁、吴某、黄某甲、林某、王某乙对起诉书指控的事实及罪名无异议，并当庭表示认罪。

被告人赵松明的辩护人提出:①关于被害人黄某乙一节的数额不应计入犯罪数额；②赵松明归案后如数供述犯罪事实，自愿认罪，能够退赃，无前科劣迹，建议对其从轻或者减轻处罚。

被告人沙某甲的辩护人提出:①沙某甲无诈骗的主观故意，其行为不构成诈骗罪；②即使沙某甲的行为构成诈骗罪，其系从犯，归案后如实供述犯罪事实，自愿认罪，能够退赃，无前科劣迹，建议对其减轻处罚并适用缓刑。

被告人李某的辩护人提出:①李某无诈骗的主观故意，其行为不构成诈骗罪；②即使李某的行为构成诈骗罪，其系从犯，归案后如实供述犯罪事实，自愿认罪，能够退赃，无前科劣迹，建议对其减轻处罚并适用缓刑。

被告人王某甲的辩护[illegible]对起诉书指控的事实及罪名无异议，同时提出:王某甲系从犯，归案后如实供述犯罪事实，自愿认罪，能够退赃，无前科劣迹，建议对其减轻处罚并适用缓刑。

被告人杨某的辩护人提出:①关于被害人黄某乙一节的数额不应计入犯罪数额；②杨某系从犯，归案后如实供述犯罪事实，自愿认罪，能够退赃，无前科劣迹，建议对其减轻处罚并适用缓刑。

被告人陈某丁的辩护人对起诉书指控的事实及罪名无异议，同时提出，陈某丁归案后如实供述犯罪事实，能够退赃，预缴罚金，无前科劣迹，建议对其从轻处罚并适用缓刑。

被告人吴某的辩护人对起诉书指控的事实及罪名无异议，同时提出，吴某系从犯，归案后如实供述犯罪事实，无前科劣迹，建议对其适用缓刑或者单处罚金。

被告人黄某甲的辩护人对起诉书指控的事实及罪名无异议，同时提出，黄某甲系从犯，归案后如实供述犯罪事实，无前科劣迹，建议对其适用缓刑或者单处罚金。

经审理查明:

一、诈骗

2017 年 6 月至 2018 年 1 月期间，被告人赵松明租用上海市闵行区浦江镇联行路某办公楼设置办公地点，先后招募被告人沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、

沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙等人，以代理、运营嘀嘀商城、哒哒商城、抱抱商城等投资网站为名诱骗他人钱款。

被告人赵松明、沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙明知所代理、运营的投资网站系以赌博的方式进行所谓的投资，经常更换网站名称、微信公众号，网站所交易的红酒等产品无实际的市场交易，且系未经国家许可的违规网站，先后在微信社交软件上以虚假的身份引诱被害人添加微信好友获取对方信任，诱使对方进入网站内以买涨买跌方式进行所谓投资交易，并以投资专家、投资人的虚假身份在微信聊天群中发言，诱使被害人在网站充值交易，骗取钱款。

2017 年 6 月 23 日至 9 月 2 日，上述十五名被告人以嘀嘀商城、哒哒商城等投资网站为名诱骗被害人黄某乙向网站充值共计人民币 345929 元，期间，被害人黄某乙于 2017 年 6 月 23 日至 8 月 5 日从网站提取人民币 98000 元。

2018 年 1 月，上述十五名被告人以抱抱商城投资网站为名诱骗被害人陈某戊、王某丙、王某丁、田某等人向抱抱商城充值共计人民币 97518 元，期间，被害人提某共计人民币 51399 元。

上述抱抱商城网站系被告人赵松明指使被告人陈某丁等人制作，该网站的交易后台可以人为控制涨跌。

其中，被告人赵松明、沙某甲、杨某、李某、王某甲、周某、程某、冯某、龙[illegible] 参与全部犯罪；被告人沙某乙、陈某乙参与诱骗被害人向网站充值共计人民币 108028 元；被告人潘某、陈某丙参与诱骗被害人向网站充值共计人民币 97518 元。

二、帮助信息网络犯罪活动

2017 年 10 月至 12 月，被告人陈某丁经他人介绍结识被告人赵松明，赵向其提出帮忙设计一个能让玩家买涨跌的网络微交易网站，且该交易网站能人为操纵涨跌的数据。

被告人陈某丁即联系被告人吴某、黄某甲、王某乙、林某按被告人赵松明的要求设计上述微交易网站。

被告人陈某丁、吴某、黄某甲、王某乙、林某明知该微交易网站能人为控制涨跌数据，可能被用于犯罪活动，仍由被告人黄某甲编写程序，由被告人吴某购买对应网站的微信公众号，由被告人林某、王某乙完成网站第三方通道对接，共同制作该网站，将该网站命名“抱抱商城”投资网站，并将该网站交给被[illegible] 人赵松明等人，被用于实施网络诈骗犯罪。

被告人陈某丁事后向被告人赵松明收取了该网站的设计费用人民币 40000 元。

被告人赵松明、沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙于 2018 年 1 月 16 日在上海市闵行区浦江镇被民警抓获归案；被告人陈某丁、吴某、黄某甲、王某乙、林某于 2018 年 1 月 24 日在广州市天河区被民警抓获归案。

上述二十名被告人归案后均如实供述自己的犯罪事实。

本案审理期间，赵松明亲属已向本院代为退缴赃款人民币 139048 元，沙某甲亲属已向本院代为退缴赃款人民币 20000 元，杨某、李某、王某甲的各自亲属已分别向本院退缴赃款人民币 15000 元，周某、程某、冯某、龙某已分别向本院退缴赃款 12000 元，沙某乙、陈某乙、潘某、陈某丙、陈某甲、余某已分别向本院退缴赃款 7000 元，陈某丁向本院退缴赃款人民币 40000 元。

上述事实，被告人赵松明、沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙、陈某丁、吴某、黄某甲、林某、王某乙在开庭审理中均无异议，且有上列二十名被告人在侦查阶段供述笔录，另案处理的犯罪嫌疑人侯林、刘春丽、张芳、杨京伟等人的供述笔录，被害人黄某乙、王某丁、陈某戊、王某丙、田某等人的陈述笔录，未到庭证人刘高来、黄跃鑫、陈汤怡等人的证言笔录，启东市公安局出具的发破案及抓获经过、辨认笔录、搜查笔录、电子证据检查笔录，涉案电脑等物证，手机截屏图片、银行卡交易明细、微信聊天记录及上列各被告人的户籍证明等证据证实，足以认定。

关于被告人赵松明的辩护人、被告人杨某的辩护人提出的关于被害人黄某乙一[illegible] 的数额不应计入犯罪数额的辩护意见，经查，被告人赵松明、沙某甲、李某、王某甲、杨某、冯某等人的供述及被害人黄某乙的陈述等证据能够相互印证，足以证明，本案涉及的嘀嘀商城、哒哒商城等平台以投资为幌子却无真实交易内容，赵松明团伙成员在微信社交软件上以投资专家、投资人等虚假身份与被害人黄某乙聊天，并通过发送虚假赚钱截图的方式，使黄某乙误认为可以通过投资该平台盈利，进而诱使黄某乙以买涨买跌的方式进行“投资交易”，骗取钱款。

赵松明团伙的行为是黄某乙被骗的关键环节，该团伙应对黄某乙被骗的全部数额承担责任。

故黄某乙的被骗数额不应从指控的犯罪数额中剔除。

上述辩护意见与查证事实及法律规定不符，本院不予采纳。

关于被告人沙某甲的辩护人、被告人李某的辩护人分别提出的沙某甲、李某无诈骗的主观故意，其行为不构成诈骗罪的辩护意见，经查，沙某甲的多次稳定供述能够证明，因为涉案的微信公众号经常被封，公司经常更换网站名称、微信公众号，且很多客户投资都是亏损的，沙某甲遂已经怀疑涉案的平台系人为操控，可以控制客户盈亏。

李某的多次稳定供述能够证明，李某清楚涉案的微信公众号经常被封，其曾感觉涉案平台的产品与市场实际行情不符，并经上网查找，发现涨跌的 K 线图是假的。

但沙某甲、李某仍伙同他人利用话术，以投资专家、投资人的名义，诱使被害人投资，进而骗取钱款。

故沙某甲、李某伙同他人实施诈骗的主观故意明显，上述辩护意见与查证事实不符，本院不予采纳。

关于被告人沙某甲、李某、王某甲、杨某的辩护人分别提出对上述各被告人适用缓刑的辩护意见，经查，上述各被告人犯罪数额巨大，且在犯罪团伙中行使一□□□组织管理职能，犯罪情节较重，不宜适用缓刑。

故上述辩护意见与法律规定不符，本院不予采纳。

关于被告人赵松明的辩护人提出赵松明无前科劣迹，具有坦白、认罪、退赃等情节，建议对其从轻处罚的辩护意见，关于被告人沙某甲、李某、王某甲、杨某的各辩护人分别提出沙某甲、李某、王某甲、杨某无前科劣迹，具有从犯、坦白、认罪、退赃等情节，建议对其减轻处罚的辩护意见，关于被告人陈某丁的辩护人提出陈某丁无前科劣迹，具有坦白、退赃、预缴罚金等情节，建议对其从轻处罚并适用缓刑的辩护意见，关于被告人吴某、黄某甲的各辩护人分别提出吴某、黄某甲无前科劣迹，具有从犯、坦白等情节，建议对其单处罚金的辩护意见，与查证事实及法律规定相符，本院予以采纳。

本院认为，被告人赵松明、沙某甲、李某、王某甲、杨某□□□冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙以非法占有为目的，利用电信网络技术手段实施诈骗，数额巨大，其行为均已构成诈骗罪，依法应追究刑事责任。

被告人陈某丁、吴某、黄某甲、林某、王某乙明知他人利用信息网络实施犯罪，仍为其犯罪提供互联网接入等技术支持，情节严重，其行为均已构成帮助信息网络犯罪活动罪，依法应追究其刑事责任。

公诉机关指控上列二十名被告人的犯罪事实清楚，证据确实、充分，指控罪名成立，本院予以支持。

本案系共同犯罪。

被告人赵松明、陈某丁在共同犯罪中起主要作用，是主犯，应当按照其所参与的全部犯罪处罚。

被告人沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙、吴某、黄某甲、林某、王某乙在共同犯罪中起次要作用□□是从犯，应当从轻或者减轻处罚。

上列二十名被告人归案后均如实供述犯罪事实，可以从轻或者减轻处罚。

被告人赵松明、沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙、陈某丁退缴违法所得并预缴罚金，被告人吴某、黄某甲、林某、王某乙预缴罚金，均可酌情从轻处罚。

综上，根据各被告人的犯罪情节及认罪悔罪表现，本院决定对被告人赵松明从轻处罚，对被告人沙某甲、李某、王某甲、杨某减轻处罚，对被告人冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙减轻处罚并适用缓刑，对被告人陈某丁从轻处罚并适用缓刑，对被告人吴某、黄某甲、林某、王某乙从轻处罚并单处罚金。

为维护公共秩序，保护公私财产权利不受侵犯，惩罚犯罪，依照《中华人民共和国刑法》

第二百六十六条　、第二百八十七条　之二第一款　、第二十五条　第一款　、第二十六条　第一、四款、第二十七条　、第六十七条　第三款　、第七十二条　第一、三款、第七十三条　第二、三款、第六十四条　之规定，判决如下:

一、被告人赵松明犯诈骗罪，判处有期徒刑三年三个月，并处罚金人民币五万元（已预缴）。

（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 1 月 17 日起至 2021 年 4 月 16 日止。

被告人沙某甲犯诈骗罪，判处有期徒刑一年六个月，并处罚金人民币二万元（已预缴）。

（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 1 月 17 日起至 2019 年 7 月 16 日止。

被告人李某犯诈骗罪,判处有期徒刑一年四个月,并处罚金人民币一万八千元(已预缴)。

（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 1 月 17 日起至 2019 年 5 月 16 日止。

被告人王某甲犯诈骗罪，判处有期徒刑一年四个月，并处罚金人民币一万八千元（已预缴）。

（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 1 月 17 日起至 2019 年 5 月 16 日止。

被告人杨某犯诈骗罪，判处有期徒刑一年五个月，并处罚金人民币一万八千元（已预缴一千元）。

（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2018 年 1 月 17 日起至 2019 年 6 月 16 日止。

被告人冯某犯诈骗罪，判处有期徒刑一年三个月，缓刑一年六个月，并处罚金人民币一万三千元（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人潘某犯诈骗罪,判处有期徒刑一年,缓刑一年三个月,并处罚金人民币九千元(已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人周某犯诈骗罪，判处有期徒刑一年三个月，缓刑一年六个月，并处罚金人民币一万三千元（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人程某犯诈骗罪，判处有期徒刑一年三个月，缓刑一年六个月，并处罚金人民币一万三千元（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人沙某乙犯诈骗罪，判处有期徒刑一年，缓刑一年三个月，并处罚金人民币一万元

（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人龙某犯诈骗罪，判处有期徒刑一年三个月，缓刑一年六个月，并处罚金人民币一万三千元（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人陈某甲犯诈骗罪，判处有期徒刑一年，缓刑一年三个月，并处罚金人民币九千元（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人余某犯诈骗罪，判处有期徒刑一年，缓刑一年三个月，并处罚金人民币九千元（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人陈某乙犯诈骗罪，判处有期徒刑一年，缓刑一年三个月，并处罚金人民币一万元（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人陈某丙犯诈骗罪，判处有期徒刑一年，缓刑一年三个月，并处罚金人民币九千元（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人陈某丁犯帮助信息网络犯罪活动罪，判处有期徒刑一年三个月，缓刑一年六个月，并处罚金人民币一万元（已预缴）。

（缓刑考验期限，从判决确定之日起计算）

被告人吴某犯帮助信息网络犯罪活动罪，判处罚金人民币七千元（已预缴）。

被告人黄某甲犯帮助信息网络犯罪活动罪，判处罚金人民币七千元（已预缴）。

被告人林某犯帮助信息网络犯罪活动罪，判处罚金人民币七千元（已预缴）。

被告人王某乙犯帮助信息网络犯罪活动罪，判处罚金人民币七千元（已预缴）。

二、被告人赵松明、沙某甲、李某、王某甲、杨某、冯某、潘某、周某、程某、沙某乙、龙某、陈某甲、余某、陈某乙、陈某丙已退缴在案的赃款人民币 294048 元，发还各被害人。

被告人陈某丁已退缴在案的赃款人民币 40000 元，予以没收，上缴国库。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向江苏省南通市中级人民法院提出上诉。

书面上诉的，应当提交上诉状正本一份，副本二十一份。

审判长王麒锟

人民陪审员朱伯平

人民陪审员顾凯贤

二〇一八年九月十七

案例五、朱长余、肖申等诈骗罪郑奎、李继斌等帮助信息网络犯罪活动罪邓少华、杨佳林等侵犯公民个人信息案

绍兴市越城区人民法院刑事判决书

案号：（2017）浙 0602 刑初 293 号

公诉机关绍兴市越城区人民检察院。

被告人朱长余，男，1988 年 10 月 25 日出生于天津市，汉族，高中文化，无业，住天津市宝坻区。因涉嫌犯诈骗罪于 2016 年 6 月 1 日被原绍兴市公安局高新分局刑事拘留，同年 7 月 8 日变更为取保候审。2017 年 6 月 23 日，经本院决定被逮捕。现羁押于绍兴市看守所。

辩护人谢伟强，浙江法校律师事务所律师。

被告人肖申，男，1988 年 4 月 10 日出生于天津市，汉族，初中文化，无业，住天津市宝坻区。因涉嫌犯诈骗罪于 2016 年 6 月 2 日被原绍兴市公安局高新分局刑事拘留，同年 7 月 8 日变更为取保候审。2017 年 6 月 23 日，经本院决定被逮捕。现羁押于绍兴市看守所。

辩护人于岩，浙江和畅律师事务所律师。

被告人戎丹平，男，1990 年 5 月 21 日出生于江苏省丹阳市，汉族，大专文化，无业，住江苏省丹阳市。因涉嫌犯诈骗罪于 2016 年 6 月 2 日被原绍兴市公安局高新分局刑事拘留，同年 7 月 8 日变更为取保候审。2017 年 6 月 23 日，经本院决定被逮捕。现羁押于绍兴市看守所。

辩护人蔡政伟，江苏朱方律师事务所律师。

被告人郑奎，男，1989 年 2 月 4 日出生于四川省富顺县，汉族，职高文化，无业，住四川省富顺县。因涉嫌犯侵犯公民个人信息罪于 2016 年 7 月 6 日被原绍兴市公安局高新分局刑事拘留，同年 8 月 12 日被逮捕。现羁押于绍兴市看守所。

辩护人王牡丹，浙江国大律师事务所律师。

被告人李继斌，男，1985 年 7 月 6 日出生于广西壮族自治区临桂县，汉族，高中文化，原系广西买号街网络科技有限公司法定代表人，住广西壮族自治区临桂县。因涉嫌犯侵犯公民个人信息罪于 2016 年 7 月 6 日被原绍兴市公安局高新分局刑事拘留，同年 8 月 12 日被逮捕。现羁押于绍兴市看守所。

辩护人谢佑息，广西嘉宸律师事务所律师。

辩护人祝云昌，浙江法校律师事务所律师。

被告人周建国，男，1978 年 10 月 1 日出生于广西壮族自治区临桂县，汉族，小学文化，原系广西买号街网络科技有限公司股东，住广西壮族自治区临桂县。因涉嫌犯侵犯公民个人信息罪于 2016 年 7 月 6 日被原绍兴市公安局高新分局刑事拘留，同年 8 月 12 日变更为取保候审。2017 年 6 月 23 日，经本院决定被逮捕。现羁押于绍兴市看守所。

被告人蒋培密，男，1989 年 1 月 30 日出生于广西壮族自治区全州县，汉族，大专文化，

原系广西买号街网络科技有限公司员工，住广西壮族自治区全州县。因涉嫌犯侵犯公民个人信息罪于2016年7月6日被原绍兴市公安局高新分局刑事拘留，同年8月12日变更为取保候审。2017年6月23日，经本院决定被逮捕。现羁押于绍兴市看守所。

被告人蓝红峰，男，1989年10月4日出生于广西壮族自治区忻城县，壮族，大专文化，原系广西买号街网络科技有限公司员工，住广西壮族自治区桂林市象山区。因涉嫌犯侵犯公民个人信息罪于2016年7月6日被原绍兴市公安局高新分局刑事拘留，同年8月12日变更为取保候审。2017年6月23日，经本院决定被逮捕。现羁押于绍兴市看守所。

被告人蒙昌华，男，1996年6月4日出生于广西壮族自治区桂林市，汉族，职高文化，原系广西买号街网络科技有限公司员工，住广西壮族自治区桂林市秀峰区。因涉嫌犯侵犯公民个人信息罪于2016年7月6日被原绍兴市公安局高新分局刑事拘留，同年8月12日变更为取保候审。2017年6月23日，经本院决定被逮捕。现羁押于绍兴市看守所。

辩护人王青松、方彩虹，北京中银（杭州）律师事务所律师。

被告人邓少华，男，1993年1月29日出生于湖南省邵阳市，汉族，初中文化，无业，住湖南省邵阳市双清区。因涉嫌犯侵犯公民个人信息罪于2016年6月26日被原绍兴市公安局高新分局刑事拘留，同年8月2日被逮捕。2017年1月11日变更为取保候审。2017年6月23日，经本院决定被逮捕。现羁押于绍兴市看守所。

辩护人章观庆，浙江敏杰律师事务所律师。

被告人杨佳林，曾用名杨金林，男，1993年10月8日出生于浙江省平湖市，汉族，初中文化，无业，住浙江省平湖市。2012年10月12日因犯盗窃罪被浙江省平湖市人民法院判处有期徒刑十个月，并处罚金人民币三千元。因涉嫌犯侵犯公民个人信息罪于2016年6月29日被原绍兴市公安局高新分局刑事拘留，同年8月2日被逮捕。2017年1月11日变更为取保候审。2017年6月23日，经本院决定被逮捕。现羁押于绍兴市看守所。

辩护人陈忠杰，浙江信专律师事务所律师。

被告人王安，男，1986年4月13日出生于湖南省浏阳市，汉族，初中文化，农民，住湖南省浏阳市。因涉嫌犯诈骗罪于2016年6月22日被原绍兴市公安局高新分局刑事拘留，同年7月15日变更为取保候审。2017年6月23日，经本院决定被逮捕。现羁押于绍兴市看守所。

被告人彭永新，男，1991年2月18日出生于湖南省宁远县，汉族，高中文化，农民，住湖南省宁远县。因涉嫌犯诈骗罪于2016年6月8日被原绍兴市公安局高新分局刑事拘留，同年7月8日变更为取保候审。2017年6月23日，经本院决定被逮捕。同日，变更为指定居所监视居住。同年12月9日，变更为取保候审。现取保候审于居住地。

辩护人唐佳莉，浙江敏杰律师事务所律师。

被告人杨迪红，男，1981年7月12日出生于湖南省ＸＸ瑶族自治县，瑶族，中专文化，无业，住湖南省ＸＸ瑶族自治县。因涉嫌犯诈骗罪于2016年6月24日被原绍兴市公安局高

新分局刑事拘留，同年 7 月 24 日变更为取保候审。2017 年 6 月 23 日，经本院决定被逮捕。现羁押于绍兴市看守所。

被告人黄为帅，男，1989 年 8 月 10 日出生于湖北省汉川市，汉族，初中文化，无业，住湖北省汉川市。因涉嫌犯诈骗罪于 2016 年 6 月 22 日被原绍兴市公安局高新分局刑事拘留，同年 7 月 22 日变更为取保候审。2017 年 6 月 23 日，经本院决定被逮捕。现羁押于绍兴市看守所。

辩护人刘胤，浙江大公律师事务律师。

被告人王玉建，男，1985 年 2 月 7 日出生于湖北省宜城市，汉族，大学文化，无业，住湖北省宜城市。因涉嫌犯诈骗罪于 2016 年 6 月 24 日被原绍兴市公安局高新分局刑事拘留，同年 7 月 24 日变更为取保候审。2017 年 6 月 23 日，经本院决定被逮捕。现羁押于绍兴市看守所。

辩护人鲁萧迪，浙江大公律师事务所律师。

绍兴市越城区人民检察院以越检公诉刑诉〔2017〕214 号起诉书指控被告人朱长余、肖申、戎丹平犯诈骗罪，被告人郑奎、李继斌、周建国、蒋培密、蓝红峰、蒙昌华犯帮助信息网络犯罪活动罪，被告人邓少华、杨佳林、王安、彭永新、杨迪红、黄为帅、王玉建犯侵犯公民个人信息罪，于 2017 年 4 月 7 日向本院提起公诉。本院于同月 10 日立案受理，并依法组成合议庭，适用简易程序审理。因在审理中发现本案具有不宜适用简易程序审理的情形，遂将本案转为普通程序审理。同年 6 月 6 日，绍兴市越城区人民检察院以越检公诉刑变诉〔2017〕4 号变更起诉决定书对起诉法律适用予以变更，本院受理后公开开庭进行了审理。绍兴市越城区人民检察院指派检察员潘某、朱某 1、徐某出庭支持公诉，上列十六被告人及被告人的辩护人均到庭参加了诉讼。经绍兴市越城区人民检察院建议，本院分别于 2017 年 8 月 14 日、2017 年 12 月 12 日决定对本案延期审理，并于 2017 年 9 月 12 日、2018 年 1 月 12 日分别决定恢复对本案的审理。现已审理终结。

绍兴市越城区人民检察院指控:

一、诈骗

2016 年 4 月以来，被告人朱长余、肖申、戎丹平合谋采用“钓鱼软件”形式骗取被害人钱款。

其中，被告人戎丹平负责编写“钓鱼软件”，通过软件修改被害人支付宝充值页面上的显示金额，由被告人朱长余、肖申负责租赁淘宝店铺，将上述加载“钓鱼软件”的虚构的映客钻石充值等商品在淘宝店铺出售，被告人肖申还负责转账、取现等工作。

截止案发，三被告人共骗取被害人蔡某等人支付宝内钱款合计人民币 60000 余元。

二、帮助信息网络犯罪活动

1.2014 年以来，被告人郑奎开发建立 PEAS 云网络交易平台，在明知他人利用该平台进行实名注册账号交易的情况下，仍提供网站存储、通讯传输等技术支持，以及支付结算等帮

助，并通过收取 2%的交易手续费获得非法利益。

截至案发，通过 PEAS 云网络交易平台成交的账号交易金额为人民币 23496417 元，被告人郑奎共收取手续费 469928 元。

2.2015 年 5 月以来，被告人李继斌、周建国以买号街网站为平台，会同被告人蒋培密、蓝红峰、蒙昌华等人，在明知他人利用买号街网站进行实名注册账号销售的情况下，仍提供网站存储、通讯传输等技术支持，以及支付结算等帮助，并通过收取每笔 3.8%至 7%不等的交易手续费及每笔 0.5%的提现手续费获得非法利益。

其中被告人李继斌负责买号街网站的总体运营，被告人周建国负责后勤保障等工作，被告人蒋培密、蓝红峰负责网站日常维护，被告人蒙昌华负责网站业务推广等工作。

至案发，共有 689514 个实名账号通过买号街网站进行销售。

三、侵犯公民个人信息

1.2015 年 5 月以来，被告人邓少华从他人处购得含有公民姓名、身份号码等信息的支付宝、淘宝实名账号，多次在买号街网站贩卖获利。

至案发，被告人邓少华通过在买号街网站注册的“zz5104393”账号，出售上述实名账号××个，并提现人民币 3920 元。

2.2015 年 5 月以来，被告人杨佳林从他人处购得含有公民姓名、身份号码等信息的支付宝、淘宝实名账号，多次在买号街网站贩卖获利。

至案发，被告人杨佳林通过在买号街网站注册的“至尊宝”账号，出售上述实名账号××个，并提现人民币 8690 元。

3.2015 年 11 月以来，被告人王安从他人处购得含有公民姓名、身份号码等信息的支付宝、淘宝实名账号，多次在买号街网站贩卖获利。

至案发，被告人王安通过在买号街网站注册的“anan888”账号，出售上述实名账号××个，并提现人民币 10800 元。

4.2015 年 11 月以来，被告人彭永新从他人处购得含有公民姓名、身份号码等信息的支付宝、淘宝实名账号，多次在买号街网站贩卖获利。

至案发，被告人彭永新通过在买号街网站注册的“小号专卖店”账号，出售上述实名账号××个，成交金额人民币 17987.96 元，尚有非法获得的 50 万个实名账号存储于百度云盘未予出售。

5.2016 年 3 月以来，被告人杨迪红从他人处购得含有公民姓名、身份号码等信息的支付宝、淘宝实名账号，多次在买号街网站贩卖获利。

至案发，被告人杨迪红通过在买号街网站注册的“SCOTT”账号，出售上述实名账号××个，并提现人民币 25680 元。

6.2016 年 3 月以来，被告人黄为帅从他人处购得含有公民姓名、身份号码等信息的支付宝、淘宝实名账号，多次在买号街、PEAS 云网络交易平台贩卖获利。

至案发，被告人黄为帅通过在买号街网站注册的“小黄工作室”账号，出售上述实名账号××个，并提现人民币 26644 元；通过在 PEAS 云网络平台注册的 905×××@ｑｑ．ｃｏｍ账号，出售了包含上述实名账号在内的××余个账户，并提现人民币 24500 余元。

7.2016 年 4 月以来，被告人王玉建从他人处购得含有公民姓名、身份号码等信息的支付宝、淘宝实名账号，多次在买号街网站贩卖获利。

至案发，被告人王玉建通过在买号街网站注册的“wyjy1520”账号，出售上述实名账号××个，并提现人民币 81394 元。

2016 年 5 月 31 日，被告人朱长余被警察抓获；同年 6 月 1 日，在被告人朱长余的协助下，被告人戎丹平被警察抓获；同日，被告人肖申被警察抓获。

同年 6 月 7 日，被告人彭永新被警察抓获；同月 22 日，被告人黄为帅、王安被警察抓获；同月 23 日，被告人王玉建、杨迪红被警察抓获；同月 25 日，被告人邓少华被警察抓获；同月 28 日，被告人杨佳林被警察抓获。

同年 7 月 5 日，被告人李继斌、周建国、蒋培密、蓝红峰、蒙昌华、郑奎被警察抓获。

案发后，被告人朱长余、戎丹平、肖申、彭永新各退赃人民币 20000 元，被告人杨佳林退赃人民币 8690 元，被告人邓少华退赃人民币 3920 元。

为证明上述事实，公诉机关当庭宣读和出示了相关证据。

公诉机关认为，被告人朱长余、肖申、戎丹平以非法占有为目的，合伙采用虚构事实、隐瞒真相的手段骗取他人财物，数额巨大，且系共同犯罪，均应当以诈骗罪追究刑事责任。

被告人郑奎、李继斌、周建国、蒋培密、蓝红峰、蒙昌华明知他人利用信息网络实施犯罪，仍提供帮助行为，情节严重，且被告人李继斌、周建国、蒋培密、蓝红峰、蒙昌华系共同犯罪，均应当以帮助信息网络犯罪活动罪追究刑事责任。

被告人邓少华、杨佳林、王安、彭永新、杨迪红、黄为帅、王玉建违反国家有关规定，向他人出售公民个人信息，情节严重，应当分别以侵犯公民个人信息罪追究刑事责任。

被告人朱长余协助公安机关抓获同案犯，属立功。

后公诉机关变更指控认为被告人邓少华、杨佳林、王安、彭永新、杨迪红、黄为帅、王玉建违反国家有关规定，非法获取、向他人出售公民个人信息，其中被告人邓少华、彭永新、王玉建均属情节特别严重，被告人杨佳林、王安、杨迪红、黄为帅均属情节严重，均应当以侵犯公民个人信息罪追究刑事责任。

提请本院分别依照《中华人民共和国刑法》第二百六十六条　、第二百八十七条　之二、第二百五十三条　之一、第六十八条　、第二十五条　之规定判处。

被告人朱长余、肖申、戎丹平当庭表示对起诉指控的事实及罪名无异议，并请求从轻处罚。

被告人朱长余、肖申同时辩解到几人的获利由“钓鱼软件”、“秒单”两种方式获得，对于“秒单”的获利方式被告人戎丹平不知情。

被告人郑奎辩解称，在 PEAS 云平台交易的账号包括非实名账号，账号交易金额及收取的手续费的认定应当扣除非实名账号部分。

收取的手续费中有 50%的成本支出。

被告人郑奎同时请求从轻处罚。

被告人李继斌辩称:1.在买号街平台销售的实名账号不足起诉指控的数量，该数量与网站的交易额及账号单价的换算结果不符。

在买号街平台上销售的账号有实名、非实名之分，在数量认定上应予以区分。

卖家在买号街平台销售账号时有刷单的情况。

2.在经营中未收取“每笔 0.5%的提现手续费”，该手续费为支付宝的转账手续费，非其等人的获利所得。

3.其在经营买号街过程中，没有验证过账号的真实性，因此其等人的行为不属于明知他人实施销售实名账号的违法行为而提供网络帮助。

4.买号街平台只是一个通用交易网站，在网站上发布商品有实名与非实名的区分，但这不意味着平台允许销售未经授权的实名账号。

5.周建国只是投资股东，并不负责买号街平台的任何工作。

被告人周建国对起诉指控的事实及罪名无异议，并请求从轻处罚。

同时辩称其只是名义上的股东，其在公司仅是一个打杂的角色。

被告人蒋培密辩称，其与公司系正常的劳动用工关系，其与其他被告人非共同犯罪。

其只在指控的部分时间段从事了网站开发工作，非全程参与。

其未意识到销售实名账号违法。

被告人蒋培密同时请求从轻处罚。

被告人蓝红峰辩称，其只是给公司打工，不知道公司的行为违法。

被告人蓝红峰同时请求从轻处罚。

被告人蒙昌华辩称，其不知道其的行为属于犯罪，其与被告人李继斌等人不构成共同犯罪，且其也不是推广部的负责人。

被告人蒙昌华同时请求从轻处罚。

被告人邓少华辩称，2015 年 11 月之前的统计数据不应当计算在销售数据中。

其有举报他人违法犯罪的立功表现。

被告人邓少华同时请求从轻处罚。

被告人杨佳林辩称，统计数据中有重复信息，并请求从轻处罚。

被告人王安辩称，其销售的账号有实名与非实名之分，对提现的总金额及销售总量无异议。

被告人彭永新辩称，尚未销售的 50 万个账号其未核实真假，并请求从轻处罚。

被告人杨迪红对起诉指控的事实及罪名无异议，并请求从轻处罚。

被告人黄为帅辩称，其的销售记录中有大约一千条自卖自买的情况，但自卖自买时使用的账号已经记不清楚了。

其销售的未实名账号（××%至 30%左右的比例）不应计算在指控数额中。

被告人王玉建辩称，其对提现钱款的认定有异议，提现的钱款中包括非公民个人信息的销售收入以及“白号”的销售收入，其总共的获利不到 20000 元。

被告人王玉建同时请求从轻处罚。

被告人朱长余的辩护人主要提出以下意见:1.现有证据不足以证明被告人的诈骗所得为 6 万元，有被害人陈述证实的犯罪金额仅有 6 千余元。

且该 6 万元系通过“钓鱼软件”、“秒单”两种方式获得，而“秒单”的情况在本案中属事实不清。

2.被告人朱长余到案后如实供述了自己的犯罪事实，并积极退赃，悔罪态度良好，且已获得了已查明的 4 名被害人的谅解。

3.被告人朱长余有立功表现，亦系初犯、偶犯。

综上，请求对被告人朱长余减轻处罚并适用缓刑。

被告人肖申的辩护人主要提出以下意见:1.起诉指控的 6 万元获利中，只有部分属于通过“钓鱼软件”方式取得，还有部分系通过“秒单”方式获得，而现有证据无法认定“秒单”的行为性质，故指控犯罪金额不应认定为 6 万元。

被告人当庭供述“钓鱼软件”的获利为 2 万余元，应认定为“数额较大”。

2.被告人的行为定性应当认定为盗窃，虽然被害人有部分错误认识，但被告人系通过秘密手段取得钱款，被害人并无处分财产的行为。

3.被告人的行为全部发生在 2016 年 12 月 20 日之前，最高人民法院、最高人民检察院、公安部于 2016 年 12 月 20 日出台的《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》不应适用到本案中。

被告人戎丹平的辩护人主要提出以下意见:1.本案指控的 6 万元获利系通过两种行为方式取得，被告人戎丹平对“秒单”的行为方式不知情，通过“钓鱼软件”获得的金额为 25000 元左右，故应认定为犯罪数额较大。

2.被告人戎丹平到案后如实交代了案发事实，系初犯，且积极退赃，并获得了已查明的被害人的谅解。

综上，请求对被告人戎丹平从轻处罚并适用缓刑。

被告人郑奎的辩护人主要提出以下意见:1.在交易金额、手续费数额的认定中应当扣除非实名账户的部分。

2.被告人郑奎涉嫌的罪名系刑法修正案九新设罪名，故 2015 年 11 月 1 日之前的销售数据应当予以扣除。

3.被告人郑奎在行为过程中有向第三方支付手续费，应当在金额认定中予以考量。

4.被告人郑奎系初犯，且如实供述了自己的罪行。

综上，请求对被告人郑奎从轻处罚并适用缓刑。

被告人李继斌的辩护人主要提出以下意见:1.被告人李继斌等人的主观恶性较小，买号街平台只起到中介作用，系被他人恶意利用。

2.起诉指控在买号街平台销售的账号××万余个与事实不符，买号街平台销售的部分账号系非实名账号，且存在刷单现象，对该部分数据应予以扣除。

3.被告人涉及的罪名系刑法修正案九新设罪名，刑法修正案九实施之前的行为不应认定为犯罪。

4.被告人李继斌系初犯，到案后如实供述了犯罪事实，且有悔罪表现。

综上，请求对被告人李继斌从轻处罚并适用缓刑。

被告人蒙昌华的辩护人主要提出以下意见:1.被告人蒙昌华的行为不构成帮助信息网络犯罪活动罪。

首先，买号街是一个中介平台，被告人不直接参与账号的交易行为，且网络账号的销售并不为法律所禁止；其次，涉案事实亦属于单位行为，被告人蒙昌华的行为只是履行正常的工作职务，其不是公司主管及直接责任人员，不是推广部的负责人，不应当追究其刑事责任；再次，本罪以“明知”为犯罪构成要件，而被告人无核实平台销售信息真实性的能力，因此其并不明知在平台上交易的账号侵犯了公民个人信息。

2.被告人蒙昌华的涉案行为情节显著轻微，危害不大，应当免予刑事处罚。

3.如若构成犯罪，根据本案事实应当区分主从犯，且被告人蒙昌华应当认定为从犯。

被告人邓少华的辩护人主要提出以下意见:1.被告人邓少华销售的账户应当认定为3万余条，2015年11月1日之前销售的数量应当予以扣除，因此被告人邓少华的行为并不属于情节特别严重。

2.被告人邓少华销售信息的真实性存疑，公安机关仅对其中的50条进行了验证，可信度不高。

3.被告人邓少华有立功表现，且认罪、悔罪，积极退赃。

综上，请求对被告人邓少华减轻处罚并适用缓刑。

被告人杨佳林的辩护人主要提出以下意见:1.起诉指控被告人杨佳林销售的实名账号的数量及提现金额的证据不足，统计数据中存在信息重复、错误等情况。

辩护人通过软件去重后，实名账户最多只有4508个。

2.被告人杨佳林已经退缴了指控认定的非法所得8690元。

综上，请求对被告人杨佳林减轻处罚。

被告人彭永新的辩护人主要提出以下意见:1.被告人彭永新销售数据的真实性未经验证，且未销售的50万条数据未产生危害后果。

2.被告人彭永新到案后如实供述了犯罪事实，其系初犯，且积极退赃。

综上，请求结合被告人彭永新的身体健康状况对其适用缓刑。

被告人黄为帅的辩护人主要提出以下意见:1.起诉指控的事实中未对账号进行区分，对于虚假账号、一号多卖、重复账号、被告人自卖自买等情况应当予以核减。

公安机关随机验证的50条信息不足以推定所有信息的真实性。

2.被告人黄为帅系初犯、偶犯，且积极退赃。

综上，请求对被告人黄为帅适用缓刑。

被告人王玉建的辩护人主要提出以下意见:1.现有证据不足以证实起诉指控的销售账号的数量以及提现的金额，服务器后台记录的数据属于孤证，不足以作为销售数量认定。

被告人销售的账号包括非实名账号、“白号”、账号真实性存疑、有误、信息不全、不能识别等情况，应当对上述账号在数量及金额上予以核减。

综上，本案认定被告人王玉建属“情节特别严重”的事实不清、证据不足。

2.被告人王玉建的行为构成自首，且在案发前已经主动停止了犯罪。

3.被告人王玉建已根据起诉指控的获利金额进行了全额退赃。

综上，请求对被告人王玉建从轻处罚并适用缓刑。

经审理查明:

一、盗窃

2016年4月以来，被告人朱长余、肖申、戎丹平合谋采用“钓鱼软件”修改实际支付金额的形式占有被害人钱财。

其中，被告人戎丹平负责编写“钓鱼软件”，被告人朱长余、肖申负责租赁淘宝店铺，并通过“销售”映客钻石充值等商品的形式诱骗被害人通过“钓鱼软件”支付与页面显示金额不符的钱款。

至案发，三被告人共计非法获利人民币6万余元。

2016年5月31日，被告人朱长余被警察抓获归案；同年6月1日，在被告人朱长余的协助下，被告人戎丹平被警察抓获归案；同日，被告人肖申被警察抓获归案。

案发后，三被告人分别退缴赃款人民币2万元。

上述事实，由公诉机关提交，并经庭审质证的下列证据予以证实:

（1）被告人朱长余的供述，证实其对起诉指控的事实供认不讳。

其等人的诈骗行为始于2016年4月，行为方式是利用钓鱼软件修改支付金额实施的，具体内容为淘宝店铺映客钻石充值、CF刷枪、生死狙击刷枪等，软件由戎丹平编写，肖申与其负责租赁淘宝店铺、转账、取款等工作，共骗得钱款合计人民币6万余元，其分得2万余元。

其用过“恭喜发财”、“奶牛”的QQ账号发布租用淘宝店铺的信息，作案用的支付宝账号系从买号街平台购买，控制被害人的钱款后通过“泡泡”洗钱。

（2）被告人肖申的供述，证实其对起诉指控的事实供认不讳。

2016年4月以来，其与朱长余、戎丹平经事先商议通过钓鱼软件进行网络诈骗，戎丹平编写、维护映客充值钓鱼软件，软件功能就是修改支付金额，朱长余与其负责租赁淘宝店铺、发布广告、购买作案用支付宝账号、转账、取现等。

其三人共骗得钱款合计人民币6万余元，其分得2万余元。

租用淘宝店铺的广告有通过“恭喜发财”的QQ账号发布过。

被告人肖申供述行为过程中使用过的支付宝账号包括姓名为车某、陈某、任某、蒙美琼、韩某的账号，相关账号有通过买号街平台购买。

（3）被告人戎丹平的供述，证实其对起诉指控的事实供认不讳。

2016年4月以来，其与朱长余、肖申经商量通过钓鱼软件进行网络诈骗，其负责编写钓鱼软件、网页设计，并将软件链接编写入虚构的映客钻石充值商品，后上传至淘宝店铺。

钓鱼软件可以修改页面上显示的买家支付金额，买家实际支付的金额要高于页面显示金额。

朱长余、肖申负责租赁淘宝店铺、转账等工作。

通过钓鱼软件获得的钱款三人平分，其分得2万余元。

（4）证人顾某的证言，证实2016年3月26日以来，其曾在网络上将几个淘宝店铺以100元每天的价格租给“恭喜发财”、“奶牛”的QQ号主使用。

支付宝交易记录证实其与“奶牛”的交易情况，对方使用的支付宝账号包括杨某、李某。

聊天记录，证实其与“恭喜发财”、“奶牛”在租赁淘宝店铺时的交流情况。

（5）证人郭某、朱某2、成某的证言，证实几人曾将注册的淘宝店铺通过其同学顾某出租给他人使用。

（6）被害人蔡某的陈述，证实2016年4月15日下午，其在绍兴东方宾馆上网，其在淘宝店购买映客礼物过程中非正常支付了2059元，当时淘宝上显示购买价格是2元。

支付宝转账记录证实了其的转账情况，对方账户为陈某。

（7）被害人张某的陈述，证实2016年4月13日中午，其在淘宝店铺购买映客充值商品时被骗了1800元，充值时其选择的充值金额为98元，实际转走的金额是1800元。

对方账户是车某。

支付宝转账记录证实张某的转账情况。

聊天记录证实张某在充值时与“嵩哥的小店”的交流情况。

（8）被害人王某的陈述，证实2016年4月9日，其在淘宝店购买映客钻石充值时被骗了1900元，对方账户是任某，后对方通过蒙美琼的支付宝返还了200元。

支付宝转账记录印证了被害人王某的陈述。

（9）被害人林某1的陈述，证实2016年4月6日，其在淘宝店购买映客钻石充值时被骗了900元，其选择的充值金额为30元，对方账号叫韩某。

支付宝转账记录印证了被害人林某1的陈述。

（10）收款账户信息，证实被告人朱长余在微博上的收款账户情况。

富贵论坛截屏，证实被告人朱长余在富贵论坛发布租赁淘宝店铺信息的情况。

买号街界面截图证实被告人朱长余在买号街购买账号的记录。

钓鱼软件源代码截图，证实被告人戎丹平编写的部分钓鱼软件源代码情况。

支付宝账号清单，证实被告人朱长余购买的实名支付宝账号情况，包括李某、林某2、蒙美琼等人的账号。

（11）搜查笔录、搜查照片、扣押清单，证实公安机关对被告人戎丹平住所、工作地的搜查情况，在其住所扣押白色外壳电脑主机1台，在其工作地扣押红黄外壳、黑色外壳电脑主机各1台。

公安机关已扣押了被告人朱长余、肖申、戎丹平赃款各2万元。

（12）抓获经过，证实被告人朱长余、戎丹平、肖申的到案情况。

关于被告人及三被告人的辩护人就三被告人非法占有被害人钱款的行为方式提出的意见，审理认为:1.通过“秒单”方式非法占有被害人钱款的事实只有被告人朱长余、肖申的部分供述证明，无其他证据印证。

三被告人在审查起诉阶段均未提及有通过“秒单”方式非法占有被害人钱款的情况。

2.被告人肖申在第一次讯问笔录中明确供述“通过映客钓鱼软件骗来的钱每人分到了2万多元”。

其在审查起诉阶段供述“通过‘钓鱼软件’占有的被害人的钱款，其转给了‘泡泡’，‘泡泡’洗钱后再转到银行卡，其再把钱取出三人平分，其分到2万多”，而在被告人朱长余、肖申的供述中，并未提及“泡泡”系“秒单”的合作参与者，即被告人肖申再次确认了“每人2万元”非“秒单”所得。

3.被告人朱长余、肖申均辩解“秒单”的方式被告人戎丹平不知情，若此供述属实，且“平分后，每人2万元”的非法获利包含“秒单”方式占有的钱款亦属实，则出现被告人戎丹平对“秒单”收入“不劳而获”的事实，且“不劳而获”的数额超过非法获利的一半，不符合常理。

4.被告人戎丹平自始至终供述其分得的2万元系通过“钓鱼软件”获利所得。

综上，应当认定涉案的6万元钱款系被告人朱长余、肖申、戎丹平通过“钓鱼软件”修改支付金额的方式获得。

被告人及辩护人就上述事实提出的异议，本院均不予采纳。

二、非法利用信息网络

1.2014年以来，被告人郑奎开发设立PEAS云网络交易平台，在明知他人进行公民个人信息账号交易的情况下，仍将上述交易平台提供给他人使用，供交易者存储、流转公民个人信息，并收取交易手续费以牟取利益。

至案发，被告人郑奎通过PEAS云网络交易平台共计收取交易手续费41万余元。

2016 年 7 月 5 日，被告人郑奎被警察抓获归案。

上述事实，由公诉机关提交，并经庭审质证的下列证据予以证实:

（1）被告人郑奎的供述，证实 PEAS 云网站是 2014 年开始运行的，是一个数字商品交易平台，卖家在网站上可以卖 QQ、微信、邮箱、淘宝、支付宝等账号。

在网站上交易，每天晚上 23 点自动结算一次，次日早上人工处理给卖家打款。

在网站上，有一些卖家在出售通过公民姓名、身份号码、邮箱、手机、银行卡等信息实名验证的淘宝、支付宝账号，这种情况在 PEAS 云网站一开始运营就有的，其是在处理维权纠纷、日常订单审核时发现的。

其看很多网站都在卖，所以也没太在意。

卖家上传的实名账号基本是批量上传的，因此不会是卖家本人的，这些账号是用去刷单的。

网站收取卖家提现金额的 2%作为交易管理费，其至少赚了 20 万元。

网站是一个交易中介，为交易提供担保服务以及第三方支付服务。

买家和卖家通过网站交易后，买家可以有 24 小时的时间验证账号的可用性，如果出现问题可以申请退款。

有上万个商户在平台上出售实名信息，通过网站已经出售的实名账号估计有个几十万个。

网站的服务器在阿里云，PEAS 云是其一个人运营的。

（2）被告人黄为帅的供述及其在 PEAS 云平台的提现记录、销售记录及清单，证实被告人黄为帅曾在 PEAS 云平台销售涉及公民个人信息相关数据的事实，具体信息清单显示被告人黄为帅在 PEAS 云平台销售的单条数据信息内容包括账号、密码、公民姓名、身份号码、销售状态等。

（3）PEAS 云数据库镜像还原过程，证实公安机关对 PEAS 云数据库进行还原，还原结果显示 PEAS 云平台收取的手续费为 411672.46 元。

（4）抓获经过，证实被告人郑奎的到案情况。

关于被告人郑奎及其辩护人对本节事实提出的意见，审理认为:被告人郑奎在行为过程中向第三方支付的手续费系其从事本案牟利行为的违法成本支出，不应在事实认定中予以扣减。

被告人郑奎及其辩护人就此提出的意见，本院不予采纳。

2.2015 年 5 月，被告人李继斌（股东、负责平台总体运营）、周建国（股东、负责后勤保障等）设立、运行买号街网站，并由被告人蒋培密、蓝红峰提供网站技术支持，被告人蒙昌华进行业务推广，在明知他人进行公民个人信息账号交易的情况下，仍将买号街交易平台提供给他人使用，供交易者存储、流转公民个人信息，并以收取手续费牟取利益。

至案发，买号街网络交易平台销售金额达 276 万余元，获利 18 万余元，注册会员近 3

万。

2016 年 7 月 5 日，被告人李继斌、周建国、蒋培密、蓝红峰、蒙昌华被抓获归案。

上述事实，由公诉机关提交，并经法庭质证的下列证据予以证实:

（1）被告人李继斌的供述，证实其是买号街的法人代表兼实际老板，周建国是股东，他平时在公司主要是做后勤保障、维护等工作，技术部有蒋培密、蓝红峰等人，客服有蒙昌华等人。

买号街是一个网站，提供淘宝账号密码、支付宝账号密码、邮箱账号密码、京东账号密码等虚拟账号交易的平台。

买号街是 2015 年 5 月开始运营的，卖家发布销售信息时需要填宝贝标题、设置价格、选择账号类型、选择账号属性即实名或非实名等。

买家买了账号后，钱是到卖家买号街的会员账户上，卖家提现需要申请。

卖家发布的信息买号街是不审核的。

平台上销售的实名账户就是绑定了姓名、身份号码、银行卡号等信息的账户，绑定的账号信息肯定不是卖家自己的，因为卖家在网站上寄售账号都是批量上传的。

买号街的作用就是提供交易平台、发布销售广告、提供服务器存储、自动发货、资金结算的服务等。

平台根据每笔交易成交金额的不同，收取成交金额 3.8%-7%不等的手续费。

客户提现的话，还会收取提现金额 0.5%的手续费，这个手续费是成本，没有利润。

其知道在平台上交易的账号是用来刷信誉、发广告之类用的。

买号街的后台数据在阿里云上，所有数据服务器里都存着的。

从 2016 年 2 月以来，平台每个月的成交金额大约在 20 万元左右。

平台业务员进行网站推广后，可以拿到成交金额 1%的提成。

（2）被告人周建国的供述，证实其是买号街的股东，占 10%的股份，在公司其主要从事后勤工作。

其没有实际出资，也没有参与分红。

买号街平台是 2015 年 5 月左右的开始运营的，主要从事微信、陌陌、京东、淘宝、支付宝等账号的交易，其知道买号街平台有实名账号交易的情况，跟买号街平台有关的人都知道这个情况，网站页面上也有实名、非实名账号的描述。

平台从账号交易中赚取手续费，卖家要从平台提现时需要提出申请，买家购买账号是用于发广告、刷信誉的。

公司主要负责人是李继斌，蒋培密、蓝红峰是技术员，蒙昌华是业务员。

（3）被告人蓝红峰的供述，证实公司的负责人是李继斌，周建国是股东，主要负责公司的日常后勤管理和维护工作，其属于公司的技术部，主要负责网站的页面设计。

买号街就是一个 QQ、歪歪、微信、淘宝、陌陌等账号的交易平台，是 2015 年 5 月开始

运营的。

账号是通过平台自动发货的，主要是淘宝、支付宝账号，QQ、微信等账号相对较少。

平台销售的账号有实名的，也有非实名的。

平台在销售实名账号的事情大家都知道的，页面上就能够看到。

平台是通过收手续费来获利，手续费从 3.8%到 7%不等。

买家的钱是支付到平台上的，卖家需要申请提现才能将平台上的钱转到自己的账户里。

（4）被告人蒋培密的供述，证实其是 2015 年 1 月到买号街上班的。

买号街的法定代表人是李继斌，主要负责公司的管理和运营。

公司还有一个经理周建国，主要负责公司的日常后勤管理和维护，其和蓝红峰是公司的程序员，主要负责网站的开发和维护，蒙昌华主要负责处理客服遇到的问题以及在网上推广平台。

买号街主要是为销售微信、QQ、淘宝、陌陌、京东、歪歪、支付宝等虚拟账号提供第三方交易平台，在平台上销售的有些账号是实名认证的，买家购买账号主要是用来刷信誉、发广告的。

平台是通过收取交易手续费获利的，费用从 3.8%到 7%不等，另外还要收取提现金额 0.5%的手续费。

平台上销售实名账号的情况，公司的人都是知道的，网站上也可以看到。

卖家上传账号的真实性，平台是不验证的。

（5）被告人蒙昌华的供述，证实其是 2015 年 11 月到公司上班的，其进去以后做的是推广员。

公司的老板叫李继斌，经理叫周建国，负责整个公司的所有日常事宜。

买号街是出售支付宝、QQ、淘宝、京东、vv 等账号的中介担保平台，其中有 80%是销售的淘宝、支付宝账号，公司从中收取交易手续费，卖家提现也会收取 5%的手续费。

其的工作是负责推广，加入 QQ 群发送广告、推广链接，客户点击链接交易后，就属于其做出来的业绩。

公司在百度贴吧也有一个发布推广广告的“买号街吧”。

公司的技术部会对账号的真实性进行验证，是用软件批量认证的。

买家购买账号时需要将钱款打入平台账户。

在售的支付宝账号包含有支付宝账号名称、密码、实名认证的人名、身份号码等信息。

这些出售的账号都是有问题的，账号经实名认证，一个人不可能有这么多账号的。

买家购买账号都是用于刷单、诈骗等用途。

到目前，其的总销售额 40 万是有的，工资加提成一共赚了 2 万多元。

（6）被告人邓少华、杨佳林、王安、彭永新、杨迪红、黄为帅、王玉建、朱长余等人的供述，证实几名被告人均在买号街网络交易平台进行实名网络账号交易的事实。

（7）全国企业信用信息公示系统截图，证实买号街的基本情况。

公司成立于成立日期为2015年1月，法定代表人为李继斌，注册资本500万元，股东李继斌认缴出资450万元，周建国认缴出资50万元。

（8）买号街网站部分页面截图，证实网页的“帮助中心”、“新手教程”为用户提供使用指引。

在交易纠纷处理中，平台有评判功能。

平台商品可以寄售，也可以担保形式销售。

在上架商品时，“选择账号分类”有明确“实名号”、“非实名号”的指示，上架的账号信息可以包括账号、密码、支付密码、邮箱账号、邮箱密码、姓名、身份号码、银行卡、手机号码等。

买家可以在网站购买的账号包括淘宝、阿某、支付宝、腾讯、歪歪、陌陌、京东等。

经蓝红峰辨认，证实了其设计的买号街网页的情况。

经蒋培密辨认，证实了买号街销售实名账号的网页情况。

经蒙昌华辨认，证实了其下线会员的销售、消费情况，总业绩46万余元。

（9）买号街数据库资料、买号街数据库统计结果、情况说明，证实买号街网络交易平台销售金额达276万余元，获利18万余元，注册会员近3万。

（10）抓获经过，证实被告人李继斌、周建国、蒋培密、蓝红峰、蒙昌华的到案情况。

在本节事实认定中，被告人李继斌等人向卖家收取提现手续费的事实已为本节事实涉案被告人及平台卖家被告人的供述所证实，即便该费用支付给了第三方，亦应当作为违法成本予以计算，不应从非法获利中予以扣除。

被告人李继斌就上述事实提出的意见，本院不予采纳。

三、侵犯公民个人信息

1.2015年5月以来，被告人邓少华非法获取他人个人信息后，在买号街平台予以销售牟利。

至案发，被告人邓少华共计通过买号街平台售出他人个人信息26000余条，其在平台作为卖家的交易额为4200余元，在2016年期间从平台提现人民币3920元。

2016年6月25日，被告人邓少华被警察抓获归案。

案发后，被告人邓少华已退赃人民币3920元。

上述事实，由公诉机关提交，并经庭审质证的下列证据予以证实:

（1）被告人邓少华的供述，证实其从2015年5月左右开始在网上出售公民个人信息。

身份号码和姓名的个人信息是通过百度的“网盘搜索”后，从网上下载下来的。

身份信息带银行卡的个人信息是从“社工库”网站上下载下来的。

实名支付宝账号是从“浮云网”购买来的。

这些个人信息其都是拿到买号街卖掉的。

其是在精易论坛上看到买号街上可以出售上述信息，网站是自助发货的，上传账号可以区分实名、非实名，在网站上销售的账号都是有销售记录的。

其在网上销售公民个人信息，网站肯定是知情的，其销售、提现都要收取手续费。

其销售的信息是经过其整理的，一共卖了二三万个账号信息，信息的具体内容包括身份号码和姓名，大部分还包括手机号码，有部分关联了银行账号、邮箱等。

一般信息几分钱一条，有银行卡等关联信息的可以卖到两三毛，其总共赚了 4300 多元。

（2）买号街页面账号截图，证实经被告人邓少华指认，其在该平台以卖家身份成功交易 301 笔，成交金额 4241.06 元。

（3）买号街账号提现明细，证实案发时，被告人邓少华的买号街平台账户尚存××年的提现记录 22 笔，共计 3920 元。

（4）出售账号的销售记录，证实被告人邓少华在买号街网络平台出售账号的详细信息，部分销售信息包括账号、姓名、身份号码、邮箱密码、支付密码等，部分销售信息显示为姓名、身份号码等。

（5）买号街后台数据库统计电子数据，证实该数据系从阿里云计算有限公司调取，被告人邓少华的“zz5104393”账号在买号街平台售出带身份号码的信息，且有买家账号信息显示的记录为 26652 条。

（6）情况说明，证实公安机关从被告人邓少华销售的公民个人信息记录中选取 50 条身份号码进行验证，经查询，上述 50 条身份号码均真实。

（7）抓获经过，证实被告人邓少华的到案情况。

（8）扣押、移送清单，证实被告人邓少华已向公诉机关退缴赃款人民币 3920 元。

2.2015 年 5 月以来，被告人杨佳林非法获取他人个人信息后，在买号街平台予以销售牟利。

至案发，被告人杨佳林共计通过买号街平台售出他人个人信息 4600 余条，其在买号街平台的成交金额为 9500 余元，从买号街平台提现人民币 8690 元。

2016 年 6 月 28 日，被告人杨佳林被警察抓获归案。

案发后，被告人杨佳林已退缴赃款人民币 8690 元。

2012 年 10 月 12 日，被告人杨佳林因犯盗窃罪被浙江省平湖市人民法院判处有期徒刑十个月，并处罚金人民币三千元。

该次犯罪时，被告人杨佳林系未成年人。

上述事实，由公诉机关提交，并经庭审质证的下列证据予以证实:

（1）被告人杨佳林的供述，证实其是从 2015 年 5 月开始销售实名支付宝账号的。

其销售的账号是从“拉牛网”、QQ 群买来的，然后再去买号街卖掉，其是在 QQ 群里看到买号街平台的广告。

销售账号平台是自动发货的，平台可以销售微信、QQ、支付宝、淘宝、阿某、京东等账

号，其中支付宝账号分实名、未实名，买号街对销售实名账号的情况肯定是知情的。

其销售的实名支付宝账号包含的信息有账号、登录密码、支付密码、身份号码、姓名等。

买号街是通过收取手续费获利的。

（2）买号街网络平台账号截图，证实被告人杨佳林的买号街平台账户“至尊宝”作为卖家共计交易609笔，成交金额为9588.1元。

（3）买号街账号提现明细，证实案发时，被告人杨佳林的买号街平台账户尚存××年的提现记录16笔，共计8690元。

（4）出售账号的销售记录，证实被告人杨佳林在买号街网络平台出售账号的详细信息，包括账号、姓名、身份号码、支付密码、银行卡等。

（5）买号街后台数据库统计数据，证实该数据系从阿里云计算有限公司调取，被告人杨佳林的“至尊宝”账号在买号街售出带身份号码的信息共计6058条，其中有买家账号信息显示的记录有4600余条。

（6）情况说明，证实公安机关从被告人杨佳林销售的公民个人信息记录中选取50条身份号码进行验证，经查询，选取的50条身份证号码均真实。

（7）抓获经过，证实被告人杨佳林的到案情况。

（8）刑事判决书，证实被告人杨佳林的前科情况。

（9）扣押清单，证实被告人杨佳林家属已向公诉机关退缴赃款人民币8690元。

3.2015年5月以来，被告人王安非法获取他人个人信息后，在买号街平台予以销售牟利。

至案发，被告人王安共计通过买号街平台售出他人个人信息3100余条，其在买号街平台的总成交金额11800余元，从买号街平台提现人民币10000元。

2016年6月22日，被告人王安被警察抓获归案。

上述事实，由公诉机关提交，并经庭审质证的下列证据予以证实:

（1）被告人王安的供述，证实其是2015年5月开始销售实名支付宝账号的，其销售的实名账号信息是通过QQ购买的，然后到买号街卖掉。

买号街有人在QQ群里发广告推广的，在平台上销售的账号有QQ、微信、淘宝、支付宝、陌陌、京东等，支付宝、微信的账号有实名、未实名。

买号街平台有一定的知名度，实行担保交易，且是自动发货的，提现需要支付手续费。

其销售的实名账号的信息包括淘宝ID、支付宝账号、登陆密码、支付密码、邮箱密码、姓名、身份号码等。

其在买号街平台上还有的销售记录有5000多条，有部分销售数据其已经删掉了，其获利有40000多元。

（2）买号街网络平台账号截图，证实被告人王安的买号街平台账户“anan888”作为卖家共计交易513笔，总成交金额11893元。

（3）买号街账号提现明细，证实案发时，被告人王安的买号街平台账户尚存××年间提现记录22笔，共计提现10000余元。

（4）出售账号的销售记录，证实被告人王安在买号街网络平台出售账号的详细信息，包括账号、邮箱账号及密码、支付登录、支付密码、姓名、身份号码等。

（5）买号街后台数据库统计数据，证实该数据系从阿里云计算有限公司调取，被告人王安的“anan888”账号在买号街售出带身份号码的信息共计7422条，其中有买家账号信息显示的记录有3100余条。

（6）情况说明，证实公安机关从被告人王安销售的公民个人信息记录中选取50条身份号码进行验证，经查询，选取的50条身份证号码均真实。

（7）抓获经过，证实被告人王安的到案情况。

4.2015年11月以来，被告人彭永新非法获取他人个人信息后，在买号街平台予以销售牟利。

至案发，被告人彭永新共计通过买号街平台售出他人个人信息620余条，其在买号街平台的成交总金额为人民币17900余元。

此外，被告人彭永新尚有非法获取的50万条公民个人信息存储于百度云盘欲予出售。

2016年6月7日，被告人彭永新被警察抓获归案。

案发后，公安机关从被告人彭永新处扣押了人民币2万元。

上述事实，由公诉机关提交，并经庭审质证的下列证据予以证实:

（1）被告人彭永新的供述，证实其知道网上倒卖实名支付宝、淘宝账号可以赚钱后，就于2015年11月开始做账号买卖的事情。

其在网上销售的账号有实名、非实名支付宝、淘宝账号、邮箱账号等，其中主要是实名的支付宝、淘宝账号。

实名账号就是绑定了姓名、身份号码等信息的账号。

其销售的账号是通过QQ群、买号街买来的，还有一些账号是其通过邮箱、身份信息等内容自己匹配出来的，其销售的账号其是验证过的，其销售的实名注册账号有××多个，获利一共有15000元左右。

其曾一次性向上家买过一批有50万人的12306的注册信息，信息包括注册账号、密码、手机号码、身份号码等，买来的价格是200多元，其验证过其中的30多个账号在支付宝的注册情况，验证通过后其卖掉了。

买号街是一个账号交易平台，平台上交易的账号主要有淘宝、支付宝、歪歪、QQ、陌陌、京东等，交易成功后平台会收取一定比例的费用。

其在买号街平台有两个账号，一个专门用来卖号，一个专门用来买号。

其通过买号街销售账号的情况网站都有记录的。

（2）搜查笔录及照片、扣押清单，证实公安机关对被告人彭永新的租房进行了搜查，

扣押了笔记本电脑 1 台、电脑主机 1 台。

（3）买号街网络平台账号截图，证实被告人彭永新的买号街平台账户“小号专卖店”作为卖家共计交易 526 笔，总成交金额 17987.96 元。

（4）出售账号的销售记录，证实被告人彭永新在买号街网络平台出售账号的详细信息，包括账号、登陆密码、支付密码、邮箱密码、姓名、身份号码等。

（5）买号街后台数据库统计数据，证实该数据系从阿里云计算有限公司调取，被告人彭永新的“小号专卖店”账号在买号街售出带身份号码的信息共计 735 条，其中 620 余条记录有买家账号信息显示。

（6）百度云管家截图、公民个人信息详情截图，证实被告人彭永新保存于百度云的 50 万条 12306 数据信息的情况，单条信息详情包括手机号码、邮箱地址、密码、用户名、密保、姓名、身份号码等。

（7）扣押清单，证实公安机关从被告人彭永新处扣押钱款人民币 2 万元。

（8）抓获经过，证实被告人彭永新的到案情况。

关于被告人及其辩护人对本节事实提出的意见，审理认为:被告人彭永新存储于“百度云”的 50 万条涉公民个人信息数据，被告人彭永新庭前供述对其中的部分数据进行过验证、匹配，且已出售，其当庭翻供未提出合理理由。

非法获取公民个人信息数据本身即是一种法益侵害后果。

故被告人彭永新提出其未对数据进行核实及辩护人提出该 50 万条数据未产生危害后果的意见，本院均不予采纳。

5.2016 年 3 月以来，被告人杨迪红非法获取他人个人信息后，在买号街平台予以销售牟利。

至案发，被告人杨迪红共计通过买号街平台售出他人个人信息 1700 余条。

2016 年 6 月 23 日，被告人杨迪红被警察抓获归案。

案发后，被告人杨迪红已向本院退缴钱款人民币 25680 元。

上述事实，由公诉机关提交，并经庭审质证的下列证据予以证实:

（1）被告人杨迪红的供述，证实其是 2016 年 3 月左右销售网络账号的，其销售的实名支付宝账号都是从网上买来的。

其是通过百度搜索找到买号街这个平台的。

买卖双方交易的钱是打在平台的，在平台交易需要支付手续费，卖家提现也需要支付手续费。

平台上销售的账号有微信、QQ、支付宝、淘宝、阿某、京东等，支付宝账号有实名、未实名的区别。

买号街平台有较高的知名度，实行担保交易，遇到交易纠纷，平台客服就会介入验证，发货由平台自动完成。

其在买号街平台一共卖了1800多个账号，获利在25000多元。

其在买号街平台销售的实名账号的信息具体包括支付宝账号、登录密码、支付密码、绑定的姓名、身份号码等。

其销售的账号记录原来电脑上是有记录的，后来其的亲戚彭永新因为倒卖账号被抓了，其就把记录删除了。

被告人供述的获利情况能与其在平台的提现情况相印证。

（2）实名账号详情，证实被告人杨迪红在买号街出售的公民信息的详细情况，信息内容包括用户名、密码、支付密码、姓名、身份号码等。

（3）买号街后台数据库统计数据，证实该数据系从阿里云计算有限公司调取，被告人杨迪红的“SCOTT”账号在买号街售出带身份号码的信息共计3768条，其中3400余条记录有买家账号信息显示。

该3400余条记录系以卖家姓名“000000”与卖家姓名“周秀华”进行了重复计算，故被告人杨迪红通过买号街平台售出的信息数量为1700余条，该记录基本能够与被告人的供述印证。

（4）情况说明，证实公安机关从被告人杨迪红销售的公民个人信息记录中选取50条身份号码进行验证，经查询，选取的50条身份号码均真实。

（5）抓获经过，证实被告人杨迪红的到案情况。

（6）本院执行、调解款票据，证实被告人杨迪红向本院退缴钱款的情况。

6.2016年3月以来，被告人黄为帅非法获取他人个人信息后，在买号街、PEAS云平台予以销售牟利。

至案发，被告人黄为帅共计通过买号街平台售出他人个人信息3000余条，其在买号街平台的成交金额达3万余元，并从该交易平台提现人民币26600余元。

被告人黄为帅共计通过PEAS云平台售出他人个人信息600余条，并从该交易平台提现人民币24500余元。

2016年6月22日，被告人黄为帅被警察抓获归案。

上述事实，由公诉机关提交，并经庭审质证的下列证据予以证实:

（1）被告人黄为帅的供述，证实其是从2016年3月开始销售网络账号的，其销售的淘宝、支付宝账号都是从网上买来的，其买来的账号一部分是淘宝账号和密码，一部分是实名支付宝账号，这些账号都绑定有姓名、身份号码等个人信息。

其销售的平台主要有PEAS云和买号街。

平台可以销售的账号包括QQ、微信、淘宝、支付宝、陌陌、京东等，支付宝、微信账号又分实名号和未实名号。

平台实行担保交易，可以售后维权。

卖家在平台提现需要支付手续费。

其销售的实名支付宝账号信息包括淘宝 ID、支付宝账号、登陆密码、支付密码、邮箱密码、姓名、身份号码等。

（2）买号街网络平台账号截图，证实被告人黄为帅的买号街平台账户“小黄工作室”作为卖家共计交易 1475 笔，总成交金额 30156.42 元。

（3）提现明细，证实 PEAS 云平台尚存被告人黄为帅 2016 年 5 月、6 月的提现记录，共计 29 条、24578.95 元。

买号街平台尚存被告人黄为帅的提现记录 21 条、26644 元。

（4）出售信息详情，证实被告人黄为帅在 PEAS 云平台销售的个人信息内容包含账号、密码、姓名、身份号码等，销售数量为 600 余条。

被告人黄为帅在买号街平台销售的个人信息内容包含账号、邮箱地址、邮箱密码、支付宝支付密码、姓名、身份号码等。

（5）买号街后台数据库统计数据，证实该数据系从阿里云计算有限公司调取，被告人黄为帅的“小黄工作室”账号在买号街售出带身份号码的信息共计 4432 条，其中有买家信息显示的记录有 3000 余条。

（6）情况说明，证实公安机关从被告人黄为帅销售的公民个人信息记录中选取 50 条身份号码进行验证，经查询，选取的 50 条身份号码均真实。

（7）抓获经过，证实被告人黄为帅的到案情况。

关于被告人及其辩护人对本节事实提出的意见，审理认为:被告人黄为帅提出在公民个人信息数据交易中，其有“自卖自买”情况的意见，除了其个人辩解外无其他证据印证，对该意见本院不予采信。

7.2016 年 4 月以来，被告人王玉建非法获取他人个人信息后，在买号街平台予以销售牟利。

至案发，被告人王玉建共计通过买号街平台售出他人个人信息 7700 余条，其在该平台的成交金额为 88200 余元，并从该交易平台提现人民币 80000 余元。

2016 年 6 月 23 日，被告人王玉建被警察抓获归案。

案发后，被告人王玉建向本院退缴钱款人民币 81394 元。

上述事实，由公诉机关提交，并经庭审质证的下列证据予以证实:

（1）被告人王玉建的供述，证实其是从 2016 年 4 月开始倒卖支付宝账号的，这些账号都是其买来的，上家给其的账号就已经绑定了身份信息。

其的账号进价是 0.4 元一个，出售价是 0.7 元一个。

其出售账号的平台是买号街，交易都在平台完成，提现需要向平台支付手续费。

其在买号街平台出售了 7000 多个账号，获利 10000 多元，销售额有 80000 多元。

其出售的账号信息包括账号、密码、邮箱、支付宝登录密码、支付密码、姓名、身份号码等。

（2）买号街网络平台账号截图，证实被告人王玉建的买号街平台账户“wyjy1520”作为卖家共计交易1248笔，总成交金额88221.06元。

（3）提现明细，证实买号街平台尚存被告人王玉建的提现记录29条、共计80000余元。

（4）出售信息详情，证实被告人王玉建在买号街平台销售的个人信息内容包含账号、支付密码、邮箱密码、姓名、身份号码等。

（5）买号街后台数据库统计数据，证实该数据系从阿里云计算有限公司调取，被告人王玉建的“wyjy1520”账号在买号街售出带身份号码的信息共计11512条，其中有买家信息显示的记录有7700余条，该数据能与被告人的供述基本印证。

（6）情况说明，证实公安机关从被告人王玉建销售的公民个人信息记录中选取50条身份号码进行验证，经查询，选取的50条身份号码均真实。

（7）抓获经过，证实被告人王玉建的到案情况。

（8）本院执行、调解款票据，证实本院扣押被告人王玉建钱款的情况。

户籍证明、常住人口信息证实各被告人的身份情况。

关于本案的事实认定问题，本院作如下评析:

关于侵犯公民个人信息数据的数量问题，审理认为:（1）公诉机关起诉指控的信息数量虽有买号街后台数据库统计结果证实，但该统计结果中部分没有买家信息显示，故以此认定“已售出”的依据不足。

本院根据买号街后台数据库数据统计结果，筛选有买家信息显示的数据，并结合被告人的供述，综合认定各被告人在买号街平台出售公民个人信息数据的数量。

故对公诉机关起诉指控的数据数量予以调整。

（2）根据司法解释的规定，“对批量公民个人信息的条数，根据查获的数量直接认定”。

本案中无直接证据证明本院认定的公民个人信息存在重复或者不真实的情况，结合“向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算”的规定，本院对被告人及辩护人就信息数据重复、有误提出的意见均不予采纳。

（3）在刑法第九次修正之前，通过窃取等非法方法获取公民个人信息的行为具有刑事违法性，涉案被告人通过购买、网络下载等途径获取公民个人信息无合法性依据，刑法修正案九对“窃取或者以其他方法非法获取公民个人信息”的内容并未修订，故被告人及辩护人提出2015年11月1日之前被告人销售的信息数据数量应当从事实认定中予以扣除的意见，本院均不予采纳。

关于涉案公民个人信息数据的类型认定问题，审理认定:（1）本院在数据数量认定时系以“身份号码”为节点对买号街平台后台数据进行筛选，因此足以认定对被告人科处责任的系实名公民个人信息，足以关联到具体自然人。

被告人及辩护人就实名、未实名账户区分提出的意见，本院不予采纳。

（2）根据收集在案的买号街平台的销售信息详情以及买号街后台数据显示的具体信息，

足以认定被告人邓少华、杨佳林、王安、彭永新、杨迪红、黄为帅、王玉建已出售的信息数据涵盖内容有实名认证情况、支付宝账户信息、淘宝账户信息、银行账户信息等，而支付宝账号、淘宝账号、银行账户等或反映交易情况，或反映财产状况，因此涉案信息应当认定为最高人民法院、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》第五条第一款第（四）项规定的其他可能影响人身、财产安全的公民个人信息。

本案中，有关非法利用信息网络的事实认定问题，审理认为:（1）在侵犯公民个人信息的事实认定中，“对批量公民个人信息的条数，根据查获的数量直接认定”，被告人郑奎、李继斌、周建国、蒋培密、蓝红峰、蒙昌华设立、制作网络交易平台供他人进行公民个人信息数据的存储、流转、买卖，相关的交易事实认定当以侵犯公民个人信息的认定为参照，以网站后台统计结果直接认定。

且根据两平台的交易量、交易金额、平台的非法获利情况，以及两平台运营产生的实际影响，结合本案中已查清的侵犯公民个人信息的事实，足以作出被告人郑奎、李继斌、周建国、蒋培密、蓝红峰、蒙昌华的行为属非法利用信息网络情节严重的事实认定。

被告人及辩护人就非法利用信息网络事实认定提出的异议意见，本院均不予采纳。

（2）关于通过平台出售的数据系公民个人信息及被告人明知的问题，该事实已由被告人的供述、交易平台的功能设计、已查证的平台销售数据的实际内容等予以证实，被告人就此提出的异议意见，本院不予采纳。

（3）被告人郑奎及被告人李继斌等人运营网络账号交易平台的行为具有持续性，涉公民个人信息数据的交易为非法获取公民个人信息的途径，无论在刑法修正之前还是之后，该行为均系违法，故被告人郑奎、李继斌的辩护人提出 2015 年 11 月 1 日之前，两交易平台销售数据信息的事实不应认定的意见，本院均不予采纳。

本院认为，被告人朱长余、肖申、戎丹平以非法占有为目的，秘密窃取他人财物，数额较大，其行为均已构成盗窃罪，且系共同犯罪。

被告人郑奎、李继斌、周建国、蒋培密、蓝红峰、蒙昌华设立、制作网络交易平台供他人进行公民个人信息数据的存储、流转、买卖，并以此牟取非法利益，其行为均已构成非法利用信息网络罪，且被告人李继斌、周建国、蒋培密、蓝红峰、蒙昌华系共同犯罪。

被告人邓少华、杨佳林、王安、彭永新、杨迪红、黄为帅、王玉建违反国家有关规定，非法获取并向他人出售公民个人信息，其行为均已构成侵犯公民个人信息罪，根据七被告人售出公民个人信息数据的数量情况，被告人邓少华、彭永新、王玉建均属侵犯公民个人信息情节特别严重，被告人杨佳林、王安、杨迪红、黄为帅均属侵犯公民个人信息情节严重。

公诉机关指控被告人邓少华、杨佳林、王安、彭永新、杨迪红、黄为帅、王玉建的行为构成侵犯公民个人信息罪的罪名成立，本院予以支持。

根据最高人民法院指导案例的裁判意见，“行为人利用信息网络，诱骗他人点击虚假链接而实际通过预先植入的计算机程序窃取财物构成犯罪的，以盗窃罪定罪处罚”，故类似被

告人朱长余、肖申、戎丹平的行为应定性为盗窃，公诉机关指控三被告人的行为构成诈骗罪的罪名有误，本院依法予以纠正，对辩护人提出的三被告人的行为应定性为盗窃的意见，本院予以采纳。

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》的规定，“设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚”，故被告人郑奎、李继斌、周建国、蒋培密、蓝红峰、蒙昌华的涉案行为应定性为非法利用信息网络，公诉机关指控六被告人的行为构成帮助信息网络犯罪活动罪的罪名有误，本院依法予以纠正。

关于被告人李继斌、蒋培密、蓝红峰、蒙昌华及相关辩护人提出的无罪意见，审理认为:首先，被告人李继斌、周建国作为股东发起设立买号街网络交易平台的初衷即在于为他人进行个人信息数据存储、流转、交易提供方便，在明知他人在平台上销售侵犯他人个人信息数据的情况下，被告人李继斌等人不是积极地阻止交易行为，而是有针对性地、积极地对外推广平台，扩大平台的影响力，该行为已经突破了平台的中立性。

被告人蒋培密、蓝红峰在此过程中为平台提供网络技术支持，被告人蒙昌华对外积极推广平台（被告人蒙昌华是否是买号街平台推广部的负责人不影响对其行为系非法的定性评价），均应当承担相应的行为违法责任。

其次，买号街平台在运营中主要从事信息的非法交易、流转，被告人李继斌等人在明知他人利用平台上获取的数据信息进行刷单、刷信誉等非诚信的违法经营活动，甚至实施盗窃等犯罪活动的情况下，设立、运营买号街平台开展的经营活动应认定为非法，因此依法不应当以单位犯罪论处。

再次，已查证的被告人邓少华、杨佳林、王安、彭永新、杨迪红、黄为帅、王玉建、朱长余等人的行为，亦足以印证被告人李继斌等人运营买号街平台的刑事违法性。

综上，涉买号街平台相关被告人及相应辩护人提出的无罪意见，本院均不予采纳。

根据被告人蒙昌华在买号街平台工作产生的实际社会影响，以及其个人的获利情况，辩护人提出被告人蒙昌华的涉案行为情节显著轻微，危害不大，应当免予刑事处罚的意见，本院不予采纳。

在买号街平台运营过程中，被告人蒙昌华等人的行为均表现积极，属于买号街平台运营中的不同角色分工，角色之间相互协同、配合，不足以对各被告人的作用作出主从犯的区分。

被告人蒙昌华的辩护人提出区分主从犯的意见，本院不予采纳。

但可根据各被告人在买号街平台运营中的行为表现，在量刑时予以区别考量。

被告人朱长余协助公安机关抓获同案犯，属立功，可依法对其从轻处罚。

辩护人根据被告人朱长余的立功情节，请求对被告人朱长余从轻处罚的意见，本院予以采纳。

根据各被告人的认罪悔罪态度、一贯表现、退赃情况，可分别酌情对各被告人予以从轻处罚。

被告人及辩护人根据上述情节，请求从轻处罚的意见，本院均予以采纳。

本案中，各被告人利用电信网络技术，侵犯不特定多数人的合法权益，可酌情对各被告人予以从重处罚。

被告人王玉建的辩护人提出被告人王玉建具有自首情节的意见与被告人王玉建系被目的明确的抓捕归案的事实不符，该意见本院不予采纳。

但可根据被告人王玉建到案后对案件事实的交代情况，酌情对其予以从轻处罚。

关于被告人邓少华及其辩护人提出被告人邓少华具有立功情节的意见，审理认为:根据辩护人提交的由邵阳市公安局双某分局石桥派出所出具的情况说明，被告人邓少华检举揭发的系他人的吸贩毒线索，吸毒事实虽经查证属实，但该行为非他人的犯罪事实，而线索涉及的贩毒事实未能查证。

线索涉及违法人员最后虽被公安机关刑事拘留，但涉嫌事实为盗窃，非被告人邓少华举报线索来源。

综上，被告人邓少华的行为依法不应认定为立功，被告人邓少华及其辩护人就此提出的意见，本院不予采纳。

但就被告人邓少华积极举报他人违法行为的表现，可酌情对其予以从轻处罚。

本案中，各被告人的行为组成了一个完整的“黑色”产业链，成千上万名被害人的合法权益被侵害，被告人的行为社会危害性大、影响范围广，根据被告人的犯罪情节，均不宜适用缓刑。

辩护人提出的适用缓刑的意见，本院均不予采纳。

综上，依照《中华人民共和国刑法》第二百六十四条　、第二百八十七条　之一第一款　、第二百五十三条　之一、第二十五条　第一款　、第六十八条　、第六十四条之规定，判决如下:

一、被告人朱长余犯盗窃罪，判处有期徒刑二年，并处罚金人民币五千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年六月一日起至二〇一九年五月十五日止。

罚金在本判决生效后十日内缴纳）；

二、被告人肖申犯盗窃罪，判处有期徒刑二年二个月，并处罚金人民币五千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年六月二日起至二〇一九年七月十六日止。

罚金在本判决生效后十日内缴纳）；

三、被告人戎丹平犯盗窃罪，判处有期徒刑二年二个月，并处罚金人民币五千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六

年六月二日起至二〇一九年七月十六日止。

罚金在本判决生效后十日内缴纳）；

四、被告人郑奎犯非法利用信息网络罪，判处有期徒刑一年十个月，并处罚金人民币四千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年七月六日起至二〇一八年五月五日止。

罚金在本判决生效后十日内缴纳）；

五、被告人李继斌犯非法利用信息网络罪，判处有期徒刑一年九个月，并处罚金人民币四千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年七月六日起至二〇一八年四月五日止。

罚金在本判决生效后十日内缴纳）；

六、被告人周建国犯非法利用信息网络罪，判处有期徒刑一年六个月，并处罚金人民币三千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年七月六日起至二〇一八年十一月十五日止。

罚金在本判决生效后十日内缴纳）；

七、被告人蒋培密犯非法利用信息网络罪，判处有期徒刑一年六个月，并处罚金人民币三千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年七月六日起至二〇一八年十一月十五日止。

罚金在本判决生效后十日内缴纳）；

八、被告人蓝红峰犯非法利用信息网络罪，判处有期徒刑一年六个月，并处罚金人民币三千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年七月六日起至二〇一八年十一月十五日止。

罚金在本判决生效后十日内缴纳）；

九、被告人蒙昌华犯非法利用信息网络罪，判处有期徒刑一年三个月，并处罚金人民币三千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年七月六日起至二〇一八年八月十五日止。

罚金在本判决生效后十日内缴纳）；

十、被告人邓少华犯侵犯公民个人信息罪，判处有期徒刑三年六个月，并处罚金人民币一万元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年六月二十六日起至二〇二〇年六月四日止。

罚金在本判决生效后十日内缴纳）；

十一、被告人杨佳林犯侵犯公民个人信息罪，判处有期徒刑二年，并处罚金人民币五千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年六月二十九日起至二〇一八年十二月七日止。

罚金在本判决生效后十日内缴纳）；

十二、被告人王安犯侵犯公民个人信息罪，判处有期徒刑一年八个月，并处罚金人民币四千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年六月二十二日起至二〇一九年一月二十九日止。

罚金在本判决生效后十日内缴纳）；

十三、被告人彭永新犯侵犯公民个人信息罪，判处有期徒刑四年，并处罚金人民币一万元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；罚金在本判决生效后十日内缴纳）；

十四、被告人杨迪红犯侵犯公民个人信息罪，判处有期徒刑一年，并处罚金人民币二千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年六月二十四日起至二〇一八年五月二十二日止。

罚金在本判决生效后十日内缴纳）；

十五、被告人黄为帅犯侵犯公民个人信息罪，判处有期徒刑一年十个月，并处罚金人民币四千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年六月二十二日起至二〇一九年三月二十二日止。

罚金在本判决生效后十日内缴纳）；

十六、被告人王玉建犯侵犯公民个人信息罪，判处有期徒刑三年，并处罚金人民币六千元（刑期从判决执行之日起计算；判决执行以前先行羁押的，羁押一日折抵刑期一日；即自二〇一六年六月二十四日起至二〇二〇年五月二十一日止。

罚金在本判决生效后十日内缴纳）；

十七、被告人朱长余、肖申、戎丹平退缴的人民币 60000 元，已查明被害人的，退赔给被害人，未查明被害人的作为非法获利予以没收；被告人邓少华退缴的人民币 3920 元、被告人杨佳林退缴的人民币 8690 元、被告人王玉建退缴的人民币 81394 元、被告人杨迪红退缴的人民币 25680 元，均作为非法获利予以没收；被告人彭永新退缴的人民币 20000 元，其中人民币 17987.96 元作为非法获利予以没收，余款抵作被告人彭永新的罚金；从被告人戎丹平处扣押的电脑主机 3 台、从被告人彭永新处扣押的笔记本电脑 1 台、电脑主机 1 台，均予以没收。

尚未追缴的非法获利，继续向被告人追缴。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向浙江省绍兴市中级人民法院提出上诉，书面上诉的，应当提交上诉状正本一份，副本二份。

审判长张毅

人民陪审员章定安

人民陪审员钱美新

二〇一八年三月二十二日

书记员陈雨燕

（六）赌博罪、开设赌场罪

案例一、何友坦、陈德倍、王世庞等赌博案

审理法院： 苍南县人民法院

案　　号： （2018）浙 0327 刑初 870 号

案　　由： 赌博罪

裁判日期： 2019 年 09 月 25 日

苍南县人民法院

刑事判决书

（2018）浙 0327 刑初 870 号

被告人何友坦，男，1976 年 5 月 10 日出生于浙江省苍南县，汉族，高中文化，浙江剑龙网络科技有限公司总经理，住苍南县。因本案于 2017 年 10 月 16 日被苍南县公安局抓获，次日被刑事拘留，同年 11 月 23 日被逮捕，2018 年 5 月 23 日被苍南县人民检察院取保候审，2019 年 5 月 15 日被本院取保候审。

辩护人陈军文，北京乾成律师事务所律师。

被告人陈德倍，男，1983 年 7 月 24 日出生于浙江省苍南县，汉族，小学文化,浙江剑龙网络科技有限公司法人代表、副总经理，户籍所在地苍南县，住苍南县。因本案于 2017 年 10 月 16 日被苍南县公安局抓获，次日被刑事拘留，同年 11 月 23 日被逮捕，2018 年 5 月 23 日被苍南县人民检察院取保候审，2019 年 5 月 15 日被本院取保候审。

辩护人吴双，浙江天和律师事务所律师。

被告人王世庞（曾用名王从武），男，1986 年 11 月 28 日出生于四川省筠连县，汉族，初中文化，浙江剑龙网络科技有限公司副总经理，户籍所在地四川省筠连县，现住平阳县。因犯开设赌场罪于 2016 年 10 月 25 日被平阳县人民法院判处有期徒刑一年六个月，缓刑二年。因本案于 2017 年 10 月 16 日被苍南县公安局抓获，次日被刑事拘留，同年 11 月 23 日被逮捕。现羁押于苍南县看守所。

辩护人易叶雄，浙江泽苍律师事务所律师（苍南县法律援助中心指派）。

被告人温兴奉，男，1988 年 5 月 24 日出生于浙江省平阳县，汉族，大学文化，浙江剑龙网络科技有限公司市场部主管,户籍所在地平阳县，住苍南县。因本案于 2017 年 10 月 16 日被苍南县公安局抓获，次日被刑事拘留，同年 11 月 23 日被逮捕。2019 年 1 月 30 日被本院取保候审。

辩护人杨乃柱，浙江法之剑律师事务所律师。

被告人陈菩菩，女，1986 年 9 月 26 日出生于浙江省苍南县，汉族，大专文化，浙江剑龙网络科技有限公司财务部主管，住苍南县。因本案于 2017 年 10 月 17 日被苍南县公安局刑事拘留，同年 11 月 23 日被逮捕，2018 年 5 月 23 日被苍南县人民检察院取保候审，2019 年 5 月 15 日被本院取保候审。

辩护人钱益寒，浙江靖霖（温州）律师事务所律师。

被告人王世芹，女，1988年9月3日出生于四川省筠连县，汉族，初中文化，浙江剑龙网络科技有限公司财务部员工，户籍所在地四川省筠连县。因本案于2017年10月16日被苍南县公安局抓获，次日被刑事拘留，同年11月16日被取保候审，2018年11月15日被本院取保候审。

辩护人朱杰春，浙江望舟律师事务所律师（苍南县法律援助中心指派）。

被告人谢苏芬，女，1987年7月28日出生于浙江省苍南县，汉族，大专文化，浙江剑龙网络科技有限公司财务部员工，住苍南县。因本案于2017年10月16日被苍南县公安局抓获，次日被刑事拘留，同年11月16日被取保候审，2018年11月15日被本院取保候审。

辩护人罗明开，浙江人民联合律师事务所律师。

被告人王蓓蓓，女，1995年10月18日出生于浙江省苍南县，汉族，大专文化，浙江剑龙网络科技有限公司市场部员工，住苍南县。因本案于2017年10月16日被苍南县公安局抓获，次日被刑事拘留，同年11月16日被取保候审，2018年11月15日被本院取保候审。

辩护人赖振国，浙江中欣律师事务所律师（苍南县法律援助中心指派）。

被告人王振水，男，1982年1月3日出生于浙江省苍南县，汉族，大专文化，浙江剑龙网络科技有限公司市场部员工,住苍南县。因本案于2017年10月16日被苍南县公安局抓获，次日被刑事拘留，同年11月23日被逮捕，2018年5月23日被苍南县人民检察院取保候审，2019年5月15日被本院取保候审。

辩护人曾志荣，北京京大（杭州）律师事务所律师。

被告人杨立银，男，1995年4月4日出生于浙江省苍南县，汉族，大学文化，浙江剑龙网络科技有限公司客服部员工,户籍所在地苍南县，现住苍南县。因本案于2017年11月28日被苍南县公安局抓获，次日被刑事拘留，2018年1月5日被逮捕，同年5月24日被苍南县人民检察院取保候审，2019年5月15日被本院取保候审。

辩护人王伦峰，浙江卓朗律师事务所律师。

被告人陈荣伟，男，1989年2月22日出生于浙江省苍南县，汉族，高中文化，住苍南县。因本案于2017年10月16日被苍南县公安局抓获，次日被行政拘留，10月21日转为刑事拘留，同年11月23日被逮捕，2018年7月18日被苍南县人民检察院取保候审，2019年5月16日被本院取保候审。

辩护人施孔全，浙江瓯南律师事务所律师（苍南县法律援助中心指派）。

被告人朱绍晓，男，1988年5月11日出生于浙江省苍南县，汉族，初中文化，户籍所在地苍南县，现住。因酒后驾驶机动车于2013年8月12日被苍南县公安局暂扣机动车驾驶证六个月并处罚款;又因酒后驾驶机动车于2016年5月30日被苍南县公安局行政拘留九日。因本案于2017年10月16日被苍南县公安局抓获，次日被行政拘留，10月22日转为刑事

拘留，同年11月23日被逮捕，2018年7月18日被苍南县人民检察院取保候审，2019年5月16日被本院取保候审。

辩护人陈慧敏，浙江泽瓯律师事务所律师（苍南县法律援助中心指派）。

被告人宋瑞炘，男，1980年3月19日出生于浙江省苍南县，汉族，初中文化，户籍所在地苍南县，现住苍南县。因本案于2017年10月15日被苍南县公安局抓获，次日被行政拘留,10月20日转为刑事拘留，同年11月24日被逮捕，2018年7月18日被苍南县人民检察院取保候审，2019年5月16日被本院取保候审。

辩护人苏松建，浙江瓯鼎律师事务所律师（苍南县法律援助中心指派）。

被告人谢金婵，女，1987年2月4日出生于浙江省平阳县，汉族，初中文化，户籍所在地苍南县，住苍南县。因本案于2017年12月13日被苍南县公安局抓获，次日被刑事拘留，2018年1月19日被取保候审，2019年1月17日被本院取保候审。

辩护人陈焕付，浙江瓯鼎律师事务所律师（苍南县法律援助中心指派）。

被告人谢金钗，女，1989年5月26日出生于浙江省平阳县，汉族，高中文化，户籍所在地苍南县，住苍南县。因本案于2017年12月13日被苍南县公安局抓获，次日被刑事拘留，2018年1月5日被取保候审，2019年1月3日被本院取保候审。

辩护人林春娥，浙江法之剑律师事务所律师（苍南县法律援助中心指派）。

被告人陈萍萍，女，1993年6月15日出生于浙江省苍南县，汉族，初中文化，住苍南县。因本案于2017年10月16日被苍南县公安局抓获归案，次日被行政拘留，10月22日转为刑事拘留，同年11月24日被逮捕，2018年5月24日被苍南县人民检察院取保候审，2019年5月16日被本院取保候审。

辩护人苏雨霞，浙江泽苍律师事务所律师（苍南县法律援助中心指派）。

被告人张传武，男，1981年5月25日出生于浙江省苍南县，汉族，初中文化，户籍所在地苍南县。因本案于2017年10月16日被苍南县公安局抓获，次日被行政拘留，10月21日转为刑事拘留，同年11月24日被逮捕，2018年5月23日被苍南县人民检察院取保候审，2019年5月16日被本院取保候审。

辩护人林明霞，浙江瓯鼎律师事务所律师（苍南县法律援助中心指派）。

被告人薛彦泽，男，1982年9月25日出生于浙江省苍南县，汉族，高中文化，户籍所在地苍南县，现住苍南县。因本案于2017年10月17日被苍南县公安局抓获，次日被刑事拘留，同年11月24日被逮捕，2018年5月23日被苍南县人民检察院取保候审，2019年5月15日被本院取保候审。

辩护人林培，浙江玉山律师事务所律师（苍南县法律援助中心指派）。

被告人杨昶辉，男，1986年9月29日出生于浙江省苍南县，汉族，高中文化，户籍所在地苍南县，现住温州市瓯海区。因本案于2017年10月23日被苍南县公安局抓获，次日被刑事拘留，同年11月16日被取保候审，2018年11月15日被本院取保候审。

辩护人吴登球，浙江泽瓯律师事务所律师（苍南县法律援助中心指派）。

被告人陈海哨，女，1982 年 4 月 2 日出生于浙江省苍南县，汉族，大专文化，户籍所在地苍南县，现住。因本案于 2017 年 10 月 16 日被苍南县公安局抓获归案，次日被行政拘留，10 月 22 日转为刑事拘留，同年 11 月 16 日被取保候审，2018 年 11 月 15 日被本院取保候审。

辩护人朱小凤，浙江浙信律师事务所律师（苍南县法律援助中心指派）。

被告人王如浪，男，1987 年 4 月 25 日出生于浙江省苍南县，汉族，大学文化，户籍所在地苍南县，现住。因本案于 2017 年 10 月 16 日被苍南县公安局抓获归案，次日被行政拘留，10 月 21 日转为刑事拘留，同年 11 月 23 日被逮捕，2018 年 5 月 23 日被苍南县人民检察院取保候审，2019 年 5 月 16 日被本院取保候审。

辩护人黄嘉盈，浙江正昌律师事务所律师。

苍南县人民检察院以苍检公诉刑诉〔2018〕737 号起诉书指控被告人何友坦、陈德倍、王世庞、温兴奉、陈菩菩、王世芹、谢苏芬、王蓓蓓、王振水、杨立银、陈荣伟、朱绍晓、宋瑞炘、谢金婵、谢金钗、陈萍萍、张传武、薛彦泽、杨昶辉、陈海哨、王如浪犯赌博罪，于 2018 年 8 月 2 日向本院提起公诉。本院于当日立案，并依法组成合议庭，经庭前会议后公开开庭审理了本案。苍南县人民检察院指派检察员李以恒出庭支持公诉，被告人何友坦、陈德倍、王世庞、温兴奉、陈菩菩、王世芹、谢苏芬、王蓓蓓、王振水、杨立银、陈荣伟、朱绍晓、宋瑞炘、谢金婵、谢金钗、陈萍萍、张传武、薛彦泽、杨昶辉、陈海哨、王如浪，辩护人陈军文、吴双、易叶雄、杨乃柱、钱某 2、朱杰春、罗明开、赖振国、曾志荣、王某、施孔全、陈慧敏、苏松建、陈焕付、林春娥、苏雨霞、林明霞、林培、吴登球、朱小凤、黄嘉盈到庭参加诉讼。期间，应公诉机关要求补充侦查延期审理二次，经温州市中级人民法院批准延长审限三个月。现已审理终结。

苍南县人民检察院指控：

一、浙江剑龙网络科技有限公司（以下简称剑龙公司）主要经营网络游戏产品开发及网络游戏虚拟币发行。2016 年 11 月，剑龙公司经开发推出“指尚游麻将”游戏 APP，为进行游戏推广，剑龙公司招募被告人陈荣伟、朱绍晓等人成为“游戏钻石”销售代理，让他们组建玩家微信群，并将公司微信号派驻在各个玩家微信群内统计各群每天游戏场次，进而发放奖励。在此期间，作为剑龙公司高管的被告人何友坦等人在发现被告人陈荣伟、朱绍晓等人组织他人在微信群内利用“指尚游麻将”游戏 APP 进行赌博的情况下，不仅未予制止，反而为谋取经济上的利益继续向他们提供游戏服务、发放奖励。

二、2017 年 4 月至 7 月份，被告人张传武为贩卖游戏钻石营利而组建了“速度与激情 2 毛某”微信群，成员有黄某 2、邵某 2、邵某 1 等约五十人，利用“指尚游麻将”游戏进行赌博，每天进行约三四十场，每场输赢约人民币 20 元（以下所涉货币均为人民币）。

为证明指控之事实，公诉机关当庭提供了被告人供述、证人证言等相应证据材料，并据

此认为，被告人王振水、杨立银、陈荣伟、朱绍晓、宋瑞炘、谢金婵、谢金钗、陈萍萍、张传武、薛彦泽、杨昶辉、陈海哨、王如浪以营利为目的，组织他人赌博；被告人何友坦、陈德倍、王世庞、温兴奉、陈菩菩、王世芹、谢苏芬、王蓓蓓明知他人实施赌博犯罪活动，而为其提供帮助。其行为均已触犯了《中华人民共和国刑法》第三百零三条的规定，犯罪事实清楚，证据确实充分，应当以赌博罪追究其刑事责任。被告人王世庞在刑罚执行期间重新故意犯罪，应予以数罪并罚。被告人王世芹、谢苏芬、王蓓蓓在共同犯罪中起次要、辅助作用，系从犯，应从轻、减轻处罚。各被告人在归案后均能如实供述犯罪事实，可从轻处罚。提请本院依法判处。

被告人何友坦、陈德倍、王世庞、温兴奉对起诉指控的事实无异议，但辩解自己对公司人员组织赌博的行为不知情，没有犯罪，被告人温兴奉另辩解自己没有抽取赌博微信群的违法利益。

被告人何友坦的辩护人辩称：证据方面，1.怀疑公安机关存在诱供行为，对何友坦供述的证据三性均有异议；2.部分赌博人员的证人证言未按照刑事证据要求进行转换、电子证据提交时间较迟，对合法性均有异议。定性方面，何友坦的行为不构成赌博罪，1.根据《治安管理处罚法》和《浙江省行政处罚裁量标准》等规定，亲属之间进行带有财物输赢或者其他人之间带有少量财物输赢的打麻将、玩扑克等娱乐活动应不予处罚。本案中的娱乐方式主要是打麻将，且单次输赢额在几毛钱到几块钱之间，按照法律和社会观念不宜认定为赌博；2.微信群内虽然人数较多，但并非所有人员都参与了上述“娱乐行为”，且有部分人员系各被告人的亲属和朋友，公诉机关不能直接推定群内所有人参赌或存在 20 人以上参赌；3.剑龙公司收取游戏场地费和服务费系正常经营行为，不构成犯罪；4.剑龙公司为推广游戏组建了多个玩家微信群，即使群内存在赌博情况，何友坦作为剑龙公司总经理也无法主动明知。综上，请求法庭依法判决。

被告人陈德倍的辩护人辩称：证据方面，陈德倍的供述与何友坦的供述内容高度相似，怀疑公安机关存在诱供行为，对陈德倍供述的合法性有异议。定性方面，陈德倍的行为不构成赌博罪，1.剑龙公司收取场地费和服务费系正常经营行为，不构成犯罪；2.剑龙公司已尽到监督义务，从现有技术层面来说无法发现线下赌博情况，剑龙公司也没有与代理人共谋组织赌博。如果法庭认为陈德倍的相关行为构成赌博罪，鉴于陈德倍没有前科劣迹，请求法庭对其从轻处罚并判处缓刑。

被告人王世庞的辩护人辩称：证据方面，1.怀疑王世庞的供述系在公安机关疲劳审讯下作出，对王世庞供述的合法性有异议；2.证人何某的证言对剑龙公司高层明知线下赌博的陈述系主观猜测，对关联性有异议。定性方面，王世庞的行为不构成赌博罪，1.剑龙公司的设立和运营是合法的；2.王世庞对线下赌博不知情。如果法庭认为王世庞的相关行为构成赌博罪，鉴于王世庞尚在服刑阶段，请求法庭对其从轻处罚。

被告人温兴奉的辩护人辩称：温兴奉的行为不构成赌博罪，1.剑龙公司为推广游戏组建

玩家微信群，并未组织赌博；2.微信群内人员都是亲戚朋友，偶尔少量打赌的行为不构成犯罪；3.公司高层没有收取高额服务费或修改服务器的行为，不能认定为明知他人赌博并提供工具。综上，请求法庭依法判决。

被告人陈菩菩、王世芹、谢苏芬、王蓓蓓、王振水、杨立银、陈荣伟、朱绍晓、宋瑞炘、谢金婵、谢金钗、陈萍萍、薛彦泽、杨昶辉、陈海哨、王如浪、张传武对起诉指控的事实和罪名均无异议。

被告人陈菩菩的辩护人辩称：被告人的行为不构成赌博罪。如果法庭认为陈菩菩的相关行为构成赌博罪，对量刑情节发表以下意见。陈菩菩没有前科劣迹，归案后如实供述自己的犯罪事实，当庭认罪态度好，且在本案中起次要、辅助作用，仅为公司雇佣人员，未直接组织赌博，系从犯、帮助犯。陈菩菩已临近预产期，符合社区矫正要求。综上，请求法庭对陈菩菩从轻处罚并适用缓刑。

被告人王世芹的辩护人辩称：同意以上辩护人关于无罪的辩护意见，如果法庭认为王世芹的相关行为构成赌博罪，对量刑情节发表以下意见。王世芹归案后如实供述自己的犯罪事实，且在本案中作用较小，仅为公司雇佣人员，系从犯。综上，请求法庭对王世芹从轻处罚并适用缓刑。

被告人谢苏芬的辩护人辩称：谢苏芬的行为不构成赌博罪，1.谢苏芬系剑龙公司一般职员，没有制止赌博行为的管理权限，向被告人陈荣伟发放工资也仅为履行岗位职责；2.微信群中亲属之间打赌不构成赌博罪，谢苏芬既不清楚群中打赌情况，也没有为赌博犯罪提供帮助；3.谢苏芬已有身孕，符合从轻条件。综上，请求法庭对谢苏芬免予刑事处罚。

被告人王蓓蓓的辩护人辩称：同意以上辩护人关于无罪的辩护意见，如果法庭认为王蓓蓓的相关行为构成赌博罪，对量刑情节发表以下意见。王蓓蓓系初犯、偶犯，没有前科劣迹，主观恶性较小，且涉案时间短，犯罪情节轻微。王蓓蓓归案后如实供述自己的犯罪事实，当庭认罪态度好，在本案中起次要、辅助作用，系从犯。综上，请求法庭对王蓓蓓从轻或减轻处罚，并适用缓刑。

被告人王振水的辩护人辩称：证据方面，1.赌博人员的证人证言未按照刑事证据要求进行转换；2.被告人供述笔录存在记录不全、选择性记录、偷换概念情况；3.微信群的电子数据无法证实除亲友外的参赌人员人数，并且提取程序不合规。定性方面，同意以上辩护人关于无罪的辩护意见。综上，请求法庭依法判决。

被告人杨立银的辩护人辩称：对指控的事实和罪名无异议。杨立银没有前科劣迹，主观恶性较小，且微信群中都是亲戚朋友，社会危害性小，获利较少，犯罪情节轻微。杨立银归案后如实供述自己的犯罪事实，当庭认罪态度好，愿意退出全部违法所得。综上，请求法庭对杨立银从轻处罚并适用缓刑。

被告人陈荣伟的辩护人辩称：同意以上辩护人关于无罪的辩护意见，如果法庭认为陈荣伟的相关行为构成赌博罪，对量刑情节发表以下意见。陈荣伟系初犯、偶犯，没有前科劣迹，

获利较少，社会危害性小，且归案后如实供述自己的犯罪事实，悔罪态度良好。综上，请求法庭对陈荣伟从轻处罚。

被告人朱绍晓的辩护人辩称：对指控的事实和罪名无异议。朱绍晓没有前科劣迹，归案后如实供述自己的犯罪事实，悔罪态度良好，且愿意退出全部违法所得。综上，请求法庭对朱绍晓从轻处罚并适用缓刑。

被告人宋瑞炘的辩护人辩称：对指控的事实和罪名无异议。宋瑞炘没有前科劣迹，犯罪情节轻微，归案后如实供述自己的犯罪事实，悔罪态度良好。综上，请求法庭对宋瑞炘从轻处罚并适用缓刑。

被告人谢金婵的辩护人辩称：对指控的事实和罪名无异议。谢金婵主观恶性较小，且微信群中都是亲戚朋友，社会危害性小，犯罪情节轻微。谢金婵归案后如实供述自己的犯罪事实，已退出大部分违法所得，且幼子尚在哺乳期内。综上，请求法庭对谢金婵从轻处罚并适用缓刑。

被告人谢金钗的辩护人辩称：对指控的事实和罪名无异议。谢金钗没有前科劣迹，主观恶性较小，归案后如实供述自己的犯罪事实，已退出大部分违法所得。综上，请求法庭对谢金钗从轻处罚并适用缓刑。

被告人陈萍萍的辩护人辩称：对指控的事实和罪名无异议。陈萍萍系初犯、偶犯，主观恶性较小，归案后如实供述自己的犯罪事实，愿意退出全部违法所得，且家中有一个小孩需要抚养。综上，请求法庭对陈萍萍从轻处罚并适用缓刑。

被告人张传武的辩护人辩称：对指控的事实和罪名无异议。张传武系初犯、偶犯，归案后如实供述自己的犯罪事实，愿意退出全部违法所得。综上，请求法庭对张传武从轻处罚并适用缓刑。

被告人薛彦泽的辩护人辩称：同意以上辩护人关于无罪的辩护意见，如果法庭认为薛彦泽的相关行为构成赌博罪，对量刑情节发表以下意见。薛彦泽归案后如实供述自己的犯罪事实，悔罪态度良好，且微信群内都是亲戚朋友，社会危害性小。综上，请求法庭对薛彦泽从轻处罚并适用缓刑。

被告人杨昶辉的辩护人辩称：同意以上辩护人关于无罪的辩护意见，如果法庭认为杨昶辉的相关行为构成赌博罪，对量刑情节发表以下意见。杨昶辉系初犯、偶犯，归案后如实供述自己的犯罪事实，且已退出全部违法所得。综上，请求法庭对杨昶辉从轻处罚并适用缓刑。

被告人陈海哨的辩护人辩称：对指控的事实和罪名无异议。陈海哨没有前科劣迹，归案后如实供述自己的犯罪事实，微信群内都是亲戚朋友，社会危害性较小，且已退出全部违法所得。综上，请求法庭对陈海哨从轻处罚并适用缓刑。

被告人王如浪的辩护人辩称：对指控的事实和罪名无异议。王如浪归案后如实供述自己的犯罪事实，微信群内都是亲戚朋友，社会危害性较小。王如浪获利较少，并已退出全部违法所得，且家庭情况较差，还有一个孩子需要抚养。综上，请求法庭对王如浪适用缓刑或免

予刑事处罚。

经审理查明：

一、2013 年 7 月，剑龙公司注册登记成立，主要经营网络游戏产品开发及网络游戏虚拟币发行。2016 年 11 月，剑龙公司经开发推出“指尚游麻将”游戏 APP，为进行游戏推广，剑龙公司招募被告人陈荣伟、朱绍晓等人成为“游戏钻石”销售代理，让他们组建玩家微信群。为达到鼓励玩家多玩游戏以提升“游戏钻石”销售额而盈利的目的，剑龙公司推出多种奖励措施，并将公司微信号派驻在各个玩家微信群内统计各群每天游戏场次，进而发放奖励。在此期间，作为剑龙公司负责人的被告人何友坦、陈德倍、王世庞，以及参与剑龙公司管理、经营的被告人温兴奉、陈菩菩、王世芹、谢苏芬、王蓓蓓在发现被告人王振水、杨立银、陈荣伟、朱绍晓、宋瑞炘、谢金婵、谢金钗、陈萍萍、薛彦泽、杨昶辉、陈海哨、王如浪以及杨鸽鸽、方某 2（另案处理）组织他人在微信群内利用“指尚游麻将”游戏 APP 进行赌博的情况下而未予以制止，反而为谋取经济上的利益继续向他们提供游戏服务、发放奖励。具体事实如下：

1．2017 年 4 月至 8、9 月，被告人陈荣伟为贩卖游戏钻石营利而组建了“二毛”等微信群，群内成员有黄某 1、陈某 1、林某 1 等约七十人，利用“指尚游麻将”游戏 APP 进行赌博，每天赌博约三十场，每场输赢约三十元，被告人陈荣伟共通过贩卖游戏钻石获利 3000 元。

2．2017 年 4、5 月至 10 月，被告人温兴奉、朱绍晓为贩卖游戏钻石营利而组建了“龙港一班 2 毛一分群（打 2 毛、押金 50 元）”、“中发财 2 毛某（台炮麻将）”等微信群，群内成员有李某、曾某、陈某 3 等约七八十人，利用“指尚游麻将”游戏 APP 进行赌博，每天赌博约五十场，每场输赢约二十元，被告人温兴奉、朱绍晓共通过贩卖游戏钻石获利 10000 元。

3．2016 年 12 月至 2017 年 5 月，被告人谢金钗、谢金婵为贩卖游戏钻石营利而共同组建了“携手共创三台麻将”等微信群，群内成员有钱某 1 等约五十人，利用“指尚游麻将”游戏 APP 进行赌博，每天赌博约一百场，每场输赢约一百元。2017 年 5 月至 10 月 16 日，被告人谢金婵为贩卖游戏钻石营利而单独组建了“龙港麻将五毛某”等微信群，群内成员有钟某等约四五十人，利用“指尚游麻将”游戏 APP 进行赌博，每天赌博约五十场，每场输赢约一百元。2017 年 5 月至 9 月，被告人谢金钗为贩卖游戏钻石营利而单独组建了“谢紫依”等微信群，群内成员约有四十人，利用“指尚游麻将”游戏 APP 进行赌博，每天赌博约二十场，每场输赢约一百元，被告人谢金钗、谢金婵分别通过贩卖游戏钻石获利 8000 元、15000 元。

4．2017 年 4 月份至 10 月，被告人宋瑞炘为贩卖游戏钻石营利而组建了“娱乐 1 场所”等微信群，群内成员有林某 2、陈某 4、郑某、叶某 1 等约七十人，利用“指尚游麻将”游戏 APP 进行赌博，每天赌博约八十场，每场输赢约一百元，被告人宋瑞炘共通过贩卖游戏钻

石获利4000元。

5.2017年5月至10月16日，被告人陈萍萍为贩卖游戏钻石营利而组建了“Mah-jong2毛（打2毛）”等微信群，群内成员有李某、叶某2等约一百人，利用“指尚游麻将”游戏APP进行赌博，每天赌博约七八十场，每场输赢约二十元，被告人陈萍萍共通过贩卖游戏钻石获利4000元。

6．2017年8月至10月，被告人王振水为贩卖游戏钻石营利而组建了“台炮麻将3毛友谊群”、“台炮麻将20-50一盅玩法”等微信群，群内成员有六十余人，利用“指尚游麻将”游戏APP进行赌博，每天赌博约二十场，每场输赢约三十元。

7．2017年7月至10月，被告人杨立银为贩卖游戏钻石营利而组建了“龙港2毛”等微信群，群内成员有陈某2等约五六十人，利用“指尚游麻将”游戏APP进行赌博，每天赌博约五十场，每场输赢约二十元，被告人杨立银共通过贩卖游戏钻石获利1000元。

8．2016年12月至2017年2月下旬，被告人薛彦泽为贩卖游戏钻石营利而组建了“新年快乐⑤猫娱乐群”等微信群，群内成员有陈某5、朱某、金某等约八九十人，利用“指尚游麻将”游戏APP进行赌博，每天赌博约四五十场，每场输赢约五六十元，期间被告人杨昶辉曾帮忙管理这些赌博微信群。2017年2月下旬至3月下旬，被告人薛彦泽将上述赌博微信群陆续移交给被告人杨昶辉管理。被告人薛彦泽、杨昶辉分别通过贩卖游戏钻石获利3000元、2500元。

9．2017年5月至7、8月，被告人陈海哨为贩卖游戏钻石营利而组建了“五毛某，买钻石联系群主”等微信群，成员有陈某6、林某3、谢某等约三十人，利用“指尚游麻将”游戏APP进行赌博，每天赌博约二十五场，每场输赢约五十元，被告人陈海哨共通过贩卖游戏钻石获利1000元。

10．2017年5、6月至2017年10月，被告人王如浪为贩卖游戏钻石营利而组建了“龙港麻将五毛某”、“麻将五毛某”、“五毛某”等微信群，成员有陈某7、陈某8、方某1等约三十余人，利用“指尚游麻将”游戏APP进行赌博，每天赌博约二三十场，每场输赢约五十元，被告人王如浪共通过贩卖游戏钻石获利500元。

二、2017年4月至7月，被告人张传武为贩卖游戏钻石营利而组建了“速度与激情2毛某”微信群，成员有黄某2、邵某2、邵某1等约五十人，利用“指尚游麻将”游戏APP进行赌博。因该微信群并非在剑龙公司授意下组建，因此剑龙公司也没有向该微信群派驻公司微信号以统计该群每天游戏场次。该微信群每天约进行三四十场赌博，每场输赢约二十元，被告人张传武通过贩卖游戏钻石共获利2000元。

另查明，在本案侦查阶段，被告人谢金婵向苍南县公安局退出18000元、被告人谢金钗向苍南县公安局退出16000元、被告人杨昶辉家属代为退出违法所得2500元、被告人陈海哨家属代为退出违法所得1000元。

在本案审理过程中，各被告人退出违法所得情况如下：杨立银1000元、陈荣伟3000

元、朱绍晓10000元、宋瑞炘4000元、陈萍萍4000元、张传武2000元、薛彦泽3000元、王如浪500元。

1．被告人陈荣伟组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人黄某1、陈某1、林某1的证言，证明该三人于2017年5月开始在名为“二毛”的赌博微信群内进行赌博，该群群主为“陈、大大（卖钻）TM《平台认证》”，群内成员有六十至八十人，赌博比例为每积分2毛（赌博资金按游戏积分计算，每一积分按设定的基数2毛/3毛/5毛/1元不等进行兑换，下文简称“赌博比例”），每场输赢几元到几十元不等。该群曾用名为“一毛”，群主主要负责拉人、踢人、卖钻、维持秩序，后于2017年10月中旬解散。黄某1的微信名为“如果你是我”；陈某1的微信名为“非诚勿扰”，在群内赌过几天，后来没玩就被群主踢出微信群；林某1的微信名为“林静”。

（2）检查、提取笔录，证明2017年10月17日对林某1的苹果5S手机进行检查、10月18日对陈某1的WellPhone手机进行检查、10月19日对黄某1的苹果6S手机进行检查，发现该三部手机虽没有“二毛”微信群，但在2017年5月下旬均有与不同微信人员大量红包收发记录，并予以截屏提取。

（3）被告人陈荣伟的供述，供认自己于2016年农历12月成为“指尚游麻将”游戏代理，2017年4月从他人处接手了名为“一毛”的微信群并改名为“二毛”，群内成员有七十人左右，每天游戏场次三十场左右，每场输赢四十元左右，每天赌资1000元左右。该群内有“指尚游麻将”公司客服，统计每天的游戏场次，后于2017年8、9月解散。自己在群里的微信昵称为“陈、大大（卖钻）TM《平台认证》”（微信号×××？？crw），共通过销售游戏钻石获利3000元。此与上述证据能相互印证。

2．被告人温兴奉、朱绍晓组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人陈某2的证言，证明自己曾加入名为“中.发.财.2毛”的赌博微信群进行赌博，该群群主为“Ace”（微信号×××），群内成员有六十人左右，每天游戏场次七十场，玩的是对杀。自己的微信名为“Hevs”（微信号×××）。

（2）检查、提取笔录，光盘，证明2017年11月28日对陈某2的手机进行检查，提取该手机内“龙港2毛”、“中.发.财.2毛”微信群截图照片1427张，进而证明上述二微信群运营情况。

（3）证人李某的证言，证明自己于2017年5月开始加入名为“龙港一班2毛一分群（打2毛、押金50元）”的赌博微信群内进行赌博，该群群主为“Ace”，群主小号昵称为“A008指尚游麻将”，群内成员从三四十人发展到七十多人，每场输赢二十元至六七十元不等，自己曾向“Ace”购买过游戏钻石。

（4）证人曾某、陈某3的证言，证明该二人于2017年5月开始加入名为“龙港一班2毛一分群（打2毛、押金50元）”的赌博微信群内进行赌博，群成员七十人左右，每场输赢十元至四十元不等。曾某另证明该群存在了2、3个月，陈某3另证明自己在群内赌了十

几天后退出。

（5）同案人员陈志钻的供述，供认被告人温兴奉于2016年12月底找自己和黄某3、陈某9合股代理游戏钻石销售，自己利用黄某3担任客服拥有玩家资源的便利条件，按照两毛、五毛、一块的赌博比例分别帮助温兴奉、黄某3拉了十多个群，每个群基本有四五十人左右，拉群之后将群主转交给黄某3，自己退群，群内有剑龙公司客服号进驻，客服号负责审核群里赌博场次，发放奖励。

（6）同案人员黄某3的供述，供认自己与被告人温兴奉共同管理群名为“雀神龙港麻将五毛某”的赌博微信群，自己当群主之后将微信群改名为“龙港麻将五毛某”，群内成员有四五十人，都有参与赌博，每天游戏场四十场左右，每场输赢一百元左右，经营了四十天。2017年4月离职后，温兴奉将代理账户交予朱绍晓。

（7）检查、提取笔录，证明2017年10月17日对被告人朱绍晓的两只手机进行检查，发现：①黑色苹果手机内微信名为“Ace”（微信号×××），该微信内有“中.发.财.2毛”、“两只熊龙港麻将群”微信群，群内成员分别有60人、71人，群主均为“Ace”，群内有龙港麻将APP相关信息及发红包信息。②杂牌手机内微信名为“A008指尚游麻将直营”（微信号×××），里面有红包交易记录等。

（8）被告人温兴奉的供述，供认龙港麻将的大代理有陈荣伟、朱绍晓等七八人，王振水、陈菩菩也都有自己的微信赌博群。

（9）被告人朱绍晓的供述，供认自己于2017年4、5月分别组建了名为“龙港一班2毛一分群（打2毛、押金50元）”、“中.发.财.2毛”、“两只熊龙港麻将”的赌博微信群，群内成员七八十人左右，每天游戏场次七十场，每场输赢十元至三四十元不等，每天赌资七百元至二千元不等，不认识的赌客需交50元押金。自己的微信名为“Ace”（微信号×××），另一个微信“A008指尚游麻将直营”（微信号×××）是温兴奉的。自己在新旧系统中都有龙港麻将和台炮麻将代理号，这些代理号与温兴奉共用，产生的利润两人对半分，共通过销售游戏钻石获利10000元。此与上述证据能相互印证。

3．被告人谢金婵、谢金钗组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人钱某1的证言，证明自己于2017年2月加入“谢紫依”组建的群名为“一块赌博群”的赌博微信群，“请叫我萍姐”在该群内排第二，群内成员有六十多人，每天游戏场次一百场左右，自己赌了半天多就因为“抬赌”被群主踢出微信群。2017年3、4月左右，自己被拉入“请叫我萍姐”组建的“5毛某”，群内成员有四十多人，每天游戏场次五六十场，赌了一个月左右。自己的微信名为“you”。

（2）检查、提取笔录，证明2017年12月13日对钱某1的OPPO手机进行检查，提取该手机内微信与“请叫我萍姐”、“如梦无痕”、“谢紫依”的转账交易记录。

（3）证人钟某的证言及辨认笔录，证明自己于2017年4月加入谢金婵组建的名为“龙港麻将五毛某”的赌博微信群，赌博比例为每积分5毛，群内成员有四五十人，每天游戏场

次至少五十场，每场输赢一百多元。自己的微信名为“驾校钟教练”，曾向谢金婵购买过游戏钻石。辨认出谢金婵，谢金婵的微信曾用名为“请叫我萍姐”，微信现用名为“如梦无痕”。

（4）检查、提取笔录，证明：①2017 年 12 月 13 日对钟某的苹果 6sPlus 手机进行检查，提取该手机内微信与“如梦无痕”的转账交易记录。②2017 年 12 月 13 日对谢金婵的苹果 6Plus 手机进行检查，发现该手机内微信名为“如梦无痕”（微信号×××），提取手机内微信转账记录及支付宝交易记录，内含谢金婵在剑龙公司购买钻石的记录清单。③2017 年 12 月 14 日对谢金钗的苹果 6sPlus 手机进行检查，提取手机内指尚游麻将的微信转账交易记录。

（5）被告人谢金婵的供述，供认自己于 2016 年 12 月与谢金钗共同组建名为“携手共创三台麻将”的赌博微信群，群内成员有一百多人，每天游戏场次一百多场，赌博比例从每积分 2 毛、3 毛逐渐提升到 5 毛。自己于 2017 年 5 月退出该群，由谢金钗管理。2017 年 5 月至 10 月 16 日，自己单独组建了名为“龙港麻将 5 毛某”的赌博微信群，每天游戏场次五十多场，每场输赢一百元，每天赌资五千元。是“阿奉”在“招募群主代理号”微信群中提议组建微信赌博群进行游戏钻石售卖，群内有剑龙公司客服号“×××”进驻，自己共通过卖钻获利 15000 元。此与上述证据能相互印证。

（6）被告人谢金钗的供述，供认自己于 2016 年 12 月与谢金婵共同组建名为“携手共创三台麻将”的赌博微信群，群内成员有五十多人，赌博比例从每积分 2 毛、3 毛逐渐提高到 5 毛，每天游戏场次一百场左右，每场输赢一百元左右，每天赌资一万元左右，2017 年 3 月因没人玩而解散该群。2017 年 5 月，自己单独组建名为“谢紫依”的赌博微信群，赌博比例为每积分 5 毛，群内成员有四五十人，每天游戏场次二十多场，每场输赢一百元左右，每天赌资 2000 元左右。自己与另一朋友“伟”一起管理该群，2017 年 9 月后将赌博微信群交给“伟”管理，自己共通过卖钻获利 8000 元左右。剑龙公司客服于 2017 年 7 月进驻赌博微信群，自己跟“阿奉”讲过自己的群是有赌博的。此与上述证据能相互印证。

4．被告人宋瑞炘组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人林某 2 的证言及辨认笔录，证明自己于 2017 年 4 月加入“阿炘”组建的名为“娱乐 1 场所”的赌博微信群，群内成员七八十人，后于 2017 年 5 月 26 日至 28 日先后共计四次进行麻将赌博，赌博比例为每积分 1 元。自己的微信名为“轩寒宇”，辨认出群主“阿炘”就是宋瑞炘。

（2）检查、提取笔录，证明 2017 年 10 月 19 日对林某 2 的 VIVO 手机进行检查，提取该手机内微信号“轩寒宇”与微信号“时光飞扬”之间的红包往来及转账记录。

（3）证人陈某 4、郑某、叶某 1 的证言及辨认笔录，证明该三人于 2017 年 5 月加入名为“娱乐 1 场所”的赌博微信群进行赌博，群主是“小宋”，群内成员七十多人，赌博比例为每积分 1 元，每场输赢一二百元。陈某 4 微信名为“燕”，郑某微信名为“（嘉宝莉）漆”、

叶某1微信名为“叶某3尚某”，三人均曾向“小宋”购买游戏钻石。叶某1另辨认出群主“小宋”就是宋瑞炘。

（4）检查、提取笔录，证明：①2017年10月19日对陈某4的OPPO手机进行检查，提取其微信号“燕”与微信号“叶某4服装”、“枫影陌客”之间的红包往来及转账记录。②2017年10月19日对郑某的OPPO进行检查，提取其微信号“（嘉宝莉）漆！”与微信号“叶某4服装”、“轩寒宇”、“小宋”之间的红包往来及转账记录。③2017年10月16日对叶某1的苹果6Plus手机进行检查,提取其微信号“叶某4服装”与微信号“（嘉宝莉）漆”、“枫影陌客”之间的红包往来及转账记录。

（5）检查、提取笔录，证明2017年10月20日对被告人宋瑞炘的两只手机进行检查，①发现VIVO手机内有与微信号“指尚游官方客服2”、“指尚游龙港麻将群主活动号10”之间的聊天记录。②发现金色苹果手机桌面上有龙港麻将APP，支付宝内有指尚游充值客服的大额转账记录。

（6）被告人宋瑞炘的供述及辨认笔录,供认自己于2017年4月组建名为“娱乐1场所”的赌博微信群进行赌博，群内成员有七十人左右，由“指尚游龙港招募群主”的剑龙公司工作人员微信号在群内统计游戏场次并发放奖励，赌博比例为每积分1元。自己的微信名为“小宋”（微信号×××），共通过销售游戏钻石获利4000元。此与上述证据能相互印证。

5．被告人陈萍萍组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人李某的证言，证明自己于2017年6、7月加入名为“Mah-jong2毛（打2毛）”的赌博微信群内进行赌博，曾向微信号“only、one”购买过游戏钻石。

（2）证人叶某2的证言，证明自己于2017年8月开始在名为“Mah-jong2毛（打2毛）”的赌博微信群内进行赌博，群内成员有七八十人，后来增加到一百多人，每场输赢二十元至六七十元不等。

（3）证人曾某的证言，证明自己于2017年5月开始先后在名为“龙港一班2毛一分群（打2毛、押金50元）”、“Mah-jong2毛（打2毛）”的赌博微信群内进行赌博，每个群内成员均有七十人左右，每场输赢二十元至四十元不等，“Mah-jong2毛（打2毛）”微信群从2017年7、8月开始，到10月中旬结束。

（4）检查、提取笔录，证明2017年10月17日对被告人陈萍萍的手机进行检查，发现该手机内微信名为“only、one”（微信号×××），微信内有“麻将对杀群”、“龙港中3”等赌博微信群，群内成员分别有13人、74人，群主均为“only、one”，“麻将对杀群”内有龙港麻将APP相关信息及发红包信息。

（5）清单，证明被告人陈萍萍销售钻石情况及与被告人朱绍晓之间微信转账情况。

（6）被告人陈萍萍的供述，供认自己于2017年5月开始组建名为“Mah-jong2毛（打2毛）”的赌博微信群进行赌博，赌博比例为每积分2毛，群内成员有一百多人，每天游戏场次七八十场，每场输赢二十元，每天赌资1400元，群内有客服微信“A008指尚游麻将直

营”（微信号 138××××****）。自己的微信名为“only、one”，共通过销售游戏钻石获利 4000 元。此与上述证据能相互印证。

6．被告人王振水组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人何某的证言，证明自己进被告人王振水拉的群赌博，后来输了些钱就退群了。

（2）被告人温兴奉的供述，供认被告人王振水有自己的赌博微信群，同时也是“台炮麻将”的钻石代理。

（3）被告人谢苏芬的供述，供认王振水有自己的赌博微信群，会到自己这里领取奖励。

（4）被告人陈菩菩的供述，供认自己与王振水共用两个一级代理号，王振水有组建台炮麻将群。

（5）被告人王振水的工作日记，记录“3-11，自己组建的微信麻将群每天都有稳定的十多个人在打，一天大概有 30 场差不多（3 分）”

（6）被告人王振水的供述，供认自己于 2017 年 4 月开始在剑龙公司上班，5 月至 7 月偷偷做销售钻石代理赚了 500 元。同年 8 月中旬，自己组建了“台炮麻将 3 毛某”微信群，群内成员六十多人，与陈菩菩共用一级、二级代理号各一个，自己的微信名为“JACK 钻石渠道部”。此与上述证据能相互印证。

7．被告人杨立银组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人陈某 2 的证言，证明自己于 2017 年 7 月加入杨立银组建的名为“龙港 2 毛”的赌博微信群进行赌博，群内成员有六十人左右，每天游戏场次二百场左右，每场输赢二十元左右。自己的微信名为“Hevs”（微信号×××）。

（2）检查、提取笔录，光盘，证明 2017 年 11 月 28 日从陈某 2 手机内提取“龙港 2 毛”、“中.发.财.2 毛”微信群截图照片，证明该二群运营情况。

（3）证人徐某的证言，证明自己于 2017 年 8 月至 9 月加入名为“龙港 2 毛某”的赌博微信群进行赌博，群主为“卖钻小达人”，当时群内成员有 37 人。

（4）检查、提取笔录，证明 2017 年 11 月 28 日对被告人杨立银的手机进行检查，发现该手机内有两个微信号，分别为“等一人”（微信号×××）、“卖钻小达人”（微信号×××）。微信内有“龙港 10 元 20 颗”、“龙港 50 元 110 颗”等多个微信好友及部分被邀请加入群聊的聊天记录，另有“指尚游龙港麻将群主活动号”（微信号×××）向其发送微信红包的记录。

（5）被告人杨立银的供述，供认自己于 2017 年 2 月至 10 月在剑龙公司上班，负责用公司提供的客服号回答玩家问题，期间分别于 2017 年 7 月、9 月组建了名为“龙港 2 毛”、“台炮 2 毛”的赌博微信群。“龙港 2 毛”赌博微信群内成员最多有八十人，赌博人员有二三十人，每天游戏场次五十场，每场输赢在十元到一百元不等，通过红包奖励、卖钻收益等获利 900 元。“台炮 2 毛”赌博微信群内成员有三十多人，每天游戏场次十场左右，每场输赢一二十元，通过红包奖励、卖钻收益等获利 100 元。自己有两个微信号，分别为“×××”、

“×××”，微信名为“卖钻小达人”，曾通过被告人陈菩菩开通二级代理的二维码。此与上述证据能相互印证。

8．被告人薛彦泽、杨昶辉组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人杨某1、陈某5、金某的证言，证明该三人于2017年2月前后加入名为“新年快乐⑤猫娱乐群”的赌博微信群进行赌博，群主为“麻将群主”，群内成员最多时有一百多人。杨某1的微信名为“杨某1”；陈某5的微信名为“新时代”；金某的微信名为“美食仙水煮海鲜”；三人均曾向群主购买过游戏钻石。杨某1的证言另证明该群于2017年4月解散，金某的证言另证明该群内每场输赢二十元至六七十元不等。

（2）检查、提取笔录，证明：①2017年10月16日对杨某1的手机进行检查，提取其微信号“杨某1”与“若川”等人之间的红包往来及转账记录。②2017年10月16日对陈某5的手机进行检查，提取其手机内微信号“新时代”与“钱氏麦片”等人之间的红包往来及转账记录。③微信号“若川”、“钱氏麦片”均在薛彦泽组建的⑤猫娱乐群。

（3）证人朱某的证言，证明自己于2016年11月加入名为“新年快乐⑤猫娱乐群”的赌博微信群，群主为“麻将群主”，群内成员有一百多人。自己的微信名为“阿某”，2017年3月就没怎么玩了。

（4）检查、提取笔录，证明：2017年10月16日对朱某的手机进行检查，提取该手机内微信号“阿某”与“若川”之间的红包往来及转账记录。

（5）检查、提取笔录，证明①2017年10月18日对薛彦泽的手机进行检查，发现该手机内有以其女儿手机号码注册的微信号“麻将群主（×××）”。②2017年10月24日对杨昶辉的手机进行检查，发现该手机内有微信名为“哎呦！生活”（微信号×××）、“麻将群主”（微信号×××）两个微信号，内有“新年快乐⑤猫娱乐群”微信群，群内成员有102人，群主为“麻将群主”，群公告显示“本群只用二维码！不支持红包！发红包者被人领了，群主概不负责！在本群注意下陌生名字，先确认好再开始游戏，否则直接终止游戏！”。

（6）被告人薛彦泽的供述及辨认笔录，供认自己于2017年2月分别组建三个赌博比例为每积分3毛、5毛、1块的微信赌博群，其中一个赌博微信群名为“新年快乐⑤猫娱乐群”。5毛某的群员最多有九十多人，3毛某和1块群各有五六十人，但三个群的群员大部分是重叠的，剑龙公司的客服微信在群内帮忙解决技术问题，各群每天游戏场次十五场左右，3毛某每场输赢十几元至四五十元，5毛某每场输赢四五十元至一百元，1块群每场输赢八九十元至两百元，自己共通过销售游戏钻石获利3000元。2017年2月至4月，由表弟杨昶辉帮忙管理这三个微信群。辨认出温兴奉就是向其出售钻石的“阿奉”，另辨认出表弟杨昶辉。此与上述证据能相互印证。

（7）被告人杨昶辉的供述及辨认笔录，供认自己于2017年1月开始在表哥薛彦泽的烟酒行里帮忙，当时薛彦泽说他创建了三个微信群组织他人使用龙港麻将软件进行赌博，但因为白天没有太多时间管理赌博微信群，让自己帮忙管理。2017年2月下旬，因为自己之前

加入到赌博微信群里打赌输了一些钱，就要求薛彦泽把这三个微信群给自己管理来赚钱，运营至3月下旬，共通过销售游戏钻石获利2500元左右。微信群内有剑龙公司客服微信号，“阿奉”曾告诉自己要管理好微信群。辨认出温兴奉即为“阿奉”，另辨认出表哥薛彦泽。此与上述证据能相互印证。

9．被告人陈海哨组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人谢某、陈某6的证言及辨认笔录，证明该二人于2017年4、5月加入陈海哨组建的名为“五毛某，买钻石联系群主”的赌博微信群进行赌博，群内成员有四十多人，每场输赢一两元到七八十元不等。谢某的微信名为“英子”，陈某6的微信名为“味蕾蓝颜蛋糕”，陈某6曾向陈海哨购买过游戏钻石。两人均辨认出陈海哨。

（2）检查、提取笔录，证明：①2017年10月17日对谢某的乐视手机进行检查，提取其微信号“英子”（微信号×××）的聊天记录截屏。②2017年10月17日对陈某6的乐视手机进行检查，提取其微信号“味蕾蓝颜蛋糕”（微信号×××）的聊天记录截屏，微信内有“五毛某，买钻联系群主”微信群，群内成员有37人，群主为“哨”（微信号×××）。

（3）证人林某3的证言，证明自己于2017年5月加入“哨”组建的名为“五毛某，买钻石联系群主”的赌博微信群进行赌博，群内成员有四十人左右，拉新人要经过群主同意，长久不参与赌博会被踢出微信群。微信群内有“哨”和“A008指尚游麻将钻石专营”在卖钻石，自己的微信名为“你在叫我吗”、“你别说话我不听”，曾向群主“哨”购买过游戏钻石。

（4）检查、提取笔录，证明2017年10月17日对林某3的苹果6sPlus手机进行检查，提取该手机内微信号“你别说话我不听”的聊天、转账记录及截屏，微信内有“五毛钱，买钻石联系群主”微信群，群主为“哨”（微信号×××），另存在多次发送龙港麻将房间号链接后，约定“一块、五毛”的赌博比例并发送微信红包的记录。

（5）检查、提取笔录，2017年10月20日对陈海哨的苹果6sPlus手机进行检查，提取该手机内微信名为“哨”（微信号×××）的聊天、转账记录，内有“五毛某，买钻石联系群主”微信群，群内成员有28人，群主为“哨”，陈海哨曾向微信号“指尚游招募群主”抱怨“群主真难做，自己钱都输光了”。

（6）被告人陈海哨的供述，供认自己于2017年5月从他人手中接手了名为“五毛欢乐群”的赌博微信群，成为代理后将群名改为“五毛某，买钻石联系群主”，群内成员有三四十人，每天游戏场次三十场左右，每场输赢四五十元，2017年7月开始就没有再运营了。上级代理是“A008指尚游麻将钻石直营”，剑龙公司客服微信号有在微信群内监督游戏场次，自己共销售游戏钻石获利1000元。此与上述证据能相互印证。

10．被告人王如浪组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人陈某7、陈某8的证言及辨认笔录，证明该二人于2017年6、7月加入王如浪（微信名为“孤浪”）组建的名为“麻将五毛某”、“龙港麻将五毛某”的赌博微信群，

赌博比例为每积分 5 毛，群内成员有三十人左右，不认识的人进群需要交押金，每场输赢几十元到一两百元不等，以几十元居多。陈某 7 的微信名为“恩典”，辨认出王如浪、陈某 8。陈某 8 的微信名为“人来，人往”，赌博总计输了两三百元，于 2017 年 7 月退群，曾向王如浪购买过游戏钻石，辨认出王如浪、陈某 7。

（2）证人方某 1 的证言，证明自己于 2017 年 5、6 月加入“孤浪”组建的赌博微信群，赌博比例为每积分 5 毛，群内成员有三十人左右，群内成员有“恩典”、“人来，人往”等，群里如果出现玩家“逃包”，群主则会垫付红包。自己的微信名为“可可麦”，大概输了五六百元。

（3）检查、提取笔录，证明 2017 年 10 月 17 日对王如浪的两只手机进行检查，①发现号码为 152××××****的苹果手机内微信名为“卡洛淋”（微信号×××），微信中有“雀神争霸中”微信群，群内成员有 31 人，群主为“孤浪”。②发现号码为 158××××****的苹果手机内微信名为“孤浪”（微信号×××），微信中有“雀神争霸中”微信群，群内成员有 29 人，群主为“孤浪”，群内有指尚游官方客服微信，聊天中涉及龙港麻将房间链接、微信红包。

（4）被告人王如浪的供述及辨认笔录，供认自己于 2017 年 5、6 月左右在一个微信群内通过龙港麻将 APP 与群内其他成员赌博，后来群主把这个赌博微信群交给自己管理。该群前后取过多个名字，有“龙港麻将五毛某”、“麻将五毛某”、“五毛某”、“雀神争霸中”等等，群内成员有三十多人，每天游戏场次二三十场，每场输赢几十元到一百元不等，每天赌资两千元左右。自己的微信名为“孤浪”，共通过销售游戏钻石获利 500 元。剑龙公司客服“指尚游龙港招募群主（zsyniuniu001）”在 2017 年 6、7 月份左右进入赌博微信群内，统计游戏场次发放奖励。辨认出陈某 7、陈某 8。

11. 被告人何友坦、陈德倍、王世庞、温兴奉、陈菩菩、王世芹、谢苏芬、王蓓蓓默许或帮助他人组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人何某的证言（剑龙公司员工），证明自己于 2017 年 6 月 1 日到剑龙公司上班，平时负责进行游戏测试。曾在“A008 指尚游麻将直营”（微信号为“×××”）开设的台炮麻将 3 毛某内赌博过，群内成员有 34 人；也曾在“台炮麻将充值”（微信号：×××）开设的台炮麻将 2 毛某内赌博过，群内成员有 30 人，每场输赢三十元至六十元不等。剑龙公司的人知道各个群内赌博的情况，只是不会管。如果不赌钱的话，打“龙港麻将”或者“台炮麻将”是没有娱乐性的。

（2）同案人员金礼浅的供述，供认剑龙公司清楚自己将游戏钻石售卖给赌博微信群内赌客的情况，自己于 2017 年 1 月向公司里的温兴奉和何友坦提出，大家都是利用“龙港麻将”在微信群里赌博的，他们两个都表示知道这个情况，并且和我说公司是有正规手续和证件的，代理不会违法犯罪。

（3）同案人员杨鸽鸽、方某 3 的供述，供认该二人组建的赌博微信群内有剑龙公司客

服微信“zsyniuniu001”、“×××”统计游戏场次，微信名为“A008 指尚游麻将自营”的微信号有在群里售卖钻石，微信名为“指尚游龙港麻将群主活动号”也在群内。

（4）同案人员缪某的供述，供认自己于 2017 年 2 月开始经温兴奉介绍，在剑龙公司以自己名义和他人名义共开设了 8 个代理账号，缪某、陈某 10、蔡某与被告人陈荣伟、朱绍晓共用一个一级代理账号，曾进入过温兴奉、陈荣伟组建的赌博微信群内。自己曾问过何友坦、温兴奉卖钻石给赌客有无关系，他们回答没有关系。2017 年 4 月，被告人温兴奉搭股 20%与缪某、胡某、杨某 2、项秉旺申请注册台炮麻将代理，经营了几个月。另被告人温兴奉分得 4000 元。

（5）同案人员陈某 10 的供述，供认自己与缪某、蔡某、被告人朱绍晓、陈荣伟共用一个一级代理号，剑龙公司客服号有进驻赌博微信群内。曾向剑龙公司询问过卖钻石是否违法，“阿奉”和何友坦都说公司是有证的，卖钻石不违法。后又向剑龙公司询问拉微信群赌博的事情，他们就说的很含糊，没有直接回答，就说没事情的，公司是正规的。

（6）同案人员倪立座的供述，供认自己于 2016 年年底开始与妻子陈菩菩代理龙港麻将、台炮麻将的游戏钻石销售，陈菩菩曾组建三个赌博比例分别为 2 毛、3 毛、5 毛的台炮麻将赌博微信群。

（7）同案人员林某 4 的供述，供认自己经倪立座介绍成为其二级代理，但未组建赌博微信群。剑龙公司客服微信“指尚游龙港麻将群主活动号”、“zsyniuniu001”、“×××”有进驻各个赌博微信群，监督游戏场次。自己曾多次询问剑龙公司员工陈菩菩在赌博微信群内售卖游戏钻石是否违法，陈菩菩说公司有经营许可证和虚拟货币销售许可证，只要不做微信群主和不玩麻将，只销售游戏钻石是不会违法的。

（8）同案人员陈某 9 的供述，供认自己于 2016 年 12 月与黄某 3、陈志钻、被告人温兴奉合股代理龙港麻将游戏钻石，温兴奉、黄某 3 有组建赌博微信群。

（9）同案人员黄某 3 的供述，供认自己和温兴奉组建赌博微信群，利用龙港麻将手机 APP 进行赌博。剑龙公司对微信群赌博的事情肯定是清楚的，因为要卖钻石的话，肯定得拉群，没有微信群钻石也不好卖，当时代理都是有赌博微信群的，而且温兴奉拉代理群的时候也直接在群里教他们怎么维护赌博微信群，温兴奉做这些也都是公司老总们的意思，所以公司很清楚。

（10）被告人陈荣伟的供述，供认剑龙公司安排客服号进驻各微信群，客服对群内赌博情况是知道的。公司就是靠卖钻石赚钱，所以不会出台禁赌措施，反而还变相宣传、支持（比如组织群主奖励活动或者搞代理奖励等等）下面的代理和玩家这么做。

（10）检查、提取笔录，证明对各被告人、同案人员的手机进行检查，大部分赌博微信群内均有剑龙公司客服微信号入驻。

（11）被告人何友坦的供述，供认自己是剑龙公司总经理，负责公司全面运营管理；王世庞、陈德倍是副总经理，王世庞负责市场部、客服部工作，陈德倍负责技术部工作；温兴

奉是市场部主管，市场部确定好活动推广方案后，由温兴奉向王世庞汇报，王世庞同意后，再向自己和陈德倍汇报，王世庞不在时由温兴奉直接向自己和陈德倍汇报。从入驻微信群的剑龙公司客服号所掌控的信息来看，微信群内存在赌博行为，那些玩家会事先商量好赌注，玩好后玩家根据得分情况再换算成钱，然后把输的钱发到群里转账给赢钱的人。剑龙公司是禁止在微信群里赌博的，并在龙港麻将APP登录界面上放了《健康游戏忠告》，显示两秒左右切换到下一界面，除此外其他禁赌措施记不清了。剑龙公司于2017年2月公测“龙港麻将”APP，5月开始钻石充值收费和推广群主奖励活动，剑龙公司客服号有“zsyniuniu001”、“×××”等十来个，通过公司授权后给员工使用进驻到各推广微信群内，监督、统计各群游戏场次并发放奖励，早期有跟代理口头讲过微信群内禁止赌博，后来就没有讲了。

（12）被告人陈德倍的供述，供认自己是剑龙公司副总经理，负责产品开发和系统维护。“zsyniuniu001”、“×××”等微信号都是通过公司授权后给员工使用的，原由市场部员工王蓓蓓、王世芹使用，后由财务部员工陈菩菩、谢苏芬轮流值班操作，主要负责进驻微信群监督、统计各群游戏场次并发放奖励。自己听说过微信群里有赌博情况，剑龙公司也知道有一部分人在微信群里面利用“龙港麻将”APP赌博，客服人员有将这些情况反馈会公司。最早的时候有跟群主、代理口头说过发现赌博可以举报到公司，公司会进行封号，后来就没有继续讲了。

（13）被告人王世庞的供述，供认自己是剑龙公司副总经理，主管行政和游戏推广，温兴奉是市场部主管，陈菩菩是财务部主管。市场部负责使用公司名下的客服微信号进驻微信群监督、统计各群游戏场次并发放奖励，在此过程中有市场部员工反映微信群里存在赌博行为，自己当时建议查封账号，但是这个情况屡禁不止，没有什么解决办法，也就听之任之没管了。

（14）被告人温兴奉的供述，供认自己是市场部主管，提出推广策划方案，经何友坦、王世庞、陈德倍商量后实施。自己知道剑龙公司钻石代理所组建的微信群存在利用“龙港麻将”APP进行赌博的情况，公司领导也都知情，目的就是通过学习“闲来麻将”的运营方式来营利。大家都知道在群里打麻将就是赌博的，只不过有些群赌大点有些群赌小点，在群里赌博之后就可以消耗钻石了，这样公司和代理都可以依靠玩家充值钻石获得利益。

（15）被告人陈菩菩、谢苏芬、王世芹、王蓓蓓的供述，供认该四人轮流操作剑龙公司“zsyniuniu001”、“zsyniuniu001”、“tpmj789”等微信号进驻各赌博微信群，负责监督、统计各群游戏场次并发放奖励，并清楚代理群里面利用指尚游麻将游戏进行赌博的情况。此与上述证据能相互印证。

12.被告人张传武组织赌博的事实，有经庭审质证的下列证据予以证明：

（1）证人黄某2的证言，证明自己于2017年5月加入名为“速度与激情2毛某”的赌博微信群进行赌博，群内成员有几十个人，自己玩了几天就退群了。

（2）证人邵某1、邵某2的证言，证明该二人分别于2017年2月、4月加入名为“速度与激情2毛某”的赌博微信群，群主为“大武钻石充值”，群内成员有五十多人，每天有二三十人玩，后分别于2017年9月、7月退群，两人均向群主购买过游戏钻石。

（3）被告人张传武的供述及辨认笔录，供认自己于2017年4月接手了蔡某的名为“速度与激情2毛某”的赌博微信群，群内成员有五十多人，每天参与赌博的有二十多人，每天游戏场次三四十场，每场输赢三四十元，群内没有剑龙公司客服号。自己的微信名为“大武钻石充值”（微信号×××），至2017年7月解散该群时，共通过贩卖钻石获利2000多元。辨认出蔡某。此与上述证据能相互印证。

13．其余全案事实，有经庭审质证的下列证据予以证明：

（1）剑龙公司章程、营业执照、股权转让协议书、变更登记情况，证明剑龙公司生产经营情况。

（2）计算机软件著作权登记证书、网络文化经营许可证，证明剑龙公司对龙港麻将软件享有著作权，并具有“利用信息网络经营游戏产品（含网络游戏虚拟货币发行）从事网络文化产品的展览比赛活动”的许可经营权。

（3）立案决定书，证明苍南县公安局于2017年2月13日立案侦查。

（4）搜查笔录，证明2017年10月16日对龙港镇德雅花苑21幢三楼剑龙网络科技有限公司进行搜查，现场查获办公电脑主机、手机、纸质笔记本、银行卡、经营许可证等物；2017年10月26日，对龙港镇德雅花苑18幢一单元102室（何友坦住处）及浙C×××**白色宝马轿车进行搜查，在车辆后备厢内发现一个棕色男士手提皮包，在皮包内搜得一本黑色外壳笔记本。

（5）行政处罚决定书，证明被告人陈荣伟、朱绍晓、宋瑞炘、陈萍萍、张传武、陈海哨、王如浪受行政处罚情况。

（6）刑事判决书，证明被告人王世庞因犯开设赌场罪于2016年10月25日被平阳县人民法院判处有期徒刑一年六个月，缓刑二年。

（7）扣押决定书、扣押清单，证明扣押在案的物品情况。

（8）收款收据，证明被告人谢金婵、谢金钗、杨昶辉、陈海哨退出违法所得情况。

（9）户籍信息、归案经过，证明各被告人的身份情况及被抓获归案的事实。

关于被告人何友坦、陈德倍、王世庞、温兴奉对公司人员组织赌博的行为是否知情的问题，经查，四被告人在侦查阶段均稳定供述自己收到客服反馈，大部分微信群内均存在赌博行为，在庭审中又改口称自己四人对此情况不知情。因四被告人均未作出合理解释，本院不予采信。

归纳控辩双方争议的焦点，本院综合评判如下：

一、关于本案是否存在非法证据排除的问题。

经查，针对各辩护人在庭前会议中提出的部分被告人供述笔录不实的问题，各被告人相

关讯问笔录均已经过本人签字确认，归案后作了多次供述稳定，且和同案人员的供述、相关证人证言等证据能相互印证。针对证据提取程序不规范的问题，本案中部分证人证言系行政证据，未转化为刑事证据，在程序上确有一定的瑕疵。该部分证言受证人人数众多、地点分散难以寻找的客观条件限制，无法重新逐一收集，但从证据的来源以及与本案的关联性分析，可以作为本案的证据使用。至于电子数据虽缺少相应清单，但并无发现有剪裁、拼凑、篡改、添加等伪造、变造情形，均能与其他证据相互印证。综上，本院未发现刑讯逼供、暴力、威胁等非法方法及其他可能严重影响司法公正情形的存在，在各被告人及辩护人未进一步提供有效线索的情况下，没有必要启动非法证据排除程序。

二、关于本案中微信群主的行为是否构成组织赌博的问题。

首先，微信群内成员利用麻将活动打赌的行为应当认定为赌博行为，而非亲友间带有少量财物输赢的娱乐活动。从组建目的来看，各被告人组建微信群主要是为了推广“指尚游麻将”APP 和销售游戏钻石营利；从职责定位来看，群主主要负责拉人、踢人、卖钻石和维持秩序，并且存在由他人接手管理微信群的情形，与日常生活中亲友群人员组成相对固定、以亲情友情为联系纽带的特征不符。各微信群内成员利用麻将活动打赌的赌博比例为每积分 2 毛到 1 块不等，换算成单局输赢为二十元到一百元不等，数额较大，且有时赌输的人会逃发红包，微信群内成员打赌的营利目的明显，即使存在少量人员为微信群主亲友，在整体微信群内赌博环境下，也与一般赌客无异。其次，各被告人组织赌博的行为符合赌博罪的构成要件。经查，微信群主主要利用群内成员赌博消耗钻石而销售游戏钻石营利，各被告人管理的微信群内成员均有 30 人以上，结合群主会踢出长期不参赌的人员、部分短期赌客退群等情形，各微信群内参赌人数均累计达 20 人以上，应当认为以营利为目的聚众赌博。

三、关于剑龙公司工作人员的行为是否构成赌博罪的问题。

本案是新型的网络犯罪，以网络游戏平台的形式招揽代理，通过手机下载“指尚游麻将”手机 APP，并由代理组建微信群招揽赌博人员购买游戏钻石（相当于房某），在微信群内进行赌博并结算赌资，各被告人通过销售游戏钻石获利。剑龙公司工作人员的行为与一般网络游戏平台正常经营行为的区分之处在于，剑龙公司派遣客服号进驻各微信群，各客服在明知微信群内存在大规模赌博行为的情况下，仍然为赌博微信群提供统计游戏场次、发放游戏奖励等服务。被告人何友坦、陈德倍等高管收到公司客服关于微信群内赌博情况的反馈后，仍然默许客服继续提供相应服务，且具有非法牟利的目的。

综上所述，剑龙公司工作人员明知他人实施赌博犯罪活动，而为其提供计算机网络、统计游戏场次、发放游戏奖励、费用结算等直接帮助，应以赌博罪共犯论处。辩护人有关各被告人无罪的辩护意见，不予采纳。

本院认为，被告人王振水、杨立银、陈荣伟、朱绍晓、宋瑞炘、谢金婵、谢金钗、陈萍萍、薛彦泽、杨昶辉、陈海哨、王如浪、张传武以营利为目的，组建微信群并聚众赌博；被告人何友坦、陈德倍、王世庞、陈菩菩、王世芹、谢苏芬、王蓓蓓明知他人聚众赌博，而为

其提供计算机网络、统计游戏场次、发放游戏奖励等直接帮助；被告人温兴奉既与朱绍晓共同组建微信群聚众赌博又为他人聚众赌博提供直接帮助，其行为均已构成赌博罪。公诉机关指控罪名成立，本院予以支持。被告人王世庞在缓刑考验期内犯新罪，依法应当撤销缓刑，实行数罪并罚。被告人朱绍晓有前科劣迹，酌情从重处罚。本案各被告人在归案后均能如实供述自己的犯罪事实，系坦白，均可从轻处罚。被告人陈菩菩、王世芹、谢苏芬、王蓓蓓受雇参与剑龙公司管理，操作剑龙公司客服号进驻各赌博微信群，提供统计游戏场次、发放游戏奖励等服务，在网络管理服务中起到了重要作用，而并非次要或辅助作用，故不属于从犯。但其作用相对于公司其他高管较轻，可酌情从轻处罚。被告人杨立银、陈荣伟、朱绍晓、宋瑞炘、谢金婵、谢金钗、陈萍萍、薛彦泽、杨昶辉、陈海哨、王如浪、张传武主动退出全部违法所得，均可酌情从轻处罚。各辩护人提出的与上述相符的辩护意见，予以采纳，其余意见，不予支持。根据各被告人的犯罪事实、犯罪性质及对社会的危害程度和悔罪表现，可对除被告人王世庞外的其余各被告人均适用缓刑。各被告人在缓刑考验期限内必须自觉接受社区矫正，服从社区矫正组织的管理教育。据此，依照《中华人民共和国刑法》第三百零三条第一款、第二十五条第一款、第七十七条、第六十九条第一、三款，第六十七条第三款、第七十二条第一、三款，第七十三条第二、三款，第六十四条以及《最高人民法院、最高人民检察院关于办理赌博刑事案件具体应用法律若干问题的解释》第一条第三项、第四条之规定，判决如下：

一、被告人何友坦犯赌博罪，判处有期徒刑十个月，缓刑一年，并处罚金人民币 8000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

二、被告人陈德倍犯赌博罪，判处有期徒刑十个月，缓刑一年，并处罚金人民币 8000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

三、被告人王世庞犯赌博罪，判处有期徒刑十个月，并处罚金人民币 8000 元。撤销平阳县人民法院（2016）浙 0326 刑初 1105 号刑事判决书主文对被告人王世庞宣告的缓刑。与原犯开设赌场罪所判处的有期徒刑一年六个月，并处罚金人民币 30000 元并罚，决定执行有期徒刑二年，并处罚金人民币 38000 元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2017 年 10 月 17 日起至 2019 年 10 月 16 日止。罚金限于本判决生效之日起十日内缴纳）。

四、被告人温兴奉犯赌博罪，判处有期徒刑一年六个月，缓刑二年，并处罚金人民币 15000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

五、被告人陈菩菩犯赌博罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币 6000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

六、被告人王世芹犯赌博罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币 6000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

七、被告人谢苏芬犯赌博罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币 6000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

八、被告人王蓓蓓犯赌博罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币 6000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

九、被告人王振水犯赌博罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币 6000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十、被告人杨立银犯赌博罪，判处有期徒刑十个月，缓刑一年，并处罚金人民币 8000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十一、被告人陈荣伟犯赌博罪，判处有期徒刑十个月，缓刑一年，并处罚金人民币 8000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十二、被告人朱绍晓犯赌博罪，判处有期徒刑一年二个月，缓刑一年六个月，并处罚金人民币 12000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十三、被告人宋瑞炘犯赌博罪，判处有期徒刑一年六个月，缓刑二年，并处罚金人民币 15000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十四、被告人谢金婵犯赌博罪，判处有期徒刑一年六个月，缓刑二年，并处罚金人民币 15000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十五、被告人谢金钗犯赌博罪，判处有期徒刑一年六个月，缓刑二年，并处罚金人民币 15000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十六、被告人陈萍萍犯赌博罪，判处有期徒刑一年二个月，缓刑一年六个月，并处罚金人民币 12000 元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十七、被告人张传武犯赌博罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币6000元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十八、被告人薛彦泽犯赌博罪，判处有期徒刑十个月，缓刑一年，并处罚金人民币8000元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

十九、被告人杨昶辉犯赌博罪，判处有期徒刑十个月，缓刑一年，并处罚金人民币8000元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

二十、被告人陈海哨犯赌博罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币6000元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

二十一、被告人王如浪犯赌博罪，判处有期徒刑八个月，缓刑一年，并处罚金人民币6000元。

（缓刑考验期限从判决确定之日起计算，罚金限于本判决生效之日起十日内缴纳）。

二十二、暂扣于苍南县公安局的各被告人违法所得，谢金婵15000元、谢金钗8000元、杨昶辉2500元、陈海哨1000元；暂扣于本院的各被告人违法所得，杨立银1000元、陈荣伟3000元、朱绍晓10000元、宋瑞炘4000元、陈萍萍4000元、张传武2000元、薛彦泽3000元、王如浪500元，均予以没收，上缴国库。

二十三、扣押于苍南县公安局的作案工具，均予以没收;扣押于苍南县公安局的涉案银行卡、部分电脑主机等非用于犯罪的财物，由该局负责发还。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向浙江省温州市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审 判 长　章荣旻

人民陪审员　　陈华淼

人民陪审员　　林文军

二〇一九年九月二十五日

书 记 员　林庆锌

案例二、周子渊、陈海孟、冯闰闰等开设赌场案

湖州市吴兴区人民法院刑事判决书

（2016）浙0502刑初1602号

公诉机关湖州市吴兴区人民检察院。

被告人周子渊，曾用名周飞，男，1987年2月22日出生，汉族，大学文化程度，江苏

省徐州市人，住址江苏省徐州市铜山区。因本案于2016年1月17日被湖州市公安局吴兴区分局刑事拘留，同年2月23日被依法逮捕。现羁押于湖州市看守所。

辩护人汝亚国、顾正伟，江苏淮海明镜律师事务所律师。

被告人陈海孟，男，1981年11月22日出生，汉族，高中文化程度，浙江省慈溪市人，住址浙江省慈溪市。因本案于2016年1月17日被湖州市公安局吴兴区分局刑事拘留，同年2月23日被依法逮捕。现羁押于湖州市看守所。

辩护人沈佩珏，浙江正同律师事务所律师。

辩护人潘新锋，浙江汉本律师事务所律师。

被告人冯闰闰，女，1984年12月8日出生，汉族，初中文化程度，浙江省慈溪市人，住址浙江省慈溪市。因本案于2016年1月17日被湖州市公安局吴兴区分局刑事拘留，同年2月23日被依法逮捕。现羁押于湖州市看守所。

辩护人宁丽娟，浙江正同律师事务所律师。

被告人尹海燕，女，1972年7月24日出生，汉族，初中文化程度，山东省昌邑市人，住址山东省昌邑市。因本案于2016年1月18日被湖州市公安局吴兴区分局刑事拘留，同年2月23日被依法逮捕。现羁押于湖州市看守所。

辩护人程垠，浙江正同律师事务所律师。

被告人隋云莉，曾用名隋丽征，女，1983年6月5日出生，汉族，初中文化程度，吉林省梅河口市人，住址吉林省集安市。因本案于2016年1月17日被湖州市公安局吴兴区分局刑事拘留，同年2月23日被依法逮捕。现羁押于湖州市看守所。

辩护人汤鉴学、沈羿欢，浙江银湖律师事务律师。

被告人刘靖，男，1980年10月11日出生，汉族，大学文化程度，湖南省沅江市人，住址广东省深圳市宝安区。因本案于2016年3月17日被湖州市公安局吴兴区分局刑事拘留，同年4月14日被变更强制措施为取保候审，2017年4月14日由本院决定被取保候审。现在居住地候审。

辩护人张洪明，北京市未名律师事务所律师。

被告人潘奕中，女，1984年2月2日出生，汉族，大学文化程度，住址广西壮族自治区平南县。因本案于2016年3月20日被湖州市公安局吴兴区分局刑事拘留，同年4月14日被变更强制措施为取保候审，2017年4月14日由本院决定被取保候审。现在居住地候审。

辩护人刘琦，北京尚伦律师事务所律师。

被告人陈振宁，男，1987年8月31日出生，汉族，大专文化程度，广东省台山市人，住址广东省台山市。因本案于2016年3月28日被湖州市公安局吴兴区分局刑事拘留，同年4月14日被变更强制措施为取保候审，2017年4月14日由本院决定被取保候审。现在居住地候审。

辩护人迟杰，北京尚伦律师事务所律师。

被告人孙虎，男，1985年9月10日出生，汉族，大专文化程度，江苏省徐州市人，住址江苏省徐州市铜山区。因本案于2016年3月24日被湖州市公安局吴兴区分局刑事拘留，同年4月19日被变更强制措施为取保候审，2017年4月19日由本院决定被取保候审。现在居住地候审。

被告人周虹宇，男，1981年4月22日出生，汉族，初中文化程度，江苏省徐州市人，住址江苏省徐州市铜山区。因本案于2016年1月17日被湖州市公安局吴兴区分局刑事拘留，同年2月3日被变更强制措施为取保候审，2017年2月3日由本院决定被取保候审。现在居住地候审。

辩护人石怀杰、李志明，江苏天根律师事务所律师。

被告人赵俊，男，1990年9月2日出生，汉族，高中文化程度，江西省德兴市人，住址江西省德兴市。因本案于2016年1月17日被湖州市公安局吴兴区分局刑事拘留，同年2月3日被变更强制措施为取保候审，2017年2月3日由本院决定被取保候审。现在居住地候审。

辩护人胡峰，浙江银湖律师事务所律师。

被告人朱华，男，1990年12月20日出生，汉族，初中文化程度，江西省德兴市人，住址江西省德兴市。因本案于2016年3月1日被湖州市公安局吴兴区分局刑事拘留，同年3月7日被变更强制措施为取保候审，2017年3月7日由本院决定被取保候审。现在居住地候审。

辩护人谢竹颖，浙江银湖律师事务所律师。

被告人陈杨丽，女，1977年1月11日出生，汉族，初中文化程度，浙江省慈溪市人，住址浙江省慈溪市。因本案于2016年1月17日被湖州市公安局吴兴区分局刑事拘留，同年2月3日被变更强制措施为取保候审，2017年2月3日由本院决定被取保候审。现在居住地候审。

辩护人沈月娣，浙江正同律师事务所律师。

辩护人张明，浙江煜华律师事务所律师。

被告人谭恩，曾用名谭思，男，1990年6月11日出生，汉族，高中文化程度，四川省旺苍县人，住址四川省旺苍县。因本案于2016年4月27日被湖州市公安局吴兴区分局刑事拘留，同年5月23日被变更强制措施为取保候审，2017年5月23日由本院决定被取保候审。现在居住地候审。

辩护人林俊，浙江银湖律师事务所律师。

被告人朱佳伟，男，1990年8月18日出生，汉族，高中文化程度，浙江省湖州市人，住址浙江省湖州市吴兴区。2014年9月15日因寻衅滋事被湖州市公安局吴兴区分局行政拘留四日。因本案于2016年1月29日被湖州市公安局吴兴区分局刑事拘留，同年2月3日被变更强制措施为取保候审，2017年2月3日由本院决定被取保候审。现在居住地候审。

被告人叶加芳，男，1989 年 1 月 9 日出生，汉族，初中文化程度，福建省莆田市人，住址福建省莆田市荔城区。因本案于 2016 年 5 月 6 日被湖州市公安局吴兴区分局刑事拘留，同年 5 月 16 日被变更强制措施为取保候审，2017 年 5 月 16 日由本院决定被取保候审。现在居住地候审。

被告人吴畏，男，1993 年 12 月 24 日出生，汉族，大专文化程度，重庆市璧山县人，住址重庆市璧山县。因本案于 2016 年 4 月 26 日被湖州市公安局吴兴区分局刑事拘留，同年 5 月 13 日被变更强制措施为取保候审，2017 年 5 月 13 日由本院决定被取保候审。现在居住地候审。

辩护人杨世东、杨小刚，浙江浔溪律师事务所律师。

被告人魏玲，女，1981 年 1 月 18 日出生，满族，大学文化程度，辽宁省西丰县人，住辽宁省沈阳市铁西区 2。因本案于 2016 年 5 月 20 日被湖州市公安局吴兴区分局取保候审，2017 年 5 月 20 日由本院决定被取保候审。现在居住地候审。

辩护人潘文奇、卢露，浙江金鼎律师事务所律师。

被告人魏一，男，1986 年 6 月 9 日出生，满族，大学文化程度，住黑龙江省大庆市室。因本案于 2016 年 5 月 11 日被湖州市公安局吴兴区分局取保候审，2017 年 5 月 11 日由本院决定被取保候审。现在居住地候审。

辩护人沈鸿伟、邬辰敏，浙江金鼎律师事务所律师。

被告人刘凯，男，1987 年 4 月 3 日出生，汉族，初中文化程度，山东省新泰市人，住山东省泰安市新泰市号。因本案于 2016 年 4 月 28 日被湖州市公安局吴兴区分局刑事拘留，同年 5 月 17 日被变更强制措施为取保候审，2017 年 5 月 17 日由本院决定被取保候审。现在居住地候审。

湖州市吴兴区人民检察院以吴检公诉刑诉[2016]1623 号起诉书指控被告人周子渊、陈海孟、冯闰闰、尹海燕、隋云莉、刘靖、潘奕中、陈振宁、孙虎、周虹宇、赵俊、朱华、陈杨丽、谭恩、朱佳伟、叶加芳、吴畏、魏玲、魏一、刘凯犯开设赌场罪，于 2016 年 12 月 23 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，公开开庭审理了此案。湖州市吴兴区人民检察院指派检察员谈根源、谭婷，代理检察员李正、薛菁菁出庭支持公诉，被告人周子渊、陈海孟、冯闰闰、尹海燕、隋云莉、刘靖、潘奕中、陈振宁、孙虎、周虹宇、赵俊、朱华、陈杨丽、谭恩、朱佳伟、叶加芳、吴畏、魏玲、魏一、刘凯及辩护人汝亚国、顾正伟、沈佩珏、潘新锋、宁丽娟、程垠、汤鉴学、张洪明、刘琦、迟杰、石怀杰、李志明、胡峰、谢竹颖、沈月娣、张明、林俊、杨世东、杨小刚、潘文奇、沈鸿伟、邬辰敏到庭参加诉讼。期间延长审限一次，延期审理一次。现已审理终结。

湖州市吴兴区人民检察院指控：

1、2013 年底至 2016 年 1 月间，被告人周子渊在虎牙直播平台 90001 频道内开设赌博房间，以金银豆押注“英雄联盟”游戏英雄的方式组织赌客赌博，并纠集被告人隋云莉、孙

虎、周虹宇在其工作室内从事“YY豆”与人民币的兑换服务。被告人赵俊、朱华、朱佳伟、谭恩、叶加芳、谭恩、刘凯、吴畏、魏一获其准许依托其赌博房间从事“YY豆”与人民币兑换交易。期间，被告人周子渊开设赌场涉及赌资共计人民币776326579余元，获利人民币560余万元；被告人隋云莉涉及赌资共计人民币258768278余元，获利人民币371339元；被告人孙虎涉及赌资共计人民币225897367余元，获利人民币72300元；被告人周虹宇涉及赌资195742354余元，获利人民币1万元；被告人赵俊、朱华涉及赌资共计人民币800余万元，获利40余万元；被告人谭恩涉及赌资共计人民币900余万元，获利人民币22万余元；被告人朱佳伟涉及赌资共计人民币600余万元，获利人民币10万余元；被告人叶加芳涉及赌资共计人民币260余万元，获利人民币10万余元；被告人魏一涉及赌资人民币240余万元，获利人民币7万余元；被告人吴畏涉及赌资共计人民币136万余元，获利人民币4万余元；被告人刘凯涉及赌资共计人民币108万余元，获利人民币3余万元。

2、2014年8月至2016年1月间，被告人陈海孟、冯闰闰在虎牙直播平台90010频道内开设赌博房间，以金银豆押注“英雄联盟”游戏英雄的方式组织赌客赌博，由其二人在工作室内从事“YY豆”与人民币的兑换服务。被告人尹海燕、陈杨丽、魏玲获其准许依托其赌博房间从事“YY豆”与人民币兑换交易。期间，被告人陈海孟、冯闰闰涉及赌资共计人民币907472683余元，获利人民币70余万元；被告人尹海燕涉及赌资共计人民币2000余万元，获利人民币5万余元；被告人陈杨丽涉及赌资共计人民币1500余万元，获利人民币20余万元；被告人魏玲涉及赌资共计人民币190余万元，获利人民币5万余元。

3、2015年11月至2016年1月间，被告人刘靖、潘奕中、陈振宁在担任成为虎牙直播负责人、管理人员期间，在明知被告人周子渊、陈海孟在虎牙直播平台90001、90010频道内开设赌场及“豆商”存在的情况后，未关停频道内赌博房间，继续向涉赌房间提供“YY豆”抽水返利、借豆等支持。被告人刘靖、潘奕中监管期间，被告人周子渊、陈海孟开设赌场的赌资共计人民币650729082余元，抽头共计人民币13114179余元；被告人陈振宁监管期间，被告人周子渊、陈海孟开设赌场的赌资共计人民币414327628余元，抽头共计人民币9161989余元。

为证明上述指控事实，公诉机关当庭宣读、出示了证人证言、被告人的供述与辩解、书证等证据，公诉机关认为，被告人周子渊、陈海孟、冯闰闰、尹海燕、隋云莉、刘靖、潘奕中、陈振宁、孙虎、周虹宇、赵俊、朱华、陈杨丽、谭恩、朱佳伟、叶加芳、吴畏、魏玲、魏一、刘凯的行为均已构成开设赌场罪，且均属情节严重。被告人潘奕中、陈振宁、朱华、朱佳伟、叶加芳、魏玲具有自首情节，依法可以从轻或减轻处罚。被告人陈海孟、冯闰闰、隋云莉、刘靖、孙虎、周虹宇、陈杨丽、谭恩、吴畏、刘凯具有坦白情节，依法可以从轻处罚，提请本院依法判处。

被告人周子渊对起诉书指控的罪名无异议，对犯罪事实有异议，其辩解起诉书指控的赌资总额有误，存在重复计算和未剔除刷礼物金额的问题，其实际涉案赌资总额应少于7000

万，另起诉书指控被告人周虹宇、孙虎的涉案赌资额不正确，特别是被告人周虹宇参与进来才两个月。其辩护人提出本案事实不清，本案涉及的虚拟货币金豆存在买卖、竞猜、刷礼物等多种用途，公诉机关在计算赌资时未区分上述多种情形，建议由专门鉴定机构计算赌资，且YY平台的所有者广华某多网络科技有限公司客观上支持、纵容赌博，帮助豆商逃避法律打击，建议在法庭在量刑时考虑该情节对被告人周子渊从轻处罚。另被告人周子渊具有坦白情节，且当庭自愿认罪，依法可以从轻处罚。

被告人陈海孟对起诉书指控的犯罪事实和罪名均无异议，但辩解被告人冯闰闰系听从自己的安排，为自己帮忙。其辩护人提出广华某多网络科技有限公司与本案有利害关系，其就赌资数额出具的情况说明不能作为定案依据，且该公司放纵赌博、通过抽水获得较大收益，对本案犯罪结果的扩大有不可推卸责任，相应地应减轻被告人陈海孟的刑罚，以及网络赌博中存在反复下注、赌资重复计算问题，请求法庭在量刑时予以考虑，另被告人陈海孟具有坦白情节，且当庭自愿认罪，依法可以从轻处罚。

被告人冯闰闰对起诉书指控的犯罪事实和罪名均无异议，但辩解自己只负责ＹＹ豆兑换业务。其辩护人提出被告人冯闰闰仅为豆商，故应根据其支付宝进出的赌资数额来认定其涉案赌资，即其涉案赌资应为1100万元，以及被告人冯闰闰在共同犯罪中系从犯，另被告人冯闰闰具有坦白情节，且当庭自愿认罪，依法可以从轻处罚。

被告人尹海燕、隋云莉、刘靖、潘奕中、陈振宁、孙虎、周虹宇、赵俊、朱华、陈杨丽、谭恩、朱佳伟、叶加芳、吴畏、魏玲、魏一、刘凯对起诉书指控的犯罪事实和罪名均无异议。

被告人尹海燕的辩护人提出起诉书指控被告人尹海燕涉及的2000余万元赌资中未扣除合法交易部分，以及被告人尹海燕系从犯，具有坦白情节，依法可以从轻处罚。

被告人隋云莉的辩护人提出公诉机关按押注金额的三分之一认定被告人隋云莉涉案赌资不合理，以及被告人隋云莉系从犯，另被告人隋云莉具有坦白情节，且当庭自愿认罪，依法可以从轻处罚。

被告人刘靖的辩护人提出被告人刘靖非开设赌场罪的正犯，其仅实施帮助行为，应认定为从犯，以及另被告人刘靖具有坦白情节，且当庭自愿认罪，依法可以从轻处罚。

被告人潘奕中的辩护人提出被告人潘奕中系从犯，且具有自首和立功情节，依法可以从轻或减轻处罚。

被告人陈振宁的辩护人提出因单位不构成开设赌场罪主体，故YY平台不构成犯罪，在没有单位犯罪的前提下，不宜以被告人周子渊、陈海孟的赌资金额及平台系统自动运行的抽水获利金额对被告人陈振宁定罪量刑，另被告人陈振宁系从犯，具有自首情节，请求法庭减轻处罚。

被告人周虹宇的辩护人提出本案将虚拟货币换算成人民币的方法有误，实际赌资金额低于公诉机关换算的金额，请求法庭仅根据被告人周虹宇的违法所得定罪量刑。

被告人赵俊、朱华、吴畏的辩护人分别提出三被告人系从犯，且具有坦白情节，请求法

庭从轻处罚。

被告人陈杨丽的辩护人提出被告人陈杨丽获利金额应认定为5万，且其系从犯，具有坦白情节，请求法庭从轻处罚。

被告人魏玲的辩护人提出被告人魏玲系从犯，且具有自首情节，请求法庭从轻处罚。

被告人魏一的辩护人提出被告人魏一系从犯，且具有自首和立功情节，请求法庭从轻处罚。

经审理查明，2013年底至2016年1月期间，被告人周子渊、陈海孟两团伙先后在虎牙直播平台××m）90001、90010频道开设竞猜厅，以虚拟货币金银豆押注英雄联盟游戏英雄属性的方式组织赌客赌博，2015年11月至2016年1月，广华某多网络科技有限公司（以下简华某多公司）珠海分公司产品总监即被告人刘靖作为虎牙直播平台的主管人员，公司项目产品经理即被告人潘奕中、公司工作人员即被告人陈振宁作为虎牙直播平台竞猜业务负责人，明知被告人周子渊、陈海孟团伙开设的竞猜厅涉嫌赌博，仍继续为其提供网络平台、出借赌博所需的虚拟货币、按比例返还赌博抽头以及帮助规避调查。

经统计，被告人周子渊在90001频道所开设的竞猜厅共接受赌客押注776325379448金豆，换算成人民币为776325379元，其个人违法所得人民币560余万元，虎牙直播平台向赢的一方抽“税”共计人民币14462101元，被告人周子渊为经营竞猜厅在江苏省徐州市设立工作室并雇佣人员为赌客提供虚拟货币金银豆与人民币现金之间的兑换业务及解说服务，被告人隋云莉、孙虎、周虹宇均受雇佣为工作室成员且均负责虚拟货币兑换业务，另被告人隋云莉还负责兑换业务记账和解说工资统计工作，其中，被告人隋云莉参与期间涉及赌资累计人民币776325379元，其个人违法所得人民币371339元，被告人孙虎参与期间涉及赌资累计人民币377122433元，其个人违法所得人民币72300元，被告人周虹宇参与期间涉及赌资累计人民币587227062元，其个人违法所得人民币1万元。被告人周子渊除雇佣人员从事虚拟货币兑换业务外，还允许被告人赵俊、朱华、朱佳伟、谭恩、叶加芳、刘凯、吴畏、魏一作为独立“豆商”在其竞猜厅内为赌客提供虚拟货币兑换服务，其中被告人赵俊、朱华涉及赌资人民币800余万元，二人违法所得共计人民币40余万元，被告人朱佳伟涉及赌资共计人民币600余万元，其个人违法所得人民币10万余元，被告人谭恩涉及赌资共计人民币900余万元，其个人违法所得共计人民币22万余元，被告人叶加芳涉及赌资共计人民币260余万元，其个人违法所得人民币10万余元，被告人刘凯涉及赌资共计人民币108万余元，其个人违法所得人民币3万余元，被告人吴畏涉及赌资共计人民币136万余元，其个人违法所得人民币4万余元，被告人魏一涉及赌资共计人民币240余万元，其个人违法所得人民币7万余元。

被告人陈海孟与被告人冯闰闰（二人系夫妻关系）在90010频道开设赌博竞猜厅，共接受赌客押注907472683422金豆，换算成人民币为907472683元，虎牙直播平台向赢的一方抽“税”共计人民币11355485元，被告人陈海孟、冯闰闰为经营竞猜厅在慈溪市掌起镇的

家中设立工作室，雇佣人员为竞猜厅提供解说服务和网络维护，另被告人冯闰闰以“豆商”身份在竞猜厅内从事虚拟货币兑换业务，其二人违法所得共计人民币 70 余万元。除被告人冯闰闰从事虚拟货币兑换业务外，被告人尹海燕、陈杨丽、魏玲获被告人陈海孟准许亦在竞猜厅作为独立“豆商”从事虚拟货币兑换业务，其中被告人尹海燕涉及赌资共计人民币 2000 余万元，其个人违法所得人民币 5 万余元，被告人陈杨丽涉及赌资共计人民币 1500 余万元，其个人违法所得人民币 20 余万元，被告人魏玲涉及赌资共计人民币 190 余万元，其个人违法所得人民币 5 万余元。

在被告人刘靖、潘奕中主管、负责期间，被告人周子渊、陈海孟两团伙在虎牙直播平台经营赌博竞猜厅共接受赌客投注 650729082332 金豆，换算成人民币为 650729082 元，虎牙直播平台向赢的一方抽“税”共计人民币 13114179 元，在被告人陈振宁参与负责期间，被告人周子渊、陈海孟两团伙在虎牙直播平台经营赌博竞猜厅共接受赌客投注 414327628228 金豆，换算成人民币为 414327628 元，虎牙直播平台向赢的一方抽“税”共计人民币 9161989 元。

案发后，公安机关冻结被告人周子渊涉案银行账户内资金共计人民币 7855607 元（其中支付宝冻结人民币 782253 元、农行卡冻结人民币 6822494 元、建行卡冻结人民币 250860 元），冻结被告人陈海孟农行卡内资金人民币 16 万元，冻结被告人尹海燕山东昌邑农村商业银行卡内资金人民币 105000 元，另从被告人尹海燕处扣押现金人民币 223000 元，从被告人冯闰闰处扣押现金人民币 219748 元，从被告人刘靖、潘奕中、陈振宁处扣押现金人民币 2435 万元，从被告人周虹宇处扣押现金人民币 1 万元，从被告人赵俊处扣押现金人民币 446300 元，从被告人朱华处扣押现金人民币 7 万元，从被告人陈杨丽处扣押现金人民币 239581 元，从被告人朱佳伟处扣押现金人民币 2 万元，从被告人叶加芳处扣押现金人民币 12000 元，从被告人魏玲处扣押现金人民币 10 万元，从被告人魏一处扣押现金人民币 15 万元。被告人孙虎的亲属向公安机关代为退缴现金人民币 3 万元，被告人谭恩的亲属向公安机关代为退缴现金人民币 10 万元，被告人叶加芳亲属向公安机关代为退缴现金人民币 10 万元，被告人吴畏亲属向公安机关代为退缴现金人民币 8 万元，被告人刘凯亲属向公安机关代为退缴现金人民币 14 万元。在案件审理过程中，被告人隋云莉家属向本院代为退缴赃款人民币 3 万元，被告人孙虎向本院退赃人民币 42300 元，被告人谭恩向本院退赃人民币 12 万元，被告人朱佳伟向本院退赃人民币 8 万元。

另查明，被告人潘奕中、陈振宁、朱华、朱佳伟、叶加芳、魏玲案发后自动投案，并如实供述自己的罪行。被告人潘奕中、魏一协助公安机关抓获其他犯罪嫌疑人。

上述事实，有下列经庭审举证、质证的证据证实，本院予以确认：证翁某,4 清李某,齐某,4 明董某,4 杰孙某 1 轩朱某,4 生王某,4 环等人证言；公安机关侦查人员出具的抓获经过、到案经过、情况说明；搜查笔录、扣押清单、发还清单；协助冻结财产通知书、协助解除冻结财产通知书；远程勘查工作记录、数据光盘；广华某多网络科技有限公司出具的情况说明；

银行交易明细单、支付宝交易明细；YY 聊天记录、微信聊天记录；电子邮件截图、网络赌博页面截图；电子数据光盘；被告人周子渊、陈海孟、冯闰闰、尹海燕、隋云莉、刘靖、潘奕中、陈振宁、孙虎、周虹宇、赵俊、朱华、陈杨丽、谭恩、朱佳伟、叶加芳、吴畏、魏玲、魏一、刘凯及同案裴某乐孙某 2 栋冯某宣吴某 1 刚吴某 2 杰、黄笔耕吴某 3 鹏的供述与辩解等。

关于被告人周子渊及被告人周子渊、陈海孟、周虹宇的辩护人提出本案赌资计算不客观的意见，经查，公安机关在侦查过程中华某多公司调取了被告人周子渊、陈海孟所开设竞猜厅的原始押注数据，后网警根据该数据统计得出总押注金豆数，并根据官方购买金豆所需资金数额认定其实际涉案赌资，该计算结果客观准确，关于被告人周子渊的辩解及被告人周子渊、陈海孟、周虹宇辩护人的该部分意见本院不予采纳。

关于被告人陈振宁的辩护人提出在没有单位犯罪的前提下，不宜以被告人周子渊、陈海孟的赌资金额及平台系统自动运行的抽水获利金额对被告人陈振宁定罪量刑的意见，经查，被告人刘靖、潘奕中、陈振宁均系网络开设赌场的共犯，应对其参与期间网络赌场的涉案赌资承担相应的刑事责任。

关于被告人冯闰闰的辩护人提出被告人冯闰闰仅为“豆商”，故应根据其支付宝进出的赌资数额认定其涉案赌资，即其涉案赌资应为人民币 1100 万元的意见，经查，根据被告人陈海孟冯某宣吴某 2 杰及被告人冯闰闰在侦查阶段的供述，被告人陈海孟、冯闰闰夫妻二人为获取非法利益在 90010 频道开设赌博竞猜厅，并相应地在慈溪市掌起镇的家中建立工作室，被告人陈海孟主要负责竞猜厅的管理，被告人冯闰闰主要负责以“豆商”身份在竞猜厅内为赌客提供虚拟货币兑换业务，其夫妻二人虽分工不同，但均应对上述竞猜厅内全部赌资负责，关于被告人冯闰闰的辩护人意见本院不予采纳。

关于被告人尹海燕的辩护人提出公诉机关指控被告人尹海燕涉及人民币 2000 余万元赌资中未扣除合法交易部分，经查，根据被告人尹海燕的供述及公安机关调取的支付宝交易记录，人民币 2000 余万元均系赌客向被告人尹海燕兑换金豆的现金，属于赌资，已剔除其他交易部分，关于被告人尹海燕辩护人的该部分意见本院不予采纳。

本院认为，被告人周子渊、陈海孟、冯闰闰、尹海燕、隋云莉、刘靖、潘奕中、陈振宁、孙虎、周虹宇、赵俊、朱华、陈杨丽、谭恩、朱佳伟、叶加芳、吴畏、魏玲、魏一、刘凯通过网络平台组织他人赌博，情节严重，其行为均已构成开设赌场罪，公诉机关指控的罪名成立，依法应予分别惩处。在被告人周子渊、隋云莉、孙虎、周虹宇开设赌场共同犯罪中，被告人周子渊起主要作用，是主犯，依法应按其所参与的全部犯罪处罚，被告人隋云莉、孙虎、周虹宇在共同犯罪中起次要作用，是从犯，依法应当从轻或减轻处罚。关于被告人隋云莉的辩护人提出被告人隋云莉系从犯的意见，本院予以采纳，关于被告人冯闰闰、刘靖、潘奕中、陈振宁、赵俊、朱华、陈杨丽、谭恩、吴畏、魏玲、魏一的辩护人分别提出该十一被告人系从犯的意见，与本院查明的事实不符，不予采纳。被告人潘奕中、陈振宁、朱华、朱佳伟、

叶加芳、魏玲案发后自动投案，并如实供述自己的罪行，是自首，依法可以从轻或减轻处罚。关于被告人潘奕中、陈振宁、朱华、魏玲的辩护人分别提出该四被告人具有自首情节的意见，本院予以采纳，关于被告人魏一的辩护人提出被告人魏一具有自首情节的意见，与本院查明的事实不符，不予采纳。被告人陈海孟、冯闰闰、隋云莉、刘靖、孙虎、周虹宇、陈杨丽、谭恩、吴畏、魏一、刘凯到案后能如实供述犯罪事实,且能当庭认罪,依法可以从轻处罚。关于被告人陈海孟、冯闰闰、隋云莉、刘靖、陈杨丽、谭恩、吴畏的辩护人分别提出该七被告人具有坦白情节的意见，本院予以采纳，关于被告人周子渊、尹海燕、赵俊的辩护人分别提出该三被告人具有坦白情节的意见，与本院查明的事实不符，不予采纳。被告人潘奕中、魏一协助公安机关抓捕其他犯罪嫌疑人，具有立功情节，依法可以从轻或减轻处罚。关于被告人潘奕中、魏一的辩护人分别提出被告人潘奕中、魏一具有立功情节的意见，本院予以采纳。被告人朱佳伟曾有违法劣迹，酌情从重处罚。被告人尹海燕、赵俊当庭自愿认罪，酌情从轻处罚。根据各被告人犯罪的事实，犯罪的性质、情节和对社会的危害程度以及归案后的认罪态度、悔罪表现，依照《中华人民共和国刑法》第三百零三条第二款、第二十五条第一款、第二十六条第一款、第四款、第二十七条、第六十七条第一款、第三款、第六十八条、第五十二条、第五十三条、第七十二条第一款、第三款、第七十三条第二款、第三款、第六十四条之规定，判决如下：

一、被告人周子渊犯开设赌场罪，判处有期徒刑六年九个月，并处罚金人民币三百万元（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即刑期自 2016 年 1 月 17 日起至 2022 年 10 月 16 日止。罚金限于本判决生效之日起十五日内向本院缴纳。）

二、被告人陈海孟犯开设赌场罪，判处有期徒刑五年六个月，并处罚金人民币六十万元（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即刑期自 2016 年 1 月 17 日起至 2021 年 7 月 16 日止。罚金限于本判决生效之日起十五日内向本院缴纳。）

三、被告人冯闰闰犯开设赌场罪，判处有期徒刑三年六个月，并处罚金人民币三十万元（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即刑期自 2016 年 1 月 17 日起至 2019 年 7 月 16 日止。罚金限于本判决生效之日起十五日内向本院缴纳。）

四、被告人尹海燕犯开设赌场罪，判处有期徒刑三年三个月，并处罚金人民币二十八万元（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即刑期自 2016 年 1 月 18 日起至 2019 年 4 月 17 日止。罚金限于本判决生效之日起十五日内向本院缴纳。）

五、被告人隋云莉犯开设赌场罪，判处有期徒刑二年九个月，并处罚金人民币十七万元（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即刑期

自2016年1月17日起至2018年10月16日止。罚金限于本判决生效之日起十五日内向本院缴纳。）

六、被告人刘靖犯开设赌场罪，判处有期徒刑三年，缓刑五年，并处罚金人民币三十三万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

七、被告人潘奕中犯开设赌场罪，判处有期徒刑二年三个月，缓刑三年三个月，并处罚金人民币二十三万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

八、被告人陈振宁犯开设赌场罪，判处有期徒刑二年，缓刑二年九个月，并处罚金人民币十五万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

九、被告人孙虎犯开设赌场罪，判处有期徒刑二年，缓刑三年，并处罚金人民币七万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

十、被告人周虹宇犯开设赌场罪，判处有期徒刑一年九个月，缓刑二年六个月，并处罚金人民币一万五千元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

十一、被告人赵俊犯开设赌场罪，判处有期徒刑三年，缓刑四年，并处罚金人民币十八万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

十二、被告人朱华犯开设赌场罪，判处有期徒刑二年六个月，缓刑三年六个月，并处罚金人民币十一万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

十三、被告人陈杨丽犯开设赌场罪，判处有期徒刑三年，缓刑五年，并处罚金人民币二十二万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

十四、被告人谭恩犯开设赌场罪，判处有期徒刑三年，缓刑四年，并处罚金人民币十七万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

十五、被告人朱佳伟犯开设赌场罪，判处有期徒刑二年三个月，缓刑三年三个月，并处罚金人民币十万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

十六、被告人叶加芳犯开设赌场罪，判处有期徒刑二年三个月，缓刑三年三个月，并处罚金人民币十万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十

五日内向本院缴纳。）

十七、被告人吴畏犯开设赌场罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币七万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

十八、被告人魏玲犯开设赌场罪，判处有期徒刑二年，缓刑三年，并处罚金人民币五万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

十九、被告人魏一犯开设赌场罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币八万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

二十、被告人刘凯犯开设赌场罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币四万元（缓刑考验期限，从判决确定之日起计算。罚金限于本判决生效之日起十五日内向本院缴纳。）

二十一、公安机关从被告人刘靖、潘奕中、陈振宁处扣押的现金人民币二千四百三十五万元，予以没收，由扣押机关处理；追缴被告人周子渊违法所得人民币五百六十万元，追缴被告人陈海孟、冯闰闰违法所得人民币七十万元，追缴被告人尹海燕违法所得人民币五万元，追缴被告人隋云莉违法所得人民币三十七万一千三百三十九元，追缴被告人孙虎违法所得人民币七万二千三百元，追缴被告人周虹宇违法所得人民币一万元，追缴被告人赵俊、朱华违法所得人民币四十万元，追缴被告人陈杨丽违法所得人民币二十万元，追缴被告人谭恩违法所得人民币二十二万元，追缴被告人朱佳伟违法所得人民币十万元，追缴被告人叶加芳违法所得人民币十万元，追缴被告人吴畏违法所得人民币四万元，追缴被告人魏玲违法所得人民币五万元，追缴被告人魏一违法所得人民币七万元，追缴被告人刘凯违法所得人民币三万元（其中扣押的赃款及冻结在案的银行账户内违法所得依法追缴后，不足部分继续追缴；扣押及冻结的其余现金转为罚金，超出罚金部分的予以发还。）。

二十二、公安机关从被告人周子渊工作室扣押的笔记本电脑一台、电脑主机八台、监控主机一台、手机一部，从被告人陈海孟工作室扣押的电脑主机十三台、笔记本电脑一台，从被告人尹海燕处扣押的电脑主机四台，笔记本电脑一台，从被告人陈杨丽处扣押的电脑主机二台，从被告人赵俊处扣押的电脑主机二台，从被告人朱佳伟处扣押的电脑主机一台，从被告人孙虎处扣押的电脑主机一台，予以没收，由扣押机关处理；公安机关从被告人尹海燕处扣押的手机四部，从被告人陈杨丽处扣押的身份证一张，从被告人赵俊处扣押的手机一部，从被告人朱佳伟处扣押的手机一部，发还各被告人。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向浙江省湖州市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审判长　谢文浩

人民陪审员　陆雪英

人民陪审员　程刚

二〇一七年九月十二日

书记员　沈飞

第二编　扰乱公共秩序罪以外之网络犯罪

一、刑法条文

第一百七十六条　【非法吸收公众存款罪】非法吸收公众存款或者变相吸收公众存款，扰乱金融秩序的，处三年以下有期徒刑或者拘役，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑，并处罚金。

单位犯前款罪的，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，依照前款的规定处罚。

有前两款行为，在提起公诉前积极退赃退赔，减少损害结果发生的，可以从轻或者减轻处罚。

第一百九十二条　【集资诈骗罪】 以非法占有为目的，使用诈骗方法非法集资，数额较大的，处三年以上七年以下有期徒刑，并处罚金；数额巨大或者有其他严重情节的，处七年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

单位犯前款罪的，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，依照前款的规定处罚。

第二百一十七条 【侵犯著作权罪】 以营利为目的，有下列侵犯著作权或者与著作权有关的权利的情形之一，违法所得数额较大或者有其他严重情节的，处三年以下有期徒刑，并处或者单处罚金；违法所得数额巨大或者有其他特别严重情节的，处三年以上十年以下有期徒刑，并处罚金：

（一）未经著作权人许可，复制发行、通过信息网络向公众传播其文字作品、音乐、美术、视听作品、计算机软件及法律、行政法规规定的其他作品的；

（二）出版他人享有专有出版权的图书的；

（三）未经录音录像制作者许可，复制发行、通过信息网络向公众传播其制作的录音录像的；

（四）未经表演者许可，复制发行录有其表演的录音录像制品，或者通过信息网络向公众传播其表演的；

（五）制作、出售假冒他人署名的美术作品的；

（六）未经著作权人或者与著作权有关的权利人许可，故意避开或者破坏权利人为其作品、录音录像制品等采取的保护著作权或者与著作权有关的权利的技术措施的。

第二百二十五条 【非法经营罪】 违反国家规定，有下列非法经营行为之一，扰乱市场秩序，情节严重的，处五年以下有期徒刑或者拘役，并处或者单处违法所得一倍以上五倍以下罚金；情节特别严重的，处五年以上有期徒刑，并处违法所得一倍以上五倍以下罚金或者没收财产：

（一）未经许可经营法律、行政法规规定的专营、专卖物品或者其他限制买卖的物品的；

（二）买卖进出口许可证、进出口原产地证明以及其他法律、行政法规规定的经营许可证或者批准文件的；

（三）未经国家有关主管部门批准非法经营证券、期货、保险业务的，或者非法从事资

金支付结算业务的；

（四）其他严重扰乱市场秩序的非法经营行为。

第二百四十六条 【侮辱罪】【诽谤罪】 以暴力或者其他方法公然侮辱他人或者捏造事实诽谤他人，情节严重的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利。

前款罪，告诉的才处理，但是严重危害社会秩序和国家利益的除外。

通过信息网络实施第一款规定的行为，被害人向人民法院告诉，但提供证据确有困难的，人民法院可以要求公安机关提供协助。

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。

第二百六十六条 【诈骗罪】诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。本法另有规定的，依照规定。

第二百七十一条 【职务侵占罪】公司、企业或者其他单位的工作人员，利用职务上的便利，将本单位财物非法占为己有，数额较大的，处三年以下有期徒刑或者拘役，并处罚金；数额巨大的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大的，处十年以上有期徒刑或者无期徒刑，并处罚金。

第二百七十四条 【敲诈勒索罪】 敲诈勒索公私财物，数额较大或者多次敲诈勒索的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑，并处罚金。

第三百六十三条 【制作、复制、出版、贩卖、传播淫秽物品牟利罪】以牟利为目的，制作、复制、出版、贩卖、传播淫秽物品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金；情节特别严重的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

二、上述罪名相关规定

1.最高人民法院关于修改《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》的决定（法释〔2022〕5号）（2021年12月30日最高人民法院审判委员会第1860次会议通过，自2022年3月1日起施行）

根据刑法修改和司法实践，现决定对《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》（法释〔2010〕18号，以下简称《解释》）作如下修改：

一、将第一条第一款第一项修改为：“未经有关部门依法许可或者借用合法经营的形式吸收资金”，第二项修改为：“通过网络、媒体、推介会、传单、手机信息等途径向社会公开宣传”。

二、将第二条第八项修改为：“以网络借贷、投资入股、虚拟币交易等方式非法吸收资金的”，第九项修改为：“以委托理财、融资租赁等方式非法吸收资金的”，增加一项作为第十项：“以提供‘养老服务’、投资‘养老项目’、销售‘老年产品’等方式非法吸收资金的”，原第十项、第十一项改为第十一项、第十二项。

三、将第三条修改为：“非法吸收或者变相吸收公众存款，具有下列情形之一的，应当依法追究刑事责任：

“（一）非法吸收或者变相吸收公众存款数额在100万元以上的；

“（二）非法吸收或者变相吸收公众存款对象150人以上的；

“（三）非法吸收或者变相吸收公众存款，给存款人造成直接经济损失数额在50万元以上的。

“非法吸收或者变相吸收公众存款数额在50万元以上或者给存款人造成直接经济损失数额在25万元以上，同时具有下列情节之一的，应当依法追究刑事责任：

“（一）曾因非法集资受过刑事追究的；

“（二）二年内曾因非法集资受过行政处罚的；

“（三）造成恶劣社会影响或者其他严重后果的。”

四、增加一条，作为第四条：“非法吸收或者变相吸收公众存款，具有下列情形之一的，应当认定为刑法第一百七十六条规定的‘数额巨大或者有其他严重情节’：

“（一）非法吸收或者变相吸收公众存款数额在500万元以上的；

“（二）非法吸收或者变相吸收公众存款对象500人以上的；

“（三）非法吸收或者变相吸收公众存款，给存款人造成直接经济损失数额在250万元以上的。

“非法吸收或者变相吸收公众存款数额在250万元以上或者给存款人造成直接经济损失数额在150万元以上，同时具有本解释第三条第二款第三项情节的，应当认定为‘其他严重情节’。”

五、增加一条，作为第五条：“非法吸收或者变相吸收公众存款，具有下列情形之一的，应当认定为刑法第一百七十六条规定的‘数额特别巨大或者有其他特别严重情节’：

“（一）非法吸收或者变相吸收公众存款数额在5000万元以上的；

“（二）非法吸收或者变相吸收公众存款对象5000人以上的；

“（三）非法吸收或者变相吸收公众存款，给存款人造成直接经济损失数额在2500万元以上的。

“非法吸收或者变相吸收公众存款数额在2500万元以上或者给存款人造成直接经济损失数额在1500万元以上，同时具有本解释第三条第二款第三项情节的，应当认定为‘其他特别严重情节’。”

六、增加一条，作为第六条：“非法吸收或者变相吸收公众存款的数额，以行为人所吸收的资金全额计算。在提起公诉前积极退赃退赔，减少损害结果发生的，可以从轻或者减轻处罚；在提起公诉后退赃退赔的，可以作为量刑情节酌情考虑。

“非法吸收或者变相吸收公众存款，主要用于正常的生产经营活动，能够在提起公诉前清退所吸收资金，可以免予刑事处罚；情节显著轻微危害不大的，不作为犯罪处理。

“对依法不需要追究刑事责任或者免予刑事处罚的，应当依法将案件移送有关行政机关。”

七、将原第四条改为第七条。

八、将原第五条改为第八条，修改为：“集资诈骗数额在10万元以上的，应当认定为‘数额较大’；数额在100万元以上的，应当认定为‘数额巨大’。

“集资诈骗数额在50万元以上，同时具有本解释第三条第二款第三项情节的，应当认定为刑法第一百九十二条规定的‘其他严重情节’。

“集资诈骗的数额以行为人实际骗取的数额计算，在案发前已归还的数额应予扣除。行为人为实施集资诈骗活动而支付的广告费、中介费、手续费、回扣，或者用于行贿、赠与等费用，不予扣除。行为人为实施集资诈骗活动而支付的利息，除本金未归还可予折抵本金以外，应当计入诈骗数额。”

九、增加一条，作为第九条：“犯非法吸收公众存款罪，判处三年以下有期徒刑或者拘役，并处或者单处罚金的，处五万元以上一百万元以下罚金；判处三年以上十年以下有期徒刑的，并处十万元以上五百万元以下罚金；判处十年以上有期徒刑的，并处五十万元以上罚金。

“犯集资诈骗罪，判处三年以上七年以下有期徒刑的，并处十万元以上五百万元以下罚金；判处七年以上有期徒刑或者无期徒刑的，并处五十万元以上罚金或者没收财产。”

十、将原第六条改为第十条。

十一、将原第七条改为第十一条。

十二、将原第八条改为第十二条，并将原第八条第二款修改为：“明知他人从事欺诈发行证券，非法吸收公众存款，擅自发行股票、公司、企业债券，集资诈骗或者组织、领导传销活动等集资犯罪活动，为其提供广告等宣传的，以相关犯罪的共犯论处。”

十三、增加一条，作为第十三条：“通过传销手段向社会公众非法吸收资金，构成非法吸收公众存款罪或者集资诈骗罪，同时又构成组织、领导传销活动罪的，依照处罚较重的规定定罪处罚。”

十四、增加一条，作为第十四条：“单位实施非法吸收公众存款、集资诈骗犯罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，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定罪处罚。”

十五、将原第九条改为第十五条。

本决定自 2022 年 3 月 1 日起施行。

根据本决定，对《解释》作相应修改并调整条文顺序后，重新公布。

最高人民法院
关于审理非法集资刑事案件具体应用法律
若干问题的解释

（2010 年 11 月 22 日最高人民法院审判委员会第 1502 次会议通过，根据 2021 年 12 月 30 日最高人民法院审判委员会第 1860 次会议通过的《最高人民法院关于修改〈最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释〉的决定》修正，该修正自 2022 年 3 月 1 日起施行）

为依法惩治非法吸收公众存款、集资诈骗等非法集资犯罪活动，根据《中华人民共和国刑法》的规定，现就审理此类刑事案件具体应用法律的若干问题解释如下：

第一条 违反国家金融管理法律规定，向社会公众（包括单位和个人）吸收资金的行为，同时具备下列四个条件的，除刑法另有规定的以外，应当认定为刑法第一百七十六条规定的“非法吸收公众存款或者变相吸收公众存款”：

（一）未经有关部门依法许可或者借用合法经营的形式吸收资金；

（二）通过网络、媒体、推介会、传单、手机信息等途径向社会公开宣传；

（三）承诺在一定期限内以货币、实物、股权等方式还本付息或者给付回报；

（四）向社会公众即社会不特定对象吸收资金。

未向社会公开宣传，在亲友或者单位内部针对特定对象吸收资金的，不属于非法吸收或者变相吸收公众存款。

第二条 实施下列行为之一，符合本解释第一条第一款规定的条件的，应当依照刑法第一百七十六条的规定，以非法吸收公众存款罪定罪处罚：

（一）不具有房产销售的真实内容或者不以房产销售为主要目的，以返本销售、售后包租、约定回购、销售房产份额等方式非法吸收资金的；

（二）以转让林权并代为管护等方式非法吸收资金的；

（三）以代种植（养殖）、租种植（养殖）、联合种植（养殖）等方式非法吸收资金的；

（四）不具有销售商品、提供服务的真实内容或者不以销售商品、提供服务为主要目的，以商品回购、寄存代售等方式非法吸收资金的；

（五）不具有发行股票、债券的真实内容，以虚假转让股权、发售虚构债券等方式非法吸收资金的；

（六）不具有募集基金的真实内容，以假借境外基金、发售虚构基金等方式非法吸收资金的；

（七）不具有销售保险的真实内容，以假冒保险公司、伪造保险单据等方式非法吸收资金的；

（八）以网络借贷、投资入股、虚拟币交易等方式非法吸收资金的；

（九）以委托理财、融资租赁等方式非法吸收资金的；

（十）以提供“养老服务”、投资“养老项目”、销售“老年产品”等方式非法吸收资金的；

（十一）利用民间“会”“社”等组织非法吸收资金的；

（十二）其他非法吸收资金的行为。

第三条 非法吸收或者变相吸收公众存款，具有下列情形之一的，应当依法追究刑事责任：

（一）非法吸收或者变相吸收公众存款数额在100万元以上的；

（二）非法吸收或者变相吸收公众存款对象150人以上的；

（三）非法吸收或者变相吸收公众存款，给存款人造成直接经济损失数额在50万元以上的。

非法吸收或者变相吸收公众存款数额在50万元以上或者给存款人造成直接经济损失数额在25万元以上，同时具有下列情节之一的，应当依法追究刑事责任：

（一）曾因非法集资受过刑事追究的；

（二）二年内曾因非法集资受过行政处罚的；

（三）造成恶劣社会影响或者其他严重后果的。

第四条 非法吸收或者变相吸收公众存款，具有下列情形之一的，应当认定为刑法第一百七十六条规定的“数额巨大或者有其他严重情节”：

（一）非法吸收或者变相吸收公众存款数额在500万元以上的；

（二）非法吸收或者变相吸收公众存款对象500人以上的；

（三）非法吸收或者变相吸收公众存款，给存款人造成直接经济损失数额在250万元以上的。

非法吸收或者变相吸收公众存款数额在250万元以上或者给存款人造成直接经济损失数额在150万元以上，同时具有本解释第三条第二款第三项情节的，应当认定为“其他严重情节”。

第五条 非法吸收或者变相吸收公众存款，具有下列情形之一的，应当认定为刑法第一百七十六条规定的“数额特别巨大或者有其他特别严重情节”：

（一）非法吸收或者变相吸收公众存款数额在5000万元以上的；

（二）非法吸收或者变相吸收公众存款对象5000人以上的；

（三）非法吸收或者变相吸收公众存款，给存款人造成直接经济损失数额在2500万元以上的。

非法吸收或者变相吸收公众存款数额在2500万元以上或者给存款人造成直接经济损失数额在1500万元以上，同时具有本解释第三条第二款第三项情节的，应当认定为“其他特别严重情节”。

第六条 非法吸收或者变相吸收公众存款的数额，以行为人所吸收的资金全额计算。在提起公诉前积极退赃退赔，减少损害结果发生的，可以从轻或者减轻处罚；在提起公诉后退赃退赔的，可以作为量刑情节酌情考虑。

非法吸收或者变相吸收公众存款，主要用于正常的生产经营活动，能够在提起公诉前清退所吸收资金，可以免予刑事处罚；情节显著轻微危害不大的，不作为犯罪处理。

对依法不需要追究刑事责任或者免予刑事处罚的，应当依法将案件移送有关行政机关。

第七条 以非法占有为目的，使用诈骗方法实施本解释第二条规定所列行为的，应当依照刑法第一百九十二条的规定，以集资诈骗罪定罪处罚。

使用诈骗方法非法集资，具有下列情形之一的，可以认定为“以非法占有为目的”：

（一）集资后不用于生产经营活动或者用于生产经营活动与筹集资金规模明显不成比例，致使集资款不能返还的；

（二）肆意挥霍集资款，致使集资款不能返还的；

（三）携带集资款逃匿的；

（四）将集资款用于违法犯罪活动的；

（五）抽逃、转移资金、隐匿财产，逃避返还资金的；

（六）隐匿、销毁账目，或者搞假破产、假倒闭，逃避返还资金的；

（七）拒不交代资金去向，逃避返还资金的；

（八）其他可以认定非法占有目的的情形。

集资诈骗罪中的非法占有目的，应当区分情形进行具体认定。行为人部分非法集资行为具有非法占有目的的，对该部分非法集资行为所涉集资款以集资诈骗罪定罪处罚；非法集资共同犯罪中部分行为人具有非法占有目的，其他行为人没有非法占有集资款的共同故意和行为的，对具有非法占有目的的行为人以集资诈骗罪定罪处罚。

第八条 集资诈骗数额在 10 万元以上的，应当认定为“数额较大”；数额在 100 万元以上的，应当认定为“数额巨大”。

集资诈骗数额在 50 万元以上，同时具有本解释第三条第二款第三项情节的，应当认定为刑法第一百九十二条规定的“其他严重情节”。

集资诈骗的数额以行为人实际骗取的数额计算，在案发前已归还的数额应予扣除。行为人为实施集资诈骗活动而支付的广告费、中介费、手续费、回扣，或者用于行贿、赠与等费

用，不予扣除。行为人为实施集资诈骗活动而支付的利息，除本金未归还可予折抵本金以外，应当计入诈骗数额。

第九条 犯非法吸收公众存款罪，判处三年以下有期徒刑或者拘役，并处或者单处罚金的，处五万元以上一百万元以下罚金；判处三年以上十年以下有期徒刑的，并处十万元以上五百万元以下罚金；判处十年以上有期徒刑的，并处五十万元以上罚金。

犯集资诈骗罪，判处三年以上七年以下有期徒刑的，并处十万元以上五百万元以下罚金；判处七年以上有期徒刑或者无期徒刑的，并处五十万元以上罚金或者没收财产。

第十条 未经国家有关主管部门批准，向社会不特定对象发行、以转让股权等方式变相发行股票或者公司、企业债券，或者向特定对象发行、变相发行股票或者公司、企业债券累计超过 200 人的，应当认定为刑法第一百七十九条规定的“擅自发行股票或者公司、企业债券”。构成犯罪的，以擅自发行股票、公司、企业债券罪定罪处罚。

第十一条 违反国家规定，未经依法核准擅自发行基金份额募集基金，情节严重的，依照刑法第二百二十五条的规定，以非法经营罪定罪处罚。

第十二条 广告经营者、广告发布者违反国家规定，利用广告为非法集资活动相关的商品或者服务作虚假宣传，具有下列情形之一的，依照刑法第二百二十二条的规定，以虚假广告罪定罪处罚：

（一）违法所得数额在 10 万元以上的；

（二）造成严重危害后果或者恶劣社会影响的；

（三）二年内利用广告作虚假宣传，受过行政处罚二次以上的；

（四）其他情节严重的情形。

明知他人从事欺诈发行证券，非法吸收公众存款，擅自发行股票、公司、企业债券，集资诈骗或者组织、领导传销活动等集资犯罪活动，为其提供广告等宣传的，以相关犯罪的共犯论处。

第十三条 通过传销手段向社会公众非法吸收资金，构成非法吸收公众存款罪或者集资诈骗罪，同时又构成组织、领导传销活动罪的，依照处罚较重的规定定罪处罚。

第十四条 单位实施非法吸收公众存款、集资诈骗犯罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，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定罪处罚。

第十五条 此前发布的司法解释与本解释不一致的，以本解释为准。

2.《最高人民法院关于非法集资刑事案件性质认定问题的通知》（法[2011]262 号）

各省、自治区、直辖市高级人民法院，解放军军事法院，新疆维吾尔自治区高级人民法院生产建设兵团分院：

为依法、准确、及时审理非法集资刑事案件，现就非法集资性质认定的有关问题通知如下：

一、行政部门对于非法集资的性质认定，不是非法集资案件进入刑事程序的必经程序。行政部门未对非法集资作出性质认定的，不影响非法集资刑事案件的审判。

二、人民法院应当依照刑法和最高人民法院《关于审理非法集资刑事案件具体应用法律若干问题的解释》等有关规定认定案件事实的性质，并认定相关行为是否构成犯罪。

三、对于案情复杂、性质认定疑难的案件，人民法院可以在有关部门关于是否符合行业技术标准的行政认定意见的基础上，根据案件事实和法律规定作出性质认定。

四、非法集资刑事案件的审判工作涉及领域广、专业性强，人民法院在审理此类案件当中要注意加强与有关行政主(监)管部门以及公安机关、人民检察院的配合。审判工作中遇到重大问题难以解决的，请及时报告最高人民法院。

2011 年 8 月 18 日

3.《最高人民检察院关于办理涉互联网金融犯罪案件有关问题座谈会纪要》（高检诉[2017]14 号）

互联网金融是金融与互联网相互融合形成的新型金融业务模式。发展互联网金融，对加快实施创新驱动发展战略、推进供给侧结构性改革、促进经济转型升级具有积极作用。但是，在互联网金融快速发展过程中，部分机构、业态偏离了正确方向，有些甚至打着"金融创新"的幌子进行非法集资、金融诈骗等违法犯罪活动，严重扰乱了金融管理秩序，侵害了人民群众合法权益。2016 年 4 月，国务院部署开展了互联网金融风险专项整治工作，集中整治违法违规行为，防范和化解互联网金融风险。各级检察机关积极参与专项整治工作，依法办理进入检察环节的涉互联网金融犯罪案件。针对办案中遇到的新情况、新问题，高检院公诉厅先后在昆明、上海、福州召开座谈会，对办理涉互联网金融犯罪案件中遇到的有关行为性质、法律适用、证据审查、追诉范围等问题进行了深入研究。纪要如下：

一、办理涉互联网金融犯罪案件的基本要求

促进和保障互联网金融规范健康发展，是检察机关服务经济社会发展的重要内容。各地检察机关公诉部门应当充分认识防范和化解互联网金融风险的重要性、紧迫性和复杂性，立足检察职能，积极参与互联网金融风险专项整治工作，有效预防、依法惩治涉互联网金融犯罪，切实维护人民群众合法权益，维护国家金融安全。

1　准确认识互联网金融的本质。互联网金融的本质仍然是金融，其潜在的风险与传统金融没有区别，甚至还可能因互联网的作用而被放大。要依据现有的金融管理法律规定，依法准确判断各类金融活动、金融业态的法律性质，准确界定金融创新和金融违法犯罪的界限。在办理涉互联网金融犯罪案件时，判断是否符合"违反国家规定""未经有关国家主管部门批准"等要件时，应当以现行刑事法律和金融管理法律法规为依据。对各种类型互联网金融活动，要深入剖析行为实质并据此判断其性质，从而准确区分罪与非罪、此罪与彼罪、罪轻与罪重、打击与保护的界限，不能机械地被所谓"互联网金融创新"表象所迷惑。

2　妥善把握刑事追诉的范围和边界。涉互联网金融犯罪案件涉案人员众多，要按照区别对待的原则分类处理，综合运用刑事追诉和非刑事手段处置和化解风险，打击少数、教育挽救大多数。要坚持主客观相统一的原则，根据犯罪嫌疑人在犯罪活动中的地位作用、涉案数额、危害结果、主观过错等主客观情节，综合判断责任轻重及刑事追诉的必要性，做到罪责适应、罚当其罪。对犯罪情节严重、主观恶性大、在犯罪中起主要作用的人员，特别是核

心管理层人员和骨干人员，依法从严打击；对犯罪情节相对较轻、主观恶性较小、在犯罪中起次要作用的人员依法从宽处理。

3　注重案件统筹协调推进。涉互联网金融犯罪跨区域特征明显，各地检察机关公诉部门要按照"统一办案协调、统一案件指挥、统一资产处置、分别侦查诉讼、分别落实维稳"（下称"三统两分"）的要求分别处理好辖区内案件，加强横向、纵向联系，在上级检察机关特别是省级检察院的指导下统一协调推进办案工作，确保辖区内案件处理结果相对平衡统一。跨区县案件由地市级检察院统筹协调，跨地市案件由省级检察院统一协调，跨省案件由高检院公诉厅统一协调。各级检察机关公诉部门要加强与公安机关、地方金融办等相关单位以及检察机关内部侦监、控申等部门的联系，建立健全案件信息通报机制，及时掌握重大案件的立案、侦查、批捕、信访等情况，适时开展提前介入侦查等工作，并及时上报上级检察院。省级检察院公诉部门要发挥工作主动性，主动掌握社会影响大的案件情况，研究制定工作方案，统筹协调解决办案中遇到的问题，重大、疑难、复杂问题要及时向高检院报告。

4　坚持司法办案"三个效果"有机统一。涉互联网金融犯罪影响广泛，社会各界特别是投资人群体十分关注案件处理。各级检察机关公诉部门要从有利于全案依法妥善处置的角度出发，切实做好提前介入侦查引导取证、审查起诉、出庭公诉等各个阶段的工作，依法妥善处理重大敏感问题，不能机械司法、就案办案。同时，要把办案工作与保障投资人合法权益紧密结合起来，同步做好释法说理、风险防控、追赃挽损、维护稳定等工作，努力实现司法办案的法律效果、社会效果、政治效果有机统一。

二、准确界定涉互联网金融行为法律性质

5　互联网金融涉及 P2P 网络借贷、股权众筹、第三方支付、互联网保险以及通过互联网开展资产管理及跨界从事金融业务等多个金融领域，行为方式多样，所涉法律关系复杂。违法犯罪行为隐蔽性、迷惑性强，波及面广，社会影响大，要根据犯罪行为的实质特征和社会危害，准确界定行为的法律性质和刑法适用的罪名。

（一）非法吸收公众存款行为的认定

6　涉互联网金融活动在未经有关部门依法批准的情形下，公开宣传并向不特定公众吸收资金，承诺在一定期限内还本付息的，应当依法追究刑事责任。其中，应重点审查互联网金融活动相关主体是否存在归集资金、沉淀资金，致使投资人资金存在被挪用、侵占等重大风险等情形。

7　互联网金融的本质是金融，判断其是否属于"未经有关部门依法批准"，即行为是否具有非法性的主要法律依据是《商业银行法》、《非法金融机构和非法金融业务活动取缔办法》（国务院令第 247 号）等现行有效的金融管理法律规定。

8　对以下网络借贷领域的非法吸收公众资金的行为，应当以非法吸收公众存款罪分别追究相关行为主体的刑事责任：

（1）中介机构以提供信息中介服务为名，实际从事直接或间接归集资金、甚至自融或变相自融等行为，应当依法追究中介机构的刑事责任。特别要注意识别变相自融行为，如中介机构通过拆分融资项目期限、实行债权转让等方式为自己吸收资金的，应当认定为非法吸收公众存款。

（2）中介机构与借款人存在以下情形之一的，应当依法追究刑事责任：①中介机构与

借款人合谋或者明知借款人存在违规情形，仍为其非法吸收公众存款提供服务的；中介机构与借款人合谋，采取向出借人提供信用担保、通过电子渠道以外的物理场所开展借贷业务等违规方式向社会公众吸收资金的；②双方合谋通过拆分融资项目期限、实行债权转让等方式为借款人吸收资金的。在对中介机构、借款人进行追诉时，应根据各自在非法集资中的地位、作用确定其刑事责任。中介机构虽然没有直接吸收资金，但是通过大肆组织借款人开展非法集资并从中收取费用数额巨大、情节严重的，可以认定为主犯。

（3）借款人故意隐瞒事实，违反规定，以自己名义或借用他人名义利用多个网络借贷平台发布借款信息，借款总额超过规定的最高限额，或将吸收资金用于明确禁止的投资股票、场外配资、期货合约等高风险行业，造成重大损失和社会影响的，应当依法追究借款人的刑事责任。对于借款人将借款主要用于正常的生产经营活动，能够及时清退所吸收资金，不作为犯罪处理。

9　在非法吸收公众存款罪中，原则上认定主观故意并不要求以明知法律的禁止性规定为要件。特别是具备一定涉金融活动相关从业经历、专业背景或在犯罪活动中担任一定管理职务的犯罪嫌疑人，应当知晓相关金融法律管理规定，如果有证据证明其实际从事的行为应当批准而未经批准，行为在客观上具有非法性，原则上就可以认定其具有非法吸收公众存款的主观故意。在证明犯罪嫌疑人的主观故意时，可以收集运用犯罪嫌疑人的任职情况、职业经历、专业背景、培训经历、此前任职单位或者其本人因从事同类行为受到处罚情况等证据，证明犯罪嫌疑人提出的"不知道相关行为被法律所禁止，故不具有非法吸收公众存款的主观故意"等辩解不能成立。除此之外，还可以收集运用以下证据进一步印证犯罪嫌疑人知道或应当知道其所从事行为具有非法性，比如犯罪嫌疑人故意规避法律以逃避监管的相关证据：自己或要求下属与投资人签订虚假的亲友关系确认书，频繁更换宣传用语逃避监管，实际推介内容与宣传用语、实际经营状况不一致，刻意向投资人夸大公司兑付能力，在培训课程中传授或接受规避法律的方法，等等。

10　对于无相关职业经历、专业背景，且从业时间短暂，在单位犯罪中层级较低，纯属执行单位领导指令的犯罪嫌疑人提出辩解的，如确实无其他证据证明其具有主观故意的，可以不作为犯罪处理。另外，实践中还存在犯罪嫌疑人提出因信赖行政主管部门出具的相关意见而陷入错误认识的辩解。如果上述辩解确有证据证明，不应作为犯罪处理，但应当对行政主管部门出具的相关意见及其出具过程进行查证，如存在以下情形之一，仍应认定犯罪嫌疑人具有非法吸收公众存款的主观故意：

（1）行政主管部门出具意见所涉及的行为与犯罪嫌疑人实际从事的行为不一致的；

（2）行政主管部门出具的意见未对是否存在非法吸收公众存款问题进行合法性审查，仅对其他合法性问题进行审查的；

（3）犯罪嫌疑人在行政主管部门出具意见时故意隐瞒事实、弄虚作假的；

（4）犯罪嫌疑人与出具意见的行政主管部门的工作人员存在利益输送行为的；

（5）犯罪嫌疑人存在其他影响和干扰行政主管部门出具意见公正性的情形的。

对于犯罪嫌疑人提出因信赖专家学者、律师等专业人士、主流新闻媒体宣传或有关行政主管部门工作人员的个人意见而陷入错误认识的辩解，不能作为犯罪嫌疑人判断自身行为合法性的根据和排除主观故意的理由。

11　负责或从事吸收资金行为的犯罪嫌疑人非法吸收公众存款金额，根据其实际参与吸收的全部金额认定。但以下金额不应计入该犯罪嫌疑人的吸收金额：

（1）犯罪嫌疑人自身及其近亲属所投资的资金金额；

（2）记录在犯罪嫌疑人名下，但其未实际参与吸收且未从中收取任何形式好处的资金。

吸收金额经过司法会计鉴定的，可以将前述不计入部分直接扣除。但是，前述两项所涉金额仍应计入相对应的上一级负责人及所在单位的吸收金额。

12　投资人在每期投资结束后，利用投资账户中的资金（包括每期投资结束后归还的本金、利息）进行反复投资的金额应当累计计算，但对反复投资的数额应当作出说明。对负责或从事行政管理、财务会计、技术服务等辅助工作的犯罪嫌疑人，应当按照其参与的犯罪事实，结合其在犯罪中的地位和作用，依法确定刑事责任范围。

13　确定犯罪嫌疑人的吸收金额时，应当重点审查、运用以下证据：（1）涉案主体自身的服务器或第三方服务器上存储的交易记录等电子数据；（2）会计账簿和会计凭证；（3）银行账户交易记录、POS 机支付记录；（4）资金收付凭证、书面合同等书证。仅凭投资人报案数据不能认定吸收金额。

（二）集资诈骗行为的认定

14　以非法占有为目的，使用诈骗方法非法集资，是集资诈骗罪的本质特征。是否具有非法占有目的，是区分非法吸收公众存款罪和集资诈骗罪的关键要件，对此要重点围绕融资项目真实性、资金去向、归还能力等事实进行综合判断。犯罪嫌疑人存在以下情形之一的，原则上可以认定具有非法占有目的：

（1）大部分资金未用于生产经营活动，或名义上投入生产经营但又通过各种方式抽逃转移资金的；

（2）资金使用成本过高，生产经营活动的盈利能力不具有支付全部本息的现实可能性的；

（3）对资金使用的决策极度不负责任或肆意挥霍造成资金缺口较大的；

（4）归还本息主要通过借新还旧来实现的；

（5）其他依照有关司法解释可以认定为非法占有目的的情形。

15　对于共同犯罪或单位犯罪案件中，不同层级的犯罪嫌疑人之间存在犯罪目的发生转化或者犯罪目的明显不同的，应当根据犯罪嫌疑人的犯罪目的分别认定。

（1）注意区分犯罪目的发生转变的时间节点。犯罪嫌疑人在初始阶段仅具有非法吸收公众存款的故意，不具有非法占有目的，但在发生经营失败、资金链断裂等问题后，明知没有归还能力仍然继续吸收公众存款的，这一时间节点之后的行为应当认定为集资诈骗罪，此前的行为应当认定为非法吸收公众存款罪。

（2）注意区分犯罪嫌疑人的犯罪目的的差异。在共同犯罪或单位犯罪中，犯罪嫌疑人由于层级、职责分工、获取收益方式、对全部犯罪事实的知情程度等不同，其犯罪目的也存在不同。在非法集资犯罪中，有的犯罪嫌疑人具有非法占有的目的，有的则不具有非法占有目的，对此，应当分别认定为集资诈骗罪和非法吸收公众存款罪。

16　证明主观上是否具有非法占有目的，可以重点收集、运用以下客观证据：

（1）与实施集资诈骗整体行为模式相关的证据：投资合同、宣传资料、培训内容等；

（2）与资金使用相关的证据：资金往来记录、会计账簿和会计凭证、资金使用成本（包括利息和佣金等）、资金决策使用过程、资金主要用途、财产转移情况等；

（3）与归还能力相关的证据：吸收资金所投资项目内容、投资实际经营情况、盈利能力、归还本息资金的主要来源、负债情况、是否存在虚构业绩等虚假宣传行为等；

（4）其他涉及欺诈等方面的证据：虚构融资项目进行宣传、隐瞒资金实际用途、隐匿销毁账簿；等等。司法会计鉴定机构对相关数据进行鉴定时，办案部门可以根据查证犯罪事实的需要提出重点鉴定的项目，保证司法会计鉴定意见与待证的构成要件事实之间的关联性。

17　集资诈骗的数额，应当以犯罪嫌疑人实际骗取的金额计算。犯罪嫌疑人为吸收公众资金制造还本付息的假象，在诈骗的同时对部分投资人还本付息的，集资诈骗的金额以案发时实际未兑付的金额计算。案发后，犯罪嫌疑人主动退还集资款项的，不能从集资诈骗的金额中扣除，但可以作为量刑情节考虑。

（三）非法经营资金支付结算行为的认定

18　支付结算业务（也称支付业务）是商业银行或者支付机构在收付款人之间提供的货币资金转移服务。非银行机构从事支付结算业务，应当经中国人民银行批准取得《支付业务许可证》，成为支付机构。未取得支付业务许可从事该业务的行为，违反《非法金融机构和非法金融业务活动取缔办法》第四条第一款第（三）、（四）项的规定，破坏了支付结算业务许可制度，危害支付市场秩序和安全，情节严重的，适用刑法第二百二十五条第（三）项，以非法经营罪追究刑事责任。具体情形：

（1）未取得支付业务许可经营基于客户支付账户的网络支付业务。无证网络支付机构为客户非法开立支付账户，客户先把资金支付到该支付账户，再由无证机构根据订单信息从支付账户平台将资金结算到收款人银行账户。

（2）未取得支付业务许可经营多用途预付卡业务。无证发卡机构非法发行可跨地区、跨行业、跨法人使用的多用途预付卡，聚集大量的预付卡销售资金，并根据客户订单信息向商户划转结算资金。

19　在具体办案时，要深入剖析相关行为是否具备资金支付结算的实质特征，准确区分支付工具的正常商业流转与提供支付结算服务、区分单用途预付卡与多用途预付卡业务，充分考虑具体行为与"地下钱庄"等同类犯罪在社会危害方面的相当性以及刑事处罚的必要性，严格把握入罪和出罪标准。

三、依法认定单位犯罪及其责任人员

20　涉互联网金融犯罪案件多以单位形式组织实施，所涉单位数量众多、层级复杂，其中还包括大量分支机构和关联单位，集团化特征明显。有的涉互联网金融犯罪案件中分支机构遍布全国，既有具备法人资格的，又有不具备法人资格的；既有受总公司直接领导的，又有受总公司的下属单位领导的。公安机关在立案时做法不一，有的对单位立案，有的不对单位立案，有的被立案的单位不具有独立法人资格，有的仅对最上层的单位立案而不对分支机构立案。对此，检察机关公诉部门在审查起诉时，应当从能够全面揭示犯罪行为基本特征、全面覆盖犯罪活动、准确界定区分各层级人员的地位作用、有利于有力指控犯罪、有利于追缴违法所得等方面依法具体把握，确定是否以单位犯罪追究。

21　涉互联网金融犯罪所涉罪名中，刑法规定应当追究单位刑事责任的，对同时具备以下情形且具有独立法人资格的单位，可以以单位犯罪追究：

（1）犯罪活动经单位决策实施；

（2）单位的员工主要按照单位的决策实施具体犯罪活动；

（3）违法所得归单位所有，经单位决策使用，收益亦归单位所有。但是，单位设立后

专门从事违法犯罪活动的，应当以自然人犯罪追究刑事责任。

22　对参与涉互联网金融犯罪，但不具有独立法人资格的分支机构，是否追究其刑事责任，可以区分两种情形处理：

（1）全部或部分违法所得归分支机构所有并支配，分支机构作为单位犯罪主体追究刑事责任；

（2）违法所得完全归分支机构上级单位所有并支配的，不能对分支机构作为单位犯罪主体追究刑事责任，而是应当对分支机构的上级单位（符合单位犯罪主体资格）追究刑事责任。

23　分支机构认定为单位犯罪主体的，该分支机构相关涉案人员应当作为该分支机构的"直接负责的主管人员"或者"其他直接责任人员"追究刑事责任。仅将分支机构的上级单位认定为单位犯罪主体的，该分支机构相关涉案人员可以作为该上级单位的"其他直接责任人员"追究刑事责任。

24　对符合追诉条件的分支机构（包括具有独立法人资格的和不具有独立法人资格）及其所属单位，公安机关均没有作为犯罪嫌疑单位移送审查起诉，仅将其所属单位的上级单位作为犯罪嫌疑单位移送审查起诉的，对相关分支机构涉案人员可以区分以下情形处理：

（1）有证据证明被立案的上级单位（比如总公司）在业务、财务、人事等方面对下属单位及其分支机构进行实际控制，下属单位及其分支机构涉案人员可以作为被移送审查起诉的上级单位的"其他直接责任人员"追究刑事责任。在证明实际控制关系时，应当收集、运用公司决策、管理、考核等相关文件，OA 系统等电子数据，资金往来记录等证据。对不同地区同一单位的分支机构涉案人员起诉时，证明实际控制关系的证据体系、证明标准应基本一致。

（2）据现有证据无法证明被立案的上级单位与下属单位及其分支机构之间存在实际控制关系的，对符合单位犯罪构成要件的下属单位或分支机构应当补充起诉，下属单位及其分支机构已不具备补充起诉条件的，可以将下属单位及其分支机构的涉案犯罪嫌疑人直接起诉。

四、综合运用定罪量刑情节

25　在办理跨区域涉互联网金融犯罪案件时，在追诉标准、追诉范围以及量刑建议等方面应当注意统一平衡。对于同一单位在多个地区分别设立分支机构的，在同一省（自治区、直辖市）范围内应当保持基本一致。分支机构所涉犯罪嫌疑人与上级单位主要犯罪嫌疑人之间应当保持适度平衡，防止出现责任轻重"倒挂"的现象。

26　单位犯罪中，直接负责的主管人员和其他直接责任人员在涉互联网金融犯罪案件中的地位、作用存在明显差别的，可以区分主犯和从犯。对起组织领导作用的总公司的直接负责的主管人员和发挥主要作用的其他直接责任人员，可以认定为全案的主犯，其他人员可以认定为从犯。

27　最大限度减少投资人的实际损失是办理涉互联网金融犯罪案件特别是非法集资案件的重要工作。在决定是否起诉、提出量刑建议时，要重视对是否具有认罪认罚、主动退赃退赔等情节的考察。分支机构涉案人员积极配合调查、主动退还违法所得、真诚认罪悔罪的，应当依法提出从轻、减轻处罚的量刑建议。其中，对情节轻微、可以免予刑事处罚的，或者

情节显著轻微、危害不大、不认为是犯罪的，应当依法作出不起诉决定。对被不起诉人需要给予行政处罚或者没收违法所得的，应当向行政主管部门提出检察意见。

五、证据的收集、审查与运用

28　涉互联网金融犯罪案件证据种类复杂、数量庞大、且分散于各地，收集、审查、运用证据的难度大。各地检察机关公诉部门要紧紧围绕证据的真实性、合法性、关联性，引导公安机关依法全面收集固定证据，加强证据的审查、运用，确保案件事实经得起法律的检验。

29　对于重大、疑难、复杂涉互联网金融犯罪案件，检察机关公诉部门要依法提前介入侦查，围绕指控犯罪的需要积极引导公安机关全面收集固定证据，必要时与公安机关共同会商，提出完善侦查思路、侦查提纲的意见建议。加强对侦查取证合法性的监督，对应当依法排除的非法证据坚决予以排除，对应当补正或作出合理解释的及时提出意见。

30　电子数据在涉互联网金融犯罪案件的证据体系中地位重要，对于指控证实相关犯罪事实具有重要作用。随着互联网技术的不断发展，电子数据的形式、载体出现了许多新的变化，对电子数据的勘验、提取、审查等提出了更高要求，处理不当会对电子数据的真实性、合法性造成不可逆转的损害。检察机关公诉部门要严格执行《最高人民法院、最高人民检察院、公安部关于办理刑事案件收集提取和审查判断电子数据问题的若干规定》〔法发〔2016〕22 号〕，加强对电子数据收集、提取程序和技术标准的审查，确保电子数据的真实性、合法性。对云存储电子数据等新类型电子数据进行提取、审查时，要高度重视程序合法性、数据完整性等问题，必要时主动征求相关领域专家意见，在提取前会同公安机关、云存储服务提供商制定科学合法的提取方案，确保万无一失。

31　落实"三统两分"要求，健全证据交换共享机制，协调推进跨区域案件办理。对涉及主案犯罪嫌疑人的证据，一般由主案侦办地办案机构负责收集，其他地区提供协助。其他地区办案机构需要主案侦办地提供证据材料的，应当向主案侦办地办案机构提出证据需求，由主案侦办地办案机构收集并依法移送。无法移送证据原件的，应当在移送复制件的同时，按照相关规定作出说明。各地检察机关公诉部门之间要加强协作，加强与公安机关的协调，督促本地公安机关与其他地区公安机关做好证据交换共享相关工作。案件进入审查起诉阶段后，检察机关公诉部门可以根据案件需要，直接向其他地区检察机关调取证据，其他地区检察机关公诉部门应积极协助。此外，各地检察机关在办理案件过程中发现对其他地区案件办理有重要作用的证据，应当及时采取措施并通知相应检察机关，做好依法移送工作。

六、投资人合法权益的保护

32　涉互联网金融犯罪案件投资人诉求复杂多样，矛盾化解和维护稳定工作任务艰巨繁重，各地检察机关公诉部门在办案过程中要坚持刑事追诉和权益保护并重，根据《刑事诉讼法》等相关法律规定，依法保证互联网金融活动中投资人的合法权益，坚持把追赃挽损等工作贯穿到侦查、起诉、审判各个环节，配合公安、法院等部门最大限度减少投资人的实际损失，加强与本院控申部门、公安机关的联系沟通，及时掌握涉案动态信息，认真开展办案风险评估预警工作，周密制定处置预案，并落实责任到位，避免因部门之间衔接不畅、处置不当造成工作被动。发现重大风险隐患的，及时向有关部门通报情况，必要时逐级上报高检院。

随着互联网金融的发展，涉互联网金融犯罪中的新情况、新问题还将不断出现，各地检察机关公诉部门要按照会议纪要的精神，结合各地办案实际，依法办理涉互联网金融犯罪案件；在办好案件的同时，要不断总结办案经验，加强对重大疑难复杂案件的研究，努力提高

办理涉互联网金融犯罪案件的能力和水平，为促进互联网金融规范发展、保障经济社会大局稳定作出积极贡献。在办案过程中遇到疑难问题的，要及时层报高检院公诉厅。

4.最高人民法院关于印发《全国法院审理金融犯罪案件工作座谈会纪要》的通知（法[2001]8号）

各省、自治区、直辖市高级人民法院，解放军军事法院，新疆维吾尔自治区高级人民法院生产建设兵团分院；全国地方各中级人民法院，各大单位军事法院，新疆生产建设兵团各中级法院：

现将《全国法院审理金融犯罪案件工作座谈会纪要》印发，供参照执行。执行中有什么问题，请及时报告我院。

2001 年 1 月 21 日

全国法院审理金融犯罪案件工作座谈会纪要

为进一步加强人民法院对金融犯罪案件的审判工作，正确理解和适用刑法对金融犯罪的有关规定，更加准确有力地依法打击各种金融犯罪，最高人民法院于 2000 年 9 月 20 日至 22 日在湖南省长沙市召开了全国法院审理金融犯罪案件工作座谈会。各省、自治区、直辖市高级人民法院和解放军军事法院主管刑事审判工作的副院长、刑事审判庭庭长以及中国人民银行的代表参加了座谈会。最高人民法院副院长刘家琛在座谈会上做了重要讲话。

座谈会总结交流了全国法院审理金融犯罪案件工作的情况和经验，研究讨论了刑法修订以来审理金融犯罪案件中遇到的有关具体适用法律的若干问题，对当前和今后一个时期人民法院审理金融犯罪案件工作提出了明确的要求和意见。纪要如下：

一

座谈会认为，金融是现代经济的核心。随着改革开放的不断深入和社会主义市场经济体制的建立、完善，我国金融体制也发生了重大变革，金融业务大大扩展且日益多元化、国际化，各种现代化的金融手段和信用工具被普遍应用，金融已经广泛深刻地介入我国经济并在其中发挥着越来越重要的作用，成为国民经济的“血液循环系统”，是市场资源配置关系的主要形式和国家宏观调控经济的重要手段。金融的安全、有序、高效、稳健运行，对于经济发展、国家安全以及社会稳定至关重要。如果金融不稳定，势必会危及经济和社会的稳定，影响改革和发展的进程。保持金融的稳定和安全，必须加强金融法制建设，依法强化金融监管，规范金融秩序，依法打击金融领域内的各种违法犯罪活动。

近年来，人民法院充分发挥刑事审判职能，依法严惩了一大批严重破坏金融管理秩序和金融诈骗的犯罪分子，为保障金融安全，防范和化解金融风险，发挥了重要作用。但是，金融犯罪的情况仍然是严重的。从法院受理案件的情况看，金融犯罪的数量在逐年增加；涉案金额越来越大；金融机构工作人员作案和内外勾结共同作案的现象突出；单位犯罪和跨国（境）、跨区域作案增多；犯罪手段趋向专业化、智能化，新类型犯罪不断出现；犯罪分子作案后大肆挥霍、转移赃款或携款外逃的情况时有发生，危害后果越来越严重。金融犯罪严重破坏社会主义市场经济秩序，扰乱金融管理秩序，危害国家信用制度，侵害公私财产权益，造成国家金融资产大量流失，有的地方还由此引发了局部性的金融风波和群体性事件，直接影响了社会稳定。必须清醒地看到，目前，我国经济体制中长期存在的一些矛盾和困难已经或正在向金融领域转移并积聚，从即将到来的新世纪开始，我国将进入加快推进现代化的新的发展阶段，随着经济的快速发展、改革的不断深化以及对外开放的进一步扩大，我国金融业在获得更大发展机遇的同时，也面临着维护金融稳定更加严峻的形势。依法打击各种金融犯罪是人民法院刑事审判工作一项长期的重要任务。

座谈会认为，人民法院审理金融犯罪案件工作过去虽已取得了很大成绩，但由于修订后的刑法增加了不少金融犯罪的新罪名，审判实践中遇到了大量新情况和新问题，如何进一步提高适用法律的水平，依法审理好不断增多的金融犯罪案件，仍然是各级法院面临的新的课题：各级法院特别是法院的领导，一定要进一步提高打击金融犯罪对于维护金融秩序、防范金融风险、确保国家金融安全，对于保障改革、促进发展和维护稳定重要意义的认识，把审理金融犯罪案件作为当前和今后很长时期内刑事审判工作的重点，切实加强领导和指导，提高审判业务水平，加大审判工作力度，以更好地适应改革开放和现代化建设的新形势对人民法院刑事审判工作的要求。为此，必须做好以下几方面的工作：

首先，金融犯罪是严重破坏社会主义市场经济秩序的犯罪，审理金融犯罪案件要继续贯彻依法从严惩处严重经济犯罪分子的方针。修订后的刑法和全国人大常委会的有关决定，对危害严重的金融犯罪规定了更加严厉的刑罚，体现了对金融犯罪从严惩处的精神，为人民法院审判各种金融犯罪案件提供了有力的法律依据。各级法院要坚决贯彻立法精神，严格依法惩处破坏金融管理秩序和金融诈骗的犯罪单位和犯罪个人。

第二，进一步加强审理金融犯罪案件工作，促进金融制度的健全与完善。各级法院要切实加强对金融犯罪案件审判工作的组织领导，调整充实审判力量，确保起诉到法院的破坏金融管理秩序和金融诈骗犯罪案件依法及时审结。对于针对金融机构的抢劫、盗窃和发生在金融领域的贪污、侵占、挪用、受贿等其他刑事犯罪案件，也要抓紧依法审理，及时宣判。对于各种专项斗争中破获的金融犯罪案件，要集中力量抓紧审理，依法从严惩处。可选择典型案件到案发当地和案发单位公开宣判，并通过各种新闻媒体广泛宣传，形成对金融违法犯罪的强大威慑力，教育广大干部群众增强金融法制观念，维护金融安全，促进金融制度的不断健全与完善。

第三，要加强学习培训，不断提高审判水平。审理金融犯罪案件，是一项政策性很强的工作，而且涉及很多金融方面的专业知识。各级法院要重视对刑事法官的业务学习和培训，采取请进来、走出去等灵活多样的形式，组织刑事审判人员认真学习银行法、证券法、票据法、保险法等金融法律和公司法、担保法、会计法、审计法等相关法律，学习有关金融政策法规以及一些基本业务知识，以确保正确理解和适用刑法，处理好金融犯罪案件。

第四，要结合审判工作加强调查研究。金融犯罪案件比较复杂，新情况、新问题多，审理难，度大，加强调查研究工作尤为必要。各级法院都要结合审理金融犯罪，有针对性地开展调查研究。对办案中发现的管理制度方面存在的漏洞和隐患，要及时提出司法建议。最高法院和高级法院要进一步加强对下级法院的工作指导，及时研究解决实践中遇到的适用法律上的新问题，需要通过制定司法解释加以明确的，要及时逐级报请最高法院研究。

二

座谈会重点研究讨论了人民法院审理金融犯罪案件中遇到的一些有关适用法律问题。与会同志认为，对于修订后的刑法实施过程中遇到的具体适用法律问题，在最高法院相应的新的司法解释出台前，原有司法解释与现行刑法不相冲突的仍然可以参照执行。对于法律和司法解释没有具体规定或规定不够明确，司法实践中又亟需解决的一些问题，与会同志结合审判实践进行了深入的探讨，并形成了一致意见：

（一）关于单位犯罪问题

根据刑法和《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》的规定，以单位名义实施犯罪，违法所得归单位所有的，是单位犯罪。

1．单位的分支机构或者内设机构、部门实施犯罪行为的处理。以单位的分支机构或者内设机构、部门的名义实施犯罪，违法所得亦归分支机构或者内设机构、部门所有的，应认定为单位犯罪。不能因为单位的分支机构或者内设机构、部门没有可供执行罚金的财产，就不将其认定为单位犯罪，而按照个人犯罪处理：

2．单位犯罪直接负责的主管人员和其他直接责任人员的认定：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。应当注意的是，在单位犯罪中，对于受单位领导指派或奉命而参与实施了一定犯罪行为的人员，一般不宜作为直接责任人员追究刑事责任。对单位犯罪中的直接负责的主管人员和其他直接责任人员，应根据其在单位犯罪中的地位、作用和犯罪情节，分别处以相应的刑罚，主管人员与直接责任人员，在个案中，不是当然的主、从犯关系，有的案件，主管人员与直接责任人员在实施犯罪行为的主从关系不明显的，可不分主、从犯。但具体案件可以分清主、从犯，且不分清主、从犯，在同一法定刑档次、幅度内量刑无法做到罪刑相适应的，应当分清主、从犯，依法处罚。

3．对未作为单位犯罪起诉的单位犯罪案件的处理。对于应当认定为单位犯罪的案件，检察机关只作为自然人犯罪案件起诉的，人民法院应及时与检察机关协商，建议检察机关对犯罪单位补充起诉。如检察机关不补充起诉的，人民法院仍应依法审理，对被起诉的自然人根据指控的犯罪事实、证据及庭审查明的事实，依法按单位犯罪中的直接负责的主管人员或者其他直接责任人员追究刑事责任，并应引用刑罚分则关于单位犯罪追究直接负责的主管人员和其他直接责任人员刑事责任的有关条款。

4．单位共同犯罪的处理。两个以上单位以共同故意实施的犯罪，应根据各单位在共同犯罪中的地位、作用大小，确定犯罪单位的主、从犯。

（二）关于破坏金融管理秩序罪

1．非金融机构非法从事金融活动案件的处理

1998 年 7 月 13 日，国务院发布了《非法金融机构和非法金融业务活动取缔办法》。1998 年 8 月 11 日，国务院办公厅转发了中国人民银行整顿乱集资、乱批设金融机构和乱办金融业务实施方案，对整顿金融“三乱”工作的政策措施等问题做出了规定。各地根据整顿金融“三乱”工作实施方案的规定，对于未经中国人民银行批准，但是根据地方政府或有关部门文件设立并从事或变相从事金融业务的各类基金会、互助会、储金会等机构和组织，由各地人民政府和各有关部门限期进行清理整顿。超过实施方案规定期限继续从事非法金融业务活动的，依法予以取缔；情节严重、构成犯罪的，依法追究刑事责任。因此，上述非法从事金融活动的机构和组织只要在实施方案规定期限之前停止非法金融业务活动的，对有关单位和责任人员，不应以擅自设立金融机构罪处理；对其以前从事的非法金融活动，一般也不作犯罪处理；这些机构和组织的人员利用职务实施的个人犯罪，如贪污罪、职务侵占罪、挪用公款罪、挪用资金罪等，应当根据具体案情分别依法定罪处罚。

2．关于假币犯罪

假币犯罪的认定。假币犯罪是一种严重破坏金融管理秩序的犯罪。只要有证据证明行为人实施了出售、购买、运输、使用假币行为，且数额较大，就构成犯罪。伪造货币的，只要实施了伪造行为，不论是否完成全部印制工序，即构成伪造货币罪；对于尚未制造出成品，无法计算伪造、销售假币面额的，或者制造、销售用于伪造货币的版样的，不认定犯罪数额，依据犯罪情节决定刑罚。明知是伪造的货币而持有，数额较大，根据现有证据不能认定行为人是为了进行其他假币犯罪的，以持有假币罪定罪处罚；如果有证据证明其持有的假币已构成其他假币犯罪的，应当以其他假币犯罪定罪处罚。

假币犯罪罪名的确定。假币犯罪案件中犯罪分子实施数个相关行为的，在确定罪名时应把握以下原则：

（1）对同一宗假币实施了法律规定为选择性罪名的行为，应根据行为人所实施的数个

行为，按相关罪名刑法规定的排列顺序并列确定罪名，数额不累计计算，不实行数罪并罚：

（2）对不同宗假币实施法律规定为选择性罪名的行为，并列确定罪名，数额按全部假币面额累计计算，不实行数罪并罚。

（3）对同一宗假币实施了刑法没有规定为选择性罪名的数个犯罪行为，择一重罪从重处罚。如伪造货币或者购买假币后使用的，以伪造货币罪或购买假币罪定罪，从重处罚。

（4）对不同宗假币实施了刑法没有规定为选择性罪名的数个犯罪行为，分别定罪，数罪并罚。

出售假币被查获部分的处理。在出售假币时被抓获的，除现场查获的假币应认定为出售假币的犯罪数额外，现场之外在行为人住所或者其他藏匿地查获的假币，亦应认定为出售假币的犯罪数额。但有证据证实后者是行为人有实施其他假币犯罪的除外。

制造或者出售伪造的台币行为的处理。对于伪造台币的，应当以伪造货币罪定罪处罚；出售伪造的台币的，应当以出售假币罪定罪处罚。

3．用账外客户资金非法拆借、发放贷款行为的认定和处罚

银行或者其他金融机构及其工作人员以牟利为目的，采取吸收客户资金不入账的方式，将客户资金用于非法拆借、发放贷款，造成重大损失的，构成用账外客户资金非法拆借、发放贷款罪。以牟利为目的，是指金融机构及其工作人员为本单位或者个人牟利，不具有这种目的，不构成该罪。这里的“牟利”，一般是指谋取用账外客户资金非法拆借、发放贷款所产生的非法收益，如利息、差价等。对于用款人为取得贷款而支付的回扣、手续费等，应根据具体情况分别处理：银行或者其他金融机构用账外客户资金非法拆借、发放贷款，收取的回扣、手续费等，应认定为“牟利”；银行或者其他金融机构的工作人员利用职务上的便利，用账外客户资金非法拆借、发放贷款，收取回扣、手续费等，数额较小的，以“牟利”论处；银行或者其他金融机构的工作人员将用款人支付给单位的回扣、手续费秘密占为己有，数额较大的，以贪污罪定罪处罚；银行或者其他金融机构的工作人员利用职务便利，用账外客户资金非法拆借、发放贷款，索取用款人的财物，或者非法收受其他财物，或者收取回扣、手续费等，数额较大的，以受贿罪定罪处罚。吸收客户资金不入账，是指不记入金融机构的法定存款账目，以逃避国家金融监管，至于是否记入法定账目以外设立的账目，不影响该罪成立。

审理银行或者其他金融机构及其工作人员用账外客户资金非法拆借、发放贷款案件，要注意将用账外客户资金非法拆借、发放贷款的行为与挪用公款罪和挪用资金罪区别开来。对于利用职务上的便利，挪用已经记入金融机构法定存款账户的客户资金归个人使用的，或者吸收客户资金不入账，却给客户开具银行存单，客户也认为将款已存入银行，该款却被行为人以个人名义借贷给他人的，均应认定为挪用公款罪或者挪用资金罪。

4．破坏金融管理秩序相关犯罪数额和情节的认定

最高人民法院先后颁行了《关于审理伪造货币等案件具体应用法律若干问题的解释》、《关于审理走私刑事案件具体应用法律若干问题的解释），对伪造货币，走私、出售、购买、运输假币等犯罪的定罪处刑标准以及相关适用法律问题作出了明确规定。为正确执行刑法，在其他有关的司法解释出台之前，对假币犯罪以外的破坏金融管理秩序犯罪的数额和情节，可参照以下标准掌握：

关于非法吸收公众存款罪。非法吸收或者变相吸收公众存款的，要从非法吸收公众存款的数额、范围以及给存款人造成的损失等方面来判定扰乱金融秩序造成危害的程度。根据司法实践，具有下列情形之一的，可以按非法吸收公众存款罪定罪处罚：

（1）个人非法吸收或者变相吸收公众存款 20 万元以上的，单位非法吸收或者变相吸收公众存款 100 万元以上的；

（2）个人非法吸收或者变相吸收公众存款 30 户以上的，单位非法吸收或者变相吸收公

众存款150户以上的；

（3）个人非法吸收或者变相吸收公众存款给存款人造成损失10万元以上的，单位非法吸收或者变相吸收公众存款给存款人造成损失50万元以上的，或者造成其他严重后果的：个人非法吸收或者变相吸收公众存款100万元以上，单位非法吸收或者变相吸收公众存款500万元以上的，可以认定为“数额巨大”。

关于违法向关系人发放贷款罪。银行或者其他金融机构工作人员违反法律、行政法规规定，向关系人发放信用贷款或者发放担保贷款的条件优于其他借款人同类贷款条件，造成10—30万元以上损失的，可以认定为“造成较大损失”；造成50—100万元以上损失的，可以认定为“造成重大损失”。

关于违法发放贷款罪。银行或者其他金融机构工作人员违反法律、行政法规规定，向关系人以外的其他人发放贷款，造成50—100万元以上损失的，可以认定为“造成重大损失”；造成300—500万元以上损失的，可以认定为“造成特别重大损失”。

关于用账外客户资金非法拆借、发放贷款罪。对于银行或者其他金融机构工作人员以牟利为目的，采取吸收客户资金不入账的方式，将资金用于非法拆借、发放贷款，造成50—100万元以上损失的，可以认定为“造成重大损失．”；造成300—500万元以上损失的，可以认定为“造成特别重大损失”。

对于单位实施违法发放贷款和用账外客户资金非法拆借、发放贷款造成损失构成犯罪的数额标准，可按个人实施上述犯罪的数额标准二至四倍掌握。

由于各地经济发展不平衡，各省、自治区、直辖市高级人民法院可参照上述数额标准或幅度，根据本地的具体情况，确定在本地区掌握的具体标准。

（三）关于金融诈骗罪

1．金融诈骗罪中非法占有目的的认定

金融诈骗犯罪都是以非法占有为目的的犯罪。在司法实践中，认定是否具有非法占有为目的，应当坚持主客观相一致的原则，既要避免单纯根据损失结果客观归罪，也不能仅凭被告人自己的供述，而应当根据案件具体情况具体分析。根据司法实践，对于行为人通过诈骗的方法非法获取资金，造成数额较大资金不能归还，并具有下列情形之一的，可以认定为具有非法占有的目的：

（1）明知没有归还能力而大量骗取资金的；

（2）非法获取资金后逃跑的；

（3）肆意挥霍骗取资金的；

（4）使用骗取的资金进行违法犯罪活动的；

（5）抽逃、转移资金、隐匿财产，以逃避返还资金的；

（6）隐匿、销毁账目，或者搞假破产、假倒闭，以逃避返还资金的；

（7）其他非法占有资金、拒不返还的行为。但是，在处理具体案件的时候，对于有证据证明行为人不具有非法占有目的的，不能单纯以财产不能归还就按金融诈骗罪处罚。

2．贷款诈骗罪的认定和处理。贷款诈骗犯罪是目前案发较多的金融诈骗犯罪之一。审理贷款诈骗犯罪案件，应当注意以下两个问题：

一是单位不能构成贷款诈骗罪。根据刑法第三十条和第一百九十三条的规定，单位不构成贷款诈骗罪。对于单位实施的贷款诈骗行为，不能以贷款诈骗罪定罪处罚，也不能以贷款诈骗罪追究直接负责的主管人员和其他直接责任人员的刑事责任。但是，在司法实践中，对于单位十分明显地以非法占有为目的，利用签订、履行借款合同诈骗银行或其他金融机构贷款，符合刑法第二百二十四条规定的合同诈骗罪构成要件的，应当以合同诈骗罪定罪处罚。

二是要严格区分贷款诈骗与贷款纠纷的界限。对于合法取得贷款后，没有按规定的用途

使用贷款，到期没有归还贷款的，不能以贷款诈骗罪定罪处罚；对于确有证据证明行为人不具有非法占有的目的，因不具备贷款的条件而采取了欺骗手段获取贷款，案发时有能力履行还贷义务，或者案发时不能归还贷款是因为意志以外的原因，如因经营不善、被骗、市场风险等，不应以贷款诈骗罪定罪处罚。

3．集资诈骗罪的认定和处理：集资诈骗罪和欺诈发行股票、债券罪、非法吸收公众存款罪在客观上均表现为向社会公众非法募集资金。区别的关键在于行为人是否具有非法占有的目的。对于以非法占有为目的而非法集资，或者在非法集资过程中产生了非法占有他人资金的故意，均构成集资诈骗罪。但是，在处理具体案件时要注意以下两点：一是不能仅凭较大数额的非法集资款不能返还的结果，推定行为人具有非法占有的目的；二是行为人将大部分资金用于投资或生产经营活动，而将少量资金用于个人消费或挥霍的，不应仅以此便认定具有非法占有的目的。

4．金融诈骗犯罪定罪量刑的数额标准和犯罪数额的计算。金融诈骗的数额不仅是定罪的重要标准，也是量刑的主要依据。在没有新的司法解释之前，可参照 1996 年《最高人民法院关于审理诈骗案件具体应用法律的若干问题的解释》的规定执行。在具体认定金融诈骗犯罪的数额时，应当以行为人实际骗取的数额计算。对于行为人为实施金融诈骗活动而支付的中介费、手续费、回扣等，或者用于行贿、赠与等费用，均应计入金融诈骗的犯罪数额。但应当将案发前已归还的数额扣除。

（四）死刑的适用

刑法对危害特别严重的金融诈骗犯罪规定了死刑。人民法院应当运用这一法律武器，有力地打击金融诈骗犯罪。对于罪行极其严重、依法该判死刑的犯罪分子，一定要坚决判处死刑。但需要强调的是，金融诈骗犯罪的数额特别巨大不是判处死刑的惟一标准，只有诈骗“数额特别巨大并且给国家和人民利益造成特别重大损失”的犯罪分子，才能依法选择适用死刑。对于犯罪数额特别巨大，但追缴、退赔后，挽回了损失或者损失不大的，一般不应当判处死刑立即执行；对具有法定从轻、减轻处罚情节的，一般不应当判处死刑。

（五）财产刑的适用

金融犯罪是图利型犯罪，惩罚和预防此类犯罪，应当注重同时从经济上制裁犯罪分子。刑法对金融犯罪都规定了财产刑，人民法院应当严格依法判处。罚金的数额，应当根据被告人的犯罪情节，在法律规定的数额幅度内确定。对于具有从轻、减轻或者免除处罚情节的被告人，对于本应并处的罚金刑原则上也应当从轻、减轻或者免除。

单位金融犯罪中直接负责的主管人员和其他直接责任人员，是否适用罚金刑，应当根据刑法的具体规定。刑法分则条文规定有罚金刑，并规定对单位犯罪中直接负责的主管人员和其他直接责任人员依照自然人犯罪条款处罚的，应当判处罚金刑，但是对直接负责的主管人员和其他直接责任人员判处罚金的数额，应当低于对单位判处罚金的数额；刑法分则条文明确规定对单位犯罪中直接负责的主管人员和其他直接责任人员只判处自由刑的，不能附加判处罚金刑。

5.《最高人民法院、最高人民检察院、公安部关于办理侵犯知识产权刑事案件适用法律若干问题的意见》（法发[2011]3 号）

十、关于侵犯著作权犯罪案件“以营利为目的”的认定问题

除销售外，具有下列情形之一的，可以认定为“以营利为目的”：

（一）以在他人作品中刊登收费广告、捆绑第三方作品等方式直接或者间接收取费用的；

（二）通过信息网络传播他人作品，或者利用他人上传的侵权作品，在网站或者网页上

提供刊登收费广告服务，直接或者间接收取费用的；

（三）以会员制方式通过信息网络传播他人作品，收取会员注册费或者其他费用的；

（四）其他利用他人作品牟利的情形。

十二、关于刑法第二百一十七条规定的“发行”的认定及相关问题

“发行”，包括总发行、批发、零售、通过信息网络传播以及出租、展销等活动。

非法出版、复制、发行他人作品，侵犯著作权构成犯罪的，按照侵犯著作权罪定罪处罚，不认定为非法经营罪等其他犯罪。

十三、关于通过信息网络传播侵权作品行为的定罪处罚标准问题

以营利为目的，未经著作权人许可，通过信息网络向公众传播他人文字作品、音乐、电影、电视、美术、摄影、录像作品、录音录像制品、计算机软件及其他作品，具有下列情形之一的，属于刑法第二百一十七条规定的“其他严重情节”：

（一）非法经营数额在五万元以上的；

（二）传播他人作品的数量合计在五百件（部）以上的；

（三）传播他人作品的实际被点击数达到五万次以上的；

（四）以会员制方式传播他人作品，注册会员达到一千人以上的；

（五）数额或者数量虽未达到第（一）项至第（四）项规定标准，但分别达到其中两项以上标准一半以上的；

（六）其他严重情节的情形。

实施前款规定的行为，数额或者数量达到前款第（一）项至第（五）项规定标准五倍以上的，属于刑法第二百一十七条规定的“其他特别严重情节”。

十五、关于为他人实施侵犯知识产权犯罪提供原材料、机械设备等行为的定性问题

明知他人实施侵犯知识产权犯罪，而为其提供生产、制造侵权产品的主要原材料、辅助材料、半成品、包装材料、机械设备、标签标识、生产技术、配方等帮助，或者提供互联网接入、服务器托管、网络存储空间、通讯传输通道、代收费、费用结算等服务的，以侵犯知识产权犯罪的共犯论处。

6.《最高人民法院、最高人民检察院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》

为保护公民、法人和其他组织的合法权益，维护社会秩序，根据《中华人民共和国刑法》《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》等规定，对办理利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等刑事案件适用法律的若干问题解释如下:

第一条 具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“捏造事实诽谤他人”:

(一)捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的;

(二)将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实,在信息网络上散布，或者组织、指使人员在信息网络上散布的;

明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的，以“捏造事实诽谤他人”论。

第二条 利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“情节严重”:

(一)同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的;

(二)造成被害人或者其近亲属精神失常、自残、自杀等严重后果的;

(三)二年内曾因诽谤受过行政处罚，又诽谤他人的;

(四)其他情节严重的情形。

第三条 利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第二款规定的“严重危害社会秩序和国家利益”:

(一)引发群体性事件的;

(二)引发公共秩序混乱的;

(三)引发民族、宗教冲突的;

(四)诽谤多人，造成恶劣社会影响的;

(五)损害国家形象，严重危害国家利益的;

(六)造成恶劣国际影响的;

(七)其他严重危害社会秩序和国家利益的情形。

第四条 一年内多次实施利用信息网络诽谤他人行为未经处理，诽谤信息实际被点击、浏览、转发次数累计计算构成犯罪的，应当依法定罪处罚。

第五条 利用信息网络辱骂、恐吓他人，情节恶劣，破坏社会秩序的，依照刑法第二百九十三条第一款第(二)项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第(四)项的规定，以寻衅滋事罪定罪处罚。

第六条 以在信息网络上发布、删除等方式处理网络信息为由，威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

第七条 违反国家规定，以营利为目的，通过信息网络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，扰乱市场秩序，具有下列情形之一的，属于非法经营行为“情节严重”，依照刑法第二百二十五条第(四)项的规定，以非法经营罪定罪处罚:

(一)个人非法经营数额在五万元以上，或者违法所得数额在二万元以上的;

(二)单位非法经营数额在十五万元以上，或者违法所得数额在五万元以上的。

实施前款规定的行为，数额达到前款规定的数额五倍以上的，应当认定为刑法第二百二十五条规定的“情节特别严重”。

第八条 明知他人利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪，为其提供资金、场所、技术支持等帮助的，以共同犯罪论处。

第九条 利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营犯罪，同时又构成刑法第二百二十一条规定的损害商业信誉、商品声誉罪，第二百七十八条规定的煽动暴力抗拒法律实施罪，第二百九十一条之一规定的编造、故意传播虚假恐怖信息罪等犯罪的，依照处罚较重的规定定罪处罚。

第十条 本解释所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

7.《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）

第三条 向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的“提供公民个人信息”。

未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三

条之一规定的“提供公民个人信息”，但是经过处理无法识别特定个人且不能复原的除外。

8.《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》 （法发[2016]32号 2016年12月20日实施）

为依法惩治电信网络诈骗等犯罪活动，保护公民、法人和其他组织的合法权益，维护社会秩序，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》等法律和有关司法解释的规定，结合工作实际，制定本意见。

一、总体要求

近年来，利用通讯工具、互联网等技术手段实施的电信网络诈骗犯罪活动持续高发，侵犯公民个人信息，扰乱无线电通讯管理秩序，掩饰、隐瞒犯罪所得、犯罪所得收益等上下游关联犯罪不断蔓延。此类犯罪严重侵害人民群众财产安全和其他合法权益，严重干扰电信网络秩序，严重破坏社会诚信，严重影响人民群众安全感和社会和谐稳定，社会危害性大，人民群众反映强烈。

人民法院、人民检察院、公安机关要针对电信网络诈骗等犯罪的特点，坚持全链条全方位打击，坚持依法从严从快惩处，坚持最大力度最大限度追赃挽损，进一步健全工作机制，加强协作配合，坚决有效遏制电信网络诈骗等犯罪活动，努力实现法律效果和社会效果的高度统一。

二、依法严惩电信网络诈骗犯罪

（一）根据《最高人民法院、最高人民检察院关于办理诈骗刑事案件具体应用法律若干问题的解释》第一条的规定，利用电信网络技术手段实施诈骗，诈骗公私财物价值三千元以上、三万元以上、五十万元以上的，应当分别认定为刑法第二百六十六条规定的“数额较大”“数额巨大”“数额特别巨大”。

二年内多次实施电信网络诈骗未经处理，诈骗数额累计计算构成犯罪的，应当依法定罪处罚。

（二）实施电信网络诈骗犯罪，达到相应数额标准，具有下列情形之一的，酌情从重处罚：

1．造成被害人或其近亲属自杀、死亡或者精神失常等严重后果的；

2．冒充司法机关等国家机关工作人员实施诈骗的；

3．组织、指挥电信网络诈骗犯罪团伙的；

4．在境外实施电信网络诈骗的；

5.曾因电信网络诈骗犯罪受过刑事处罚或者二年内曾因电信网络诈骗受过行政处罚的；

6．诈骗残疾人、老年人、未成年人、在校学生、丧失劳动能力人的财物，或者诈骗重病患者及其亲属财物的；

7．诈骗救灾、抢险、防汛、优抚、扶贫、移民、救济、医疗等款物的；

8．以赈灾、募捐等社会公益、慈善名义实施诈骗的；

9．利用电话追呼系统等技术手段严重干扰公安机关等部门工作的；

10．利用“钓鱼网站”链接、“木马”程序链接、网络渗透等隐蔽技术手段实施诈骗的。

（三）实施电信网络诈骗犯罪，诈骗数额接近“数额巨大”“数额特别巨大”的标准，具有前述第（二）条规定的情形之一的，应当分别认定为刑法第二百六十六条规定的“其他严重情节”“其他特别严重情节”。

上述规定的“接近”，一般应掌握在相应数额标准的百分之八十以上。

（四）实施电信网络诈骗犯罪，犯罪嫌疑人、被告人实际骗得财物的，以诈骗罪（既遂）

定罪处罚。诈骗数额难以查证，但具有下列情形之一的，应当认定为刑法第二百六十六条规定的“其他严重情节”，以诈骗罪（未遂）定罪处罚：

1．发送诈骗信息五千条以上的，或者拨打诈骗电话五百人次以上的；

2．在互联网上发布诈骗信息，页面浏览量累计五千次以上的。

具有上述情形，数量达到相应标准十倍以上的，应当认定为刑法第二百六十六条规定的“其他特别严重情节”，以诈骗罪（未遂）定罪处罚。

上述“拨打诈骗电话”，包括拨出诈骗电话和接听被害人回拨电话。反复拨打、接听同一电话号码，以及反复向同一被害人发送诈骗信息的，拨打、接听电话次数、发送信息条数累计计算。

因犯罪嫌疑人、被告人故意隐匿、毁灭证据等原因，致拨打电话次数、发送信息条数的证据难以收集的，可以根据经查证属实的日拨打人次数、日发送信息条数，结合犯罪嫌疑人、被告人实施犯罪的时间、犯罪嫌疑人、被告人的供述等相关证据，综合予以认定。

（五）电信网络诈骗既有既遂，又有未遂，分别达到不同量刑幅度的，依照处罚较重的规定处罚；达到同一量刑幅度的，以诈骗罪既遂处罚。

（六）对实施电信网络诈骗犯罪的被告人裁量刑罚，在确定量刑起点、基准刑时，一般应就高选择。确定宣告刑时，应当综合全案事实情节，准确把握从重、从轻量刑情节的调节幅度，保证罪责刑相适应。

（七）对实施电信网络诈骗犯罪的被告人，应当严格控制适用缓刑的范围，严格掌握适用缓刑的条件。

（八）对实施电信网络诈骗犯罪的被告人，应当更加注重依法适用财产刑，加大经济上的惩罚力度，最大限度剥夺被告人再犯的能力。

三、全面惩处关联犯罪

（一）在实施电信网络诈骗活动中，非法使用“伪基站”“黑广播”，干扰无线电通讯秩序，符合刑法第二百八十八条规定的，以扰乱无线电通讯管理秩序罪追究刑事责任。同时构成诈骗罪的，依照处罚较重的规定定罪处罚。

（二）违反国家有关规定，向他人出售或者提供公民个人信息，窃取或者以其他方法非法获取公民个人信息，符合刑法第二百五十三条之一规定的，以侵犯公民个人信息罪追究刑事责任。

使用非法获取的公民个人信息，实施电信网络诈骗犯罪行为，构成数罪的，应当依法予以并罚。

（三）冒充国家机关工作人员实施电信网络诈骗犯罪，同时构成诈骗罪和招摇撞骗罪的，依照处罚较重的规定定罪处罚。

（四）非法持有他人信用卡，没有证据证明从事电信网络诈骗犯罪活动，符合刑法第一百七十七条之一第一款第（二）项规定的，以妨害信用卡管理罪追究刑事责任。

（五）明知是电信网络诈骗犯罪所得及其产生的收益，以下列方式之一予以转账、套现、取现的，依照刑法第三百一十二条第一款的规定，以掩饰、隐瞒犯罪所得、犯罪所得收益罪追究刑事责任。但有证据证明确实不知道的除外：

1．通过使用销售点终端机具（POS 机）刷卡套现等非法途径，协助转换或者转移财物的；

2．帮助他人将巨额现金散存于多个银行账户，或在不同银行账户之间频繁划转的；

3．多次使用或者使用多个非本人身份证明开设的信用卡、资金支付结算账户或者多次采用遮蔽摄像头、伪装等异常手段，帮助他人转账、套现、取现的；

4．为他人提供非本人身份证明开设的信用卡、资金支付结算账户后，又帮助他人转账、

套现、取现的；

5．以明显异于市场的价格，通过手机充值、交易游戏点卡等方式套现的。

实施上述行为，事前通谋的，以共同犯罪论处。

实施上述行为，电信网络诈骗犯罪嫌疑人尚未到案或案件尚未依法裁判，但现有证据足以证明该犯罪行为确实存在的，不影响掩饰、隐瞒犯罪所得、犯罪所得收益罪的认定。

实施上述行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。法律和司法解释另有规定的除外。

（六）网络服务提供者不履行法律、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，致使诈骗信息大量传播，或者用户信息泄露造成严重后果的，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追究刑事责任。同时构成诈骗罪的，依照处罚较重的规定定罪处罚。

（七）实施刑法第二百八十七条之一、第二百八十七条之二规定之行为，构成非法利用信息网络罪、帮助信息网络犯罪活动罪，同时构成诈骗罪的，依照处罚较重的规定定罪处罚。

（八）金融机构、网络服务提供者、电信业务经营者等在经营活动中，违反国家有关规定，被电信网络诈骗犯罪分子利用，使他人遭受财产损失的，依法承担相应责任。构成犯罪的，依法追究刑事责任。

四、准确认定共同犯罪与主观故意

（一）三人以上为实施电信网络诈骗犯罪而组成的较为固定的犯罪组织，应依法认定为诈骗犯罪集团。对组织、领导犯罪集团的首要分子，按照集团所犯的全部罪行处罚。对犯罪集团中组织、指挥、策划者和骨干分子依法从严惩处。

对犯罪集团中起次要、辅助作用的从犯，特别是在规定期限内投案自首、积极协助抓获主犯、积极协助追赃的，依法从轻或减轻处罚。

对犯罪集团首要分子以外的主犯，应当按照其所参与的或者组织、指挥的全部犯罪处罚。全部犯罪包括能够查明具体诈骗数额的事实和能够查明发送诈骗信息条数、拨打诈骗电话人次数、诈骗信息网页浏览次数的事实。

（二）多人共同实施电信网络诈骗，犯罪嫌疑人、被告人应对其参与期间该诈骗团伙实施的全部诈骗行为承担责任。在其所参与的犯罪环节中起主要作用的，可以认定为主犯；起次要作用的，可以认定为从犯。

上述规定的“参与期间”，从犯罪嫌疑人、被告人着手实施诈骗行为开始起算。

（三）明知他人实施电信网络诈骗犯罪，具有下列情形之一的，以共同犯罪论处，但法律和司法解释另有规定的除外：

1．提供信用卡、资金支付结算账户、手机卡、通讯工具的；

2．非法获取、出售、提供公民个人信息的；

3．制作、销售、提供“木马”程序和“钓鱼软件”等恶意程序的；

4．提供“伪基站”设备或相关服务的；

5．提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供支付结算等帮助的；

6．在提供改号软件、通话线路等技术服务时，发现主叫号码被修改为国内党政机关、司法机关、公共服务部门号码，或者境外用户改为境内号码，仍提供服务的；

7．提供资金、场所、交通、生活保障等帮助的；

8．帮助转移诈骗犯罪所得及其产生的收益，套现、取现的。

上述规定的“明知他人实施电信网络诈骗犯罪”，应当结合被告人的认知能力，既往经历，行为次数和手段，与他人关系，获利情况，是否曾因电信网络诈骗受过处罚，是否故意

规避调查等主客观因素进行综合分析认定。

（四）负责招募他人实施电信网络诈骗犯罪活动，或者制作、提供诈骗方案、术语清单、语音包、信息等的，以诈骗共同犯罪论处。

（五）部分犯罪嫌疑人在逃，但不影响对已到案共同犯罪嫌疑人、被告人的犯罪事实认定的，可以依法先行追究已到案共同犯罪嫌疑人、被告人的刑事责任。

五、依法确定案件管辖

（一）电信网络诈骗犯罪案件一般由犯罪地公安机关立案侦查，如果由犯罪嫌疑人居住地公安机关立案侦查更为适宜的，可以由犯罪嫌疑人居住地公安机关立案侦查。犯罪地包括犯罪行为发生地和犯罪结果发生地。

“犯罪行为发生地”包括用于电信网络诈骗犯罪的网站服务器所在地，网站建立者、管理者所在地，被侵害的计算机信息系统或其管理者所在地，犯罪嫌疑人、被害人使用的计算机信息系统所在地，诈骗电话、短信息、电子邮件等的拨打地、发送地、到达地、接受地，以及诈骗行为持续发生的实施地、预备地、开始地、途经地、结束地。

“犯罪结果发生地”包括被害人被骗时所在地，以及诈骗所得财物的实际取得地、藏匿地、转移地、使用地、销售地等。

（二）电信网络诈骗最初发现地公安机关侦办的案件，诈骗数额当时未达到“数额较大”标准，但后续累计达到“数额较大”标准，可由最初发现地公安机关立案侦查。

（三）具有下列情形之一的，有关公安机关可以在其职责范围内并案侦查：

1．一人犯数罪的；

2．共同犯罪的；

3．共同犯罪的犯罪嫌疑人还实施其他犯罪的；

4．多个犯罪嫌疑人实施的犯罪存在直接关联，并案处理有利于查明案件事实的。

（四）对因网络交易、技术支持、资金支付结算等关系形成多层级链条、跨区域的电信网络诈骗等犯罪案件，可由共同上级公安机关按照有利于查清犯罪事实、有利于诉讼的原则，指定有关公安机关立案侦查。

（五）多个公安机关都有权立案侦查的电信网络诈骗等犯罪案件，由最初受理的公安机关或者主要犯罪地公安机关立案侦查。有争议的，按照有利于查清犯罪事实、有利于诉讼的原则，协商解决。经协商无法达成一致的，由共同上级公安机关指定有关公安机关立案侦查。

（六）在境外实施的电信网络诈骗等犯罪案件，可由公安部按照有利于查清犯罪事实、有利于诉讼的原则，指定有关公安机关立案侦查。

（七）公安机关立案、并案侦查，或因有争议，由共同上级公安机关指定立案侦查的案件，需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的人民检察院、人民法院受理。

对重大疑难复杂案件和境外案件，公安机关应在指定立案侦查前，向同级人民检察院、人民法院通报。

（八）已确定管辖的电信诈骗共同犯罪案件，在逃的犯罪嫌疑人归案后，一般由原管辖的公安机关、人民检察院、人民法院管辖。

六、证据的收集和审查判断

（一）办理电信网络诈骗案件，确因被害人人数众多等客观条件的限制，无法逐一收集被害人陈述的，可以结合已收集的被害人陈述，以及经查证属实的银行账户交易记录、第三方支付结算账户交易记录、通话记录、电子数据等证据，综合认定被害人人数及诈骗资金数额等犯罪事实。

（二）公安机关采取技术侦查措施收集的案件证明材料，作为证据使用的，应当随案移送批准采取技术侦查措施的法律文书和所收集的证据材料，并对其来源等作出书面说明。

（三）依照国际条约、刑事司法协助、互助协议或平等互助原则，请求证据材料所在地司法机关收集，或通过国际警务合作机制、国际刑警组织启动合作取证程序收集的境外证据材料，经查证属实，可以作为定案的依据。公安机关应对其来源、提取人、提取时间或者提供人、提供时间以及保管移交的过程等作出说明。

对其他来自境外的证据材料，应当对其来源、提供人、提供时间以及提取人、提取时间进行审查。能够证明案件事实且符合刑事诉讼法规定的，可以作为证据使用。

七、涉案财物的处理

（一）公安机关侦办电信网络诈骗案件，应当随案移送涉案赃款赃物，并附清单。人民检察院提起公诉时，应一并移交受理案件的人民法院，同时就涉案赃款赃物的处理提出意见。

（二）涉案银行账户或者涉案第三方支付账户内的款项，对权属明确的被害人的合法财产，应当及时返还。确因客观原因无法查实全部被害人，但有证据证明该账户系用于电信网络诈骗犯罪，且被告人无法说明款项合法来源的，根据刑法第六十四条的规定，应认定为违法所得，予以追缴。

（三）被告人已将诈骗财物用于清偿债务或者转让给他人，具有下列情形之一的，应当依法追缴：

1．对方明知是诈骗财物而收取的；

2．对方无偿取得诈骗财物的；

3．对方以明显低于市场的价格取得诈骗财物的；

4．对方取得诈骗财物系源于非法债务或者违法犯罪活动的。

他人善意取得诈骗财物的，不予追缴。

最高人民法院
最高人民检察院
公安部
2016 年 12 月 19 日

9.《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》　（法发〔2021〕22 号　2021 年 6 月 17 日起实施）

为进一步依法严厉惩治电信网络诈骗犯罪，对其上下游关联犯罪实行全链条、全方位打击，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》等法律和有关司法解释的规定，针对司法实践中出现的新的突出问题，结合工作实际，制定本意见。

一、电信网络诈骗犯罪地，除《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》规定的犯罪行为发生地和结果发生地外，还包括：

（一）用于犯罪活动的手机卡、流量卡、物联网卡的开立地、销售地、转移地、藏匿地；

（二）用于犯罪活动的信用卡的开立地、销售地、转移地、藏匿地、使用地以及资金交易对手资金交付和汇出地；

（三）用于犯罪活动的银行账户、非银行支付账户的开立地、销售地、使用地以及资金交易对手资金交付和汇出地；

（四）用于犯罪活动的即时通讯信息、广告推广信息的发送地、接受地、到达地；

（五）用于犯罪活动的“猫池”（Modem Pool）、GOIP 设备、多卡宝等硬件设备的销售地、入网地、藏匿地；

（六）用于犯罪活动的互联网账号的销售地、登录地。

二、为电信网络诈骗犯罪提供作案工具、技术支持等帮助以及掩饰、隐瞒犯罪所得及其产生的收益，由此形成多层级犯罪链条的，或者利用同一网站、通讯群组、资金账户、作案窝点实施电信网络诈骗犯罪的，应当认定为多个犯罪嫌疑人、被告人实施的犯罪存在关联，人民法院、人民检察院、公安机关可以在其职责范围内并案处理。

三、有证据证实行为人参加境外诈骗犯罪集团或犯罪团伙，在境外针对境内居民实施电信网络诈骗犯罪行为，诈骗数额难以查证，但一年内出境赴境外诈骗犯罪窝点累计时间 30 日以上或多次出境赴境外诈骗犯罪窝点的，应当认定为刑法第二百六十六条规定的“其他严重情节”，以诈骗罪依法追究刑事责任。有证据证明其出境从事正当活动的除外。

四、无正当理由持有他人的单位结算卡的，属于刑法第一百七十七条之一第一款第（二）项规定的“非法持有他人信用卡”。

五、非法获取、出售、提供具有信息发布、即时通讯、支付结算等功能的互联网账号密码、个人生物识别信息，符合刑法第二百五十三条之一规定的，以侵犯公民个人信息罪追究刑事责任。

对批量前述互联网账号密码、个人生物识别信息的条数，根据查获的数量直接认定，但有证据证明信息不真实或者重复的除外。

六、在网上注册办理手机卡、信用卡、银行账户、非银行支付账户时，为通过网上认证，使用他人身份证件信息并替换他人身份证件相片，属于伪造身份证件行为，符合刑法第二百八十条第三款规定的，以伪造身份证件罪追究刑事责任。

使用伪造、变造的身份证件或者盗用他人身份证件办理手机卡、信用卡、银行账户、非银行支付账户，符合刑法第二百八十条之一第一款规定的，以使用虚假身份证件、盗用身份证件罪追究刑事责任。

实施上述两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。法律和司法解释另有规定的除外。

七、为他人利用信息网络实施犯罪而实施下列行为，可以认定为刑法第二百八十七条之二规定的“帮助”行为：

（一）收购、出售、出租信用卡、银行账户、非银行支付账户、具有支付结算功能的互联网账号密码、网络支付接口、网上银行数字证书的；

（二）收购、出售、出租他人手机卡、流量卡、物联网卡的。

八、认定刑法第二百八十七条之二规定的行为人明知他人利用信息网络实施犯罪，应当根据行为人收购、出售、出租前述第七条规定的信用卡、银行账户、非银行支付账户、具有支付结算功能的互联网账号密码、网络支付接口、网上银行数字证书，或者他人手机卡、流量卡、物联网卡等的次数、张数、个数，并结合行为人的认知能力、既往经历、交易对象、与实施信息网络犯罪的行为人的关系、提供技术支持或者帮助的时间和方式、获利情况以及行为人的供述等主客观因素，予以综合认定。

收购、出售、出租单位银行结算账户、非银行支付机构单位支付账户，或者电信、银行、网络支付等行业从业人员利用履行职责或提供服务便利，非法开办并出售、出租他人手机卡、

信用卡、银行账户、非银行支付账户等的，可以认定为《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第十一条第（七）项规定的“其他足以认定行为人明知的情形”。但有相反证据的除外。

九、明知他人利用信息网络实施犯罪，为其犯罪提供下列帮助之一的，可以认定为《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第十二条第一款第（七）项规定的“其他情节严重的情形”：

（一）收购、出售、出租信用卡、银行账户、非银行支付账户、具有支付结算功能的互联网账号密码、网络支付接口、网上银行数字证书 5 张（个）以上的；

（二）收购、出售、出租他人手机卡、流量卡、物联网卡 20 张以上的。

十、电商平台预付卡、虚拟货币、手机充值卡、游戏点卡、游戏装备等经销商，在公安机关调查案件过程中，被明确告知其交易对象涉嫌电信网络诈骗犯罪，仍与其继续交易，符合刑法第二百八十七条之二规定的，以帮助信息网络犯罪活动罪追究刑事责任。同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

十一、明知是电信网络诈骗犯罪所得及其产生的收益，以下列方式之一予以转账、套现、取现，符合刑法第三百一十二条第一款规定的，以掩饰、隐瞒犯罪所得、犯罪所得收益罪追究刑事责任。但有证据证明确实不知道的除外。

（一）多次使用或者使用多个非本人身份证明开设的收款码、网络支付接口等，帮助他人转账、套现、取现的；

（二）以明显异于市场的价格，通过电商平台预付卡、虚拟货币、手机充值卡、游戏点卡、游戏装备等转换财物、套现的；

（三）协助转换或者转移财物，收取明显高于市场的 “手续费”的。

实施上述行为，事前通谋的，以共同犯罪论处；同时构成其他犯罪的，依照处罚较重的规定定罪处罚。法律和司法解释另有规定的除外。

十二、为他人实施电信网络诈骗犯罪提供技术支持、广告推广、支付结算等帮助，或者窝藏、转移、收购、代为销售及以其他方法掩饰、隐瞒电信网络诈骗犯罪所得及其产生的收益，诈骗犯罪行为可以确认，但实施诈骗的行为人尚未到案，可以依法先行追究已到案的上述犯罪嫌疑人、被告人的刑事责任。

十三、办案地公安机关可以通过公安机关信息化系统调取异地公安机关依法制作、收集的刑事案件受案登记表、立案决定书、被害人陈述等证据材料。调取时不得少于两名侦查人员，并应记载调取的时间、使用的信息化系统名称等相关信息，调取人签名并加盖办案地公安机关印章。经审核证明真实的，可以作为证据使用。

十四、通过国（区）际警务合作收集或者境外警方移交的境外证据材料，确因客观条件限制，境外警方未提供相关证据的发现、收集、保管、移交情况等材料的，公安机关应当对上述证据材料的来源、移交过程以及种类、数量、特征等作出书面说明，由两名以上侦查人员签名并加盖公安机关印章。经审核能够证明案件事实的，可以作为证据使用。

十五、对境外司法机关抓获并羁押的电信网络诈骗犯罪嫌疑人，在境内接受审判的，境外的羁押期限可以折抵刑期。

十六、办理电信网络诈骗犯罪案件，应当充分贯彻宽严相济刑事政策。在侦查、审查起诉、审判过程中，应当全面收集证据、准确甄别犯罪嫌疑人、被告人在共同犯罪中的层级地位及作用大小，结合其认罪态度和悔罪表现，区别对待，宽严并用，科学量刑，确保罚当其罪。

对于电信网络诈骗犯罪集团、犯罪团伙的组织者、策划者、指挥者和骨干分子，以及利用未成年人、在校学生、老年人、残疾人实施电信网络诈骗的，依法从严惩处。

对于电信网络诈骗犯罪集团、犯罪团伙中的从犯，特别是其中参与时间相对较短、诈骗数额相对较低或者从事辅助性工作并领取少量报酬，以及初犯、偶犯、未成年人、在校学生等，应当综合考虑其在共同犯罪中的地位作用、社会危害程度、主观恶性、人身危险性、认罪悔罪表现等情节，可以依法从轻、减轻处罚。犯罪情节轻微的，可以依法不起诉或者免予刑事处罚；情节显著轻微危害不大的，不以犯罪论处。

十七、查扣的涉案账户内资金，应当优先返还被害人，如不足以全额返还的，应当按照比例返还。

最高人民法院 最高人民检察院 公安部

2021 年 6 月 17 日

10.《最高人民法院、最高人民检察院关于办理贪污贿赂刑事案件适用法律若干问题的解释》

第一条　贪污或者受贿数额在三万元以上不满二十万元的，应当认定为刑法第三百八十三条第一款规定的“数额较大”，依法判处三年以下有期徒刑或者拘役，并处罚金。

贪污数额在一万元以上不满三万元，具有下列情形之一的，应当认定为刑法第三百八十三条第一款规定的“其他较重情节”，依法判处三年以下有期徒刑或者拘役，并处罚金：

（一）贪污救灾、抢险、防汛、优抚、扶贫、移民、救济、防疫、社会捐助等特定款物的；

（二）曾因贪污、受贿、挪用公款受过党纪、行政处分的；

（三）曾因故意犯罪受过刑事追究的；

（四）赃款赃物用于非法活动的；

（五）拒不交待赃款赃物去向或者拒不配合追缴工作，致使无法追缴的；

（六）造成恶劣影响或者其他严重后果的。

受贿数额在一万元以上不满三万元，具有前款第二项至第六项规定的情形之一，或者具有下列情形之一的，应当认定为刑法第三百八十三条第一款规定的“其他较重情节”，依法判处三年以下有期徒刑或者拘役，并处罚金：

（一）多次索贿的；

（二）为他人谋取不正当利益，致使公共财产、国家和人民利益遭受损失的；

（三）为他人谋取职务提拔、调整的。

第二条　贪污或者受贿数额在二十万元以上不满三百万元的，应当认定为刑法第三百八十三条第一款规定的“数额巨大”，依法判处三年以上十年以下有期徒刑，并处罚金或者没收财产。

贪污数额在十万元以上不满二十万元，具有本解释第一条第二款规定的情形之一的，应当认定为刑法第三百八十三条第一款规定的“其他严重情节”，依法判处三年以上十年以下有期徒刑，并处罚金或者没收财产。

受贿数额在十万元以上不满二十万元，具有本解释第一条第三款规定的情形之一的，应当认定为刑法第三百八十三条第一款规定的“其他严重情节”，依法判处三年以上十年以下

有期徒刑，并处罚金或者没收财产。

第三条　贪污或者受贿数额在三百万元以上的，应当认定为刑法第三百八十三条第一款规定的“数额特别巨大”，依法判处十年以上有期徒刑、无期徒刑或者死刑，并处罚金或者没收财产。

贪污数额在一百五十万元以上不满三百万元，具有本解释第一条第二款规定的情形之一的，应当认定为刑法第三百八十三条第一款规定的“其他特别严重情节”，依法判处十年以上有期徒刑、无期徒刑或者死刑，并处罚金或者没收财产。

受贿数额在一百五十万元以上不满三百万元，具有本解释第一条第三款规定的情形之一的，应当认定为刑法第三百八十三条第一款规定的“其他特别严重情节”，依法判处十年以上有期徒刑、无期徒刑或者死刑，并处罚金或者没收财产。

第十一条　刑法第一百六十三条规定的非国家工作人员受贿罪、第二百七十一条规定的职务侵占罪中的“数额较大”“数额巨大”的数额起点，按照本解释关于受贿罪、贪污罪相对应的数额标准规定的二倍、五倍执行。

11.《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》

（2004 年 9 月 1 日最高人民法院审判委员会第 1323 次会议、2004 年 9 月 2 日最高人民检察院第十届检察委员会第 26 次会议通过）　法释[2004]11 号

为依法惩治利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息、通过声讯台传播淫秽语音信息等犯罪活动，维护公共网络、通讯的正常秩序，保障公众的合法权益，根据《中华人民共和国刑法》、《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》的规定，现对办理该类刑事案件具体应用法律的若干问题解释如下：

第一条　以牟利为目的，利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息，具有下列情形之一的，依照刑法第三百六十三条第一款的规定，以制作、复制、出版、贩卖、传播淫秽物品牟利罪定罪处罚：

（一）制作、复制、出版、贩卖、传播淫秽电影、表演、动画等视频文件二十个以上的；

（二）制作、复制、出版、贩卖、传播淫秽音频文件一百个以上的；

（三）制作、复制、出版、贩卖、传播淫秽电子刊物、图片、文章、短信息等二百件以上的；

（四）制作、复制、出版、贩卖、传播的淫秽电子信息，实际被点击数达到一万次以上的；

（五）以会员制方式出版、贩卖、传播淫秽电子信息，注册会员达二百人以上的；

（六）利用淫秽电子信息收取广告费、会员注册费或者其他费用，违法所得一万元以上的；

（七）数量或者数额虽未达到第（一）项至第（六）项规定标准，但分别达到其中两项以上标准一半以上的；

（八）造成严重后果的。

利用聊天室、论坛、即时通信软件、电子邮件等方式，实施第一款规定行为的，依照刑法第三百六十三条第一款的规定，以制作、复制、出版、贩卖、传播淫秽物品牟利罪定罪处罚。释义引用统计

第二条　实施第一条规定的行为，数量或者数额达到第一条第一款第（一）项至第（六）项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。释义引用统计

第三条　不以牟利为目的，利用互联网或者移动通讯终端传播淫秽电子信息，具有下列

情形之一的，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚：

（一）数量达到第一条第一款第（一）项至第（五）项规定标准二倍以上的；

（二）数量分别达到第一条第一款第（一）项至第（五）项两项以上标准的；

（三）造成严重后果的。

利用聊天室、论坛、即时通信软件、电子邮件等方式，实施第一款规定行为的，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚。释义引用统计

第四条　明知是淫秽电子信息而在自己所有、管理或者使用的网站或者网页上提供直接链接的，其数量标准根据所链接的淫秽电子信息的种类计算。释义引用统计

第五条　以牟利为目的，通过声讯台传播淫秽语音信息，具有下列情形之一的，依照刑法第三百六十三条第一款的规定，对直接负责的主管人员和其他直接责任人员以传播淫秽物品牟利罪定罪处罚：

（一）向一百人次以上传播的；

（二）违法所得一万元以上的；

（三）造成严重后果的。

实施前款规定行为，数量或者数额达到前款第（一）项至第（二）项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。释义引用统计

第六条　实施本解释前五条规定的犯罪，具有下列情形之一的，依照刑法第三百六十三条第一款、第三百六十四条第一款的规定从重处罚：

（一）制作、复制、出版、贩卖、传播具体描绘不满十八周岁未成年人性行为的淫秽电子信息的；

（二）明知是具体描绘不满十八周岁的未成年人性行为的淫秽电子信息而在自己所有、管理或者使用的网站或者网页上提供直接链接的；

（三）向不满十八周岁的未成年人贩卖、传播淫秽电子信息和语音信息的；

（四）通过使用破坏性程序、恶意代码修改用户计算机设置等方法，强制用户访问、下载淫秽电子信息的。释义引用统计

第七条　明知他人实施制作、复制、出版、贩卖、传播淫秽电子信息犯罪，为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、费用结算等帮助的，对直接负责的主管人员和其他直接责任人员，以共同犯罪论处。释义引用统计

第八条　利用互联网、移动通讯终端、声讯台贩卖、传播淫秽书刊、影片、录像带、录音带等以实物为载体的淫秽物品的，依照《最高人民法院关于审理非法出版物刑事案件具体应用法律若干问题的解释》的有关规定定罪处罚。释义引用统计

第九条　刑法第三百六十七条第一款规定的“其他淫秽物品”，包括具体描绘性行为或者露骨宣扬色情的诲淫性的视频文件、音频文件、电子刊物、图片、文章、短信息等互联网、移动通讯终端电子信息和声讯台语音信息。

有关人体生理、医学知识的电子信息和声讯台语音信息不是淫秽物品。包含色情内容的有艺术价值的电子文学、艺术作品不视为淫秽物品。

12.《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）》

（2010 年 1 月 18 日由最高人民法院审判委员会第 1483 次会议、2010 年 1 月 14 日由最高人民检察院第十一届检察委员会第 28 次会议通过） 法释[2010]3 号

为依法惩治利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息，通过声讯台传播淫秽语音信息等犯罪活动，维护社会秩序，保障公民权益，根据《中华人民

共和国刑法》、《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》的规定，现对办理该类刑事案件具体应用法律的若干问题解释如下：

第一条　以牟利为目的，利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息的，依照《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》第一条、第二条的规定定罪处罚。

以牟利为目的，利用互联网、移动通讯终端制作、复制、出版、贩卖、传播内容含有不满十四周岁未成年人的淫秽电子信息，具有下列情形之一的，依照刑法第三百六十三条第一款的规定，以制作、复制、出版、贩卖、传播淫秽物品牟利罪定罪处罚：

（一）制作、复制、出版、贩卖、传播淫秽电影、表演、动画等视频文件十个以上的；

（二）制作、复制、出版、贩卖、传播淫秽音频文件五十个以上的；

（三）制作、复制、出版、贩卖、传播淫秽电子刊物、图片、文章等一百件以上的；

（四）制作、复制、出版、贩卖、传播的淫秽电子信息，实际被点击数达到五千次以上的；

（五）以会员制方式出版、贩卖、传播淫秽电子信息，注册会员达一百人以上的；

（六）利用淫秽电子信息收取广告费、会员注册费或者其他费用，违法所得五千元以上的；

（七）数量或者数额虽未达到第（一）项至第（六）项规定标准，但分别达到其中两项以上标准一半以上的；

（八）造成严重后果的。

实施第二款规定的行为，数量或者数额达到第二款第（一）项至第（七）项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。

第二条　利用互联网、移动通讯终端传播淫秽电子信息的，依照《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》第三条的规定定罪处罚。

利用互联网、移动通讯终端传播内容含有不满十四周岁未成年人的淫秽电子信息，具有下列情形之一的，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚：

（一）数量达到第一条第二款第（一）项至第（五）项规定标准二倍以上的；

（二）数量分别达到第一条第二款第（一）项至第（五）项两项以上标准的；

（三）造成严重后果的。

第三条　利用互联网建立主要用于传播淫秽电子信息的群组，成员达三十人以上或者造成严重后果的，对建立者、管理者和主要传播者，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚。

第四条　以牟利为目的，网站建立者、直接负责的管理者明知他人制作、复制、出版、贩卖、传播的是淫秽电子信息，允许或者放任他人在自己所有、管理的网站或者网页上发布，具有下列情形之一的，依照刑法第三百六十三条第一款的规定，以传播淫秽物品牟利罪定罪处罚：

（一）数量或者数额达到第一条第二款第（一）项至第（六）项规定标准五倍以上的；

（二）数量或者数额分别达到第一条第二款第（一）项至第（六）项两项以上标准二倍以上的；

（三）造成严重后果的。

实施前款规定的行为，数量或者数额达到第一条第二款第（一）项至第（七）项规定标准二十五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准

一百倍以上的，应当认定为“情节特别严重”。

第五条　网站建立者、直接负责的管理者明知他人制作、复制、出版、贩卖、传播的是淫秽电子信息，允许或者放任他人在自己所有、管理的网站或者网页上发布，具有下列情形之一的，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚：

（一）数量达到第一条第二款第（一）项至第（五）项规定标准十倍以上的；

（二）数量分别达到第一条第二款第（一）项至第（五）项两项以上标准五倍以上的；

（三）造成严重后果的。

第六条　电信业务经营者、互联网信息服务提供者明知是淫秽网站，为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、代收费等服务，并收取服务费，具有下列情形之一的，对直接负责的主管人员和其他直接责任人员，依照刑法第三百六十三条第一款的规定，以传播淫秽物品牟利罪定罪处罚：

（一）为五个以上淫秽网站提供上述服务的；

（二）为淫秽网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道等服务，收取服务费数额在二万元以上的；

（三）为淫秽网站提供代收费服务，收取服务费数额在五万元以上的；

（四）造成严重后果的。

实施前款规定的行为，数量或者数额达到前款第（一）项至第（三）项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。

第七条　明知是淫秽网站，以牟利为目的，通过投放广告等方式向其直接或者间接提供资金，或者提供费用结算服务，具有下列情形之一的，对直接负责的主管人员和其他直接责任人员，依照刑法第三百六十三条第一款的规定，以制作、复制、出版、贩卖、传播淫秽物品牟利罪的共同犯罪处罚：

（一）向十个以上淫秽网站投放广告或者以其他方式提供资金的；

（二）向淫秽网站投放广告二十条以上的；

（三）向十个以上淫秽网站提供费用结算服务的；

（四）以投放广告或者其他方式向淫秽网站提供资金数额在五万元以上的；

（五）为淫秽网站提供费用结算服务，收取服务费数额在二万元以上的；

（六）造成严重后果的。

实施前款规定的行为，数量或者数额达到前款第（一）项至第（五）项规定标准五倍以上的，应当认定为刑法第三百六十三条第一款规定的“情节严重”；达到规定标准二十五倍以上的，应当认定为“情节特别严重”。

第八条　实施第四条至第七条规定的行为，具有下列情形之一的，应当认定行为人“明知”，但是有证据证明确实不知道的除外：

（一）行政主管机关书面告知后仍然实施上述行为的；

（二）接到举报后不履行法定管理职责的；

（三）为淫秽网站提供互联网接入、服务器托管、网络存储空间、通讯传输通道、代收费、费用结算等服务，收取服务费明显高于市场价格的；

（四）向淫秽网站投放广告，广告点击率明显异常的；

（五）其他能够认定行为人明知的情形。

第九条　一年内多次实施制作、复制、出版、贩卖、传播淫秽电子信息行为未经处理，数量或者数额累计计算构成犯罪的，应当依法定罪处罚。

第十条　单位实施制作、复制、出版、贩卖、传播淫秽电子信息犯罪的，依照《中华人民共和国刑法》、《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、

声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》和本解释规定的相应个人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

第十一条　对于以牟利为目的，实施制作、复制、出版、贩卖、传播淫秽电子信息犯罪的，人民法院应当综合考虑犯罪的违法所得、社会危害性等情节，依法判处罚金或者没收财产。罚金数额一般在违法所得的一倍以上五倍以下。

第十二条　《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》和本解释所称网站，是指可以通过互联网域名、ＩＰ地址等方式访问的内容提供站点。

以制作、复制、出版、贩卖、传播淫秽电子信息为目的建立或者建立后主要从事制作、复制、出版、贩卖、传播淫秽电子信息活动的网站，为淫秽网站。

第十三条　以前发布的司法解释与本解释不一致的，以本解释为准。

三、指导案例、典型案例

（一）非法吸收公众存款罪

1.最高人民检察院关于印发最高人民检察院第十七批指导性案例的通知（2020.02.05）

检例第64号：杨卫国等人非法吸收公众存款案

【关键词】

非法吸收公众存款 网络借贷 资金池

【要旨】

单位或个人假借开展网络借贷信息中介业务之名，未经依法批准，归集不特定公众的资金设立资金池，控制、支配资金池中的资金，并承诺还本付息的，构成非法吸收公众存款罪。

【基本案情】

被告人杨卫国，男，浙江望洲集团有限公司法定代表人、实际控制人。

被告人张雯婷，女，浙江望洲集团有限公司出纳，主要负责协助杨卫国调度、使用非法吸收的资金。

被告人刘蓓蕾，女，上海望洲财富投资管理有限公司总经理，负责该公司业务。

被告人吴梦，女，浙江望洲集团有限公司经理、望洲集团清算中心负责人，主要负责资金池运作有关业务。

浙江望洲集团有限公司（以下简称望洲集团）于2013年2月28日成立，被告人杨卫国为法定代表人、董事长。自2013年9月起，望洲集团开始在线下进行非法吸收公众存款活动。2014年，杨卫国利用其实际控制的公司又先后成立上海望洲财富投资管理有限公司（以下简称望洲财富）、望洲普惠投资管理有限公司（以下简称望洲普惠），通过线下和线上两个渠道开展非法吸收公众存款活动。其中，望洲普惠主要负责发展信贷客户（借款人），望洲财富负责发展不特定社会公众成为理财客户（出借人），根据理财产品的不同期限约定7%－15%不等的年化利率募集资金。在线下渠道，望洲集团在全国多个省、市开设门店，采用发放宣传单、举办年会、发布广告等方式进行宣传，理财客户或者通过与杨卫国签订债权转让协议，或者通过匹配望洲集团虚构的信贷客户借款需求进行投资，将投资款转账至杨卫国个人名下42个银行账户，被望洲集团用于还本付息、生产经营等活动。在线上渠道，望洲集团及其关联公司以网络借贷信息中介活动的名义进行宣传，理财客户根据望洲集团的要求在第三方支付平台上开设虚拟账户并绑定银行账户。理财客户选定投资项目后将投资款从银行账户转入第三方支付平台的虚拟账户进行投资活动，望洲集团、杨卫国及望洲集团实际控制的担保公司为理财客户的债权提供担保。望洲集团对理财客户虚拟账户内的资金进行调配，划拨出借资金和还本付息资金到相应理财客户和信贷客户账户，并将剩余资金直接转至

杨卫国在第三方支付平台上开设的托管账户，再转账至杨卫国开设的个人银行账户，与线下资金混同，由望洲集团支配使用。

因资金链断裂，望洲集团无法按期兑付本息。截止到2016年4月20日，望洲集团通过线上、线下两个渠道非法吸收公众存款共计64亿余元，未兑付资金共计26亿余元，涉及集资参与人13400余人。其中，通过线上渠道吸收公众存款11亿余元。

【指控与证明犯罪】

2017年2月15日，浙江省杭州市江干区人民检察院以非法吸收公众存款罪对杨卫国等4名被告人依法提起公诉，杭州市江干区人民法院公开开庭审理本案。

法庭调查阶段，公诉人宣读起诉书指控杨卫国等被告人的行为构成非法吸收公众存款罪，并对杨卫国等被告人进行讯问。杨卫国对望洲集团通过线下渠道非法吸收公众存款的犯罪事实和性质没有异议，但辩称望洲集团的线上平台经营的是正常P2P业务，线上的信贷客户均真实存在，不存在资金池，不是吸收公众存款，不需要取得金融许可牌照，在营业执照许可的经营范围内即可开展经营。针对杨卫国的辩解，公诉人围绕理财资金的流转对被告人进行了重点讯问。

公诉人：（杨卫国）如果线上理财客户进来的资金大于借款方的资金，如何操作？

杨卫国：一般有两种操作方式。一种是停留在客户的操作平台上，另一种是转移到我开设的托管账户。如果转移到托管账户，客户就没有办法自主提取了。如果客户需要提取，我们根据客户指令再将资金返回到客户账户。

公诉人：（吴梦）理财客户充值到第三方支付平台的虚拟账户后，望洲集团操作员是否可以对第三方支付平台上的资金进行划拨。

吴梦：可以。

公诉人：（吴梦）请叙述一下划拨资金的方式。

吴梦：直接划拨到借款人的账户，如果当天资金充足，有时候会划拨到杨卫国在第三方支付平台上设立的托管账户，再提现到杨卫国绑定的银行账户，用来兑付线下的本息。

公诉人补充讯问：（吴梦）如果投资进来的资金大于借款方，如何操作？

吴梦：会对一部分进行冻结，也会提现一部分。资金优先用于归还客户的本息，然后配给借款方，然后再提取。

被告人的当庭供述证明，望洲集团通过直接控制理财客户在第三方平台上的虚拟账户和设立托管账户，实现对理财客户资金的归集和控制、支配、使用，形成了资金池。

举证阶段，公诉人出示证据，全面证明望洲集团线上、线下业务活动本质为非法吸收公众存款，并就线上业务相关证据重点举证。

第一，通过出示书证、审计报告、电子数据、证人证言、被告人供述和辩解等证据，证实望洲集团的线上业务归集客户资金设立资金池并进行控制、支配、使用，不是网络借贷信息中介业务。（1）第三方支付平台赋予望洲集团对所有理财客户虚拟账户内的资金进行冻结、划拨、查询的权限。线上理财客户在合同中也明确授权望洲集团对其虚拟账户内的资金进行冻结、划拨、查询，且虚拟账户销户需要望洲集团许可。（2）理财客户将资金转入第三方平台的虚拟账户后，望洲集团每日根据理财客户出借资金和信贷客户的借款需求，以多对多的方式进行人工匹配。当理财客户资金总额大于信贷客户借款需求时，剩余资金划入杨卫国在第三方支付平台开设的托管账户。望洲集团预留第二天需要支付的到期本息后，将剩余资金提现至杨卫国的银行账户，用于线下非法吸收公众存款活动或其他经营活动。（3）信贷客户的借款期限与理财客户的出借期限不匹配，存在期限错配等问题。（4）杨卫国及其控制的公司承诺为信贷客户提供担保，当信贷客户不能按时还本付息时，杨卫国保证在债权期限届满之日起3个工作日内代为偿还本金和利息。实际操作中，归还出借人的资金都来自于线上的托管账户或者杨卫国用于线下经营的银行账户。（5）望洲集团通过多种途径向

不特定公众进行宣传，发展理财客户，并通过明示年化收益率、提供担保等方式承诺向理财客户还本付息。

第二，通过出示理财、信贷余额列表，扣押清单，银行卡照片，银行卡交易明细，审计报告，证人证言，被告人供述和辩解等证据，证实望洲集团资金池内的资金去向：（1）望洲集团吸收的资金除用于还本付息外，主要用于扩大望洲集团下属公司的经营业务。（2）望洲集团线上资金与线下资金混同使用，互相弥补资金不足，望洲集团从第三方支付平台提现到杨卫国银行账户资金为2.7亿余元，杨卫国个人银行账户转入第三方支付平台资金为2亿余元。（3）望洲集团将吸收的资金用于公司自身的投资项目，并有少部分用于个人支出，案发时线下、线上的理财客户均遭遇资金兑付困难。

法庭辩论阶段，公诉人发表公诉意见，论证杨卫国等被告人构成非法吸收公众存款罪，起诉书指控的犯罪事实清楚，证据确实、充分。其中，望洲集团在线上经营所谓网络借贷信息中介业务时，承诺为理财客户提供保底和增信服务，获取对理财客户虚拟账户内资金进行冻结、划拨、查询等权限，归集客户资金设立资金池，实际控制、支配、使用客户资金，用于还本付息和其他生产经营活动，超出了网络借贷信息中介的业务范围，属于变相非法吸收公众存款。杨卫国等被告人明知其吸收公众存款的行为未经依法批准而实施，具有犯罪的主观故意。

杨卫国认为望洲集团的线上业务不构成犯罪，不应计入犯罪数额。杨卫国的辩护人认为，国家允许P2P行业先行先试，望洲集团设立资金池、开展自融行为的时间在国家对P2P业务进行规范之前，没有违反刑事法律，属民事法律调整范畴，不应受到刑事处罚，犯罪数额应扣除通过线上模式流入的资金。

公诉人针对杨卫国及其辩护人的辩护意见进行答辩：望洲集团在线上开展网络借贷中介业务已从信息中介异化为信用中介，望洲集团对理财客户投资款的归集、控制、支配、使用以及还本付息的行为，本质与商业银行吸收存款业务相同，并非国家允许创新的网络借贷信息中介行为，不论国家是否出台有关网络借贷信息中介的规定，未经批准实施此类行为，都应当依法追究刑事责任。因此，线上吸收的资金应当计入犯罪数额。

法庭经审理认为，望洲集团以提供网络借贷信息中介服务为名，实际从事直接或间接归集资金、甚至自融或变相自融行为，本质是吸收公众存款。判断金融业务的非法性，应当以现行刑事法律和金融管理法律规定为依据，不存在被告人开展P2P业务时没有禁止性法律规定的问题。望洲集团的行为已经扰乱金融秩序，破坏国家金融管理制度，应受刑事处罚。

2018年2月8日，杭州市江干区人民法院作出一审判决，以非法吸收公众存款罪，分别判处被告人杨卫国有期徒刑九年六个月，并处罚金人民币五十万元；判处被告人刘蓓蕾有期徒刑四年六个月，并处罚金人民币十万元；判处被告人吴梦有期徒刑三年，缓刑五年，并处罚金人民币十万元；判处被告人张雯婷有期徒刑三年，缓刑五年，并处罚金人民币十万元。在案扣押冻结款项分别按损失比例发还；在案查封、扣押的房产、车辆、股权等变价后分别按损失比例发还。不足部分责令继续退赔。宣判后，被告人杨卫国提出上诉后又撤回上诉，一审判决已生效。本案追赃挽损工作仍在进行中。

【指导意义】

1.向不特定社会公众吸收存款是商业银行专属金融业务，任何单位和个人未经批准不得实施。根据《中华人民共和国商业银行法》第十一条规定，未经国务院银行业监督管理机构批准，任何单位和个人不得从事吸收公众存款等商业银行业务，这是判断吸收公众存款行为合法与非法的基本法律依据。任何单位或个人，包括非银行金融机构，未经国务院银行业监督管理机构批准，面向社会吸收公众存款或者变相吸收公众存款均属非法。国务院《非法金融机构和非法金融业务活动取缔办法》进一步明确规定，未经依法批准，非法吸收公众存款、变相吸收公众存款、以任何名义向社会不特定对象进行的非法集资都属于非法金融活动，必

须予以取缔。为了解决传统金融机构覆盖不了、满足不好的社会资金需求，缓解个体经营者、小微企业经营当中的小额资金困难，国务院金融监管机构于2016年发布了《网络借贷信息中介机构业务活动管理暂行办法》等“一个办法、三个指引”，允许单位或个人在规定的借款余额范围内通过网络借贷信息中介机构进行小额借贷，并且对单一组织、单一个人在单一平台、多个平台的借款余额上限作了明确限定。检察机关在办案中要准确把握法律法规、金融管理规定确定的界限、标准和原则精神，准确区分融资借款活动的性质，对于违反规定达到追诉标准的，依法追究刑事责任。

2.金融创新必须遵守金融管理法律规定，不得触犯刑法规定。金融是现代经济的核心和血脉，金融活动引发的风险具有较强的传导性、扩张性、潜在性和不确定性。为了发挥金融服务经济社会发展的作用，有效防控金融风险，国家制定了完善的法律法规，对商业银行、保险、证券等金融业务进行严格的规制和监管。金融也需要发展和创新，但金融创新必须有效地防控可能产生的风险，必须遵守金融管理法律法规，尤其是依法须经许可才能从事的金融业务，不允许未经许可而以创新的名义擅自开展。检察机关办理涉金融案件，要深入分析、清楚认识各类新金融现象，准确把握金融的本质，透过复杂多样的表现形式，准确区分是真的金融创新还是披着创新外衣的伪创新，是合法金融活动还是以金融创新为名实施金融违法犯罪活动，为防范化解金融风险提供及时、有力的司法保障。

3.网络借贷中介机构非法控制、支配资金，构成非法吸收公众存款。网络借贷信息中介机构依法只能从事信息中介业务，为借款人与出借人实现直接借贷提供信息搜集、信息公布、资信评估、信息交互、借贷撮合等服务。信息中介机构不得提供增信服务，不得直接或间接归集资金，包括设立资金池控制、支配资金或者为自己控制的公司融资。网络借贷信息中介机构利用互联网发布信息归集资金，不仅超出了信息中介业务范围，同时也触犯了刑法第一百七十六条的规定。检察机关在办案中要通过对网络借贷平台的股权结构、实际控制关系、资金来源、资金流向、中间环节和最终投向的分析，综合全流程信息，分析判断是规范的信息中介，还是假借信息中介名义从事信用中介活动，是否存在违法设立资金池、自融、变相自融等违法归集、控制、支配、使用资金的行为，准确认定行为性质。

【相关规定】

《中华人民共和国刑法》第一百七十六条

《中华人民共和国商业银行法》第十一条

《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》（法释〔2010〕18号）第一条

（二）集资诈骗罪

1.最高人民检察院关于印发最高人民检察院第十批指导性案例的通知（高检发研字[2018]10号）

检例第40号：周辉集资诈骗案

【关键词】

集资诈骗　非法占有目的　网络借贷信息中介机构

【基本案情】

被告人周辉，男，1982年2月出生，原系浙江省衢州市中宝投资有限公司（以下简称中宝投资公司）法定代表人。

2011年2月，被告人周辉注册成立中宝投资公司，担任法定代表人。公司上线运营“中宝投资”网络平台，借款人（发标人）在网络平台注册、缴纳会费后，可发布各种招标信息，吸引投资人投资。投资人在网络平台注册成为会员后可参与投标，通过银行汇款、支付宝、财付通等方式将投资款汇至周辉公布在网站上的8个其个人账户或第三方支付平台账户。借

款人可直接从周辉处取得所融资金。项目完成后，借款人返还资金，周辉将收益给予投标人。

运行前期，周辉通过网络平台为13个借款人提供总金额约170万余元的融资服务，因部分借款人未能还清借款造成公司亏损。此后，周辉除用本人真实身份信息在公司网络平台注册2个会员外，自2011年5月至2013年12月陆续虚构34个借款人，并利用上述虚假身份自行发布大量虚假抵押标、宝石标等，以支付投资人约20%的年化收益率及额外奖励等为诱饵，向社会不特定公众募集资金。所募资金未进入公司账户，全部由周辉个人掌控和支配。除部分用于归还投资人到期的本金及收益外，其余主要用于购买房产、高档车辆、首饰等。这些资产绝大部分登记在周辉名下或供周辉个人使用。2011年5月至案发，周辉通过中宝投资网络平台累计向全国1586名不特定对象非法集资共计10.3亿余元，除支付本金及收益回报6.91亿余元外，尚有3.56亿余元无法归还。案发后，公安机关从周辉控制的银行账户内扣押现金1.80亿余元。

【要旨】

网络借贷信息中介机构或其控制人，利用网络借贷平台发布虚假信息，非法建立资金池募集资金，所得资金大部分未用于生产经营活动，主要用于借新还旧和个人挥霍，无法归还所募资金数额巨大，应认定为具有非法占有目的，以集资诈骗罪追究刑事责任。

【指控与证明犯罪】

2014年7月15日，浙江省衢州市公安局以周辉涉嫌集资诈骗罪移送衢州市人民检察院审查起诉。

审查起诉阶段，衢州市人民检察院审查了全案卷宗，讯问了犯罪嫌疑人。针对该案犯罪行为涉及面广，众多集资参与人财产遭受损失的情况，检察机关充分听取了辩护人和部分集资参与人意见，进一步核实了非法集资金额，对扣押的房产等作出司法鉴定或价格评估。针对辩护人提出的非法证据排除申请，检察机关审查后发现，涉案证据存在以下瑕疵：公安机关向部分证人取证时存在取证地点不符合刑事诉讼法规定以及个别辨认笔录缺乏见证人等情况。为此，检察机关要求公安机关予以补正或作出合理解释。公安机关作出情况说明：证人从外地赶来，经证人本人同意，取证在宾馆进行。关于此项情况说明，检察机关审查后予以采信。对于缺乏见证人的个别辨认笔录，检察机关审查后予以排除。

2015年1月19日，浙江省衢州市人民检察院以周辉犯集资诈骗罪向浙江省衢州市中级人民法院提起公诉。6月25日，衢州市中级人民法院公开开庭审理本案。

法庭调查阶段，公诉人宣读起诉书指控被告人周辉以高息为诱饵，虚构借款人和借款用途，利用网络P2P形式，面向社会公众吸收资金，主要用于个人肆意挥霍，其行为构成集资诈骗罪。对于指控的犯罪事实，公诉人出示了四组证据予以证明：一是被告人周辉的立案情况及基本信息；二是中宝投资公司的发标、招投标情况及相关证人证言；三是集资情况的证据，包括银行交易清单，司法会计鉴定意见书等；四是集资款的去向，包括购买车辆、房产等物证及相关证人证言。

法庭辩论阶段，公诉人发表公诉意见：被告人周辉注册网络借贷信息平台，早期从事少量融资信息服务。在公司亏损、经营难以为继的情况下，虚构借款人和借款标的，以欺诈方式面向不特定投资人吸收资金，自建资金池。在公安机关立案查处时，虽暂可通过“拆东墙补西墙”的方式偿还部分旧债维持周转，但根据其所募资金主要用于还本付息和个人肆意挥霍，未投入生产经营，不可能产生利润回报的事实，可以判断其后续资金缺口势必不断扩大，无法归还所募全部资金，故可以认定其具有非法占有的目的，应以集资诈骗罪对其定罪处罚。

辩护人提出：一是周辉行为系单位行为；二是周辉一直在偿还集资款，主观上不具有非法占有集资款的故意；三是周辉利用互联网从事P2P借贷融资，不构成集资诈骗罪，构成非法吸收公众存款罪。

公诉人针对辩护意见进行答辩：第一，中宝投资公司是由被告人周辉控制的一人公司，

不具有经营实体，不具备单位意志，集资款未纳入公司财务进行核算，而是由周辉一人掌控和支配，因此周辉的行为不构成单位犯罪。第二，周辉本人主观上认识到资金不足，少量投资赚取的收益不足以支付许诺的高额回报，没有将集资款用于生产经营活动，而是主要用于个人肆意挥霍，其主观上对集资款具有非法占有的目的。第三，P2P 网络借贷，是指个人利用中介机构的网络平台，将自己的资金出借给资金短缺者的商业模式。根据中国银行业监管委员会、工业和信息化部、公安部、国家互联网信息办公室制定的《网络借贷信息中介机构业务活动管理暂行办法》等监管规定，P2P 作为新兴金融业态，必须明确其信息中介性质，平台本身不得提供担保，不得归集资金搞资金池，不得非法吸收公众资金。周辉吸收资金建资金池，不属于合法的 P2P 网络借贷。非法吸收公众存款罪与集资诈骗罪的区别，关键在于行为人对吸收的资金是否具有非法占有的目的。利用网络平台发布虚假高利借款标募集资金，采取借新还旧的手段，短期内募集大量资金，不用于生产经营活动，或者用于生产经营活动与筹集资金规模明显不成比例，致使集资款不能返还的，是典型的利用网络中介平台实施集资诈骗行为。本案中，周辉采用编造虚假借款人、虚假投标项目等欺骗手段集资，所融资金未投入生产经营，大量集资款被其个人肆意挥霍，具有明显的非法占有目的，其行为构成集资诈骗罪。

法庭经审理，认为公诉人出示的证据能够相互印证，予以确认。对周辉及其辩护人提出的不构成集资诈骗罪及本案属于单位犯罪的辩解、辩护意见，不予采纳。综合考虑犯罪事实和量刑情节，2015 年 8 月 14 日，浙江省衢州市中级人民法院作出一审判决，以集资诈骗罪判处被告人周辉有期徒刑十五年，并处罚金人民币 50 万元。继续追缴违法所得，返还各集资参与人。

一审宣判后，浙江省衢州市人民检察院认为，被告人周辉非法集资 10.3 亿余元，属于刑法规定的集资诈骗数额特别巨大并且给人民利益造成特别重大损失的情形，依法应处无期徒刑或者死刑，并处没收财产，一审判决量刑过轻。2015 年 8 月 24 日，向浙江省高级人民法院提出抗诉。被告人周辉不服一审判决，提出上诉。其上诉理由是量刑畸重，应判处缓刑。

本案二审期间，2015 年 8 月 29 日，第十二届全国人大常委会第十六次会议审议通过了《中华人民共和国刑法修正案（九）》，删去《刑法》第一百九十九条关于犯集资诈骗罪“数额特别巨大并且给国家和人民利益造成特别重大损失的，处无期徒刑或者死刑，并处没收财产”的规定。刑法修正案（九）于 2015 年 11 月 1 日起施行。

浙江省高级人民法院经审理后认为，刑法修正案（九）取消了集资诈骗罪死刑的规定，根据从旧兼从轻原则，一审法院判处周辉有期徒刑十五年符合修订后的法律规定。上诉人周辉具有集资诈骗的主观故意及客观行为，原审定性准确。2016 年 4 月 29 日，二审法院作出裁定，维持原判。终审判决作出后，周辉及其父亲不服判决提出申诉，浙江省高级人民法院受理申诉并经审查后，认为原判事实清楚，证据确实充分，定性准确，量刑适当，于 2017 年 12 月 22 日驳回申诉，维持原裁判。

【指导意义】

是否具有非法占有目的，是正确区分非法吸收公众存款罪和集资诈骗罪的关键。对非法占有目的的认定，应当围绕融资项目真实性、资金去向、归还能力等事实、证据进行综合判断。行为人将所吸收资金大部分未用于生产经营活动，或名义上投入生产经营，但又通过各种方式抽逃转移资金，或供其个人肆意挥霍，归还本息主要通过借新还旧来实现，造成数额巨大的募集资金无法归还的，可以认定具有非法占有的目的。

集资诈骗罪是近年来检察机关重点打击的金融犯罪之一。对该类犯罪，检察机关应着重从以下几个方面开展工作：一是强化证据审查。非法集资类案件由于参与人数多、涉及面广，受主客观因素影响，取证工作易出现瑕疵和问题。检察机关对重大复杂案件要及时介入侦查、引导取证。在审查案件中要强化对证据的审查，需要退回补充侦查或者自行补充侦查的，要

及时退查或补查，建立起完整、牢固的证据锁链，夯实认定案件事实的证据基础。二是在法庭审理中要突出指控和证明犯罪的重点。要紧紧围绕集资诈骗罪构成要件，特别是行为人主观上具有非法占有目的、客观上以欺骗手段非法集资的事实梳理组合证据，运用完整的证据体系对认定犯罪的关键事实予以清晰证明。三是要将办理案件与追赃挽损相结合。检察机关办理相关案件，要积极配合公安机关、人民法院依法开展追赃挽损、资产处置等工作，最大限度减少人民群众的实际损失。四是要结合办案开展以案释法，增强社会公众的法治观念和风险防范意识，有效预防相关犯罪的发生。

【相关规定】

《中华人民共和国刑法》第一百九十二条

《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》第四条

《最高人民检察院、公安部关于公安机关管辖的刑事案件立案追诉标准的规定（二）》第四十九条

（三）侵犯著作权罪

1.典型案例：8.06特大互联网侵犯著作权犯罪案--张斌锋林烽楷等侵犯著作权罪

2017年6月29日下午，重庆市两江新区知识产权法庭对被告人林某、许某、张某、韦某、何某等五人涉嫌侵犯LegendofMir2(中文名称《热血传奇》，简称“传奇”)网络游戏软件著作权一案进行公开宣判，该案即公安部督办的“8.06”特大互联网侵犯著作权犯罪案件。

经合议庭反复讨论研判，法庭最终认定五名被告人构成侵犯著作权罪，分别判处林某、许某、张某有期徒刑三年，缓刑五年，并处罚金200万元；分别判处韦某、何某有期徒刑一年，缓刑一年，并处罚金70000元；扣押的犯罪工具笔记本电脑、电脑主机、服务器硬盘予以没收;扣押的被告人林某的违法所得45.127568万元和张某的违法所得12.7728万元予以追缴。五名被告人当场认罪伏法，表示不上诉。

2013年下半年以来，为谋取非法利益，被告人林某、许某、张某未经《热血传奇》著作权人许可，非法获取《热血传奇》源程序，改编为“轩辕传奇”、“回忆传奇”和“至尊传奇”三个私服游戏，用于在互联网上发布网络游戏，供玩家下载。被告人韦某、何某明知被告人林某等人开设的是传奇私服游戏，仍借用易宝、支付宝等支付平台接受玩家的充值，为他们提供资金结算服务，共同实施犯罪。

经鉴定，“轩辕传奇”、“回忆传奇”和“至尊传奇”与“热血传奇”的相似性比例分别为98.5%、97.45%、98.35%，均构成实质性相似。

据承办法官介绍，网络游戏私服具有专业性、技术性强等特点，案件事实查明难度较大。具体到本案，由于网络游戏私服的源程序包括服务器端程序和客户端程序，那么认定网络游戏私服侵权时，对上述二者都进行比对，亦或是仅比对其中之一是个问题。此外，帮助侵权的犯罪金额是以帮助侵权人实际获利金额为准，还是以主犯私服运营者的非法经营额来认定，也是本案审理中颇具争议的问题。

近年来，随着国内计算机软件产业的迅猛发展，各种利用高科技软件实施的知识产权犯罪案件数量逐年增加，该案是极为典型的涉及网络游戏私服的知识产权刑事案件。本次公开宣判将极大地震慑著作权领域违法犯罪分子，维护网络游戏计算机软件市场正常竞争秩序，提高辖区企业知识产权保护意识，营造尊重知识、保护创新的良好氛围。

附：张斌锋林烽楷等侵犯著作权罪一审刑事判决书

审理经过

重庆市渝北区人民检察院指控，LegendofMir2网络游戏软件〔中文名称《热血传奇》简称“传奇”〕的著作权人为WemadeEntertainmentCo.,Ltd，ActozSoftCo.,Ltd。2013年下半年以来，被告人林烽楷、许斯源、张斌锋未经上述著作权人许可，非法获取《热血传奇》源程序，改编为《轩辕传奇》、《回忆传奇》、《至尊传奇》三个私服游戏。三人在浙江省等地租用服务器，将游戏登陆器绑定至域名www.20xy.com等网站，继而在广东省汕头市东等地通过电脑远程控制的方式私自架设游戏服务器端，用于在互联网上发布网络游戏，供玩家下载。并借用易宝、支付宝等支付平台接受玩家充值牟利。其中林烽楷负责租赁服务器搭建私服、游戏推广等；许斯源负责财务及后勤保障等；张斌锋负责游戏日常维护等。经司法审计，2013年12月31日至2015年12月8日，林烽楷、许斯源、张斌锋借用易宝支付平台及林烽楷本人银行账户共收取充值费642.1507万元。

2014年9月以来，被告人韦君、何友军为牟取非法利益成立重庆马首科技有限公司，二人在明知林烽楷等人未经著作权人授权经营《轩辕传奇》等游戏私服的情况下，积极编写接口程序、架设充值平台，帮助林烽楷等人通过重庆马首科技有限公司的支付宝账户收款，并对该平台进行日常维护。韦君、何友军收款后，分别扣除0.5%、0.3%的手续费后将剩余款项转入林烽楷指定的银行卡内。经司法审计，2014年9月至案发，共计为林烽楷等人收取充值费26.74884万元。

上述所获充值费共计668.89954万元，在扣除服务器租赁费、员工工资等支出后由林烽楷、许斯源、张斌锋三人平分，各分得100余万元，用于日常生活开支及购买车辆等。

2015年11月11日，被告人林烽楷被抓获到案，2016年1月3日，被告人何友军被抓获到案，2016年1月7日，被告人韦君主动到公安机关投案，2016年4月29日，被告人许斯源、张斌锋被抓获到案。各被告人到案后均如实供述了上述事实。各被告人对重庆小闲在线科技有限公司进行了赔偿并取得了谅解。

针对上述指控，公诉机关当庭举示了相关证据，公诉机关认为，被告人林烽楷、许斯源、张斌锋以营利为目的，未经著作权人许可，复制发行其计算机游戏软件作品，违法所得数额巨大，被告人韦君、何友军明知他人实施侵犯知识产权犯罪，仍以盈利为目的，为其提供资金结算等帮助，各被告人的行为均已触犯《中华人民共和国刑法》第二百一十七条第（一）项之规定，构成侵犯著作权罪。被告人林烽楷、许斯源、张斌锋在共同犯罪中起主要作用，具有《中华人民共和国刑法》第二十六条第一款规定的量刑情节，被告人韦君、何友军在共同犯罪中起次要作用，具有《中华人民共和国刑法》第二十七条第一款规定的量刑情节。被告人林烽楷、许斯源、张斌锋、何友军到案后如实供述了自己的犯罪事实，具有《中华人民共和国刑法》第六十七条第三款规定的量刑情节。被告人韦君主动投案并如实供述犯罪事实，具有《中华人民共和国刑法》第六十七条第一款规定的量刑情节。提请本院依法判处。

一审答辩情况

被告人林烽楷对指控的犯罪事实和罪名均无异议。其辩护人提出的辩护意见是被告人林烽楷协助公安机关抓获了同案犯，具有立功情节，积极赔偿被害人，系初犯，本案社会危害性较小，林烽楷认罪认罚，且已被羁押31天，建议从轻处罚，同时考虑林烽楷没有再犯罪的危险，建议对其适用缓刑。

被告人许斯源对指控的犯罪事实和罪名均无异议。其辩护人提出的辩护意见是被告人许斯源只是负责财务，在共同犯罪中所起作用较小，具有坦白情节。被告人具有自首情节，其与公安机关商定于2016年5月5日来投案自首，并告知民警自己的位置，但公安机关提前抓获。被告人获得被害人谅解，系初犯，一贯表现良好，家庭困难，认罪认罚，请求从宽处罚，希望对其适用缓刑。

被告人张斌锋对指控的犯罪事实和罪名均无异议。其辩护人提出的辩护意见是被告人张斌锋没有任何不良行为，平时遵纪守法，没有前科，系初犯、偶犯，到案后如实供述，积极

退赃，取得被害人谅解。被告人已经为自首作了准备，且他们是准备4月底来重庆自首，后因公安机关的安排准备5月5日来重庆，后被公安机关抓获。希望对其适用缓刑。
被告人韦君对指控的犯罪事实和罪名均无异议。
被告人何友军对指控的犯罪事实和罪名均无异议。
本院查明

经审理查明，2003年8月18日，国家版权局颁发计算机软件著作权登记证书，软件名称：LegendofMir2游戏软件〔中文名称《热血传奇》简称“传奇”〕V1.0，著作权人：WemadeEntertainmentCo.,Ltd，ActozSoftCo.,Ltd，权利取得方式为原始取得，权利范围为全部权利，首次发表日期：2000年8月22日。上海盛大网络发展有限公司、蓝沙信息技术（上海）有限公司、上海数龙科技有限公司获得上述原始著作权人的授权，依法取得“传奇”游戏软件在中国大陆地区的相关著作权权益。2014年9月23日，上海盛大网络发展有限公司、蓝沙信息技术（上海）有限公司、上海数龙科技有限公司授权重庆小闲在线科技有限公司对侵权的客户端游戏采取包括发出警告函、控告、形式报案、索赔等措施进行维权。
2013年下半年以来，被告人林烽楷、许斯源、张斌锋未经《热血传奇》游戏软件著作权人的许可，非法获取《热血传奇》源程序，在浙江省台州等地区租用服务器，在位于广东省汕头市东厦华园33栋201房间等地通过电脑远程控制的方式架设了《轩辕传奇》、《回忆传奇》和《至尊合击》三个私服游戏。被告人林烽楷将游戏登陆器绑定域名www.20xy.com等，私自架设游戏服务器端，用于在互联网上发布网络游戏，供玩家下载，并通过易宝、支付宝等支付平台接受玩家的充值。其中，林烽楷负责获取《热血传奇》源代码，租赁服务器、搭建私服、游戏推广等；许斯源负责财务及后勤保障等；张斌锋负责游戏的日常维护等。经司法审计，2013年12月31日至2015年12月8日，林烽楷、许斯源、张斌锋借用易宝支付平台及林烽楷本人银行账户共收取充值费642.1507万元。

2014年下半年以来，被告人韦君、何友军为牟取非法利益成立重庆马首科技有限公司，二人在明知林烽楷等人经营的是传奇私服游戏的情况下，编写接口程序、架设充值平台，为林烽楷等人提供资金结算服务。韦君、何友军收款后，分别扣除相应的手续费后将剩余款项转入林烽楷指定的银行卡内。经司法审计，2014年9月至案发，共计转入林烽楷指定银行卡的充值费为26.74884万元。

截至案发，林烽楷等人共获充值费共计668.89954万元。

2015年12月11日，被告人林烽楷被抓获到案；2016年1月3日，被告人何友军被抓获到案；2016年1月7日，被告人韦君主动到公安机关投案；2016年4月29日，被告人许斯源、张斌锋被抓获到案。各被告人到案后均如实供述了上述事实。各被告人均取得了重庆小闲在线科技有限公司的谅解，重庆小闲在线科技有限公司共获得上述五名被告人共计310万元的赔偿款。

经公安机关委托，上海市东方计算机司法鉴定所对林烽楷等人在浙江台州架设的服务器上的私服游戏服务器端程序7个与《热血传奇》服务器端程序进行同一性比对，比对结果为：7个私服游戏服务器端程序与《热血传奇》的相似性比例均为85%。

另查明，公安机关扣押林烽楷用违法所得购买轿车的等额价值的现金45.127568万元，张斌锋用违法所得购买轿车的等额价值的现金12.7728万元。

上述事实，有下列证据予以证实：

1、受案登记表、立案决定书、到案经过，证实本案的受案和立案情况以及五名被告人除韦君系自首外，其他四名被告人均系抓获到案。

2、常住人口登记信息，证实林烽楷、许斯源、张斌锋、韦君、何友军的身份信息及案发时达到完全刑事责任年龄。

3、计算机软件著作权登记证书，证实LegendofMir2游戏软件的著作权人情况、首次发

表时间、权利取得方式及权利范围。

4、著作权授权书、授权声明、进口网络游戏产品批准单，证实重庆小闲在线科技有限公司系在中国大陆地区对侵犯《热血传奇》（英文名 LegendofMir2）游戏权益的客户端游戏进行维权的唯一被许可人，有权对侵权的客户端游戏采取包括刑事报案、索赔等措施进行维权。

5、被害人刘东的陈述，证实“轩辕传奇”未经著作权人或相关授权人授权。

6、电子证据勘验工作记录、鉴定聘请书、上海东方计算机司法鉴定所司法鉴定意见书，证实对涉案服务器硬盘中的源程序进行提取，共提取到 7 个服务器端程序，将其与“热血传奇”服务器端程序比对，相似比例均为 85%。

7、证人郑树水、黄炎文、陈泽平的证言，证实该三人在轩辕传奇私服工作，林烽楷负责总的技术，许斯源负责财务，张斌锋负责技术。郑树水将自己尾号为 3681 的银行卡交给林烽楷使用。

8、证人欧小川、卢龙江、武衡，证实该三人玩过《轩辕传奇》私服，该私服与《热血传奇》基本没区别，该三人均通过支付宝向轩辕传奇充值。

9、证人符建伟、邱磊的证言，证实 QQ 号使用人从该公司租赁位于浙江宁波的服务器，该服务器已被民警扣押。

10、被告人林烽楷的供述，证实 2013 年年中开始，林烽楷与许斯源、张斌锋共同架设私服游戏，林烽楷从网上下载游戏的源程序，并上传至服务器端，取名为轩辕传奇、回忆传奇和至尊合击，虽然三个名字不一样，但进去后都是一个游戏程序，玩家都可以在一起玩，服务器租赁是林烽楷在网上用 QQ 号联系的，其架设的传奇私服没有经过授权。许斯源主要负责后勤等管理工作，张斌锋主要负责技术维护等，经营额约 670 万元，林烽楷用获利购买了凯迪拉克轿车，给其提供结算的是一个叫“阿米”的重庆人，同时，林烽楷还用易宝来结算。

11、被告人许斯源的供述，证实许斯源在共同犯罪中主要负责租赁场地、购买电脑、分配收益等。经营私服游戏的毛收入 670 万元，由易宝和重庆一个叫阿米的人结算，易宝结算了 640 多万，阿米结算了 30 万左右，林烽楷以前在汕头机房就搞过私服，听说还比较赚钱，张斌锋负责对游戏进行维护和处理，林烽楷主要负责联系租服务器，在网上找传奇的源程序来修改形成私服游戏程序，再架设到服务器上。

12、被告人张斌锋的供述，证实其开设的传奇私服，源程序是用盛大的《热血传奇》的源程序，是林烽楷获取的《热血传奇》1.80 版。事实上只架设了一个传奇私服，但对外是《轩辕传奇》、《回忆传奇》、《至尊合击》三个游戏，这三个游戏有各自的域名和登陆器，但从三个登陆器登陆进来都是一样的，三人中林烽楷负责技术，具体包括在网上寻找下载传奇源程序，购买脚本来增加游戏的可玩性，游戏推广及游戏服务器租赁搭建等。张斌锋负责游戏的日常维护、对技术人员进行培训及购买耗材等，许斯源负责财务及后勤保障。

13、被告人韦君的供述，证实 2014 年下半年，其与何友军商量一起在网上替不具备支付宝合作资质的商户代收客户款项以赚取收入。因写程序时要进入后台查看，所以其知道林烽楷是做传奇私服的。其负责在网上打广告联系客户，写接口程序，架设充值平台，对程序和平台进行维护，何友军负责申请空壳公司重庆马首科技公司去支付宝拿到支付宝账户，租赁服务器并管理服务器上订单，申请 QQ 解决客户充值问题。利润取得方式是玩家充值成功后，支付宝收取手续费后将钱转入重庆马首科技公司的支付宝账户，何友军在扣除 0.3%的利润后，将钱提现到何晓凤的招商银行卡，韦君再提取 0.5%的利润后将钱转入林烽楷等人指定的郑树水的银行卡上。

14、被告人何友军的供述，证实 2014 年下半年，其和韦君商量，由其成立重庆马首科技有限公司，帮如传奇私服等游戏收取充值款，其负责在阿里云租用了服务器并申请一个网

络域名作为支付宝收取客户充值的接口域名，并申请支付宝账号，韦君负责编写借口。其提取重庆马首科技公司支付宝账户上金额的0.3%，韦君扣除自己的利润后将钱打给轩辕传奇。

15、易宝账户交易流水、招商银行、中国银行、工商银行、民生银行等出具的银行流水、郑树水尾号为X的工行卡流水、支付宝账号交易明细、重庆万隆方正会计师事务所司法审计报告，证实2013年12月31日至2015年12月8日，林烽楷、许斯源、张斌锋借用易宝支付平台及林烽楷本人银行账户共收取充值费642.1507万元。2014年9月至案发，韦君、何友军为林烽楷等人收取充值费26.74884万元。

16、扣押、发还清单，证实案发后，公安机关从林烽楷处扣押笔记本电脑、电脑主机、银行卡及现金，从张斌锋处扣押笔记本电脑及现金，从台州安云科技公司扣押涉案的服务器硬盘等。

17、谅解书，证实小闲公司对林烽楷、张斌锋、许斯源、韦君和何友军的侵权行为予以谅解。

18、重庆马首科技有限公司营业执照、税务登记证、组织机构代码证，证实重庆马首科技有限公司的经营范围为计算机软件研究开发等。

19、渝中区公安分局经侦支队2017年4月11日出具的到案情况说明，2017年5月8日出具的情况说明，证实2016年4月下旬，林烽楷主动电话联系民警，表示许斯源、张斌锋愿意并且准备于2016年5月5日到支队投案自首，并告知民警二人所在位置，电话中，张斌锋、许斯源也表示同意。后基于支队的工作安排，民警于2016年4月29日将许斯源、张斌锋抓获。

20、跨行人民币汇款凭证、收据、现金解款单，证实，重庆小闲在线科技有限公司收到上述五名被告人赔偿款共计310万元。

上列证据，经法庭质证，收集程序合法，内容客观真实，且能相互印证，证明本案的事实，本院予以确认。

本院认为

本院认为，被告人林烽楷、许斯源、张斌锋架设了《轩辕传奇》、《回忆传奇》和《至尊合击》三个私服游戏，经鉴定，上述私服游戏的服务器端程序源代码与《热血传奇》的服务器端程序源代码相似比例高达85%，构成实质性相似。被告人林烽楷、许斯源、张斌锋架设上述私服游戏的行为属于以营利为目的，未经著作权人许可，复制发行计算机软件的行为，该行为侵害了著作权人的著作权，且被告人林烽楷、许斯源、张斌锋的非法经营数额巨大，构成侵犯著作权罪，依法应予刑事处罚。被告人韦君、何友军明知他人实施侵犯知识产权犯罪，仍以营利为目的为其提供资金结算等帮助，被告人韦君、何友军的行为亦构成侵犯著作权罪，依法应予刑事处罚。被告人林烽楷、许斯源、张斌锋、韦君、何友军系共同犯罪，其中被告人林烽楷、许斯源、张斌锋在共同犯罪中起主要作用，是主犯。被告人韦君、何友军在共同犯罪中起次要作用，是从犯，依法应减轻处罚。被告人林烽楷、许斯源、张斌锋、何友军到案后如实供述了自己的犯罪事实，依法可以从轻处罚。被告人韦君主动投案并如实供述犯罪事实，依法可以从轻处罚。各被告人有退赃情节，且取得被害人谅解，量刑时可以酌情从轻处罚。公诉机关指控的犯罪事实清楚，证据确实、充分，罪名成立。

被告人许斯源、张斌锋的辩护人均提出，两被告人系自首，两人与公安机关商定了投案时间，并指出其两人所在位置，为自首作了准备，但由于公安机关提前行动，导致两被告人被抓获。本院认为，《中华人民共和国刑法》第六十七条第一款规定，犯罪以后自动投案，如实供述自己的罪行的，是自首。《最高人民法院关于处理自首和立功具体应用法律若干问题的解释》第一条规定，自动投案，是指犯罪事实或者犯罪嫌疑人未被司法机关发觉，或者虽被发觉，但犯罪嫌疑人尚未受到讯问、未被采取强制措施时，主动、直接向公安机关、人民检察院或者人民法院投案。犯罪嫌疑人向其所在单位、城乡基层组织或者其他有关负责人

员投案的；犯罪嫌疑人因病、伤或者为了减轻犯罪后果，委托他人先代为投案，或者先以信电投案的；罪行尚未被司法机关发觉，仅因形迹可疑，被有关组织或者司法机关盘问、教育后，主动交代自己的罪行的；犯罪后逃跑，在被通缉、追捕过程中，主动投案的；经查实确已准备去投案，或者正在投案途中，被公安机关捕获的，应当视为自动投案。并非出于犯罪嫌疑人主动，而是经亲友规劝、陪同投案的；公安机关通知犯罪嫌疑人的亲友，或者亲友主动报案后，将犯罪嫌疑人送去投案的，也应当视为自动投案。犯罪嫌疑人自动投案后又逃跑的，不能认定为自首。本案中，被告人许斯源、张斌锋虽然向公安机关电话表示要去投案自首，但并未有投案的行为，且其仅陈述其所在位置，也未能证明其为自首所作了准备工作，故依法不能认定自首。被告人林烽楷的辩护人提出，林烽楷具有立功情节，其规劝许斯源和张斌锋自首。本院认为，《中华人民共和国刑法》第六十八条规定，犯罪分子有揭发他人犯罪行为，查证属实的，或者提供重要线索，从而得以侦破其他案件等立功表现的，可以从轻或者减轻处罚；有重大立功表现的，可以减轻或者免除处罚。《最高人民法院关于处理自首和立功具体应用法律若干问题的解释》第五条规定，根据刑法第六十八条第一款的规定，犯罪分子到案后有检举、揭发他人犯罪行为，包括共同犯罪案件中的犯罪分子揭发同案犯共同犯罪以外的其他犯罪，经查证属实；提供侦破其他案件的重要线索，经查证属实；阻止他人犯罪活动；协助司法机关抓捕其他犯罪嫌疑人（包括同案犯）；具有其他有利于国家和社会的突出表现的，应当认定为有立功表现。本案中，被告人林烽楷虽然有规劝自首的行为，但该规劝行为并没有实现自首的结果，不属于协助司法机关抓捕其他犯罪嫌疑人的情形，依法不能认定立功。

综上，根据被告人的犯罪事实、性质、情节和社会危害程度、认罪悔罪态度、具备的监管条件等，依照《中华人民共和国刑法》第二百一十七条第（一）项、第二十五条第一款、第二十六条第一款、第二十七条、第七十二条第一款、第三款、第七十三条第二款、第三款、第五十二条、第五十三条、第六十四条，《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》第五条、第十一条，《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（二）》第四条之规定，判决如下：

裁判结果

一、被告人林烽楷犯侵犯著作权罪，判处有期徒刑三年，缓刑五年，并处罚金 200 万元；（缓刑考验期限，从判决确定之日起计算。罚金已预缴 100 万元，余款限判决生效后十日内缴纳。）

二、被告人许斯源犯侵犯著作权罪，判处有期徒刑三年，缓刑五年，并处罚金 200 万元；（缓刑考验期限，从判决确定之日起计算。罚金已预缴 100 万元，余款限判决生效后十日内缴纳。）

三、被告人张斌锋犯侵犯著作权罪，判处有期徒刑三年，缓刑五年，并处罚金 200 万元；（缓刑考验期限，从判决确定之日起计算。罚金已预缴 100 万元，余款限判决生效后十日内缴纳。）

四、被告人韦君犯侵犯著作权罪，判处有期徒刑一年，缓刑一年，并处罚金 70000 元；（缓刑考验期限，从判决确定之日起计算。罚金已预缴 2 万元，余款限判决生效后十日内缴纳。）

五、被告人何友军犯侵犯著作权罪，判处有期徒刑一年，缓刑一年，并处罚金 70000 元；（缓刑考验期限，从判决确定之日起计算。罚金已预缴 2 万元，余款限判决生效后十日内缴纳。）

六、扣押的犯罪工具笔记本电脑、电脑主机、服务器硬盘予以没收；

七、扣押的被告人林烽楷的违法所得 45.127568 万元和张斌锋的违法所得 12.7728 万元

予以追缴。

2.典型案例：广东龙小卫等侵犯著作权案

明知他人违法运维私服游戏，仍为其提供玩家充值通道和支付结算业务，并按比例收取手续费，情节严重的，构成帮助信息网络犯罪活动罪。

案例要旨

行为人明知游戏运营方利用互联网运维私服游戏是违法犯罪行为，仍然为其提供玩家充值通道和支付结算业务，并按比例收取手续费，情节严重的，构成帮助信息网络犯罪活动罪。

广东龙小卫等侵犯著作权案

一、案件事实

2017 年 6 月始，被告人龙小卫受雇于他人（另案处理），在未经著作权人广州多益网络股份有限公司许可的情况下，到泰国协助他人架设、运营私服游戏《歪歪神武》。2017 年 9 月，被告人李勃加入《歪歪神武》的运营。期间，二人负责通过 QQ 与玩家沟通，进行游戏推广，并联系游戏充值平台管理员将玩家充值金额转至指定银行账户。

2017 年 9 月始，被告单位机械牛网络科技（苏州）有限公司和被告人程刚，在明知《歪歪神武》运营方利用互联网运维私服游戏的情况下，仍通过“派爱支付”平台与《歪歪神武》私服网站进行连接，为《歪歪神武》提供玩家充值通道和支付结算，并按比例收取手续费。经鉴定，《歪歪神武》游戏程序对著作权人自主研发的《神武》游戏程序进行了非法复制。经核算，2017 年 9 月 28 日至 2018 年 1 月 23 日，被告单位机械牛网络科技（苏州）有限公司为《歪歪神武》支付结算玩家充值金额共计 362 万余元。

二、诉讼过程

本案由广东省广州市公安局黄埔分局侦查终结，于 2018 年 6 月 15 日移送审查起诉。同年 12 月 5 日，广州市黄埔区检察院以被告人龙小卫、李勃涉嫌侵犯著作权罪，被告单位机械牛网络科技（苏州）有限公司、被告人程刚涉嫌帮助信息网络犯罪活动罪提起公诉。同年 12 月 25 日，黄埔区法院判决，被告人龙小卫犯侵犯著作权罪，判处有期徒刑二年，并处罚金 2 万元；被告人李勃犯侵犯著作权罪，判处有期徒刑一年六个月，并处罚金 1 万元；被告单位机械牛网络科技（苏州）有限公司犯帮助信息网络犯罪活动罪，判处罚金 3 万元；被告人程刚犯帮助信息网络犯罪活动罪，判处有期徒刑十个月，并处罚金 1 万元。该判决已生效。

四、评析意见

本案系一起跨国网络侵犯知识产权犯罪案件，具有手法隐蔽、跨境作案、产业化经营等特点。办案过程中，黄埔区检察院充分发挥法律监督职能，灵活运用电子证据，有效严惩犯罪，切实维护企业合法权益，为建设广东省营商环境改革创新试验区注入一剂司法“强心针”。

（一）走访挖掘侵权线索，破解侵权发现难。《歪歪神武》运营者组建多个 QQ 群用于和玩家交流、发布游戏动态，形成相对封闭的“圈子”，外人难以发现，涉案人反侦查意识强，频繁通过变换游戏网站域名逃避侦查。黄埔区检察院对驻区企业进行“全覆盖式”走访服务时获悉广州多益网络股份有限公司自主研发的《神武》游戏源代码被盗，检察官遂提醒该公司可能存在被侵犯著作权的情况。该公司随即发现网络上出现与《神武》极其相似的《歪歪神武》。在检察官的引导下，该公司通过安排员工试玩《歪歪神武》、触发代码访问充值地址、对比游戏连续运行图、源代码等方式，将被侵权的事实予以固定，并将相关证据移交侦查机关。

（二）向专业人员借力，破解网络犯罪侦破难。《歪歪神武》运营者刻意将私服架设、游戏运维、玩家充值、结算等各个环节隔断，相互间以虚拟身份联络，侦查一度陷入困境。

检察官提前介入引导侦查，充分运用专家智库，向相关专业人士咨询源代码应用、内测修复等问题，扫除技术盲点，同时，会同侦查人员通过技术手段从聊天记录中获知《歪歪神武》整体运作流程、资金流向以及人物关系。

（三）巧妙运用关联证据，破解跨境取证难。《歪歪神武》运营者至泰国租用位于韩国的服务器用于架设、运维私服游戏，又通过远程控制软件 TeamViewer 经香港、台湾服务器跳转实现后台控制。案发后，该私服游戏停止运营，涉案的电脑等设备被丢弃在境外。针对实物证据难以收集的问题，检察官从大量电子证据入手，通过其他关联证据构建完整的证据体系，结合被告人供述、酒店订单、论坛广告等证据，论证被告人的主观犯意。串联 QQ 群信息、域名回访、玩家证言等证据，核实被告人的客观行为。从数千条聊天记录和转账记录中锁定违法所得，明确犯罪数额。最终本案在境内完成了取证工作，破解了跨境取证难题，有力指控了犯罪。

（四）准确适用法律，破解链条打击难。一是追诉关联犯罪。在办理被告人龙小卫、李勃涉嫌侵犯著作权案过程中，检察官细致审查《歪歪神武》上下游产业的证据，发现被告人程刚有帮助《歪歪神武》完成支付结算的行为，遂向侦查机关制发《应当逮捕犯罪嫌疑人通知书》，对涉嫌单位犯罪的机械牛网络科技（苏州）有限公司也及时进行追诉。同时，检察官通过筛查交易记录，确认本案的犯罪数额为 362 万余元，比最初认定的犯罪数额增加了 300 多万元，做到了罚当其罪。二是依法准确定性。检察官认为本案被告人龙小卫、李勃利用计算机和互联网通过境外服务器传播网络游戏，应当认定为刑法上的复制发行行为。而被告人程刚及其公司虽然明知运维私服游戏是违法犯罪行为，但对运维游戏私服具体是否侵犯著作权、侵犯商业秘密、非法经营或其他信息网络类犯罪并不明确，认定程刚及其公司涉嫌帮助信息网络犯罪活动罪更为准确。检察官的上述意见获得法院认可。三是善用认罪认罚规定。本案如被告人认罪，将有利于庭审顺利推进，取得较好的庭审效果。为此，检察官在讯问被告人时向被告人开示案件证据、宣讲法律政策，促使被告人当庭认罪伏法。

3.最高人民检察院第二十六批指导性案例之三：陈力等八人侵犯著作权案（检例第 100 号）

【关键词】

网络侵犯视听作品著作权 未经著作权人许可 引导侦查 电子数据

【要旨】

办理网络侵犯视听作品著作权犯罪案件，应注意及时提取、固定和保全相关电子数据，并围绕客观性、合法性、关联性要求对电子数据进行全面审查。对涉及众多作品的案件，在认定“未经著作权人许可”时，应围绕涉案复制品是否系非法出版、复制发行且被告人能否提供获得著作权人许可的相关证明材料进行审查。

【基本案情】

被告人陈力，男，1984 年生，2014 年 11 月 10 日因犯侵犯著作权罪被安徽省合肥市高新技术开发区人民法院判处有期徒刑七个月，罚金人民币十五万元，2014 年 12 月 25 日刑满释放。

被告人林崟等其他 7 名被告人基本情况略。

2017 年 7 月至 2019 年 3 月，被告人陈力受境外人员委托，先后招募被告人林崟、赖冬、严杰、杨小明、黄亚胜、吴兵峰、伍健兴，组建 QQ 聊天群，更新维护“www.131zy.net”“www.zuikzy.com”等多个盗版影视资源网站。其中，陈力负责发布任务并给群内其他成员发放报酬；林崟负责招募部分人员、培训督促其他成员完成工作任务、统计工作量等；赖冬、严杰、杨小明等人通过从正版网站下载、云盘分享等方式获取片源，通过云转码服务器进行切片、转码、增加赌博网站广告及水印、生成链接，最后将该链接复制粘贴至上述盗版影视资源网站。其间，陈力收到境外人员汇入的盗版影视资源网站运营费用共计 1250 万余元，

各被告人从中获利 50 万至 1.8 万余元不等。

案发后，公安机关从上述盗版影视网站内固定、保全了被告人陈力等人复制、上传的大量侵权影视作品，包括《流浪地球》《廉政风云》《疯狂外星人》等 2019 年春节档电影。

【检察机关履职情况】

审查逮捕 2019 年春节，《流浪地球》等八部春节档电影在院线期间集体遭高清盗版，盗版电影通过各种途径流入网络。上海市人民检察院第三分院（以下简称上海三分院）应公安机关邀请介入侦查，引导公安机关开展取证固证工作。一是通过调取和恢复 QQ 群聊天记录并结合各被告人到案后的供述，查明陈力团伙系共同犯罪，确定各被告人对共同实施的运营盗版影视资源网站行为的主观认知。二是联系侵权作品较为集中的美日韩等国家的著作权集体管理组织，由其出具涉案作品的版权认证文书。2019 年 4 月 8 日，公安机关对陈力团伙中的 8 名被告人提请逮捕，上海三分院依法批准逮捕。

审查起诉 2019 年 8 月 29 日，上海市公安局以被告人陈力等人涉嫌侵犯著作权罪向上海三分院移送起诉。本案涉及的大量影视作品涵盖电影、电视剧、综艺、动漫等多种类型，相关著作权人分布国内外。收集、审查是否获得权利人许可的证据存在难度。为进一步夯实证据基础，检察机关要求公安机关及时向国家广播电视总局调取“信息网络传播视听节目许可证”持证机构名单，以证实被告人陈力操纵的涉案网站均系非法提供网络视听服务的网站。同时，要求公安机关对陈力设置的多个网站中相对固定的美日韩剧各个版块，按照从每个网站下载 300 部的均衡原则抽取了 2425 部作品，委托相关著作权认证机构出具权属证明，证实抽样作品均系未经著作权人许可的侵权作品，且陈力等网站经营者无任何著作权人许可的相关证明材料。在事实清楚、证据确实、充分的基础上，8 名被告人在辩护人或值班律师的见证下均自愿认罪认罚，接受检察机关提出的有期徒刑十个月至四年六个月不等、罚金 2 万元至 50 万元不等的确定刑量刑建议，并签署了认罪认罚具结书。

2019 年 9 月 27 日，上海三分院以被告人陈力等 8 人构成侵犯著作权罪向上海市第三中级人民法院（以下简称上海三中院）提起公诉。

指控与证明犯罪 2019 年 11 月 15 日，上海三中院召开庭前会议，检察机关及辩护人就举证方式、鉴定人出庭、非法证据排除等事项达成共识，明确案件事实、证据和法律适用存在的分歧。同年 11 月 20 日，本案依法公开开庭审理。8 名被告人及其辩护人对指控的罪名均无异议，但对本案非法经营数额的计算提出各自辩护意见。陈力的辩护人提出，陈力租借服务器的费用及为各被告人发放的工资应予扣除，其他辩护人提出应按照各被告人实得报酬计算非法经营数额。此外，本案辩护人均提出境外人员归案后会对各被告人产生影响，应当对各被告人适用缓刑。公诉人对此答辩：第一，通过经营盗版资源网站的方式侵犯著作权，其网站经营所得即为非法经营数额，租借服务器以及用于发放各被告人的报酬等支出系犯罪成本，不应予以扣除。公诉机关按照各被告人加入 QQ 群以及获取第一笔报酬的时间，认定各被告人参与犯罪的起始时间，并结合对应期间网站的整体运营情况，计算出各被告人应承担的非法经营数额，证据确实、充分。第二，本案在案证据已能充分证实各被告人实施了共同犯罪及其在犯罪中所起的作用，按照相关法律和司法解释规定，境外人员是否归案不影响各被告人的量刑。第三，本案量刑建议是根据各被告人的犯罪事实、证据、法定酌定情节、社会危害性等因素综合判定，并经各被告人具结认可，而且本案侵权作品数量多、传播范围广、经营时间长，具有特别严重情节，且被告人陈力在刑罚执行完毕后五年内又犯应当判处有期徒刑以上刑罚之罪，构成累犯，故不应适用缓刑。合议庭采纳了公诉意见和量刑建议。

处理结果 2019 年 11 月 20 日，上海三中院作出一审判决，以侵犯著作权罪分别判处被告人陈力等 8 人有期徒刑十个月至四年六个月不等，各处罚金 2 万元至 50 万元不等。判决宣告后，被告人均未提出上诉，判决已生效。

【指导意义】

（一）充分发挥检察职能，依法惩治网络侵犯视听作品著作权犯罪，切实维护权利人合法权益

依法保护著作权是国家知识产权战略的重要内容。检察机关坚决依法惩治侵犯著作权犯罪，尤其是注重惩治网络信息环境下的侵犯著作权犯罪。网络环境下侵犯视听作品著作权犯罪具有手段日益隐蔽、组织分工严密、地域跨度大、证据易毁损和隐匿等特点，且日益呈现高发多发态势，严重破坏网络安全与秩序，应予严惩。为准确指控和证明犯罪，检察机关在适时介入侦查、引导取证时，应注意以下方面：一是提取、固定和保全涉案网站视频链接、链接所指向的视频文件、涉案网站影视作品目录、涉案网站视频播放界面；二是固定、保全涉案网站对应的云转码服务器后台及该后台中的视频链接；三是比对确定云转码后台形成的链接与涉案网站播放的视频链接是否具有同一性；四是对犯罪过程中涉及的多个版本盗版影片，技术性地针对片头片中片尾分别进行作品的同一性对比。

（二）检察机关办理网络侵犯著作权犯罪案件，应围绕电子数据的客观性、合法性和关联性进行全面审查，依法适用认罪认罚从宽制度，提高办案质效

网络环境下侵犯著作权犯罪呈现出跨国境、跨区域以及智能化、产业化特征，证据多表现为电子数据且难以获取。在办理此类案件时，一方面要着重围绕电子数据的客观性、合法性和关联性进行全面审查，区分不同类别的电子数据，采取有针对性的审查方法，特别要注意审查电子数据与案件事实之间的多元关联，综合运用电子数据与其他证据，准确认定案件事实。另一方面，面对网络犯罪的复杂性，检察机关要注意结合不同被告人的地位与作用，充分运用认罪认罚从宽制度，推动查明犯罪手段、共犯分工、人员关系、违法所得分配等案件事实，提高办案效率。

（三）准确把握“未经著作权人许可”的证明方法

对于涉案作品种类众多且权利人分散的案件，在认定“未经著作权人许可”时，应围绕涉案复制品是否系非法出版、复制发行，被告人能否提供获得著作权人许可的相关证明材料予以综合判断。为证明涉案网站系非法提供网络视听服务的网站，可以收集“信息网络传播视听节目许可证”持证机构名单等证据，补强对涉案复制品系非法出版、复制发行的证明。涉案侵权作品数量众多时，可进行抽样取证，但应注意审查所抽取的样本是否具有代表性、抽样范围与其他在案证据是否相符、抽样是否具备随机性等影响抽样客观性的因素。在达到追诉标准的侵权数量基础上，对抽样作品提交著作权人进行权属认证，以确认涉案作品是否均系侵权作品。

【相关规定】

《中华人民共和国刑法》第二百一十七条

《中华人民共和国著作权法》第十条

《中华人民共和国刑事诉讼法》第十五条

《音像制品管理条例》第三条

《计算机信息网络国际互联网安全保护管理办法》第五条

《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》第五条、第十一条

《最高人民法院、最高人民检察院、公安部关于办理侵犯知识产权刑事案件适用法律若干问题的意见》第十一条、第十五条

《人民检察院刑事诉讼规则》第二百五十二条

4.2020年度浙江法院十大知识产权案件之九：蔡韩羿、吴承林、张少华侵犯著作权罪案

(2019)浙0106刑初788号

【入选理由】

随着信息网络的发展，互联网已成为传播盗版影视作品的主要渠道，大量电影刚刚上映就出现资源泄露，盗版电影通过微信、微博、视频APP等途径广泛传播，严重损害了电影作品权利人的合法利益，对我国电影产业的发展造成不良影响。本案中，法院依法严厉打击通过信息网络传播盗版电影的著作权犯罪行为，体现了加大知识产权刑事司法保护力度的价值导向，切实维护了著作权人的合法权益。

【案情介绍】

2018年7月始，吴承林以营利为目的，建立多个影视资源微信群，共吸纳会员3800余人，并在未经著作权人许可的情况下，向会员传播《流浪地球》《飞驰人生》《疯狂的外星人》《新喜剧之王》《神探蒲松龄》《熊出没?原始时代》《廉政风云》等多部影视作品。

2019年2月5日至6日期间，张少华通过付费成为吴承林建立的影视资源微信群的会员并获取了上述影片，并于同月6日至7日期间将上述影片提供给“麻花影视”APP，获得1000“麻花币”奖励。“麻花影视”APP在获得上述影片遂后向其会员播放。蔡韩羿在明知“麻花影视”APP侵犯他人著作权的情况下，作为“麻花影视”APP工作人员，从事APP客服以及APP运营、编辑工作。

截至2019年2月14日，“麻花影视”APP累计传播700余部未经著作权人许可的影视作品。截至同年2月12日，《流浪地球》的点击播放量为526.25万，《飞驰人生》的点击播放量为255.93万，《疯狂的外星人》的点击播放量为332.58万，《熊出没?原始时代》的点击播放量为109.79万，《廉政风云》的点击播放量为75.69万。

杭州市西湖区人民检察院指控蔡韩羿、吴承林、张少华犯侵犯著作权罪，向杭州市西湖区人民法院提起公诉。

【裁判内容】

杭州市西湖区人民法院经审理认为：蔡韩羿、张少华、吴承林以营利为目的，未经著作权人许可，复制发行他人电影作品，其行为已构成侵犯著作权罪。其中，张少华为了获取利益，明知“麻花影视”APP的获利方式来源于广告或植入的游戏，仍提供盗版影片给该款APP，蔡韩羿作为“麻花影视”APP的工作人员，明知“麻花影视”APP侵犯他人著作权，仍从事客服、运营等工作，故张少华与蔡韩羿构成共同犯罪。“麻花影视”APP中《流浪地球》等影片点击量高达数十万至数百万，蔡韩羿与张少华均属于情节特别严重，吴承林情节严重。张少华在共同犯罪中起次要作用，系从犯，故对张少华予以减轻处罚。三被告人到案后均如实供述罪行，故均予以从轻处罚。三被告人自愿认罪认罚，故均予以从宽处罚。综上，该院于2020年12月14日判决：蔡韩羿犯侵犯著作权罪，判处有期徒刑三年，并处罚金20万元；吴承林犯侵犯著作权罪，判处有期徒刑二年二个月，并处罚金10万元；张少华犯侵犯著作权罪，判处有期徒刑二年，并处罚金3万元；扣押在案的吴承林的手机1部、张少华的手机1部予以没收。

宣判后，各被告人均未提出上诉，一审判决已发生法律效力。

【裁判要旨】

以营利为目的，未经著作权人许可，复制发行其文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品，违法所得数额较大或者有其他严重情节的，构成侵犯著作权罪。通

过信息网络实施上述行为的，可以根据传播他人作品的实际被点击次数，或根据以会员制方式传播他人作品的注册会员的人数等，认定属于刑法第二百一十七条规定的“其他严重情节”或“其他特别严重情节”。

5.2020年度北京市检察机关知识产权保护典型案例之七：尹某某、张某某侵犯著作权案

(2020)京0105刑初1821号

【案件事实】

北京某科技有限公司为制作、开发手机游戏软件的公司，因业务亏损严重于2018年初停止经营，尹某某、张某某曾为该公司员工，二人在离职时以拖欠工资为由将公司用于开发游戏软件的电脑、测试用手机等私自拿回家中，经劳动仲裁和法院调解解决劳资纠纷后一直未归还公司。2018年5月至2019年10月间，尹某某、张某某租用阿里云服务器，将私自保管的游戏软件调试后上线运营，通过专门从事帮助联系发行渠道的董某、王某某（经追捕并另案起诉，已判决），将游戏软件上传至手机应用的分发平台，宣传、推广游戏供用户下载、充值，非法经营额共计人民币30余万元。经鉴定，尹某某、张某某复制发行的游戏软件与公司的3D贴图模型资源、文字、音频等文件绝大部分一致。董某、王某某在明知他人以营利为目的，复制、发行侵权软件的情况下提供帮助，分别收取2万余元、5万余元好处费。尹某某、张某某于2020年1月15日被公安机关抓获归案。

【履职过程】

2020年9月5日，朝阳区检察院以被告人尹某某、张某某犯侵犯著作权罪向朝阳区法院提起公诉。2020年11月27日，朝阳区法院判处两名被告人犯侵犯著作权罪，被告人张某某被判处有期徒刑三年，并处罚金人民币十二万元；被告人尹某某被判处有期徒刑二年六个月，并处罚金十万元。被告人尹某某、张某某分别退缴在案的八万元、十万元，发还被害单位。一审判决宣告后，两名被告人均上诉，后北京市第三中级人民法院裁决驳回二名被告人上诉、维持原判，现判决已生效。

【评析意见】

本案是一起离职员工将原公司所有的游戏软件私自复制、发行，架设服务器运营的侵犯著作权案件，具有代码与多媒体资源鉴定复杂，电子数据提取、固定困难，被告人无罪辩解多等特点，朝阳区检察院全面收集证据，依法追加漏罪、漏犯，有力地指控犯罪行为，强化释法说理促成赔偿，切实履行知识产权保护职责。

1.重点破解电子数据取证难点。

为解决电子数据取证难、利用信息技术实施的犯罪成案率低的问题，朝阳区检察院高度重视，引导公安机关根据侵权游戏下载网站线索委托鉴定，对被告人上传的侵权游戏软件客户端提取、鉴定，并通过追捕同案犯、查找上游发行渠道公司等，对调取的数据与犯罪行为之间的关联性进行补强。

2.依法准确认定犯罪性质。

被告人私自使用工作中接触到的公司游戏软件，包括源代码、多媒体资源等，未经权利人许可，以营利为目的，简单修改后私自架设服务器运营，其行为同时涉嫌侵犯商业秘密和侵犯著作权，虽然按照行为时法律规定，未达到侵犯商业秘密罪的立案追诉标准，但仍可以以侵

犯著作权罪认定。在综合考虑犯罪情节、主观动机、行为手段及两个罪名的法定刑等因素后，检察机关以侵犯著作权罪提起公诉。

3.促成被告人主动赔偿权利人损失。

检察官认真分析在案证据，对权利公司提供的相关线索核实后，认定本案非法经营数额为30万元。权利公司最初表示拒不谅解被告人。经过充分的释法说理，被告人尹某某主动退赔权利人损失，权利人亦出具谅解书。庭审过程中，被告人张某某亦主动退赔。权利公司在案发前因严重亏损，有多起正在被强制执行的民事案件，通过挽回损失，也有利于其偿还债务。

6.检察机关知识产权综合性司法保护典型案例之一：大某视界文化传媒有限公司、张某等四人侵犯著作权案

【关键词】

网络侵犯著作权　平等保护　行刑衔接　企业合规

【要　旨】

信息化时代，检察机关要加大对网络侵犯著作权行为的惩治力度，依法平等保护境内外著作权人的合法权利。推动建立健全行政执法与刑事司法衔接机制，积极发挥法律监督在“行刑衔接”中的作用。结合办案推动行业治理，促进企业合规经营。

一、案件事实

2017年5月，大某视界文化传媒有限公司（以下简称大某视界公司）成立，张某和李某负责公司日常经营管理，刘某、马某绿为该公司内容制作部主管。2018年5月，大某视界公司开发了名为“大某视界”的视频播放App上线运行。该程序上线后，大某视界公司未经权利人许可，由刘某、马某绿组织部门人员下载、编辑大量境内外影片，通过视频App提供给用户观看，并以收取会员费的方式牟利。2020年1月10日，公安机关将张某等四人抓获。经对后台数据进行提取和鉴定：“大某视界”App编辑、上传的侵权影片中，包括美国电影协会成员公司享有版权的作品302部，用户观看42万余次，下载1.9万余次；腾讯公司享有版权的作品70部，用户观看8.1万余次，下载4千余次。“大某视界”App共有注册用户83万余个，充值支付订单9万余个，支付金额人民币140余万元。

二、检察机关履职情况

2019年12月，广东省深圳市市场稽查局执法中发现“大某视界”App可能涉嫌刑事犯罪，向深圳市南山区人民检察院（以下简称南山区检察院）通报相关情况，南山区检察院启动行政执法与刑事司法衔接工作机制。2020年1月，深圳市市场稽查局将该线索移送深圳市公安局南山分局，南山区检察院及时介入侦查，引导公安机关取证。2020年2月13日，南山区检察院以涉嫌侵犯著作权罪对张某等四人批准逮捕，并提出继续侦查意见。

2020年3月30日，公安机关将该案移送南山区检察院审查起诉。2020年4月29日，南山区检察院以侵犯著作权罪对大某视界公司以及张某、李某、刘某、马某绿等四人提起公诉。

2020年11月11日，深圳市南山区人民法院以侵犯著作权罪判处被告单位大某视界公司罚金人民币四十万元，判处被告人张某等四人有期徒刑一年至三年不等，并处罚金人民币两万元至十万元不等。部分被告人不服一审判决提出上诉。2021年3月11日，深圳市中级

人民法院裁定驳回上诉，维持原判。

三、典型意义

（一）依法打击网络侵犯著作权犯罪，平等保护境内外著作权人的合法权利。随着信息网络技术的快速发展，作品的传播更加便捷迅速，一些不法分子借助互联网实施侵犯著作权违法犯罪行为，不仅破坏社会主义市场经济秩序，也给权利人的合法权益造成损害，应当依法惩治。按照《伯尔尼公约》和我国著作权法的规定，涉案外国影视作品受我国法律保护。本案中检察机关秉持平等保护理念，加强对境内外权利人著作权的刑事司法保护，切实维护创作者、传播者、使用者的合法权利。

（二）完善知识产权“行刑衔接”机制，形成保护知识产权合力。为畅通衔接渠道，解决信息不畅、“以罚代刑”等问题，南山区检察院会同相关部门，建立健全知识产权案件“行刑衔接”工作机制。对于涉嫌犯罪的疑难复杂知识产权案件，有关部门商请检察机关提前介入的，南山区检察院主动作为，依法提出法律适用意见，强化引导取证。在案件受理后，及时向行政执法机关通报案件处理进展情况，对案件办理中发现的共性问题进行梳理反馈，形成全方位保护知识产权合力。

（三）积极推动行业治理，促使企业合规经营。南山区检察院积极发挥职能，促使涉案企业剥离违法业务，进行全面合规整改。大某视界公司完善了法律风险防控机制，将 App 中侵权内容全部删除，并发布公告通报侵权情况，对充值用户进行退费，组织专门团队开展版权购买谈判。检察机关落实“谁执法谁普法”的普法责任制，会同深圳市版权协会，结合案例有针对性开展知识产权刑事合规宣讲，引导更多企业合法合规经营。

（四）侮辱罪

1.典型案例：人肉搜索致人死亡--被告人蔡晓青构成侮辱罪

一、案情介绍

广东省陆丰市人民法院经公开审理查明：被告人蔡晓青因怀疑徐某在蔡的”服装店试衣服时偷了一件衣服，将徐某在该店的视频截图配上“穿花花衣服的是小偷”等字幕后，上传到其新浪微博上，并以求“人肉搜索”等方式对徐某进行侮辱。之后，徐某因不堪受辱而自杀。案发后，蔡的父母与徐某父母达成和解协议，蔡父母一次性赔偿徐某父母 12 万元，徐某父母出具谅解书，请求对蔡晓青从轻处罚。

陆丰市人民法院认为，被告人因怀疑徐某在其经营的服装店试衣服时偷了一件衣服，在该店的视频截图配上“穿花花衣服的是小偷”等字幕后，上传到其新浪微博上，公然对她人进行侮辱，致徐某因不堪受辱跳水自杀，情节严重，其行为构成侮辱罪。案发后被告人亲属与被害人亲属达成调解协议，被告人亲属对被害人亲属的经济损失进行赔偿，取得被害人家属的谅解。被告人当庭认罪，确有悔罪表现，依法可以从轻处罚。根据被告人的犯罪事实、情节及对社会的危害程度，依照《刑法》第 246 条之规定，陆丰市人民法院以侮辱罪判处被告人蔡晓青有期徒刑一年。

一审宣判后，被告人不服，向汕尾市中级人民法院提起上诉,提出其发微博的行为属于正常寻人，不构成犯罪；没有足够证据证明其行为与徐某的自杀行为之间存在因果关系；一审法院量刑过重。其辩护人提出，一审法院认定本案可以提起公诉，属于程序不当，适用法律错误。一审认定上诉人犯侮辱罪的证据不足。

汕尾市中级人民法院经审理认为，肯定上诉人的行为构成侮辱罪；同时，上诉人利用网络侮辱他人，造成的影响大，范围广，并造成了被害人死亡的严重后果，属于严重危害社会秩序，陆丰市人民检察院提起公诉并无不当。从而裁定驳回上诉，维持原判。

二、专家释法

在本案的案情介绍中涉及一个名词“人肉搜索”，这也是被告人涉案行为中的重要部分。确实，“人肉搜索”并非一个规范的汉语表达，各种辞书中均未收录。不过可以肯定的是，人肉搜索现象是伴随着网络技术发展而出现的一种寻找具体的人和线索的途径，其在带来巨大便利的同时，也总是和网络暴力相伴而生。“一方面因为其可能通过网络公开了特定人的信息，而这些信息多涉及隐私，另一方面则是特定人隐私等信息被网络公开后所产生的名誉受损的可能。” 本案首先如何认定“人肉搜索”致人自杀死亡的行为性质。

有学者进一步将人肉搜索行为细分为两大类，单纯公开隐私型与损害名誉型。这样来看，本案之中行为人的行为显然不仅仅是公开他人隐私，其在并无确切证据的情况下所发布的“穿花花衣服的是小偷”等用语，具有明显的损害名誉的属性。进一步说，虽然被害人徐某的父亲认为蔡晓青发微博进行“人肉搜索”指责其女儿是偷衣服的小偷属于无中生有，但由于徐某已逝，无法查清其是否有盗窃行为，从“事实存疑有利于被告”的原则出发，就不能认定蔡晓青有捏造、虚构事实的行为，故其不构成诽谤罪。

本案中，被告人把被害人购物的视频监控截图发到微博上，且明确指明徐某是小偷并要求“人肉搜索”，本质上属于公然侮辱他人人格的行为。“人肉搜索”具有强烈的放大功能，当被搜索的人和某个具有消极影响的事件联系在一起时，被搜索人的品德、才干、信誉等在社会中所获得的评价明显降低，致使当事人的名誉权受到严重损害。就此而言，认为蔡晓青发微博要求“人肉搜索”的行为属于侮辱行为，符合刑法中侮辱行为的本质。

再者，本案中，被告人认为其发微博的行为是正常的网络寻人行为，现有证据只能说明其行为和被害人的自杀结果在时间上有先后关系，无法直接证明二者存在刑法上的因果关系。但是在裁判者看来，从蔡晓青的行为来看，其不仅发布微博称“穿花花衣服的是小偷。求人肉，经常带只博美小狗逛街。麻烦帮忙转发”，还附上徐某购物时的多张监控视频截图。该微博发出仅一个多小时，网友迅即展开的“人肉搜索”就将徐某的个人信息，包括姓名、所在学校、家庭住址和个人照片全部曝光，蔡又把这些信息在微博上曝光。一时间，在网络上对徐某的各种批评甚至辱骂开始蔓延。从蔡要求“人肉搜索”的第一条微博发布，到第二天晚上徐某在河边发出最后一条微博后自杀，仅持续了 20 多个小时。多名证人证言证实，这次微博事件对被害人伤害很大，明显感觉徐某情绪低落。徐某作为一个尚未步入社会、生活在经济不发达小镇的在校未成年少女，面对“人肉搜索”的网络放大效应及众多网民先人为主的道德审判，对未来生活产生极端恐惧，最终导致了自杀身亡的严重后果，故蔡晓青发微博的行为与徐某的自杀具有刑法上的因果关系。此外，被害人不堪“人肉搜索”受辱而跳河自杀身亡，明显属于侮辱罪所要求的“情节严重”的情形。

2.最高人民检察院第三十四批指导性案例（2022.02.21）

案例一、仇某侵害英雄烈士名誉、荣誉案（检例第 136 号）

【关键词】

侵害英雄烈士名誉、荣誉　情节严重　刑事附带民事公益诉讼

【要旨】

侵害英雄烈士名誉、荣誉罪中的“英雄烈士”，是指已经牺牲、逝世的英雄烈士。在同一案件中，行为人所侵害的群体中既有烈士，又有健在的英雄模范人物时，应当整体评价为侵害英雄烈士名誉、荣誉的行为，不宜区别适用侵害英雄烈士名誉、荣誉罪和侮辱罪、诽谤罪。《刑法修正案（十一）》实施后，以侮辱、诽谤或者其他方式侵害英雄烈士名誉、荣誉的行为，情节严重的，构成侵害英雄烈士名誉、荣誉罪。行为人利用信息网络侵害英雄烈士名誉、荣誉，引起广泛传播，造成恶劣社会影响的，应当认定为“情节严重”。英雄烈士没有近亲属或者近亲属不提起民事诉讼的，检察机关在提起公诉时，可以一并提起附带民事公益诉讼。

【基本案情】

被告人仇某，男，1982年出生，南京某投资管理有限公司法定代表人。

2020年6月，印度军队公然违背与我方达成的共识，悍然越线挑衅。在与之交涉和激烈斗争中，团长祁发宝身先士卒，身负重伤；营长陈红军、战士陈祥榕突入重围营救，奋力反击，英勇牺牲；战士肖思远突围后义无反顾返回营救战友，战斗至生命最后一刻；战士王焯冉在渡河支援途中，拼力救助被冲散的战友脱险，自己却淹没在冰河中。边防官兵誓死捍卫祖国领土，彰显了新时代卫国戍边官兵的昂扬风貌。同年6月，陈红军、陈祥榕、肖思远、王焯冉被评定为烈士；2021年2月，中央军委追授陈红军“卫国戍边英雄”荣誉称号，追记陈祥榕、肖思远、王焯冉一等功，授予祁发宝“卫国戍边英雄团长”荣誉称号。

2021年2月19日上午，仇某在卫国戍边官兵英雄事迹宣传报道后，为博取眼球，获得更多关注，在住处使用其新浪微博账号“辣笔小球”（粉丝数250余万），先后发布2条微博，歪曲卫国戍边官兵祁发宝、陈红军、陈祥榕、肖思远、王焯冉等人的英雄事迹，诋毁、贬损卫国戍边官兵的英雄精神。

上述微博在网络上迅速扩散，引起公众强烈愤慨，造成恶劣社会影响。截至当日15时30分，仇某删除微博时，上述2条微博共计被阅读202569次、转发122次、评论280次。

【检察履职情况】

（一）引导侦查取证

2021年2月20日，江苏省南京市公安局建邺分局对仇某以涉嫌寻衅滋事罪立案侦查并刑事拘留。当日，江苏省南京市建邺区人民检察院经公安机关商请介入侦查，围绕犯罪对象、动机、情节、行为方式及造成的社会影响等方面提出收集证据的意见，并同步开展公益诉讼立案调查。

（二）审查逮捕

2021年2月25日，建邺分局以仇某涉嫌寻衅滋事罪提请批准逮捕。3月1日，建邺区人民检察院以仇某涉嫌侵害英雄烈士名誉、荣誉罪批准逮捕。检察机关认为：首先，仇某发布微博，以戏谑口吻贬损英雄团长“临阵脱逃”，并提出四名战士因为营救团长而牺牲、立功，质疑牺牲人数、诋毁牺牲战士的价值，侵害了祁发宝等整个战斗团体的名誉、荣誉，根据刑法第二百九十三条、《最高人民法院、最高人民检察院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》（以下简称《网络诽谤的解释》）第五条的规定，已涉嫌寻衅滋事罪；其次，仇某的行为符合3月1日实施的《刑法修正案（十一）》增设的侵害英雄烈士名誉、荣誉罪的规定，根据刑法第十二条规定的“从旧兼从轻”原则，应当按《刑法修正案（十一）》处理；再次，仇某作为有250余万粉丝的微博博主，在国家弘扬卫国戍边官兵英雄事迹的特定时间节点实施上述行为，其言论在网络迅速、广泛扩散，造成恶劣社会影响，应当认定为“情节严重”。

（三）审查起诉

2021年3月11日，建邺分局以仇某涉嫌侵害英雄烈士名誉、荣誉罪移送审查起诉。因本案系新罪名案件，没有类案和量刑指导意见供参考，建邺区人民检察院在依法审查证据、认定事实基础上，邀请不同职业、年龄、文化程度的群众参加听证，就量刑问题听取意见，并对仇某依法开展认罪认罚教育工作。仇某认罪认罚，同意量刑建议和程序适用，在辩护人见证下自愿签署具结书。

4月26日，建邺区人民检察院以仇某涉嫌侵害英雄烈士名誉、荣誉罪提起公诉，提出有期徒刑八个月的量刑建议。同时，检察机关就公益诉讼听取祁发宝和烈士近亲属的意见，他们提出希望检察机关依法办理。检察机关遂提起附带民事公益诉讼，请求判令仇某在国内主要门户网站及全国性媒体公开赔礼道歉、消除影响。

（四）指控与证明犯罪

2021 年 5 月 31 日，江苏省南京市建邺区人民法院依法公开开庭审理本案。仇某对检察机关指控的事实、证据及量刑建议均无异议，当庭再次表示认罪认罚，真诚向英雄烈士及其家属道歉，向社会各界忏悔。辩护人对指控罪名不持异议，认为仇某主观恶性较小，发布的微博虽多次发酵，但绝大多数网友对仇某的观点是不赞同的，造成的不良影响较小。公诉人答辩指出，仇某作为具有媒体从业经历的“网络大 V”，恶意用游戏术语诋毁、贬损卫国戍边官兵，主观恶性明显。其微博账户拥有 250 余万粉丝，其不当言论在网络上迅速扩散、蔓延，网友对其口诛笔伐，恰恰说明其言论严重伤害民众情感，损害社会公共利益。

公益诉讼起诉人出示证据，证明仇某的行为、后果，发表了公益诉讼的意见。仇某及其诉讼代理人对检察机关提起刑事附带民事公益诉讼的事实、证据及诉讼请求均无异议。

（五）处理结果

建邺区人民法院审理后当庭宣判，采纳检察机关指控的事实、罪名及量刑建议，支持检察机关的公益诉讼，以仇某犯侵害英雄烈士名誉、荣誉罪判处有期徒刑八个月，并责令仇某自判决生效之日起十日内通过国内主要门户网站及全国性媒体公开赔礼道歉，消除影响。判决宣告后，仇某未提出上诉，判决已生效。2021 年 6 月 25 日，仇某在《法治日报》及法制网发布道歉声明。

【指导意义】

（一）对侵害英雄烈士名誉、荣誉罪中的“英雄烈士”应当依照刑法修正案的本意作适当解释。本罪中的“英雄烈士”，是指已经牺牲、逝世的英雄烈士。如果行为人以侮辱、诽谤或者其他方式侵害健在的英雄模范人物名誉、荣誉，构成犯罪的，可以适用侮辱罪、诽谤罪追究刑事责任。但是，如果在同一案件中，行为人的行为所侵害的群体中既有已牺牲的烈士，又有健在的英雄模范人物时，应当整体评价为侵害英雄烈士名誉、荣誉的行为，不宜区别适用侵害英雄烈士名誉、荣誉罪和侮辱罪、诽谤罪。虽不属于烈士，但事迹、精神被社会普遍公认的已故英雄模范人物的名誉、荣誉被侵害的，因他们为国家、民族和人民作出巨大贡献和牺牲，其名誉、荣誉承载着社会主义核心价值观，应当纳入侵害英雄烈士名誉、荣誉罪的犯罪对象，与英雄烈士的名誉、荣誉予以刑法上的一体保护。

（二）《刑法修正案（十一）》实施后，侮辱、诽谤英雄烈士名誉、荣誉，情节严重的，构成侵害英雄烈士名誉、荣誉罪。《刑法修正案（十一）》实施前，实施侮辱、诽谤英雄烈士名誉、荣誉的行为，构成犯罪的，可以按照寻衅滋事罪追究刑事责任。《刑法修正案（十一）》实施后，对上述行为认定为侵害英雄烈士名誉、荣誉罪，符合立法精神，更具有针对性，更有利于实现对英雄烈士名誉、荣誉的特殊保护。发生在《刑法修正案（十一）》实施前的行为，实施后尚未处理或者正在处理的，应当根据刑法第十二条规定的“从旧兼从轻”原则，以侵害英雄烈士名誉、荣誉罪追究刑事责任。

（三）侵害英雄烈士名誉、荣誉罪中“情节严重”的认定，可以参照《网络诽谤的解释》的规定，并可以结合案发时间节点、社会影响等综合认定。《网络诽谤的解释》第二条规定，同一诽谤信息实际被点击、浏览次数达到 5000 次以上，或者被转发次数达到 500 次以上的；造成被害人或者其近亲属精神失常、自残、自杀等严重后果的；二年内曾因诽谤受过行政处罚，又诽谤他人的；具有其他情节严重的情形的，属于“情节严重”。办理利用信息网络侵害英雄烈士名誉、荣誉案件时，可以参照上述标准，或者虽未达到上述数量、情节要求，但在特定时间节点通过具有公共空间属性的网络平台和媒介公然侵害英雄烈士名誉、荣誉，引起广泛传播，造成恶劣社会影响的，也可以认定为“情节严重”。对于只是在相对封闭的网络空间，如在亲友微信群、微信朋友圈等发表不当言论，没有造成大范围传播的，可以不认定为“情节严重”。

（四）刑事检察和公益诉讼检察依法协同履职，维护社会公共利益。检察机关办理侵

害英雄烈士名誉、荣誉案件，在英雄烈士没有近亲属，或者经征询意见，近亲属不提出民事诉讼时，应当充分履行刑事检察和公益诉讼检察职能，提起公诉的同时，可以向人民法院一并提起附带民事公益诉讼，同步推进刑事责任和民事责任的追究，实现审判阶段刑事诉讼、附带民事公益诉讼由人民法院同一合议庭审理、同步判决，提高诉讼效率、确保庭审效果。

【相关规定】

《中华人民共和国刑法》第十二条、第二百九十九条之一

《中华人民共和国民法典》第一百八十五条

《中华人民共和国英雄烈士保护法》第二十二条、第二十五条、第二十六条

《中华人民共和国国家勋章和国家荣誉称号法》第二条、第三条、第四条

《国家功勋荣誉表彰条例》第一条、第二条、第五条、第六条、第七条、第八条、第十四条

《最高人民法院、最高人民检察院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》第二条、第五条

《最高人民法院、最高人民检察院关于检察公益诉讼案件适用法律若干问题的解释》第二十条

案例二、郎某、何某诽谤案（检例第 137 号）

【关键词】

网络诽谤　严重危害社会秩序　能动司法　自诉转公诉

【要旨】

利用信息网络诽谤他人，破坏公众安全感，严重扰乱网络社会秩序，符合刑法第二百四十六条第二款“严重危害社会秩序”的，检察机关应当依法履行追诉职责，作为公诉案件办理。对公安机关未立案侦查，被害人已提出自诉的，检察机关应当处理好由自诉向公诉程序的转换。

【基本案情】

被告人郎某，男，1993 年出生，个体工商户。

被告人何某，男，1996 年出生，务工。

被害人谷某，女，1992 年出生，务工。

2020 年 7 月 7 日 18 时许，郎某在杭州市余杭区某小区东门快递驿站内，使用手机偷拍正在等待取快递的被害人谷某，并将视频发布在某微信群。后郎某、何某分别假扮快递员和谷某，捏造谷某结识快递员并多次发生不正当性关系的微信聊天记录。为增强聊天记录的可信度，郎某、何某还捏造“赴约途中”“约会现场”等视频、图片。7 月 7 日至 7 月 16 日期间，郎某将上述捏造的微信聊天记录截图 39 张及视频、图片陆续发布在该微信群，引发群内大量低俗、侮辱性评论。

8 月 5 日，上述偷拍的视频以及捏造的微信聊天记录截图 27 张被他人合并转发，并相继扩散到 110 余个微信群（群成员约 2.6 万）、7 个微信公众号（阅读数 2 万余次）及 1 个网站（浏览量 1000 次）等网络平台，引发大量低俗、侮辱性评论，严重影响了谷某的正常工作生活。

8 月至 12 月，此事经多家媒体报道引发网络热议，其中，仅微博话题“被造谣出轨女子至今找不到工作”阅读量就达 4.7 亿次、话题讨论 5.8 万人次。该事件在网络上广泛传播，给广大公众造成不安全感，严重扰乱了网络社会公共秩序。

【检察履职情况】

（一）推动案件转为公诉程序办理

2020 年 8 月 7 日，谷某就郎某、何某涉嫌诽谤向浙江省杭州市公安局余杭分局报案。

8 月 13 日，余杭分局作出对郎某、何某行政拘留 9 日的决定。10 月 26 日，谷某委托诉讼代理人向浙江省杭州市余杭区人民法院提起刑事自诉，并根据法院通知补充提交了相关材料。12 月 14 日，法院立案受理并对郎某、何某采取取保候审强制措施。

因相关事件及视频在网络上进一步传播、蔓延，案件情势发生重大变化。检察机关认为，郎某、何某的行为不仅侵害被害人的人格权，而且经网络迅速传播，已经严重扰乱网络社会公共秩序。由于本案被侵害对象系随意选取，具有不特定性，任何人都可能成为被侵害对象，严重破坏了广大公众安全感。对此类案件，由自诉人收集证据并达到事实清楚，证据确实、充分的证明标准难度很大，只有通过公诉程序追诉才能及时、有效收集、固定证据，依法惩罚犯罪、维护社会公共秩序。12 月 22 日，浙江省杭州市余杭区人民检察院建议公安机关立案侦查。

12 月 25 日，余杭分局对郎某、何某涉嫌诽谤罪立案侦查。12 月 26 日，谷某向余杭区人民法院撤回起诉。

（二）引导侦查取证

余杭区人民检察院围绕诽谤罪“情节严重”的标准以及“严重危害社会秩序”的公诉情形，向公安机关提出对诽谤信息传播侵害被害人人格权与社会秩序、公众安全感遭受破坏的相关证据一并收集固定的意见。公安机关经侦查，及时收集、固定了诽谤信息传播扩散情况、引发的低俗评论以及该案给广大公众造成的不安全感等关键证据。

（三）审查起诉

2021 年 1 月 20 日，余杭分局将该案移送审查起诉。余杭区人民检察院审查认为，郎某、何某为寻求刺激、博取关注，捏造损害他人名誉的事实，在网络上散布，造成该信息被大量阅读、转发，严重侵害谷某的人格权，导致谷某被公司劝退，随后多次求职被拒，使谷某遭受一定经济损失，社会评价也遭受严重贬损，且二被告人侵害对象选择随意，造成不特定公众恐慌和社会安全感、秩序感下降；诽谤信息在网络上大范围流传，引发大量低俗评论，对网络公共秩序造成严重冲击，严重危害社会秩序，符合刑法第二百四十六条第二款“严重危害社会秩序”的规定。

2 月 26 日，余杭区人民检察院依法对郎某、何某以涉嫌诽谤罪提起公诉。鉴于二被告人认罪认罚，对被害人进行赔偿并取得谅解，余杭区人民检察院对二被告人提出有期徒刑一年，缓刑二年的量刑建议。

（四）指控与证明犯罪

2021 年 4 月 30 日，余杭区人民法院依法公开开庭审理本案。庭审中，二被告人再次表示认罪认罚。

辩护人对检察机关指控事实、定性均无异议。郎某的辩护人提出，诽谤信息的传播介入了他人的编辑、转发，属于多因一果。公诉人答辩指出，郎某作为成年人应当知道网络具有开放性、不可控性，诽谤信息会被他人转发或者评论，因此，他人的扩散行为应当由其承担责任。而且，被他人转发，恰恰说明该诽谤信息对社会秩序的破坏。

（五）处理结果

余杭区人民法院审理后当庭宣判，采纳检察机关指控的犯罪事实和量刑建议，判决二被告人有期徒刑一年，缓刑二年。宣判后，二被告人未提出上诉，判决已生效。

【指导意义】

（一）准确把握网络诽谤犯罪“严重危害社会秩序”的认定条件。网络涉及面广、浏览量大，一旦扩散，往往造成较大社会影响，与传统的发生在熟人之间、社区传播形式的诽谤案件不同，通过网络诽谤他人，诽谤信息经由网络广泛传播，严重损害被害人人格权，如果破坏了公序良俗和公众安全感，严重扰乱网络社会公共秩序的，应当认定为《最高人民法院、最高人民检察院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》

第三条规定的“其他严重危害社会秩序的情形”。对此，可以根据犯罪方式、对象、内容、主观目的、传播范围和造成后果等，综合全案事实、性质、情节和危害程度等予以评价。

（二）坚持能动司法，依法惩治网络诽谤犯罪。网络诽谤传播广、危害大、影响难消除，被害人往往面临举证难、维权难，通过自诉很难实现权利救济，更无法通过自诉有效追究犯罪嫌疑人刑事责任。如果网络诽谤犯罪侵害了社会公共利益，就应当适用公诉程序处理。检察机关要适应新时代人民群众对人格尊严保护的更高需求，针对网络诽谤犯罪的特点，积极主动履职，加强与其他执法司法机关沟通协调，依法启动公诉程序，及时有效打击犯罪，加强对公民人格权的刑法保护，维护网络社会秩序，营造清朗网络空间。

（三）被害人已提起自诉的网络诽谤犯罪案件，因同时侵害公共利益需要适用公诉程序办理的，应当依法处理好程序转换。对自诉人已经提起自诉的网络诽谤犯罪案件，检察机关审查认为属于“严重危害社会秩序”，应当适用公诉程序的，应当履行法律监督职责，建议公安机关立案侦查。在公安机关立案后，对自诉人提起的自诉案件，人民法院尚未受理的，检察机关可以征求自诉人意见，由其撤回起诉。人民法院对自诉人的自诉案件受理以后，公安机关又立案的，检察机关可以征求自诉人意见，由其撤回起诉，或者建议人民法院依法裁定终止自诉案件的审理，以公诉案件审理。

【相关规定】

《中华人民共和国刑法》第二百四十六条

《中华人民共和国民法典》第九百九十条、第九百九十一条、第一千零二十四条

《最高人民法院、最高人民检察院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》第二条、第三条

《最高人民法院关于适用<中华人民共和国刑事诉讼法>的解释》第一条、第三百二十条

案例三、岳某侮辱案（检例第 138 号）

【关键词】

网络侮辱　裸照　情节严重　严重危害社会秩序　公诉程序

【要旨】

利用信息网络散布被害人的裸体视频、照片及带有侮辱性的文字，公然侮辱他人，贬损他人人格、破坏他人名誉，导致出现被害人自杀等后果，严重危害社会秩序的，应当按照公诉程序，以侮辱罪依法追究刑事责任。

【基本案情】

被告人岳某，男，1982 年出生，农民。

被害人张某，女，殁年 34 岁。

二人系同村村民，自 2014 年开始交往。交往期间，岳某多次拍摄张某裸露身体的照片和视频。2020 年 2 月，张某与岳某断绝交往。岳某为报复张某及其家人，在自己的微信朋友圈、快手 APP 散布二人交往期间拍摄的张某的裸体照片、视频，并发送给张某的家人。后岳某的该快手账号因张某举报被封号。5 月，岳某再次申请快手账号，继续散布张某的上述视频及写有侮辱性文字的张某照片，该快手 APP 散布的视频、照片的浏览量达到 600 余次。

上述侮辱信息在当地迅速扩散、发酵，造成恶劣社会影响。同时，岳某还多次通过电话、微信骚扰、挑衅张某的丈夫。张某倍受舆论压力，最终不堪受辱服毒身亡。

【检察履职情况】

（一）审查逮捕

2020 年 7 月 6 日，张某的丈夫以张某被岳某强奸为由到公安机关报案。7 月 7 日，河北省肃宁县公安局立案侦查。7 月 13 日，肃宁县公安局以岳某涉嫌强奸罪向河北省肃宁县

人民检察院提请批准逮捕。

肃宁县人民检察院审查认为，因张某死亡，且无其他证据，无法证实岳某实施了强奸行为，但岳某为报复张某，将张某的裸体视频及带有侮辱性文字的照片发送到微信朋友圈和快手等网络平台，公然贬损张某人格、破坏其名誉，致张某自杀，情节严重，应当以侮辱罪追究其刑事责任。岳某侮辱他人，在当地造成恶劣影响，范围较广，严重危害社会秩序，应当适用公诉程序追诉。7 月 20 日，肃宁县人民检察院以岳某涉嫌侮辱罪对其批准逮捕。

（二）审查起诉

2020 年 9 月 18 日，肃宁县公安局以岳某涉嫌侮辱罪移送审查起诉。肃宁县人民检察院受理后，根据审查情况，要求公安机关向腾讯、快手公司补充调取岳某的账号信息及发布内容，确定发布内容的浏览量，以及在当地造成的社会影响。审查后，肃宁县人民检察院于 10 月 9 日以岳某涉嫌侮辱罪提起公诉，并结合认罪认罚情况，对岳某提出有期徒刑二年八个月的量刑建议。

（三）指控与证明犯罪

2020 年 11 月 25 日，河北省肃宁县人民法院依法不公开开庭审理本案。

被告人岳某表示认罪认罚。岳某的辩护人提出，岳某的行为不构成犯罪。一是岳某的行为属于民事侵权行为，散布隐私尚未达到“情节严重”；二是岳某出于专门散布张某隐私视频和照片的目的而开设快手账号，两个账号粉丝共 4 人，不会有粉丝以外的人浏览，不符合侮辱罪“公然性”要求。公诉人答辩指出，岳某的行为已构成侮辱罪。一是张某因岳某的侮辱行为而自杀，该侮辱行为与死亡结果存在因果关系，属于“情节严重”；二是侮辱行为具有“公然性”。岳某将被害人的裸照、视频发送到网络上，使不特定多数人均可以看到，符合侮辱罪“公然性”的规定。而且，快手 APP 并非只有成为粉丝才能浏览，粉丝人数少不代表浏览人数少，在案证据证实视频和照片的浏览量分别为 222 次、429 次，且证人岳某坤等证实曾接收到快手同城推送的带有侮辱性文字的张某照片。

（四）处理结果

2020 年 12 月 3 日，肃宁县人民法院作出判决，采纳检察机关指控的犯罪事实和量刑建议，以侮辱罪判处岳某有期徒刑二年八个月。判决宣告后，岳某未提出上诉，判决已生效。

【指导意义】

（一）侮辱他人行为恶劣或者造成被害人精神失常、自残、自杀等严重后果的，可以认定为“情节严重”。行为人以破坏他人名誉、贬低他人人格为目的，故意在网络上对他人实施侮辱行为，如散布被害人的个人隐私、生理缺陷等，情节严重的，应当认定为侮辱罪。侮辱罪“情节严重”，包括行为恶劣、后果严重等情形，如当众撕光妇女衣服的，当众向被害人泼洒粪便、污物的，造成被害人或者其近亲属精神失常、自残、自杀的，二年内曾因侮辱受过行政处罚又侮辱他人的，在网络上散布被害人隐私导致被广泛传播的，以及其他情节严重情形。

（二）侮辱罪“严重危害社会秩序”可以结合行为方式、社会影响等综合认定。侮辱罪属于告诉才处理的犯罪，但严重危害社会秩序和国家利益的除外。行为人利用信息网络侮辱他人犯罪案件中，是否属于“严重危害社会秩序”的情形，可以根据《最高人民法院、最高人民检察院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》的相关规定予以认定。行为人在网络上散布被害人裸照、视频等严重侵犯他人隐私的信息，造成恶劣社会影响的，或者在网络上散布侮辱他人的信息，导致对被害人产生大量负面评价，造成恶劣社会影响的，不仅侵害被害人人格权，而且严重扰乱社会秩序的，可以认定为“其他严重危害社会秩序的情形”，按照公诉程序依法追诉。

（三）准确认定利用网络散布他人裸照、视频等隐私的行为性质。行为人在与被害人交往期间，获得了被害人的裸照、视频等，无论其获取行为是否合法，是否得到被害人授权，

只要恶意对外散布，均应当承担相应法律责任，情节严重的，要依法追究刑事责任。对上述行为认定为侮辱罪还是强制侮辱罪，要结合行为人的主客观方面综合判断。如果行为人以破坏特定人名誉、贬低特定人人格为目的，故意在网络上对特定对象实施侮辱行为，情节严重的，应当认定为侮辱罪。如果行为人出于寻求精神刺激等动机，以暴力、胁迫或者其他方式，对妇女进行身体或者精神强制，使之不能反抗或者不敢反抗，进而实施侮辱的行为，应当认定为强制侮辱罪。

【相关规定】

《中华人民共和国刑法》第二百四十六条

《最高人民法院、最高人民检察院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》第二条、第三条、第五条

（五）侵犯公民个人信息罪

1.最高检发布六起侵犯公民个人信息犯罪典型案例之二：张某某、姚某某侵犯公民个人信息案（2017 年 5 月 16 日）

案例要旨

利用恶意程序批量非法获取网站用户个人信息的，构成侵犯公民个人信息罪

一、基本案情

2015 年 6 月，被告人张某某在登录浏览“魅力惠”购物网站时发现，通过修改该网站网购订单号可以查看到包含用户姓名、手机号、住址等内容的订单信息。为谋取利益，张某某委托他人针对上述网站漏洞编制批量扒取数据的恶意程序，在未经网站授权的情况下，进入该网站后台管理系统，从中非法获取客户订单信息 12503 条，通过 QQ 等联络方法将上述客户信息分数次卖给被告人姚某某，获利人民币 5359 元。被告人姚某某购得上述订单信息后，又在网络上分别加价倒卖从中牟利。

上海市黄浦区人民检察院于 2015 年 9 月 30 日以涉嫌非法获取公民个人信息罪对张某某批准逮捕，于 10 月 20 日以证据不足对姚某某不批准逮捕，并要求公安机关补充侦查。此案提起公诉后，2016 年 3 月 29 日，黄浦区人民法院以侵犯公民个人信息罪，判处张某某有期徒刑一年九个月，罚金人民币五万元，判处姚某某有期徒刑一年六个月，罚金人民币二万元。

二、典型意义

本案通过网络实施侵犯公民个人信息犯罪，在远程、非接触的状态下跨省区、多地域完成，作案手段技术含量高，涉案人员关系松散，特别是犯罪活动涉及的电子证据源中电脑、QQ、移动存储介质、手机、银行卡等证据的数据提取、固定、转化和验证等给案件取证工作带来一定困难，增加了检察机关在案件审查逮捕中的工作难度。

检察机关从多个方面加强案件指导和审查，确保案件质量和监督效果。

一是注重引导案件侦查，确保取证工作扎实到位。鉴于案件系当地首例以黑客手段窃取公民个人信息的案件，公安机关立案后即商请检察机关提前介入，检察机关高度重视，会同公安机关刑侦、网安等部门商讨案情、引导侦查。检察机关就捕前侦查取证方向、证据标准规定、所涉罪名法律适用等问题与公安机关进行详细分析沟通，有效提升案件侦办的效率和质量。如针对犯罪嫌疑人主要犯罪手法系利用恶意程序批量扒取网站用户信息的手段，检察机关对所涉现场勘验检查、远程勘验记录、电子证据检查、作案工具扣押等环节的取证要点与规范要求予以明确，确保证据收集工作的合法性和有效性。

二是严格案件证据审查，确保核心证据固定。本案证据体系中，认定犯罪事实的核心证据之一系犯罪嫌疑人非法获取公民身份信息的电子数据。如果该核心证据缺失，即使犯罪嫌疑人作有罪供述亦难以定罪处罚。犯罪嫌疑人姚某某移送审查逮捕过程中，检察机关对电子

数据仔细比对后发现，有关姚某某非法获取公民数据信息情况的鉴定意见存在重大瑕疵，难以作为定案依据，需重新鉴定，故综合案件证据情况，对姚某某作存疑不捕决定，同时向公安机关说明不捕理由并提出五条补侦建议。公安机关根据上述要求逐一进行补侦，待证据达到要求后移送起诉，后法院对姚某某作出有罪判决。

三是重视后续跟踪指导，确保案件质量过硬。加强不捕案件补侦工作的指导监督。姚某某案中鉴定意见存在重大瑕疵，检察机关在该案补充侦查过程中多次与鉴定人员联系沟通，重新梳理证据情况，明确相关鉴定要求，及时修正证据瑕疵问题。加强捕诉联动交流。检察机关侦查监督部门与公诉部门围绕案件定性、证据认定、涉案情节等疑难问题进行充分沟通，形成统一意见。庭审中，公诉人运用充分证据指控犯罪，张某某、姚某某均供认指控事实，庭审效果良好。

2.最高人民检察院第三十四批指导性案例之五：柯某侵犯公民个人信息案（检例第 140 号）

【关键词】

侵犯公民个人信息　业主房源信息　身份识别　信息主体另行授权

【要旨】

业主房源信息是房产交易信息和身份识别信息的组合，包含姓名、通信通讯联系方式、住址、交易价格等内容，属于法律保护的公民个人信息。未经信息主体另行授权，非法获取、出售限定使用范围的业主房源信息，系侵犯公民个人信息的行为，情节严重、构成犯罪的，应当依法追究刑事责任。检察机关办理案件时应当对涉案公民个人信息具体甄别，筛除模糊、无效及重复信息，准确认定侵犯公民个人信息数量。

【基本案情】

被告人柯某，男，1980 年出生，系安徽某信息技术有限公司经营者，开发了“房利帮”网站。

2016 年 1 月起，柯某开始运营“房利帮”网站并开发同名手机 APP，以对外售卖上海市二手房租售房源信息为主营业务。运营期间，柯某对网站会员上传真实业主房源信息进行现金激励，吸引掌握该类信息的房产中介人员（另案处理）注册会员并向网站提供信息，有偿获取了大量包含房屋门牌号码及业主姓名、电话等非公开内容的业主房源信息。

柯某在获取上述业主房源信息后，安排员工冒充房产中介人员逐一电话联系业主进行核实，将有效的信息以会员套餐形式提供给网站会员付费查询使用。上述员工在联系核实信息过程中亦未如实告知业主获取、使用业主房源信息的情况。

自 2016 年 1 月至案发，柯某通过运营“房利帮”网站共非法获取业主房源信息 30 余万条，以会员套餐方式出售获利达人民币 150 余万元。

上海市公安局金山分局在侦办一起侵犯公民个人信息案时，发现该案犯罪嫌疑人非法出售的部分信息购自“房利帮”网站，根据最高人民法院、最高人民检察院、公安部《关于办理网络犯罪案件适用刑事诉讼法若干问题的意见》的规定，柯某获取的均为上海地区的业主信息，遂对柯某立案侦查。

【检察履职情况】

（一）引导侦查取证

2017 年 11 月 17 日，金山分局以柯某涉嫌侵犯公民个人信息罪向上海市金山区人民检察院提请批准逮捕。

11 月 24 日，金山区人民检察院作出批准逮捕决定，并建议公安机关从电子数据、言词证据两方面，针对信息性质和经营模式继续取证。公安机关根据建议，一是调取了完整的运营数据库进行鉴定，确认了信息数量；二是结合“房利帮”网站员工证言，进一步向柯某确认了该公司是由其个人控制经营，以有偿获取、出售个人信息为业，查明本案属自然人犯

罪而非单位犯罪。

（二）审查起诉

2018 年 1 月 19 日，金山分局将本案移送审查起诉。经退回补充侦查并完善证据，查清了案件事实。一是对信息数据甄别去重，结合网站的资金支出和柯某供述，进一步明确了有效业主房源信息的数量；二是对相关业主开展随机调查，证实房产中介人员向“房利帮”网站上传信息未经业主事先同意或者另行授权，以及业主在信息泄露后频遭滋扰等情况。

7 月 27 日，金山区人民检察院以柯某涉嫌侵犯公民个人信息罪提起公诉。

（三）指控与证明犯罪

2019 年 1 月 16 日，上海市金山区人民法院依法公开开庭审理本案。审理中，柯某及其辩护人对柯某的业务模式、涉案信息数量等事实问题无异议，但认为柯某的行为不构成犯罪。

辩护人提出，第一，房源信息是用于房产交易的商用信息，部分信息没有业主实名，不属于刑法保护的公民个人信息；第二，网站的房源信息多由房产中介人员上传，房产中介人员获取该信息时已得到业主许可，系公开信息，网站属合理使用，无须另行授权；第三，网站对信息核实后，将真实房源信息整合，主要向房产中介人员出售，促进房产交易，符合业主意愿和利益。

公诉人答辩指出，柯某的行为依法构成犯罪。第一，业主房源信息中的门牌号码、业主电话，组合后足以识别特定自然人，且部分信息有业主姓名，符合刑法对公民个人信息的界定；第二，业主委托房产中介时提供姓名、电话等，目的是供相对的房产中介提供服务时联系使用，不能以此视为业主同意或者授权中介对社会公开；第三，柯某安排员工冒充房产中介向业主核实时，仍未如实告知信息获取的途径及用途。而且，该网站并不从事中介业务帮助业主寻找交易对象，只是将公民个人信息用于倒卖牟利。

（四）处理结果

2019 年 12 月 31 日，金山区人民法院作出判决，采纳金山区人民检察院指控的犯罪事实和意见，以侵犯公民个人信息罪判处柯某有期徒刑三年，缓刑四年，并处罚金人民币一百六十万元。宣判后，柯某未提出上诉，判决已生效。

【指导意义】

（一）包含房产信息和身份识别信息的业主房源信息属于公民个人信息。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，包括姓名、身份证件号码、通信通讯联络方式、住址、账号密码、财产状况、行踪轨迹等。业主房源信息包括房产坐落区域、面积、售租价格等描述房产特征的信息，也包含门牌号码、业主电话、姓名等具有身份识别性的信息，上述信息组合，使业主房源信息符合公民个人信息“识别特定自然人”的规定。上述信息非法流入公共领域存在较大风险。现实生活中，被害人因信息泄露被频繁滋扰，更有大量信息进入黑灰产业链，被用于电信网络诈骗、敲诈勒索等犯罪活动，严重威胁公民人身财产安全、社会公共利益，甚至危及国家信息安全，应当依法惩处。

（二）获取限定使用范围的信息需信息主体同意、授权。对生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息，进行信息处理须得到信息主体明确同意、授权。对非敏感个人信息，如上述业主电话、姓名等，应当根据具体情况作出不同处理。信息主体自愿、主动向社会完全公开的信息，可以认定同意他人获取，在不侵犯其合法利益的情况下可以合法、合理利用。但限定用途、范围的信息，如仅提供给中介供服务使用的，他人在未经另行授权的情况下，非法获取、出售，情节严重的，应当以侵犯公民个人信息罪追究刑事责任。

（三）认定公民个人信息数量，应当在全面固定数据基础上有效甄别。侵犯公民个人

信息案件中，信息一般以电子数据形式存储，往往数据庞杂、真伪交织、形式多样。检察机关应当把握公民个人信息“可识别特定自然人身份或者反映特定自然人活动情况”的标准，准确提炼出关键性的识别要素，如家庭住址、电话号码、姓名等，对信息数据有效甄别。对包含上述信息的认定为有效的公民个人信息，以准确认定信息数量。

【相关规定】

《中华人民共和国刑法》第二百五十三条之一

《中华人民共和国网络安全法》第四十一条、第四十二条

《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、第二条、第三条、第四条、第十一条

3.最高人民检察院发布11件检察机关个人信息保护公益诉讼典型案例九至十一（2021.04.22）

案例一、上海市宝山区人民检察院诉H科技有限公司、韩某某等人侵犯公民个人信息刑事附带民事公益诉讼案

【关键词】

刑事附带民事公益诉讼　网络运营者责任　关闭网站　删除数据

【要旨】

针对网络服务提供者、网络用户利用互联网侵犯公民个人信息的犯罪行为，网络运营者未依法履行其社会管理职责的情形，检察机关在提起刑事附带民事公益诉讼时，可以依法追加其为附带民事公益诉讼被告，要求其承担侵权责任。

【基本案情】

H科技有限公司（以下简称H公司）主要从事网络游戏及相关产品研发和技术咨询，韩某某任经理。2019年2月，该公司设立“数迈网”，为数据信息交易提供平台，并雇用杨某某、黄某某、管某某参与运营。其间，韩某某明知用户上传数据中有大量个人信息，仍为非法交易个人信息提供平台。网站涉及确切有用的个人信息共37万余条，交易数量达3万余条。软件工程师管某某明知网站有买卖个人信息行为，仍帮助推送关键字搜索。2019年2月，陈某某注册“数迈网”会员，并上传其在“某公司天猫旗舰店”就职时获取的淘宝买家姓名、手机号、收货地址等数据信息5757条，欲贩卖牟利。

【调查和诉讼】

2019年9月，上海市人民检察院（以下简称上海市院）从办案系统和媒体报道中获知上海公安机关破获一起特大贩卖个人信息案，经研判后将该案线索交由宝山区人民检察院（以下简称宝山区院）办理。宝山区院立案后，邀请专家辅助办案，对案件中涉及的QQ聊天记录、30余万条公民个人信息、银行卡交易明细、交易台账等文件逐一梳理、交叉比对，查清非法获利数额，确定赔偿数额。宝山区院经审查认为，H公司虽没有被追究刑事责任，但应承担民事侵权责任。

宝山区院经公告，没有法律规定的机关和有关组织提起诉讼。2019 年 11 月 25 日，宝山区院对韩某某等人以侵犯公民个人信息罪向宝山区人民法院提起公诉。同时，对 H 公司、韩某某等人侵害社会公共利益的行为提起刑事附带民事公益诉讼。针对本案中网站服务器、QQ 中保存的公民个人信息仍存在被传播、买卖的危险，宝山区院积极探索侵权责任承担方式，除了要求被告在国家级新闻媒体上向社会公开赔礼道歉、赔偿损失之外，还向法院提出要求关闭网站、注销侵权用QQ号码并永久删除保存在QQ内的公民个人信息数据的诉讼请求。

宝山区人民法院经公开开庭审理，于 2020 年 3 月 27 日作出一审判决，在附带民事公益诉讼部分，判决被告 H 公司、韩某某、杨某某、管某某连带赔偿损失人民币 3900 元，被告黄某某在上述赔偿款 3600 元范围内承担连带赔偿责任；H 公司关闭“数迈网”网站；H 公司、韩某某、杨某某、黄某某、陈某某注销买卖公民个人信息所用 QQ 号码，并永久删除保存在 QQ 内的公民个人信息数据；H 公司、韩某某、杨某某、黄某某、管某某、陈某某在国家级媒体上向社会公众赔礼道歉。一审判决后，刑事案件被告人提起上诉，二审判决维持原判。

为促进源头治理，宝山区院将案件中“某公司天猫旗舰店”涉嫌违法的线索移送有管辖权的广东省广州市白云区人民检察院（以下简称白云区院），并就调查取证等工作开展跨省协作。白云区院审查线索后以行政公益诉讼立案，并与负有监督管理职责的行政机关进行磋商。行政机关认定“某公司天猫旗舰店”的经营公司在执行网络安全信息制度的防范措施上存在明显漏洞，遂对该公司立案调查，并针对咨询、房地产中介、汽车销售、保险等重点行业发出预警信息公告，开展系统治理。

【典型意义】

对刑事附带民事公益诉讼被告的确定不能囿于刑事被告人范围，应结合个案情况具体明确侵权人。通过追究网络运营者的民事侵权责任，警示网络运营主体落实网络安全保护责任，加强内部安全管理、规范操作规程。对涉案的网站服务器，QQ 中保存的公民个人信息通过传统扣押方式不能消除危险的，检察机关可以提出关闭网站、注销侵权使用的 QQ 号码并永久删除保存在 QQ 内的公民个人信息数据等诉请，彻底消除危险。针对网络侵害的跨地域性等特点，检察机关协同相关行政机关治理侵害个人信息行为，有利于互联网领域损害公益问题的系统治理、综合治理、源头治理，彰显了公益诉讼的独特价值。

案例二、贵州省安顺市西秀区人民检察院诉熊某某等人侵犯公民个人信息刑事附带民事公益诉讼案

【关键词】

刑事附带民事公益诉讼　公开听证　支付赔偿金

【要 旨】

针对在互联网上非法获取、出售公民个人信息，损害社会公共利益的行为，检察机关在依法追究违法行为人刑事责任的同时，依法提起刑事附带民事公益诉讼，要求其支付赔偿金并公开赔礼道歉。

【基本案情】

2018 年 10 月，熊某某通过技术软件非法获取大量公民个人信息，并在网上出售给他人获利。同年 12 月，熊某某传授其女友王某甲，并由王某甲协助其在网上出售公民个人信息共同获利。其间，王某甲又传授给其弟王某乙，使王某乙亦在网上售卖公民个人信息获利。至 2019 年 4 月，熊某某、王某甲、王某乙非法出售公民个人信息获利共计 70 余万元。

【调查和诉讼】

贵州省安顺市西秀区人民检察院（以下简称西秀区院）在审查熊某某等 3 人涉嫌侵犯公民个人信息罪一案时，发现熊某某等 3 人的行为可能损害社会公共利益，遂将该案线索移送至公益诉讼检察部门审查。2019 年 11 月 13 日，西秀区院对熊某某等 3 人以侵犯公民个人信息刑事附带民事公益诉讼立案。本案侵犯公民个人信息数量多、非法获利金额大。为确保证据充分，西秀区院在办理该案时提前介入、引导侦查，及时固定熊某某等 3 人出售公民个人信息和非法获利的相关书证和电子数据，查清侵害众多不特定人员个人信息安全的事实，并邀请区人大代表、政协委员、人民监督员、基层群众代表作为听证员进行公开听证。听证员在听取案情介绍、刑事附带民事公益诉讼立案的相关法律依据，并就相关问题进行询问后，一致认为西秀区院应该对熊某某等 3 人侵犯公民个人信息案提起刑事附带民事公益诉讼。

西秀区院经公告，没有法律规定的机关和有关组织提起诉讼。2020 年 6 月 1 日，西秀区院向西秀区人民法院提起刑事附带民事公益诉讼，请求依法判令刑事附带民事公益诉讼被告人熊某某等 3 人自行彻底删除所有非法获取的公民个人信息；支付赔偿金共计人民币 70 余万元；在国家级媒体上公开赔礼道歉。

2020 年 7 月 23 日，西秀区人民法院公开开庭审理本案。庭审中，公诉人及公益诉讼起诉人出示、宣读了本案被告人供述、证人证言、被害人陈述、鉴定意见及勘验检查笔录等证据，证明熊某某等 3 人非法获取、出售大量公民个人信息的行为，侵害公民合法权益，损害了社会公共利益。西秀区人民法院在当庭判决熊某某等 3 名被告人犯侵犯公民个人信息罪，判处有期徒刑及罚金的同时，全部支持了检察机关提出的附带民事公益诉讼请求。一审判决后，熊某某、王某甲提出上诉，二审法院维持了附带民事公益诉讼判决。本案判决现已生效并移送执行，赔偿金将存入检察机关与财政部门共同建立的公益诉讼专项资金账户。

【典型意义】

通过互联网非法获取、出售公民个人信息，导致众多不特定公民个人信息被泄露，侵害公民个人信息安全，损害社会公共利益。检察机关作为公共利益的代表，可以对侵犯公民个人信息的违法行为人依法提起刑事附带民事公益诉讼，要求其承担赔偿损失等公益损害责任，加重侵犯公民个人信息违法犯罪成本，全面维护公民个人信息安全。

案例三、广东省广宁县人民检察院诉谭某某等人侵犯公民个人信息刑事附带民事公益诉讼案

【关键词】

刑事附带民事公益诉讼　业主个人信息保护　庭审观摩　行业治理

【要旨】

检察机关以侵犯公民个人信息刑事附带民事公益诉讼为切入点，通过诉讼判决被告承担停止侵害、消除危险等侵权责任，并督促行政主管部门全面依法履职，以案为鉴推动行业规范治理，全方位保护公民个人信息安全。

【基本案情】

2018 年至 2020 年 7 月，谭某某等 5 人违反国家规定，通过出售、购买、交换等方式非法获取广东省广宁县辖区多个住宅小区业主的个人信息共计 13784 条，并组建微信群用以分享、买卖所获取的业主信息。

【调查和诉讼】

2020 年 9 月 22 日，广宁县公安局将谭某某等 5 人以涉嫌侵犯公民个人信息罪移送广宁县人民检察院（以下简称广宁县院）审查起诉。广宁县院在履行批准逮捕职责中发现，谭某某等人存在侵犯公民个人信息行为，可能损害社会公共利益，于 2020 年 8 月 18 日作为刑事附带民事公益诉讼案件立案调查。在充分把握刑事案件证据的基础上，办案人员通过询问被告人、走访有关部门和企业等方式进行调查核实，补强民事侵权的证据，为提起刑事附带民事公益诉讼构建完整证据链条。广宁县院经审查认为，被告人谭某某等人所获取的小区业主信息，足以识别公民的个人身份，属于影响人身、财产安全的个人信息。上述被告人不仅侵害了业主及其同住人员的个人信息和隐私等人格权利，还具有危害其财产安全的可能性，损害了社会公共利益，除应受到刑事处罚外，还应当承担相应的公益损害责任。

广宁县院经公告，没有法律规定的机关和有关组织提起诉讼。2020 年 11 月 12 日，广宁县院向人民法院提起刑事附带民事公益诉讼，请求判令谭某某等 5 名被告解散用于收集、买卖公民个人信息的微信群，删除保存在微信的公民个人信息数据，在媒体上赔礼道歉，委托电信部门向被侵权人发送风险提示短信。

2020 年 12 月 4 日，广宁县人民法院对该案开庭审理，广宁县院检察长出席法庭履行职责，县法院院长担任审判长。县人大代表、政协委员，公安机关、住建部门有关负责人及县房地产企业、物业服务企业等代表受邀观摩庭审，庭审还通过现场网络直播形式向社会公开。经审理，法院当庭判决谭某某等 5 名被告人犯侵犯公民个人信息罪，分别判处有期徒刑及罚金，并全部支持检察机关提出的附带民事公益诉讼请求，目前已全部履行完毕。

针对本案暴露出的行业监管薄弱环节，广宁县院向广宁县市场监督管理局发出行政公益诉讼诉前检察建议，并召开听证会督促其依法履职，做好公民个人信息保护工作。县市场监督管理局依法对涉案装饰装修企业作出了停业整顿的行政处罚。同时，广宁县院向广宁县住房和城乡建设局发出社会治理类检察建议，县住房和城乡建设局于本案庭审当天召开全县物管企业整顿会议，并邀请检察官开展法治教育，教育警示物管企业采取措施预防公民个人信息被不当使用。

【典型意义】

在互联网时代，侵犯公民个人信息行为多发频发，严重侵害人民群众合法权益和社会公共利益。检察机关对侵犯公民个人信息违法犯罪采用“一案三查”模式，对刑事案件犯罪情节、民事公益诉讼案件侵权情形和行政机关及有关运营主体监管履职情况统筹把握，综合运用刑事检察、公益诉讼检察职能打击违法犯罪行为，弥补了公民个人维权相对困难的不足，有效维护了社会公共利益。同时，通过个案办理促进类案整改，结合庭审观摩等方式，以司法公开激活行政机关、相关运营主体的监管职责，取得良好的社会治理成效。

（六）诈骗罪

1. 最高人民检察院关于印发最高人民检察院第十八批指导性案例的通知（高检发办字[2020]21 号）

各级人民检察院：

经 2020 年 1 月 3 日最高人民检察院第十三届检察委员会第三十一次会议通过，现将张凯闵等 52 人电信网络诈骗案等三件指导性案例（检例第 67－69 号）作为第十八批指导性案例发布，供参照适用。

最高人民检察院

2020 年 3 月 28 日

最高人民检察院第十八批指导性案例

检例第 67 号：张凯闵等 52 人电信网络诈骗案

【关键词】

跨境电信网络诈骗 境外证据审查 电子数据 引导取证

【要旨】

跨境电信网络诈骗犯罪往往涉及大量的境外证据和庞杂的电子数据。对境外获取的证据应着重审查合法性，对电子数据应着重审查客观性。主要成员固定，其他人员有一定流动性的电信网络诈骗犯罪组织，可认定为犯罪集团。

【基本案情】

被告人张凯闵，男，1981 年 11 月 21 日出生，中国台湾地区居民，无业。

林金德等其他被告人、被不起诉人基本情况略。

2015 年 6 月至 2016 年 4 月间，被告人张凯闵等 52 人先后在印度尼西亚共和国和肯尼亚共和国参加对中国大陆居民进行电信网络诈骗的犯罪集团。在实施电信网络诈骗过程中，各被告人分工合作，其中部分被告人负责利用电信网络技术手段对大陆居民的手机和座机电话进行语音群呼，群呼的主要内容为“有快递未签收，经查询还有护照签证即将过期，将被限制出境管制，身份信息可能遭泄露”等。当被害人按照语音内容操作后，电话会自动接通冒充快递公司客服人员的一线话务员。一线话务员以帮助被害人报案为由，在被害人不挂断电话时，将电话转接至冒充公安局办案人员的二线话务员。二线话务员向被害人谎称“因泄露的个人信息被用于犯罪活动，需对被害人资金流向进行调查”，欺骗被害人转账、汇款至指定账户。如果被害人对二线话务员的说法仍有怀疑，二线话务员会将电话转给冒充检察官的三线话务员继续实施诈骗。

至案发，张凯闵等被告人通过上述诈骗手段骗取 75 名被害人钱款共计人民币 2300 余万元。

【指控与证明犯罪】

（一）介入侦查引导取证

由于本案被害人均是中国大陆居民，根据属地管辖优先原则，2016 年 4 月，肯尼亚将 76 名电信网络诈骗犯罪嫌疑人（其中大陆居民 32 人，台湾地区居民 44 人）遣返中国大陆。经初步审查，张凯闵等 41 人与其他被遣返的人分属互不关联的诈骗团伙，公安机关依法分案处理。2016 年 5 月，北京市人民检察院第二分院经指定管辖本案，并应公安机关邀请，介入侦查引导取证。

鉴于肯尼亚在遣返犯罪嫌疑人前已将起获的涉案笔记本电脑、语音网关（指能将语音通信集成到数据网络中实现通信功能的设备）、手机等物证移交我国公安机关，为确保证据的客观性、关联性和合法性，检察机关就案件证据需要达到的证明标准以及涉外电子数据的提取等问题与公安机关沟通，提出提取、恢复涉案的 Skype 聊天记录、Excel 和 Word 文档、网络电话拨打记录清单等电子数据，并对电子数据进行无污损鉴定的意见。在审查电子数据的过程中，检察人员与侦查人员在恢复的 Excel 文档中找到多份“返乡订票记录单”以及早期大量的 Skype 聊天记录。依据此线索，查实部分犯罪嫌疑人在去肯尼亚之前曾在印度尼西亚两度针对中国大陆居民进行诈骗，诈骗数额累计达 2000 余万元人民币。随后，11 名曾在印度尼西亚参与张凯闵团伙实施电信诈骗，未赴肯尼亚继续诈骗的犯罪嫌疑人陆续被缉捕到案。至此，张凯闵案 52 名犯罪嫌疑人全部到案。

（二）审查起诉

审查起诉期间，在案犯罪嫌疑人均表示认罪，但对其在犯罪集团中的作用和参与犯罪数额各自作出辩解。

经审查，北京市人民检察院第二分院认为现有证据足以证实张凯闵等人利用电信网络实施诈骗，但案件证据还存在以下问题：一是电子数据无污损鉴定意见的鉴定起始基准时间晚于犯罪嫌疑人归案的时间近 11 个小时，不能确定在此期间电子数据是否被增加、删除、修改。二是被害人与诈骗犯罪组织间的关联性证据调取不完整，无法证实部分被害人系本案犯罪组织所骗。三是台湾地区警方提供的台湾地区犯罪嫌疑人出入境记录不完整，北京市公安局出入境管理总队出具的出入境记录与犯罪嫌疑人的供述等其他证据不尽一致，现有证据不能证实各犯罪嫌疑人参加诈骗犯罪组织的具体时间。

针对上述问题，北京市人民检察院第二分院于 2016 年 12 月 17 日、2017 年 3 月 7 日两次将案件退回公安机关补充侦查，并提出以下补充侦查意见：一是通过中国驻肯尼亚大使馆确认抓获犯罪嫌疑人和外方起获物证的具体时间，将此时间作为电子数据无污损鉴定的起始基准时间，对电子数据重新进行无污损鉴定，以确保电子数据的客观性。二是补充调取犯罪嫌疑人使用网络电话与被害人通话的记录、被害人向犯罪嫌疑人指定银行账户转账汇款的记录、犯罪嫌疑人的收款账户交易明细等证据，以准确认定本案被害人。三是调取各犯罪嫌疑人护照，由北京市公安局出入境管理总队结合护照，出具完整的出入境记录，补充讯问负责

管理护照的犯罪嫌疑人，核实部分犯罪嫌疑人是否中途离开过诈骗窝点，以准确认定各犯罪嫌疑人参加犯罪组织的具体时间。补充侦查期间，检察机关就补侦事项及时与公安机关加强当面沟通，落实补证要求。与此同时，检察人员会同侦查人员共赴国家信息中心电子数据司法鉴定中心，就电子数据提取和无污损鉴定等问题向行业专家咨询，解决了无污损鉴定的具体要求以及提取、固定电子数据的范围、程序等问题。检察机关还对公安机关以《司法鉴定书》记录电子数据勘验过程的做法提出意见，要求将《司法鉴定书》转化为勘验笔录。通过上述工作，全案证据得到进一步完善，最终形成补充侦查卷 21 册，为案件的审查和提起公诉奠定了坚实基础。

检察机关经审查认为，根据肯尼亚警方出具的《调查报告》、我国驻肯尼亚大使馆出具的《情况说明》以及公安机关出具的扣押决定书、扣押清单等，能够确定境外获取的证据来源合法，移交过程真实、连贯、合法。国家信息中心电子数据司法鉴定中心重新作出的无污损鉴定，鉴定的起始基准时间与肯尼亚警方抓获犯罪嫌疑人并起获涉案设备的时间一致，能够证实电子数据的真实性。涉案笔记本电脑和手机中提取的 Skype 账户登录信息等电子数据与犯罪嫌疑人的供述相互印证，能够确定犯罪嫌疑人的网络身份和现实身份具有一致性。75 名被害人与诈骗犯罪组织间的关联性证据已补充到位，具体表现为：网络电话、Skype 聊天记录等与被害人陈述的诈骗电话号码、银行账号等证据相互印证；电子数据中的聊天时间、通话时间与银行交易记录中的转账时间相互印证；被害人陈述的被骗经过与被告人供述的诈骗方式相互印证。本案的 75 名被害人被骗的证据均满足上述印证关系。

（三）出庭指控犯罪

2017 年 4 月 1 日，北京市人民检察院第二分院根据犯罪情节，对该诈骗犯罪集团中的 52 名犯罪嫌疑人作出不同处理决定。对张凯闵等 50 人以诈骗罪分两案向北京市第二中级人民法院提起公诉，对另 2 名情节较轻的犯罪嫌疑人作出不起诉决定。7 月 18 日、7 月 19 日，北京市第二中级人民法院公开开庭审理了本案。

庭审中，50 名被告人对指控的罪名均未提出异议，部分被告人及其辩护人主要提出以下辩解及辩护意见：一是认定犯罪集团缺乏法律依据，应以被告人实际参与诈骗成功的数额认定其犯罪数额。二是被告人系犯罪组织雇佣的话务员，在本案中起次要和辅助作用，应认定为从犯。三是检察机关指控的犯罪金额证据不足，没有形成完整的证据链条，不能证明被害人是被告人所骗。

针对上述辩护意见，公诉人答辩如下：

一是该犯罪组织以共同实施电信网络诈骗犯罪为目的而组建，首要分子虽然没有到案，但在案证据充分证明该犯罪组织在首要分子的领导指挥下，有固定人员负责窝点的组建管理、人员的召集培训，分工担任一线、二线、三线话务员，该诈骗犯罪组织符合刑法关于犯罪集团的规定，应当认定为犯罪集团。

二是在案证据能够证实二线、三线话务员不仅实施了冒充警察、检察官接听拨打电话的行为，还在犯罪集团中承担了组织管理工作，在共同犯罪中起主要作用，应认定为主犯。对从事一线接听拨打诈骗电话的被告人，已作区别对待。该犯罪集团在印度尼西亚和肯尼亚先后设立 3 个窝点，参加过 2 个以上窝点犯罪的一线人员属于积极参加犯罪，在犯罪中起主要

作用，应认定为主犯；仅参加其中一个窝点犯罪的一线人员，参与时间相对较短，实际获利较少，可认定为从犯。

三是本案认定诈骗犯罪集团与被害人之间关联性的证据主要有：犯罪集团使用网络电话与被害人电话联系的通话记录；犯罪集团的 Skype 聊天记录中提到了被害人姓名、公民身份号码等个人信息；被害人向被告人指定银行账户转账汇款的记录。起诉书认定的 75 名被害人至少包含上述一种关联方式，实施诈骗与被骗的证据能够形成印证关系，足以认定 75 名被害人被本案诈骗犯罪组织所骗。

（四）处理结果

2017 年 12 月 21 日，北京市第二中级人民法院作出一审判决，认定被告人张凯闵等 50 人以非法占有为目的，参加诈骗犯罪集团，利用电信网络技术手段，分工合作，冒充国家机关工作人员或其他单位工作人员，诈骗被害人钱财，各被告人的行为均已构成诈骗罪，其中 28 人系主犯，22 人系从犯。法院根据犯罪事实、情节并结合各被告人的认罪态度、悔罪表现，对张凯闵等 50 人判处十五年至一年九个月不等有期徒刑，并处剥夺政治权利及罚金。张凯闵等部分被告人以量刑过重为由提出上诉。2018 年 3 月，北京市高级人民法院二审裁定驳回上诉，维持原判。

【指导意义】

（一）对境外实施犯罪的证据应着重审查合法性

对在境外获取的实施犯罪的证据，一是要审查是否符合我国刑事诉讼法的相关规定，对能够证明案件事实且符合刑事诉讼法规定的，可以作为证据使用。二是对基于有关条约、司法互助协定、两岸司法互助协议或通过国际组织委托调取的证据，应注意审查相关办理程序、手续是否完备，取证程序和条件是否符合有关法律文件的规定。对不具有规定规范的，一般应当要求提供所在国公证机关证明，由所在国中央外交主管机关或其授权机关认证，并经我国驻该国使、领馆认证。三是对委托取得的境外证据，移交过程中应注意审查过程是否连续、手续是否齐全、交接物品是否完整、双方的交接清单记载的物品信息是否一致、交接清单与交接物品是否一一对应。四是对当事人及其辩护人、诉讼代理人提供的来自境外的证据材料，要审查其是否按照条约等相关规定办理了公证和认证，并经我国驻该国使、领馆认证。

（二）对电子数据应重点审查客观性

一要审查电子数据存储介质的真实性。通过审查存储介质的扣押、移交等法律手续及清单，核实电子数据存储介质在收集、保管、鉴定、检查等环节中是否保持原始性和同一性。二要审查电子数据本身是否客观、真实、完整。通过审查电子数据的来源和收集过程，核实电子数据是否从原始存储介质中提取，收集的程序和方法是否符合法律和相关技术规范。对从境外起获的存储介质中提取、恢复的电子数据应当进行无污损鉴定，将起获设备的时间作为鉴定的起始基准时间，以保证电子数据的客观、真实、完整。三要审查电子数据内容的真实性。通过审查在案言词证据能否与电子数据相互印证，不同的电子数据间能否相互印证等，核实电子数据包含的案件信息能否与在案的其他证据相互印证。

（三）紧紧围绕电话卡和银行卡审查认定案件事实

办理电信网络诈骗犯罪案件，认定被害人数量及诈骗资金数额的相关证据，应当紧紧围绕电话卡和银行卡等证据的关联性来认定犯罪事实。一是通过电话卡建立被害人与诈骗犯罪组织间的关联。通过审查诈骗犯罪组织使用的网络电话拨打记录清单、被害人接到诈骗电话号码的陈述以及被害人提供的通话记录详单等通讯类证据，认定被害人与诈骗犯罪组织间的关联性。二是通过银行卡建立被害人与诈骗犯罪组织间的关联。通过审查被害人提供的银行账户交易明细、银行客户通知书、诈骗犯罪集团指定银行账户信息等书证以及诈骗犯罪组织使用的互联网软件聊天记录，核实聊天记录中是否出现被害人的转账账户，以确定被害人与诈骗犯罪组织间的关联性。三是将电话卡和银行卡结合起来认定被害人及诈骗数额。审查被害人接到诈骗电话的时间、向诈骗犯罪组织指定账户转款的时间，诈骗犯罪组织手机或电脑中储存的聊天记录中出现的被害人的账户信息和转账时间是否印证。相互关联印证的，可以认定为案件被害人，被害人实际转账的金额可以认定为诈骗数额。

（四）有明显首要分子，主要成员固定，其他人员有一定流动性的电信网络诈骗犯罪组织，可以认定为诈骗犯罪集团

实施电信网络诈骗犯罪，大都涉案人员众多、组织严密、层级分明、各环节分工明确。对符合刑法关于犯罪集团规定，有明确首要分子，主要成员固定，其他人员虽有一定流动性的电信网络诈骗犯罪组织，依法可以认定为诈骗犯罪集团。对出资筹建诈骗窝点、掌控诈骗所得资金、制定犯罪计划等起组织、指挥管理作用的，依法可以认定为诈骗犯罪集团首要分子，按照集团所犯的全部罪行处罚。对负责协助首要分子组建窝点、招募培训人员等起积极作用的，或加入时间较长，通过接听拨打电话对受害人进行诱骗，次数较多、诈骗金额较大的，依法可以认定为主犯，按照其参与或组织、指挥的全部犯罪处罚。对诈骗次数较少、诈骗金额较小，在共同犯罪中起次要或者辅助作用的，依法可以认定为从犯，依法从轻、减轻或免除处罚。

【相关规定】

《中华人民共和国刑法》第六条、第二十六条、第二百六十六条

《中华人民共和国刑事诉讼法》第十八条、第二十五条

《中华人民共和国国际刑事司法协助法》第九条、第十条、第二十五条、第二十六条、第三十九条、第四十条、第四十一条、第六十八条

《最高人民法院、最高人民检察院、公安部关于办理诈骗刑事案件具体应用法律若干问题的解释》第一条、第二条

《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》

《最高人民法院、最高人民检察院、公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》

《检察机关办理电信网络诈骗案件指引》

《最高人民法院关于适用＜中华人民共和国刑事诉讼法＞的解释》第四百零五条

2.最高人民法院发布 10 起电信网络诈骗犯罪典型案例（2019 年 11 月 19 日）

典型案例目录

案例一、陈文辉等 7 人诈骗、侵犯公民个人信息案

（一）基本案情

2015 年 11 月至 2016 年 8 月，被告人陈文辉、黄进春、陈宝生、郑金锋、熊超、郑贤聪、陈福地等人交叉结伙，通过网络购买学生信息和公民购房信息，分别在江西省九江市、新余市、广西壮族自治区钦州市、海南省海口市等地租赁房屋作为诈骗场所，分别冒充教育局、财政局、房产局的工作人员，以发放贫困学生助学金、购房补贴为名，将高考学生为主要诈骗对象，拨打诈骗电话 2.3 万余次，骗取他人钱款共计 56 万余元，并造成被害人徐玉玉死亡。

（二）裁判结果

本案由山东省临沂市中级人民法院一审，山东省高级人民法院二审。现已发生法律效力。

法院认为，被告人陈文辉等人以非法占有为目的，结成电信诈骗犯罪团伙，冒充国家机关工作人员，虚构事实，拨打电话骗取他人钱款，其行为均构成诈骗罪。陈文辉还以非法方法获取公民个人信息，其行为又构成侵犯公民个人信息罪。陈文辉在江西省九江市、新余市的诈骗犯罪中起组织、指挥作用，系主犯。陈文辉冒充国家机关工作人员，骗取在校学生钱款，并造成被害人徐玉玉死亡，酌情从重处罚。据此，以诈骗罪、侵犯公民个人信息罪判处被告人陈文辉无期徒刑，剥夺政治权利终身，并处没收个人全部财产；以诈骗罪判处被告人郑金锋、黄进春等人十五年至三年不等有期徒刑。

（三）典型意义

电信网络诈骗类案件近年高发、多发，严重侵害人民群众的财产安全和合法权益，破坏社会诚信，影响社会的和谐稳定。山东高考考生徐玉玉因家中筹措的 9 000 余元学费被诈骗，悲愤之下引发猝死，舆论反应强烈，对电信网络诈骗犯罪案件的打击问题再次引发了社会的

广泛关注。为加大打击惩处力度，2016 年 12 月，“两高一部”共同制定出台了《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》，明确对诈骗造成被害人自杀、死亡或者精神失常等严重后果的，冒充司法机关等国家机关工作人员实施诈骗的，组织、指挥电信网络诈骗犯罪团伙的，诈骗在校学生财物的，要酌情从重处罚。本案是适用《意见》审理的第一例大要案，在罪责刑相适应原则的前提下，对被告人陈文辉顶格判处，充分体现了对电信网络诈骗犯罪分子依法从严惩处的精神。

案例二、杜天禹侵犯公民个人信息案

（一）基本案情

被告人杜天禹通过植入木马程序的方式，非法侵入山东省 2016 年普通高等学校招生考试信息平台网站，取得该网站管理权，非法获取 2016 年山东省高考考生个人信息 64 万余条，并向另案被告人陈文辉出售上述信息 10 万余条，非法获利 14 100 元，陈文辉利用从杜天禹处购得的上述信息，组织多人实施电信诈骗犯罪，拨打诈骗电话共计 1 万余次，骗取他人钱款 20 余万元，并造成高考考生徐玉玉死亡。

（二）裁判结果

本案由山东省临沂市罗庄区人民法院一审，当庭宣判后，被告人杜天禹表示服判不上诉。现已发生法律效力。

法院认为，被告人杜天禹违反国家有关规定，非法获取公民个人信息 64 万余条，出售公民个人信息 10 万余条，其行为已构成侵犯公民个人信息罪。被告人杜天禹作为从事信息技术的专业人员，应当知道维护信息网络安全和保护公民个人信息的重要性，但却利用技术专长，非法侵入高等学校招生考试信息平台的网站，窃取考生个人信息并出卖牟利，严重危害网络安全，对他人的人身财产安全造成重大隐患。据此，以侵犯公民个人信息罪判处被告人杜天禹有期徒刑六年，并处罚金人民币六万元。

（三）典型意义

侵犯公民个人信息犯罪被称为网络犯罪的“百罪之源”，由此滋生了电信网络诈骗、敲诈勒索、绑架等一系列犯罪，社会危害十分严重，确有打击必要。本案系被害人徐玉玉被诈骗案的关联案件，被告人杜天禹窃取并出售公民个人信息的行为，给另案被告人陈文辉精准实施诈骗犯罪得以骗取他人钱财提供了便利条件，杜天禹应当对其出售公民个人信息行为所造成的恶劣社会影响承担相应的责任。法院在审理过程中适用“两高”《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》相关规定，案件宣判后，被告人认罪服判未上诉，取得了良好的法律效果和社会效果。

案例三、陈明慧等 7 人诈骗案

（一）基本案情

被告人陈明慧纠集范治杰、高学忠、叶奇锋、熊运江等人结成诈骗团伙，群发“奔跑吧

兄弟”等虚假中奖信息，诱骗收到信息者登录“钓鱼网站”填写个人信息认领奖品，后以兑奖需要交纳保证金、公证费、税款等为由，骗取被害人财物，再通过冒充律师、法院工作人员以被害人未按要求交纳保证金或领取奖品构成违约为由，恐吓要求被害人交纳手续费，2016 年 6 月至 8 月间，共骗取被害人蔡淑妍等 63 人共计 681 310 元，骗取其他被害人财物共计 359 812.21 元。蔡淑妍得知受骗后，于 2016 年 8 月 29 日跳海自杀。陈明慧还通过冒充“爸爸去哪儿”等综艺节目发送虚假中奖诈骗信息共计 73 万余条。

（二）裁判结果

本案由广东省揭阳市中级人民法院一审，广东省高级人民法院二审。现已发生法律效力。

法院认为，被告人陈明慧等人以非法占有为目的，结成电信诈骗犯罪团伙，采用虚构事实的方法，通过利用“钓鱼网站”链接、发送诈骗信息、拨打诈骗电话等手段针对不特定多数人实施诈骗，其行为均已构成诈骗罪。陈明慧纠集其他同案人参与作案，在共同诈骗犯罪中起主要作用，系主犯，又有多个酌情从重处罚情节。据此，以诈骗罪判处被告人陈明慧无期徒刑，剥夺政治权利终身，并处没收个人全部财产；以诈骗罪判处被告人范治杰等人十五年至十一年不等有期徒刑。

（三）典型意义

本案作为高考学生被骗后猝死、自杀等重大案件之一，经媒体报导后，舆论高度关注，法院审理过程中适用“两高一部”《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》规定，以陈明慧组织、指挥电信诈骗团伙，有利用“钓鱼网站”链接、冒充司法机关工作人员、诈骗未成年人、在校学生、造成一名被害人自杀等多个从重处罚情节，在陈明慧实施诈骗既有既遂又有未遂，且达到同一量刑幅度的情况下，以诈骗罪既遂处罚，充分体现了对此类犯罪从严惩处的精神。

案例四、李时权等 69 人诈骗案

（一）基本案情

被告人李时权曾从事传销活动，掌握了传销组织的运作模式，在该模式下建立起 140 余人的诈骗犯罪集团。李时权作为诈骗犯罪集团的总经理，全面负责掌握犯罪集团的活动，任命被告人吴月琼、吴贵飞、闫群霞、闫燕飞、骆金、胡平安等人为主要管理人员，设立诈骗窝点并安排主要管理人员对各个窝点进行监控和管理，安排专人传授犯罪方法，收取诈骗所得资金，分配犯罪所得。该犯罪集团采用总经理-经理-主任-业务主管-业务员的层级传销组织管理模式，对新加入成员要求每人按照 2900 元一单的数额缴纳入门费，按照一定的比例数额层层返利，向组织交单作为成员晋升的业绩标准，层层返利作为对各层级的回报和利益刺激，不断诱骗他人加入该诈骗集团。2016 年 1 月至 2016 年 12 月 15 日期间，该犯罪集团在宁夏回族自治区固原市设立十个诈骗窝点，由多名下线诈骗人员从“有缘网”“百合网”等婚恋交友网站上获取全国各地被害人信息，利用手机微信、QQ 等实时通讯工具将被害人加为好友，再冒充单身女性以找对象、交朋友为名取得被害人信任，能骗来加入组织的加入组织，不能骗来的向其索要路费、电话费、疾病救治费等费用，对不特定的被害人实施诈骗活动，诈骗犯罪活动涉及全国 31 个省市自治区，诈骗非法所得 920 余万元。

（二）裁判结果

本案由宁夏回族自治区固原市原州区人民法院一审，固原市中级人民法院二审。现已发生法律效力。

法院认为，以被告人李时权为首的69名被告人以非法占有为目的，采取虚构事实和隐瞒真相的方式，骗取他人财物，其行为均已构成诈骗罪。本案属于三人以上共同实施犯罪组织的较为固定的犯罪组织，系犯罪集团。李时权对整个犯罪集团起组织、领导作用，是犯罪集团的首要分子，按照集团所犯的全部罪行处罚。被告人吴月琼、骆金、闫燕飞、闫群霞、吴贵飞、胡平安等协助首要分子对整个犯罪集团进行组织、领导、策划，是犯罪集团的骨干分子，系主犯，按照其所参与的或组织指挥的全部犯罪处罚。其他一般犯罪成员按照其在犯罪集团中所起的作用及其个人诈骗数额予以量刑。据此，以诈骗罪判处被告人李时权有期徒刑十四年，并处罚金人民币十万元；以诈骗罪判处被告人吴月琼等人十二年至一年三个月不等有期徒刑。

（三）典型意义

本案以被告人李时权为首的69人犯罪集团利用传销模式发展诈骗成员，计酬返利，不断发展壮大，集团内部层级严密，分工明确，组织特征鲜明。该诈骗集团的犯罪手段新颖，利用社会闲散青年创业找工作的想法，以偏远经济欠发达地区作为犯罪场所，在全国范围内不断诱骗他人加入诈骗集团，利用手机微信、QQ等互联网软件，冒充单身女性，以索要交通费、疾病救治费等为名通过网络诈骗不特定被害人钱财，遍及全国31个省市自治区，造成了恶劣的社会影响。人民法院在审理过程中，对案件的事实、证据、适用法律、定罪、量刑等方面进行全面审查，最终对各被告人判处相应的刑罚，有力打击了猖獗的电信网络诈骗犯罪，维护了社会秩序，挽回了人民群众财产损失。

案例五、陈杰等9人诈骗案

（一）基本案情

被告人陈杰伙同被告人张振、姚登峰等人于2012年9月在湖北省武汉市成立了“武汉康伴益生科技有限公司”和“武汉益生康伴商贸有限公司”。陈杰等人以合法公司为掩护，在武汉市江岸区和江汉区分别设立两个窝点，组织朱娇娇、夏宗禄、刘琼等一百余名团伙成员实施电信诈骗。该团伙购买电脑、电话、手机等工具后，为每名团伙成员注册微信，统一使用伪造的“马天长”“吕柳荫”等人的图片为微信头像和以“秦小姐的补肾方”“马氏中医补肾方”“吕柳荫膏滋团队”等为微信昵称，专门针对患有各种男女生理疾病或脱发人群为目标，在网络、微信公众号等载体上发布治疗男女生理疾病或治疗脱发的广告，诈骗被害人浏览广告并填写联系电话或添加微信号，之后由团伙成员假扮名医或医疗机构专业人员的亲属、学生，根据“话术剧本”，使用电话或微信对被害人进行“问诊”，向被害人介绍产品，让被害人发送舌苔照和手指甲照片，再以客服名义对被害人进行“问诊”，以“指导老师”“健康顾问”名义与被害人沟通，取得信任后诱骗被害人购买不具有药品功效的保健品或食品。自2016年6月16日至11月1日期间，陈杰、姚登峰、张振组织该团伙成员共计诈骗被害人8945人，诈骗钱款1000余万元。

（二）裁判结果

本案由内蒙古自治区达拉特旗人民法院一审，鄂尔多斯市中级人民法院二审。现已发生法律效力。

法院认为，被告人陈杰等人以非法占有为目的，通过虚构事实、隐瞒真相的方式，利用电信网络技术手段，骗取他人财物，数额特别巨大，其行为均已构成诈骗罪。其中，被告人陈杰系共同犯罪中的主犯，应按照其组织的全部犯罪处罚。据此，以诈骗罪判处被告人陈杰有期徒刑十三年，并处罚金人民币四十万元；以诈骗罪判处被告人姚登峰等人十二年至三年不等有期徒刑。

（三）典型意义

当前，一些诈骗分子利用广大群众特别是一些患有特殊疾病或者中老年群众关注自身身体健康的心理，专门针对这些群体，推销所谓的“药品”或者是不具有药品功效的保健品、食品，骗取巨额款项，社会影响极为恶劣。本案以被告人陈杰为首的诈骗集团成立公司为掩护，专门以各种男女生理疾病人群为目标，通过在网络、微信等载体发布虚假广告，假扮名医利用电话或微信“问诊”，采用扩大病情、发送“成功案例”等手段实施诈骗，受害人遍布全国多地，涉案金额高达 1000 余万元，系特大电信诈骗案件，与本案关联的其他 7 起窝案、串案经依法审理，85 名涉案被告人均以诈骗罪定罪处罚。

案例六、黄国良等 9 人诈骗案

（一）基本案情

被告人黄国良、吴希金、廖以冬、龙昌腾、梁宏卫等人谎称一批“海外要员”“海外老人”要回国，每人都有一笔巨额款项要带回大陆发放给老百姓，联系指使童敬侠（另案处理，已判刑）、被告人韩立军等人从事“民族资产解冻大业”，并向童、韩二人发送“国际梅协民族资产解冻委员会”“中华人民共和国委员会馈赠资金发放证明书”“馈赠资金各类收取费用通知”“国家外汇管理局中国银行总行证明”等文件，任命童敬侠、韩立军二人为“国际梅协民族资产解冻委员会”总指挥、副总指挥，以有巨额民族资产需要解冻为由，指使童敬侠、韩立军吸收会员收取会员费。自 2015 年 12 月至 2016 年 5 月，童敬侠、韩立军向全国各地人员收取会费并许诺发放巨额“民族资产解冻善款”，共向全国数十个省份近百万人次收取会费 6 300 余万元，二人将 2 800 余万元转账汇入黄国良、吴希金、龙昌腾等人指定的银行账户。

（二）裁判结果

本案由内蒙古自治区鄂尔多斯市中级人民法院一审，内蒙古自治区高级人民法院二审。现已发生法律效力。

法院认为，被告人黄国良等人以非法占有为目的，虚构民族资产解冻可获得巨额回报的事实，骗取他人财物，数额特别巨大，其行为均已构成诈骗罪。其中，被告人黄国良指使龙

昌腾、梁宏卫等人冒充其助理给童敬侠、韩立军打电话，并多次使用或指使他人使用涉案银行卡在 POS 机上刷卡套现，系共同犯罪中的主犯。据此，以诈骗罪判处被告人黄国良、吴希金、廖以冬无期徒刑，剥夺政治权利终身，并处没收个人全部财产；以诈骗罪判处被告人龙昌腾等人十五年至四年不等有期徒刑。

（三）典型意义

“民族资产解冻”类诈骗犯罪早已有之，随着打击力度的加大，此类犯罪的发案率已经大幅下降甚至在一些地方已经销声匿迹，但近年来随着信息技术的发展，此类犯罪又借助现代通信和金融工具进行传播，逐渐演变成集返利、传销、诈骗为一体的混合型犯罪，极具诱惑性和欺骗性。犯罪分子往往抓住被害人以小博大、以小钱换大钱的心理，唆使被害人加入由被告人虚构的所谓“民族大业”“民族资产解冻”项目或“精准扶贫”等其他假借国家大政方针和社会热点的虚假项目，允诺被害人可以小投入获得大回报，积极组织和发展会员，以办证费、手续费、保证金等名目骗取他人财物。此类诈骗犯罪迷惑性强、传播速度快，往往在短时间内就能造成众多人员受骗，且涉案金额巨大，严重侵害人民群众财产安全，严重损害政府公信力，严重危害社会安定。被告人黄国良等人作为幕后的策划者、组织者和操纵者，指挥、指使童敬侠、韩立军以代理人身份骗取他人巨额财物并从中获取了巨额钱财，系民族资产解冻类犯罪链条的最顶端，也是打击的重点，人民法院对黄国良等人依法判处重刑，可谓罚当其罪。

案例七、童敬侠等 7 人诈骗案

（一）基本案情

被告人童敬侠（女）以前曾参与过号称“民族大业”的活动，随着类似活动的演变，从 2015 年 12 月开始，有所谓的“海外老人”“海外要员”与童敬侠联系，声称海外有三千多亿人民币要发放给老百姓，但不愿意通过政府，想邀请童敬侠具体实施。童敬侠表示同意后，对方发给童敬侠“大陆民族资产解冻委员会总指挥”的任命书。为获取群众信任，童敬侠等人在微信群内散发大量伪造的“任命书”“委托书”“中央军库派令”“梅花令”等身份证明及文件，伪造国务院、财政部、国家扶贫开发领导小组文件，以受中央领导和军委指示及国务院的指派来解冻民族资产为由，对外宣称只要民众交纳报名费、办证费、会员费加入“中华民族大业”组织后，就可以获得等次不同的扶贫款和奖励等高额回报。在童敬侠的领导下，被告人郜玉、张志峰等人先后加入“民族大业”组织，积极从事“解冻民族资产”活动。童敬侠所领导的整个组织实行层级负责制，管理层下设省、市团队负责人，每个团队下设若干大组长，大组长下设小组长，小组长之下就是会员。该组织运行方式为：“海外老人”们的助理将包含“民族资产解冻”内容的宣传资料发送到童敬侠邮箱，管理层人员把项目内容加工整理后以童敬侠名义在手机微信群里发布，要求会员按项目内容交纳几十元、几百元不等的办证费，称在短时间内可获得几十万、几百万不等的高额回报。该组织还以到人民大会堂开会为由收取统一服装费，以公证、转账手续费、保证金等理由收取费用。会员所交的费用由各省市负责人汇总后转款到童敬侠的银行卡上，童敬侠再把款项转到相应项目的“海外老人”助理的银行卡上，“海外老人”及其助理使用 POS 机套现后将资金隐匿。童敬侠所发展的“民族大业”组织遍布全国十多个省市，共骗取他人财物合计 9 500 余万元，其中 4 800 余万元转入“海外老人”助理的银行账户。

（二）裁判结果

本案由湖南省桑植县人民法院一审，张家界市中级人民法院二审。现已发生法律效力。

法院认为，被告人童敬侠等人以非法占有为目的，利用“民族资产解冻”的幌子，虚构事实骗取他人财物，诈骗金额特别巨大，其行为均已构成诈骗罪。童敬侠利用虚假的任命身份等文件，以“民族资产解冻”的名义开展各种以小博大的收费活动，在被群众揭穿及公安机关介入后，又编造谎言继续实施欺骗行为，且系犯罪组织的领导者，纠集、支配其他组织成员。据此，以诈骗罪判处被告人童敬侠有期徒刑十三年，剥夺政治权利三年，并处罚金人民币二十万元；以诈骗罪判处被告人张志峰等人六年至三年不等有期徒刑。

（三）典型意义

本案系被告人黄国良等人诈骗案的关联案件，被告人童敬侠系受民族资产解冻类犯罪代理人，即受幕后组织操纵者黄国良等人的指使，负责推广虚假项目，发展、管理会员，收取钱财的管理人员。各级代理人对幕后组织操纵者言听计从，建微信群、拉人头，大肆发展下线，收取各种名目的费用，沦为诈骗犯罪分子的工具。部分代理人甚至在识破幕后操纵者的骗局后，自行巧立名目，捏造各种虚假项目继续实施诈骗。代理人的存在，对于“民族资产解冻”类诈骗犯罪能够在短时间内迅速层层发展下线，呈裂变式传播，不断扩大涉案被害人规模起到巨大作用，危害后果十分严重，是司法机关依法从严打击的对象。

案例八、朱涛等人诈骗案

（一）基本案情

2013 年 5 月，被告人朱涛出资组建榆林农惠现货交易平台，纠集和聘用被告人艾阳、陈超、姚伟林加入，与代理商勾结，先以可提供所谓的内幕交易信息为由，诱骗客户进入电子商务平台进行交易，后通过指令操盘手，采用抛单卖出或用虚拟资金购进产品的手段，控制产品大盘行情向客户期望走势相反的方向发展，通过虚假的产品行情变化，达到使被诱骗加入平台交易的客户亏损的目的。朱涛等人有时也刻意在客户小额投资后，促其盈利，以骗其投入大额资金，牟取大额客损。2013 年 9 月至 2014 年 2 月期间，朱涛、艾阳、陈超、姚伟林通过上述以虚拟资金操控交易平台的手段，共骗取客户资金 215 余万元。按照事先与代理商约定的比例计算，朱涛、艾阳、陈超、姚伟林从中获得诈骗资金约 75 万元。

（二）裁判结果

本案由湖南省南县人民法院一审，益阳市中级人民法院二审。现已发生法律效力。

法院认为，被告人朱涛以非法占有为目的，纠集和聘用被告人艾阳、陈超、姚伟林，利用电子商务平台，操纵农产品行情诱骗客户交易，从客损中获利，数额特别巨大，其行为均已构成诈骗罪。在共同犯罪中，朱涛纠集人员参与犯罪，发起、组织和统筹运作交易活动，艾阳通过给操盘手下达指令控制平台虚拟行情走势，实施欺诈行为，均系主犯。据此，以诈骗罪判处被告人朱涛有期徒刑十四年，以诈骗罪判处被告人艾阳、陈超、姚伟林十一年至四年不等有期徒刑，并处十万元至六万元不等罚金。

（三）典型意义

电信网络诈骗案件的犯罪手法隐蔽性强，花样翻新快。本案中，被告人先成立网上交易平台，利用业务员及代理商吸收客户，以提供虚假内幕交易信息为由，骗取客户进入平台交易，当客户高价买入相关农产品后，再指令操盘手运作人为造成跌势，迫使客户低价卖出，以牟取大额客损。此种新型网络诈骗犯罪手段更加隐蔽，迷惑性强，容易使人上当受骗。虽然被告人是借助电子商务平台进行交易，但其行为本质仍在于虚构事实、隐瞒真相，以达到非法占有他人财物的目的，其行为完全符合诈骗罪特征，本案定罪准确。

案例九、邵庭雄诈骗案

（一）基本案情

2014 年底，被告人邵庭雄受他人纠集，明知是通过电信诈骗活动收取的赃款，仍然从银行取出汇入上线指定的银行账户，并从中收取取款金额的 10%作为报酬。之后，邵庭雄发展张阳作为下线，向张阳提供了数套银行卡，承诺支付取款金额的 5%作为报酬，同时要求张阳继续发展多名下线参与取款。通过上述方式，邵庭雄逐步形成了相对固定的上下线关系。自 2014 年 12 月至 2015 年 7 月，被告人邵庭雄参与作案 38 起，涉案金额 48.44 万元。2016 年 2 月，邵庭雄到公安机关投案。

（二）裁判结果

本案由湖南省津市市人民法院一审，被告人邵庭雄服判未上诉。现已发生法律效力。

法院认为，被告人邵庭雄以非法占有为目的，伙同他人利用电信网络采取虚构事实的方法，骗取他人财物，数额巨大，其行为已构成诈骗罪。本案系通过拨打电话、发短信对不特定的人进行诈骗，且系多次诈骗，酌情对被告人邵庭雄从重处罚。本案系共同犯罪，在犯罪过程中，邵庭雄仅参与了转移诈骗赃款的过程，起辅助作用，系从犯，可从轻处罚。且邵庭雄有自首情节，可依法从轻处罚。据此，以诈骗罪判处被告人邵庭雄有期徒刑五年三个月，并处罚金人民币五万元。

（三）典型意义

围绕电信网络诈骗犯罪，诱发、滋生了大量上下游关联违法犯罪，这些关联犯罪为诈骗犯罪提供各种“服务”和“支持”，形成以诈骗为中心的系列“黑灰色”犯罪产业链，如出售、提供公民个人信息、帮助转移赃款等活动。“两高一部”《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》对于全面惩处关联犯罪作出了明确规定。本案中，被告人邵庭雄明知赃款是诈骗犯罪所得，仍为诈骗分子转移犯罪赃款提供帮助和支持，对其以诈骗罪的共犯判处，体现了司法机关对电信网络诈骗关联犯罪从严惩处的态度。

案例十、杨学巍诈骗案

（一）基本案情

2018 年 7 月，被告人杨学巍伙同他人在海南省儋州市兰洋镇，利用电信网络，实施招嫖诈骗活动。杨学巍等人冒充可上门提供性服务的女性，使用作案微信与被害人聊天，获取被害人信任后，其他同伙负责给被害人打电话并发送二维码诱骗被害人转账付款，诈骗所得款由杨学巍分得 20%。通过以上方式，杨学巍共计骗取被害人 12 696 元。

（二）裁判结果

本案由海南省儋州市人民法院一审，被告人杨学巍服判未上诉。现已发生法律效力。

法院认为，被告人杨学巍以非法占有为目的，伙同他人通过互联网发布虚假信息，实施诈骗，骗取他人数额较大的财物，其行为已构成诈骗罪。杨学巍在犯罪过程中负责使用作案微信与被害人聊天，并分得诈骗所得款的 20%，在共同犯罪中是主犯，且系诈骗累犯，依法应从重处罚。据此，以诈骗罪判处被告人杨学巍犯有期徒刑二年一个月，并处罚金人民币二万元。

（三）典型意义

近年来，微信招嫖类诈骗案件在多地发生。作为一种新型的诈骗案件，因案件受害人系招嫖被骗，发案后心存顾虑，多选择吃哑巴亏而不予报案，导致侦破和打击难度加大。此类案件虽然案值不大，但严重败坏了社会风气，对当地治安形势造成恶劣影响。本案的审理体现了人民法院对此类新型诈骗犯罪行为从严打击的决心和力度。

3.最高人民法院发布六起惩治电信诈骗犯罪典型案例（2016 年 9 月 30 日）

电信诈骗犯罪典型案例（北京）

案例一、戴春波等 32 人诈骗案

（一）基本案情

2013 年 8 月，北京市海淀区人民法院审结一起跨国团伙电信诈骗案，对戴春波等三十余名被告人以诈骗罪判处刑罚。

2011 年 8 月底，被告人戴春波、王瑞讯、周娟受雇佣参加他人组织的针对中国大陆公民的电信诈骗团伙，并持旅游签证出境到老挝人民民主共和国，后被安排在位于万象市西沙达腊彭巴报村的 24 组一栋别墅内从事电信诈骗活动。三人主要负责接听被害人回拨的电话，并按月领取工资及提成。戴春波等实施诈骗行为的方式为：一名台湾男子每天通过互联网向全国各地发送语音包，内容是对方因涉嫌恶意透支信用卡被法院传唤，需要查询详情的就会给转接人工查询，戴春波等三人便冒充法院工作人员接听电话，并按照话术内容告诉对方恶意透支信用卡未还钱涉嫌刑事犯罪，若对方予以否认，便帮助对方将电话转接给二线人员，由二线人员冒充公安局工作人员继续进行诈骗，诱导被害人向指定账户内转账或汇款，从而骗取被害人钱财。同年 9 月 26 日，戴春波等三人在该别墅内被老挝国家警察局抓获，同年 9 月 30 日被移交我国公安机关。

2011 年 8 月底至 9 月初，被告人黄辉云等二十九人相继受雇佣参加他人组织的针对中国大陆公民的电信诈骗团伙，并持旅游签证出境到老挝人民民主共和国，在位于万象市西沙达腊县撒潘通村 19 组的一栋别墅内从事电信诈骗活动。黄辉云等二十九人主要负责接听被

害人回拨的电话，并按月领取工资及提成。诈骗团伙成员冒充公安局、检察院和法院等司法机关工作人员，按照话术要求，接听被害人回拨的电话，虚构被害人的信用卡因购物等被恶意透支的虚假信息，诱使对方向指定账户内转账或汇款，从而骗取被害人钱财。同年 9 月 16 日，该团伙于从被害人马某某处成功骗取人民币 41 万元。经马某某报案，9 月 26 日，黄辉云等二十九人在该别墅内被老挝国家警察局抓获， 9 月 30 日被移交我国公安机关。

（二）裁判结果

海淀法院经审理认定，戴春波等三十二名被告人以非法占有为目的，利用拨打电话等电信技术手段对不特定多数人实施诈骗，构成诈骗罪；该诈骗团伙冒充公检法工作人员实施的跨国电信诈骗行为不仅损害司法机关声誉，而且严重干扰了广大群众的正常生活，故对三十二名被告人以诈骗罪分别判处二年六个月至六年不等的有期徒刑，并处罚金。

（三）典型意义

电信诈骗犯罪多为团伙作案，根据统计，北京法院有 50%以上的电信诈骗案件出现三人及三人以上的诈骗团伙。本案系近年来北京法院受理的个案中被告人人数最多的跨国电信诈骗犯罪，诈骗团伙通过在互联网上发布“招聘信息”招揽人手并将其安置于境外，冒充公检法单位工作人员，通过向境内拨打电话的方式，形成严密的话术体系，从而获得被害人信任，诱使被害人向其汇款，达到诈骗钱款的目的。近年来，电信诈骗借助互联网技术的发展，愈发呈现出跨地域、团伙作案、难辨认、受害范围广等特点，给人民财产造成了巨大损失，社会危害性极大。海淀法院通过本案的审理给所有参与诈骗的犯罪分子以法律制裁，有效打击了电信诈骗犯罪，为办理跨国类电信诈骗案件积累了宝贵的经验。

案例二、吉秀燕等 14 人诈骗案

（一）基本案情

2011 年 8 月至 9 月间，被告人吉秀燕、李开琴、欧阳秀真、夏凤仪、夏秋怡、赖炳同、赖庆汉、陈冬冬、赖韩韩、庄敬意、林智强、杨剑、张西、张叶伙同赖伟城（已判刑）先后出境前往印度尼西亚，于 2011 年 9 月 16 日至 9 月 26 日期间，在印度尼西亚雅加达市一别墅内，分别作为一线、二线、三线人员，冒充中华人民共和国公安机关工作人员身份，通过电信技术手段，采用向中国居民拨打电话的方法，向被害人虚构个人信息泄露、涉嫌犯罪、资产需要保全等事实，诈骗 48 名被害人共计人民币 462 万余元。其中被告人陈冬冬、赖韩韩、庄敬意、林智强参与诈骗金额共计人民币 405 万余元，被告人杨剑参与诈骗金额共计人民币 303 万余元。14 名被告人于 2011 年 9 月 26 日被抓获。

（二）裁判结果

北京市东城区人民法院经审理认为，被告人吉秀燕、李开琴、欧阳秀真、夏凤仪、夏秋怡、赖炳同、赖庆汉、陈冬冬、赖韩韩、庄敬意、林智强、杨剑、张西、张叶以非法占有为目的，共同通过电信技术手段，采取虚构事实、隐瞒真相的方法，骗取他人钱财，且数额特别巨大，14 名被告人的行为侵犯了公民的财产权利，均已构成诈骗罪，依法应予刑罚处罚。其中，被告人吉秀燕、李开琴共同负责对别墅内人员的诈骗活动进行管理，且作为三线话务员直接骗取被害人钱款，二被告人在共同犯罪中起主要作用，属于主犯。依照刑法有关规定，以诈骗罪判处 14 名被告人五年至十二年不等的有期徒刑，并处相应数额的罚金。

（三）典型意义

在电信诈骗案件中，诈骗金额、被害人人数、诈骗次数、诈骗手段、情节、危害后果等因素都会影响被告人的量刑。本案中，14 名被告人在境外集中居住于别墅内，共同参与电信诈骗活动，且分工明确，有一定的组织性，已形成固定的犯罪团伙。每名被告人参与的诈骗金额均在百万元以上，且案发后赃款并未追回，给 48 名被害人造成了巨大的经济损失，故东城法院最终对 14 名被告人全部判处了有期徒刑五年以上的重刑，两名主犯被判处十二

年有期徒刑，对于电信诈骗犯罪案件形成了极大的震慑。

电信诈骗犯罪典型案例（福建）

案例三、陈观湖、陈礼华、陈黄华诈骗案

2015 年 3 月 28 日至 4 月 16 日，被告人陈观湖、陈礼华从陈某华、张某鑫（均另案处理）处拿来数十张银行卡，相互配合，共同保管、使用涉案银行卡，在福建福州、厦门、泉州等地将 27 名被害人因受骗汇入的钱款取出，收取相应提成后，汇入诈骗人员提供的账户，涉案金额人民币 637721 元。2015 年 3 月 2 日至 7 日期间，被告人陈黄华伙同陈某华、张某鑫，明知是被害人因受骗汇入的钱款，仍驾驶车辆前往江西等地多次取款，涉案金额共计人民币 108888 元。

（二）裁判结果

本案由福建省闽侯县人民法院一审，福建省福州市中级人民法院二审，现已发生法律效力。

法院认为，被告人陈观湖、陈礼华、陈黄华明知他人进行电信诈骗，仍结伙对涉案诈骗款项实施取款并转移，致使被害人被骗款项无法追回，其行为已构成诈骗罪的共同犯罪，诈骗数额应当按照共同取款数额计算。三名被告人所实施的提取并转移被骗款项的行为，是诈骗集团成功控制诈骗款的最后一个环节，三人在整个电信诈骗的共同犯罪中仅有分工不同，并无主次之分。据此，依法以诈骗罪对被告人陈观湖判处有期徒刑十三年，并处罚金人民币十万元；对被告人陈礼华判处有期徒刑十三年，并处罚金人民币十万元；对被告人陈黄华判处有期徒刑四年三个月，并处罚金人民币二万元。

（三）典型意义

近年来，随着网络电信诈骗日益猖獗，此类犯罪行为形成的产业链也呈现出专业化、跨区域性、集团化之趋势，涵盖了购买设备、拨打电话、群发短信、假冒身份虚构事实、骗取钱款、转账取款等行为过程。为了逃避侦查，电信诈骗犯罪中的取款、转移赃款等行为往往由犯罪行为实施地以外的多个地方的专门取款人完成。本案中的三名被告人，虽未参与前一阶段对被害人的具体诈骗行为，但其明知所取款项是诈骗犯罪所得，而与前阶段诈骗犯罪人员相互配合，辗转各地为诈骗犯罪团伙转取款，其行为是整个骗局得逞、诈骗分子获得钱款的重要环节，应以诈骗犯罪共犯定罪量刑。

案例四、林炎、胡明浪诈骗案

（一）基本案情

2015 年 10 月 18 日至 21 日，被告人林炎、胡明浪和杨东昊（另案处理）经事先共谋，由杨东昊提供伪基站并事先编辑好诈骗短信，指使被告人林炎、胡明浪在福州市鼓楼区、台江区、仓山区、闽侯县上街镇等地使用伪基站，屏蔽干扰以该伪基站为中心一定范围内的通讯运营商信号，搜取屏蔽范围内用户手机卡信息，冒充“95533、10086、95588”等相关客服号码向手机用户发送虚假短信 30801 条，企图骗取手机用户的信任，点击短信中的钓鱼网站、填写相关银行账户信息，以达到骗取手机用户钱款的目的。

（二）裁判结果

本案由福建省福州市鼓楼区人民法院一审，福建省福州市中级人民法院二审，现已发生法律效力。

法院认为，被告人林炎、胡明浪以非法占有为目的，伙同他人利用电信技术手段发送虚假短信，对不特定多数人实施诈骗，情节严重，其行为已构成诈骗罪。被告人林炎、胡明浪已经着手实行犯罪，由于意志以外的原因而未得逞，是犯罪未遂，可以比照既遂犯从轻处罚。

被告人林炎、胡明浪如实供述自己的罪行，是坦白，可以从轻处罚。据此，依法以诈骗罪分别对被告人林炎、胡明浪判处有期徒刑三年七个月，并处罚金人民币五千元。

（三）典型意义

近两年来，利用伪基站实施电信诈骗的手段翻新、案件频发，最高人民法院、最高人民检察院专门出台了相关司法解释，加大对此类违法犯罪行为的打击力度，明确规定：对电信诈骗数额难以查证，但发送诈骗信息5000条以上，拨打诈骗电话500人次以上的，或者诈骗手段恶劣、危害严重的，即可以诈骗罪（未遂）追究刑事责任。本案被告人林炎、胡明浪通过“伪基站”，向不特定多数人发送冒充银行或移动运营商客服电话的虚假短信三万余条，诱骗手机用户点击短信中的钓鱼网站、填写相关银行账户信息以达到骗取手机用户钱款的目的。虽因意志以外的原因，被告人的犯罪目的未能最终得逞，但其犯罪行为仍具有严重的社会危害，公民个人若未及时查觉，其财产便会处于一种极不安全的状况。

案例五、邓之桂、龙碧燕、刘春艳、刘海英诈骗案

（一）基本案情

台湾地区人员“阿水”等人（均另案处理）组织犯罪团伙在老挝万象一栋别墅内进行电信诈骗活动，将事先编辑好的诈骗语音包通过网络电话向中国大陆各省市固定电话用户群发送语音信息，谎称被害人涉嫌用医保卡购买违禁药品需向公安机关报备。待被害人回拨时，电话转到冒充医保中心工作人员的被告人刘春艳、龙碧燕等一线人员，让被害人“报案”并让其拨打预先改好显示号码的“公安局号码”，后由冒充公安机关工作人员的二线人员接听，谎称被害人银行账户存在安全问题，将电话转给冒充检察院工作人员的被告人邓之桂等三线人员要求被害人将银行卡内的存款转到指定账户进行资金清查比对，以此实施诈骗犯罪。被告人刘海英主要负责为该犯罪团伙做饭，同时亦冒充一线医保中心人员参与诈骗。邓之桂、刘海英、龙碧燕、刘春艳与其他同案人诈骗数额达人民币10369340元。

（二）裁判结果

本案由福建省晋江市人民法院一审，福建省泉州市中级人民法院二审，现已发生法律效力。

法院认为，被告人邓之桂、龙碧燕、刘春艳、刘海英的行为均已构成诈骗罪，且犯罪数额特别巨大。在共同犯罪中，四被告人受纠集在该团伙中按照分工，互相配合共同实施诈骗犯罪，获利相对较少，起次要、辅助作用，是从犯，予以减轻处罚。被告人龙碧燕、刘春艳犯罪后自动投案，并如实供述自己的罪行，是自首，可以从轻或减轻处罚。被告人邓之桂、刘海英归案后如实供述自己的罪行，是坦白，可以从轻处罚。被告人刘春艳、刘海英归案后协助公安机关抓获同案犯、其他犯罪嫌疑人，有立功表现，可以从轻或减轻处罚。本案部分赃款被追缴，可对四被告人予以酌情从轻处罚。综上，对四被告人均予以减轻处罚，以诈骗罪对被告人邓之桂、龙碧燕、刘春艳、刘海英判处有期徒刑七年至三年不等，并处罚金人民币八万元至一万元不等。

（三）典型意义

本案是台湾地区人员在境外组织实施的以发送医保卡出现异常的虚假语音信息进行诈骗的典型案件。被告人邓之桂等人受纠集参加他人组织的诈骗团伙，发送医保卡异常的虚假语音信息，而后分别冒充医保中心工作人员、公安人员、检察院工作人员进行连环诈骗，

套取被害人的个人信息，并诱骗被害人将存款转至“指定银行账户”，从而骗取钱款，社会危害性大。在此提醒广大参保人员不要轻信医保卡出现异常的电话语音信息，更不要轻易将银行账号、密码等个人重要信息告知陌生人，以免上当受骗。

案例六、杨海鸿、黄晋河、吴彩云诈骗，杨海鸿、黄晋河侵犯公民个人信息案

（一）基本案情

2015 年 7 月至 9 月 9 日，被告人杨海鸿单独或伙同被告人黄晋河通过购买的方式非法获取公民个人信息 2 万余条，并雇用被告人吴彩云在福建省龙岩市武平县平川镇租住房等地，通过拨打上述公民个人信息中的手机号码，谎称可以向对方发放残疾人补贴、教育补贴等方式，骗取被害人将钱款转入指定的账户。截至 2015 年 9 月 9 日被查获时，被告人杨海鸿、吴彩云共骗取人民币 70000 元，其中，被告人黄晋河自 2015 年 8 月 12 日以来参与骗取 17700 元。

（二）裁判结果

本案由福建省安溪县人民法院一审，福建省泉州市中级人民法院二审，现已发生法律效力。

法院认为，被告人杨海鸿、黄晋河、吴彩云以非法占有为目的，采用虚构事实的方法，骗取公民财物，数额较大，其行为均已构成诈骗罪，属共同犯罪；被告人杨海鸿单独或伙同被告人黄晋河通过购买的方式非法获取公民个人信息，情节严重，其行为均已构成侵犯公民个人信息罪，部分属共同犯罪。在共同犯罪中，被告人杨海鸿、黄晋河起主要作用，是主犯，应按其参与的全部犯罪处罚；被告人吴彩云起次要作用，是从犯，依法从轻处罚。被告人杨海鸿、黄晋河在判决宣告前一人犯数罪，应当数罪并罚。归案后，三被告人如实供述自己的罪行，是坦白，可以依法从轻处罚。据此，以诈骗罪、侵犯公民个人信息罪判处被告人杨海鸿有期徒刑二年四个月，并处罚金人民币一万七千元，以诈骗罪判处被告人吴彩云有期徒刑一年三个月，并处罚金人民币三千元，以诈骗罪、侵犯公民个人信息罪判处被告人黄晋河有期徒刑八个月，并处罚金人民币六千元。

（三）典型意义

近年来，信息技术的广泛应用让我们的生产生活变得更高效便捷，但也给犯罪分子利用信息技术实施犯罪提供了便利条件。本案中，被告人杨海鸿、黄晋河通过互联网非法购买公民个人信息数万条，雇佣他人共同冒充政府工作人员拨打诈骗电话，通过提供被害人准确的身份信息，骗取被害人的信任，以达到实施诈骗犯罪的目的。公民个人信息权利保护已成为信息化社会中公民权利保护的一个重点。要从源头整治电信网络诈骗犯罪，信息安全保护是关键。除了公民要提高信息保护意识以外，各有关单位等也需加强信息管理与信息安全保护工作，不给犯罪分子以可乘之机。

4.京东刷单骗局

加专员 QQ ⟶ 下载注册京东 APP ⟶ 扫码登录 ⟶ 专员给发派订单，代付款 ⟶ 截图返还本金+佣金 ⟶ 再继续发单代付款（需付 3 次，3 单一任务）⟶ 查看我的订单，几分钟后订单已被删除 ⟶ 无法退还代付款的本金与该单的佣金

5.最高人民检察院充分发挥检察职能推进网络空间治理典型案例之一：陈某、宋某琦等 5 人诈骗案(2020)鲁 0991 刑初 20 号

一、基本案情

2018 年 6 月，陈某伙同他人套牌搭建了 FXDD 外汇投资平台，纠集宋某琦等人作为代理商，对外虚构系正规平台、大量交易可获利的信息，诱骗被害人向平台转入资金。该投资平台实行资盘分离，被害人资金并未进入真实交易市场，而是由陈某转移控制支配。陈某与代理商约定，以客户资金亏损数额为分成依据。

其中，2018 年 7、8 月起，宋某琦在河南省许昌市购置电脑、租赁民房作为诈骗场所，招募郭某辉、卢某、胡某波等人作为业务员，以婚恋网站女性会员为目标实施诈骗。宋某琦安排业务员，使用虚假的身份信息，冒用他人头像，包装为投资经验丰富的中年成功男士，在某知名婚恋网站上搭识许某某等 3 名有经济实力的单身中年女性。业务员通过事先培训的话术与被害人建立虚假恋爱关系，骗取感情信任后，通过宣称自己是投资高手，有好的投资渠道，能够指导被害人投资快速赚钱，引诱被害人向陈某搭建的 FXDD 平台投资，并通过鼓励追加投资、代为操作等方式致其账面亏损，营造投资损失假象，以掩饰资金已被非法占有并分赃的事实，共计诈骗人民币 774 万余元。此外，陈某还通过其他代理商诈骗 43 名被害人资金，合计人民币 534 万余元。

二、诉讼过程

2019 年 10 月 16 日，山东省泰安市公安局高新技术产业开发区分局以陈某等 5 人涉嫌诈骗罪，移送泰安高新技术产业开发区人民检察院审查起诉。本案在移送审查起诉时，涉嫌诈骗金额 510 余万元。检察机关审查后两次退回补充侦查，提出明确可行的补充侦查提纲，引导公安机关补充相关证据，深挖案件线索，认定诈骗金额 1300 余万元。2020 年 4 月 3 日，泰安高新技术产业开发区人民检察院以诈骗罪对陈某等 5 人提起公诉。同年 11 月 13 日，泰安高新技术产业开发区人民法院作出一审判决，以诈骗罪分别判处陈某、宋某琦、郭某辉、卢某、胡某波等 5 名被告人有期徒刑五年六个月至十二年不等，并处罚金。

三、典型意义

（一）“杀猪盘”式诈骗多发高发，社会危害大，应当依法严惩。以网络婚恋交友为诱饵实施的虚假投资诈骗，俗称“杀猪盘”，已经成为电信网络诈骗犯罪的主要方式之一。犯罪分子为实现诈骗目的，招募人员在婚恋网站或使用即时通讯工具搭识被害人，通过将自己包装为成功男士或美貌女性，使用专门话术，骗取被害人感情信任、建立虚假恋爱关系，诱导、怂恿其到虚假交易平台大量投资，从而骗取钱财。当被害人察觉被骗或者已无钱可供诈骗后，犯罪分子即将被害人“拉黑”或关闭平台账号。与传统诈骗犯罪不同，“杀猪盘”式诈骗以感情为诱饵，迷惑性强，持续时间长，严重侵害被害人的财产安全，欺骗被害人感情，甚至可能造成被害人自杀等严重后果，应当依法严厉打击，斩断犯罪链条，全面查处犯罪黑灰产，形成有力震慑。

（二）切实提高防范意识，谨慎交友投资。单身男女在网络征婚交友中，要提高警觉性和防范意识，不要被网络爱情冲昏头脑，不轻信陌生人，不轻信花言巧语，认真核实对方真实身份。当对方提出带领自己投资时，要尤其慎重，投资前充分了解平台资质、投资方式、投资对象、获利模式以及国家的相关法律政策，防止误入骗局。一旦发现被骗，要第一时间向公安机关报案，有利于对犯罪行为的及时惩处。

（三）加强婚恋交友网站监管，防止成为犯罪“温床”。婚恋网站、交友平台要严格按照国家法律法规和行业规则，切实履行平台责任，加强注册人员管理和风险提示。对于会员的举报，及时受理核实，积极向有关部门提供相关证据材料。

（七）职务侵占罪

1.《刑事审判参考》指导案例第 461 号：王一辉、金珂、汤明职务侵占案

裁判摘要：

被告人利用职务上的便利，在设定的游戏角色身上，通过修改数据生成极品“武器、装备”出售给其他玩家进行获利的行为构成职务侵占罪。

（一）虚拟财产可以成为《刑法》保护的对象

“网络虚拟财产”一般指网民、游戏玩家在网络游戏中的账号积累的“装备”“货币”“宠物”等“财产”，已经具备了商品的一般属性，寻求法律保护是合理的。近年来，随着互联网用户的激增，少数不法分子利用互联网，大肆进行盗窃、诈骗等侵犯网络虚拟财产的犯罪，给公私财产造成很大的损失，这种犯罪手段往往较为隐蔽，不易查获，其社会危害性也较大，仅通过民事或行政处罚手段尚难以遏制日益猖獗的网络犯罪活动，需要动用刑法手段进行惩处。对此，2000 年 12 月 28 日《全国人大常委会关于维护互联网安全的决定》第 4 条就明确规定：“为了保护个人、法人和其他组织的人身、财产等合法权利，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：（一）利用互联网侮辱他人或者捏造事实诽谤他人；（二）非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密；（三）利用互联网进行盗窃、诈骗、敲诈勒索。”

（二）利用职务便利盗卖游戏“武器、装备”的行为构成职务侵占罪

被告人王一辉利用职务上的便利将所在单位的财产盗出后出售牟利的行为构成职务侵占罪。对于被告人金珂、汤明，虽然不属于被害单位的工作人员，但其与被告人王一辉共同勾结、相互配合，共同利用王一辉的职务便利实施了侵占盛大公司财产的犯罪行为，符合 2000 年《最高人民法院关于审理贪污、职务侵占案件如何认定共同犯罪的问题的解释》第 2 条的规定，三被告人属于共同犯罪，应当以职务侵占罪的共犯论处，因此法院以职务侵占罪对本案三被告人进行定罪处罚是正确的。

——《刑事审判参考》2007 年第 5 集（总第 58 集）

来源：《最高人民法院司法观点集成(新编版)·刑事卷 III》1669 页

附：王一辉、金珂、汤明职务侵占案判决

一、基本案情

被告人王一辉，男，1977 年 8 月 31 日出生，大学本科文化，原系上海盛大网络发展有限公司游戏项目管理中心运维部副经理。因涉嫌犯侵犯著作权罪于 2005 年 10 月 13 日被逮捕。

被告人金珂，男，1977 年 10 月 23 日出生，高中文化，系浙江省师范大学教务处多媒体办公室工作人员。因涉嫌犯侵犯著作权罪于 2005 年 11 月 24 日被逮捕。

被告人汤明，男，1977 年 5 月 30 日出生，大学本科文化，无业。因涉嫌犯侵犯著作权罪于 2005 年 10 月 13 日被逮捕。

上海市浦东新区人民检察院以被告人王一辉、金珂、汤明犯侵犯著作权罪向上海市浦东新区人民法院提起公诉。

被告人王一辉对公诉机关指控其获利120余万元有异议，对其余事实无异议。其辩护人认为被告人的行为不构成犯罪，理由是：（1）被告人的行为不符合侵犯著作权罪的构成要件。首先，王一辉等人实施的是修改数据的行为，而不是复制计算机软件的行为，且游戏中的虚拟“武器”及“装备”不能认定为软件，因此被告人王一辉的行为不能认定是对软件的复制；其次，被告人的行为不属于发行计算机软件，被告人并未实施销售“热血传奇”游戏软件的行为，其销售的是从属于“热血传奇”游戏软件的“武器”及“装备”；最后，数据并不是我国著作权法保护的范围，“热血传奇”游戏数据库中的数据并不具有独创性，因此被告人对不具有知识产权利益的数据库文件中的数据进行修改，不构成侵犯著作权罪。（2）我国刑法对财产权的保护仅限于有形财产和无形财产，不涉及虚拟财产，根据罪刑法定原则，被告人的行为不能以犯罪论处。（3）公诉机关以三被告人之间银行卡资金往来的数额认定获利是不科学的，因为不排除银行卡资金往来存在错误的可能性或者存在其他来源和用途的可能性。同时，即便被告人认可了这些数额，没有其他证据印证也不能作为认定的依据，而只有通过“5173”交易网站和找到具体交易的玩家，才能认定获利的金额。（4）被告人王一辉有自首情节。

被告人金珂对公诉机关指控的事实无异议。其辩护人认为被告人的行为不构成犯罪，理由是：（1）被告人金珂实施的行为是修改游戏玩家的数据库，与复制、发行有着本质的区别，被告人没有复制软件，也没有向公众提供软件的复制件。刑法对于侵犯著作权所规定的打击范围并不包括修改行为，根据法无明文规定不为罪的原则，被告人的行为不构成侵犯著作权罪。（2）起诉书认定被告人金珂的获利金额没有充分的证据支持，审计结论是在没有银行原始凭证的情况下所作的一种推断，在金珂与王一辉的资金往来中有一部分是合法的借款关系。（3）被告人金珂有自首情节，应从轻或减轻处罚。

被告人汤明对公诉机关指控的事实无异议。其辩护人认为被告人的行为不构成犯罪，理由是：（1）修改不同于复制，修改并非著作权犯罪的构成要件。被告人是通过修改数据以实现其获利，玩家游戏数据库的修改并没有改变著作权人编写的计算机软件，故本案不涉及修改、复制计算机软件。（2）“热血传奇”游戏的著作权人是韩国公司而不是盛大公司，软件的复制发行权属于著作权人，而本案中著作权人的利益并未因被告人的行为受到损害，因此不存在社会危害性。

（3）我国刑法对被告人的行为并无相关的法律规定，因此也不构成其他犯罪。

上海市浦东新区人民法院经公开审理查明：

被告人王一辉原系盛大公司游戏项目管理中心运维部副经理，主要负责对服务器、游戏软件进行维护和游戏环境内容的更新等。2004年8月底，被告人王一辉与被告人金珂通过网上聊天，预谋利用王一辉在盛大公司工作，有条件接触“热血传奇”游戏软件数据库的便利，复制游戏武器装备予以销售。2004年9月起，被告人王一辉、金珂开始实施上述行为。由金珂首先在“热血传奇”游戏中建立人物角色，然后将游戏角色的相关信息通过聊天记录发送给王一辉，王一辉在盛大公司内利用公司的电脑进入游戏系统，同时打开“热血传奇”服务器6000端口，通过增加、修改数据库Mir.DB文件中的数据，在金珂创建的游戏人物身

上增加或修改游戏“武器”及“装备”。然后由金珂将游戏人物身上的武器及装备通过“www.5173.com”网站或私下交易出售给游戏玩家。2005 年 2 月，王一辉又趁回金华老家探亲的机会将此事告诉被告人汤明，汤明表示愿意一起加入，并采用同样的方法与王一辉共同实施，非法复制并销售游戏“武器”及“装备”。一段时间后，由于王一辉认为上述操作方法比较麻烦，就让金珂、汤明从网上下载了“热血传奇”私服游戏服务器端，并生成一个伪造的数据包，王一辉负责打开“热血传奇”游戏服务器 6000 端口，同时将服务器的 IP 地址告诉金珂、汤明，由金珂、汤明将每次修改后的数据包发送到服务器，王一辉在收到数据包后，提取数据信息再传送到数据库中，在游戏人物的身上增加或修改游戏“武器”及“装备”。三被告人约定金珂、汤明在出售游戏“武器”及“装备”得款后，分给被告人王一辉 60%的获利，由金珂、汤明将款项汇人王一辉以其本人及“张存”的名义在中国工商银行上海市分行设立的账户内。至 2005 年 7 月三被告人共计非法获利人民币 202 万余元，其中王一辉非法获利 122 万余元，金珂获利 42 万余元，汤明获利 38 万余元。金珂得款后挥霍 20 余万元，汤明以非法获利 32 万余元购买了房屋一套。案发后公安机关冻结了金珂在工商银行浙师大支行中的银行存款 208,454.25 元，查封了汤明用赃款购买的上述房屋。

2006 年 3 月 9 日上海市公安局浦东分局委托上海公信扬知识产权司法鉴定所对被告人发送的软件数据包进行鉴定，司法鉴定所于 2006 年 3 月 13 日委托上海市软件评测中心进行测试，测试结论表明：通过手动修改数据库文件和软件修改数据库文件这两种方式都可导致玩家在游戏中的级别、“武器”、“装备”等属性值完全发生变化。2006 年 7 月 21 日，该司法鉴定所又根据上海市公安局浦东分局的委托，出具了补充说明，内容为：网络游戏软件分为客户端和服务器端两部分，在服务器端软件中包含有游戏数据库文件和玩家数据库文件，前者包括物品“武器”及“装备”、魔法技能、动物怪物三个数据库，后者用于存储与玩家有关的武器装备、级别的信息，这两个数据库都是由游戏作者设计的。本案中的软件修改者修改了某一玩家数据库中的数据，并没有修改游戏软件作者设计并编写的软件，也不会引起该游戏软件中的其他部分的改变，但是可以对玩家运行该游戏软件的结果产生重大变化，改变或增加玩家的“武器装备”级别。

另查明，2001 年 6 月 29 日盛大公司与韩国 Actoz 软件有限责任公司签订软件许可协议，协议约定 Actoz 公司授予盛大公司独家且排他许可使用、促销、分发、市场营销、改编或修改“热血传奇”软件，并将该软件转换为中文版本的权利。2003 年 8 月 18 日，韩国 Actoz 软件有限责任公司和 WeMade 娱乐有限公司取得我国国家版权局就“热血传奇”游戏软件颁发的计算机软件著作权登记证书。2003 年 8 月 19 日双方又签订修正协议，约定软件许可的条款可以延长到 2005 年 9 月 28 日，当且仅当协议双方对于“热血传奇”不存在争议时，上述特许期限期满日应延长到 2006 年 9 月 28 日。

本案审理中，被告人王一辉的家属帮助王一辉退赃 120 万元。被告人金珂表示愿意将被公安机关冻结的银行存款 208，454.25 元作为退赃，其余赃款也愿意以工作收入退出。被告人汤明的家属帮助汤明退赃 5 万元，汤明以赃款购买的房屋愿意作为退赃处理，不足部分也愿意以工作收入退出。

上海市浦东新区人民法院针对三被告人及其辩护人对公诉机关指控的事实及定性提出的意见，综合查明的事实及认定的证据作如下评判：

1.关于公诉机关指控三被告人犯侵犯著作权罪罪名是否成立。

公诉机关认为被告人修改数据生成、销售游戏“武器”及“装备”的行为属于复制、发行计算机软件的行为，因此三被告人构成侵犯著作权罪。法院认为，三被告人的行为不符合侵犯计算机软件著作权罪的构成要件，我国刑法第二百一十七条第一款第（一）项规定的侵犯著作权的情形指：“未经著作权人许可，复制、发行其文字作品、音乐、电影、电视、录像作品，计算机软件及其他作品的。”复制、发行是构成侵犯著作权罪的两个行为要件。本案中三被告人实施的行为是修改游戏软件数据库中的数据的行为，而修改数据后产生的“武器”及“装备”是软件运行后产生的结果，并不是软件本身。根据《计算机软件保护条例》第六条的规定，对软件著作权的保护不延及开发软件所用的处理过程、操作方法等，故本案涉及的游戏中的“武器”及“装备”不属于计算机软件著作权的保护范围。三被告人通过修改数据而复制武器及装备不构成复制计算机软件，因此对三被告人的行为不应以侵犯计算机软件著作权罪论处。公诉机关指控三被告人犯侵犯著作权罪的罪名不成立。

2.关于三被告人的行为定性。

法院认为，三被告人的行为构成职务侵占罪。被告人王一辉在盛大公司任游戏项目运维部副经理，其有条件对游戏软件中的数据进行修改，其拥有的数据修改权是因其职责而直接赋予的，因此王一辉的行为符合职务侵占罪中“利用职务上的便利”这一构成要件。网络游戏中的“武器”及“装备”是计算机软件运行后生成的结果，是一种虚拟财产，其在虚拟环境中的作用决定了其可以被人占有、使用等，但游戏玩家要取得虚拟财产除了花费时间外，还必须付出一定的费用，如购买游戏点卡的费用、上网费等，同时该虚拟财产通过现实中的交易能转化为货币，因此虚拟财产既有价值，又有使用价值，具有现实财产的属性。盛大公司通过许可取得了“热血传奇”游戏在一定时间内的独家运营权，在此期间，盛大公司对游戏“武器”及“装备”享有所有权和处分权，因此被告人非法侵占的游戏“武器”及“装备”属于盛大公司所有。关于金珂、汤明是否构成职务侵占罪共同犯罪的问题，《最高人民法院关于审理贪污、职务侵占案件如何认定共同犯罪的问题的解释》第二条规定行为人与公司、企业或者其他单位的人员勾结，利用公司、企业或者其他单位人员的职务便利，共同将单位财物非法占为己有，数额较大的，以职务侵占罪共犯论处。”被告人金珂、汤明虽然不是盛大公司的工作人员，但其与被告人王一辉共同勾结，侵占公司财产，根据上述规定，三被告人属共同犯罪。综上所述，三被告人的行为符合职务侵占罪的构成要件，应以职务侵占罪论处。

3.关于三被告人获取违法所得的金额。

公信中南会计师事务所调取了三被告人在银行开设的 6 个账户（其中王一辉在中国工商银行上海市分行有 2 个账户，金珂在工行金华市分行有 1 个账户，汤明在工行金华市分行有 3 个账户），会计师事务所根据银行对账单资金收付日期、金额、交易注释等内容，按照以下原则判断三被告人间因出售游戏“武器”、“装备”后分成而发生的交易金额：（1）资金收付日期均为同一天；

（2）资金收付金额相同；（3）资金收付可能由于手续费等因素造成收付金额稍有差异，但差异不大。即如被告人王一辉收进的款项与被告人金珂、汤明在同一天支出的款项相同，或差异极小，且交易注释也一致的，作为三被告人销售“武器”及“装备”获利的金额。会计师事务所的这一审计方法应是合理的，除非三被告人提供证据证明这笔资金往来与其销售

“武器”及“装备”的获利无关。庭审中被告人金珂、汤明均称与王一辉有借款关系存在，但三被告人均未提供相应的证据，而从三被告人较为一致的部分陈述判断，借款额也只有3万余元，扣除之后，并不影响公诉机关对被告人获利金额的认定，因此会计师事务所的审计报告可予采纳。而从被告人王一辉的获利金额按照四六分成的比例可以推算汤明和金珂的获利金额。

综上所述，法院认为，被告人王一辉利用其在盛大公司担任游戏项目运维部副经理的便利，与被告人金珂、汤明共同合谋通过非法手段获取游戏“武器装备”并销售，数额巨大，其行为已触犯刑法第二百七十一条之规定，构成职务侵占罪。三被告人系共同犯罪，被告人王一辉在共同犯罪中起主要作用，是主犯。鉴于被告人王一辉认罪态度较好，且其家属能积极帮助退赃，故对被告人王一辉从轻处罚。被告人金珂、汤明在共同犯罪中起次要作用，系从犯，认罪态度较好，并作了退赃的努力，故根据刑法第二十七条的规定，对被告人金珂、汤明减轻处罚。鉴于公安机关在接到盛大公司报案后即展开了侦查，在将被告人抓获前已基本掌握了被告人的犯罪事实，其中金珂是经公安机关布控后抓获，被告人到案后能如实交代犯罪行为只能以坦白论处，故被告人王一辉、金珂的辩护人提出王一辉、金珂有自首情节的辩护意见本院不予支持。据此，依照《中华人民共和国刑法》第二百七十一条，第二十五条，第二十六条，第二十七条，第六十四条，第七十二条，第七十三条第二、三款之规定，判决如下：

1.被告人王一辉犯职务侵占罪，判处有期徒刑五年。

2.被告人金珂犯职务侵占罪，判处有期徒刑三年，缓刑四年。

3.被告人汤明犯职务侵占罪，判处有期徒刑二年六个月，缓刑三年。

4.被告人王一辉退赃款人民币120万元，包括现金420，198元和银行存款779，802元，被告人汤明退赃款人民币5万元，发还被害单位上海盛大网络发展有限公司；被告人汤明用赃款购买的坐落于浙江省金华市柳湖小区27幢4号401室的房屋变价发还被害单位上海盛大网络发展有限公司。尚未退缴的赃款，待追缴后发还被害单位上海盛大网络发展有限公司。

一审宣判后，被告人王一辉、金珂、汤明不服，提出上诉。上海市第一中级人民法院经二审审理后认为，原审判决认定事实清楚，证据确实、充分，定性正确，量刑适当，审判程序合法，依法裁定：驳回上诉，维持原判。

（八）制作、复制、出版、贩卖、传播淫秽物品牟利罪

1.典型案例：深圳市快播科技有限公司传播淫秽物品牟利案

案例要旨

网络平台服务者以牟利为目的，设置缓存服务器抓取、存储淫秽视频，变更为碎片化存储视频，供不特定用户下载观看的行为，属于在技术应用阶段的传播淫秽物品，不具有技术中立性，并且在此过程中，网络平台服务者并未丧失对缓存服务器的实际控制和监管的，其行为构成传播淫秽物品牟利罪。

案例正文

深圳市快播科技有限公司传播淫秽物品牟利案

［基本案情］

被告单位深圳市快播科技有限公司（以下简称“快播公司”）成立于2007年12月26日，通过免费提供QSI软件（QVOD资源服务器程序）和QVODPlayer软件（快播播放器程序）的方式，为网络用户提供网络视频服务。任何人（被快播公司称为“站长”）均可通过QSI发布自己所拥有的视频资源。为提高热点视频下载速度，快播公司搭建了以缓存调度服务器为核心的平台，通过自有或与运营商合作的方式，在全国各地不同运营商处设置缓存服务器1000余台。在视频文件点播次数达到一定标准后，缓存调度服务器即指令处于适当位置的缓存服务器抓取、存储该视频文件。当用户再次点播该视频时，若下载速度慢，缓存调度服务器就会提供最佳路径，供用户建立链接，向缓存服务器调取该视频，提高用户下载速度。部分淫秽视频因用户的点播、下载次数较高而被缓存服务器自动存储。缓存服务器方便、加速了淫秽视频的下载、传播。

2012年8月，深圳市公安局公安信息网络安全监察分局对快播给予行政警告处罚，并责令整改。随后，快播公司成立了网络安全监控小组开展了不到一周的突击工作，于8月8日投入使用“110”不良信息管理平台，截至9月26日共报送“色情过滤”类别的不良信息15836个。但在深圳网监验收合格后，网络安全监控小组原有4名成员或离职或调到其他部门，“110”平台工作基本搁置，检查屏蔽工作未再有效进行。2013年8月5日，深圳市南山区广播电视局执法人员对快播公司开展调查，执法人员登录快播网站很快便找到了可播放的淫秽视频。但快播公司随后仅提交了一份整改报告，其“110”平台工作依然搁置，检查屏蔽工作依然没有有效落实。

2013年上半年，北京网联光通技术有限公司与快播公司开展合作。光通公司提供四台服务器，快播公司提供内容数据源以及降低光通公司网络出口带宽，同时提升用户体验的数据传输技术解决方案，负责远程对软件系统及系统内容的维护。2013年8月，光通公司提供四台服务器开始上线测试，快播公司为四台服务器安装了快播公司的缓存服务器系统软件，并通过账号密码远程登录进行维护。2013年11月18日，北京市海淀区文化委员会在行政执法检查时，从光通公司查获此四台服务器。2014年4月11日，北京市公安局海淀分局决定对王欣等人涉嫌传播淫秽物品牟利罪立案。公安机关从服务器里提取了29841个视频文件进行鉴定，认定其中属于淫秽视频的文件为21251个。

2013年底，为了规避版权和淫秽视频等法律风险，在王欣的授意下，张克东领导的技术部门将原有的完整视频文件存储变为多台服务器的碎片化存储，将一部视频改由多台服务器共同下载，用户点播时需通过多台服务器调取链接，集合为可完整播放的视频节目。

另查，快播公司盈利主要依靠广告费、游戏分成、会员费和电子硬件等来源，快播事业部是快播公司盈利的主要部门。根据账目显示，快播事业部的主要收入来源于网络营销服务，其中资讯快播和第三方软件捆绑是最为主要的盈利方式。

被告人吴铭、张克东、牛文举于2014年4月23日在深圳被抓获，被告人王欣于2014年8月8日从韩国济州岛被押解回京。

［疑难问题］

1.快播公司是否构成传播淫秽物品牟利罪？如果构成，是以作为还是不作为方式？

2.辩护人主张的“技术中立”原则能否为快播公司免责？

［法理分析］

一、快播公司是否构成传播淫秽物品牟利罪

本案定性的首要问题是快播公司的行为是否构成传播淫秽物品牟利罪。对此问题，学界主要有以下几种观点：

观点一：快播公司及其主管人员的行为构成不作为形式的传播淫秽物品牟利罪。一审判决认定：“快播公司及王欣等被告人明知快播的网络服务系统被用于传播淫秽视频，但出于扩大经营、非法牟利目的，拒不履行监管和阻止义务，放任快播公司构建的网络服务系统被

用于传播大量淫秽视频，具有明显的社会危害性和刑事违法性，对被告单位快播公司及各被告人应当依法追究刑事责任。”如有论者认为，在刑法教义学上，行为人拒不履行安全管理义务罪而又同时构成其他犯罪的情形属于不作为犯的想象竞合，并且其中一个是纯正的不作为，而另一个是不纯正的不作为。

观点二：快播公司及其主管人员的行为构成作为与不作为形式相结合的传播淫秽物品牟利罪。如有论者认为：“一审判决还从快播公司负有网络视频信息服务提供者应当承担的网络安全管理义务，并且具备管理的可能性但没有履行网络安全管理义务的角度，论证了快播公司构成传播淫秽物品牟利罪。据此，快播公司同时存在作为与不作为。”

观点三：快播公司及其主管人员拒不履行网络监管义务的不作为行为并不构成传播淫秽物品牟利罪，而是构成拒不履行信息安全管理义务罪，但又因为快播案发生在《刑法修正案（九）》颁布之前，所以快播无罪。如有论者认为：“理论上，传播淫秽物品牟利罪，既可以由作为构成，也可以由不作为构成。但是，网站不履行管理义务，不属于本罪的不作为表现方式。法官充分论证了王欣没有履行管理义务，如果据此认定构成不作为犯罪——拒不履行信息网络安全管理义务罪（最高 3 年），没有问题。但把拒不履行管理义务等于作为犯罪——传播淫秽物品牟利罪（最高无期），是可怕的逻辑。需要说明，拒不履行信息网络安全管理义务罪是 2015 年才确立的罪名，法不溯及既往，不构成此罪。”

观点四：快播公司及其主管人员的行为构成作为形式的传播淫秽物品牟利罪。如有论者认为：“定罪的合理论证思路似乎应当主要针对被告人的缓存这一陈列淫秽物品行为，从作为犯的角度切入，分析行为的支配性和正犯性，将缓存行为评价为以存放、陈列方式实施的传播行为，从而将定罪的关键事实定位于存在论上难以否认的作为，使得定罪的正当性得以充分展示。”

依据我国当前的刑法立法和相关理论来分析，笔者更倾向于采纳第四种观点。本案没有任何争议的是快播公司的行为构成拒不履行信息网络安全管理义务罪，其在接到深圳网监局的行政警告处罚之后，投入使用“110”不良信息管理平台，但在深圳网监验收合格后，检查屏蔽工作未再有效进行。2013 年 8 月 5 日，深圳市南山区广播电视局执法人员对快播公司开展调查，执法人员登录快播网站很快便找到了可播放的淫秽视频。但快播公司随后仅提交了一份整改报告，其“110”平台工作依然搁置，检查屏蔽工作依然没有有效落实，从而导致大量淫秽物品在网络上传播。快播公司通过“110”不良信息管理平台确实有效过滤掉了不良信息，但通过了检验之后又搁置该平台，这确实证明了快播公司能够以较低的成本实现对自身平台的监管，在有能力履行网络安全管理义务情况下拒不履行，构成拒不履行信息网络安全管理义务罪。但是，由于此罪由《刑法修正案（九）》规定，而本案发生于《刑法修正案（九）》颁布之前，依据法不溯及既往的原理，对快播公司拒不履行信息网络安全管理义务的行为不可罚。

那么，快播公司的行为究竟有没有触犯传播淫秽物品牟利罪？如果答案是肯定的，又如何按照观点四的逻辑对快播公司的行为作出合理的解释？笔者认为，观点一、二都认为在具有牟利目的的情况下，快播公司不履行安全管理义务就可以转化为不作为的传播淫秽物品牟利罪行为。这样的解释确有移花接木和偷换概念的嫌疑，难以使公众信服。同时，将监管义务上升到刑法义务无疑是扩大了打击范围，不可避免地产生法律阻碍技术进步的不良影响。所谓传播淫秽物品牟利罪，是指以牟利为目的，传播淫秽物品的行为。传播即广泛散布。快播公司的行为主要包含两个层面，第一个层面是为用户提供 QVODPlayer 播放器，第二个层面是其缓存服务器抓取、存储达到点击率要求的视频。为用户提供播放器的行为是快播公司和站长之间的双向行为，不构成传播行为，而缓存视频的行为实则是展览、陈列行为，符合传播行为的实质要求。最后，辩护人拿来做“免罪金牌”的技术中立原则是否能够成立呢？

二、辩护人主张的“技术中立”原则能否为快播公司免罪

技术中立与否实际上是当代技术哲学范畴的一大核心议题。技术是否是中性的？技术发展是否有自主性？在技术哲学领域，这些问题有着不同的答案。如挪威卑尔根大学科学与人文研究中心拉格纳·费尔兰德（Ragnar Fjelland）认为，技术是非中性的，具有自主性，“隧道目光”可能是在“技术命令”后面的一种主要驱动力：凡是技术上可行的，就应该去实现。主流观点则认为技术仅仅是工具，而工具通常被看作是能够产生不同结果的手段，因此技术对于各种结果而言是中性的。

关于技术中立原则，又称技术无罪原则，由美国联邦最高法院首次在知识产权领域提出，又在之后不断对其作出细化和调整。20 世纪 70 年代，日本索尼公司开始在美国销售 Betamax 录像机，该录像机可以通过电视机录制正在播放的节目，也可以录制其他频道的节目。不仅如此，它还可以定时录制节目，甚至可以跳过广告。美国环球电影制片公司和迪士尼制片公司于 1976 年向加利福尼亚州中区地区法院起诉索尼公司协同侵权。最终，美国最高法院采纳实质性非侵权用途规则（即使制造商和销售商知道其设备可能被用于侵权，也不能推定其故意帮助他人侵权并构成“帮助侵权”）驳回了原告的诉讼请求。

在 2001 年阿莫唱片公司诉纳普斯特（Napster）案件中，纳普斯特公司向用户提供其开发的 P2P（Peer to Peer）点对点音乐共享软件（Music-Share），用户可以直接通过其他用户的电脑下载盗版音乐软件。法院却作出了不同于索尼案的判决，认定此案不再适用技术中立原则。这是因为纳普斯特公司在提供了共享软件之后仍然对用户存在管理的能力，一旦公司关闭信息检索服务器，用户便不能使用音乐共享软件，而索尼公司在出售了录像机后丧失了对用户的管理能力。2005 年，格罗斯科特公司（Grokster）开发了一种与 MusicShare 类似但更为先进的 P2P 技术，并且新一代的 P2P 的音乐共享软件开始脱离网络服务提供者的控制。最高法院因此提出“引诱规则”，也即公司在推广设备时具有侵犯版权的目的，比如用明确表示或者暗示等其他方式帮助侵权，那么公司就应当承担责任。

号称我国第一起 P2P 案件的是酷乐案（Kuro）。2006 年 12 月 19 日，上海步升音乐文化传播有限公司诉北京飞行网音乐软件开发有限公司、北京舶盛舫安信息技术有限公司利用酷乐软件侵犯录音制作者权。酷乐软件同样是一种利用 P2P 技术的软件。在该案中，法院使用“非中立性技术应用”对两被告行为作出了分析，认定两被告共同承担侵权责任。“非中立性技术应用”是指中立的技术一旦用于“非中立性技术应用”，技术就不再中立。

有学者指出，目前整个世界都处于 P2P 的结构下，每个人都难逃网络用户或网络服务提供者的角色，如何在避免网络平台借“技术中立”当“免罪金牌”的同时又做到避免法律过多地限制技术的发展与进步呢？快播案中王欣及其辩护人一直拿来抗辩的“菜刀理论”，也即“技术中立原则” 真的可以成为快播的出罪理由吗？笔者认为，对“技术中立”的细化研究是解决上述问题的一个绝佳突破口。所谓“技术中立原则”，其实是在狭义空间内对技术的讨论。技术是由人创造的，因此我们所称的“技术中立” 仅仅局限于完完全全的技术工具本身。但不可忽视的是，在上述讨论的案件中，我们却在潜意识里扩大了“技术中立原则”的适用空间。任何一项以使用为目的的技术从无到有都不得不经过两个阶段——技术开发和技术应用。最后得到的技术产品是中立的，但是在技术开发和技术应用这两大阶段因为人的参与从而不可避免产生非中立性。正如有论者言，所有的技术非中性论思想家都将思考的目光放在了技术的社会使用和现实影响方面。首先，在技术开发阶段，往往是基于某种需求或者创新使得技术开发者开发某种技术。甚至在技术还没出现之时，已经存在非中立性的类型了，比如说“洗脑术”。其次，在技术生产出来以后，进入投入使用阶段，除了技术开发者明示或者暗示技术在某一方面的便捷和高效从而指导技术使用者去使用以外，技术本身也是有自己的意向结构的。也就是说，在技术使用者使用该技术产品的过程中自主发现该技术在某一方面的进步与优势以后，技术使用者也会继续该种使用。尤其是在互联网领域，这种使用方式更有可能呈现出爆炸式的增长规模。“如果一个人看不到我们的行为，比他能够

看到我们的行为，我们更容易对他加以伤害；他能看到我们对他施加伤害的行为可能会让我们产生羞愧或罪恶感，从而停止正在做出的伤害行为。”就快播案来说，如果快播可以方便地传播淫秽物品，那么在当前的社会，就必然会被用来传播淫秽物品。从这个角度我们也就该明白，我们所能做的就是加强对网络平台的控制和监管。

［结论归纳］

基于本文论述以及刑法学的相关理论，快播公司以作为方式构成传播淫秽物品牟利罪，“技术中立原则”无法成为快播公司的“免罪金牌”。快播公司客观上为用户提供上传和下载视频的服务，适用狭义的“技术中立原则”，不构成犯罪。但是，其设置缓存服务器抓取、存储淫秽视频，变更为碎片化存储视频的行为，属于在技术应用阶段的传播淫秽物品，不具有技术中立性，并且在此过程中，快播公司并未丧失对缓存服务器的实际控制和监管。就主观方面来说，快播公司具有传播淫秽物品的间接故意。在快播平台运营过程中，快播公司对外以“宅男神器”做推广宣传，并且在快播平台的播放页面不乏淫秽色情广告。即便被告辩称自己不知道快播有缓存和播放大量淫秽物品的行为，但是在屡次因此受到行政处罚之后，其辩解显然难以令人信服。另外，传播淫秽物品牟利罪还要求行为人具有牟利的目的。在快播案中，其盈利主要依靠广告费、游戏分成、会员费和电子硬件等来源，事业部是快播公司盈利的主要部门。根据账目显示，快播事业部的主要收入来源于网络营销服务，其中资讯快播和第三方软件捆绑是最为主要的盈利方式。而其网络营销服务中常常伴有“宅男福利”等类似宣传广告，甚至绑定淫秽视频，快播公司主观上显然具有牟利的目的。

在当今 P2P 技术发展越来越迅速的社会，新兴网络平台层出不穷，与之相伴的问题也越来越多地困扰着我们。前不久，国家网信办依法约谈“快手”和“火山小视频”相关负责人，提出严肃批评，并责令全面整改。在法律滞后性的制约下，积极构建前置约谈机制，明确划分网络服务提供者类型并依据广义“技术中立原则”对不同类型的网络服务提供者设置有区分度的注意义务，认识到人与技术的互相建构作用，谨慎把握“技术中立原则”，才能为法律规制和科技发展构建出一片合理的缓冲区间。

2. 最高人民检察院第三十四批指导性案例之四：

钱某制作、贩卖、传播淫秽物品牟利案（检例第 139 号）

【关键词】

制作、贩卖、传播淫秽物品牟利　私密空间行为　偷拍　淫秽物品

【要旨】

自然人在私密空间的日常生活属于民法典保护的隐私。行为人以牟利为目的，偷拍他人性行为并制作成视频文件，以贩卖、传播方式予以公开，不仅侵犯他人隐私，而且该偷拍视频公开后具有描绘性行为、宣扬色情的客观属性，符合刑法关于“淫秽物品”的规定，构成犯罪的，应当以制作、贩卖、传播淫秽物品牟利罪追究刑事责任。以牟利为目的提供互联网链接，使他人可以通过偷拍设备实时观看或者下载视频文件的，属于该罪的“贩卖、传播”行为。检察机关办理涉及偷拍他人隐私的刑事案件时，应当根据犯罪的主客观方面依法适用不同罪名追究刑事责任。

【基本案情】

被告人钱某，男，1990 年出生，无固定职业。

钱某曾因偷拍他人性行为被行政拘留，仍不思悔改，产生通过互联网贩卖偷拍视频文件从中牟利的想法。2017 年 11 月，钱某从网络上购买了多个偷拍设备，分别安装在多家酒店客房内，先后偷拍 51 对入住旅客的性行为，并将编辑、加工的偷拍视频文件保存至互联网云盘，通过非法网站、即时通讯软件发布贩卖信息。2018 年 5 月 9 日，公安机关将钱某抓获，并在上述互联网云盘中检出偷拍视频 114 个。

此外，钱某还以“付费包月观看”的方式，先后182次为他人通过偷拍设备实时观看入住旅客性行为或者下载偷拍视频提供互联网链接。

【检察履职情况】

（一）引导侦查取证

2018年6月8日，四川省成都市公安局锦江分局以钱某涉嫌传播淫秽物品罪向检察机关提请批准逮捕。

四川省成都市锦江区人民检察院审查认为，钱某偷拍他人性行为后既有传播扩散行为，也有编辑加工、贩卖牟利行为，故以制作淫秽物品牟利罪对钱某批准逮捕，并向公安机关提出对扣押在案的手机进行电子数据检查和恢复，对其注册使用的互联网云盘信息进行提取和固定的取证意见。此后，公安机关进一步查明了钱某的作案方式、获利情况和危害后果。

（二）审查起诉

2018年8月15日，锦江分局以钱某涉嫌制作、贩卖、传播淫秽物品牟利罪移送锦江区人民检察院审查起诉。审查起诉期间，钱某辩解其上传到互联网云盘的淫秽视频文件并非偷拍所得，而是从他人处获取后上传互联网用于个人观看。对此，检察机关自行补充侦查，对涉案多家酒店实地察看，详细了解装有偷拍设备的酒店客房布局、特征和偷拍设备安装位置、取景场域，通过与起获的视频文件中拍摄的客房画面逐一比对，结合其有罪供述，发现有114个视频文件中的场景与偷拍现场具有同一性，结合其他证据认定相关视频确系钱某偷拍。

2019年1月29日，锦江区人民检察院以钱某涉嫌制作、贩卖、传播淫秽物品牟利罪提起公诉。

（三）指控与证明犯罪

2019年7月17日、7月24日，四川省成都市锦江区人民法院不公开开庭审理本案。

庭审中，辩护人对视频文件的性质和数量认定等提出了辩护意见。一是涉案的视频文件形式上不具有实物特征，内容上不具有淫秽特征，不属于淫秽物品；二是多个视频文件描绘的是同一对旅客的性行为，即便属于淫秽物品，也应当以被偷拍的旅客的对数认定数量，不能以设备自动分段或人为编辑制作的数量认定。

公诉人答辩指出，偷拍的视频文件属于淫秽物品，数量应当以钱某编辑、制作的数量为标准。一是涉案的视频文件属于淫秽物品。形式上，淫秽物品的视频文件形式与刊物、光盘等有形物具有同质性。对此，《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》明确规定，在互联网上建立淫秽网站、网页，提供淫秽站点链接服务，或者传播淫秽书刊、影片、音像、图片的，依照刑法有关规定追究刑事责任。最高人民法院、最高人民检察院的司法解释对制作、贩卖、传播视频文件、音频文件等淫秽电子信息也有明确规定。内容上，自然人在私密空间的性行为本身不具有淫秽性，但被告人将其编辑、贩卖、对外传播，则具有描绘性行为或者露骨宣扬色情的客观属性，符合刑法对“淫秽物品”的界定；二是视频文件的数量应当以钱某编辑、制作数量为标准，而非依据旅客区分。本案中每个视频文件都是钱某偷拍后通过筛选、剪辑而成；每个视频文件都能够独立播放，内容涉及不同性行为；每个视频文件都是露骨宣扬色情，被非法传播后都能给观看者带来淫秽性刺激，社会危害性不会因为数个片段均反映同一对旅客的性行为而降低。

（四）处理结果

2019年7月26日，锦江区人民法院作出判决，采纳检察机关指控的犯罪事实和意见，以制作、贩卖、传播淫秽物品牟利罪判处钱某有期徒刑三年六个月，并处罚金人民币五千元。宣判后，钱某未提出上诉，判决已生效。

（五）制发检察建议

旅客入住酒店偷拍事件频发，导致隐私安全无法得到保障，严重侵犯消费者的个人隐

私，暴露出相关行业主管部门监管不力、经营者管理不善问题，检察机关从建立健全旅客隐私保护、落实实名登记入住制度、增加安防设施投入、加强日常检查巡查等方面，向治安主管部门和行业组织发出检察建议。治安主管部门落实整改，对辖区旅馆业进行滚动摸排、对场所软硬件开展检查，强化旅客入住“人证合一”，开展公民隐私权法制宣传，会同市场监管部门联合核查网络摄像头生产、销售商家，督促落实市场主体责任。行业组织开展了旅馆、酒店会员单位法制宣传、隐私安全保护培训，增加安防设备，会同治安主管部门制定治安安全防范规范，加强旅馆业安全管理水平，加大保护公民隐私安全力度。

【指导意义】

（一）准确界定“淫秽物品”“贩卖、传播行为”，依法严惩网络背景下传播淫秽物品犯罪。自然人的私人生活安宁和不愿受他人干扰的私密空间、私密活动、私密信息，依法不受侵犯。发生在酒店、旅馆、民宿等非公开空间内的性行为，属于隐私保护的范围。行为人偷拍他人性行为并经互联网传播扩散的视频，不仅侵害个人隐私，而且客观上具有描绘性行为的诲淫性，具有宣扬色情的危害性，符合刑法对“淫秽物品”的界定。行为人有偿提供互联网链接，他人付费后可以实时在线观看，与建立并运营“点对面”式互联网直播平台的传播行为性质相同，应当认定为贩卖、传播行为。

（二）行为人偷拍他人隐私，行为方式、目的多样，应当区分不同情形依法惩处。行为人非法使用偷拍设备窥探他人隐私，未贩卖、传播的，如果相关设备经鉴定属于窃听、窃照专用器材，造成严重后果的，应当以非法使用窃听、窃照专用器材罪追究刑事责任；如果行为人又将偷拍的内容贩卖、传播的，应当按照处罚较重的罪名追究刑事责任。行为人通过远程操控侵入他人自行安装的摄像头后台信息系统，对他人私密空间、行为进行窥探，进行遥控并自行观看，情节严重的，应当以非法控制计算机信息系统罪追究刑事责任；如果行为人在侵入上述计算机信息系统以后，又将偷拍的视频贩卖、传播的，应当按照处罚较重的罪名追究刑事责任。行为人以非法占有他人财物为目的，通过偷拍获取他人隐私，进而要挟他人、获取财物，构成犯罪的，应当以敲诈勒索罪追究刑事责任。上述行为尚未构成犯罪的，应当依法从严追究其行政违法责任。

（三）通过制发检察建议促进社会治理。个人隐私被非法收集、买卖，成为电信网络诈骗、网络传播淫秽物品等犯罪的源头，并催生出一条黑灰产业链，严重侵扰公民生活安宁、财产安全，破坏社会秩序。检察机关办案中要注意剖析案发地区、案发领域管理、制度上的漏洞，研究提出有针对性、可操作性的检察建议，推动有关部门建章立制、堵塞漏洞、消除隐患，促进完善社会治理。

【相关规定】

《中华人民共和国刑法》第三百六十三条、第三百六十七条

《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释》第一条

《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）》第一条

四、普通案例

（一）非法吸收公众存款罪

案例一、陈维熙、陈尧集资诈骗、非法吸收公众存款案

广东省高级人民法院

刑 事 裁 定 书

（2019）粤刑终824、825、826号

原公诉机关广东省深圳市人民检察院。

上诉人（原审被告人）陈维熙，男，1971 年 11 月 27 日出生，汉族，中专文化，户籍所在地湖南省沅江市，经常居住地广东省深圳市龙华新区。因本案于 2016 年 8 月 21 日被羁押，次日被刑事拘留，同年 9 月 27 日被逮捕。现押于深圳市第二看守所。

辩护人郑懿，广东正大方略律师事务所律师。

上诉人（原审被告人）陈尧，男，l984 年 12 月 7 日出生，汉族，中专文化，户籍所在地浙江省温州市平阳县。因本案于 2017 年 2 月 18 日被羁押，当日被刑事拘留，同年 3 月 24 日被逮捕。现押于深圳市第二看守所。

辩护人周连斌，广东泰旭律师事务所律师。

上诉人（原审被告人）吴迪，男，l985 年 9 月 20 日出生，汉族，大专文化，户籍所在地天津市河北区。因本案于 2017 年 3 月 29 日被羁押，当日被刑事拘留，同年 5 月 5 日被逮捕。现押于深圳市第二看守所。

辩护人杜占森，广东天津天关律师事务所律师。

广东省深圳市中级人民法院审理广东省深圳市人民检察院指控原审被告人陈维熙、陈尧犯集资诈骗罪、被告人吴迪犯非法吸收公众存款罪一案，于 2019 年 3 月 15 日作出（2017）粤 03 刑初 497 号、（2018）粤 03 刑初 15 号、65 号刑事判决。宣判后，原审被告人陈维熙、陈尧、吴迪均不服，提出上诉。本院依法组成合议庭，决定以不开庭方式进行审理。通过阅卷、讯问上诉人、听取辩护人的意见，本案现已审理终结。

原判认定，被告人陈维熙于 2014 年 12 月成立深圳市保奇通股权投资基金管理有限公司（以下简称“保奇通公司”），通过虚假宣传“湖南保奇通砂石产业”投资项目，吸引被害人韩某东、王某伟、孔某悦等人投资。陈维熙在取得上述被害人资金后不用于生产经营活动，致使投资款不能返还，被害人损失数额计人民币（以下未注明币种均为人民币）1809567.72 元。

陈维熙于 2015 年 8 月 18 日以股权转让形式取得深圳前海众投互联网金融服务有限公司（以下简称“前海众投公司”），被告人陈尧任该公司总裁、被告人吴迪任该公司高级投资顾问。陈维熙、陈尧作为该公司运营负责人，依托该公司及该公司的“融促汇”P2P 网络借贷平台，虚构投资项目进行非法集资，在取得资金后不用于生产经营活动，大部分款项被转入陈尧的个人账户，致使被害人损失数额高达 6178286.42 元。

吴迪作为前海众投公司高级投资顾问，明知该公司无金融许可，仍依托该公司的“融促汇”P2P 网络借贷平台，以高息保本为诱饵，变相向社会公众吸收资金。经查，2015 年 8 月 18 日至 2016 年 6 月 27 日，前海众投公司吸收公众投资款 l5181436.92 元，吴迪个人非法吸收资金计 260 万元。

原判认定上述事实，有书证、证人证言、被害人陈述、被告人供述、鉴定意见等证据证实。

原判认为，被告人陈维熙、陈尧以非法占有为目的，使用诈骗方法非法集资，数额特别巨大，其行为已构成集资诈骗罪。被告人吴迪在未取得金融许可资格的情况下，向社会不特定对象吸收存款，扰乱金融秩序，数额巨大，其行为已构成非法吸收公众存款罪。陈尧是主犯。吴迪是非法吸收公众存款的直接实施者，不应认定为从犯。依照《中华人民共和国刑法》第一百九十二条、第一百七十六条、第二十五条第一款、第二十六条第一款、第四款、第六十四条、第六十七条第三款之规定，作出判决：（一）被告人陈维熙犯集资诈骗罪，判处有期徒刑十一年，并处罚金人民币五十万元。（二）被告人陈尧犯集资诈骗罪，判处有期徒刑十年，并处罚金人民币五十万元。（三）被告人吴迪犯非法吸收公众存款罪，判处有期徒刑五年，并处罚金人民币十万元。（四）扣押在案的物品依法没收，上缴国库。（五）责令被告人将尚未退还的涉案款项退赔给被害人。

上诉人陈维熙上诉及其辩护人辩护提出：第一，《审计报告》的鉴定结论未能反映真实客观情况，认定投资人的实际投资额及损失额，缺乏客观证据佐证，不应作为定案证据使用。第二，前海众投公司及“融促汇”平台不是为了非法集资而成立，陈维熙仅为投资人，未参与该公司的经营管理，未在该平台获取收益，反而投入大量资金，不具有非法占有目的；陈维熙在湖南长沙有茶油林及砂石厂的实体产业，未虚构事实；陈维熙积极赔偿被害人款项，并取得部分被害人的谅解；综上，陈维熙的行为不构成集资诈骗罪，应构成非法吸收公众存款罪。第三，本案进行活动的主体是公司，投资者的资金都进入公司账户，且大部分投资款用于支付投资人的本息及公司生产运营，应为单位犯罪。第四，陈维熙系初犯，如实供述，主观恶性小。请求依法改变陈维熙的罪名并减轻处罚。

上诉人陈尧上诉及其辩护人辩护提出：第一，投资人的资金均进入前海众投公司账户，投资款均用于公司开支，陈尧没有占有投资款，没有非法占有的目的；现无证据证实前海众投公司发布的标的是虚假的，不能证明陈尧使用诈骗方法进行非法集资。因此，陈尧的行为不构成集资诈骗罪，应构成非法吸收公众存款罪。第二，陈尧不是前海众投公司的法定代表人或股东，仅受陈维熙雇佣参与该公司的管理，仅领取固定的工资，在本案中是起次要作用的从犯。第三，投资人的资金均进入公司账户，且大部分用于公司经营，违法所得也归公司所有，应认定为单位犯罪。请求依法改判。

上诉人吴迪上诉及其辩护人辩护提出：吴迪不是前海众投公司的股东或高管，不参与决策，仅领取固定工资，在共同犯中是起次要作用的从犯；涉案资金的吸收或出借均以前海众投公司的名义进行，且大部分资金用于公司的运营，应当认定为单位犯罪；吴迪归案后认罪态度好，具有坦白情节。请求对吴迪从轻处罚。

经审理查明，一、上诉人陈维熙于 2012 年 9 月 10 日通过股权转让形式取得深圳铁建投资有限公司的实际控制权，该公司经营范围为投资管理（不含证券、期货、保险及其他金融业务）、企业管理咨询、国内贸易、货物及技术进出口，法定代表人为陈维熙，股东为陈维熙（90%的股份）和郑惠祥。同年 12 月 1 日，深圳铁建投资有限公司更名为保奇通公司。2014 年 12 月至 2015 年 8 月，陈维熙纠集同案人周毅等人（均另案处理），以保本金付高息为诱饵，采取公开授课等方式，虚假宣称投资保奇通公司的砂石产业项目能够获取稳定和高额回报，诱骗韩某东、王某伟、孔某悦、曾某红、薛某芳、张某恒、姜某发等多名集资参与人将资金支付到保奇通公司账户。陈维熙在取得资金后不用于公司的实际生产经营活动。经统计，陈维熙以保奇通公司名义非法集资款计 240 万元，未返还投资款计 1809567.72 元。

上述事实，有下列证据证实：

1.集资参与人王某伟、张某恒、曾某红、孙某悦、姜某发、李某煌等提供的委托投资协议、借款合同、报案材料，证明：集资参与人王某伟、张某恒、曾某红、孙某悦、姜某发、李某煌等人向保奇通公司投资理财的情况。具体如下：

（1）王某伟提供的委托投资协议，证明：王某伟于 2015 年 11 月 30 日与保奇通公司签订委托投资协议，约定王某伟将 20 万元投资于保奇通公司的砂石经营项目，委托期限为一年，年化收益率为 15%,按月支付收益。

（2）张某恒提供的借款合同，证明：张某恒于 2015 年 1 月 27 日与湖南保奇通砂卵石供销有限公司签订借款合同，约定张某恒借给该公司 30 万元，借款用途为扩大砂石产业生产规模，借款期限为一年，年利率为 15%。

（3）曾某红提供的借款合同，证明：曾某红于 2015 年 1 月 27 日与湖南保奇通砂卵石供销有限公司签订借款合同，约定曾某红借给该公司 40 万元，借款用途为扩大砂石产业生产规模，借款期限为一年，年利率为 15%。

（4）孔某悦提供的委托投资协议，证明：孔某悦于 2014 年 12 月 14 日与保奇通公司签订委托投资协议，约定孔某悦将 20 万元投资于保奇通公司的砂石经营项目，委托期限为

一年，年化收益率为15%,按月支付收益。

（5）姜某发提供的借款合同，证明：姜某发于2015年2月2日与湖南保奇通砂卵石供销有限公司签订借款合同，约定姜某发借给该公司10万元，借款用途为扩大砂石产业生产规模，借款期限为一年，年利率为15%。

（6）李某煌提供的报案材料、收据，证明：李某煌于2015年1月27日通过签订合同的方式投资了50万元到湖南保奇通砂卵石供销有限公司的账户410**********798。

（7）韩某东提供的委托投资协议，证明：韩某东于2014年12月5日与保奇通公司签订委托投资协议，约定韩某东将20万元投资于保奇通公司的砂石经营项目，委托期限为一年，年化收益率为15%,按月支付收益。

2.集资参与人王某伟、张某恒等人提供的银行交易明细、银行进账单、转账单、银行对账单、收据等资料，证明：集资参与人王某伟、张某恒等向保奇通公司转账的情况。

3．侦查机关调取的保奇通公司登记资料，证明：深圳铁建投资有限公司成立于2010年11月25日，法定代表人为蒋建国，经营范围为投资管理（不含证券、期货、保险及其他金融业务）、企业管理咨询、国内贸易、货物及技术进出口，股东为蒋建国、刘丽亚。2012年9月10日，蒋建国、刘丽亚将上述公司股份分别转让给陈维熙（90%的股份）、郑惠祥，法定代表人变更为陈维熙。2012年12月1日，深圳铁建投资有限公司名称变更为保奇通公司。

4.证人周某勇的证言，证明：我通过苏某毅认识了陈维熙，后来苏某毅叫我到保奇通公司担任总监，公司共三名总监，每名总监带一个团队，其中有一名业务员叫唐某芸，公司拉投资差不多一个月，募集了大概200多万元，资金去向不清楚。

5．被害人韩某东的陈述，证明：保奇通公司老板是陈维熙、总经理是苏某毅、业务员李某用。2014年，我到保奇通公司听课，他们让我向保奇通公司的沙石项目投资，有担保，保本付息，年化利率12%。当天，我和苏某毅签了一份协议，投资了20万元。2015年11月开始我就收不到利息。据我所知保奇通公司共有10个投资人，共计投资了240万元，210万元没收回。

6．被害人王某伟的陈述，证明：保奇通公司老板是陈维熙，总经理是苏某毅。2014年11月，保奇通公司的工作人员打电话给我说他们公司有投资项目问我有没有兴趣。于是我就到他们公司了解情况，苏某毅给我介绍该项目是投资砂卵石，主要是从长沙湘江流域打捞沙子，这些沙子是稀缺资源，可以稳健赚钱，该项目由保奇通公司（法定代表人是陈维熙）、保奇通砂卵石供销有限公司（法定代表人是陈维熙）等做担保。保奇通公司投资项目的投资期限是一年，保本付息，年化利率15%，按月付息，最低投资金额是20万元，我当日就签订了委托投资协议书。12月1日，我通过我的招商银行账户转了20万元到保奇通公司的农业银行账户（账号410**********389）。之后每月我的招商银行卡都能收到投资的利息2500元左右。2015年12月，按照投资合同约定保奇通公司应将本金还给我，但我没收到本金，于是我找陈维熙还钱。陈维熙说长沙砂卵石项目的公司欠他的钱，他要去长沙才能拿回钱。之后我多次向陈维熙催促还钱，他以各种理由推脱不还钱，至今未还。我共收了12个月的利息，共计3万元，扣除收回的利息还损失17万元。

经辨认照片，王某伟指认出陈维熙、苏某毅。

7．被害人张某恒的陈述，证明：2014年初，我在深圳任达山庄养老服务中心购买养老产品认识了唐某芸。2015年1月，唐某芸让我到深圳福田区经贸中心深圳聚宝隆金融控股公司参加该公司的投资会。我到那里看到公司挂牌是保奇通公司，有二三十个老人参加投资会，会上介绍保奇通砂卵石供销有限公司投资的砂卵石项目很有发展前景，该公司的老板陈维熙很有实力，因需要扩大投资，需要集资，最低投资10万元，保本付息，保证年化利率15%。唐某芸文问我要不要投资，我答应投资30万元并签订了“湖南砂石投资项目借款合

同”，借款方为湖南保奇通砂卵石供销有限公司，借款用途为扩大砂石生产规模，借款期限为一年，保本付息，年利率为15%，每个季度付我利息3.75%，一年内全部付清利息及本金。之后唐某芸带我到银行转账，我转了30万元到湖南保奇通砂卵石供销有限公司的账户（账号为410**********798）。4月28日，我收到利息1万元；8月3日，我收到利息1.12万元，10月28日，我收到利息1.1258万元，之后再没有收到利息，本金也没有收回。2016年1月，我找不到唐某芸。之后我就找陈维熙，陈维熙以各种理由推脱，直至2016年3月18日，陈维熙给我转账了5万元，后来再没有音讯了。我大部分的投资款都亏损了，我们投资人认为对方从开始就是利用保奇通公司投资业务进行非法融资，募集的资金没有用于扩大砂石经营，而是被用来融资了。据我所知，有10个投资人投资了保奇通公司，共投资240万元，有210万元未收回。

经辨认照片，张某恒指认出陈维熙、唐某芸。

8.上诉人陈维熙的供述：保奇通公司成立于2014年9月，法定代表人是陈俊，我是股东，苏某毅是总经理，负责公司运营，周某勇是副总经理，负责风险控制及产品包装，张哲是顾问，负责风控和产品包装，公司成员还有唐某芸、张连波等人。我们商量私募基金，针对养老院的老人，向他们宣传我在湖南的砂石产业项目，承诺投资该项目保本付息，年化利率15%，本金一年返还。大概有七八个投资人，共投资了240万元，我们与投资人签订委托投资合同，合同上有我的签名和盖章。投资款都用于公司的装修了。尚未给投资人兑付的投资款大概120万元。

9.深圳市司法会计鉴定中心出具的深司审字[2017]第60号专项审计报告，证明：（1）2014年12月1日至2015年3月31日，湖南保奇通公司农业银行账号410**********798和深圳保奇通公司农业银行账号410**********389收取10名投资参与人投资款240万元，截止2015年8月31日，共支付投资参与人款项计121241.30元，10名投资参与人投入资金与收到资金差额为1809567.72元。

（2）湖南保奇通公司农业银行账号410**********798和深圳保奇通公司农业银行账号410**********389收到投资参与人240万元后，连同收款前账户余额，大部分款项转到陈维熙、苏某毅、陈俊等个人账户。

二、前海众投公司成立于2014年6月13日，法定代表人为陈某逵，股东为陈某逵、吴某峰、张某周，经营范围为金融中介服务、互联网信息咨询、投资管理、投资咨询、投资顾问、受托管理股权投资基金（不得以任何方式公开募集和发信基金）。上诉人陈维熙于2015年8月18日通过股权转让形式取得前海众投公司的实际控制权并担任法定代表人，股东变更为陈维熙（占股90%）、郭某冬（占股10%）。在未经相关金融部门批准的情况下，陈维熙纠集上诉人陈尧、同案人唐某芸（另案处理）等人依托前海众投公司运营的“融促汇”P2P网络借贷平台(http://www.Rongcuhui.com)，以高息保本（年化利率12%-18%）为诱饵，发布虚假借贷项目标的，吸引大量投资者在该平台投资。期间，陈维熙负责管理公司，陈尧担任公司总裁并负责在“融促汇”平台发布虚假项目标的，还纠集上诉人吴迪担任投资顾问，负责招揽投资人及平台操盘；唐某芸担任总裁助理，负责公司财务。2015年8月18日至2016年6月27日，前海众投公司非法吸收投资参与人款项计I5181436.92元，未返还投资参与人款项计6178286.42元。其中，吴迪个人非法吸收投资参与人款项计260万元。

另查明，投资参与人的投资款未用于前海众投公司的实际经营，大部分款项被转入陈尧等个人账户。

上述事实，有下列证据证实：

1.侦查机关出具的受案登记表、立案决定书，证明：2016年7月14日，被害人庄颖到深圳市公安局福强派出所报案称其向前海众投公司“融促汇”平台投资29万元后无法收回。同年7月27日，深圳市公安局福田分局决定对该案立案侦查。

2.侦查机关出具的抓获经过，证明：2016 年 8 月 22 日，民警在广西壮族自治区梧州市璟景尚都 A 区地下停车场将陈维熙抓获；2017 年 2 月 18，民警在浙江省温州市平阳县水头镇双川路将陈尧抓获；2017 年 3 月 29 日，民警在北京市首都机场将吴迪抓获。

3.侦查机关出具的情况说明，证明：前海众投公司对公账户（400**********055 中国工商银行账号）在 2015 年 8 月 18 日前卡内余额计 76686.69 元，至 2016 年 6 月 21 日该卡收入 339 笔，共收入 28419402.79 元；2015 年 8 月 18 日至 2016 年 6 月 27 日，该卡支出 1775 笔，共支出 28496089.48 元，至 2016 年 6 月 27 日该卡余额为 0 元。

4.中国银行业监督管理委员会深圳监督局出具的证明，证明：该局未向前海众投公司颁发金融许可证。

5.侦查机关调取的银行开户资料、银行交易明细，证明：前海众投公司的账户为工商银行账号 400**********055，陈维熙名下开设的账户及各投资参与人的账户资料及交易情况。

6．侦查机关调取的工商登记资料，证明：前海众投公司成立于 2014 年 6 月 13 日，法定代表人为陈某逵，公司认缴注册资本为 1000 万元，股东为陈某逵、吴某峰、张某周，经营范围为金融中介服务、互联网信息咨询、投资管理、投资咨询、投资顾问、受托管理股权投资基金（不得以任何方式公开募集和发信基金）等。2015 年 8 月 18 日，前海众投公司股东陈某逵、吴某峰等转让股权给陈维熙（占 90%股份）、郭某冬（10%股份），公司法定代表人变更为陈维熙。

深圳市华茂源贸易有限公司成立于 2013 年 3 月 7 日，法定代表人为万某顺，股东为万某顺、汪某香，经营范围为服装服饰、电子产品等。

深圳聚宝隆金融控股有限公司成立于 2016 年 7 月 18 日，法定代表人为李某昌，股东为李某昌、艾某洲。

7．投资参与人提供的报案登记表、投资合同、投资项目网上截图、银行交易明细、转账凭证，证明：集资参与人繆小平、卢海波等人向“融促汇”网络借贷平台投资理财的情况。

8.证人胡某军的证言，证明：我在前海众投公司帮陈维熙开车。前海众投公司的老板是陈维熙，总裁是陈尧、行政助理是唐某芸，这几名高层管理人都是陈维熙找来的，陈尧负责公司的运营，陈尧与唐某芸负责招揽投资人，吴迪负责拉投资客户。陈维熙还了被害人 200 多万元，具体由我操作，目前投资人的损失大概八九百万元。

9.证人郑某国的证言，证明：2014 年，我通过吴迪推荐到前海众投公司工作，该公司做砂石和茶油林方面的融资，老板是陈维熙，总裁是陈尧、总裁助理是唐某芸，高级顾问是吴迪。我刚到该公司主要是与吴迪接触，作为投融资部经理，我主要对陈尧负责。我们为了茶油林和砂石业务融资跑了很多地方都没成功，吴迪说公司转型，主要通过 P2P 做车贷，我于 12 月初接触公司的网站并开始拉客户到该网站平台。用于融资的车只有两辆，一辆路虎、一辆奔驰，我没看到其它标的。大部分是小额融资，大概几千元至几万元的标的，我的团队只拉到庄颖夫妻投资的 20 万元。

公司的经营是陈尧负责，也是陈尧让我做 P2P，经营的问题都是向陈尧汇报。唐某芸是公司总裁助理，负责公司发布标的、统计投资人数、金额，茶油林的资料和砂石厂的资料都是她保管。吴迪是顾问，主要负责拉大额客户及为公司的项目决策。我在公司只看到两辆车，共发了 5 个车标。

10.证人梁某兰的证言，证明：我经同事介绍认识陈尧，之后陈尧招聘我去前海众投公司做出纳。公司每月 14 万元租金，公司的会计是李某娟。陈尧是我的直属领导，他让我转钱我就转钱了，没有什么审批手续，另外陈尧交代过如果他不在，唐某芸让我转账我也得操作。陈维熙一般不会让我转账，只有偶尔一两次经陈尧同意转了 1 万元左右，一般是陈尧或唐某芸打电话让我转账，金额也比较大，他们转账都是转到他们自己的银行卡。有一次唐某

芸提供了一张银行卡让我转了 40 多万元。公司的财务都是陈尧和唐某芸说了算，陈维熙基本不过问，给陈尧转了上百万元，我印象中没有与我们公司频繁资金往来的公司，只有投资人的钱转进转出。

11.证人李某娟的证言，证明：我于 2015 年 8 月开始在前海众投公司做会计，由唐某芸招聘我进公司，陈维熙是老板。陈尧是公司总裁，负责全面工作，唐某芸负责人事行政。公司出账一般都是陈尧签批，偶尔陈维熙签批，唐某芸负责报销员工的开销。公司做理财业务，就是客户向我们公司投资，我们公司支付利息。我不知道公司有什么标的，公司没有跟其他公司有业务及资金往来。

12．证人周某勇的证言，证明：2016 年，陈维熙说他要搞 P2P，请陈尧帮运营，我给他们介绍了朋友的前海众投公司，当时该公司已欠款大概 600 万元，我们都很犹豫接不接，后来我们开会讨论该问题，参加会议的有陈维熙、我、陈尧、吴迪及一名律师，吴迪说这个平台在公交车上面有广告，可以做得很大，陈尧也支持吴迪的观点，最后陈维熙表示要做。陈维熙是老板，陈尧是总裁，吴迪是投资顾问，负责帮公司拉投资，并且对接大资金客户，我负责公司的投资，潘某南负责运营，唐某芸是陈尧的助理。陈维熙不管公司的事，主要是陈尧负责。2016 年 8 月，我曾经和陈尧一起到云南的烟厂，准备投资上千万元，后来吴迪没融到资，投资的事作罢了。公司的财务由陈尧负责，最后审批环节是陈尧。唐某芸负责行政，后他作为陈尧的助理，也开始负责财务，我报销要把票据给唐某芸，但还需要陈尧审批。运营的标的及风险控制都是陈尧负责。

13.证人唐某芸的证言，证明：我在前海众投任总裁助理，听从陈维熙和陈尧的工作安排，我们公司是做 P2P 平台的，吸引老百姓投资，年化利息是 16－18%。标的的种类有车贷和房子相关的，承诺保本付息。我刚到公司时是行政经理，到 2015 年 10 月陈尧让我做他的助理并兼职行政方面的工作，我于 2016 年 1 月离职，陈维熙说陈尧挪用了公款，我记得陈尧承认了挪用公款的事，我梳理出来的有 100 万元左右。

公司老板是陈维熙，总裁是陈尧，我是总裁助理，运营部（发放投资标的）开始是潘某南负责，他做了一两个月离职，后来由陈尧接手负责，投资部（负责风控）负责人开始是周某勇，他做了三四个月左右也离职了，之后来了一名姓郑的，财务部负责人是李某娟。平时公司的运营和管理由陈尧负责。吴迪是做策划和方案的，项目能否通过由陈尧审批，他是公司的顾问。

陈维熙带我们到他湖南的砂石场和油茶林实地考察过，证明他有产业有资金，让我们放心做这个平台。车贷是陈尧找的，是否真实我不清楚。我在公司负责采购、备用金的管理、传达文件、接待投资客等。我的工资是：2015 年 8、9 月份 5500 元，10 月份 7000 元，11 月份 10000 元，没有提成，我的工资由陈维熙支付。

前海众投公司的标的从哪里来的不清楚，标的是谁定的也不清楚，陈尧拿了公司的 100 万元说是来做车的标的，拿钱去收车抵押。陈尧还拿了公司 180 万元，他说是用来投资一个上市公司的项目，但后来没做成。陈尧拿钱可以不通过陈维熙。我知道公司的车贷项目，但没见过运作，也没见过谈相关业务。

14．被害人庄某颖的陈述，证明：2015 年 12 月份，我经朋友介绍，知道了一个“融促汇”P2P 网络借贷平台，在公交车上也看过这个平台的广告，该平台所属公司地址在深圳市福田区大中华国际金融中心 A 座 1002，我于 2015 年 12 月 14 日到该地点考察。“融促汇”的销售总监向我介绍该投资平台，该平台的老板是陈维熙。郑某国当场帮我注册成了该平台的会员，充值了 100 元。我回家后让我丈夫也在网上注册了该平台的会员并于 12 月 15 日充值了 10 万元，12 月 16 日又充值了 19 万元，后来又投了 28 万元。2016 年 1 月 15 日，投资到期了，我在家电脑上做了提现操作，成功后会在三个工作日打款到我绑定的银行卡中，但我没收到回款，所以我就上门找陈维熙要钱，但没有任何答复。2016 年 5 月份的一天，

我们投资人在罗湖见到胡某军，他说给我们登记投资记录并退钱，但至今没有退钱。胡某军电话也不接，我们就报警了。

关于“融促汇”的情况：聚宝隆金融控股公司位于深圳市中华国际金融中心 A 座 1002 室，该办公室的门口标示“融促汇”，公司的法定代表人是胡某军，实际控制人是陈维熙，该公司成立于 2014 年 12 月，“融促汇”是一个 P2P 网络借贷平台，经营业务是通过平台撮合投资人资金出借给借款人，期限有 7 天、1 个月、3 个月或 6 个月回款，分别年化收益 13.5/12.6/16/18.6。承诺保本付息。该平台通过网站发布不同的投标项目，相关的项目标注有期限、利息，投资人根据自己的选择进行投标，投标的钱就是投资人充值在平台个人账户的钱，投资期限届满后，投标的本金和利息返回平台的个人账户，可以手动申请提现，三个工作日内打到绑定的银行卡内。直到 1 月 15 日我投资到期发现无法提款。我从没有见过陈维熙，我认为陈维熙开始就是利用“融促汇”进行非法融资，所募集的资金没有真正用于供应链金融，而是用于自融了，资金去向不明。

我通过线上绑定银行卡后充值，通过汇潮支付和宝付支付这两个第三方支付公司去充值，进入到前海众投公司绑定的银行卡（中国工商银行账号：400**********055）。我丈夫田小宝使用账号投资了 29 万元。目前余额为 293075 元，无法提现。

陈维熙是前海众投公司的法定代表人，也是聚宝隆金融控股有限公司的实际控制人，前海众投公司的总裁是陈尧，我在大中华国际金融中信 A 座 1002 室见过他，他负责公司运营。陈尧于 2016 年 1 月离职后，郑奇国接手，不久也辞职了。

经辨认照片，庄颖指认出陈维熙，胡某军。

15.被害人关某环的陈述，证明：2014 年 9 月，我在深圳市的公交车上看到“融促汇”P2P 网络借贷平台的广告，该广告声称为广东中小企业融资，后来我登录该平台，该平台发布的投资标的年化收益率在 12%-22%，我投资了 5 次共 16000 元，到期后均能拿回本金与利息，我就相信了这个平台。但在 2015 年 10 月到 12 月间，我投了 7 次共 35000 元，到了 2016 年 2 月提现 5000 元则无法提现了，后来 3 月份与其他投资人到了该公司催款，才拿回来 5000 元。2016 年 2 月 29 日，“融促汇”投资平台就关停了取现服务功能，3 月 1 日后到期的投资资金全部被平台冻结。5 月 10 日，我去催款时，该公司已经关门了，经询问，得知前海众投公司已经拖欠数月租金和管理费，也无法联系该公司的人了。我所投资的本金加利息共计 35690.21 元无法提现，本金 31704.16 元，利息是 3986.05 元。

我先在平台上注册成为会员，再把钱充值到会员账户上，通过会员账户上的钱投资到平台发布的标的上，到期就会返还本金和利息，需要提现的话三日内把钱汇入投资者的银行账户，若没有继续提现或者投资，账户上的钱不会产生利息。根据借款协议书，“融促汇”属于中间方，提供标的。我通过其它投资者知道该公司的老板是陈维熙，该平台发布有很多标，比如游戏运营、无人机项目、酒店公寓融资等，不同的标有不同的期限与利率。

经辨认照片，关某环指认出陈维熙。

16．被害人刘某杰的陈述，证明：我在“融促汇”平台共投本金加利息计 10930 元，其中本金 1 万元，利息 930 元，2016 年 4 月 26 日后就无法提现了。我打电话给陈维熙询问为何不能提现，陈维熙说公司周转出现问题，现在在想办法办理贷款，承诺 6 月 15 日左右恢复提现。但 6 月 15 日还是无法提现。该平台有两个第三方支付平台，一个是宝付，一个是汇潮付，我通过后者支付。

17．被害人王某宇的陈述，证明：我是受邓某元委托报案的，邓某元从公交车上的广告看到了“融促汇”P2P 网络借贷平台。2015 年 3 月，投了三笔本金和利息都收回了。从 2015 年 8 月 1 日开始共投了 8 笔，共 464482 元，2016 年春节，仍没有收到本金与利息，我于 2016 年 4 月份，我催公司还款，收回来 2 万元，之后就再也没有收到还款了。

经辨认照片，王某宇指认出陈维熙。

18．被害人付某竹的陈述，证明：经朋友介绍认识了吴迪，2015 年 8 月的一天，吴迪叫我到他公司，他介绍了这个平台的情况，说老板很有实力，让我们投资，并承诺保本付息，18%的年收益，之后吴迪当场给我们在“融促汇”上注册了账号，后来给我介绍认识了他们公司的总裁陈尧，告诉我以后公司业务都是陈尧来负责跟进。后来陈尧联系我到公司签订协议，我到公司与陈维熙签了一份借款协议书。随后提供了转款账户。

2015 年 9 月至 12 月，我共投入了 105 万元，收回了 215364 元，还有本金 834636 元无法提现。我经吴迪了解到“融促汇”P2P 网络借贷平台的，也在公交车上看过广告，陈尧是该平台的负责人，我最初投资时与陈尧沟通业务，实际控制人是陈维熙，追款找陈维熙，唐某芸是总裁助理。

我们投资人认为陈维熙从开始就是利用“融促汇”平台进行非法融资，募集的资金没有用于公司的经营项目，而是用于自融了。

经辨认照片，付某竹指认出陈维熙、陈尧、唐某芸。

19．被害人孟某伟的陈述，证明：2015 年 3 月，我在深圳的公交车上看到“融促汇”的广告，利息回报可高达 20%，之后我根据公交车上的网址登陆了该“融促汇”网站并注册了会员，我共投资了 22 万元。2016 年 1 月，该网站就不能提现了，我就到深圳市福田区大中华 A 座 1002 房找到“融促汇”的负责人陈维熙，他安慰我说钱会还给我的，过后陈维熙就转账了 5 万元给我，其余钱没还，后来公司关门了，我也找不到陈维熙了。

经辨认照片，孟某伟指认出陈维熙。

20．被害人廖某惠的陈述，证明：2015 年 9 月，我经付某竹认识了吴迪，吴迪介绍了前海众投公司，我共投入了 41.25 万元，收回 1 万元。我还作为投资者代表参观了陈维熙在湖南的资产，2015 年 9 月，吴迪、陈尧还有一些其他工作人员带我及其他三十多名投资人到湖南长沙一个采砂厂参观，说是陈维熙的资产，我们相信陈维熙很有实力，吴迪与陈尧还在酒店拿了一些资产证书给我们看，陈维熙向我们保证如果还不上钱，就将云泉镇上资产的持有人转到我们投资人名下。

陈维熙在长沙向我鼓吹公司实力，并保证可以将名下资产转到投资人名下，陈维熙还说他有林业公司、采沙厂、云泉镇等资产，让我放心投资。吴迪和陈尧也积极让我投资，教我在平台上操作。唐某芸负责讲解前海众投公司项目。胡某军是负责处理还款事宜。2015 年 11 月，我到前海众投公司的办公地点，吴迪、陈尧、唐某芸鼓动我买一个原始股的项目，我又投了 20 万元，签好合同后唐某芸拿去给陈维熙签字，线下转账到前海众投公司的工商银行卡（账号 400**********055）。2016 年 1 月，我购买的部分理财产品到期了，但无法提现。于是我到前海众投公司找陈维熙，他说陈尧把钱卷走了。后来我打陈维熙的电话打不通或打通了不接。目前我有 40 万元没收回。

经辨认照片，廖某惠指认出陈维熙、陈尧、唐某芸、胡某军。

21．上诉人陈维熙的供述：2015 年 1 月，我认识了陈尧。2015 年 7 月，陈尧提出搞一个 P2P 平台融资，因为当时国家已经不允许注册这种互联网金融性质的公司，所以我们就想办法找一个公司接手，最后在 2015 年 8 月 l8 日以股权转让形式取得深圳前海众投公司，我在商谈收购股权时已经知道这个公司已经亏损了 586 万元。我是法定代表人，陈尧任公司总裁，负责营运，每月工资 2 万元，提成约每月 3 万元；唐某芸任总裁助理，负责财务，每月工资 12000 元，提成约每月 1000 元至 2000 元；周某勇任副总，梁某兰任出纳，每月工资 6000 元，还有一名会计，每月工资 8000 元。

在未经相关金融部门批准的情况下，公司建立“融促汇”P2P 网络借贷平台，通过招标方式吸收资金，发标种类包括车贷和保理，周期为 7 天、1 个月、3 个月或半年，承诺保本付息，年化利率 12%-18%。平台通过线上和线下两种方式募款，每个月募集资金 300 万元左右，到 2015 年 10 月，公司已经无法正常兑付，我与部分投资人协商还款，到 2016 年 5 月，

我把房产抵押贷款还了一部分投资人180多万元，通过业务回款给部分投资人还了120万元，目前还差投资人600万元没法还。

我建立“融促汇”P2P网络借贷平台的目的是为了湖南株洲攸县一个茶油林基地募集资金，该基地法定代表人是我表弟曹硕，但还未将融资的钱进入该基地，平台就无法兑付了，因为陈尧将公司的480万元挪用了，他通过提现及转账的方式挪用，转账是转到唐某芸的账上后再转到陈尧的账上。

公司每月以运营费用支出有房租15万元、员工工资15万元、奖金十几万元，总共50万元左右。这些营运支出从我的工商银行卡打到公司账上，再由公司的账户支付。

平台发展客户的方式主要是广告和由陈尧、唐某芸、吴迪等人拉客户。客户大部分是深圳的，平台注册用户有两三千人，频繁投资用户有两三百人。平台发的标是否真实存在我不清楚，都是陈尧弄来的，我给陈尧的指令是能募集到资金就行。吸收资金方式一是线下通过银行账号直接汇款到前海众投绑定的银行卡，还有一种是线上充值方式，通过汇潮支付和宝付支付这两个第三方支付公司去充值，也是进入到前海众投绑定的银行卡。

我向投资人吹嘘“融促汇”平台有很大的经济实力，许以高额利息回报，吸引投资者。陈尧教我带部分投资者到了湖南看一些我的物业，如砂场、茶油林地、砂场码头等，吸引投资者，让投资者有信心，但其实这些产业都是亏损的，短期内无法盈利，更不可能有高达12%-18%的回报给投资人。是陈尧教我这么说的，他说只有这样说才能让公众来投资。我早已向陈尧、唐某芸、吴迪等说过无法维持下去，但他们还是向投资者不断吹嘘，不断拉人进来投资。他们三人后来跑路了。

员工工资由我前海众投公司绑定的工商银行账户发放，具体由陈尧负责。吴迪只负责拉客户，胡某军帮我开车，郑奇国是公司出事后才由陈尧介绍过来的，我发现陈尧跑路后就将郑奇国解雇了。陈尧是2016年1月离开的，那时公司已经无法偿还投资人的钱了，陈尧就走了。目前吸收的资金大部分都是给陈尧和唐某芸卷走。聚宝隆公司是我让两名员工在2014年9月注册的，准备弄基金的，但一直没有弄，到了2015年9月18日开始营运“融促汇”P2P时，就把公司的地址放在聚宝隆所在地大中华进行营运。我不记得投入1000万元到华茂源公司，问陈尧可能知道。

“融促汇”平台无法兑现后，我向被害人还款差不多300万元，湖南保奇通公司停业了，还有700万元的账没收回来。

22．上诉人陈尧的供述：我于2015年6月认识陈维熙，他准备成立一个P2P公司，他在湖南有个项目需要资金，叫我过来帮忙开设平台募集资金。当时我们的团队有陈维熙、唐某芸、周某勇和我，那时国家政策已经不允许注册P2P公司。2015年8月，陈维熙和周某勇收购了前海众投公司，该公司有一个P2P平台叫“融促汇”。陈维熙是公司的法定代表人，我是总裁，唐某芸是总裁助理，吴迪负责拉投资人投资，潘虹南负责操盘，周某勇是投资部经理。我只负责安排接待投资人，其它事不管。吴迪和潘虹是我招聘来公司的。这个平台通过招标的方式吸收资金，发标的种类包括车贷和保理，周期为7天、一个月、三个月及半年，承诺保本付息，年化利率为12%-24%，平台通过线上和线下两种方式募款。募集到的资金我不清楚有无用于陈维熙在湖南的项目。我接手找了一些车标是真实的。我于2015年10月离职。

2015年9月我经陈维熙的同意借了公司100万元，这笔钱至今未还，公司每个月固定支出50万元左右。我每个月2万元工资，没有提成。

23．上诉人吴迪的供述：2015年8月，我通过朋友潘虹南介绍认识了陈尧，他招聘我进入前海众投公司，陈维熙是老板，陈尧是总裁。8月18日，陈维熙接手“融促汇”平台，平台通过招标的方式吸收资金，发标的种类包括保理、车贷等，承诺保本付息，年化利率为36%。陈维熙安排我做公司的高级顾问，负责招揽大额投资人，陈尧负责平台运营，周某勇

是投资部经理。后来陈维熙说陈尧转走了300万元，之后平台无法兑付。我共招揽了三个大客户：付竹、徐楠、任宽，付竹筹集朋友的资金投了100万元，徐楠和他妹妹凑了100多万元投资到平台，任宽投资了20万元，他们的投资基本没有提现，平台无法兑付。我通过平台募集资金共计260多万元。

我带我的客户考察陈维熙的产业，让他们相信投资可以有回报。我不知道投到公司的钱的去向。我工资是每个月2万元，报销费用是5000－6000元，没有提成。公司的运营和标的都是陈尧负责。我于2015年12月离职。我看到“融促汇”的营业执照上有金融许可资质。唐某芸是公司助理，我找她报销我在公司的出差费、公司活动的费用。

24.侦查机关制作的现场勘验笔录及拍摄的照片，证明：深圳市公安局福田分局刑警大队四中队于2016年8月31日16时8分至17时38分对深圳市福田区大众化国际金融中信A座1002室进行勘验的情况。

25.深圳市司法会计鉴定中心出具的专项审计报告，证明：（1）2015年8月18日至2016年6月27日，前海众投公司收取投资参与人资金计15181436.92元，返还投资参与人计9003150.5元，未返还投资参与人计6178286.42元。

（2）前海众投公司工商银行账户400**********055（以下简称“1055账户”）大部分资金转到陈尧、唐某芸等个人账户。具体如下：

①前海众投公司1055账户支付给陈尧银行账户资金去向：2015年9月11日至2016年2月1日，前海众投规定1055账户支付给陈尧三个银行账户4094000.00元（不含已注明为“工资和费用的报销”的金额），其中：陈尧工商银行账户635000.00元、农业银行账户145000.00元、平安银行账户3314000.00元。

前海众投公司1055账户收到陈尧平安银行2585账户转入资金计933500.00元。

陈尧平安银行2585账户净收到前海众投公司1055账户2380500.00元，在追查其去向的同时又收到其他账户转入600000.00元，大部分款项回到陈尧、陈维熙等个人账户。

②前海众投公司1055账户支付给唐某芸银行账户资金去向：2015年11月13日，前海众投公司1055账户支付给唐某芸工商银行账户622112.49元（不含已注明为“工资和费用的报销”的金额），收款后账户余额622227.27元。2015年11月18日，唐某芸该账户转出600000.00元给张某鑫招商银行4141账户。前海众投公司工商银行1055与唐某芸银行的其他资金往来均为小额交易，未予追查。

③前海众投公司1055账户支付给何某芳银行账户资金去向。前海众投公司1055账户支付给何某芳招行0990账户计177332.00元，该账户收款后付给何志平中国邮政储蓄银行2434账户37000.00元、何某芳招行信用卡还款76800.00元、张某净额54000.00元，其他有消费、取现等。

④前海众投公司1055账户支付给佟某华银行账户资金去向。2015年10月27日，前海众投公司1055账户支付给佟某华农业银行5412账户200000.00元，收款后账户余额215197.66元。2015年10月29日，佟某华该账户转出180000.00元给黄某盔8176账户、转出20000.00元给佟某华交通银行账户。前海众投公司用于支付工资、津贴、税款、社保、公积金、房租、水电、其他各项费用等计1906303.21元。

关于本案的审计报告是否客观真实的问题。经查，本案的专项审计报告是由具备法定资质的鉴定机构根据侦查机关提供的投资参与人的转账凭证、银行交易明细、涉案公司及陈维熙、陈尧名下的银行账户交易流水等涉案资料作出，相关审计意见与在案书证、证人证言等其他证据能相互印证，内容客观真实，原判予以采信理据充分。因此陈维熙及辩护人对此提出异议依据不足，不予采纳。

关于上诉人陈维熙、陈尧的行为是否构成集资诈骗罪的问题。经查，首先，陈维熙、陈尧虚构事实，隐瞒真相。陈维熙、陈尧在前海众投公司没有取得政府部门融资行政许可的情

况下，通过该公司的“融促汇”平台发布虚假标的并向投资人谎称保本付息及年化利率高达12%至18%，以此为诱饵向公众进行非法集资活动。其次，陈维熙辩称其通过“融促汇”平台募集的资金是为了投资湖南茶油林和砂石项目，但根据投资参与人提供的转账凭证、银行流水及会计鉴定中心出具的审计报告，前海众投公司吸收公众投资款中除小部分资金用于公司的房租、员工工资等外，大部分资金被转入陈尧等个人账户，涉案款项未用于实际生产经营活动，更没有流入陈维熙所述的茶油林、砂石等项目，且陈维熙供认上述茶油林、砂石等项目都是亏损的，没有实际盈利，更不可能有高达12%至18%的回报给投资人，最终造成巨额集资款无法偿还。根据《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》规定，“集资后不用于生产经营活动或者用于生产经营活动与筹集资金规模明显不成比例，致使集资款不能返还的”，应视为“以非法占有为目的”。综上，陈维熙、陈尧作为前海众投公司的实际负责人，明知公司没有盈利项目，还通过虚假宣传非法集资，导致投资人损失巨大，原判认定他们的行为构成集资诈骗罪理据充分。因此，陈维熙、陈尧及其辩护人辩称陈维熙、陈尧的行为构成非法吸收公众存款罪理据不足，不予采纳。

关于本案是否是单位犯罪的问题。经查，上诉人陈维熙取得前海众投公司的控制权后，一直伙同上诉人陈尧、吴迪利用前海众投公司的“融促汇”P2P网络借贷平台，虚构投资标的，诱骗投资者在该平台投资，且取得的大部分投资款均转到陈尧等个人账户中，没有证据证明用于实际生产经营活动，陈维熙、陈尧、吴迪等人经营前海众投公司期间主要从事集资诈骗活动，依法不应以单位犯罪论处。因此，陈尧、吴迪及其辩护人辩称本案系单位犯罪缺乏理据，不予采纳。

关于上诉人陈尧是否是从犯的问题。经查，陈尧作为前海众投公司的总裁，主要负责在“融促汇”平台发布虚假项目标的，还纠集吴迪参与，将投资人的大部分投资资金转入个人账户中，其在共同犯罪中明显起主要作用，依法应认定是主犯。因此，陈尧及其辩护人辩称陈尧是从犯理据不足，不予采纳。

关于上诉人吴迪是否是从犯的问题。经查，在案证据证实吴迪伙同陈维熙等人以前海众投公司的名义向公众非法吸收存款，主要负责招揽投资人到“融促汇”平台投资并负责在该平台操盘，但其未参与决策或指挥，不了解涉案投资款的去向，更未使用或分取涉案投资款，其主观上不具有非法占有涉案投资款的目的。因此，原判以非法吸收公众存款罪而非集资诈骗罪追究吴迪的刑事责任，符合本案事实和法律规定，在此情况下不认定吴迪为从犯并无不当。因此，吴迪及其辩护人辩称吴迪是从犯理据不足，不予采纳。

本院认为，上诉人陈维熙、陈尧以非法占有为目的，虚构事实，隐瞒真相，使用诈骗方法非法集资，数额特别巨大，其行为均已构成集资诈骗罪。上诉人吴迪在未取得金融许可资格的情况下，向社会不特定对象吸收存款，扰乱金融秩序，数额巨大，其行为已构成非法吸收公众存款罪。在以前海投资公司名义实施的集资诈骗共同犯罪中，陈维熙、陈尧各起主要作用，均是主犯，依法均应按其参与的全部犯罪处罚。原审判决认定事实清楚，证据确实、充分，定罪准确，量刑适当，审判程序合法，唯未认定陈维熙是主犯不当，应予纠正。陈维熙、陈尧、吴迪及辩护人要求从轻处罚理由不成立，不予采纳。依照《中华人民共和国刑法》第一百九十二条、第一百七十六条、第二十五条第一款、第二十六条第一款、第四款、第六十四条、第六十七条第三款及《中华人民共和国刑事诉讼法》第二百三十六条第一款第（一）项的规定，裁定如下：

驳回上诉，维持原判。

本裁定为终审裁定。

审判长　　王晓文

审判员　　黄玉良

审判员　　梁　美

二〇一九年九月十九日
书记员　　喻　勋

案例二、甘宇兵夏平珍集资诈骗、非法吸收公众存款案

广东省高级人民法院
刑 事 裁 定 书

（2017）粤刑终 58 号

原公诉机关广东省广州市人民检察院。

上诉人（原审被告人）甘宇兵，男，1964 年 12 月 13 日出生，汉族，文化程度高中，户籍地湖北省天门市。因涉嫌集资诈骗罪于 2015 年 1 月 27 日被刑事拘留，同年 3 月 5 日被逮捕。

辩护人李华，广东信德盛律师事务所律师。

上诉人（原审被告人）夏平珍，女，1965 年 2 月 1 日出生，汉族，文化程度小学，户籍地湖北省天门市。因涉嫌集资诈骗罪于 2015 年 1 月 27 日被刑事拘留，同年 3 月 5 日被逮捕。

上诉人（原审被告人）罗志新，男，1988 年 3 月 7 日出生，汉族，文化程度高中，户籍地广东省梅州市梅县区。因涉嫌集资诈骗罪于 2015 年 1 月 27 日被刑事拘留，同年 3 月 5 日被逮捕，现已取保候审。

广东省广州市中级人民法院审理广东省广州市人民检察院指控被告人甘宇兵犯集资诈骗罪、被告人夏平珍、罗志新犯非法吸收公众存款罪一案，于 2016 年 12 月 15 日作出（2015）穗中法刑二初字第 188 号刑事判决认定被告人甘宇兵犯集资诈骗罪，判处有期徒刑十五年，并处罚金人民币四十五万元；被告人夏平珍犯非法吸收公众存款罪，判处有期徒刑四年，并处罚金人民币十万元；被告人罗志新犯非法吸收公众存款罪，判处有期徒刑二年，并处罚金人民币三万元；追缴被告人甘宇兵的违法所得，按比例发还被害人，追缴数额以被害人损失和甘宇兵违法所得数额为限,不足以弥补的被害人损失，责令被告人甘宇兵退赔。宣判后，被告人甘宇兵、夏平珍、罗志新均不服，提出上诉。本院依法组成合议庭，经审阅案卷，提讯上诉人，听取辩护人意见，认为案件事实清楚，决定以不开庭的方式进行审理。现已审理终结。

原审判决认定：被告人甘宇兵于 2010 年投资成立广州市环宇投资有限公司（简称环宇公司），2014 年 2 月环宇公司开设“中大财富 P2P 网络理财平台”（www.zhongdacaifu.com），对外宣称该平台是为借贷双方提供信息服务，由投资人通过该平台借款给借款人，投资人可获得借款利率 22%左右的回报。被告人甘宇兵虚构借款人需要借款的信息，将虚假借款信息发布到平台，利用该平台共接受被害人黄某等 367 人资金共计人民币 8398.960530 万元，甘宇兵将上述款项用于偿还个人债务及支付投资人回报、维持平台运营，被害人在累计提现共计人民币 3347.702096 万元后，剩余款项无法提取，造成被害人损失共计人民币 5051.258434 万元。被告人罗志新作为该平台运营总监，被告人夏平珍作为该平台财务负责人，参与了该平台吸收公众款项的行为。

2015 年 1 月 26 日晚，部分被害人聚集在该平台办公场所，要求支付投资款项，交涉未果后报警，甘宇兵在知道已有警察到场的情况下赶到平台，后警方于次日凌晨将甘宇兵、夏平珍、罗志新带到公安机关进行调查。

原判认定上述事实，有被害人陈述、书证、证人证言、被告人甘宇兵、夏平珍、罗志新的供述和辩解等证据证实。

原审法院认为，被告人甘宇兵以非法占有为目的，使用诈骗方法非法集资，数额特别巨大，其行为已构成集资诈骗罪。被告人夏平珍、罗志新参与变相吸收公众存款，扰乱金融秩

序，数额巨大，均已构成非法吸收公众存款罪。甘宇兵在犯罪以后自动投案，如实供述自己的罪行，是自首，可以从轻处罚。夏平珍、罗志新在共同犯罪中起次要作用，是从犯，依据两人在共同犯罪中的地位和作用，对夏平珍可以从轻处罚，对罗志新可以减轻处罚。依照《中华人民共和国刑法》第一百九十二条、第一百七十六条第一款、第二十六条第一款、第四款、第二十七条、第五十二条、第五十三条、第六十四条、第六十七条第一款、《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》第三条第二款、第三款、第五条第一款、第三款、《最高人民法院关于适用财产刑若干问题的规定》第二条第一款、第五条、第十条第一款之规定，作出前述判决。

甘宇兵上诉提出：（1）一审法院认定上诉人构成集资诈骗罪的主要依据是强调上诉人将集资款用于偿还个人债务，忽略了形成债务的原因是由于投标纺织品市场经营权以及对市场进行升级改造，因此没有认定集资款用于经营活动，是不符合事实的。（2）上诉人没有非法占有目的，对募集的资金没有肆意挥霍，没有携款逃匿，没有用于违法犯罪活动，其在环宇市场还有巨额的租金可以用于清偿债务，应改判其构成非法吸收公众存款罪。（3）一审认定黄某等部分被害人的损失数额不准确，出入较大。（4）一审法院虽认定上诉人有自首情节，但在量刑时并没有体现从轻处罚。

甘宇兵的辩护人提出：（1）上诉人甘宇兵没有以非法占有为目的的主观故意。甘宇兵将集资款用于偿还此前为了获得环宇纺织品市场经营权所欠债务，实质上就是用于生产经营行为，不能因为其用于偿还债务就认定其具有非法占有目的。甘宇兵也不符合没有归还能力而大量骗取资金的情形，其投资的纺织品市场具有较强的盈利能力。甘宇兵也不存在逃避返还资金的行为，为了解决困难其多方筹措，在出现挤兑之后也是积极面对。因此必须坚持主客观相一致原则，不能仅凭较大数额的非法集资款不能返还的结果就推定行为人具有非法占有的目的。对上诉人甘宇兵的行为应认定为非法吸收公众存款罪。（2）一审法院认定甘宇兵有自首情节，但在量刑时没有体现从轻处罚。请求二审对上诉人甘宇兵予以改判。

夏平珍上诉提出：（1）一审判决认定上诉人是中大财富理财平台的财务负责人没有依据。上诉人在成立理财平台前曾担任环宇公司的财务工作，但平台成立后从未参与。第一次笔录是在不知情的情况下签名的，该笔录的内容也有多处与其他证据明显矛盾之处。同案被告人、证人罗某都没有指认上诉人是财务负责人；谭某的证言前后不一致，也与其他证人的陈述矛盾。（2）一审判决没有全面审查证据，而是以上诉人和甘宇兵夫妻关系、对公司有重大影响为由，只采信了对上诉人不利的证据，刻意忽略对上诉人有利的证据。（3）上诉人在案中所起作用极小，比罗志新轻得多，量刑却比罗志新重，极不公平。

罗志新上诉提出：（1）一审判决对中大财富平台的运作模式认定错误。平台作为独立于投资人与借款人之间的中介，只是收取投资人获利的8%作为管理费，而非赚取利差，与银行的存贷款业务模式完全不同。这种运营模式并不违法。（2）上诉人任职线上运营部运营总监，只负责平台网络的优化、网站推广等，并非环宇公司所有部门的总监，没有涉及“线下运营部”（不在一处办公）的财务、借款项目。（3）甘宇兵设立平台之初并非就是为了犯罪，只是当他觉得盈利慢之后，才变相控制借款项目上的借款人账户从而非法获得投资人款项，这是他的个人所为，而相关的事务都是由其亲属负责。（4）上诉人一直认为网络借贷平台是国家大力扶持的，不知道甘宇兵虚构借款标的自己骗取款项，否则坚决不会受雇，从这个角度说上诉人也是受害人，不应当与甘宇兵相提并论。（5）在公安人员到公司处理投资人聚集期间，上诉人有机会离开而没有离开，最后被带回公安机关，应当认定其有自首情节。综上，上诉人运营中大财富的行为不符合非法吸收公众存款和变相吸收公众存款的特征，不构成非法吸收公众存款罪。

经审理查明：

2014年2月，为了缓解投资纺织品市场所造成的资金周转困难，上诉人甘宇兵以其控

制的广州市环宇投资有限公司名义与刘某等人合作开设“中大财富 P2P 网络理财平台”（www.zhongdacaifu.com）,甘宇兵出资并负责借贷业务，对方负责建立和运营网上平台。经营一段时间后，上诉人甘宇兵急于获取资金用于偿还巨额高息借款，于是出资向对方买下平台自己控制，从同年 5 月间开始，在没有取得吸收公众存款资格的情况下，宣称投资人通过该平台借款给借款人，可获得借款利率 22%左右的回报，然后利用其经营环宇市场、掌握大量租户信息的便利，用部分租户名义或者编造公司员工经营市场档口需要资金，虚构借款需求放到平台上，并为他们的借款账户办理委托支付，当有投资人向上述“借款人”贷款时资金就会转到甘宇兵指定的账户，实际上由甘宇兵自己作为借款人吸收投资人资金。上诉人罗志新受雇作为该平台线上运营总监，负责网站管理、优化、营销、推广等工作；资金及账户由上诉人甘宇兵通过财务人员直接操控，上诉人夏平珍协助甘宇兵处理部分财务工作。至案发，上诉人甘宇兵通过该平台先后接受了黄某等 367 人出借的资金共计人民币 83989605.30 元。甘宇兵将上述款项用于偿还此前所欠债务以及支付投资人回报、维持平台运营等。在投资人先后提现人民币 33477020.96 元后，剩余款项甘宇兵无法归还，造成投资人损失人民币 50512584.34 元。

2015 年 1 月 26 日晚，部分投资人聚集在该平台办公场所，要求收回投资款项，交涉未果后报警。甘宇兵在知道已有警察到场的情况下回到平台，次日凌晨与夏平珍、罗志新一起被带回公安机关处理。

认定上述事实，有经一审质证的以下证据证实：

1、被害人黄某的陈述，主要内容为：2014 年 7 月份，我去广东金融博览会（琶洲会展中心）上看到一个叫中大财富网站的金融平台，工作人员向我们宣传鼓吹，称该平台是全国首创最大的金融平台，可以接收我们的钱帮我们投资借贷，平台旗下有上百间商户，我们的钱是借给平台的商户做资金周转的，年化收益率 22.4%。后来我就在中大财富网平台上购买了多份融资合同。2014 年 8 月份，我购买的第一份合同到期时就开始有收益，12 月 25 日左右发现没有收益，大量投资者挤提导致平台无法支付，于是我从 12 月 26 日开始到该公司追讨本钱。

我所购买的标的都是在中大财富网站上签订的，支付款项都是通过网银转账到指定的账户。都是网上电子合同，上有三间担保公司的盖章，标的书上标明了借款种类、借款本金、借款利率（22.4%）、还款日期和还款方式等。该平台称款项是用作服装类投资，我不清楚他们公司有无实际投资行为和平时的运作情况。他们在网络大肆宣传高回报、高奖励，进行宣传、推广和营销。我平时是通过 QQ 与他们公司的客服接触的，QQ 号是 26×××16，客服名字叫 Kitty，真实身份我不知道。他们的实际控制人是甘宇兵。我投入人民币约 420 万元，收回人民币 100 万元，实际损失人民币 320 万元。

经辨认照片，黄某辨认出上诉人甘宇兵、夏平珍、罗志新。

2、被害人赵某的陈述，主要内容为：2014 年 6 月份左右，我在广东金融博览会（琶洲会展中心）上看到了一个叫中大财富网站的金融平台，当时他们宣传说可以接收我们的钱帮我们投资借贷，每年有高于 22.4%的年化收益率，还跟我们说他们的平台是全国首创最大的金融平台，光是商户就上百家，我们的钱是借给平台的商户做资金周转的，收益丰厚。我与他们公司在网上平台签订了很多租赁借款合同，8 月份开始有收益，到了 12 月 25 日左右发现没有收益，就开始怀疑并核查，最终发现我的钱不能提取出来，于是我从 12 月 26 日开始到位于广州市天河区珠江新城富力盈通大厦×室的公司所在地追讨本钱。我把钱投资进的公司是广州市环宇投资有限公司、广东环银投资集团有限责任公司和广州市环宇纺织品市场经营管理有限公司。他们在网上运作的中大财富平台的实际控制人是甘宇兵。我是通过 QQ 聊天的方式与涉案单位一名叫 KETY（谐音）的客服接触的。他们通过在网络用高回报、高奖励的宣传方式来推广和营销。我总共投资 1721365.312 元，现在网上显示余额为 560503.51

元。我不清楚该公司的具体投资行为和运作情况，他们声称将我的投资借贷给他们所管辖的商户，至于他们有无将我的投资真正借贷给商户，或者这些商户是否真实存在我就不得而知。

经辨认照片，赵某辨认出上诉人甘宇兵、夏平珍、罗志新。

3、被害人报案材料，包括《借贷担保合同》、在中大财富网站上的相关信息、银行交易查询资料等，证实被害人在中大财富网站的投资情况。

4、广东创信会计师事务所有限公司出具的创信审字（2015）0034 号之二《专项审计报告》，证实本案 367 名被害人在中大财富平台累计充值金额为人民币 8398.960530 万元，累计提现金额为人民币 3347.702096 万元，累计损失金额为人民币 5051.258434 万元。

5、证人罗某的证言，主要内容为：我是 2014 年 5 月入职广州市环宇投资有限公司的。我主要负责制作财务账册、依照平台后台统计数据，包括统计中大财富 P2P 网络管理平台的充值金额，以及审核贷款招标到期的贷款人提现的利息、奖励，同时也看看这些贷款人的提现是否需要按照规定扣除手续费等，然后把提现总数报老板甘宇兵过目后，由甘宇兵指示公司出纳邓某姗进行转账。公司老板甘宇兵，全面负责公司业务；罗志新是总监，全面负责公司业务；曾某欢是副总监，负责宣传业务；钟某波是技术总监，负责网络技术。财务部有四人，我是会计，邓某姗是出纳，陈某华是数据分析员，还有周某香负责线下充值审核以及续投奖励发放。夏平珍在广州环宇投资有限公司没有具体任职，但邓某姗每次将款打入借款人的账户时都会联系夏平珍向其请示。

中大财富 P2P 网络理财平台主要以 P2P 的形式经营网络借贷，即借款人向我们公司申请借款，然后我们公司在平台上以招标的形式发布其借款信息及利息信息，再由贷款人通过平台看到以上信息后向我公司以“充值”的形式汇款，并且在平台上操作投标，然后我们公司便把贷款人的资金交给相应的借款人，等该标的贷款到期后，借款人把本金、利息及相应的手续费交还公司，公司收取手续费后把利息和本金再汇入贷款人的账户。因为该平台发布借款人信息及借款需求这部分工作我没有接触过，所以我不清楚这些借款人信息及其借款需求是否真实。该平台发布借款标的的流程我也没接触，不清楚情况。

经过辨认照片，罗某辨认出上诉人甘宇兵、夏平珍、罗志新。

6、证人朱某的证言，主要内容为：广州市环宇投资有限公司主要经营中大财富 P2P 网络借贷平台。中大财富 P2P 网络借贷平台是针对全国纺织专业市场的商户为借款人，如果这些商户有借款需求，可以在平台上发布需求进行招标，网络上的注册用户可以对这些招标进行投标，将钱汇入平台账户，然后平台将钱转给这些借款人。借款人按照合同要求向贷款人支付利息。简单来说，该平台就是贷款人和借款人的贷款中介。但该平台的具体经营和管理我都没有参与，具体情况不清楚。公司的实际老板是我岳父甘宇兵，该公司股东甘某 1、李某群及我的股份都是甘宇兵出资的。甘宇兵全面经营该公司，甘某 2、夏某华只是挂个名没有实际参与经营，罗志新是运营总监，全面负责该公司及平台运营，曾某欢也负责管理该公司及平台运营。据我所知夏平珍没有参与该公司实际运营。

经过辨认照片，朱某辨认出被上诉人甘宇兵、夏平珍、罗志新。

7、证人刘某的证言，主要内容为：2013 年 9 月，当时我和郭某锋受甘宇兵委托，以广州律巡网络科技有限公司的名义，帮广州环宇投资有限公司建立了“中大财富 P2P 网贷平台”的软件和网站，完成网站建设后将该平台经营至 2014 年 5 月，便与甘宇兵经营的广州环宇投资有限公司签订合同，把该平台交付广州环宇有限公司使用，甘宇兵前后付出了 250 万元。当时我们为整个平台的运营提供了技术、招聘的服务，而该平台的借贷业务则由广州环宇投资有限公司负责。主要运营模式为：平台为借款客户发布其借款需求信息，然后投资者在该平台看到信息后，将资金汇入平台，平台作为中介把投资款汇给借款客户，到期后借款客户将借款本金及约定利息还至平台，投资者便可从平台取现。平台会收取利息中的一些差额作为盈利。资金上的事由甘宇兵负责，我不清楚“中大财富 P2P 网贷平台”的盈利是如何操作

的。

夏某华是广州环宇投资管理有限公司的法人代表，甘宇兵是该公司实际老板，全面负责该公司业务。夏平珍应该是公司财务，我经常见到她坐在该公司的财务室，但她具体负责什么我不清楚。我跟甘宇兵打交道一直都是由夏平珍帮甘宇兵管钱，该平台交付给广州环宇投资管理有限公司使用后就不清楚了。罗志新是该公司运营总监，由我和郭某锋于2014年2月将其招聘至“中大财富P2P网贷平台”，全面负责该平台的线上运营，该平台交付给广州环宇投资管理有限公司使用后就不清楚了。我们和甘宇兵有过协议，我们经营该平台只负责技术及招聘，客户及资金业务都是由甘宇兵负责，因此对于甘宇兵提供的借款人信息及资金流向都是甘宇兵负责的，甘宇兵说这是他的客户资源，叫我们不要干涉。我们无法对其提供的信息进行核实，因此平台发布的借款人的借款信息以及资金流向的真实性我们不清楚。2015年1月27日，甘宇兵被公安机关抓获，我才从别人那里知道甘宇兵虚构了借款人的信息及借款需求进行诈骗，在此之前我不清楚。

经过辨认照片，刘某辨认出上诉人甘宇兵、夏平珍、罗志新。

8、证人谭某的证言，主要内容为：广州环宇投资有限公司大约在2010年登记成立，老板甘宇兵是实际控制人。我于2014年6月入职该公司任风控总监。我负责线下业务，就是负责审核贷款人资料的真实性，保证将投资人的投资款安全地贷款给需要借款的商户；罗志新负责线上业务，就是招揽投资人到公司的平台上投资，在线上发布贷款商户的资料；夏平珍是公司的财务负责人，发工资的款项是夏平珍负责的，有些支付资金是她负责的，她参与了公司的经营。2014年10月我发现投资人的投资款被老板用了，我没有办法解决，有客户投诉，告诉客户自己打电话给甘宇兵自己解释。罗志新对于老板私用投资人投资款的事情是知情的。据我所知，所有的投资人的投资款被老板私用了，没有落到提供资料的商户手中。2014年11月我自己离职。

经过辨认照片，谭某辨认出上诉人甘宇兵、夏平珍、罗志新。

9、银行账户查询资料，证实夏某华等账户余额很少或者余额为零。

10、中国银行业监督管理委员会广东监管局《关于广州市环宇投资有限公司经营资格认定的复函》，证实：广州市环宇投资有限公司不是经银行业监督管理机构批准设立的银行业金融机构，不具备吸收公众存款的资格。

11、《个人名下房地产登记情况查询证明》，证实上诉人甘宇兵名下无房产登记，上诉人夏平珍名下登记有海珠区荷红径×号×房，目前该房产已被广州市越秀区人民法院、天河区人民法院轮候查封。

12、广州市公安局天河区分局经济犯罪侦查大队民警出具的《抓获经过》，证实2015年1月27日，该大队接群众举报称广州市环宇投资有限公司通过其设立的“中大财富网络理财平台”从事非法集资，该大队于2015年1月27日2时在广州市天河区珠江新城富力盈通大厦×室将甘宇兵、罗志新、夏平珍带回公安机关调查。

13、上诉人甘宇兵、罗志新、夏平珍的户籍材料，证实他们的身份情况。

14、甘宇兵的一审辩护人提交的手机截屏，证实：2015年1月26日夜，甘宇兵和黄某、夏平珍、朱某、罗志新有多次通话，黄某在与甘宇兵的短信中表示：“如果今晚没人到的话恐怕有人要报警，很难控制”。

15、甘宇兵的一审辩护人提交的证人彭某书写的《情况说明》，主要内容为：2015年1月26日晚，我与甘宇兵回到广州后，甘宇兵接到电话说甘宇兵的老婆在公司跟投资人吵起来了，投资人报了警，甘宇兵就去了公司。

16、被告人甘宇兵的供述，主要内容为：因我公司开设P2P平台（即融资平台），吸收了许多投资者的投资款，无法还投资者的利息。我通过伪造虚假的借款人信息向公众集资，大约吸收了1000多人的款项，其中有许多都是投资100多元的小额投资人，投资比较大的

人大约有 100 人，我吸收的投资款总数大约 6000 万元人民币，都是向网上不特定的人吸收的，投资者我大部分不认识。我实际控制的广州市环宇投资有限公司、广州市环宇纺织品经营管理有限公司、广东环银投资集团公司、广州森宇投资有限公司都不具有向公众集资的资质。

广州市环宇投资有限公司于 2010 年登记成立，2014 年 2 月 17 日才开始用中大财富网络管理平台进行集资，P2P 平台就是在互联网上开设一个网络管理平台，在平台（广州市环宇投资有限公司中大财富网络管理平台）向不特定人群发布借款方及放贷方的相关信息，包括借贷双方的基本情况，资金需求情况，借款利息等。通过这个平台促成双方达成借贷协议，在网络管理平台上投资的投资者可以收取年利息约 22%的利息，我公司收取 8%的中介服务费作为我公司的利润。初期中大财富网络管理平台是真实经营的，借款客户是广州市环宇纺织品市场的商户。由于我资金短缺，所以自 2014 年 5 月起，我通过虚构借款人的信息，承诺可以支付年息 22.4%的高利，借助中大财富网络管理平台向投资人集资。我利用租户、员工的信息，虚构了这些租客、员工的借款需求放在该平台作为招标，我再与这些“借款人”达成协议，为他们借款账户办理了委托支付。我让实际投资人将投资款项打进夏某华的私人银行账户（中大财富网上公布了 8 个夏某华的个人银行账户，银行账户的情况我不清楚），财务人员罗某通过网银转到我本人控制、支配的“借款人”的账户支付到我指定的账户中。2014 年 5 月至 2015 年 1 月，我以虚构借款需求的方式以中大财富网络管理平台招募 6000 多万资金。被我用于偿还高利贷及融资平台的开发、运营费用。

中大财富 P2P 网络平台实际控制人应该是我本人，运营总监是罗志新，平时全面负责公司的经营。夏平珍没有参与经营或者任职广州环宇投资有限公司或中大财富 P2P 网络平台。她有时会按照我的指示帮忙操作汇款，但汇款用途她不知情，有时她也帮我记录一些公司经营相关的账户信息，但她对公司的经营不知情。

17、上诉人夏平珍的供述及辨认笔录，供述主要内容为：我丈夫甘宇兵注册了广东环银投资集团有限责任公司，广州环宇投资有限公司和广州森宇物业管理有限公司，广州森宇物业管理有限公司也是环宇纺织品市场，甘宇兵是该三公司的实际控制人，甘宇兵以广州环宇投资有限公司名义经营了中大财富 P2P 网络贷款平台，即我公司设置商户需要贷款的需求投资标，在该平台发布投资标，让投资者投资，交付投资款，我公司再将投资者的投资款进行资本运作。中大财富 P2P 网络贷款平台是甘宇兵负责的，具体是小罗运作；投资者的投资款是依据平台的提示汇入到夏某华的账户的，平台账户是公司财务在管理，财务会将账目的汇总给我看，我也可以在平台看到。汇入平台的账户是甘宇兵支配的。投资款会用于支付投资者的利息，公司日常费用如租金、平台费用等，支付公司员工的提成，其他的钱用于甘宇兵安排。客户投资款是否会用来支付贷款需求我就不清楚，我们家欠了高利贷的钱，甘宇兵用部分客户的投资款还高利贷的欠款，具体多少我不清楚。我是广东环银投资集团有限责任公司的法人代表，是广州环宇投资有限公司的财务总监，我会关注和过问中大财富 P2P 网贷平台上的资金情况，具体财务工作是公司的财务人员在做。

我没有参与广州环宇投资有限公司或中大财富 P2P 网络平台经营或任职。我只是平时帮我丈夫甘宇兵记录一些有关经营的账户信息等，但这些账户是用来做什么事的我不清楚。这些账户信息平时就由我本人保管着。我从来没有以广东环银投资集团有限责任公司法人代表的身份签署过合同或文件，该公司公章及“夏平珍”印鉴都是甘宇兵保管的，我不知道放在何处。该公司的经营状况、有没有担保资质和能力我不清楚。

2016 年 1 月 26 日晚，我去到公司，10 多分钟后警察来了，我就打电话给我老公让他不要来了，他说一人做事一人当，半个钟后就一个人来了。

18、上诉人罗志新的供述，主要内容为：我是 2014 年 5 月 1 日招聘进环宇公司任线上运营总监，负责管理公司客服部、技术部、网络推广部、企划部的工作，具体工作是负责公

司网站的优化、公司业务网上营销、推广、企划，每月工资 15000 元。环宇公司主要做中大财富互联网理财平台，理财产品是“商户贷”，具体是跟三家专业市场管理公司（广州市环宇纺织品市场经营管理公司、武汉金昌隆市场经营管理公司、广州市大时代网络批发城）合作，给市场有资金周转需求的商户做资金中介，通过吸取公司投资人资金转贷给商户获利。环宇公司与客户、商户的三方合同都是网上签订的，由投资人（甲方）在中大财富账户的资金余额作为投资资金、借款商户（乙方）、见证人环宇公司（丙方）、广东环银投资集团有限责任公司与三家专业市场管理公司的一家组成担保联合体（丁方）四家签订合同，年息 20.4%22.4%不等，环宇公司收取利息的 8%手续费作为中介费用。

我在公司主要负责管理公司日常事务，老板不在公司时，我就要全面管理公司日常工作，我决定不了的事情，例如财务、项目等，就要向公司老板甘宇兵和公司总经理甘某 2 请示。甘宇兵是老板，全面负责公司业务。夏平珍没有在公司上班，但她负责每个月向我提供一份风险保证金的截图，由我交代公司人员将该截图上传至中大财富 P2P 网贷平台公示。夏某华是公司法人代表，他很少来上班，但公司有重大活动或者宣传会议他都会出席，另外我们公司很多文件以及宣传文章都由他审核修改，再交由我负责交代公司员工在中大财富 P2P 网贷平台发布。甘某 2 是公司总经理，我来该公司任职时甘某 2 已经在公司上班了，他全面负责公司事务，我有时决定不了的时候我也会向甘某 2 请示，甘某 2 直接听命于甘宇兵。谭某是公司风控总监，负责市场调研以及审核借款人、贷款人的接待情况，具体情况不清楚。

中大财富 P2P 网贷平台发布的借款人的借款需求是否真实我不清楚。借款人及其借款需求是由谭某负责审核的，他审核完会将报告交给我，由我负责在网站上发布借款招标。然后公司每一笔贷款也会将汇给借款人的银行凭证公布在网站上。因此，就没有再深究以上信息的真实性了。中大财富 P2P 网贷平台与贷款人的合同是系统生成的，至于借款人的合同我不负责审核，我不清楚合同的真实性。因为我不管财务工作，因此我不清楚公司是否存在将募集的贷款不交给借款人而用于公司自身经营的情况。我看到公司会将每一笔贷款汇给借款人的银行凭证公布在网站上，因此我认为该贷款是真正交到借款人处。但借款人如何使用资金我就不清楚了，甘宇兵也没有向我透露。

对于上诉人甘宇兵的上诉理由及其辩护人所提辩护意见，经查：

（1）上诉人甘宇兵明知自己不具备向社会公众募集资金的资格，利用开设“中大财富 P2P 网络理财平台”的方式为掩护，以高利息、高回报吸引投资者通过理财平台向“借款人”投资，而自己通过利用控制平台运转的便利条件，利用掌握市场租户、公司员工资料的便利而借用其名义、虚构借款用途，通过操控“借款人”账户将投资者投入的资金转到自己控制的账户，供自己使用，其行为属于采用诈骗手段非法募集资金。

（2）上诉人甘宇兵运营 P2P 平台是为了在资金链断裂、资金无法周转的情况下非法筹集公众资金以归还此前因为支付高息而造成的巨额债务，实际上还需支付投资人的高额利息以及维持平台运转，完全不是用于与投资人所约定的用途，且不存在产生增值以归还投资人的可能性，其辩解所声称的纺织品市场盈利并没有因此而实现，最终造成所募集资金巨额亏空的后果，对此其显然有清醒的认识。故原判认定其主观上有非法占有的故意是正确的。

（3）原判认定各被害人的损失数额以及全案所造成投资人的损失情况，依据的是审计机构根据环宇公司与投资人签订的合同、投资人充值、提取的银行流水等材料所作的审计结论，甘宇兵上诉对此提出质疑没有依据。

（4）虽然上诉人甘宇兵有自首情节，但其集资诈骗数额特别巨大，造成投资人的巨额损失，原判对其处以有期徒刑十五年已经体现了从轻处罚，辩护人提出“法定最高刑只适用于加重情节”等理由没有法律依据，不予采纳。

对于上诉人夏平珍的上诉理由，经查：

（1）本案中“中大财富 P2P 网络理财平台”的运作与上诉人甘宇兵通过控制“借款人”

并利用平台获得投资人资金的行为是分别进行的，即平台只是一个掩护，甘宇兵在背后操纵账户和资金才是其实施集资诈骗的关键，因此上诉人夏平珍是否构成犯罪，与其在环宇公司或者“中大财富 P2P 网络理财平台”担任什么职务无关，关键是其参与了非法募集资金的行为。

（2）上诉人甘宇兵、夏平珍的在供述中均承认夏平珍协助甘宇兵管理公司账户等工作，而夏平珍亦知道甘宇兵欠下巨额高息债务，存在用投资人资金归还自己所欠债务的情况；这与证人谭某、罗某以及上诉人罗志新各自从自己所了解的角度指认夏平珍具体参与了与平台相关的财务管理的陈述能够相互印证。

（3）本案中甘宇兵集资诈骗的关键环节在于操纵“借款人”账户自己使用资金，操纵账户、使用资金独立于平台的运营，主要由自己及亲属参与，夏平珍基于与甘宇兵夫妻关系协助管理财务所起的作用，与作为雇员的上诉人罗志新所负责的运营网络平台所起的作用，显然是有区别的，原判在认定他们同为从犯但所起作用有区别的基础上在量刑方面相应体现差别是合适的。

对于上诉人罗志新的上诉理由，经查：

（1）现有证据足以证实，上诉人甘宇兵控制下的“中大财富 P2P 网络理财平台”实际上并没有成为在用款人和投资人之间起搭桥作用的中介平台，在甘宇兵操控了“借款人”后已经成为其自己吸收投资人资金的途径，“平台”成为掩盖真相、欺骗投资人的骗局，一审对此的认定没有不当。

（2）甘宇兵设立“中大财富 P2P 网络理财平台”之初是否为了犯罪对其后续行为并没有影响，相反按照其陈述的初衷设立平台是为了解决资金困局，而单纯依靠收取一定比例的中介费对于其巨大的债务负担而言显然杯水车薪，走向变相吸收公众存款是必然的。

（3）鼓励金融创新与惩处金融诈骗犯罪并不矛盾，从事互联网金融活动必须得到监管部门的批准、符合国家的相关规定，而无论是环宇公司还是“中大财富 P2P 网络理财平台”都未经银行业监督管理机构批准，不具备吸收公众存款的资格。

（4）上诉人罗志新受雇负责管理维护推广“中大财富 P2P 网络理财平台”，客观上为甘宇兵的集资诈骗活动起了帮助作用，正因为其对甘宇兵骗取款项不知情，主观方面与甘宇兵不同，故原判认定其属于非法吸收公众存款的从犯予以减轻处罚体现了罚当其罪。

（5）罗志新在被投资人围堵在办公场所并报案、公安人员到场后带回公安机关处理，其到案缺乏主动性，不属于自动投案，不构成自首。

综上，上诉理由及辩护意见经查均不能成立，不予采纳。

本院认为，上诉人甘宇兵以非法占有为目的，使用诈骗手段非法集资，数额特别巨大，其行为已构成集资诈骗罪。上诉人夏平珍、罗志新参与变相吸收公众存款，扰乱金融秩序，数额巨大，其行为均已构成非法吸收公众存款罪。甘宇兵在犯罪以后自动投案，如实供述自己的罪行，是自首，依法可予从轻处罚。上诉人夏平珍、罗志新在共同犯罪中起次要作用，是从犯，依法可予从轻或者减轻处罚。上诉人甘宇兵、夏平珍、罗志新的上诉理由以及甘宇兵的辩护人所提辩护意见经查不能成立，不予采纳。原审判决认定的事实清楚，证据确实、充分，适用法律准确，量刑适当，审判程序合法。依照《中华人民共和国刑法》第一百九十二条、第一百七十六条第一款、第二十七条、第六十四条、第六十七条第一款、《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》第三条第二款、第三款、第五条第一款、第三款、《中华人民共和国刑事诉讼法》第二百二十五条第一款第一项之规定，裁定如下：

驳回上诉，维持原判。

本裁定为终审裁定。

审判长　　吴铭泽

审判员　　文建平
审判员　　陈亦光
二〇二〇一七年三月九日
书记员　　林俊达

案例三、林双宝、林振建、洪东健非法吸收公众存款罪一审刑事判决书

浙江省泰顺县人民法院

刑 事 判 决 书

（2020）浙0329刑初136号

公诉机关浙江省泰顺县人民检察院。

被告人林双宝，男，1986年5月17日出生，汉族，大专文化，中共党员，经商，住浙江省泰顺县，因本案于2019年11月13日被泰顺县公安局刑事拘留，同年12月20日被逮捕。现羁押在泰顺县看守所。

辩护人郑志锦，浙江京衡律师事务所律师。

辩护人林晓辉，浙江泰辉律师事务所律师。

被告人林振建，男，1990年7月17日出生，汉族，初中文化，无职业，住浙江省苍南县，因本案于2020年1月9日被泰顺县公安局刑事拘留，同年2月14日被逮捕。现羁押在泰顺县看守所。

辩护人沈海燕，浙江欧扬律师事务所律师。

被告人洪东健，男，1992年5月17日出生，汉族，大专文化，经商，住浙江省泰顺县，因本案于2020年1月14日被泰顺县公安局刑事拘留，同年2月14日被逮捕，经泰顺县人民检察院决定于2020年8月14日取保候审。

辩护人钱招脉，浙江招脉律师事务所律师。

泰顺县人民检察院以泰检公诉刑诉〔2020〕895号起诉书指控被告人林双宝、林振建、洪东健犯非法吸收公众存款罪向本院提起公诉。本院于2020年8月20日受理后，适用普通程序依法组成合议庭，公开开庭审理了本案。泰顺县人民检察院指派检察员钱益奉华出庭支持公诉，被告人林双宝、林振建、洪东健、辩护人郑志锦、林晓辉、沈海燕、钱招脉到庭参加诉讼。现已审理终结。

公诉机关指控：

一、“通证银行”项目

2019年，高鹏（另案处理）等人利用境外服务器设立“通证银行”投资平台，对外宣称可存储主流“虚拟货币”理财，承诺随存随取，不设锁仓，以日息千分之一至千分之八的高额回报等静态收益模式向公众吸收比特币、以太坊等虚拟货币，并以“拉人头”收取返利的动态收益模式予以传销式推广，诱使他人将持有的虚拟货币存入“通证银行”平台。同年6月，该平台虚拟货币无法提取。同年7月，该平台将储户的主流货币强制转化成TB资产。此后，该平台关闭，无法登陆。经链上资产追踪调查分析发现，该平台通过上述方式吸收的虚拟货币价值人民币10067.4095万元。

2019年2月至3月，被告人林双宝、顾**（另案处理）等人获悉“通证银行”项目，前往马来西亚考察，参加由高*等人组织的宣讲会、签约仪式。回国后，林双宝伙同顾**、胡***、罗**（均另案处理）等人，以“通证银行”平台为依托，以投资该平台可持币生息、推荐投资人可获得返利等高额回报为诱饵，分别在杭州、宁波、温州、泰顺等地召开推介会、宣讲会等方式进行宣传、分享投资理财经验，并通过微信推广，鼓励社会公众将虚拟货币存入“通证银行”。根据目前报案人员统计，经林双宝、顾**等人宣传，共吸收毛某、张某2、

钟某等59人虚拟货币价值达人民币1500万元以上。期间，被告人林振建提供账号供林双宝从事“通证银行”推广使用，负责费用开支、报销、数字货币处置等；被告人洪东健帮助林双宝开展宣传，积极与投资人分享经验、讲解操作流程、帮助他人操作平台等，为通证银行吸纳投资人。经链上资产追踪调查分析发现，价值人民币673.659万元的虚拟货币充值到林振建的钱包地址中。

二、DGU、BAC项目

2017年至2018年期间，被告人林双宝经他人介绍参与ＤＧＵ、ＢＡＣ项目，未经有关部门依法批准，在温州地区以帮助他人投资理财为由，通过“口口相传”的方式向他人介绍ＤＧＵ、ＢＡＣ项目，以高额回报为诱饵，诱使王某3、金某3、何某1、齐**等十余人投入资金合计约人民币500万元。林双宝将上述投资款转交给上线公司。

2019年11月13日，被告人林双宝主动到泰顺县公安局投案；2020年1月9日，被告人林振建主动到泰顺县公安局投案；同年1月14日，被告人洪东健主动到泰顺县公安局投案。

本院经审理查明的案件事实与公诉机关指控的事实相一致。另查明：公安机关已冻结林振建购买国泰基金管理有限公司的基金份额20.78份；已冻结以王某5（330329198205200033，ｕｉｄ:1208691）名义在Ｇａｔｅ.ｉｏ购买的301.306ＥＴＨ，资金均来源于林双宝从通证银行平台变现转换而来；已查封的罗阳镇*******幢**室房屋，于2015年4月14日进行不动产登记，权利人为林双宝、陶某某。2019年5月28日，陶某某用林双宝从通证银行平台变现转换而来的款项为该房屋解除了抵押负担，提前结清住房公积金贷款220393.47元。在案的认罪认罚具结书是被告人林双宝、林振建、洪东健在律师在场见证的情况下自愿签署，各被告人对指控事实、罪名及量刑建议没有异议并认罪认罚。

上述事实，被告人林双宝、林振建、洪东健在开庭审理过程中亦无异议，并有公诉机关举证经庭审质证的调取证据通知书、杭州湾大酒店宾客住宿登记、房费报表、宾客账单、红巨大厦办公楼租赁合同、营业执照、消费记录、宴会定金收据、台州卡奇诺旅店账单、台州市椒江大酒店住宿及消费记录、泰顺中益假日酒店住宿及消费记录、嘉运国际大酒店消费资料、出入境记录、银行交易明细、温州市住房公积金管理中心材料、泰顺县联众汽车销售有限公司材料、税收缴款书、机动车登记材料、中华人民共和国机动车行驶证、交易记录、机动车信息查询结果单、不动产登记信息查询记录、温州立人教育集团有限公司处置工作领导小组投资材料、扣押决定书、扣押笔录、协助冻结财产通知书、查封决定书、查封清单、协助查封通知书、上海市公安局嘉定分局关于ＢＡＣ项目的相关材料、前科情况核查记录表、户籍信息等；温州经侦案件分析报告（杭州派盾信安科技有限公司提供）、河北中经天平司法鉴定中心司法鉴定意见书、司法鉴定意见补正书、鉴定意见通知书；视频、火币网、中币网、支付宝、微信交易记录等视听资料与电子数据；电子数据检查笔录、提取电子数据清单、辨认笔录；被害人姜某、赖某、吉某、金某1、李某、陈某1、叶某1、钟某、谭某、杨某、叶某2、林某1、赵某、戴某、蒋某、张某1、陈某2、周某1、陈某3、林某2、吴某1、王某1、吴某2、周某2、王某2、刘某1、谢某、唐某1、周某3、徐某1、刘某2、郑某1、董某1、陈某4、钱某、齐某、毛某、苏某、罗某1、罗某2、翁某、叶某3、尹某、曾某、程某、潘某、骆某、袁某、庄某、刘某3、徐某2、张某2、林某3、沈某、朱某、金某2、王某3、金某3、周某4、詹某、胡某、陈某5、黄某、陈某6、金某4、王某4、何某1、邹某、陈某7、周某5、何某2、董某2虽等人的陈述；证人陶某1、陶某2、唐某2、陶某3、郑某2、王某5、陶某4等人的证言；归案经过、情况说明、认罪认罚从宽制度告知书、认罪认罚具结书等；被告人林双宝、林振建、洪东健的供述和辩解等证据予以证实，足以认定。

本院认为，被告人林双宝、林振建、洪东健未经有关部门依法批准，以投资虚拟货币为名，以高额回报为诱饵向社会公众吸收资金，扰乱金融秩序，数额巨大。其行为已构成非法

吸收公众存款罪。公诉机关指控罪名成立。林双宝、林振建、洪东健犯罪以后自动投案，如实供述自己的罪行，系自首，依法可以从轻处罚。林振建、洪东健在共同犯罪中起次要或者辅助作用，系从犯，依法应当分别从轻、减轻处罚。林双宝、林振建、洪东健自愿认罪认罚，依法可以从宽处理。洪东健经审前调查适于实行社区矫正，可予适用缓刑。*******幢***室房屋系林双宝在本案犯罪之前的合法财产，但提前偿还该房屋住房公积金贷款的数额来自于本案违法所得，依法应予追缴；同样，已冻结的林振建在国泰基金管理有限公司的基金份额、以王某5名义购买的虚拟币以太坊均来自于本案违法所得，也应当予以追缴。根据被告人林双宝、林振建、洪东健各自的犯罪事实、性质、情节和对社会的危害程度，依照《中华人民共和国刑法》第一百七十六条第一款、第二十五条第一款、第二十七条、第六十七条第一款、第七十二条第一款和第三款、第七十三条第二款和第三款、第六十四条，《中华人民共和国刑事诉讼法》第十五条之规定，判决如下：

一、被告人林双宝犯非法吸收公众存款罪，判处有期徒刑五年六个月，并处罚金15万元（限于判决生效之日起十日内缴纳）。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2019年11月13日起至2025年5月12日止。）

二、被告人林振建犯非法吸收公众存款罪，判处有期徒刑三年，并处罚金5万元（限于判决生效之日起十日内缴纳）。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2020年1月9日起至2023年1月8日止。）

三、被告人洪东健犯非法吸收公众存款罪，判处有期徒刑二年，缓刑三年，并处罚金2万元（限于判决生效之日起十日内缴纳）。

（缓刑考验期限从判决确定之日起计算。缓刑考验期间，应接受社区矫正，服从社区矫正机构的监督管理。）

四、冻结的林振建在国泰基金管理有限公司的基金20.78份和以王某5（330329198205200033，ｕｉｄ:1208691）名义在Ｇａｔｅ.ｉｏ购买的301.306ＥＴＨ，予以追缴，上缴国库。

六、追缴林双宝用以提前偿还住房公积金贷款的相应数额220393.47元（实际缴交到位后，*******幢**室房屋应予解除查封），上缴国库。继续追缴其违法所得。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向浙江省温州市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份、副本二份。

审　判　长：季龙斌

人民陪审员：林太伟

人民陪审员：周　倩

二〇二〇年十一月十二日

书　记　员：王　炜

（二）集资诈骗罪

案例一、陈文华集资诈骗

陈文华集资诈骗一审刑事判决书

广东省广州市中级人民法院

刑事判决书

(2018)粤01刑初189号

公诉机关广东省广州市人民检察院。

被告人陈文华。2003 年 4 月 7 日因犯盗窃罪被湖南省攸县人民法院判处有期徒刑九年，服刑期间经减刑，于 2009 年 5 月 16 日刑满释放。因本案于 2017 年 5 月 30 日被刑事拘留，2017 年 7 月 4 日被逮捕，现羁押于广州市天河区看守所。

辩护人谢新民，广东德纳律师事务所律师。

广州市人民检察院以穗检公二刑诉〔2018〕79 号起诉书指控被告人陈文华犯集资诈骗罪，于 2018 年 4 月 13 日向本院提起公诉。本院依法组成合议庭，公开开庭审理了本案。广州市人民检察院指派检察员董李培出庭支持公诉，被告人陈文华及其辩护人谢新民到庭参加诉讼。本案现已审理终结。

广州市人民检察院指控：广州市宏量资产管理有限公司（以下简称“宏量公司"）注册成立于 2015 年 8 月 6 日，被告人陈文华任法定代表人、总经理。被告人陈文华及同案人在明知宏量公司不具备吸收公众存款资格的情况下，注册“宏量财富"网站（网址：××），于 2015 年 9 月起运营宏量财富 P2P 网络借贷平台，以 16%的高年息、奖励返点、采用第三方资金托管保障资金安全为诱饵，在上述网贷平台发布借款标的，诱骗社会不特定对象通过乾某网贷自主清算系统（以下简称“乾某系统"）向该网站充值投资。被告人陈文华及同案人将被害人通过乾某系统投资出借的款项转入宏量公司在乾某系统的账户，再经由被告人陈文华等人的乾某系统账户提现至被告人陈文华等人个人银行账户。2015 年 11 月 23 日，“宏量财富"网站突然关闭，被告人陈文华潜逃。经统计，被告人陈文华及同案人通过宏量公司共收取投资款共计人民币 27072463.1 元，骗取已报案 224 名被害人投资款人民币 9313695.3 元，造成被害人损失共计人民币 8708612.55 元。2017 年 5 月 30 日，被告人陈文华在本市广州南站被抓获。

为证实指控内容，公诉机关向本院提交了相关书证、被害人陈述、证人证言、司法鉴定意见等证据，并据此认为，被告人陈文华以非法占有为目的，使用诈骗方法非法集资，数额特别巨大，其行为触犯了《中华人民共和国刑法》第一百九十二条，犯罪事实清楚，证据确实、充分，应当以集资诈骗罪追究其刑事责任。提请本院依法判处。

自辩及辩护意见如下。

侦查阶段陈文华辩称：其没有租用过广州天河华明路 9 号 711 房，没有使用过自己的身份证去注册公司，不知道广州市宏量资产管理有限公司的存在，没有在上述公司的办公地点照过相。2015 年，一个其坐牢时认识的牢友拿其（陈文华）身份证去银行办了一张银行卡，给了其（陈文华）两万元钱好处费，但没有把身份证还给其。

庭审中陈文华辩称：其没有实施公诉机关指控的犯罪行为，是有人拿其的身份证办了银行卡，并雇佣其去取过钱，公司设立时的签名不是其签的。拿其身份证办银行卡是其牢友联系的，后有老板叫其去过宏量公司三次，其在公司里拍了照，其无法提供对方的真实姓名和联系方式。

辩护人提出的辩护意见是：

1.对公诉机关指控陈文华构成集资诈骗罪的罪名没有异议，但陈文华在本案集资诈骗的共同犯罪中仅起帮助辅助作用，应认定为从犯。陈文华仅是在本案中借用了身份证给他人开设银行卡以及注册了公司，在借用身份证过程中收取了 2 万元酬金。

2.公诉方所指控的诈骗金额与事实不符。

3.陈文华存在如下从轻处罚情节。是从犯，应当从轻、减轻处罚或免除处罚；陈文华文化程度为文盲，法律意识淡薄，未充分认识借用身份证的法律危险，主观恶性不大；陈文华在整个集资诈骗中获利仅为 2 万元，没有明显的犯罪动机；报案人损失金额与同类型集资诈骗金额比较，所造成的社会影响及危害相对较小。

经审理查明：广州市宏量资产管理有限公司（以下简称“宏量公司"）于 2015 年 8 月 6

日在广州市注册成立，被告人陈文华任法定代表人、总经理。之后陈文华及同案人注册“宏量财富"网站，于 2015 年 9 月起运营宏量财富 P2P 网络借贷平台，以 16%的高年息、奖励返点、采用第三方资金托管保障资金安全为诱饵，在上述网贷平台发布借款标的，诱骗社会不特定对象通过乾某网贷自主清算系统（以下简称“乾某系统"）向该网站充值投资。陈文华及同案人将被害人通过乾某系统投资出借的款项转入宏量公司在乾某系统的账户，再经由陈文华等人的乾某系统账户提现至陈文华等人个人银行账户。2015 年 11 月 23 日，“宏量财富"网站突然关闭，陈文华潜逃。经统计，陈文华及同案人通过宏量公司共收取投资款人民币 2707.24631 万元（以下均为人民币），骗取已报案 224 名被害人投资款 931.36953 万元，造成被害人损失共计 870.861255 万元。2017 年 5 月 30 日，陈文华被抓获归案。

上述事实，有公诉机关提交并经法庭出示、质证后的如下证据证实：

1.证明宏量公司集资诈骗及陈文华参与的书证

1.1 宏量公司工商登记信息，主要内容为：该公司于 2015 年 8 月 6 日申请设立登记，申请人及有权签署人签字处签名均为“陈文华"，申请材料中有陈文华身份证复印件。登记设立的委托代理人是翁某，公司执行董事兼总经理为陈文华，公司监事何洋。

1.2 宏量公司办公地点租赁文件，广州银华物业管理有限公司客户服务部 2015 年 11 月 24 日出具的证明，证实：天河区华明路 9 号华普广场西塔 711 单元租户陈文华于 2015 年 7 月 29 日在华普广场管理处办理了迁入手续，2015 年 11 月 23 日起，该单元已无人办公，一直处于关闭状态。

银华物业公司提供的广州市房屋租赁合同复印件、宏量公司营业执照、陈文华身份证复印件（身份证有效期为 2009 年 5 月 18 日到 2029 年 5 月 18 日），合同出租人为高某，承租人为陈文华，承租天河区华明路一街 9 号 711 房号房地产做办公使用。合同上有“陈文华"签名。合同签署日期为 2015 年 7 月 27 日。

经侦查人员记录，上述资料给陈文华辨认，陈文华称其不清楚该租赁合同，并称其没有在广州租过任何办公场所。

1.3 陈文华招商银行账户（尾号 7517）开户资料。陈文华招商银行账户开户于 2015 年 7 月 29 日，开户资料显示教育程度为大学本科，有开户时人像采集照片，开户申请书上有陈文华签名。侦查人员记录，上述资料给陈文华辨认，陈文华称身份信息是其本人，下面的视频截图不是他本人，签名也不是他本人签的。审查起诉阶段公诉人提审时陈文华表示照片是其本人。证实：陈文华本人于 2015 年 7 月 29 日在招商银行开立了个人账户，预留地址为宏量公司注册地址。

1.4 陈文华建设银行开户资料，其中军民身份证联网核查信息结果为公民身份证号码与姓名核对一致，照片核对无误，证实：陈文华本人于 2015 年 7 月 29 日在建设银行开立个人账户，预留地址为宏量公司注册地址。

1.5 陈文华兴业银行开户资料，其中联网核查结果为公民身份证号码与姓名一致，且存在照片，证实：陈文华本人于 2015 年 7 月 29 日在兴业银行开立个人账户，预留地址为宏量公司注册地址。

1.6 中国银行业监督管理委员会广东监管局办公室 2015 年 11 月 27 日出具的《关于广州市宏量资产管理有限公司经营资格认定的复函》，证实：广州市宏量资产管理有限公司不是经银行业监督管理机构批准设立的银行业金融机构，不具备吸收公众存款的资格。

1.7 宏量财富工作人员合照，经侦查人员记录，该照片给陈文华辨认，陈文华称该相片中的人均不认识，其本人也不在里面。

证人廖某签认，照片中左 3 男子就是广州市宏量资产管理有限公司法人代表兼老板陈文华，右 4 女子是其本人。

证人李某 1 签认，照片中左数第三位男子是宏量公司老板及法人代表陈文华，右二是其

本人。

证人罗某 1 签认，照片中左数第三位男子是宏量公司老板及法人代表陈文华。

1.82 名男子在办公室中的会谈照片

证人廖某签认，照片中右边男子就是广州市宏量资产管理有限公司法人代表兼老板陈文华。

证人李某 1 签认，照片中右边男子就是广州市宏量资产管理有限公司法人代表兼老板陈文华。

证人罗某 1 签认，照片中右边男子就是广州市宏量资产管理有限公司法人代表兼老板陈文华。

1.9 陈文华于涉案期间在广州的住宿、交通记录，主要内容为：2015-9-422:49 至 2015-9-504:30，登记入住广东大浪淘沙酒店有限公司珠江新城分公司

2015-10-921:00，登记入住维也纳酒店松南店

2015-10-2823:25 至 2015-10-3016:14，登记入住广州市哈尔滨冰花酒店

2015-3-6 乘坐 G1018 从深圳北到衡阳东

证实陈文华在 2015 年 9 月至 2015 年 10 月期间多次登记入住广州的酒店。

1.10 陈文华身份证补办信息，证实：陈文华于 2015 年 8 月 5 日在攸县公安局谭桥派出所菜花坪服务处以证件丢失为由补领身份证。

2.证明资金去向的书证及电子证据

2.1 双乾网络支付有限公司提供的电子数据及侦查机关出具的《双乾网络支付有限公司调取证据情况说明》，

（1）侦查机关出具的《双乾网络支付有限公司调取证据情况说明》主要内容为：苏州双乾支付有限公司共提供两份光盘文件，分别为“广州宏量财富资产管理有限公司交易明细"（1 号盘），“广州宏量财富资产管理有限公司补正材料"（2 号盘）。①1 号盘中“广州市宏量财富资产管理有限公司网贷转账记录"文件可以看出，投资人的投资款直接通过乾某支付平台汇入借款人的乾某支付平台账号。而借款人的乾某支付平台账号并未进行提现，而是通过二次分配的功能直接转入广州市宏量财富资产管理有限公司的乾某支付平台账户。②2 号盘中“单笔余额变动记录表-688886-自有资金账户及转账记录"文件可以看出，广州市宏量财富资产管理有限公司的乾某支付平台账号向刘华、陈文华、李永毕的乾某支付账号进行转账，金额达 19790570 元。③1 号盘中“提现信息记录-陈文华"文件及“提现信息记录-李某 2"文件可以看出，陈文华从其本人乾某支付账号中提现 10762299 元，李某 2 从其本人乾某支付账号中提现 8977960 元。

（2）双乾公司提供的宏量财富交易数据光盘 1 张。

（3）乾某网贷自主清算系统合作协议复印件。由甲方宏量公司与乙方双乾网络支付有限公司于 2015 年 8 月 13 日签订。宏量公司法定代表人签名为“陈文华"。约定甲方作为为网贷投资人和借款人提供供求信息的合法的网贷平台，由双乾网络支付有限公司为网贷平台提供乾某网贷自主清算系统。

2.2 双乾网络支付有限公司 2018 年 3 月 13 日出具的说明函，证实：该公司与宏量公司签订的合作协议系异地签署，并未与宏量公司人员直接见面。

2.3 陈文华招商银行账户（尾号 7517）交易流水，证实：最后交易日为 2015 年 11 月 23 日，当日 19:27 跨行 ATM 取款 1000 元。该账户自开户至 2015 年 9 月 10 日前，收入多为现金存款，支出包括向双乾网络支付有限公司付款。9 月 10 日后收入大多来自双乾公司，支出有 ATM 取现、转账至陈文华尾号 1454 的账户及其他个人名下账户。该账户合计收入 879.9886 万元，支出 881.548935 万元。

2.4 陈文华兴业银行账户交易流水，证实该账户开户日期 2015-7-29，最后交易日

2015-12-21。

2.5 陈文华建设银行账户交易流水，证实：该账户开户日期 2015-7-29，最后交易日 2015-11-4.账户支出多通过取现、ATM 取款或网络 ATM 取款。流水可体现出取现网点有***区广从公路 6 号首层，广州沙太支行等。

2.6 李某 2 农业银行账户交易流水，证实：开卡日期 2015-10-26，最后交易日 2015-11-19，转账支出全部转至朱志勇账户。

3.证人证言

3.1 证人廖某（宏量公司财务）的证言，主要内容为：其 2015 年 9 月 1 日入职广州市宏量资产管理有限公司，任公司财务，该公司主要经营宏量财富 P2P 网络借贷平台。宏量财富 P2P 网络借贷平台于 2015 年 9 月 6 日上线。宏量公司的法人代表陈文华全面管理公司业务。总经理吴某全面管理公司业务，如果陈文华不在公司的时候，有工作上的事都请示他。运营总监刘某 1 全面管理宏量财富 P2P 网络借贷平台的运营。有一次陈文华让其（廖某）操作公司账户向陈文华个人账户转账，陈文华的个人银行账户是尾号 7517 的招商银行账户。

3.2 证人陈某 2 贤（宏量公司运营经理）的证言，主要内容为：其负责宏量公司网站系统优化以及在其他线上网站对宏量财富 P2P 网络借贷平台进行宣传推广，2015 年 10 月 8 日入职，11 月 23 日离开公司。宏量公司靠项目利差及居间服务费盈利。其入职时，公司法人代表陈文华、总经理吴某及运营总监刘某 1 向其表示，公司现在还不盈利，不赚取利差，先将平台成交量和注册人数做大，然后吸引风险投资从而实现盈利。2015 年 11 月 23 日早上 7 点左右，其 QQ 被从“宏量财富投资交流群"踢出，“宏量财富公司工作群"也被解散，有同事表示宏量财富 P2P 网络借贷平台的网页关闭了。其打电话给陈文华、吴某和刘某 1 等高管，对方均关机。公司技术人员知情后登陆平台服务器，发现密码被更改，也无法登陆了。广州市宏量资产管理有限公司法人代表为陈文华，全面管理公司业务；总经理吴某，全面管理公司业务，如果陈文华不在公司的时候，工作上的事都请示吴某；运营总监刘某 1，全面管理宏量财富 P2P 网络借贷平台的运营业务。

3.3 证人李某 1（宏量公司客服）的证言，主要内容为：其 2015 年 9 月入职宏量资产管理公司任客服。上班时候见过宏量公司的法人代表兼老总陈文华。第一次在 2015 年 9 月，拍照了陈某 3 及公司当时的在职人员，照片放在当时官网；第二次是 10 月，陈文华在陈文华的办公室说员工工作比较辛苦，买水果给员工；第三次也是在办公室，他说最近公司运营较好，表扬员工。合影的照片可以提供给公安机关。

3.4 证人罗某 1（宏量公司客服）的证言，主要内容为：其 2015 年下半年入职宏量公司做客服工作。在公司见过法人代表陈文华。当时公司客服主管叫其到总经理办公室内向其介绍了陈文华。其对陈某 3 很有印象。其见到陈文华到公司就一直呆在公司总经理的办公室内。

3.5 证人陈某 1（陈文华兄）的证言，主要内容为：2015 年 6 月份其父亲生病，其自己回来照顾父亲，陈文华就去广州打工，大概做了几个月陈文华就回老家来了。陈文华回来后没几天就去湖北，直到 2016 年春节前回来过春节，春节过后陈文华带了十几万跟朋友去广州做了一个月超市，亏本了，后来把超市卖了几万块就回来老家，一起帮忙照顾父亲直到 2017 年 5 月 14 日过世，等做完 10 天法事，2017 年 5 月 26 日陈文华就过去广州直到 2017 年 5 月 30 日被广州公安机关拘留。2015 年 6 月份父亲生病期间，其和陈文华有通电话，只知道陈文华那段时间在广州，但是做什么生意不清楚。2015 年下半年是其一个人在照顾父亲，陈文华是 2016 年年底才过来帮忙照顾的。

3.6 证人颜某（双乾公司事业一部负责人）的证言，主要内容为：宏量公司与双乾公司签订合作协议不需要见面，通过 QQ、电话联系，网络交流。陈文华是宏量公司负责人，2015 年 8 月通过双乾公司官网电话联系其（颜某），QQ 和电话交流后，其（颜某）将合同电子版通过 QQ 发送陈文华，修改核对确认合同后，双乾公司将纸质版合同打印出来盖好公章寄

给陈文华，陈文华签名并加盖公章后连同身份资料及公司相关证件寄回双乾公司。未见过陈文华。双方合作后，陈文华只是 2015 年 9 月 6 日至 2015 年 11 月 22 日在双乾公司有业务。

4.辨认笔录

4.1 廖某辨认笔录，廖某辨认出被告人陈文华就是宏量公司法人代表兼老板陈文华。

4.2 陈某 2 贤辨认笔录，陈某 2 贤辨认出被告人陈文华就是宏量公司法人代表兼老板陈文华，并辨认出刘某 1（该人真名为刘某 1，尚未归案），辨认出吴某（该人真名为李某 2，尚未归案）。

4.3 李某 1 辨认笔录，李某 1 辨认出被告人陈文华就是宏量公司老总陈文华。

4.4 罗某 1 辨认笔录，罗某 1 辨认出被告人陈文华就是宏量公司法人代表兼总经理陈文华。

5.被害人报案材料

5.1 被害人黄某的报案材料，受案登记表、立案决定书、黄某陈述、报案情况说明、平台投资记录截屏、银行账号等，共同证实黄某的报案和投资情况，其陈述主要内容为：2015 年 10 月通过 Q 群上广告得知“宏量财富"P2P 投资平台，在该网络借贷网站投资可获得高额利息回报。其登陆宏量财富网站，该公司公布的借款人的投资标的利息均为 16%左右，还有一些奖励返点。其 10 月 23 日开始通过向乾某第三方支付平台充值，获得宏量财富网站投资余额，可以用该余额向宏量财富网站公布的借款人进行 P2P 投资，乾某第三方平台会将投资款直接汇入借款人账户。且该公司对借款标的均承诺保本保息。网站上会公布借款人信息，包括身份证、抵押的机动车或房产的手续等，但均经过处理，无法看到详细信息。其通过个人工商银行尾号 4117 账户共充值 9 万元，并获奖励汇款 9000 元左右。均未提现。

5.2 被害人王某某的报案材料，受案登记表、王某某陈述、报案情况说明、平台借款协议书、平台投资记录截屏、银行流水等，共同证实王某某的报案和投资情况，其陈述主要内容为：2015 年 10 月在 QQ 聊天时，一个陌生人向其介绍“宏量财富"这个类似 P2P 的理财产品，“宏量财富"许诺 16%年化收益率。从 10 月 23 日起以本人、老婆刘某 2 的名义注册，并充值 7 次共计 296992 元，拿回 37219.2 元（转账 10219.2，支付宝返 27000 元），损失 259772.8 元。通过王某某尾号 4317 兴业银行账户充值。提现到工行 1784 账户。介绍其投资的人不完整的支付宝号是“180××××3033"，支付宝“春华"。对方就是在 QQ 里向其介绍这个“广州市宏量资产管理有限公司"有 2000 万元的实缴资金，有风险准备金 500 万元，有其他公司担保等，钱是投资给外面的融资方的。

5.3 被害人叶某的报案材料，受案登记表、叶某陈述、李某 3 报案书、宏量公司 2015 年验资报告、网银交易截图、平台投资记录截屏、平台借款协议书、李某 3 招商银行账户流水，双乾公司招商银行收款账号部分流水，共同证实叶某的报案和投资情况，其陈述主要内容为：2015 年 10 月 24 日在网上发现宏量公司，与业务员联系后，用其老婆李某 3 的名义注册会员。宏量财富公司位于广州天河区华明路 9 号 711，实缴注册资本为 2000 万元，是一个 P2P 平台，而且这个平台上面宣称的借款都是以借款人的房产作为抵押的。法定代表人为陈文华，总经理吴某、运营总监刘某 1。其当时看了宏量财富的介绍，发现这家公司的注册资本都是缴全的，而且资金是通过第三方乾某进行资金托管的，同时借款都是有房产作抵押的，其感觉是比较安全的，风险比较低。在 2015 年 10 月 26 日的时候，其在宏量财富上面发现有一宏量财富用户名为王小姐的人需要 5 万元资金，借款期限就一个月，其（叶某）当时就通过宏量财富的平台同意出借 5 万元资金。这 5 万元资金，其是通过第三方交易平台乾某将钱汇入的。5 万元资金出借后，没多久就收到了宏量财富发过来的《借款协议书》，是以电子邮件的形式发送到其老婆李某 3 的 QQ 邮箱内。其看了一下借款协议书，对这个投资渠道感到比较放心。在 2015 年 10 月 27 日的时候其又通过宏量财富平台出借了 5 万元给一宏量财富用户名为李流泉的人，钱也是通过乾某这个第三方交易平台汇款的，也收到了宏

量财富发过来的《借款协议书》。这两笔借款的期限都是一个月。到了 2015 年 11 月 23 日凌晨 1 时左右，宏量财富的网络平台登不进去了，网站也进不去了，投资者的 1000 多人的 QQ 群突然解散了，而陈文华、吴某、刘某 1 等人也都联系不到了，宏量财富公司也已经人去楼空，其出借的 10 万元没有拿回来，目前直接损失是 97492 元。

5.4 被害人郑某的报案材料，郑某陈述、平台投资记录截屏、银行流水，共同证实郑某的报案和投资情况，其陈述主要内容为：广州市宏量资产管理有限公司的 P2P 平台叫“宏量财富"，这个公司由“乾某托管公司"托管，担保公司是“深圳深业担保公司"。其 2015 年 11 月 17 号开始投资该平台，17 号投资 8 万元，返利 800 元约标钱和 1388 元满标奖励，20 号投资两个 6 万元，返利 600 元约标钱，还有 600 元约标钱在乾某托管公司的账户上提不出来。其用网银打给“乾某托管公司"的账户，至于钱怎么转给“宏量财富"公司的其不知道。

5.5 被害人彭某某的报案陈述，主要内容为：宏量财富的被害人成立了维权 QQ 群，以维护自己的权益。

5.6 其他被害人的报案表及材料，其中包括：

被害人韩某提供的 QQ 聊天记录，其中显示：宏量财富，乾某托管，30 天标，1000 撸 130 返 70，5000 撸 605 返 370，1 万撸 1151 返 700，5 万撸 6074 返 3700，18 万撸 17520+苹果 6s 返 1.5 万。多投，多号可议价。

被害人任某提供的宏量公司宣传页面截图。团队介绍页面，介绍陈文华为宏量财富平台创始人、董事长，简历为“毕业于浙江大学，经济学专业，多年从事金融工作，曾就职于银行信贷部门，小额贷款公司风控部门，担任担保公司总经理，长期积累了丰富的民间借贷…"公司风采页面，列有陈文华与他人在公司交谈的照片。

被害人杨某提供的宏量财富网贷平台宣传截图，陈文华以宏量公司董事长身份在宏量公司与员工合影。该合影已由宏量公司员工对其中的陈文华做了辨认，判决书前文已列述。

被害人王某提供的 QQ 信息截屏，其中显示：宏量财富，乾某托管，实收资本 2000 万，网贷之家有导航，投 980 一月撸 122 元，投 1W 撸 1121 元……。

6.广东诚安信司法会计鉴定所《司法鉴定意见书》（粤诚司鉴字[2018]20-2 号），证实：

（1）根据《充值记录》反映，艾某等 3884 人充值投入宏量公司的金额共计 2707.24631 万元，其中梁某等 224 名被害人乾某账户通过乾某平台充值投入宏量公司金额共计 931.36953 万元，

（2）根据《提现记录》反映，安某等 1544 人共计提现 470.140493 万元，其中分润状态为“无"的提现金额 453.94313 万元，分润状态为“未结算"的提现金额 16.197363 万元。经比对统计，《提现记录》反映梁某等 224 名被害人乾某账户从乾某平台提现到账的金额共计 60.508275 万元，其中分润状态为“无"的金额 58.170333 万元，分润状态为“未结算"的金额 2.337942 万元。

224 名被害人实际损失 870.861255 万元（931.36953-60.508275=870.861255 万元）

7.被告人陈文华的供述与辩解，陈文华归案后否认自己实施过犯罪行为，其侦查阶段供述和辩解的主要内容为：其没有租用过广州天河华明路 9 号 711 房，没有使用过自己的身份证去工商局登记注册成立过公司，不知道广州市宏量资产管理有限公司存在，没有在上述公司的办公地点照过相。其去过广州的银行开设账号，那是 2015 年的事情，当时有一个其坐牢时认识的广州这边的牢友，这个牢友打电话让其来广州，并且拿了其（陈文华）身份证去银行办了一张银行卡，然后就给了其（陈文华）两万元钱好处费，但没有把身份证还给其。其不知道这名牢友的真名。对方把两万元给了其以后，说身份证还要借用一下，之后就跑了，再也找不到了。当时其没有立即报警。其在广州的时候，不认识一个叫“吴某"和一个叫“刘某 1"的男子，不知道“乾某"的支付平台，没有使用过这个叫“乾某"的支付平台开展过借钱项目。

庭审中陈文华辩称：其没有实施公诉机关指控的犯罪行为，是有人拿其的身份证办了银行卡，并雇佣其去取过钱，公司设立时的签名不是其签的。拿其身份证办银行卡是其牢友联系的，后有老板叫其去过宏量公司三次，其在公司里拍了照，其无法提供牢友和老板的真实姓名以及联系方式。

本案另有综合证据如下

1.公安人员出具的《归案情况说明》，主要内容为：2017 年 5 月 30 日，在广州南站抓获陈文华。

2.陈文华身份材料，证实其身份情况。

3.陈文华犯盗窃罪的刑事判决书、释放证明书及释放后户口登记笔录，证实：陈文华因犯盗窃罪于 2003 年 4 月 7 日被湖南省攸县人民法院判处有期徒刑九年，刑期至 2011 年 8 月 1 日止。服刑期间经减刑，于 2009 年 5 月 16 日释放。

对自辩意见和辩护意见的回应。

对陈文华及其辩护人提出的陈文华没有实施指控的犯罪行为的意见，经查，

宏量公司工商登记显示陈文华是该公司法定代表人、执行董事兼总经理；

陈文华案发前亲自开户设立的其个人银行账户，在本案中接收了多笔涉案款项，相关账户的预留地址为宏量公司注册地址；

相关照片证实陈文华在背景为宏量公司名称的墙壁前与公司工作人员站立合影；

宏量公司多名工作人员均指认陈文华为该公司老板，管理该公司运营，该公司财务人员并指认曾在陈文华安排下从公司账户向陈文华个人账户转款；

证人陈某 1 证实陈文华案发期间在广州，相关住宿登记亦证实陈文华案发期间在广州酒店有过住宿；

被害人提供的该公司宣传推介材料中有陈文华作为该公司董事长所拍摄的照片及对陈文华学历、工作经历的虚假宣传；

陈文华对案发期间自己在何处，无法给出明确说明；

陈文华侦查阶段坚称自己不知道宏量公司，没有到过该公司，没有在该公司办公地点照过相，庭审中改称自己去过该公司，在里面呆过，还照过相，但其无法对供述上的这一改变给出合理解释；

陈文华称有人用其身份证办银行卡，并向其支付好处费 2 万元，有老板叫其去过宏量公司三次，其在公司里拍了照，其受雇取钱，每次收取 1 千元好处费，但称其无法提供对方这些人的真实姓名及联系方式，陈文华该辩解与日常经验不符，不可信。

综合全案证据，可以认定陈文华与其他同案人一起，实施了通过宏量公司、宏量财富网络借贷平台以非法集资方式骗取被害人款项并予以转移占有的行为，对其自辩意见和辩护人的辩护意见，本院不予支持。

对于辩护人提出的陈文华在本案中属从犯、指控的诈骗金额与事实不符、陈文华主观恶性不大、犯罪动机不明显、社会危害性较小的意见，经查，陈文华在其与同案人为实施犯罪而设立的宏量公司中担任法定代表人、总经理，对宏量公司的经营运转实施管理，积极参与宏量公司的推广宣传，并开设银行卡用于收取赃款，经其名下银行卡转出的赃款数额较大，综合全案情况，其在本案的共同犯罪中不属从犯，公诉机关指控的诈骗金额有相关证据和司法会计鉴定予以证实，真实可信，对辩护人提出的上述意见本院不予支持。

本院认为，被告人陈文华以非法占有为目的，使用诈骗方法非法集资，数额特别巨大，其行为已构成集资诈骗罪。公诉机关指控的陈文华的犯罪事实清楚，证据确实、充分，罪名正确，本院予以支持。陈文华因犯盗窃罪于 2003 年 4 月 7 日被湖南省攸县人民法院判处有期徒刑九年，刑期至 2011 年 8 月 1 日止，服刑期间经减刑，于 2009 年 5 月 16 日被释放。陈文华本次所犯集资诈骗罪与其前罪释放时间相隔已超过五年，虽不构成累犯，但在量刑时

可予考虑。依照《中华人民共和国刑法》第一百九十二条、第五十二条、第五十三条、第六十四条、《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》第五条第一款、第三款之规定，判决如下：

一、被告人陈文华犯集资诈骗罪，判处有期徒刑十三年，并处罚金45万元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2017年5月30日起至2030年5月29日止。罚金在本判决发生法律效力第二日起一个月内向本院缴纳。）

二、追缴被告人陈文华违法所得870.861255万元，发还各被害人（被害人名单及金额见附表），追缴数额不足上述数额的，按比例发还，不足部分责令陈文华退赔。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向广东省高级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审判长　边　龙

审判员　梁　敏

审判员　唐军国

二〇一八年九月二十八日

书记员　林泽峰

陈文华集资诈骗二审刑事裁定书

广东省高级人民法院

刑 事 裁 定 书

(2018)粤刑终1465号

原公诉机关广东省广州市人民检察院。

上诉人（原审被告人）陈文华，男，1968年9月7日出生，汉族，户籍所在地湖南省攸县。2003年4月7日因犯盗窃罪被湖南省攸县人民法院判处有期徒刑九年，2009年5月16日刑满释放。因本案于2017年5月30日被刑事拘留，同年7月4日被逮捕。现押于广东省广州市天河区看守所。

广东省广州市中级人民法院审理广东省广州市人民检察院指控原审被告人陈文华犯集资诈骗罪一案，于2018年9月28日作出(2018)粤01刑初189号刑事判决：（一）被告人陈文华犯集资诈骗罪，判处有期徒刑十三年，并处罚金45万元。（二）追缴被告人陈文华违法所得870.861255万元，发还各被害人（被害人名单及金额见附表），追缴数额不足上述数额的，按比例发还，不足部分责令陈文华退赔。宣判后，原审被告人陈文华不服，提出上诉。本院审理期间，上诉人陈文华于2018年10月12日向本院申请撤回上诉。

本院认为，原判认定上诉人陈文华犯集资诈骗罪的事实及适用法律正确，量刑适当。陈文华申请撤回上诉符合法律规定，应予准许。依照《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》第三百零五条第一款的规定，裁定如下：

准许上诉人陈文华撤回上诉。

广东省广州市中级人民法院(2018)粤01刑初189号刑事判决自本裁定送达之日起发生法律效力。

本裁定为终审裁定。

审判长　　吴铁城

审判员　　石春燕

审判员　　邓敏波

二〇一八年十一月十三日

书记员　　邓碧霞

案例二、何锦业集资诈骗案

广东省广州市天河区人民法院

刑 事 判 决 书

（2017）粤 0106 刑初 863 号

公诉机关广州市天河区人民检察院。

被告人何锦业，男，1984 年 8 月 29 日出生于广东省佛山市，汉族，文化程度大学本科，户籍住址广东省广州市天河区。因本案于 2016 年 9 月 27 日被羁押，同日被刑事拘留，同年 10 月 29 日被逮捕。现羁押于广州市天河区看守所。

辩护人王启星，广东古谷律师事务所律师。

广州市天河区人民检察院以穗天检刑诉〔2017〕876 号起诉书、穗天检刑补诉〔2017〕27 号补充起诉决定书指控被告人何锦业犯集资诈骗罪，于 2017 年 6 月 2 日向本院提起公诉，后于 2017 年 8 月 9 日补充起诉。本院受理后，依法组成合议庭，公开开庭审理了本案。广州市天河区人民检察院指派检察员张广斌、岑杰出庭支持公诉。被告人何锦业及其辩护人王启星到庭参加了诉讼。现已审理终结。

广州市天河区人民检察院指控：2014 年 3 月，被告人何锦业注册成立广州哆哆贷投资咨询有限公司，2015 年 4 月公司名称变更为广州多多贷互联网金融信息服务有限公司，办公地址先由本市天河区车陂北街 168 号二楼 256 房变更至本市越秀区东风东路 836 号三座 1303 房，再变更至本市天河区华夏路 16 号富力盈凯大厦 1309 房。何锦业在该公司担任执行董事兼经理。何锦业在该公司的多多贷 P2P 网络借贷平台发布虚假的借款人信息和投资人信息，造成借贷业务正常运转的假象，对外宣传投资该平台可以获得高额回报，骗取社会公众的投资款。2016 年 9 月 27 日，民警接到无法领取投资款本息的群众报警后前往富力盈凯大厦 1309 房抓获何锦业。

经核实，何锦业以广州多多贷互联网金融信息服务有限公司的名义非法吸收群众投资金额 27956169.48 元，返还群众金额 23980088.82 元。已向公安机关报案的被害人共 15 人，涉及实际投资总金额 220 万余元，实际收回总金额 77 万余元，实际损失总金额 144 万余元。

起诉后，被害人陈某 1 向公安机关报案，涉及实际投资总金额 186846.13 元，没有收回。

公诉机关认为被告人何锦业的行为已构成集资诈骗罪，数额特别巨大，提请本院依法判处，并列举了相关证据。

被告人何锦业辩称其行为应构成非法吸收公众存款罪，具体意见为：1.其发布的借款资料都是真实的，没有发布虚假信息；2.投资款都外借了，只是还没收回来；3.损失情况无法确认；4.其主动打电话给民警介入调查，属于主动归案，有自首情节。

辩护人提出以下辩护意见：1.被告人何锦业没有把集资款用于个人消费、挥霍，而是用于公司经营、广告投放、项目投资，资金的流向有合理的说法，因此被告人何锦业的行为不构成集资诈骗罪，而是构成非法吸收公众存款罪；2.本案是单位犯罪。

经审理查明：何锦业于 2014 年 3 月成立广州哆哆贷投资咨询有限公司，股东及法定代表人为何锦业，2015 年 4 月公司名称变更为广州多多贷互联网金融信息服务有限公司（以下简称“多多贷公司”），办公地址变更至广州市天河区华夏路 16 号富力盈凯大厦 1309 房。何锦业在该公司担任执行董事兼经理。何锦业在未取得国务院银行业监督管理机构批准，不具备吸收公众存款资格的情况下，以多多贷公司经营的多多贷网贷平台（××）对外宣传投资可获得高额回报，非法吸收投资款。2016 年 9 月，因资金链断裂导致投资人无法提现。2016 年 9 月 27 日，何锦业在多多贷公司与投资人协商还款事宜未果后报警处理，公安人员将其抓获归案，归案后如实供述上述事实。

经核实，向公安机关报案的被害人共 14 人，吸收投资款共计人民币 4253999.33 元，返还投资款共计人民币 2842880.51 元，导致损失共计人民币 1411118.82 元。其中徐某投资

215073，损失 143882.11 元；王某 1 投资 697373.3 元，损失 77685.12 元；闵某投资 100000 元，损失 90000 元；曲某投资 222800 元，损失 199364.8 元；蔡某投资 59000 元，损失 53748.46 元；郭某投资 114000 元，损失 73884.34 元；洪某投资 19705.01 元，损失 19705.01 元；谢某 1 投资 282965 元，损失 159447.45 元；张某投资 717708.08 元，损失 189114.65 元；丁某真投资 35150 元，损失 35150 元；李某 1 投资 167830 元，损失 122831.52 元；刘志尧投资 876459.93 元，损失 32734.65 元；程某投资 130000 元，损失 79130.87 元；陈某 1 投资 615935 元，损失 134439.84 元。

上述事实，有下列经庭审举证、质证的证据证实，本院予以确认：

1.被害人徐某的报案陈述、辨认笔录及报案材料：2015 年 10 月左右，我经朋友介绍了一个广州多多贷互联网金融信息服务有限公司的 P2P 平台，前后共投资了本金 17 万到这个平台，2016 年 9 月 20 日我从东莞来到这间公司所在地富力盈凯 1309 房找公司的老板提现，我当天从这个平台提取了 11695.89 元，剩下 160439.54 元无法提现，后来老板何锦业出具了一份承诺书给我，答应本月 25 日前可以提现 5 万元，剩下的在下月 20 日前全部结清，但到了 2016 年 9 月 26 日，还是提不了现金，我于是就再次来到公司找这个老板提现，但这个老板就表态没有钱给不了，我就一直在公司和这个老板谈提现的事情，后来这个老板报警了，我们就一起来到派出所处理了。

我先通过多多贷的网页:××用自己的名字注册了一个帐号，捆绑了本人工商银行卡的帐号:62×××95，注册后我主要投了年利率 14%、12%、10%。这个 P2P 平台到期后就可以提现。投资后会自动生成一份电子合同，投资到期后本金和利息会返回到平台的个人帐号内。

2015 年 10 月 31 日会员充值过 15000 元，2015 年 11 月 11 日会员充值过 20000 元，11 月 20 日会员充值过 20000 元，12 月 31 日会员充值过 9044 元，2016 年 4 月 4 日会员充值过 46009 元，7 月 2 日会员充值过 4920 元，7 月 19 日会员充值过 42000 元，7 月 21 日会员充值过 50000 元，9 月 1 日会员充值过 8000 元，9 月 10 日会员充值过 100 元。

2015 年 11 月 18 日申请提现过 20095 元，2016 年 1 月 7 日申请提现过 3500 元，2016 年 1 月 17 日申请提现过 5000 元，2016 年 3 月 19 日申请提现过 20400 元，2016 年 7 月 23 日申请提现过 500 元，2016 年 7 月 28 日申请提现过 10000 元，2016 年 9 月 12 日申请提现 11695.89 元。

经照片辨认，其辨认出何锦业。

2.被害人王某 1 的报案陈述、辨认笔录及报案材料：我在 2014 年上网了解到一家叫“多多贷”的网上金融借贷网站，该网站的全名是“广州多多贷互联网金融信息服务有限公司”。我上网了解，该公司有正规的工商登记信息，有第三方担保，具体投资项目，导致我认为这家公司可信。我在 2015 年 9 月份在“多多贷”平台注册三个账号，该三个账号详细的使用情况如下:1.我本人身份注册账号:麒麟玉，从 2015 年 9 月开始投钱，累计投入本金 2 万元人民币，现在该账号本息显示是 20280.46 元。2.我母亲杜玉芹，账号是 chance，该账号我从 2015 年 9 月开始投钱，累计投入本金 8 万元人民币，现在该账号本息显示是 81454.03 元。3.我父亲王某 3，账号 wendy，该账号我从 2015 年 9 月开始投钱，累计投入本金 6 万元人民币，现在该账号本息显示是 60736.51 元。以上账号我投的种类是 7 天为一期，利息每期每 10000 元 26 元利息，合年息是 14%。

之前我投钱提钱都是正常的，到了 2016 年 9 月 1 日，我在“多多贷”提钱开始异常，就是拖时间，到了 2016 年 9 月 4 日“多多贷”平台是一点钱都提不出，每次要求提钱。该平台网上答复要多等几日，但是屡屡失信，到现在我也没有收到钱。我于 2016 年 9 月 22 日来到广州，来到广州富力盈凯 1309“多多贷”公司，我见到了“多多贷”法人代表何锦业，何锦业告诉我因为资金紧张要我等待。何锦业向我写了一份承诺书(详见承诺书复印件)，该承诺书承诺在 2016 年 9 月 30 日前将我账户 chance、wendy 内的共 142190 元钱给我，但

是现在也没有给我。

在网上有签订电子合同，我合同签名是注册名。签的名字分别是“麒麟玉”、“wandy”、“chance”。平时我往账号里面投钱，“多多贷”没有具体人员和我联系，我每投一笔钱，“多多贷”网站都会说明该钱用于何处、何项目，让人比较相信，这次我来广州，“多多贷”根本不能向我提供我投钱用于何处的合同等证明，存在明显诈骗。

经照片辨认，其辨认出何锦业。

3.被害人闵某的报案陈述、辨认笔录：因为我在一个叫多多贷的网络借贷平台上投资了共 10 万资金，现在无法进行提现，公司负责人何锦业一直以各种理由推脱，不给我们提现，也不给我们退款，所以来报案。2016 年 7 月份我在网上搜索理财的项目，无意间看到一个叫多多贷的网络借贷平台，我就进去这个官网里，我在这个官网里看到该公司的基本情况，同时我看到官网里有该平台的安全保障介绍，说该公司有一千万风险备用金，还附有在中国民生银行的一千万存款证明，同时说明当出现逾期和违约时将由风险备用金向投资者进行代偿。于是 2016 年 8 月 5 日我在该平台网页上注册了一个账号（13×××42），在平台里充值了五万元，投资年利率 10%的项目，期限是一个月。到了 2016 年 8 月 16 日我又在多多贷的网页里注册了一个账号(18×××61)，后在平台里充值了五万元，还是投资年利率 10%的项目，期限是一个月。到了 2016 年 9 月 4 日，我登入多多贷网页申请账号 13×××42 的提现，之后网页里显示审核通过处理中，但是一直没有钱到账。到了 9 月 15 日我又申请另一个账号 18×××61 的提现，但是一直显示待审核的状态，也没有钱到账。第一次提现不成功我就在多多贷的官方群里询问情况，群里的一个客服称提现要延迟一到两周，但是到了时间我还是提不出来，之后我继续问情况，群里的客服说因中秋放假，过了中秋再处理，但是过了中秋之后，我还是提现不了。于是 2016 年 9 月 21 我来到广州市天河区富力盈凯大厦 1309 房，后来一个叫何锦业的负责人接待我的，当时还有其他人也来咨询提现不了的事情，何锦业说提现全额款是当天处理不了的，何锦业当场口头答应我一周内解决 9 月 4 日的那笔五万元的提现，在我们的强烈要求下何锦业还从他的个人的银行账户里转了一万元给我，之后我就离开了。等了一个多礼拜我还是没收到款，于是 2016 年 9 月 26 日我再一次来到广州市天河区富力盈凯大厦 1309 房，我就问何锦业怎么处理，对方就说现在处理不了，叫我们等，他也没说期限。后来在等待的过程中我们双方都报了案。

多多贷平台的法人是何锦业。我在多多贷平台进行投资没有手签合同，只是在充值投资项目后会生成一个借款协议。内容有投资账号及投资金额，借款人的信息等，还有一些相关权利义务。我不清楚充值后这些钱去到什么账号里，也不清楚这些钱具体做什么用。多多贷网络借贷的公司名称是广州多多贷互联网金融信息服务有限公司，但是在该平台网页里的一千万元存款证明上显示的确是广州多多贷投资咨询有限公司。多多贷的 QQ 群是 489137784，群名称是多多贷官方交流群 2，其中那个答复我的客服 QQ 号是 34×××24，昵称是多多贷-子洪。我没有成功提现过。

经照片辨认，其辨认出何锦业。

4.被害人曲某的报案陈述、辨认笔录及报案材料：2016 年 8 月 12 日开始，我陆续使用了本人和我妻子金某的账户进行多笔投资，我的账户投资 113452 元(连同利息)，在 9 月 5 日提现成功 10000 元。金某的账户投资 103392 元(连同利息)，没提现成功。所以我损失的金额是 113452-10000+103392=206844 元人民币。

2016 年 8 月 10 日左右，我在偶然的机会上网看到一个叫多多贷的互联网 P2P 金融服务平台。我看了一下这个平台的介绍，它自称是中川集团旗下的金融平台。而中川集团是四川省比较有实力的上市公司，我就相信上面的介绍了。然后就想在多多贷上面进行投资。我投资金额多达 20 万，之后想提现，但只成功了 10000 元，就连同其它投资者在 2016 年 9 月 26 日早上来到广州市天河区华夏路 16 号富力盈凯大厦 1309 房找法人何锦业，但他不在。

我们就约了下午 15 时再见面。到了下午，我和王某 1、王某 3、徐某、闵某见到了何锦业，问他为什么到期了却不能提现，怎么解决。何锦业一直在推脱，只说尽快把钱还我们，但我们都觉得他态度不好，只是说说而已。后来王某 1 父女和何锦业都报了警。

我在吉林省的家里使用手机操作的。流程是，先登录多多贷官网或手机客户端进行注册，绑定银行卡，就会在系统里面生成一个多多贷的账户，然后从银行卡转账到账户内，就可以投资了。这个平台承诺的是，投资一笔款项之后，根据投资期限的不同，会获得不同的收益，比如投资一个月的年利率有 10%，3 个月有 11%等。到期之后，就可以本金连利息一起提现，将平台账户里的钱转回银行卡内。整个过程都可以在官网或手机客户端上操作。

全名广州多多贷互联网金融信息服务有限公司，法人是何锦业，广告上标榜自己的中川集团旗下的，实际上有维权的人查过，多多贷是有工商登记的，但并不是中川集团旗下的。一个月的年利率有 10%，三个月有 11%，我的 20 余万是分成若干笔投资的，有十五天的，有一个月的，也有三个月的。在多多贷官网上，会有电子版的借款协议。

经照片辨认，其辨认出何锦业。

5.被害人蔡某、郭某、洪某、谢某 1、张某、丁某、李某 1、刘某、程某、陈某 1 的报案陈述及报案材料，证实其在多多贷平台投资，后来导致损失的情况。

6.证人邝惠琪证言及其提交的账号资料、运营报表、投资金额数据表、运营数据统计、发标资料：我于 2016 年 5 月 24 日入职多多贷公司，任职运营助理。月薪 3000 元（试用期三个月），没有提成，也没有其他绩效提成。我每天的主要工作就是按照总经理何锦业的要求，在多多贷网贷平台发布借款标和统计运营数据（浏览量、访客量、访客回访量、访客登陆地址量、注册量、投资量、新增投资客户数、客户实际投资金额和公司自投金额），工作结果主要体现在《运营报表》、《投资金额数据表》中。其中《运营报表》每日都要通过邮箱发到老板的邮箱中。

我到公司上班后，上一任留给我一个用于运营数据统计的文档，我按照该文档的操作提示统计浏览量、访客量、访客回访量、访客登陆地址量。统计注册量、投资量、新增投资客户数、客户实际投资金额和公司自投金额。为方便统计客户实际投资金额和公司自投金额，我设计了《投资金额数据表》，其中自投金额就是《营运报表》中的投资量。

《投资金额数据表》按上线时间，每天逐一统计每一个借款标的借款总额，客户实际投资金额、公司自投金额，以及客户实际投资比例。我一般是在发布借款标的第二天进行统计，如果客户实际投资金额未满标（例如，2016 年 9 月 1 日发布的一个三个月期的 11 万元借款标，9 月 2 日我统计发现实际客户实际只投资 100 元，然后使用多个系统原来就设定了的账户（含密码）进行虚假投资 109900 元。系统原来就设定虚假投资账户大约有 200 个，交接时电脑内有文档，我已经提交给了公安机关。

按照交接时的要求，何锦业经理交给我若干份用于发布借款标的信息资料，其中包括新手标信息资料一套、保理标信息资料一套、富申担保公司资料一套、桉树标资料一套。然后，何经理给我的要求是在工作日每天发布借款标八个，包括 4 个 7 天借款标（资金总额约 55 万元）、2 个 30 天借款标（资金总额约 30 万元）、三个月和六个月的各一个（资金总额约 20-30 万元）；累计发布借款标的借款总额为 100 万元左右。节假日或者周末就发 6 个借款标，其中 4 个 7 天借款标（资金总额约 55 万元）、1 个 30 天借款标（资金总额约 15 万元）、三个月一个（资金总额约 10-15 万元）；累计发布借款标的借款总额为 85 万元左右。发布借款标的时候用账号“fengling”，借款人是原来就在网贷平台里就设置好的，借款人信息是否真实我不清楚，何锦业经理交待我，选用原来网站上面当天到期的借款标的借款人信息进行发布借款标。借款标的内容则按照对应的资料黏贴上去。例如新手标网上发布的内容和老板交给我的电子文档就是一模一样的；担保标网上发布的内容就是按照老板交给我的电子文档的 1-7 顺序黏贴到网页上。

工作期间累计发布借款的具体情况我不记得了，工作日就是发布 8 个借款标 100 万元左右；节假日就是 6 个借款标 85 万元左右；累计发布 600 余个借款标，具体情况要以我的《投资金额数据表》为准。

经照片辨认，其辨认出何锦业。

其提交了账号资料，其签认是上一任运营助理交给其，何锦业让其用这 201 个虚拟账号账号对未满的标进行投标的。

其提交了运营报表、投资金额数据表、运营数据统计，其签认是其按何锦业要求统计并每天发给何锦业的数据

其提交了发标资料，其签认是上一任营运助理交给其，何锦业让其粘贴在后台系统，每天进行发标。

7.受案登记表、立案决定书、抓获经过、破案经过、抓获录像，证实 2016 年 9 月 27 日 1 时许，公安机关接到报警称在广州市天河区华夏路 16 号富力盈凯大厦 1309 房发生纠纷，公安人员在现场将双方带回公安机关。经了解，报警人报称其在多多贷网贷平台进行投资，该平台涉嫌非法集资。

8.工商登记资料，证实广州哆哆贷投资咨询有限公司在 2014 年 3 月成立，股东及法定代表人为何锦业，2015 年 4 月公司名称变更为广州多多贷互联网金融信息服务有限公司。

9.实际投资金额列表，被告人何锦业签认就是从多多贷 P2P 平台下载，是多多贷 P2P 平台投资人实际投资金额列表。

10.平台客户提现金额列表，被告人何锦业签认是从多多贷 P2P 平台下载，是平台客户实际提现金额列表。

11.借款标的数据，被告人何锦业签认是多多贷 P2P 平台九月份发布借款标的的数据。

12.投资金额未满的借款标，被告人何锦业签认是反映平台的借款标在投资人投资金额未满标的情况下，平台会安排人员操作虚拟账号进行虚假投资，使借款标达到收取投资款目的。

13.还款中的借款标列表，被告人何锦业签认为多多贷平台显示为“还款中”状态的借款标列表，累计共 302 个借款标 58 个借款人，3455 万元借款，借款人均为虚拟。

14.常住人口基本信息查询、情况说明，证实公安人员经对前述还款中的借款标列表借款人信息进行核查，发现全国人口信息库内没有借款人身份信息。

15.192 个账户明细，被告人何锦业签认该 192 个账户资金余额在 1000 万元以上（共计 20.14 亿元）实际没有真实资金充值，为虚拟资金账户。

16.何锦业名下银行账户开户资料及交易流水，证实被告人何锦业名下 4270300059172774 、 6222300472612046 、 6222300472612095 、 6212263602077521706 、6212263602077521714、6217003320023116596、6227003324650036910 账户的交易情况。

17.广州多多贷互联网金融信息服务有限公司（广州哆哆贷投资咨询有限公司）在中国民生银行 62×××65 账户的交易流水，证实该司基本账户的交易情况。

18.搜查笔录、扣押决定书及扣押清单，证实 2016 年 9 月 27 日 14 时，公安人员对何锦业位于天河区华夏路 16 号富力盈凯大厦 1309 房的涉案公司进行搜查，扣押借款协议原件 18 份、借款资料复印件 12 份、电脑 1 台。

何锦业对扣押的借款协议原件、借款资料复印件签认情况：

（1）被告人何锦业签认其与潘某、钟某、阮某、谢某 2、黄某、谢某 3、成某、李某 2、谢某 4、陈某 2、林某、罗某、谢某 5、黎某等人的借款合同是其以个人名义出借，资金来源是多多贷平台投资款，共 16 笔 71.8 万元。

（2）肇庆市高要区禄步镇洞头村大冬瓜、丹竹尾山场的林木买卖协议书（金额 68 万元），被告人何锦业签认购买林权的资金是多多贷平台吸收的投资款，合同约定的总金额为 68 万

元，实际已支付 58 万元。

（3）借款资料复印件，被告人何锦业签认为其放在办公室的各类合同，用于平台发标挂网用，实际上这些合同都没有证实借款和担保。

19.广州市公安局电子数据检验鉴定实验室穗公网勘【2016】1844 号电子物证检查工作记录，证实对扣押的何锦业的 1 台电脑主机进行检查的情况。

20.银监会广东局出具的关于广州哆哆贷投资咨询有限公司等经营资格认定的复函，证实广州哆哆贷投资咨询有限公司、广州多多贷互联网金融信息有限公司不是该局批准设立的银行业金融机构，不具备吸收公众存款的资格。

21.户籍材料，证实被告人何锦业的身份情况。

22.被告人何锦业的供述：我是广州多多贷互联网金融信息服务有限公司的股东和法定代表人、实际负责人，主要负责整个公司的运营，公司接纳的借款人标的、审核、以及财务部由我负责。该公司现有员工约 7 人，主要经营多多贷 P2P 网络借贷平台，平台于 2014 年 4 月上线，主要模式是有借款需要的借款人会找到我们公司，然后向公司交手续费便可以在平台上发标，然后网络上的注册用户可以对这些招标进行充值，然后用充值的钱可以投标，平台收到投资者资金后将钱转给这些借款人。借款人按照合同要求向平台还款，借款人和投资者之间的利息存在利息差，我们平台就是靠赚取利息差获利盈利的。简单来说，该平台就是一个投资人和借款人的贷款中介。因我公司这个月一些投资人的投资款因公司出了一些状况而无法提取，他们来公司讨说法，警察来了解后将我带到派出所协助调查。造成平台提现困难有两种情况，一种是因为我们平台会对一些借款人的借款进行拆分，例如某借款人需要借 100 万资金，期限为 6 个月，但由于市场上的投资者较倾向于投资一个月左右的短期标的，因此我们会将借款人的借款标的标为 1 个月，然后将一个月到期后又发布借款人借 100 万期限 1 个月的，以此类推，最后等借款人还款再将还款还给剩余的投资者。但今年 8 月，国家对 P2P 平台的新政策，导致拆分标的投资者出现集中提现，但没有足够的新用户对借款标的进行投资，而借款人的借款期限没有到期，导致无法兑付投资人投资款。另一种原因是公司盈利无法支持公司的运营成本，且因自身经营不善，我于 2014 年 5 月开始挪用部分投资人的投资款用于公司的自身经营，而资金运营也不成功，导致挪用投资者投资款无法及时偿还，造成了对投资人的资金缺口。该平台实际投资人约为 90 人，累计交易额约 1 亿元，现对投资款的资金缺口约为 280 万，涉及投资者七八十人，现未收回的借款人借款额约有 150 万元，有约 130 万的投资资金是由于挪用至平台自身经营所导致的缺口。

我们平台根据不同的标的，向投资者发布的标的利息为年利率 8%至 12%，个别老用户达年利息 14%，对于借款人根据不同的借款数额和期限，利息为年利率 24%至月息 6%不等。

根据我电脑中从 P2P 网络借贷平台下载的数据，多多贷 P2P 网络借贷平台投资人的实际充值投资金额为 27956169.48 元（数据 A），多多贷 P2P 网络借贷平台投资人的实际提现金额为 23980088.82 元（数据 B），我向个别投资人直接支付现金作为提现的数额为 37 万元（数据 C），借款人实际借款数额为约 70 万元（数据 D），还有约 100 万元（数据 E）是我朋友充值进平台，让帮其放贷使用的，那么我利用多多贷 P2P 网贷平台募集投资款并挪用至我自身经营所需的金额数为：数据 A（27956169.48 元）减去数据 B（23980088.82 元）减去数据 C（37 万元）减去数据 D（70 万元）减去数据 E（约 100 万元），因此数额约为 200 万元，其中，有 58 万我用于购买广东省高要市禄步镇洞头村大冬瓜、丹竹尾山场的林权，打算投资经营（合同金额为 68 万元，有 10 万元我还没有支付）。

我们平台与第三方支付平台宝付支付签订合作协议，投资者若要对平台标的投资，首先要开设投资者自己的宝付支付账户，并充值进入该宝付支付账户中，然后投资者在多多贷网络借贷平台进行操作投标，其投资款则通过其宝付支付账户转入多多贷网络借贷平台开设的宝付支付账户中去，平台再将投资者的投资款集中支付到借款人的宝付账户中去，也有的时

候，多多贷网络借贷平台也会从平台的宝付账户直接汇入借款人的银行账户。

因为投资者的投资款会首先在平台的宝付支付账户中集中，而该平台账户我是可以操作的，于是有时我会操作该账户，将一些款项汇入本人的银行账户中，一个是本人的工商银行南沙旺阁支行账户，一个是本人的建设银行体育西支行，然后再将资金用作公司的正常使用。我是从 2014 年 5 月开始将投资者的投资款挪用作平台自身的运营的，但当时挪用的资金量很少，从 2015 年初开始，挪用的资金量较多，2016 年 8 月，我大概就挪用了 20 万投资款用作经营，公司运营支出主要是用于公司场地租金，员工工资，网站维护等。此外，每月还将 5000 元的投资款用于我自己的个人开销。我没有对挪用的投资款进行记账。

多多贷 P2P 网贷平台的借款标的，其借款人身份及借款信息不是真实的，这些借款人的身份信息及其借款信息都是虚构的，由于真实的借款人及借款需求并不多，因此我便虚构了一些借款人的身份，并参照其他公司借款客户的借款需求，虚构了一些借款标的让公司员工在平台发布，用于吸引投资人投资。即便我们公司有一些真实的借款人客户，但我认为投资客户根本不关心借款人的真实身份，因此我也没有使用真实的借款人客户的身份信息及借款需求在平台上发布借款标的。发布标的的公司员工不知道平台的借款标的是虚构的。

多多贷 P2P 网贷平台的投资客户，包括投资标的里的投资客户，其投资事实不是全部都是真实的，由于我们在平台上放出的标的金额通常依靠真实的投资客户投资，是不能够投满这些标的的金额，这样的话这些标的就会流标，就不能顺利进行。因此如果我看到有真实的投资客户对投资标的进行投资后，我就会利用一些我操控的虚拟投资人账户对标的进行投标，投够标的所需金额，让标的顺利进行。这些虚拟的投资人账户大约有 200 多个，要识别这些账户的话，只要打开平台的后台数据，查看投资人账户情况，通常没有实际充值的就是虚拟的投资者账户。

在我办公室发现一些借款资料的复印件共 12 份，是我从别的融资公司拿来的，资料里都是这些融资公司的借款客户，我拿他们的资料来参照其借款需求来虚构一些借款信息在多多贷 P2P 网贷平台上发布。在我办公室发现一些借款资料的原件共 18 份，是我全部的真实的借款人客户签订的借款协议，现在约为 70 万元左右。另外，还有一份是我用于购买广东省高要市禄步镇洞头村大冬瓜、丹竹尾山场的林权的合同，合同金额为 68 万元，我支付了 58 万元，有 10 万元我还没有支付。这些真实借款大部分还未收回，我已委托表弟帮我催收。

我利用多多贷 P2P 网贷平台募集投资款并挪用至我自身使用的资金，基本上都是用于支付公司自身经营所需的工资、房租、运营费用，还有就是用于购买广东省高要市禄步镇洞头村大冬瓜、丹竹尾山场的林权，打算用于投资经营。除了将投资款用于公司的运营，我还有将投资款用于我自己个人开销，大约每月有 5000 元左右。在多多贷 P2P 网贷平台网站上，宣传多多贷 P2P 网贷平台的部分投资标的有广州富申投资发展有限公司作担保，但我们公司和其并没有实际担保的协议，该公司实际也不为平台的标的作任何担保。

根据不同的标的，我们向投资者发布的标的的利息为年利率 8%至 12%，个别老用户达年利率 14%。对于借款人根据不同的借款数额和期限，利息为年利率 24%至月息 6%不等。

我从 2015 年 6 月开始，累计把投资款用于平台自身运营大概有两百万元左右。出现客户提现困难的情况后，我一个是催促投资项目回款，二是卖了我自己的车，还向亲戚朋友借了 20 万来支付到期投资人的投资款。公司成立至今，平台真正投钱的投资者有七八十人，还有一些会员只为进来拿些奖励或者红包的就太多了，没办法统计。公司成立至今，平台累计的交易额有约一个亿左右。

公司为了吸引客户投资，有进行宣传或者广告，通过搜狗等搜索引擎做广告，还有一些门户网站的论坛，微博、微信等，广告公司介绍等。我公司的网站主页的内容文字内容基本上都是我安排的，我们网站主页上写“中川集团旗下的金融平台”，中川集团法人代表也是我，是今年 7 月登记注册的。我们网站主页上写明“有一千万风险备用金”实际上是没有的，

就是给客户一个信心。邝惠琪是运营助理，她的工作内容就是每天在公司网站上滚动发布投资标的，统计投资数据及网站访问量等。

关于控辩双方的意见，本院综合评析如下：

一、关于本案定性问题，经查，经被告人何锦业签认的从平台提取的充值金额表与提现金额表证实，何锦业通过多多贷网贷平台非法吸收的存款，大部分已返还给投资者；何锦业供认其虽虚构了部分借款标的，挪用部分资金，但都用于购买林权准备经营以及公司运营费用，公诉机关未提供证据证实该部分辩解不属实。故现无证据证实被告人何锦业对吸收的公众存款具有非法占有的目的，不足以认定为集资诈骗行为，应定性为非法吸收公众存款行为。公诉机关指控被告人何锦业犯集资诈骗罪的证据不足，本院不予支持。被告人何锦业及辩护人辩称其行为构成非法吸收公众存款罪的意见，本院予以采纳。

二、关于犯罪数额问题，经查，经核对各被害人的报案陈述、报案材料、被告人何锦业的供述及其签认的平台投资、提现记录，采信能够相互印证的部分，确认在本案中向公安机关报案的被害人共 14 人，何锦业吸收被害人投资款共计人民币 4253999.33 元，返还投资款共计人民币 2842880.51 元，导致损失共计人民币 1411118.82 元。公诉机关对被告人何锦业犯罪数额的指控有误，本院予以纠正。

三、关于单位犯罪问题，经查，被告人何锦业设立的多多贷公司的主要业务是吸收存款进行放贷。根据《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》第二条的规定，公司、企业、事业单位设立后，以实施犯罪为主要活动的，不以单位犯罪论处。故本案不应认定为单位犯罪。辩护人辩称本案为单位犯罪的辩护意见据理不足，本院不予采纳。

四、关于被告人何锦业辩称其主动打电话给民警介入调查，属于自首的辩解意见，经查，被告人何锦业的供述与被害人徐某、曲某的报案陈述、抓获录像共同证实，徐某等多名被害人因无法提现到何锦业办公室与之协商还钱事宜未果，何锦业报警处理，其在归案后如实供述了本案犯罪事实，应认定为自首。被告人何锦业本节辩解意见本院予以采纳。

本院认为，被告人何锦业违反国家法律、法规的规定，未经国家有关监管部门批准，以多多贷公司名义向社会不特定公众变相吸收公众存款，数额巨大，严重扰乱金融秩序，其行为已构成非法吸收公众存款罪。被告人何锦业在犯罪以后自动投案，如实供述罪行，自愿认罪，是自首，可以从轻处罚。辩护人关于对被告人从轻处罚的辩护意见，本院予以采纳。被告人何锦业的违法所得应予追缴并发还被害人。依照《中华人民共和国刑法》第一百七十六条、第五十二条、第五十三条、第六十七条第一款、第六十四条以及《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》第三条第二款、《最高人民法院关于处理自首和立功具体应用法律若干问题的解释》第一条的规定，判决如下：

一、被告人何锦业犯非法吸收公众存款罪，判处有期徒刑三年三个月，并处罚金人民币二十万元（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日，即从 2016 年 9 月 27 日起至 2019 年 12 月 26 日止；罚金应自判决发生法律效力第二日起十日内向本院缴纳）。

二、追缴被告人何锦业的违法所得，按比例发还各被害人，追缴数额以被害人损失和何锦业违法所得数额为限,不足以弥补的被害人损失，责令被告人何锦业退赔。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向广东省广州市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审　判　长　　方洪立

人民陪审员　　吴文涛

人民陪审员　　田常国

二〇一七年十月二十日

书 记 员 谭珊珊
李丹丹

案例三、周玉齐犯集资诈骗案

广东省高级人民法院
刑 事 裁 定 书

（2017）粤刑终 151 号

原公诉机关广东省惠州市人民检察院。

上诉人（原审被告人）周玉齐，男，1973 年 8 月 24 日出生，汉族，高中文化，户籍所在地广东省惠州市惠城区。因本案于 2015 年 10 月 14 日被刑事拘留，同年 11 月 20 日被逮捕。现押于广东省惠州市看守所。

辩护人朱启珍、广东启鑫律师事务所律师。

辩护人吴志强，广东启鑫律师事务所律师。

广东省惠州市中级人民法院审理广东省惠州市人民检察院指控原审被告人周玉齐犯集资诈骗罪一案，于 2016 年 12 月 12 日作出（2016）粤 13 刑初 94 号刑事判决。宣判后，原审被告人周玉齐不服，提出上诉。本院依法组成合议庭，决定以不开庭方式进行审理，通过阅卷及讯问上诉人、听取辩护人的意见，现已审理终结。

原判认定，2013 年初，被告人周玉齐以其占股 80％的惠州市艺商文化投资发展有限公司的名义创建了“艺商贷”P2P 网络平台。周玉齐在该网络平台上虚构借款人及标的等信息，承诺给予高额回报并进行非法集资，然后将大部分集资款用于炒股、支付集资参与人的本金及利息和偿还个人债务。2015 年下半年，周玉齐炒股亏损 2525.0951 万元，导致无法支付集资参与人的本息，但其仍继续非法集资，并用集资款项支付高额利息。2015 年 10 月 14 日，周玉齐主动到公安机关投案。经司法审计，2015 年 5 月 1 日至 10 月 14 日，周玉齐向 445 人非法集资计 4493.667621 万元，偿还本息计 2283.97152 万元，无法偿还集资款计 2221.617062 万元（其中未用真实姓名、姓名不详者 17 人，涉及金额计 44970 元）。

原判认定上述事实，有书证、证人证言、被害人陈述、鉴定意见、被告人供述及辩解等证据证实。

原判认为，被告人周玉齐的行为已构成集资诈骗罪。周玉齐犯罪后主动投案，并如实供述自己的基本犯罪事实，是自首，依法可以从轻处罚。依照《中华人民共和国刑法》第一百九十二条、第六十七条第一款、第五十二条、第五十三条第一款、第六十四条及《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》第五条第一款之规定，作出判决：（一）被告人周玉齐犯集资诈骗罪，判处有期徒刑十三年，并处罚金人民币三十万元。（二）公安机关冻结在案被告人周玉齐、惠州市艺商文化投资发展有限公司名下的存款（详见冻结存款清单），依法按比例向王某凤等 428 名被害人发还，公安机关查封、扣押在案的钢琴 5 台、古筝 10 件、电子钢琴 4 台、吉他 6 把、电吉他 2 把，以及周玉齐名下的房产（详见查封清单）经依法处理后的得款，用于赔偿各被害人损失，差额部分责令被告人周玉齐退赔。

上诉人周玉齐上诉及其辩护人辩护提出，1、原判认定周玉齐犯集资诈骗罪事实不清，适用法律错误，应认定其行为构成非法吸收公众存款罪。2、审计报告未及时送达给周玉齐，损害其诉讼权利；且审计报告是不全面、不客观的，原判对于周玉齐及其辩护人提出的重新鉴定申请未作处理而采信审计报告，属认定事实不清、违反法定程序。周玉齐具有自首情节，主观恶性较小，原判量刑过重，请求减轻处罚。

经审理查明，2013 年初，上诉人周玉齐以其经营的惠州市艺商文化投资发展有限公司的名义创建了“艺商贷”P2P 网络平台。随后，周玉齐未经国家金融主管部门批准，通过“艺

商贷”P2P 网络平台发布虚假的借款人、借款项目等信息，以支付高额回报为诱饵，非法吸收社会公众的资金。期间，周玉齐将集资款项主要用于其个人炒股并造成巨额亏损。经审计，截至案发，周玉齐尚欠他人的集资款计 2221.617062 万元。2015 年 10 月 14 日，周玉齐主动向公安机关投案自首。

认定上述事实，有下列证据证实：

（一）书证

1、受案登记表、立案决定书及抓获经过：2015 年 10 月 14 日，周玉齐因将“艺商贷”网络借贷平台的资金用于投资股市失败，导致资金周转困难，无法向投资者偿还本息，主动到惠州市公安局投案自首。同日，该局立案侦查本案。

2、搜查笔录及扣押物品、文件清单：（1）2015 年 5 月 31 日，惠州市公安局从证人刘某婷处扣押钢琴 5 台、古筝 10 件、电子钢琴 4 台、吉他 6 把及电吉他 2 把。

（2）2015 年 11 月 2 日，惠州市公安局从证人刘某婷处扣押中国银行卡（卡号 XXXXXXXXXXXXXXXXXX）、光大银行卡（卡号 XXXXXXXXXXXXXXX）、农业银行卡（卡号 XXXXXXXXXXXXXXXXXX）、招商银行（卡号 XXXXXXXXXXXXXXX）及招商银行（卡号 XXXXXXXXXXXXXXX）各 1 张。

（3）2015 年 10 月 16 日，惠州市公安局派员对位于惠州市下埔大道的惠州市艺商文化投资发展有限公司进行搜查，并查扣账本 2 本、书面资料 1 箱及电脑主机 3 台。

3、查封决定书、协助查封通知书及协助冻结财产通知书等：（1）案发后，惠州市公安局依法查封周玉齐名下的惠州市环城西二路商铺。

（2）案发后，惠州市公安局依法查封周玉齐名下的惠州市惠城区房。

（3）案发后，惠州市公安局依法查封姚某虹名下的惠州市下埔大道 7 号紫荆大厦 3003 房。

（4）案发后，惠州市公安局依法冻结周玉齐名下的农业银行卡 XXXXXXXXXXXXXXXXXX 内的余额 682.26 元。

（5）案发后，惠州市公安局依法冻结周玉齐名下的中国银行账户 XXXXXXXXXXX 内的余额 877.69 元。

（6）案发后，惠州市公安局依法冻结周玉齐名下的招商银行卡 XXXXXXXXXXXXXXX 内的余额 776.35 元。

（7）案发后，惠州市公安局依法冻结周玉齐名下的工商银行账号 XXXXXXXXXXXXXXXXXX 内的余额 20077.53 元。

（8）案发后，惠州市公安局依法冻结惠州市艺商文化投资发展有限公司名下的广发银行账号 XXXXXXXXXXXXXXXXX 内的余额 4537 元。

4、中国银行业监督管理委员会惠州监管分局出具的函件：惠州市艺商文化投资发展有限公司的“P2P”网络平台未向该分局申请注册。

5、“艺商贷”P2P 网络平台借贷项目宣传资料、借款承诺书及房产证、人民币卡在线支付服务协议、易瑞通平台使用协议、投标成功待收利息记录表、投标全返款步骤说明、投资者通过线下充值奖励记录表及继续投标奖励表等：周玉齐通过上述网络平台以高息吸收投资的情况。

6、银行账户交易明细资料：（1）周玉齐名下的农业银行账户 XXXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXX 及 XXXXXXXXXXXXXX 的交易情况，该三个银行账户于 2015 年 11 月 4 日的余额分别为 682.26 元、579.66 元及 0 元。

周玉齐名下的建设银行账户 XXXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXXX、XXXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXXXXX 及 XXXXXXXXXXXXXXXXXX 的交易情况，该六个银行账户于 2015 年 11 月 3 日的余额分别为 21.73

元、28.22 元、19.67 元、0 元、0 元、及 0 元。

周玉齐名下的光大银行账户 XXXXXXXXXXXXXXXX 的交易情况，该账户于 2015 年 11 月 4 日的余额为 500.3 元。

周玉齐名下的中国银行账户 XXXXXXXXXXXX、XXXXXXXXXXXX、XXXXXXXXXXXX、XXXXXXXXXXXX 的交易情况，该账户于 2015 年 11 月 3 日的余额为 877.69 元、0 元、73.32 元、22.72 元。

周玉齐名下的招商银行账户 XXXXXXXXXXXXXXXX 的交易情况,该账户于 2015 年 11 月 3 日的余额为 776.35 元。

周玉齐名下的工商银行账户 XXXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXXXXXX 及 XXXXXXXXXXXXXXXXXX 等的交易情况，该四个银行账户于 2015 年 11 月 3 日的余额为 20077.53 元、465.86 元、1411.98 元及 234.86 元。

周玉齐名下的广发银行账户 XXXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXXXXXX 等的交易情况，账户于 2015 年 11 月 5 日的余额为 5049.79 元、5.66 元、1.04 元及 20.98 元。

（2）惠州市艺商文化投资发展有限公司名下的广发银行账户 XXXXXXXXXXXXXXXXX、XXXXXXXXXXXXXXXXX 等的交易情况,该二账户于 2015 年 11 月 5 日的余额为 4537 元、37.53 元。

（3）证人赖某锋名下的招商银行账户 XXXXXXXXXXXXXXX 的交易情况,于 2015 年 10 月 13 日的余额为 0.38 元。

7、上诉人周玉齐提供的会员投资目录表：周玉齐尚欠 180 名客户的本金计 2188.419102 元。

上诉人周玉齐经辨认，对上述资料确认无误。

8、股票账户交易明细资料：（1）2012 年 11 月至 2015 年 11 月,周玉齐名下的光大证券股票账户 XXXXXXXX、融资融券账户 XXXXXXXX 的交易情况，该二账户于 2015 年 11 月 4 日的资金余额分别为 101.74 元、1789.51 元，市值合计均为 0。

（2）2009 年 11 月至 2016 年 3 月，周玉齐名下的长江证券股票账户 XXXXXXXX 的交易情况，该账户于 2016 年 3 月 23 日的资金余额及资产总值均为 0。

（3）2015 年 6 月至 2016 年 3 月，周玉齐名下的中信证券股票账户 XXXXXXXXXXX 的交易情况，该账户于 2016 年 3 月 23 日的资金余额及资产市值均为 0。

（4）1996 年 6 月至 2016 年 3 月，周玉齐名下的广发证券账户 XXXXXXXX 的交易情况，该账户于 2016 年 3 月 23 日的资金余额及资产总值均为 109.62 元。

9、惠州市房屋权属查询信息、广东省房屋买卖合同、销售不动产发票、商品房买卖合同等：（1）惠州市环城西二路 XX 号 XX 大厦 XXXX 号商铺的所有权人为周玉齐。

（2）2015 年 10 月 9 日,周玉齐、刘某婷与姚某虹签订房地产买卖合同,约定周玉齐、刘某婷将惠州市下埔大道 X 号 XX 大厦 XXXX、XXXX 房转让给姚某虹，合同约定的转让价分别为 88 万元、95 万元,发票的计税金额分别为 102.46 万元、110.62 万元。

（3）2014 年，周玉齐与惠州白鹭湖旅游实业开发有限公司签订商品房买卖合同，约定周玉齐向对方按揭购买惠州市惠城区 XX 镇 XXX 大道 X 号房，房价计 185 万元。

（4）惠州市 XX 路 X 号 XX 花园 X 号房的所有权人为袁某辉，抵押权人为广发银行惠州文华路支行；惠州 XXX 路 X 号房的所有权人为叶某党；惠州市惠城区 XXXXX 路 X 号房的所有权人为严某华；惠州市 XXXXXX 路 X 房的所有权人为余某春。

惠州市 XXX 号小区 X 号房及惠州市 XXXXX 路 X 号房均非有效地址。

10、户籍证明资料：周玉齐的个人身份情况。

11、企业机读档案登记资料、公司年检报告书（2012 年度）、资产负债表等：（1）惠

州市艺商文化投资发展有限公司成立于 2012 年 8 月 24 日，法定代表人为周玉齐，股东为周玉齐（占股 80%）、刘某婷（占股 20%），注册资本为 500 万元，经营范围原为视光保健仪器（许可经营项目）、商业贸易投资、实业投资、商务信息咨询与经济信息咨询服务、网络技术服务及销售乐器、工艺品、眼镜；后于 2013 年 8 月变更为商业贸易投资、实业投资、投资管理、资产管理、商务信息与经济信息咨询服务、电脑、网络技术服务及教育咨询服务。惠州市艺商文化投资发展有限公司于 2013 年 6 月 19 日出具的公司年检报告书（2012 年度）显示，该公司全年销售收入、全年利润总额、全年净利润、全年亏损额、年末负债总额等均为 0，年末资产总额为 2 万元。

（2）惠州市惠城区喜悦琴行成立于 2009 年 8 月 24 日，经营者为周玉齐，经营资金 3 万元，经营范围为批发、零售乐器及乐器指导。

（3）惠州市惠城区喜悦琴行 XXXX 店成立于 2009 年 3 月 11 日，经营者周玉齐，经营资金 1 万元，经营范围为销售乐器。

（4）惠州市学琴在线文化传媒有限公司成立于 2015 年 6 月 16 日，法定代表人、股东为周玉齐，注册资本 1000 万元，经营范围为互联网传播技术、互联网游戏及娱乐技术、广播影视娱乐技术、视频制作技术等文化及娱乐产品的技术开发、咨询、服务及转让等。

（二）证人证言

1、证人刘某婷的证言：惠州市艺商文化投资发展有限公司由我丈夫周玉齐一手建立，他是该公司的法定代表人，他和我各自出资 400 万元及 100 万元。我没有参与该公司的日常管理，也不清楚该公司的日常运营情况。我知道周玉齐创建了“艺商贷”P2P 网络借贷平台，但不清楚该平台如何运营，也不清楚周玉齐吸收的资金的流向。周玉齐平时不赌博，但是有炒股。我不清楚周玉齐炒股的资金来源及数额。惠州市惠城区喜悦琴行的法定代表人是周玉齐，分别有两个点，前者主要销售乐器，后者主要负责教学。喜悦琴行的日常管理全部由我负责。喜悦琴行主要依靠销售乐器及教学收费维持日常经营。艺商公司员工江某凤会帮喜悦琴行做广告宣传及网络、微信推广。喜悦琴行与艺商公司没有经济往来，但是周玉齐有时会拿走琴行收取的学费，他一共从喜悦琴行拿走了大约 20 万元。周玉齐因涉嫌非法吸收公众存款，于 2015 年 10 月 13 日向公安机关投案自首后，喜悦琴行就暂停营业了，目前尚欠学生家长大约 25 万元学费。

周玉齐于 2014 年底左右贷款购买了惠州市惠城区 XX 镇 XXX 大道 X 号房，他在惠城区 XX 电子城还有一个小档口，现出租给他人销售电子产品。

2、证人赖某锋的证言：我于 2013 年 1 月至 3 月在惠州市艺商文化投资发展有限公司做琴行网站推广，2013 年 3 月至今担任该公司客服主管。我公司的法定代表人及老板是周玉齐，主要下设客服部，工作人员包括罗某勤、孙某宜、吕某静及文某莉，钟某洪是兼职技术人员，江某凤负责琴行的推广。

我公司主要通过“艺商贷”网站(ysdai.cc)做汽车、房产的抵押贷款业务。平时，周玉齐提供汽车行驶证、登记证、驾驶证及房产证、他项产权证等复印件给客服部,由我负责把上述复印证件展示至我公司的 QQ 群内,并根据周玉齐提供的“艺商贷”网站借款需求信息发布给客户。客户根据我发送到“艺商贷”网站的资料，自己选择投资。客户先在“艺商贷”网站通过汇潮、贝付、宝付等第三方支付平台充值,再进行投标,投标后经我公司客服部复审,投标复审通过后生效,生效后我公司在网站上生成对应的电子合同,我们在网站上将这种业务称为 P2P 互联网金融。客户在汇潮、贝付、宝付等第三方支付平台充值后的款项由第三方在每天 10 时及 16 时的两个时间段结算给周玉齐。我不知道周玉齐提供的汽车行驶证、登记证、驾驶证及房产证、他项产权证等复印件的来源及其内容是否真实，我没有见过原件。大约 380 名客户投资至“艺商贷”网站的 P2P 业务的金额大约计 2000 万元。客户从周玉齐处按照月收取利息，月息从 2.85%至 3.5%不等。我不清楚周玉齐将客户投资款用于何处。周玉齐

向公安机关投案自首后，我公司已停止运营，“艺商贷”网站业务已停止。

3、证人罗某勤的证言：我于2013年10月至今担任惠州市艺商文化投资发展有限公司客服。我公司的大股东、小股东分别是周玉齐、刘某婷，实际控制人是周玉齐，刘某婷很少来公司，几乎不参与公司的运营管理。我主要负责在一些“网贷之家”、“网贷天眼”等投资类网站、论坛或投资者QQ群宣传我们的“艺商贷”网络借贷平台的收益，吸引投资者前来投资。除了股东，我公司一共有7名员工，赖某锋主要负责管理孙某宜、吕某静、江某凤、文某莉等客服，及与一些第三方广告平台商谈业务、做广告宣传。孙某宜还负责记账，她垫钱支付平时我公司采购的物品，再持单据向周玉齐报销。吕某静负责电话推广宣传，江某凤负责琴行、微信推广，文某莉负责广告设计。钟某洪负责兼职维护我公司的网站。我公司财务都是由周玉齐负责，连水电费都是他自己交纳的。我们不知道公司资金的去向。我们不清楚“艺商贷”网站吸收的资金存在何处，只有周玉齐才知道。我们客服平时负责做推广、拉投资，周玉齐负责制作“艺商贷”网站的“标”（“艺商贷”网站发布的“标”的最高利率是51.8%，最低是28.2%，一般为30%左右。这些“标”最多的是房产抵押标，其次是“约标”。“约标”是指投资者直接找到我们客服，双方约定利率并经周玉齐同意后，我们在“艺商贷”网站发布“约标”，这个“约标”是设定密码的，只有投资者才知道密码，才可以中标。“约标”的投资者不知道资金的用途，周玉齐教我们说如果投资者询问，就回答“约标”资金将会匹配至合适的投资者手上。“约标”的年利率比普通月标高一点，“约标”的实际年利率一般为41%左右，月标为32%左右。普通月标一般都是房产抵押标。），投资者到我们的网站投资。我们都不知道这些“标”用于什么项目。周玉齐告诉我们,如果投资问我们这些投资资金用于何处，就回答不知道，如果要看就要到我公司来看，所以无论是我公司员工，还是广大投资者都不知道这些资金的去向。直至周玉齐向公安机关投案自首时，他打电话给我，我才知道原来资金几乎都被他用于股市。我之前知道周玉齐很会炒股，但不知道他的炒股资金是“艺商贷”网站吸收的资金。周玉齐平时的经济是比较宽裕的，他以前开比亚迪小汽车，2015年初换了一辆奔驰小汽车，但从6月开始又换回了原来的比亚迪小汽车。

4、证人孙某宜的证言：我于2014年11月担任惠州市艺商文化投资发展有限公司客服。我公司的大股东、小股东分别是周玉齐、刘某婷，实际控制人是周玉齐。刘某婷平时很少来公司，只是偶尔到公司打印资料，几乎不参与公司的运营管理。除了股东，我公司一共有7人。我和吕某静、文某莉都是客服。赖某锋和罗某勤平时管理我们客服。江某凤负责琴行的微信推广。

我们客服的工作主要是每天通过QQ与投资者交流、解答问题。每天早上，赖某锋和罗某勤都会发一份公告给我们,公告上面有当日准备发布的标的信息,我们将这份公告转发至我公司的3个投资者群,并在发标时间到达时,将投资标的的网站链接发送至投资者群。其他的我不知道。我不清楚3个投资者群一共有多少个账号，应该超过1500个。我们每天发布的公告上主要是当日要发的“标”的资金数额、年收益率、奖励、“标”的类型、当日预计发“标”时间等信息，待时间一到，我们就会将这个“标”的网站链接添加在公告后面。我不清楚这些标的信息是否真实、是谁制作的、“艺商贷”网站吸收的资金数额及流向等。我还负责我公司的日常采购及因公误餐的财务记账，我不清楚我公司的财务由谁负责。我公司要一次5万元以上的投资才能“约标”。我做过几次“约标”，就是投资者找到我说要投资多少钱，我再将投资金额的截图发给赖某锋及罗某勤，他们会发一个投标的链接给我（上面有“约标”的密码），我再发送给投资者。

5、证人吕某静的证言：我是惠州市艺商文化投资发展有限公司的客服。我公司的法定代表人、老板是周玉齐。我公司下设客服部，客服部的负责人是赖某锋，工作人员包括罗某勤、孙某宜、文某莉及我。我公司创建了“艺商贷”网站并经营P2P网贷业务,没有经营其他业务。赖某锋在“艺商贷”网站发布标的信息,再由我们客服部复制信息并发送到3个QQ

群（约计 1400 多人）,让“艺商贷”网站的客户进行选择。客户看中标的后到“艺商贷”网站投标,待标的投满以后，我公司按每个客户投标的金额支付利息。我们将我公司的账户发送给投资者，投资者通过我公司账户直接进行充值。我们在 QQ 群上发布的标的都是房产抵押标及汽车抵押标，以及这些标的年利率及奖励金额。我公司根据客户的投资金额乘以年利率、奖励计算利息。我不知道“艺商贷”网站上发布的标的信息是否真实。

6、证人钟某洪的证言：2012 年初左右，当时周玉齐还没有成立惠州市艺商文化投资发展有限公司，我在喜悦琴行做了几个月网站设计，之后因工资低而辞职。2014 年底，周玉齐打电话问我是否想到他的艺商公司兼职做网站维护。我在艺商公司负责维护“艺商贷”网络借贷平台及喜悦琴行的网站。我不清楚艺商公司平时如何运作。

7、证人姚某虹的证言：我是惠州市保信实业发展有限公司的法定代表人。周玉齐是教钢琴的，我小孩以前到他那里上过钢琴课。周玉齐至少欠我丈夫郭某 130 万元，这是有借条的，他应该欠郭某 200 多万元。借条是郭某与周玉齐签订的，债权人签的是我的名字。2015 年 10 月，周玉齐将惠州市惠城区 XX 大厦 XXXX、XXXX 房过户给我以抵偿债务。郭某对我说，周玉齐还不了钱，就用上述 3002、3003 房抵债。

证人姚某虹提供的借条二份，证实周玉齐分别于 2013 年 5 月 11 日、2014 年 4 月 9 日向姚某虹借款 80 万元、50 万元，借款期限分别为 180 天、360 天，担保人均为刘某婷。

8、证人郭某的证言：2000 年左右，我在惠州市开设一家西餐厅，当时周玉齐到我餐厅应聘担任了一年多的钢琴师，我们成为了朋友。2006 年以来，周玉齐陆续向我借钱（用途不详），期间有借有还，借款期限最短的有一两个月，最长的有 2、3 年，利息一般是月息 2 分，2015 年 10 月，因周玉齐无法偿还一笔 80 万元及一笔 50 万元的欠款，他自愿以惠州市惠城区 XX 大厦 XXXX、XXXX 房抵债并过户至我妻子姚某虹名下。周玉齐目前至少尚欠我 50 万元本息。

（三）被害人的陈述

1、被害人王某凤的陈述：2013 年 2 月,我在“网贷之家”与一些朋友通过 QQ 聊天时，了解到“艺商贷”网络借贷平台,并在该平台尝试投资两、三千元，觉得效益不错。2014 年 4 月，我卖房后投资于“艺商贷”网络借贷平台，当时应该投资了 70 多万元。之后，我陆续向亲戚借钱投资，但到了 2015 年 10 月 10 日无法提现。后来，我听说“艺商贷”网络借贷平台的老板周玉齐逃跑了。我在“艺商贷”网络借贷平台一共投资 448.0123 万元,包括股权投资 5 万元，实际提现 226.2541 万元，账面待回收本息 264.7367 万元,净损失 221.7582 万元本金。我不认识周玉齐，但是我如果有不清楚的问题，会打电话问他或赖某锋。我一直以为周玉齐将“艺商贷”网络借贷平台吸收的资金用于艺术投资，因我投的大部是艺术支持标，而且“艺商贷”网络借贷平台的投资奖励经常是一些乐器，直到周玉齐被公安机关拘留之后，我才知道他原来将这些资金用于股市。

2015 年 9 月 1 日以来,“艺商贷”网络借贷平台推出三周年庆祝活动,每天都会发布一个 120 万元的“秒标”,只要一投标马上能得到千分之三的奖励,但是奖励不能提现出来,一定要继续投“月标”后才能提现,但是 10 月 10 日后该平台就无法提现。另外，2015 年 9 月 29 日以来,“艺商贷”网络借贷平台发布股权认购 2 千万元,说是“艺商贷”网络借贷平台入股 XXX 乐器制造公司,二年内要上新三板。我投资的年利率以前一般是 18%左右，从 2015 年 9 月开始提至 22%左右。

2、被害人黎某辉的陈述：2014 年初，我在网上偶然了解到“艺商贷”网络借贷平台，并逐渐在上面增加资金进行投资，后来逐渐撤了出来。2015 年 6 月，“艺商贷”网络借贷平台更换系统后，我的本金固定只投入 8 万元，所得利息全部当月提出，但到了 2015 年 10 月 10 日就无法提现了。“艺商贷”网络借贷平台目前尚欠我 80000 元本金、12703 元利息。我一直以为周玉齐将“艺商贷”网络借贷平台吸收的资金用于艺术投资，因我投的标几乎是

艺术支持标，直到周玉齐被公安机关拘留之后，我才知道他原来将这些资金用于股市。2015年9月1日以来,“艺商贷”网络借贷平台推出三周年庆祝活动,每天都会发布一个120万元的“秒标”,只要一投标马上能得到千分之三的奖励,但是奖励不能提现出来,一定要继续投“月标”后才能提现,但是10月10日后该平台就无法提现。另外，2015年9月29日以来,“艺商贷”网络借贷平台发布股权认购2千万元,说是“艺商贷”网络借贷平台入股XXX乐器制造公司,二年内要上新三板，如果上不了市，承诺投资满两年以总价款的15%的溢价及本金进行回购。我投资的年利率最高是48%左右，一般为36%左右。

3、被害人储某新的陈述：我从2015年5月22日开始在“艺商贷”P2P网络借贷平台注册帐户，一共投资289017元本金,利息为2971.62元。2015年6月22日至10月8日，我一共提现213085.03元，尚有87095.57元本息待付。“艺商贷”P2P网络借贷平台在网上发布秒标、一个月标、三个月标、六个月标及十二个月标，每个标的年利率为18%至22%不等，另外按照不同标的一次性有1%至6%的奖励。投资秒标有0.3%的奖励，但奖励不能立即提现，只有通过投资月标到期后才能提现。我投资的标的没有具体标的物,网络上的借款人的姓名、公司名称等重要信息都被模糊处理了,房产证、行驶证等资料也以保密为由不能查询。我在“网贷之家”看到“艺商贷”P2P网络借贷平台经营时间长、利息高、信誉好所以才投资。另外，2015年9月，“艺商贷”P2P网络借贷平台大力宣传入股即将上市的XXX乐器制造公司。2015年10月12日,周玉齐在“艺商贷”P2P网络借贷平台称平台正在维护,不能操作。我听QQ群的其他投资者说“艺商贷”P2P网络借贷平台吸收的资金被周玉齐拿去炒股了。

4、被害人彭某民的陈述：2015年7月24日，我经朋友介绍在“艺商贷”P2P网络借贷平台注册了一个账户并存入3万元。但到了2015年10月8日，“艺商贷”P2P网络借贷平台的账户无法登陆，网站上说机房正在维护。过了两三天，我听其他投资者在QQ群里说周玉齐投案自首了，还说我们的投资款被他挪作他用了。

5、被害人徐某的陈述：2015年初，我朋友向我介绍说“艺商贷”网络借贷平台的投资收益高，运作稳定，并有实体店喜悦琴行。该平台宣传本息提现有保障，并已入股即将上市的知名钢琴制造企业XXX乐器（营口）有限公司。我加入“艺商贷”网络借贷平台的官方投资QQ群并了解到该平台已正常运作近三年，且提现及时，就从2015年7月10日以来投资了四个月标（满一个月返还本息，利率为18%至22%不等），计40万元，并于9月15日提取209158.5元本息。当时我分四次将这40万元转账至周玉齐个人的招商银行账户6228481134810832119。我投资的标的没有具体的标的物。“艺商贷”网络借贷平台标注投资用于借贷给第三方进行资金周转，称第三方有房产、汽车等实物抵押并公布了房产证或车辆行驶证，但是证件上的名字会被处理，看不清楚。10月12日，“艺商贷”网络借贷平台停止支付本息。我从QQ群了解到资金被周玉齐用于股市及经营惠州市喜悦琴行。

6、被害人段某建的陈述：我于2013年在“网贷之家”看到“艺商贷”网络借贷平台的广告后开始投资，一开始投资金额很小，后我于2015年5月到惠州市艺商文化投资发展有限公司实地考察后，觉得该平台还是比较安全的，投资金额才增多。我通过第三方支付平台充值至“艺商贷”网络借贷平台，年化收益率一般为28%左右，但我只投一月标，所以收益率会低一点。我到惠州现场考察时，“艺商贷”网络借贷平台向我解释说投资款用于正常的借贷，赖某锋、罗某勤还向我出示了一些借款人的合同及抵押红本。周玉齐被抓后，我才知道他将投资款用于股市。我早期在“艺商贷”网络借贷平台曾看到几个投资项目的相关资料，后来就看不到了。我还有大约78000元本息尚未提现。

7、被害人张某华的陈述：2013年4月，我根据QQ客服发送的网络链接及邀请，开始在惠州市艺商文化投资发展有限公司的“艺商贷”网络平台投资。截至2015年10月，我陆续投资1042867元本金，期间取回40多万元本金，尚有60多万元本金未能取回。因为“艺

商贷”网络平台的投资回报比较可观，年利率大约为30%，而且网站上也显示出有多个琴行等实体，当时我认为是比较可靠的。“艺商贷”网络平台平时宣传的抵押物包括房产、汽车（我没有看过实物，只是看到一些复印件或图片说明），以及准备在全国布局开多家琴行，于2015年9月还宣传入股XXX公司，鼓励投资人购买股权，并计划于2015年10月17日开股东大会等。“艺商贷”网络平台在网站上推出1月标、2月标、3月标等，并让投资者进行投标。我们通过网站充值和线下充值方式投标，前者是通过网银转账至“艺商贷”网络平台，后者是直接转账至周玉齐名下的招商银行账户6212867525299338。“艺商贷”网络平台的客服说投资款用于借给别人或投资于琴行。2015年10月10日，客服以机房故障为由停止提现。12月12日，客服通知我“艺商贷”网络平台的老板周玉齐已向公安机关投案自首，我才知道被骗了。

8、被害人柳某的陈述：2014年2月，“艺商贷”网络平台宣传称为惠州当地企业募资，并以月息3.7%回报投资者，20万元以上的投资者设为VIP客户并有适当奖励；该平台老板周玉齐在网上大力宣扬该平台入股XXX公司并以1万元/份销售2000份股权，计划两年内在新三板上市，如果不能上市两年后按照1.6元/股回购，五年计划主板上市，还准备在全国各地设立分支机构，所吸收的资金部分用于“艺商贷”网络平台名下的琴行的投资经营等，而且该平台运营的时间近三年，所以我就投资了。我先后投资4925705元，提现3893729元本息，尚欠1096307.51元本息。2015年10月10日，“艺商贷”网络平台称出现机房故障，正在维修。

9、被害人付某的陈述：2015年10月初，我在网上发现惠州市艺商文化投资发展有限公司的P2P网络平台有理财产品，网上承诺保证支付本息，年化利率根据投资产品的不同为18%、22%。我于2015年10月6日、8日分别投资1000元及10万元至周玉齐个人的工商银行账户6222082008001127461，在“艺商贷”网络借贷平台一共投资了2个房产抵押借贷产品一月标、3个房产抵押借贷产品六月标等5个投资产品。10月12日，我发现“艺商贷”网络借贷平台服务器无法开启，便联系投资QQ群的管理人员，对方称“艺商贷”网络借贷平台正在维护中。我听QQ群的投资者反映，周玉齐将大部分资金投资至股市。10月6日，我在网站看到艺商公司发布股权认购2000万元，并将于10月17日在惠州市皇冠假日酒店召开股权认购大会。周玉齐被抓后，我到惠州市皇冠假日酒店询问时，对方反映没有艺商公司开会的事情。

10、被害人杜某松的陈述：我于2014年经朋友介绍得知了“艺商贷”网络借贷平台，于2015年9月6日在该网站注册并存入22500元（其中2万元转至该网站老板周玉齐名下的工商银行账户XXXXXXXXXXXXXXXXXXX）。10月8日，“艺商贷”网络借贷平台的账户不能正常登陆，网站上说机房正在维护。过了大约2、3天，我听其他投资人说周玉齐向惠州市公安局自首了，还说他把我们的投资款都挪作他用了。我不清楚周玉齐将投资款挪用至何处。“艺商贷”网络借贷平台会审核一些需要借贷的商家的资料，再以标的形式放在网上，投资者看见后按照网上资料及该平台所称的审核情况来投标，但是需要投资者先注册，充值后才能进行投标。

11、被害人吕某加的陈述：我从网上了解到惠州市艺商文化投资发展有限公司的情况。艺商公司将很多标的放在“艺商贷”网站上供客户选择投标。客户先从网上了解投标标的，选中后点开项目，再将资金转至项目下面。我们在网站上只看见投标物品的相关证件，从来没有看到过实物。我在艺商公司投资的资金分为两部分：一部分是履行完合同的待提资金48955.08元，另一部分是正在履行中的19个合同金额123154.74元（一些项目是公司需要资金周转，一些项目是公司需要资金采购原料、新设备或装潢等），共计172109.82元。我通过银行卡从网上支付投资款。我投资的都是一个月的短期投资，年利息为16%至22%不等。2015年10月11日，我发现“艺商贷”网站停止运转。

12、被害人邓某金的陈述：我从惠州市艺商文化投资发展有限公司在网上发布的情况了解到，该公司经营平台已有 2 年多时间，支付的利息比较高，月利率为 3.2%。艺商公司设立了一个一定数额的月标，由投资者进行竞投，投资金额满额后投标结束，一个月后就可以提取本息。我从艺商公司的投资平台了解到，该公司吸收投资款后用于其他公司的资金周转，从而赚取利息差价。我通过网上银行转账充值 2 万元至艺商公司提供的银行账户。我们参加投标时没有实物。2015 年 10 月 14 日，艺商公司的投资平台显示正在维护中，无法提现。我通过投资人 QQ 群了解到艺商公司的法定代表人周玉齐已向公安机关投案自首。

13、被害人梁某丽的陈述：我在网上发现惠州市艺商文化投资发展有限公司的网络投资平台，便于 2014 年 9 月 18 日至 2015 年 10 月 8 日多次通过线上三方支付及线下充值的方式投资计 50359 元（我用信用卡通过线上支付功能充值至“艺商贷”网站，用银行卡转账充值至该网站提供的周玉齐名下的一个工商银行账户 XXXXXXXXXXXXXXXXXX）。后来，我发现平台关闭了。“艺商贷”网站标注将我们的投资通过抵押借贷给其他个人或企业，并承诺年回报率为 18%至 22%。投资到期后，“艺商贷”网站会将本息显示在我的账户上，如果我要提现，“艺商贷”网站会通过赖某锋的光大银行账户 XXXXXXXXXXXXXXX、招商银行账户 XXXXXXXXXXXXXXX 转账至我的银行账户。每次投资后，“艺商贷”网站都会提供一份借款协议给我下载，协议上有借款人或者借款公司等信息，并称每笔借款均有抵押，但其抵押的资料均以保密为由未能查询详细信息，我不清楚是否有真正的借款人及有无抵押物。我一般发送咨询问题至“艺商贷”网站的客户 QQ 群，会有客服回答我的问题。“艺商贷”网站于 2015 年 9 月以来开展一些活动：1、以庆祝成立三周年庆典为由每天发送秒标，收益为每天万分之三十五。2、续投 6 个月或以上的月标送 5000 元现金或 1 台苹果 6 手机。3、为庆祝 10 月 17 日股权认购会议顺利召开，10 月 1 日至 17 日每天发布秒标。4、2015 年 10 月左右，宣扬该网站将入股 XXX 公司，并以 1 万元/股销售股权，并称上市将以 1.6 倍的价格回购股权。

（四）鉴定意见

惠州市 XX 会计师事务所有限公司出具的审计报告：1、2015 年 5 月 1 日至 10 月 14 日，周玉齐通过“艺商贷”P2P 网络借贷平台非法集资产生的充值（本金）金额计 44936676.21 元，提现金额计 22839715.2 元，未付金额计 22216170.62 元，涉及 445 名借款人。

2、期间，周玉齐通过个人银行账号向“艺商贷”P2P 网络借贷平台借款人非法吸收集资款 33224456.90 元，吸收其他单位和个人流入款项 14479696.35 元，吸收其他资金流入 5560075.10 元，流入总计 53264228.35 元。周玉齐通过个人银行账号支付借款人款项 34643538.52 元，支付其他单位和个人款项 18592970.85 元（其中支付惠州市艺商文化投资发展有限公司 2378600 元,支付各项费用开支（包括个人消费）566780.04 元），流出总计 53236509.37 元。流入减流出的净额为 27718.98 元。

3、依据周玉齐个人的银行账号和惠州市艺商文化投资发展有限公司的银行账号银行流水资料显示，截止至所有账户最后交易日期，银行存款余额合计 27718.98 元。其中，周玉齐个人的银行账户存款余额为 23144.45 元，惠州市艺商文化投资发展有限公司的银行账户存款余额为 4574.53 元。

4、期间，周玉齐的光大证券股票账户（账号：XXXXXXXX）盈利 637172 元，其融资融券账户（账号：XXXXXXXX）亏损 25888123 元，合计亏损 25250951 元。

（五）上诉人的供述及辩解

上诉人周玉齐的供述及辩解：我于 1993 年至 2001 年在惠州市惠城区 XX 局工作，2001 年至 2003 年待业，2003 年至今一直从事音乐培训及乐器销售。

2012 年 8 月，我与我妻子刘某婷设立了惠州艺商文化投资发展有限公司。2013 年 2 月，我以惠州艺商文化投资发展有限公司的名义创建“艺商贷”P2P 网络借贷平台。艺商公司的

法定代表人及老板是我，刘某婷不参与管理公司，她只是挂干股，负责看管惠州市喜悦琴行。我公司一共有 9 人,主要分为运营部和客服部。其中运营部由我、赖某锋和罗某勤，客服部有钟某洪、孙某宜、吕某静、孙江凤及文某莉。我负责我公司的所有业务。赖某锋和罗某勤负责帮我处理我公司内部事务。

我当初成立艺商公司主要有两个原因：一是助推我的琴行事业,二是想通过艺商公司的名义创建“艺商贷”P2P 网络借贷平台,涉足互联网金融行业。2012 年，我在琴行协会聚会时发现很多琴行在运营过程中需要资金,大家都觉得如果有一个 P2P 平台提供资金支持,会促进琴行事业发展,所以我开始产生成立“艺商贷”P2P 网络借贷平台的想法,也想利用该平台筹集资金用于促进自己的事业发展。“艺商贷”P2P 网络借贷平台经营的业务未经相关金融部门审批。

“艺商贷”P2P 网络借贷平台从 2013 年开始向客户吸收资金。客户先通过“艺商贷”网站注册账户并成为会员,再通过第三方支付平台转账至我个人的银行账户,一部分资金由客户直接转账至我个人的银行账户。不同的标的的回报率有所不同,年回报率为 24%至 72%,大部分为 40%左右（月息大约为 2 分多到 5 分多）。“艺商贷”P2P 网络借贷平台的标的主要是音乐艺术支持标、钢琴乐器标、汽车抵押标、房产标及“约标”等（“约标”是指投资者先与我协商好投资回报率后,我按照约定设定好密码并发标后由投资者投资），音乐艺术支持标及“约标”的数量最多。这些标绝大部分由我公司发出,一小部分由一些通过审核的借款者发出。我公司在“网贷之家”等做宣传，投资者据此获知招标信息。大部分标的内容都是虚构的。我将房产、汽车等的证件复印件或照片发放到“艺商贷”P2P 网络借贷平台来发布标的。这些证件复印件或照片小部分是真实的，大部分是虚假的。其中一些是我自己通过朋友弄来的，一部分是我叫赖某锋弄来的。我将投资者的资金大部分用于股市,一小部分用于我公司的日常周转。

“艺商贷”P2P 网络借贷平台吸收的资金都是转账至我个人的光大银行账户 XXXXXXXXXXXXXXXX 、招商银行账户 XXXXXXXXXXXXXXXX 、工商银行账户 XXXXXXXXXXXXXXXXXX 、建设银行账户 XXXXXXXXXXXXXXXX 及农业银行账户 XXXXXXXXXXXXXXXXXX。用于股市交易的投资资金都是先转账至我的中国银行卡 XXXXXXXXXXXXXXXXXX，再用于股市投机。我用于股市投机的金额约计 1800 万元。当时我想通过股市赚钱来偿付投资者的本息。

我从 2013 年开始通过股市操作来还本付息，2014 年初开始融资融券，2015 年 6 月中旬加大了融资融券杠杆。2015 年 6 月，我因遭遇股灾而亏损严重。当时，我的股票市值约 9000 万元（其中本金 3000 万元，融资 6000 万元）。2015 年 9 月，我将市值约 9000 万元的股票全部抛光,剩余现金 400 万元,其中 220 多万元用于支付广发银行的房产抵押贷款（惠州市惠城区 XX 大厦 XXXX、XXXX 房）,余款用于支付投资者的本息。在此之后，我继续吸收投资者的资金，我想挽救公司并继续经营，并有还款计划：1、我公司与 XX 软件公司合作开发互联网音乐现场教学视频网站并收取学费；2、我公司入股 XXX 乐器制造公司；3、喜悦琴行的运营收入可以还款给投资者。我的光大证券股票账户现在没有任何股票及余额。2015 年 9 月，当时我在银行最后还有大约 100 万元，我都支取出来并还款给彭某胜、曾某光等惠州朋友。我没有银行存款了。我最后一次偿还投资者的本息是 2015 年 10 月 9 日。

“艺商贷”P2P 网络借贷平台的投资者有 300 多人，截止至 2015 年 10 月 14 日的投资本金计 1800 多万。我先后支付 5000 万元利息。我向公安机关提供的会员投资目录表上的 180 个会员、投资金额计 2188.419102 万元是真实的。2015 年 10 月初，我将惠州市惠城区 XX 大厦 XXXX、XXXX 房抵债过户给债权人姚某虹（我欠她 130 多万元）。我个人的其他借款还有大约 150 万元。

2015 年 9 月 1 日，我的股票已经亏空，“艺商贷”P2P 网络借贷平台的投资者每天都

要提现，但我公司没有资金支付，为了留住投资者的现金不被提现，让我公司能够继续运营，我就推出三周年庆祝活动，每天发布一个120万元的“秒标”让投资者继续投资，以留住资金，避免投资者提取现金（如果投资者没有投够，我公司会用数据投满，以实现“秒标”活动成功）。2015年3、4月，我和XXX乐器制造公司的法定代表人尹总谈好，我公司投资2000万元入股XXX公司，占股30%。之后，我在“艺商贷”P2P网络借贷平台发布这个信息，让投资者参与投资入股。但是，我公司没有成功入股XXX公司。XXX公司两年内要上新三板，是我和尹总设想的计划。

我按揭购买的一栋别墅（月供8800多元）尚未取得房产证。我名下的一部比亚迪电动小汽车（粤BDD442）在我投案自首前已被债权人姚某奎开走了。我按揭购买的一部奔驰小汽车（粤XXXXXX）在2015年7月卖给了他人。我名下还有惠州市环城西二路X号商铺。

上诉人周玉齐经辨认，对借款承诺书、个人信用报告、房产证等资料确认无误。

关于涉案审计报告能否作为证据采信的问题。经查，涉案审计报告系由具有相关审计资质的审计机构根据合法的审计数据、法定程序经审计作出，审计结论合法、有效，且与上诉人周玉齐自认的其尚欠投资者的资金数额相近，足以采信。周玉齐及其辩护人辩称不能采信涉案审计报告理据不足，不予采纳。

关于上诉人周玉齐的罪名认定问题。经查，在案证据足以证实周玉齐违反国家金融管理法律规定，未经有关部门依法批准，编造并通过网络发布借款人、借款项目等虚假信息，以支付高额回报为诱饵，非法吸收社会公众的大量资金，集资后亦未用于实际的生产经营活动而主要用于个人炒股，其在因炒股而造成巨额亏损的情况下仍继续向社会公众非法集资，致使不能及时返还集资款，且案发至今，其始终没有偿还债务的强烈意愿及实际行为，足见其非法占有他人财物目的明显。原判认定其构成集资诈骗罪依据充分。周玉齐及其辩护人认为原判对周玉齐定罪不当理据不足，不予采纳。

本院认为，上诉人周玉齐违反国家法律，以非法占有为目的，使用诈骗方法非法集资，数额特别巨大，其行为已构成集资诈骗罪。周玉齐犯罪后主动投案，并如实供述其主要的犯罪事实，系自首，依法可以从轻处罚。原判认定事实清楚，证据确实、充分，定罪准确，量刑适当，审判程序合法。周玉齐及其辩护人所提上诉、辩护理由均不成立，不予采纳。依照《中华人民共和国刑法》第一百九十二条、第六十七条第一款、第六十四条，《最高人民法院关于审理非法集资刑事案件具体应用法律若干问题的解释》第四条、第五条及《中华人民共和国刑事诉讼法》第二百二十五条第一款第（一）项之规定，裁定如下：

驳回上诉，维持原判。

本裁定为终审裁定。

审判长　　傅曜天

审判员　　吴铁城

审判员　　邓敏波

二〇一七年三月八日

书记员　　邓碧霞

案例四、叶小军集资诈骗案

广东省高级人民法院

刑 事 裁 定 书

（2017）粤刑终152号

原公诉机关广东省惠州市人民检察院。

上诉人（原审被告人）叶小军，男，1982年3月22日生，汉族，户籍所在地：广东省惠州市惠城区。因本案于2015年6月2日被刑事拘留，同年7月9日被逮捕。

辩护人叶碧波、邬可忠，广东方正联合律师事务所律师。

广东省惠州市中级人民法院审理广东省惠州市人民检察院指控原审被告人叶小军犯集资诈骗罪一案，于2016年12月1日作出（2016）粤13刑初42号刑事判决。宣判后，原审被告人叶小军不服，提出上诉。本院依法组成合议庭，经过阅卷、讯问上诉人、听取辩护人意见，认为本案事实清楚，决定以不开庭的方式审理本案。现已审理终结。

原审法院根据原公诉机关的指控及经过庭审出示、质证查证属实的被害人陈述，证人证言，借款借据、借款过桥合同、银行交易明细流水清单、线下借款详情表及利息支付表、“文妥财富”P2P平台报案者报案材料、线上吸收资金情况统计表、借款标的统计表、报案统计表等书证、视听资料、被告人的供述与辩解等证据，认定：2013年5月开始，被告人叶小军与周稳妥（另案处理）为筹集赌资、支付借款利息，谎称从事银行短期拆借及其他抵押业务，以借款方式向社会公众集资。2013年5月至2015年1月，叶小军、周稳妥骗取曾某等63人共人民币31506.2万元，为取得被害人的信任，叶小军、周稳妥先后支付利息人民币8321.86万元给曾某等人，并将其余款项用于赌博等活动进行挥霍。期间，叶小军、周稳妥让钟某梁帮他们筹集资金，并许诺按筹集资金的月利息0.5%的利息差作为报酬。钟某梁遂以银行短期拆借业务为由向社会公众筹集资金，先后为叶小军、周稳妥直接筹集资金人民币8742万元，作为担保人为叶小军、周稳妥筹集资金人民币8967万元。

2014年5月开始，被告人叶小军与周稳妥为支付上述借款利息，成立“文妥财富”P2P网络借贷平台，冒用、伪造他人抵押借款材料虚构借款“标的”，并在相关的互联网平台宣传该网站的投资获利功能，以月息2%-3%不等的回报进行集资，骗取林某等140人本金人民币11165451.97元。叶小军、周稳妥骗得上述款项后用于赌博、支付利息等活动。

2015年6月2日，叶小军主动到公安机关投案。

原审法院认为，被告人叶小军以非法占有为目的，虚构事实，隐瞒真相，非法向不特定多数人的筹集资金，数额特别巨大，其行为已构成集资诈骗罪。被告人叶小军自动投案，在侦查阶段如实供述部分犯罪事实，可予以从轻处罚。依照《中华人民共和国刑法》第一百九十二条、第五十七条、第五十九条、第六十四条、第六十七条之规定，作出如下判决：

一、被告人叶小军犯集资诈骗罪，判处无期徒刑，剥夺政治权利终身，并处没收个人全部财产。

二、被告人叶小军诈骗所得人民币243008851.97元，责令退赔给被害人林某等140人。

上诉人叶小军上诉及其辩护人辩护提出，一审法院认定叶小军参与文妥财富P2P网络线上集资诈骗，以及将叶小军将所骗得的借款用于赌博均与事实不符；叶小军与钟某梁是合作关系，不是雇佣关系，叶小军与钟某梁犯同一种罪，叶小军的量刑应与钟某梁的量刑相当；叶小军有自首情节，一审判决量刑过重，要求改判有期徒刑。

经审理查明：2013年5月开始，上诉人叶小军与周稳妥（另案处理）等为获取非法利益，虚构从事银行短期拆借及其他抵押业务的事实，以高利为诱饵向社会公众集资。2013年5月至2015年1月，叶小军、周稳妥骗取曾某等63人共人民币31506.2万元，为取得被害人的信任，叶小军、周稳妥先后支付利息人民币8321.86万元给曾某等人，并将其余款项用于赌博等活动进行挥霍。

2014年5月开始，叶小军与周稳妥为支付上述借款利息成立“文妥财富”P2P网络借贷平台，冒用、伪造他人抵押借款材料虚构借款“标的”，并在相关的互联网平台宣传该网站的投资获利功能，以月息2%-3%不等的回报进行集资，骗取林某等140人本金人民币11165451.97元。叶小军、周稳妥骗得上述款项后用于赌博、支付利息等活动。

2015年6月2日，叶小军主动到公安机关投案。

上述事实，有下列证据证实：

（一）被害人陈述

1、刘某文的陈述：我是来投案自首的，我利用新懿公司非法吸收公众（约196人）存款人民币约1.8亿元。2008年开始，河南岸的医生王某天以4分息拿给我10万元人民币让我去放数，操作还可以，他介绍同事黄某良给我，黄某良以4分息拿给我20万让我放数，一直合作至今。从那时开始，陆续有人开始将钱放到我处，月息2.5%-4%，我付息非常准时，形成了高度的营业信用。至2015年，有务工人员、个体老板、老师及公司内部员工等人以高息放款到我这里，除已退还本金的，累计有196人放约1.8亿元，都写了借条，月息2.5%-4%。2013年3月1日至2014年12月1日期间，我以月息8%累计出借给9000多万给周稳妥、钟某梁、叶小军等人。2015年1月，该三人因集资诈骗被抓，无法偿还欠款，导致我资金链断裂。现每月我需支付约800万元，实在无法支撑，所以投案自首。借款给我的人有亲戚朋友，认识的占一半以上，其他是经他人介绍认识的。我没有通过媒体及广告进行宣传，都是通过放款在我这里的人口口相传的。我是以个人名义向他人借款，都写了借条，没有标明利息，口头协定利息。我基本上通过5个账号来吸存，分别有中国工商银行账号62×××18、62×××08、62×××95；中国建设银行账号62×××68；中国农业银行账号62×××78。付息账号在公司财务刘某友手上。现我在外债务约1.8亿元，除周稳妥等人的9000万外，还有约6千万的欠款，共约1.5亿。资产有2套房、2部车、8家公司，具体价值待评估后才清楚。营运从2013年开始亏损，每年都有本金无法收回，公司运营也亏损，基本靠借贷维持。

大概2013年年中，黄某良向我介绍说钟某梁、叶小军、周稳妥三人是合伙做银行“过桥”业务的，需要融资，而且利息比较高，问我有没有兴趣筹集资金借给他们，我就答应借钱给钟某梁、叶小军、周稳妥。钟某梁、叶小军、周稳妥还欠我9100万元本金尚未归还给我，我借钱给这三人都是黄某良牵线搭桥的，具体的借款金额、期限、利息，都是黄某良帮我跟他们协商确定，也是他负责保管借款借据的，我只是将借款转账给钟某梁、叶小军、周稳妥三人。我提供的15份借条我没有签名，是黄某良向我担保说钟、叶、周三人所宣称的“过桥”没问题，我放心借给这三人，也放心由黄某良去写借据、保管借据，直到2015年4月，我从黄某良处拿回这些借据才知道上面没有写明我是借款人。我向公安机关提供的15份借据，每笔借款利息不一样，月息大概是6-9%。这三人到了2014年12月底开始不付利息，但2013年下半年至2014年12月这段时间，钟某梁、叶小军、周稳妥三人都有准时支付给我的利息，利息是6-9%，具体支付给我的利息我算不清楚了，应该有借款本金的70%。可以以借据上的借款日期、金额，月息以7.5%来算，大概差不多。

2、余某林的陈述：我和钟某梁是朋友。2014年9月，我侄子余某跟我说他朋友钟某梁和周稳妥、叶小军一起做银行短期资金拆借（俗称“过桥”），还说月息是2%，钟某梁是干部，钱借给他比较稳，所以我就和我侄女婿赖某茂凑了600万元给钟某梁，借款期限2个月。我和赖某茂之前就有钱放在余某那里，决定借钱给钟某梁之后，就叫余某把我们放在他那里的钱各借300万元给钟某梁，而余某把我和赖某茂的钱借给了王某平，于是余某汇了100万元到钟某梁的父亲钟某泉的工商银行的账户，余某又按照钟某梁的要求叫王某平分几次把500万元汇入叶小军、王某红的银行账户，具体账户不记得。上述借款有写借据，钟某梁写了借款600万元的借据给我和赖某茂。钟某梁没有支付借款利息给我，也没有把借款还给我。钟某梁就说用于和周稳妥、叶小军一起做银行“过桥”生意，具体用途我不清楚。

3、熊某峰的陈述：2003年左右我认识周稳妥，我们是做门窗生意的同行。2013年2、3月，周稳妥以做生意需要资金周转为由，向我借270多万元，期限一年，月息1.8%。至2014年12月，周稳妥一直以做生意需要资金周转的为由向我借钱，借款11次，合计借给他1011万元，期限均为一年，月息为1.8%至2%，其中我自己的钱约300万元，700多万元是我先借亲戚、朋友的钱再转借给他，周稳妥前后向我支付了约40万元。2015年1月，我追问周稳妥资金的去向，要求他还款，周稳妥声称叶小军赌博输了很多钱，他从公司挪了

4000 多万元给叶小军，导致公司资金出现漏洞，无法支付利息和偿还本金。我是出于对其十几年的信任才相信他，借钱给他。周稳妥偶尔要我去帮他拉借款，没有约定我帮他拉客户成功后如何支付“介绍费”，我借亲戚的钱，大部分我是以 1%至 1.5%的月息先借过来，一部分借款我是没有赚利息差的。我不清楚周稳妥、叶小军、钟某梁等人声称所从事的银行”过桥”短期拆借业务，周稳妥没有向我提过。文妥公司的法人、实际控制人是周稳妥，其他情况我不清楚。周稳妥被公安机关抓获后我才听说他有参与网络赌博，以前不知道。我不清楚“文妥财富”网络借贷 P2P 平台的情况，我只知道这个平台发布的一些宣传资料，其他情况我不清楚。

4、陈某城的陈述：2013 年 12 月，我在河南岸松记修理厂听老板曾某说叶小军、周稳妥、钟某梁三人在合伙做银行短期拆借业务。2014 年 1 月，经曾某向我介绍叶小军、周稳妥、钟某梁三人在合伙做银行短期拆借业务，0.2%的日息，我便和曾某合伙筹钱投资此业务。至 2014 年 8 月，我合计投入本金约 750 万元，但叶小军、周稳妥、钟某梁三人从未归还过本金，至 2014 年 12 月合计向我支付利息 100 多万元，仍欠我本金约 750 万元。通过我四个银行账号（东莞银行账号 18×××60，招行银行账号 62×××88，我妻子康某姬工行账号 62×××20，朋友樊某珍东莞银行账号 62×××81）先转账给曾某，再由曾某转账给钟某泉（钟某梁的父亲）的工行账户：62×××70 和叶小军的工行账户:62×××34，曾某告诉我他将钱转给了钟某梁和叶小军。大部分给曾某的钱我是通过银行转账的方式，小部分是直接给现金，大部分转账给曾某的钱我存有银行交易凭证。只有一次我直接转账约 50 万元给叶小军工行账户 62×××34，其他本金都是通过曾某转给钟某梁和叶小军的。叶小军、周稳妥、钟某梁三人自称做银行短期拆借业务，但真实用途我不清楚。曾某将钱转给叶小军、钟某梁有借据等凭证。据我所知，曾某先期是与钟某梁签订的借据，其中借款人是钟某梁，担保人是叶小军、周稳妥。后期，至 2014 年 10 月，叶小军、周稳妥、钟某梁无法按时支付利息及归还本金，于是叶小军、周稳妥、钟某梁便在三环装饰城文妥公司与曾某签订了一份借款额为 4000 多万元的“总单”，借款人是叶小军，后我又要求曾某、钟某梁要将我的出借款项分清楚，于是叶小军、周稳妥、钟某梁、曾某在 2015 年 1 月 1 日在麦地叶小军经营的亿丰达酒庄签订了一份金额 750 万元的借款借据，其中借款人是叶小军，担保人是钟某梁和周稳妥，见证人是曾某。我之前说我的钱是通过曾某转账给钟某梁和叶小军，但在 2015 年 1 月 1 日签订的借款借据借款人只有叶小军、钟某梁作为担保人。是因为钟某梁是公职人员，不方便作为借款人，钟某梁多次当面告诉我说他和叶小军、周稳妥是合伙在做银行短期拆借业务，且钟某梁也当面向我提过，他和叶小军、周稳妥是合伙人，一起经营文妥公司和亿丰达担保公司，周稳妥负责文妥公司，叶小军负责亿丰达担保公司，钟某梁负责筹集资金，所以我就同意将借据的借款人写成叶小军。“文妥财富”P2P 是文妥公司运营的，是一个网络贷款平台。据该公司官网介绍，周稳妥是总经理，也是法人代表；周某阳是财务总监，据说和周稳妥是同乡；张某是风控经理；还有催收团队的凌某栋及另外两名周姓员工，上述人员是文妥实业公司的骨干。

我还有两个情况要补充:（1）2015 年 1 月 11 日晚，叶小军、周稳妥、钟某梁三人召集大部分债权人在三环装饰城三楼文妥公司（旧址）开会，会上他们三个股东向债权人承诺，他们会利用“文妥财富”P2P 平台骗取线上投资者的钱来还线下债权人的钱，当时我、曾某、黄某平等债权人在场，并对当时的情况进行录音及拍照；（2）经我了解，叶小军、周稳妥等人跟恒基创业投资有限公司的法人朱某交往密切，2015 年 1 月 11 日晚，也是朱某在现场安抚债权人的情绪，同时告诉债权人要相信叶小军、周稳妥、钟某梁等人会把钱还给债权人，而且据文妥公司的财务总监周某阳说，文妥公司的大部分资金都转给了朱某，我怀疑朱某是该事件的幕后操纵的人。

5、郭某的陈述：2012 年左右，我通过朋友介绍认识叶小军。2014 年 7、8 月份，叶小

军多次向我提出他和钟某梁、周稳妥一起做银行“过桥”业务，需要筹集资金，要我借钱给他，所以我在2014年9月1日借30万元给叶小军（通过我工行账号62×××01一次性转账28.5万元给叶小军的工行账号，另1.5万元作为借款利息现行支付），并写了借条，借款人叶小军，担保人钟某梁、周稳妥，口头约定期限3个月，月息1.7%。叶小军、钟某梁、周稳妥三人是生意上的合伙人关系，一起做银行“过桥”业务，一起经营文妥公司，一起运营“文妥财富”P2P平台，我多次听叶小军提起，其与钟某梁、周稳妥是合伙人关系。我与叶小军写的借条，之所以钟某梁、周稳妥会作为担保人，是因为三人是合伙关系，无论谁作为借款人，其余两人都会作为担保人，且钟某梁是公职人员，是市环卫局“余泥”办主任，作为借款人或担保人，会比较安全，债权人才放心借钱给他们。至2014年12月1日，还款期限到期后，叶小军一直无法归还30万元本金。我多次去麦地叶小军经营的茶庄（名字记不清）找叶小军、钟某梁，要求归还本金，叶小军、钟某梁均以资金在银行“过桥”，资金困难为由推脱，至今一直无法归还，并且无法联系叶小军和周稳妥，不知去向。叶小军自称是和钟某梁、周稳妥一起做银行“过桥”业务和运营“文妥财富”P2P平台，需要筹集资金，但真实用途我不清楚。据我所知是叶小军、钟某梁、周稳妥三人一起在运营网络借贷平台，我自己也在平台上投资1000多元，据我所知，该平台上大部分都是假“标”，黄某平告诉我，叶小军、钟某梁、周稳妥三人曾经对其车辆、房产资料进行过拍照，然后将上述信息放在“文妥财富”P2P上作为假“标”，但黄某平实际上没有向平台借过钱。

6、黄某平的陈述：2013年12月至今累计借款人民币约1100万元给钟某梁，月息2%，钟某梁归还了其中200万元本金给我，另外有300万本金我通过“改单”的方式转给了赖某茂，合计钟某梁现在还欠我638万元。钟某梁一直都以做银行“过桥”短期拆借业务为由向我借款。借款中约有800万元我是和曾某合伙出借给钟某梁，由曾某与钟某梁签订借款协议，另外300万元是我与钟某梁签订借款协议的，都是短期的借款，最长一、两个月。我都是通过银行转账从我工行账号（62×××48）分多次转账300万元给钟某梁指定的两个账户，其指定的账户分别为：王某红工行账户62×××51，叶小军工行账户62×××34。另外以曾某的名义出借给钟某梁的800万元，具体次数及数额我记不清了，但是通过查询我工行账户62×××48、王某红工行账户62×××51、叶小军工行账户62×××34）可查明转账的次数及数额。

钟某梁、叶小军每次都以银行资金紧张，很难放款为由拖延还款。2014年11、12月钟某梁将仍未归还我的合约638万元分成了三份“总单”借据，其中一份200万元的由钟某梁作为借款人，另外两份380万元、58万元的由叶小军作为借款人，此三份借据的原件由我保管。之所以两份借款人由钟某梁变更成叶小军，是因为钟某梁是公职人员，不方便作为借款人，且钟某梁称他或叶小军作为借款人、担保人都是一样的，叶小军也同意作为借款人与我签订借款借据，所以“总单”中借款人由钟某梁变更为叶小军。2014年10月20日左右，钟某梁、叶小军带曾某去工商银行惠州分行二楼保险库看银行“过桥”业务单据，2015年1月11日晚周稳妥告知我单据是假的，是他和叶小军为了应付我才伪造假的。我不清楚出借给钟某梁的款项的去向，因为大多数款项是转入叶小军、王某红的账户，所以我质问过叶小军、周稳妥资金的去向，叶小军称因为赌博输光了，后曾某去银行打叶小军的工行账户62×××34的流水，通过该账户2013年、2014年的交易记录来看，大多数资金是流向王某红工行账户62×××51。“文妥财富”P2P简介公司法人是周稳妥。大约2014年6、7、8月，钟某梁和叶小军在宝泰商行（河南岸）要求过我和其他债主提供资产信息（车、房产等相关资料），以此伪造假“标”，放在“文妥财富”P2P平台上供投资者投资。2015年1月17日，我接到一名自称“文妥财富”P2P的深圳投资者的电话（0755-223××××3），向我了解否有借“文妥财富”P2P的钱，是否已还清，当时我知道“文妥财富”有借用我的个人信息伪造假“标”。2015年1月11日18时许，钟某梁、叶小军、周稳妥的债主聚集

在文妥公司（三环装饰城）追债时，周稳妥在所有债主面前保证他会把“文妥财富”P2P 业务做大，把线上所有投资者的钱骗来归还线下债主的钱，我现存有当晚的录音和图片。

7、方某灿的陈述：我借了 800 万元给钟某梁、周稳妥和叶小军，他们现在还不了钱，而且叶小军失去联系。上述借款有借据，借条时间是 2014 年 10 月 1 日，借条实际签署时间是 2015 年 1 月 10 日，而借款的实际发生时间是 2014 年 9 月，该借条是之前几笔借款的汇总，金额是 800 万，月息 2%，借款人是周稳妥，钟某梁和叶小军是担保人，他们说用于个人银行业务短期拆借（俗称“过桥”）。借给他们的 800 万元是分好几笔转账支付的，800 万元是我和亲戚方某龙凑的，借钱给他们时，先从我或方某龙的个人账户转账到亲戚曾某的账户，曾某再把钱转给钟某梁，收款账户是钟某梁父亲钟某泉的工商银行账户 62×××67。2014 年 5 月，钟某梁说他跟周稳妥、叶小军合伙做银行“过桥”生意，刚开始只有几十万，期限只有五至七天，因为还款及时，所以我陆续增加借款数额给他们，每一笔借款他们都分别写一张借据给我。直到 2014 年 9 月底，钟某梁他们没有及时还款给我，于是他们说把所有借款汇总之后写一张借据给我，以月息 2%计算利息，当时我同意了。当时借据的借款人是钟某梁，叶小军和周稳妥是担保人，但是借款汇总以后他们又不能归还本金和全额付息给我。2015 年 1 月初，叶小军失去联系。1 月 10 日，我和其他债权人一起在三环装饰城华熙广场找到钟某梁、叶小军和周稳妥，经过协商，三人同意一起承担各自以个人名义所借款项，对所有借款相互担保，还答应利用周稳妥经营的 P2P 平台所得款项和其他方式所得资金支付我们的欠款，2015 年 3 月以后逐步还清，于是他们三人重新写了目前我提供的这张借据，并注明 2015 年 3 月以后逐步还款。付息过程是他们把钱转账到曾某的账户上，曾某再把钱转给我和方某龙，我共收到约 60 万元。

8、余某的陈述：我借了 130 万元给钟某梁、周稳妥和叶小军，其中 2015 年 1 月 7 日 40 万元是叶小军写的借据，2014 年 1 月 18 日 40 万元、4 月 2 日 40 万元、11 月 16 日 10 万元是钟某梁写的借据，没有抵押，月息 2%，我共收到 152000 元利息。是通过银行转账将借款交给钟某梁、周稳妥、叶小军三人的，我的汇款账户是我个人在工商银行的账户 6222U82008002531018，收款账户是钟某梁父亲钟某泉工商银行的账户 62×××67。

2014 年 1 月钟某梁说他和人家做银行资金“过桥”生意，所以我才借钱给他们。2014 年 9 月，叶小军名下的亿丰信用担保有限公司、亿丰达酒庄法人成立时请我们吃饭，那时我才知道钟某梁、周稳妥、叶小军三个是合伙的。上述借款钟某梁、周稳妥、叶小军三人没有把本金还给我。2015 年 1 月 6 日，钟某梁、叶小军把我、黄某平、曾某等七八个债权人召集在亿丰达酒庄，钟某梁当时说他们公司有危机，还需要 180 万元，希望我们借钱给他们度过难关，还说 1 月 20 日就可以还钱。我当时问钟某梁有没有问题，钟某梁说没问题，所以第二天又借了 40 万元给钟某梁。2015 年 1 月 10 日，我和其他债权人一起把钟某梁、周稳妥、叶小军叫到三环装饰城，他们三人当时一起承诺所有借款他们将三人合力承担，且 2015 年 4 月起将周稳妥经营的网络 P2P 平台所融资的款项给我们支付本金，每个月还 1000 万。当时，他们三人还给每位债权人签署的借条互为担保。有的债权人把当时的情况用手机拍照和录音。我不知道钟某梁、周稳妥、叶小军把借我们的钱用到哪里，不过当时叶小军说他把钱输掉了，他说他在三环酒店租了一间房赌“快乐十分”（外围）输了 1.5 亿元，不过我们都不相信。我妻子刘某琴经过我的手把她外家的钱 130 万元借给了钟某梁，钟某梁写了借据给刘某琴，我还介绍我叔叔余某林和我姐夫赖某茂借了 600 万元给钟某梁，介绍朋友邱某民借了 340 万元给钟国梁，此外还有四、五十人借了钱给他们三人，具体情况我不清楚。

9、曾某的陈述：2013 年 12 月至 2014 年 12 份累计借款人民币 5600 万元给钟某梁，月息是 2%，现在借款无法收回，至今收到叶小军和钟某泉支付的利息大约 200 万元，大约归还本金 200 万元。现仍有约 5400 万元本金未归还。钟某梁一直以来都是以做银行“过桥”短期拆借业务为由向我借款。

2013 年 12 月，钟某梁主动提出向我借款，我大概分了 15 次将总数约 5600 万元借给他，具体次数和金额可通过我工行账号 62×××31 来查明。钟某梁约定支付我 2%的利息，每次借款都与我签订借款借据，从 2013 年 12 月至 2014 年 12 月签订了约 15 张，总数约 5600 万元，都是短期借款，最短的 5 天，最长有 1 个月的。我通过银行转账的方式从工行账号转账给钟某梁指定的 3 个账户，分别有：钟某泉工行账户 62×××70，王某红工行账户 62×××51，叶小军工行账户 62×××34。因为钟某梁是公职人员，在市环卫局工作，不方便使用其本人的账户从事此业务，所以要求我将借款转入其指定的他人账户，我同意此做法。我认识钟某梁的父亲钟某泉，比较熟悉。我不认识王某红，询问钟某梁才知她是周稳妥的妻子，我才放心将借款转入王某红的账户。2014 年 12 月 20 日左右，我将约 15 份借款借据原件给了钟某梁，2015 年 1 月 11 日与叶小军签订了一份“总单”，其中出借人是我，借款人由钟某梁变更为叶小军，担保人是钟某梁和周稳妥，借款金额为 3402 万元，期限为不定期，利息为 2%。借款人由钟某梁变更为叶小军，是因为我借给钟某梁的钱大多是转入叶小军的工行账户，钟某梁是公职人员，我不想他作为借款人，且叶小军也同意作为借款人与我签订借款借据，所以“总单”中借款人由钟某梁变更为叶小军。原先我说钟某梁仍有约 5400 万元本金未归还，而“总单”中借款金额变成了 3402 万元，是因为借款总数中的 3402 万元是我的，800 万元是方某灿的，750 万元是陈某城的，438 万元是黄某平的。所以我、叶小军、钟某梁、周稳妥、黄某平、陈某城、方某灿都同意将我原先总数约 5600 万元的本金分为 3402 万元（出借人:曾某）、800 万元（出借人:方某灿）、438 万元（出借人:黄某平）、750 万元（出借人:陈某城）四份借款借据“总单”。借款时钟某梁自称与叶小军、周稳妥做银行“过桥”业务，但在其未能如期归还本金、支付利息后，我要求钟某梁、叶小军、周稳妥提供业务单据，他们一直推拖。2014 年 10 月 20 日左右，钟某梁、叶小军带我去工商银行惠州分行二楼保险库看他们所说的“过桥”业务单据，但 2015 年 1 月 11 日晚周稳妥告知我“过桥”业务单据是假的，是他和叶小军为了应付我才伪造的。我不清楚我出借给钟某梁的款项的去向，因为大多数款项是转入叶小军的账户，所以我质问过叶小军、周稳妥资金的去向，叶小军自称其所接资金赌博输光了。后我去银行打印叶小军的工行账户流水，该账户 2013 年、2014 年大多数资金是流向王某红工行账户。我清楚周稳妥经营“文妥财富”P2P 业务的情况，公司法人是周稳妥，据周稳妥说其公司网站发布的大多数标的都是假的，所吸纳资金大多也是用来做银行“过桥”业务。2015 年 1 月 17 日，我接到一名自称“文妥财富”P2P 的深圳投资者的电话，向我了解我是否有借“文妥财富”P2P 的钱，是否已经还清，当时我就知道“文妥财富”有借用我的个人信息伪造假“标”。2015 年 1 月 11 日 18 时许，钟某梁、叶小军、周稳妥的债主聚集在文妥公司（三环装饰城）追债时，周稳妥在所有债主面前保证他会把“文妥财富”P2P 业务做大，把线上所有投资者的钱骗来归还线下债主的钱，当时陈某城有现场录音及图像。

侦查人员给我的“文妥财富”编号 319、707 号的抵押借款标的的相关材料，经我确认，我从未通过“文妥财富”平台向周稳妥抵押借款，标的上的房产并不是我的，但是汽车维修中心我能辨认出是我的，两部车也曾经是我的，这两份抵押借款标的的资料是伪造的、虚假的。粤Ｌ×××××奔驰车、粤Ｂ×××××是我的车。2014 年 7、8 月份，周稳妥曾因公司开张为由，想充场面，向我借了上述两辆车，松泰汽车维修中心的照片不知道他什么时候照的，我从来没有借过房产证给他。

10、周某阳的陈述：周稳妥是我表弟。2012 年，周稳妥在惠城区三环装饰城开了一家叫佳富豪实业有限公司做借贷生意，我当时借了约 100 万给周稳妥。2013 年 4 月，文妥公司成立，周稳妥知道我在做建材生意，认识人也比较广，所以他叫我去文妥公司挂个财务经理的名，帮拉一些客户和融资。2014 年 4 月，文妥公司开始做互联网 P2P 业务，2014 年 11 月，公司搬到华贸大厦。一直以来，我主要负责财务工作（发放员工工资、支付部分线下债

权人利息、报销部分公司日常支出）。我不清楚文妥公司如何开展网上 P2P 业务的，公司线下业务我没有参与，连平时开会我也没有参加，我知道周稳妥在线下做融资放贷生意。文妥公司开展线下融资放贷业务通过个人借款的方式，经比较高的利息（月息 2-4%不等），向亲戚、同乡、朋友等借款，或者通过亲戚、同乡、朋友的介绍在对外借款，周稳妥把所融的资金如何运作我不清楚。周稳妥线上融资约 3000 万、线下的情况我不清楚。我个人借了 775 万（2013 年 4 月至 2014 年 12 月，月息约 3%），陈某财借了约 200 万。我借给周稳妥的钱是分好多次陆续借的，周稳妥向我借款时基本都是说他跟合作伙伴叶小军有短期资金拆借业务，刚开始的时候是说短期借款，后来他又以其它借口说资金还在用，所以短期款就变成了长期借款。695 万元借款有写借据，2014 年 11 月 27 日借的 50 万元、12 月 18 日借的 30 万，这两笔没有写借据。大部分是转账，小部分是现金，我通过工商银行账户（尾数 451）。我前后共收到周稳妥支付的利息约 150 万元。

11、谢某娣的陈述：2014 年 4 月份左右，我通过朋友翟某映知道叶小军、周稳妥、钟某梁合伙做银行短期拆借业务生意，可以借钱给他们赚一点利息，于是我和钟某梁开始短信联系，钟某梁用短信告知我转账的账号。我分别于 2014 年 4 月 6 日、7 月 8 日各出借 10 万元、20 万元给他，合计 30 万元，至今未归还借款本金。2014 年 4 月 7 日，我通过东莞农商银行账号 28×××37 转账 10 万元到周稳妥账号 62×××46；2014 年 7 月 8 日，我通过云浮新兴东盈村镇银行账号 62×××89 转账 20 万元到叶小军账号 62×××34。支付利息时，钟某梁通过钟某泉账号 62×××70、周稳妥账号 62×××46，以转账方式共向我支付利息 5.25 万元。因为钟某梁一直称他和周稳妥、叶小军是合伙开公司，经营银行短期拆借业务的，他考虑到国家工作人员的身份，以短信的方式告知我将钱转到周稳妥、叶小军的账号，至于为何是通过钟某泉、周稳妥向我支付利息，我不清楚。

12、翟某月的陈述：2014 年初，钟某梁告诉我他和叶小军、周稳妥合伙做银行短期拆借业务，我借钱给他，可以赚一点利息。于是，我于 2014 年 4 月 6 日、2014 年 7 月 8 日分两笔借款 40 万元、20 万元给钟某梁，合计借款 60 万元，约定月息百分之二点五，至今未归还本金，钟某梁有向我支付利息，前后支付 13.5 万元。钟某梁通过周稳妥 62×××46、钟某泉 62×××70 向我支付利息。2014 年 1 月 16 日，我通过我的东莞农商行存折向周稳妥的惠州农商行账号转账 20 万元；2014 年 4 月 7 日，我通过我的东莞笔农商行存折向周稳妥的惠州农商行账号转账 20 万元，上述两笔合计 40 万元的借款，钟某梁就合并写了一张借款借据给我；2014 年 7 月 8 日，我通过东莞农商行存折向叶小军的工行账转账 20 万元。因为钟某梁一直对我宣称他和周稳妥、叶小军是合伙开公司，经营银行短期拆借业务的，他又考虑到国家工作人员的身份，就以短信、微信的方式告知我将钱转到周稳妥、叶小军的账号。

13、张某的陈述：2014 年 6 月 12 日我通过妻子廖某娟的建设银行账号 43×××52 借给周稳妥 47.5 万元；2014 年 11 月 23 日，我又通过妻子廖某娟的建设银行账号借给周稳妥 17 万元，后于 2014 年 12 月 3、4 日在周稳妥运营的“文妥财富”P2P 平台投资 2.3 万元，至今我借给周稳妥的上述 64.5 万元本金未收回，投资在“文妥财富”P2P 平台的 2.3 万元也未能提现，我至今只收到周稳妥向我支付的 5.7 万元。周稳妥均已临时周转为由分别于 2014 年 6 月 12 日向我借款 47.5 万元，于 2014 年 11 月 23 日向我借款 17 万元，其中第一笔 47.5 万元借款我和周稳妥口头约定月息为 2%，第二笔 17 万元的借款周稳妥说几天后就会归还我，所以我们并未约定利息，上述两笔借款均未约定借款期限，也未签借据；2.3 万元的投资这是我在周稳妥经营的文安实业公司上班后，在其运营的“文妥财富”P2P 平台投资的。在“文妥财富”P2P 平台投资 2.3 万元，我无法提供相关凭证，据说该平台现已无法登录。2014 年 9 月 12 日后我开始在其经营的文妥公司上班，任风控部经理。周稳妥安排我培训公司员工、管理客服。我不清楚“文妥财富”P2P 平台上标的的真实性。周稳妥自己负责审核借款人的借款资料、资质，运营主管王某洋负责发布借款标的，我不清楚这些借款标的资料

存放在何处，但之前我见过周稳妥将这些资料存放在其办公桌后面的书柜里。周某阳、周某云负责文妥公司的财务工作。我不清楚周稳妥、叶小军线下借贷的情况，他们就是做民间借贷，以利息吸引客户。

14、叶某明的陈述：周稳妥用个人借款的方式诈骗了我 2784.5 万元。2014 年 6 月 30 日至 2015 年 1 月 6 日，周稳妥分 19 次向我借款 2784.5 万元，月息 2%。周稳妥跟我说他自己做银行短期过桥拆借生意。我通过亲戚叶某梅工商银行账号 62×××47、黄某生账户转账给周稳妥的老婆王某红的工商银行账户。我借款给周稳妥有写借据，周稳妥在 2015 年 1 月之后就没有支付利息给我了，周稳妥通过银行转账共支付我利息约 160 万元，我用叶某梅上述工商银行账户收取借款利息，他没有归还借款本金。

15、叶某青的陈述：周稳妥以资金周转为由，于 2014 年 6 月 18 日向本人借款 10 万元，一年还回，月利 3 分，利息从 2014 年 6 月 18 日至 2014 年 12 月 18 日共支付 7 个月利息，其余至今没付利息。第二笔 7 月 23 日，又以资金周转困难借 10 万元，月息 3 分，从 2014 年 7 月 23 日至 2014 年 12 月 23 日仅付 6 个月的利息，剩下至今没付。第三笔 2014 年 10 月 17 日又借 10 万元，月息 3 分，从 2014 年 10 月 17 日至 2014 年 12 月 17 日已付 3 个月利息。本人及叶某芬 2 人共借给周稳妥 30 万元，共收利息仅 48000 元。

16、蔡某生的陈述：叶小军、周稳妥分别通过与我朋友关系向我借款，叶小军从 2014 年 4 月 1 日至 2015 年止共分 9 次借款总额 2045 万元整；周稳妥从 2014 年 4 月 13 日至 2014 年 12 月 31 日止总共分 8 次借款共计 2712 万元整。所有借款均签有借据，约定月息 2-4 分不等，至今未拿到利息，也没归还本金。

17、朱某万的陈述：2014 年 10 月-2015 年 1 月分三次借款共 340 万给周稳妥，担保人钟某梁、叶小军，后面经多次打电话催款，最后失联。

18、叶某安的陈述：我分三次借给叶小军 260 万，约定月利息 1.8 分，共支付利息 21.6 万，三次款以银行“过桥”为由。我从 2013 年至 2014 年分三次借给周稳妥 600 万元、200 万元、100 万元，共 900 万元，约定月息 1.8 分，共支付利息 216 万，从 2014 年 9 月开始无法支付利息，我是通过叶某城认识周稳妥的，三期借款周稳妥均以银行“过桥”为由。我没有通过“文妥财富”平台以抵押房产的形式向周稳妥借款 60 万元，也没有与周稳妥签订抵押借款合同，我名下的三套房产没有做过抵押。刚侦查人员向我出示“文妥财富”平台借款标的 329 号借款标的，抵押物为一套位于惠州江北文明路的房产，内容还包括转账交易凭证、房产抵押合同、房产证、借款借据、车辆行驶证等信息，经我确认，这些资料中的房产信息不是我的，所有签名都不是我的，我也没有作为借款人向周稳妥抵押借款 60 万，其中只有身份证是我的。大约在 2014 年 8 月份左右，周稳妥以记账为由向我借过一次我的身份证，我借给了他，当时在他三环装饰城办公室，他复印了我的身份证，我不清楚他借我身份证的真实用途。

19、张某新的陈述：我是在亲戚聚餐时认识借款人钟某梁的，在 2014 年 2 月份共借 10 万，并签订借款借据，借据上无注明借款利息，利息双方口头约定按月息 2.5 分计，到 2014 年 12 月底共收利息 27500 元，没有归还本金。本人到报案时一直没到过其公司，借款人已失去联系。

20、黄某明的陈述：2014 年 2 月 16 日借款 40 万给钟某梁，并签订借款借据，利息是双方口头约定，月息 2.5 分。到 2014 年 12 月 31 日共收过利息 11 次，每次 1 万元共计 11 万。

21、黄光某的陈述：在 2014 年 6 月通过朋友认识钟某梁的，在 2014 年 6 月 16 日借款 20 万给钟某梁，并签订借款借据，利息口头约定千分之二十五月息，到 2014 年 12 月 31 日共收 7 次利息，每次 5000 元共计 35000 元。

22、黄伟某的陈述：我在学校读书时认识钟某梁，2014 年 2 月和 7 月分两次共借款 90

万，并签订借款借据，口头约定月息2.5分，到2014年12月底共收利息22万左右。2013年底钟某梁叫我介绍身边的亲朋好友借款给他，我介绍了张某新、黄光某、黄某明借款给钟某梁。

23、郑某曼的陈述：2013年11月4日，叶小军向本人借款50万元，然后叶小军又提出向本人借款，作为老乡帮他度过难关，一共向本人借款总金额320万。

24、张某阳的陈述：叶小军于2014年7月1日向我借款10万元，自12月起拖欠本息。

25、曾某萍的陈述：叶小军两次向我借款，2014年9月15日10万元，2014年12月1日15万元，共25万元，通过转账方式给对方（指叶小军、周稳妥和钟某梁）。

26、彭某玲的陈述：叶小军两次向我借款，2014年9月15日借25万元；2014年8月12日借30万元，共55万元，由转账方式给对方（指叶小军、周稳妥和钟某梁）。

27、陈某伟的陈述：周稳妥、钟某梁、叶小军以借用短期拆借和其他抵押业务为由，分别于2014年2月及2014年5月共向本人借款210万元。

28、邹某华的陈述：我和钟某梁是朋友关系，2010年通过叶小军认识。2014年，钟某梁以银行“过桥”名义向我借15万元，月息2分，至今钟某梁支付利息22000元。

29、刘某琴的陈述：钟某梁、周稳妥、叶小军自2014年11月11日以银行拆借为由，向本人借款130万元，但至今未还。

30、蔡某强的陈述：钟某梁、叶小军、周稳妥自2013年12月开始，借用短期拆借及其他抵押业务为由，通过虚实事实，向我借款970万，借款金额转到叶小军、钟某泉的工行账上，2014年8月到现在没有付息。

31、朱某明的陈述：2014年12月18日，钟某梁经陈某强介绍向我借了120万，约定利息二分，至今为止没收到钟某梁付利息。钟某梁、叶小军、周稳妥以借用短期拆借及其他抵押业务为由，通过虚构事实，向本人借款的。

32、陈某媚的陈述：钟某梁、叶小军、周稳妥以借用短期拆借及其他抵押业务为由，于2014年4月向本人借款80万元。

33、赖某香的陈述：我与叶小军是通过朋友介绍，借款前不认识。从2013年起，叶小军以银行“过桥”名义向我借款70万，约定月利息2分。从2014年9月至今未付利息，未归还本金。

34、陈某婵的陈述：我与叶小军是通过朋友介绍认识，但借款前不认识。钟某梁、叶小军、周稳妥以借用短期拆借及其他抵押业务为由，分别于2014年11月及2015年1月向本人借款110万元，约定月利息二分。期间叶小军向我支付一个月利息，但至今未归还本金。

35、陈某萍的陈述：我与叶小军在借款前是不认识的，通过朋友关系认识的。钟某梁、叶小军、周稳妥以借用短期拆借及其他抵押业务为由，向本人借款530万元。从2014年6月份起，叶小军向我借款530万，说是与银行“过桥”用的，约定月利息2分，期间叶小军向我支付2个月利息，但至今未归还本金。

36、邱某民的陈述：我是于2014年10月经余某介绍认识钟某梁，因借钱才认识钟某梁。2014年11月1日，钟某梁以银行短期拆借业务名义向我借了340万元，月息二分，至今为止没收到利息。

37、陈某强的陈述：经朋友介绍认识叶小军，借款前不认识。钟某梁、叶小军、周稳妥以借用短期拆借及其他抵押业务为由，从2014年5月和7月先后二次叶小军以银行过桥抵押名义借我一次60万和40万，共100万。月息2分。但在去年10月到现未归还本金及利息。

38、赖某波的陈述：钟某梁、叶小军、周稳妥自2013年10月开始，以借用短期拆借及其他抵押业务为由，向本人借款42万元。借款金额分别以现金和转账到叶小军、周稳妥、钟某梁的工行账户。

我们约定月利息5%，期间叶小军向我支付12个月利息，但至今未归还借款本金。我在借款前不认识叶小军，后经朋友介绍在茶庄认识叶小军。本人从叶小军处拿到利息共25.2万元。

39、陈某好的陈述：我通过朋友介绍认识叶小军，借款前不认识他。钟某梁、叶小军、周稳妥自2013年10月开始，以借用短期拆借及其他抵押业务为由，向我借款100万元，约定利息每月二分。期间叶小军自2014年9月至今未支付利息、本金。

40、潘某满的陈述：借款前不认识叶小军。钟某梁、叶小军、周稳妥自2012年11月开始，以借用短期拆借及其他抵押业务为由，向本人借款38万元。借款金额分别以现金和转账到叶小军、周稳妥、钟某梁的工行账上，约定月息2分，但至今未归还本金。借款用途叶小军说是与银行“过桥”、抵押。

41、骆某强的陈述：周稳妥自2014年7月开始，以短期借用为由，向本人借款20万元。

42、邹某文的陈述：我2014年3月15日借给叶小军20万用于资金周转用途，担保人钟某梁、周稳妥。最近一笔在2014年11月1日借款10万，叶小军跟我说周转一个月。当时约定借款利息为3分。上述两笔借款的担保人均是钟某梁、周稳妥。共收到叶小军支付利息5700元，本金全部未归还。借款前是朋友关系。

43、陈某财的陈述：周稳妥自2014年2月-12月，以公司生意周转为由，向本人借款260万元。

44、赖某发的陈述：我2014年11月19日借给叶小军20万元，担保人钟某梁、周稳妥，叶小军当时说让我借给他周转几个月，我作为朋友觉得他有困难，就借给他，他借到我的钱后就不接我的电话，有时就故意关机，而后我感觉不对就报案了。

45、罗某浓的陈述：周稳妥称做生意需资金周转，2014年8月向我借款10万，月息付3500元。从2015年1月开始不付息，我向他追讨本金他也不归还。

46、黄某辖的陈述：周稳妥称公司生意需资金周转，于2014年12月11日向我借款200万，月息千分之1.8。并用名下车辆宝马（车牌号粤L×××××）、房子作为抵押。

47、邹某文的陈述：我2014年6月15日借给叶小军、周稳妥10万，担保人钟某梁。当时叶小军说借给他们生意周转，作为朋友我借给他，大概在7、8月份就经常不接电话，后来我要求退还借款，直至2015年1月份出问题，才知道被骗了。

48、杨某文的陈述：2013年12月至2014年12月，钟某梁、周稳妥、叶小军向我借款170万元。2014年9月我一直向钟某梁、周稳妥、叶小军要回借款，直到现在都没有偿还，在借款时说月息2分，从2014年9月起没有给利息。

49、王某飞的陈述：我和叶小军是朋友关系，2005年认识。2014年8月初，叶小军以公司资金周转为名，提出向我借款，2014年8月14日在我的档口（河南岸公园小区C栋14号）将现金7万元借给叶小军，当场签订借款借据，借款期限1年，利息没有具体说多少，当时叶小军说一年借款期限到期后会适当的支付利息。叶小军一直未归还本金，从未支付利息，现在叶小军失踪、无法联系。

50、周某生的陈述：2014年3月，叶小军以公司资金周转为由，向我提出借款，2014年4月10日和叶小军签订借款借据，并分两次通过银行转账将合计50万元出借给叶小军。叶小军一直未归还借款本金，从未支付利息，且无法联系他，我怀疑被他诈骗了。我提供的出借人是空白的，是因为我和叶小军是多年朋友关系，我比较信任他，借款的时候他说一年借款期限到了后一定会还给我的，就不用写明出借人了。借款期限是1年，借款的时候并未约定利息，叶小军只是说借款到期后会适当的给我一点利息。我借给叶小军钱从我哥周某生的账号转账。

51、刘某平的陈述：2014年7月8日起，钟某梁以做生意周转为名向我借款50万元，

约定每月利息 1.5 万。期间钟某梁向我支付六个月的利息共 9 万元，但从 2015 年 1 月起至今未支付利息，借款本金至今未归还，其中有 30 万是钟某梁指定汇入叶小军的工行账号（尾号 7170）。

52、朱某勇的陈述：2014 年 6 月 30 日起，周稳妥以资金周转名义向我借款 30 万，约定月息 3%，期间，周稳妥向我支付 5.4 万元，从 2015 年 1 月未支付利息。但至今未归还本金。

53、彭某吟的陈述：2014 年 8 月 12 日、2014 年 9 月 15 日经曾某介绍，叶小军以资金周转为由，分别向我借款 30 万元、25 万元，合计 55 万元。当时约定借款利息为月息 2 分。上述两笔借款的担保人均是钟某梁。至今为止共收到叶小军支付利息 38000 元，本金全部未归还。借款前我不认识他。

（二）证人证言

1、黄某婷的证言：2014 年 10 月，我进入文妥公司工作，担任行政部经理，负责公司的后勤、考勤、会议管理、办公文具采购、行政制度监督等工作。公司主要从事网络信贷业务（“文妥财富”P2P 平台），向借款人和投资者提供第三方交易平台，我从 2014 年 11 月份开始也在该平台投资，至 2015 年 1 月 14 日，共投资本金约 3 万元，应得利息没仔细算过，期间我只从账户中提现 1000 元。2015 年 1 月 15 日公司开完早会后，有人上门来追债，我才知道公司资金周转困难，老板周稳妥也失联了，线上投资者在官方群里讨论周稳妥跑路的事，16 日，网上投资者纷纷聚集在公司楼下商讨解决方法。17 日，投资者报警，派出所出警。当天下午，周稳妥在金华悦酒店与投资者见面，承诺不跑路并且答应有回款的投资者提现 5%。1 月 29 日，线上投资者反映周稳妥又失联了，后来我才从投资者处得知周稳妥已被公安机关抓获。公司实际控制人、老板（法人）是周稳妥，负责所有事务的决策，财务报销工作由周某阳负责，周某云负责线上的财务工作，王某洋负责标的的发布，张某负责风控部工作，郑秀云是客服部主管，主要负责与线上投资者沟通业务。我不知道“文妥财富”P2P 平台有无从事真实的网络借贷业务，也不知道平台的投资标的的真实性。公司运营部负责平台的宣传工作，王某洋、吴某豪、张某中，负责在“网贷之家”等网站宣传。公司要求员工拉客户，周稳妥经常会在每周例会上要求员工拉客户，口头承诺会有奖励，但没有规定具体提成比例，实际上从未实施过。我猜测这些标的是周稳妥负责选取的，我也不清楚公司有无安排专人去负责这些标的资质的审核把关，运营部负责发布。

2、王某洋的证言：我 2014 年 3 月至 2015 年 1 月在文妥公司上班，担任运营部主管。公司法人和实际控制人是周稳妥，公司地址惠州市惠城区江北华贸大厦一号楼 25 楼 05、06，公司做 P2P 网贷（“文妥财富”网址 www.wtdai.Com）。我名义上是运营部的主管，实际上是按照周稳妥的要求把公司开展网贷业务的一些投资标的的资料上传到公司网站，周稳妥把资料中的借款人身份证明文件、房产证、车辆行驶证、借款协议书等扫描成图片，然后用 U 盘拷贝后交给我，我再按他的要求用图片修改软件把上述资料涉及到一些个人身份信息、房产证、行驶证等证明文件的文号等一些具体的重要信息遮盖掉，再逐一上传。同时周稳妥叫我在平台的后台输入每一个借款标的的借款人的姓名、身份证号等信息。我今天来主要是将文妥平台后台中保存的借款人的姓名、身份证号等信息提交给公安机关。我在“文妥财富”平台使用的账号叫王某洋，密码：qweXXXXXXX9。平台投资者账号无权限看到我上述所说的借款人的姓名、身份证号等信息。除了我，公司所有客服、财务，只要能登录后台的人都能看到这些信息。投资标的资料是否真实我不知道，不过周稳妥交给我之前说资料已经核实过了，公司是风控部门（负责人张某）负责核实上述资料的。周稳妥保管投资标的的原始资料，具体情况他才清楚。我不知道公司有集资诈骗行为，我和我老婆沈某燕也投资了 4 万元，收回 721 元，损失 39279 元，后来我才知道老板周稳妥因集资诈骗被公安机关刑事拘留。

3、王某红的证言：我是周稳妥前妻，因周稳妥隐瞒家里巨额债务，引起我抑郁症、焦

虑症复发，我们决定协议离婚，2015 年 1 月 16 日办理离婚手续。2012 年开始，周稳妥和叶小军一起从事民间借贷。2013 年，周稳妥注册成立文妥实业公司，公司主要业务是民间借贷，还有装饰建材生意。2014 年 3、4 月份，周稳妥开始运营“文妥财富”P2P 网络借贷平台，我不清楚周稳妥和叶小军以何种名义从事民间借贷，我不清楚周稳妥供述其伙同叶小军，通过虚构银行”过桥”业务向他人集资。我的工商银行账号之所以有大笔资金交易记录，是因为周稳妥在工商银行无法办理开户，我在工商银行惠州金田苑支行办了两个银行账户，并开通了网银给他用，具体账号不记得，他说用于和投资者资金往来，具体谁使用我不清楚。周稳妥未经我同意在文妥公司给我安排会计职务，但我从未在公司上过班，没有领取过工资。我不清楚“文妥财富”P2P 平台的情况，不清楚文妥公司的人员架构，也不知道文妥公司哪些员工是周稳妥比较信任的、跟周稳妥接触较多。我认识梁建生、朱某万、周某阳、周某云、王某洋、张某、周某发、周某宇、周某满、朱某华、凌某栋、宋某亮、周某晶。我不清楚周稳妥玩“快乐十分”网络赌博游戏的情况，我不认识李某，见过邓某几次，他是河源龙川人，认识周稳妥有两年了，具体从事什么行业我不清楚。我认识叶小军，好像也是龙川人，他和周稳妥 2012 年认识，一起从事民间借贷生意。叶小军 2013 年在惠州鸿润花园后面开了一间茶庄（名字不记得）。周稳妥的债主反映，2015 年 1 月底看到我和周稳妥，还有叶小军夫妻在惠州茶博城附近的天佑炖品一起吃早餐，情况不属实，2015 年 1 月 24、25 号左右，我回汕尾老家，上述和周稳妥一起吃早餐的女子不是我。

4、张某的证言：我是文妥公司员工，我与周稳妥之间没有签订过抵押借款合同。我名下有一辆黑色福特蒙迪欧，号牌：粤 L ×××××，车辆识别代号:LVSHBFAF19FO98178，2010 年 1 月买车时，我在建设银行麦地支行办理了购车贷款，贷款 10 万元，期限五年，车辆抵押给建设银行惠州分行，但购车后一年半左右我还清了贷款，之后没有用该辆车做过抵押，更没有用该车作为抵押跟周稳妥借款。公安机关查询周稳妥所运营的“文妥财富”P2P 平台的后台数据及建行账号交易流水记录，发现有我和周稳妥签订的抵押借款资料和周稳妥于 2014 年 4 月 29 日通过其建行 62XXXXXXXXXXXXXXX84 转账给我 76000 元的记录，经我确认，车辆抵押借款资料是伪造的，我之前毫不知情。至于周稳妥转账 76000 元给我属实，具体情况我要查询银行交易记录后才清楚。我有向周稳妥提供过车辆信息资料，时间我不记得，应该是 2014 年 9 月之前，当时周稳妥没有跟我说具体理由，叫我拿身份证、车辆信息复印件给他用一下，我当时没想这么多就给他了。

5、邓某的证言：我 2008 年开始在龙川车田镇车田村的赌场做荷官及自己做“六合彩”，2011 年 6 月 20 日因赌博被龙川县公安局治安管理大队刑事拘留。2012 年开始做高利贷生意。我听说过“快乐十分”的网络赌博游戏，但我没有参与过，也没有向他人宣传、介绍过。我没有介绍周稳妥玩“快乐十分”网络赌博游戏，也没有向周稳妥提供“快乐十分”网络赌博游戏的网址链接、账号、密码。我不认识叶小军。2012 年 10 月份左右，在惠州陈某江经朱某介绍认识了周稳妥，认识后，他以做“过桥”业务为由向我借款 30 万元，之后他就一直以同样的理由向我借款，次数越来越多，数额越来越大，直到 2014 年 12 月份，他共借我 2000 多万元，后因拖欠利息，我停止借钱给他，目前，周稳妥还欠我 1670 万元。我通过建行账号 62×××03 或者深圳农行账号转账给周稳妥的建行账号、农行账号（上述账号均记不清）。周稳妥向我支付利息的情况：利息不定，一般月息 2%-3%，他都是转账到我的建行、农行账号归还我的本金。我和周稳妥的资金往来主要是通过我的建行账号，少部分是通过农行。我和周稳妥之间，除了借钱给他做“过桥”生意，无其他资金往来。我不清楚周稳妥“过桥”生意的真实情况，没有核实过，但他准时支付利息，我就相信他。2014 年 5、6 月份我借 400 万给周稳妥（有借据），第二笔是借 600 万给周稳妥（有借据），2015 年 1、2 月我借 670 万给周稳妥（有借据）。上述三笔的资金来源其中 300、400 万元是我自己的，其余是跟亲友借的，邓某标借给我 l00 万元、邓某奋借给我 100 万元、朱某镇借给我 30 万元、

李某借给我 800 万元、谢某冲借给我 40 万元、刘某松借给我 50 万。上述借款，除周某发我没写借条，其余我都写了。我出借给周稳妥的三笔借款的借据我会叫我的律师找出来提供给公安机关。我也不清楚过了一个月，为什么我家人或律师一直未向公安机关提供我所说的借据。公安机关出示我在建设银行龙川支行 62×××03 账号的交易流水，内有编号 1-15 笔周稳妥转账给我的款项，经我核实，该 15 笔周稳妥转账给我的款项是周稳妥还我的钱。周稳妥以资金周转、做银行过桥生意为由跟我借款，我借了钱给周稳妥，所以周稳妥要还钱给我。公安机关跟我讲说周稳妥说这 15 笔是他跟我赌博支付的赌资，我不认可，周稳妥陷害我。我没有通过“文妥财富”平台以抵押房产的形式向周稳妥借款 60 万，我现在名下没有房产，不可能做过抵押。经我确认借款合同、借据等信息，这些资料中的借款合同、借据等信息不是我的，所有签名都不是我的，其中只有身份证是我的。我的身份证没有出借给周稳妥使用过。2009 年，我在深圳经朋友彭某勇介绍认识李某，据说他在深圳做投资公司，我和他之间有债务关系，认识后，我陆续向他借钱来放贷，共向他借了 1000 多万元，因为我信用好，跟他很熟，没写借据、没抵押，现在还欠他约 600 万元没还，他从深圳农行的账号转给我深圳农行的账号。李某有无参与“快乐十分”网络赌博游戏我不知道，他没有向我提供游戏的网址链接、账号、密码。

6、周某云的证言：我是周稳妥堂弟。2013 年 4 月周稳妥注册成立了文妥公司，叫我负责财务，主要是帮他操作网银转账，帮他转账至指定的银行账号。至 2015 年 1 月底，周稳妥因被债主追债失联，我离开公司。周稳妥之所以安排我到公司工作，是因为 2014 年 4 月我借给他 70 万元，没写借据，我爸从 2011 年 10 月至 2013 年 9 月合计借了 150 万元给周稳妥，他为了让我放心，安排我在公司工作，而且我们是堂兄弟，帮他转账汇款，他比较放心。帮他操作网银转账的情况：从 2013 年 4 月上班起，周稳妥把他在农业银行、建设银行、中国银行、惠州农商银行、招商银行及他妻子王某红在工商银行开设的网银 U 盾交由我保管，他需要向线下的债主转账汇款时，先将对方的账号和开户名告知我，再打电话给我告诉我具体的转账金额，我按他指示将款项转到指定账户。2014 年 4 月，文妥公司开始运营“文妥财富”网络借贷 P2P 平台后，当平台用户需要提现时，我负责审核，审核通过后我用周稳妥的招商银行账户转给平台用户。经用我在“文妥财富”网络借贷 P2P 平台后台（网址:sys.wtdai.com）的账户查询，周稳妥、王某红的具体银行账号有：（1）周稳妥的农业银行网银关联了三个账号：62×××76（线上投资者充值账号），62XXXXXXXXXXXXXXX12（线下投资者收款或者汇款给周稳妥用），62XXXXXXXXXXXXXXX73 作为应付投资者的备用金。（2）周稳妥的建设银行网银，关联了两个账号：62×××00（线上投资者充值账号），62XXXXXXXXXXXXXXX84（线下投资者收款或者汇款给周稳妥用）。（3）周稳妥的中国银行网银账号:60×××05（线上投资者充值、线下投资者收款或汇款给周稳妥用）。（4）周稳妥的惠州农商银行网银账号不详（线上不用此账号，线下投资者也很少用）。（5）周稳妥的招商银行账户：62×××88（用于给线上投资者提现转账和公司日常开支）。（6）王某红的工商银行网银关联了两个账号:62×××41（线上投资者充值账号），22XXXXXXXXXXXXXXX51（线下投资者收款或者汇款给周稳妥用）。通过我的后台账号查询得知，“文妥财富”网络借贷 P2P 平台至今注册用户总数 3222，实际有投资的人数为 945，资产总额为 3210 万元，实际资产总额大约是 2700 万元左右，资产总额包括用户的投资本金和利息。从“文妥财富”后台导出的数据中资产总额为 3210 万元，我却说实际资产总额大约 2700 万元左右，是因为有 10 个左右的假用户是周稳妥为了安抚投资者，吸引更多投资者，指使运营部的王某洋和我注册假用户，通过虚填投资金额的方式，将未“满标”的标的投满。只有周稳妥安排我和王某洋去虚假投标，我和王某洋才去操作。是周稳妥自己收集标的资料，然后交给王某洋，由王某洋负责将标的发布在“文妥财富”平台上。“文妥财富”从运营至今发布标的的数量及涉及资金总具体数量及资金总额我不清楚，开始运营“文妥财富”平台

时，每天发布一、两个标的，到后期每天发布四、五个，每天发布标的的金额也从十几万上涨到四、五十万。该标的的真实性具体我不清楚，2014 年 4 月份“文妥财富”平台上线时，我问过这些标的的真实性，周稳妥说都是真实的，我不清楚“文妥财富”平台上标的来源。周稳妥没有安排人员负责审核标的，这些标的的资料都是他准备的。我认识叶小军，2013 年 4、5 月叶小军来文妥公司找周稳妥，周稳妥介绍我认识叶小军。我认识钟某梁，2013 年钟某梁来公司找周稳妥，周稳妥介绍我认识钟某梁。我不清楚周稳妥、叶小军、钟某梁有无业务来往，据我所知，钟某梁有借钱给叶小军（数额不详，据其他投资者说金额上千万元），我听周稳妥说他和叶小军在做银行短期拆借业务（“过桥”）。之前一直都不清楚周稳妥赌博的情况，周稳妥被公安机关抓获之后，我才听债主说他有参与赌博。我不认识李某，我帮周稳妥转账给他，转账记录显示李某是深圳的银行账号，有工商银行、农业银行、建设银行等银行的账号。我不清楚周稳妥为何转账给李某，我通过这些账号帮周稳妥转账给李某，62XXXXXXXXXXXXXXX12（农业银行）、62XXXXXXXXXXXXXXX84（建设银行）、62×××51（工商银行），以王某红 22XXXXXXXXXXXXXXX51 的账号居多。我印象中，从 2014 年 4 月份后，周稳妥开始安排我给李某转账，每个月大概转账两、三次以上，每次 200 万元左右，直到 2014 年 10 月份之后我较少看到这个名字，转账的总金额我不清楚。平台的网站系统自动记录，我有作粗略统计，从平台上线 2014 年 4 月到 2015 年 1 月份，我有记录每天资金进出的情况，这些文件我保存在我的办公桌面上。我老婆在“文妥财富”投资 2 万多元，两个妹妹分别投资 1 万多元，都没归还本金。

7、朱某的证言：2011 年 7、8 月，周稳妥经人介绍来我经营的双基信用担保公司借钱，然后我们认识，之后往来逐渐增多。2012 年，我听说周稳妥也做民间借贷，偶尔会打电话向我借钱，之后业务往来增多逐渐熟悉。2014 年 2 月，周稳妥向我了解网络借贷 P2P 平台的情况，并提出想开展此项业务，经洽谈价格后，以 30 万元包括平台开发、人员培训、一年维护期达成协议，并签订合同。2014 年 4 月 12 日，“文妥财富”P2P 研发成功正式上线，人员培训工作也完成了。期间，周稳妥偶尔因为线下借贷业务资金不足会向我借钱，之前他都能准时还款。周稳妥前前后后向我借款的总数应该有 2000 多万元，2014 年 12 月分别向我借两笔合计 550 万元直到现在仍无法归还，该两笔借款是由钟某梁、叶小军担保的。我一般通过我的招商银行账户和我的工商银行账户向周稳妥支付借款，都是我安排我公司的财务黄某博操作网银转账的，转到周稳妥的建设银行、农业银行、招商银行账户或者他妻子王某红的工商银行。2014 年 12 月份后，因为“文妥财富”平台提现困难，周稳妥经常向我咨询解决意见，我当时教他一定要面对此事，不能逃避，但周稳妥期间失踪过两次，后来周稳妥就被公安机关抓获了。2014 年 2、3 月份经周稳妥介绍认识的叶小军，叶小军经营亿丰担保公司，周稳妥向我借钱经常是由叶小军作担保。我认识钟某梁，是通过叶小军认识的，2014 年 12 月份我出借给周稳妥的最后一笔 350 万元的借款是钟某梁作担保。2014 年 11 月份，钟某梁在叶小军经营的亿丰达担保公司向我提过：他和叶小军、周稳妥是一起做民间借贷的，当时叶小军、周稳妥都在场肯定了钟某梁的说法。我没听说叶小军、周稳妥、钟某梁做银行短期拆借的事，也没听说过叶小军、周稳妥参与网络赌博的情况。

8、叶某的证言：2010 年左右我认识周稳妥，我们是老乡。公安机关刚出示叶小军（身份证、陈某民（身份证、宋某彬（身份证）和韩某来（身份证）的户籍照片，我都不认识。我使用的手机号码 134××××2339，不是实名注册的，是 2014 年 6、7 月我在惠州惠城区麦地景园商务酒店对面的手机维修店购买的，我没有其他手机号码。公安机关向我出示的 11 份《借款过桥合同》及《借据》，我之前从未见过，今天才看到。我不清楚该合同上为何有我的电话号码，可能是周稳妥告诉叶小军我的联系方式，不是我写上去的。

9、李某的证言：侦查人员给我看“文妥财富”编号 97、229、586 号抵押借款标的，资料中涉及的房产、车辆等信息不是我本人的，我没有用房产、车辆等物品向周稳妥抵押借

款。我没有向周稳妥借钱，也没有跟叶小军、周稳妥赌博。

10、周某华的证言：我是周稳妥的表弟。我是在五星国墅园周稳妥的1208房住的时候认识了叶小军。周稳妥被公安机关抓后，我才想起2013年在国墅园1208房和2014年12月份在万饰城3001房进行网络赌博的事。我后来才知道周稳妥、叶小军他们在一起玩赌博。我记得他们会一前一后或者一起去开房，开完房后，他们会一个人先去休息，一个人开电脑，然后凑过来一起讨论。经常会听到他们讨论第一个球买单还是双和今天又没买中的话。

（三）书证、物证

1、受案登记表、立案决定书，证实案件的来源及由此启动的侦查程序合法、有效。

2、叶小军、周稳妥、钟某梁线下借款详情表、利息支付表，叶小军、周稳妥、钟某梁线下担保统计表，证实经叶小军、周稳妥、钟某梁签名确认，叶小军、周稳妥骗取曾某等63人共人民币31506.2万元；叶小军、周稳妥先后支付利息人民币8321.86万元给曾某等人。

3、借条、借款借据复印件，证实经叶小军、周稳妥、钟某梁确认，借条及借款借据上的借款及担保情况属实。

4、《证明》，证实2015年1月12日，叶小军、周稳妥、钟某梁三方出具了一张证明，由叶小军、周稳妥、钟某梁三方共同签字的所有借据，经三方协商同意，由叶小军、周稳妥两方承担一切债务，与钟某梁无关，此证明有见证人曾某签名确认。

5、线上吸收资金情况统计表、借款标的统计表、报案统计表，证实经周稳妥签名确认，统计表上的名单及吸收资金情况是其所运营的“文妥财富”P2P平台受害投资者的受害情况，共骗取林某等140人本金人民币11165151.97元。

6、“文妥财富”P2P平台下载投资标的，证实经周稳妥签名确认，由其所运营的“文妥财富”P2P平台下载并打印，除编号3、4、6、32、59、79、315、320、662、682、689号标的外，其他标的材料由叶小军伪造并提供，再由其发布在该平台上。

7、“文妥财富”P2P平台报案者报案材料（经被害人签名确认），证实受害人林某等人在“文妥财富”P2P平台的充值和损失等情况。

8、中国工商银行保管箱租约、借款过桥合同，证实叶小军为安抚被害人而伪造的虚假材料。

9、银行交易明细流水清单，证实周稳妥及其前妻王某红、钟某梁、叶小军的银行卡号曾由各被害人转入大笔资金，目前均仅有几十至数百元余额等情况。

10、企业机读档案登记资料，证实惠州市文妥实业投资有限公司于2013年3月22日成立，周稳妥占股份90%，周某发占股份10%。

11、协助查封通知书及惠州市房屋权属档案信息查询结果、商品房预售合同登记备案、预告登记信息查询结果，证实侦查机关依法对周稳妥及其前妻王某红、叶小军的前妻林某媛所有的5套房产进行了轮候查封，并查询了王某红及林某媛已签订买卖合同的2套房屋进行了查询。

12、抓获经过，证实叶小军系自动投案。

13、常住人口基本信息，证实叶小军的出生时间、户籍地址等基本情况。

（四）勘验、检查、辨认等笔录

1、辨认笔录：叶小军分别辨认出周稳妥、钟某梁；周稳妥分别辨认出李某和邓某；证人周某华辨认出叶小军就是2013年至2014年期间与周稳妥在惠城区五星国墅园1208房、万饰城3001房等地一起玩网络赌博游戏的叶小军。

2、指认笔录：

（1）叶小军分别指认了其线下借款详情和作为出借人或担保人的借条、其与周稳妥一起伪造的其作为贷款人的文妥实业投资有限公司《借款过桥合同》和借据等材料。

（2）周稳妥分别指认了线下借款统计表、线下借款详情、线上吸收资金情况统计表、

作为出借人或担保人的借条等材料；指认了其银行账号与李某、邓某银行交易流水为其所付赌博资金。

（3）钟某梁分别指认了其作为借款人和担保人出具给债权人的借条，借款统计表等材料。

（4）证人邓某指认“文妥财富”平台下载的在其名下的房产抵押借款资料是假的，该房产并非其名下所属。

（5）证人叶某指认了11份《借款过桥合同》及《借据》，指出其从未见过上述材料，手机号码134××××2339是其从2014年7月份开始使用至今。

（6）证人李某指认了在“文妥财富”P2P平台下载的编号为97、229、586借款材料，指出上述材料均是伪造的，其没有向周稳妥借款，抵押物也不是其本人的。

（7）证人王某洋指认由其账号登录“文妥财富”P2P平台的后台提取并整理的资料是“文妥财富”P2P平台上借款标的详细情况。

（8）证人张某辨认在“文妥财富”P2P平台下载的在其名下的车辆抵押借款协议资料是伪造的。

（五）视听资料：

1、讯问同步录音录像，证实侦查机关依法对叶小军进行了讯问。

2、三环装饰城录音，证实叶小军、周稳妥及钟某梁在三环装饰城召集债主开会的内容。

（六）同案人及上诉人的供述和辩解

1、同案人周稳妥供称：2012年10月，我通过朋友介绍知道了“快乐十分”网络赌博游戏，从邓某处获取了网址、账号、密码，然后开始和叶小军一起玩。我和叶小军约定好一起下注，一起分赌资。我迷上“快乐十分”后，开始以和叶小军、钟某梁合伙做银行“过桥”业务的名义去骗钱。我和叶小军赌博共输了8、9千万元，为筹集赌资，2012年12月，我和叶小军以银行“过桥”业务名义通过钟某梁帮我们借钱，前后大约筹集一亿多元资金。我线下借了约5000多万元，线上通过在“文妥财富”网络借贷P2P平台发布假“标”的方式筹集了2000多万元资金，至于叶小军线下的借款情况我不是很清楚。我和叶小军没有真实从事“过桥”业务，很多债主反映称我和叶小军在工商银行惠州分行开设保险柜存放银行“过桥”业务的凭证，这些凭证都是叶小军伪造来安抚债主。钟某梁之所以会帮我和叶小军筹集资金，是因为钟某梁认识叶小军多年，对叶小军比较信任，而且我和叶小军会支付其1%左右的利息。借款人通过银行转账方式，将借款转到我、我妻子王某红、叶小军的工行账户。我与线下债主约定的利息是5天或10天的借款，一般是4%-5%，月息超过10%。我在“文妥财富”P2P平台发布的“标”只有约200万元是真实的，其余总额1800多万元的“标”是我伪造的。我通过伪造房产、车辆等假证，叶小军也会拿线下债主的房产、车辆等信息资料给我，我拿到上述假资料后就安排公司技术员王某洋在平台发布这些假“标”。2014年4月，我委托朱某帮我搭建“文妥财富”网络借贷P2P平台，从朱某处购买服务器，他帮我培训客服、技术等人员，后期为了安抚线上投资者、线下债主，好让他们继续借钱给我，我才发布假“标”骗钱。线上投资者直接转账至我招商银行账户。我所收到线上投资者的钱来支付我和叶小军借款利息和公司日常开支。我和叶小军之间资金往来分不清楚、没有做账，我和他共同承担借款本金和利息。2015年1月11日，叶小军和我、钟某梁又重新出现在三环装饰城三楼304室，召集所有债主开会，承诺会归还债主的钱，并告诉债主会通过“文妥财富”P2P平台骗线上投资者的钱来还线下债主的欠款。后来，为了躲避线下债主，我2015年1月31日让公司停业关门，直到2015年2月2日被公安机关抓获。钟某梁之所以在我和叶小军的借款借据上签名作为担保人，是因为2015年1月11日太多债主在在三环装饰城逼我和叶小军还钱，且我和叶小军告诉钟某梁不需要他负责，只要他签名作担保人先安抚债主。钟某梁帮我融了1000多万元，我和钟某梁约定我向其支付月息百分之十二、十三作为

回报，钟某梁则赚取其中百分之五的月息。我和叶小军通过虚构从事银行短期拆借业务的方式所借资金总额约5、6千万元。我弟周某治经营的汇通投资的情况是没有注册的公司，作为文妥公司的分公司，地址在河源建设大道锦天大厦13楼，基本没有业务。

公安机关给我看我的建行流水，有15笔交易记录是我向邓某支付的赌资。我所注册登记的惠州文妥实业投资有限公司没有从事金额业务的相关资质。我伪造大量虚假标的资料上传至“文妥财富”P2P平台。公安机关根据“文妥财富”P2P平台报案人的材料统计制作的线上受害投资者投资情况表给我看，经我确认属实。公安机关根据我和叶小军、钟某梁线下受害人的报案材料统计制作线下借款情况表给我看，经我确认，邹某华和邹某文的借款的实际借款人是叶小军，当时叶小军把借条拿给我，在借款人那栏也签了我的名，但钱是叶小军借的，其他我所借的款项情况属实。叶小军借款的部分，除了曾某、黄某平、陈某城、叶某安、黄某生、蔡某生、陈某好、刘某文的借款我清楚是真实的，其他的我不清楚；钟某梁借款的部分，除了黄某平、刘某文的借款我清楚是真实的，其他的我不清楚。我和叶小军线下自筹及通过钟某梁筹集的资金总额近3亿元。上述近3.3亿款项主要是付息和支付赌资，有近9000万是我和叶小军用于支付赌资，其余主要是支付借款人的利息。2015年1月17日，我有过自首的想法，也和叶小军去过公安机关，当时接待我的民警告诉我现在没人报案，要求我和叶小军写清楚我们的犯罪情况，但叶小军受到债权人的恐吓，就要我快点走，不要被债权人抓到，后来我们没有写犯罪情况就先走了。我资金出现困难后，一直与债权人协商还款事宜。1月17日后我没有继续前往公安机关说明自己的犯罪情况，是因为我和线上债权人已协商成功了，就没有自首的打算了。我举报了邓某、李某赌博一事，我希望检察院和法院考虑我的情节及立功表现。

公安机关向我的刘某文提供的15张借条复印件，其中有7张借款人注明是我，经我确认，上述借款属实。刘某文从2012年10月开始，陆续借了9205万给我、钟某梁和叶小军，其中借了2710万给我，月息9%。直到公安机关抓获我之前都有支付利息给刘某文，支付了多少记不清，估计已超过本金。

公安机关根据报案人的报案材料制作了我、钟某梁、叶小军三人的借款、利息情况统计表，经我确认，部分属实。我认可借款理由、借款金额、出借人与我的关系，但是月利息和已支付的利息与我掌握的情况有出入。我掌握的情况是：我借款前认识有熊某峰，月息5%；叶某城，月息10%；朱某万，月息5%；骆某强，月息5%；陈某财，月息6%；张某，月息5%；黄某辖，月息10%。借款前不认识的有叶某明，月息10%；刘某文，月息7-9%；叶某安，月息8%；罗某浓，月息3%；蔡某生，月息10%；至于已支付的利息，由于出借人太多，时间太久，我无法暂时计算清楚。至于，邹某华、陈某好、邹某文的借条我是2015年1月初在华西广场304房被迫签名的。至于方某灿，我不认识他，也不清楚借款的情况，但借条我是认可的。

2、同案人钟某梁供称：2013年4月至2014年10月，我分别借了2825万元给叶小军、借了270万给周稳妥。借据情况:2014年3月10日借70万元、2014年12月10日借200万元给周稳妥；2014年1月15日借420万元、2014年5月1日借900万元、2014年10月1日借865万元给叶小军。此外，我亲戚张某崇于2014年10月6日借了100万元、苏某忠2014年8月25日借了540万元给叶小军，这两笔借款是张某崇和苏某忠把钱给我，由我转交给叶小军，叶小军直接写了借据给他们两人，所以叶小军认这两笔借款的债权人是我。上述借款无抵押，利息是月息2.5%。借款给叶小军、周稳妥是2013年至2014年之间发生的，而借据之所以全部是2014年写的，这个涉及周稳妥借款的借据的实际借款日期与借据时间是相符，涉及叶小军的借款有部分是2013年发生的，后来为了便于统计在2014年重新写的借据。叶小军、周稳妥向我借款他们说用于个人银行业务短期拆借（俗称资金“过桥”）。我借给叶小军、周稳妥钱之所以均汇入叶小军和王某红的账户，是因为他们合伙做生意，每

次汇款都按照他们的要求做。我有收到叶小军和周稳妥支付的利息。上述我借给叶小军、周稳妥的款项，约 900 万元是我本人的，其余 2000 多万元是我向其他人借了之后再转借给叶小军、周稳妥。我与吴某霞等人是朋友、亲戚关系，我有支付利息给吴某霞等人，部分支付到 2014 年 12 月、部分支付到 2015 年 1 月，其中部分支付现金，部分通过银行转账。我还介绍他人向叶小军、周稳妥借款或替叶小军、周稳妥做担保向其他人借款，其中曾某借 3402 万给叶小军、借 800 万给周稳妥；陈某城借 750 万给叶小军、黄某平借 348 万给叶小军都是我担保。我之所以做担保，是因为这部分借款开始是我向曾某、陈某城、黄某平借的，也是我写借据给他们的，后来他们知道我把钱转借给了叶小军、周稳妥，所以他们要求要叶小军、周稳妥重新写借据，我做担保。2015 年 1 月 9 日至 10 日，叶小军失去联系。11 日下午，我在河南岸汽车站找到叶小军，当时我通知曾某等 4 人把叶小军带到三环装饰城（后来债权人陆续有五、六十人）逼问叶小军借款去向和为什么关机，结果叶小军说所借款已被用于赌博和支付借款利息，其他债权人知道情况后觉得我和叶小军、周稳妥是一起合伙做生意的，所以他们就逼我在他们借款给叶小军的借据上的担保人一项签下我的名字，要我作为借款担保人，具体借款情况我也不清楚，当时比较混乱，有些人我都不认识。我只收取借款的利息和抽取转借款项的利息差。

2014 年 10 月 19 日，叶小军带我和曾某去工商银行惠州分行江北支行，把存放在银行保险柜的银行业务短期业务单据给我们看，经统计，涉及业务金额约 l.48 亿元。2015 年 1 月 11 日，在三环装饰城华熙广场，周稳妥告诉我们上述单据都是虚假的，是为打消我们的疑虑而伪造，不过他们确实是有做银行短期业务生意。此外，周稳妥还跟我们说他还利用其开设的网络 P2P 融资平台骗取其他投资者的钱来还我们的借款利息。

2013 年 4 月至 2014 年 12 月底，我共帮叶小军和周稳妥介绍了十几个亲友客户，总共帮叶小军和周稳妥拉了 9000 万元左右款项，共收到他们 4 万元的“介绍费”。叶小军和周稳妥拖欠的本金约 9000 万元，拖欠的利息我不清楚，但我知道叶小军和周稳妥从 2014 年 12 月份开始没有支付利息。从 2014 年 4 月份到 10 月份，我向叶小军和周稳妥介绍的借款人签订的借据中借款人是我，叶小军和周稳妥作为担保人；10 月之后，叶小军和周稳妥作为借款人，我作为担保人。

我至今不清楚叶小军和周稳妥所说的银行“过桥”业务的真实，我现已变卖家产偿还部分借款，会尽力去偿还借款人的借款。我是没有欺诈亲友的。我也是被叶小军和周稳妥欺骗的。周稳妥和叶小军有承诺我的 0.5%利息差（介绍费）连同归还的本金和出借的利息一起转账给我父亲钟某泉的工商银行账号，但是我的父亲的工商银行的网银一直由叶小军的表弟波仔支配的，我没有用这 0.5%利息差，又被叶小军转走了。

据报案人黄伟某等 14 人提供给公安机关的报案材料，我以月息 2.5%不等的利息，向黄伟某等 14 人借款约 1810 万元的情况属实。我作为借款人的款项有 3000 多万，我作为担保人的款项有 5000 多万。我亲戚通过我借钱给周稳妥、叶小军的有邓某芳借了 330 万元、苏某忠借了 350 万、邓某芬借了 170 万、我本人借了 70 万，均未归还。我上述亲戚没有跟周稳妥、叶小军签订借据，只有邓某芬和我签订了借据，其他人没有签。

我认识刘某文，向其借了 1530 万元，此外其借款给叶小军、周稳妥约 7675 万元我做了担保。2013 年 12 月至 2014 年 7 月，我分多次陆续向刘某文借款 1500 万元，7 月 4 日，经协商我把 1500 万元借款汇总成一张借条，2014 年 12 月我又分两次向刘某文借款 30 万元，2015 年 1 月 7 日写了借条，上述借款月息 2%。刘某文是通过他的工商、农业银行、还有余某强的建设银行转给我父亲钟某泉、叶小军和周稳妥妻子王某红账户。刘某文借款利息由叶小军、周稳妥直接支付，我该赚的利息差叶小军、周稳妥并没有支付给我。公安机关刚给我出示刘某文提供的 15 张借条复印件，其中 2 张借款人是我，其余借条担保人是我，经我核对属实。具体他们借给我们的钱的来源我也不清楚。我之所以做担保，是因为刘某文和黄某

良比较信任我。上述借款本金未还给叶某文、黄某良。刘某文、黄某良借给我的1530万元没有包含在我之前向公安人员所交代的转借给周稳妥、叶小军的对外借款中。

3、上诉人叶小军供称：2011年开始，我先后认识了周稳妥和钟某梁，那时我们三人都在从事放贷生意，并开始相互间有资金往来，直到2013年初周稳妥提出来，他、我和钟某梁要合伙一起做放贷生意，我和钟某梁同意了，于是到了2013年6月份我们三人就对外向借款人宣称我们三人一起做“过桥”银行拆借业务，用这种方式来向线下借款人吸收资金。直到2014年底我们三人一共向线下借款人吸收了大量资金，我自己通过这种方式吸收了5000万元左右，钟某梁和周稳妥吸收了多少资金我不清楚。到了2014年9月开始，我们开始出现付息困难，之后资金越来越紧张，到了2014年12月份，就无法向线下借款人支付利息了，那些借款人开始逼我、周稳妥、钟某梁还钱，于是我和周稳妥就商量逃跑了，直到今天（2015年6月2日）我向公安机关自首。我们没有真实从事“过桥”业务，我在工商银行惠州分行开设的保险箱中存放的11份“借款过桥合同”都是我和周稳妥一起伪造的。我自己以“过桥”名义借了5000万元左右，还有1.5亿元左右的实际借款人是钟某梁，但由我在借据上签名作为借款人。我将上述约2亿元资金都转借给周稳妥了，但没有写借据。

2012年夏天，当时周稳妥在三环装饰城8楼租了一间办公室做放贷业务，他找到我说需要资金，要我借钱给他，我就从那时起长期借钱给他，他到期就给我一定的利息，利息数额由我和周稳妥协商确定。2014年6月份左右，周稳妥的资金出现紧张，回款和利息都开始不准时了，于是我多次逼问他，直到2014年10月周稳妥告诉我他一直宣称的“银行过桥”业务是假的，是他虚构的。因为我借给周稳妥的资金，有90%以上都是我通过钟某梁去向借款人筹集的，2014年10月份开始，钟某梁多次逼问我资金的去向及过桥业务的真实，我为了稳住钟某梁，就答应和周稳妥一起伪造了上述11份虚假的《借款过桥合同》。2013年4月份开始，我通过钟某梁调第一笔钱的时候，钟某梁就知道我是将钱转给周稳妥，一直以来钟某梁都知道他帮我筹集的资金都是转给周稳妥。2014年12月左右，钟某梁逼问我资金的去向，我就逼问周稳妥资金的去向，周稳妥告诉我他借我的钱一部分玩“快乐十分”网络赌博游戏输掉了，一部分用于支付借款利息。我有参加“快乐十分”网络赌博游戏，2011年底开始玩，大概玩了2、3个月，之后就没玩了，该游戏的账号、密码、网址是2012年周稳妥提供给我的。周稳妥玩该游戏是跟邓某、李某下注。

公安机关根据报案材料制作了我、钟某梁、周稳妥三人的借款、利息情况统计表，经我确认，部分属实。我认可借款金额，但是借款理由、出借人与我的关系、月利息和已支付的利息与我掌握的情况有出入。

利息及付息情况：黄某平月息5-6%，已支付约200万元；余某月息6%，已支付约5万元；曾某月息5-6%，已支付约1500万元；蔡某生和黄某生的借款是一起的，月息6-8%，已支付约1500万元；叶某安月息8%，已支付约200万元；郑某曼月息4%，已支付约100万元；张某明月息2%，已支付约2万元；曾某萍月息3%，已支付约12万元；彭某玲月息3%，我已支付约30万元；邹某华月息3%，已支付约3万元；蔡某强月息4%，已支付约300万元；陈某媚月息4%，已支付约7万元；赖某香月息4%，已支付约3万元；陈某婵月息4%，已支付约7万元；赖某波月息4%，已支付约24万元；潘某满月息4%，我已支付约16万元；邹某文月息5%，已支付约20万元；赖某发月息3%，已支付约7万元；周某生月息4%，已支付约10万元；王某飞月息4%，已支付约3万元；刘某文月息6-8%，总借款金额是4960万，具体支付了多少利息我暂时算不清楚，但已超过本金；邹某华月息3%，已支付约2.2万元；陈某好月息4%，已支付约70万元；邹某文月息3%，已支付约8万元。

跟出借人的关系：借款前认识的有曾某、黄某平、邹某华、蔡某强、邹某文、邹某文。借款前不认识叶某安；刘某文、余某借款前不认识、都是钟某梁介绍认识；蔡某生、黄某生借款前不认识、都是叶某城介绍认识；郑某曼借款前不认识、罗东阳介绍认识；曾某萍、彭

某玲借款前不认识、都是曾某介绍认识；赖某发借款前不认识、邹某文介绍认识。张某明、陈某伟、杨某文、陈某眉、赖某香、陈某婵、陈某萍、陈某强、赖某波、潘某满、张某崇、苏某忠等人均不认识、没见过。

借款理由：对郭某、叶某安、邹某华、邹某文、周某生、王某飞、邹某文的借款理由均为普通借贷。

我名下有一家亿丰信用担保公司，大约是在2014年2、3月份在惠州注册成立的。大约在2014年3、4月份，周稳妥向我借了亿丰信用担保有限公司的营业执照，我就借给了他。直到2014年12月底，我浏览文妥财富的官网，才发现网站上贴出了亿丰信用担保有限公司的营业执照，并且贴出了一份《担保函》，内容大致是文妥财富P2P网络借贷平台是由亿丰信用担保有限公司进行担保。但这些都是在我不知情的情况下周稳妥私自贴出了亿丰信用担保有限公司的营业执照，并且伪造了《担保函》。当时周稳妥说他有客户想看亿丰信用担保有限公司的营业执照，叫我借给他。我不认识周稳妥所说的客户。我既不知晓周稳妥向我借亿丰信用担保有限公司的营业执照的具体用途，又不清楚他所称的客户的具体情况，仍出借亿丰信用担保有限公司的营业执照是因为我信任他。大约2015年1月份，我去周稳妥位于花茂的办公室找他，问他为何私自在文妥财富的官网贴出亿丰信用担保有限公司的营业执照和伪造《担保函》，并要求他立即将这些东西从文妥财富的官网上撤下来，他向我解释这些“不关事的”，并且称他正在办理另一个担保公司的营业执照，到时执照办出了就把亿丰信用担保有限公司的营业执照和《担保函》从文妥财富的官网上撤下来。而且亿丰信用担保有限公司的经营范围并不包括融资性担保，周稳妥这份《担保函》是没用的。

2015年1月10日，在三环装饰城三楼，因为我和周稳妥的大部分债主都是通过钟某梁介绍才认识我们，所以当时在场的债主表示他们不认和我、周稳妥的借贷关系，只认钟某梁，并要求钟某梁在我和周稳妥的借条上签名作担保，钟某梁也同意这么做。

对于上诉人叶小军及其辩护人提出的辩解和辩护意见，查证并评判如下：（1）涉案的“文妥财富”P2P网络平台网页上显示亿丰担保有限责任公司为该P2P平台的担保公司，并有相应的《担保函》，对此叶小军予以供认，且其还供认亿丰担保有限责任公司为其名下的公司。周稳妥供认指证叶小军也会拿线下债主的房产、车辆等详细资料给周稳妥在平台上发布假“标”；周稳妥对“文妥财富”P2P平台下载投资标的进行了签认，称涉案投资标的由其所运营的“文妥财富”P2P平台下载并打印，除编号3、4、6、32、59、79、315、320、662、682、689号标的外，其他标的材料由叶小军伪造并提供，再由其发布在该平台上；其和叶小军、钟某梁在三环装饰城三楼304室召集所有债主开会，承诺会通过“文妥财富”P2P平台用线上投资者的钱来还线下债主的欠款。被害人郭某证言称据其所知是叶小军和周稳妥一起做“过桥”业务和运营“文妥财富”P2P平台，该平台上大部分都是假“标”；被害人黄某平证称在2014年6-8月叶小军和钟某梁要求过其和其他债主提供车、房等资产信息，以此伪造假“标”放在“文妥财富”P2P平台上供投资者投资；被害人黄某平、余某、曾某、陈某城等证称周稳妥和叶小军、钟某梁在三环装饰城在所有债主面前承诺会把“文妥财富”P2P平台业务做大，用线上融资所得的款项给线下债主支付欠款。以上证据相互印证，形成的证据链足以证实叶小军参与了“文妥财富”P2P网络线上集资诈骗的事实。叶小军否认参与“文妥财富”P2P网络平台线上集资诈骗及辩护人所提相关意见，不予采纳。（2）同案人周稳妥供述称其与叶小军迷上“快乐十分”网络赌博游戏后，为筹集赌资，两人以银行“过桥”业务的名义进行“借钱”；证人周某华证称叶小军于2013年至2014年期间与周稳妥在惠城区五星国墅园1208房、万饰城3001房等地一起玩网络赌博游戏，并辨认出叶小军；叶小军虽在一审庭审及上诉否认但在侦查阶段曾供述称其有参与“快乐十分”网络赌博游戏；此外，本案还有被害人黄某平、余某、曾某等证称听叶小军说叶将所骗的借款用于赌博。以上证据相互印证，足以认定叶小军将所骗的借款用于赌博的事实，叶小军上诉及辩护人所提

叶小军没有将“借款”所得用于赌博的意见不予采信。（3）在案证据不能证实钟某梁受雇于叶小军，故叶小军上诉所提其与钟某梁没有雇佣关系的意见，予以采信。（4）关于叶小军是否有自首情节的问题，抓获经过证实2015年6月2日9时许，惠州市公安局经济犯罪侦查支队接林某媛报案称其丈夫即叶小军在位于惠城区麦地鸿润花园F栋1403房中，要求向公安机关投案自首，该队民警前往将叶小军抓获归案，叶小军系自动投案。审讯笔录、一审庭审笔录反映，叶小军归案后虽否认参与“文妥财富”P2P网络平台线上集资诈骗（该部分涉案金额1千1百多万）、但如实供述了其伙同同案人周稳妥等虚构银行“过桥”业务进行诈骗的事实，该部分涉案金额达2亿多元，根据最高人民法院法发（2010）60号《关于处理自首和立功若干具体问题的意见》，叶小军投案后虽然没有交代全部犯罪事实，但如实交代的犯罪数额多于未交代的犯罪数额，可以认定为如实供述自己的主要犯罪事实，综上，叶小军系自动投案且归案后能够如实供述自己的主要犯罪事实，应认定叶小军有自首情节。

本院认为，上诉人叶小军以非法占有为目的，伙同他人使用虚构事实、隐瞒真相的诈骗方法，非法集资，数额特别巨大，其行为已构成集资诈骗罪，应依法惩处，其违法所得应予以继续追缴并责令退赔。叶小军自动投案且归案后能够如实供述自己的主要犯罪事实，应认定叶小军具有自首情节。原审判决认定叶小军的犯罪事实清楚，证据确实、充分，定罪准确，量刑适当，审判程序合法，唯未认定叶小军有自首情节不当，应予以纠正。叶小军虽有自首情节，但其诈骗数额特别巨大，对被害人未有实际的退赔，造成被害人重大经济损失，犯罪后果特别严重，依法不予从轻处罚。上诉人叶小军上诉及其辩护人辩护所提叶小军有自首情节的理由成立，应予支持。其它上诉理由及辩护意见不成立，不予采纳。依照《中华人民共和国刑法》第五十七条、第五十九条、第六十四条、第六十七条、第一百九十二条，以及《中华人民共和国刑事诉讼法》第二百二十五条第一款第（一）项之规定，

裁定如下：

驳回上诉，维持原判。

本裁定为终审裁定。

审判长　　傅曜天

审判员　　吴铁城

审判员　　郑小明

二〇一七年三月三日

书记员　　蓝世荣

（三）侵犯著作权罪

案例一、唐振彪、李民侵犯著作权、销售侵权复制品案

审理法院：　罗田县人民法院

案　　号：　（2019）鄂1123刑初122号

案　　由：　侵犯著作权罪

裁判日期：　2019年12月05日

罗田县人民法院

刑事判决书

（2019）鄂1123刑初122号

公诉机关湖北省罗田县人民检察院。

公诉机关湖北省罗田县人民检察院。

被告人唐振彪，男，1993年2月22日出生于广州市化州市，汉族，大学本科，系武汉森林时代科技有限公司程序员，户籍所在地广东省化州市，现住广州市天河区。因涉嫌破坏计算机信息系统罪，于2017年5月18日被罗田县公安局刑事拘留，同年6月15日被逮捕，

2017 年 7 月 13 日被罗田县公安局取保候审，2018 年 6 月 28 日被罗田县公安局监视居住。现在家。

辩护人胡素文，湖北秋筠律师事务所律师。执业证号 14201201811075871。

被告人李民，男，1991 年 1 月 17 日出生于湖南省武冈市，汉族，小学文化，个体工商户，户籍所在地湖南省武冈市，案发前住广东省深圳市宝安区。因涉嫌破坏计算机信息系统罪，于 2017 年 5 月 10 日被罗田县公安局抓获，次日被刑事拘留，同年 6 月 15 日被逮捕，2017 年 7 月 13 日被罗田县公安局取保候审，2018 年 6 月 28 日被罗田县公安局监视居住。现在家。

被告人张旺，男，1992 年 8 月 15 日出生于河北省易县，汉族，大专文化，无业，户籍所在地河北省保定市易县，案发前住北京市大兴区。因涉嫌破坏计算机信息系统罪，于 2017 年 12 月 2 日被北京市公安局丰台分局岳各庄派出所抓获，次日被罗田县公安局刑事拘留，2017 年 12 月 8 日被罗田县公安局取保候审，2018 年 12 月 8 日经罗田县人民检察院决定被取保候审。现在家。

辩护人张良，湖北神宇律师事务所律师。执业证号 14211200910219940。

被告人王子晗，男，1997 年 2 月 17 日出生河南省桐柏县，汉族，大学本科，学生，户籍所在地河南省桐柏县。因涉嫌破坏计算机信息系统罪，于 2018 年 2 月 7 日被罗田县公安局取保候审。现在家。

辩护人叶世格，湖北神宇律师事务所律师。执业证号 14211200810469877。

被告人李庆国，男，1996 年 10 月 6 日出生于山东省莒南县，汉族，大专文化，无业，住山东省莒南县。因涉嫌破坏计算机信息系统罪，于 2018 年 4 月 11 日被罗田县公安局刑事拘留，同年 5 月 9 日被罗田县公安局取保候审。现在家。

辩护人李汉文，湖北神宇律师事务所律师。执业证号 14211200810778444。

湖北省罗田县人民检察院以罗检公诉刑诉〔2019〕94 号起诉书，指控被告人唐振彪、李民、张旺、王子晗、李庆国侵犯著作权罪、销售侵权复制品罪，于 2019 年 9 月 11 日向本院提起公诉。本院依法适用普通程序并组成合议庭，公开开庭审理了本案。罗田县人民检察院指派检察员王丹出庭支持公诉。被告人唐振彪、李民、张旺、王子晗、李庆国及其辩护人胡素文、张良、叶世格、李汉文到庭参加诉讼。现已审理终结。

罗田县人民检察院指控：斗鱼直播平台所使用的软件是武汉斗鱼网络科技有限公司研发并经国家版权局合法登记，熊猫直播平台所使用的软件是上海熊猫互娱文化有限公司研发并经国家版权局合法登记，均受国家著作权法的保护。两直播平台均以人气的高低直接影响正常直播间和签约主播直播间的排位，同时是两公司考核签约主播是否达标并结算签约主播酬金的重要指标，对此两公司均对其直播间人气进行了通信保密。

2016 年 7 月，被告人唐振彪认为制作斗鱼直播间人气外挂软件有利可图，遂研发出了可以提升斗鱼直播间虚假人气的“斗鱼人气软件”、“斗鱼人气代挂”、“斗鱼弹幕软件”等软件和代挂斗鱼人气的平台，并根据斗鱼平台更新的情况不断更新软件和平台；之后还成功研发出了可以提升熊猫直播平台直播间虚假人气的熊猫代挂软件。

2016 年 7 月份至 2017 年 5 月份，被告人唐振彪通过 QQ 联系的方式发展被告人李民、张旺、王子晗、李庆国四人为其下级销售代理，李民、张旺、王子晗、李庆国四人通过互联网向斗鱼、熊猫平台的用户出售斗鱼、熊猫人气软件，从中牟取暴利。被告人唐振彪与被告人李民、张旺、王子晗、李庆国约定五五分成，唐振彪非法获利 122.267905 万元，李民非法获利 11.0827 万元，张旺非法获利 42.986305 万元，王子晗非法获利 33.0734 万元，李庆国非法获利 35.1255 万元。经鉴定，斗鱼人气外挂软件所提供的功能可对斗鱼直播平台的人气数据造成破坏，属于破坏性程序。

针对上述指控，公诉机关当庭宣读和出示了受案登记表、报案材料、营业执照、户籍信

息、到案情况、交易记录、著作权登记证书等书证，证人陈某、张某的证言，鉴定意见，搜查、检查、远程勘验等笔录，视听资料、电子数据，被告人唐振彪、李民、张旺、王子晗、李庆国的供述与辩解等证据材料。

公诉机关认为，被告人唐振彪以营利为目的，制作、销售外挂软件，违法所得数额巨大，其行为触犯了《中华人民共和国刑法》第二百一十七条第一款，应当以侵犯著作权罪追究其刑事责任；被告人李民、张旺、王子晗、李庆国以营利为目的，销售外挂软件，违法所得数额巨大，其行为触犯了《中华人民共和国刑法》第二百一十八条，应当以销售侵权复制品罪追究其刑事责任。

被告人唐振彪、李民、张旺、王子晗、李庆国及其辩护人对起诉书指控的事实及罪名均无异议。

辩护人认为被告人唐振彪、张旺、李庆国归案后均如实供述自己的罪行、被告人王子晗主动投案并同时供述自己的罪行，均系初犯、自愿认罪、积极退赃、认罪悔罪态度好、社会危害性相对较小，均建议对被告人唐振彪、张旺、王子晗、李庆国从轻、减轻处罚并适用非监禁刑。其中唐振彪家庭困难，王子晗案发时系在校大学生。

广东省广州市天河区司法局经调查暂未发现被告人唐振彪有不适宜社区矫正的情形。

湖南省武冈市司法局经调查认为，被告人李民案发前无其他违法犯罪记录，案发后如实供述犯罪事实，积极退缴非法所得，有悔罪表现；其亲属及所在村委会愿意对其进行监管和帮教，监管条件较好，如适用非监禁刑对所居住的社区没有重大不利影响，建议对李民适用社区矫正。

河北省易县社区矫正工作领导小组经调查认为，被告人张旺对社会没有现实危险性，适宜对其社区矫正。

河南省桐柏县社区矫正工作领导小组经调查认为，被告人王子晗具备适用社区矫正条件，同意接收其实行社区矫正。

山东省莒南县司法局经调查，评估了被告人李庆国对所居住社区的影响，同意对其适用社区矫正。

经审理查明，斗鱼直播平台所使用的软件是武汉斗鱼网络科技有限公司研发并经国家版权局合法登记，熊猫直播平台所使用的软件是上海熊猫互娱文化有限公司研发并经国家版权局合法登记，均受国家著作权法的保护。两直播平台均以人气的高低直接影响正常直播间和签约主播直播间的排位，同时是两公司考核签约主播是否达标并结算签约主播酬金的重要指标，对此两公司均对其直播间人气进行了通信保密。

2016 年 7 月，被告人唐振彪认为制作斗鱼直播间人气外挂软件有利可图，遂研发出了可以提升斗鱼直播间虚假人气的“斗鱼人气软件”、“斗鱼人气代挂”、“斗鱼弹幕软件”等软件和代挂斗鱼人气的平台，并根据斗鱼平台更新的情况不断更新软件和平台；之后还成功研发出了可以提升熊猫直播平台直播间虚假人气的熊猫代挂软件。

2016 年 7 月份至 2017 年 5 月份，被告人唐振彪通过 QQ 联系的方式发展被告人李民、张旺、王子晗、李庆国四人为其下级销售代理，李民、张旺、王子晗、李庆国四人通过互联网向斗鱼、熊猫平台的用户出售斗鱼、熊猫人气软件，从中牟取暴利。被告人唐振彪与被告人李民、张旺、王子晗、李庆国约定五五分成，唐振彪非法获利 1222679.05 万元，李民非法获利 110827 元，张旺非法获利 429863.05 元，王子晗非法获利 330734 元，李庆国非法获利 351255 元。经鉴定，斗鱼人气外挂软件所提供的功能可对斗鱼直播平台的人气数据造成破坏，属于破坏性程序。

在侦查阶段，被告人唐振彪退缴非法所得 70 万元、李民退缴非法所得 11 万元、张旺退缴非法所得 35 万元、王子晗退缴非法所得 20 万元、李庆国退缴非法所得 20 万元。在审判过程中，五被告人退清了下差的违法所得。

另查明，2018 年 2 月 7 日，被告人王子晗主动到罗田县公安局投案并如实供述其犯罪事实。

上述事实，被告人唐振彪、李民、张旺、王子晗、李庆国在开庭审理过程中均无异议，并表示自愿认罪，且有报案材料、受案登记表、立案决定书，相关计算机软件著作权登记证书、中国版权保护中心回复、软件著作权登记概况查询结果，代理资料，QQ、支付宝、微信等社交软件聊天记录及交易支付记录，暂扣款缴款书，户籍信息、到案情况、违法犯罪记录情况说明、缴款回执等书证，证人陈某、张某的证言，湖北三真司法鉴定中心司法鉴定意见书，搜查笔录、检查笔录、辨认笔录、远程勘验笔录、扣押发还物品清单、视听资料及电子数据光盘等证据证实，足以认定。

本院认为，被告人唐振彪以营利为目的，制作、销售外挂软件，违法所得数额巨大，其行为构成侵犯著作权罪；被告人李民、张旺、王子晗、李庆国以营利为目的，销售外挂软件，违法所得数额巨大，其行为均构成销售侵权复制品罪；均应依法追究其刑事责任，其违法所得应追缴没收。公诉机关指控的事实、罪名成立，本院予以确认。五被告人归案后均能如实供述犯罪事实并当庭自愿认罪、退清了赃款、认罪悔罪态度较好，其中被告人王子晗系主动投案，均可从轻处罚。社区矫正机关认为对五被告人均可适用社区矫正的建议予以采纳。辩护人建议对各被告人从轻处罚并适用非监禁刑的意见予以采纳。据此，根据各被告人犯罪的事实、犯罪的性质、情节和对社会的危害程度，依照《中华人民共和国刑法》第二百一十七条第一款第（一）项、第二百一十八条、第六十四条、第六十七条、第七十二条、第七十三条之规定，判决如下：

一、被告人唐振彪犯侵犯著作权罪，判处有期徒刑三年，缓刑三年六个月，并处罚金人民币 123 万元。

二、被告人李民犯销售侵权复制品罪，判处拘役六个月，缓刑八个月，并处罚金人民币 12 万元。

三、被告人张旺犯销售侵权复制品罪，判处有期徒刑一年九个月，缓刑二年，并处罚金人民币 43 万元。

四、被告人王子晗犯销售侵权复制品罪，判处有期徒刑一年，缓刑一年六个月，并处罚金人民币 34 万元。

五、被告人李庆国犯销售侵权复制品罪，判处一年六个月，缓刑一年十个月，并处罚金人民币 36 万元。

（上述五被告人的缓刑考验期限，均自判决确定之日起计算。判处的罚金限判决生效后缴纳）。

六、对被告人唐振彪的违法所得 1222679.05 元、李民的违法所得 110827 元、张旺的违法所得 429863.05 元、王子晗的违法所得 330734 元、李庆国的违法所得 351255 元，由各扣押机关予以追缴，上缴国库。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向湖北省黄冈市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本七份。

审 判 长　李怡焕
审 判 员　肖玉玲
人民陪审员　　刘胜松
二〇一九年十二月五日
法官助理　管海林
代书 记员　陈乡远

案例二、单位上海昱宫网络科技有限公司、刘某某等侵犯著作权案

审理法院： 上海市徐汇区人民法院

案　　号： （2018）沪 0104 刑初 373 号

案　　由： 侵犯著作权罪

裁判日期： 2019 年 08 月 29 日

上海市徐汇区人民法院

刑事判决书

（2018）沪 0104 刑初 373 号

被告单位上海昱宫网络科技有限公司，住所地上海市金山工业区。

诉讼代表人王亚晨，女，1995 年 3 月 24 日出生，户籍在浙江省乐清市。

辩护人李振林，上海日盈律师事务所律师。

辩护人黄楠，上海日盈律师事务所律师。

被告人刘某某，男，1995 年 1 月 4 日生，汉族，户籍地浙江省乐清市。

辩护人吴允锋，上海日盈律师事务所律师。

被告人吴某某，男，1990 年 10 月 23 日生，汉族，户籍地浙江省温岭市。

辩护人刘宪权，上海日盈律师事务所律师。

辩护人傅建平，上海七方律师事务所律师。

上海市闵行区人民检察院以沪闵检金融刑诉(2018)80 号起诉书指控被告单位上海昱宫网络科技有限公司(以下简称“昱宫公司”)、被告人刘某某、吴某某犯侵犯著作权罪，向上海市闵行区人民法院提起公诉。上海市闵行区人民法院根据上海市高级人民法院知识产权刑事案件集中管辖的规定，将案件移送至本院审理。本院于 2018 年 7 月 3 日受理后，依法适用普通程序，组成合议庭，公开开庭审理了本案。上海市闵行区人民检察院指派检察员徐某出庭支持公诉。被告单位昱宫公司的诉讼代表人王亚晨及其辩护人李振林、黄楠、被告人刘某某及其辩护人吴允锋、被告人吴某某及其辩护人刘宪权、傅建平均到庭参加了诉讼。期间，根据法律规定，本案曾延期审理。现已审理终结。

上海市闵行区人民检察院指控：腾讯科技(深圳)有限公司(以下简称：“腾讯公司”)于 2011 年 1 月 21 日开发完成并原始取得腾讯微信软件(以下简称“微信”)著作权，其计算机软件著作权登记号为 2014SRI63722。腾讯公司通过《腾讯微信软件许可及服务协议》对用户复制使用微信作出约束规定。

2016 年 8 月，被告人刘某某注册成立被告单位昱宫公司，实际经营地位于本市闵行区中春路 XXX 弄 XXX 层，主要从事计算机信息科技专业领域内技术开发、技术服务等业务。公司成立后，被告人刘某某陆续从华硕电脑(上海)有限公司购入手机，雇佣被告人吴某某针对此款手机制作了含有能改变微信功能的外挂软件的刷机包，并将刷机方法传授给公司相关技术人员，通过刷机安装上述外挂软件的方式，使该款手机的微信在未经腾讯公司许可的情况下增加了自动转发、点赞、群发等数十种新功能，并以此命名为“瞬”微商营销手机，对外销售牟利。截止案发，被告单位昱宫公司累计销售上述“瞬”微商营销手机 2381 台。

2016 年 10 月 20 日，上海市公安局闵行分局侦查人员在被告单位昱宫公司经营地查获尚未销售的手机 619 台及电脑等物。被告人刘某某于当日主动至公安机关投案，被告人吴某某于当日被抓获归案，二人到案后均如实供述了上述犯罪事实。

公诉机关认定被告单位昱宫公司及其直接负责的主管人员被告人刘某某伙同被告人吴某某，以营利为目的，未经著作权人许可，复制发行其计算机软件作品共计 2300 余份，属于有其他严重情节，其行为均已触犯《中华人民共和国刑法》第二百一十七条(一)项、第二百二十条、第三十条、第三十一条之规定，犯罪事实清楚，证据确实、充分，应以侵犯著作权罪追究其刑事责任，且符合《中华人民共和国刑法》第二十五条第一款之规定，属共同犯

罪。被告单位昱宫公司及其直接负责的主管人员被告人刘某某在共同犯罪中起主要作用，系主犯，适用《中华人民共和国刑法》第二十六条第一款、第四款；被告人吴某某在共同犯罪中起次要、辅助作用，系从犯，适用《中华人民共和国刑法》第二十七条，应当从轻或减轻处罚。被告单位昱宫公司及被告人刘某某有自首情节，根据《中华人民共和国刑法》第六十七条第一款，可以从轻或者减轻处罚。被告人吴某某到案后如实供述自己的罪行，根据《中华人民共和国刑法》第六十七条第三款，可以从轻处罚。被告人吴某某在缓刑考验期内犯新罪，根据《中华人民共和国刑法》第七十七条第一款，应当撤销缓刑，并依照《中华人民共和国刑法》第六十九条，实行数罪并罚。提请依法审判。

被告单位昱宫公司、被告人刘某某、吴某某对起诉书指控的犯罪事实及罪名均无异议。

被告单位昱宫公司的辩护人辩称，昱宫公司销售华硕“瞬”手机的行为不构成侵犯著作权罪。一、本案被告人不具有侵犯著作权罪中的“以营利为目的”。首先，昱宫公司销售的是手机而非微信或者与微信实质性相似的软件；再次，提供外挂软件下载方式是配套服务，而不是销售外挂软件，且外挂软件并未落入腾讯公司著作权保护范围；最后，微信软件可在网上免费下载且本身没有商品价值，本案不符合利用软件牟利的情形。二、本案存在事实不清、证据不足的问题。昱宫公司销售华硕“瞬”手机存在两种模式，第一种是公司预先安装搭载外挂的微信至手机后将手机售出，第二种是售出手机后，提供刷机软件供客户下载安装。其中第一种模式确实系侵权行为，认定犯罪需达到刑法规定的入罪标准；第二种模式不属于侵犯著作权中的“复制、发行”行为。且在本案中对昱宫公司两种模式销售的手机数量没有证据予以证明，起诉书也未加以区别。即便最终认定昱宫公司构成犯罪，被告单位昱宫公司也系自首，应当从轻或者减轻、免除处罚。

被告人刘某某的辩护人辩称，本案不构成侵权著作权罪。本案昱宫公司与被告人销售手机具有两种销售模式，而起诉中未将两种模式加以区分，现有证据仅能证明被告人销售的200多台华硕“瞬”手机中搭载有外挂微信软件，且该200多台未达到刑事入罪标准。

被告人吴某某的辩护人辩称，被告人吴某某、昱宫公司的行为不构成侵犯著作权罪。被告人基本未实施侵犯著作权罪中的“复制、发行”行为，其销售的华硕“瞬”手机大部分未安装搭载外挂的微信，被告人仅销售200余台装有搭载外挂微信的手机，虽属于复制发行行为，但未达侵犯著作权的入罪标准，其余销售的2100余台手机未安装搭载外挂的微信软件，仅提供增加微信功能的方法不属于复制、发行他人作品；起诉书指控昱宫公司复制发行计算机软件2300余份存在事实不清、证据不足的问题，现有证据无法证明昱宫公司销售的2381台华硕“瞬”手机全部预先安装了搭载外挂的微信，仅可勉强证明被告单位刷机安装了200多台手机；若认定犯罪，被告人吴某某具有法定从宽处罚情节，系从犯；系坦白。

经审理查明，公诉机关指控的被告人犯罪事实，有被害单位腾讯公司员工杨翔宇的报案陈述及腾讯公司出具的《计算机软件著作权登记证书》、《腾讯微信软件许可及服务协议》、被告单位昱宫公司的工商登记资料、《华硕手机经销商合作协议》及附件、证人陈某1、王某某、郑某1、黄某1、陈2、张某某、韩某、孙某某、黄某2、任某、郑某2、赖某某的证言、上海弘连网络科技有限公司计算机司法鉴定所出具的《计算机司法鉴定意见书》、上海汉光知识产权数据科技有限公司司法鉴定所出具的《司法鉴定意见书》、浙江省台州市椒江区人民法院的《刑事判决书》、上海市公安局闵行分局案件审理队出具的《搜查笔录》、《扣押清单》、《工作情况》、被告人刘某某、吴某某的供述等经庭审质证的证据予以证实，足以认定。

本院认为，综合诉辩双方的意见，本案的争议焦点主要为一、被告单位昱宫公司及其直接负责的主管人员被告人刘某某是否构成侵犯著作权罪？二、本案中被告人吴某某是否构成侵犯著作权罪的共同犯罪？三、如果构成犯罪，被告单位及被告人应承担的刑事责任？

关于争议焦点一，刑法第二百一十七条第(一)项规定，以营利为目的，未经著作权人许

可，复制发行其文字作品、音乐、电影、电视、录像作品、计算机软件及其作品的，属侵犯著作权情形之一，应按违法所得数额大小及情节严重程度处以不同刑罚。最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释第十一条第二款规定，刑法第二百一十七条规定的“未经著作权人许可”，是指没有得到著作权人授权或者伪造、涂改著作权人授权许可文件或者超出授权许可范围的情形。第十四条第一款规定，实施刑法第二百一十七条规定的侵犯著作权犯罪，又销售该侵权复制品，构成犯罪的，应当依照刑法第二百一十七条的规定，以侵犯著作权罪定罪处罚。最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释(二)第一条规定，以营利为目的，未经著作权人许可，复制发行其文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品，复制品数量合计在五百张(份)以上的，属于刑法第二百一十七条规定的“有其他严重情节”；复制品数量在二千五百张(份)以上的，属于刑法第二百一十七条规定的“有其他特别严重情节”。第二条第一款规定，刑法第二百一十七条侵犯著作权罪中的“复制发行”，包括复制、发行或者既复制又发行的行为。最高人民法院、最高人民检察院、公安部关于办理侵犯知识产权刑事案件适用法律若干问题的意见第十条规定，关于侵犯著作权犯罪案件“以营利为目的”的认定问题：除销售外，具有下列情形之一的，可以认定为“以营利为目的”。第十二条规定，关于刑法第二百一十七条规定的“发行”的认定及相关问题：“发行”，包括总发行、批发、零售、通过信息网络传播以及出租、展销等活动。非法出版、复制、发行他人作品，侵犯著作权构成犯罪的，按照侵犯著作权罪定罪处罚，不认定为非法经营罪等其他犯罪。本案中，被告单位利用被告人吴某某制作的刷机软件，下载安装微信程序及外挂软件或提供教程供用户自行刷机下载安装微信程序及外挂软件至“瞬”微商营销手机并加价销售牟利的行为，无疑系刑法所规定的“以营利为目的”；该行为显然也非《腾讯微信软件许可及服务协议》中所规定的“为非商业目的在单一台终端设备上安装、使用、显示、运行本软件”，当然也不会得到著作权人的许可或授权。故被告单位应属“未经著作权人许可”；关于本案中被告单位是否复制、发行了腾讯公司的微信软件，本院认为，被告单位销售的华硕“瞬”微商营销手机必须下载安装刷机软件、微信软件、外挂软件后方能实现其功能，该手机上的“微信+外挂”软件，经鉴定，与腾讯公司的微信软件在资源文件、库文件上的相似度为99.73%，程序代码文件上的相似度为97.26%，构成高度的实质性相似，应解释为著作权法及刑法意义上的复制。那么核心问题就是被告单位在本案中是否实施了著作权法及刑法意义上的复制，发行，或者既复制又发行的行为？庭审中，被告单位及被告人刘某某均辩称被告单位仅是在经营初期在华硕“瞬”微商营销手机上刷机后下载安装了微信软件、外挂软件并予以销售，数量仅为二百余台，裸机进价为一千余元，销售批发价为二千余元，后期的二千余台均是提供刷机、下载、安装视频教程后由用户方自行操作，销售价格不变。相关辩护人也支持这一观点，并认可该二百余台手机上的刷机、下载、安装、销售行为确为复制及发行，会侵犯相关权利人计算机软件的著作权，但数量不至涉罪。本院认为，关于复制，就是在有形物质载体之上再现作品并使该作品被相对稳定、持久地固定在有形物质载体之上从而形成有形复制件，发行就是向公众以转移作品有形物质载体所有权的方式提供作品的原件或复制件，被告单位将与腾讯公司微信软件高度实质性相似的“微信+外挂”软件下载、安装在二百余台华硕“瞬”微商营销手机上的行为，无疑系复制行为，事后的销售行为，即为典型的发行。本案最大之争议在于被告单位及辩护人所称的其余二千余台“提供刷机、下载、安装视频教程+裸机销售”的手机，是否构成复制、发行行为从而构成侵犯著作权？首先，华硕“瞬”微商营销手机的用户群系有特殊需求的固定群体，即“微商”，并非普通社会公众，购买该手机的用途及目的是为了在微信上从事商品交易或提供相关服务时获得相较同业人员的便捷及竞争优势，该使用目的决定了手机必然需要下载安装刷机软件、微信软件、外挂软件；其次，该手机裸机进货价仅为一千余元，被告单位刷机安装微信软件及外挂

软件后，销售批发价即达二千余元，零售价更高达三千余元，为便利采取“提供刷机、下载、安装视频教程+裸机”销售模式的手机售价与售前已安装好相关软件的手机售价完全一致，可见刷机软件+微信软件+外挂软件形成的特殊功能费即达千元以上，用户在已支付大额费用的情况下不按被告单位提供的教程下载安装相关特殊功能软件用于经营几无可能。本院确认不论是售前下载安装还是通过视频教程指导下载安装，被告单位所售的华硕“瞬”微商营销手机均已实际安装微信软件+外挂软件，且销售金额中均包含了实现软件功能的特别费用。自行下载安装软件后销售与提供下载安装软件路径、教程后销售仅为具体形式、手段的不同，目的一致、结果一致、获利一致、对相关法益造成的侵害一致，其复制行为的发生仅是单独实施及与他人分工后共同实施的区别，复制后加价销售牟利的行为，即为典型的发行，故被告单位的行为构成著作权法意义及刑法意义的复制发行他人计算机软件作品，按侵权作品数量计算属“有其他严重情节”，依法已构成侵犯著作权罪。被告人刘某某系被告单位直接负责的主管人员，亦应当按刑法单位犯罪的相关规定追究其侵犯著作权的刑事责任。被告单位及被告人的辩护人关于被告单位及被告人不构成侵犯著作权罪的辩称本院不予采信。最后，本院注意到，违法所得数额较大(三万元以上)或者有其他严重情节(非法经营额五万元以上)，亦系构成侵犯著作权罪的情形，超过规定数额五倍以上将构成数额巨大及其他特别严重情节，本案中按庭审时查证的被告单位的违法所得及非法经营额，均已远超相关规定的衡量标准，公诉机关在起诉时选择按侵权复制品的数量认定本案属情节严重，系有利于被告单位及被告人，本院不再另行评判。

关于争议焦点二，刑法规定的共同犯罪是指二人以上共同故意犯罪。本案公诉机关指控被告单位及被告人刘某某伙同被告人吴某某以营利为目的，未经著作权人许可，复制发行其计算机软件作品 2300 余份，构成了侵犯著作权的共同犯罪。在焦点一的分析中本院已经认定被告单位及被告人刘某某构成侵犯著作权罪，那么被告人吴某某是否系共同犯罪？本院认为，本案中被告单位、被告人刘某某及被告人吴某某系事先共同合谋，被告人吴某某制作刷机软件、提供微信及外挂软件来源、传授下载安装方法的行为，与被告单位下载、安装侵权软件后销售华硕“瞬”微商营销手机牟利的行为，均指向侵权后营利同一目的，系互相配合、分工合作的犯罪活动整体，与侵犯他人著作权的犯罪结果均有不可分割的因果关系，被告单位销售的每一台含有侵权软件的手机，被告人吴某某均可提成七十元，合计获利达二十余万元，本案中没有被告人吴某某的技术支持及帮助，被告单位也不可能完成之后的复制及发行，故本院认定被告人吴某某构成与被告单位及被告人刘某某侵犯著作权的共同犯罪。但本案复制发行他人计算机软件作品的主要行为系由被告单位所实施，被告人吴某某在共同犯罪中居次要地位，起辅助作用，公诉机关认定被告人吴某某构成从犯，本院予以采纳。

关于争议焦点三，被告单位复制发行他人计算机软件作品 2300 余份而构成侵犯著作权罪，依法应处以罚金；被告人刘某某作为被告单位的直接负责的主管人员，也应当按侵犯著作权罪判处刑罚。被告单位及被告人刘某某在共同犯罪中起主要作用，系主犯，应当按照其所参与的或者组织、指挥的全部犯罪处罚；被告单位及被告人刘某某具有自首情节，依法可以从轻处罚；公诉机关关于本案应当对被告单位判处罚金，对被告人刘某某判处一年六个月以上二年六个月以下有期徒刑并处罚金的量刑建议本院予以采纳。对被告人刘某某可以适用缓刑。被告人吴某某在共同犯罪中起次要、辅助作用，系从犯，依法应当从轻处罚。被告人吴某某到案后如实供述自己的罪行，系坦白，可以从轻处罚。被告人吴某某在前罪缓刑考验期内犯新罪，依法应当撤销缓刑，把前罪和本罪所判处的刑罚实行数罪并罚后决定执行的刑罚。

综上所述，本院认为，被告单位昱宫公司以营利为目的，未经著作权人许可，复制发行其计算机软件作品 2300 余份，属情节严重，其行为已经构成侵犯著作权罪，应予处罚，公诉机关指控成立。被告人刘某某作为被告单位直接负责的主管人员，也应当按照侵犯著作权

罪处罚。本案系共同犯罪，被告单位及被告人刘某某系主犯，被告人吴某某系从犯，应当从轻处罚。被告单位及被告人刘某某系自首，可以从轻处罚。被告人吴某某系坦白，可以从轻处罚，其在缓刑考验期内犯新罪，应当撤销缓刑数罪并罚。根据被告单位及被告人犯罪的事实、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》第二百一十七条第(一)项、第二百二十条、第三十条、第三十一条、第二十五条第一款、第二十六条第一款、第四款、第二十七条、第六十七条第一款、第三款、第七十二条第一款、第三款、第七十三条第二款、第三款、第七十七条第一款、第六十九条、第五十三条、第六十四条之规定，判决如下：

一、被告单位上海昱宫网络科技有限公司犯侵犯著作权罪，判处罚金人民币五十万元。(罚金自本判决生效之日起一个月内向本院缴纳。)

二、被告人刘某某犯侵犯著作权罪，判处有期徒刑一年六个月，缓刑一年六个月，并处罚金人民币十万元。

(缓刑考验期限，从判决确定之日起计算。罚金自本判决生效之日起一个月内向本院缴纳。)

三、撤销浙江省台州市椒江区人民法院(2016)浙 1002 刑初 651 号刑事判决书中对吴某某宣告缓刑二年的执行部分。

四、被告人吴某某犯侵犯著作权罪，判处有期徒刑一年，并处罚金人民币五万元，与前罪判决有期徒刑一年六个月，并处罚金人民币十万元(已执行)合并，决定执行有期徒刑一年九个月，并处罚金人民币十五万元。

(刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日。罚金自本判决生效之日起一个月内向本院缴纳。)

五、被告单位上海昱宫网络科技有限公司、被告人刘某某、被告人吴某某的违法所得予以追缴。

刘某某：在社区中，应当遵守法律、法规，服从监督管理，接受教育，完成公益劳动，做一名有益社会的公民。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或直接向上海市第三中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本一份。

审 判 长　王利民

审 判 员　王欣元

人民陪审员　　郑誉华

二〇一九年八月二十九日

书 记 员　沈 雯

案例三、邱本侵犯著作权案

审理法院：　成都高新技术产业开发区人民法院

案　　号：　（2018）川 0191 刑初 529 号

案　　由：　侵犯著作权罪

裁判日期：　2019 年 01 月 22 日

成都高新技术产业开发区人民法院

刑事判决书

（2018）川 0191 刑初 529 号

公诉机关成都高新技术产业开发区人民检察院。

被告人邱本，男，1985 年 6 月 8 日出生，汉族，大学文化，户籍地成都市高新区，因涉嫌侵犯著作权罪于 2017 年 11 月 22 日被成都市公安局刑事拘留，同年 12 月 27 日被执行

逮捕，现羁押于成都市看守所。

辩护人刘欣，四川凯盈律师事务所律师。

成都高新技术产业开发区人民检察院以成高新检公诉刑诉[2018]437 号起诉书指控被告人邱本犯侵犯著作权罪，于 2018 年 8 月 3 日向本院提起公诉。本院依法组成合议庭，公开开庭审理了本案。成都高新技术产业开发区人民检察院指派检察员李飞出庭支持公诉，被告人邱本及其辩护人刘欣到庭参加诉讼。现已审理终结。

成都高新技术产业开发区人民检察院指控，2016 年 10 月，著作权人深圳市圣盛网络科技有限公司（以下简称圣盛网络公司）授权深圳市盛大美游信息技术有限公司（以下简称盛大美游公司）发行、运营“圣盛人人棋牌麻将”游戏（以下简称“人人”棋牌游戏）。2017 年 2 月至 8 月，邱本任职于盛大美游公司期间，邱本通过他人获知公司 SVN 服务器账号、密码，私自取得“人人”棋牌游戏源代码。2017 年 5 月至 6 月，邱本先后成立成都九颗星科技有限公司（以下简称九颗星科技公司）、成都天天乐科技有限公司（以下简称天天乐科技公司）并化名“陈刚”进行实际控制。邱本在未经著作权人许可的情况下，对“人人”棋牌游戏进行换皮、加工等形式修改后，更名为“大赢家”棋牌游戏，经司法鉴定，“大赢家”棋牌游戏源代码与“人人”棋牌游戏源代码相似度达 99%。2017 年 8 月，邱本从盛大美游公司正式离职。之后，邱本利用九颗星科技公司负责“大赢家”棋牌游戏的技术支持，利用天天乐科技公司上线运营“大赢家”棋牌游戏营利。直至案发，游戏玩家总数达 14 万余人，游戏充值金额达 8476 万余元。2017 年 11 月 21 日，邱本被警察挡获。

公诉机关认为，被告人邱本以营利为目的，未经著作权人许可，复制发行其计算机软件，情节特别严重，应当以侵犯著作权罪追究其刑事责任。

被告人邱本对指控的犯罪事实和罪名均无异议并当庭表示认罪。

辩护人认为被告人邱本的行为已经构成侵犯著作权罪，并提出了如下辩护意见：1.起诉书指控系邱本个人犯罪，本案的犯罪金额应以邱本的个人获利来认定。本案的充值金额中天天乐科技公司分配了 15%约为 1200 万元，按股份比例由邱本与林某 2 各自分配约 600 万元。邱本负责公司日常经营和员工工资发放，扣除该部分支出，邱本个人获利约 200 万元，应以 200 万元认定邱本的违法所得并据此适用刑罚。2.被告人邱本缺乏法律专业知识，不知道使用他人的源代码发行、运营网络游戏系犯罪行为，一时不慎误入歧途，案发后被告人积极配合公安机关调查，如实供述全部事实，在法庭审理中亦当庭认罪，具有坦白情节。3.被告人邱本认识到自己的错误行为并积极改正，委托辩护人转告家属及员工采取措施，关闭了涉嫌侵权的网游平台，及时停止了侵权行为，有效避免了被害人经济损失的扩大。4.被告人委托其亲属代其向被害人赔礼道歉，积极主动赔偿了被害人的损失并取得了被害人的谅解。5.被告人系初犯、偶犯，其已向受害人承诺在三年内不再从事与之相竞争的商业行为，诚心改过，不具有再犯的可能性。6.被告人系家庭主要劳动力和收入来源，恳请法庭考虑到邱本真诚悔罪，在本案中具有法定与酌定从轻处罚情节、主观恶性和社会危害性小，给予其改过自新、重新做人机会，对其从轻量刑并适用缓刑。

经审理查明，2017 年 4 月 1 日，国家版权局颁发证书号为“软著登字第 1686634 号”的《计算机软件著作权登记证书》，该证书载明圣盛网络公司以原始取得方式取得了“人人”棋牌游戏软件的著作权。圣盛网络公司将该游戏软件的发行权和运营权授权给了盛大美游公司。2017 年 2 月初，被告人邱本入职盛大美游公司，任总经理职务；其通过职务上的便利获知了盛大美游公司 SVN 服务器账号、密码，并私自取得“人人”棋牌游戏源代码。2017 年 5 月至 6 月期间，邱本通过他人分别设立九颗星科技公司与天天乐科技公司，邱本为该两公司的实际控制人。邱本在未经著作权人许可的情况下，对“人人”棋牌游戏进行换皮、加工等形式修改后，更名为“大赢家”棋牌游戏。2017 年 8 月，邱本从盛大美游公司正式离职后，利用九颗星科技公司负责“大赢家”棋牌游戏的技术支持，利用天天乐科技公司上线

运营“大赢家”棋牌游戏营利。

2017 年 9 月，盛大美游公司向公安机关报案，2017 年 11 月 21 日，被告人邱本被抓获到案。

公安机关委托四川神琥司法鉴定所对被告人邱本存放于天天乐科技公司 SVN 服务器中的“大赢家”棋牌游戏源代码与“人人”棋牌游戏源代码进行同一性鉴定，鉴定意见为：SVN 服务器中存放的“大赢家”棋牌游戏源代码与“人人”棋牌游戏源代码相似度达 99%，存在实质性相似。公安机关对“大赢家”棋牌游戏数据库进行了现场勘查，结果显示，在 2017 年 7 月 1 日至 11 月 22 日期间，“大赢家”棋牌游戏共有玩家 141721 人，游戏玩家在 2017 年 8 月 17 日至 11 月 21 日期间共计充值 82241801.03 元。

另查明，1.被告人邱本的家属代邱本向盛大美游公司支付了 220 万元赔偿款，被告人邱本取得了盛大美游公司的谅解。

2.公安机依法冻结了被告人邱本开设于招商银行股份有限公司深圳分行尾号为 6331 的银行账户中的 1138490.32 元、中信银行成都高新支行尾号为 4729 的银行账户中的 364059.04 元，冻结了以邱本的配偶游某 2 的名义开设于中信银行成都天府支行尾号为 0525 的银行账户中的 304568.25 元，冻结了天天乐科技公司在汇元银通（北京）在线支付技术有限公司的账户余额 1243746.68 元。

上述事实，有下列证据予以证实：

1、受案登记表、立案决定书、到案经过，证明本案的受案和立案情况以及被告人邱本系抓获到案。

2、常住人口信息表，证明邱本的身份信息及案发时达到完全刑事责任年龄。

3、计算机软件著作权登记证书，证明受著作权保护的计算机软件名称为“圣盛人人棋牌麻将游戏软件[简称：人人棋牌麻将]V1.0”；著作权人为“深圳市圣盛网络科技有限公司”；权利取得方式为“原始取得”；权利范围为“全部权利”；开发完成日期为“2016 年 8 月 1 日”；首次发表日期为“2016 年 8 月 15 日”。

4、《情况说明书》及王玉洁的报案材料，证明盛大美游公司未授权给天天乐科技公司、九颗星科技公司以及邱本个人享有“人人”棋牌游戏的著作权；天天乐科技公司、九颗星科技公司的棋牌游戏源代码与“人人”棋牌游戏源代码一样。

5、《<圣盛人人棋牌麻将>游戏授权发行与运营协议》，证明圣盛网络公司于 2016 年 10 月 8 日授权盛大美游公司在中国大陆区域独家享有“人人”棋牌游戏的发行权和运营权，授权期限为 3 年，盛大美游公司有权对侵犯著作权的行为以自己的名义进行维权。

6、鉴定聘请书、四川神琥司法鉴定所司法鉴定意见书，证明天天乐科技公司 SVN 服务器中存放的“大赢家”棋牌游戏源代码与“人人”棋牌游戏源代码相似度达 99%，存在实质性相似。

7、证人许某的证言，证明其就职于盛大美游公司，负责游戏服务端源代码编写，源代码存于 SVN 服务器内，邱本时任盛大美游公司 CEO 并向其索取了 SVN 服务器的账号和密码，邱本向其讲述准备以“换皮”的方式做自己的网络棋牌游戏。

8、证人沈某的证言，证明其由邱本招聘进入九颗星科技公司，邱本在公司自称“陈刚”；沈某负责游戏的逻辑开发，具体是“大赢家”棋牌游戏服务端的程序开发。

9、证人文某的证言，证明其通过招聘方式入职九颗星科技公司，主要负责“大赢家”棋牌游戏平台的策划，公司负责人为邱本、公司内部称邱本为“刚哥”。

10、证人余某的证言，证明其由邱本招聘进入九颗星科技公司，负责修改公司的棋牌游戏服务端程序，听说公司有一款名叫“大赢家”的棋牌游戏在运营，公司内部称邱本为“刚哥”。

11、证人龙某的证言，证明其由邱本招聘进入九颗星科技公司，负责 UI 的设计、美化

并按邱本的要求对棋牌文档进行“换皮”；公司主要运营“大赢家”棋牌游戏平台、公司法定代表人为游某2；“大赢家”棋牌游戏源代码由邱本提供、公司内部称邱本为“刚哥”。

12、证人游某1证言，证明邱本让其从其他公司跳槽到盛大美游公司，负责分析“人人”棋牌游戏的玩家数据；后邱本又让其从盛大美游公司跳槽到九颗星科技公司上班，担任客服主管，负责“大赢家”棋牌游戏维护，“大赢家”棋牌游戏的源代码存放于九颗星科技公司的SVN服务器中。

13、证人林某1证言，证明其通过应聘入职九颗星科技公司，主要负责公司的财务以及日常开销支出，公司研发了一款名为“大赢家”的棋牌游戏，老板叫陈刚，法定代表人为游某2，二人系夫妻关系；在员工进入公司后，邱本会鼓励每人交一张银行卡，公司给予500元的奖励。九颗星科技公司的主要收入为天天乐科技公司支付的50万元研发费用。

14、证人游某2证言，证明其系九颗星科技公司的法定代表人，股东为游某2与刘某，游某2持股51%、刘某持股49%，刘某不参与公司经营，邱本是公司经营的决策人；公司的唯一收入为天天乐科技公司支付的50万元。天天乐科技公司的法定代表人为王某，邱本占天天乐科技公司49%的股份；天天乐科技公司负责“大赢家”棋牌游戏的营销，九颗星科技公司负责“大赢家”棋牌游戏研发；两个公司的负责人都是邱本。以游某2名义在中信银行成都天府支行开立的尾号为0525的银行账户用于九颗星科技公司的办公开销，账户中存入的款项主要由邱本提供。

15、证人林某2证言，证明其原系九颗星科技公司股东，因为不懂技术后来没有参与公司，向九颗星科技公司投资了30万左右，公司上线了一款名为“大赢家”的棋牌游戏。

16、证人唐某证言，证明其通过应聘入职九颗星科技公司，从事网站开发、维护以及后台管理平台的搭建、维护，网站内容主要展示、下载“大赢家”游戏平台；公司内部称邱本为“刚哥”。

17、证人陈某证言，证明其在九颗星科技公司负责客户端开发，客户端名叫“大赢家”棋牌游戏，游戏源代码为邱本所给；其听邱本说过“大赢家”棋牌游戏源代码系邱本从盛大美游公司盗取，存放于九颗星科技公司的SVN服务器；公司的法定代表人为游某2、实际负责人为邱本；邱本在创建九颗星科技公司时对外自称“陈刚”；游戏玩家可以通过微信支付、QQ支付以及支付宝支付等方式为游戏充值。

18、被告人邱本的供述，证明在任职盛大美游公司总经理期间，盛大美游公司的技术总监将“人人”棋牌游戏的部分源代码的权限授予了邱本，后邱本利用职务上的便利，于2017年6月中旬左右以工作的名义获取了盛大美游公司存放“人人”棋牌游戏全部源代码的SVN服务器的账号和密码，后其将“人人”棋牌游戏的源代码拷贝。2017年5月被告人以其配偶游某2的名义成立九颗星科技公司、邱本为该公司的实际控制人，由游某2担任公司法定代表人并代其持股51%，林某2持股49%，林某2在该公司只负责投资和分成，2017年10月，股东林某2变更为了刘某。待九颗星科技公司的全部研发人员到位后，被告人邱本将其拷贝出的所有“人人”棋牌游戏源代码存放在了九颗星科技公司的SVN服务器上，并根据研发人员不同的职责开放不同的权限，由研发人员对源代码进行加工，对游戏界面的外观、部分功能进行修改后，上线运行了一款名为“大赢家”的棋牌游戏。九颗星科技公司主要负责游戏的研发、技术支持工作。2017年6月，邱本让游某2找代办公司办理成立天天乐科技公司，其利用王某的身份信息并借用张贵的身份证注册成立该公司，由王某担任法定代表人，持股51%，张贵持股49%。天天乐科技公司负责“大赢家”棋牌游戏的运营，为了避免玩家因游戏输钱而被找麻烦，邱本化名为“陈刚”负责公司经营活动。“大赢家”棋牌游戏上线运行后，其将服务器交由阿里云进行托管，通过两种模式进行营利，一是游戏玩家通过微信、QQ钱包等平台以充值的形式购买游戏币；从充值金额中扣除手续费后即为天天乐科技公司的收益。二是对游戏玩家收取房间费，按照房间的不同等级收取每局金额不等的房间

费。游戏玩家通过上述两种通道充值的钱到达腾讯公司，腾讯公司将钱打入汇付宝，汇付宝在收取充值通道费用后直接将钱打到公司在汇付宝申请的支付账号上，由此收钱。所获得的收益除用于游戏推广、充值通道费用以及代理商的费用外，天天乐科技公司实际获益占15%，其个人获利在200万元左右。

19、现场勘验笔录，证明在2017年7月1日至11月22日期间，“大赢家”棋牌游戏共有玩家141721人。“大赢家”棋牌游戏玩家在2017年8月17日至11月7日期间共计充值75297355.03元，在11月7日至11月21日期间共计充值6944446元。

20、搜查笔录、扣押清单、协助冻结财产通知书，证明案发后，公安机关对九颗星科技公司办公室以及被告人邱本居住地进行搜查并扣押笔记本电脑、手机、组装电脑主机、银行卡、U盘、移动硬盘、账本等，并将天天乐科技公司、邱本及游某2的有关账户予以了冻结。

21、谅解协议、谅解书、收据，证明盛大美游公司对邱本的侵权行为予以谅解且已经收到了邱本支付的220万元赔偿款。

22、九颗星科技公司、天天乐科技公司营业执照，证明九颗星科技公司的经营范围为计算机技术、网络技术等，天天乐科技公司的经营范围为软件开发等。

上列证据，经法庭质证，收集程序合法，内容客观真实，且能相互印证，证明本案的事实，本院予以确认。

本院认为，圣盛网络公司系“圣盛人人棋牌麻将游戏软件V1.0”的著作权人，盛大美游公司经圣盛网络公司的授权取得该款游戏的发行权与运营权，该款网络游戏的计算机软件著作权受我国法律保护。被告人邱本未经著作权人许可，以营利为目的，以其窃取的“圣盛人人棋牌麻将游戏软件V1.0”源代码为基础，通过复制原程序的原始数据，以换皮、加工等形式制作成“大赢家”棋牌游戏并上线运营，符合《中华人民共和国刑法》第二百一十七条所规定的侵犯著作权罪的“复制发行”要求。被告人邱本以盈利为目的，未经著作权人许可，复制发行“圣盛人人棋牌麻将游戏软件V1.0”，该行为侵犯了著作权人的著作权。综上，被告人邱本以营利为目的，未经著作权人许可，复制发行“圣盛人人棋牌麻将游戏软件V1.0”，该行为侵害了著作权人的著作权。构成侵犯著作权罪，依法应予刑事处罚。公诉机关指控的犯罪事实清楚，证据确实、充分，罪名成立。

根据《中华人民共和国刑法》第二百一十七条的规定，构成侵犯著作权罪，违法所得数额巨大或者有其他特别严重情节的，处三年以上七年以下有期徒刑并处罚金。《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》第五条规定，非法经营数额在二十五万元以上的属于侵犯著作权罪的有其他特别严重情节的情形；第十二条规定，本解释所称的“非法经营数额”是指行为人在实施侵犯知识产权行为过程中，制造、储存、运输、销售侵权产品的价值。本案中，被告人邱本在2017年11月21日的讯问中供述“大赢家”棋牌游戏所获得的收益除各类开销外所剩无几。在2017年12月5日的讯问中，邱本供述，“大赢家”棋牌游戏玩家的充值金额中，公司只占15%的利润，最多赚到1000万元，其个人获利六七百万左右。在2018年1月18日的讯问中，邱本供述，玩家充值金额中公司占利润为15%，最多赚取1000万左右，个人获利六七百万左右；亦是在该次讯问中，邱本又供述，因为公司有很多开销，其个人实际分得200多万元。即被告人邱本在多次供述中对其个人获利的金额呈现出前后不一的情况，即便在同一次讯问中，其供述的获利金额也前后不一致。公安机关所勘查的结果显示，在“大赢家”棋牌游戏上线运营期间，玩家充值金额为8224万余元，故应当以游戏玩家的充值金额为本案的犯罪金额即本案的非法经营数额为8224万余元，属于侵犯著作权罪的其他特别严重情节，按照《中华人民共和国刑法》第二百一十七条的规定，应当判处三年以上七年以下的有期徒刑。被告人邱本到案后如实供述了自己的犯罪事实，积极赔偿被害单位部分损失并取得了被害单位谅解，量刑时可以酌情从轻处罚。对辩护人提出的被告人如实供述罪行、具有坦白、积极赔偿损失、真诚

悔罪等酌情从轻处罚的辩护意见，本院予以采纳。本院综合考量被告人的犯罪事实、性质、情节和社会危害程度、认罪悔罪态度、非法经营数额等，决定对被告人邱本判处有期徒刑五年，对辩护人提出的对邱本适用缓刑的辩护意见，本院不予采纳。

关于罚金数额的确定问题。《中华人民共和国刑法》第五十二条规定："判处罚金，应当根据犯罪情节决定罚金数额"、《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（二）》第四条规定："对于侵犯知识产权犯罪的，人民法院应当综合考虑犯罪的违法所得、非法经营数额、给权利人造成的损失、社会危害性等情节，依法判处罚金。罚金数额一般在违法所得的一倍以上五倍以下，或者按照非法经营数额的50%以上一倍以下确定"、《最高人民法院关于适用财产刑若干问题的规定》第二条规定："人民法院应当根据犯罪情节，如违法所得数额、造成损失的大小等，并综合考虑犯罪分子缴纳罚金的能力，依法判处罚金"，本案系被告人邱本个人犯罪，从公诉机关提供的证据看，被告人邱本的违法所得金额不低于其本人所供述的最低数额200万元，虽然该数额除个人供述外无其他相关证据予以佐证，但按照有利于被告人的原则，本院在确定罚金数额时，将被告人邱本个人供述的违法所得200万元作为参考基数，即个人违法所得不低于200万元。本院结合本案被告人邱本的犯罪事实，从有利于执行的角度，综合考虑被告人缴纳罚金的能力，犯罪给权利人造成的损失和社会危害性等情节并体现刑法的谦抑性原则，决定对被告人邱本判处罚金400万元。

综上，依照《中华人民共和国刑法》第二百一十七条第一项、第五十二条、第五十三条、第六十七条、第六十四条，《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》第五条第二款，《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（二）》第四条、《最高人民法院关于适用财产刑若干问题的规定》第二条之规定，判决如下：

一、被告人邱本犯侵犯著作权罪，判处有期徒刑五年，并处罚金人民币四百万元；

（刑期从判决执行之日起计算。判决执行之前先行羁押的，羁押一日折抵刑期一日，即自2017年11月22日起执行至2022年11月21日止。罚金于本判决生效十日内缴纳。）

二、对扣押在案的7台笔记本电脑、7台手机、2台移动硬盘、2台U盘、6台组装电脑主机、1台S**服务器（详见《扣押清单》）予以没收，对扣押在案的12张银行卡（详见《扣押清单》）卡内存款予以没收，对冻结在案的存款予以没收。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向成都市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审判长　梁　瑛

审判员　晏　锐

人民陪审员　钟　明

二〇一九年一月二十二日

书记员　李瑞琳

案例四、私自架设服务器运营网络游戏--陈某侵犯著作权案

海摩力游数字娱乐有限公司开发的《海盗王online》游戏在网络上非常受欢迎。陈某、邹某也因在互联网玩该游戏而相识。这款游戏如此受欢迎，盈利肯定丰厚，两人不禁动了歪脑筋。2010年5月，经陈某提议，邹某至江苏省无锡市共同私自架设服务器运营网络游戏，约定营利由两人分。

2010年5月至2011年3月，陈某、邹某在无锡市某小区内，由陈某非法取得网络游戏《海盗王online》源代码，通过租借两台服务器架设游戏服务器端，将游戏改名为《逍遥海

盗王》、《追梦海盗王》、《无极海盗王》后，在其设立的网站上非法运营上述游戏，并由邹某负责修改游戏装备及网站日常维护等。陈某在互联网上与玩家联系出售虚拟游戏装备、出租游戏等事宜，通过银行转账、网络支付工具等收取交易款项。经审计，非法经营数额共计人民币 6 万余元。其间，陈某共计支付邹某人民币 1.5 万余元作为报酬。

2011 年 3 月 3 日，摩力游数字娱乐有限公司向警方报案，同年 3 月 8 日，公安民警在江苏省无锡市惠山区抓获陈某、邹某，并查获涉嫌侵权的网络服务器 8 台。

案件移送静安区检察院金融和知识产权科审查批捕后，检察官针对电子证据的高科技性、无形性、多样性、易被破坏性的特点，加强网络犯罪案件电子证据客观性、真实性和合法性的甄别判断，重点审查电子证据文书材料所依据的电子证据是否真实、完整、充分，证明电子证据来源的材料是否齐全，有无瑕疵，电子证据的制作、储存、传递、获得、搜集等程序是否合法，方法是否科学、及时等。

经鉴定，送鉴的服务器硬盘中被检网络游戏软件，注册用户共计 9868 人，使用用户数共计 8194 人，与《海盗王 online》网络游戏之间存在实质性相似，构成侵权。

静安区检察院认为，陈某、邹某以营利为目的，未经著作权人许可，共同复制发行其计算机软件，情节严重，其行为构成侵犯著作权罪。陈某被法院以犯侵犯著作权罪判处拘役 6 个月、罚金 3.6 万元，邹某被判处拘役 5 个月、罚金 1.6 万元。

（四）侵犯公民个人信息罪

案例一、陈远城侵犯公民个人信息案

广东省广州市白云区人民法院

刑事判决书

(2019)粤 0111 刑初 3069 号

公诉机关广州市白云区人民检察院。

被告人陈远城，男，1995 年 8 月 23 日出生，汉族，出生地 广东省陆河县，文化程度初中，户籍地广东省陆河县(以上身份 信息均系被告人自报)。因本案于 2019 年 6 月 3 日被羁押并于次 日被刑事拘留，同年 7 月 12 日被逮捕。现羁押于广州市白云区看 守所。

辩护人黄泽珊，广东金桥百信律师事务所律师。 '

广州市白云区人民检察院以穗云检公诉刑诉[2019] 2881 号 起诉书指控被告人陈远城犯侵犯公民个人信息罪，于 2019 年 10 月 16 日向本院提起公诉。本院依法适用普通程序，组成合议庭， 三次公开开庭审理了本案。广州市白云区人民检察院指派检察员 徐卉、夏慧娟出庭支持公诉，被告人陈远城及其辩护人黄泽珊到 庭参加诉讼。

广州市白云区人民检察院指控，2019 年 5 月始，被告人陈远 城在本市白云区龙归镇永兴榕树塘街北一巷 12 号 203 房,通过网 络以购买等方式获取他人身份信息共计约 105 万余条以注册微信并实名认证，后将微信号出售或用以浏览网页提现。6 月 3 日， 公安人员在上址抓获陈远城，并缴获笔记本电脑 1 台、iPad 1 台、 小米牌无线移动电话机 1 台，在龙归镇永兴榕树塘街北二巷 28 号二楼缴获电脑主机 15 台、电话卡 10000 张、卡槽 102 个。为证 实指控的事实，公诉机关随案移送了物证、书证、证人证言、被 告人供述、鉴定意见、勘验、搜查、辨认笔录等证据。根据上述 事实和证据，公诉机关认为，被告人陈远城违反国家有关规定， 非法获取公民个人信息，情节特别严重，其行为已触犯《中华人 民共和国刑法》第二百五十三条之一第一、三款之规定，应当以 侵犯公民个人信息罪追究其刑事责

任。提请本院依法判处。

被告人陈远城对公诉机关指控的事实、罪名无异议，当庭表 示认罪。但辩解称其只购买了 200 余条他人身份信息，其他都是 他人在 QQ 群里发给其的，从来也没有使用过。并且缴获的电脑 主机、电话卡和卡槽是其与他人一同购买的，与本案犯罪没有关 系＞

被告人陈远城的辩护人黄泽珊发表辩护意见称：一、对公诉 机关指控被告人犯侵犯公民个人信息罪的定性没有意见，但认为 不属于“情节特别严重”的情形。起诉书指控陈远城通过网络购 买等方式获取他人身份信息共约 105 万余条，但根据陈远城的供 述，这些信息并不全部是其购买的，其只购买了 200 多条，其余 均是在一个 QQ 群里别人免费发给其的，而且已明确告诉其这些 信息已经被很多人注册过，用处不大，如果想注册微信成功，需要购买新的公民信息，陈远城接收后确实曾试过注册微信，但发 现很多用不了，后来其才向他人购买 200 多条新的公民信息。对 于上述大部分公民信息是陈远城在 QQ 群免费下载的，但没有用 于注册微信并实名认证后再出售或提现获利。本案没有证据证明 指控的 105 万余条公民个人信息全部是陈远城购买的，且涉案的 大部分公民信息不是真实存在的，无法用于注册微信。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》第十一条的规定“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。”因此，现有证据证明部分公民信息是不真 实的，应当不予计算在内，本案也不应认定为“情节特别严重” 的情形。二、被告人主观恶性小，犯罪情节不大，社会危害性小， 具有以下法定或酌定从轻处罚的情节。1.陈远城系初犯、偶犯， 犯罪之前无任何刑事犯罪或行政处罚记录，其是一时贪图小利而 偶起犯意，且涉案时间不长，所获取利润不大，社会危害性小。

2.陈远城自愿认罪，认罪态度较好，归案后一直能如实供述自己 的犯罪事实，有明显的悔罪表现。综上，建议法庭对被告人陈远 城在三年以下有期徒刑量刑，最大限度地从轻处罚并依法判处缓 刑。

经审理查明：2019 年 5 月始，被告人陈远城在本市白云区龙 归镇永兴榕树塘街北一巷 12 号 203 房，通过网络以购买、下载等 方式获取他人身份信息共计约 105 万余条以注册微信并实名认 证，后将微信号出售或用以浏览网页提现。6 月 3 日，公安人员 在上址抓获陈远城，并缴获笔记本电脑 1 台、iPad 1 台、小米牌 无线移动电话机 1 台。

上述事实，有下列经庭审举证、质证，本院予以确认的证据 证实：

1.被告人陈远城的供述，该证据证实了：我是广州大淘客网 络科技有限公司（2017 年 6 月成立）的法定代表人，公司经营范 围是网络推广服务、电子设备销售，员工有蒋魁、谢菁菁，出资 人包括我（出资 18 万元人民币）、李泽震（出资 12 万元人民币）、 蒋魁（出资 10 万元人民币），其中李泽震已经离开公司，公司的 临时办公地址位于广州市白云区龙归永兴榕树塘街北一巷 12 号 2 楼。我、李泽震、蒋魁 3 人所出资的约 40 万元用在场地租金、装 修房屋、购置家具，还买了 10000 张电话卡、200 台猫池、十几 台电脑以及一些酒店客户的开房信息，这个猫池跟广州大淘客网 络科技有限公司是没有关系的。我用电话卡来收各类 App 的注册 验证码；猫池是为了批量处理电话卡，主要是在电脑上操作；客 户信息主要是用来在各 App 上提现奖励金。我用电话卡帮互联网 上一些人虚开各类 App 的账户、虚增热度，并从中获利。具体操 作是：我在火云等验证码中间平台作为手机验证码的供应方提供 大量手机号码在平台上，客户如果不想使用自己的手机号码注册 App 账户，客户可以通过这类平台发起注册各种 App 的要求，平 台会随机分配平台上的电话号码（包括我提供的号码）给客户用 于注册，如果分配了我持有的号码给客户，客户用我的号码注册 App 就会发对应的验证码到我的电话卡上，火云等平台会直接通 过酷卡平台抓取数据库获取我的号码收到的验证码并提供给客 户，每次这样的交易我能获得几分钱到几毛钱不等的收益。例如，客户在火云平台上注册一个抖音的账户，客户要在火云平台上付 费 1 毛钱，

平台收费后就再给我 5-6 分钱，一个手机号码只能在 同一个 App 上注册一个账号，后台系统自动会筛选的。不计投资 的 40 万元成本的话，我们总共获利 10 来万，目前还处于亏损状 态。赚到的钱用在日常开销（房租、水电、伙食），支付先前欠的 装修款，其余的钱被我、李泽震、蒋魁 3 人分掉了。2019 年 5 月 份的一天晚上，我加入到一个“痴羊毛”的 QQ 群，想看看他人 是怎么操作的。一个微信叫做“天线宝宝死于谋杀”的朋友就说 需要交 3500 元的学费，我当时就觉得贵。对方就称会给我资料（即 公民个人信息），我就叫对方发来看看。为了让我相信他，对方就 发了 一个叫“料子”的压缩包，里面有大量（上百万条）的公民 个人信息（包括开房记录）。对方就称这些公民个人信息是十几年 前某酒店的开房记录，现在作用不是很大，这些资料被很多人注 册过了。我就跟对方说先看看再说。后来我有试了使用其中的一 些公民资料去注册微信号，但有些注册不了，已经被人注册过了， 也有一些能注册，但不到三天，就会被封号。后来对方跟我说， 如果想能成功注册，就得使用一些新的身份资料注册，并建议我 购买一些新的公民个人信息，压缩包里面的一百多万条公民信息 是不用钱的，别人只是发给我看看，证明他是有公民信息可以出 售。我后来也没有向他购买，因为他发给我的这些都是很旧的公 民信息，基本上没什么用的了。后来我就在群里面向其他人购买 了 200 条左右公民信息，每条信息 2-4 元钱不等，用于“爲羊毛”， 存在我使用的笔记本电脑桌面上“成都 x50.txt”、“5.15 德阳.txt” 等文档里面。我购买的公民信息主要是用来给微信进行实名制认 证的，然后将这些通过实名认证的微信用于登陆东方头条、闲来 斗地主、趣看天下等 App 或者微信小程序，由于这些 App 或小 程序都会给新用户奖励现金或者价值对等的商品，我就用不同的 微信对各 App、微信小程序进行“赫羊毛”，并把赚取的现金提到 微信之后转账到我个人使用的微信号。如果没有通过微信实名认 证的话，就没办法提现出来，每天可以赚十到二十块钱。我就是 利用这些公民信息在微信上面赚取一些 APP 的注册金。我没有利 用这些身份信息做过别的事情了。就是我一个人在做这个，与公 司经营无关，只赚了几百块钱。民警在我的手提电脑里面查获了 1048576 条公民信息，其中第一次别人发给我的开房信息是有名 字，身份证号码，开房的地址信息。第二次我向别人买的公民身 份信息就只有名字和身份证号码。

2.证人蒋魁的证言，该证据证实了：我朋友陈远城之前在江 西做淘宝推广，然后他知道通过帮他人虚刷流量以及关注度等方 式可以获利，就找上我租了龙归永兴村榕树塘村北三巷 28 号 201 房一起用这种方法开始“营业”，房子是我向本地人租的，每个月 2300 元租金。2018 年 9 月份的时候，陈远城、我、李泽震三人分 别出资 18 万、10 万 3 千、13 万元用于购买现在公司的设备，陈 远城、我、李泽震各占公司 45%、25%、30%的股份，然后 2019 年 5 月中旬，李泽震以 2 万 4 千元的价格把公司的股份都转给了 我，我占公司股份的 55%。陈远城、我、李泽震三人用这些钱找 到陈远城通过网上认识的一个叫冯克雨的人，这个叫冯克雨的是 一个温州的 90 后，他在江西省樟树市做卡商，他邀请我们三人去 他的公司看了他的卡房，然后告诉我们买一万张卡投入使用，半 年可以有 40 万元的收入。我们现场看了之后就向冯克雨以 20 元 一张的价格购买了 1 万张，这一万张电信卡是 13、18、15 开头的 中国移动手机卡，显示地是湖北黄冈，我们叫这些卡为“白卡”， 这些“白卡”已经由冯克雨和他的几个股东实名认证过，但是不 能拨打电话，不能发短信，不能上网。我们三人还向冯克雨买了 200 台“猫石”机，每台猫石机能够插 16 张电信卡。我们把买来的电话卡号段发布在：火云、共享、神话、易码、玉米这几个第 三方卡商平台，然后在微信群里找到有需要的用户，谈好价钱后 以每条验证码 1 角至 2 块 5 的价格出售。淘宝、京东等大电商平 台会对新注册用户发现金券，可以让用户购物使用，以及这些电 商平台在某些日子会发布重大的优惠活动，只限制一个注册用户 领取，这时候就会有客户在微信群里找卡商，需要卡商帮他们注 册大量的用户后拿优惠券，客户拿了优惠券之后可以去汇总提现 进而从中获利.除了买这些设备外我们还买了 20 多台电脑和一百多万条公民信息以及 20

多台手机。公民信息是陈远城在网上购, 的，具体金额和数量我都不清楚，这些信息是我们用来注册微信 并实名后再卖出去。我们购买的公民信息每一条的内苗包括有 名字、身份证号、电话号码这几项内容，我们先会在网上找对接 群，专门负责帮我们辅助注册微信，这些辅助商把微信帮我们注 册好后交给我们，我们收到这些注册好的微信用买来的公民信息加以实名认证，然后再通过网上以每个微信号 23 元的价格卖出 去，一个微信号的成本大约是十元，我们就从中赚取差价。从 2018 年 9 月至今，陈远成、我、李泽震通过卖微信号和卖验证码获利 大概有 20 万元左右。民警在陈远城的手提电脑内查获的公民信息 是陈远城购买回来的。我与陈远城每个月固定工资四千元，每个 月的月底会按照每个人的股份进行分红，至今我拿到四万多元的 分红。

3.证人谢菁菁的证言，该证据证实了： 2019 年 6 月 3 日 12 时许，我和男朋友陈远城、同学吴可可正在地址位于广州市白云 区永兴村榕树塘北一巷 12 号 203 房休息，这时就有民警带着蒋魁、“公牛”过来 203 房间找到了我们，经民警盘查在现场发现一台 笔记本电脑、一台 ipad 平板电脑及我和男朋友陈远城各一台手机， 经民警检查怀疑我们涉嫌侵犯公民个人信息，随后将我们传唤到 龙归派出所调查处理。我的主要工作就是推广淘宝、拼多多内的 商品，为了能更好地推广淘宝、拼多多内的商品，我还在快手进 行直播吸引粉丝后进行推广。我的工作就是推广淘宝、拼多多内的商品，每天工作都是在家里用手机、电脑就可以完成了，推广 的流程就是每天在淘宝、拼多多浏览平台的商品，随意点击商品 联系该商品的商家客服并询问对方是否需要做推广，有些有需求 的商家就通过加微信、QQ 详谈，然后我就将这些商家需要推广 的商品通过发到我的微信粉丝群、大淘客放单平台等“推手”用 来放单推广的平台上，如果有人点击进入我推广分享的商品链接 我就可以从中赚取 1-3 元的佣金。广州市白云区永兴村榕树塘村 北三巷 28 号 201 房是我男朋友陈远城、蒋魁合租的，他们租来用 作机房的，陈远城告诉我机房是他们用来帮中国移动公司养电话 卡的，这些电话卡不能打电话、不能发短信，没有流量的，只能 收短信，平时蒋魁、“公牛”二人都住在机房的。我以前在手机店 上过班，据我了解每个手机营业厅都有电话卡销量的任务数，为 了达标就把这些电话卡插到十几个或上百的卡槽设备，这样电话 卡就自动激活并假象使用，实际就是移动公司营造业绩增长的假 象，这就是养电话卡的意思。陈远城跟我说过，电话卡是他们从 南昌的一承包公司拿回来的，他们就帮忙养这些电话卡，南昌的 承包公司就会给他们一定的提成。我不清楚陈远城等人是否在通 过养电话卡进行诈骗。我不清楚现场查获的 SIM 卡卡槽来源。我 不知道民警在永兴村榕树塘村北三巷 28 号 201 房的电脑发现大量 的公民个人身份信息，他们用来干什么，也不知道来源情况。

4.证人吴可可的证言，该证据证实了：我就读于广州工商学 院，现在广州大淘客网络科技有限公司实习，我的主要工作就是 推广淘宝、拼多多的商品。有时候我通过谢菁菁给我的淘宝、拼 多多账号浏览平台上的商品，并主动联系上家询问对方是否需要 商品推广，有时候是上家会找到我们，我们就帮有需要的商家在 谢菁菁的微信粉丝群发布商品链接进行推广。如果有人点击我分 享的商品链接进行购买，我就可以从中获利，都是谢菁菁、陈远 城转账给我的。陈远城在我们居住的附近租了一个出租屋（具体 地址我不清楚），他们称这里“机房”，陈远城、蒋魁、“公牛”都 在这里工作，但我不知道他们从事的是什么工作。

5.证人黄嘉华的证言，该证据证实了：我是负责树塘街北 28 号 201 室内 12 台电脑启动、关闭、发现故障和问题后报告等工作 的。主要看火云卡商端 V21.3、酷卡 1000 系统是否自动运行，这 两个系统是自动操控室内其他电脑运行的，用来注册微信号的， 里面电脑不需要显示屏。我电脑里的公民个人信息、电话号码是 通过网络上 QQ 群内一个群名叫“……”（名字我忘记了），以 2 元一条，我买了 100 元，但有 50 条是可以用来注册微信、推广网 络产品，同事蒋魁、负责人陈远城买了多少，我就不清楚了。从 拼多多 APP 平台

上复制产品、链接网址，我就把商品、链接发给 “微信朋友圈”；而这些“微信朋友圈”，是通过以上火云卡商端 V21.3、酷卡 1000 系统自动注册的，“微信朋友圈”就吸纳其他“好友”，来点击这些产品和链接。蒋魁负责的那台电脑提供易码平台 的验证码，我就把这些来源于手机号码的验证码向 QQ 群（名字 我忘记了）发布，让客户购买手机号码、在 QQ 群（名字我忘记 了）注册、并获取验证码。蒋魁是我在嘉禾广信中学的初中同学, 是他今年 5 月初就叫我帮他做事，我就与蒋魁吃住工作都在这个 房间，都是蒋魁、陈远城付款的，他们至今都没有给我工钱。我 在网上购买公民个人信息，是陈远城给钱给我叫我在网上买的， 我买回来之后就发给陈远城，陈远城就利用这些公民信息注册微 信和推广网络产品，然后我就把这些微信号和网络产品发到朋友 圈让有需要的网友点击，网友购买后我们就会获得 10%-20%的佣 金，这些钱都会转给陈远城。

6.辨认材料，该证据证实了：对被告人陈远城的辨认情况。

7.手机、笔记本电脑、iPad、电脑主机、卡槽、电话卡等物 证照片，该证据证实了：涉案作案工具的基本情况。

8.扣押清单、扣押决定书，该证据证实了：扣押涉案物品笔 记本电脑 1 台、ipadl 台、小米牌无线移动电话机 1 台及电脑主机、 电话卡、卡槽等物品 1 批。

9.公民信息截图，该证据证实了：名为“500w 料子” excel 文档内约 1048576 条公民信息，主要为公民姓名、身份证号、手 机号、邮箱，来自陈远城笔记本电脑（机房主机电脑亦保存）。陈 远城认签是其用来注册微信号等。名为“某酒店 2000W 开房信息” 截图显示 1520 条公民信息，主要为公民姓名、身份证号、出生日 期、（酒店）地址，共计 51 页，来自陈远城笔记本电脑。陈远城 认签是其用来注册微信号等。证人谢菁菁、吴可可、黄嘉华认签 陈远城笔记本电脑内公民信息截图。

10.现场勘查笔录及现场照片，该证据证实了：涉案现场的概 貌特征。

11.搜查笔录、附搜查证，该证据证实了：公安人员对白云区 龙归永兴榕树塘街北一巷 12 号 203 房、榕树塘街北二巷 28 号 201 房进行搜查的经过及查获物品情况。

12.被告人陈远城的身份材料，该证据证实了：被告人陈远城 犯罪时已满 18 周岁，已达完全刑事责任年龄。

13.到案经过，该证据证实了：抓获本案被告人陈远城归案的 具体时间、地点、详细经过。

关于被告人陈远城及其辩护人辩称被告人仅购买公民个人 信息 200 余条，不构成情节特别严重的意见，本院综合评析如下: 根据现有物证、书证、证人证言、被告人供述等证据显示，从被 告人电脑内发现了共计 105 万余条公民个人信息。被告人虽辩称 仅购买 200 余条信息，其余均系他人通过互联网免费发给其，但 被告人并不具备合法获取公民个人信息的资质，且其获取该信息 的目的是为了注册微信号并用于出售或以其他方式牟取非法利益，主观上存在非法获取公民个人信息的故意。因此，被告人违 反国家有关规定，通过购买、收受等方式获取公民个人信息，属 于刑法所规定的“以其他方法非法获取公民个人信息”的情形。 本案中，被告人以购买、收受等方式获取公民个人信息数量达 105 万余条，已达到刑法规定的“情节特别严重”标准。故上述辩解、 辩护意见，本院不予采纳。

关于辩护人提出涉案大部分信息已经被注册过，用处不大， 且非真实存在的辩护意见。经查，涉案信息含有姓名、公民身份 证号码、手机号、邮箱等信息，属于公民个人信息的范畴。即使 大部分信息无法用于微信账号的实名认证，但该信息仍属于真实 存在的公民个人信息。被告人及其辩护人也未提供相关证据证明 该信息非真实存在。另外，现有证据显示，被告人长期向多人出 售微信账号，足以证实被告人获取的公民个人信息的真实性。故 该辩解意见，本院不予采纳。

本院认为，被告人陈远城违反国家有关规定，非法获取公民 个人信息，其行为已构成

侵犯公民个人信息罪。公诉机关指控被 告人陈远城犯侵犯公民个人信息罪，事实清楚，证据确实、充分，罪名成立。被告人陈远城当庭表示认罪，可以酌情从轻处罚。辩 护人系初犯、偶犯、自愿认罪等辩护意见，本院在量刑时予以考 量。本院综合全案的性质、情节、危害后果及被告人的认罪态度， 依照《中华人民共和国刑法》第二百五十三条之一第一、三款、 第五十二条、第五十三条及第六十四条之规定，判决如下：

一、 被告人陈远城犯侵犯公民个人信息罪，判处有期徒刑三 年，并处罚金人民币五千元（刑期从判决执行之日起计算。判决 执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 6 月 3 日起至 2022 年 6 月 2 日止。罚金自本判决生效第一日起五日 内缴纳）。

二、 缴获的作案工具笔记本电脑 1 台、诣'11 1 台、小米牌无

线移动电话机 1 台等物品（以扣押清单为准），予以没收（由广州 市公安局白云区分局执行）。

如不服本判决，可在接到判决书的第二日起十日内，通过本 院或直接向广东省广州市中级人民法院提出上诉。书面上诉的， 应当提交上诉状正本一份，副本二份。

审 判 长 刘侃

人民陪审员 李清萍

人民陪审员 唐翠梅

二 0 二 0 年八月十八日

案例二、李志冲等人侵犯公民个人信息案

广东省广州市白云区人民法院

刑事判决书

（2020）粤 0111 刑初 1116 号

公诉机关广州市白云区人民检察院。

被告人陈勇，男，1992 年 12 月 15 日出生，汉族，文化程度 初中，户籍地为江西省丰城市拖船镇后村村楼台组 8 号。因本案 于 2019 年 8 月 20 日被羁押并于同日被刑事拘留，同年 9 月 27 日被逮捕。现羁押于广州市白云区看守所。

辩护人张丽梅，广东知荣律师事务所律师。

被告人李志冲，男，1992 年 12 月 11 日出生，汉族，文化程 度初中，户籍地为广州市从化区鳌头镇上西村禾塘队月星 16 号。 因本案于 2019 年 10 月 26 日被羁押并于同日被刑事拘留，同年 11 月 19 日被逮捕。现羁押于广州市白云区看守所。

辩护人黄泽珊，广东金桥百信律师事务所律师。

被告人张奇，男，1994 年 9 月 2 日出生，汉族，文化程度初 中，户籍地为湖北省天门市（以上身份情况均系被告人自报）。因 本案于 2019 年 8 月 20 日被羁押并于同日被刑事拘留，同年 9 月 27 日被逮捕。现羁押于广州市白云区看守所。

辩护人李汉林，广东合邦律师事务所律师（由广州市白云区 法律援助处指派）。

被告人张耿伟，男，1992 年 3 月 10 日出生，汉族，文化程 度初中，户籍地为广东省惠来县葵潭镇长春管区长青里一巷 6 号。 因本案于 2019 年 8 月 20 日被羁押并于同日被刑事拘留，同年 9 月 27 日被逮捕。现羁押于广州市白云区看守所。

辩护人邓艳琴，广东联合发展律师事务所律师（由广州市白 云区法律援助处指派）。

被告人唐伟奇，男，1997 年 1 月 8 日出生，汉族，文化程度 初中，户籍地为广州市从化区良口镇仙溪村中间社 10 号。因本案 于 2019 年 8 月 20 日被羁押并于同日被刑事拘留，同年 9 月 27 日被逮捕。现羁押于广州市白云区看守所。

辩护人刘秋霞，广东南磁律师事务所律师（由广州市白云区 法律援助处指派）。

被告人曾芳琴,女，1986 年 10 月 6 日出生，汉族，文化程 度初中，户籍地为广东省潮

州市潮安区沙溪镇高厦一村新厝中区 西三巷 1 号。因本案于 2019 年 8 月 20 日被羁押并于同日被刑事 拘留，同年 9 月 27 日被逮捕。现羁押于广州市白云区看守所。

辩护人李军、薛李锡灿，广东为峰（白云）律师事务所律师。

广州市白云区人民检察院以穗云检二部刑诉[2020] 514 号 起诉书，指控被告人陈勇、李志冲、张奇、张耿伟、唐伟奇、曾 芳琴犯侵犯公民个人信息罪，于 2020 年 4 月 23 日向本院提起公 诉。本院依法适用普通程序，组成合议庭，公开开庭审理了本案。 广州市白云区人民检察院指派检察员冯杏华出庭支持公诉，被告 人陈勇、李志冲、张奇、张耿伟、唐伟奇、曾芳琴及其辩护人均到庭参加诉讼。本案现已审理终结。

公诉机关指控：2018 年年底开始，被告人陈勇从被告人李志 冲、张奇等人处购买以真实身份信息登记的电话卡并加价转卖。 2019 年 8 月 20 日晚，陈勇在本市白云区永平街东达工业园时代 公寓 B 栋 609 房被抓获，并从其处缴获手机 1 台、空选白卡 2000 张等物。经统计，陈勇的转卖收入为人民币（下同）68892 元以 上。

2018 年 12 月开始，被告人李志冲通过帮助被告人陈勇开展 “地推”业务，收集以真实身份信息登记的电话卡并售卖给陈勇。

2019 年 10 月 26 日下午，李志冲在本市从化区江浦街红荔新村 3 栋 101 房其经营的手机店内被抓获，并从其处缴获手机 1 台。经 统计，李志冲的售卖收入为 64632 元。

2018 年 7 月开始，被告人张奇从被告人陈勇、唐伟奇、曾芳 琴等人处购买以真实身份信息登记的电话卡并加价转卖。2019 年 8 月 20 日上午，张奇在本市白云区永平街东平村沙园二路 38 号 503 房被抓获，并从其处缴获手机 1 台等物。经统计，张奇的转 卖收入为人民币 51650 元。

2019 年 3 月开始，被告人张耿伟从被告人唐伟奇、曾芳琴等 人处购买以真实身份信息登记的电话卡并加价转卖。同年 8 月 20 日上午，张耿伟在本市白云区永平街东平马市里南街 14 号 601 房被抓获，并从其处缴获手机 6 台、开卡器 1 部等物。经统计， 张耿伟的转卖收入为 11112 元。

2019 年 1 月开始，被告人唐伟奇通过帮助他人开展“地推”

业务，收集以真实身份信息登记的电话卡并售卖给被告人张奇、 张耿伟。同年 8 月 20 日上午，唐伟奇在本市白云区永平街永兴庄 永兴西街 49 号 901 房被抓获，并从其处缴获手机 5 台、读写卡多 功能设备 1 部等物。经统计，唐伟奇的售卖收入为 9622 元。

2019 年 3 月开始，被告人曾芳琴通过经营通讯业务，收集以 真实身份信息登记的电话卡并售卖给被告人张奇、张耿伟。2019 年 8 月 20 日上午，曾芳琴在本市白云区东平村东平路曾芳琴新动 力通讯手机店内被抓获，并从其处缴获手机 1 台等物。经统计， 曾芳琴的售卖收入为 6880 元。

公诉机关认为，被告人陈勇、李志冲、张奇、张耿伟、唐伟 奇、曾芳琴违反国家有关规定，非法获取、出售公民个人信息， 陈勇、李志冲、张奇均属情节特别严重，张耿伟、唐伟奇、曾芳 琴均属情节严重，应以侵犯公民个人信息罪追究其刑事责任。张 奇、张耿伟、唐伟奇、曾芳琴犯罪后如实供述自己的罪行，可以 从轻处罚。建议对张耿伟在有期徒刑六个月至一年间量刑，并处 罚金二万元至四万元；建议对唐伟奇、曾芳琴在有期徒刑六个月 至一年间量刑，并处罚金一万元至三万元。提请本院依法判处。

被告人陈勇对起诉指控的罪名不持异议，辩称其销售的电话 卡只有 1.1 万元左右，且其是接公安的电话后回来配合调查的， 是自首，请求从宽处理。

辩护人提出：一、对起诉指控的罪名无异议。二、指控金额 有误，现有证据只能证实陈勇与张奇之间存在交易，与他人的交 易金额证据不足；同时陈勇也有向张奇购买电话卡，该部分金额 应予剔除；综上，根据陈勇与张奇之间的微信聊天记录和转账记 录，陈勇售卖实名电话卡的金额应为 21655 元。三、本案比较特 殊，陈勇转卖的都是实名电话卡而不是

公民个人信息，都是信息 所有人自愿登记的电话卡并放弃使用，亦对电话卡交付他人使用是明知，且公民信息难以被读取，故陈勇主观恶性较小。四、陈 勇是初犯，其有两个未满两岁的孩子需要抚养，请求法庭对其在 三年以下量刑并宣告缓刑。

被告人李志冲对起诉指控的罪名不持异议，请求法庭考虑其 孩子年仅三岁需要其照顾，对其从宽处理。

辩护人提出：一、对起诉指控的罪名无异议，李志冲是合法 经营手机及电话卡业务并办理了营业执照，只是因为法律意识淡 薄而不慎触犯刑律。二、李志冲收取的是正常开设电话卡的佣金，客户也是自愿实名登记并放弃电话卡，有别于一般的侵犯公民信 息犯罪。三、指控数额 64632 元不当，该数额包含了正常开卡首 次充值金额、空白卡成本等，该部分应予剔除，李志冲当庭陈述 其贩卖了 200-300 张电话卡，每张佣金 22-45 元，按照最大数额 计算，本案犯罪金额为 13500 元。四、李志冲犯罪时间短，案发 前半年已经没有再实施罪行，且有三岁的孩子需要抚养，请求法 庭对其在三年以下量刑并宣告缓刑。

被告人张奇对起诉指控的罪名不持异议，辩称指控的犯罪金 额过高，其售卖实名电话卡的金额只有 3 万多元，请求法庭核实 并对其从宽处理。

辩护人提出：一、对起诉指控的罪名无异议。二、指控张奇

犯罪数额 51650 元无审计报告予以佐证，仅通过手机微信截图的 推算不能成立，应采信其当庭供述的 3 万多元作为犯罪数额。三、 张奇是初犯，一直如实供述罪行，有明显的悔罪表现。

被告人张耿伟对起诉指控的事实及罪名不持异议，请求法庭 考虑其法律意识淡薄，如实供述罪行，对其从宽处理。

辩护人提出：一、张耿伟犯罪后如实供述罪行，有悔罪表现。 二、张耿伟主观恶性不大，其罪行没有造成严重后果，请求法庭 对其从宽处理。

被告人唐伟奇对起诉指控的事实及罪名不持异议，请求法庭 考虑其家庭状况不好，对其从宽处理。

辩护人提出：一、唐伟奇与本案其他被告人不是团伙作案， 所造成的危害性较小。二、唐伟奇到案后如实供述罪行，有悔罪 表现，请求法庭对其宣告缓刑。

被告人曾芳琴对起诉指控的事实及罪名不持异议，请求法庭 考虑其法律意识淡薄，对其从宽处理。

辩护人提出：一、曾芳琴如实供述罪行，悔罪表现明显。二、 曾芳琴涉案金额最小，只是因为法律意识淡薄而不慎触犯刑律， 请求法庭对其宣告缓刑。

经审理查明：H2018 年年底开始，被告人陈勇从被告人李志 冲、张奇等人处购买以他人真实身份信息登记开设而未取走的电 话卡（下称“实名电话卡”）约 270 张并以每张 60 元至 70 元的价 格加价转卖牟利。2019 年 8 月 20 日上午，公安人员前往陈勇居 住的本市白云区永平街东达工业园时代公寓 B 栋 609 房抓捕陈 勇,，因陈勇不在家，公安人员要求陈勇家属电话通知其返回家中 接受调查，陈勇返回后被公安人员抓获。公安人员并从该处缴获空选白卡 2000 张、移动及联通公司实名电话卡 16 张等物。经统 计，陈勇转卖实名电话卡收入约 20020 元。

㈡2018 年 12 月开始，被告人李志冲通过帮助被告人陈勇开 展“地推”业务，为移动及联通等通讯公司推销实名电话卡，并 将客户开设后未取走的实名电话卡约 600 张，以每张 20 元至 45 元的价格转卖给陈勇等人。2019 年 10 月 26 日下午，李志冲在本 市从化区江浦街红荔新村 3 号 101 房其经营的手机店内被抓获， 并从其处缴获手机 1 台。经统计，李志冲转卖实名电话卡收入约 27000 元。

㈢2018 年 7 月开始，被告人张奇从被告人陈勇、唐伟奇、曾 芳琴等人处购买以他人名义开设的实名电话卡约 500 余张，并以 每张约 70 元至 85 元的价格转卖牟利。2019 年 8 月

2。日上午， 张奇在本市白云区永平街东平村沙园二路 38 号 503 房被抓获，并 从其处缴获移动及联通公司实名电话卡 77 张、手机 1 台等物。经 统计,张奇转卖实名电话卡收入约 42500 元。

㈣2019 年 3 月开始，被告人张耿伟从被告人唐伟奇' 曾芳琴 等人处购买以他人身份信息登记的实名电话卡并加价转卖。同年 8 月 20 日上午，张耿伟在本市白云区永平街东平马市里南街 14 号 601 房被抓获，并从其处缴获手机 6 台、开卡器 1 部等物。经 统计，张耿伟转卖实名电话卡收入为 mu 元。

㈤2019 年 1 月开始，被告人唐伟奇通过帮助他人开展“地推”

业务，收集客户以真实身份信息登记开设而未取走的实名电话卡 并售卖给被告人张奇、张耿伟。同年 8 月 20 日上午，唐伟奇在本 市白云区永平街永兴庄永兴西街 49 号 901 房被抓获，公安机关从 其处缴获手机 5 台、读写卡多功能设备 1 部等物。经统计，唐伟 奇转卖实名电话卡收入为 9622 元。

只 2019 年 3 月开始，被告人曾芳琴通过经营通讯业务，收集 客户以其实身份信息登记开设而未取走的电话卡并售卖给被告人 张奇、张耿伟。2019 年 8 月 20 日上午，曾芳琴在本市白云区东 平村东平路曾芳琴新动力通讯手机店内被抓获，并从其处缴获手 机 1 台等物。经统计，曾芳琴转卖实名电话卡收入为 6880 元。

上述事实，有以下经庭审举证、质证，本院予以确认的证据 证实：被告人陈勇、李志冲、张奇、张耿伟、唐伟奇、曾芳琴的 供述，证人钟海森、黄家晖、周凯、黄丽仪的证言，辨认材料， 现场勘查笔录、搜查笔录及赃物照片，微信聊天记录、转账记录 的截图，实名电话卡销售单据，电子数据检查勘验记录及鉴定书， 视听资料，移动、联通及电信公司的实名制入网办理规定，调取 证据通知书，扣押清单，到案经过，公安机关出具的到案情况说 明，身份材料，受案登记表及立案决定书。

关于被告人及辩护人提出有关犯罪金额、自首等的意见，现 评析如下：一、本案多名被告人均系电信通讯业务的经营者，虽 现有证据中各被告人手机内存有非法转卖实名电话卡的微信聊天 记录、转账记录等内容，但该部分证据不能完全对应一致，同时 未能剔除陈勇、李志冲、张奇手机内合法通讯业务的交易金额，

且侦查机关未对被告人手机内涉及犯罪金额的内容进行甄别，全 盘导出及审计，故陈勇、李志冲、张奇的犯罪金额应以其在侦查 阶段初期供述的数量、金额及当庭的供述为准。二、被告人陈勇 虽有主动投案的情节，但其归案后未能如实供述其售卖实名电话 卡牟利的事实，故不应认定具有自首情节。

本院认为，被告人陈勇、李志冲、张奇、张耿伟、唐伟奇、 曾芳琴违反国家有关规定，采取蒙骗、利诱等手段非法获取并出 售公民个人信息，情节严重，其行为已构成侵犯公民个人信息罪。 被告人张奇、张耿伟、唐伟奇、曾芳琴如实供述自己罪行，其中 张耿伟、唐伟奇、曾芳琴自愿认罪认罚，均可从轻处罚。被告人 陈勇、李志冲当庭自愿认罪，可以酌情从轻处罚。公诉机关的量 刑建议合理，本院予以采纳。各辩护人提出的量刑意见，本院在 量刑时将予以酌情考量。综合本案的事实、情节、危害后果及各 被告人的悔罪表现，依照《中华人民共和国刑法》第二百五十三 条之一、第六十七条第三款、第五十二条、第五十三条、第六十 四条、《中华人民共和国刑事诉讼法》第十五条之规定，判决如下:

一、被告人陈勇犯侵犯公民个人信息罪，判处有期徒刑二年, 并处罚金八万元。（刑期从判决执行之日起计算。判决执行以前先 行羁押的，羁押一日折抵刑期一日，即自 2019 年 8 月 20 日起至 2021 年 8 月 19 日止。罚金自本判决生效第二日起五日内缴纳。）

二、被告人李志冲犯侵犯公民个人信息罪，判处有期徒刑二 年，并处罚金六万元。（刑期从判决执行之日起计算。判决执行以 前先行羁押的，羁押-日折抵刑期一日，即自 2019

年 1 月 26 日起至 2021 年 10 月 25 日止。罚金自本判决生效第二日起五日内 缴纳。）

三、被告人张奇犯侵犯公民个人信息罪，判处有期徒刑二年，并处罚金六万元。（刑期从判决执行之日起计算。判决执行以前先 行羁押的，羁押一日折抵刑期一日，即自 2019 年 8 月 20 日起至 2021 年 8 月 19 日止。罚金自本判决生效第二日起五日内缴纳。）

四、被告人张耿伟犯侵犯公民个人信息罪，判处有期徒刑一 年，并处罚金二万元。（刑期从判决执行之日起计算。判决执行以 前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 8 月 20 日 起至 2020 年 8 月 19 日止。罚金自本判决生效第二日起五日内缴纳。）

五、被告人唐伟奇犯侵犯公民个人信息罪，判处有期徒刑一 年，并处罚金一万元。（刑期从判决执行之日起计算。判决执行以 前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 8 月 20 日 起至 2020 年 8 月 19 日止。罚金自本判决生效第二日起五日内缴 纳。）

六、被告人曾芳琴犯侵犯公民个人信息罪，判处有期徒刑一 年，并处罚金一万元。（刑期从判决执行之日起计算。判决执行以 前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 8 月 20 日 起至 2020 年 8 月 19 日止。罚金自本判决生效第二日起五日内缴 纳。）

七、缴获的作案工具手机、开卡器等物（详见扣押清单）， 予以没收（由广东省五华县公安局执行）。

八、缴获的赃物手机空白卡、实名卡-批（详见扣押清单），予以没收（由广东省五华县公安局执行）。

如不服本判决，可在接到判决书的第二日起十日内，通过本 院或直接向广东省广州市中级人民法院提出上诉。书面上诉的， 应当提交上诉状正本一份，副本二份。

审 判 长 邓盗华
审 判 员 魏晶晶
审 判 员 黄丽娜
书 记 员 方赛卿

案例三、颜建顺、郑榕侵犯公民个人信息、寻衅滋事案

审理法院： 永安市人民法院
案 号： （2019）闽 0481 刑初 275 号
案 由： 侵犯公民个人信息罪
裁判日期： 2019 年 11 月 26 日

永安市人民法院
刑事判决书

（2019）闽 0481 刑初 275 号

公诉机关永安市人民检察院。

被告人颜建顺，男，1993 年 5 月 2 日出生于福建省大田县，汉族，初中文化，务工人员，住福建省大田县。因涉嫌侵犯公民个人信息犯罪于 2019 年 3 月 20 日被永安市公安局刑事拘留，同年 4 月 11 日逮捕。现羁押于永安市看守所。

辩护人郑晓军、邱杰，福建枫桦律师事务所律师。

被告人郑榕，男，1988 年 5 月 21 日出生于福建省尤溪县，汉族，初中文化，务工人员，暂住永安市（户籍地址：福建省尤溪县）。因涉嫌侵犯公民个人信息犯罪于 2019 年 1 月 18 日被永安市公安局刑事拘留，同年 2 月 22 日逮捕。现羁押于永安市看守所。

辩护人刘珍福，福建枫桦律师事务所律师。

杨博，福建枫桦律师事务所实习律师。

被告人曹世鑫，男，1988 年 5 月 5 日出生于福建省尤溪县，汉族，初中文化，务工人员，暂住永安市（户籍地址：福建省尤溪县）。因涉嫌侵犯公民个人信息犯罪于 2019 年 1

月 18 日被永安市公安局刑事拘留，同年 2 月 22 日逮捕。现羁押于永安市看守所。

辩护人陈达映，福建建州联兴律师事务所律师。

被告人林建梁，男，1987 年 12 月 9 日出生于福建省尤溪县，汉族，初中文化，务工人员，住尤溪县。因涉嫌侵犯公民个人信息犯罪于 2019 年 3 月 19 日被永安市公安局刑事拘留，同年 4 月 11 日逮捕。现羁押于永安市看守所。

辩护人黄柏超、陈羽，福建泰岚律师事务所律师。

被告人苏国令，男，1987 年 9 月 15 日出生于福建省尤溪县，汉族，中专文化，务工人员，住福建省厦门市集美区（户籍地址：福建省厦门市同安区）。因涉嫌侵犯公民个人信息犯罪于 2019 年 3 月 19 日被永安市公安局刑事拘留，同年 4 月 11 日逮捕。现羁押于永安市看守所。

辩护人范丁宝、肖芳红，福建永杭律师事务所律师。

被告人林生甲，男，1990 年 4 月 13 日出生于福建省大田县，汉族，初中文化，务工人员，住福建省大田县。因涉嫌侵犯公民个人信息犯罪于 2019 年 3 月 5 日被永安市公安局刑事拘留，同年 4 月 11 日逮捕。现羁押于永安市看守所。

辩护人熊长江，福建商通律师事务所律师。

被告人吴先桥，男，1992 年 2 月 28 日出生于福建省大田县，汉族，初中文化，务工人员，住福建省大田县。因涉嫌侵犯公民个人信息犯罪于 2019 年 3 月 19 日被永安市公安局刑事拘留，同年 4 月 11 日逮捕。现羁押于永安市看守所。

辩护人廖永华，福建商通律师事务所律师。

永安市人民检察院以永检公诉刑诉〔2019〕282 号起诉书指控被告人颜建顺、林生甲、郑榕、曹世鑫、林建梁、苏国令、吴先桥侵犯公民个人信息罪、寻衅滋事罪，于 2019 年 6 月 6 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。永安市人民检察院指派检察员罗奕炫出庭支持公诉，被告人颜建顺、郑榕、曹世鑫、林建梁、苏国令、林生甲、吴先桥及其辩护人郑晓军、邱杰、刘珍福、陈达映、黄柏超、陈羽、范丁宝、熊长江、廖永华等到庭参加诉讼。现已审理终结。

永安市人民检察院指控：2018 年 3 月至 2019 年 1 月期间，被告人林生甲、颜建顺先后召集被告人郑榕、苏国令、吴先桥、林建梁、曹世鑫、郑祥铭、肖胜，陆续成立“兴融”、“融 E 借”、“万顺金服”等网络放贷公司，形成了利用网络实施放贷、购买公民个人信息、当借款人逾期未归还借款时通过电话轰炸软件、编辑侮辱性短信和微信的“软暴力”手段对借款人及其亲朋、好友、领导、同事等人进行、恐吓、辱骂和滋扰，逼迫借款人及其亲友归还借款的恶势力犯罪团伙，该恶势力犯罪团伙严重影响他人的正常生活和工作。其中：

1、2018 年年初至 2018 年 6 月间，被告人林生甲召集苏国令、吴先桥、林建梁、曹世鑫、郑榕、郑祥铭（另案处理）共同出资 50 万元进行网络高利放贷，租用永安市和北门小区出租房作为放贷地点，成立“兴融”放贷公司，使用手机、电脑等作案工具，通过微信、ＱＱ软件向借款人放款，利用“有凭证”等平台签订电子借条，收取高额服务费、逾期费。其中，被告人林生甲、吴先桥负责购买公民个人信息 6242 条用于网络放贷，被告人吴先桥、苏国令、林建梁、曹世鑫、郑榕分别负责推广放款、审核、催收。在借款人逾期未及时还款的情况下，采取短信、电话轰炸，发送恶意、侮辱性信息和微信等方式对借款人及其朋友进行威胁、恐吓、

辱骂和滋扰，迫使借款人还款，致使借款人及其朋友的正常生活、工作受到严重影响。

2、2018 年 7 月至 2018 年 9 月间，被告人颜建顺召集被告人郑榕、曹世鑫，苏国令、林建梁共同出资 20 万元，成立“融 E 借”网络放贷公司，在颜建顺位于大田县家里和永安市燕景小区租的房子里进行高利放贷。为了增加贷款客源和扩大贷款业务，由被告人颜建顺去购买公民个人信息用于放贷，被告人苏国令负责公民个人信息的整理，被告人林建梁、曹世

鑫、郑榕分别负责推广、审核、放款、财务和催收。在借款人逾期未及时还款的情况下，采取短信、电话轰炸，发送恶意、侮辱性信息等方式滋扰、辱骂借款人及其亲友，迫使借款人还款。经统计，五被告人共非法获取公民个人信息 7996 条用于网络放贷。

3、2018 年 9 月至今，被告人颜建顺召集郑榕、曹世鑫、苏国令、林建梁、肖胜（另案处理）共同出资 110 万元，购买“万顺金服”ＡＰＰ，并成立以被告人颜建顺为首的“万顺金服”网络放贷公司，在永安市进行高利放贷。被告人颜建顺和苏国令负责财务收支，被告人苏国令还负责与ＡＰＰ的对接，被告人曹世鑫和林建梁负责客户信息的审核，被告人郑榕和肖胜负责催款。同时线下经营“万顺借条”网络放贷，为了增加贷款客源和扩大贷款业务，将原购买的公民个人信息与其他放贷公司进行交换。在借款人逾期未及时还款的情况下，采取短信、电话轰炸，发送恶意、侮辱性信息和微信等方式，对借款人进行威胁、恐吓、辱骂和滋扰，迫使借款人还款，严重影响借款人及其亲友的正常生活、工作。另查明，被告人颜建顺还非法获取公民个人信息 243904 条用于网络放贷。

为证实上述指控，公诉机关当庭宣读、出示了物证、书证、被害人陈述、证人证言、被告人供述、电子数据等证据。公诉机关认为，被告人颜建顺、林生甲、郑榕、曹世鑫、林建梁、苏国令、吴先桥为实施网络小额贷款，非法购买公民个人信息用于不法用途，其行为均触犯了《中华人民共和国刑法》第二百五十三条之一的规定，应当以侵犯公民个人信息罪分别追究其刑事责任。被告人颜建顺、林生甲、郑榕、曹世鑫、林建梁、苏国令、吴先桥在追讨债务过程中，对借款人及其亲朋好友以电话轰炸、短信轰炸的方式进行辱骂、滋扰，情节恶劣，其行为均触犯了《中华人民共和国刑法》第二百九十三条第一款第（二）项之规定，应当以寻衅滋事罪分别追究其刑事责任。本案中，被告人颜建顺、林生甲、郑榕、曹世鑫、林建梁、苏国令、吴先桥在永安市区长期聚集在一起，以“软暴力”的手段，实施侵犯公民个人信息、寻衅滋事的违法犯罪行为，为非作恶、欺压百姓，扰乱社会生活秩序，造成恶劣的社会影响，应当认定为恶势力团伙。被告人颜建顺、林建梁、苏国令、吴先桥具有自首情节，被告人林生甲、郑榕、曹世鑫具有坦白情节，均自愿认罪认罚，建议判处被告人颜建顺有期徒刑二年二个月至三年，并处罚金人民币一万元至二万元；判处被告人郑榕有期徒刑一年八个月至二年二个月，并处罚金人民币四千元至八千元；判处被告人曹世鑫有期徒刑一年八个月至二年二个月，并处罚金人民币四千元至八千元；判处被告人林建梁有期徒刑一年四个月至一年十个月，并处罚金人民币四千元至八千元；判处被告人苏国令有期徒刑一年四个月至一年十个月，并处罚金人民币四千元至八千元；判处被告人林生甲有期徒刑一年至一年六个月，并处罚金人民币四千元至八千元；判处被告人吴先桥有期徒刑十个月至一年四个月，并处罚金人民币四千元至八千元。

被告人颜建顺、郑榕、曹世鑫、林建梁、苏国令、林生甲、吴先桥对公诉机关指控的犯罪事实、罪名及量刑建议均没有异议且签字具结，在开庭审理过程中亦均无异议。

辩护人郑晓军、邱杰对公诉机关指控被告人颜建顺构成侵犯公民个人信息、寻衅滋事罪的定性不持异议。认为被告人颜建顺当庭表示自愿认罪，具有自首情节，此前表现一贯良好，没有任何违法犯科，此次犯罪系初犯，人身危险性相对较小。从引发寻衅滋事犯罪的原因分析，部分被害人对本案的发生具有一定的过错。建议对被告人颜建顺予以较大幅度的减轻处罚。

辩护人刘珍福对公诉机关指控被告人郑榕的罪名和量刑建议没有异议。认为被告人郑榕不是本案犯意的提起者，所参与的三个阶段犯罪都是股份最少者，同意退赃和缴纳罚金，应以量刑建议最低刑对郑榕进行量刑，或者有条件的进行再降低量刑。

辩护人陈达映认为，曹世鑫在起诉书中指控的侵犯公民个人信息、寻衅滋事罪两起案件中所起的作用相对较小，情节相对较轻，如实供述自己的罪行，自愿认罪认罚，一贯表现良好，无前科劣迹，系初犯，认罪态度好、悔罪程度深。

辩护人黄柏超、陈羽认为，涉案公民个人信息数量应当扣除借款人自愿提供信息的部分。林建梁并非犯罪发起人，在犯罪活动中所起作用较小，应当认定为从犯。本案尚未造成被害人重大经济损失、重伤、精神失常甚至死亡等严重后果，情节较轻。被害人为了满足自身经济利益需要而向被告人以高额利息借款未及时还款付息，本身也存在过错。林建梁无前科劣迹，具有自首情节，且自愿认罪认罚，悔罪态度好，社会危害性较低。建议对林建梁从宽处罚。

辩护人范丁宝、肖芳红认为，被告人苏国令并未实施购买个人信息和催收借款这一犯罪核心的环节，只是负责推广放款、整理公民个人信息、财务做账，其在本案中程所起作用相对较小。本案的起因是被害人（借款人）逾期未归还借款而引发，被害人存在一定的过错。被告人苏国令具有自首情节，一贯表现良好，是初犯，建议判处被告人苏国令一年四个月以下有期徒刑，并适用缓刑。

辩护人熊长江认为，被告人林生甲具有坦白情节，自愿认罪，愿意接受法律的惩罚，以前没有犯罪记录，未受过刑事处罚，本次属于初犯，且平常一贯表现良好，社会危害性较小，悔罪表现深，且被害人有过错。建议对被告人林生甲判处一年有期徒刑。

辩护人廖永华对公诉机关指控被告人吴先桥的犯罪事实和罪名没有异议。认为被告人吴先桥具有自首情节，自愿认罪，愿意接受法律的惩罚，系初犯。在涉嫌寻衅滋事罪案件中被害人主观上存在一定的过错；被告人吴先桥主要负责放贷行为中的业务推广，在案件中起的作用较小，社会危害性较小。悔罪表现深，建议对被告人吴先桥从轻处罚，并适用缓刑。

经审理查明，2018 年 3 月至 2019 年 1 月期间，被告人林生甲、颜建顺先后纠集被告人郑榕、苏国令、吴先桥、林建梁、曹世鑫、郑祥铭、肖胜，陆续成立“兴融”、“融 E 借”、“万顺金服”等网络放贷公司，购买公民个人信息实施网络放贷，当借款人逾期未归还借款时，采取使用电话轰炸软件、编辑侮辱性短信和微信的“软暴力”等手段，对借款人及其亲朋、好友、领导、同事等人进行、恐吓、辱骂和滋扰，逼迫借款人及其亲友归还借款，严重影响他人的正常生活和工作，形成恶势力犯罪团伙。其中：

1、2018 年年初至 2018 年 6 月间，被告人林生甲纠集被告人苏国令、吴先桥、林建梁、曹世鑫、郑榕和郑祥铭（另案处理）商议共同出资 50 万元进行网络高利放贷，租用永安市和北门小区出租房作为放贷地点，成立“兴融”放贷公司，使用手机、电脑等作案工具，通过微信、ＱＱ软件向借款人放款，利用“有凭证”等平台签订电子借条，收取高额服务费、逾期费，并进行分工实施高利放贷。其中，被告人林生甲、吴先桥负责购买公民个人信息 6242 条用于网络放贷，被告人吴先桥、苏国令负责推广放款，被告人林建梁、曹世鑫负责审核工作，被告人郑榕负责催收。在借款人逾期未及时还款的情况下，采取短信、电话轰炸，发送恶意、侮辱性信息和微信等方式对借款人吴宪澎、潘某 1、余旭、张呈凤以及潘某 1 的朋友蔡某进行威胁、恐吓、辱骂和滋扰，迫使借款人还款，致使借款人及其朋友的正常生活、工作受到严重影响。

2、2018 年 7 月至 2018 年 9 月间，被告人颜建顺召集被告人郑榕、曹世鑫，苏国令、林建梁作为股东共同出资 20 万，成立“融Ｅ借”网络放贷公司，在颜建顺位于大田县家里和永安市燕景小区租的房子里进行高利放贷。为了增加贷款客源和扩大贷款业务，由被告人颜建顺负责购买公民个人信息用于放贷，被告人苏国令负责公民个人信息的整理，被告人林建梁负责推广，被告人曹世鑫负责审核，被告人郑榕负责放款、财务和催收。在借款人逾期未及时还款的情况下，采取短信、电话轰炸，发送恶意、侮辱性信息等方式滋扰、辱骂借款人及其亲朋好友，迫使借款人还款。经统计，五被告人共非法获取公民个人信息 7996 条用于网络放贷。

3、2018 年 9 月至 2019 年 1 月，被告人颜建顺纠集被告人郑榕、曹世鑫、苏国令、林建梁和肖胜（另案处理）共同出资 110 万元，购买“万顺金服”ＡＰＰ，并成立以被告人颜建

顺为首的“万顺金服”网络放贷公司，在永安市进行高利放贷，同时线下经营“万顺借条”网络放贷。在实施网络高利放贷过程中，被告人颜建顺和苏国令负责财务收支，被告人苏国令还负责与ＡＰＰ的对接，被告人曹世鑫和林建梁负责客户信息的审核，被告人郑榕和肖胜负责催款。为了增加贷款客源和扩大贷款业务，将原购买的公民个人信息与其他放贷公司进行交换。在借款人逾期未及时还款的情况下，采取短信、电话轰炸，发送恶意、侮辱性信息和微信等方式，对借款人余某、林某2、郭某1、石某、刘某1、解某、李某1、刘某2、李某2、李某3、潘某2、郭某1、李来斌、自芹枝、郭某2及其亲朋好友钟某、周某1、林某1、罗某、陈某、周某2等人进行威胁、恐吓、辱骂和滋扰，迫使借款人还款，严重影响借款人及其亲友的正常生活、工作。

另查明，被告人颜建顺在实施网络放贷过程中，还通过网络非法获取公民个人信息243904条，用于个人使用。

案发后，被告人郑榕、曹世鑫于2019年1月18日被抓获到案；被告人林生甲于2019年3月5日被抓获到案；被告人苏国令、林建梁、吴先桥于2019年3月19日主动到永安市公安局投案；被告人颜建顺于2019年3月20日主动到永安市公安局投案。永安市公安局扣押的手机20部、笔记本电脑1台、电脑主机6台、银行卡4张；从被告人郑榕处扣押的闽Ｇ×××××号凯迪拉克牌小车1辆，从被告人曹世鑫处扣押的闽Ｇ×××××号别克牌小车1辆，从被告人林生甲处扣押的ｉＰｈｏｎｅＸ手机1部，从被告人吴先桥处扣押的华为牌手机1部，从被告人林建梁处扣押的ｉＰｈｏｎｅ6手机1部，从被告人苏国令处扣押的ｉＰｈｏｎｅ7手机1部，从被告人颜建顺处扣押的ｉＰｈｏｎｅ7Ｐ手机1部，均未随案移送。

上述事实有经庭审质证、确认的下列证据证实，足以认定：

1.搜查笔录、扣押笔录、扣押决定书、扣押清单；2.电脑记录截图、房屋租赁协议书、报销清单、万顺金服总表、兴融薪资发放表；3.微信、短信记录截图，微信聊天记录、转账记录，短信记录及支付宝信息；4.还款提醒消息模板ｔｘｔ、售后短信轰炸模板ｔｘｔ、售后怼人信息模板ｔｘｔ等资料；5.调取证据清单、银行账户交易明细；6.颜建顺购买的公民个人信息、电脑文件“1”记录、公民信息数据记录、说明；7.户籍证明、人员基本信息、到案经过、归案情况说明、违法犯罪经历查询情况表；8.证人杜某、吴某、潘某1、蔡某、余某、钟某、周某1、林某2、林某1、赵某、石某、黄某、刘某1、解某、李某1、刘某2、李某2、李某3、潘某2、郭某1、李某4、自芹枝、罗某、陈某、周某2、郭某2、郭某3等人的证言；9.电子数据检验报告和电子数据光盘；10.同案人肖胜、郑祥铭的供述；11.被告人颜建顺、郑榕、曹世鑫、林建梁、苏国令、林生甲、吴先桥的供述与辩解。

本院认为，被告人颜建顺、林生甲、郑榕、曹世鑫、林建梁、苏国令、吴先桥为实施网络小额款贷，非法购买公民个人信息用于不法用途，情节严重，其行为均已构成侵犯公民个人信息罪，其中被告人颜建顺属情节特别严重。被告人颜建顺、林生甲、郑榕、曹世鑫、林建梁、苏国令、吴先桥在追讨债务过程中，对借款人及其亲朋好友采取电话、短信轰炸的方式进行辱骂、滋扰，情节恶劣，其行为又均已构成寻衅滋事罪。公诉机关的指控成立，应予依法惩处，七被告人的行为属共同犯罪。七被告人均一人犯数罪，应数罪并罚。被告人颜建顺、林生甲、郑榕、曹世鑫、林建梁、苏国令、吴先桥在永安市区长期聚集在一起，以“软暴力”的手段，实施侵犯公民个人信息、寻衅滋事的违法犯罪行为，为非作恶、欺压百姓，扰乱社会生活秩序，造成恶劣的社会影响，属恶势力团伙，应从重处罚。七被告人在共同犯罪中，按照事先分工分别实施了出资、购买公民个人信息、通过网络实施放贷、催讨欠款等行为，各自均在共同犯罪中起到不可或缺的作用，不宜区分主从犯。被告人颜建顺、林建梁、苏国令、吴先桥在案发后主动到公安机关投案，如实供述自己的犯罪事实，属自首，可以从轻或者减轻处罚。被告人郑榕、曹世鑫、林生甲归案后均能如实供述自己的犯罪事实，属坦白，可以从轻处罚。七被告人主动缴纳罚金，有较好的悔罪表现，且愿意接受处罚，可以从

轻处罚。综合以上量刑情节，对被告人颜建顺可以减轻处罚，对被告人郑榕、曹世鑫、林建梁、苏国令、林生甲、吴先桥可以从轻处罚。公诉机关提出的量刑建议适当，本院予以采纳。辩护人提出的以上辩护意见，本院予以采纳，其他辩护意见，本院不予采纳。据此，依照《中华人民共和国刑法》第二百五十三条之一第一款、第三款、第二百九十三条第一款第（二）项、第二十五条第一款、第六十九条、第六十七条第一款、第三款、第六十四条，《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》第四条、第五条第一款第（五）项、第二款第（三）项、第十一条、第十二条，《最高人民法院、最高人民检察院关于办理寻衅滋事刑事案件适用法律若干问题的解释》第三条第（一）项、第（五）项，《中华人民共和国刑事诉讼法》第十五条、第二百零一条第一款的规定，判决如下：

一、被告人颜建顺犯侵犯公民个人信息罪，判处有期徒刑一年九个月，并处罚金人民币二万元，犯寻衅滋事罪，判处有期徒刑一年五个月，决定执行有期徒刑三年，并处罚金人民币二万元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 3 月 20 日起至 2022 年 3 月 19 日止。罚金已缴纳。）

二、被告人郑榕犯侵犯公民个人信息罪，判处有期徒刑八个月，并处罚金人民币八千元，犯寻衅滋事罪，判处有期徒刑一年十个月，决定执行有期徒刑二年二个月，并处罚金人民币八千元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 1 月 18 日起至 2021 年 3 月 17 日止。罚金已缴纳。）

三、被告人曹世鑫犯侵犯公民个人信息罪，判处有期徒刑八个月，并处罚金人民币八千元，犯寻衅滋事罪，判处有期徒刑一年十个月，决定执行有期徒刑二年二个月，并处罚金人民币八千元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 1 月 18 日起至 2021 年 3 月 17 日止。罚金已缴纳。）

四、被告人林建梁犯侵犯公民个人信息罪，判处有期徒刑七个月，并处罚金人民币七千元，犯寻衅滋事罪，判处有期徒刑一年七个月，决定执行有期徒刑一年十个月，并处罚金人民币七千元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 3 月 19 日起至 2021 年 1 月 18 日止。罚金已缴纳。）

五、被告人苏国令犯侵犯公民个人信息罪，判处有期徒刑七个月，并处罚金人民币七千元，犯寻衅滋事罪，判处有期徒刑一年七个月，决定执行有期徒刑一年十个月，并处罚金人民币七千元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 3 月 19 日起至 2021 年 1 月 18 日止。罚金已缴纳。）

六、被告人林生甲犯侵犯公民个人信息罪，判处有期徒刑一年，并处罚金人民币五千元，犯寻衅滋事罪，判处拘役五个月，决定执行有期徒刑一年，并处罚金人民币五千元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 3 月 5 日起至 2020 年 3 月 4 日止。罚金已缴纳。）

七、被告人吴先桥犯侵犯公民个人信息罪，判处有期徒刑十个月，并处罚金人民币四千元，犯寻衅滋事罪，判处拘役四个月，决定执行有期徒刑十个月，并处罚金人民币四千元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自 2019 年 3 月 19 日起至 2020 年 1 月 18 日止。罚金应于判决生效后 10 日内缴纳。）

八、扣押的手机、笔记本电脑、银行卡等涉案物品，由永安市公安局予以没收；扣押的

闽Ｇxxxxx号凯迪拉克牌小车、闽Ｇxxxxx号别克牌小车，由永安市公安局发还被告人郑榕、曹世鑫。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或者直接向福建省三明市中级人民法院提出上诉。书面上诉的，应提交上诉状正本一份，副本八份。

审 判 长　陈华蓉

审 判 员　宋明泉

人民陪审员　　蔡文洋

二〇一九年十一月二十六日

书 记 员　林燕榕

案例四、杭州魔蝎数据科技有限公司、周江翔、袁冬侵犯公民个人信息案

杭州魔蝎数据科技有限公司、周江翔、袁冬侵犯公民个人信息罪一审刑事判决书

杭州市西湖区人民法院

（2020）浙 0106 刑初 437 号

公诉机关杭州市西湖区人民检察院。

被告单位杭州魔蝎数据科技有限公司，住所地杭州市滨江区滨安路******。

法定代表人周江翔，总经理。

诉讼代表人金敏浩，男，1976 年 1 月 27 日出生，汉族，住杭州市西湖区。

辩护人孙建保、陈沛文，上海靖予霖律师事务所律师。

被告人周江翔，男，1976 年 1 月 19 日出生，汉族，硕士研究生文化，、总经理，住杭州市西湖区。因本案于 2019 年 9 月 7 日被刑事拘留，同年 10 月 13 日被逮捕。

辩护人徐传水，浙江中格律师事务所律师。

辩护人吴卫明，上海市锦天城律师事务所律师。

被告人袁冬，男，1987 年 9 月 2 日出生，汉族，大学本科文化，住浙江省杭州市余杭区。因本案于 2019 年 9 月 7 日被刑事拘留，同年 10 月 13 日被逮捕。

辩护人姚品信、魏紫琼，上海浩信（杭州）律师事务所律师。

杭州市西湖区人民检察院以西检一部刑诉〔2020〕1629 号起诉书指控被告单位杭州魔蝎数据科技有限公司（以下简称魔蝎公司）、被告人周江翔、袁冬犯侵犯公民个人信息罪，于 2020 年 9 月 10 日向本院提起公诉。本院依法组成合议庭，公开开庭审理了本案。杭州市西湖区人民检察院检察员裘少波、检察官助理庄远出庭支持公诉，被告单位魔蝎公司诉讼代表人金敏浩及辩护人孙建保、陈沛文，被告人周江翔及其辩护人徐传水、吴卫明，被告人袁冬及其辩护人姚品信、魏紫琼均到庭参加诉讼。现已审理终结。

杭州市西湖区人民检察院指控，2016 年初，被告单位魔蝎公司由周江翔等人出资成立，被告人周江翔系魔蝎公司法定代表人、总经理，负责公司整体运营，被告人袁冬系魔蝎公司技术总监，系技术负责人，负责相关程序设计。魔蝎公司主要与各网络贷款公司、小型银行进行合作，为网络贷款公司、银行提供需要贷款的用户的个人信息及多维度信用数据，方式是魔蝎公司将其开发的前端插件嵌入上述网贷平台 A**中，在网贷平台用户使用网贷平台的 APP 借款时，贷款用户需要在魔蝎公司提供的前端插件上，输入其通讯运营商、社保、公积金、淘宝、京东、学信网、征信中心等网站的账号、密码，经过贷款用户授权后，魔蝎公司的爬虫程序代替贷款用户登录上述网站，进入其个人账户，利用各类爬虫技术，爬取（复制）上述企、事业单位网站上贷款用户本人账户内的通话记录、社保、公积金等各类数据，并按与用户的约定提供给网贷平台用于判断用户的资信情况，并从网贷平台获取每笔 0.1 元至 0.3 元不等的费用。期间，魔蝎公司在和个人贷款用户签订的《数据采集服务协议》中明确告知贷款用户“不会保存用户账号密码，仅在用户每次单独授权的情况下采集信息”，但未经用

户许可仍采用技术手段长期保存用户各类账号和密码在自己租用的阿里云服务器上。被告人周江翔明知公司存在保存用户账户密码的行为，未尽管理职责；被告人袁冬负责编写具有保存用户账户密码功能的网关程序。截至 2019 年 9 月案发时，对魔蝎公司租用的阿里云服务器进行勘验检查，发现以明文形式非法保存的个人贷款用户各类账号和密码条数多达 21241504 条。其中大部分账号密码，如淘宝、京东等，无法二次使用，仅有邮箱等部分账号密码存在未经用户授权被魔蝎公司二次使用的情况。上述事实，有被告人供述和辩解、证人证言及相关书证等证据予以证实。认为被告单位魔蝎公司的行为已构成侵犯公民个人信息罪。被告人周江翔、袁冬分别系对被告单位魔蝎公司侵犯公民个人信息行为直接负责的主管人员和其他直接责任人员，其行为均已构成侵犯公民个人信息罪。建议判处被告单位魔蝎公司罚金人民币 3000 万元；判处被告人周江翔、袁冬有期徒刑三年，适用缓刑，并处罚金。

被告单位魔蝎公司诉讼代表人、被告人周江翔、袁冬对指控的犯罪事实和罪名均无异议且签字具结。

被告单位魔蝎公司的辩护人提出，被告单位犯罪作用较轻，未产生严重后果，也尽到了一定的注意义务，请求判处较轻的罚金刑。

被告人周江翔的辩护人提出，被告人周江翔具有坦白情节、自愿认罪认罚，请求对刑期及罚金均从轻处罚并适用缓刑。

被告人袁冬的辩护人提出，被告人袁冬具有坦白情节，自愿认罪认罚，家庭困难，请求从轻处罚并适用缓刑。

经审理查明：2016 年初，被告单位魔蝎公司由周江翔等人出资成立，被告人周江翔系魔蝎公司法定代表人、总经理，负责公司整体运营，被告人袁冬系魔蝎公司技术总监，系技术负责人，负责相关程序设计。魔蝎公司主要与各网络贷款公司、小型银行进行合作，为网络贷款公司、银行提供需要贷款的用户的个人信息及多维度信用数据，方式是魔蝎公司将其开发的前端插件嵌入上述网贷平台 A**中，在网贷平台用户使用网贷平台的 APP 借款时，贷款用户需要在魔蝎公司提供的前端插件上，输入其通讯运营商、社保、公积金、淘宝、京东、学信网、征信中心等网站的账号、密码，经过贷款用户授权后，魔蝎公司的爬虫程序代替贷款用户登录上述网站，进入其个人账户，利用各类爬虫技术，爬取（复制）上述企、事业单位网站上贷款用户本人账户内的通话记录、社保、公积金等各类数据，并按与用户的约定提供给网贷平台用于判断用户的资信情况，并从网贷平台获取每笔 0.1 元至 0.3 元不等的费用。期间，魔蝎公司在和个人贷款用户签订的《数据采集服务协议》中明确告知贷款用户“不会保存用户账号密码，仅在用户每次单独授权的情况下采集信息”，但未经用户许可仍采用技术手段长期保存用户各类账号和密码在自己租用的阿里云服务器上。被告人周江翔明知公司存在保存用户账户密码的行为，未尽管理职责；被告人袁冬负责编写具有保存用户账户密码功能的网关程序。截至 2019 年 9 月案发时，对魔蝎公司租用的阿里云服务器进行勘验检查，发现以明文形式非法保存的个人贷款用户各类账号和密码条数多达 21241504 条。其中大部分账号密码，如淘宝、京东等，无法二次使用，仅有邮箱等部分账号密码存在未经用户授权被魔蝎公司二次使用的情况。

2019 年 9 月 6 日下午，被告人周江翔、袁冬被抓获归案。

庭审中，被告单位魔蝎公司确认因本案犯罪，被告单位魔蝎公司的违法所得为人民币 3000 万元。审理过程中，被告单位魔蝎公司退出违法所得人民币 3000 万元。

上述事实，被告单位魔蝎公司及被告人周江翔、袁冬在开庭审理过程中亦无异议，并有证人江某 1、刘某 1、郭某、周某 1、翁某、缪某、张某 1、费某、李某 1、李某 2、潘某 1、江某 2、程某、严某、杜某、梁某、陈某、张某 2、宦某、凌某、葛某、游某、潘某 2、李某 3、张某 3、周某 2、黄某 1、郑某、沈某、刘某 2、邹某、黄某 2、刘某 3、张某 4、李某 4、王某的证言，调取证据通知书、远程勘验工作记录、杭州魔蝎数据科技有限公司工商信息、数

据采集服务协议、查封、冻结、扣押决定书及清单、杭州吸铁石科技有限公司、杭州信邦科技有限公司、杭州抖音科技有限公司的工商登记资料、银行账户交易清单、中国人民银行杭州中心支行关于魔蝎公司有关调查情况的说明、委托书、抓获经过、户籍信息、转账凭证等书证以及移动硬盘、电子证物检查工作记录、提取的电子数据等证据证实，足以认定。

本院认为，被告单位杭州魔蝎数据科技有限公司以其他方法非法获取公民个人信息，情节特别严重，其行为已构成侵犯公民个人信息罪。被告人周江翔、袁冬分别系对被告单位魔蝎公司侵犯公民个人信息行为直接负责的主管人员和其他直接责任人员，其行为均已构成侵犯公民个人信息罪。公诉机关的指控成立。被告人周江翔、袁冬自侦查阶段如实供述主要犯罪事实，自愿认罪认罚，酌情予以从宽处罚。根据被告人周江翔、袁冬的犯罪情节、悔罪表现以及没有再犯罪的危险，适用缓刑对其所居住社区没有重大不良影响，故依法对其宣告缓刑。辩护人所提相应辩护意见，本院予以采纳。公诉机关的量刑建议适当，应予采纳。据此，依照《中华人民共和国刑法》第二百五十三条之一第三款、第四款、第三十条、第三十一条、第七十二条第一、三款、第七十三条第二、三款、第五十二条、第五十三条、第六十四条以及《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》第五条、第七条、第十二条之规定，判决如下：

一、被告单位杭州魔蝎数据科技有限公司犯侵犯公民个人信息罪，判处罚金人民币 30000000 元（罚金限判决生效后十日内缴清）。

二、被告人周江翔犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑四年，并处罚金人民币 500000 元（缓刑考验期限，从判决确定之日起计算；罚金限判决生效后十日内缴清）。

三、被告人袁冬犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑三年，并处罚金人民币 300000 元（缓刑考验期限，从判决确定之日起计算；罚金限判决生效后十日内缴清）。

四、扣押于公安机关的作案工具电脑等予以没收，被告单位杭州魔蝎数据科技有限公司退缴至本院的违法所得款人民币 30000000 元予以没收，并上缴国库。

如不服本判决，可在接到判决书的第二日起十日内通过本院或直接向浙江省杭州市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本两份。

审　判　长：陈　琪

人民陪审员：王　辉

人民陪审员：秦　华

二〇二一年一月十四日

书　记　员：周栋栋

（五）诈骗罪

案例一、叶辉、朱兆崇诈骗案

广东省广州市中级人民法院

刑 事 裁 定 书

（2020）粤 01 刑终 937 号

原公诉机关广东省广州市从化区人民检察院。

上诉人(原审被告人)叶辉，男，1961 年 10 月 6 日出生，汉族，大学文化，案发前系从化维准法律咨询有限公司法定代表人，住广东省广州市从化区。因本案于 2019 年 4 月 24 日被羁押，同日被刑事拘留，同年 5 月 31 日被逮捕。于 2020 年 4 月 23 日被广州市从化区人民法院取保候审。

辩护人钟东贵，广东格林律师事务所律师。

原审被告人朱兆崇，曾用名“朱兆充”，男，1987 年 6 月 21 日出生，汉族，初中文化，

无职业，户籍地河南省南方市方城县，住广州市从化区。因本案于 2019 年 4 月 24 日被羁押，同日被刑事拘留，同年 5 月 31 日被逮捕。现羁押于广州市从化区看守所。

原审被告人赖天龙，男，1990 年 12 月 22 日出生，汉族，初中文化，户籍地广东省广州市从化区，住广东省广州市从化区。因本案于 2019 年 4 月 24 日被羁押，同日被刑事拘留，同年 5 月 31 日被逮捕。现羁押于广州市从化区看守所。

原审被告人李柏华，男，1985 年 6 月 27 日出生，汉族，初中文化，户籍地广东省广州市从化区，住广州市从化区。因本案于 2019 年 4 月 24 日被羁押，同日被刑事拘留，2019 年 5 月 31 日被逮捕。现羁押于广州市从化区看守所。

原审被告人周广文，男，1992 年 8 月 5 日出生，汉族，小学文化,户籍地广州市从化区，住广东省广州市番禺区。因本案于 2019 年 4 月 24 日被羁押，次日被刑事拘留，同年 5 月 31 日被逮捕。于 2020 年 1 月 23 日被广州市从化区人民法院取保候审。

原审被告人邓斌，男，1996 年 10 月 1 日出生，汉族，中专文化，住广东省广州市从化区。因本案于 2019 年 4 月 24 日被羁押，同日被刑事拘留，同年 5 月 31 日被逮捕。于 2020 年 1 月 23 日被广州市从化区人民法院取保候审。

广州市从化区人民法院审理广州市从化区人民检察院指控原审被告人朱兆崇、赖天龙、李柏华、叶辉、周广文、邓斌犯诈骗罪一案，于 2020 年 4 月 1 日作出（2020）粤 0117 刑初 19 号刑事判决，原审被告人叶辉不服，提出上诉。本院依法组成合议庭，经过阅卷，讯问原审被告人，听取了辩护人的意见。本案现已审理终结。

原审判决认定：2018 年至 2019 年 4 月期间，被告人朱兆崇、赖天龙、李柏华以非法牟利为目的，在广州市从化区城郊街宝城路一商铺和从城大道 584 号钱隆公馆十九号商铺从事高利放贷业务，通过被告人周广文、邓斌等人介绍和发布“贷款”广告，以无抵押、快速放款等为诱饵吸引被害人借款，以行业惯例为名骗取被害人签订虚高借款合同，并制造资金走账流水等虚假给付事实，再以“手续费”、“砍头息”等名义将部分资金收回。当被害人逾期或无力偿还时就以虚高借款合同起诉为要胁，采取电话或上门等方式向被害人及其家人索要“债务”，以及委托被告人叶辉代理以虚高借款合同向本院提起诉讼。朱兆崇主要负责出资，赖天龙负责与客户洽谈、签订借款合同、放款等，李柏华向朱兆崇、赖天龙拆借资金放贷或向朱兆崇、赖天龙介绍客户并协助催收等，周广文、邓斌负责发布广告、介绍客户、上门家访和催收，叶辉代理向法院起诉被害人，逐步形成了以朱兆崇、赖天龙、李柏华为首的，叶辉、周广文、邓斌为成员的恶势力犯罪集团，扰乱经济、社会生活秩序，造成较为恶劣的社会影响。其中：

被告人朱兆崇、赖天龙、李柏华诈骗得被害人邓某、陈某良、陈某均、卢某聪、李某子、余某健、黄某辉、邵某石、张某愉、邓某文、冯某兴、谢某娇、黄某昌、李某勇等人人民币共计 54961 元。委托被告人叶辉向法院起诉蔡某强、梁某宜、戚某添、陈某彬、张某愉、李某勇、陈某标、邝某能、徐某凡、白某伦、江某明、黄某斌、黄某发、余某斌和罗某成，诉讼标的共计人民币 238020 元，其中诈骗的虚高金额共计人民币 127716 元，因被法院驳回起诉而未得逞。

被告人周广文介绍被害人陈某良、张某愉、陈某均、徐某凡借款，诈骗金额共计人民币 14381 元。

被告人邓斌介绍被害蔡某强、黄某辉、邓某文借款，诈骗金额共计人民币 10710 元。

2019 年 4 月 24 日，朱兆崇、赖天龙、李柏华、叶辉、周广文、邓斌被公安机关抓获。

原审判决根据原公诉机关提供的移送函、附件情况报告、案件材料、系列案件清单，商铺租赁合同复印件，银行流水清单，微信、支付宝交易记录，搜查笔录、扣押决定书、扣押清单，现场勘查检查工作记录、平面示意图、现场方位图及现场照片，财富调查表、冻结财产通知书，视听资料、电子数据，手机电子数据检查工作记录，被害人黄某辉、陈某、邵某

石、邝某能、张某愉、陈某标、陈某彬、邓某文、冯某兴、谢某娇、黄某昌、蔡某强、陈某良、梁某宜、黄某发、卢某聪、李某子、余某健、李某勇的陈述及相关的辨认、签认、指认笔录，证人梁某英、陈某文、邓某葵、邓某洪、洪某花、娄某然、凌某桃、邝某葵的证言及相关的辨认、指认笔录，被告人朱兆崇、赖天龙、李柏华、叶辉、邓斌、周广文的供述及相关的辨认、指认笔录、户籍材料，抓获经过等证据作为认定上述事实的依据。

原判据此认为，被告人朱兆崇、赖天龙、李柏华、叶辉、周广文、邓斌以非法占有为目的，实施“套路贷”，采取隐瞒真相提起诉讼等方式骗取他人财物，其中被告人朱兆崇、赖天龙、李柏华、叶辉诈骗数额巨大；被告人周广文、邓斌诈骗数额较大，其行为均已构成诈骗罪。朱兆崇、赖天龙、李柏华作为恶势力犯罪集团的首要分子，应按照集团所犯的全部罪行承担责任；叶辉、周广文、邓斌是从犯，应当从轻处罚；朱兆崇、赖天龙、李柏华、周广文、邓斌归案后如实供述自己的罪行且认罪认罚，依法从轻处罚；朱兆崇、赖天龙、李柏华、叶辉的部分罪行是犯罪未遂，该部分诈骗数额可以比照既遂犯从轻处罚。依照《中华人民共和国刑法》第二百六十六条、第六十七条第三款、第二十三条、第二十六条、第二十七条、第五十二条、第五十三条、第六十四条之规定，判决如下：一、被告人朱兆崇犯诈骗罪，判处有期徒刑一年六个月，并处罚金 5000 元。二、被告人赖天龙犯诈骗罪，判处有期徒刑一年六个月，并处罚金 5000 元。三、被告人李柏华犯诈骗罪，判处有期徒刑一年三个月，并处罚金 5000 元。四、被告人叶辉犯诈骗罪，判处有期徒刑一年，并处罚金 2000 元。五、被告人周广文犯诈骗罪，判处有期徒刑九个月，并处罚金 1000 元。六、被告人邓斌犯诈骗罪，判处有期徒刑九个月，并处罚金 1000 元。七、责令被告人朱兆崇、赖天龙、李柏华、周广文、邓斌于本判决发生法律效力之次日起十日内退赔被害人陈某良等 54961 元，其中：被告人朱兆崇、赖天龙、李柏华、周广文共同退赔被害人陈某良 13040 元、张欣愉 201 元、陈榕均 1140 元；被告人朱兆崇、赖天龙、李柏华、邓斌共同退赔被害人黄某辉 3960 元、邓焕文 6750 元；被告人朱兆崇、赖天龙、李柏华共同退赔被害人邓斌 2100 元、卢浩聪 1000 元、李慧子 3500 元、余伟健 2400 元、邵宇石 9720 元、冯建兴 3750 元、谢伙娇 5000 元、黄宇昌 1000 元、李梓勇 1400 元。八、扣押的作案工具贷款广告纸 2 箱，被告人朱兆崇的金色华为手机一台、金色 iPhone 手机一台、黑色 1+手机一台，被告人赖天龙的华为 P10 手机一台、360 牌 1713-A01 手机一台，被告人李柏华的黑色天语牌手机一台、黑色魅族 V8 手机一台，被告人叶辉的白色华为手机一台，被告人周广文的黑色小米手机一台、白色小米手机一台，被告人邓斌的黑色 iPhone7Plus 手机一台，依法予以没收，由广州市公安局从化区分局执行。九、本案冻结的被告人朱兆崇、赖天龙银行账户内的资金依法予以追缴，追缴后退赔相应被害人，退赔完成后依法予以解除冻结，由广州市公安局从化区分局执行。

上诉人叶辉及其辩护人提出：1、叶辉事前与李柏华等人互不相识，不知道原审被告人实施“套路贷”的犯罪行为，其没有非法占有的目的，亦无诈骗的主观故意；2、叶辉客观上没有实施欺诈行为；3、叶辉作为李柏华等人的代理人，其仅根据客户提供的资料提出法律意见，没有义务对客户业务进行合法性审查；4、本案行为系发生在《最高人民法院、最高人民检察院、公安部、司法部关于办理“套路贷”刑事案件若干问题的意见》施行前，应适用从旧兼从轻的原则，视为民事纠纷解决；综上，叶辉的行为不构成犯罪。

经审理查明，原审判决认定上诉人叶辉、原审被告人朱兆崇、赖天龙、李柏华、周广文、邓斌以非法占有为目的，实施“套路贷”，采取隐瞒真相提起诉讼等方式骗取他人财物的事实清楚，证据确实、充分，本院予以确认。

对于上诉人叶辉及其辩护人提出叶辉的行为不构成犯罪的意见。经查，同案人朱兆崇、赖天龙、李柏华证实其于起诉前将向借款合同、转账等情况向叶辉作了说明，叶辉对于借款合同金额虚高的情况是知悉的；被害人梁某宜、黄某发及证人梁某英证实其与赖天龙、李柏华等人因虚高借款合同的偿还问题进行调解时，叶辉代为赖、李二人的代理人在场参与调解，

清楚知悉借款合同金额虚高的情况；叶辉亦供述其在参与两宗案件调解以及参加庭审过程中知悉其代理的案件是“套路贷”，仍出庭参加诉讼，相关证据足以证实叶辉对于赖天龙等人的“套路贷”行为是知悉的，为了获取利益，仍协助他人以虚假事实提起诉讼，其行为已构成诈骗罪的共犯，构成诈骗罪。本案案发时间为2018年至2019年4月间，犯罪行为持续至《最高人民法院、最高人民检察院、公安部、司法部关于办理“套路贷”刑事案件若干问题的意见》施行时，原判据此适用相关法律规定并认定上诉人、原审被告人行为构成诈骗罪，依法有据。上诉人叶辉及其辩护人提出叶辉的行为不构成犯罪的意见据理不足，本院不予以采纳。

本院认为，上诉人叶辉、原审被告人朱兆崇、赖天龙、李柏华、周广文、邓斌以非法占有为目的，实施“套路贷”，采取隐瞒真相提起诉讼等方式骗取他人财物的事实清楚，朱兆崇、赖天龙、李柏华、叶辉诈骗数额巨大；周广文、邓斌诈骗数额较大，其行为均已构成诈骗罪。朱兆崇、赖天龙、李柏华作为恶势力犯罪集团的首要分子，应按照集团所犯的全部罪行承担责任；叶辉、周广文、邓斌是从犯，应当从轻处罚；朱兆崇、赖天龙、李柏华、周广文、邓斌归案后如实供述自己的罪行且认罪认罚，依法从轻处罚；朱兆崇、赖天龙、李柏华、叶辉的部分罪行已经着手实行犯罪，由于意志以外的原因而未得逞，是犯罪未遂，该部分诈骗数额可以比照既遂犯从轻处罚。原判认定事实清楚，证据确实、充分，定罪准确，量刑适当，审判程序合法。依照《中华人民共和国刑事诉讼法》第二百三十六条第一款第（一）项之规定，裁定如下:

驳回上诉，维持原判。

本裁定为终审裁定。

审判长　　陈小丹

审判员　　李晓刚

审判员　　庞美娟

二〇二〇年六月十五日

书记员　　姚　琳

案例二、孟陈林、刘铸诈骗案

审理法院：　温州市瓯海区人民法院

案　　号：　（2019）浙0304刑初229号

案　　由：　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

裁判日期：　2019年06月04日

温州市瓯海区人民法院

刑事判决书

（2019）浙0304刑初229号

公诉机关浙江省温州市瓯海区人民检察院。

被告人孟陈林，男，1996年11月5日出生，汉族，贵州省毕节市人，大专文化，无业，户籍地毕节市七星关区，因本案于2018年5月23日被抓获并被刑事拘留，同年6月15日被取保候审。经本院决定于2019年4月15日被逮捕。现羁押于温州市瓯海区看守所。

辩护人孟天明，贵州威迪律师事务所律师。

被告人刘铸，男，1998年5月20日出生，汉族，贵州省毕节市人，高中文化，无业，户籍地毕节市七星关区，因本案于2018年5月23日被抓获并被刑事拘留，同年6月15日被取保候审。经本院决定于2019年4月15日被逮捕。现羁押于温州市瓯海区看守所。

辩护人龙杰、李朝胜，贵州众正律师事务所律师。

温州市瓯海区人民检察院以瓯检公诉刑诉〔2019〕174号起诉书指控被告人孟陈林、刘

铸犯诈骗罪，于2019年3月6日向本院提起公诉。本院于2019年3月8日立案并依法组成合议庭，召开庭前会议并形成庭前会议报告，公开开庭审理了本案。温州市瓯海区人民检察院指派员额检察官李翔、检察官助理温小燕出庭支持公诉，被告人孟陈林、刘铸及辩护人孟天明、龙杰、李朝胜到庭参加诉讼。现已审理终结。

公诉机关指控，被告人刘铸、孟陈林创建“BTCETH担保交易群”微信群，以对以太坊虚拟币（以下简称以太币）提供交易担保的名义发展成员，并收取担保费。2017年12月30日，被害人朱某在该微信群里发布出售以太币的信息。被告人刘铸、孟陈林合谋由被告人刘铸在微信上与被害人朱某联系并谎称以5000多元（以下币种均为人民币）每个的价格收购被害人朱某50个以太币。当日15时许，被害人朱某将50个以太币转到被告人刘铸指定的以太坊钱包后，被告人刘铸、孟陈林将被害人朱某微信拉黑随即踢出微信群，并将50个以太币占为己有。同日，被告人刘铸、孟陈林以同样的作案手法骗取安徽籍网友“夜”10个以太币。之后，被告人孟陈林将骗取的60个以太币出售套现，共计现金30余万元，后被告人刘铸、孟陈林将违法所得平分。

对于以上事实，公诉机关提供了相关证据并认为，被告人孟陈林、刘铸以非法占有为目的，结伙虚构事实骗取他人财物，数额巨大，其行为触犯了《中华人民共和国刑法》第二百六十六条，犯罪事实清楚，证据确实、充分，应当以诈骗罪追究其刑事责任，建议各判处有期徒刑四至六年并处罚金。

被告人孟陈林当庭对指控其与刘铸共同获取涉案60个以太币无异议，并称其将该60个以太币与其所有的其他虚拟货币一并转至境外平台销售（该平台存在“吞币”而显示为52个以太币）获利38万余元，现认为以太币并非财物，故其无罪。

辩护人孟天明提出，孟陈林获取涉案60个以太币后与其原有其他虚拟货币一并出售得款38万余元，且涉案60个以太币价值未经鉴定，孟陈林案发后支付的购车款由其父孟某支付（提供个人账户明细账查询单予以证明），故本案违法所得金额不清，温州市区两级检察院因此不予批准逮捕，现公诉机关没补充新事实、新证据仍以此提起公诉显属矛盾；中国人民银行等七部委于2017年9月4日发布的《关于防范代币发行融资风险的公告》（以下简称七部委公告）否定虚拟货币的货币属性及交易合法性，多地的判例也证实以太币等虚拟货币不能成为民事法律关系的客体，也不属于刑法上“公私财物”范畴，故以太币不受法律保护，本案指控诈骗罪错误，被告人应无罪。

被告人刘铸当庭对指控其与孟陈林共同获取涉案60个以太币无异议，且供认是孟陈林将该60个以太币及其他虚拟货币一并销售获利后给其汇款19万余元，现认为以太币并非财物，故其无罪。

辩护人龙杰、李朝胜认同辩护人孟天明的上述意见，且认为本案以拍照固定电子数据的取证程序不符合规定。

经审理查明，被告人刘铸、孟陈林创建“BTCETH担保交易群”微信群，以对以太币提供交易担保的名义发展成员。2017年12月30日，被害人朱某在该微信群里发布出售以太币的信息，刘铸、孟陈林经合谋后由刘铸通过微信联系朱某并谎称以每个以太币5000多元的价格收购朱某50个以太币。当日15时许，朱某将50个以太币转到刘铸指定的以太坊钱包后，刘铸、孟陈林即将朱某的微信“拉黑”并“踢出”微信群。同日，刘铸、孟陈林以同样手段获取被害人倪某（网友“夜”）10个以太币。此后，孟陈林将获取的60个以太币等虚拟货币出售套现30余万元并与刘铸予以瓜分。

上述事实，有公诉机关提交并经法庭质证、认证的下列证据予以证明：

1、被害人朱某、倪某的陈述和被告人孟陈林、刘铸的供述及微信聊天记录、手机取证分析报告、情况说明等证据，共同证实被害人朱某于2017年12月30日在“BTCETH担保交易群”微信群内发布出售以太币信息，后刘铸（微信号为×××）联系其并约定以5000多

元的单价收购50个以太币，朱某因此于当日15时许将50个以太币转到刘铸指定的以太坊钱包，后朱某的微信即被拉黑并被踢出微信群；被害人倪某于同日因同样手段被骗取10个以太币等情况。

2、被告人孟陈林、刘铸的供述及以太币交易平台流转记录及情况说明、Gate.io平台客服技术部回复邮件、虚拟货币平台交易记录、银行交易记录等证据，共同证实孟陈林、刘铸已实际获取涉案60个以太币，后将此60个以太币等虚拟货币出售套现30余万元并予以瓜分等情况。

3、证人柳某、叶某的证言，证实单个以太币在2017年12月30日前后的市场价格为5000元左右等情况。

4、扣押决定书、扣押清单，证实被告人孟陈林、刘铸被扣押的物品情况。

5、抓获经过及情况说明，证实被告人孟陈林、刘铸被抓获的经过情况。

6、身份情况，证实被告人孟陈林、刘铸等人的身份情况。

辩护人孟天明提供的个人账户明细账查询单证实孟某（孟陈林的父亲）于2018年1月15日在贵州毕节农村商业银行生机支行支取16万元的情况与本案事实缺乏关联性，不予采信。

本案中，侦查机关采取拍照方式固定电子数据等证据，且能够清晰反映相关内容，被告人孟陈林、刘铸等相关人员对此亦予认可并签名、按指印确认，此举符合收集提取电子数据的有关规定，故辩护人龙杰、李朝胜就此提出的相关意见于法无据，不予采纳。

对于被告人的辩解及辩护人的意见，本院分析评判如下：

1、关于以太币是否属于刑法保护对象的问题。

经查认为:首先，以太币作为一种特定的虚拟商品，与金钱财物等有形财产、电力燃气等无形财产存在明显差别，将其解释为刑法意义上的“公私财物”，超出了司法解释的权限，将诈骗以太币认定为诈骗罪有违罪刑法定原则，故各辩护人就此提出的相关意见予以采纳。其次，七部委公告仅否定以太币等“虚拟货币”的货币属性并禁止代币发行融资活动，并未否定私人持有以太币的合法性，也未禁止其成为私人间交付或流转的客体；我国民法总则第127条有关“法律对数据、网络虚拟财产的保护有规定的，依照其规定”等内容标志数据、网络虚拟财产正式进入民法调整和保护的范围，以太币是依据特定的算法通过大量的计算产生，实质上是动态的数据组合，其法律属性是计算机信息系统数据，依法属于刑法“非法获取计算机信息系统数据罪”所保护的对象，故各辩护人提出的以太币不能成为民事法律关系的客体、不属于我国法律所保护对象等意见于法无据，不予采纳。

2、关于被告人孟陈林、刘铸行为定性的问题。

经查认为，我国刑法规定的非法获取计算机信息系统数据罪是指非法获取他人计算机信息系统中存储、处理或者传输的数据的行为，“获取”包括从他人计算机信息系统中窃取，如直接侵入他人计算机信息系统中，秘密窃取他人存储的数据，也包括从他人计算机信息系统中骗取，如采用建立假冒网站、发送钓鱼链接等其他技术手段，在受骗者登录时，要求用户输入数据信息等；其中的“其他技术手段”是指“侵入”之外的其他犯罪手段，具有兜底性，囊括所有可采用的技术手段。本案中，被告人通过微信发出其收购以太币的虚假信息而取得被害人的信任，被害人因此将以太币转入其指定的以太坊钱包，但被告人随即通过将被害人微信拉黑并踢出微信群等手段，导致被害人无法即时对其进行追踪，该手段行为利用了微信作为即时通讯应用程序所具有的远程性、非接触性等技术特点，来实现其即能非法获取以太币又能“隐身”的目的，此效果类似于以上所述的“从他人计算机信息系统中骗取”，属于非法获取计算机信息系统数据罪的“其他技术手段”范畴。何况，我国刑法规定“一切危害国家主权、领土完整和安全，分裂国家、颠覆人民民主专政的政权和推翻社会主义制度，破坏社会秩序和经济秩序，侵犯国有财产或者劳动群众集体所有的财产，侵犯公民私人所有

的财产，侵犯公民的人身权利、民主权利和其他权利，以及其他危害社会的行为，依照法律应当受刑罚处罚的，都是犯罪”，被告人的行为明显已经侵犯其他公民权利，具有社会危害性，依法应予刑事处罚。

3、关于本案违法所得金额问题。

经查认为，本案现有证据证实涉案以太币交易单价为5000余元（符合交易行情），被告人孟陈林、刘铸供认涉案60个以太币与其他虚拟货币一并转至境外平台销售（因销售平台“吞币”而仅显示为52个以太币）即获利38万余元，结合其供述投资其他虚拟货币仅几千元、交易担保获利一次等情况，足以认定指控的30余万元主要来源于涉案的60个以太币，故本案违法所得金额明显高于2.5万元。

本院认为，被告人孟陈林、刘铸结伙采用其他技术手段，非法获取他人计算机系统中存储的数据，违法所得2.5万元以上，属于情节特别严重，其行为均已构成非法获取计算机信息系统数据罪。公诉机关指控的罪名不当，予以更正。依法唯有判决才能定罪，逮捕仅为强制措施，各辩护人以不批准逮捕即认定无罪的意见于法无据，不予采纳。被告人孟陈林、刘铸在侦查阶段如实供述自己的罪行后翻供，但当庭能够如实供述本案主要犯罪事实，其他辩解是对法律的理解认识不同，仍应认定有坦白情节，结合本案实际情况，均予从轻处罚；公诉机关的量刑建议不当，予以调整。依照《中华人民共和国刑法》第二百八十五条第二款、第二十五条第一款、第六十七条第三款、第六十四条之规定，判决如下：

一、被告人孟陈林犯非法获取计算机信息系统数据罪，判处有期徒刑三年十个月，并处罚金4万元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2019年4月15日起至2023年1月21日止；罚金限判决生效后十日内缴纳）

二、被告人刘铸犯非法获取计算机信息系统数据罪，判处有期徒刑三年十个月，并处罚金4万元。

（刑期从判决执行之日起计算。判决执行以前先行羁押的，羁押一日折抵刑期一日，即自2019年4月15日起至2023年1月21日止；罚金限判决生效后十日内缴纳）

三、责令被告人孟陈林、刘铸退赔违法所得分别返还被害人朱某、倪某。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或直接向温州市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审 判 长　毛小雨

人民陪审员　　彭国清

人民陪审员　　陈奇平

二〇一九年六月四日

代书 记员　张芳炜

（六）非法经营罪

案例一、王海洋、宁焱非法经营、洗钱案

审理法院：　淄博市张店区人民法院

案　　号：　（2019）鲁0303刑初153号

案　　由：　帮助信息网络犯罪活动罪

裁判日期：　2019年10月10日

淄博市张店区人民法院

刑事判决书

（2019）鲁0303刑初153号

公诉机关淄博市张店区人民检察院。

被告人王海洋，男，1980 年 1 月 2 日出生于江苏省泰州市，汉族，博士研究生文化，个体，户籍所在地广东省深圳市罗湖区，住广东省佛山市顺德区。因涉嫌犯帮助信息网络犯罪活动罪于 2018 年 4 月 20 日被淄博市公安局刑事拘留，2018 年 5 月 23 日经淄博市人民检察院批准并于同日被淄博市公安局执行逮捕。现羁押于淄博市看守所。

辩护人王承敏，山东般阳律师事务所律师。

辩护人张梅，山东长城长律师事务所律师。

被告人宁焱，女，1981 年 8 月 4 日出生于黑龙江省肇东市，满族，大学文化，无业，户籍所在地及住均为广东省佛山市顺德区。因涉嫌犯帮助信息网络犯罪活动罪于 2018 年 4 月 21 日被淄博市公安局刑事拘留，因涉嫌犯帮助信息网络犯罪活动罪于 2018 年 5 月 23 日被淄博市公安局取保候审。

辩护人周彦民，辽宁书源律师事务所律师。

淄博市张店区人民检察院以张检公刑诉（2019）124 号起诉书指控被告人王海洋犯非法经营罪、帮助信息网络犯罪活动罪、洗钱罪，指控被告人宁焱犯非法经营罪、帮助信息网络犯罪活动罪，于 2019 年 2 月 18 日向本院提起公诉。本院于同日立案。本院依法组成合议庭，公开开庭审理了本案。淄博市张店区人民检察院指派检察员王研出庭支持公诉，被告人王海洋及其辩护人王承敏、张梅、被告人宁焱及其辩护人周彦敏到庭参加诉讼。现已审理终结。

淄博市张店区人民检察院指控，2016 年 10 月至 2018 年 4 月，被告人王海洋、宁焱等人未经批准，未取得《支付业务许可证》的情况下，搭建 SPA 第四方支付平台，为商户提供人民币和外汇的资金结算服务，从中赚取手续费，共计非法结算资金人民币 1103788527.92 元。其中，被告人王海洋、宁焱在明知“12BET”、“大发”、“沙某”等网站为赌博网站的情况下，购买伪造的公司印章 38 枚，为赌博网站伪造公司营业执照、开户许可证明等资料，用上述资料在“天下支付”、“易某支付”等第三方支付平台开通商户号，获取资金支付结算通道，为赌博网站提供支付结算等服务。

公诉机关认为被告人王海洋的行为构成非法经营罪、帮助信息网络犯罪活动罪、洗钱罪，被告人宁焱的行为构成非法经营罪、帮助信息网络犯罪活动罪，并向本院提供了相关证据，请求本院依照《中华人民共和国刑法》第二百二十五条、第二百八十七条之二、第一百九十一条的规定，追究被告人王海洋、宁焱的刑事责任。

被告人王海洋对公诉机关的指控有异议，其辩解称自己对公诉机关指控的事实无异议，对帮助信息网络犯罪活动罪的罪名无异议，但对公诉机关指控自己犯有非法经营罪、洗钱罪，自己认为不构成非法经营罪、洗钱罪。

被告人王海洋的辩护人王承敏的辩护意见是，一、被告人王海洋的行为不属于刑法 191 条的情形，被告人王海洋不构成洗钱罪。二、被告人王海洋的行为的表现形式不符合非法经营罪的构成要件，被告人王海洋不构成非法经营罪。三、公诉机关指控被告人王海洋犯帮助信息网络犯罪活动罪，证据不足。

被告人王海洋的辩护人张梅的辩护意见是，一、公诉机关指控被告人王海洋犯洗钱罪事实不清、证据不足，被告人王海洋不构成洗钱罪。二、被告人王海洋不构成非法经营罪。三、被告人王海洋、宁焱提供线索，公安机关破获了“小罗”等人伪造公司印章案件，王海洋应认定自首。

被告人宁焱对公诉机关的指控有异议，其辩解称自己只是辅助王海洋，在他忙的时候帮一下忙，自己主要负责经营自己的保健店和照顾孩子。

被告人宁焱的辩护人周彦民的辩护意见是，被告人所搭建的 SPA 第四方支付平台，实际上该平台并不提供结算业务，只是为商户、客户利用第三方平台进行结算提供了支付渠道，被告人从事了一种行为，属于想象竞合犯，应择一重罪处罚，被告人宁焱不构成两项罪名，应以帮助信息网络犯罪活动罪定罪处罚。被告人宁焱在共同犯罪中系从犯，可从轻或免除处

罚。

经审理查明，2016 年 10 月至 2018 年 4 月，被告人王海洋、宁焱等人未经批准，搭建 SPA 第四方支付平台，为商户提供人民币和外汇的资金结算服务，从中赚取手续费，共计结算资金人民币 1103788527.92 元。其中，被告人王海洋、宁焱在明知“12BET”、“大发”、“沙某”等网站为赌博网站的情况下，购买伪造的公司印章 38 枚，为赌博网站伪造公司营业执照、开户许可证明等资料，用上述资料在“天下支付”、“易某支付”等第三方支付平台开通商户号，获取资金支付结算通道，为赌博网站提供支付结算等服务。

诉讼中，被告人王海洋、宁焱已退赔违法所得 400000 元。

上述事实，被告人王海洋、宁焱在开庭审理过程中对公诉机关指控的事实无异议，且有受案登记表、发破案经过、抓获经过、办案说明、电子数据检验工作记录、远程勘验工作记录、银行账户交易资料、搜查笔录、扣押决定书及扣押清单、企业信息资料、中国人民银行淄博市中心支行复函、结算业务委托书、证人黄某、毕某、刘某、苏某、樊致礼证言、视听资料、被告人王海洋、宁焱的供述及身份资料等证据为证，足以认定。

本院认为，被告人王海洋、宁焱明知他人利用信息网络实施犯罪，为其提供支付结算等帮助，情节严重，其行为均构成帮助信息网络犯罪活动罪。公诉机关指控被告人王海洋、宁焱犯帮助信息网络犯罪活动罪的事实及罪名成立。

关于公诉机关指控被告人王海洋、宁焱犯非法经营罪、指控被告人王海洋犯洗钱罪，事实不清，证据不足。本院不予支持。采纳被告人及其辩护人对此的相关辩解辩护意见。

被告人王海洋在共同犯罪中起主要作用，系主犯。被告人宁焱在共同犯罪中起次要辅助作用，系从犯，应对其减轻处罚。采纳被告人及其辩护人对此的相关辩解辩护意见。据此，依照《中华人民共和国刑法》第二百八十七条之二第一款、第二十五条第一款、第二十六条第一、四款、第二十七条第一、二款、第六十一条、第七十二条第一款、第七十三条第二、三款、第五十二条、第五十三条之规定，判决如下：

一、被告人王海洋犯帮助信息网络犯罪活动罪，判处其有期徒刑一年六个月，并处罚金人民币 10000 元。

（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押一日折抵刑期一日。即自 2018 年 4 月 20 日起至 2019 年 10 月 19 日止。罚金限判决生效后一个月内缴纳。）

二、被告人宁焱犯帮助信息网络犯罪活动罪，单处罚金人民币 10000 元。（限判决生效后一个月内缴纳。）

三、没收被告人王海洋、宁焱违法所得 400000 元，上交国库。

四、继续追缴被告人王海洋、宁焱违法所得，上交国库。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或直接向山东省淄博市中级人民法院提出上诉。书面上诉的，应当提交上诉状正本一份，副本二份。

审判长　崔洪栋

人民陪审员　李秀芹

人民陪审员　程玉华

二〇一九年十月十日

书记员　李　雪

案例二、卫王磊非法经营案

审理法院：　河北省保定市中级人民法院

案　　号：　（2019）冀 06 刑终 309 号

案　　由：　非法经营罪

裁判日期：　2019 年 04 月 17 日

河北省保定市中级人民法院

刑事裁定书

（2019）冀06刑终309号

原公诉机关河北省高碑店市人民检察院。

上诉人（原审被告人）卫王磊，男，1983年2月6日出生，汉族，高中文化，个体，户籍地山西省永济市，捕前住河北省高碑店市。2016年9月9日因涉嫌犯侵犯著作权罪被保定市公安局白沟·白洋淀温泉城分局刑事拘留，同年10月15日被取保候审，2018年5月8日因涉嫌犯非法经营罪被刑事拘留，同年5月22日被逮捕。现押于高碑店市看守所。

河北省高碑店市人民法院审理河北省高碑店市人民检察院指控原审被告人卫王磊犯非法经营罪一案，于2018年12月20日作出（2018）冀0684刑初332号刑事判决。原审被告人卫王磊不服，提出上诉。本院受理后，依法组成合议庭，经过阅卷，讯问上诉人，认为事实清楚，决定不开庭审理。现已审理终结。

原判决认定，《火影忍者ONLINE》是经新闻出版广电总局批准引进，由深圳市腾讯计算机系统有限公司运营的网络游戏出版物。2015年5月份开始，被告人卫王磊未经授权或许可，研发出《火影忍者OL辅助（脱机版）》外挂软件，在淘宝网上进行非法发行销售，至2016年9月份，被告人卫王磊通过淘宝网络方式经营上述外挂软件金额达人民币269760元。

上述事实，有公诉机关提交并经法庭质证的下列证据予以证实：

1.受理案件登记表、立案决定书，证实2016年9月9日保定市公安局白沟·白洋淀温泉城分局接深圳市腾讯计算机系统有限公司报案称，发现互联网上有人提供针对《火影忍者OL》的外挂软件，破坏游戏平衡。2016年9月9日对该侵犯著作权案立案侦查。

2.深圳市腾讯计算机系统有限公司报案书，证实《火影忍者OL》是该公司运营的网络游戏，该公司发现自2015年出现火影忍者OL辅助（脱机版）游戏外挂，链接为https://item.taobao.com/item.htm?id=45050138257,网店名称是火影0L辅助，店主叫edisonpang2009)，该外挂软件通过分析破解《火影忍者OL》的通信协议，跳过《火影忍者OL》客户端，实现了自动打怪、自动做任务等客户端手动功能，目前使用外挂玩家达数千人，获利数额巨大，严重侵犯了该公司的权益。

3.证人毛某证言，证实内容和报案书内容基本一致，该公司是2016年5月份发现外挂存在，外挂出现时间大概是2015年，具体时间无法确定。

4.《火影忍者OL》的著作权登记证书、深圳市腾讯计算机系统有限公司运营该游戏的授权书。

5.中国版权保护中心版权鉴定委员会关于《火影忍者OL》游戏软件与《火影忍者OL（脱机版）》软件关联性检验鉴定报告、《火影忍者OL（脱机版）》软件是否为外挂软件的认定及出具上述报告的人员说明、资质证明，证实从https://item.taobao.com/item.htm.htm?id=45050138257账号购买下载的《火影忍者OL（脱机版）》软件正常运行时，通过修改《火影忍者OL》游戏软件的运行程序，可以改变《火影忍者OL》游戏软件的运行过程、结果。该软件未取得深圳市腾讯计算机系统有限公司授权的情况下，属于外挂软件。

6.扣押决定书、扣押物品清单，证实2016年9月9日从被告人卫王磊处扣押台式电脑主机一台。

7.福建中证司法鉴定中心司法鉴定意见书，证实对上述扣押电脑硬盘中“houying\"\"huoyingfuzhu\"源代码工程进行功能性鉴定，鉴定意见为，送检硬盘”E/myproject/huoying\"目录下的“HuoYingFuZhu.dpr\"源代码工程具有以下功能：通过向《火影忍者online》游戏服务器发送数据方式实现自动签到、自动免费招财猫、自动刷野、自动

护送、刷竞技场等功能。送检硬盘 E/myproject/huoyingfuzhu”目录下的“HuoYingFuZhu.dpr\"源代码工程具有以下功能：通过向《火影忍者 online》游戏服务器发送数据的方式实现自动答题、自动更换忍者、自动扫荡、自动兑换、自动购买物品等功能。

8.被告人卫王磊农业银行账号、庞某工商银行账号交易明细（2015 年至 2017 年），证实被告人卫王磊及其妻子庞某的银行卡交易情况。与支付宝账号交易相关。

9.支付宝(中国）网络技术有限公司关于被告人卫王磊及庞某的支付宝交易记录（附光盘），证实本案的交易金额总计 269760 元。

10.被告人卫王磊供述，供认其玩《火影忍者 OL》感觉到手动操作比较累，就开始琢磨研发一个全自动的辅助器，最早是 2015 年 5 月开始研发这款软件的，2015 年 6 月开始可以正常使用，用这款软件在游戏里挂机可以实现游戏的自动打怪、自动做任务，不用人为操作。其通过淘宝出售研发出的软件，以每个月 30 元、二个月 50 元、三个月 70 元的价格出售，网店是用妻子庞某的身份证注册的，网店名称是“火影忍者 OL 辅助”，店主名是“edisonpang2009”，淘宝店绑定了一个支付宝，支付宝账号也是“edisonpang2009”。支付宝绑定了一张工商银行的卡，账号也是用庞某的身份证办理的。其研发辅助软件用是自己的组装电脑，存放在电脑 E 盘“myproject/huoying\"文件夹和“huoyingfuzhu"文件夹内。网上下载地址是 www.921hy.com。其通过淘宝成交软件大约 3000 笔，交易金额 18 万左右，这些钱通过支付宝绑定的银行卡提现后保障家庭消费用了。

11.证人庞某证言，证实其是卫王磊的妻子，2015 年 5 月卫王磊开始在淘宝上出售“火影忍者”游戏的辅助软件，这款软件能实现自动挂机、自动打怪等功能。关于出售软件的价格、淘宝店的情况、支付宝等情况与被告人卫王磊供述一致，卫王磊通过出售软件挣了大概 10 多万块钱。

12.被告人卫王磊的身份证复印件。

13.抓获证明，证实 2016 年 9 月 9 日保定市公安局白沟•白洋淀温泉城分局民警在白沟镇水晶域小区 2 号楼 1 单元 702 室将卫王磊抓获。

14.被告人卫王磊无违法犯罪前科证明。

原审法院认为，被告人卫王磊违反国家规定，利用互联网站出版发行非法出版物，严重危害社会秩序和扰乱市场秩序，犯罪情节特别严重，其行为构成非法经营罪。被告人卫王磊提出的无罪意见与查明的事实不符，不予采信。依照《中华人民共和国刑法》第二百二十五条第（四）项、第五十二条、第五十三条，《最高人民法院关于审理非法出版物刑事案件具体应用法律若干问题的解释》第十一条、第十二条的规定，认定被告人卫王磊犯非法经营罪，判处有期徒刑五年，并处罚金人民币五万元。

上诉人卫王磊上诉提出，其未经著作权人许可，复制原版通信协议及数据发行计算机软件作品，只是对原版进行复制、修改，对社会秩序不产生影响，其行为属侵犯著作权，不构成非法经营罪。综上，要求依法判处。

经审理查明，原判决认定自 2015 年 5 月上诉人卫王磊未经授权或许可，研发出《火影忍者 OL 辅助（脱机版）》外挂软件，在淘宝网上发行销售，至 2016 年 9 月非法经营数额共计人民币 269760 元的事实清楚，证据充分，据以定案的证据均经原审法院庭审质证，本院予以确认。

本院认为，上诉人卫王磊违反国家规定，利用互联网站出版发行非法出版物，扰乱市场秩序，情节特别严重的行为构成非法经营罪。上诉人卫王磊未经授权或许可，研发出《火影忍者 OL 辅助（脱机版）》软件，在淘宝网上出售并谋利，该软件经中国版权保护中心认定可以改变《火影忍者 ONLINE》游戏软件的运行过程、结果，属于外挂软件，外挂等违法行为属于非法互联网出版活动，且经营数额达到人民币 269760 元，扰乱了市场秩序，情节特别严重，上诉人卫王磊的行为构成非法经营罪，上诉人卫王磊称其不构成非法经营罪的上诉

意见与查明事实不符，不予采纳。综上，原判定性准确，适用法律正确，审判程序合法，量刑在法定幅度之内，并无不当。依据《中华人民共和国刑事诉讼法》第二百三十六条第一款第（一）项、第二百四十四条之规定，裁定如下：

驳回上诉，维持原判。

本裁定为终审裁定。

审判长　田银娇

审判员　齐金谦

审判员　张彦林

二〇一九年四月十七日

书记员　刘 曼

案例三、李某某非法经营案

审理法院：　杭州市余杭区人民法院

案　　号：　（2016）浙 0110 刑初 726 号

案　　由：　非法经营罪

裁判日期：　2017 年 06 月 01 日

杭州市余杭区人民法院

刑事判决书

（2016）浙 0110 刑初 726 号

公诉机关浙江省杭州市余杭区人民检察院。

被告人李某某，男，住江苏省盐城市滨海县。因本案于 2015 年 5 月 19 日被取保候审，2017 年 6 月 9 日被逮捕。现押于杭州市余杭区看守所。

辩护人汪振阳，浙江泽厚律师事务所律师。

杭州市余杭区人民检察院以杭余检未检刑诉[2016]392 号起诉书指控被告人李某某犯非法经营罪，于 2016 年 6 月 20 日向本院提起公诉。本院依法适用普通程序，二次公开开庭审理了本案。杭州市余杭区人民检察院指派检察员徐芬出庭支持公诉。被告人李某某及其辩护人汪振阳到庭参加诉讼。其间，经上一级人民法院批准，延长审理期限三个月，且由于不能抗拒的原因致使本案在较长时间内无法继续审理，本院于 2016 年 12 月 1 日裁定对本案中止审理，后因被告人李某某被抓获归案，本院于 2017 年 6 月 9 日裁定对本案恢复审理。现已审理终结。

杭州市余杭区人民检察院指控：2013 年 2 月，被告人李某某通过创建“零距网商联盟”http：//www.5sbb.com 网站和利用 YY 语音聊天工具建立刷单炒信平台，吸纳淘宝卖家注册账户成为会员，并收取 300-500 元不等的会员费和 40 元的平台管理维护费。被告人李某某通过制定刷单炒信规则与流程，组织及协助会员通过该平台发布或接受刷单炒信任务。会员在承接任务后，通过与发布任务的会员在淘宝网上进行虚假交易并给予虚假好评的方式，赚取任务点，从而有能力在该平台自行发布刷单任务，使得其他会员为自己刷单，进而提升自己淘宝店铺的销量和信誉，欺骗淘宝买家。期间，被告人李某某通过向会员销售任务点的方式谋利。截至 2014 年 6 月，被告人李某某共计获利 90 余万元人民币。经查询，由江苏省通信管理局回函，http：//www.5sbb.com 网站不具备获得增值电信业务经营许可的条件。

据以指控的证据有证人证言、户籍证明等书证、支付宝信息数据、光盘、搜查笔录、被告人的供述和辩解等。公诉机关认为，被告人李某某的行为已构非法经营罪，情节特别严重，提请本院依照《中华人民共和国刑法》第二百二十五条之规定惩处。

被告人李某某辩称，1）其是 2013 年农历过完年后加入“迅爆军团”的，入会后二、三个月成为一般管理员，2013 年夏天才成为高级管理员并将平台改名为“零距网商联盟”，

其没有组织会员刷单，刷单仅是违规行为；2）支付宝记录中备注为“买点”的部分钱款并非是会员向其直接买点，而是通过其向客服人员购买客服通过刷单积累的任务点，其自己直接卖点的钱款数额在1万元左右；3）如果其的行为构成犯罪，请求对其减轻处罚。

辩护人同意被告人李某某的第1）点辩解，另提出，1）不能简单地将《互联网信息服务管理办法》中关于“是否具有经营性互联网服务资格”的规定等同于“国家规定”，被告人李某某收取网站维护费和保证金是一种代为保管的行为，并不违法，且会员是自愿交纳相关费用的，被告人李某某并无非法占有的故意，亦不能因此认为本案所涉网站系经营性网站，且炒信行为涉及的虚假信息发布在淘宝网上，与本案所涉网站没有直接关系，在平台发布任务点并非发布虚假信息，故被告人李某某的行为不属于法律明确规定的构成非法经营犯罪的情形；2）即使网站因没有经营性互联网服务许可而经营需要被查处的，亦应属于江苏省通信管理局、工商行政等部门监管的范畴，不属于刑法调整的范围；3）刷单炒信扰乱的仅为淘宝网的排名秩序，而非市场秩序；4）被告人李某某仅代收会员费444000元，维护费44400元，未达情节严重标准；5）如果被告人李某某的行为构成非法经营罪，则被告人李某某系初犯，接电话通知后到案，系自首，并且主动退出平台，系犯罪中止，其检举他人犯罪，具有从轻或减轻处罚的情节，请求对被告人李某某免予刑事处罚或单处罚金。

经审理查明：

被告人李某某通过创建“零距网商联盟”（前身为“迅爆军团”）http：//www.5sbb.com”网站和利用YY语音聊天工具建立刷单炒信平台，吸纳淘宝卖家注册账户成为会员，并收取300元至500元不等的保证金和40元至50元的平台管理维护费及体验费，并通过制定刷单炒信规则与流程，组织会员通过该平台发布或接受刷单炒信任务。会员在承接任务后，通过与发布任务的会员在淘宝网上进行虚假交易并给予虚假好评的方式赚取任务点，使自己能够采用悬赏任务点的方式吸引其他会员为自己刷单炒信，进而提升自己淘宝店铺的销量和信誉，欺骗淘宝买家。其间，被告人李某某还通过向会员销售任务点的方式牟利。从2013年2月至2014年6月，被告人李某某共收取平台管理维护费、体验费及任务点销售收入至少人民币30万元，另收取保证金共计人民币50余万元。

另查明，http：//www.5sbb.com网站不具备获得增值电信业务经营许可的条件。

再查明，被告人李某某归案后检举他人犯罪，但无法查证属实。

又查明，被告人李某某因涉嫌侵犯公民个人信息于2016年9月10日被江西省宜春市公安局刑事拘留，同年9月30日被逮捕，2017年5月16日，江西省宜春市袁州区人民法院作出（2017）赣0902刑初136号刑事判决书，以被告人李某某犯侵犯公民个人信息罪，判处其有期徒刑九个月，并处罚金人民币二万元（刑期自2016年9月10日起至2017年6月9日止），所判罚金人民币二万元，被告人李某某已缴纳。

证明以上事实并经庭审质证的证据有：

1、证人王某1（系浙江淘宝网络有限公司安全专员）的证言、关于“零距网商联盟”炒信平台的情况报告，证实2014年4月，浙江淘宝网络有限公司在处理会员举报并结合网上查巡时发现“零距网商联盟”（http：//www.5sbb.com）系信用炒作平台，该平台通过广告、拉人等形式吸收淘宝卖家为会员，淘宝卖家需向“零距网商联盟”的控制人被告人李某某掌控的支付宝或财付通账户缴纳一定金额的钱款，通过简单培训和考试后成为正式会员，会员通过该平台接受和发布虚假交易任务，互相炒作实现信用等级或销量的提升；平台通过收取会员费和管理费、出售任务点、帮助他人提升信用等级、代会员进行空包虚假销售等方式获取利益，据了解，“零距网商联盟”已有1500余名会员，通过相关支付宝账户收入74万余元，以及“零距网商联盟”原名“迅爆军团”，成立于2011年左右，最早为游戏平台，在江苏备案，租用阿里云服务器的事实；

2、证人李某1的证言，证实其于2013年2月成为“零距网商联盟”的管理人员，YY

昵称为“小辰”，并按照该平台负责人和控制人被告人李某某的要求负责审核新加入会员的身份，具体为要求新会员（均为淘宝卖家）提供手持身份证的照片及淘宝店铺截图，其根据对方提供的信息确认店铺的真实性后即可审核通过；据其统计，“零距网商联盟”先后有会员2010名（其中部分已退会），至案发时，在册会员为1500名左右；会员通过该平台进行虚假交易炒作店铺信誉，以获得更好的销售位置、评价即炒信，具体过程为平台接待人员通过YY聊天，告诉对方如何炒作店铺信誉，淘宝卖家理解流程之后会在平台上发布任务点，其他会员接任务后通过YY聊天确定炒信的商品，根据事先约定，通过阿里旺旺聊天，并讨价还价（以达到欺骗淘宝监控的目的），后接受任务的会员通过支付宝付款，卖家通过物流邮寄空包，再通过财付通将收到的货款还给接受任务的会员，对方收到包裹后对商品进行好评；其也参与炒信，被告人李某某每月会给其100-200个任务点，以及其提供的“零距网商联盟”会员清单、平台流程、每月会员等级明细等资料均为真实材料的事实；

3、证人肖某的证言，证实其应被告人李某某之邀于2014年3月到“零距网商联盟”YY频道做娱乐主持，YY的ID为柠檬，4月初开始处理会员投诉，5月调至外宣部；“零距网商联盟”系炒信平台，通过网上宣传或会员间介绍招募会员，入会需缴纳押金500元及40元会员费，其中押金可退；会员必须使用任务点才能发布任务，任务点可通过接任务取得，部分会员也可从平台购买，每个点价格在5-6元；炒信的具体流程为会员在平台发布任务（内容包括商品价格、链接、任务完成获得点数和YY频道里面的ID），其他会员接任务后与发布者进行沟通，协商一致后双方通过阿里旺旺进行虚假的交易聊天（为了使虚假交易从表面上看是正常交易以避开淘宝公司的监控），后接受任务方在淘宝网上购买商品，发任务方则通过财付通将相同金额回款给接任务方，同时通过快递公司发空包给接任务方，将快递单号填写到淘宝交易流程里完成交易，接任务方接到空包后确认付款并对商品给予好评，之后即可得到发任务方悬赏的任务点的90%，平台则抽取10%的任务点，以及被告人李某某为“零距网商联盟”的建立者和管理者，平台所有收入都打入被告人李某某的支付宝和财付通账户，2014年3、4月，被告人李某某与其约定每月给其工资3000元，后曾向其打款3000元和5000元的事实；

4、证人张某1的证言，证实其于2013年7月左右开始担任炒信平台“零距网商联盟”的管理员，负责协调处理炒信双方的纠纷，被告人李某某为该平台的创始人及老板，该平台的前身为因违规操作被关闭的“迅爆军团”，被告人李某某在“迅爆军团”被关闭后一周左右即重新组建了“零距网商联盟”，淘宝卖家须通过支付宝、财付通等途径缴纳500元会员费（根据平台规则，理论上会员费可退，但需完成规则内的条款，客观上退会员费较为困难）及每年40元的平台维护费至被告人李某某的个人账户后才能注册成会员，之后才可以查看其他会员发布在平台上的帖子，如有炒信的需要，双方在平台上交流再通过淘宝网进行虚假交易，刷单后即可以从任务发布者处获得相应的任务点用于自行发布虚假交易任务，任务点可以买卖和转让，每个任务点价格为3-6元，管理员的报酬也通过发放任务点的方式支付，平台还提供发空包快递的业务，以及平台共有会员2000余名，平时在线的有1000余名的事实；

5、证人王某2的证言，证实其与李某1一起成为炒信平台“零距网商联盟”的会员（其的YY语音昵称为“空空”，网站昵称为“无赖”），该平台负责人为被告人李某某，网站建设是被告人李某某找程序员制作的；成为平台会员需向管理员提供淘宝店铺名称及个人身份证，并向被告人李某某控制的支付宝或财付通账户缴纳500元押金及40元网站服务费；成为会员后即可请求其他会员帮忙刷信用评级，具体流程为先在网站上发帖公告，悬赏任务点，有兴趣的会员接任务后通过YY语音软件等与发单者沟通，之后双方就货物情况通过阿里旺旺进行虚假聊天，接单者购买发单者的商品并通过支付宝支付货款，发单者再通过物流发空包，并将货款通过财付通回款至接单者账户同时支付悬赏的任务点，但接单者只能获得

悬赏任务点的90%，另外10%由平台收取用于支付管理人员报酬等，任务点只能在网站内部流转，且总量受到控制，会员还可以通过介绍新人或者向被告人李某某收购的方式获得任务点；按照平台规定，会员须长时间上线，每周须刷单15-20个，据其所知，每天长时间上线的会员有1000余人，其中内部管理人员20-30人，其表哥李某1从2013年下半年开始负责做新人的背景资料收集工作，其于2014年5月25日左右受被告人李某某的委托担任H组组长，负责监督本组会员按照网站要求进行操作，及时上线及按量接单，完成任务，被告人李某某给其和李某1的报酬为各100余个任务点的事实；

6、证人张某2的证言，证实其于2013年7月左右通过YY语音软件认识YY昵称为“零零”的被告人李某某，后其加入了创始人为被告人李某某的炒信平台“零距网商联盟”，该平台通过发布广告等方式招揽欲刷信誉的淘宝卖家成为会员，会员入会前需缴纳540元入会费至被告人李某某的账户，在由被告人李某某对会员进行分组，同时通过平台上的教育模块对会员进行刷信誉的教学，通过培训后，会员通过帮其他会员炒信的方式获得任务点用于悬赏发布自己的炒信公告，招揽其他会员炒信以提高自己店铺的信誉及销量等，同时会员每天需完成一定量的任务，否则管理员会对会员进行扣点；炒信的具体流程为会员发布悬赏公告后，接任务者与发任务者通过阿里旺旺进行虚假聊天，之后拍下物品并通过支付宝支付“货款”，“卖家”则以空邮包的方式发货，并在“买家”确认收货后将“货款”还给“买家”，每笔虚假交易完成后，会员可获得1个任务点用于发布悬赏公告；平台共有会员1000余人，其中管理人员10余人，被告人李某某负责团队的管理、整个平台的运行、给会员加点、扣点等，被告人李某某没空时也会让管理员帮忙加点、扣点，其曾登录管理员账户并按照被告人李某某给予的名单帮被告人李某某操作扣点1、2次，被告人李某某还有创建点数的权限，以及被告人李某某通过收取入会费获利，管理员则接受被告人李某某发放的任务点作为报酬的事实；

7、证人方某1、陈某1、翟某、汤某1、汤某2、徐某1、徐某2、顾某1、陈某2、赵某1、沈某1、陈某3、陈某4、沈某3、陈某5、李某2、邱某1、石某、王某3、范某1、柯某、施某1、赵某2、王某4、蔡某1、钟某2、冯某1、徐某3、许某、吴某、荆某，杜某1、娄某、商某、李某3、姚某、敖某，陈某6、宋某1、贺某、车某，金某、项某、潘某，4、鲍某2、夏某、蔡某2、施某2、李某4、陈某7、李某5、洪某、谢某、梁某、程某1、杨某、杜某2、范某2、张某3、周某、卓某、罗某1、尹某、顾某2、王某5、罗某2、蒋某、陈某8、王某8、高某1、张某4、冯某2、刘某1、赖某、刘某2、李某6、林某1、邱某2、陈某9、李某7、余某、钟某1、程某2、童某、华某、王某6、林某2、左某、方某2、方某3、冯某3、盛某，4、刘某3、李某8、陈某10、叶某、宋某3、刘某4、陈某1鲍某1、张某5等人的证言、个人成员资料、支付宝交易记录，证实上述人员均通过朋友介绍、百度搜索、广告等方式得知炒信平台“零距网商联盟”（该平台曾用名为迅爆军团），并向平台提供的账户（包括李某某、王某7的支付宝账户及财付通账户）支付相应的钱款（其中部分证人称支付了50元体验费，部分证人称支付了340元保证金，部分证人称支付了300元保证金及40元管理费，部分证人称支付400元保证金，部分证人称支付了500元保证金，部分证人称支付了500元保证金及40元管理费，部分证人称支付了500元保证金及50元管理费）后成为平台会员，按照规定，会员需要接受炒信操作的培训并经过考核后才可以正式接受刷单任务，但在培训期间给其他会员刷单不能获得任务点；刷单的具体流程是在平台寻找合适的任务后联系需要刷单方，对方会提供需刷单商品的链接等信息，接任务方在淘宝网上找到需要刷单商品后用阿里旺旺与对方进行虚假聊天，之后拍下商品并付款，对方收到钱款后会通过财付通等方式将钱返还，同时安排发空包快递，接任务方收到快递后确认收货并给予好评，一笔刷单即完成，接任务方可以获得发任务方悬赏的任务点的80%-90%，其余任务点为平台抽点，会员获得的任务点可用于在平台上发布悬赏刷单公告；平台还提供代发

空包快递的业务，以及平台的负责人和创建人是“零零”即被告人李某某，管理员为“空空”、“飞猪”、“山鸡”等人，部分证人证言还证实虽然入会时管理员承诺会退还保证金，但实际上部分证人因无法完成平台任务而被踢出平台，部分证人找管理员或被告人李某某讨要保证金未果，部分证人因从他人处得知无法退还保证金或提出退还保证金的要求即会被踢出平台而未向管理员提出退还保证金的要求，仅有3名证人称收到了退还的保证金（其中2名证人是在平台解散时收到退还的保证金）等事实；

8、搜查笔录、扣押清单、发还清单，证实2014年5月28日，侦查人员对杭州市余杭区五常街道陈家角4号李某1住所进行搜查，查获并扣押黑色“百盛”、“普易达”牌台式电脑主机各1台，“Dell”牌笔记本电脑1台，后将上述物品发还李某1；2014年5月28日，侦查人员对被告人李某某居住的杭州市丽江公寓进行搜查，查获并扣押“segotep鑫谷”牌电脑主机1台，2014年5月28日，侦查人员对位于杭州市江干区九堡镇某室被告人李某某的办公场所进行搜查，查获并扣押黑色“cooto”电脑主机1台、中国工商银行储蓄卡2张（卡号分别为62×××68、62×××29），后将2台电脑主机发还被告人李某某的事实；

9、“零距网商联盟”会员清单、个人成员资料（根据李某1台式电脑上记载的会员审核资料整理形成），证实李某1收集的“零距网商联盟”的会员情况；

10、调取证据通知书、李某某等人相关支付宝信息、支付宝数据筛选，证实李某某及王某7的支付宝账户交易信息，根据支付宝交易信息结合证人证言及被告人李某某的供述和辩解，上述支付宝数据筛选显示2013年2月至2014年6月期间，被告人李某某通过上述账户收取会员保证金、平台维护费、体验费及购买任务点的费用共计人民币80余万元，其中平台维护费、体验费及购买任务点的费用至少为人民币30余万元的事实；

11、关于商请核查“http：//www.5sbb.com”有无经营性互联网信息服务资格的函、关于核查“http：//www.5sbb.com”有无经营性互联网信息服务资格的复函，证实经核查，“http：//www.5sbb.com”主办单位名称为顾倩影，备案/许可证号为苏ICP备12076560号，网站名称为我刷宝贝，网站域名为5sbk.com，5sbb.com，主办单位性质为个人，不具备获得增值电信业务经营许可证条件的事实；

12、营业执照、关于域名taobao.com的whois信息及网站信息、关于淘宝网架设的云服务器及分布区域的说明，证实浙江淘宝网络有限公司住所地为杭州市余杭区五常街道，该公司所属淘宝网（××）的运营服务器架设在阿里巴巴集团下属阿里云计算有限公司的云服务器，并根据实际使用流量变化等因素由阿里云公司调配各地（含余杭）云服务器空间资源综合使用的事实；

13、协助查询财产通知书、银行明细，证实被告人李某某被扣押的2张的工商银行储蓄卡（卡号62×××68、62×××29）的交易明细，其中两账户的余额分别为0元、0.54元的事实；

14、情况说明，证实被告人李某某归案后检举他人犯罪，但无法查证属实的情况；

15、受案登记表、受案回执、抓获经过，证实本案的侦破经过，以及被告人李某某系被抓获归案的事实；

16、户籍证明、刑事判决书、执行通知书、释放证明、缴款单，证实被告人李某某的身份情况，以及被告人李某某因犯侵犯公民个人信息罪于2016年9月10日被江西省宜春市公安局刑事拘留；2017年5月16日，江西省宜春市袁州区人民法院作出（2017）赣0902刑初136号刑事判决书，以被告人李某某犯侵犯公民个人信息罪，判处其有期徒刑九个月，并处罚金人民币二万元（刑期自2016年9月10日起至2017年6月9日止）；该案所判罚金人民币二万元，被告人李某某已缴纳的事实；

17、被告人李某某的供述和辩解，证实其为炒信平台“零距网商联盟”的负责人（该平台前身是“迅爆军团”），平台创立的目的是为了通过刷信誉来提升淘宝店铺销量，以便淘

宝买家在选择商品时更容易选择该淘宝店铺的商品；平台按金字塔结构进行管理，最高权限的管理员有3名，为其（YY昵称为零零）、肖某（YY昵称为柠檬）及“飞猪”（系YY昵称），另有黄马甲管理员30余名，其等人主要负责处理平台纠纷、发放任务点、组织娱乐活动等；淘宝卖家或淘宝店铺客服需提供店铺信息、身份证信息到网站进行注册，并需通过支付宝或财付通账户向其或者管理员的账户缴纳300-500元押金（淘宝店铺等级高的支付押金数额少一些，在收取时告知会员押金可以退还，但退还需要一定的条件，如入会一定期限，做了一定量的刷单任务，参与的刷单必须完结等）及40-50元平台维护费，平台维护费是每个会员均需缴纳的，管理员收到钱款后会转账给其，其一般通过自己、王某7及毕某的支付宝账户收取钱款，其已收取相关费用五、六十万元，收取的费用用于购买YY频道、维护网站、加程序、公关应酬及个人消费；平台炒信的流程为：淘宝卖家注册账户并加入YY频道，使用平台账户接受刷单任务，与发布任务的另一卖家使用YY进行联系，发布任务者会告诉接任务者所要刷单的商品信息，接任务者在淘宝网上“购买”并使用支付宝完成付款，发布任务者发送空包（空包一般为发任务者自发，也可由“科比”代发，目的是为了使交易看起来是真实交易），接任务者确认收货并给予好评后，发布任务者通过财付通回款给接任务者（使用财付通回流资金是为了规避淘宝的监管），接任务者可获得发任务者悬赏的90%的任务点，平台则抽取另10%的任务点，用于给管理员发工资或作为平台活动的奖励，完成多次任务的会员可以在平台上发布任务，让其他会员帮助刷单；管理员每月可获得500个任务点，任务点可用于发布任务，也可以每个5元或6元的价格卖给平台，需要任务点的会员可以上述价格向平台购买任务点；李某1系资料管理员，具体负责会员申请时的审核工作，王某2、张某1为管理员，张某2为其女友；关于其何时加入炒信平台，其在侦查阶段第一次供述时称“零距网商联盟”的前身“迅爆军团”是其于2012年5月18日创建成立的，后称其一开始只是一般管理员，是2013年夏天才成为平台的最高管理员，在庭审中称其于2013年1月左右加入“迅爆军团”，2013年下半年，其成为最高管理员后将平台更名为“零距网商联盟”；关于平台会员数量，其在侦查阶段称至案发已有共计1000余名正式会员，在庭审中称在其负责期间加入的会员有七、八百名，其他会员是其负责之前就已经存在，部分会员是使用他人的身份信息注册多个账号，一人注册多个账号只需要交纳一次押金和平台维护费等。

上述证据确实充分且相互印证，足以认定。

被告人李某某提交刻录有关于其他炒信平台被工商部门查处等新闻内容的光盘，欲证实淘宝炒信现象比较普遍，一般是由工商部门处罚，经查，上述材料与本案不具有关联性，依法不作为本案的定案依据。

公诉机关指控截至2014年6月，被告人李某某共计获利90余万元人民币；辩护人提出被告人李某某仅代收会员费444000元，维护费44400元，经查，公诉机关据以认定该金额的主要依据为支付宝交易数据筛选，但该数据筛选存在同一交易记录重复计算的情况，根据在案的证人证言、被告人的供述和辩解等相互印证的证据证实的交纳会员费等费用的数额标准，按照有利于被告人的原则，经核算，交易记录记载的平台管理维护费、体验费及任务点销售收入至少人民币30万元及收取保证金人民币50余万元，故公诉机关指控的数额有误，本院予以更正，辩护人的上述辩护意见，本院亦不予采纳。

被告人李某某辩称其是2013年农历过完年后加入“迅爆军团”的，入会后二、三个月成为一般管理员，2013年夏天才成为高级管理员并将平台改名为“零距网商联盟”；辩护人同意被告人的辩解，经查，1）在案的证人张某1关于被告人李某某是“零距网商联盟”的创始人及老板，该平台的前身系因违规操作被关闭的“迅爆军团”，被告人李某某在“迅爆军团”被关闭后一周左右即重新组建了“零距网商联盟”的证言与被告人李某某在侦查阶段关于“零距网商联盟”的前身“迅爆军团”是其于2012年5月18日创建成立的供述相互

印证，证实被告人李某某系“零距网商联盟”平台的创建者；2）上述证据与证人李某1的证言相互印证，足以证实被告人李某某在2013年2月之前即为炒信平台的负责人。上述辩解及辩护意见，本院均不予采信。

本院认为，被告人李某某违反国家规定，以营利为目的，明知是虚假的信息仍通过网络有偿提供发布信息等服务，扰乱市场秩序，情节特别严重，其行为已构成非法经营罪。公诉机关指控的罪名成立，但指控的数额有误，本院予以更正。被告人李某某辩称自己没有组织刷单，刷单仅是违规行为；辩护人提出，1）不能简单地将《互联网信息服务管理办法》中关于“是否具有经营性互联网服务资格”的规定等同于“国家规定”，被告人李某某收取网站维护费和保证金是一种代为保管的行为，并不违法，且会员是自愿交纳相关费用的，被告人李某某并无非法占有的故意，亦不能因此认为本案所涉网站系经营性网站，且炒信行为涉及的虚假信息发布在淘宝网上，与本案所涉网站没有直接关系，在平台发布任务点并非发布虚假信息，故被告人李某某的行为不属于法律明确规定的构成非法经营犯罪的情形；2）即使网站因没有经营性互联网服务许可而经营需要被查处的，亦应属于江苏省通信管理局、工商行政等部门监管的范畴，不属于刑法调整的范围；3）刷单炒信扰乱的仅为淘宝网的排名秩序，而非市场秩序，经查，1）《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》系全国人民代表大会常务委员会制定的决定，《互联网信息服务管理办法》系国务院令，依法均属于《刑法》第九十六条规定的“国家规定”的范畴；2）被告人李某某创建并经营的“零距网商联盟”（前身为“迅爆军团”）以收取平台维护管理费、体验费、销售任务点等方式牟利，属于提供经营性互联网信息服务，根据《互联网信息服务管理办法》的相关规定，应当取得互联网信息服务增值电信业务经营许可证；3）本案中炒信行为即发布虚假好评的行为虽系在淘宝网上最终完成，但被告人李某某创建炒信平台，为炒信双方搭建联系渠道，并组织淘宝卖家通过该平台发布、传播炒信信息，引导部分淘宝卖家在淘宝网上对商品、服务作虚假宣传，并以此牟利，其主观上显具在淘宝网上发布虚假信息的故意，且系犯意的提出、引发者，客观上由平台会员即淘宝卖家实施完成发布虚假信息，其行为符合《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》第三条中规定的“利用互联网对商品、服务作虚假宣传”，构成犯罪的，依照刑法有关规定追究刑事责任；4）网络交易亦属市场交易，被告人李某某的行为扰乱了市场秩序；5）最高人民法院、最高人民检察院为保护公民、法人和其他组织的合法权益，维护社会秩序，根据《中华人民共和国刑法》、《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》等规定，对办理利用信息网络实施诽谤、非法经营等刑事案件作出《最高人民法院、最高人民检察院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》，该解释第七条规定，违反国家规定，以营利为目的，通过信息网络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，扰乱市场秩序，达到相应数额标准的，以非法经营罪定罪处罚，其中个人非法经营数额在二十五万元以上的，属于《刑法》第二百二十五条规定的“情节特别严重”。综上，被告人李某某的行为既违反国家规定，又系以营利为目的，通过信息网络有偿提供发布虚假信息等服务的其他严重扰乱市场秩序的非法经营行为，其行为符合《刑法》关于非法经营罪的构成要件，依法应定性为非法经营犯罪，且情节特别严重，会员是否自愿交纳相关费用并不影响非法经营的定性。上述辩护意见，本院不予采纳。被告人李某某辩称支付宝记录中备注为“买点”的部分钱款并非是会员向其直接买点，而是通过其向客服人员购买客服通过刷单积累的任务点，其自己直接卖点的钱款数额在1万元左右，经查，被告人李某某系采用组织他人通过其创建并经营管理的炒信平台炒信来获取非法利益，任务点的获取、流通是其非法经营的基础和方式，被告人李某某帮忙联系销售任务点的目的是为了维护炒信平台的经营运作，不论任务点实际是否系其所有，其均对销售任务点牟利具有故意，均应计入其非法经营的数额。上述辩解，本院不予采纳。辩护人提出被告人李某某主动退出平台，系犯罪中止，

经查，被告人李某某组织他人炒信，并收取相关费用，其非法经营行为系既遂，该辩护意见，本院不予采纳。被告人李某某无主动到案的行为，且虽在归案之初供述了自己的主要罪行，但在侦查阶段后期的供述及庭审中就其非法经营的时间等影响定罪量刑的情节予以翻供，不应认定为如实供述自己的罪行，辩护人关于被告人李某某系自首的辩护意见与法律规定不符，本院不予采纳。被告人李某某检举他人犯罪，但无法查证属实，辩护人据此要求对被告人李某某从轻或减轻处罚的辩护意见，本院不予采纳。被告人李某某请求对其减轻处罚的意见及辩护人请求对被告人李某某免予刑事处罚或单处罚金的辩护意见与审理查明的事实及法律规定不符，本院均不予采纳。被告人李某某一人犯两罪，依法应当数罪并罚。据此，依照《中华人民共和国刑法》第二百二十五条第（四）项、第五十二条、第五十三条第一款、第六十九条第一款、第三款、《最高人民法院、最高人民检察院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》第七条及《最高人民法院关于适用财产刑若干问题的规定》第一条、第二条第一款之规定，判决如下：

被告人李某某犯非法经营罪，判处有期徒刑五年六个月，并处罚金人民币九十万元；连同原判有期徒刑九个月，并处罚金人民币二万元，予以并罚，决定执行有期徒刑五年九个月，并处罚金人民币九十二万元（刑期自判决执行之日起计算。判决执行前先行羁押的，羁押一日折抵刑期一日。即自 2016 年 9 月 10 日起至 2022 年 6 月 9 日止。罚金人民币二万元已缴纳，其余罚金限判决生效后十日内缴纳）。

如不服本判决，可在接到判决书的第二日起十日内，通过本院或直接向浙江省杭州市中级人民法院提出上诉。书面上诉的，应交上诉状正本一份，副本二份。

审判长　俞潇

人民陪审员郑秋娇

人民陪审员徐贵林

二〇一七年六月二十无

书记员　卢雨思

第三编 观点文章

文章一、网络犯罪怎么定义

网络犯罪，是指行为人运用计算机技术，借助于网络对其系统或信息进行攻击，破坏或利用网络进行其他犯罪的总称。既包括行为人运用其编程，加密，解码技术或工具在网络上实施的犯罪，也包括行为人利用软件指令，网络系统或产品加密等技术及法律规定上的漏洞在网络内外交互实施的犯罪，还包括行为人借助于其居于网络服务提供者特定地位或其他方法在网络系统实施的犯罪。简言之，网络犯罪是针对和利用网络进行的犯罪，网络犯罪的本质特征是危害网络及其信息的安全与秩序。

文章二、网络犯罪概念和特点

核心内容：在网路极速发展的二十一世纪里面，我们需要面对的除了是一个相关的网络安全外，还需要注意一些关于网络犯罪的问题。网络犯罪的特点主要是需要如何进行防范？主要有哪些要素呢？下文将会详细分析，法律快车小编希望下文内容可以帮助到您。

网络技术的恶意运用，扰乱社会的经济秩序，对各国的国家安全、社会文化等构成威胁。目前，在具体的立法上，很多国家都将网络犯罪直接归到网络犯罪，对网络犯罪作出定义。我国一般把以计算机为主要工具的犯罪和以计算机资产为对象的犯罪总称为网络犯罪。网络犯罪是在虚拟的世界借助高新技术的手段实施的一种犯罪行为，网络犯罪与当今信息时代发展是联系在一起的，这是一种新型的高智能的犯罪，其产生和发展的原因也是多方面的。因此，犯罪特点不同于一般的犯罪。具体说：

(一)网络犯罪的隐蔽性高风险小，犯罪主体确定困难。

利用计算机信息技术犯罪不受时间地点限制，犯罪行为的实施地和犯罪后果的出现地可以是分离的，甚至可以相隔十万八千里，而且这类作案时间短、过程简单，可以单独行动，不需借助武力，不会遇到反抗。由于这类犯罪没有特定的表现场所和客观表现形态，有目击者的可能性很少，而且即使有作案痕迹，也可被轻易销毁，发现和侦破都十分困难。因而，对犯罪主体的确定就很困难。

(二)网络犯罪预谋性居多

网络犯罪是一种高智能的犯罪，大多数情况下，都是行为人经过狡诈而周密的安排，运用计算机专业知识，所从事的智力犯罪行为，因而犯罪人的主观故意性居多，并且犯罪决心大。比如入侵银行信息管理系统，犯罪人事先要使用计算机通过网络做大量的事前准备，在犯罪实施过程中，大多是进行大量的攻击测试，最后达到破解系统，实现自己犯罪目的。

(三)犯罪主体的低龄化趋势

青少年网络犯罪中，不经允许侵入他人网络是经常发生的，而且在黑客中，青少年的比例比较大，他们多没有商业动机和政治目的，更多是类似富有挑战性的攻关游戏，以取得满足感为目的。比如，最近美国国防部被黑客侵入，联邦调查局、司法部、航空航天署等很多有关部门会同国外警方经过很长时间的追踪，终于在以色列将黑客抓住。这名 18 岁的以色列少年，和两个美国加州的嫌疑人，曾数次进入美国防部的电脑系统，但没有进行实质性破坏。犯罪嫌疑人称，他们还为该系统弥补了几个安全上的漏洞。

(四)监控管理及司法规定的相对滞后性

目前，社会上有许多人对高技术有一种盲目的迷信，以为一旦使用了高技术设备就会万无一失地实现科学管理、达到高效率。而社会原有的监控管理和司法系统中的人员往往对高

技术不熟悉，对高技术犯罪的特点、危害性认识不足，或没有足够的技术力量和相应的管理措施来对付它们。

(五)犯罪侵害的目标较集中

就国内已经破获的网络犯罪案件来看，作案人主要是为了非法占有财富和蓄意报复，因而目标主要集中在金融、证券、电信、大型公司等重要经济部门和单位，其中以金融、证券等部门尤为突出。

(六)具有极大的社会危害性

国际计算机安全专家认为，网络犯罪社会危害性的大小，取决于计算机信息系统的社会作用，取决于社会资产计算机网络化的程度和计算机普及应用的程度，其作用越大，网络犯罪的社会危害性也越来越大。随着社会网络化的不断发展，包括国防、金融、航运等国家各个部门都将实行网络化管理，整个社会对网络的依赖日益加深，一旦这些部门遭到侵入和破坏，后果将不堪设想。分析人士到 21 世纪，电脑入侵在美国国家安全中可能成为仅次于核武器、生化武器的第三大威胁。

文章三、网络犯罪一些特有的表现形式

核心内容：网络犯罪在行为方式上以计算机网络为犯罪工具和以计算机网络为攻击对象两种，在行为性质上包括网络一般违法行为和网络严重违法即犯罪行为两种。随着逐年上升的网络犯罪趋势，我们需要注意以下描述的 4 种行为可能构成犯罪。

网络犯罪行为主要可以概括为以下几种形式：

1.制造、传播计算机病毒或实施黑客行为，危害计算机信息网络安全。

实施危害计算机信息网络安全的犯罪主要有两种形态。一是未经许可非法侵入计算机信息系统，进行破坏，使其功能不能正常运行，这是人们通常所说的黑客行为。二是制造并传播计算机病毒。计算机病毒具有潜伏性、隐蔽性、可激发性，更具传染性。通过网络可以不特定地传播，对计算机信息网络安全危害巨大，轻则造成数据丢失、局部功能损坏，重则造成计算机系统瘫痪，甚至造成局部或区域性信息网络的瘫痪。

2.利用网络窃取账号、信用卡资料等，侵害公私财产。

网络自身存在的缺陷和漏洞，为网络犯罪提供了可乘之机。利用网络窃取他人的上网账号用来自己上网、网上购物等个人消费活动。或者利用网络窃取他人金融系统的账号、信用卡资料、股市的账号及密码等，对账户上的资金进行消费、挪用、转移，对股票低抛低购，而无视给他人造成的经济损失。

3.利用网络进行诈骗。

网络诈骗，是以非法占有为目的，利用互联网采用虚拟事实或者隐瞒事实真相的方法，骗取公私财物的行为。由于网络诈骗违法犯罪行为可以不亲临现场的间接性特点，使这类违法犯罪行为有着形形色色的表现形式。如网络拍卖诈骗、网络传销诈骗、信用卡诈骗及网络休闲诈骗等。

4.利用计算机网络制作、复制、传播、贩卖色情淫秽物品，破坏市场经济秩序，妨碍社会管理秩序。

主要是互联网上建立色情网站或制作色情网页，在网上制作、复制、贩卖、传播色情淫秽电影、表演、动画等视频文件、音频文件以及淫秽图片、电子书刊、文章、短信等。

另外是通过互联网散布反动言论，危害国家安全；利用网络泄露他人的隐私，妨害他人的名誉等等。

文章四、如何确定网络犯罪案件管辖

【案例】

陈某与李某担任法定代表人的某公司曾发生经济纠纷，陈某为此怀恨在心，向其住所地公安局举报该公司经理涉嫌合同诈骗等罪。陈某在得到有关机关不予立案回复后，分别向中纪委、北京市纪检委、北京市顺义区政府、顺义区委寄发举报信，举报李某伙同特定关系人苑某涉嫌贪污等犯罪的事实。后陈某自 2009 年 6 月起陆续在互联网的“人民网”、“新华网”、“证券之星”等多家商业网站上发表涉及李某“涉嫌贪污等经济犯罪”、“有情妇”等内容的文章。

北京市顺义区委接到举报后，责成有关机关对陈某反映的问题进行调查， 并于 2009 年 8 月 24 日出具报告，结论是陈某反映的问题均属严重失实。

2009 年 8 月 31 日，李某以陈某犯诽谤罪，向北京市顺义区人民法院提起控诉，因李某身份特殊，北京市第二中级人民法院指定北京市平谷区人民法院管辖。

平谷区法院经审理认为，陈某举报某公司经理犯罪在得到有关机关不予立案的回复后，故意捏造事实，并大肆利用互联网，在多家网站上公然散布上述言论，损害了自诉人李某的人格和名誉，属情节严重，其行为已构成诽谤罪，判处其有期徒刑一年。

陈某以该案诉讼程序违法，应由其住所地人民法院管辖为由提出上诉，北京市第二中级人民法院认定，陈某的主要诽谤行为发生地在北京，故北京市的人民法院具有管辖权，且北京市第二中级人民法院指定下级人民法院审判并无不当，最终驳回陈某的上诉，维持原判。

【分析】

关于本案管辖权的问题，本人不赘述。由本案所联想到的是，假使陈某并未有举报行为，仅以在互联网上散布不实言论的方式诽谤他人，北京市法院是否有管辖权？推而广之，利用网络实施的犯罪案件，如何确定管辖？

随着互联网的日益普及，网络犯罪也呈燎原之势。网络空间的全球性、虚拟性和不确定性，给刑事犯罪认定尤其是刑事管辖权的认定带来了新的问题。犯罪人的居住地、犯罪行为和结果发生地等因素之所以能够成为刑事司法管辖权的基础，是因为它们和某个刑事司法管辖区域有着物理空间的关联。然而，将上述因素适用于网络空间，它们与刑事司法管辖区域的物理空间的关联性变得极不确定。于是，有论者提出针对网络管辖的新理论，如以网址作为新的管辖基础的网址管辖论、以网络技术比较发达的北京、上海等城市优先管辖的技术优先管辖论、取消侵权行为地而仅以被告住所地及可执行标的所在地确定管辖的取消侵权行为地作为管辖识别因素论等。

本人认为，我们不应盲目地、不假思索地认为传统管辖规则过于滞后而缺乏时代价值，而应保持刑法理论的固有稳定性，充分发挥现有司法制度的弹性和灵活性，根据传统管辖理论来冷静思考网络犯罪的管辖问题，并伴随技术的进步而进行相应的调整，只有这样才能最大限度地填充和减少网络空间中的刑事管辖权空白和冲突。本人认为，在具体确认网络犯罪刑事管辖权时应以网络行为的最终目的地、网络犯罪行为实施地、网络犯罪行为结果地作为合理依据。

1、网络行为的目的地。

网络行为必然具有目的性。因此，行为的目的可以作为确定管辖的联结点。如果行为人使网络上的特定人得到信息数据，并希望他人访问该网页，或者有意向特定的目标发送信息、数据，这种积极的、主动的接触目的与目标所在地构成直接故意的关联。这种直接故意的关联，可以推定为行为人的意思表示是接受被指向地的法律，构成被指向地法院管辖的基础。

2、网络犯罪行为实施地。

网络犯罪行为须通过一定的计算机设备进行，应当以行为人为中心，以实施犯罪行为的

设备为线索，认定犯罪行为地。行为人实施犯罪的计算机终端、服务器等设备是相对固定的，因此，行为人实施网络犯罪的服务器、计算机终端等设备所在地可以视为犯罪行为地。

3、网络犯罪行为结果地。

由于网络传输的全球性，对于任何上网的行为，受其危害影响的地点都会数不胜数，若以此作为管辖权的基础，必然会造成管辖法院的泛滥。但网上侵犯商业秘密、间谍犯罪、网络入侵、散布破坏性病毒、逻辑炸弹、放置后门程序、偷窥、复制、更改或者删除计算机信息等犯罪有一个共性，就是必须侵入他人的计算机信息网络才能作案。因此，将所侵入的系统局域网、计算机终端等设备所在地作为犯罪结果地，其所在地法院拥有管辖权当无异议。

在刑事诉讼管辖方面，我国对网络犯罪案件没有具体的管辖规定，结合办案实践和相关的司法解释，对于具体网络犯罪案件地域管辖权的确定，本人认为应坚持以下几点：

1、对利用互联网销售假冒、伪劣商品等犯罪案件，实施网络犯罪行为的计算机终端所在地可以视为犯罪行为地。在侦办利用互联网销售假冒、伪劣商品等犯罪案件过程中，司法机关可以通过网络服务提供商来确定网址所对应服务器的物理地址，即网络犯罪行为实施地，进而确定地域管辖权。

2 、对利用计算机网络实施的侵犯著作权等知识产权犯罪案件以及损害他人商业信誉、商品声誉等案件，被发现侵权内容的网络服务器、计算机终端设备所在地可以视为犯罪行为地。

虽然对网络犯罪案件的犯罪行为地的确定问题，并没有专门的司法解释，但最高人民法院在 2000 年 12 月 19 日颁布的《关于审理涉及计算机网络著作权纠纷案适用法律若干问题的解释》第 1 条就明确规定了管辖问题：著作权纠纷案件由侵权行为地或被告住所地人民法院管辖。侵权行为地包括实施被诉侵权行为的网络服务器、计算机终端等设备所在地。对难以确定侵权行为地、被告住所地的，原告发现侵权内容的计算机终端设备所在地可以视为侵权行为地。2001 年 7 月 17 日颁布的《关于审理涉及计算机网络域名民事纠纷案件适用法律若干问题的解释》第二条关于涉及域名的侵权纠纷案件管辖：对难以确定侵权行为地和被告住所地的，原告发现该域名的计算机终端等设备所在地可以视为侵权行为地。上述两个解释在一定程度上解决了侵权行为地难以确定的问题。同样，这对于此类网络犯罪案件地域管辖中的犯罪行为地较难确定的问题，也有一定的借鉴作用。

3、对利用计算机网络实施的盗窃、贪污、挪用公款、职务侵占、挪用资金、诈骗等犯罪案件，犯罪行为人操作计算机的地点和网络行为所指向的最终目的地可视为犯罪行为地。

2010 年 2 月 5 日，最高人民法院给北京市高级人民法院《关于远程操控类诈骗案件审判管辖问题的函》中认为，对犯罪嫌疑人利用电话、网络等技术手段虚构事实进而实施的远程操控类诈骗案件，虚假信息所达之地即被害人所在地是犯罪行为的延续之地，可视为犯罪行为发生地。

4、对行为人通过侵入、修改受害单位或个人系统程序、系统参数等手段实施网络犯罪的案件，被侵害的计算机网络系统、设备终端的所在地可视为网络犯罪的犯罪结果地。

文章五、陈兴良：互联网帐号恶意注册黑色产业的刑法思考

摘要：如何在刑法上惩治恶意注册黑色产业，已成为当前我国刑法理论应当面对的问题。互联网恶意注册黑色产业可以分为三个环节：上游行为、中游行为和下游行为。恶意注册黑色产业链上游行为是指为恶意注册黑色产业提供注册所用的信息和资料、程序工具和技术支持等。中游行为是指利用从接码平台处取得的手机号和验证码以及打码平台获得的图像验证码识别，利用公民信息、自动化运行工具和突破安全保护措施的工具，完成整个注册过程和养号过程。下游行为是指出售恶意注册的账号，以及利用恶意注册的账号从事各种违法犯罪活

动。在我国刑法中，互联网账户的恶意注册行为本身并没有规定为独立罪名，在这种情况下，需要通过法律解释，对互联网恶意注册黑色产业的上述三种行为按照现有刑法规定进行惩治。

关键词：互联网 恶意注册 黑色产业 互联网犯罪

随着互联网技术的不断普及和快速发展，网络已彻底改变了人们的生活方式和思维方式，几乎每个人都享受着互联网发展带来的各种红利。然而，互联网生态同时伴生了各种违法犯罪行为。这些网络违法犯罪可以分为三种类型：

第一种类型是针对计算机信息系统的犯罪。对此，我国刑法设置了相关罪名，例如非法侵入计算机信息系统罪、破坏计算机信息系统罪等。这些网络犯罪主要是针对计算机以及计算机信息系统实施的，具有破坏性、毁坏型和侵入型犯罪的特征，但它又不同于对公共设施的破坏（危害公共安全罪）、对财产的毁坏（侵犯财产罪）和对住宅或者居所的侵入（侵犯人身罪）的性质。针对计算机信息系统的犯罪所具有的独具一格的属性，决定了它在刑法中应当单独设置罪名。

第二种类型是利用计算机网络实施传统犯罪，例如网络诈骗、网络盗窃、网络诽谤等，这是传统犯罪的网络化，对此《刑法》第 287 条规定：“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚”。在刑法教义学中，上述规定称为注意规定。它的功能在于：在刑法已有规定的情况下，提示司法人员注意对相关规定的适用。因此，注意规定也称为提示性规定。注意规定不同于特别规定，特别规定是刑法对某一特别事项所做的规定，因而对于已有的规定来说，是一种补充性规定。《刑法》第 287 条的规定，提示司法人员对于利用计算机实施刑法已经规定的犯罪的，应当按照相关规定定罪处罚。可以说，大多数传统犯罪都可以利用网络（以网络为工具）实施或者在网络空间（以网络为地点）实施。对于这些发生在网络上的传统犯罪，完全可以根据现行刑法规定进行认定处罚，只不过需要对刑法教义学的犯罪认定原理进行适当的调整。

第三种类型是破坏网络业务活动、妨害网络秩序的犯罪。随着网络空间越来越成为社会生活的重要组成部分，大量的社会活动或者经济活动都以网络空间为平台而展开。其中，破坏网络业务活动犯罪的侵害客体主要是网络经营活动，因而具有破坏经济秩序的性质。而妨害网络秩序犯罪的侵害客体主要是网络空间的公共秩序，因而具有妨害社会管理秩序的性质。在我国刑法中，此类网络犯罪呈现空白的现状。因此，在司法实践中如何处理这些破坏网络秩序的行为，成为一个亟待解决的问题。

本文以互联网帐号恶意注册黑色产业作为一个切入点，对破坏网络业务活动、妨害网络秩序的行为如何认定处罚进行刑法教义学的思考。

一、互联网恶意注册黑色产业概述

网络空间不同于真实的实体空间，它具有一定的虚拟属性。也就是说，现实社会中的人并不都是以真实身份存在于网络空间。计算机技术使得真实的人以匿名的方式存在于网络空间成为可能。如果网络空间中活动主体的身份都是匿名的，就会极大增加网络空间秩序管理的难度，甚至使这种网络空间管理完全不可能。在这种情况下，在客观上就提出了网络身

份实名制的需求。为此，我国《网络安全法》第 24 条规定：“网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务”。对网络空间的有效管理，就是建立在网络身份的实名制基础之上的。实名制提高了在网络空间实施违法犯罪活动的成本，同时也为网络安全奠定了基础。值得注意的是，《网络安全法》确立的网络注册实名制，是对网络运营商设立的法律义务，而并没有对个人违反网络注册实名制规定为违法行为并设置处罚。

在现实生活中，某些个人或者单位为了在网络空间从事违法犯罪活动，就会对抗网络身份的实名制，因而出现了互联网账号的恶意注册现象。互联网帐号的恶意注册存在狭义和广义之分：狭义上的恶意注册是指不以正常使用为目的，违反国家规定和平台注册规则，使用虚假的或非法取得的身份信息（包括自然人和法人），以手动方式或通过程序、工具自动进行，批量创设网络帐号的行为。广义上的恶意注册，除了单一的注册行为以外，还包括了注册行为结束后，为防止恶意注册的账户被封禁和提升帐号牟利价格，而突破互联网安全策略，模拟正常使用帐号形态，保持帐号的正常存续和使用的行为，俗称养号行为。〔在以网络帐号体系为基础的互联网环境中，网络违法犯罪产业都以大量帐号资源为前提，这些账号资源为其提供网络身份，并隐蔽真实身份、制造虚假流量、增加溯源难度、逃避法律追究。在这种需求的刺激下，催生了互联网上的恶意注册黑色产业，并使得原本正常的帐号注册与使用行为异化为黑色产业人员牟取非法利益的工具。在某种意义上可以说，正是恶意注册黑色产业的存在，为其他互联网犯罪提供了条件。在这种情况下，恶意注册行为就成为源头之恶。

根据腾讯公司《互联网账号恶意注册黑色产业治理报告》的描述，恶意注册黑色产业链可以分为以下三个环节：第一是产业链上游。为恶意注册黑产提供注册所用的信息和资料、程序工具和技术支持。第二是产业链中游。黑产人员利用从接码平台处取得的手机号和验证码以及打码平台获得的图像验证码识别，利用公民信息、自动化运行工具和突破安全保护措施的工具，完成整个注册过程和养号过程。第三是产业链下游。各种恶意注册帐号的贩卖商人和代理，负责将大量帐号出售贩卖，供下游用于多种用途。如何在刑法上惩治恶意注册黑色产业，成为当前我国刑法理论应当面对的问题。在我国刑法中，互联网账户的恶意注册行为本身并没有规定为独立罪名，在这种情况下，基于刑法教义学的立场，能否通过法律解释，对恶意注册行为按照现有刑法规定进行惩治，这是值得研究的。

二、 恶意注册黑色产业链上游行为是否构成犯罪的评析

恶意注册黑色产业链上游行为是指为恶意注册黑色产业提供注册所用的信息和资料、程序工具和技术支持等。这是恶意注册的帮助或者预备行为，对于形成恶意注册黑色产业链具有推波助澜的作用。其中，帮助行为是指为他人恶意注册提供信息和资料以及技术支持等。在被帮助行为，即恶意注册行为不构成犯罪的情况下，该帮助行为不能根据共犯原理而入罪。只有在该帮助行为本身符合相关犯罪的构成要件的情况下，才能以犯罪论处。预备行为是指为本人恶意注册获取信息和资料，在恶意注册行为不构成犯罪的情况下，该预备行为也不能根据预备犯的原理而入罪。只有在该预备行为符合相关犯罪的构成要件的情况下，才能以犯罪论处。根据我国现行刑法的规定，为恶意注册专门提供用于注册的身份（包括公民自然人和法人）信息和身份资料（身份证照片、营业执照照片等）的行为主要涉及是否构成侵犯公

民个人信息罪等相关罪名。

（一）为恶意注册提供或者获取个人信息和身份资料行为是否侵犯公民个人信息罪？

为恶意注册提供或者获取个人信息和身份资料，可以分为两种情形：第一种是提供或者获取真实的个人信息和身份资料；第二种是提供或者获取虚假的个人信息和身份资料。

1．为恶意注册提供或者获取真实的个人信息和身份资料行为的定性

对于为恶意注册提供或者获取真实的个人信息和身份资料的行为，主要涉及是否构成侵犯公民个人信息罪。我国《刑法》第 253 条之一规定：“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。”由此可见，在我国刑法中，侵犯公民个人信息罪的行为可以分为两种情形：第一种是向他人出售或者提供公民个人信息；第二种是盗窃或者非法获取公民个人信息。在恶意注册黑色产业中，为他人恶意注册出售或者提供公民个人信息的行为，完全符合侵犯公民个人信息罪的构成要件，应当以该罪论处。因此，为他人恶意注册提供公民个人信息的行为，虽然是恶意注册的帮助行为，由于该行为已经构成独立的犯罪，因而应当按照该罪定罪量刑。

在恶意注册黑色产业中，除了为他人提供个人信息和身份资料以外，还存在为本人的恶意注册获取公民个人信息的情形，该行为也构成侵犯公民个人信息罪。在恶意注册黑色产业中，非法获取公民个人信息的方式是多种多样的，其中包括通过交易、互换等方式批量获取公民信息。

在司法实践中，恶意注册的公民个人信息主要是通过交易，亦即购买的方式获取的。那么，批量购买公民个人信息的行为是否构成侵犯公民个人信息罪呢？我国《刑法》第 253 条之一规定向他人出售公民个人信息属于侵犯公民个人信息的行为，但在获取行为中，则规定为窃取或者以其他方法非法获取公民个人信息，并没有明确规定购买这种行为方式。在这种情况下，购买公民个人信息是否属于侵犯公民个人信息的行为，就是一个存在争议的问题。对此，存在一种观点认为，这里的“其他方法”应当是与窃取相当的方法，因而排除购买的方法，因为购买方法与窃取方法不具有性质上的同一性。这是基于同类解释所得出的结论，似乎具有一定的合理性。然而，在《刑法》第 253 条之一的规定中，与窃取相并列的是“以其他方法非法获取公民个人信息”。这一规定源自《网络安全法》第 44 条，根据该条的规定：“任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息”。这里的“其他非法方法“应当从广义上理解，这一理解同样适用于《刑法》第 253 条之一。2017 年 6 月 1 日实施的最高人民法院、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》（以下简称《解释》）第 4 条明确规定：“违反国家有关规定，提供购买、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’”。因此，采取购买的非法方法获取公民个人信息的行为，应当构

成侵犯公民个人信息罪。

在司法实践中，恶意注册的公民个人信息，无论是提供者或者获取者都可能采取技术手段取得。因此，通过技术手段非法获取公民个人信息，在恶意注册黑色产业中也是较为常见的现象。这里的技术手段获取公民信息主要包括拖库、撞库等方式。拖库是指黑客对目标网站进行扫描，查找其存在的漏洞，常见漏洞包括ＳＱＬ注入、文件上传漏洞等。通过该漏洞在网站服务器上建立后门（ｗｅｂｓｈｅｌｌ），通过该后门获取服务器操作系统的权限，或者实施权限绕过，最后利用系统权限直接下载备份数据库，或查找数据库链接，将其导出到本地。撞库则是指黑产人员在掌握了部分公民信息（多包括网络帐号、密码）后，通过批量登录的方式，利用部分用户在不同互联网平台使用相同账户名和密码的习惯，获取用户多个网络账户名和密码，进而获取更多公民信息。这种通过技术手段非法获取公民个人信息的行为，首先符合侵犯公民个人信息罪的构成要件，应当以该罪论处。同时，还要分析这种行为是否构成侵入计算机信息系统罪。根据我国《刑法》第 285 条的规定，非法获取计算机信息系统数据罪，是指违反国家规定，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，情节严重的行为。因此，通过技术手段非法获取公民个人信息的行为，在通常情况下，都是侵入计算机信息系统而实现的，其所获取的公民个人信息都表现为计算机信息系统的数据，因而该行为同时构成非法获取计算机信息系统数据罪。在这种情况下，侵犯公民个人信息罪与非法获取计算机信息系统数据罪之间存在竞合关系，应当以一重罪处断。

２． 为恶意注册提供或者获取虚假的个人信息和身份资料行为的定性

在恶意注册黑色产业链中，恶意注册的账号可能是所谓白号，即并不存在真实主体的账号。那么，这种根据虚假的公民个人信息进行恶意注册的行为是否构成侵犯公民个人信息罪呢？根据最高人民法院和最高人民检察院《解释》第 1 条的规定：“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，包括姓名、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。”公民个人信息是自然人的信息，这里的自然人是否要求是真实存在的人，这是该问题的核心。从我国法律规定来看，对公民个人信息的保护，并不仅仅是对互联网秩序的保护，更为重要的是对公民个人隐私的保护，即对公民个人人身权利的保护。因此，侵犯公民个人信息罪的保护法益具有双重性：一方面是互联网的正常秩序；另一方面是公民个人权利。例如《网络安全法》第 1 条规定：“为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。”在此，《网络安全法》将公民个人的合法权益和互联网的安全同时规定为该法保护的客体。而侵犯公民个人信息罪就是对公民个人信息保护的最为重要的法律规定。因此，这里的公民个人信息是指真实存在的、能够与个人对于的信息，而不能包括非实名的，即并非真实存在的个人信息。此外，我国刑法中的伪造国家机关、公司、企业、事业单位、人民团体证件、印章罪，也以与其对应的真实的国家机关、公司、企业、事业单位、人民团体为前提。如果捏造并不存在的国家机关、公司、企业、事业单位、人民团体，并制作其印章，并不构成伪造国家机关、公司、企业、事业单位、人民团体证件、印章罪。因为该罪的保护法益是国家机关、公司、企业、事业单位、人民团体的信誉，这种信誉受损以这些单位真实存在为前提。如果并不存在这种单位，虽然这种伪造行为也会扰乱社会管理秩序，但并不会损害国家机关、公司、企业、事业单位、人民团体的信誉，因此不能构成该罪。基于以上论证，笔者认为，对于利用白号等非实名手机号卡进行注册的行为不能构

成侵犯公民个人信息罪。如果利用这些号卡进行其他犯罪活动的，应当以其他犯罪论处。

（二）利用公开渠道收集的公民个人信息进行恶意注册能否构成侵犯公民个人信息罪？

在恶意注册产业链中，有些公民个人信息是通过公开途径收集的。在互联网环境中，大量公开场景提供了公开的公民信息和企业信息，例如通过遗失申明、转让申明等公开面登报的方式，可以获取相关公民个人身份证；通过部分企业信息查询ＡＰＰ、国家企业信用信息公示系统，亦可以获取到企业相关注册信息，而这些信息可能被利用在需要使用企业信息注册的场景之中。这里的问题是侵犯公民个人信息罪中的公民个人信息是否包括公开的公民个人信息？信息法律保护主要区分为两种模式，这就是美国的隐私保护模式和欧盟的人格权保护模式。隐私保护模式将公民个人信息保护理解为对公民个人隐私的保护，因此，如果已经公开的公民个人信息就不在保护之列。而人格权保护模式则认为，个人信息的保护是超越隐私保护利益范围的，它是对公民个人基本权利的保护，因此，即使是公开的个人信息也同样受到保护。我国学者指出：我国关于侵犯公民个人信息罪的司法解释第 1 条没有采用“涉及个人隐私信息”的表述，而是表述为“反映特定自然人活动情况的各种信息”。因此，公民个人信息不要求具有隐私的特征。即便相关信息已经公开，不属于个人隐私的范畴，仍然有可能成为公民个人信息。当然，对于已经公开的公民个人信息可以成为侵犯公民个人信息中的个人信息，应当进行适当的限制。例如，被告人收集以广告形式出现的公民个人信息，进行加工，并进行出卖，该行为是否构成收集公民个人信息罪呢？笔者的观点是不能构成该罪。因为虽然被告人收集的是公开的公民个人信息，但这些信息是从广告上收集来的，广告本身具有广而告之的性质，对于该信息进行传播并不侵犯公民个人信息权益。

（三）在涉及提供身份信息资料的场景，除认定侵犯公民个人信息罪之外，能否认定身份证类型犯罪？

这里的身份证类型的犯罪，是指我国《刑法》第 280 条第 3 款规定的伪造、变造、买卖身份证件罪和第 280 条之一规定的使用伪造、变造、买卖的身份证件罪。这里的伪造、变造、买卖身份证件罪，是指伪造、变造、买卖居民身份证、护照、社会保障卡、驾驶证等依法可以用于证明身份的证件的行为。这里的使用伪造、变造、买卖的身份证件罪，是指依照国家规定应当提供身份证明的活动中，使用伪造、变造的或者盗用他人的居民身份证、护照、社会保障卡、驾驶证等依法可以用于证明身份的证件，情节严重的行为。在网络账号恶意注册黑色产业中，黑产人员利用伪造、变造的或者盗用他人的居民身份证、护照、社会保障卡、驾驶证等依法可以用于证明身份的证件进行虚假注册，当然可以构成上述身份证类型的犯罪。因为这里的使用行为，不仅包括伪造、变造、买卖身份证件的行为人自己使用，而且还包括其他明知是伪造、变造、买卖身份证件的人使用。因此，只要黑产人员恶意注册的行为符合上述犯罪的构成要件，就可以构成使用伪造、变造、买卖的身份证件罪。

（四）利用公民自愿提供的个人信息进行注册和身份绑定如何定罪？

在现实生活中，社会上部分人员为生活所迫或对个人信息的安全意识不强，将自己的身份证、银行卡等信息以一定价格售卖给他人。这些公民个人信息被恶意注册黑产人员所利用，以少量金钱报酬利诱防范意识相对较差的老人，从而使对方自愿地出售个人信息甚至身份证件照片等。在这种公民个人自愿提供个人信息的情况下，不存在侵犯公民个人信息权益的问题，因此收购者和使用者的行为不构成侵犯公民个人信息的犯罪。对于这些大批量地收

购公民身份证等个人信息的行为，确实具有较大的社会危害性，但我国刑法对此没有明文规定，目前尚不构成犯罪。

三、 恶意注册黑色产业链中游行为是否构成犯罪的评析

恶意注册黑色产业链的中游行为就是指广义上的恶意注册行为，这是恶意注册产业链的核心行为。行为人利用从接码平台处取得的手机号和验证码以及打码平台获得的图像验证码识别，利用公民信息、自动化运行工具和突破安全保护措施的工具，完成整个注册过程和养号过程。应当指出，我国刑法对于恶意注册行为本身并没有规定为犯罪，因此，不能对恶意注册行为直接定罪。然而，在我国刑法理论上，对于这种恶意注册行为能否通过法律解释方法，对其按照相关法律处罚，存在一定的争议。

（一）恶意注册黑产行为是否构成非法经营罪？

恶意注册作为一种经营行为是否构成认定非法经营罪呢？恶意注册在我国已经形成一个黑色产业，黑产人员基于主观上的营利目的，专门从事恶意注册及养号活动，以此作为营利手段，这就提出了恶意注册黑产行为能否按照非法经营罪论处的问题。对恶意注册黑产行为按照非法经营罪论处观点的主要理由，我国学者周光权教授归纳为三点：首先，非法经营罪观点认为，被告人的行为违反了关于实名制的国家规定。国家已经全面实施了网络服务实名制的规则，根据全国人大常委会《关于加强网络信息保护的决定》和《电话用户真实身份信息登记规定》（工业和信息化部令第２５号），电话用户真实身份信息登记已于 2013 年９月１日起全面实施；2017 年 6 月 1 日起施行《网络安全法》第 24 条亦明确规定了网络服务的前提是用户提供真实身份信息。由此，销售不具有实名的黑卡和利用黑卡注册不具有实名的互联网账号是违反了国家规定的行为。其次，被告人的行为违反了关于互联网服务的国家规定。

依照全国人大常委会《关于维护互联网安全的决定》的规定，利用互联网实施该决定第 1 条、第 2 条、第 3 条、第 4 条所列行为以外的其他行为，构成犯罪的，依照刑法有关规定追究刑事责任。依照《互联网信息服务管理办法》，国家对经营性互联网信息服务实行许可制度，对非经营性互联网信息服务实行备案制度，未取得国家有关部门的许可，不得从事互联网有偿信息服务。提供互联网账号这一行为本身是互联网信息服务中的一种，恶意注册账号和养号群体虽然并非提供用户注册、使用账号的平台，但其行为实质上是为那些不通过自身注册账户的人员提供了账户服务，可以理解为一种互联网服务，由此也违反了关于互联网服务的国家规定。最后，恶意注册账号和养号产业的存在，客观上规避了通信及网络服务实名制的规定，其社会危害性是显而易见的。

在以上三个理由中，前两个理由是违反国家规定，这是非法经营罪的规范构成要件要素；第三个理由是行为具有社会危害性，这是非法经营罪的实质处罚根据。根据我国《刑法》第 225 条的规定，非法经营罪是指违反国家规定，有下列非法经营行为之一，扰乱市场秩序，情节严重的情形：①未经许可经营法律、行政法规规定的专营、专卖物品或者其他限制买卖的物品的；②买卖进出口许可证、进出口原产地证明以及其他法律、行政法规规定的经营许可证或者批准文件的；③未经国家有关主管部门批准非法经营证券、期货、保险业务的，或者非法从事资金支付结算业务的；④其他严重扰乱市场秩序的非法经营行为。值得注意的是，非法经营罪以违反国家法律规定为前提，即使是《刑法》第 225 条第 4 项的兜底规定，

即其他严重扰乱市场秩序的非法经营行为，也应当以违法国家法律规定为前提，它只是对于某种经营行为属于国家法律所禁止，只是刑法没有将这种国家法律所禁止的经营行为列入《刑法》第 225 条的规定。在这种情况下，司法机关可以援引第 4 项的规定，以其他严重扰乱市场秩序的非法经营行为而认定为非法经营罪。

对于恶意注册黑产行为来说，该行为本身具有较大的法益侵害性，在刑法上具有处罚必要性，这是没有争议的。同时，这里所讨论的恶意注册黑产行为并不是单一个人违反网络注册实名制的虚假注册行为，而是指以营利为目的，进行产业化的网络恶意注册黑产行为，因而具有经营活动的性质，符合非法经营罪所要求的经营行为的特征。恶意注册黑产行为能否按照非法经营罪论处，关键在于是否具备违反国家法律的规范构成要件要素。

非法经营罪观点援引我国关于网络注册实名制的规定，以此论证恶意注册黑产行为违反国家规定。非法经营罪观点认为恶意注册黑产行为违反国家规定，其逻辑是：我国法律确立了网络注册实名制，而恶意注册黑产行为违反了网络注册实名制，因而恶意注册黑产行为违反国家规定。笔者认为，这个逻辑推理是难以成立的。非法经营罪的违反国家规定，是指违反国家法律的禁止性规定。因此，违反国家规定应当根据国家规定的具体内容进行判断。在非法经营罪观点列举的国家规定中，《电话用户真实身份信息登记规定》是工业和信息化部颁布的，属于部门规章，不能认定为非法经营罪规范构成要素中的国家规定。其他法律或者行政法规属于国家法律规定。《关于加强网络信息保护的决定》立法宗旨在于保障公民个人网络信息安全，其第 6 条涉及网络注册实名制，指出：“网络服务提供者为用户办理网站接入服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。”在此，法律规范的主体是网络服务提供者，因而违法的主体也是网络服务提供者。根据这一规定，不能认为公民没有提供真实身份信息是违法行为，因而不存在违反国家规定的问题。同样，《国家安全法》也并没有将个人在网络注册时没有提供真实身份信息行为规定为违法。至于《关于维护互联网安全的决定》第 1 、 2 、 3 、 4 条提示性规定的各种应当追究刑事责任的网络违法行为，也不包括网络恶意注册行为。至于第 5 条关于利用互联网实施本决定第 1 条、第 2 条、第 3 条、第 4 条所列行为以外的其他行为，构成犯罪的，依照刑法有关规定追究刑事责任的规定，是一个兜底性规定，不能据此认定个人恶意注册行为违反国家规定。

不仅如此，而且我国法律也并没有对经营性的恶意注册黑产行为的禁止性明文规定，因而恶意注册黑产行为也缺乏违反国家法律规定的根据。此外，非法经营罪观点还论及《互联网信息服务管理办法》规定国家对经营性互联网信息服务实行许可制度，这一规定与网络恶意注册是否违法并没有关系，而只是涉及恶意注册黑产人员以营利为目的，为他人违法犯罪活动提供恶意注册的互联网账户行为是否构成非法经营罪的问题。基于以上分析，笔者认为网络恶意注册行为不具备违反国家规定的规范构成要素，根本就不存在适用《刑法》第 225 条的规范基础，因而不能构成非法经营罪。

（二）批量自动化注册行为是否构成侵害计算机信息系统罪？

我国《刑法》第 285 条第 2 款规定的非法获取计算机信息系统数据罪，是指违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统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的行为。非法控制计算机信息系统罪，是指对计算机信息系统实施非法控制，情节严重的行为。我国《刑

法》第 285 条第 3 款规定的提供侵入、非法控制计算机信息系统的程序、工具罪，是指提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的行为。上述三种犯罪都是侵害计算机信息系统的犯罪，具有对计算机信息系统重大的危害性。

在现实生活中，存在批量自动化注册的程序工具，这些程序、工具如果只是追求注册的速度，但并没有进入计算机信息系统，则不涉及侵害计算机信息系统的犯罪。但如果具有在软件客户端修改程序的功能，因而能够进入计算机信息系统，则可以理解为侵入和非法控制计算机信息系统，并且提供该种功能和程序的行为，可以认定为刑法 285 条第 3 款规定的提供侵入、非法控制计算机信息系统程序、工具罪。例如 2018 年 10 月浙江省兰溪市人民法院做出（2018）浙 0781 刑初字第 300 号《刑事判决书》，对首例恶意注册账号案进行宣判。在本案中，被告人汤某某制作畅游注册机．ｅｘｅ注册机用于出售获利，该畅游注册机．ｅｘｅ软件能够实现自动产生注册信息并通过第三方平台获取手机号，以数据包方式发送给畅游注册平台服务器，借助第三方平台自动将获取的手机验证码发送回畅游注册平台完成批量注册，对畅游注册平台的正常操作流程和正常运行方式能造成干扰，属于破坏性程序。法院经审理以提供侵入、非法控制计算机信息系统程序、工具罪对各被告人定罪处罚。上述案件虽然被称为首例恶意注册账号案，但这并不意味着恶意注册行为可以入罪，而只是恶意注册的手段行为触犯法律而被入罪。

（三）为实施犯罪而恶意注册黑产行为是否构成帮助信息网络犯罪活动罪？

根据我国《刑法》第 287 条之二的规定，帮助信息网络犯罪活动罪是指明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的行为。由此可见，帮助信息网络犯罪活动罪的构成要件是：第一，客观上具有帮助信息网络犯罪活动的行为。这里的帮助信息网络犯罪活动的行为是指为他人的互联网犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助。第二，主观上具有对他人利用信息网络实施犯罪的明知。第三，情节严重，这是该罪的罪量要素。只有同时具备以上三个条件，才能构成该罪。

帮助信息网络犯罪活动罪在立法上具有帮助行为正犯化的性质，因而涉及该罪与互联网犯罪的共犯之间的区分问题。从共犯理论上来说，明知他人犯罪而提供帮助的，构成帮助犯，而帮助犯属于共犯。但立法机关考虑到某些帮助行为的特殊性，将这种帮助行为直接规定为正犯。例如我国刑法规定了组织卖淫罪，但同时又规定了协助组织卖淫罪。这里的协助组织卖淫罪其实就是组织卖淫罪的帮助犯，但刑法将其设立为单独犯罪。帮助信息网络犯罪活动罪也是如此，在该罪设立之前，我国司法实践都把这种网络犯罪的帮助行为按照共犯处理。但考虑到网络犯罪的帮助行为具有其特殊性，因而我国刑法单独设立了帮助信息网络犯罪活动罪。在该罪设立之后，网络犯罪的帮助行为就不再以共犯论处，而是以帮助信息网络犯罪活动罪论处。

恶意注册黑产行为是否可以构成帮助信息网络犯罪活动罪，首先要考察他人行为是否属于网络犯罪活动，其次还要考察行为人对于网络犯罪是否明知。从恶意注册行为黑产的性质来看，具有帮助性质，如果其帮助的对象属于信息网络犯罪活动，则可以构成帮助信息网络犯罪活动罪。

四、 恶意注册黑色产业链下游行为是否构成犯罪的评析

恶意注册黑色产业链的下游行为是指出售恶意注册的账号，以及利用恶意注册的账号从事各种违法犯罪活动。这里的出售恶意注册的账号行为其实就是恶意注册账号的营利行为，因而这是一个是否构成非法经营罪的问题。笔者认为，在刑法对此没有明文规定的情况下，难以按照非法经营罪论处。在此，主要讨论他人利用恶意注册的账号从事非法活动的定罪问题。

（一）利用恶意注册的账号从事网络正向炒信刷单行为是否构成非法经营罪？

网络正向炒信刷单，是指虚构交易量，以此提高商户的信誉，因此该行为具有不正当竞争的性质。这里应当指出，网络正向炒信刷单，即可能是利用真实互联网账户，也可能是利用恶意注册的互联网账号。在利用恶意注册的互联网账号进行网络正向炒信刷单的情况下，就离不开恶意注册黑色产业的支撑。尤其是某种大规模的炒信刷单，背后都存在恶意注册黑色产业的背景。例如，在电商平台存在大量恶意注册帐号，它不仅影响了个别商家的商誉，而且使得电商平台的评价机制受到根本动摇，互联网场景的诚信体系遭受根本破坏。然而，随着刷单、刷量黑产的逐步成熟，提供的刷单服务日趋细化，并且刷手所使用的电商帐号大多跟正常买家无异，导致电商平台识别刷单行为需要提取更多的维度特征加以分析，给平台识别刷单带来诸多难题。

这种利用恶意注册的账号进行网络炒信刷单，具有对网络交易秩序的破坏性，因而在刑法上如何惩治是一个值得研究的问题。从我国司法实践情况来看，对于网络正向炒信刷单行为，涉及是否构成非法经营罪的问题。

正向炒信刷单具有组织性，并且已经成为一种黑色产业，相关商家专门有组织地从事炒信刷单，以此作为一种经营活动。对此，我国有的法院将这种网络正向炒信刷单行为认定为非法经营罪。例如 2013 年，李某某通过创建零距网商联盟网站，利用ＹＹ语音聊天工具建立刷单炒信平台，吸纳淘宝卖家注册账户成为会员，并收取 300 元至 500 元不等的保证金和 40 元至 50 元的平台管理维护费及体验费。该案被告人李某组织炒信刷单的行为被法院认定为非法经营罪，判处有期徒刑 5 年 6 个月。这个案件的争议焦点在于如果认定非法经营罪所要求的违反国家规定？对此，法院判决认为，《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》系全国人民代表大会常务委员会制定的决定，《互联网信息服务管理办法》系国务院令，依法均属于《刑法》第 96 条规定的国家规定的范畴。

被告人李某某创建并经营的零距网商联盟以收取平台维护管理费、体验费、销售任务点等方式牟利，属于提供经营性互联网信息服务，根据《互联网信息服务管理办法》相关规定，应当取得互联网信息服务增值电信业务经营许可证。本案中，炒信行为即发布虚假好评的行为虽系在淘宝网上最终完成，但被告人李某某创建炒信平台，为炒信双方搭建联系渠道，并组织淘宝卖家通过该平台发布、散播炒信信息，引导部分淘宝卖家在淘宝网上对商品、服务作虚假宣传，并以此牟利，其主观上显具在淘宝网上发布虚假信息的故意，且系犯意的提出、引发者，客观上由平台会员即淘宝卖家实施完成发布虚假信息，其行为符合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》第 3 条规定的“利用互联网对商品、服务作虚假宣传”，构成犯罪的，依照刑法有关规定追究刑事责任。

对于该案，首先涉及是否属于《关于维护互联网安全的决定》的内容是否属于罪状规定的问题。如果属于罪状，当然可以以此作为定罪根据；如果不是罪状，则不能作为定罪根据。纵观《关于维护互联网安全的决定》，只是对利用互联网实施犯罪的提示性规定，而不是罪状规定。具体到第 3 条利用互联网对商品、服务作虚假宣传构成犯罪的规定，这里的构成犯罪只能是构成诈骗类犯罪。至于《互联网信息服务管理办法》，确实规定了国家对经营性互联网信息服务实行许可制度。但这里所说的互联网信息服务，是指通过互联网向上网用户提供信息的服务活动。其中，经营性互联网信息服务是指通过互联网向上网用户有偿提供信息或者网页制作等服务活动。这种服务本身具有中立性：如果取得许可即为合法，未取得许可即为非法。而提供虚假交易的炒信刷单并不是这里的互联网信息服务，因为这种活动本身具有非法性，不可能取得许可而成为合法。因此，不能简单地认为炒信刷单行为违反国家规定。2017 年修订的《反不正当竞争法》第 20 条第 1 款才将对其商品作虚假或者引人误解的商业宣传，或者通过组织虚假交易等方式帮助其他经营者进行虚假或者引人误解的商业宣传的行为规定为不正当竞争的行为，由此获得违法性。然而，在《反不正当竞争法》修订以后，这种正向炒信刷单仍然不能当然构成非法经营罪，而是有待于法律对此加以明确规定。

（二）利用恶意注册的账号从事网络反向炒信刷单行为是否构成破坏生产经营罪？

网络反向炒信刷单则是指进行恶意交易或者给予差评，以此损害商户的商誉，因此该行为具有毁坏商誉的性质。在我国刑法理论上，对于网络反向炒信刷单行为，一般以破坏生产经营罪论处。例如南京反向炒信案：被告人董某为谋取市场竞争优势，指使谢某多次以同一账号恶意大量购买北京智齿公司南京分公司淘宝店铺商品，致使淘宝公司错误判定该店铺从事虚假交易，进而对其商品做出搜索降权的处罚，造成消费者无法通过淘宝网搜索到该公司在淘宝网店铺的商品，从而严重影响到该公司的正常经营活动，并由此造成了 10 万余元的经济损失。南京市雨花台区法院一审认为，被告人董某、谢某出于打击竞争对手的目的，其行为属于以其他方法破坏生产经营活动，构成破坏生产经营罪。

网络反向炒信刷单行为能否认定为破坏生产经营罪，关键在于如何理解破坏生产经营罪的性质，以及如何解释。根据我国《刑法》第 276 条的规定，破坏生产经营罪是指由于泄愤报复或者其他个人目的，毁坏机器设备、残害耕畜或者以其他方法破坏生产经营的行为。在刑法理论上，破坏生产经营罪属于毁坏型财产犯罪，而不是经营性财产犯罪。之所以误解为经营性犯罪，主要是被罪状与罪名中“破坏生产经营”的表述所误导。高铭暄教授在论及 1979 年刑法中破坏集体生产罪和故意毁坏公私财物罪的关系时，指出：“前者的目的破坏生产，而毁坏机器设备等只不过是为了达到破坏生产的目的所使用的方法；后者则不直接破坏生产，故意的内容是毁坏公私财物本身。”

由此可见，在 1979 年刑法中，破坏集体生产罪和故意毁坏公私财物罪之间就是一种法条竞合关系：前者是以破坏集体生产为目的的故意毁坏公私财物行为。在 1997 年刑法修订中，将破坏集体生产罪从刑法分则第三章移入刑法分则第五章，使其成为侵犯财产罪，并且罪名也相应修改为破坏生产经营罪。而故意毁坏公私财物罪的罪名则删去“公私”二字，修改为故意毁坏财物罪。在 1997 年刑法中，破坏生产经营罪和故意毁坏财物罪之间的法条竞合关系更为明显。故意毁坏财物罪的手段———毁坏机器设备、残害耕畜，是一种毁坏工农业领域生产资料的行为，因而破坏生产经营罪中的“其他方法”也应当同类解释为对其他生产领域的生产资料的方法。例如，对计算机公司来说，砸毁计算机就属于破坏生产经营罪的“其他方法”。如果破坏计算机信息系统，尽管也会对计算机公司的生产经营造成损失，但

该行为不构成破坏生产经营罪，而是构成破坏计算机信息系统罪。

在网络反向炒信刷单案中，董某等人通过虚假交易，严重影响到受害公司的正常经营活动，但并没有任何财物受到毁坏。南京中院二审认为，上诉人董某等人具有报复及从中获利的主观目的，客观上实施了通过损害他人商业信誉的方式破坏生产经营的行为，实际造成被害单位 10 万余元的经济损失，而且上诉人的行为与财产损失之间具有因果关系，其行为符合破坏生产经营罪的构成要件，应以破坏生产经营罪定罪处罚。在此，二审判决认定，在本案中董某等人破坏生产经营罪的“其他方法”表现为“损害他人商业信誉。”显然，商业信誉并不是财物，不可能成为毁坏型财产犯罪的侵害客体。笔者认为，本案属于妨害业务行为，而我国目前刑法中妨害业务罪的立法缺失，导致对于这种行为不具有处罚根据。

值得注意的是，我国学者从刑法解释与时俱进的角度提出了肯定性的解释结论，认为将破坏生产经营罪中的“其他方法”的对象限定于与机器设备、耕畜类似的生产资料，将行为方式限定于暴力、物理性的破坏方式，这完全是停留于农耕社会和机器工业时代的固有思维和解释水平，不能适应如今以第三产业为主体的后工业社会和网络时代的要求。这些学者认为，“其他方法”并不限于破坏工农业生产资料，而是只要危害行为侵犯了生产经营者基于生产经营的利益，就可以认为是“其他方法”。这是一种客观主义的解释立场，不同于主观主义的解释立场。我国刑法理论和司法实践中一般都坚持这种客观解释论，对此并没有问题。问题在于：如何限定刑法解释的边界？周光权教授将这种解释称之为软性解释，并将其归结为类推解释，指出：如果不考虑刑法客观解释的限度，破坏生产经营罪势必会沦为口袋罪。反向刷单客观上会造成竞争对手的损失，但被告人的行为手段是损害他人的商业信誉和商品声誉，而不是故意毁坏他人的生产资料。换言之，反向刷单的手段行为并不符合破坏生产经营罪的客观构成要件，对其行为在刑法增设妨害业务罪这一新罪之前，按照《网络交易管理办法》（2014 年 1 月 26 日原国家工商行政管理总局颁布）第 19 条第 4 项的规定，网络商品经营者、有关服务经营者销售商品或者服务，不得利用网络技术手段或者载体等方式，以虚构交易、删除不利评价等形式，为自己或他人提升商业信誉，因此对该类行为处以行政处罚可能更为合适。对于这种观点，笔者是完全赞同的。虽然刑法对破坏生产经营罪设置了“其他方法”的兜底式规定，但并不意味着这里的“其他方法”可以不受任何限制。否则，就会违反罪刑法定原则。

（三）恶意注册虚假账号的利用行为是否构成非法利用信息网络罪？

恶意注册虚假账号的利用行为可以分为两种：第一种是营利活动，例如褥羊毛，即不以正常消费为目的，将获取优惠卡券作为牟利途径，通过机器批量获取的方式，在短时间内大量囤积优惠券，再高价倒卖给需要优惠券的用户赚取差价获利。第二种是违法犯罪活动，例如黑产人员注册利用大量非实名帐号，冒充特定身份，购买公民个人信息，精准定位目标人群，使用自动化工具添加好友，编造话术和剧本，对被害人实施精准诈骗。当黑产人员利用恶意注册的账号从事诈骗等违法犯罪活动的时候，就存在其行为是否构成非法利用信息网络罪的问题。

根据我国《刑法》第 287 条之一的规定，非法利用信息网络罪是指将利用信息网络实施下列行为之一，情节严重的情形：①设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；②发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；③为实施诈骗等违法犯罪活

动发布信息的。从上述规定可知，我国刑法中的非法利用信息网络罪，是利用网络实施某种犯罪。例如《刑法》第 287 条之一所列举的诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪、毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪、诈骗等违法犯罪。这实际上是将这些犯罪的预备行为规定为犯罪。因此，恶意注册行为能否构成非法利用信息网络罪，关键问题在于对利用行为的违法犯罪性质的判断。

文章六、新型网络犯罪涌现详细情况 新型网络犯罪涌现套路一览

据中国之声《新闻晚高峰》报道，“京医通”是网上就医挂号平台，但是不少人都反映，部分知名医院的号源一放出就被“秒抢”，总也挂不上号。还有人反映，自己在网上明明加入的是网聊群，但是却被教唆自杀和他杀……这些事情听起来匪夷所思，但它们就发生在我们身边——这是公安部最新发布的一批新型网络犯罪典型案例。

面对不断涌现的新型网络犯罪形式，普通公众应该如何保障自身权益，避免上当受骗？公安部门又将会采取什么样的措施来保障人民群众的安全？

去年 12 月，北京公安机关网安部门接到群众报案，“京医通”挂号平台中北京部分知名医院号源一经放出即被“秒抢”，患者无法通过此渠道正常挂号。公安部网络安全保卫局副局长张宏业介绍：“网上非法屯号、恶意抢号等违法犯罪活动猖獗，违法犯罪人员利用患者求医心切的心理，非法制作恶意软件抢占各大医院专家号源，再高价倒卖牟取非法利益。”

经侦查，今年 1 月 10 日，专案组在北京、河南、山西、云南等地将高某等 4 名主要犯罪嫌疑人抓获。4 月 15 日，又在广东揭阳将非法制作、传播该恶意软件的某软件公司负责人李某某等 4 名犯罪嫌疑人抓获。北京市公安局网安总队案件侦查支队副支队长郑浩表示，北京公安机关网安部门持续对网络挂号环境进行监测，发现恶意抢占号源的情况有所缓解：“下一步，北京公安机关网安部门将继续会同北京市卫健委及"京医通"挂号平台加强合作，对网上非法屯号、恶意抢号并牟利的行为开展持续打击，维护正常的网上挂号秩序。”

今年 2 月，浙江嘉兴公安机关网安部门在工作中发现，一名河北网民李某在网上雇佣贵州网民赖某前往河北省廊坊市文安县预谋杀害一名男子。经侦查，赖某已经到达文安县并伺机作案。河北廊坊公安机关网安部门迅速查明李某、赖某 2 人活动轨迹，于 2 月 25 日凌晨将 2 人成功抓获。

浙江省公安厅网安总队副总队长黄海涛介绍，这一案例是典型的网络相约暴力犯罪，重要特征之一是团伙成员往往之前互不相识：“这一类案件当中，从嫌疑人的招募到进行案件的作案策划，包括他们聚集以及犯罪工具的一些准备，都是依赖于互联网。作案以后又马上散伙，甚至有些案件当中通过互联网来进行销赃。”

分析过往案件，嫌疑人还具备一定反侦查意识，作案对象主要是反抗能力比较弱的女性及经济能力较强的企业老板。

不仅如此，近年来，一些有自杀倾向人员也通过网络社交平台相识，相约共赴特定地点集体自杀的事件也屡有发生。张宏业表示，当前，网约犯罪人员呈现年轻化趋势：“尤其是一些心智不成熟、易冲动的年轻人由于赌博等原因欠下大额外债，滋生犯罪念头。犯罪分子多在网上联络交易，策划实施犯罪方案、细节，目标明确，作案迅速，严重破坏社会公共安全和人民群众生命财产安全，影响十分恶劣。”

根据介绍，截至今年 5 月，仅浙江公安机关网安部门就向全国推送网约犯罪线索 215 条，破获严重暴力刑事案件 101 起；推送网约自杀线索 88 条，及时挽救自杀人员 152 名。

张宏业介绍，当前，传统违法犯罪正加速向以电信、互联网等为媒介的非接触性犯罪转移，借助网络的新型犯罪日益增多。公安机关提醒广大群众，要树立合法上网意识，面对网上各类违法犯罪信息一定要提高警惕。公安机关也将在全国范围内继续组织开展“净网

2019”专项行动，对网上违法犯罪活动始终保持严打高压态势。

张宏业表示：“加大对为电信网络诈骗、网络赌博等违法犯罪活动提供公民个人信息或资金支付结算帮助等黑色产业链条的打击力度，加强对网上相约实施暴力犯罪的预警和处置工作，坚决遏制网上违法犯罪滋生、蔓延势头。”（记者李欣）

文章七、网络直播平台犯罪

中国报告网指出：截止 2019 年，我国直播用户数量达 5.07 亿，播主们全年礼物收入超过 500 亿。这个数字相当于五粮液集团 2019 年全年的收入。在网传的主播收入排行榜中，李佳琦、冯提莫、PDD 等人年收入均高于 1 亿元，而福布斯公布的 2019 中国明星收入排行榜“天王”刘德华年收入为 8900 万。

可见，随着技术变革的到来，5G 时代、可穿戴设备、物联网、人工智能.....直播行业的发展越来越快。但是任何新事物也逃不过“十祸九快”这一哲理，原因是近年来有关主播涉黄、涉赌、涉毒、涉骗、涉假的违法犯罪行为层出不穷，播主们的一言一行通过网络不断放大和效仿，以至于网络监管部门也措手不及，不断地通过颁发《办法》《规定》来填补新行业的法律漏洞。

“打铁还需自身硬，无须扬鞭自奋蹄”，层出不穷的违法犯罪问题，除了监管不力，更多的主播们认为网络乃是“法外之地”，或者以言论自由、个人隐私来“掩耳盗铃”。所以，做一名杜绝歪风邪气的“良心”主播，既要不断提升品格素质，更要提高法律意识，结合本文揭示的几种常见刑事风险，引起足够重视。

一、涉黄犯罪

1.行为模式

一些网络主播为了快速获得观众们的“欢心”，聊着“情感夜话”、“悲惨经历”、“生活日记”等，或者偶尔展露自己“迷人”的身姿吸粉。有的网络主播穿着暴露，聊着“黄段子”打法律的“擦边球”。有的手段更是简单粗暴，有意无意中来个“一脱成名”。甚至彻底放弃了自己的底线，通过与“家族长”、“公会会长”联络，再由其推荐到涉黄直播平台上，只要看客们肯“打赏”，就会无所不为。有些主播认为直播的内容只要不被平台“超管”点名提醒，即是“合理合法”。有些主播认为即便“涉黄”吃亏的也是自己，怎么会跟犯罪扯上关系？

2.涉嫌罪名

（1）传播淫秽物品牟利罪。根据刑法第三百六十三条的规定，以牟利为目的，制作、复制、出版、贩卖、传播淫秽物品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金；情节特别严重的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

（2）组织淫秽表演罪。根据刑法第三百六十五条的规定，组织进行淫秽表演的，处三年以下有期徒刑拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金。

3.举例解读

（1）2016 年，网络直播圈的“当红女主播”林某，21 岁，网名“雪梨枪”，伙同另外两男一女，录制了“成都 4P”淫秽视频。经查实，林某以牟利为目的，利用互联网、移动通讯终端等制作、传播淫秽视频共计 31 部，注册会员达 1100 人以上，获利达七万五千余元。林某的行为已构成制造、传播淫秽物品牟利罪，被判处有期徒刑和巨额罚金。

除“雪梨枪”外，至今各网络平台上依然充斥着知名主播、红人卖照、卖视频的现象。殊不知根据我国的司法解释，通过制作、传播淫秽物品牟利，金额达到 1 万元以上就构成了

犯罪；即便没有谋取利益，只要传播面达到了 200 人以上也会构成犯罪。

（2）2017 年，张某、夏某二人通过在直播时发广告的方式，宣扬加微信并发送红包后即可加入 QQ 群观看淫秽直播，收取会员费后，二人通过在线视频方式，供群内网友观看其正在实施的性交等淫秽行为。三个月内先后组织 90 余人进群观看，非法获利 12000 余元。由于其二人以牟利为目的，通过网络招揽顾客在线观看，既是表演者亦是组织者，达到了在网络这个公众空间内的群体观影氛围，与现实中面对面的表演没有任何差别，属于直播时代的新型“组织”方式，最终被法院以组织淫秽表演罪判处刑罚和罚金。

根据法律规定，淫秽物品是指传播淫秽信息的固定载体，可反复观看。所以在线直播停止后，不存在反复观看性和被不特定的多数人获取的可能，但是主播的行为却有可能涉嫌组织淫秽表演罪。此外，在网络时代下“组织”还体现在主播参与违法平台后，除了扮演表演者外，还会在巨额分红利益的驱使下成为平台“家族长”，招募更多主播参与其中，如 2019 年“一点直播”平台淫秽表演一案，众多“家族长”与表演者均被判处有期徒刑和罚金。

二、涉赌犯罪

1.行为模式

违法赌博平台用“超高提成、专题曝光机会、首秀人气捧场”等诱人广告招募主播，再用低俗、色情的广告放到不同 APP 里做引流，吸引顾客前来。其中两种常见模式，一是利用平台充值功能，让顾客以“中奖”的方式获得倍数“筹码”，然后通过主播提现；二是利用主播做“荷官”，引导观众参与游玩赌博游戏，并刺激观众消费，最终通过主播将“筹码”提现。

2.涉嫌罪名

开设赌场罪，根据刑法第三百零三第二款的规定，开设赌场的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金。

3.举例解读

2019 年，董某在某平台观看主播“才艺”表演时，被告知可以和主播一起互动玩猜颜色的游戏，通过给主播“刷礼物”兑换游戏币，之后还可以通过给主播“刷礼物”后，主播微信转账的方式将游戏币提现。董某小赢了几把后，在主播的娇声鼓励下，筹码越压越大，一下午输了 10 万元，后陆续几天共损失 80 多万。董某报警，主播也难逃法网，最终成为开设赌场罪的共犯。

我国法律规定，以营利为目的，利用互联网直播平台开设赌场，最高可判十年有期徒刑。而主播明知是赌博平台，为其提供服务，领取薪酬、参与分成，承办赌资的变现支付服务属于共犯。

三、涉毒犯罪

1.行为模式

网络主播直播吸毒、贩毒的时代已经过去了，这种行为涉嫌构成贩卖毒品罪或非法持有毒品罪，所以一经举报，主播难逃法网。现在更多的不法分子为牟利，雇佣“技术型”人才架设平台，招募有“才艺”的主播在各种社交网络中为平台“打广告”，吸引“瘾君子”前来加入，打造“庇护所”，然后提供给其需要充值升级会员的各项服务以此牟利，比如高等会员买卖毒品的渠道更广。这种模式下的主播们并不吸毒、贩毒，怎么又涉嫌犯罪了呢？

2.涉嫌罪名

非法利用信息网络罪，根据刑法第二百八十七条之一的规定，利用信息网络实施下列行为之一，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：（一）设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；（二）发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；（三）为实施诈骗等违法犯罪活动发布信息的。

3.举例解读

2017 年，徐某开始吸食毒品，迷恋上了吸毒时听着刺激的音乐，和女性聊着天等方式，两年后徐某租服务器，架设吸毒直播平台，并邀请众多主播当陪聊，供他们在直播吸毒时活跃氛围，组织群吸活动。还提拔主播们做管理员，以高额提成利诱主播在网络中积极发展“毒友”加入平台，接着通过视频验证的方式保证“毒友”们身份真实。“毒友”越来越多，还可在平台相互买卖毒品。最终徐某和某主播们犯非法利用信息网络罪，被法院判处有期徒刑并处高额罚金。

根据 2019 年最新的司法解释规定，发布信息包括利用信息网络提供信息的链接、截屏、二维码、访问账号密码及其他指引访问服务的行为。在网站上发布有关信息一百条以上的、向二千个以上用户账号发送有关信息的、向群组成员数累计达到三千以上的通讯群组发送有关信息的、利用关注人员账号数累计达到三万以上的社交网络传播有关信息的，都有可能被认定为“情节严重”的行为。所以，主播们充当管理员的角色积极发展“毒友”，设立非法平台的通讯群组，发布暗含“黑话”的违法信息，便会涉嫌非法利用信息网络罪这一新的罪名。

四、涉骗犯罪

1.行为模式

网络中常见的模式有三种：一是“只闻其声不见其人”，“乔碧萝”事件就是典型的代表；二是“无中生有型”，平台、主播、销售员在统一的话术培训下，销售员以女主播私人账号为名，以诱惑性文字、语音、照片、视频等与被害人“谈恋爱”，被害人到直播间见到主播后深信不疑，销售员接着冒充女主播引诱被害人“刷礼物”并许诺与其“奔现”等；三是“空手套白狼”，招募客服，男女均可，在网络中四处“拉客”，被害人至诱惑性平台后，以录像代替直播，要求其必须充钱才能进一步观看，充钱后又以技术故障等理由继续骗取财物。

2.涉嫌罪名

诈骗罪，根据刑法第二百六十六条规定，诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

3.举例解读

（1）“乔碧萝殿下”，因其在直播中遮脸的卡通图像掉落，引发“萝莉变大妈”的热议，一名给她“打赏”了 10 万余元礼物的粉丝愤怒的注销了自己的账号。“乔碧萝”的行为，假装“美少女”引诱观众给她送礼，观众基于对“美少女”的幻想，处分了自己的财物，确实可能涉嫌诈骗犯罪。这个例子提醒主播们切莫以“技术手段”欺骗观众，除非“分文不取”，否则“收礼”过多，侵犯诈骗罪所保护的“财产性利益”，一样会令自己身陷险境。

（2）2019 年烟台警方破获的特大网络直播平台（星海直播）诈骗案，抓获了 225 名犯罪嫌疑人，涉案金额 2000 万元以上。此平台采用的就是“无中生有”模式的骗术，这种模式下主播成为了诈骗罪的共犯。诈骗金额在 2000 元以上就达到了立案标准，金额在 50 万以上可能被判处无期徒刑。在如今一个“礼物”就动辄几万元的直播时代中，主播无论参与何种模式的骗术，违法的贪念有多重，刑罚就有多重。

五、涉假犯罪

1.行为模式

一名不涉“黄”“赌”“毒”“骗”的守法主播，吸金的潜力又有多大呢？今年的愚人节刷新了所有人对带货能力的想象。那就是薇娅直播“卖火箭”，并且最终以 4000 万元的价格成交了“火箭”的发射服务。带货宣传的回报高，一般能达到产品销售额的 20%，所以

“万物皆可直播，直播就能带货”。但在直播带货过程中，如果对商品不加辨别，对宣传夸大其词，仍然存在刑事风险。

2.涉嫌罪名

（1）生产、销售假药罪，根据刑法第一百四十一条的规定，本罪是指生产者、销售者违反国家药品管理法规，生产、销售假药，足以危害人体健康的行为。

（2）生产、销售伪劣商品罪，根据刑法第一百四十条的规定，本罪是指生产者、销售者在产品中掺杂、掺假，以假充真，以次充好或者以不合格产品冒充合格产品。

（3）虚假广告罪，根据《中华人民共和国刑法》第二百二十二条规定，本罪是指广告主、广告经营者、广告发布者违反国家规定，利用广告对商品或服务作虚假宣传，情节严重的行为。

3.举例解读

（1）2016 年，赵本山的徒弟“胖丫”赵丹在未经取得药品生产、销售许可的情况下，与郭静、王爽通过映客直播、微信等网络平台宣传“纯中药减肥胶囊”，称该减肥药为老中医独门配方、纯中药、无副作用。而有些用户吃完后，导致心脏病、急性荨麻疹，最终赵丹犯生产、销售假药罪被判处有期徒刑并处罚金（该罪与虚假广告罪想象竞合，司法实践中从一重罪判处）。

如果可销售的商品遵守相关法律规定，那是否意味着只要产品无违法，就可以肆无忌惮的通过直播做广告了呢？答案还是否定的。网络直播者带货直播的过程中，因其对广告内容有支配力，也会被认定为广告经营者，符合此罪对主体资格的要求，所以存在虚假广告的风险，此时故意虚假宣传，将会涉嫌犯罪。

（2）2019 年，口红达人李佳琦在与炊大王（炊具公司）直播推广中，宣传一款不粘锅，结果实际放入鸡蛋后却未奏效，不粘锅最终还是粘锅了。此事过后，又在直播销售“阳澄状元蟹”时，将不是产自阳澄湖的螃蟹介绍为“阳澄湖大闸蟹”。另外，还宣传该品牌是“23 年老品牌”，结果却被扒出“阳澄状元蟹”所属公司是一家仅成立 4 年的新公司。

这两件事由于未产生严重后果，且主播工作室及时采取补救措施，没有达到犯罪的程度，但其虚假宣传的行为，依然可以给所有主播提个醒。虚假广告罪的追诉标准一般看消费者的实际损失与是否造成严重后果等，在如今网络直播的高速传播下，损失后果将更难以预估和控制。

最后，直播行业的刑事风险还远不止本文罗列的几种，比如某主播在军事营区直播，涉嫌危害国家安全的罪名；某直播宣扬恐怖主义等内容，将涉嫌恐怖活动犯罪、以危险方法危害公共安全罪等；根据司法解释，网络空间也可认定为公共场所，在网上“信口开河”引发骚乱，还会涉嫌寻衅滋事等犯罪。

当然，直播行业乱象丛生，不光是直播者的责任，更是直播平台与监管部门的责任。比如在国家公祭日当天，爱奇艺旗下奇秀直播平台上演涉黄事件，爱奇艺事后选择午夜道歉辩称是技术原因。所以即便作为知名视频平台，法律意识尚且如此淡薄，对于网络直播者来说，更要时刻注意着悬在头顶上的“刑罚利刃”，认清犯罪的行为特征，洁身自好才能走的更长远。

文章八、网络直播刑事风险的制裁逻辑

摘要

当前网络直播乱象频生，政府监管与行业自治收效有限。《互联网直播服务管理规定》《网络安全法》《网络表演经营活动管理办法》的相继颁行意义显著。网络直播裹挟大量刑事风险，网络主播、直播平台、监管部门、用户均是危险制造者。应根据主播的直播内容与

形式、直播平台的法定网络安全管理义务、网络监管部门的法定监管职责、用户的参与形式，确定各方的刑事责任范围与制裁边界。网络直播牵扯出网络平台犯罪问题，应树立积极预防、必要的刑罚处罚思维并启用认罪认罚从宽制度，依法确认网络平台的新型犯罪主体地位并增设专门的网络罪名，有序推动网络刑法体系的知识变革，以整体上解决网络犯罪的挑战。

互联网时代加速新型网络消费时代的到来，以网络表演等为内核的互联网直播成为时代的弄潮儿，但也是网络技术异化风险的携带源与传播体。日益失范的涉黄、涉暴、涉淫秽等违规违法直播现象层出不穷，持续制造刑法不能容忍的高度风险。当前，各方高度重视网络直播风险的治理，主要包括加强网络直播监管与行业自治两方面。但是，由网络直播衍生的法律风险仍高位运行，刑事风险的异化速度攀升难止。审视当前相关的法律法规等规范性文件，仍未解决适法不明问题，导致直播平台运营不规范、主播“擦边球”、监管主体失职等行为的刑事责任边界模糊，也拷问刑法制度的“买单”能力。

在全民直播时代，既不能以牺牲网络自由创新为代价换得网络的片刻安宁，扼杀网络技术的转化与创新也不应毫无底线地一味克制，纵容网络直播风险的泛滥，危及网络安全法益。《互联网直播服务管理规定》（2016 年 11 月，网信办）、《网络安全法》（2016 年 11 月，全国人大常委会）、《网络表演经营活动管理办法》（2016 年 12 月，文化部）相继发布。既宣告全面依法治理网络直播现象的决心，也为防控刑事风险和追究刑事责任提供新依据。其中，如何有效地应对网络平台这一新型犯罪主体成为当前的重要任务。

一

网络直播刑事风险的类型

网络直播是网络技术与网络商业模式的创新典范，但直播平台管理疲软、直播主体自治不足、网络监管乏力等，共同导致网络直播进入疯狂的野蛮生长期。网络直播刑事风险高居不下，主播、直播平台、监管部门、广大用户均涉其中。

（一）网络主播引发的刑事风险

《互联网直播服务管理规定》二条第二款规定，互联网直播服务使用者，包括互联网直播发布者和用户。网络主播作为网络直播产业衍生而来的新型职业群体，是最重要的网络直播服务使用者暨发布者，也是网络直播风险的首要隐患，并往往是女性。当前，网络主播的违规违法直播行为大体包括两类：

（1）相对轻微的失范行为。如穿着暴露、举止轻佻、言行低俗、直播“自杀”过程、擅入校园宿舍直播等。这类直播往往超越道德与社会伦理底线，甚至扰乱社会公共秩序。

（2）严重的失范行为或违法犯罪行为，可能需要承担行政责任与刑事责任。包括直播“造人”、直播淫秽活动、直播聚众吸毒、直播强奸过程等。比如，全国“扫黄打非”办公室已严肃处理“直播造人”事件，并追究了责任人员的法律责任。但是，对于大多数的严重失范行为，受制于“法不责众”的传统观念、广大网民的“助推”效应、刑法规定阙如等消极因素，仍难以追究网络主播的刑事责任。

网络直播平台是公众平台，维系信息网络安全。网络主播是直播平台的核心人物，是直播平台的信息源与数据池，往往成为网络直播刑事风险的首要来源。网络主播严重违规违法直播，不仅扰乱网络空间的社会管理秩序和公共场所秩序，往往波及现实物理社会秩序，引发以下刑事风险：

（1）破坏网络空间社会的信息安全、网络空间社会秩序或网络空间场所公共秩序。

（2）引发现实物理社会的关联性危险或危害。

（3）原则上可能破坏所有传统刑法法益或新型网络安全对应的刑法法益，具体由直播内容、受众对象、直播形式及时间、地点等因素决定。

（二）网络直播平台裹挟的刑事风险

根据《网络表演经营活动管理办法》二条第二、三款，《互联网直播服务管理规定》二

条第二款的规定，互联网直播服务提供者是指提供互联网直播平台服务与网络表演经营活动的主体。在网络直播的商业运行模式中，直播平台与主播利益互绑，为网络直播提供网络技术支撑。直播平台往往采取事后补救管理，而内部管理往往流于形式，平台管理失位与缺位成为诱发直播风险的重要内因。

按照《网络安全法》《网络表演经营活动管理办法》《互联网直播服务管理规定》的相关规定，直播平台作为网络服务提供商负有法定的网络安全管理义务，应当承担安全管理的主体责任。目前，直播平台的内部审查不力与管理缺位，往往成为直播风险的主要来源。对此，全国“扫黄打非”办公室负责人强调，“净网 2016”行动专项整治网络直播平台，追究违法平台主体的刑事责任。

网络直播平台是新型的公众媒体平台，具有高度的网络主体聚合性，制造的风险具有广泛性、蔓延性等特征。其风险主要包括：

（1）危害直播空间的公共管理秩序，直接或间接影响现实物理社会及用户的消费权益与公共秩序。

（2）直播平台不履行或故意违反网络安全（信息）管理义务，将危害网络直播平台的正常运行秩序、经营活动，侵犯用户的合法权益。

（3）网络直播平台的运营基础与核心是网络系统安全，网络直播平台的运行安全、信息网络安全，尤其是数据安全与用户个人信息安全都可能成为被害对象。

（4）网络直播平台是互联网经济的新兴方式，网络平台为了获取竞争优势和市场份额，可能实施非法干扰、排挤竞争等破坏正常经营的不正当竞争行为，可能引发网络直播产业的重大市场风险。因此，网络直播平台可能制造网络运行风险、网络经营秩序风险、网络空间秩序及管理风险等。

（三）网络安全监管部门制造的刑事风险

《网络安全法》八条、《互联网直播服务管理规定》四条第一款、《网络表演经营活动管理办法》十七条与第十八条，先后分别对网络安全监管部门及其监管职责作出相应的规定，逐步扭转了之前“九龙治水”的监管局面。

网络安全监管部门也是制造刑事风险的重要源头之一。主要包括：

（1）国家网络安全风险。网络安全事关国家安全战略，是国家主权的重要内容。网络监管部门是制定网络空间行为规范准则的合法主体，是指导网络空间自治的官方机构，是维护网络安全的国家力量，是防控直播风险的基础防线。监管缺位是国家网络安全、网络主权及数据主权风险的重大隐患。

（2）监管渎职风险。网络安全监管部门及其负责人或主要责任人员渎职的，包括滥用职权、玩忽职守与违反其他法定职责的，可能导致网络直播平台陷入失控无序的危险状态。

（3）共同制造风险。监管部门的工作人员利用工作之便或职务上的便利，教唆、组织、帮助或参与网络直播平台的违法犯罪活动的，直接制造多重的网络直播刑事风险。

（四）网络用户诱发的刑事风险

网络直播平台乱象频发，庞大的网络用户作为“看客”，不能全身而退。网络直播具有高度的互动性与公众参与性，用户购买是网络直播平台营销模式的基本保障，用户消费的偏好客观上主导网络直播平台的内容及形式。用户抵制是最好、最廉价的社会抗衡制度与措施，直接从源头切断诱发网络直播风险的外部不良因素。

网民参与网络直播，可能诱发以下刑事风险：

（1）“犯因”风险。对于网络直播行为失范，甚至变成违法犯罪活动，尽管直播平台、主播与监管部门难辞其咎，但网络消费受众的低俗化、媚俗化、庸俗化、快餐化等不良文化与社会风气，是最终的“买单者”。

（2）参与风险。网络消费者作为整体无须承担法律责任，但并不必然排除个别或不特

定的多数人作为消费者应当承担责任。比如，网民实施网络起哄闹事、网络侮辱诽谤、网络聚众、网络敲诈勒索等现象屡禁不止，作为组织者、策划者、领导者、积极参与者，是刑事风险的促发者与制造者。

二

网络直播中的刑事责任厘清

不能置网络直播现象于“法外空间”，更不能纵容网络直播的刑事风险处于“无法无天”状态。尽管传统刑法理论和立法规范深陷有效性困境，但是仍应根据网络直播的相关主体及其行为，明确网络直播各方的刑事责任类型、存在范围及制裁边界。

（一）网络主播的刑事责任范围

应根据网络主播的具体直播行为，比照现行法律，明确不同行为对应的刑事责任清单。

1.主要的直播危害行为

根据违规违法网络直播的现状，主要的危害行为包括：

（1）直播色情或极端不雅行为。目前，有关色情的法律定义与法律责任等不够明确，特别是对儿童色情制品及其处罚缺乏具体规定，导致网络主播借色情“噱头”频打“擦边球”的行为层出不穷，网络不雅，低俗风气充斥其中。在实践中，已有公安机关将直播色情内容的行为按照传播淫秽物品牟利罪的做法，事实上意味着采取了扩张解释，将网络直播平台与直播中的色情行为，与现实物理社会中的淫秽物品等同。

但有观点认为，直播过程中的动作、语言等并不必然是固定的有形载体，即使包含淫秽内容或淫秽场景，却很难认为是传播淫秽物品；否则，犯罪主体在传播淫秽物品时，竟然以自己及色情行为作为犯罪对象，与传统刑法理论存在尴尬的一面。但直播平台是网络社会的公共空间，网络直播平台聚集庞大的网民，信息共享与传播速度极快，与现实物理社会高度链接，危害丝毫不减，利用网络平台直播色情行为，情节严重，应当追究刑事责任，理由为：

一是直播色情和极端不雅行为，可能涉嫌构成寻衅滋事罪。根据《刑法》二百九十三条第四款、《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》五条第二款、《关于办理寻衅滋事刑事案件适用法律若干问题的解释》五条的规定，公共场所不限于现实物理空间，已经延伸到网络空间。信息网络空间与现实物理空间并无差异，在网络空间实施犯罪，造成公共场所秩序严重混乱，应承担刑事责任。

二是直播色情行为严重破坏直播平台与现实物理社会的公共秩序与善良风俗，导致公共空间发生混乱，情节严重的，可以按照传播淫秽物品牟利罪、组织播放淫秽物品罪等处罚。但《治安管理处罚法》与“网络内容分级办法”应明确网络色情行为或极端不雅行为具有违法性。

（2）直播淫秽表演。当前，利用直播平台直播淫秽表演屡禁不止。通过信息网络播放淫秽物品及音像制品的，主要可能涉嫌构成《刑法》三百六十四条规定的传播淫秽物品牟利罪、传播淫秽物品罪、组织播放淫秽音像制品罪与第三百六十五条规定的组织淫秽表演罪。司法机关应当采取扩张解释，将传统物理空间社会扩大到网络空间社会，并可以不区分组织者、网络技术的支持者与帮助者的主、从犯关系，追究刑事责任。但主播单独实施淫秽直播表演的，按照传播淫秽物品罪论处仍显牵强，因为单独的网络真人直播行为不是传统的静态“淫秽物品”，除非采取扩张解释，将网络空间的直播表演行为认定为“动态”的淫秽物品。

（3）涉未成年的猥亵性直播。“注意力经济”已经开始渗透于未成年人群体，未成年可能牵扯直播。通常认为，猥亵是指除奸淫以外的能够满足性欲和性刺激的有伤风化、损害人性心理、性观念，有碍身心健康的性侵犯行为。从解释学看，面向未成年人的涉色情或不雅直播行为是否属于“猥亵”确有争议。《网络表演经营活动管理办法》七条规定，网络表演经营单位应当加强对未成年人的保护，有未成年人参与的网络表演，不得侵犯未成年人权益。

因此，“猥亵”的刑法含义应当与社会文化观念保持同步。比如，《刑法修正案（九）》将二百三十七条的猥亵“妇女”修改为猥亵“他人”，扩大猥亵的犯罪对象，体现性文化与性观念的时代变迁。“立法者的任务不是建立某种特定的秩序，而只是创造一些条件，在这些条件下，一个有序的安排得以自生自发地建构起来，并得以不断地重构。”从侧重保护未成年的政策导向和直播内容分级制度等看，对明显属于向未成年人传播色情信息或实施具有猥亵性质的语言、举止等不雅行为的，网络直播平台明显属于“当众”，情节严重的，可能涉嫌构成猥亵儿童罪。造成轻伤以上危害结果的，依照处罚较重的规定处罚；直播有关淫乱活动、吸毒等违法犯罪活动的，同时涉及未成年人的，可能涉嫌构成引诱未成年人聚众淫乱罪、引诱他人吸毒罪等；教唆、组织、聚众参与或提供技术帮助的，应按照共犯形态论处。

（4）直播虚假广告。在互联网经济背景下，利用网络直播进行宣传往往可以起到更好的效果。当前，利用网络直播发布各类型广告不胜枚举，但大量网络虚假宣传也夹杂其中，严重威胁直播平台的信息安全和现实物理社会的秩序。根据《广告法》（2015 年修订）、《互联网广告管理暂行办法》（2016 年）的规定，主播利用直播平台发布虚假广告的，具有传播范围大、受体人数多、影响恶劣等情形或造成严重危害结果的，目前应以虚假广告罪追究网络主播的刑事责任。今后应考虑对虚假广告罪进行网络化修正。

（5）其他严重失范直播。《网络表演经营活动管理办法》六条规定禁止表演的内容，包括表演方式恐怖、残忍、暴力、低俗等多种情形。对游走于法律边缘的严重失范直播行为，在确定刑事制裁边界时，应当注意三点：一是援引寻衅滋事罪等罪名，容易落入“口袋罪”的指责，制裁的边界容易失控；但一律放任不管，类似行为将发生甚至加码，危险不断增大。二是第二百八十七条之一的客观行为主要是发布违法犯罪（活动）信息或为实施违法犯罪活动发布信息，与严重直播失范行为相比有本质差异，使该条规制的针对性不强。三是第二百八十七条之二可以制裁主播实施帮助信息网络犯罪活动的行为，但需情节严重。在实践中，应根据直播内容及其形式作出实质判断，关键看刑事制裁是否必要和有效。

2.主要的刑事责任类型

根据网络主播的行为及其内容，可能承担的刑事责任类型主要包括：

（1）破坏网络直播空间公共秩序与社会管理秩序的，情节严重的，可能涉及聚众扰乱社会秩序罪、寻衅滋事罪、传授犯罪方法罪、聚众淫乱罪、引诱未成年人聚众淫乱罪、开设赌场罪、传播淫秽物品罪、组织播放淫秽音像制品罪、组织淫秽表演罪等罪名。

（2）网络直播宣扬恐怖主义、极端主义以及恐怖活动的，严重危害公共安全或国家安全的，可能构成恐怖活动犯罪、以危险方法危害公共安全罪等罪名。

（3）侵犯公民人身权利、民主权利的，涉嫌罪名由直播内容等因素决定，如网络诽谤情形；教唆、帮助或参与实施的，应当承担共犯责任。

（4）利用直播平台发布违法犯罪活动信息或利用直播形式作为违法犯罪活动的网站及通讯群组的，可以援引第二百八十七条之一，追究非法利用信息网络行为的正犯责任。

（5）其他罪名。网络主播的直播可能侵犯所有的刑法法益内容，包括国家安全、军事利益、公共安全、社会主义市场经济秩序与社会管理秩序等法益。比如，网络直播与著作权息息相关，直播可能侵犯《信息网络传播权保护条例》《著作权法》规定的网络信息传播权，涉嫌构成侵犯著作权罪。

（二）直播平台的刑事责任边界

网络直播行业主要面临直播产品很新、主播行为不可控、用户参与方式跨度大等难题。但《互联网直播服务管理规定》、《网络安全法》均规定网络直播服务提供者负有法定的网络安全管理义务，直播平台难以推卸其相应的刑事责任。

1.网络安全管理义务是归责前提

现行法律规定，网络直播平台是服务提供商，负有法定的网络安全管理义务，择要而言：

（1）《网络安全法》。第十条、第三章“网络运行安全”、第四章“网络信息安全”、第五章“监测预警与应急处理”规定，直播平台负有“防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性”、“立即停止传输该信息，停止提供服务，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告”等内容审查、信息安全保护等法定的义务。第四十三条、第四十七条、第四十八条、第五十条规定，网络运营者、电子信息发送服务提供者、应用软件下载服务提供者等发现禁止发布或者传输的信息的，负有保存或要求保存有关记录的义务或职责。《网络安全法》对网络服务提供商的法定义务作出最新的概况性规定。

（2）《互联网直播服务管理规定》。第十四条规定，互联网直播服务提供者应对违反法律法规和服务协议的互联网直播服务使用者，视情形采取警示、暂停发布、关闭账号等处置措施，及时消除违法违规直播信息内容，保存记录并向有关主管部门报告。第十五条规定，应建立互联网直播发布者信用等级管理体系，建立黑名单管理制度，并执行相应的惩戒措施。第十六条规定，应记录互联网直播服务使用者发布内容和日志信息，保存六十日。这为网络直播平台提供了服务、规定了更具体的义务。

（3）《网络表演经营活动管理办法》。第三条规定，从事网络表演经营活动，应遵守宪法和有关法律法规。第五条规定，应对本单位开展的网络表演经营活动承担主体责任，建立健全内容审核管理制度，配备满足自审需要并取得相应资质的审核人员，建立适应内容管理需要的技术监管措施。这也为网络直播平台设置法定的义务。

2.主要的刑事责任类型

网络直播平台违反国家规定的法定义务，可能构成普通犯罪、不作为犯罪、重大管理（监督）过失犯罪等形态，大致包括：

（1）共犯责任。直播平台与主播或用户存在共同犯罪的意思联络，明知违反网络安全管理义务，仍积极提供直播平台技术服务或采取放任不管的态度，不采取网络切断、取消主播资格、关闭直播间等必要的安全措施，参与和帮助他人实施犯罪，甚至从中获利，直播平台应当承担共同犯罪的责任。但在追究共犯责任时，共犯从属性理论、共犯故意的认定等难题，使司法运行并不理想。

（2）不作为责任。网络直播平台作为网络服务提供商负有法定的信息网络安全管理义务，应当具备相应的网络安全管理能力和应急条件。根据第二百八十六条之一的规定，在可以积极预防和控制危险因素或危害结果发生的情况下，却消极对待或放任不管，导致危害结果发生或危险状态出现的，应当承担不作为犯罪的刑事责任。不作为犯罪可以是故意犯罪，也可以是过失犯罪。

（3）独立的正犯责任。网络直播平台明知他人利用直播平台实施违法犯罪活动，仍提供直播平台所包含的网络技术支持或帮助，导致发生危害结果的，应独立承担帮助网络犯罪活动的刑事责任，而不论正犯或主犯实施的犯罪是否成立，具体以《刑法》二百八十七条之二为依据。

（4）重大管理或监督过失责任。当直播内容特殊、直播受众面极其广泛时，即使属于重大管理或监督过失的，若造成严重结果，网络直播平台应承担网络过失犯罪的刑事责任。对于前三种刑事责任形式，现行刑法基本上都有相关规定或直接规定；而且，不作为犯责任与独立的正犯责任是主要责任形态，也是刑法最新修正的重点对象。但是，目前并无网络过失责任规定，填补网络过失犯罪的立法空白应提上议程，进而才能为追究网络平台等网络主体的过失犯罪的刑事责任提供合法依据。

3.具体罪名的适用

基于网络直播平台的属性及其负有的法定义务内容，直播平台违反国家规定的网络安全管理义务，造成危害结果的，可能涉嫌构成下列犯罪：

（1）拒不履行信息网络安全管理义务罪。网络直播平台是网络服务提供商，承担法定的信息安全管理义务。故意违反信息网络安全管理义务，同时符合“经监管部门责令采取改正措施而拒不改正的”客观处罚要件，造成危害结果的，应承担刑事责任。在认定时，应充分考虑网络运营商履行管理义务的现实可能，严格把握入罪范围。涉及公民信息安全等具体保护义务等的，按照侵犯公民个人信息犯罪和帮助毁灭证据罪等特殊罪名论处。

（2）非法利用信息网络罪。利用直播平台实施传播淫秽物品、洗钱等违法犯罪信息的，将直播平台变为实施违法犯罪活动的预备场、信息群的，情节严重，构成非法利用信息网络罪。

（3）帮助信息网络犯罪活动罪。网络直播平台是新型网络空间场所，网络直播的运行高度依附于网络直播平台的技术支持。当前，除非是中立的网络技术行为，一些网络技术帮助行为的危害性或危险性明显偏高，故意提供或消极放任并造成危害结果的，应当承担刑事责任。为网络直播活动提供互联网接入、网络存储、通讯传输等技术支持或支付结算等帮助行为的，网络直播平台可能成为“技术”帮凶。

（4）网络中立业务行为的正当化处置。根据《网络安全法》、《互联网直播服务管理规定》与《刑法修正案（九）》的规定，直播平台负有网络安全管理义务是归责前提，但也应对网络直播平台实施的中立业务行为予以除罪化，划清其与严重的网络技术帮助或支持行为的界限。在确定是否应当设置法定的管理义务、判断是否具备实施义务的能力这两个实质条件时，应当充分考虑网络代际的本质特征、网络技术的发展阶段、网络主体的认识能力与避免能力、所制造的法律风险是严重脱离相当性还是属于可以容忍的合理限度等因素。既要严厉制裁网络直播平台实施的网络违法犯罪行为，也要鼓励正常的网络业务经营行为与自由创新。

（三）监管部门的刑事责任认定

《网络安全法》八条对网络安全保护和监督管理的主体及其职责作出概括性规定。《互联网直播服务管理规定》四条确立以互联网信息办公室为核心的自上而下的监管体制。《网络表演经营活动管理办法》十七条、第十八条规定，文化部负责全国网络表演市场的监督管理工作。在此基础上，网络监管部门及其责任人员的刑事责任情形，主要包括：

（1）监管部门或监管人员违反监管职责，滥用职权或严重失职的，应承担渎职责任。《网络安全法》七十三条第二款规定：“网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。”目前，由于缺乏像环境监管失职罪、食品监管渎职罪等具体的监管渎职罪名，对网络监管渎职犯罪的，只能概括地适用滥用职权罪或玩忽职守罪，其他渎职行为可以援引受贿罪等关联罪名。但应考虑增设“网络监管渎职罪”。

（2）违反特定的重大网络安全监管义务，破坏国家安全、国防安全、军事安全等重大法益的，依照分则的规定从重论处。

（3）利用工作之便或职务之便实施或参与共同犯罪的，按照总则规定追究共犯责任。

（4）重大监管过失或管理过失，导致严重社会危害的，可能构成大型群众性活动重大安全事故罪等。

（四）网民参与的刑事责任限度

《互联网直播服务管理规定》二条第二款、第九条、第十一条第三款等规定，用户作为互联网直播服务使用者，应当遵守法律法规的规定，依法上网。

广大网民作为互联网直播服务使用者，集消费者、被害者与加害者等身份于一身，通常不应当对直播平台的失范直播行为承担刑事责任。但是，网民可能实施聚众、片面教唆与帮助等行为，甚至在户外直播中直接或积极参与各种违法违规的直播行为，或干扰正常的网络直播过程、破坏网络直播平台的系统秩序运行，造成严重的危害结果的，不作为犯罪处理显然不妥。鉴于此，刑事责任类型可能包括：

（1）非法利用信息网络罪与帮助信息网络犯罪活动罪。二者旨在维护信息网络管理秩序以及信息网络安全，是制裁用户参与网络直播违法犯罪行为的重要依据。用户的参与行为情节严重的，可以追究刑事责任。

（2）寻衅滋事罪。用户参与或聚众，形成“起哄闹事”的危害结果，可能涉嫌构成网络空间下的寻衅滋事罪；对他人实施侮辱、诽谤且情节严重的，可能涉嫌构成侮辱罪、诽谤罪。

（3）其他罪名。根据直播内容与形式、网民的行为及参与程度，确定涉嫌的具体罪名。比如，网民的行为导致网络直播平台不能正常运行或非法控制、非法获取平台数据的，根据司法解释的规定，属于情节严重的，可能构成非法控制计算机信息系统罪、非法获取计算机信息系统数据罪及破坏计算机信息系统罪等相关罪名。

综上，根据《网络安全法》《刑法》等的规定，网络主播、直播平台、监管者、网民都负有相应的网络安全管理义务，违反法定义务，造成严重后果，符合立案标准或入罪条件的，应追究刑事责任。目前，受限于立法的滞后性，定罪思路仍以传统罪名的网络化扩张适用为主；同时，考虑到网络直播犯罪的司法解释或指导意见尚未出台，应建立网络犯罪案例指导制度并发挥适法指导作用。

三

因应网络直播平台犯罪治理的体系协同

网络直播刑事风险的增量，是网络技术更迭与网络社会变迁的正常现象。其中，直播平台是关键因素，既是控制直播风险的首要主体，也是治理网络直播乱象的首要对象。应树立网络平台犯罪的专属治理思维，通过立法修正着力解决网络平台犯罪治理的规范不足问题，重视推动网络刑法知识变革解决本源困境。

（一）积极网络制裁思维的转变

应正视刑法中积极预防理念与必要的处罚理念的时代意义，导入认罪认罚从宽制度，以有限的司法资源，有效遏制以网络平台为主体的网络直播刑事风险。

1.积极预防理念

风险社会充斥于后工业革命社会的末期，无处不在的风险加剧人类对安全与秩序的渴望，也抬升安全秩序价值的优先地位。由此，积极应对不确定的风险和维护社会安全秩序已成为刑法迫切需要实现的重要目标。比如，《刑法修正案（九）》对网络犯罪的修改，充分体现了“秩序价值的优先性”的预防策略，将网络预备行为犯罪化、网络不作为犯罪化、网络技术帮助行为犯罪化，都呈现出刑法介入的早期化迹象。

在此基础上，安全价值与公共秩序作为刑法优先保护的价值，必然对自由价值和网络创新精神形成一定的压制效应，也对传统刑法理念及其立法产生了深层次影响。在安全秩序价值相对优先的理念指导下，将直播平台、主播、监管部门以及用户的刑事责任作为首要任务具有必然性与合理性，是保护信息网络安全与管理秩序的迫切需要。

而且，网络技术风险不同于传统现实物理社会的危害行为，大量预备行为、未遂行为、技术帮助行为、片面技术支持行为等技术参与行为都具有明显偏高的刑事风险。按照传统报应性司法模式倡导的危害原则、结果犯立法、事后的报应措施等，往往无法处置。传统报应性司法模式应对网络技术风险频现短板，未充分激活刑法理论体系的积极预防功能，导致传统刑法陷入“亦步亦趋”的怪圈。

为了稀释报应性司法模式的制度失灵窘境，刑法应保持积极介入社会治理的姿态，激活刑法介入的早期化功能与预防性理念。网络预防性刑法理念有别于传统的报应性司法理念，是因应网络技术风险而自发形成的新思维，并不全面否定传统刑法体系，更关注危险提前化的现状和防控危险的预先性、事前性，将一些高度危险的网络技术行为纳入刑法介入的范围，确保刑法可以有效保障社会安定的基本条件。

预防性刑法思维旨在解决网络技术风险的犯罪化原则、犯罪圈设定及制裁措施，集中表现为增设网络危险犯等预防性立法举措。预防性刑法思维及其立法是制衡网络直播刑事风险的重要途径，确保可以积极介入一些高度危险的“零界”行为，而不再受制于“事后救火”的消极反应与被动干预困境。然而，网络积极预防功能观也不宜绝对化，应警惕一味从严、从重、从早打击的片面看法，仍应以宽严相济刑事政策为指导，遵循区分对待的策略，实现网络犯罪控制观下的科学与有效治理。

2.必要的处罚理念

传统理论认为，刑法是最严厉的法律制裁，只在其他部门法“无能为力”时才能介入。刑法是事后法和保障法。由此，也将刑法置于“消极防守”位置，刑罚处罚主要立足于“面向过去”而非“面向未来”。诚然，将刑法定位为其他部门法的“保障法”，可以从逻辑上防止滥用刑罚权，确保启动的正当性与有效性。但是，并不能借此过度弱化刑法的保护机能与刑法治理犯罪的基本任务安排，更不能忌惮刑罚权的“法定的恶”而不敢发动，使刑法背离保障人权的本质属性与保障社会安全功能设定。

网络技术风险是网络社会创新与风险社会相互交织而成的伴生物，网络技术风险的不确定性，源自大量网络技术型的预备行为、未遂行为、共犯参与行为、不作为以及过失行为等都具有明显偏高的刑事风险，甚至不亚于实行行为或正犯的危险度。在此背景下，如若不介入，刑法保障社会的功能则形同虚设。因此，与其一味地从静态层面限制处罚范围，不如从动态层面对处罚范围进行合理的分流，保持犯罪化与非犯罪化的理性配置。犯罪圈也不是“越小越好”，动态层面的“必要的处罚”是正当的，因为并非“越少的处罚就是对的”。

网络刑法理论体系应当适度坚持网络安全价值优位的理念，将积极预防主义植入刑法规定与司法过程，合理松绑刑法的谦抑精神，倡导由“过度的限制的处罚”转向“必要的处罚”。“必要的处罚”摄入积极预防理念，试图平衡法益保护功能与人权保障功能；在合理释放刑法保护网络安全的内在张力之际，适度提前刑法的介入时机，通过刑事处罚的前置化实现预防的早期化。“必要的处罚”主张仍坚持立法的审慎性理念，纠偏过度的犯罪化，贯彻必要的非犯罪化，使犯罪圈的变动处在可控与可接受的范围内。

3.认罪认罚从宽制度的试用

相比于传统犯罪现象，以网络技术为基础的网络犯罪现象，在行为主体、行为方式、危害结果等方面伴随诸多的不确定性和易变性，犯罪主体的具体性、行为的可追踪性、结果的可视化等均明显下降，进而，使管辖原则、证据收集、诉讼证明、庭审技术化等新型难题接踵而至。这给公安司法机关带来前所未有的司法挑战。为了降低网络犯罪的侦查与追责难度，在审查起诉阶段合理引导程序分流，真正促进庭审实质化，对其适用认罪认罚从宽制度有积极的现实意义。

比如，“快播”案被认为是适用认罪认罚从宽制度的首案。对于以网络直播刑事风险为代表的网络平台犯罪而言，在认定是否具有网络安全管理义务、是否充分履行、是否具有履行的可能性、是否情节严重等问题时，也面临侦查难、取证难、起诉难、审判难等“诉讼技术”难题。适用认罪认罚从宽制度，不仅可以降低追诉难度，也可以起到惩治犯罪的积极效果，还可以更好地贯彻积极防控思维，夯实必要的处罚理念，节约司法资源。

（二）立法修正的基本要领

直播平台应承担防控直播刑事风险的主体责任。直播平台是网络平台的一种具体情形。网络平台犯罪正演变为网络犯罪的重要方式。为此，首先应加快立法修正步伐，确立网络平台的犯罪主体地位，直击网络平台犯罪的治理痛点。

1.网络平台犯罪主体的法定化

从网络直播的运营服务看，网络主播、网络用户都是网络平台的依附者或寄生者，网络主播与用户同时扮演生产者与购买者；网络监管者是法定的规制主体，网络平台的风险防控

是网络监管者面临的新事物。因而，在网络直播迅猛发展的过程中，最大的新变量正是网络平台，内在的诸多不确定性，使网络直播平台成为网络风险的制造者。

与此同时，网络平台犯罪相比于其他网络犯罪类型及传统犯罪，犯罪主体的特殊性是其最大挑战。网络平台本身并非法定的犯罪主体类型，套用自然人或法人均不匹配，也不是聚众、共同犯罪、有组织犯罪、犯罪集团等其他变体；而且，网络平台具有显著的主体聚合性与行为集聚性，网络平台与主播、用户往往高度相连；网络平台的运营服务依赖具体负责人员和工作人员，网络平台实施的行为具有多重属性，如网络实行行为或正犯行为、网络技术帮助行为、网络预备行为、网络中立行为等相互交错。从网络技术的发展趋势、互联网经济的演进，尤其是网络平台经济的崛起等因素看，网络平台犯罪形态将呈现出一定的增量态势，但犯罪属性异常复杂。

传统犯罪主体理论未能同步作出改变，直接制约理论与立法的协同配合，加大司法处置的难度。为了实现理论、立法与司法的三位一体效应，应调整传统犯罪主体理论，确立网络平台作为新型网络犯罪主体的资格和地位。对此，可以通过立法修正的方式，在总则中直接明确，进一步辐射分则的修改与司法适用。

2.网络平台安全犯罪的增设

虽然《刑法修正案（七）》《刑法修正案（九）》先后作出修改，但仍需再次修正刑法中的网络犯罪规定。不过，单纯着眼于修改或完善已有的刑法规定并不可行，而应继续增设新的罪名。对于以网络平台为动向的新型网络犯罪现象，立法完善的方向为：

（1）增设破坏网络平台安全罪。目前，第二百八十五条、第二百八十六条、第二百八十六条之一、第二百八十七条之一、第二百八十七条之二都并非直接规定网络平台犯罪，后三个新罪名虽有很强的解释空间，仍不足以解决网络平台犯罪的规范供给严重不足问题。

一方面，第二百八十六条之一是典型的网络不作为犯罪，是以网络平台负有法定的作为义务为基础，难以规制目前并无法定的作为义务，但客观上造成严重危害结果的情形。

另一方面，第二百八十七条之一属于网络预备犯罪，第二百八十七条之二是网络帮助行为的正犯规定。虽然网络平台在实施犯罪的过程中，可能放任和纵容其他犯罪，但新增加的两个罪名并非直接用于打击网络平台犯罪。

鉴于此，应当增设新条文，既与第二百八十五条、第二百八十六条这两个传统的计算机犯罪规定划清网络立法的代际界限，也与第二百八十六条之一、第二百八十七条之一、第二百八十七条之二保持合理的功能区分。在网络平台作为新型犯罪主体的基础上，根据《网络安全法》与其他行政法规、部门规章对网络主体类型及其相应义务等规定，拟增加二百八十七条之三，具体可以表述为：“网络运营者、网络服务提供者等网络平台，违反国家规定，破坏网络安全运行与网络管理秩序，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。对网络平台判处罚金，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。有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。”

理由为：一是网络运营者、网络服务提供者是主要的网络平台主体类型，也是网络直播风险的主要制造者；二是网络平台犯罪是法定的网络犯，考虑网络法律体系的变动性，应以“违反国家规定”来延续刑事违法性判断的有效性，增强立法的适宜性；三是在情节犯、法定刑配置、犯罪竞合处置等问题上，可以参照第二百八十六条之一、第二百十七条之一、第二百八十七条之二，保持网络犯罪罪名体系的整体协调性，妥善解决犯罪竞合问题；四是罪名可以初步定为“破坏网络平台安全罪”。

（2）增设网络安全监管渎职罪。《网络安全法》奉行网络安全治理的强监管理念，以多层次、综合化的网络安全概念为基本面向，重在强化国家对网络安全的管制力，在当今世界的网络安全专门立法中可谓独树一帜。但《网络安全法》对监督者的法律责任，尤其是刑事责任的规定明显不足。为了对接《网络安全法》的立法导向，将强监管理念充分植入整个

网络安全治理体系中，同时督促国家监管部门积极作为，可以考虑增设专门的网络监管渎职犯罪。

这一专门立法的本意，与《刑法修正案（八）》增设四百零八条之一暨食品监管渎职罪如出一辙，突显网络安全监管的重要性，剑指网络监管渎职行为，以实现网络安全监管、网络安全管理以及自治的良性对接，营造更有力的共治生态。从立法技术上看，可以借鉴第四八零八条之一的做法，暂时增加第四八零八条之二。法条表述可以为：“负有网络安全监管管理职责的国家机关工作人员，滥用职权或者玩忽职守，导致发生重大的网络安全事故，或者造成网络空间主权和国家网络安全、社会网络公共利益，公民、法人和其他组织的合法网络权益，经济社会网络信息化发展遭受严重损失的，处五年以下有期徒刑或者拘役；造成特别严重后果的，处五年以上十年以下有期徒刑。徇私舞弊犯前款罪的，从重处罚。”借此，可以对网络平台监管不力的严重渎职行为加以直接规制，夯实网络安全保障的国家力量体系。

（三）传统刑法体系的知识变革

网络直播刑事风险的“定罪困题”之所以频发，其症结在于传统刑法理论、规定与司法模式“失灵”或“失效”。只有积极拥抱网络社会与正视网络犯罪形态，从源头上扭转传统刑法体系的束缚局面，才能从根本上解决网络平台犯罪等一系列挑战。

1.传统体系的思维桎梏

网络直播是网络平台兴起下的流行应用物。网络平台正全面参与生产生活，网络平台犯罪不断演变。网络直播刑事风险高居不下，并非网络平台技术的“罪过”，反而折射出网络平台的治理体系“拖了后腿”。受制于网络技术代际与网络社会时代的突飞猛进，我国传统刑法立法缺乏概括性或预见性规定，对大量新出现的模棱两可的失范直播行为，是否应进行刑事处罚的适法依据不明。这些疑难个案或类案导致刑事制裁的灰色地带有所扩大。而且，网络直播引发的刑事风险具有不确定性与复杂性，持续加剧刑法评价对象与评价标准的科学设计难度，遵循传统刑法体系及其立法规定，治理网络直播平台犯罪的收效不佳。

应当看到，并非传统刑法体系及其立法规定“无用”，而是扩张解释、立法修补等举措，已难以弥合传统犯罪形态与网络犯罪形态之间的沟壑，不断扩大了传统刑法体系与治理网络犯罪之间的裂痕。传统刑法理论的形成与制定背景，与网络空间社会相距甚远，不断放大传统刑法理论体系的时代滞后性，因应网络直播刑事风险的不适是这场裂变的缩影。可以说，冲破传统刑法理论体系的主导地位，正是建立网络刑法学及其理论体系的开始，与解决新问题的根本之策。

2.网络刑法体系的胎变

网络直播乱象暴露了网络平台犯罪的治理难题，也倒逼刑法理论体系在局部领域的转变。比如，刑法理论应确认网络平台作为新型犯罪主体的资格，而不能完全套用传统犯罪主体理论；在打击网络直播犯罪并依法追究刑事责任的规范依据中，网络安全管理义务是关键和难点，未来刑法修正应当联动附属刑法，以科学的立法原则和必要的犯罪化理念为前提，确定刑法义务的范围和内容；在应对网络犯罪时，传统刑事禁止令难以展开，需要修正为网络刑事禁止令措施，等等。

然而，因应网络直播平台犯罪而自发形成的片段性或局部性理论转变，只是传统刑法体系迈向网络刑法体系的一部分。而且，传统刑法体系的改变，是一个渐进性的系统工程，无法在短时期内彻底完成，更缺乏可以临摹的范本。尽管如此，及时有效填补应对网络直播平台犯罪时暴露的问题仍有积极意义，可以与其他理论的网络化调试共同形成可观的集成效应。

四

结语

网络直播引发的刑事风险高居不下，导致传统刑法理论、立法规定、司法应对不适等问题相继出现，触发传统刑法体系的制度供给危机。当前，首先应根据《网络安全法》《互联网直播服务管理规定》等法律法规的规定，依法追究网络主播、直播平台、监管部门、用户的刑事责任，遏制网络直播风险的蔓延态势。同时，应当主动在立法完善上求变，尽快改变刑法规范供给不足的现实困题，尤其是针对网络平台犯罪的立法修正刻不容缓。更重要的是，《刑法修正案（九）》对网络犯罪的重大修改，宣告“我国刑法的一个专门领域即网络刑法的真正诞生”。立法者应重新审视传统刑法体系在网络犯罪时代的功能与命运，树立网络刑法知识转型的前瞻意识，采取相应的措施，加快理论体系的衔接和转轨。

孙道萃（1988—），男，江西泰和人，北京师范大学刑事法律科学研究院博士后，华南理工大学法学院讲师，法学博士，主要从事刑法研究。

文章九、网络游戏公司运营中的刑事合规

1.网络游戏公司运营中的刑事合规

韩旸 常康爽 金杜研究院

近年来游戏行业大热，我国游戏市场规模在过去 9 年皆保持高速增长，行业销售规模突破 2000 亿元，[1]成为了全球移动游戏最具活力的地区，预计未来几年我国移动游戏市场仍将维持快速增长。与此同时，网络游戏公司其在运营过程中所暴露出的法律风险也日益增多。

以“网络游戏”为关键词，在“威科先行”法律信息库检索相关刑事判决（数据截至 2020 年 2 月 18 日），我们发现，涉及网络游戏的刑事案件数量逐年增多（图 1）。其中浙江、江苏、广东的案件数量位居全国前三位，约占总数的三分之一。（图 2）

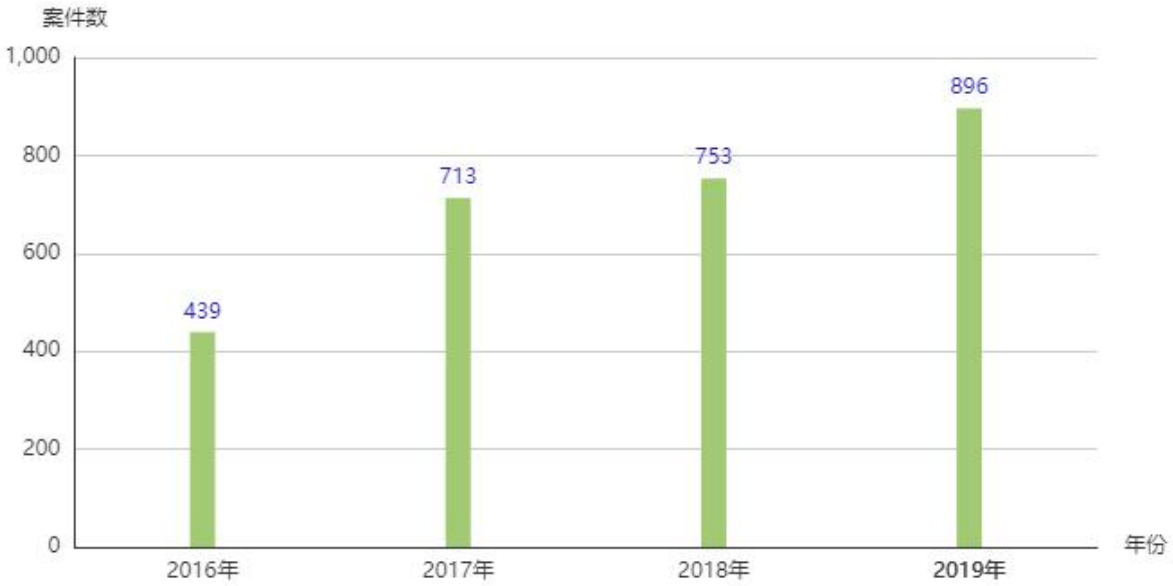


图 1　来自威科先行法律信息库

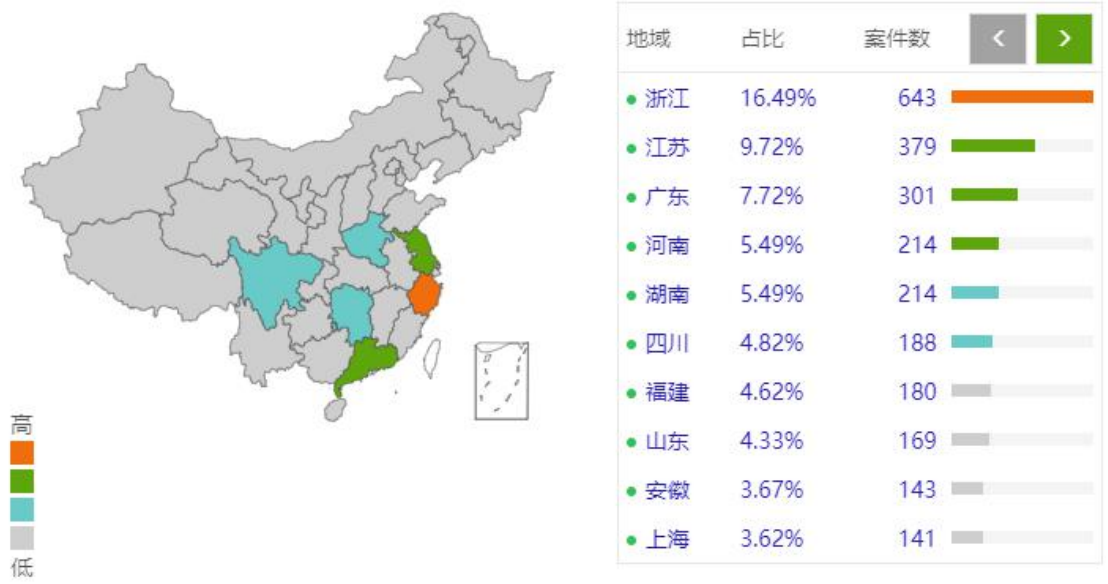


图 2　来自威科先行法律信息库

本文将从公司（或其高管）涉嫌刑事犯罪、公司利益被他人侵害两个角度，探讨和分析网络游戏公司可能涉及的主要刑事风险。相关观点仅供读者参考，不作为专业法律意见使用。

一、网络游戏公司（或其高管）可能涉及的刑事风险

（一）赌博、开设赌场

近年来，游戏公司涉嫌网络赌博的案件数量逐年增长，这与国家对游戏公司监管力度增大的大环境有一定的关系。公安部、最高人民法院、最高人民检察院《关于办理网络赌博犯罪案件适用法律若干问题的意见》对网络赌博犯罪的认定、处罚、以及定罪量刑标准作出了明确规定。此外，依据公安部《关于规范网络游戏经营秩序查禁利用网络游戏赌博的通知》，收取或以“虚拟货币”等方式变相收取与游戏输赢相关的佣金，开设使用游戏积分押输赢、竞猜等游戏，提供游戏积分交易、兑换或以“虚拟货币”等方式变相兑换现金、财物的服务，提供用户间赠予、转让等游戏积分转账服务等行为均可能涉嫌刑事犯罪。

需说明的是，赌博罪、开设赌场罪中未规定单位犯罪。而根据全国人民代表大会常务委员会关于《中华人民共和国刑法》第三十条的解释，“公司、企业、事业单位、机关、团体等单位实施刑法规定的危害社会的行为，刑法分则和其他法律未规定追究单位的刑事责任的，对组织、策划、实施该危害社会行为的人依法追究刑事责任。”

一方面，以营利为目的，提供物质便利、组织多人赌博的行为涉嫌赌博罪。《最高人民法院、最高人民检察院关于办理赌博刑事案件具体应用法律若干问题的解释》规定，以营利为目的，有下列情形之一的，属于刑法第三百零三条规定的“聚众赌博”:（1）组织 3 人以上赌博，抽头渔利数额累计达到 5000 元以上的；（2）组织 3 人以上赌博，赌资数额累计达到 5 万元以上的；（3）组织 3 人以上赌博，参赌人数累计达到 20 人以上的；（4）组织中华人民共和国公民 10 人以上赴境外赌博，从中收取回扣、介绍费的。例如，某游戏公司管理人员发现他人在微信群内利用其游戏 APP 进行赌博的情况下而未予以制止，反而为谋取经济上的利益继续向他们提供游戏服务、发放奖励，被法院认定构成赌博罪的共同犯罪。[2]

另一方面，根据相关规定，在计算机网络上建立赌博平台，或者为赌博网站担任代理，接受投注的或明知是赌博网站，而为其提供互联网接入、服务器托管等服务的，可能构成开设赌场罪。在司法判例中，行为人多以营利为目的，建立游戏网站设置插件接受投注或利用移动通讯终端开设赌场，同时明知是赌博网站，提供服务或者帮助，担任代理接受投注，参与利润分成等行为都被认定为构成开设赌场罪。例如，某网络公司开发并单独运营一游戏网站，玩家以人民币充值获取游戏积分，玩家之间可以相互转让积分。为增加网站人气，被告人姜某甲（网络公司总经理）、张某甲（网络公司法定代表人）发展游戏玩家刘某甲作为该网站的银商及客服人员，在网站内按一定比例买卖游戏积分的行为构成开设赌场罪。[3]

一般认为，开设赌场罪与赌博罪在组织方式、参与人员等方面存在区别。例如某案例中法院判决认为，其一，组织结构、赌具来源、赌博方式的不同：开设赌场罪中，参赌人员规模较大，赌具也由赌场提供，其赌博方式由赌头设定；而赌博罪中，赌博规模较小，赌具由参赌人员提供，其赌博方式也由参赌人员临时确定。其二，参赌人员的来源不同：开设赌场罪中，赌头以开设赌场的方式吸引他人参与赌博；赌博罪中，参赌人员均由赌头直接召集而至。其三，参赌人员的性质不同：开设赌场罪中，参赌人员具有不特定性，参赌人员不固定；赌博罪中，参赌人员有特定性，即由赌头或其他参赌人员召集、指引特定的人参与赌博，参赌人员一般较为固定。[4]

（二）组织、领导传销活动

实践中，部分不法分子通过网络游戏组织、领导传销活动，常见的是利用网络游戏要求参加者注册、缴纳费用取得资格，并按照一定顺序组成层级，直接或间接以发展下线获取利益，引诱参加者继续发展他人参加，骗取钱财，构成组织、领导传销活动罪。

例如，被告人李某某伙同他人以网络游戏的形式，组织、领导以推销商品为名，要求参加者以缴纳费用的方式获得加入资格，并按照一定顺序组成层级，直接或者间接以发展人员的数量作为计酬或者返利依据，引诱参加者继续发展他人参加，骗取财物，其行为构成组织、领导传销活动罪。[5]

（三）非法经营

在刑事判例中，存在无照经营非法搭建网络游戏平台、未经批准开展业务的现象，均构成非法经营罪。例如：

行为人以牟利为目的，未经批准非法接受投注，擅自发行销售彩票；非法搭建网络游戏私服进行资金支付结算业务等。

（四）侵犯著作权

根据《刑法》第 217 条第（一）项的规定，以营利为目的，未经著作权人许可，复制发行其文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品，违法所得数额较大或者有其他严重情节的，构成侵犯著作权罪。

实践当中，网络游戏公司构成本罪常见的行为包括：未经许可擅自使用他人作品、转载侵权、网络抄袭与剽窃、网页设计侵权以及链接侵权。例如，被告单位公司以营利为目的，未经著作权人许可，复制发行其计算机软件作品 2300 余份，被认定构成侵犯著作权罪，判处罚金人民币伍十万元，被告单位直接负责的主管人员被告人刘某某犯侵犯著作权罪。[6]

（五）侵犯公民个人信息

当今时代，公民个人信息已成为重要资源，部分不法分子通过网络实施侵犯公民个人信息犯罪活动，甚至形成了“源头—中间商—非法使用人员”利益链条和黑色产业。网络游戏公司在业务开展过程中不可避免地接触和收集大量的公民个人信息，如管理不善，极有可能引发刑事风险。

《刑法》第二百五十三条之一规定，违反国家有关规定，向他人出售或者提供公民个人信息，窃取或者以其他方法非法获取公民个人信息的，情节严重的，构成侵犯公民个人信息罪。《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》对本罪中“公民个人信息”、“情节严重”等要件的内涵作出了具体规定。

此外，根据相关司法解释，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，应当以拒不履行信息网络安全管理义务罪定罪处罚。

二、网络游戏公司利益被侵害的刑事风险

（一）员工舞弊

1. 职务侵占

职务侵占罪虽是常见的传统罪名，但随着经济社会的发展，无论是单位法律属性、主体形式、履职方式、还是财物表现形式，都有新的变化。[7]游戏公司的工作人员，利用自身职务上的便利，使用管理员账号修改游戏系统内数据，私自生成、分发游戏武器装备换取个人利益，数额较大的，有可能涉嫌构成职务侵占罪。

对于游戏中的武器装备等网络虚拟财产是否属于职务侵占的对象，在理论界和实务界仍存在争议。部分司法判例认为，武器、装备可认定为物体财产性利益，是计算机软件运行后生成的结果，在虚拟环境中的作用决定了其可以被人占有、使用等，但游戏玩家要取得虚拟财产除了花费时间外，还必须付出一定的费用，如购买游戏点卡的费用、上网费等，同时该虚拟财产通过现实中的交易能转化为货币，具有一定的财产属性。因此，犯罪数额可按其销赃获利数额计算。[8]

2.非国家工作人员受贿

游戏公司的工作人员存在成立非国家工作人员受贿罪的可能。例如，2008 年 9 月至 11 月，唐某利用自身的职务便利，擅自为游戏中的游戏玩家增加装备、修复装备、提升等级，并收受玩家的贿赂，被判处非国家工作人员受贿罪。[9]

（二）被侵犯著作权

网络游戏公司在避免侵犯他人著作权的同时，也需要特别关注自身著作权的保护。实践中，公司被内部员工或第三方人员侵犯著作权的现象频频发生，以下情况尤其值得警惕：游戏源代码被他人非法泄露、出售，将游戏换皮加工后重新上市；[10]公司源代码被离职员工

抄袭、利用，开发同类产品；[11]软件源代码被他人非法获取，并利用服务器端程序及相关的客户端程序、登陆器软件，架设私服。[12]

（三）被侵犯计算机信息系统、数据：

由于网络游戏以互联网为传输媒介，以游戏运营商服务器和用户计算机为处理终端，以游戏客户端软件为信息交互窗口，因此也给许多对计算机信息系统的犯罪留下可乘之机。

1.破坏计算机信息系统

如果他人对计算机信息系统功能或其中存储、处理或传输的数据、应用数据进行删除、修改、增加、干扰等行为可能涉及破坏计算机信息系统罪。

例如，2015 年 8 月，胡某通过破译账户密码方式进入游戏后台系统，利用他人权限更改其指定用户系统中的游戏金币数量，并且通过后续操作获取游戏装备出售牟利，破坏整个游戏系统的运行和平衡，被判处破坏计算机信息系统罪。[13]

2. 非法获取计算机信息系统数据、非法控制计算机信息系统

如果他人非法侵入计算机信息系统或采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对计算机信息系统实施非法控制，可能涉嫌非法获取计算机

信息系统数据、非法控制计算机信息系统罪。例如，2017 年 6、7 月间，王某违规登录网络游戏服务器，擅自利用软件生成并使用虚拟游戏装备，同时擅自将这些装备予以出售，非法获利，被判处非法获取计算机信息系统数据罪。[14]

三、网络游戏公司的风险防控

针对网络游戏公司的合规运营，我们提出如下初步建议：

严格依法开展相关业务，不得未经批准擅自进行活动，不得从事与许可不符的经营活动，严格监管运营模式，诚信合法经营。

增强合规意识，完善合规制度建设，重视合规培训，借助合规途径正确防范企业自身责任。

游戏推广中以合法渠道、合法形式开展工作，不得虚构身份信息进行引诱，公司领导不得伙同、批准、默许赌博、诈骗等违法犯罪行为，建立和完善举报机制。

对管理员账号中的附属管理工具进行有效技术控制：例如对管理员的权限设置多重认证，减少单个员工单独掌握修改权限的情况，相互监督。

加强自身知识产权、商业秘密保护，重视计算机信息系统和数据安全，完善保密措施；与员工签订完善的竞业禁止协议、保密协议。

疫情之下，游戏行业极有可能迎来新一轮的发展。但在看到机遇的同时，其涉及诸多合规监管问题同样不容忽略，游戏公司在运营过程既要防范业务开展过程中可能引发的刑事风险，也要注意避免自身利益遭受内、外部人员的不法侵害。因此，如何识别和防控运营的法律风险，应当成为网络游戏公司的必修课。

附：

[1] 中国报告大厅:“游戏行业概况及现状”,http://m.chinabgao.com/k/youxi/48621.html

[2] 浙江省苍南县人民法院(2018)浙 0327 刑初 870 号刑事判决书

[3] 江西省宜春市袁州区人民法院(2015)袁刑初 308 号刑事判决书

[4] 青海省同仁县人民法院(2019)青 2321 刑初 12 号刑事判决书

[5] 广东省东莞市第二人民法院(2018)粤 1972 刑初 289 号刑事判决书

[6] 上海市徐汇区人民法院(2018)沪 0104 刑初 373 号刑事判决书

[7] 董鑫欣：《职务侵占罪疑难问题的司法认定》，http://victory.itslaw.cn/victory/api/v1/articles/article/263684d8-7fae-4da0-a0e4-e513f967b493

[8] 《刑事审判参考》第 461 号案例：王一辉等职务侵占案（利用职务便利盗卖单位游戏"武器装备"的行为构成职务侵占罪）

[9] 中国法院网：“擅自帮玩家修复游戏装备 工程师受贿 3 万获刑 2 年”，https://www.chinacourt.org/article/detail/2010/09/id/428525.shtml

[10] 四川省成都高新技术产业开发区人民法院(2018)川 0191 刑初 529 号刑事判决书

[11] 朱骏超：《游戏源代码的刑事法律风险》，https://zhuanlan.zhihu.com/p/77758895

[12] 北京市海淀区人民法院(2014)海刑初字 1633 号刑事判决书

[13]上海市普陀区人民法院(2016)沪 0107 刑初 1395 号刑事判决书

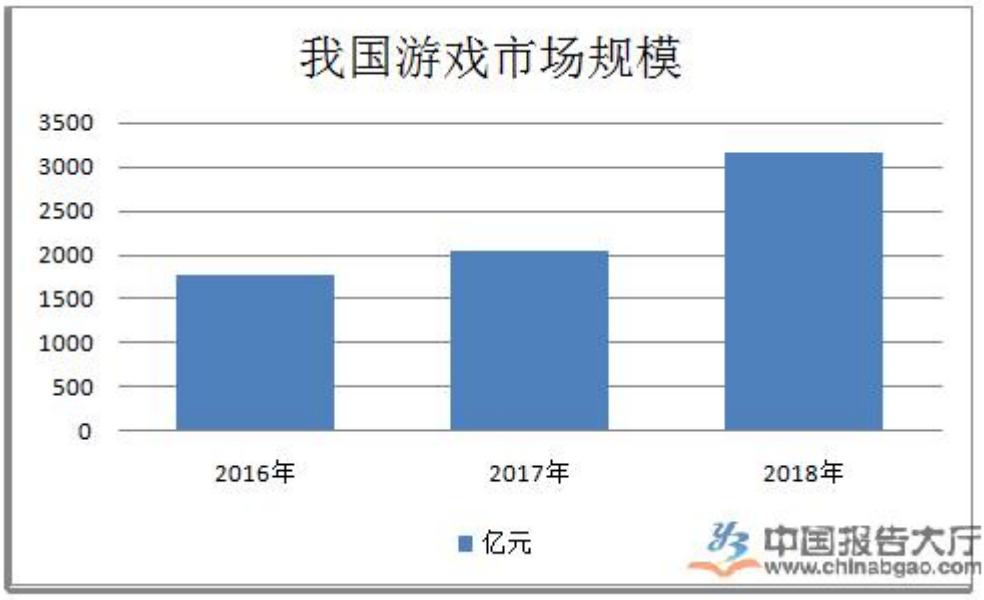
[14] 北京市海淀区人民法院(2018)京 0108 刑初 114 号刑事判决书

2.游戏行业概况及现状——中国报告大厅

标签：游戏　　2019-07-09 15:01:09

导语：我国是全球移动游戏最具活力的地区之一，2018 年市场规模达到 3150.3 亿元，同比增长+24.61%%，预计在端游回暖，页游收入和用户双降下，今年自主研发移动游戏的海外市场规模将进一步扩大，以下是游戏行业概况及现状分析。

我国是全球移动游戏最具活力的地区之一，2018 年市场规模达到 3150.3 亿元，同比增长+24.61%%，预计在端游回暖，页游收入和用户双降下，今年自主研发移动游戏的海外市场规模将进一步扩大，以下是游戏行业概况及现状分析。



我国游戏市场规模在过去 9 年皆保持高速增长，行业销售规模突破 2000 亿元，最近 3 年复合增长率达到 21.2%。游戏行业分析指出，2011 年前，市场规模的扩大主要来自于用户数量的飞速增长以及页游的快速发展。

2011 年后，我国游戏市场增速有所放缓，增量仍然保持稳定。游戏行业概况及现状指出，2016 年增量部分来自移动游戏的高速增长，移动游戏 2016 年实际销售收入同比增长

59.2%，达到 819 亿，一举超过 PC 客户端游戏 的占比达到 49.5%，成为我国游戏行业的最大细分市场。

2017 年，我国游戏市场规模达到 2036.1 亿（同比增长+22.98%），其中移动游戏市场规模为 1161.2 亿（同比增长+41.75%），端游市场规模为 648.6 亿（同比增长+11.3%），页游市场规模为 156 亿（同比增长-16.6%）。

2018 年，我国端游增速略有回暖，手游增速继续放缓，页游连续第二年负增长。移动游戏规模占比达到 57.03%，端游占比连续 6 年下滑，页游占比连续 3 年下滑，预计 2019 年移动游戏占比有望进一步提升。

预计到 2020 年我国游戏市场规模可突破 2000 亿元。根据数据显示，近年来我国移动游戏市场呈现高速发展态势，2018 年我国移动游戏市场实际销售收入达到 1259.2 亿元，同比增长 41.7%。而根据预计，我国移动游戏市场在未来几年仍将维持快速增长 2020 年我国移动游戏市场规模预计可以达到 2218 亿元。

游戏行业概况及现状认为，自《诛仙》、《花千骨》等热门 IP 改编成游戏并取得不俗成绩后，实力雄厚的研发商纷纷积极物色优质 IP 并进行游戏改编，市场上 IP 改编移动游戏比例持续提升。2018 年 IOS 平台畅销榜 TOP100 的游戏中，IP 改编的游戏比例已超过 50%，较 2017 年有明显提升。

在 IP“粉丝效应”下，网络游戏、文学、影视、动漫、综艺等各领域相互交融，协同打造同一优质 IP 的趋势愈发明显，为移动游戏提供了全新的发展平台。拥有知名 IP 资源的游戏企业可聚合 IP 粉丝人群与企业品牌游戏用户，扩大游戏产品的受众群体，并在新玩家中进一步提高企业品牌知名度，增强企业的竞争优势。

我国游戏企业不仅在全球占有一席之地，而且研发实力、品牌形象和国际化水平都较 PC 时代取得巨大提升，更有很多游戏企业走出国门迈向世界。譬如《王者荣耀》海外版已经在全球 80 多个国家和地区上线运营，其他多款动作、RPG 和策略类游戏也正在服务亿万

海外玩家。腾讯研发并在全球运营的《绝地求生》，也标志着中国企业已经能够为全球顶级 IP 赋予高水平的研发和运营。

目前，中国、日本和韩国分别占据着亚太地区游戏市场规模的前三名。未来几年内，中、日、韩的游戏市场将保持稳定增长。亚洲其他地区（不包括中国、日本和韩国）的游戏收入增长将会呈现快速增长的态势。未来几年内，亚太地区人口红利仍将持续推动当地游戏市场快速增长。相比于其他地区，亚太地区人口基数庞大。以上便是游戏行业概况及现状分析所有内容了。

3.董鑫欣：《职务侵占罪疑难问题的司法认定》

刑法第 271 条第 1 款规定了职务侵占罪，职务侵占罪是司法实践中的常见犯罪，也是理论研究的重中之重。但是，无论是理论界还是实务界，对本罪的"其他单位"、犯罪主体、职务便利、财物等构成要素的争议不断，至今未有消弭。2016 年 4 月 18 日施行的《最高人民法院、最高人民检察院关于办理贪污贿赂刑事案件适用法律若干问题的解释》大幅度提高职务侵占罪的定罪量刑数额标准，拉大了职务侵占罪和盗窃罪、诈骗罪、贪污罪的定罪量刑标准，进一步激化了上述争议。笔者不揣浅陋，拟结合司法裁判实例，围绕上述争议焦点提出个人浅见，以期对理论研究和司法实践有所裨益。

一、职务侵占罪的"公司、企业或者其他单位"认定

（一）"其他单位"是否要求法人或者依法成立

刑法第 271 条规定：公司、企业或者其他单位的人员，利用职务上的便利，将本单位财物非法占为己有，数额较大的，处五年以下有期徒刑或者拘役；数额巨大的，处五年以上有期徒刑，可以并处没收财产。国有公司、企业或者其他国有单位中从事公务的人员和国有公司、企业或者其他国有单位委派到非国有公司、企业以及其他单位从事公务的人员有前款行为的，依照本法第三百八十二条、第三百八十三条的规定定罪处罚。据此，职务侵占罪的"公司、企业或者其他单位"，从所有权性质上而言，一般而言是指非国有单位。问题是，"其他单位"，还包括哪些单位？其内涵和外延该如何界定？是否要求是"法人"？是否与刑法第 30 条和第 163 条的"单位"一致？

第一种观点认为，此处的单位，应当是和公司、企业同样具有法人资格的非企业法人，比如

私立学校、社会团体等，不包括村民小组、业主委员会等群众性自治组织。第二种观点认为，此处的单位，不要求具有法人主体资格。笔者同意第二种观点。

应当说，此处的"单位"，实质上是"被害单位"，应当与犯罪主体的"单位"具有一致性。根据刑法第 30 条，犯罪主体的单位，一般指具有法人格的公司、企业、事业单位、机关、团体。但我国刑法的单位犯罪毕竟不同于国外的法人犯罪。我国单位犯罪的主体，还包括非法人组织，既包括村民委员会、居民委员会、村民小组等常设性机构，也包括为组织体育赛事、文艺演出或者其他正当活动而成立的组委会、筹委会、工程承包队等临时性组织。现代刑法罪刑法定原则的形成、演变过程，充分说明刑法从过去单纯强调形式层面到现代同时强调实质层面。也就是说，刑法中的单位范畴，要大于民法中的单位范畴，并非限于法人，只要依法成立、实行独立的经济核算能力，具有相对独立的财产和意志、能够以自己的名义承担一定责任的组织，都应当认定为刑法中的"单位"。

刑事司法解释及规范性文件也多次予以确认。比如，1999 年 7 月 3 日施行的《最高人民法院关于村民小组组长利用职务便利非法占有公共财物行为如何定性问题的批复》规定：对村民小组组长利用职务上的便利，将村民小组集体财产非法占为己有，数额较大的行为，应当依照刑法第二百七十一条第一款的规定，以职务侵占罪定罪处罚。村民小组只是村民委员会下设的组织，并不具备法人格，但实践中的村民小组往往具有班子成员、议事规则和村民自筹的集体财产，具备单位的相关属性。因此，最高人民法院的批复确认了其作为刑法中的"单位"属性。根据当然解释的原理，村民小组的上级组织村民委员会，更应认定为单位。

又如，最高人民法院 2001 年 1 月 21 日印发的《全国法院审理金融犯罪案件工作座谈会纪要》规定：单位的分支机构或者内设机构、部门，以单位的分支机构或者内设机构、部门的名义实施犯罪，违法所得亦归分支机构或者内设机构、部门所有的，应认定为单位犯罪。不能因为单位的分支机构或者内设机构、部门没有可供执行罚金的财产，就不将其认定为单位犯罪，而按照个人犯罪处理。显然，单位的分支机构或者内设机构、部门不仅并非法人，往往还不能独立承担刑事责任。最高人民法院明确了刑法的"单位"不同于民法中的"法人"，凸显了刑法解释不同于民法解释的独立品格。刑法关注对犯罪行为的谴责，民法关注对损害的弥补。

再如，最高人民法院、最高人民检察院 2008 年 11 月 20 日发布的《关于办理商业贿赂刑事案件适用法律若干问题的意见》规定：刑法第一百六十三条、第一百六十四条规定的"其他单位"，既包括事业单位、社会团体、村民委员会、居民委员会、村民小组等常设性的组织，也包括为组织体育赛事、文艺演出或者其他正当活动而成立的组委会、筹委会、工程承包队等非常设性的组织。根据体系解释的原理，职务侵占罪的"单位"，应当与非国家工作人员受

贿罪的"单位"一致，也应当与单位犯罪中的"单位"一致。

根据 1997 年 7 月 3 日施行的《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》相关规定，如果具备单位特征，不属于"为进行违法犯罪活动而设立"或"设立后以实施犯罪为主要活动"，就应当认定为单位犯罪。因此，职务侵占罪的"其他单位"，也应适用此规定。即使由于没有依法登记或者没有经主管部门依法批准或备案，形式上存在瑕疵的，都不影响单位的属性认定。司法实践中也持此观点。

【案例 1】覃某职务侵占案（单位的合法性质认定直接影响有罪无罪的定性）

广西柳江县人民检察院起诉书指控：1998 年 3 月至 12 月，被告人覃某在担任柳江县百朋镇农村合作基金会（下称农基会）服务部主任期间，指使服务部工作人员在收取部分借款利息时，以占用费和虚设的管理费开票，从中截留 72642 元不入账，并于 12 月底造册分掉。其中覃某分得 2.7 万元，出纳、会计等人各分得 1.5 万余元不等。公诉机关认为覃某身份国家工作人员，利用职务之便截留公款私分侵吞，构成贪污罪。

广西柳江县人民法院经审理认为：农基会是未经依法批准擅自设立，从事吸收存款、发放贷款等金融业务的机构，不是合法组织，并非国有单位。被告人覃某虽为国家工作人员（百朋镇农经站的农经员），但其在与其公职身份无关且不具备合法主体的组织内从事活动，未受机关委托，不属于从事公务，侵犯的对象是不合法组织从事金融业务产生的利润，不属于刑法意义上的公共财物。故被告人覃某的行为不符合贪污罪的构成要件，也不属于刑法调整范围。

广西柳江县人民检察院抗诉后，柳州市中级人民法院经审理，除了确认一审事实外，还查明：农基会成立后，于 1996 年取得了广西壮族自治区农村合作基金会办公室办法的"内部融资许可证"。柳州市中院认为：基金会农村、农业的互助组织，并非金融机构，也不是企业，无需中国人民银行批准及进行工商登记。根据《广西农村基金会设立、变更、撤销审批管理试行办法》（以下简称《办法》），基金会按照《办法》规定取得了"内部融资许可证"，原判认定为不合法组织不当（笔者注：国务院于 1999 年 1 月发布 3 号文件宣布正式统一取缔农村合作基金会）。农基会是集体组织，覃某任职系理事会推选，虽无镇政府等机关委派不属于从事公务，但隐瞒其他股东将不入账的"管理费"私分，属于利用服务部主任的职务便利且具有非法占有的故意。鉴于覃某具有自首、退赃情节，据此，柳州市中院撤销一审判决，以职务侵占罪判处覃某有期徒刑一年缓刑一年。

【案例 2】卢某职务侵占案（群众性自治组织属于职务侵占罪的被害单位）：

1997 年，卢某经上海市闵行区虹光小区上海虹中房屋业主大会推选，被任命为业主管理委员会（下称业管会）执行秘书，负责物业维修资金的筹集、使用和管理工作。其在履职期间，与某投资公司相关人崔某、顾某的结伙，将存于该公司的业管会基金按照存款年息 22%产生的利息，通过告知业管会年息为 11%的方式，将利息 44 万元与崔某、顾某瓜分，其得款 25 万元。后上海市闵行区人民法院以职务侵占罪判处卢某有期徒刑 6 年。

笔者认为，上述二个案例体现了职务侵占罪"其他单位"法律属性认定的原则。案例 1 的一审法院认为基金会系不合法组织，营业款并非公款，被告人在该组织内从事活动并非公务，言下之意即不合法组织、不合法活动、不合法财物不属于刑法保护的法益，不宜追究行为人的刑事责任。案例 1 的二审法院和案例 2 的法院则认为，即便被害组织并非法人主体，没有经过严格的业务许可，只要符合相关规定，依然应当纳入刑法调整范围。

（二）"其他单位"是否包括个体工商户和个人合伙

职务侵占罪的单位是否包括个体工商户和个人合伙？第一种意见认为应当包括,主要理由刑民不同，刑法更注重平等保护，个体工商户和个人合伙虽在民法上属于自然人范畴，但可认定为刑法中的单位。第二种意见认为不应当包括，理由主要是个体工商户和个人合伙均是特殊的自然人，均不是经济实体，也不是独立的诉讼主体，不符合单位的本质特征。

笔者同意第二种意见。判定个体工商户、个人合伙是否具有职务侵占的犯罪主体资格，关键看是否具备"单位"的组织体特征。法律对个体工商户和个人合伙具有明确规定。根据《民法通则》第 26 条和《最高人民法院关于贯彻执行<民法通则>若干问题的意见》第 41 条、《最高人民法院关于适用<中华人民共和国民事诉讼法>的解释》第 59 条等相关规定，个体工商户不是组织，而是与自然人、法人、非法人组织并列的民事主体，可以营业执照登记的业主（户主）名义作为诉讼主体参与民事诉讼。根据上述相关规定，个人合伙是非法人组织的一种，按是否起字号分别以登记的字号或者全体合伙人为诉讼当事人，负责人或者推举人作为诉讼代表。可见，个人合伙属于松散的组织。

如上所述，刑法中的单位，无论是犯罪主体还是被害对象，都是具有相对独立财产和意志且能够承担法律责任的相对独立组织。个体工商户，顾名思义，是指"个体"和"家庭户"，是个人或者家庭投资经营、以个人和家庭财产承担责任的特殊民事主体，本质上与自然人无异。个人合伙，并不是企业形态，也不是独立的诉讼主体，该"组织"松散，法律也并不对合伙的

人数、书面协议、议事规则、登记备案等组织体要素进行强制要求，不具备单位的组织体特征，本质上依然是自然人的简单联合。因此，法律也明确规定，其合伙人对外必须承担无限连带责任。个体工商户、个人合伙既非民法意义上的单位，更非刑法意义上的单位。诚然，笔者并不否认个体工商户需经有关部门核准取得营业职照，个体工商户、个人合伙可起字号，也可聘请雇员，享有一些自然人所没有的特殊的权利，但这些权利均系为了方便其从事民事活动，并不能改变其自然人松散组合、无组织体相对独立的本质特征。理论界和司法实践中也主要持第二种意见。

【案例 3】张建忠侵占案（侵占个体工商户财物不属于职务侵占）

广东省佛山市禅城区人民法院对自诉人朱绚丽提起自诉的被告人张建忠涉嫌侵占罪一案，经审理查明：2003 年，被告人张建忠利用其任佛山市禅城区红太阳不锈钢加工厂(以下简称红太阳加工厂，系个体工商户，投资人朱绚丽)驾驶员的职务之便，在该厂安排其独自一人开车将一批价值人民币 8 万余元的不锈钢卷带外出送货之际，将该批货物擅自变卖他人，并弃车携变卖所得款 4 万元逃匿，后被抓获。法院以张建忠犯侵占罪判处有期徒刑一年。

笔者认为，由于个体工商户、个人合伙不属于单位，对于个体工商户、个人合伙所聘的雇员、帮工、学徒，故无论被雇佣或者聘请的人员称谓如何，均不属于具有"职务"，不能成为职务侵占罪的主体。

（三）"公司"是否包括自然人成立的一人公司

现行《公司法》于 2005 年修订时增设了关于一人有限责任公司的规定。职务侵占罪的公司是否包括自然人成立的一人公司？在当时公司法修订前后确存有争议，但经过刑法理论界和实务界的研究，现在主流意见一致认为只要一人公司依法成立，具有独立的人格、财产和法人治理结构，不属于"为进行违法犯罪活动而设立"或"设立后以实施犯罪为主要活动"，即只要一人公司从事了一定的合法经营活动，其实施的犯罪应当按照单位犯罪而不是个人犯罪处理。据此，一人公司也应当成为刑法保护的被害单位，即职务侵占罪的公司包括一人公司。

（四）"企业"是否包括个人独资企业和合伙企业

按照《个人独资企业法》和《合伙企业法》，个人独资企业是自然人以其个人财产对企业债务承担无限责任的经营实体，普通合伙企业是以（普通）合伙人对合伙企业债务承担无限连带责任的经营实体。二者与一人公司具有法人格不同，也与个体工商户和个人合伙本质上属

于自然人的属性不同。职务侵占罪的"企业"是否包括个人独资企业和合伙企业？一般认为，个人独资企业和合伙企业都是商主体，具有较为独特的法律属性和法律地位，在法律属性上介于法人和自然人之间。故刑法理论界和实务界除了肯定说、否定说的二种观点外，尚有区别说（也称折中说）。

笔者同意区别说，认为原则上职务侵占罪的其他单位不包括个人独资企业和合伙企业，但特殊情况下则可以包括。主要理由如下：首先，按照《个人独资企业法》和《合伙企业法》的规定，个人独资企业和合伙企业毕竟并非法人主体，不具备独立的意志和财产，一般不宜认定为单位犯罪的主体，故一般也不宜认定为被害单位。其次，刑法认定毕竟不同于民法认定，对于规模较大的个人独资企业和合伙企业，尤其是人数众多的按份所有的有限合伙企业，如果具有相对独立的组织机构、财产和意志形成机制，基于刑法重实质认定和公平认定的原则，从法理上看，可以且应当将这类个人独资企业和合伙企业认定为单位犯罪的主体。但是，基于罪刑法定的原则，目前尚不宜将个人独资企业和合伙企业解释为职务侵占罪中的"企业"，从长远来看，可以通过司法解释或者指导案例予以明确。

二、职务侵占罪的特殊主体认定

是不是只要被害单位具备上述"公司、企业或者其他单位"的条件，该单位的人员均能构成职务侵占罪的主体呢？实践中，驾驶员、保安、快递员等服务行业的体力劳动者，临时工、实习生、兼职人员等并非单位固定用工人员，通过冒充成为职员和离职后冒充原单位职员的人员，是否属于本罪的主体，都是常见的争议焦点。笔者认为，对于上述人员是否纳入本罪主体应着眼于法益保护，关键在于如何解释"公司、企业或者其他单位人员"的"人员"。

刑法第 93 条专门对"国家工作人员"进行了解释，全国人民代表大会常务委员会于 2000 年 4 月 25 日专门就"其他依照法律从事公务的人员"进行了立法解释，最高人民法院 2003 年 11 月 13 日印发的《全国法院审理经济犯罪案件工作座谈会纪要》还进一步对"国家机关"、"委派"、"从事公务"、"其他依照法律从事公务"进行了司法诠释。与此不同，职务侵占罪的"人员"并无任何对应的对应解释，仅有上述的最高人民法院《关于村民小组组长利用职务便利非法占有公共财物行为如何定性问题的批复》就个案进行了批复。理论和实践中对"人员"是否要求要求限定为正式员工、从事管理工作，曾经历了一个从严格要求到具体区别的转变过程。

（一）驾驶员、保安、快递员等人员是否属于本罪主体

驾驶员、保安、快递员基本上属于从事体力劳动，且从事的工作往往是辅助性的工作，如果其占有的单位财物并非其职权所管理、经手的，不能成为职务侵占罪的主体，反之，原则上都应当认定为职务侵占罪的主体。

【案例 4】邵某职务侵占案（驾驶员属于职务侵占罪主体）

2015 年 1 月 21 日下午，被告人邵某、顾某某经预谋后，利用被告人邵某系被害单位张家港保税区诚安达运输有限责任公司驾驶员负责运送乙二醇 37 吨（连车总重 54.3 吨）的职务便利，在苏州市吴江区盛泽镇吴江新民化纤有限公司卸货时，采用由被告人邵某控制阀门进行截留 18 吨，在出门过磅称重作弊制造全车已卸货假象并由被告人顾某某以几百元收买 A 保安的手段，希望让保安签收 37 吨的磅单。在保安接到库房要求重新检查过磅电话且未签单时，二人随即匆忙开车逃离，后将其车内的价值人民币 104200 余元的乙二醇销赃得款人民币 79700 元。一审法院以职务侵占罪，判处邵某有期徒刑二年三个月，判处顾某某有期徒刑二年十个月，二审维持原判。

对本案的定性，存在三种意见：第一种是认为邵某、顾某某构成职务侵占罪，理由又分为利用邵某的职务便利和利用 A 保安职务便利；第二种认为邵某、顾某某构成盗窃罪，理由在于邵某仅是运输驾驶员，不具备职务便利，乙二醇是封缄物；第三种认为邵某、顾某某构成诈骗罪，理由在于邵某、顾某某主要作案手段是过秤作弊，A 保安打出榜单主要是因为受骗而非拿到好处。笔者认为，第二种、第三种意见虽有一定理由，但均不够准确。第三种意见没有正确认识到本案的受害单位是张家港保税区诚安达运输有限责任公司而非吴江新民化纤有限公司，保安打单后并未签单确认，并无处分行为，自然不会依单向张家港保税区诚安达运输有限责任公司付款，吴江新民化纤有限公司并无实际损失。第二种意见认为邵某是运输驾驶员而无职务便利，并不准确。应该说，除了公私属性不同，职务侵占罪的"职务"并不等同于贪污罪的"职务"。就内涵而言，"职务"的基本含义指职位规定应当担任的工作。但是，职务是一项工作，并不等同于"职权"，利用职务便利不限于利用管理职权。职务除了职权性的管理活动，也包括具体的业务活动，即持续地、反复地从事的工作，也区别于临时性、一次性的委托事项。显然，邵某作为驾驶员，并非临时受托运输，而是基于其长期、固定的岗位职责，应当认定为职务侵占罪的主体。当然，如果驾驶员是临时性接受委托从事某事务，则不应当认定为其职务便利，自然也不属于职务侵占罪的主体。比如，阳某原系某公司的驾驶员，平时经常驾车送公司出纳员赴银行提取单位的工资款。一次，公司出纳员因身体不适请阳某代为提取，阳某提款 40 万元以后卷款而逃。此案驾驶员阳某将临时代为保管的他人

财物非法占为己有，应当构成侵占罪而非职务侵占罪。

随着现代运输业、物业、快递业的迅猛发展和劳务派遣的广泛兴起，驾驶员、保安、快递员确实已不像以往仅仅从事辅助性的工作，基本上都是独立开展某方面的工作。根据具体职责情况，驾驶员、保安、快递员是完全可以成为职务侵占罪的主体。

（二）临时工、实习生、兼职人员等非正式员工是否属于本罪的主体

司法实践中，临时工、实习生、兼职人员等利用从事单位业务活动的便利条件，侵占所在单位财物的现象并不鲜见，这些主体是否属于本罪的主体存有争议。比如笔者所办理的卜某职务侵占案。

【案例 5】卜某职务侵占案（用人单位非法用工的员工属于职务侵占罪主体）

2011 年 4 月，卜某到杭州某汽车配件有限公司应聘，公司让担任售后退货员利用管理售后退货，约定先试用一段时间，公司未与其签署劳动合同也不缴纳社会保险，工资给其发放现金。试用期间，卜某单独或伙同公司销售员、仓库发货员等人，利用管理售后退货、经手公司仓库的汽车配件等职务便利，多次侵占经手配件、从公司仓库窃取配件，合计价值人民币 2.2 万余元。

公安机关以盗窃罪移送审查起诉，笔者提出了职务侵占罪的定性意见，检察机关以此罪名起诉后，获得了法院生效判决支持。本案中，汽配公司违法用工，卜某并非公司的正式员工。但是，如上所述，相对于民商法注重刑事合理性，刑法注重的是实质合理性。职务侵占罪主体评价的关键并非是有无在职、在编人员身份的形式，而是在一定时期内是否履行工作职责。理论界和实务界也持此观点。比如于庆伟职务侵占案。于庆伟是北京市联运公司海淀公司临时工，负责从本单位领出货物并办理托运手续等发送业务，在发货时将价值 2 万余元的货物取出，分别藏匿于女友处和寄给朋友。法院将起诉罪名盗窃罪改判为职务侵占罪。又如贺豫松职务侵占案。贺豫松系郑州火车站委外装卸工，2003 年至 2005 年间，其在当班装卸旅客托运的行李、包裹时，多次窃取手机、电脑、电磁炉等物品，合计价值 4 万余元。法院将起诉罪名盗窃罪改判为职务侵占罪。再如刘宏职务侵占案。刘宏在公司担任车间代理主任，2007 年 7 月合同到期后，因公司暂停生产，未与其续签合同。9 月，刘宏利用其保管的仓库的一把钥匙（仓库有二把锁），趁车间暂停生产无人之机，采用开锁和撬锁的方式，进入仓库窃得合计价值 5 万余元的财物并销赃。法院将起诉罪名盗窃罪改判为职务侵占罪。这些指导案例充分说明，临时工等非正式用工可以成为职务侵占罪的主体。

（三）冒用身份取得职务的人员能否成为本罪的主体

对于冒用身份取得职务的人员，是否可以成为职务侵占罪的主体，笔者认为不可一概而论。一般而言，对于冒用身份取得职务，如果是基于职务较长一段时间稳定履行职责，在此过程中利用职务之便侵占所在单位财物的，应当认定为职务侵占罪；反之，如果是基于隐瞒身份取得信任，随即骗取财物逃离的，则应当认定为诈骗罪。

【案例 6】马某诈骗案（虚构事实同时或先后应聘，向招聘单位以项目招待费用报销等名义骗取财物应认定为诈骗罪）

被告人马某虚构其长期和军队做项目，到有关公司应聘销售经理、采购经理、客户经理等职务，尔后虚构项目招待费、报销等名义从公司领取款物。2011 年 4 月至 2012 年 10 月，马某以上述手段先后或者同时到九个公司应聘并担任经理，在每个公司分别骗得价值 2 万至 10 余万不等的款物，合计 68 万余元。公诉机关以诈骗罪起诉，辩护人以职务侵占罪辩护。法院审判认为，马某虽经应聘取得了被害单位客户经理的职位，其虚报的招待费等款项亦属于利用职务便利谋取公司财物的行为，但其连续 9 次通过虚构项目而获得职务，并借此虚报职务费用的行为，本质上系马某为达到诈骗目的而实施的手段行为，故应当认定为诈骗罪。最终，马某被一审法院判处有期徒刑 11 年后未上诉，判决随后生效。

本案中，一审法院认为，诈骗罪和职务侵占罪存在法条交叉竞合。一般情况下，诈骗通常作为职务侵占的手段行为，应当按照目的行为吸收手段的原则，应认定为职务侵占罪。但是，在目的行为系轻行为手段行为系重行为、特定案件事实中目的行为和手段行为吸收关系逆转、职务侵占罪的构成要件不完全的特殊情况下，应当认定为诈骗罪一罪。本案符合前二种情形，其一，诈骗罪的处断重于职务侵占罪；其二，马某在较短时间内在 9 家公司任职，且同一时段内在不同公司的任职，可见并非真正意义的履职，不应当认定为职务主体。

笔者认为，一审判决的结论是对的，第二点理论作为依据也是较为充足的，但是第一点理由并不能成立。诈骗罪和职务侵占罪是有所交叉的，但重合部分属于一般和特殊关系，应当适用特别法条优先的处断原则，并非牵连犯关系适用从一重的处断原则。马某之所以被判处诈骗罪，体现出了刑法实质认定原则。如果行为人因其他原因而不是因非法占有的动机冒充身份应聘取得职务，在履职过程中侵占财物的，则应认定为职务侵占罪。

【案例 7】姚某诈骗案（冒用身份应聘后利用职务便利侵吞货款应性职务侵占罪）

2014 年 3 月份，被告人姚某以"古瞻峰"的虚假身份证通过网上应聘到汕头市潮阳区棉北街道得源饲料厂担任货运驾驶员。同年 7 月 18 日，得源饲料厂负责人安排被告人姚某与江某一起运载货物往揭阳市并收回货款，被告人姚某见有机会侵吞货款，便说服郑某由其一人负责送货。随后被告人姚某便独自一人开货车将货物运载至揭阳市交还货主郑某，并收回货款现金人民币 37550 元，被告人姚某随即携带货款逃离，后用于偿还赌债。公诉机关以职务侵占罪起诉，被告人和辩护人对指控罪名没有异议，法院以职务侵占罪判处姚某有期徒刑一年。本案就是典型的冒充他人身份应聘，后再履职过程中产生非法占有目的，利用职务便利占有单位财物的典型案例。应当说，以虚假的身份证应聘后在履职过程中利用职务便利非法占有所在单位财物的定性，在理论界和实务界均争议很大。《最高人民法院研究室关于对行为人通过伪造国家机关公文、证件担任国家工作人员职务并利用职务上的便利侵占本单位财物收受贿赂挪用本单位资金等行为如何适用法律问题的答复》规定：行为人通过伪造国家机关公文、证件担任国家工作人员职务以后，又利用职务上的便利实施侵占本单位财物、收受贿赂、挪用本单位资金等行为，构成犯罪的，应当分别以伪造国家机关公文、证件罪和相应的贪污罪、受贿罪、挪用公款罪等追究刑事责任，实行数罪并罚。笔者认为，基于客观主义立场，上述答复意见值得参照，对于冒充身份担任公司、企业或者其他单位职务的，又利用职务上的便利实施侵占本单位财物的，应当认定为职务侵占罪。当然，笔者提出的仅是一般的区分意见，关键还是要结合具体案情具体分析。

（四）离职后冒充原单位职员能否成为本罪的主体

离职后冒充原单位职员的人员，是否可以成为职务侵占罪的主体，不可一概而论。一般而言，只要被害单位在解除行为人的职务时履行了公示义务而无过错，行为人冒充原单位职员骗取原单位客户货款，一般应认定为诈骗罪；反之，被害单位并未有效解除行为人的职务时，行为人实质上仍继续履行职务的，造成单位客户基于表见代理情形下的合理信赖，一般则应定性为职务侵占罪。

【案例 8】梁某职务侵占案（离职后继续利用原单位职务身份取得客户货款应认定为职务侵占罪）

被告人梁某长期担任某保险公司职员，期间，利用职务之便收取投保人保费 40290 元后挥霍。2010 年 3 月 1 日，公司对其作出通报批评并解除保险代理合同，但未收回空白合同、保单、

收据等物。后梁某隐瞒被解除保险代理的事实，继续持相关手续，收取投保人保费 78132 元并挥霍。后梁某投案自首。一审法院认定梁某分别构成职务侵占罪和诈骗罪，分别判处有期徒刑一年六个月和三年，合并执行有期徒刑是三年。梁某上诉后，二审法院改判为职务侵占罪一罪，判处其有期徒刑三年，缓刑五年。

笔者认为，本案二审法院改判是正确的。梁某虽然被解除保险代理关系，但其仍拥有空白合同、保单、收据，足以以原职务身份履行职责，从民事角度上而言成立表见代理，投保人并无过错，也不应承担损失，并非实际被害人；而保险公司应当履行保险合同，属于实际上的被害方。故梁某被解除代理合同的后续行为应构成职务侵占罪而非诈骗罪。

三、职务侵占罪的利用职务便利认定

（一）职务便利与劳务的区分

根据我国职务侵占罪的立法演变可以看出，"职务"是严格区分于"公务"的。最高人民法院 2003 年 11 月 13 日印发的《全国法院审理经济犯罪案件工作座谈会纪要》专门规定：公务主要表现为与职权相联系的公共事务以及监督、管理国有财产的职务活动。如国家机关工作人员依法履行职责，国有公司的董事、经理、监事、会计、出纳人员等管理、监督国有财产等活动，属于从事公务。那些不具备职权内容的劳务活动、技术服务工作，如售货员、售票员等所从事的工作，一般不认为是公务。问题是，职务是否包括劳务活动、技术服务工作呢？

笔者认为，所谓"职务"，指职位规定应当担任的工作，其本质在于对单位财产的控制、支配地位。职务侵占罪的保护法益是公司、企业或者其他单位的财产占有关系，而现代服务业的兴起，决定了大量的劳务型单位、服务型单位的广泛存在，为了平等、充分保护此类单位的财产，利用职务上的便利应当包括从事职权性管理活动的便利和从事劳务活动、技术服务工作的便利。否则，劳务人员利用劳务之便侵占本单位财物的行为，不可能归入侵占罪或者其他罪名进行评价，显失公平。司法实践中，驾驶员、保安、快递员等基本从事劳务活动的人员被认定为职务侵占罪的主体，也充分说明了职务包括劳务活动、技术服务活动，在此不再赘述。

当然，对于并非利用从事劳务对财物控制、支配的职务便利，而是利用对工作环境的熟悉来窃取财物的行为，应认定为盗窃罪而非职务侵占罪。

【案例 9】赵某盗窃案（利用熟悉工作环境窃取财物应认定为盗窃罪）

被告人赵某原系河南省濮阳市"腾力大厦"总服务台收银员。"腾力大厦"总服务台收银员采用

轮流值班制，收银员在值班时收取的钱款保存于总服务台现金抽屉，并应于轮班时交接或上缴。该现金抽屉及钥匙由当值收银员轮流保管使用。1999 年 3 月中旬某日，赵某在"腾龙大厦"总服务台值班时，利用其当值掌管钥匙之便，私配了一把总服务台现金抽屉的钥匙，伺机行窃。3 月 17 日凌晨 4 时许，赵某选择在他人值班之日，趁无人之际，用私配的钥匙打开存放现金的抽屉，窃得现金 19905 元后逃离。

本案就是典型的利用熟悉工作环境而窃取所在单位财物的典型案例。赵某从事劳务性质的收银工作，具有管理、支配账款的职务便利，但其并没有利用此职务便利侵吞账款，而是选择自己不当班又无人之际的窃取手段，尽管客观上也利用了其在履职过程中掌管钥匙的职务之便，但这并非是认定其犯罪行为性质的决定因素。

（二）代理公司业务签署合同而非法占有货款是利用职务之便还是利用合同进行诈骗

【案例 10】宋某职务侵占案（利用代理公司业务的职务之便将签订合同所得财物予以侵吞应认定为职务侵占罪）

2011 年 8-9 月，被告人宋某经人介绍与"瑞阳公司"口头约定，为该公司销售无氧铜丝，对外以"瑞阳公司"名义与客户签约，货款由客户打入指定账户，对内被告人宋某不受公司人事管理的约束，不参与考勤等事项，仅按照其销售数量获取每吨 50 元的报酬。2013 年 3 月至 4 月，宋某以"瑞阳公司"名义与多家公司达成供货协议，上述公司按照协议将货款打入宋某指定账户。到款后，宋某将其中 81 万余元占为己有，用于购买彩票。后宋某投案自首。

公诉机关以合同诈骗罪和职务侵占罪提起公诉，被告人和辩护人认为宋某签约行为系职务行为，购买彩票不属于非法占有，应认定为挪用资金罪一罪。法院经审判以职务侵占罪判处有期徒刑十三。梁某以同样理由上诉后，二审法院维持原判。

笔者认为，本案宋某利用了职务之便，也存在一些的欺骗客户和公司的行为，但界定宋某行为性质的关键在于其非法占有款项的归属性质和其是否利用职务之便。如果宋某占有的款项属于其所在单位，则其行为应认定为职务侵占罪，如果宋某占有的款项属于客户支付给宋某个人，则其行为应认定为合同诈骗罪。宋某行为属于代理"瑞阳公司"的行为而非个人行为，其与客户签署的合同也是有效的，客户打入的款项应当认定为"瑞阳公司"所有。宋某采用欺诈方式要求客户打入自己指定的账户而非"瑞阳公司"账户、未上交货款给"瑞阳公司"并非占有财物的决定方式，其具有收取货款的职务之便才是决定方式。因此，判决是正确的。实际上，司法实务主要持此意见。比如《刑事审判参考》刊载的虞秀强职务侵占案，与本案极其相似。金维公司与陈敏公司开展合作，由金维公司提供资金、陈敏公司提供场地和设备。后

陈敏公司亏损，虞秀强作为金维公司的副总经理，以金维公司名义与巨化锦纶厂发生业务关系，巨化锦纶厂按惯例将 38 吨己内酰胺销售给代表金维公司的虞秀强，虞秀强在收到本应交给公司的货物后，以非法占有为目的，擅自将货物予以销售，取得货款及销售款 759750 元后，除用于支付宏大经营部等三家单位货款及运费，个人将其余 444310 元予以侵吞。公诉机关和一审法院认定虞秀强构成合同诈骗罪和职务侵占罪二罪，虞秀强上诉后，二审法院改判为职务侵占罪一罪。

（三）超越职权范围实施欺诈行为而非法占有财物是否属于利用职务之便

司法案例中，有的行为人在履职过程中超越职权范围，对所在单位的客户、顾客实施欺诈行为，骗取客户、顾客支付款项。此种行为该认定为职务侵占罪还是照诈骗罪，存有争议。

【案例 11】董佳、岑佳、胡群等职务侵占案（以假充真侵占门票收入款的行为构成职务侵占罪）

2000 年 8-9 月，被告人董佳、岑炯、胡群经预谋后商定，利用董、岑两人在上海东方明珠广播电视塔有限公司工作的便利，伪造东方明珠塔观光券出售牟利，随后由胡群负责伪造观光券。后胡群找人伪造观光券并交给董、岑两人。董佳将伪造的东方明珠塔观光券在东方明珠观光塔售票处出售，岑炯则检票让购买伪造观光券者进入东方明珠电视塔进行游览观光。至案发时，已扣押伪造并使用的东方明珠塔观光券 4313 张，其中 65 元票面存根 1392 张，50 元票面 2921 张，董佳、胡群、岑炯从而侵占东方明珠公司的票房收人人民币 236530 元。法院判处董佳、胡群、岑炯构成职务侵占罪。

本案中，被告人董佳、岑炯等以假的观光券冒充真的观光券向游客出售，客观上存在欺骗游客及倒卖伪造票证行为，但不应以诈骗罪和倒卖有价票证罪定罪处罚。董佳等被告人虽实施了以假充真、欺骗游客的行为，但其所意图占有的对象并非游客的财物，而是东方明珠塔的门票收入。欺骗游客、倒卖伪造票证只是被告人达到侵占所在单位东方明珠塔门票收入的一种手段，一种具体的行为方式，意在通过这种"偷梁换柱"的方式来掩盖对单位票款的非法侵占。所以在本案性质的判定中，立足点应当放在非法占有的对象物这点上。首先，本案表面上所直接侵占的是游客的钱款，实质上属于东方明珠公司的应得的门票收入，应当认定为东方明珠公司的财产；其次，游客并未受到损失，并非实质上的被害人，电视塔公司损失了票款，是真正的被害人；再次，董佳、岑炯分别利用售票员和检票员的职务便利，侵占了所在单位的票款收入，完全符合职务侵占罪的构成特征，构成职务侵占罪。

（四）内外勾结的职务侵占案件和贿赂对合案件认定

2000 年 7 月 8 日施行的《最高人民法院关于审理贪污、职务侵占案件如何认定共同犯罪几个问题的解释》第 2 条规定：行为人与公司、企业或者其他单位的人员勾结，利用公司、企业或者其他单位人员的职务便利，共同将该单位财物非法占为己有，数额较大的，以职务侵占罪共犯论处。但是，司法实践中，对于何为利用"利用公司、企业或者其他单位人员的职务便利"理解，存在争议。比如说，内外勾结的职务侵占案件与贿赂案件难以区分，不少职务侵占案件都曾被当作贿赂案件处理。笔者办理的钱某职务侵占案便是一例。

【案例 12】钱某职务侵占案（利用采购职务便利抬高采购价格并要求供应商账外给予"

2009 年底至 2011 年 6 月，钱某在某公司担任采购员期间，利用负责与供应商谈判采购业务并拟定采购价格的职务便利，与供应商应某在商定采购价格的基础上，再抬高的采购价要求供应商按高价签订合同，并要求公司在多支付采购资金至供应商后，再由供应商扣除因虚高采购款产生的税费后，将余款以"回扣"方式通过现金、转账到个人账户的形式返给钱某。钱某以此方式得款 76 万余元。

公安机关以钱某涉嫌非国家工作人员受贿罪、应某涉嫌对非国家工作人员行贿罪移送审查起诉。笔者提出了职务侵占罪的整体定性意见，并认为应某属从犯，属情节轻微可不起诉。检察机关以此罪名仅对钱某起诉（对应某以情节轻微不起诉），获得了法院生效判决支持。本案中，表面上是应某在供销业务中给予某公司的钱某商业"回扣"，应某采购某公司的产品，实质上是钱某利用采购商的优势地位，要求应某配合，采用抬高采购价的诈骗方式，骗取所在单位某公司的钱款，应认定为职务侵占罪。浙江省高级人民法院后将此类案件作为指导案例发布。职务侵占行为限于作为而包括不作为，对于企业员工履职过程中不作为且收受对方"好处费"，造成所在单位财物损失，则构成非国家工作人员受贿罪。

【案例 13】余建军、赵德夫职务侵占案（职务侵占罪的主观故意是直接故意，且具有非法占有被单位财物的目的，履职过程中单纯不作为而收受"好处费"的构成非国家人员受贿罪）

A 公司是经营供电供热的企业，被告人余建军是该公司的员工，负责供汽管道检查、修理和供汽单位蒸汽流量表安装、检查、修理、抄录蒸汽用量数据以及收取蒸汽价款。

2007 年 6 月，A 公司向 B 公司供应蒸汽。B 公司的赵德夫为了少付蒸汽使用费，擅自拆开蒸汽流量表人为减少用量数据。余建军在抄录蒸汽供应单位，怀疑 B 公司在蒸汽流量表做手脚，但未反映给 A 公司，按照蒸汽流量表的数据抄录，而 A 公司则按照余建军抄录数据与 B 公司结算价款。为了让余建军不将蒸汽流量表动手脚一事反映。2007 年 10 月至 2009 年 3 月，赵德夫先后每月送给余建军 2000 元或者 3000 元现金或者等价的购物卡券，合计 38000 元。期间，B 公司少付给 A 公司蒸汽价款 20 万余元。

2009 年 4 月至 12 月，余建军不再抄表，采用编造数据的方法报至 A 公司并据此结算蒸汽价款并告知赵德夫。赵德夫为了使蒸汽流量表显示的真气用量与 B 公司已付蒸汽使用量享福，有时则适用上述方式认为调整蒸汽流量表显示数据。期间，赵德夫送给余建军财物合计 31000 元，B 公司少付给 A 公司蒸汽价款 24 万余元。

公诉机关以二人涉嫌共同职务侵占罪起诉，一审法院认定，赵德夫构成盗窃罪、职务侵占罪，余建军构成非国家工作人员受贿罪、职务侵占罪。公诉机关抗诉后，二审法院维持原判。

笔者认为，法院对余建军行为的定性是正确的。本案可分为二个阶段，第一阶段，余建军主观上并没有非法占有本单位蒸汽的故意和目的，客观上也没有积极编造数据骗取本单位蒸汽的行为，A 公司应收款损失是余建军不作为的后果，并非是其积极侵占的对象。虽然客户有调整流量表数据的行为，但余建军并未实施配合或者教唆的行为，二人也不构成共同犯罪。余建军收受的是客户单位的贿款并为其谋取利益，未将客户在蒸汽表动手脚的事项反映给 A 公司造成单位财产损失，同时也是在履行合同过程中玩忽职守的行为（因其并非国有公司员工，该行为不能追究以国有公司、企业、事业单位人员失职罪追究刑事责任），构成非国家工作人员受贿罪。第二阶段，余建军客观上与赵德夫分工实施，其负责积极编造数据，赵德夫负责人为调整用量数据，共同采用诈骗方式骗取 A 公司的蒸汽，主观上其已认识其和赵德夫的行为是骗取 A 公司蒸汽用量的行为，仍积极为之，二人共同构成职务侵占罪。

四、职务侵占罪的财物认定

（一）财产性利益是否属于本罪的犯罪对象

我国刑法并没有对"财物"进行定义，也没有区分财产和财产性利益。根据通说，刑法分则第五章的"财物"包含了财产性利益。司法实践中，一般也将财产性利益作为财产罪和贿赂犯罪的犯罪对象。比如，2002 年 4 月 17 日施行的《最高人民法院关于审理非法生产、买卖武装部队车辆号牌等刑事案件具体应用法律若干问题的解释》第 3 条第 2 款（现已被两高 2011 年 8 月 1 日起施行《关于办理妨害武装部队制式服装、车辆号牌管理秩序等刑事案件具体应

用法律若干问题的解释》取代，该解释第6条沿用并扩充了该规定）明确规定：使用伪造、变造、盗窃的武装部队车辆号牌，骗免养路费、通行费等各种规费，数额较大的，依照刑法第二百六十六条的规定定罪处罚。

又如，最高人民法院、最高人民检察院2008年11月20日印发的《关于办理商业贿赂刑事案件适用法律若干问题的意见》之"七"规定：商业贿赂中的财物，既包括金钱和实物，也包括可以用金钱计算数额的财产性利益，如提供房屋装修、含有金额的会员卡、代币卡（券）、旅游费用等。具体数额以实际支付的资费为准。

再如，2016年4月18日施行的《最高人民法院、最高人民检察院关于办理贪污贿赂刑事案件适用法律若干问题的解释》贿赂犯罪中的"财物"，包括货币、物品和财产性利益。财产性利益包括可以折算为货币的物质利益如房屋装修、债务免除等，以及需要支付货币的其他利益如会员服务、旅游等。后者的犯罪数额，以实际支付或者应当支付的数额计算。

司法实践中，对职务侵占罪的犯罪对象是否包括财产性利益，也基本参照上述文件，持认可意见，笔者在此不再举例赘述。

（二）信息、数据是否属于本罪的犯罪对象

财产性利益是否包括信息、数据等？《最高人民法院公报》2006年第11期就曾刊载"上海市黄浦区人民检察院诉孟动、何立康网络盗窃案"，认定网络虚拟财产可以成为盗窃罪的对象，但是在理论界和实务界均存在争议。职务侵占罪的行为方式是将合法管理、支配财产变成非法占有，不同于盗窃罪、诈骗罪的将未曾持有的财物变成非法占有。而根据我国刑法关于非法提供信用卡信息罪、泄露内幕信息罪、侵犯公民个人信息罪、非法获取计算机信息系统数据罪等规定，信息、数据可以成为其他罪的犯罪对象，也可能是职权管理的范围。对于利用职务便利窃取、出售信息、数据的行为，需要具体分析区别对待。

【案例14】王一辉等职务侵占案（利用职务便利盗卖单位游戏"武器装备"的行为构成职务侵占罪）

被告人王一辉原系盛大公司游戏项目管理中心运维部副经理，主要负责对服务器、游戏软件进行维护和游戏环境内容的更新等。2004年8月底，被告人王一辉与被告人金珂通过网上聊天，预谋利用王一辉在盛大公司工作，有条件接触"热血传奇"游戏软件数据库的便利，复制游戏武器装备予以销售。后被告人王一辉通过在盛大公司内利用公司的电脑进入游戏系统，同时打开"热血传奇"服务器6000端口，通过增加、修改数据库Mir. DB文件中的数据，

在金珂创建的游戏人物身上增加或修改游戏"武器"及"装备"，再由金珂将游戏人物身上的武器及装备通过"w!arw．5173．com"网站或私下交易出售给游戏玩家。至2005年7月三被告人共计非法获利人民币202万余元，其中王一辉非法获利122万余元，金珂获利42万余元。本案公诉机关以王一辉等人涉嫌侵犯著作权罪起诉，辩护人认为不符合侵犯著作权罪的构成要件，因刑法对财产权的保护仅限于有形财产和无形财产，不涉及虚拟财产，故被告人的行为不能以犯罪论处。法院判决王一辉等人构成职务侵占罪。

法院认为，本案涉案"武器"及"装备"可认定为无体财产性利益。网络游戏中的"武器"及"装备"是计算机软件运行后生成的结果，是一种虚拟财产，其在虚拟环境中的作用决定了其可以被人占有、使用等，但游戏玩家要取得虚拟财产除了花费时间外，还必须付出一定的费用，如购买游戏点卡的费用、上网费等，同时该虚拟财产通过现实中的交易能转化为货币，因此虚拟财产既有价值，又有使用价值，具有现实财产的属性。王一辉等人构成职务侵占罪，犯罪数额可按其销赃获利数额计算。

笔者认为，法院判决虽有道理，但也存在瑕疵。虚拟财产毕竟不同于现实财产，实际上并不具有真正的价值属性。1998年《最高人民法院关于审理盗窃案件具体应用法律若干问题的解释》（已废止）第五条第七款曾规定："销赃数额高于按本解释计算的盗窃数额的，盗窃数额按销赃数额计算"，销赃价格可以作为犯罪数额。但是，以销赃价格作为犯罪数额，本身也反映了犯罪数额决定于行为人销赃时和购买者议价的偶然因素，显然有悖法理。销赃数额高于实际盗窃数额的，被害人所遭受的损害并没有增加，以销赃数额作为盗窃数额，进而决定对行为人的定罪量刑，有失妥当。2013年4月4日施行的《最高人民法院、最高人民检察院关于办理盗窃刑事案件适用法律若干问题的解释》第四条第（五）项规定：盗接他人通信线路、复制他人电信码号出售的，按照销赃数额认定盗窃数额。似乎可以说明，除非"电信码号"等特殊物质可以销赃价认定犯罪数额，对于其他物品，销赃价能否作为犯罪数额并不明确。实际上，对于利用职务之便非法提供信用卡信息、泄露内幕信息、侵犯公民个人信息、非法获取计算机信息系统数据出售获利的，并非一律构成职务侵占罪，有可能构成其他犯罪。

【案例15】刘淼金等受贿案（国有医院员工利用管理、统计医院统方信息的职务便利将统方数据出售行为，应认定为受贿罪）

被告人刘淼金、姚传林均系庆元县人民医院信息科合同工，负责统计、管理医院计算机信息系统和数据信息。2010年1月至2014年1月，刘淼金单独或伙同姚传林，利用职务之便，

将医院计算机信息系统的"统方"数据信息非法提供给医药代表，并收取好处费。其中，刘淼金单独出售"统方"获利 209400 元，二人共同出售"统方"获利 109100 元。公诉机关以受贿罪提起公诉，有的辩护人认为应当按照非公家工作人员受贿罪定性，有的辩护人认为应当按照职务侵占罪定性。法院支持了公诉机关的指控，认定二被告人构成受贿罪。

本案中，暂不考虑二被告人的职务属于公务还是劳务，从判决结论可以发现，判决没有将二人职务便利之下的"统方"认定为"财物"，否则，二人构成的将是贪污罪或者是职务侵占罪，而非受贿罪（或者是非国家工作人员受贿罪）。实际上，刑法第 253 条之一的出售、非法提供公民个人信息罪的立法演变也说明了"信息"区别于"财物"。《刑法修正案（七）》增设此条文，并含有"国家机关或者金融、电信、交通、教育、医疗等单位的工作人员"的表述，《刑法修正案（九）》则删除了该有关主体的表述，并增设一款规定：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。"两高"则将原来的二个罪名"出售、非法提供公民个人信息罪"和"非法获取公民个人信息罪"同一调整为"侵犯公民个人信息罪"。从这可以看出，对于履行职责或者提供服务过程中获得的公民个人信息，并不属于财物，否则，出售个人信息的，将构成贪污、职务侵占罪而非侵犯公民个人信息罪。同理，对于在履职过程中出售国家秘密、内幕信息的，应当按照相应的犯罪进行处理，而非认定贪污罪或者职务侵占罪。

五、结语

职务侵占罪虽是常见的传统罪名，但随着经济社会的发展，无论是单位法律属性、主体形式、履职方式、还是财物表现形式，都有新的变化。笔者基于法益保护的目的，在刑法平等保护和实质认定的原则下，探讨了职务侵占罪疑难问题的相关司法认定。笔者认为，唯有法益保护的目的，贯通刑法平等保护和实质认定的原则，"往返于规范和事实之间"进行正义的解释，才能正确处理职务侵占罪与贪污罪、盗窃罪、（合同）诈骗罪的关系，才能协调职务侵占罪和其他在履职过程中谋取经济利益犯罪的关系，"实现'同案同判'的司法正义"，舒缓因所有制性质、身份不同所造成的刑法条文之间的紧张关系，从而提升司法公信力。

4.报道：擅自帮玩家修复游戏装备 工程师受贿 3 万获刑 2 年

中国法院网讯 （方一鸣） 27 岁的游戏工程师唐昊山擅自修复游戏装备，收受他人贿赂款 3 万余元。日前，北京市海淀区人民法院以非国家工作人员受贿罪判处被告人唐昊山有

期徒刑 2 年，缓刑 3 年。

2008 年 9 月至 11 月间，唐昊山利用其担任北京世模科技有限责任公司技术部数据库工程师，负责管理游戏数据的职务便利，擅自为该公司开发的网络游戏“丝路传说”的游戏玩家葛先生修复损坏的游戏角色装备、提升游戏角色装备的属性等级，先后五次收受葛先生贿赂款人民币 3.1 万元及中华牌香烟两条。

2008 年 11 月 9 日，北京世模科技有限公司将被告人唐昊山扭送至北京市公安局海淀分局经侦大队。

法院在审理过程中，被告人唐昊山将上述贿赂款人民币 32100 元主动上缴。

法院审理后认为，唐昊山身为有限责任公司职员，利用职务便利，非法收受他人财物，为他人谋取利益，数额较大，其行为已构成非国家工作人员受贿罪。鉴于唐昊山是初犯，在归案后及庭审过程中认罪态度较好；且主动退缴了全部贿赂款，具有悔罪表现，法院对其酌予从轻处罚，并适用缓刑，以观后效。最后，法院作出上述判决。

5.朱骏超：《游戏源代码的刑事法律风险》

1.离职员工抄袭老东家源代码获刑 2 年以上

近日，广东省广州市天河区人民法院审理了一起侵犯商业秘密案件。原告北京麒麟合盛科技有限公司(以下简称麒麟科技)主要从事提供海外移动互联网服务方面业务，其公司核心技术以及商业模式均应用在海外市场。

被告黄礼强、钱振鹏、李娴、裴智松 4 名被告人曾受雇于麒麟科技，在职期间，4 名被告人事先合谋，利用工作时掌握的产品源代码、商业运营资料等商业秘密，研发与公司类似的手机安卓系统清理软件产品营利，并在离职前将资料带走。

2016 年 10 月 26 日，4 名被告人筹备设立上海厚乘信息技术有限公司(以下简称厚乘公司)，公司营利性业务为手机安卓系统清理软件，这些软件基本功能相同，涉嫌源代码抄袭。

2019 年 5 月 16 日，广州市天河区人民法院认为黄礼强等 4 名被告人的行为已构成侵犯商业秘密罪。据此作出一审判决，判处黄礼强有期徒刑 2 年 4 个月 15 天，并处罚金 24 万元；对钱振鹏、李娴、裴智松分别判处有期徒刑 2 年 3 个月 15 日，并处罚金 15 万元；追缴 4 名被告人以及厚乘公司违法所得 680059.29 元，予以没收。同时，麒麟科技保留追究民事法律责任的权利。

2.员工泄露、出售、使用公司源代码属于犯罪

一般来说，员工为完成公司任务所完成的源代码属于职务作品，著作权归公司所有。因此，员工在离职时员工无权带走、泄露、出售源代码，否则可能涉嫌侵犯著作权罪或者侵犯商业秘密罪。

《刑法》第二百一十七条规定侵犯著作权罪规定，以营利为目的，未经著作权人许可，复制发行计算机软件的，违法所得数额较大的，处三年以下有期徒刑或者拘役，并处或者单处罚金；违法所得数额巨大的，处三年以上七年以下有期徒刑，并处罚金。

《刑法》第二百一十九条规定侵犯商业秘密罪，是指以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密，或者非法披露、使用或者允许他人使用其所掌握的或获取的商业秘密，给商业秘密的权利人造成重大损失的行为。给商业秘密的权利人造成重大损失的，处三年以下有期徒刑或者拘役，并处或者单处罚金；造成特别严重后果的，处三年以上七年以下有期徒刑，并处罚金。

案例

离职程序员带走《征途》网游源代码出售获利 13 万 法院判处有期徒刑 1 年 6 个月

2006 年 3 月，王某某进入上海征途网络公司，担任研发中心开发部程序员一职，负责征途网络游戏部分源代码的研发工作。3 个月后，王某某离开征途公司，还私自复制了服务端源代码、客户端源代码及辅助文档，这是征途公司具有独立著作权的征途游戏的程序。2007 年 3 月王某某，向两名买家出售了上述代码。同月 15 日、30 日，王某某又将上述服务端源代码等分别以 7 万元和 6 万元的价格卖给了其他人。与此同时，征途公司发现了征途游戏源代码被秘密复制外泄的情况，并立即报警。

法院经审理后认为，被告人王某某利用职务便利，未经著作权人许可，复制计算机软件并予以发行，违法所得数额较大，其行为已构成侵犯著作权罪，被判处有期徒刑 1 年 6 个月，并处罚金 5 万元。

3.付费购买/免费下载源代码牟利同样属于犯罪

特别强调的是，明知他人是非法获得源代码而付费购买、免费下载源代码，并以此进行牟利的同样可能构成侵犯著作权罪或者侵犯商业秘密罪。

案例 1

付费购买源代码架设私服，五被告被判构成侵犯著作权罪

上海网之易网络科技发展有限公司经暴雪娱乐国际公司授权，并经新闻出版总署、文化部批准，在中国大陆地区出版运营网络游戏《魔兽世界：熊猫人之谜》并享有相应的著作权。2012 年 10 月至 2013 年 5 月间，被告人池×、池×1、胡×、李×、吕×等人，在浙江省台州市东港大厦浙江拓讯网络技术有限公司内，利用从境外获取的服务器端程序及相关的客户端程序、登陆器软件等，架设《魔兽世界》私服，并以收会员费、贩卖虚拟物品等形式进行牟利。

最终五被告人被判犯侵犯著作权罪，判处有期徒刑二年六个月至五年不等。

案例 2

免费下载游戏软件源代码搭设私服，构成侵犯著作权罪

2012 年 6 月 21 日，上海易娱网络科技有限公司将计算机游戏软件《勇者之塔》在国家版权局进行了著作权登记，后授权深圳市腾讯计算机系统有限公司推广、运营该游戏。

2014 年 2 月初，嫌疑人李某未经著作权人许可，从网上下载该游戏的源代码，并租用服务器，非法运营名为“极品勇者之塔”的私服网站，通过游戏玩家向被告人李某控制的彩 8 平台、利保卡平台账户充值而获利，非法经营数额计人民币 14 万余元。同年 2 月 24 日起，被告人杨某明知被告人李某非法运行“极品勇者之塔”私服游戏，仍帮助其非法维护运营私服游戏。

最终，被告人李某、杨某被判犯侵犯著作权罪，判处有期徒刑并处罚金。

4.投资人明知盗窃源代码进行合作，涉嫌犯罪

投资人明知是盗窃的源代码仍进行合作的，可能涉嫌构成以营利为目的，侵犯著作权罪或者侵犯商业秘密罪的行为。

案例

投资人出资支持离职员工利用前东家源代码生产同类产品被判构成侵犯商业秘密罪

2006 年 6 月前后，周利勇、顾超峰与英迈克公司员工颜东红、褚立（四人均已判刑）商定自行成立公司，用英迈克公司的技术生产伺服电机及控制器。为此，顾超峰绘制了伺服电机电路图，褚立绘制了伺服电机机械图，颜东红、周利勇、顾超峰窃取了公司伺服电机控制系统的源代码等技术资料。后周、颜、褚以不同理由离开英迈克公司。

2007 年 2 月，被告人吴某知颜、周等人以窃得的英迈克公司源代码生产同类产品，仍与上述人员签订协议，以出资 50 万元入股，获得广数公司 15%的股权，并参与产品生产及销售。

最终被告人吴某犯侵犯商业秘密罪，判处有期徒刑二年六个月，缓刑三年，并处罚金十二万元。

5.源代码保护的实务建议与反思

游戏行业源代码的泄露非常严重，导致私服、外挂、抄袭严重泛滥，这是也是由于游戏公司未规划保密制度导致的，因此游戏公司在内部应制定相应保密制度，防止源代码泄露。

1、游戏公司应对其游戏软、硬件等核心商业秘密采取保密措施，限制接触人员，防止单个员工掌握全部游戏代码；

2、设立源代码风控制度，规定所有接触游戏代码的人员必须登记、签字确认；在游戏源代码中埋伏特殊、错误或无效的代码或标记，以便举证；

3、与接触源代码、游戏核心设计的员工签订保密协议，并根据情况增减保密内容；

4、对于游戏核心人员应签订完善的竞业禁止协议，约定不超过两年的合理竞业禁止期限，避免核心员工加入其他竞争游戏公司而造成对本公司游戏产品的重大冲击和破坏。

5、对离职核心员工的去向进行必要监测，以便在游戏公测期而非上市期能够尽快发现、遏制侵权行为。

6、对于已经发生的代码泄露或员工私自截留代码的，公司应当及时采取维权手段。采取法律手段不仅能够挽回公司损失，还能通过维权对公司现有员工进行教育警示。

文章十、利用恶意程序“打劫”个人信息牟利如何定性

浙江省绍兴市越城区检察院曾办理一起案件：2013 年 5 月，邢某（另案处理）成立了北京瑞智华胜科技股份有限公司（下称“瑞智华胜”）。其后，瑞智华胜通过邢某成立的其他关联公司与运营商签订精准广告营销协议，获取运营商服务器登录许可，并通过部署 SD 程序（一种可以私下采集运营商流量里 cookie 数据的程序），从运营商服务器抓取、采集网络用户的登录 cookie 数据，并将上述数据保存在运营商 redis 数据库中，之后利用研发的爬虫软件、加粉软件远程访问 redis 数据库中的数据，非法登录用户网络账号，实施强制加粉、爬取公民个人信息等行为，从中牟利。

案发前，瑞智华胜发现浙江某网络有限公司（下称“网络公司”）调查公民个人信息被爬情况，遂将服务器数据删除。经鉴定，SD 程序运行后可以实现对指定网卡网络传输流量数据包进行获取并解析的功能；爬虫软件运行后可以绕过系统保护措施，提取公民个人信息；加粉软件运行后可以绕过系统保护措施获取用户信息，并对指定账号添加好友。案发后经查，

周某系瑞智华胜的法定代表人，负责公司运维部的各项工作；黄某系瑞智华胜股东，负责通过关联公司与运营商签订营销协议，获取运营商服务器登录权限；梁某、石某、袭某等系瑞智华胜员工，主要负责 SD 程序、爬虫软件、加粉软件的部署、研发和维护。该案办理中，司法人员对于计算机信息系统的判断、非法获取计算机信息系统数据罪中“情节严重”的认定以及涉计算机类犯罪和侵犯公民个人信息犯罪之间的罪数关系等方面存在分歧。

近日，《人民检察》杂志特邀请专家学者和办案单位代表对有关焦点、难点问题进行研讨。

关于计算机信息系统的判断

依照国务院《计算机信息系统安全保护条例》（下称《条例》）的规定，计算机信息系统是由计算机及其配套设备、设施作为信息载体的系统。网络时代背景下，有观点主张应将网络平台、移动客户端、App 软件系统等应用程序纳入“计算机信息系统”。对此，浙江大学光华法学院互联网法律研究中心主任、副教授高艳东认为，随着信息技术的发展，计算机已经从硬盘、CPU 等硬件设备，演变成数据处理系统。刑事立法设计时“计算机信息系统”的重点是“计算机”，而今天其重点是“信息系统”。对法条术语应当按照社会的发展变化进行与时俱进的客观解释，而不能拘泥于立法者的原意，这是解释新型犯罪的基本原则。中国社会科学院大学副校长、教授林维分析，按照最高人民法院、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》（下称《解释》）第 11 条规定，“计算机信息系统”和“计算机系统”是指具备自动处理数据功能的系统，包括计算机、网络设备、通信设备、自动化控制设备等。由此可知，设备仅仅是计算机信息系统的外在载体。诸如网络平台、移动客户端、App 软件系统等作为计算机信息系统的要素之一，其通过一系列硬件设施和应用程序，实现对信息和数据的采集、加工、存储、传输、检索，毫无疑问应当认定为计算机信息系统。

具体到该案，浙江省绍兴市越城区检察院副检察长汤隽认为，行为人侵害计算机信息系统的行为分为两个阶段：一是非法获取运营商服务器上网络用户的上网流量；二是通过筛选获取的 cookie 数据非法登录网络用户的账号，进行信息窃取或强制加粉。无论哪一个阶段，都离不开对服务器数据的侵害。因此，应当将某网络平台纳入“计算机信息系统”的范畴内。

非法获取计算机信息系统数据罪中“情节严重”的认定标准

非法获取计算机信息系统数据罪的认定须达到“情节严重”的程度。这里的“情节”，是指已发生的现实危害，还是包括有可能发生的实害，以及对于《解释》第 1 条规定的“其他情节严重的情形”应如何界定，目前司法实务中还存在一定的分歧，尚未形成统一的标准。

对此，林维谈到，考虑到《解释》第 1 条规定的前四项“情节严重”的范围已经包括了网络金融服务类的身份认证信息、其他身份认证信息以及非法控制计算机信息系统的数量和违法所得、经济损失等因素，那么第五项规定的兜底条款就没有必要也不应等同于前述情形。对于“其他情节严重的情形”的解释，核心在于情节严重的综合判断。“其他情节严重的情形”可以包括犯罪前、犯罪过程中乃至犯罪后表征行为的客观危害性和行为人的主观危险性等各种情节。阿里巴巴集团安全部高级专家谢虹燕认为，非法获取计算机信息系统数据罪作为结果犯，须达到“情节严重”的标准方可入罪，行为人一旦非法获取了计算机信息系统中的数据，就已经发生了现实危害。至于后续对非法获取的数据的其他不法利用，应当另行评价。

涉计算机类犯罪和侵犯公民个人信息犯罪之间的罪数关系

不管是司法实践中，还是刑事法理论层面，对于涉计算机类犯罪和侵犯公民个人信息犯罪之间的罪数关系都有颇多争议，焦点往往集中在牵连犯与吸收犯、想象竞合犯与数罪并罚之间。对于该案所涉及的非法获取计算机信息系统数据罪、破坏计算机信息系统罪和侵犯公民个人信息罪之间的罪数关系，高艳东认为，cookie 数据的主要内容是登录凭证，是一种网

络身份认证信息，属于数据。但这种网络身份认证信息只用于用户与网站之间的登录，并不包含可以识别个人身份信息的内容，因而不属于公民个人信息，对其进行非法获取也就不构成侵犯公民个人信息罪。其次，利用爬虫软件等爬取公民个人信息的行为，既构成侵犯公民个人信息罪，也构成非法获取计算机信息系统数据罪，属于两罪的想象竞合。再次，使用加粉软件强行加粉的行为，是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，构成破坏计算机信息系统罪。

具体到该案，谢虹燕认为，首先，周某等人在运营商不知情的情况下在运营商服务器中私自部署 SD 程序非法抓取网络用户的登录 cookie 数据并予以保存，这一行为系通过恶意软件从运营商服务器中非法获取数据，破坏了运营商计算机信息系统的安全性，应当构成非法获取计算机信息系统数据罪。其次，获取到用户 cookie 数据后，周某等人又利用爬虫软件从不同的网络平台爬取用户的公民个人信息，应构成侵犯公民个人信息罪。再次，周某等人爬取用户个人信息的目的是为了分析用户的行为，利用加粉软件对用户账号进行强制添加好友，从中牟利。在强制加粉这一环节，周某等人冒用用户的身份登录相关网络平台，采用不断更换 IP 地址、破解网站接口加密验证等技术手段，强行为用户账号添加好友，构成破坏计算机信息系统罪。可见，周某等人爬取用户个人信息的目的是为了给用户账号强制加粉并以此非法牟利，属于手段和目的的牵连犯，其行为同时构成侵犯公民个人信息罪和破坏计算机信息系统罪，应择一重罪处罚，即按照破坏计算机信息系统罪定罪处罚。综上，该案中，对周某等人应当按照非法获取计算机信息系统数据罪和破坏计算机信息系统罪数罪并罚。

关于该案定性，高艳东认为，对周某等人应按照非法获取计算机信息系统数据罪、侵犯公民个人信息罪和破坏计算机信息系统罪三罪数罪并罚。谢虹燕认为，该案中，周某等人的行为构成非法获取计算机信息系统数据罪和破坏计算机信息系统罪，应数罪并罚。汤雋认为，该案中，瑞智华胜及周某等人的行为均构成非法获取计算机信息系统数据罪。

（详见《人民检察》2019 年第 18 期）

文章十一、 江苏海门破坏计算机信息系统案

1.一起彻头彻尾的冤假错案—从庭审直播看徐昕律师代理的江苏海门计算机案

江苏南通海门计算机案是一起彻头彻尾的冤案，为完成指标业绩，跨省抓捕民营企业家、大学生创业团队，炮制冤案，幸得北京理工大学法学教授徐昕出面喊冤、推动冤案平反，最终结果仍待法院判决。

2018 年 12 月 13 日、2019 年 1 月 10 日于江苏南通市海门法院公开审理的一起破坏计算机信息系统案，是知名法学家、北理大徐昕教授参与推动的一起重大冤案，作为最后一名被告张某的辩护人，徐教授坚持“证据完全断裂、无罪理由非常充分”并通过多种渠道为其喊冤，多名微博媒体人、知名律师也认为“这就是一起彻头彻尾的冤案”。

海门检察院起诉书称，被告单位武汉粤楚公司于 2018 年 1 月期间，由公司主管人员被告人张某在 59DDOS 网站注册会员并充值，提交对被害人陈某等人经营的教育培训公司的网站 IP 的 DDOS 攻击任务，由被告人唐小平等进行操作，共造成 11 台计算机信息系统不能正常运行的后果。

从二次庭审直播来看，起诉所指控内容不仅遭全盘否定，而且多方观点反而印证了本案是一起彻头彻尾的假案。庭审直播表明，控方提出的观点均遭辩方驳回且控方或没有证据、或证据本身错误。笔者从中整理了 6 大疑点、1 大亮点，其中的任何一点，都能够证明本案是一起彻头彻尾的冤假错案、不仅徐律师代理人张某无罪、其余 3 名购买者也应宣告无罪，

暂未遭到起诉的3000余名会员，也不应当追究刑事责任。我们按起诉逻辑逐条分析：

疑点一：张某和粤楚公司究竟是什么关系 是否是“公司主管人员”？

庭审中，张某否认、粤楚公司法人代表否认、粤楚公司高管否认。

张某辩护人之一、季刚律师指出其没有拿到教育公司工资、奖金、社保医保，没有参与公司管理、负责公司事务，因此指控事实错误。公诉人以工商执照上的注册信息支撑其论点。那么张某究竟是否是公司主管人员、法律上的主管人员又该如何认定呢？

最高人民法院关于单位犯罪的司法认定规则：《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，法〔2001〕8号）单位犯罪直接负责的主管人员和其他责任人员的认定：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。应当注意的是，在单位犯罪中，对于受单位领导指派或奉命而参与实施了一定犯罪行为的人员，一般不宜作为直接责任人员追究刑事责任。

公开资料显示，张某是粤楚公司早期投资人，实际持股20%，后于2015年6月离开教育公司并创立人力资源公司、并在人力公司全职工作至今。不难看出，张某和粤楚公司的关系是投资人关系，不是雇佣关系、更不是“公司主管人员”。就好比你购买一家公司股票，你和出售股票的公司的关系是投资人和被投资单位关系，投资人违法、被投资单位就该被追究吗？如此逻辑，全球上市公司，谁还敢发行股票？

显然，张某是公司主管人员，这一指控是错误的。值得一提的是，公诉人并没有指出公司主管究竟管什么，张某究竟管什么。作为一起计算机案的单位犯罪，单位技术负责人无疑是排查重点，而这个重点、负责该公司网络技术陈某却被撤案、作为出纳员的张某被公诉，着实令人费解。

疑点二：在59DDOS网站注册会员并充值的人是谁？

庭审中，张某认可支付行为，因其在人力公司负责出纳，日常支出都是通过其支付宝，但对注册59DDOS会员行为不知情。

公诉人指出张某与陈某一同前去购买了一张未实名电话卡，由陈某出资，用于注册会员。张某辩解是陈某让他陪同去购买，买了有什么用并不知情，而陈某也持同样的辩解。这里结合在审判长陆卫东法官宣读的陈某第一次笔录里，陈某讲到他提出的DDOS、张某并不懂这些来看，陈某的嫌疑无疑更大。

在双方各执一词的前提下，警方从张某支付宝中找到了几笔充值付款记录，以证明张某是注册人。张某也对付款行为表示认可，但提出“我是公司出纳、扫码支付没有显示付款内容（购买DDOS）、陈林告诉我是买优化工具，在公司他是我领导、在家他是我哥，他要我付我就付了”等情况以证明其对注册会员并不知情。警方也在陈某手机里，找到了用陈某手机号注册会员的记录、接受短信验证码记录、加平台客服QQ好友的记录，但警方却不知何故将陈某撤案。

因此，究竟是谁在59DDOS上注册会员，警方未查明、公诉人凭感觉、法官也很困惑。

疑点三：提交攻击任务的人又是谁？

庭审中，张某否认在2018年1月提交对11台计算机的攻击。

根据常理，登录网站会留下相关痕迹，用户可以通过360安全卫士删除或者点击浏览器右上方设置删除，未删除的则会保留在电脑cookie、历史访问记录里。公诉人认为根据现场查扣的电脑登录名来看，有一台以张某名称拼音命名的27寸苹果一体机里存在相关记录。笔者了解到，被扣电脑一共6台，其中3台机器为苹果公司产品，其中张某日常使用的一台是21寸苹果一体机、陈某使用的是一台27寸苹果一体机、另一台27寸苹果一体机属于公司成员办公共用。三台苹果机均是由陈某购买、设置账户，除陈某自行使用的苹果机外，其

余 5 台电脑的密码都是一样的。但由于该电脑登入账户名称是以张某命名，故检察机关直接将此台机器定性为张某个人使用设备。但公司成员都承认这台设备一直都是被大家公用着，一直被用来查阅资料、看看视频而已。

这里有几个疑问，第一，6 台电脑中，究竟有几台涉案？第二，这 6 台电脑，分别是谁使用，公诉人未当庭指出。第三，作为公司公用使用的电脑，有没有可能被其它人使用？换句话来说，陈某有没有可能使用？第四，这 6 台电脑的保存、取证是否符合《电子数据取证规则》，有没有造假可能？

上述问题，从庭审举证、质证来看，都没有查明。

疑点四：平台开发商唐小平究竟有没有操作攻击？—全案关键、最大亮点

庭审中，唐小平表示，“会员提交的攻击任务需要我手动执行，确实存在遗漏的情况、有遗漏攻击的情况。”

平台开发商唐小平、平台制作人王岩、操作攻击人肖媛，三人的供词共同揭露了二个关键问题，第一，攻击平台是假的、需要平台老板手动攻击。2017 年 3 月份平台制作人王岩在猪八戒上以 1 万余元的报酬接受了唐小平的委托，制作的一个“供用户提交攻击任务”的平台，但该平台本身并不具备攻击性，即是一个用于骗人敛财的虚假产品。第二，攻击经常遗漏、没时间操作还可以多挣钱。真正能够攻击的工具是唐小平通过比特币付款向境外一个名为 str3ssed 的网站上购买的。唐小平本质是一个中介，多收钱少做事，利益才能最大化。

第二，唐小平和肖媛，都表示出去玩、睡觉、上班的时候，对于会员提交的任务视而不见、没有执行，经常遗漏也不会补，那么他们究竟操作了哪些、哪些又没有操作的？

显然，一个虚假的平台不可能有攻击能力、人为操作又遗漏了哪些攻击任务，遗漏的任务是不是本案的对象，办案人员依旧没有查明。

疑点五：多少台计算机受到影响 用什么来证明？—张某案关键、入刑标准

庭审中，季刚律师认为 11 台中有 3-4 台受到影响，徐昕则表示一台也没有。

破坏计算机信息系统罪是一个结果犯，必须要有客观证据来证明。而在张某案中，一点检方指控的 11 台也只是刚刚好达到入刑标准；二点究竟有几台受到影响、怎么证明受到了影响？这也是庭审交锋的一大看点，而这一点也直接决定了张某是否构成犯罪。

从证据来看，目前仅有按照警方“结果式设问”而得到的言词证据，几乎没有一份客观证据，例如服务器运行日志、流量防火墙日志等。据笔者从腾讯、阿里云了解到，国内服务器托管公司为配合公安办案，多设有专门部门负责证据的收集和提交，海门市公安、检察院为何没有调取？结合上一个疑点来看，是无法调取、还是担心调取结果不利于案件的发展而不敢调取？另外，作为受害者之一的北京一家公司有二个网址遭到攻击竟被指是张某所谓，但其主观故意是什么？公诉人无法回答。在场所有律师、被告人、审判长，连同旁听群众似乎都困惑。

当庭质证时，徐昕律师指出，11 个网站中 1 个根本没有任何证据、至少 3 个网站或 ip 不可能被 DDOS 攻击，其余只有被害人陈述，也不能证明受到了 DDOS 攻击，按两高一部《电子证据规定》来看，一个也没有。

可见，作为另一定案关键的造成后果方面，证据同样严重不足。到底多少台计算机收到影响，也没有任何客观证据。

疑点六：违法和犯罪区别在哪 检查员起诉的法条用对了吗？

事实上，徐昕教授还提出本案法律适用存在严重错误。

徐教授根据两高《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》指出，本案法律适用存在二大错误。

一、造成后果方面，应当适用《计算机解释》第 4 条第四款，造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机

信息系统不能正常运行累计一小时以上的。而不应按起诉书中指控第一款，造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的。这是因为 DDOS 的攻击危害在于网络，而不在于电脑软件和硬件。相关判例的法律适用亦能佐证这一观点。

二、购买行为不应当被追究，依法不构成共同犯罪，《计算机解释》第 9 条中，认定共同犯罪的三种情形，只有上述三种情形才能构成破坏计算机信息系统罪的共犯，而购买 DDOS 行为不包括在内，即并不是所有购买行为都构成犯罪。正如刑法规定贩卖淫秽物品是犯罪，没规定购买淫秽物品是犯罪，故该行为无罪。

不难看出，江苏南通海门计算机案是一起彻头彻尾的冤案、假案、错案，不仅事实不清、证据不足，还存在严重的法律适用错误问题。徐昕律师在庭审直播中展现的法学家风范、为当事人喊冤的态度、纠正办案单位错误的精神值得每一个法律人学习。

能否落实最高人民法院江必新副院长倡导的新裁判理念："坚持罪行法定原则，凡是刑事法律没有规定为犯罪的，一律不得作为犯罪追究；坚持疑罪从无原则，凡属证据不足、事实不清的案件，一律做无罪处理；坚持证据裁判原则，对证据不足的，不能认定为犯罪并给予刑事处罚。"就看这次南通市海门法院如何判决。

2.江苏海门破坏计算机信息系统案徐昕辩护词

江苏海门破坏计算机信息系统案系中国首例消费者在合法网站上被误导购买非法服务而追究刑责，也是迄今为止近千例同类案件中首例由知名律师推动喊冤的一例。北京理工大学法学院教授徐昕律师及南通市律协刑委会主任季刚律师为本案七名被告人中的最后一位做无罪辩护。

案件回顾：2016 年 5 月在深圳龙华新区注册的小灵猴公司在其合法备案的网站上推出网站排名优化、网页加速收录等服务，一年时间吸引了千余名会员注册、使用。为了增加收入，又于 2017 年 3 月起向注册会员推销网络压力测试服务（DDoS），并通过百度竞价推广、站长工具广告位等方式扩大知名度招募会员，以合法外衣误导消费者充值 17 万余元。3 月到 9 月期间，由于并未实际提供压力测试服务，遭到大量会员投诉，遂于同年 9 月通过比特币向境外购买 DDoS 工具，对会员提交的压力测试任务有选择性地、手动地、带欺骗性地执行。2017 年 11 月，本案被告单位粤楚公司因遭受同行长期恶意竞争，百余篇原创学术文章被抄袭、网站排名急转直下，在要求侵权人停止抄袭、寻求法律救济无果的前提下，公司前网络主管、网站设计制作者陈某迫于无奈，私下接受了小灵猴公司的推销，购买了相关服务。而张某（不在公司任职）作为陈林表弟，为其代付了相关款项，被卷入此案。海门检察院以其是公司主管人员、注册会员并充值、提交攻击任务并造成 11 台计算机信息系统不能正常运行而追究个人和公司刑责。

该案四名购买者均取保候审，海门检察院以证据不足两次退回补充侦查，一次延长审查起诉期限；法院两次开庭审理后，检察院以补充证据为由提出建议延期审理。近日此案已恢复审理，暂无新证据出现，海门法院将择日宣判。

该案的判决结果将直接影响到，民营企业在著作权遭受侵犯而得不到法律上的及时救济，面对正在发生的、紧迫的不法网络侵害、导致巨大经济损失时，要不要维护自身合法权益、要不要进行"正当防卫"；也为今后消费者在被不法分子以正规公司合法名义误导购买非法网络服务、产品后，是否应当承担责任、应承担怎样的责任这一问题提供了范本。以下为徐昕律师对本案的辩护词。

计算机犯罪应规范取证，坚持证据裁判

——张某涉嫌破坏计算机信息系统罪一审辩护词

尊敬的审判长、人民陪审员：

审判长在庭审时说，“我们的案件一般都要庭审直播，面向全世界的直播，不庭审直播的要经过法院纪检组同意”，海门法院对庭审直播的态度和刚性规定是国内少见的，希望全国法院向江苏海门法院学习!审判长多次强调要把事情搞清楚，有罪就是有罪，无罪就是无罪，不会冤枉一个公民，令人敬佩。我还要感谢审判长的慎重和耐心，尽管表现出有罪推定的倾向，甚至有点像公诉人，但我非常理解，劝张某是为张某好。

本案涉及两个法律问题：DDoS 攻击不可能造成计算机系统的主要软件或者硬件不能正常运行，起诉书适用法律适用错误；购买 DDoS 会员服务并非破坏计算机信息系统罪的共犯。关于事实问题，本案是能够也必须用客观证据证明的，但没有充分证据证明唐小平全部实施了 DDoS 攻击行为，更没有充分证据证明作为犯罪构成要件的“后果严重”之存在。因此，无论是严格适用法律，还是坚持证据裁判原则，皆应当宣告张某和粤楚公司无罪。其他三位购买者蔡季星、李荣洋、刘昌龙也应该宣告无罪，虽然前两人的律师不作无罪辩护，其中一位还责备我们的辩护耽误了她的宝贵时间。

一、DDoS 攻击对计算机软件和硬件并没有实际的破坏，不可能造成计算机系统的主要软件或者硬件不能正常运行，起诉书适用法律错误

起诉书指控，因为 DDoS 攻击，造成 11 台计算机信息系统不能正常运行，进而依据两高《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》（下称《计算机解释》）第 4 条第 1 款第 1 项“造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的”，认为张某构成犯罪。该指控是错误的。

（一）DDoS 攻击，不可能造成计算机信息系统的主要软件或者硬件不能正常运行

1、何为 DDoS 攻击？

DDoS 攻击即分布式拒绝服务(Distributed Denial of Service)攻击，是指借助于客户/服务器技术，将多个计算机联合起来作为平台，对目标服务器在较短时间内发出大量服务请求，占用部分网络资源。这种行为不会损坏计算机信息系统，不会删除、修改、增加计算机信息系统功能，而只是造成“网络堵车”，使网站或服务器短时间不能访问。在 DDoS 攻击下，被攻击的服务器收到超出其服务能力的大量请求，造成其服务质量降低，但软硬件仍在正常运行之中，软件和硬件的功能、数据和应用程序并没有破坏。DDoS 实际上只是造成了网络问题，并没有破坏计算机系统的软件和硬件。

《计算机解释》第 4 条第 1 款第 1 项的适用前提，是“计算机信息系统的主要软件或者硬件”。软件指一系列按照特定顺序组织的计算机数据和指令的集合，一般分为系统软件、应用软件；硬件指计算机系统中电子、机械和光电元件等组成的各种物理装置。网站是架设于网络服务器上的网络应用软件，对外部用户提供信息服务，是计算机信息系统的一部分。外部用户通常使用网络浏览器来浏览网站。通过浏览器访问网站的动作和行为，不会破坏计算机系统的数据和功能，显然不属于破坏计算机信息系统的软件或硬件的行为。因此，即便 DDoS 造成网站无法正常运行，也不会“破坏计算机信息系统功能、数据或者应用程序”、“造成计算机信息系统的主要软件和硬件无法正常运行”。

根据 DDoS 攻击的原理，DDoS 攻击使网站无法正常提供服务的原因，是短时间内大量访问请求占用了网站的“带宽”和“流量”。但这不等于使网站服务器无法正常运行，“网站无法提供服务≠网站服务器无法正常运行”，只要网络服务器没有硬件故障或软件故障，就仍然在正常运行。

2、公诉意见违反逻辑和常识

公诉人在法庭辩论阶段，长篇论述 DDoS 攻击符合破坏计算机信息系统罪的特征，辩护人从来没有说过 DDoS 攻击不是犯罪行为，不构成犯罪。我们提出的是：DDoS 攻击无法造

成计算机信息系统的主要软件或者硬件不能正常运行。公诉人逻辑跳跃，所谓 DDoS 攻击侵犯计算机信息系统的安全，干扰计算机信息系统的功能，这些说词无法达到证明目的。

公诉人说“破坏计算机信息系统罪所要求的破坏并不是狭义的，破坏的结果也不一定要求对受攻击计算机的硬件或软件遭到损坏。”这一说法与起诉书适用的《计算机解释》第 4 条第 1 款第 1 项“造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的”完全是相互矛盾的。

公诉人还说，“计算机信息系统主要包括软件和硬件。计算机信息系统不能正常运行当然符合计算机信息系统的主要软件或者硬件不能正常运行。”这个论证逻辑完全错误。计算机信息系统不能正常运行的原因很多，没电、断网都会导致不能正常运行，难道也是软件、硬件坏了吗？网络堵车就说是服务器坏了，这相当于堵车却说公路坏了。

公诉人甚至还称，“一个 IP 就是一台计算机”。这完全是信口开河。辩护人咨询了计算机专家：根据 IP 协议标准 RFC 791，IP 地址对网络节点的标识在于 2 个维度：（1）用网络号区分不同的 IP 网络；（2）用主机号识别该网络内的一个 IP 节点。因此，IP 的唯一值是相对于同一网络而言的，如果是不同的网络，IP 并不是唯一的。

IP 网络的复杂性决定了同一外网 IP 地址可能对应着多个内网 IP 的计算机，IP 地址不一定对应这服务器，对 IP 地址的攻击不一定是对服务器的攻击。IP 网络由多个网段构成，每个网段对应于一个链路，网络设备（路由器）负责将网段连接起来，在网络之间转发数据包。

上图为一个典型的 IP 网络拓扑图，路由器 1、路由器 2、路由器 3 接入 ISP 网络之后，形成了与互联网相互通信的三个网络。“用户主机”只能通过 IP 地址 149.82.58.207 访问“服务器 1”和“服务器 2”，同样只能通过 IP 地址 182.55.32.134 访问“服务器 3”和“服务器 4”。IP 地址 149.82.58.207、182.55.32.134 起到了路由寻址的作用，“用户主机“通过这些 IP 地址访问的也可能是其他的电脑和主机。因此，多次对同一 IP 实施攻击的行为，只是有可能影响到使用该 IP 地址进行路由的网络，并不会对特定的计算机进行破坏。

3、相关判例

辩护人检索中国裁判文书网等数据库，找到近年来 DDoS 攻击行为被认定为破坏计算机信息系统罪的案件约 50 件。这些案件中，法院认定“后果严重”和“后果特别严重”，一般都采取《计算机解释》第 4 条第 1 款第 3、4、5 项以及第 2 款第 2 项进行认定，即考量违法所得、经济损失、造成计算机系统累计不能运行时间。该类案件不适用第 1 项应当是现有司法裁判的共识。如提交的(2014)湖吴刑初字第 4 号，艾某破坏计算机信息系统案，适用第 3 项；(2018)浙 0110 刑初 266 号，刘某某、金某破坏计算机信息系统案，适用第 4 项；《刑事审判参考》第 1029 号，乐姿等破坏计算机信息系统案，适用第 5 项兜底条款。

综上，DDoS 攻击危害在于网络，而不在于电脑软件和硬件。DDoS 攻击结果是：网站对外部用户在网络上的服务质量下降，而不会造成网络服务器软件无法正常运行，而网站提供的网络信息服务不属于计算机信息系统的软件或硬件。因此，DDoS 攻击不可能造成计算机信息系统的主要软件或者硬件不能正常运行，故本案不应适用《计算机解释》第 4 条第 1 款第 1 项。

（二）本案只能适用《计算机解释》第 4 条第 1 款第 4 项

由于本案中不涉及《计算机解释》第 4 条第 1 款第 2 项的情形，也没有证据证明粤楚公司有任何违法所得或者造成了经济损失一万元以上，且网站属于计算机信息系统，因此本案只能适用《计算机解释》第 4 条第 1 款第 4 项的规定——“造成为一百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为一万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的”——来认定是否“后果严重”。

但本案中，涉及的被攻击网站，均为教育培训行业的宣传、招生网站，均不属于提供基础服务的计算机信息系统，也没有任何证据能够证明涉案网站或服务器是为一万以上用户提供服务的计算机信息系统，相反被害人陈述中提到的网站日常访问量、招生人数等内容，恰恰能证明被攻击网站的用户远低于一万。同样没有证据证明被告人行为导致网站不能运行累计一小时以上。故即便根据第 4 项的规定，也没有证据证明达到“后果严重”的入罪标准。

二、购买 DDoS 会员服务并非破坏计算机信息系统罪的共犯

《计算机解释》第 9 条规定，明知他人实施刑法第二百八十五条、第二百八十六条规定的行为，具有下列情形之一的，应当认定为共同犯罪，依照刑法第二百八十五条、第二百八十六条的规定处罚：

（一）为其提供用于破坏计算机信息系统功能、数据或者应用程序的程序、工具，违法所得五千元以上或者提供十人次以上的；

（二）为其提供互联网接入、服务器托管、网络存储空间、通讯传输通道、费用结算、交易服务、广告服务、技术培训、技术支持等帮助，违法所得五千元以上的；

（三）通过委托推广软件、投放广告等方式向其提供资金五千元以上的。

实施前款规定行为，数量或者数额达到前款规定标准五倍以上的，应当认定为刑法第二百八十五条、第二百八十六条规定的“情节特别严重”或者“后果特别严重”。

公诉人提出，购买方出资让攻击方进行攻击，两者构成了合意，购买方起指挥、决定作用。但根据该规定，只有上述三种情形才能构成破坏计算机信息系统罪的共犯，而购买 DDoS 的行为不包括在内。这意味着，法律通过沉默的方式表明购买 DDoS 服务的行为不属于犯罪。公诉人说没有买卖就没有伤害，这一流行的说法不是认定犯罪的理由，罪行法定，并不是所有的购买行为都是犯罪。正如刑法规定买卖野生动物是犯罪，但没规定吃野生动物是犯罪，故吃野味不构成犯罪；刑法规定贩卖淫秽物品是犯罪，没规定购买淫秽物品是犯罪，故该行为无罪；刑法规定贩毒是犯罪，没规定购买毒品自己吸食是犯罪，故该行为无罪。如此解释，才是罪刑法定原则的基本逻辑。公诉人认为提供技术的王岩、提交任务的肖媛是从犯，而购买者不仅构成犯罪，还是主犯。但我们检索判例，却没有发现追究购买者刑事责任的判例。本罪到底什么情况下构成共同犯罪，购买能否构成共同犯罪，值得研究。

如果将购买 DDoS 会员服务也认定为共犯，这意味着要追究 59ddos 网站 3000 余名注册会员的刑事责任，至少要追究几十名充值会员的刑事责任，但为何目前只起诉了四人？而且，公诉人将购买者确定为主犯，那岂不是放纵了 3000 主犯？明显荒唐！

三、本案证据严重不足，证据链断裂，特别是没有充分证据证明 DDoS 攻击行为已经实施

从粤楚公司购买 DDoS 服务到目标网站被攻击之间共有四个环节：

①购买 DDoS 服务并提交攻击目标→

→②唐小平获取攻击目标后登录 str3ssed.me 网站提交 DDoS 攻击任务→

→③str3ssed.me 网站对目标实施 DDoS 攻击→

→④被攻击目标遭到唐小平提交的 DDoS 攻击且攻击成功。

要想证明粤楚公司构成犯罪，必须证明上述每一个关键环节都全部实施了，且这 4 个环节本来都存在大量客观证据，可以且必须通过客观证据证明。但所有环节，均无充分证据予以证实。

（一）环节①，究竟是谁购买 DDoS 服务，谁提交攻击目标，证据并不确实充分

庭审中，粤楚公司的诉讼代表人陈述非常清楚，公司对此毫不知情，没有开会讨论过，没有谁决定过，也没有谁以购买 DDoS 服务为由找他报销，案发之后，公司才知道此事。

关于购买 DDoS 服务，张某的支付宝账号支付过，陈林的支付宝也支付过，且张某辩称有几次支付钱款是陈林直接让他扫码支付，称用于购买网络优化工具，但具体是什么，他并

不知情。

关于账号 17160254200 在 59DDoS 网站提交攻击目标，只能证明是尾号 4200 的用户提交了攻击目标，到底是张某提交还是陈林提交，因张某与陈林均否认，结合陈林懂技术、买黑卡、教张某等行为可以推断，主要任务应当是陈林操作。

（二）环节②，小灵猴公司即唐小平，并没有全部实施 DDoS 攻击任务

唐小平、肖媛、王岩供述证实，2018 年 4 月以前，www.59DDoS.com 不能自动进行攻击，必须在会员提交攻击任务后，唐小平手动去 str3ssed.me 网站操作。法庭调查表明，唐小平并没有全部执行会员提交的攻击任务。

1、本案鉴定意见存在严重问题，公诉人对辩护人的质疑并无进行有效回应，不能作为定案依据。

第一，鉴定的委托事项之一是“对 scy.087.com.cn 的功能进行分析，该网站是否具备对其他网络设备进行 DDoS 流量攻击的功能，上述流量攻击是否对被攻击目标具有破坏性。”但起诉书指控的是，粤楚公司于 2018 年 1 月期间，在 59ddos 网站注册会员并充值，提交攻击任务，对相关公司网站 IP 进行 DDoS 攻击。鉴定意见恰恰没有对 59ddos 网站进行鉴定。

第二，鉴定意见第 4 点，从上述网站“DDoS 攻击管理”页面检出攻击历史记录共 274 条。但这 274 条中，没有一个是尾号 4200 的用户提交的 IP 或网址。

第三，鉴定意见不明确。鉴定意见第 5 点称，从“用户操作记录”页面检出用户操作记录 1414 条，“用户操作记录”是什么？是攻击记录，还是提交记录？第 6 点称检出 1233 条任务记录，什么是任务记录？是接受任务，执行任务，还是攻击任务记录？

第四，鉴定称 scy.087.com.cn 网站具备向指定 IP 或域名的计算机发起 DDoS 流量攻击的功能与能力，对被攻击目标具有破坏性。这一意见与唐小平、王岩的供述完全矛盾，2018 年 4 月之前，该网站根本没有攻击能力。鉴定意见称有攻击功能与能力的时间点是何时？

第五，电子数据很容易编辑修改，但本案检材的同一性无法保证，鉴定的是不是扣押封存的检材，是否遭到编辑删改，没有任何证据证明。

2、唐小平当庭陈述，www.59DDoS.com 2018 年 4 月份之前没有攻击功能，此前的攻击任务，在他方便的时候，才会手动输入 str3ssed.me 网站，对目标 IP 进行攻击。可见，即便会员提交了攻击任务，账户费用被扣除，也存在唐小平不全部执行的情况。

唐小平庭前也曾供述，曾经有过接受会员充值以及提交任务但实际未实施攻击的情况。唐小平供述称“2017 年 5 月份就开始了，虽然当时开始接受会员充值，但是我当时没找到发动 DDoS 攻击的平台，没办法完成会员提交的任务”、“如果在 2017 年 9 月底之前提交任务使用了，费用就从他的账户上扣掉了，我也没有帮他发动 DDoS 攻击”、“所以一开始虽然我没有帮会员进行 DDoS 攻击，但是我还利用会员需要发动 DDoS 攻击来吸引会员充值。扣费的问题我当时确实没考虑好，没有帮会员发动网络攻击，我却把攻击的费用扣掉了，这个确实是我不对，是我欺骗了人家”。（补充侦查卷 P21）“59DDoS 网站可以增加会员攻击任务并执行攻击任务是 2017 年 9 月份左右，之前会员的充值都是没办法执行的，也就是 9 月份之前只有付费没有任务执行。也就是 5 月到 8 月会员付费是没有攻击任务执行，因为我没有可以执行攻击任务的平台网站，具体收费以充值记录为准，但是我会在 59ddos 攻击平台上显示攻击已执行，这些就是骗骗会员的。”（卷 2 P59）

3、肖媛庭前供述证明，并非所有会员提交的攻击任务都会执行。肖媛 2018 年 4 月 27 日的讯问笔录提到“唐小平还和我说，如果网址 PING 出很多 IP 地址，我们就不添加到空白处，这个攻击任务就放弃不执行了”、“执行攻击后会导致网站瘫痪，因为唐小平在执行攻击之前会检测这个网站，如果有用才会攻击，没有效果就不攻击。”肖媛当庭供述也印证了这一点。

4、接受平台发送会员提交攻击任务短信的手机持有人是肖媛和唐小平二人，肖媛庭前

供述证明，她并没有将其接收到的所有任务都准确无误、毫无遗漏地告诉唐小平。且还完全存在肖媛告知了唐小平但唐小平因疏忽或工作繁忙等原因而没有实施的合理怀疑。侦查人员问唐小平“如果肖媛在外面接到攻击任务，怎么办？”唐小平答：肖媛会视而不见；又问“既然肖媛不会跟你说，那你是如何增加攻击任务的？”唐小平答：看不到就算了。”又问“肖媛出去之后，是否还会收到任务攻击短信？”答“如果我忘记修改手机号码，她就会收到手机短信，但是她会视而不见。”（卷 2 P54）

5、唐小平存在虚假供述的动机。如果唐小平承认接受会员任务而不实际执行，则不仅仅会涉嫌破坏计算机信息系统罪，而且还涉嫌诈骗罪，出于趋利避害的心理，唐小平有可能虚假供述称全部执行了会员提交的攻击任务。

6、现有证据不足以证明唐小平购买了 DDoS 服务。不论是 str3ssed.me 网站还是 critical-boot 网站，均需要用比特币充值，唐小平供述是找一个叫支付宝名为“姚瑶”的购买后“姚瑶”帮其充值，但侦查机关出具的情况说明称“比特币的卖家姚瑶经多方查找尚未找到”，意即无法查证唐小平是否购买了 DDDoS 攻击网站的服务。

7、唐小平、王岩均证实，59ddos 网站，仅仅是用户提交攻击任务、用户充值的平台，而不是实施 DDoS 攻击的平台，由 59ddos 网站生成的套餐任务管理文档，不能证明唐小平实际操作了相关攻击任务，顶多证明会员提交了攻击任务。

8、李荣洋曾指责唐小平未执行攻击任务。（卷 13 P109-112 李荣洋和唐小平的聊天记录）

9、刘昌龙案中，以攻击目标 IP47.96.13.219 为例，套餐任务管理文档中显示，2 月 26 日，刘昌龙等（用户名 15360660648）提交了 11 次任务，但当天被害人没有收到阿里云服务器通知“被攻击”的短信。而同样的 IP 地址，2 月 3 日，刘昌龙等提交了 11 次套餐任务，被害人却收到了 2 条被攻击通知短信。这证明存在刘昌龙提交了攻击任务，但唐小平没有执行任务的情况。

10、套餐任务管理文档中的状态“已完成”，不能证明唐小平已执行用户 17160254200 提交的任务。scy.087.com.cn 远程勘验笔录所记录的“套餐任务管理文档”是基于 scy.087.com.cn 网站形成的，并不是真正实施 DDoS 攻击的网站所形成的，而仅仅是 087 网站中的用户操作记录以及网站程序设定给用户看到的状态的记录。用户在网站提交任务后，便会形成用户操作记录和套餐任务管理文档。但在 2018 年 4 月以前，59ddos 仅仅是接受会员任务的平台，不具有 DDoS 攻击功能，唐小平为了“欺骗”会员，使之误以为该网站有 DDoS 攻击功能，才在网站中设定了用户提交任务后的 6 分钟内会由“刷新中”变为“已完成”的程序。庭审已经查明，要想真正完成 DDoS 攻击，还需要唐小平在收到网站的通知短信后手动操作，加之唐小平有时不在电脑前或有其他拖延操作等原因，这一时间必然远超过 6 分钟。因此，套餐任务管理文档中的状态一栏，是程序自动设定的结果，而不是唐小平真实攻击的结果，不能证明唐小平已执行会员提交的任务。

关于唐小平的涉案金额，公诉人说“2017 年 5 月底开始收取会员费用，2017 年 9 月底唐小平开始接受任务去境外网站攻击，期间金额的认定，唐小平表示会员充值后若提交任务，会显示虚假的攻击已完成，若等到 9 月份提交任务，其还是会帮助攻击的……从有利于嫌疑人的角度出发，金额无法认定的情况下，对 5-9 月期间的收款仍认为 DDoS 攻击为目的，不再另定诈骗罪。”这说明公诉人认可唐小平不完全提交攻击任务的这一客观事实。既然如此，恰恰印证辩护人的主张，小灵猴公司即唐小平并没有全部实施 DDoS 攻击任务。

（三）环节③，没有证据证明唐小平提交的 DDoS 攻击任务全部实施

鉴定意见称“网站 scy.087.com.cn 具备向指定 IP 或域名的计算机发起 DDoS 流量攻击的功能与能力”，上文已论述，59ddos 网站在 2018 年 4 月前仅是一个收集会员任务信息的平台，4 月份以后王岩才帮唐小平将 critical-boot 网站攻击端口接入该网站，因此鉴定意见所鉴定

的结果只能反映 2018 年 4 月份之后 087 网站的功能，而不能反映之前的。而且鉴定意见至多能说明 critical-boot 网站有攻击功能，但 2018 年 4 月以前，唐小平使用的 DDoS 攻击网站是 str3ssed.me 网站，而非 critical-boot，因此鉴定意见不能证明 str3ssed.me 网站具有攻击性。

检方也没有任何证据能够证明，str3ssed.me 网站在唐小平提交了攻击指令后就实际执行了指令。侦查机关情况说明提到，str3ssed.me 网站服务器位于境外，无法调取网站镜像文件进行相关数据分析，只能远程勘验，且勘验发现该网站不保存日志，无法调取到以前的日志记录。因此，没有任何证据能够证明该网站实施了唐小平提交的 DDoS 攻击任务。

四、不存在作为犯罪构成要件的“后果严重”

环节④，远无充分证据证明。起诉书指控粤楚公司共造成 11 台计算机信息系统不能正常运行（起诉意见书为 10 台），如前所述，指控适用的法律错误，应适用前述第 4 项的规定。但即便按照第 1 项的规定，也没有充分证据证明存在“后果严重”。第一，11 台计算机信息系统受到攻击的证据严重不足；第二，11 台计算机信息系统不能正常运行完全没有证据证明；第三，即便 11 台计算机信息系统受到攻击且不能正常运行，也不一定是唐小平 DDoS 攻击所致。

虽然弘连司鉴【2018】计鉴字第 411 号鉴定意见中，17160254200 手机号在 scy.087.com.cn (www.59DDoS.com) 网站的攻击记录所显示的被攻击网站或 IP 有 14 个。但其中 www.318edu.com 的 IP 地址是 39.104.53.209， www.aolingaokao.com 的 IP 地址是 121.42.120.88，www.yb027.com 的 IP 地址是 121.199.250.170，因此实际上至多是 11 个目标网站。

目标网站受到了 DDoS 攻击的证据存在以下五个特点：

（一）除 4 份不具可采性的客观证据外，没有任何客观证据证明遭到 DDoS 攻击且不能正常运行

11 个目标网站或 IP 曾受 DDoS 攻击且因此导致网站无法正常运行，没有任何客观证据予以证明。特别是本案完全可以通过调取网站访问记录、网站服务器的访问日志等客观证据，多位被害人陈述有条件调取相关客观证据，但侦查机关不调取客观证据。虽然部分被害人提交了 4 份电子数据，但均不具可采性。

1、“www.whlexuejiaoyu.com”的管理公司武汉乐学世纪教育咨询有限公司皮之炼提供的聊天记录

该聊天记录只是复印件，且严重违反了电子数据的收集、提取程序。最高人民法院、最高人民检察院、公安部《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》第 8 条第 1 款规定，收集、提取电子数据，能够扣押电子数据原始存储介质的，应当扣押、封存原始存储介质，并制作笔录，记录原始存储介质的封存状态。该证据不仅违反该款，也不存在第 10 条规定的情形——“由于客观原因无法或者不宜依据第八条、第九条的规定收集、提取电子数据的”；即便存在也应当采取“打印、拍照或者录像等方式”固定相关证据，并在笔录中说明原因。

《最高人民法院关于适用<<font face="宋体">中华人民共和国刑事诉讼法>的解释》第 93 条要求对电子数据着重审查“是否随原始存储介质移送；在原始存储介质无法封存、不便移动或者依法应当由有关部门保管、处理、返还时，提取、复制电子数据是否由二人以上进行，是否足以保证电子数据的完整性，有无提取、复制过程及原始存储介质存放地点的文字说明和签名”。根据该解释第 94 条的规定，经审查无法确定真伪的电子数据，不得作为定案的根据。

退一万步，即便该聊天记录属实，也只能证明其公司网站曾受过 DDoS 攻击，但是否是唐小平实施的攻击，没有证据证明。而聊天记录恰恰证明，2017 年 9-10 月份也存在被攻击

的情况，但 17160254200 的注册时间是 2017 年的 11 月中下旬，完全不可能在 9-10 月份去攻击乐学公司的网站。

2、北京易维云数据科技有限公司刘涛提供的阿里云通知短信截图和服务器流量图

这两份电子数据均为复制件，如前所述，违反了电子数据的收集、提取程序，无法确定真实性，不得作为定案根据。即便属实，短信内容也无法印证 DDoS 攻击的时间，谁实施的攻击，服务器流量图也不能证明受到了 DDoS 攻击。

3、“www.aolingaokao.com”的管理公司武汉奥林文化发展有限公司法人陈庆安提供的“网站流量访问图”

该证据不仅是复印件，而且是武汉奥林文化发展有限公司自行制作、自己盖章的图表，图表内容没有任何来源，内容完全无法证实。即便是依据该图表，也仅仅能证明 2018 年 1 月，其公司网站已用流量为 1.96G，不能证明受到了 DDoS 攻击。该图表还显示其公司网站的流量标准值为 15G，因此 1.96G 的流量不可能导致其网站无法访问。而且陈庆安多次强调 1 月份是招生旺季，很多考生会点击其网站，既然如此，相比较 2018 年 2 月的流量 759.13M，1 月份 1.96G 的流量并不异常。因此，该图表无法印证该网站曾遭受过 DDoS 攻击。

（二）只有被害人陈述，不能证明网站受到了 DDoS 攻击且有影响

证明网站或服务器受到 DDoS 攻击影响，实际上只有被害人陈述这一孤证，孤证不能定案。

第一，严重利害关系。8 个被害人陈述证明相应网站遭到攻击且产生影响，但他们的公司与粤楚公司是竞争关系，与张某、与粤楚公司有严重利害关系，其陈述的真实性存疑。

第二，被害人自己都称不知道是否受到攻击，影响多大。例如：“www.027yk.com”的管理公司武汉邦德世纪信息科技咨询有限公司的员工杨杰陈述中明确提到“我也不确定这种异常的访问情况是否和大流量的 DDoS 攻击是否有关系”；“www.yb027.com”的管理公司武汉文英博艺教育咨询有限公司的张国令明确表示“具体详细情况，我自己也不太清楚”，且其没有提供公司营业执照，该被害人是否是公司员工，是否具备被害人资格存疑。

（三）1 个网站是否遭到攻击，根本没有任何证据，应当排除

公诉人在法庭辩论时说：“网络犯罪有其特殊性等，结合已收集的被害人陈述及其他相应的客观证据等证据，完全可以作出综合认定，不需要对被害人全部进行取证。”这一说法运用在本案中，完全违背证据裁判的原则。根据起诉书适用的《计算机解释》第 4 条第 1 款第 1 项，就粤楚公司涉及的所谓 11 台计算机，除了被害人陈述，还有什么证据证明攻击后果？法律法规是规定了可以根据电子数据、书证等证据综合认定，但仅有的 4 个电子数据，来源不明，真伪不知，取证严重违反电子数据取证规则。

“hb529.shop.liebiao.com”是否受到过 DDoS 攻击，甚至没有被害人陈述。没有任何证据证明这个网站受到了 DDoS 攻击。

（四）至少还有 3 个网站或 IP 根本不可能被 DDoS 攻击，应当排除

粤楚公司不可能攻击与其毫无竞争关系的两个位于北京的 IP 服务器。北京易维云数据科技有限公司负责人刘涛称，其公司 IP 为 139.129.230.210 和 118.190.40.71 的两个服务器 2018 年 1 月份曾遭到 DDoS 攻击。现有证据无法证明粤楚公司有何动机和理由攻击两个物理地址为北京的 IP 服务器。

唐小平和肖媛庭前及当庭供述均表明具有两个及以上的 IP 地址的网站，因无法确定攻击目标而不会发动攻击。张某与陈林的聊天记录表明攻击美国的服务器没有效果。而该公司李磊提到，网站放到了美国的服务器。辩护人通过网站“站长之家”PING 检测（http://ping.chinaz.com）后发现，www.kedayikao.com 响应 IP 的归属地都在美国，与李磊的陈述印证。

（五）即便确实受到影响，也不一定是唐小平 DDoS 攻击所致

网站服务质量降低的原因很多，DDoS 攻击只是一个原因，网站自身的容量，一段时间内访问人数的剧烈增加，甚至没交网费、断网、电脑故障、电脑设置错误、临时停电、民工挖断电缆、雷电袭击，都会导致网站无法访问。要证明被攻击的网站是因为被 DDoS 攻击而服务质量降低，必须排除其他所有可能导致网站服务质量降低的因素，得出唯一结论。显然，这是各被害人都无法确定的事实，起诉书是如何排除其他所有因素而确定是 DDoS 攻击所致，而且还是唐小平发动 DDoS 攻击所致？

公诉人说，“正因为张某查看攻击效果，且有效果的情况下才会多次长期提交任务，根据一般经验，只有花钱有效果才会乐于继续花钱，张某 2018 年 3 月又再次充值 200 元的事实进一步证明了攻击的效果。”这一论证逻辑完全错误。第一，李荣洋曾指责唐小平，DDoS 攻击没有效果。第二，花钱和效果完全是两回事。当庭打个比方，花钱请了律师就一定有效果吗？律师没有效果就不找律师吗？

综上，要证明 11 台计算机信息系统不能正常运行，必须要有客观证据，否则根本不能证明。但控方却没有一份有证明力的客观证据，有的甚至没有证据，有的则仅有被害人陈述这一孤证，根本不足以认定 11 台计算机信息系统遭受到了 DDoS 攻击影响。退一万步，即便有证据证明受到了 DDoS 攻击，也没有证据证明这些 DDoS 攻击是唐小平所致，被害人所称的 DDoS 攻击完全有可能是其他人实施的 DDoS 攻击。再退一万步，即便强行依据被害人陈述认定网站受到了 DDoS 攻击，至少 hb529.shop.liebiao.com、www.kedayikao.com（武汉世纪金科教育投资有限公司）、139.129.230.210、118.190.40.71（北京易维云数据科技有限公司）这 4 个网址和 IP 不应认定，受攻击的计算机信息系统数量不符合“十台以上”。

五、张某不是粤楚公司购买 DDoS 会员服务的直接责任人员

粤楚公司辩解，此事非公司行为，公司从未开会研究过，张某、陈林也未报销过相关费用。张某仅是粤楚公司的股东之一，公司业务由各股东分工合作，公司事务共同决定，张某不是粤楚公司主管或实际控制人，且张某在公司中没有任何职位。粤楚公司中只有陈林懂技术，技术方面的事务由陈林负责，粤楚公司诉讼代表人姜皓严以及张亚中、陈林的证言都证实了这一点，相反张某不懂技术，不可能负责网站排名优化，只可能是陈林负责。张某的辩解和陈林的第一次讯问笔录能够印证，张某不懂技术，是陈林提出的 DDoS 攻击，是陈林提出要买匿名黑卡。DDoS 攻击从提出设想到具体实施，完全由陈林负责，张某只是起到辅助的作用。综上，不应当将张某认定为对单位直接负责的主管人员和其他直接责任人员。

六、量刑辩护

退一万步，本案即便要强行认定犯罪，也应减轻处罚，适用免于刑事处罚，或情节轻微不认为是犯罪。

（一）张某不是主犯，应认定从犯

公诉人认为被告人唐小平、蔡季星、李荣洋、刘昌龙、张某在共同犯罪中起主要作用，是主犯，而王岩、肖媛在共同犯罪中起次要作用或者辅助作用，是从犯。这一意见明显不合理。

第一，前文已经指出，法无明文规定，购买者不应当认定为共同犯罪。

第二，退一万步而言，对破坏计算机信息系统罪所保护的法益的侵害程度方面，张某的作用远小于唐小平甚至王岩和肖媛。粤楚公司所购买的 DDoS 攻击，数量较之于唐小平实施的 DDoS 攻击而言数量极少，危害也较小，远不能跟唐小平、肖媛实施的 DDoS 所造成的危害相提并论。就王岩而言，王岩为唐小平提供技术支持，没有王岩的设计和日常维护，唐小平就不可能推出 DDoS 平台吸引客户购买服务；就肖媛而言，肖媛全程参与了唐小平的 DDoS 攻击，即便处于辅助地位，但较之张某，其所造成的社会危害程度显然更大，如果肖媛是从犯，张某更应认定属于从犯。

第三，唐小平凭借平台发挥着绝对的主导作用，粤楚公司则仅仅是购买服务，且是 2000

余名会员之一，如果认定粤楚公司的张某是主犯，理论上 2000 余名会员都有可能是主犯，这种结论显然会导致处罚失衡。

（二）犯罪情节轻微，主观恶性不大，且系初犯

1、没有违法所得，也没有证据证明谁有损失，损失多少

粤楚公司 DDoS 攻击的目的在于优化自己公司网站的排名，进而推广自己，但没有任何证据证明粤楚公司实现了这一目的，相反张某、陈林等人供述均称排名变化不明显。虽然几名所谓被害人称其公司因网站被 DDoS 攻击受到了影响，影响了招生等，但除其一方说法外，没有任何证据证明他们的招生情况有何变化，更没有证据证明这种变化是被告人的 DDoS 攻击造成。

2、即便按照起诉书指控，粤楚公司的行为也刚刚达到够罪标准，犯罪情节显著轻微

根据《计算机解释》的规定，造成十台以上计算机信息系统的主要软件或者硬件不能正常运行的，才属于后果严重，而公诉机关指控粤楚公司造成 11 台计算机系统不能正常运行，刚刚超过入罪标准 1 台，情节显著轻微。

3、被攻击的网站，流量较少，即便被攻击，也不会对其公司业务造成较大影响

例如，武汉前程世纪教育科技发展公司员工肖浩陈述，其公司网站 www.318edu.com，遭到 DDoS 攻击后无法打开，阿里云的客服建议花钱买高防护。但该公司的做法是“一直忍着他的攻击，一直持续到 1 月底，我们招生的黄金时段结束才停止 DDoS 我们的网站”。如果该公司网站真的如其所述对招生影响很大的话，特别是还处于所谓招生黄金时段，怎么可能不舍得花钱购买高防护？合理的解释是该网站对其公司宣传或招生的作用微乎其微。其他作证的被害单位绝大多数是类似情况。

4、部分被害单位存在过错，大量抄袭粤楚公司原创文章，恶意竞争在先

不完全统计，武汉邦德、武汉远博、武汉英博等公司的网站抄袭粤楚公司原创文章数量在 45 篇以上，而网站的原创文章数量直接影响到网站的排名，这才引发粤楚公司在被迫寻求网络优化的过程中犯错。粤楚公司并不是真的想害谁，进行 DDoS 攻击实际是其权益受到侵害后自力救济的一种被迫手段，其行为符合朴素的正义观念，定罪量刑时应当予以考虑。

5、张某等人响应国家号召，自主创业，误走弯路，系初犯，保证以后会吸取教训

张某上大学时勤工俭学从事家教工作，后跟陈林、张某中等创立粤楚公司，再后来又成立了武汉仟橙科技有限公司和武汉仟橙人力资源管理有限公司。他们的公司免费帮助了至少 2000 多名高考学生、大学生和找工作的毕业生。张某响应国家号召，自主创业，误走弯路，有一定的过错，但人非圣贤、孰能无过。恳请法院对于张某这样的创业青年，秉持宽严相济精神给予其最大的宽容和关怀，审慎对待本案定罪证据严重不足的问题，坚持证据裁判，即便要判决有罪，也希望免予刑事处罚，给予张某改过的机会。

6、张某认罪认罚

即使辩护人认为张某不构成犯罪，但张某仍然愿意认罪而想求得一个“好态度”。可是，张某的认罪不为法官和检察官接受，仍称他拒不认罪。关于认罪认罚，应当澄清如下理念：第一，认可基本事实，不等于认可全部指控事实，被告人仍然可以进行辩解，辩解并不等于不认罪。第二，认罪认罚是一种形式，没有必要强迫被告人展示内心，没有使法官、检察官达到内心确信被告人悔罪的必要。第三，审判长让被告人在认罪与支持辩护人无罪辩护之间作单项选择，如果不支持，就不考虑律师的观点，这是不对的。律师依据证据和法律独立进行辩护，无论被告人是否认罪，是否同意律师的观点，法院都应当依法考虑辩护人的观点，依法裁判。

在粤楚公司及张某案件中，侦查机关没有做到规范、全面取证，导致证据链断裂，定罪证据严重不足。对于被害单位的网站是否受到攻击，仅仅依赖唐小平的供述以及被害人的单方陈述，在完全有可能调取服务器中网站访问记录等进行印证的情况下，侦查机关“偷懒”

而没有调查取证。由于境外服务器无法取证以及网站设置的原因，无法查证唐小平是否将粤楚公司的攻击任务提交进行，也没有证据证明 str3ssed.me 网站实施了唐小平提交的任务，导致证据链断裂。而且，起诉书适用法律适用错误。恳请尊敬的审判长、人民陪审员坚持证据裁判，准确适用法律，依法宣告张某无罪

此致

海门市人民法院

张某的辩护人

徐昕

北京圣运律师事务所律师

根据 2019 年 1 月 10 日法庭辩论整理而成

（十二） “断卡”行动重点打击的“帮信罪”是个什么罪？

2020 年 10 月 10 日，国务院打击治理电信网络新型违法犯罪工作部际联席会议全国“断卡”行动部署会召开，这标志着打击、治理、惩戒开办贩卖电话卡、银行卡（简称“两卡”）专项行动的集结号正式吹响。

此次“断卡”行动中的“卡”是广义上的“卡”。

手机卡既包括我们平时所用的三大运营商的手机卡，也包括虚拟运营商的电话卡，同时还包括物联网卡。

银行卡包括个人银行卡，也包括对公账户及结算卡，同时还包括非银行支付机构账户，即我们平时所说的微信、支付宝等第三方支付。

当前电信网络诈骗持续高发的一大根源，是大量“实名不实人”的银行卡、电话卡被骗子购买后实施诈骗，给警方的追查和打击带来巨大困难。因此，斩断电话卡、银行卡的买卖链条，就等于给骗子“断奶”，对于压发电诈案件具有特别重大的意义。

自 2020 年 10 月 10 日开展“断卡”行动以来，泉州市安溪县人民检察院与安溪县公安局召开严打帮助信息网络犯罪活动罪（简称“帮信罪”）业务交流会，严厉打击“两卡”违法犯罪，并且取得积极战果。此前已对买卖、租借银行卡的 360 名违法犯罪嫌疑人进行了惩戒。

案 例

被告人王某自 2019 年 9 月至 2020 年 6 月间，明知他人实施信息网络犯罪活动，仍将本人户名的四张银行卡租借给他人，用于接收网络赌博等网络犯罪活动所得款项 8800 余万元。至被查获时，被告人王某共获利约 3500 元。其中，一名受害人刘某在赌博 APP 上共参赌 200 余万元，家庭因此陷入困境。而被告人王某因犯帮助网络信息犯罪活动罪被判处有期徒刑一年三个月，并处罚金人民币十一万元。

释 法

案例中的银行卡，属于“两卡”之一，犯罪嫌疑人在明知他人将用这些银行卡实施信息网络犯罪活动，仍然将卡租借给他人，这已经涉嫌帮助信息网络犯罪活动罪（简称“帮信罪”）。

那什么是“帮信罪”呢？

我们来看一下司法解释：

《刑法修正案（九）》所增设，作为《刑法》第 287 条之二的帮助信息网络犯罪活动罪规定：“明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，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。单位犯前款罪的，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。有前两款行为，同时构成其他

犯罪的，依照处罚较重的规定定罪处罚。2019 年 11 月 1 日起施行。

情节严重有以下七种：

（1）为三个以上对象提供帮助的；

（2）支付结算金额二十万元以上的；

（3）以投放广告等方式提供资金五万元以上的；

（4）违法所得一万元以上的；

（5）二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又帮助信息网络犯罪活动的；

（6）被帮助对象实施的犯罪造成严重后果的；

（7）其他情节严重的情形。

此外,《解释》规定，确因客观条件限制无法查证被帮助对象是否达到犯罪的程度，但相关数额总计达到前述标准五倍以上，或者造成特别严重后果的，应当以帮助信息网络犯罪活动罪追究行为人的刑事责任。

买卖、租借“两卡”均属于违法行为，切勿将自己办理的手机卡、个人银行卡、对公账户及结算卡、以及微信、支付宝等第三方支付平台账户买卖、租赁给犯罪分子，否则将面临信用惩戒、限制业务、严管账户、法律处分等四大惩戒。

自身“两卡”不应出售，

他人“两卡”更不应购买！

生财有道，

切勿以身试法！

四大惩戒措施：

1. 信用惩戒：人民银行将相关信息移送金融信用基础数据库，违法违规记录到个人征信报告，将在一定时间内影响相关人员的贷款和信用卡申请；

2. 限制业务：5 年内暂停相关单位和个人银行账户非柜面业务，支付账户所有业务。也就是说，相关单位和个人 5 年内不能使用银行卡在 ATM 机存取款、不能使用网银、手机银行转账，不能刷卡购物，不能通过购物网站快捷支付，不能注册支付宝账户、不能使用支付宝、微信收发红包、和扫码付款；

3. 严管账户：银行和支付机构 5 年内不得为相关单位和个人新开账户。惩戒期满申请开户的，银行和支付机构将加大审核力度；

4. 法律处分：非法买卖个人银行账户和企业对公账户，除受到上述惩戒外，还可能涉嫌《中华人民共和国刑法》规定的帮助信息网络犯罪活动罪、妨害信用卡管理罪、买卖国家机关证件罪和掩饰、隐瞒犯罪所得罪，甚至构成诈骗罪，可能给个人带来牢狱之灾。

（十三）网络赌博

1.网络赌博隐藏于直播平台涉案 118人赌资达 3.4 亿

2019 年 4月,公安部督办的“2· 23”开设赌场案尘埃落定。这起涉案人员来自21 个省份 118 人、 赌资达 3.4 亿元的利用网络直播平台组织赌博的新型案件,118 名被告人的判决已陆续生效。经江苏省张家港市检察院指控,张家港市法院以开设赌场罪对曾某等 118 名被告人判处有期徒刑五年零六个月至有期徒刑十一个月,缓刑一年零二个月,并处罚金100 万元至2.5 万元不等的刑事处罚。该案一审判决后,曾某等 5 名被告人不服一审判决,向苏州市中级法院提出上诉。2019 年 1月,苏州市中级法院对该案曾某等人裁定驳回上诉,维持原判。

网络赌博,隐藏于直播平台

2016 年 12月的一天,刘某晚上回到家,像往常一样打开电脑上网,他经一名网友的推荐进入到一个网络直播平台,女主播隔着屏幕与其互动后,刘某打赏了对方几个小礼物,女主播非常高兴,就和刘某热络起来。女 主播告诉刘某,直播平台除了主播表演外,还有一些有意思的小游戏,可以尝试一下。刘某听后,便按照女主播 的指示,进入到一款名为“猜车标”的游戏入口。问及如何进入游戏,女主播告诉他,可以通过给她刷“礼
物”的方式兑换游戏币,若账户有盈余的游戏币还能兑换成人民币。随后,刘某为主播刷了价值 500 元的“礼物”,刘某的游戏账户显示已经获得相应的游戏币。于是,他进入到“猜车标”游戏中,该游戏界面有八个格子,对应四种汽车车标,每种车标有大小之分,玩家用游戏币“竞猜”车标,不同的车标对应不同赔率,押 中车标就会赢得游戏币,没有押中就会输掉游戏币。

一开始,刘某抱着试试看的心态,投注了几次比较小赔率的车标,但他运气特别好,一连小胜了几把,游戏 币在屏幕中滚滚而来,女主播也为他叫好鼓劲,这让他有些忘乎所以,在之后的游戏中,他的底气越来越足,筹 码越押越大。

短短几个月时间,他在这个直播平台参与“猜车标”游戏,损失共计 5 万余元。2017 年 2月,刘某向张家 港市公安局报案。次日,公安机关对该线索立案侦查,赴上海、浙江等地将一个庞大的网络赌博组织中一系列的犯罪嫌疑人陆续抓捕归案。

经侦查,这个网络赌博组织分工明确、职责清晰,最上游为两家企业,即网络赌博程序及直播平台的开发 商和运营商。从网络赌博组织的最上端向下呈线性辐射状,运营商旗下有三家网络直播网站,网站中开设若干虚拟直播“房间”,每个“房间”又有代理和工作人员,负责“房间”内赌博组织和赌资流转。从上游的开发商、运营商到“房间”的代理以及其他工作人员,这个赌博组织的涉罪人员已达百余人。

提成诱惑,从赌客变帮凶

上海某网络科技有限公司正是这个“猜车标”游戏及所在直播平台的开发商。2017 年 3 月16日,侦查人员来到位于上海某高档写字楼,将该公司负责人曾某抓捕归案。

出生于上世纪 70 年代的曾某,研究生毕业后,赶上了“创业大潮”,创办了这家网络科技公司。公司主要经营内容就是网络技术研发,研发维护网络社区,包含其中的直播业务,同时还开发了一些网络游戏。这家公司创立5 年有余,在业界及网民群体中有一定知名度和影响力。曾某作为外地人通过自身的努力,凭借专业技术和经营头脑,在上海站稳了脚跟,并成为家乡人交口称赞的“精英人物”。而运营商负责人朱某则只有高中文化,但他很早就跻身于高精尖的网络信息技术产业。

会运营的朱某和懂技术的曾某在同一领域中产生了交集并擦出“火花”。他们优势互补、谋求合作,尝 试进行新的平台建设和技术开发,并形成相对默契的合作关系。在利益面前,他们逐渐迷失方向,试图违反法律规定寻找“捷径”并想方设法打“擦边球”。

作为这起网络赌博犯罪的“始作俑者”,面对司法机关的讯问,曾某、朱某对自己的犯罪行为矢口否认。他们将实际进行的开设网络赌场行为与普通的网络直播和网络游戏相混同,为

自己的行为寻找合法的说　　辞。同时,为了掩盖犯罪事实逃避法律追究,他们在游戏设计、赌资流转等方面做足了“功课”。赌博链接　　隐藏在正常的网络直播之中、赌资通过现实货币与虚拟游戏币在第三方支付平台、“房间”代理、直播主　　播等媒介之间多次转化,中断的赌资流转链条,模糊了赌资的本来面目。

他们公司积极进行直播平台推广,很多网民被直播表象所吸引,进而进入到直播“房间”中的赌博链接, 通过充值从“游客”变为“赌客”。同样家住张家港的陆某,和报案人刘某一样,进入直播平台,参与到“猜车标”游戏当中,接连押错“车标”,一夜之间,他就损失了 2 万余元。然而,他没有选择和刘某一样向公安机关报案。他了解到当直播平台“房间”代理可以拿到 15%的提成,觉得有利可图,便开了“房间”,招募主 播,引诱他人参与赌博。报案人刘某就是经主播引诱在陆某代理“房间”参与赌博的,而陆某也成为公安机　　关最早抓捕的犯罪嫌疑人,该案中像陆某一样的人还有很多。

该网络组织的绝大多数涉罪人员被网络直播、网络游戏的幌子吸引,成为赌客,后逐渐了解该网站赌博规则,为获取赌博活动中 15%的提成,他们选择成为开设网络赌场犯罪中的一分子。这些人大多沉迷于赌博, 是开设赌场犯罪的被害人,但随后又成了网络赌博组织的帮凶,整个网络赌博组织通过这样“发展下线”的方式,呈现出一种蔓延状态,短短 1 年间,涉案人员涉及来自21 个省份的 118人、赌资达 3.4 亿元。

开庭审理,众被告人各得其罚

在公安机关侦查该案之初,苏州以及张家港两级检察院多次派出经验丰富的检察官通过现场阅卷、与公安民警探讨等方式,针对犯罪嫌疑人讯问、电脑资料等证据补充侦查方向提出了建议,明确将证明赌资流转以及上下游之间的抽头渔利关系作为侦查的关键。通过公安机关大量工作,在该网络赌博运营商财务负责人处查获的与各“房间”代理之间抽成的电子账目明细成了最终的定案关键证据。

2017 年 4月,经公安机关提请批捕,张家港市检察院对这起新型网络赌博案件中起组织领导作用的曾 某、朱某等 6 名犯罪嫌疑人以开设赌场罪依法作出批准逮捕决定,对其余 100 余名犯罪嫌疑人作出取保候审决定。

案件进入审查起诉阶段,张家港市检察院调派 4 名员额检察官成立办案组,负责案件的审查起诉工作。两名检察官针对上游的开发商和运营商、网络直播平台负责人进行审查,另两名检察官则针对下游 100 多名“房间”代理进行审查。

如何对赌博组织中的人员进行犯罪认定?除了开发商、运营商、直播平台的相关人员之外,更多的是网络直播平台的“房间”代理。他们从事了犯罪的行为,但无论在主观恶性上还是社会危害性上还是不能与“上游”人员即网络赌场的开发者和运营者相提并论。办案检察官们对相关法律进行了认真研究后认为,对　　于下级代理而言,其主观目的是为了获得赌博网站的利润分成,而且这些代理除吸引赌客赌博外也存在获得赌博网站的利润自行充值的情况,因此从主客观相统一、量刑均衡原则出发,以参与赌博利润分成认定其数额较为合理。对于上级管理层来说,其经营的平台存在赌博行为,以总共的赌资数额更能准确认定其开设赌场的数额。

2017 年 6月26日,除了被关押的曾某等 6人外,来自全国各地的 112 名犯罪嫌疑人陆续来到张家港接受权利与义务告知。按照事先的协调、统筹,他们被分别通知至张家港市 10 个辖区的派出所接待大厅接受权　　利义务告知工作,每个驻点都有检察人员负责接待。当天,每个告知点上,犯罪嫌疑人依次排队、接受告知、 进行签名画押,既无拖延,也无拥挤。

经过了百余天,张家港市检察院审查起诉工作如期完成,并向法院提起公诉。2018 年 4月24日,该案在张家港市法院开庭。整个案件开庭持续 4 天,被告人委托辩护律师达 20人。在讯问阶段,部分被告人当庭翻供,2 名律师做无罪辩护,控辩双方围绕网站是否属于赌博网站、网站赌资数额如何计算等问题展开激烈辩论。张家港市检察院出庭支持公诉的检察官们针对庭审情况,及时调整讯问策略,结合事实和证据,围绕开设　赌场罪的构成要件充分阐述和答辩,对辩护人提及的网站定性、数额计算等理由有力有据地予以辩驳。其时,被告人近亲属、人大代表、政协委员、新闻记者及各界群众 200 余人旁听了庭审。

在开庭审理过程中,一名被告人正值怀孕待产且腿部骨折,无法至张家港市法院开庭。考虑到其实际情况,张家港市检察院与法院派出检察官、法官赴被告人所在的贵州省纳雍县开庭审理,该被告人认罪服法,并　　对办案人员体量困难、异地办案表示感谢。2018 年 6月28日,张家港市法院对 118 名被告人以开设赌场罪分别判处相应的刑事处罚。

案后说法

近年来,随着互联网高速发展,传统的线下赌博大有迁移到线上的趋势。一些网络科技公司精心策划,将一些赌博游戏经“包装”和“掩饰”,诱人参与,让很多不明真相的网民深受其害。可以说,搭上互联网便车的赌博模式,其危害性和隐蔽性比起传统赌博模式有过之而无不及,迷惑性更大,传播范围更广。因此,从根源　上铲除这一网络毒瘤,已势在必行。

根据相关司法解释,以营利为目的,在网络上建立赌博网站,或者在赌博网站担任代理,接受投注的,将构　　成开设赌场罪;网络平台提供者,明知他人利用该网站从事违法活动而不及时制止、报告的,也将承担相应法　　律责任;明知他人实施赌博犯罪活动,而为其提供资金、计算机网络、通讯、费用结算等直接帮助的,则将以赌博罪的共犯论处。由此可以证明,类似于“猜车标”的网络赌博游戏,其组织者、经营者、提供网站者、 担任代理者已经触犯了法律,将承担法律责任。

网络赌博不需要持有大量现金,加上网络传播的广泛性,参与者的不特定性等特点,在证据固定方面、人员调查方面存在很大难度。甚至,在高额利益之下,一些网络赌博网站被处罚后可能依然会改头换面,重新出现。要想有效遏制网络赌博这一社会公害,需多措并举。一方面要加大对网络赌博犯罪的打击力度。对网络　　赌博犯罪加大刑法惩治力度,提高犯罪分子的犯罪成本,打消他们的侥幸心理。另一方面要加强网络平台监管和排查力度。不断提高技术手段、拓展监管渠道,注重对网络赌博相关精细检索,从中发现网络赌博犯罪的苗头隐患。同时,要加强法治宣传力度。通过网络、电视、报纸、微博、微信等媒体,结合案例,多渠道、多形式开展宣传,引导广大群众提高防范意识,及时发现和举报违法犯罪线索。只有多方重视,营造良好的网络秩序,才能让网络赌博这一社会公害无处藏身。

(江苏省张家港市检察院检委会专职委员　马建新)

2.探案：以直播平台作掩护 干网络赌博勾当

热闹非凡的直播间，盛情洋溢的主播，频繁融洽的互动，看起来似乎就是一场普普通通的网络直播。然而，光鲜亮丽的直播背后却隐藏着一个在互联网上开设赌场的违法 犯罪团伙。近日，浙江省瑞安市公安局在省公安厅治安总队指导下，经过缜密侦查和 深入分析研判，成功破获一起利用直播平台抽头、结算赌资的互联网开设赌场案件， 抓获犯罪嫌疑人180 余名，涉案赌资达 13 亿元以上。

去年上半年起，浙江公安陆续接到线索，称某视频聊天平台可能涉嫌赌博。通常的网络赌博案件中，赌博平台显而易见，赌博架构一目了然。但该赌博团伙却作案手段隐 蔽，且涉及全国多个地市，没有过往成功侦办的案例可资借鉴，民警一经手就发现困难重重涉案视频聊天平台表面为普通多人视频直播网站，网站内设多个直播间，主播和观众频繁互动，没有任何网络赌博迹象。民警同时发现，该直播平台经营有一款名为“车行争霸”的游戏，游戏界面却明确地注明网站不以任何形式回收金币。玩家赢得的金币只能用于在直播间给主播送礼物，并无直接兑现渠道。

前期调查遇到瓶颈，办案民警决定注册成为网站的高级会员，假扮成游戏玩家，试玩平台内的休闲娱乐游戏。随着民警玩游戏次数的增多，平台管理的结构、层级，工作人员的分工以及平台组织赌博、抽头、套现的整个流程也逐渐被摸清。民警侦查发现，该网站以直播平台为外衣，招募客服、代理、财务等工作人员运营“车行争霸”游戏开设赌场。参与者通过支付宝、微信、网上银行等渠道购买金币并参与“车行争霸” 游戏，在游戏过程中赢得金币后，需向平台指定的主播房间赠送礼物，平台会根据参与者赠送礼物的价值将等价的人民币转账给玩家，站点公司在赌博时抽取 2%左右的头薪，在兑现时抽取最低 20%比例的头薪。该赌博站点由玩家轮流申请坐庄，其他玩家利用游戏币押注，35 秒一轮，一天就能进行2400 多局。在前期侦查基础上，民警对网站经营地点所在的公司进行收网抓捕，成功抓获 10 名犯罪嫌疑人。

查明了赌博网站假借“直播平台”的幌子开设赌场的流程后，又一个巨大的问题浮现出来。民警注意到，该平台并没有自主研发赌博软件和维护服务器的能力，难道在该平 台背后藏有更大的涉赌犯罪链条？

经办案民警进一步审讯，犯罪嫌疑人终于交代，该公司经营网站所需的服务器均租自杭州某公司，并购买同一公司的技术维护支持、资金结算等服务，“车行争霸”游戏的 赌博数据均存储在该公司提供的服务器上。侦查人员通过大数据分析排查等手段，很 快锁定了该公司的服务器。同时，侦查人员发现，该公司还同时向多家网络公司出售 20 多个赌博平台，各赌博平台分散全国各地，各站点的涉案人员总计达百余人。侦查人员兵分五路，对其公司总部、技术维护公司、服务器所在地等进行跨区域集中抓捕，抓获涉案人员 20 余名，将赌博团伙老窝彻底端掉。（中国警察网记者 谢佳 通讯员 韩深明）

3.斗鱼直播间借网络游戏“开赌场”

记者暗访发现，存在主播坐庄或组局抽佣等赌博形式，每个涉赌直播间每小时“赌资”近万元

“斗鱼上有游戏直播间在搞赌博”，有网友 7 月 5 日向南都记者爆料称，斗鱼 TV (以下

简称：斗鱼)上有主播借助网络游戏中“开宝箱环节”来设置赌局。南都记者调查发现，在斗鱼的《梦幻西游》板块中，的确有主播通过开设所谓的“宝图吃鸡局”、“小宝图”等，在直播平台利用游戏作为开奖工具、以微信或支付宝作为交易渠道，来绕开监管进行赌博。

A

直播平台成“赌外围”媒介

7 月 8 日晚，斗鱼 TV。“现在 10 号位还空着，哪个老板补上，满人就开车了”，在《梦幻西游》板块里热度排名靠前的某直播间，南都记者看到主播卖力地叫喊着，并表示新来的观众可以添加直播界面右上角的微信，主播会发送“游戏玩法”给用户。

南都记者以玩家的身份添加上述微信，在通过微信好友验证后，该主播立即给南都记者发了一张图片。图片上写着“288 上车，加支付宝 X X X 买票，挖出(挖宝)最高价值为‘吃鸡者’”的红色加粗字样，其余内容则标记有各类物品的回收价格。据了解，该回收价格用于衡量产出物品的价值，并决定最终输赢。其中，“吃鸡者”根据参与人数获得相对应奖励，人数越多积分越高，7 人获得 1488 积分，8 人 1688 积分，9 人获得 1888 积分，10 人获得 2188 积分。此外，“吃鸡者”还将获得本轮开出的所有物品。

“许多主播会以‘宝图吃鸡’的噱头来开设赌局，使用《梦幻西游》游戏中的藏宝图的随机概率做文章。以其中物品产出的价值大小为输赢依据，主播则在其中抽成”，曾参上述赌局的爆料人张超(化名)向记者表示，主播在直播时为了规避平台的监控，在拉客与结算的时候会以积分或者“鱼翅”等虚拟道具为单位，“其实就是实打实的钱”。

据了解，早在 2007 年，公安部等四部委就联合发出了《关于规范网络游戏经营秩序查禁利用网络游戏赌博的通知》，其中明确规定不得提供将游戏虚拟货币兑换成法定货币的服务。因此，“双向兑换”被视为判定网络游戏是否涉赌的红线之一。

张超在爆料时向南都记者表示，涉赌现象就一直存在，只是玩法不断发生变化，“以前有种玩法叫‘砍尾数’，但是这个是官方认定的赌博行为，很少有这么明目张胆的了。”

B

主播每小时抽成可观

南都记者以玩家身份进入了一间“X X X 吃鸡”的直播间。据了解，在 5 人份的“高级宝图吃鸡局”，每个参与者(“老板”)需缴纳 288 元的“车票”费用，随后获得 35 元等值的“高级藏宝图”。最后，谁的“高级藏宝图”产出的物品最有价值，谁便是“吃鸡者”，独享该局所有产出物品和保底现金奖励。

主播在整个过程中扮演的是组局者的角色，提成是其最直接的收入方式。以 5 人局为例，5 人的“车票”费用共为 1440 元，而某主播出示的图片中，5 人局的保底为 1050 元，而每张高级藏宝图的费用约为 35 元，综合计算下来，主播可以 5 人局中抽取 215 元的佣金。

南都记者发现，如果赌局参与人数越多，主播的佣金收入也就越高。

“在结算时，虽说出了价值高的物品，‘吃鸡者’的奖励也相对应提高，但主播也没吃亏，因为上述物品在游戏中出售，也能通过某些渠道兑换成等值现金”，张超向南都记者表示，主播开这个基本稳赚不亏。

经南都记者观察，该主播一局会耗费 5 分钟在寻找“老板”补位上，另外 10 分钟则会耗费在“老板选位置”以及挖宝图的过程中。按照每小时 4 局“4 人车”来算，一小时“抽佣”收入至少近 800 元，开播六小时的收入提成约为四五千元。

而在一间名为“晚上 X X X X”红包的直播间中，主播几乎每 5 分钟的时间便组建一局 10 人的“高级宝图局”，随后在 10 分钟内挖完所有宝图并进行结果结算。按照一个小时能够开 4 局 10 人的“高级宝图局”来算，该直播间主播每小时现金流水近万元，而综合其出示的“10 人保底 2188”奖励为标准，该主播一个小时的收入提成便达超过 1200 元。

“主播通过‘抽水’，一天开 30 轮左右，就能拿到 7000 多元的盈利”，张超表示这个金额

一般主播都能达到，“有些热门主播，盈利多的每天三四万”。

C

除了抽佣，还有主播坐庄模式

另一种则是‘小宝图’玩法。就是由主播坐庄，对产出物品设置回收价格，自负盈亏”，张超向南都记者透露。7 月 9 日，南都记者继续对斗鱼进行调查时发现，仍有一些以“挖宝”、“宝图吃鸡”、“包车”等命名的直播间。南都记者还见到了张超提到“小宝图”玩法。

“咱们车上已经有六个人了，还有没有人要上车？”斗鱼《梦幻西游》板块的某直播间中，一主播卖力地喊道。在直播页面中，该主播将其游戏界面中的物品栏展示给观众查看，其中物品栏已被 20 张“藏宝图”完全填满，“想了解玩法的，可以加右上角的微信”，主播还时不时说道。

南都记者以玩家身份通过微信验证后，便立即收到主播发送的名为“小宝图玩法”的图片说明。据介绍，该直播间每张宝图的价格从 2 元到 20 元不等，20 张宝卡的投注总金额可从 40 元到 400 元。

据了解，玩家需要先支付 20 张宝图的钱给主播，再由主播将 20 张宝图陆续使用，随机获得宝物，然后比对“玩法”中规定的分值，折算成钱返还给玩家。宝物对应的总分低，返还玩家的钱就少；反之，宝物对应总分值高，玩家得到返款就多。此外，玩家投注金额越高，分值对应的金额也就越高。

在南都记者微信支付了 40 元(每张宝图 2 元)后，主播便开始用宝图进行“挖宝”。20 张宝图用完以后，所获物品总分值为 160 分。之后，主播通过微信将 16 元转回。这一局共耗时 18 分钟，南都记者输了 24 元。

爆料人张超向南都记者透露，主播搞“高级宝图吃鸡局”中的抽佣，收入最为稳定，而用“小宝图玩法”搞坐庄，主播会赚的更多，“毕竟小宝图出好东西概率很低”。

D

斗鱼平台游戏赌局屡禁不止

值得一提的是，南都记者曾于今年 6 月报道过一起斗鱼主播涉赌案例。在一款名为《问道》游戏中，有一个“五行竞猜”小游戏，玩家可以通过游戏币参与赌博竞猜。当时的爆料人告诉南都记者，他在斗鱼这类主播的直播间里输了几万元。(详见南都 6 月 25 日 A 20 版《微信投注网游开奖斗鱼直播间成赌场》报道)

斗鱼方面当时回应称，涉事主播涉嫌违规，已被永久封禁，并表示平台一旦发现主播存在违规行为，将第一时间采取关闭直播间、封禁账号等措施，绝不姑息。

此外，今年 5 月份以来，有多家媒体曝光称，斗鱼的粉丝福利社、幸运宝藏等抽奖活动涉嫌赌博。

E

主播闻风　暂避风头

“这两天不‘吃鸡’了”，在斗鱼《梦幻西游》板块某主播于 7 月 10 日在“吃鸡群”中表示。另一名曾开设“高宝图吃鸡局”的斗鱼主播在微信朋友圈留言道：“最近高宝图严打，可能这几天不会直播，谢谢”。

当晚，南都记者在斗鱼中发现，以往带有“宝图吃鸡”、“大乱斗”字样的直播间已经消失，取而代之更多是，以“鉴定”、“估价”为主的游戏直播间。

7 月 11 日，南都记者就直播间涉赌之事联系斗鱼，但至截稿时为止未获回应。

采写：南都记者　张志霖

律师说法

开设赌场罪已不仅限于实体场所，虚拟空间也包括

广东合邦律师事务所肖锦阳律师表示，赌博违法犯罪活动与正常娱乐活动的界限为是否

以营利为目的，个人参赌超过 5000 元属于赌博犯罪。直播游戏中的赌注数额高于正常的娱乐活动数额，涉嫌赌博违法犯罪活动。

两高司法解释明确规定，开设赌场罪的范围已经不仅限于实体场所，虚拟空间包括在内。同样，《刑法》对赌博罪也有相关规定，以营利为目的，聚众赌博或者以赌博为业的，处三年以下有期徒刑、拘役或者管制，并处罚金。开设赌场的，处三年以下有期徒刑、拘役或者管制，并处罚金;情节严重的，处三年以上十年以下有期徒刑，并处罚金。

而对于直播平台应承担何种责任，肖锦阳律师认为，直播平台的内容应当符合社会主义价值观，具有正面导向，而直播平台在其中需要承担审核和管理的义务。根据《互联网直播服务管理规定》要求，互联网直播服务提供者应积极落实企业主体责任，建立健全各项管理制度，配备与服务规模相适应的专业人员，具备即时阻断互联网直播的技术能力。

（十四）侵犯网络著作权

1.新型利用网络侵犯著作权罪中的问题

(1)关于侵犯著作权人作品电子版权认定问题

侵犯图书著作权已经不仅仅是采取传统盗印纸质图书的方式，而是转向了电子化的侵权行为。最高人民法院《关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》明确规定受著作权法保护的作品，包括《著作权法》第 3 条规定的各类作品的数字化形式。以海淀区检察院办理的花某某侵犯著作权案件为例。花某在经营某电子商务咨询有限公司期间，开发出标准自动更新管理软件进行销售，并对该软件进行了计算机软件著作权登记。该软件具有对建筑类等标准的管理和检索功能，但软件中没有标准、建筑图集等具体内容，软件里的具体内容会根据客户的个性化需求进行采集录入。花某自行或者安排员工，通过购买建筑行业出版社出版的标准纸质图书，通过扫描等方式形成电子数据，由技术人员将电子数据加入软件数据库，再通过软件实现服务器数据和标准自动更新管理软件客户端的数据同步。虽然软件开发商对其开发的软件本身享有著作权，但其未获得出版社授权和许可，以软件为载体将他人享有著作权的图书内容扫描成电子版而后销售，属于未经著作权人许可，侵犯了著作权人的复制、发行权的行为。

(2)提供搜索引擎服务行为的定性

在知识产权民事理论中，提供搜索引擎服务仅可能构成帮助侵权(或间接侵权)，间接侵权行为能否被认定为刑事法律中的“通过信息网络传播他人作品的行为”争议较大。根据 2011 年最高人民法院、最高人民检察院和公安部出台的《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》第 15 条的规定，明知他人实施侵犯知识产权犯罪，而为其提供互联网接入、网络存储空间等服务的，应以侵犯知识产权犯罪的共犯论处的规定。首先，判断行为人是否系明知，应结合在案的同案犯供述、证人证言、电子数据，以及行为人的从业经历等综合判断。其次，看行为人具体实施的侵权行为，如提供互联网接入，网络存储空间服务等行为。如行为人建立搜索引擎网站，依靠收取广告费营利，该搜索引擎网站表面上提供搜索引擎服务，对网络文学小说网站进行搜集和排名整合，实际上行为人在明知被链接网站是盗版网站的情况下仍为对方提供租赁服务器及链接服务，聚合了盗版资源，网络用户登录到该搜索引擎网站后，在搜索栏输入关键词，即可以根据需要进入相应的网站阅读网络小说，因此，可以认定行为人具有侵权的主观明知。

(3)将作品制作成“种子”文件发布在互联网上的行为是否属于通过信息网络传播他人作品的行为

“种子”是互联网用户利用 P2P 技术下载的必备文件，也是被下载文件的真正来源。如果

用户未经权利人许可，在某个平台上发布受到著作权法保护的作品的“种子”文件，使不特定的公众能够通过网络获得该作品，根据相关法律规定构成对权利人信息网络传播权的侵犯。“种子”发布者可能会承担民事责任、行政责任，甚至触犯刑法。在中国数字高清第一门户网站“思路网”侵权案件中，行为人实施的具体行为有两种：一种是直接将作品制成“种子”文件上传至 HDstar 论坛，这种行为是他人在利用 P2P 技术下载时，技术上第一指向的定是被告人的服务器，被告人的服务器收到下载要求后，会复制侵权作品的数码资料，再传递到他人的电脑上。该行为在民事上属于直接侵权行为，刑事上符合“通过信息网络传播他人作品”特征。另一种是鼓励注册会员在其 HDstar 论坛上传侵权作品“种子”的行为。这种行为是指行为人专设“保种组”，确保“种子”文件处于有效状态，以使下载者得到完整的涉案作品。其主观上对他人上传的是侵权作品“种子”明知，客观上鼓励、纵容他人上传，并提供上传空间，聚合了侵权“种子”的数量，使侵权达到更为严重的程度。该行为同样具有严重的社会危害性，在民事上属于间接侵权行为，在刑事上仍符合“通过信息网络传播他人作品”。

(4)民刑交织案件的区分

新型民刑交织案件也给时间紧迫的审查逮捕工作带来了很大挑战。对于一些理论界和实务中存在较大争议的案件，检察机关一般会按照法律、司法解释规定进行严格把握。如侵犯著作权类案件中，由于作品类型不同、侵权手段不同，经常会出现新类型案件，在无成型案件参考、存在民刑交织问题的情况下，检察机关在短短的 7 日内仍要严格证据标准谨慎处理。如东某侵犯著作权案中，东某设立百度云论坛，使得网友拥有一个可以分享百度云链接的空间，论坛用户注册后可在其论坛上发帖上传相关百度云资源链接（网友个人注册的百度云），其他论坛用户可通过回帖等形式查看相关链接后，前往百度云进行播放、保存、下载。东某在论坛内开设《资源周刊》系列主题，将每周论坛各版块中最热门资源集中推荐给用户。公安机关以侵犯著作权罪对其提捕，海淀区检察院审查后认为，本案与传统侵犯著作权罪中所表现出的“以营利为目的，复制、发行他人作品”的客观行为不同；涉案论坛上的大部分链接资源均系论坛注册用户所发，且系大量分散的论坛用户基于娱乐等非营利目的上传少量他人作品，犯罪嫌疑人的行为主要是为上述用户提供了一个网络存储空间，并筛选、整理、推荐热门资源帖。对于该案，在取证上侦查思路、方向均不甚明确，亦无成型案件参考;在案件定性上，对于筛选、整理、推荐热门资源帖，是否可以被评价为侵犯著作权罪的实行行为也存在争议。因此，检察院认为，基于罪刑法定原则，并兼顾罪责刑相适应的标准，决定不批捕该犯罪嫌疑人。

2.侵犯网络著作权犯罪的认定及辩护要点

侵犯著作权犯罪纷纷“触网”，是近年来侵犯知识产权犯罪的一大特点。几乎所有的作品都可以转换为数字形式在网络上传播，尤其是网络技术的快速发展，使作品的创作、传播和保护方式都发生了深刻变化，原有的著作权制度受到冲击和挑战，著作权的刑法保护制度也同样接受着新的考验与检视。无论是理论研究，还是司法实践，网络著作权领域都有不少争议性的问题和认定上的难点，有大量模糊地带需要填补和完善，这也为律师在侵犯网络著作权案件上的成功辩护提供了适度的可能和空间。

一、网络著作权的概念和特征

“网络著作权”，有的称为“网络环境下的著作权”，它其实不是一个法律术语，也不是一个法律概念，只是学者和法律实务工作者对网络环境下著作权的一种习惯称谓而已。网络著作权的本质是著作权在网络空间的延伸，著作权从现实空间移植到网络空间，分为两种情形：一是传统作品数字化后受到著作权的保护；二是在网络空间直接产生的作品受著作权的保

护。简言之，网络著作权就是著作权人对网络作品享有的著作权。与传统的作品相比，网络作品具有高科技性、交互性、难以类型化、与载体的联系淡化、作者判定更加复杂等特点，它主要包括多媒体、数据库、博客等类型的作品。

二、网络著作权保护的刑事法律依据

关于网络著作权保护的刑事法律依据，首先最基础的是《刑法》和《著作权法》。1997年《刑法》第二百一十七条奠定了刑法保护著作权的基础。《刑法》第二百一十七条规定“以营利为目的，有下列侵犯著作权情形之一，违法所得数额较大或者有其他严重情节的，处三年以下有期徒刑或者拘役，并处或者单处罚金；违法所得数额巨大或者有其他特别严重情节的，处三年以上七年以下有期徒刑，并处罚金：（一）未经著作权人许可，复制发行其文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品的；（二）出版他人享有专有出版权的图书的；（三）未经录音录像制作者许可，复制发行其制作的录音录像的；（四）制作、出售假冒他人署名的美术作品的。”2001年修订的《著作权法》开启了网络著作权刑法保护之先河，《著作权法》第四十七条第1、3、4等项明确规定了涉及侵犯网络著作权的刑事责任。第四十七条规定“有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任;同时损害公共利益的，可以由著作权行政管理部门责令停止侵权行为，没收违法所得，没收、销毁侵权复制品，并可处以罚款;情节严重的，著作权行政管理部门还可以没收主要用于制作侵权复制品的材料、工具、设备等;构成犯罪的，依法追究刑事责任:(一)未经著作权人许可，复制、发行、表演、放映、广播、汇编、通过信息网络向公众传播其作品的，本法另有规定的除外;…(三)未经表演者许可，复制、发行录有其表演的录音录像制品，或者通过信息网络向公众传播其表演的，本法另有规定的除外;(四)未经录音录像制作者许可，复制、发行、通过信息网络向公众传播其制作的录音录像制品的，本法另有规定的除外”，从而首次在立法上确认了网络著作权。2001年《著作权法》与1997年《刑法》从法律层面为网络著作权的刑法保护提供了依据，使得侵犯信息网络传播权的行为可通过侵犯著作权罪来追究刑事责任。

其次，2006年的《信息网络传播权保护条例》在行政法层面细化了刑法对网络著作权的保护。《信息网络传播权保护条例》第十八条规定“违反本条例规定，有下列侵权行为之一的，根据情况承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任；同时损害公共利益的，可以由著作权行政管理部门责令停止侵权行为，没收违法所得，并可处以10万元以下的罚款；情节严重的，著作权行政管理部门可以没收主要用于提供网络服务的计算机等设备；构成犯罪的，依法追究刑事责任：（一）通过信息网络擅自向公众提供他人的作品、表演、录音录像制品的；（二）故意避开或者破坏技术措施的；（三）故意删除或者改变通过信息网络向公众提供的作品、表演、录音录像制品的权利管理电子信息，或者通过信息网络向公众提供明知或者应知未经权利人许可而被删除或者改变权利管理电子信息的作品、表演、录音录像制品的；（四）为扶助贫困通过信息网络向农村地区提供作品、表演、录音录像制品超过规定范围，或者未按照公告的标准支付报酬，或者在权利人不同意提供其作品、表演、录音录像制品后未立即删除的；（五）通过信息网络提供他人的作品、表演、录音录像制品，未指明作品、表演、录音录像制品的名称或者作者、表演者、录音录像制作者的姓名（名称），或者未支付报酬，或者未依照本条例规定采取技术措施防止服务对象以外的其他人获得他人的作品、表演、录音录像制品，或者未防止服务对象的复制行为对权利人利益造成实质性损害的。”该条例在“上传问题”、“技术措施”、“扶助贫困”等方面明确细化了侵犯网络著作权、可追究刑事责任的行为类型。

第三，2004年、2005年、2007年司法解释进一步将网络著作权的刑法保护落到实处。2004年《关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》有四个重要规定：

一是将“信息网络传播”解释为“复制发行”。该解释第十一条第三款规定：通过信息网络向公众传播他人文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品的行为，应当视为刑法第二百一十七条规定的“复制发行”。该规定使得《著作权法》第四十七条第一项与《刑法》第二百一十七条第一项相对应，从而使刑法对信息网络传播权的保护落到实处；二是对“以营利为目的”作了扩大解释。第十一条第一款规定：以刊登收费广告等方式直接或者间接收取费用的情形，属于刑法第二百一十七条规定的“以营利为目的”；三是规定了入罪的“数额”和“情节”。第五条规定了“违法所得数额较大”的最低入罪数额为 3 万元，“有其他严重情节”的非法经营数额标准为 5 万元、复制品最低数量标准为 1000 件（份）；四是规定了“数罪并罚”、“共犯”、“缓刑”等内容。2005 年《关于办理侵犯著作权刑事案件中涉及录音录像制品有关问题的批复》、2007 年《关于办理知识产权刑事案件具体应用法律若干问题的解释（二）》则进一步发展、重申了 2004 年司法解释的相关内容。

2011 年 1 月 10 日，两高与公安部联合发布《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》。该意见虽然不是司法解释，但具有司法解释的性质，其进一步扩张了“以营利为目的”的理解，将“捆绑第三方作品”、“获取广告服务费”、“收取会员注册费”等行为列入“以营利为目的”的范围。该文件还对网络著作权犯罪的“严重情节”、“特别严重情节”重新做了规定：（第十三条）以营利为目的，未经著作权人许可，通过信息网络向公众传播他人文字作品、音乐、电影、电视、美术、摄影、录像作品、录音录像制品、计算机软件及其他作品，具有下列情形之一的，属于刑法第二百一十七条规定的“其他严重情节”：（一）非法经营数额在五万元以上的；（二）传播他人作品的数量合计在五百件（部）以上的；（三）传播他人作品的实际被点击数达到五万次以上的；（四）以会员制方式传播他人作品，注册会员达到一千人以上的；（五）数额或者数量虽未达到第（一）项至第（四）项规定标准，但分别达到其中两项以上标准一半以上的；（六）其他严重情节的情形。实施前款规定的行为，数额或者数量达到前款第（一）项至第（五）项规定标准五倍以上的，属于刑法第二百一十七条规定的“其他特别严重情节”。该文件规定的入罪数额虽然在形式上表现为恒定，起刑标准也更加详细明确，但实质上入罪标准在降低，这也表明高层司法机关对侵犯网络著作权的行为加大打击力度的态度。

三、侵犯网络著作权犯罪的辩护要点

侵犯网络著作权犯罪具有隐蔽性、跨地域性等特征，犯罪行为不易被发现、犯罪嫌疑人的真实身份也不易被确认，而且侵权技术手段更新快，侵权内容容易被删改，原始证据容易灭失，证据材料收集、认定困难，也带来一系列法律适用的疑难。针对这类案件的特点，辩护律师可以着重从以下几个方面来进行辩护。

（一）实体之辩：

1、行为主体之辩

在整个侵犯网络著作权的犯罪过程中，有三类人参与其中：一是网络信息内容的上传者；二是为信息传播提供服务的网络服务者；三是接收并最终使用信息的终端使用者。网络信息内容的上传者可以成为该罪的主体，后两类则未必。

首先，接收并最终使用信息的终端使用者一般情况下是不太可能成为侵犯网络著作权的责任主体。在境外，有网络最终用户因为侵犯著作权被定罪判刑的案件，例如美国的帕尔文·哈利瓦案，哈利瓦从网上非法下载音乐被判有罪，又如日本的“Winny”案，“winny”软件的使用者未经授权使用而被判有罪，只是目前在我国网络最终用户通常不能成为侵犯著作权犯罪的责任主体。当然，随着国家对知识产权保护越来越严，也不排除成为犯罪主体的可能性。对此，可以着重从三个方面进行辩护：一是没有擅自复制，没有再次向第三人、社会公众提供该软件；二是个人合理使用。《计算机软件保护条例》规定了软件的合理使用，使用目的

是学习或者研究的目的，使用的方式只是对该侵权软件的安装、显示、传输或者存储。三是非商业用途的使用，也即不是“以营利为目的”。对于非商业性使用盗版软件，其社会危害性不足以通过刑法来进行评价，至多是承担侵权的民事责任。

其次，网络服务提供者，包括网络内容服务提供者（ISP）和网络技术服务提供者（ICP）。第一，由于确保网络信息内容来源真实合法是网络内容服务提供者的义务，违反这个义务是网络内容服务提供者（ICP）承担责任的前提。对此，着重从审查义务上进行辩护：在网络作品上传到网络平台向公众传播之前，网络内容服务提供者（ICP）审查了该网络作品是否合法有效，至少在形式上审查了是否有不发布侵权违法网络作品的承认和声明；在作品已经上传到网络平台向公众传播之后，则要遵循“通知---删除”规则和“红旗”规则，发现侵权违法的网络作品，及时停止该网络作品的在该信息网络传播平台的继续传播，那么网络内容服务提供者（ICP）就尽到了审查义务，不承担刑事责任；第二是从“实行犯不成立犯罪，导致共犯不成立”的角度进行辩护。帮助犯与实行犯一起构成共犯，而实行犯的成立是帮助犯成立的前提。只要实施侵犯网络著作权的人不构成犯罪，那么，依附于实行犯的帮助者网络技术服务提供者（ISP）也就不可能构成帮助犯。

2、主观方面之辩

侵犯著作权罪是目的犯，该罪的主观罪过是直接故意，且“以营利为目的”是构成侵犯著作权罪的必要要件。2004 年《关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》第十一条规定，以刊登收费广告等方式直接或间接收取费用的情形，属于刑法第二百一十七条规定的“以营利为目的”。2011 年 1 月《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》第十条对“以营利为目的”予以具体化，规定除销售外、具有下列情形之一的，可以认定为“以营利为目的”：以在他人作品中刊登收费广告、捆绑第三人作品等方式直接或者间接收取费用的；通过信息网络传播他人作品，或者利用他人上传的侵权作品，在网站或者网页上提供刊登收费广告的服务，直接或者间接收取费用的；以会员制方式通过信息网络传播他人作品，收取会员注册费或者其他费用的；其他利用他人作品牟利的情形。“以营利为目的”从根本上讲是行为人的一种主观心理态度。行为人犯罪的主观心理态度是通过行为人在实施犯罪行为前后的一系列外在客观活动表现出来的。因此，在行为人是否出于“以营利为目的”方面，可以着重从这些具体因素来进行辩护：侵权行为发生的背景，如行为人系在日常学习生活中实施的行为，则可以构成合理使用；侵权行为人经营网站纯属公益、实际并未获利等，不具有严重社会危害性等等。

3、客观行为之辩

首先，客观行为“通过信息网络向公众传播”是否等同于《著作权法》里的“信息网络传播”，存在一定的争议。大部分学者认为，著作权法第四十八条从侵权行为的角度规定“未经著作权人许可，复制、发行、表演、放映、广播、汇编、通过信息网络向公众传播其作品的，本法另有规定的除外”，属于侵犯信息网络传播权的行为，其表述与上述司法解释一致，因此“通过信息网络向公众传播”应当等同于“信息网络传播”。但也有部分观点否定两者是同一概念，并对“通过信息网络向公众传播”采取广义的解释，认为其包含信息网络传播权在内的所有的传播行为，这一观点在司法实践中对于“深度链接”的认定上最为突出。理论上的争议导致“通过信息网络向公众传播”这一行为的边界并不清晰，这就为辩护提供了一定的空间。

“通过信息网络向公众传播”的客观行为中，最没有争议的核心行为就是“作品提供行为”，而按照距离“作品提供行为”的远近，我们可以大致罗列一些相近的行为，依次为：WAP 转码服务、网页快照、浅层链接、提供网络服务、非交互式网络传播（网络直播、定时播放，其他如平台“陪看服务”等），而这些行为是否构成本罪，是辩护的重点。

（1）提供作品的行为

提供未授权的作品内容是侵犯信息网络传播权的核心行为，毫无疑问包含在“通过信息

网络向公众传播”之内，对此无争议。

（2）WAP 转码服务

WAP 是一种移动终端浏览转码技术，通过该技术可使 Web 资源在移动终端浏览器浏览。WAP 转码技术作为技术本身并不违法。深圳市福田区人民法院（2010）深福法知产初字第 70 号民事判决书“蔡骏诉深圳宜搜案”也肯定了技术本身不违法。该判决认为，“宜搜网站并没有对涉案小说进行永久复制，因为没有替代第三方网站提供内容”。根据该判决确立的利用 WAP 转码技术等技术手段是否构成直接侵权的标准：一是是否永久复制；二是是否实质性替代对方，对此，在相关案件中，这两个标准也是辩护的重点，即要具体考察 WAP 转码技术抓取的作品是否有合法的授权、正当的依据，是否进行了加工编辑、是否是临时复制等方面来进行辩护。

（3） 网页快照

网页快照，又称快照或网页缓存，术语网络搜索引擎类的技术服务，目的在于帮助网络用户更加快捷方便地得到所想要的内容，而这些内容是事先备份缓存与搜索引擎的服务器，所以网络用户点击快照链就能直接访问。网页快照不同于一般的链接，网络用户点击快照并没有访问其想要访问的目标网站或网页，而是访问了存在搜索引擎服务器上的目标网站或网页的内容，即使目标网站或者网页已经被删除、修改甚至失效，网络用户也能从快照上获得。正是因为网页快照复制了目标网站或网页内容存储在其搜索引擎的服务器内，当快照未经著作权人许可时，快照行为是否会被认定为侵权甚至追究其刑事责任？学界尚有争议。对此，辩护律师重点从两方面进行辩护：一是搜索引擎提供快照的内容本身是侵权作品，则要考查被告人是否尽到了注意义务和审查义务，如果被告人尽到了义务，则无主观恶性、可免责；二是搜索引擎提供的快照是否实际上已经替代了目标网站，给目标网站造成了实质性损害。如果没有实质性替代目标网站，仅仅是正常的网络服务提供行为或合理使用行为，则无需承担刑事责任。

（4）浅层链接与深度链接

网络链接有浅层链接和深度链接之分。设链者在网站或者网页中设置链接标志，网络用户通过点击链接，链接目标网站和网页，从而与被链接的网站或者网页建立联系。浅层链接的网络用户非常清楚哪个是设链的网站和网页、哪个是被链接的网站和网页；深度链接由于并不经过被链接的网站的首页，而是直接跳转到被链接的网站中的具体内容或非网页文件，网络用户不清楚被链接显示的内容是设链的网站网页的内容还是被链接的网站网页的内容。如果行为仅是浅层链接，一般不会涉及到侵犯著作权，也就谈不上相关的刑事责任。深层链接的性质则较为复杂。深层链接首先是帮助行为，这几乎没有什么争议，但其是否可能成为直接提供的实行行为，学界还有不同的看法。对此，辩护的重点应放在深层链接系间接侵权的帮助行为，还是直接侵权的实行行为上，如果认定是帮助行为，则再根据共犯构成理论再进行下一步的辩护。

（5）提供网络服务行为

提供网络服务行为包括提供自动接入、自动传输、信息存储空间、搜索、链接、文件分享技术（包括 P2P 技术）等网络服务。从最终承担的法律责任来看，一些国家例如美国、日本除了要求上述用户承担民事责任外，有的还承担了刑事责任。在民事侵权领域，提供网络服务行为一般只会构成间接侵权、帮助侵权，除非网络服务提供者与作品内容提供者有合作行为。在刑事责任的认定上，由于技术中立、科技无罪，只有在明知对方是侵权行为、违法行为的前提下还以希望或者放任的方式提供网络服务时，才有构成犯罪的可能。

（6）非交互式网络传播

随着网络传播技术越来越进步，尤其是在“三网融合”之后，非交互式网络传播越来越多，这种行为与广播行为非常相似，但却不是广播行为。非交互式网络传播包括网络直播、定时

播放、“陪看”服务等。理论上，非交互式网络传播是否属于“通过信息网络向公众传播”存在争议，一般认为非交互式网络传播不满足信息网络传播权“点对点”交互式的特点，不属于信息网络传播权的规制范围，同时其技术实现方式又不同于广播权的无线传播技术，也不属于广播权的范畴。对此，无论是《世界知识产权组织版权条约》还是《世界知识产权组织表演和录音制品条约》，都将公众从网络获取上传作品的方式限制在交互式传播上，而将非交互式传播排除在外，我国的《著作权法》也是如此。虽然民事司法实践中部分判决有认定非交互式网络传播属于“应当由著作权人享有的其他权利”，如央视诉 PPTV 案。只是至今，笔者尚未发现一例网站由于这种非交互式的网络直播而受到刑事指控，尽管有不少呼吁要用刑事手段解决其侵犯著作权的问题。因此，在现有法律框架内，提供非交互式网络传播的平台只要尽到了合适的注意义务，通常是不太可能会被刑事追责的。

（二）罪轻之辩

1、轻罪之辩：因侵犯著作权罪与生产销售伪劣产品、非法经营等罪名存在牵连关系，而量刑差异较大，如侵犯著作权罪的法定最高刑为七年，非法经营罪可判处五年以上有期徒刑，生产销售伪劣产品罪则判处至无期徒刑，所以对犯罪行为的性质进行有效的界定，能够影响后续的量刑轻重。此罪还是彼罪，重罪还是轻罪，这是辩护律师需要考虑的一个有效辩护策略。

2、轻刑之辩：准确认定涉案情节和涉案价值，实现由“重刑”到“轻刑”的辩护。侵犯著作权案件及涉及著作权的生产销售伪劣产品案件中，法律条文规定了“情节严重”、“情节特别严重”等不同的量刑幅度，或者根据涉案金额规定了“数额较大”、“数额巨大”等不同的量刑幅度。对此，辩护律师可根据案件具体情况，在数额、情节上做文章，实现量刑“由重到轻”的辩护。

（三）证据之辩

随着侦查机关执法规范化建设的深入推进，侦查机关、公诉部门应当根据法律规定收集有罪和无罪、罪轻和罪重的全部证据。辩护律师在辩护过程中，对于侦查环节由控方取得的证据，如授权证明、网上的销售记录等，可以对证据的合法性、客观性、关联性等进行进一步细致审查，排除合理怀疑。另外，因为侵犯著作权罪的网络化、智能化，这种案件电子数据显得尤为重要。然而，电子数据具有高关联性和低真实性的特征，容易被修改，可以被复制，对此，辩护律师在办案中需要从以下三方面进行重点审查：一是要审查电子数据是否由被告人操作计算机系统，或者访问互联网而产生的；二是审查电子证数据在搜集、固定过程中有无被人为破坏或修改；三是审查电子数据所反应出的相关信息是否能够证实嫌疑人实施犯罪。关于侵犯网络著作权犯罪电子数据的以上三点，不仅是侦查机关侦查工作中固定、搜集电子数据的关键点，也是刑辩律师辩护工作中在法庭质证的关键点，对最终的定罪量刑至关重要。

综上，侵犯网络著作权案件的办理，专业性强，对办案人员的专业知识要求高，如果缺乏对专业知识和行业经验的了解，则很难应对此类案件的办理。检察机关和审判机关已经开始探索并实行知识产权检察、审判专业化，并且已经设置有专门的知识产权法院，这对刑事律师提出了更高的要求。对此，刑事律师应加强专业队伍与办案团队建设，切实提高辩护与代理能力，在此类犯罪中切实维护被告人的合法权益。

3.试析侵犯知识产权犯罪中的电子证据审查

一、侵犯知识产权犯罪中电子证据的种类

电子证据是一种借助于现代数字化电子信息技术及其设备进行存储、处理、传输、输出

的证据。此类证据不同于传统意义上的证据。最初证据法学的主流理论将电子计算机所记录的资料纳入到视听资料的范畴，但随着对电子数据认识的逐步深入，电子数据开始有了独立的地位。睥 2013 年 1 月 1 日实施的《刑事诉讼法》，首次在基本法律层面涉及到电子证据问题，并将电子证据列为八大类可以用于证明案件事实的证据之一，这也使得电子证据有了明确的立法依据。在侵犯知识产权犯罪案件中，电子证据形式主要有以下三种类型。

（一）网店交易记录

犯罪分子通过开设网络虚拟店铺，利用网络交易平台销售假冒伪劣商品或者销售假冒注册商标的商品或者销售侵犯他人著作权的图书，并通过物流公司以快递的方式完成产品的交易和销售。以罗孝聪、罗孝明案为例，二人在淘宝网上注册网上书店来销售盗版的医学类考试用书。通过对网站交易情况记录的调取和分析，最终确认网店的非法经营数额达人民币 20 余万元。

（二）互联网广告链接

犯罪分子通过互联网传播其广告链接，扩大受众范围，并以网络为媒介，一方面从上游联系购货渠道，另一方面，拓宽下游的销售渠道，来扩充其作案空间。以姚立明假冒注册商标案为例，姚立明在网上发布信息，联系客户收购二手的思科产品，然后经过测试、清洗、灌粉、打标、贴标和包装后又通过网络发布广告，招揽卖家进行销售。

（三）互联网站截图

犯罪分子搭建互联网网站运营牟利，从事新型犯罪活动。以李玉峰等人侵犯著作权案件为例，犯罪分子利用网络游戏《剑侠世界》源代码架设服务器运营游戏私服，从中非法获利。犯罪分子开设“私服”《情缘剑侠世界》网站，在界面、地图、场景、人物设置和功能方面都同正版的《剑侠世界》网络游戏一样，并且可以和《剑侠世界》的官方网站进行链接。通过对游戏网站的截图对比可以得出私服游戏和官方游戏的相似度，同时也可以反映出“私服”游戏网站的会员注册情况。

二、电子证据的取证现状

目前公安机关在搜集和移送电子证据过程中主要存在以下四大问题。

第一，公安机关有时不能及时搜集、固定证据。在姚立明假冒注册商标案中，嫌疑人供述曾在淘宝网开设网店销售假货，但由于年代久远网店被关闭，公安机关无法调取网店销售交易记录，故对网络销售的事实无法指控。

第二，公安机关提供的电子证据缺乏实质证明力。如在刘修贵等人侵犯著作权一案中，刘修贵等人在淘宝网开设书店来销售各类盗版教材，公安机关在移送审查批捕时提供了案发前几个月网店销售情况的 Excel 表格。由于“淘宝交易宝贝”在一套书与一本书上并无区分，均显示为一，仅从表格记载的“淘宝宝贝”数量无法准确得出实际的销售的册数。故此类 Excel 表格记载的内容缺乏实质证明力。

第三，公安机关提取电子证据的程序存在瑕疵。侦查人员违反程序搜集扣押证据，会降低证据的证明力，导致其面临被排除的风险。即使检察机关可以将此类案件退回补充侦查或要求公安机关进行说明或解释，但这也在一定程度上降低了诉讼效率。

第四，公安机关提交电子证据的形式过于简单。公安机关通常只对电子证据进行简单收集，装订成册或刻录光盘移送了事。公安机关在内容上并未对提取的对象、方法、程序和过程予以说明，也不会将扣押的存储介质一并移送审查。

三、电子证据的审查方法

《关于死刑案件审查判断证据若干问题的规定》第二十九条对电子证据的审查方法有明确的要求，包括：电子证据的制作、储存、传递、获得、收集、出示等程序环节是否合法，电子证据的内容是否真实、有无裁剪、拼凑、篡改、添加等伪造、编造情形，电子证据与案件事实有无关联性等。笔者认为，此种审查方法对一般刑事案件中的电子证据审查同样具有较大的指导意义，可以从以下三个大的方面审查知识产权犯罪案件中的电子证据。

第一，审查电子证据的合法性。电子证据的收集主体必须合法。根据刑事诉讼法的相关规定，证据的收集主体只能是拥有侦查权的侦查机关。在侵犯知识产权刑事案件中，网络服务商作为收集的证据不能作为定罪的直接证据使用，只有公安机关对网页或电脑进行勘验检查后提取的证据，才符合电子证据合法性的要求。电子证据的收集程序也必须合法。根据公安部在 2005 年颁布的《计算机犯罪现场勘验与电子证据检查规则》的规定，电子证据的收集涉及犯罪现场勘验，应严格按照规范进行。该规定对电子证据的制作、存储、传递、获得、收集、出示等环节做出了明确的规定。但实践中，公安机关仅将电子证据的打印件提交，却不对提取的过程、方法予以说明，也不提供相应的检验报告文书，有的甚至只是移送一张电子证据内容的光盘，即便上面有犯罪嫌疑人的签字确认，也违反了电子证据收集的程序性规定。如果程序上存在瑕疵或者手续不全，承办人必须要求侦查机关的办案人员对程序上存在的瑕疵进行补正或做出合理的解释，否则该份电子证据则会由于收集程序不合法，可能面临不能被采用的风险。承办人应重点审查公安机关在勘察过程中程序是否合法，对勘察的过程是否进行全程同步录像。审查公安机关是否在勘验检查报告中记载了目标设备和系统名称等必备信息，对于远程勘察的计算机网络系统还应当记录目标网络的地址、服务器名称、网络运营商等信息。

第二，审查电子证据的真实性。只有查证属实的证据才能作为定案的依据。要确定电子证据的真实性，首先，要对电子证据原始性进行审查，以确定电子证据的数据和内容是否被篡改、修改或删除。其次，要保证电子证据收集的全面性，防止侦查机关片面的收集证据，遗漏重要的犯罪证据。以上两点就要求侦查机关在移送电子证据时将电子证据的原始存储设备连同电子证据的打印件或光盘文件一并移送。承办人应重点审查电子介质中所记载的内容是否同打印件和光盘文件一致。因为电子证据的打印件或光盘文件并非原始证据，而是电子证据的转化物，一旦转化证据出现了错误而不能及时被发现，就会导致依据转化证据而做出的审查结论存在问题。

第三，审查电子证据的关联性。审查关联性关键在于把握电子证据与事实的连接点，电子证据可以证明的事实必须和其他证据结合才能有效指控犯罪。如利用淘宝网店销售假冒注册商标的商品案件中，除了公安机关提取的网店的销售记录外，还需结合买家的证言、汇款凭证、起获的实物、快递公司的证言、发货单据等一系列其他证据材料，进行综合判断才能得出结论。承办人应重点审查侦查机关提供的电子证据同在案的物证、书证、证人证言、犯罪嫌疑人的供述和辩解以及鉴定结论是否互相吻合，是否互相印证。

四、完善电子证据对策

（一）电子证据法律层面的完善

电子证据不能套用传统证据的程序法规定，应在立法层面上制定出一套符合电子证据特征的取证规则。一种做法是可以借鉴其他国家或者地区的经验，制定统一的电子证据法，也可以根据《计算机犯罪现场勘验与电子证据检查规则》等相关规定，在刑事诉讼法中设立专章对刑事诉讼中的电子证据收集和审查问题作出具体的规定。另一种做法是可以由公安部、最高人民检察院、最高人民法院等机关联合出台对刑事案件中电子证据收集、审查方法的相

关司法解释。这就可以在立法层面形成一个电子证据收集和审查方面的明确系统的规范。

（二）电子证据制度层面的完善

电子证据的固定和调取离不开网络运营商的配合，但现在主要存在两大困难。一是网络运营商不配合；二是电子证据受时效限制。常见的淘宝交易记录、QQ 聊天记录的保存时限通常仅有六个月，大部分案件在案发时都已经过了电子证据的保存时限，导致公安机关无法有效的开展侦查工作。笔者建议，司法机关可以和互联网服务提供商签署合作协议，互联网信息服务提供者应适当延长信息的保存期限，对发现可能涉及犯罪的电子数据应予以恢复以配合司法机关工作，保证电子证据调取过程的顺畅。

（三）电子证据人才建设层面的完善

电子证据的审查需要建立一个专业化的队伍。审查电子证据的过程不仅需要承办人有极大的耐心和细致度，而且还需要承办人及时更新知识和技能。承办人往往会受计算机水平的限制，无法达到计算机网络技术审查水平的要求。检察机关应定期开设专门的电子培训业务，提高承办人审查电子证据的能力，保证电子证据审查工作的顺利开展。

4.网络侵犯著作权案件中电子证据的审查判断

【案情】

江苏省扬州市人民检察院以被告人李旭东、赵朋飞犯侵犯著作权罪，且二人系共同犯罪，向扬州市中级人民法院提起公诉。

公诉机关指控被告人李旭东、赵朋飞在明知韩国 ACTOZ 软件有限公司和 WEMADE 娱乐有限公司享有网络游戏《传奇 2》（又名《热血传奇》）的著作权，其授权在中国境内由上海盛大网络发展有限公司特许独家经营的情况下，于 2006 年 1 月 1 日至 3 月 16 日，擅自对《传奇 2》网络游戏程序的非关键性程序进行修改，并以上海银月网络科技有限公司的名义，租用上海欧网网络科技发展有限公司托管于江苏省江阴市定山路电信机房的 46 台服务器，先后架设仿《传奇 2》的“银月传奇”、“小二传奇”等私服程序，在互联网上为网络游戏玩家提供上述游戏，通过出售会员资格、出售游戏装备、为玩家调整级别等方式获取非法所得计人民币 24 万余元。

经依法鉴定，被告人李旭东、赵朋飞所架设的私服程序，与《传奇 2》网络游戏软件大部分存在复制关系。

案发后，被告人李旭东主动向公安机关投案自首，并退出赃款人民币 6 万元。

被告人李旭东、赵朋飞对公诉机关指控的犯罪事实供认不讳，未作辩解。

【审判】

扬州市中级人民法院经审理认为，被告人李旭东、赵朋飞以营利为目的，未经著作权人许可，私自架设他人享有著作权的网络游戏服务器端程序，并通过互联网非法运营，其行为属复制发行计算机软件的行为，且违法所得数额巨大，已构成侵犯著作权罪。公诉机关指控的犯罪事实清楚，证据确实、充分，指控的罪名成立，应予支持。被告人李旭东有自首情节，且认罪态度较好，依法可从轻处罚，并给予一定的缓刑考验期；被告人赵朋飞认罪态度较好，可酌情从轻处罚，并给予一定的缓刑考验期。依照《中华人民共和国刑法》第二百一十七条第（一）项，第二十五条第一款，第二十六条第一、四款，第六十七条，第五十二条，第七十二条，第七十三条第二、三款，第六十四条以及最高人民法院、最高人民检察院《关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释》第五条第二款，第十一条第三款之规定，于 2006 年 12 月 19 日作出（2006）扬刑二初字第 0018 号刑事如下判决：

一、被告人李旭东犯侵犯著作权罪，判处有期徒刑三年，缓刑三年，并处罚金人民币三万元；

二、被告人赵朋飞犯侵犯著作权罪，判处有期徒刑三年，缓刑三年，并处罚金人民币二万元；

三、扣押在案的犯罪工具和已退出的赃款人民币六万元予以没收，上缴国库；未退出的赃款继续予以追缴。

宣判后，两被告人没有上诉，检察机关也没有抗诉，判决现已发生法律效力。

【评析】

近年来，利用网络进行各种犯罪的案例在各地都时有发生。本案是江苏省首例利用互联网侵犯著作权的刑事案件。互联网的普及，在丰富与便捷人民生活的同时，也为网络犯罪提供了一定的空间。网络本身的数字化、虚拟化、开放性使得网络犯罪呈隐蔽性、智能性、跨地域性等特征，这就为此类案件的查处带来了前所未有的挑战。在侦破、审理这类案件时，电子证据发挥了不可替代的作用。

一、电子证据的概念

关于电子证据的概念，有着广义与狭义之说。广义的电子证据是指以电子形式存在的，作为证据使用的一切材料及其派生物，包括计算机证据以及传统的视听资料等，它涵盖但不限于电子数据交换、电传、电子邮件。联合国国际贸易法委员会以及美、德等国家有关电子证据的立法基本采广义之说。狭义的电子证据即指在计算机或者计算机系统运行过程中产生的，以其记录的内容来证明案件事实的电磁记录物，如 BBS 留言、网络聊天记录、EDI 电子邮件、软件使用界面等。欧盟、加拿大、韩国等主要的狭义的语境里使用电子证据概念。

我国的主流观点也主张在狭义意义上使用电子证据说。以笔者之见，可以将电子证据定义为：在计算机或计算机系统运行过程中借助电子技术或者电子设备而形成的、以电子介质形式存在并能存储于磁性介质之中，用作证据使用的一切材料及其派生物。

二、电子证据的特征

电子证据往往是以磁盘、光碟、ROM 等磁性材料、光学材料、半导体材料为载体，容易被修改、删除或者转移。

较之传统证据形式，电子证据具有以下特征：（一）技术性。电子证据是通过各种电子介质以电子形式而存储的，其必须通过计算机等电子设备或者类似的设备生成、发送、接收、存储和演示，具有较高的技术性。（二）无形性。在计算机内，信息被数字化，以不可见的编码来传递，不能直接为人所感知。（三）脆弱性。电子证据不但容易被改变、损坏或销毁，如常见的电磁干扰、删除操作或不当操作，而且破坏后具有隐蔽性，故而作为电子证据的计算机信息是以非连续性的数字存储方式记录的，信息是否曾被删除、编辑、截断等是难以查明的。（四）多样性。存储在计算机内的各种信息可以通过计算机屏幕显示、通过打印机打印到纸上，还可以与其他外部设备连接转换成各种格式输出，呈现出各种各样的外部形态。

三、电子证据的归类

电子证据产生于信息传输的中间环节，不是事实直接作用形成，其具有的上述特征也说明电子证据较之其他类证据来说欠缺一定的稳定性，这也是司法实践中对电子证据争议较多的主要原因之所在。

我国刑事诉讼法明文规定，能够证明案件真实情况的一切事实，都是证据。因此，当前理论界和司法实务界对电子数据可以作为证据使用意见基本一致，但由于刑事诉讼法没有将电子证据作为法定的证据种类，因此，理论界更多争执的是电子证据的归类，如视听资料说、书证说、物证说、鉴定结论说，甚或混合证据说，等等，莫衷一是。

笔者认为，电子证据作为一种特殊的证据形式进入诉讼领域无可厚非。刑事诉讼法规定的七种法定证据形式没有哪一种能够完全把电子证据包容进去，电子数据证据本身具有自己的特性，简单的将其归入到某种证据种类中是不可取的，因为不同的证据形式有不同的审查判断标准。随着计算机网络犯罪呈不断上升趋势，我们有必要将电子证据作为一种独立的证

据形式进入诉讼领域，以针对电子证据的特殊性，采取不同的审查判断标准，以便能更加准确、科学地界定案件的事实。

四、电子证据的审查判断

证据的审查判断，就是对所收集的证据，根据证据的客观性、合法性、关联性要素，综合案件的具体情况，进行分析、鉴别与判断。我国刑事诉讼法第四十二条规定，证据必须经过查证属实，才能作为定案根据。要使得证据材料转变为定案的证据，必须经由司法人员依据一定标准进行去粗取精、去伪存真、由此及彼、由表及内、表里结合的审查判断。

任何一个刑事证据都是真实的证据内容与合法的证据形式的统一，电子证据也是如此。对电子证据的审查判断，除了同其他证据一样，从证据客观性、关联性和合法性基本特征进行审查判断以外，还应当兼顾到电子证据本身的特殊性，进行综合的审查判断，以达到准确适用法律，依法保护公民的合法权益。

笔者认为，对于电子证据，可以从以下几个方面去审查判断：

（一）审查电子证据的收集主体。收集证据是公安司法机关和律师为了证明特定的案件事实，按照法律规定的范围和程序，收集证据和证据材料的法律活动。刑事诉讼法第四十五条第一款、第三十七条明确规定，证据的收集主体是公安司法机关和辩护律师，而其他主体都不是证据收集的合法主体。尤其对于电子证据，根据国家安全法和人民警察法的有关规定，只有国家安全机关因侦察危害国家安全行为的需要以及公安机关因侦查犯罪的需要，才可以采取技术侦查措施。因此，合法的电子证据收集主体目前仅限于国家授权的专门执法机关，也就是国家安全机关和公安机关的技术侦查部门，未经国家授权的任何其他部门、团体或个人都不是电子证据收集的合法主体。同时，鉴于电子证据智能性的本质要求，审查电子证据是还必需考查收集人员本身对计算机信息技术的掌握能力，不至于在收集过程中对证据造成人为的损害和疏失。

（二）审查电子证据的收集过程。收集证据，必须遵守法定的程序。电子证据的收集同样必须以合法的程序为保证。刑事诉讼法第八十九条至一百二十二条对如何讯问犯罪嫌疑人，询问证人、被害人，勘验、检查、搜查、鉴定，扣押书证、物证等都作出了具体的法律规定。在电子证据的收集过程中可以参照执行。另外，由于电子证据易被篡改、时刻处于变化之中、难以固定，为了提高其证明效力，在收集电子证据时，可以邀请具有信息技术的专业人士或者公证部门对收集的全过程进行见证或公证。法官在采信该类证据时，应当注意对于那些通过非法软件以及非核证软件所获取的电子证据不予采纳。在最后认定时，并有必要借助计算机专家对电子证据是否被修改、收集手段是否正确等提出权威意见，从而为司法人员全面审查证据提供有力的帮助和科学依据。

（三）审查电子证据本身的内容。客观性是证据材料能成为证据的最本质的要求。因而，首先要对电子数据证据的客观真实性进行审查：即证据应该是在案发过程中形成、不以人的主观意志为转移，是伴随着案件事实而产生的。电子数据证据应当符合案件事实的真相，是对象行为的本意和自然地表现。电子数据证据的客观真实性不仅取决于其记载是否属实，还得审查其记载的案件信息的客观真实的物质表现形式，因为如实记载并不能保证它的物质表现形式被真实地收集。电子数据能证实是客观真实记载后，还必须审查其与案件事实是否具有关联性。任何证据都必须与案件具有关联，其所反映的内容必须与案件事实密切相关，才具有证明效力，否则，即使其内容是客观真实的，也会因其不具有关联性而失去证据意义。在审查电子证据时，必须紧紧抓住电子证据所反映的信息与案件事实之间有无必然联系，认真分析对比，综合印证，以排除其他可能性。

（四）审查电子证据依托的技术设备的性能。电子证据往往以磁盘、光碟等光电材料为载体，并借助于一定的多媒体设备才能显示出来。鉴于此，对电子数据所依托的技术器材设备的性能和可靠性审查就很有必要了。要保证通过电子侦查手段获取的电子数据的高质量，

就必须适用具有较高灵敏度、高分辨率以及高清晰度的专用电子设备，否则获取的电子证据将可能失真、模糊或者不完好的，会大大降低其证明力和可靠性。因此，必须审查这些设备的性能、提取时是否正常运作、有无人为破坏或者感染病毒等，要做好这项工作，可以邀请具有专门计算机信息技术的专业人士进行。

五、电子证据的审查判断方法

电子证据因其容易被删除、增补和篡改，因而对其审查判断必须采取一些方法手段，以便准确界定案件事实。通常对电子证据我们可以采取以下审查判断方法：

（一）庭审质证法。庭审作为控辩双方进行直接言词对抗的重要阵地，一直以来就作为中外古今案件审理的最主要方式，在这里双方的分歧与主张可以得到透明的解决。最高人民法院《关于执行中华人民共和国刑事诉讼法若干问题的解释》第55条规定："证据必须经过当庭出示辨认、质证等程序查证属实，否则不能作为定案的根据。"因此，法庭质证是审查证据必须遵守的法定诉讼程序，也是审查证据的重要方法。对电子证据也是如此。除了法律规定，涉及国家秘密、商业秘密或者出于保护手段秘密性等原因除外，在法庭审理阶段，应当尽可能地将相关的电子证据在法庭上借助多媒体设备利用信息技术出示、播音或播放，认真听取提供人对证据情况的介绍，并征询控辩双方的意见，从而作出正确的判断。不宜当庭出示的上述电子证据也应当在庭审中释明原因。

（二）技术检查法。比起普通证据，电子证据往往具有一定的技术性，因而对其审查判断也就必然需要具有一定计算机网络专业知识的人员运用相关的信息技术对电子证据中技术因素进行检查。主要是运用科学技术知识以及先进的科技设备对获得的电子证据的设备和形成过程进行检查验证。如检验电子介质的分辨率；记录载体与运行设备的性能；电子数据生成的日期与原始提取记录是否吻合等。

（三）科学鉴定法。电子数据是以电磁或光子信号等物理形式存在于各种各样的存储介质上，因而被轻易地改动或删除，而这单凭普通人的感官感觉无法辩明真伪，必须要由具有专门鉴定人员利用其所掌握的技术知识对电子证据进行鉴定。因为电子证据基本是以全方位的全息资料形式呈现，能够反映出案件发生全程或部分动态过程，作案人无论有多高的伪造和伪装手段，终不能面面俱到，往往难逃过利用科技设备所做的鉴定。如鉴定某一时段（刻）互联网上某网页的真伪，可以利用网络截屏来鉴别；鉴别录像资料中画面有无利用录像编辑机重新编辑，就可以通过高能分辨仪予以鉴核；看录音磁带是否属于原始生成还是剪辑合成，可以利用音素分辨仪进行鉴定等。

（四）对比印证法。任何证据的真实性，都不是靠自己证明自己，而是要依赖于其他证据进行佐证。对于运用电子侦查手段获取的录音、录像、网页截屏、电子数据等资料进行审查检验其是否科学可靠，同样也应当把它同其他经过核实的证据进行对照。经过对照能够互相印证，并能排除合理怀疑的，由此得出的结论往往是可靠的。否则若存在矛盾，则需要找出矛盾之所在，再对全案证据进行认真梳理审核后方能作出审查判断结论作出最后的评断。

（五）模拟验证法。电子证据具有一定的脆弱性，往往是稍纵即逝，失去了就无法再次得到。在司法实践中，也对电子证据很难固定。而有些电子证据却对定案起着决定性作用。鉴于此，我们可以模拟场景和掌握的案发时的条件，进行检测，促使电子证据"再现"，从而有效地认定案件事实。

本案在侦查过程，侦查人员通过网络截屏、网上远程勘验记录以及电子证据检查比对等技术手段获取了相应的电子数据证据。合议庭在审查判断上述证据时，要求公安机关提供提取电子数据证据的相关说明，以证明提取电子证据时，计算机系统硬件完好、软件安全可靠、机体运行正常、没有病毒侵蚀和人为改动的可能。在提取、复制电子证据后，由提取、复制电子证据的制作人、电子证据的持有人和能够证明提取、复制过程且通晓计算机知识的见证人签名或者盖章等。通过上述手段，排除了电子数据证据发生变化的可能，为案件的审理提

供了坚实的基础。

5.著作权纠纷如何质证经公证的电子证据

在著作权纠纷案件中，对网络信息等电子数据组成的电子证据进行公证举证已经是目前著作权诉讼中的常见信息，尤其在关于信息网络传播权的案件中，此种证据固定方法被广泛采用。

但是需要指出的是公证仅仅是固定证据的一种方式。从证据固定方式的角度而言，其不能直接证明被告是否构成侵权，真正起决定作用的仍然是由某种公证方式所固定的证据本身。另外，如果公证程序有瑕疵也有可能造成侵权难以构成。作为被告也不要被原告所谓的公证文件所吓倒，冷静质证，全面分析仍然是作为被告应当完成的工作。

1、基础证据的可信性

著作权纠纷中原告的基础证据是涉案作品原告是否具备著作权。原告如果仅对侵权行为作了大量举证，但是就此基础问题缺乏说服力的证据，后面的公证其实是没有多大意义的。

2、网站登录地点

质证时应关注公证文件中所体现的网站登录地点。尤其对于教育或科研机构侵权案件中，如果原告所选择的网站登录地点为上述机构的内部，那么气所采用的网络很有可能是内部局域网或其他少数科研人员才能登录的网页，该登录地点的选择显然不具有代表性。

3、证据直接性、连贯性

无论是邮箱公证还是网站公证很关键的一点就是各证据页面之间必须实现连贯性。如果不能连贯性取证，则会使得公证的电子证据不具有唯一性的特征。在连贯性和唯一性丧失的情况下，很难构成被告的侵权。例如对某段视频的公证，如果仅仅公证了通过各种链接实现该网站某网页显示了侵权视频的首镜头，然后公证人员进行了截图。

单凭该截图其实并不能直接证明该网站的视频是否可以连续播放。即便公证人员抽样式的截图视频内容，质证时也应当对照原告公布的正版视频内容，审查抽样截图的镜头在正版视频中是否存在。

4、截图质证

经过公证的网站截图是否完整体现了网页信息，所体现的网页信息是否为被告网站等情况，被告应当全面审核截图内容作出质证回应。

5、两次以上提交公证材料

由于电子证据的多变性，原告应当一次性将一个公证业务下的所有公证材料向法院提交完毕。如果出现原告二次或多次提供公证材料包括就提供就某公证事项的情况说明（法院要求的除外），被告有权拒绝对新提供的公证材料提起质证并对整个公证业务向法院提出质疑。

该情况法律虽然没有直接规定，但是对于多次提交公证材料的情况，往往是因为前一次公证内容遗漏，甚至公证内容错误等情况所导致的。对于该类情况，已经丧失了公证本身的严肃性，降低了公众对公证的信赖。在被告提出上述质疑的情况下，法院一般支持被告的意见。

6、灵活使用对方公证证据

电子证据本身所体现的内容有时并非完全对被告不利。例如在对某段视频或图片进行公证时，网页截图内容有时会显示图片或视频的点击率，如果点击率过低，则被告可以此为理由请求法院降低赔偿数额。

7、费用票据

公证费用一般为法院所支持，但是经过公证人员公证的在电子数据公证时花费的其他费用，被告应当严格质证该票据信息与案件的关联性。

以上对公证电子证据的质证角度也是原告在起诉前办理公证时所应当注意的关键之处，盲目的迷信公证形式，而对公证点缺乏理性的筹划，同样可能输了官司。

（十五）侵犯公民个人信息

1.侵犯公民个人信息罪的理解与适用

时间：2016-07-13　　作者：薛培　叶小舟　王斌
来源：检察日报

刑法修正案（九）将刑法第253条之一修改为：“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。”从以上条文内容可以看出，刑法修正案（九）在刑法修正案（七）的基础上再次将侵犯公民个人信息犯罪纳入修改的范围，且修改幅度较大，在司法实践中亟须正确理解和适用。

“公民个人信息”的内涵

由于我国目前尚未制定出台个人信息保护法,因而如何确定个人信息的概念和范围，是一个重要问题。公民个人信息，是指公民个人不愿为一般普通社会公众所知，并对公民个人有保护价值的信息。在刑法语境里，非法获取公民个人信息意指侵犯了公民的隐私权，即自然人享有的私人生活安宁与私人信息不被他人非法知悉、搜集、利用和公开的一项人格权。该条文规定的公民个人信息即为任何单位或个人在履行职责或者提供服务过程中获得的公民个人信息。从信息的内容看，其涉及公民的个人隐私权。刑法修正案（九）将犯罪主体扩大到一般主体，而不仅局限于刑法规定的国家机关、金融、电信、交通、医疗等单位的工作人员。

笔者认为，公民个人信息应当是“与公民个人密切相关的、其不愿被特定人群以外的其他人群所知悉的信息”。

“出售、提供、获取”是否为非法的适用理解

刑法修正案（九）将刑法修正案（七）所规定的“出售、非法提供公民个人信息”中的“非法”予以删除。笔者认为，此举既是一种立法应然的理性价值取向，同时也是一种立法应然的规范取向。事实上，“出售、提供、获取”行为本身即侵犯了公民的个人隐私权，这种行为无论从何种角度来说，都是违背公民之主观愿望而“非法”的。由此，笔者认为，“出售、提供、获取”之“非法”并非指出售、提供、获取手段或者方法行为的性质，而是指行为人的出售、提供、获取行为在本质上就是非法的。不能单纯以获取、出售、提供行为违背法律禁止性规定予以认定，即行为人只要没有出售、提供、获取公民个人信息的法律依据或者资格，也没有得到公民个人的许可，就可能构成犯罪。

对于“出售、提供、获取”的方式，目前理论界和实务界关注不多，笔者认为，无论以何种方式出售、提供、获取公民个人信息，只要其超越了公民个人相应授权和许可，即没有出售、提供、获取资格或者根据的人，以窃取或者其他方法出售、提供公共服务提供者在服务过程中收集或者发布公民个人信息的，即可认定为“非法”。易言之，刑法既要制裁公共服务提供者将自己保有的公民个人信息非法出售、提供给他人的行为，又要处罚他人侵犯公共服务提供者对公民个人信息之保有状态的行为。从这个层面上看，出售、提供、获取等方式均

为侵犯公民个人信息之行为。公民在接受公共服务时,相关单位也应对其所保存的个人信息予以保密，如擅自获取并出售、提供给他人或单位，只要造成相应的严重后果，也应追究其刑事责任，而能获取公民个人信息之主体，无论其出于何种目的或主观愿望，皆不能擅自通过任何手段、方式获取公民个人信息。

“出售”与“提供”之间有何区别与联系

刑法修正案（九）第 17 条第 1 款、第 2 款将出售与提供行为并列表述。有观点认为，所谓的出售，是指以获得对价为目的的提供行为；提供，是指不以获得对价为目的的提供行为，出售与提供两者是并列关系。该观点值得肯定的地方在于其认为出售亦是一种提供行为，但对于提供须具有不以获得对价的目的的看法。笔者认为，该观点值得商榷。

从语义上分析，“出售”是指将自己掌握的公民信息卖给他人，自己从中牟利的行为；“提供”是指不应将自己掌握的公民信息提供给他人（包括单位和个人）而予以提供的行为。易言之，提供并非指不以获得对价为目的的提供行为，立法上对其主观目的并无限制；而出售是指以谋取对价后将某物提供给他人，其亦属提供行为的一种。如果认为出售行为比单纯的提供行为具有更为严重的主观恶性及客观危害，则在罪状的表述上应能体现出来。但遗憾的是，不管是刑法修正案（七）抑或刑法修正案（九），从罪状的表述上看，出售与提供行为均为并列关系，两者在达到情节严重后，均可入罪惩治，并无量刑上的差异。如若认为出售与提供行为危害性方面无异，那么出售也是一种提供行为，直接规定提供行为即可。可见，刑法修正案（九）将出售与提供行为进行并列表述的方式有待商榷。

关于“情节严重”的理解及适用

对于侵犯公民个人信息罪中“情节严重”的认定，目前尚无司法解释作出规定。笔者认为可依次考虑三个因素：一是只要该信息被用于实施犯罪活动，均可认定为情节严重；二是看是否严重危及公民个人的正常生活，或者给公民个人带来较大经济损失或导致其他后果；三是在无法认定前两者的情况下，根据出售、提供或者获取信息的数量、次数加以确定，其中，在出售的情况下还包括获利金额，在提供、获取的情况下还要考虑手段的恶劣程度或者支付的对价金额，等等。即情节是否严重，可以从出售、提供、获取的公民个人信息的数量、次数、获利金额、手段、持续时间、动机目的、危害后果等多个方面进行综合判定。具体而言，具有以下情形之一的，可以判定为情节严重：

1.利用出售、提供、获取的公民个人信息进行违法犯罪活动的。实践中，有些行为人出售、提供、获取公民个人信息是为了拓展公司业务或是个人人脉，有些行为人则是为了进行违法犯罪活动，其主观恶性差异较大。对于为了实施违法犯罪目的而获取、使用公民个人信息的，应当属于情节严重。

2.出售、提供、获取公民个人信息对公民合法权益造成严重损害的，其中包括造成公民严重精神损害或者重大经济损失。严重扰乱公民正常的生活、工作和学习的，应当认定为侵犯公民个人信息的行为造成了严重后果，应确定为情节严重。当然，并非只有犯罪后果实际发生才构成情节严重，可以结合犯罪结果的发生与否，或是特定公民的人身权利、财产权利所面临的风险大小来确定是否属于情节严重。一般而言，产生实际损害的情节重于面临极大风险的情节。

3.出售、提供、获取公民个人信息手段恶劣的。有的行为人为了达到出售或获取公民个人信息的目的，往往会额外实施一些辅助行为；有些行为人则是组织化、规模化或者用恶劣手段获取公民个人信息。因而，就行为方式而言，行为人以暴力、胁迫、欺诈等方式，或纠集、雇用多人出售、提供、获取公民个人信息的，可视为情节严重。

4.利用所掌握的公民个人信息从中获利数额较大的。即行为人出售公民个人信息违法所得数额较大的。数额较大的标准，可以根据经济社会发展情况及相关犯罪立案标准综合确定，笔者认为，出售公民个人信息获利数额达 5000 元以上的，可确定为情节严重。

5.其他应当认定为出售、提供、获取公民个人信息情节严重的行为。虽未达到以上标准，但综合考量案件的全部情况，有两个以上情节接近以上标准，或者有一个情节接近以上标准，同时具有其他从重情节的，也应当认定为非法获取公民个人信息情节严重。

(作者单位：四川省成都市人民检察院、四川省成都市龙泉驿区人民检察院、广东省珠海市人民检察院)

2.降低入罪门槛，严惩侵犯公民个人信息犯罪--“两高”《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》解读

侵犯公民个人信息罪入罪要件“情节严重”如何界定？拒不履行公民个人信息安全管理义务的行为是否担责？涉案公民个人信息的数量计算遵守怎样的规则？今天上午，最高人民法院、最高人民检察院联合召开新闻发布会，发布《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》），对侵犯公民个人信息犯罪的定罪量刑标准和有关法律适用问题作了全面、系统的规定。最高法、最高检有关部门负责人就《解释》相关亮点在新闻发布会上回应了媒体关切。

从五个角度准确认定“情节严重”

侵犯公民个人信息罪的入罪要件为“情节严重”。

最高法研究室主任颜茂昆介绍说，根据法律精神，结合司法实践，《解释》第五条第一款设十项对“情节严重”的认定标准作了明确规定，大致涉及如下五个方面：

一是信息类型和数量。基于不同类型公民个人信息的重要程度，《解释》分别设置了“五十条以上”“五百条以上”“五千条以上”的入罪标准，以体现罪责刑相适应。

二是违法所得数额。出售或者非法提供公民个人信息往往是为了牟利，基于此，《解释》将违法所得五千元以上的规定为“情节严重”。

三是信息用途。《解释》将“非法获取、出售或者提供行踪轨迹信息，被他人用于犯罪”“知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供”规定为“情节严重”。

四是主体身份。公民个人信息泄露案件不少系内部人员作案，对此，《解释》明确，“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，认定“情节严重”的数量、数额标准减半计算。

五是前科情况。曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的，行为人屡教不改、主观恶性大，《解释》将其也规定为“情节严重”。

设立网站侵犯个人信息可构成非法利用信息网络罪

实践中，一些行为人建立网站、通讯群组供他人进行公民个人信息交换、流转、销售，以非法牟利。

颜茂昆说，根据刑法有关规定，设立用于实施违法犯罪活动的网站、通讯群组，情节严重的，构成非法利用信息网络罪。供他人实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组实际上属于“用于实施违法犯罪活动的网站、通讯群组”。

对此，《解释》规定：“设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定，以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。”

拒不履行管理义务，网络运营者或触刑法

当前，不少网络运营者因为履行职责或者提供服务的需要，掌握着海量公民个人信息，这些信息一旦泄露将造成恶劣社会影响和严重危害后果。对此，网络安全法明确规定：“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。”

为进一步促使网络服务提供者切实履行个人信息安全保护义务，《解释》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。

破解公民个人信息数量“计算难”

公民个人信息数量是侵犯公民个人信息案件定罪量刑标准的主要依据，至关重要。实践中，司法机关查获的涉案信息数量动辄上万条、数十万条，甚至以兆计算，怎样科学、合理认定信息数量是办案部门一直难以解决的问题。

新闻发布会上，最高检法律政策研究室副主任缑杰介绍说，为增强《解释》的可操作性，《解释》专门规定了数量计算规则。如《解释》规定：“非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算。”

“非法获取了他人拨打电话的记录五十条，将其出售给同一人或者单位的，应当认定为侵犯公民个人信息五十条。”缑杰解释道。

按照《解释》，公民个人信息向不同对象分别出售、提供的，属于重复出售或者提供个人信息，社会危害性较一次性出售或提供危害性更大，数量应累计计算。比如，非法获取了他人拨打电话的记录五十条，将其出售给两个人或者单位的，应当认定为侵犯公民个人信息一百条。

针对涉案的公民个人信息上万条甚至更多的，可能存在信息重复的情况，《解释》特别规定：“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。”

3.公安部“净网”行动

2016 年以来，全国公安机关在打击整治网络侵犯公民个人信息犯罪专项行动、打击整治黑客攻击破坏犯罪和网络侵犯公民个人信息犯罪专项行动、“净网 2018”“净网 2019”“净网 2020”专项行动中，持续重拳打击整治侵犯公民个人信息违法犯罪活动，侦破侵犯公民个人信息案件 1.7 万余起，抓获各行业内部人员 3000 余名，发现并通报一大批涉及金融、教育、电信、交通、物流等重点行业信息系统及安全监管漏洞，打掉了一批非法采集、贩卖公民个人信息的公司。

公安部提供的数据显示，在“净网 2019”专项行动中，全年共侦破网络犯罪案件 5.9 万余起，抓获犯罪嫌疑人 8.8 万余名，行政处罚互联网站及联网单位 7.8 万余家次。其中，破获侵犯公民个人信息类案件 5000 余起，抓获各行业“内鬼”900 余名；破获网络赌博类案件 8300 余起；破获网络淫秽色情类案件 3300 余起；破获“助考”类案件 380 余起；破获网约绑架、抢劫等严重暴力刑事案件 290 余起，抓获犯罪嫌疑人 600 余名。

据了解，今年新冠肺炎疫情发生以来，公安机关坚决打击网上借疫情制造传播虚假信息、网上借机诈骗、网上制售假冒伪劣防护用品等违法犯罪行为，全力保障涉疫情防控工作关键信息基础设施和重要信息系统安全。

——严打借疫情危害公共秩序的涉网违法犯罪。疫情期间，网安部门依法严厉打击网上侵害公民个人信息犯罪活动，治安处罚 1500 余人；发现并推送违法犯罪线索，截至目前，配合有关部门抓获利用疫情实施网络诈骗嫌疑人 6300 余人，相关案件涉案金额累计人民币 6 亿余元人民币。

——切实筑牢涉疫情防控重要信息系统网络安全屏障。针对在线教育学习系统开展风险排查，限期整改责任单位 500 余家。

“净网 2020”是公安部为了打击整治网络违法犯罪活动，深入整顿网上秩序，进一步营造安全、清朗、有序的网络环境而开展的专项行动。

“净网 2020”专项行动中，认真贯彻落实了习近平总书记

重要批示指示精神，进一步强化对网络违法犯罪打击和网络空间秩序整治力度，坚决打掉网络黑灰产业链，整治网络违法犯罪生态，遏制了网络犯罪高发势头。

开展“净网 2020”专项行动，严厉打击淫秽色情信息，坚决清除文化垃圾，目标是着力维护青少年身心健康，切实维护人民群众文化权益，有力构建良好网络秩序、清朗网络空间。

警方将严打黑客攻击破坏、侵犯公民个人信息、电信网络诈骗、套路贷等新型网上违法犯罪，以及网上贩枪、涉毒、色情、赌博、传销等传统违法犯罪。同时，依法打击为各类网络犯罪提供推广营销、技术支持、网络账号买卖、支付结算等非法利用信息网络、帮助信息网络犯罪活动的行为。

以下是 2019 年以来公安机关侦破的十起侵犯公民个人信息违法犯罪典型案件：

1、江苏南通公安机关侦破“1023”暗网侵犯公民个人信息案

2019 年 10 月，江苏南通市公安局网安部门工作发现，网民“wolinxuwei”多次在“暗网”交易平台出售银行开户、手机注册等公民个人信息，数量高达 500 余万条。

经侦查，公安机关查明，“wolinxuwei”真实身份为林某。2019 年初，林某在“telegram”群组结识某公司安全工程师贺某，林某以 40 万的价格从贺某处购得银行开户、手机卡注册等各类公民信息 350 余万条，并通过“暗网”销售给经营期货交易平台、推销 POS 机的费某、王某等人，非法牟利 70 余万元。

11 月 12 日至 26 日，南通公安机关先后在上海、苏州、武汉等地抓获犯罪嫌疑人林某、费某、王某、贺某等犯罪嫌疑人 11 名，查获公民个人信息 2000 余万条。

2、江苏南京公安机关侦破“4.2”暗网侵犯公民个人信息案

2019 年 4 月，江苏南京公安机关接到南京市某单位信息中心报案，称该中心管理的南京市 1400 余万条居民社保数据被非法盗取，并在暗网中文网站“暗网交易平台”内被售卖。

南京市公安局网安部门综合运用技术手段，迅速查明盗取并在“暗网”上兜售社保数据的犯罪嫌疑人熊某及其上下线犯罪嫌疑人任某、薛某。经查，任某为江苏某计算机技术有限公司工程师，在为南京市某单位进行信息系统漏洞测试时，利用系统漏洞盗取了居民社保数据，后伙同在柬埔寨违法犯罪人员熊某在“暗网”上销售。其中，熊某将 7 万条数据卖给了薛某。

5 月 16 日，南京公安机关在柬埔寨警方配合下，于柬埔寨巴域市抓获犯罪嫌疑人熊某，后在境内抓获犯罪嫌疑人任某、薛某。

3、湖北武汉公安机关侦破吴某“暗网”侵犯公民个人信息案

2018 年 11 月，湖北武汉公安机关接到报案，某汽车金融服务平台服务器被黑客入侵，包括身份证、手机号、家庭住址、贷款情况在内的 30 余万条客户信息被盗取，被人以 1 比特币（时值 3.5 万元人民币）的价格在“暗网”上出售。

武汉市公安局网安部门经过深入侦查，于 2019 年 1 月 22 日在四川成都抓获犯罪嫌疑人吴某。

经审查，吴某交代其曾在成都市某软件技术专修学院学习，毕业后从事互联网技术工作。2018 年，吴某利用暴力破解手段非法获取涉案网站后台管理权限，盗取大量公民个人信息在“暗网”叫卖。

4、北京公安机关侦破高某“暗网”侵犯公民个人信息案

2019 年 6 月，北京市公安局网安部门工作发现，网民“yuhong”在“暗网”贩卖国内某银行 6.02 万条用户个人信息。

北京市公安局网安部门缜密侦查，锁定犯罪嫌疑人高某。7 月 24 日，北京公安机关将

高某抓获归案。

经审查，高某交代其利用网站漏洞非法窃取了某银行等单位网站上存储的公民个人信息，截至被抓获，非法牟利 3 万余元。

5、江苏徐州公安机关侦破“12.21”侵犯公民个人信息案

2018 年 12 月，江苏徐州市公安局网安部门工作发现，一网民在网上购买他人名下手机号码等公民个人信息。

徐州网安部门以此入手，挖掘出一个以电信运营商、银行内部员工为源头的买卖公民个人手机信息、征信信息等信息的犯罪网络，犯罪嫌疑人分布于多省。

2019 年 1 月 2 日，徐州公安机关组织 60 余名民警组成 23 个抓捕组，分赴 20 余个省市开展集中收网行动，先后抓获嫌疑人 45 名，其中电信运营商、银行等部门内部人员 20 余名，查获公民征信报告、手机注册、快递信息等各类公民个人信息 43 万余条，冻结涉案资金 120 余万元。

6、河南开封公安机关侦破赵某等人侵犯公民个人信息案

2018 年 12 月，河南开封市公安局网安部门工作发现，网民“夕阳红”通过微信群大肆贩卖手机机主姓名、财产信息、个人户籍资料等公民个人信息。

公安机关侦查掌握了一个由移动、联通、电信、社区、保险、快递、计生等部门“内鬼”与外部人员勾结，层层倒卖公民个人信息至下游电信诈骗、暴力催债、网络赌博等违法犯罪人员的侵犯公民个人信息犯罪网络。

开封公安机关历时 12 个月，辗转 20 多个省市，先后抓获犯罪嫌疑人 200 余名，其中，电信运营商、社区干部、物流行业等内部人员 80 余名、暴力催收人员 50 余名，打掉非法暴力催收公司 2 个，查获住宿信息、计生信息、人员轨迹、快递信息、银行财产信息等公民个人信息 1 亿余条，冻结涉案资金 1000 余万元。

7、山东济南公安机关侦破徐某等人公民个人信息被侵犯案

2019 年 3 月，山东济南公安机关接山东某高校学生徐某等人举报，其与同学个人身份信息被他人非法收集用于注册实名手机卡出售。

济南市公安局网安部门立即开展侦查工作。经查，济南某区联通公司某高校网点负责人葛某与其他高校网点业务员勾结，利用工作便利非法收集学生身份信息，开设实名手机卡后，向下游网络账号注册商、手机卡倒卖商刘某等人销售。刘某等人在销售手机卡的同时，使用“猫池”设备利用贾某、徐某等人提供的注册工具，通过接码平台大量注册、解封网络账号出售牟利。

济南公安机关历时 6 个月，先后抓获庄某、刘某、贾某、徐某在内的犯罪嫌疑人 22 名，扣押“猫池”设备 163 台、手机卡 5 万余张，查获上述人员非法注册 QQ 号 150 余万个、新浪微博号 200 余万个、“12306”账号 100 余万个。

8、江苏连云港公安机关侦破梅某等人侵犯公民个人信息案

2019 年初，江苏连云港公安机关侦破一起搭建虚假炒股平台实施诈骗案。

连云港市公安局网安部门随后顺线追踪，发现一条以证券公司内部人员范某等人为源头，层层倒卖股民信息至境内外网络炒股诈骗团伙的跨境侵犯公民个人信息犯罪链条，下游诈骗分子使用股民信息实施诈骗，涉案金额高达 2220 余万元。

连云港公安机关据此先后抓获犯罪嫌疑人 53 名，包括某证券公司内部员工 2 名，查获股民信息 300 余万条。

9、贵州安顺公安机关查处杨某侵犯涉疫情公民个人信息违法案件

2020 年 1 月，贵州安顺市公安局网安部门工作发现，一新浪网民在网上举报有人在微信朋友圈内大肆传播疫情防控重点人员信息。

安顺网安部门立即开展网上侦查，查明该批涉疫情公民个人信息传播源头为安顺市天

柱县某街道社区工作人员杨某，杨某在工作中获取了社区疫情防控人员信息后向好友发送，造成相关信息在微信中迅速扩散，造成恶劣影响。

安顺公安机关依法对杨某行政拘留 15 日、罚款 5000 元。

10、贵州黔东南州公安机关查处王某侵犯涉疫情公民个人信息违法案件

2020 年 1 月 25 日，贵州黔东南州公安局网安部门工作发现，一份名为“新型冠状病毒感染肺炎防控重点人员台账”在互联网上大肆传播。

黔东南州网安部门立即开展网上侦查，查明该台账由黔东南州凯里市某幼儿园员工王某在工作中获取，发布于小区微信群中，随后被层层转发，造成恶劣影响。

黔东南州公安机关依法对王某行政拘留 12 日、罚款 5000 元。

4.数据合规背景下，企业建设个人信息保护制度需明确这 8 点

来源： WeLegal 公司法务联盟

随着我国数据合规领域立法逐渐完善，出台的多部法律均对企业提出了明确的数据合规领域制度设立要求。例如，《个人信息保护法》（以下简称“个保法”）第五十一条规定个人信息处理者应当制定内部管理制度和操作规程；又如，《数据安全法》（以下简称“数安法”）第二十七条规定企业应当建立全流程数据安全管理制度；再如，《网络安全法》（以下简称“网安法”）第四十条要求企业建立用户信息具体企业组织架构的设立要求。

那么，困扰企业的问题是应该如何设立系列数据合规制度以及制度应当囊括哪些内容？本文结合我国目前一线企业的实践经验，以个人信息保护制度为例，提出该制度应当囊括的几个方面以便各位同行进行参考与讨论。

一、明确个人信息保护制度政策在公司的适用范围

建议在个人信息保护制度开篇就明确所适用的范围，尤其对集团公司、跨国公司而言则尤为重要。一方面，不同的国家对数据合规的要求不尽相同，若不作区分地制定一份制度简单粗暴的全部适用于所有集团公司、跨国公司的业务场景，容易使得该制度被迫成为一纸空文被束之高阁；另一方面，对于子公司、分公司等如果可适用同一制度的，可通过适用范围明确，进而精简公司整体冗余制度。

二、个人信息处理原则应兼顾其他数据保护法基本原则

对于企业数据合规而言其重点之一就是个人信息的处理合规。个保法第一章总则篇中，明确规定了个人信息处理的基本原则。如个保法第五条所规定的合法、正当、必要和诚信原则，以及第七条所规定的处理个人信息过程中的公开、透明原则等。因此，我们建议在公司制度政策中设立与个保法及其他数据保护法律相一致的原则性规定，以弥补制度所规定的具体情形不足时，能够从原则层面适用制度，以达到数据合规的要求。

三、明确业务场景及数据生命全流程保护

我们认为对于个人信息保护制度中，对于对企业数据流转的业务场景及数据生命全流程的相关规定应当是最重要的篇幅。因此，从业务场景和数据生命全流程两个角度综合考量尤为重要。

3.1 综合行业视角和企业视角考量业务场景合规要求

对于制度细化规定的条款中，第一视角应当审视公司业务场景。我们建议从行业视角和自身

视角两个角度出发综合考量业务场景的合规要求。一方面，核查企业自身是否属于特殊行业如金融、医疗等对数据合规有专章规定的；另一方面，核查企业自身业务场景涉及到数据的环节。针对企业自身业务场景，我们建议从企业-消费者、企业-企业、企业-雇员端三个维度出发分别针对个保法、数安法、网安法及其它数据合规领域法律法规的内容进行回应，设立专门的制度，从而规制公司经营行为以达到合规要求。

3.2 数据生命全流程审视合规要求

对于制度细化规定的条款中，我们认为第二视角应当审视公司所涉及的数据生命全流程。针对数据全流程而言，我们建议分别从数据采集前的通知义务、数据主体本身的选择（如同意、撤销以及删除）、数据收集、使用、存储、向第三方披露、个人数据跨境转移等几个方面分别进行专门规定。同时，可以对部分场景下作出个别示例性的规定，以使企业内部员工更好地理解制度的条款。

四、明确组织架构与部门职能

作为公司内部制度，我们建议企业在起草制度时，针对整体组织架构和部门职能进行明确规定。以现有的成熟企业为例，组织架构通常已经明确包含如法务部、人力资源部、业务部、总经办等多部门。随着企业数据合规领域的要求提升，目前越来越多的企业将数据合规官这一职位调整至企业组织架构中。我们建议企业根据自身运营和原有流程设计，融入数据合规官或数据合规领域职能人员的架构。

同时，在制度中确定各部门的组织职能。以法务部为例，企业可在制度中要求法务部跟踪并分析全球的数据合规领域法律法规规定，要求法务部门自身开展或在第三方中介机构协助下开展 PIA 专项评估等。再如人力资源部门，可赋能并要求人力资源部负责雇员端视角下数据合规领域治理，在劳动合同签订过程、员工管理过程中所获得、处理的个人信息、敏感信息等数据内容合规化治理。

需要提示的是，各省市对数据合规领域架构的治理要求或有不同。近日，杨浦区检察院联合市信息服务业行业协会、市数据合规与安全产业发展专家工作组、区工商业联合会，制定发布上海市首份《企业数据合规指引》，其中第七条针对数据合规的管理部门之规定，鼓励各类企业设置专门的数据合规管理部门，不建议由法务部门履行合规管理职能。指引中提出，企业应当向数据合规管理部门负责人提供足够的授权和人力，一般由董事会直接设立企业合规部门，下设数据合规管理部门等各类专业合规部门。从指引中也可以看出，针对大型跨国企业、集团企业，设立专门的合规部门，在合规部门下设各专业合规管理部或许是未来发展的监管要求趋势。

五、明确数据事件响应机制

根据个保法第五十一条的规定，个人信息处理者应当制定并组织实施个人信息安全事件应急预案。据此，在企业制度中明确数据事件响应机制成为应有之义。对于响应机制，我们建议至少应当包括调查、报告、补救措施三个环节，明确事件发生后的归属的安全等级与报告的直接责任主体及报告对象。同时，对于重大安全事件应当同时确定对内报告和对外报告的双重机制。

六、明确问责机制
我们建议问责机制应当包含企业内部因员工过错、管理过失、程序漏洞等产生的数据安全危机事件。此外，还应当包含当供应商、合作伙伴之过错导致数据安全危机事件发生的，案涉企业是否进入本企业合作灰名单、以及追索赔偿机制等。

七、明确法律冲突、解释、维护等规则
为避免公司制度制定过程中存在与现行法律或业务运营所在地的法律规定存在冲突性规定，我们建议在制度中作出所在国法律法规优先制度适用的规定以保持制度的稳定性。示例："当本制度与所在国法律法规发生冲突时，以当地法律法规之规定为准。"一方面，公司企业制度的建立受制于制定政策人员的专业知识水平及对业务场景的预设，因而有可能存在不足之处；另一方面，法律法规的更新和企业制度的迭代存在的时间差也可能导致制度不符合法律法规的规定的情况出现。

八、明确定义及解释
我们建议在制度的最后对制度全文所涉及到的专有名词作出与法律法规一致或业务场景一致的定义及解释。简化制度整体的冗余度，同时确保制度体系的完整性。
数据合规治理的时代已经到来，数据合规领域的立法、执法活动密切开展的当下，企业内部更应该及早建立相应制度树立合规治理的第一道屏障。个人信息的处理与保护作为数据合规中重要的一环，我们建议可以从上述八个部分出发，制定公司内部的管理制度以对现有法律法规中的要求进行回应，提升企业合规治理水平。

5.检察机关积极维护个人信息安全 2021 年办理个人信息保护领域公益诉讼案件 2000 余件

2021 年 8 月通过的个人信息保护法，专设公益诉讼条款，明确将个人信息保护纳入检察公益诉讼法定领域。检察机关全面贯彻习近平法治思想，聚焦网络时代公民个人信息保护更高需求，依法履行公益诉讼检察职能，坚决维护个人信息安全。2021 年，共办理个人信息保护领域公益诉讼案件 2000 余件，同比上升近 3 倍。办案发现，当前个人信息保护面临四方面突出问题，须加强综合治理。
一是利用手机 APP 等违规收集个人信息问题突出。2021 年，检察机关共办理网络侵害个人信息公益诉讼案件 800 余件，同比上升约 1.7 倍。办案发现，一些手机 APP 存在强制授权、过度索权、超范围收集个人信息等情况。如，某市检察机关履职中发现，有 13 款手机 APP 不同程度存在违法违规收集使用个人信息问题，包括未公开信息收集使用规则，未明示收集使用个人信息的目的、方式和范围，违反必要原则收集与其提供的服务无关的个人信息，未经用户同意收集使用个人信息等。检察机关通过调查核实固定证据，与行政机关进行磋商并制发检察建议，督促行政机关依法履职，推动涉案企业自查整改，依法保护公民个人信息安全。
二是特定群体个人信息需要加大保护力度。检察机关办案发现，未成年人、老年人等群体防范意识薄弱，更易成为个人信息侵害的对象。如，一公司 APP 在运营过程中，未有效落实国家互联网信息办公室《儿童个人信息网络保护规定》，没有以显著、清晰的方式告知并征得儿童监护人有效明示同意，便允许注册儿童账号，并擅自收集、存储儿童网络账号、位置、联系方式，以及儿童面部识别特征、声音识别特征等个人敏感信息。同时，运用后台算法向

具有浏览儿童内容视频喜好的用户直接推送含有儿童个人信息的短视频，没有对儿童账号采取区分管理措施，也没有采取技术手段对儿童信息进行专门保护。检察机关向法院提起民事公益诉讼，请求判令该公司立即停止实施利用公司 APP 侵害儿童个人信息的侵权行为，赔礼道歉、消除影响，赔偿损失并将款项交至相关儿童保护公益组织，专门用于儿童个人信息保护公益事项。经法院调解，该公司接受了检察机关的全部诉讼请求，针对存在问题全面开展整改。

三是个人信息泄露导致骚扰电话和电信网络诈骗风险。泄露的个人信息经网络黑灰产业链交易传输，有的引发骚扰电话、垃圾短信，有的被用于实施电信网络诈骗等犯罪，严重危害人民群众人身财产安全。如，张某多次从某保险公司员工曹某处购买投保客户信息，信息内容包括客户姓名、身份证号、地址、联系方式、保单号、投保日期、金额等。张某利用购买的客户信息，伙同他人冒充原投保公司售后人员实施诈骗，诈骗金额达 510 余万元。检察机关以张某涉嫌侵犯公民个人信息罪、合同诈骗罪，曹某涉嫌侵犯公民个人信息罪向法院提起公诉，同时提起附带民事公益诉讼。张某被判处有期徒刑十二年，并处罚金；曹某被判处有期徒刑九个月十五日，并处罚金；法院同时判决张某、曹某在新闻媒体上公开赔礼道歉，曹某就其侵犯公民个人信息的获利赔偿 1 万元。

四是个人信息保护监管合力不足。个人信息保护涉及对象多、领域广，多个部门职责交叉或者职权定位不够明晰，亟需形成监管合力。如，某省级检察院办理的 APP 违法违规收集使用个人信息行政公益诉讼案中，相关行政机关反映，由于监管职权交叉、技术保障滞后等原因，导致监管缺乏系统性、有效性。检察机关组织相关单位召开案件磋商会，联合会签意见，通过联合调查、挂牌督办、专项整治等方式，联合惩戒违法违规主体，协同治理 APP 违法违规收集使用个人信息问题，取得良好成效。

下一步，检察机关将继续加大公益诉讼办案力度，推动个人信息保护法落地落实。一是突出保护重点。聚焦重点人员、重点领域，为个人信息安全保驾护航。严格保护生物识别、宗教信仰、特殊身份、医疗健康、金融账号、行踪轨迹等敏感个人信息；特别保护儿童、妇女、残疾人、老年人、军人等特定群体的个人信息；重点保护教育、医疗、就业、养老、消费等领域处理的个人信息，以及涉及 100 万人以上的大规模个人信息；精准保护因时间、空间等联结形成的特定对象的个人信息。二是强化检察机关内部衔接配合。充分发挥检察一体化办案优势，上级检察机关加大自办案件力度和对下指导力度，采取交办、提办、督办、领办等方式，积极应对个人信息公益损害网络化。畅通检察机关内部线索审查移送机制，注重在涉及个人信息保护的刑事、民事、行政检察案件中同步发现公益诉讼案件线索，加强全流程、全链条保护，实现惩治违法和保护公益的多重效果。三是形成个人信息保护监管合力。加强与网信、工信、公安、市场监管、教育等职能部门在线索移送、信息共享、专业咨询、办案辅助等方面的协作配合，健全行政执法与公益诉讼检察衔接机制，积极稳妥办理涉及网络黑灰产、数据安全的重大网络侵害类公益诉讼案件。加强与法院的沟通协调，深化个人信息保护公益诉讼制度探索。通过提出检察建议等方式，督促相关单位或部门采取有效防范措施，从源头上强化信息安全，筑牢个人信息保护“防火墙”。

6.利用爬虫技术窃取 2.1 亿条简历数据 某科技公司被判罚 4000 万元

来源：海淀检察院 作者：北京政法网

近日，海淀区检察院起诉某科技（北京）有限公司（以下简称某科技公司）王某某等人涉嫌侵犯公民个人信息罪一案，经北京市第一中级人民法院裁定维持原判，案件一审判决生效。被告单位某科技公司被判处罚金人民币四千万元，被告人王某某被判处有期徒刑七年，罚金人民币一千万元，其他被告人均被判处相应刑罚。据了解，本案对被告单位判处的罚金数额、对被告人判处的刑期和罚金数额，均系近年来全国同类案件判罚最重案例。

案情回顾：

某科技公司成立于 2014 年，主要经营招聘工具软件和大数据分析等业务。2015 年至 2019 年期间，该公司组建专门爬虫技术团队，在未取得求职者和平台直接授权的情况下，秘密爬取国内主流招聘平台上的求职者简历数据。

本案具有涉案人员多、涉案电子存储设备多、涉案数据量特别巨大、被告人作案手段呈现高技术化等特征。针对上述问题，海淀区检察院科技犯罪检察团队适时提前介入案件，并密切配合公安机关取证工作。案件审查过程中，针对海量涉案公民简历数据，检察官提出具体指导意见，从涉案数据中发现具有爬虫特征的 2.1 亿余条个人信息。

经查，某科技公司获取上述数据后，对数据进行重整，并用于开发产品意图谋利。期间，某科技公司爬虫技术团队负责人欧某某，私自将公司窃取的简历数据对外出售，个人非法获利人民币 30 余万元。

检察官提示：

《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》，体现出我国对加强数据和个人信息保护的立法态度，司法机关也会更加严厉打击侵害公民个人信息、侵害数据权属的各类不法行为。建议相关行业主体更加重视数据安全和个人信息保护，不仅不能越权获取个人信息和关键数据，更要注重数据和个人信息保护工作。

（十六）网络犯罪黑灰产业链的刑事规制

1.网络犯罪黑灰产业链的样态与规制

作者：喻海松 最高人民法院研究室刑事处

来源：《国家检察官学院学报》

摘　要：

网络犯罪分工日益细化，形成了“流水线”式作业分工，滋生出与之相关联的黑灰产业链。黑灰产业为网络犯罪“输血供粮”，危害严重，对其如何加以有效规制，已经成为我国刑法理论和司法实务必须面对的问题。立足当下，对网络犯罪黑灰产业链的刑事规制应立基于积极解释的立场，用足用好刑事立法现有规定，以帮助信息网络犯罪活动罪作为堵截性罪名，并注重实现刑事规制的罪刑均衡。着眼长远，针对当前刑事规制的困境，应当注重分析相应黑灰产滋生的原因，完善相关前置法律，综合施策、标本兼治，真正实现对网络犯罪黑灰产业链的有效规制。

关键词：黑灰产业链；堵截性罪名；手机黑卡；网络账号；网络流量；资金通道；

随着互联网的不断普及和信息技术的飞速发展，网络犯罪日益分工细化，黑灰产业链迅速滋生蔓延。黑灰产为网络犯罪“输血供粮”，严重危害网络安全和秩序，侵犯人民群众合法权益，亟须有效规制。对此，应当对网络犯罪黑灰产业链的产业逻辑、业内生态进行专门研究，并相应调整刑事规制和司法适用的基本立场，有针对性地对网络黑灰产业链进行类型化分析和刑事规制困境检视，继而形成相应的刑事规制完善之策，综合施策、标本兼治，真正实现对网络犯罪黑灰产业链的有效规制。

一、网络犯罪黑灰产业链与刑事规制立场

（一）网络犯罪的分工细化与黑灰产业链

当下，网络犯罪呈现出高发频发态势。与传统犯罪、甚至早期黑客犯罪（危害计算机信息系统安全犯罪）的“单打独斗”完全不同，当前网络犯罪通常表现为“协同作案”。从网络犯罪案件的审判情况来看，平均每件网络犯罪案件涉及 2.73 名被告；超四成网络犯罪案件为两人及以上团伙犯罪，三人及以上共同犯罪的案件占比逐年提高。[1]值得进一步关注的是，网络犯罪不仅表现为共同犯罪凸显和共犯人数众多，更为重要的是犯罪活动分工细化，逐步形成“流水线”式作业。在此背景下，各类网络犯罪盘根错节，滋生进化出复杂的网络犯罪生态体系，形成了分工合作、彼此依赖、利益共享的黑灰产业链。

网络犯罪黑灰产并非严谨的法律术语，而是基于实践状况的形象概述。一般认为，黑产通常是指触犯法律的网络违法犯罪行为。例如，为下游网络犯罪窃取、提供账号密码和研制钓鱼网站、仿冒网站等黑产行为，显属违法、甚至犯罪行为。与黑产有所不同，灰产则游走在法律边缘，通常距离直接实施的网络犯罪较远，甚至只是为黑产提供辅助，对其定性需要视具体情况而定、甚至存在一定争议。例如，恶意注册账号、身份认证等灰产行为，本身并未明显违反规定，相关行为又并非只能用于违法犯罪，故对其定性难以一概而论。但是，黑产与灰产之间的界限并非泾渭分明，而是相互依附、交织，形成庞大的黑灰产业链。据有关数据，网络黑色产业与灰色产业交织在一起，产业规模保守估计过千亿元，社会危害性巨大。[2]

（二）网络犯罪的要素与黑灰产业链的样态

各类网络犯罪方式有异，所需要素也会相应不同。概而观之，网络犯罪的实施通常离不开推广、技术、物料（信息类物料和工具类物料）、支付等要素：[3](1）宣传推广成为网络犯罪行为人吸引受害人或者参与人的主要渠道，发挥着桥梁纽带的作用。例如，网络开设赌场需要通过宣传推广吸引参赌人员，电信网络诈骗需要通过宣传推广吸引被骗群众。（2）当前，行为人通过使用他人研发的各种程序、工具实施网络犯罪，大大降低了犯罪成本和技术门槛，导致网络犯罪迅速蔓延。（3）信息类物料主要为网络犯罪提供虚假身份，如提供公民身份证信息、银行卡信息等，成为其逃避实名制的重要“屏障”。工具类物料主要为网络犯罪提供猫池、卡池、手机群控设备或者其他工具，以通过自动化手段组合各种资源实施违法犯罪活动。（4）网络犯罪的主要目的在于非法牟利，资金支付结算和变现是关键。正是通过资金支付环节，网络犯罪行为人套取、漂白违法所得，逃避国家资金监管，最终实现犯罪目的。

由此可见，在宣传推广、信息类物料供应、工具类物料供应、技术支撑、资金结算等五个关键阶段滋生出大量的黑灰产，形成了复杂的网络犯罪生态体系。具体而言：(1）在宣传推广环节，主要包括搜索引擎排名、微信公众号广告、短信群发等推广引流活动；（2）在信息类物料供应环节，主要包括提供银行卡四件套[4]、企业八件套[5]、精准公民个人信息以及计算机信息系统数据等；（3）在工具类物料供应环节，主要包括提供猫池、卡池、手机群控设备等；（4）在技术支持环节，主要包括非法 APP 制作研发、网站开发维护、虚拟定位、服务器租赁、网站域名技术服务、伪客户端工具平台等；（5）在资金结算环节，主要包括支付渠道、跑分平台、卡商平台、电商平台、话费充值、地下钱庄等。需要注意的是，上述黑灰产的关键环节和节点，不仅与网络犯罪相连，而且彼此相互交织，最终形成产业链。

（三）刑事对策的调整与刑法适用的立场

1. 新近刑法修正案对网络犯罪黑灰产业链的规制

日益壮大的黑灰产业链是网络犯罪迅速蔓延的关键，故一段时期以来对网络犯罪的应对主要就是黑灰产业链的规制。针对网络犯罪黑灰产业链不断滋生蔓延的现状，我国及时调整刑事对策，涉及到适度扩张犯罪圈、前移刑事防线和惩治产业链等多个方面。特别是，新近刑法修正案中不少关于网络犯罪的修正，实际直指黑灰产。具体而言：

一是针对突出的黑灰产形态增设专门罪名。通过总结常见的网络犯罪黑灰产运行实际状况，刑法修正案将一些常见的黑灰产样态直接纳入刑事规制范围，设置专门罪名。例如，非法获取、提供公民个人信息是信息类黑灰产的主要样态，《刑法修正案（七）》、《刑法修正案（九）》先后通过增设和完善《刑法》第 253 条之一，设置侵犯公民个人信息犯罪专门法条的方式将其直接纳入刑事规制范围。又如，针对为黑客攻击破坏活动提供程序、工具的技术支持类黑灰产日益蔓延，且按照共犯处理证明困难的现实情况，《刑法修正案（七）》增设《刑法》第 285 条第 3 款，规定了专门的提供侵入、非法控制计算机信息系统程序、工具罪，将本属共同犯罪帮助犯的行为独立入罪评价。[6]

二是增设非法利用信息网络罪。从实践来看，不少黑灰产涉及到设立网站、通讯群组、发布信息等形式。例如，宣传推广环节的黑灰产，常见形式就是发布违法犯罪信息。又如，技术支撑环节的黑灰产，不少表现为设立用于实施违法犯罪活动的网站、通讯群组。根据“打早打小”的策略要求，《刑法修正案（九）》增设《刑法》第 287 条之一，适度前移刑法防线，将为实施违法犯罪活动而设立网站、通讯群组、发布信息的行为独立入罪。

三是增设帮助信息网络犯罪活动罪。《刑法修正案（九）》增设《刑法》第 287 条之二，针对无法构成共同犯罪，或者按照共同犯罪处罚较轻的情况，将明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的行为规定为帮助信息网络犯罪活动罪，实现了网络犯罪利益链条中的帮助行为独立入罪。显而易见，该法条在罪状描述上就直接涉及技术支持、宣传推广、资金结算等多类黑灰产。

2. 网络犯罪黑灰产业链的刑法适用立场

刑法是网络犯罪治理的重要手段，如何实现对网络犯罪黑灰产业链的有效刑事规制，是当前网络治理中的一项重要课题。就网络犯罪黑灰产业链的刑法适用而言，本文主张积极刑法观，从宏观层面而言，针对网络犯罪产业链条发展、进而形成生态的现状，要坚持全生态全链条的惩治对策；从微观层面而言，要用足用好刑法现有规定，根据网络犯罪黑灰产的特点，准确适用相关罪名，不断压制萎缩网络犯罪的生存空间。以此立场为基点，下文将选取网络犯罪黑灰产业链中手机黑卡产业链、网络账号产业链、网络流量产业链、资金通道产业链所涉问题进行探讨。在具体探讨前，有必要进一步提及如下三个基本观点：

其一，黑灰产不是犯罪绝缘体，全链条考察才是关键所在。当前，网络黑灰产实际上已经与直接实施的网络犯罪交织在一起，难以完全界分开来。例如，为电信网络诈骗、

网络赌博等违法犯罪活动提供公民个人信息或者资金支付结算等直接帮助，甚至在上游进行宣传推广、提供工具等间接帮助的，实际上已经成为整个犯罪链条的有机组成部分。基于此，本文主张将黑灰产置于整个犯罪链条之中进行分析，以准确判断行为性质，更好地适用刑法相关规定。网络犯罪黑灰产业链中的某段行为，孤立来看，可能难以查明其危害性，导致对其行为的性质难以判断，从而出现了所谓处于法律灰色地带的“灰产”。例如，所谓的恶意注册账号、虚假认证，就其行为本身难以判断性质，但如果结合后续的流向、特别是对后续电信网络诈骗等网络犯罪的影响而言，则难以否认其社会危害。一言以蔽之，黑产与灰产既非法律术语，也无难以逾越的界限，从刑法适用的角度而言，立足点应当是刑法规定，对于符合刑法犯罪构成要件的行为，无论是黑产行为还是灰产行为，都可以依法追究刑事责任。

其二，其他罪名优先适用，帮助信息网络犯罪活动罪堵截。[7] 对于网络犯罪黑灰产业链的刑事规制，在其他罪名难以适用的前提下，可以充分考虑帮助信息网络犯罪活动罪的适用。一方面，这符合《刑法》第 287 条之二第 3 款规定的立法精神，[8] 即优先适用其他罪名。另一方面，这符合帮助信息网络犯罪活动罪作为网络犯的“堵截性罪名”的属性。[9] 申言之，对于严重危害网络秩序，具有严重社会危害性的网络犯罪黑灰产行为，如果不符合其他犯罪构成的，要秉持积极解释的立场，在坚持罪刑法定原则的前提下将其纳入帮助信息网络犯罪活动罪的适用范围，以尽力堵塞刑法规制漏洞。对此，本文在“二、手机黑卡产业链的检视”部分对帮助信息网络犯罪活动罪的司法适用有详细论述。

其三，刑罚并非越重越好，罪刑均衡最为重要。网络犯罪黑灰产业链的滋生，原因较为复杂，既有刑事规制不力的原因，更有前置法律不健全和管理不到位的原因。因此，运用刑法惩治网络犯罪黑灰产切不可“一打了之”“一味从重”。特别是，我国现行刑法关于网络犯罪的部分罪名设置距今较为久远，相关司法解释的制定系在黑灰产泛滥之前，对相关定罪量刑标准的设置可能未考虑到适用于黑灰产的情况。个别情形下，可能出现罪名形式符合但刑罚过重的现象。例如后文所述的流量劫持案件，一律适用破坏计算机信息系统罪，形式上似都符合构成要件，但刑罚可能存在畸重的现象。在此背景下，宜考虑对破坏计算机信息系统罪的构成要件作适当限缩解释，对部分案件选择适用罪刑更加均衡的非法控制计算机信息系统罪。总之，对网络犯罪黑灰产业链的刑法适用，应当特别注重罪责刑相适应原则的把握，妥当选择罪名，准确裁量刑罚，在司法裁判中确保刑罚轻重与所犯罪行和承担的刑事责任相适应。

二、手机黑卡产业链的检视

买卖手机黑卡属于网络犯罪黑灰产中物料供应环节的重要组成部分，其与后续的恶意注册账号、养号等活动往往交织在一起，形成了手机黑卡产业链，为下游网络犯罪提供帮助。在手机黑卡产业链中，黑卡的作用是隐蔽身份，使得有关部门无法查证行为人的真实身份。

（一）手机黑卡的出现与流向

自 2013 年 9 月我国电话实名制登记实施以来，不仅新入网用户实现了实名登记，未实名老用户也进行了补登记。[10] 然而，由于各种原因，非实名手机卡仍在一定范围存在，不少变成“黑卡”。黑卡是指未进行实名登记或者无法查实使用人员并被用于

违法犯罪活动的移动电话卡（含无线上网卡）。实际上，使用他人身份进行实名登记的手机卡亦属黑卡范畴。

手机黑卡主要有物联网卡、海外卡以及使用他人身份注册的实名卡。具体而言：（1）物联网卡。物联网卡是指主要用于工业、交通、物流等领域的手机卡，无需实名认证，但需要以企业名义办理，提供营业执照即可办理。实践中存在利用虚假证件或者购买营业执照等方式办理物联网卡的现象。目前流通的手机黑卡中绝大部分是物联网卡。（2）海外卡。由于我国实行实名制，黑卡产业大量获取国内手机卡越来越难。在此背景下，近年来，大量来自东南亚国家的手机卡开始进入我国手机黑卡产业。这些卡支持 GSM 网络，进入国内后可以直接使用，无需实名认证。同时，这些手机卡基本是零月租、接收短信免费、成本低，在手机黑卡产业中的使用比例越来越高。（3）实名卡。此类实名卡规避实名注册，大致包括使用虚假身份注册、冒用他人身份注册以及收购他人实名注册的手机卡三种情形。

从实践来看，如图 1 所示，以手机黑卡为源头，形成了手机黑卡产业链，主要涉及如下几个环节：（1）卡源卡商，其掌握大量手机黑卡货源，加价转卖给卡商。（2）猫池产家，其负责生产猫池设备，11 并将设备出售给卡商使用。（3）卡商，其通过从卡源卡商购买大量手机黑卡，将黑卡插入猫池设备并接入卡商平台，然后通过卡商平台接各种验证码业务，以牟取利益。（4）接码平台，其负责连接卡商和羊毛党、号商等有手机验证码需求的群体。12(5）羊毛党、号商。羊毛党主要靠批量注册账号以获取企业特定活动时的奖励。13 号商则靠批量注册和维护账号，并通过出售账号获取收益。如后一部分“网络账号链”所述，部分账号可能继续流向下游的网络犯罪，成为犯罪工具。

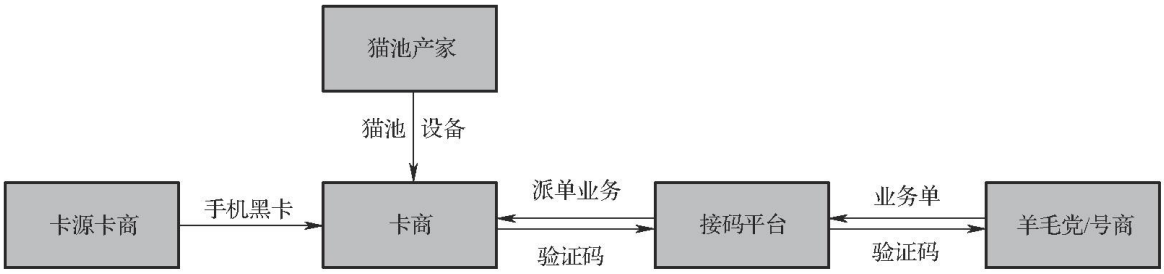


图 1 手机黑卡产业链　　下载原图

（二）买卖手机黑卡行为的定性

1. 侵犯公民个人信息罪的区分适用。

对于倒卖手机黑卡行为，司法实践中有观点主张适用侵犯公民个人信息罪。本文主张区分情况处理，对于未实名登记的黑卡，不宜适用本罪；但对于实名登记的黑卡，可以适用本罪。主要考虑如下：

其一，物联网卡和海外卡无法认定为侵犯公民个人信息罪的对象“公民个人信息”。具体而言：（1）公民个人信息的主体必须是自然人，而不包括单位。物联网卡属于单位开办的手机卡，不符合这一主体身份要求。（2）公民个人信息必须具有可识别性的特征，即“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”。但是，无论非实名卡，还是海外卡，由于未进行实名登记，在没有附加其他识别信息的情况下，似难以认为具有个人信息所要求的可识别性。

其二，批量倒卖实名登记手机卡的行为可以构成侵犯公民个人信息罪。具体而言：（1）与未实名登记的物联网卡、海外卡不同，实名手机卡符合公民个人信息的认定要求，可以成为侵犯公民个人信息罪的犯罪对象。（2）无论是收购行为，还是出售行为，手机卡实名登记人的自愿不能阻却行为的违法性。根据《刑法》第 253 条之一的规定，侵犯公民个人信息罪的前提条件是“违反国家有关规定”。司法实践中反对适用侵犯公民个人信息罪的观点认为，对于征得手机卡实名登记人的同意、甚至其主动出售手机卡的行为，不能认定为“违反国家有关规定”。[14]这一观点乍看似有道理，但细究起来是不能成立的：首先，从《民法典》关于个人信息的规定来看，最终未明确将个人信息规定为“个人信息权”，而是采用了“个人信息保护”的表述，并将自然人的个人信息权益归属于人格权益，实际上排除了自然人对其个人信息的排他权利。[15]其次，尽管《刑法》将侵犯公民个人信息罪置于“侵犯公民人身权利、民主权利罪”一章，但不能排除侵犯公民个人信息罪所保护的是双重法益，既包括其人身权益，还包括国家关于公民个人信息的管理秩序。最后，根据《网络安全法》《反恐怖主义法》等法律规定，电话卡是标识身份，依法用于身份核验的凭证。出售和收购实名手机卡的行为，无论实名登记人是否同意，均违反了有关法律规定，属于非法出售或者获取。[16](3）对于倒卖实名登记手机卡的行为适用侵犯公民个人信息罪，应当准确把握“情节严重”的入罪要件。根据宽严相济刑事政策的要求，对于相关行为的刑事追究应当限于主观恶性较大、客观危害严重的情形，重点惩治“卡头”（组织者）。[17]

2. 帮助信息网络犯罪活动罪的再解释。

对于明知他人利用信息网络实施犯罪，为其犯罪提供黑卡，情节严重的，可以视情适用帮助信息网络犯罪活动罪。具体而言：

其一，帮助信息网络犯罪活动罪纯正网络犯罪之否定。本文认为，帮助信息网络犯罪活动罪并非纯正的网络犯罪，其所涉客观方面可以由线下帮助行为构成。《刑法》第 287 条之二第 1 款将帮助信息网络犯罪活动罪的行为方式并列规定为“提供互联网接入、服务器托管、网络存储、通讯传输等技术支持”和“提供广告推广、支付结算等帮助”。这就使得对于线下的帮助行为解释为“等帮助”之中，从体系解释的角度完全没有问题。据此，可以将为网络犯罪提供手机黑卡的行为纳入“等帮助”的范畴。

其二，帮助信息网络犯罪活动罪主观明知之把握。根据《刑法》第 287 条之二第 1 款的规定，本罪的主观方面表现为“明知他人利用信息网络实施犯罪”，《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》（法释[2019]15 号，以下简称《新型网络犯罪解释》）第 11 条对主观明知的认定确立了推定规则。其中，第四项规定为“提供专门用于违法犯罪的程序、工具或者其他技术支持、帮助的”。这主要是针对“并非社会正常活动所需，而系为违法犯罪活动提供帮助的专门服务”的活动，允许对相关从业人员推定主观明知。[18]需要注意的，该项规定限定相关帮助行为系专门用于“违法犯罪”，而此处的“违法”并未明确要求限定为刑法分则规定的构成要件行为，而是应当理解为包括其他违法行为在内。据此，手机黑卡产业链中的相关行为，如果违反有关规定，且排除系正常社会所需要的活动，可以视情推定“明知”。例如，根据相关规定，“物联网行业卡不得开通点对点短信业务”，可以认为正常物联网业务活动不需要开通点

对点短信业务。故而，如果相关物联网卡违规开通点对点短信业务，且相关业务流向下游犯罪的，可以推定主观明知。

其三，帮助信息网络犯罪活动罪帮助对象之把握。根据《刑法》第 287 条之二第 1 款的规定，本罪的帮助对象为“犯罪”。根据《新型网络犯罪解释》第 12 条的规定，帮助对象“犯罪”原则上要求查实；同时，在查证帮助对象“犯罪”困难的情况下，要求查实系刑法分则规定的构成要件行为，是否达到犯罪的程度在所不论。从帮助信息网络犯罪活动罪的办案实践来看，前者是应然状况，实践中难以适用。故而，帮助信息网络犯罪活动罪主要适用的场景是帮助刑法分则规定的构成要件行为的情况。但即便如此，要求一一查明被帮助对象实施的每一笔刑法分则构成要件行为也存在相当困难。

帮助信息网络犯罪活动罪涉及的被帮助对象多系电信网络诈骗等涉众型网络犯罪。《最高人民法院、最高人民检察院、公安部关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》（公通字[2014]10 号）第 20 条对此类犯罪的查证确立了特殊规则，不要求逐一查证，而是允许综合认定。[19]据此，对于手机黑卡产业链的相关行为，最终用于下游网络犯罪的，在查实部分行为系刑法分则构成要件行为的基础上，应当允许对其他行为作综合认定。例如，通过黑卡注册大量金融账号，进而被用于电信网络诈骗，如果发现该账号共涉及多笔资金的，只要查实部分资金系电信网络诈骗所得，对于其他资金应当允许综合认定。

三、网络账号产业链的检视

网络账号是用户的“网络身份”。在以账号体系为基础的网络环境中，网络犯罪、乃至黑灰产的实施，均以大量获取账号资源为前提。在网络犯罪黑灰产业链中，这些网络账号为行为人隐蔽真实身份、逃避溯源追究，极大危害网络秩序安全。

（一）网络账号产业链的样态

当前网络犯罪持续高发多发，恶意注册产业成为滋生助长网络犯罪的核心利益链条之一。从实践来看，如图 2 所示，网络账号链条涉及上游、中游和下游三个环节：（1）上游非法获取网络账号，即通过批量注册、入侵拖库、钓鱼盗号、撞库、收购租用等方式非法获取网络账号；（2）中游养号，即通过系统模拟正常用户行为规避平台监管措施，或者通过人工添加好友等方式为下游犯罪物色目标人群，同时提升账号活跃度和价值；[20](3）下游违法犯罪，即网络账号最终被用于网络诈骗、网络招嫖等违法犯罪活动。

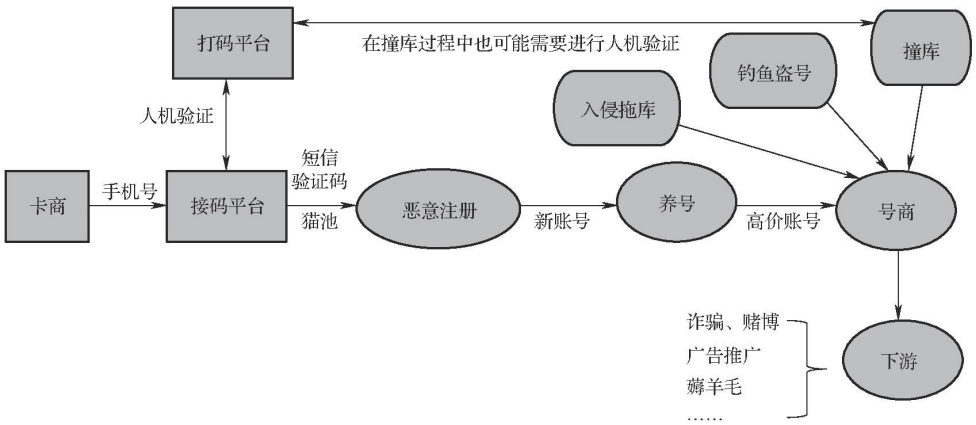


图 2 网络账号产业链　　下载原图

（二）网络账号产业链相关行为的定性

其一，非法获取计算机信息系统数据罪的适用。通过入侵、盗号、撞库等手段非法获取网络账号。具体涉及入侵拖库，即通过非法侵入并下载网络服务应用的数据库，从而获取网络账号信息；钓鱼盗号，即通过设立钓鱼网站，使用欺诈手段骗取用户的网络账号信息；撞库，包括两种情况：一是使用自动化批量处理工具，采用反复登录验证的方式，对批量获取的账号、密码信息（往往杂乱无章、无法匹配）与网络应用平台数据库中的数据信息进行关联比对，从而获取相互匹配的账号和密码，取得网络账号的控制权和使用权。二是将某一网络平台的账号秘密与其他网络平台的账号密码进行关联比对，从而获取不同网网络平台的网络账号信息。对于上述行为，特别是入侵、盗号行为，往往属于《刑法》第 285 条第 2 款规定的“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”，对于情节严重的行为可以适用非法获取计算机信息系统数据罪。

需要注意的是，实践中，对于利用网络工具绕过网络服务提供者的安全验证等风控措施，获取账号秘密等数据的行为，实践中有观点主张适用非法获取计算机信息系统数据罪。本文持否定立场。主要考虑：对于绕过网络服务提供者的账号验证、风控规则，获取验证数据的行为，确实违反了《网络安全法》等要求网络运营者对用户真实身份进行核验的法律规定。但是，非法获取计算机信息系统罪的客观方面必须表现为“侵入行为”或者“采用其他技术手段”。对于利用网络工具注册账号的行为，实际上并未侵入网络服务提供者的系统，也没用采用其他技术手段，似不符合非法获取计算机信息系统罪的客观要件。

其二，侵犯公民个人信息罪的适用。对于恶意注册账号环节涉及非法获取或者提供公民个人信息的行为，显然可以适用侵犯公民个人信息罪。对此，应无疑义。需要注意的是，对于后续倒卖恶意注册账号的行为，也可以构成侵犯公民个人信息罪。网络账号密码，特别是具有信息发布、即时通信、支付结算等功能的网络账号密码，应当认定为公民个人信息。对此，《侵犯公民个人信息罪解释》第 1 条也作了明确列举。因此，对于符合可别性特征的自然人网络账号密码，可以纳入公民个人信息的范畴，对其非法出售、获取的行为可以适用侵犯公民个人信息罪。

其三，其他罪名。例如，《刑法》第 280 条之一规定了使用虚假身份证件、盗用身份证件罪。对于在网络账号恶意注册产业链中，黑产人员利用使用伪造、变造的或者盗

用他人的居民身份证、护照、社会保障卡、驾驶证等依法可以用于证明身份的证件，进行虚假注册，如相关行为属于依照法律、行政法规等国家规定应当提供身份证明的活动的，则可以考虑适用该罪名。此外，对于明知他人利用信息网络实施犯罪，为其犯罪提供账号，情节严重的，可以视情适用帮助信息网络犯罪活动罪。

四、网络流量产业链的检视

在网络犯罪中，网络流量多被作为网络犯罪的目标和工具。就前者而言，主要是指修改网页数据，将用户强制跳转至目标网页，以窃取、劫持流量；就后者而言，主要是指通过非法侵入计算机信息系统等方式，大量控制计算机信息系统，形成“肉鸡”，进而实施倒卖。从司法适用来看，对于以网络流量作为目标的行为，多表现为实施 DDo S 攻击，可以适用破坏计算机信息系统罪，对此并无争议，兹不赘言。在此只探讨流量劫持行为的定性问题。

（一）流量劫持的样态

从实践来看，流量劫持案件的表现有多种形态：有的篡改正规网站数据，将定制的数据展现在修改后的网页上，从而窃取正规网站用户流量；有的通过黑客技术对域名解析服务器进行攻击，篡改域名解析策略，将网民流量牵引到目标网站。流量劫持的目的行为多种多样，但主要涉及如下几种：（1）劫取流量，即劫取目标网站的流量，进而将获取的流量出售套现。（2）非法获取身份信息，即通过仿制需要登录或者支付的官方网站，再通过流量劫持等方式使用户访问，获取用户登录或者支付所用的账号密码等信息资料。这些身份信息被进而用于注册各类网络账号服务或者其他违法犯罪。（3）骗取资金，即通过仿制官方网店、第三方线上交易网站，通过流量劫持等方式让用户点击登录假网站进而进行支付，从而骗取支付的资金。

（二）流量劫持案件的区别对待

案例 1:[21]2013 年底至 2014 年 10 月，行为人租赁多台服务器，使用恶意代码修改互联网用户路由器的 DNS 设置，使用户登录“2345.com”等导航网站时跳转至其设置的“5w.com”导航网站，被告人再将获取的网络用户流量出售给“5w.com”导航网站所有者，违法所得合计 754762.34 元。法院经审理认为，行为人违反国家规定，对计算机信息系统中存储的数据进行修改，后果特别严重，均已构成破坏计算机信息系统罪。

案例 2:[22]自 2017 年 7 月开始，行为人为赚取赌博网站广告费用，对存在防护漏洞的目标服务器进行检索、筛查后，向目标服务器植入木马程序进行控制，再使用“菜刀”等软件链接该木马程序，获取目标服务器后台浏览、增加、删除、修改等操作权限，将添加了赌博关键字并设置自动跳转功能的静态网页，上传至目标服务器，提高赌博网站广告被搜索引擎命中几率。截止 2017 年 9 月底，行为人链接被植入木马程序的目标服务器共计 113 台，其中包含部分政府服务器。法院经审理认为，行为人构成非法控制计算机信息系统罪。

案例 1 是全国首例流量劫持入刑案件，审理过程中，对于具体罪名适用，存在盗窃罪和破坏计算机信息系统罪等不同主张，法院最终认定为破坏计算机信息系统罪。案例 2，审理过程中，对于具体罪名适用存在非法控制计算机信息系统罪与破坏计算机信

息系统罪等不同主张，法院最终认定为非法控制计算机信息系统罪。本文赞同上述两个案件的最终裁判结果，认为对流量劫持类案件的罪名适用应当注意如下几个问题：

第一，不宜适用盗窃罪。根据《刑法》第 264 条的规定，盗窃罪的对象为公私财物，构成盗窃罪的前提是犯罪对象具有财产属性。但是，网络流量是否具有财产属性，尚无明确的前置法律规定。特别是，《民法典》第 127 条尚未明确承认数据、网络虚拟财产的财产属性（“法律对数据、网络虚拟财产的保护有规定的，依照其规定。”）。基于刑法“二次法”的属性要求，在前置法律规定不明的情况下，对于盗窃网络流量案件适用盗窃罪尚需慎重。

第二，适用非法控制计算机信息系统罪和破坏计算机信息系统罪应当具体情况具体分析。根据《刑法》第 286 条的规定，破坏计算机信息系统罪在客观方面表现为三种行为方式：（1）破坏计算机信息系统功能。（2）破坏计算机信息系统数据、应用程序。（3）以传播计算机病毒等破坏性程序形式破坏计算机系统。对于流量劫持类案件，不会涉及到第三种行为方式，而主要是前两种行为方式。

就 DNS 劫持而言，行为人对域名解析服务器进行攻击，应当认定为破坏计算机信息系统功能的情形。而且，《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》（法释[2011]19 号）第 4 条专门提及了“域名解析服务器”。[23] 因此，可以认为，对于案例 1 所涉 DNS 劫持案件适用破坏计算机信息系统罪并无太大争议。需要进一步探讨的，对于案例 2 通过修改目标网站数据的方式进行浏览劫持的案件，究竟应当适用破坏计算机信息系统罪还是非法控制计算机信息系统罪。此种情形下，可能适用破坏计算机信息系统罪的情形只能是第二种行为方式，即对数据进行“删除、修改、增加的操作”。但是，从技术原理上而言，对计算机信息系统进行非法控制，也可能涉及到对数据的增删改操作。这就要求从两罪的立法精神上予以区分，以作出准确界分。所谓破坏计算机信息系统罪，应当重在破坏，虽然《刑法》第 286 条第 2 款不要求对数据的增删改达到“造成计算机信息系统不能正常运行”或者“影响计算机信息系统正常运行”的后果，但恐怕也不宜理解为只要对数据有增删改即可构成破坏计算机信息系统罪。作此理解，将无法对通过破坏非主要数据进而控制计算机信息系统的行为与破坏计算机信息系统的行为区分开来。[24] 因此，对于《刑法》第 286 条第 2 款对数据的增删改的行为应当限定为危害数据安全的相关行为，而非只要对数据进行增删改即可构成。而且，从非法控制计算机信息系统罪和破坏计算机信息系统罪的罪刑配置来看，也宜认为破坏计算机信息系统罪是重罪，应当对破坏数据的行为作适当限缩解释，解释为对主要数据进行增删改操作的情形。而就案例 2 所涉情形来看，行为人通过植入木马程序的方式，非法获取网站服务器的控制权限，进而通过修改、增加计算机信息系统数据，向相关计算机信息系统上传网页链接代码的，应当认定为《刑法》第 285 条第 2 款规定的“采用其他技术手段”非法控制计算机信息系统的行为。在此过程中，确实存在对数据进行增加、修改的操作，但所修改的并非主要数据，也未影响所针对计算机信息系统的正常运行，实际上是非法控制的操作，故认定为非法控制计算机信息系统罪更为适宜，更符合罪责刑相适应原则的要求。

五、资金通道产业链的检视

网络犯罪的目的通常在于非法获利，故资金通道是网络犯罪链条中最为关键的一环。资金通道链为网络犯罪提供支付、电子商务、游戏、取现等资金流转、掩饰、套现通道，涉及通道搭建、资金转移、取现、洗钱等环节。从实践来看，资金通道链条涉及购买虚拟产品、三方/四方支付、虚拟货币、租码跑分平台、地下钱庄等多种形式和环节。25

（一）非法经营罪的适用

对于未经批准从事网络资金支付结算业务的可以适用非法经营罪。当前，跑分平台、第四方支付等平台未获得国家支付结算许可，违反国家支付结算制度，聚拢大量个人、商户的支付宝、财付通、云闪付等支付账号或者银行账号，通过“化整为零”的方式，为网络赌博、电信诈骗、淫秽色情等网络违法犯罪提供资金代收代付服务，掩饰资金来源，规避国家反洗钱调查。对此，《最高人民法院、最高人民检察院关于办理非法从事资金支付结算业务、非法买卖外汇刑事案件适用法律若干问题的解释》（法释[2019]1号）将违反国家规定，使用受理终端或者网络支付接口等方法，以虚构交易、虚开价格、交易退款等非法方式向指定付款方支付货币资金的情形解释为《刑法》第225条第3项规定的“非法从事资金支付结算业务”。据此，对于网络犯罪资金通道链，符合上述情形的，可以适用非法经营罪。需要注意的是，对于此处规定的“资金支付结算业务”，不宜作过于泛化的理解，从而将为提供银行卡供人接收流转资金等行为也纳入其中，以符合社会一般观念的认知。26

（二）妨害信用卡管理罪的适用

当前，实践中出现了贩卖他人信用卡（包括贷记卡和借记卡）的活动，甚至出现了交易四件套的现象。由于此类交易除信用卡外，往往还包括该信用卡绑定的身份证信息、U盾、密码及手机卡，故实践中适用的罪名有异：有的适用妨害信用卡管理秩序罪，有的适用收买、非法提供信用卡信息罪。本文主张适用妨害信用卡管理秩序罪。27

根据《刑法》第177条之一第1款的规定，“非法持有他人信用卡，数量较大的”，构成妨害信用卡管理罪。而根据第2款的规定，“窃取、收买或者非法提供他人信用卡信息资料的”，构成窃取、收买、非法提供信用卡信息罪。根据《最高人民法院、最高人民检察院关于办理妨害信用卡管理刑事案件具体应用法律若干问题的解释》的规定，非法持有他人信用卡5张以上的构成前罪；窃取、收买、非法提供他人信用卡信息资料，足以伪造可进行交易的信用卡，或者足以使他人以信用卡持卡人名义进行交易，涉及信用卡1张以上的，即构成后罪。从字面意义上作客观解释，似可以认为贩卖他人信用卡的行为同时符合两罪的构成要件。但是，如果探究立法精神作主观解释，就不难发现司法解释设置相差悬殊入罪标准的原因。之所以在妨害信用卡管理罪的基础上，进而设置窃取、收买、非法提供信用卡信息罪，主要针对的是利用的是伪造信用卡的窃取、收买、非法提供信用卡信息这一预备环节，考虑到相关犯罪的查证困难，将其独立入罪。28有鉴于此，对于网络犯罪黑灰产业链中的贩卖他人信用卡行为，主要是为了转移支付资金，而通常不会涉及伪造信用卡，故不宜适用窃取、收买、非法提供信用卡信息罪。而且，从具体刑罚来看，适用妨害信用卡管理罪，也更加符合罪责刑相适应原则的要求，将危害较大的“卡头”作为主要惩治对象。29

（三）帮助信息网络犯罪活动罪的适用

对于明知他人利用信息网络实施犯罪，为其犯罪提供资金支付结算，情节严重的，可以构成帮助信息网络犯罪活动罪。就此而言，不仅相关平台可能构成，直接参与的行为人也可能构成。以租码跑分为例，租码即出租（微信、支付宝等平台的）收款码，“跑分”源自电脑或者手机的性能评测，在网络支付领域指非法网络平台利用高额收益为诱饵，诱导用户充值保证金获取相应积分，支付一定报酬，账户积分被相应扣减的一系列流程。这名义上是一种赚取佣金的网络兼职，实际上是一种新型洗钱手段。跑分平台提供的实际上是为犯罪团伙收款的服务。对于明知是信息网络犯罪活动，而为其提供跑分服务的，对于平台和参与者而言，可以认定为帮助信息网络犯罪活动罪所涉的“帮助”行为。而且，如前所述，此类跑分活动明显不是正常社会所需，可以认定为“提供专门用于违法犯罪的帮助”。

余论：网络犯罪黑灰产业链的标本兼治

近年来，网络犯罪层出不穷，背后是黑灰产业链的迅速发展和助推。在网络犯罪相当长时期内仍处于高发、频发态势的背景下，运用刑法对网络犯罪黑灰产业链进行有效规制，无疑是必要的。但也应当看到，刑法的积极作为不意味着刑法的万能，尽管刑法在黑灰产治理中作用明显、效果突出，然而单一维度依赖刑事法规制则只能治标、尚难治本。

应对网络犯罪黑灰产业链，要靠刑事惩治开路，更要靠健全相应的前置行政法律法规建立长效。以前述黑卡产业链为例，网络实名制尚未完全落实到位是主因，对物联网卡和海外卡未采取有效监管措施，导致了此类黑卡在网络犯罪黑灰产业中的泛滥。而在运用刑法进行惩治的过程中，成功追究刑事责任的实际上是少数，多数仍游离在规制之外，形成所谓的灰产，其原因还在于前置的法律规定和管理不健全。总而言之，有效应对网络犯罪黑灰产业链，既要发挥刑法惩治的功能，更要依靠行政管理、行业自治等多元手段，通过有针对性地探究网络犯罪黑灰产业滋生的具体原因，注重健全完善相关前置法律规定、强化行政法的事前规制，最终实现网络犯罪黑灰产业行业防范、事前规制、事后惩治的一体化治理。

注释

[1]参见《网络犯罪大数据报告及电信网络诈骗犯罪典型案例新闻发布会》，最高人民法院官网 http：//www.court.gov.cn/zixun-xiangqing-200651.html，最后访问日期：2020 年 3 月 21 日。

[2]参见《聚焦网络黑灰产业链：规模超千亿病毒式扩张》，《法制日报》2015 年 8 月 28 日。

[3]此外，就境外电信网络诈骗、开设赌场等案件而言，可能还需要组织人员偷越国(边)境，故还可能存在为此类网络犯罪提供人员招聘、培训、偷渡等帮助的人力资源环节。鉴于此类黑灰产主要存在跨境网络犯罪之中，且实践中法律适用争议不大，限于篇幅，本文不作详细阐释。

[4]即身份证原件、身份证对应的手机卡、身份证对应的银行卡和网银 U 盾。

[5]即对公银行卡、U 盾、法人身份证、公司营业执照、对公账户、公章、法人私章、对公开户许可证。有了这八件套，意味着一家经合法注册的公司及对公账户可以随时运营使用。

[6]参见黄太云：《〈刑法修正案(七)〉解读》，《人民检察》2009 年第 6 期。

[7]同理,《刑法》第 287 条之一规定的非法利用信息网络罪也具有堵截性质。就网络犯罪黑灰产业链的刑事规制而言,对于相关设立网站、通讯群组、发布信息的行为,在不构成其他犯罪的前提下,也可以充分考虑非法利用信息网络罪的适用。鉴于司法实践中对非法利用信息网络罪的适用并无太多争议,本文不展开讨论。

[8]《刑法》第 287 条之二第 3 款规定:“有前两款行为,同时构成其他犯罪的,依照处罚较重的规定定罪处罚。”

[9]参见喻海松:《新型信息网络犯罪司法适用探微》,《中国应用法学》2019 年第 6 期。

[10]2013 年 9 月 1 日开始,我国在全国范围内对新增固定电话、移动电话(含无线上网卡)用户实施真实身份登记,实行“先登记,后服务;不登记,不开通服务”。

[11]猫池是一种插上手机卡可以模拟手机收发短信、接打电话、上网等功能的设备,可以同时实现对多张手机卡的管理。猫池在正常行业也有广泛应用,如邮电局、证券交易所、信息呼叫中心等。

[12]目前,还存在“众包”型接码平台,让手机用户出租本人手机卡(一张或者多张)在平台上“挂单接码”。

[13]近年来,各企业为争夺用户投入大量资金,开展各种补贴大战,竞争非常激烈。广大用户在这些竞争中获取了实惠,但不少收益被掌握巨量手机黑卡资源的羊毛党获取。

[14]与之类似,有学者提出:“在这种公民自愿提供个人信息的情况下,不存在侵犯公民个人信息权益的问题,因此收购者和使用者的行为不构成侵犯公民个人信息的犯罪。对于这些大批量地收购公民身份证等个人信息的行为,确实具有较大的社会危害性,但我国刑法对此没有明文规定,目前尚不构成犯罪。”陈兴良:《互联网账号恶意注册黑色产业的刑法思考》,《清华法学》2019 年第 6 期。

[15]《网络安全法》关于个人信息的规定,更是侧重于网络信息安全和秩序,未赋予信息主体以排他权利。

[16]例如,《网络安全法》第 24 条第 1 款规定:“网络运营者为用户办理网络接入、域名注册服务,办理固定电话、移动电话等入网手续,或者为用户提供信息发布、即时通讯等服务,在与用户签订协议或者确认提供服务时,应当要求用户提供真实身份信息。用户不提供真实身份信息的,网络运营者不得为其提供相关服务。”《反恐怖主义法》第 21 条规定:“电信、互联网、金融、住宿、长途客运、机动车租赁等业务经营者、服务提供者,应当对客户身份进行查验。对身份不明或者拒绝身份查验的,不得提供服务。”虽然这些条文是从规制提供服务主体的角度,但无疑规定了用户的配合义务。根据上述规定,对于用户提供他人或者虚假身份证明骗取认证的情况下,似不能认为用户的行为属于合法行为,而应当认为其违反了法律规定。

[17]司法实践中,“两卡”案件,即倒卖手机卡、银行卡案件,对“卡头”追究刑事责任,并无争议。对于向他人出售、提供本人或者近亲属的手机卡、银行卡的案件,则应当区分情况处理:对于涉案卡的数量不大,主观明知程度不高的,不以犯罪论处;对于个别主观恶性较大、社会危害严重的,如受人组织跨越多地批量开卡,获利较大的,也可以视情纳入刑事规制范围。

[18]周加海、喻海松:《〈关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释〉的理解与适用》,《人民司法》2019 年第 31 期。

[19]该规定第 20 条规定:“对针对或者组织、教唆、帮助不特定多数人实施的网络犯罪案件,确因客观条件限制无法逐一收集相关言词证据的,可以根据记录被害人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实的电子数据、书证等证据材料,

在慎重审查被告人及其辩护人所提辩解、辩护意见的基础上,综合全案证据材料,对相关犯罪事实作出认定。”

[20]养号可以分为自动方式和人工方式：前者通过设置自动脚本或者使用群控软件等方式,让新账号模拟使用率、互动率、发布信息等正常用户行为,避免获取的网络账号被封号或者限制使用；后者通过人工添加好友等方式,未下游违法犯罪提供较为精准的目标人群,如刷单诈骗、投资理财类诈骗对象等。根据注册时间和账号内容丰富性不同,网络账号的价格会有较大差异。例如,刚注册的微信账号价格为十元左右,注册时间满一个月的为四十元左右,注册时间满一年的为二百元左右。更有甚者,活跃度较高且有固定目标人群的优质账号会被以数百元甚至数千元的价格进行倒卖。

[21]参见付宣豪、黄子超破坏计算机信息系统案,最高人民法院指导案例 102 号(2018 年)。

[22]参见江苏省南京市鼓楼区人民法院刑事判决书,(2018)苏 0106 刑初 487 号；南京市中级人民法院刑事裁定书,(2019)苏 01 刑终 768 号。

[23]该第 4 条第 2 款规定：“实施前款规定行为,具有下列情形之一的,应当认定为破坏计算机信息系统‘后果特别严重’：……(二)造成为五百台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为五万以上用户提供服务的计算机信息系统不能正常运行累计一小时以上的；……”

[24]更有甚者,如果不作限定,批量注册账号、组织刷单的行为实际都会对计算机信息系统中存储、处理或者传输的数据进行增加,形式上也符合了《刑法》第 286 条第 2 款的规定,但该结论明显有悖一般认知。

[25]鉴于司法实践中对于相关行为可以视情适用洗钱罪、掩饰、隐瞒犯罪所得、犯罪所得收益罪等罪名没有争议,兹不赘言。此部分只探讨非法经营罪、妨害信用卡管理罪和帮助信息网络犯罪活动罪的适用问题。

[26]例如,如前所述,出租、出售银行卡,后被他人用于资金流转的案件,对于相关银行卡的资金流水金额则不宜直接认定为“资金支付结算金额”,从而套用《新型网络犯罪解释》第 12 条“支付结算金额二十万元以上的”入罪标准。

[27]根据本文前述分析,对此类行为,不构成妨害信用管理秩序罪的,可以视情适用帮助信息网络犯罪活动罪。

[28]参见全国人大常委会法制工作委员会刑法室编：《中华人民共和国刑法·条文说明、立法理由及相关规定》,北京大学出版社 2009 年版,第 327-328 页。

[29]需要注意的是,具体办案中,对于《刑法》第 177 条之一第 1 款规定“非法持有他人信用卡”,似不能作过于机械的理解,要求行为人必须实际接触信用卡。例如,“卡头”让卖家直接寄给买家；又如,“卡头”雇佣他人组织开卡交易行为。上述情形中,“卡头”可能并未实际接触信用卡。基于实质解释的立场,本文主张可以认定“卡头”非法持有他人信用卡。

2、指导案例视角下网络黑灰产犯罪罪量的司法证明

吉冠浩　来源：《国家检察官学院学报》

摘　　要：

证明对象海量化以及证据与罪量的证明关系发生变化,使得在打击网络黑灰产犯罪时,对其罪量的司法证明问题成为当前的最大难题。现有罪量司法证明应对方案没有给予中国司法实践中的经验事实以足够关注。在对现有方案检讨的基础上,通过对有关两高指导性案例、《最高人民法院公报》《刑事审判参考》及相关典型案例的系统梳理发现,对于网络黑灰产犯罪罪量的司法证明,我国司法机关业已形成了一套证

明方法,其分为三个环节：公诉方基于综合认定得出推定数量；辩护方针对推定数量承担证明责任；公诉方对反驳进一步承担证明责任。

关键词：网络黑灰产犯罪;罪量;司法证明;间接证据;事实推定;

作者简介：吉冠浩,北京航空航天大学法学院讲师、法学博士。;

一、问题的提出

2020 年突如其来的新冠疫情在刺激我国数字经济发展的同时，也对网络黑灰产犯罪产生了重大影响。疫情期间，随着远程办公占比的上升，网络安全受到了空前威胁。据统计，黑灰产针对医疗、在线教育及在线办公、游戏三大行业的 DDo S 攻击和 Web 应用攻击均在 2020 年一季度呈现出高发态势。与此同时，网络内容生态的健康也受到黑灰产的严重侵害。“黑灰产利用互联网平台实施网络犯罪，不仅扰乱市场正常经营秩序，威胁关键信息基础设施稳定运行，更加危害到用户的个人信息安全，影响互联网行业的健康发展。”[1]所谓“网络黑灰产”，是指借助互联网技术与平台，进行有目的、有组织、有分工且规模化的网络违法犯罪。一般来说，网络黑灰产的链条分为上、中、下游：上游的黑灰产负责收集并提供各种数据资源，包括公民个人信息、手机黑卡、商业秘密等；中游的黑灰产负责开发定制大量黑灰产工具，以自动化的方式利用各类黑灰产资源实施各种网络违法犯罪活动；下游的黑灰产则负责将其上述“成果”进行交易变现，涉及众多黑灰网络交易与支付渠道。[2]换言之，“互联网产业的发展伴随着的是网络黑色产业和灰色产业，利用网络实施犯罪属于黑色产业，为网络犯罪提供技术支持、帮助的是灰色产业”[3]。

与上述情形相伴的大背景是，网络犯罪业已成为我国第一大犯罪类型，成为危害社会的一大毒瘤，占犯罪总数近三分之一，并且每年以近 30%幅度上升。[4]网络犯罪具有以下三大特点：“一是跨地域作案，被侵害人的人数众多、分散、随机性强；二是运用最新的网络和通信技术，采取非接触方式实施犯罪，由传统犯罪中人对人的基本模式改变为人对机的基本模式，犯罪人与被害人之间基本不直接接触；三是技术性强，作案方式隐蔽，侦查、取证难度大。”[5]我们日益发现，预备犯罪之人往往显示出对新技术、大环境以及生活方式改变的适应能力，这种适应性却让我们的执法者处于一种不利状态——执法者经常不能及时认识到新兴技术所带来的犯罪潜力。[6]

需要注意的是，与传统犯罪不同，网络犯罪的跨地域性、技术性、分工合作等特点导致传统刑事诉讼程序相关规定与司法经验存在很多不适应的地方,给网络犯罪案件的侦查、起诉和审判带来了不少挑战。[7]而当前网络犯罪呈现分工细化的态势，并逐步形成由各个作案环节构成的利益链条，这是网络犯罪泛滥的关键原因。因此，打击网络犯罪的关键是斩断利益链，突出对网络黑灰产犯罪的惩治。[8]而在打击网络黑灰产犯罪时，对其罪量的司法证明问题成为当前的最大难题。

根据我国刑法学通说，“罪量是在具备犯罪构成本体要件的前提下，表明行为的法益侵害程度的数量要件”[9]。罪量具有法定性、复合性和程度性等特征，在我国刑法规定中，罪量的内容包括犯罪数额与犯罪情节。[10]在网络黑灰产犯罪的刑事规制中，对其罪量的司法证明困境表现为以下两个方面：

一方面，网络黑灰产犯罪罪量的证明对象海量化。在我国刑事法定罪与量刑标准的框架下，罪量是重要的证明对象，我国网络黑灰产犯罪也是以罪量为中心标准的，其司

法评价体系中往往将数额和数量作为评价刑事责任的要素和定罪量刑的依据，如“浏览量”“信息数”“拨打量”“侵害人数（次）”“注册会员数”等。[11]而在网络黑灰产犯罪中，其证明对象呈现出海量化的特征，罪量的认定出现困难。在网络黑灰产犯罪中，其被害人、犯罪嫌疑人分散在全国各地，对于以被害人数、被侵害的计算机信息系统数量、涉案资金数额等作为定罪量刑标准的犯罪案件，通常难以逐一对被害人、犯罪嫌疑人或是计算机信息系统进行取证。例如，对网络诈骗案件，被害人动辄成千上万，不具备向所有被害人取证认定犯罪嫌疑人违法所得的可能性。[12]有的办案人员坦言：如果要一一核实，全市民警一辈子也查不完，真是“一生办一案”。[13]对此，有论者指出：“海量化对象使得传统刑事印证证明模式面临挑战”[14]。详言之，“按照传统司法的精准计量模式对网络犯罪的数额进行计量、核实和认定存在着客观不能，包括犯罪数额难以认定、犯罪数额的认定难以精确、犯罪数额的真实性难以核实、犯罪数额的认定具有或然性等多种情形”[15]。

另一方面，证据与网络黑灰产犯罪罪量的证明关系发生变化。在传统犯罪中，对罪量的司法证明往往可以通过运用证据印证规则来完成。详言之，通过对直接证据的印证，其他证据足以与直接证据一起发挥直接证明包括罪量在内的案件主要犯罪事实的作用；而在只有间接证据的案件中，通过各项间接证据之间的相互印证与佐证，使得各项证据信息链条之间发生相互验证的关系，从而最终形成较为完整的证据锁链，使包括罪量在内的案件事实得以证明。[16]其中，所谓“印证”，是指两个以上的证据所包含的事实信息发生重合或交叉。[17]而在网络黑灰产犯罪中，其证明对象的海量化使得犯罪事实的证明和认定不再如传统犯罪简单直接，在有些案件中，网络黑灰产犯罪罪量的司法证明正在由相对不能走向绝对不能，甚至超出了司法证明的极限。[18]换言之，如图 1 所示，在对网络黑灰产犯罪罪量的司法证明中，往往存在依靠传统的印证证明模式不能证明罪量，需要根据多个证据共同拼凑、整合才有可能综合认定罪量的情况。

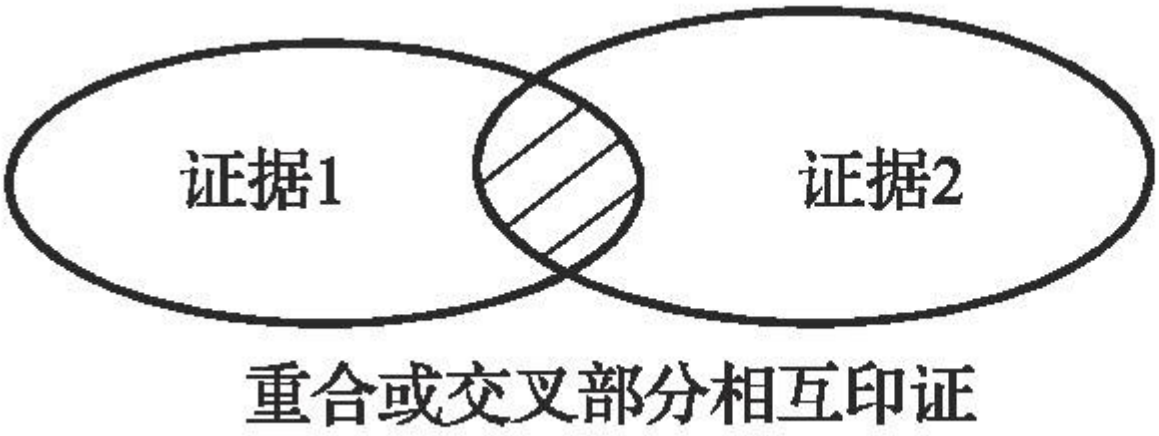


图 1 证据与网络黑灰产犯罪罪量的证明关系　　下载原图

二、现有罪量司法证明应对方案的检讨

为了应对网络黑灰产犯罪罪量的证明对象海量化以及证据与网络黑灰产犯罪罪量的证明关系发生变化这两大难题，目前存在以下三套应对方案：

其一，在传统刑事印证证明模式的框架下，尝试用“概括印证”取代传统的“一一印证”。该方案的核心内容是：以证明方式的概括印证取代计量对象的具体印证，即传统犯罪对于事实要素的认定，通常建立于证据与证据之间的一一印证关系；对于存在海量化计量对象的网络犯罪而言，无需每一计量对象的证明均要满足证据间的一一印证，只要客观存在的计量对象在整体上得到了被告人供述、被害人陈述、证人证言或书证等相关证据的印证，就可将计量对象所涉数额认定为犯罪数额。[19]

其二，仍是在印证证明模式的框架下，强调坚守“底线证明”方式。该方案的核心内容是：采取简化证明的“底线证明”方式，按照法定的入罪和加重处罚两道坎，提供能用以定案的最基本的证据。底线证明方式存在以下两步证明：若要追究网络黑灰产犯罪者的刑事责任，指控证据必须证明其已经触及法定的入罪门槛；若要追究其加重刑事责任，指控证据还必须证明其已经触及法定的加重处罚门槛。换言之，公安司法机关必须在证明作为底线的数额/数量指标方面，达到“案件事实清楚，证据确实、充分”的要求；而对超过作为底线的数额/数量指标，只需进行概要性的证明或展示即可。[20]

其三，超出传统刑事印证证明模式的框架，采用“综合认定”的方法。该方案的核心内容是：主张“综合认定”不苛求其他证据印证，在大数据时代，同一数据可以蕴含不同信息，孤证也可以认定犯罪数额。分析数据本身就可以认定数额，无须寻找其他证据加以印证。[21]与之类似，有论者提出：转变证明理念，摒弃印证的思维模式。与印证理念转变相适应，变更取证方式，重视间接证据的搜集，通过间接证据编织成证据链证明包括罪量在内的案件主要事实。[22]比如，针对电信网络诈骗犯罪活动的猖獗，2016 年两高公安部发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》（以下简称《电信网络诈骗意见》），提出“综合认定”的证明方法。有论者指出综合认定的应然进路是：吸纳法律论证理论，重视言述知识与非言述知识的统一，融体验哲学及知识的默会方式于既有认知模式中，重新体认案件事实形成中的程序及证成属性，廓清间接证据使用中的误区，认真对待情状证据所蕴含信息的加权作用。[23]

上述三种应对方案反映了学界对网络黑灰产犯罪罪量司法证明难题的关注与思考，对该问题的解决具有较高的借鉴意义，也对本文的写作产生了重要的启发。但不无遗憾的是，现有应对方案偏好于“我认为”，提出的内容多属于“应然进路”的制度设计，从而缺少“我发现”，没有给予中国司法实践中对网络黑灰产犯罪罪量司法证明的经验事实以足够关注，尤其是缺少对两高相关指导性案例的应有重视。对于此种研究进路，有论者指出：一些学术论文给人一种感觉，即由“我认为”带出的理论、观点随处可见，而这些理论观点所依据的事实证据的发现过程及其展示事实证据的方法却显得比较单薄。如果学者认为自己说出的理论很特别，那最好先说出新发现的事实。[24]需要说明的是，笔者对当前指导性案例等经典案例所反映的司法实务对网络黑灰产犯罪罪量司法证明的实然做法的研究，并非在于诉说其优于上述归纳的三种应对方案，也不是因为实然的方案符合司法实践，就对其进行一味的肯定。我们想要强调的是，如果要推进对网络黑灰产犯罪罪量的司法证明的研究，一定要先明了当前司法实践对这一问题做了哪些努力，司法现状究竟是什么样的。

当前法学研究的主流仍是社会科学领域的研究，其关键是把经验事实作为研究对象，即那些有证据证明已经发生过的事实。我国指导性案例就是重要的法律经验事实，对

于这些案例，我们不仅要关注案情本身、案件的裁判结果，更要关注裁判的理由。[25]网络黑灰产犯罪属于新类型犯罪，犯罪手法比较新颖，网络技术的发展较快，法律具有概括性和原则性，导致在司法实践中对打击此类犯罪存在一些法律适用方面的新情况、新问题。两高试图以指导性案例的方式提炼司法实践中可行的法律适用规则，有利于指导公安司法工作人员提高法律适用能力，准确打击此类新型犯罪。[26]

笔者在下文藉由对两高指导性案例、《最高人民法院公报》、《刑事审判参考》及相关典型案例的系统梳理，尝试探索因着网络信息技术的改变，刑事诉讼法及其司法解释的哪些条文仍然可以适用，哪些已经无法因应；[27]在修法前，现行法可以如何解释来因应网络黑灰产犯罪罪量司法证明的上述问题。

三、公诉方基于综合认定得出推定数量

网络黑灰产犯罪罪量证明对象的海量化使得公诉方在认定罪量时困难重重，甚至是客观不能；证据与网络黑灰产犯罪罪量的证明关系发生了变化，需要根据多个证据共同拼凑、整合才有可能综合认定罪量。对此，我国刑诉法及其司法解释作出了一定的调整。

如两高公安部《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》对包括黑灰产犯罪在内的涉众型网络犯罪的司法证明作出的规定[28]，关于该特殊证明规则，我们需要注意以下三点：[29]第一，其适用范围仅仅是涉众型网络犯罪案件，不能适用于一般的网络犯罪案件。第二，需要有电子数据、书证等证据材料记录被害人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实，即对于基本犯罪事实已经有相应的客观性证据证明。不过由于客观条件的限制，对于这些证据无法逐一收集相关的言词证据。第三，在慎重审查被告人及其辩护人所提辩解、辩护意见的基础上，综合全案证据材料，对相关犯罪事实作出认定。但是，如果犯罪嫌疑人提出诸如涉嫌诈骗的账户里有合法收入的合理怀疑的，则不能认定该笔犯罪事实。再如两高公安部《电信网络诈骗意见》第 2 条第 4 项的规定[30]与第 6 条第 1 项的规定[31]。

上述司法解释的局限性在于适用范围的限制，无法适用于所有网络黑灰产犯罪罪量的司法证明之中。那么，我们下面尝试通过对指导性案例的系统梳理，“发现”一下司法实务中，公诉方如何破解网络黑灰产犯罪罪量证明这一难题。目前指导性案例等经典案例反映出司法实务对网络黑灰产犯罪罪量的司法证明存在以下三种方法：

（一）运用证据互相印证规则，综合公诉方提供的证据，综合认定罪量

在认定诸如非法经营数额、违法所得数额等罪量时，用来综合认定的证据往往包括被告人供述、证人证言、被害人陈述、网络销售电子数据、被告人银行账户往来记录、送货单、快递公司电脑系统记录、被告人等所作记账等证据；在认定诸如被害人数量时，用来综合认定的证据往往包括犯罪嫌疑人使用网络电话与被害人通话的记录、被害人向犯罪嫌疑人指定银行账户转账汇款的记录、犯罪嫌疑人的收款账户交易明细等证据。

在最高法第 87 号指导案例中，[32]关于假冒注册商标犯罪的非法经营数额、违法所得数额，裁判要点指出：“应当综合被告人供述、证人证言、被害人陈述、网络销售电子数据、被告人银行账户往来记录、送货单、快递公司电脑系统记录、被告人等所作记账等证据认定。”[33]详言之，郭明升等三被告人在公安机关的多次供述，以及公

安机关查获的“三星数码专柜”淘宝记录、支付宝向被告人郭明锋银行账户付款记录、郭明锋银行账户对外付款记录、送货单、快递公司电脑系统记录、公安机关现场扣押的笔记等证据之间能够互相印证，综合公诉方提供的证据，可以认定公诉方关于三被告人共计销售假冒的三星 I8552 手机 20000 余部，销售金额 2000 余万元，非法获利 200 余万元的指控能够成立。需要注意的是，本案中公诉方通过银行的进货款支付记录与进货物品单价之间的计算可以佐证进货数量，由此便可进一步计算出非法经营数额，这一证明思路值得借鉴。[34]

在最高检第 67 号指导性案例中，[35]在审查起诉阶段，检察官发现在案证据存在以下问题：被害人与诈骗犯罪组织间的关联性证据调取不完整，无法证实部分被害人系本案犯罪组织所骗。遂将案件退回公安机关补充侦查，并提出以下补充侦查意见：补充调取犯罪嫌疑人使用网络电话与被害人通话的记录、被害人向犯罪嫌疑人指定银行账户转账汇款的记录、犯罪嫌疑人的收款账户交易明细等证据，以准确认定本案被害人。随后，公诉方经审查认为，75 名被害人与诈骗犯罪组织间的关联性证据已补充到位，具体表现为：网络电话、Skype 聊天记录等与被害人陈述的诈骗电话号码、银行账号等证据相互印证；电子数据中的聊天时间、通话时间与银行交易记录中的转账时间相互印证；被害人陈述的被骗经过与被告人供述的诈骗方式相互印证。[36]

在“杀鱼盘”案中，[37]由于被告人使用的各种社交软件账号和购物平台账号均为购买的“小号”，并非实名，所以大量被害人信息无法准确核实。在被害人“缺失”的情况下，案件的争点是被告人之间的转账记录能否被认定为犯罪金额。对此，公诉方指出：被告人的账户确为诈骗所得、电商平台的账户订单确为他人付款购买，且通过全案证据排除了上下线其他经济往来；再综合已查明的被害人供述、交易记录、电子数据等，足以证实“违法来源”的排他性。因此，公诉方最终将上下线转账记录认定为犯罪金额。[38]

（二）综合一系列间接证据，基于常识和经验，予以认定和评估罪量

如关于被害单位因被告人犯行遭受损失的司法证明，可以综合案发时行业发展趋势、被害单位日常收入情况、案发时收入情况，予以综合认定和评估。又如关于遭受破坏的计算机信息系统服务用户数的认定，可以根据计算机信息系统的功能和使用特点，结合网站注册用户、浏览用户等具体情况，包括日均电脑客户端访问量，作出客观判断。再如关于网络域名的价值评估的认定，可以综合考虑网络域名的购入价、销赃价、域名升值潜力、市场热度等综合认定。

南京市雨花台区检察院以被告人董志超、谢文浩犯破坏生产经营罪，向雨花台区法院提起公诉。[39]本案系“反向刷单”，案件的争点在于反向刷单造成的损失如何计算。对此，最高法指出：“被害单位因被告人犯罪行为遭受的损失，可以综合案发时行业发展趋势、被害单位日常收入情况、案发时收入情况，依照有利于被告人的原则，综合予以认定和评估。”[40]详言之，在案证据可以证实，2014 年 4 月至 5 月，淘宝网论文相似度检测行业被搜索的网络浏览量和用户个数基本处于上升态势，被害单位商品搜索降权期间的日确认收货搜索引导成交金额仅为 4019 元、419 元、70 元、19 元、23 元、4932 元，平均额为 1578.8 元，远低于其扣除搜索降权期间当年 4 月份、5 月份或 4 月至 5 月的平均额 18547 元、23352 元、21216 元，损失客观存在，依照有利于被告人的原则，就低认定损失为人民币 10 万余元。

在最高检第 33 号指导性案例中，[41]本案源于被告人劫持域名，造成计算机信息系统不能正常运行，案件的争点为如何认定遭受破坏的计算机信息系统服务用户数。该案中，对于域名劫持用户数的认定，检察院起诉及法院判决时，是根据独立 IP 用户来计算用户数量，但在论证过程中，有专家提出，根据独立 IP 用户来计算用户数量，不太符合现实，也不太符合技术实际。经综合考虑，对独立用户数的认定，指导性案例采取了较为概括谨慎的表述。[42]即最高检指出：“认定遭受破坏的计算机信息系统服务用户数，可以根据计算机信息系统的功能和使用特点，结合网站注册用户、浏览用户等具体情况，作出客观判断。”[43]本案中，经司法鉴定，该知名网站共有 559 万有效用户，其中邮箱系统有 36 万有效用户。按日均电脑客户端访问量计算，10 月 7 日至 10 月 20 日邮箱系统日均访问量达 12.3 万。李丙龙的行为造成该知名网站 10 月 21 日 19 时至 23 时长达 4 小时左右无法正常发挥其服务功能，案发当日仅邮件系统电脑客户端访问量就从 12.3 万减少至 4.43 万。进而认定李丙龙的行为符合“造成为 5 万以上用户提供服务的计算机信息系统不能正常运行累计 1 小时以上”“后果特别严重”的情形。

在最高检第 37 号指导性案例中，[44]案件的争点在于非法获取网络域名的价值评估。对此，最高检指出：“可综合考虑网络域名的购入价、销赃价、域名升值潜力、市场热度等综合认定。”[45]此外，在《刑事审判参考》第 723 号案例中，最高法指出：本案中网站淫秽电子信息实际被点击数和注册会员数不能笼统认定，应结合案件情况综合评估其对案件定罪量刑的作用。[46]

（三）对于客观不能逐一核实有关罪量信息的案件，在辩护方没有异议时，可以适用推定

需要特别强调的是，推定的适用并不意味着证明责任的转移。在辩护方提出诸如有重复计算的辩解时，应当由公诉方承担证明责任，辩护方也可以自行提交佐证材料。

司法实践中，网络黑灰产犯罪的涉案公民个人信息动辄上万条乃至数十万条。对于该类案件，不排除少数情况下存在重复信息的情形，比如针对同一对象并存“姓名+身份证号”“姓名+住址”“姓名+电话号码”等数条信息，但要求做到完全去除重复信息则较为困难，对于信息的真实性也难以一一核实。在王某琼等侵犯个人信息案中，[47]便出现了这种情况，被告人通过非法手段获取 20 余万条公民个人信息。逐一认定个人信息是否真实会消耗过多的司法资源，但无条件地全部认定为公民个人信息亦有不妥，因为客观存在上述重复情形的概率比较高。因此，有论者指出：在被告人及其辩护人不提异议的情况下，应当允许适用推定规则。[48]

（四）小结

在刑事诉讼中，司法证明存在两种不同的方式：一是通过对直接证据所包含的证据事实进行印证和补强，从而达到证明待证事实的效果；二是通过对若干间接证据所包含的证据事实进行逻辑推理，使其形成较为完整的证据锁链，从而排他性地认定待证事实的存在。[49]上述第一类证明方法，即运用证据互相印证规则，综合公诉方提供的证据，综合认定罪量，以及第二类证明方法，即综合一系列间接证据，基于常识和经验，予以认定和评估罪量，均属于第二种证明方式，即间接证据证明。

同时，作为证据裁判原则的例外，存在不通过司法证明即可认定案件事实的方法，即替代司法证明的方法。推定就是替代司法证明的方法之一，针对司法实践中的证明困难，它是一种重要的解决方式，这在我国规范性文件和司法实践中均有体现。[50]推定是在案件事实真伪不明情形下从已知事实推断未知事实的一项制度，其分为法律推定与事实推定。[51]前者是指法律上明文规定如果能证明一事实存在且无反证存在时，则另一事实的存在得以证明的推定；后者是指一事实的存在被证明时，对照一般的经验法则与论理法则，用以推定待证事实的另一事实存在，被认定合理且确定的推定。[52]换言之，法律推定和事实推定均应当是“作为间接证据的评价”提出来的，法律推定源自于法律，因此其具有直接的法律约束力，而事实推定作为经验的表述，对法官心证产生较大的影响。[53]可见，法律推定与事实推定的认识对象均是未知事实，认识方法均是推断，认识过程均是从一事实到另一事实，二者最大的不同在于有没有法律的明确规定。[54]推定包括两种事实：基础事实，作为推定前提的案件事实，其需要通过提出证据加以证明；推定事实，未经司法证明而被直接认定成立的事实。需要注意的是，在基础事实与推定事实之间，并没有建立必然的因果关系，而存在一种逻辑推理上的跳跃。[55]此外，还需要强调的两点是：关于基础事实，公诉方必须承担证明责任，提出证据证明，且需证明到事实清楚，证据确实、充分的程度，即在刑事诉讼中适用推定规则时基础事实的证明标准须是“确信无疑”。[56]关于推定事实，其是可以被推翻的，即如果有相反的证据证明该推定的基础事实不成立，该推定即被推翻。[57]只要举出不同于推定的证据，无论是法律推定还是事实推定均可以被反驳。[58]上述第三种证明方法，即对于客观不能逐一核实有关罪量信息的案件，在辩护方没有异议时，可以适用事实推定，就属于这一替代司法证明的方法。

需要注意的是，第三种证明方法区别于第一、二种证明方法的理论根基在于：事实推定与间接证据证明的理论区分。详言之，事实推定的结构为先证明基础事实，在此基础上根据经验法则、逻辑法则等认定推定事实，而间接证据证明案件事实先需通过间接证据认定与证明对象有关的间接性事实，然后运用间接性事实进行逻辑推理，证明待证事实；基础事实与推定事实之间是选择关系，而间接性事实与待证事实之间是排他性的一一对应关系；基础事实得到证明时只能初步认定推定事实成立，并给予辩护方反驳的机会，如果辩护方没有提出反驳、反驳缺乏根据或反驳意见被驳回，则推定事实生效，而对于间接证据证明，一旦公诉方承担了证明责任的要求，该证明活动即告完成。[59]

综上可知，基于网络黑灰产犯罪罪量证明对象的海量化以及证据与网络黑灰产犯罪罪量的证明关系发生的变化，公诉方可以运用间接证据进行司法证明，也可以基于综合认定得出一个推定的罪量。对于前者，公诉方需要承担证明责任并将之证明到最高的证明标准；对于后者，情况不同，我们在下文着重分析。

四、辩护方针对推定数量承担证明责任

如果公诉方基于综合认定得出了推定的罪量，那么应当给予辩护方进行反驳的机会。[60]需要注意的是，公诉方基于综合认定得出网络黑灰产犯罪罪量的推定数量属于一个推定事实，那么，作为推定事实，这一推定数量便是可以被推翻的。比如，对于上述两高一部《电信网络诈骗意见》第 2 条第 4 项的规定，如果辩护方提出诸如涉嫌诈骗的账户里的款项具有合法来源，则不能认定该笔犯罪事实。可见，推定事实在法律上是不确定的事实，辩护方只要提出证据证明了相反的事实存在，就可以推翻该项推

定事实，使得公诉方通过推定所认定的案件事实不再成立。[61]反之，则如两高一部《电信网络诈骗意见》第 7 条第 2 项的规定。[62]下面，我们继续对指导性案例等典型案例进行探讨：

在最高法第 87 号指导案例中，被告人郭明升等三人及其辩护人对其未经“SΛMSUNG”商标注册人授权许可，组装假冒的三星手机，并通过淘宝网店进行销售的犯罪事实无异议，但对非法经营额、非法获利提出异议，辩解称其淘宝网店存在请人刷信誉的行为，真实交易量只有 10000 多部。其中，对于公诉方综合认定的假冒注册商标犯罪的非法经营数额、违法所得数额之推定数量，辩护方需要承担证明责任来推翻这一推定，否则就要承担不利后果。对此，裁判要点指出：“被告人辩解称网络销售记录存在刷信誉的不真实交易，但无证据证实的，对其辩解不予采纳。”[63]这里的“不予采纳”，系证明责任的裁量转移，其内在逻辑在于固守证明责任合理调配的基本立场，防止公诉方陷入极易出现的举证客观不能之困境。[64]换言之，辩护方辩解电子销售记录总额中有部分交易系“刷单”形成，此时应当承担相应的证明责任，否则便不能采纳辩护方的“刷单”辩解。[65]

在董志超、谢文浩破坏生产经营案的二审庭审中，[66]辩护人出示了安徽省庐江县公证处出具的公证书及相关书证，证明董志超于 2016 年 1 月 31 日在相关淘宝店铺中购买 1000 余单名为“全面测试大量购买导致的行为”的商品，该店铺未被淘宝平台处罚，进而证明董志超的行为与智齿科技南京公司的降权无刑法上的因果关系，淘宝平台的处罚具有随意性和不确定性。对此，出庭检察官出示了浙江淘宝网络有限公司出具的说明，证明针对董志超购买的商品，淘宝公司发现商品类目为“邮费”，因公司规定“邮费链接无评价入口，不计销量”，所以没有搜索排名和流量，不会造成获利。淘宝平台抓取的炒信商品为有评价和销量的正常商品，所以大量购买此类商品并不会被淘宝平台的相关规则抓取到。经审查认为，辩护人出示的该部分证据所证明的董志超批量购买相关商品的行为与本案中批量购买智齿科技南京公司商品的行为不属于同一性质购买商品或服务的行为，故与本案事实无关联性，不予采信。[67]本案中，辩护方未能完成针对推定数量的证明责任，故辩护意见未被采纳。

在《刑事审判参考》第 669 号案例中，[68]被告人罗刚等及其辩护人在庭审中，均对公诉方指控的淫秽图片的点击量提出异议，认为公诉方认定点击量达 25 万余次的证据不足；由于一页多图、产品合格率、自主点击等因素的存在，涉案淫秽图片的实际点击量应远低于公诉方指控的 25 万余次；公诉方没考虑到联通公司在《中国联通公司增值业务提供商运行维护管理要求》中提出的 60%页面访问成功率的要求，请求法院查明实际点击数后依法予以从轻、减轻或者免除处罚。西城区法院经审理查明：为了提高联通 WAP 的点击率，增加公司收入，被告人罗刚指使被告人杨韬等在本公司内通过 WAP 业务传播淫秽信息。经鉴定，于 2007 年 1 月 1 日至 2007 年 5 月 9 日共上传 28 张淫秽图片，经专用工具计算页面点击并排除自点击后，28 张淫秽图片的实际被点击数为 82973 次。其中，关于如何正确计算淫秽电子信息的实际被点击数，裁判理由强调：“要排除人为设置的虚假计数、网站的自点击数、有证据证实的无效点击数以及因为手机 WAP 上网的特性导致的同一电子文件设置的重复计数，从而得出实际被点击数。对于其他需要排除的计数方式，必须有必要和充分的证据证实才能予以排除，而且实践中这种排除的范围不能过大。”[69]比如，在本案中，辩护方提出中国联通制定的《中国联通增值业务提供商运行维护管理要求》中要求增值业务提供商所提供的增值业务的最低页面访问成功率是 60%，所以实际被点击数应当按照内容请求数×

60%来计算。但这一辩解未被法官采纳，因为页面最低访问成功率只是一个下限，实际成功访问率可能远远超过该比率，依照该比率得出的不成功访问数仅是推算，并没有确实的证据可以证实，故不能依照最低页面访问成功率来作为排除不成功点击数的依据。

在《刑事审判参考》第 723 号案例中，被告人杨勇对公诉方指控其传播淫秽物品无异议，但作出如下辩解：实际的会员数量低于指控的数量。其辩护人提出如下辩护意见：公诉方指控的淫秽电子信息点击数、会员数远多于实际数量。二审法院四川省泸州市中级法院经依法审理认为：上诉人杨勇应以传播淫秽物品牟利罪追究刑事责任。一审未区分普通电子信息与淫秽电子信息的被点击数，导致淫秽电子信息实际被点击数事实不清，故不予认定。关于淫秽电子信息实际被点击数和注册会员数如何认定，裁判理由指出："在计算淫秽电子信息的实际被点击数时，如查明确实存在虚增点击数的情况，就应当扣除虚增的点击数。"[70]被告人杨勇所建网站并非专门从事制作、复制、出版、贩卖、传播淫秽电子信息活动，故该网站虽包含大量的淫秽电子信息，但有别于纯粹的淫秽网站，该网站淫秽电子信息的实际被点击数应当低于截至案发当日该网站的实际被点击数。本案中，辩护方完成了针对推定数量的证明责任，故辩护意见被采纳，电子信息的实际被点击数扣除了虚增的点击数。

在王某琼等侵犯个人信息案中，[71]计算所侵犯的公民个人信息数量时，辩护方有证据证实系重复计算的公民个人信息，最终在总数中被扣除。对此，2017 年两高发布《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》（以下简称《侵犯公民个人信息解释》）第 11 条第 3 款作出了规定。[72]该规定在一定意义上将证明责任转移给辩护方，并借助司法解释将之上升为正式的法律规则。[73]本案中，辩护人提交的实验记录虽然仅是对部分样本进行筛查后得出的，但鉴于本案涉案个人信息数量过于庞大，对每条信息进行逐一甄别不具有现实意义，而且辩护人系随机选取数据，并非有意查找具有重复信息的数据，该样本具有代表意义。所以，辩护人提交的实验记录能够证实王某琼获取的个人信息存在重复情况。本案根据有利于被告人原则，按照辩护人所做实验记录的 4.5%的重复率在总数中予以扣除。[74]

我们需要明了，推定成立的前提是基础事实得到证明；在基础事实得到证明的前提下，对推定事实就可以自动地进行认定。为推翻推定事实需要证明责任转移，即在推定规范的作用下，公诉方被免除了证明推定事实成立的义务，而证明推定事实不成立的责任则转移给辩护方。[75]换言之，关于证明责任的转移，是在刑事诉讼中，承担证明责任的一方提出一定的证据以后，由对方承担提出证据责任的情况。[76]即在遵循"谁主张，谁举证"原则的前提下，提出诉讼主张的一方在将待证事实证明到一定程度之后，另一方需要承担证明该待证事实不存在或另一新的案件事实存在的责任。证明责任转移的特殊性在于其须先存在一证明责任分配的一般原则，否则就没有"转移"可言。[77]在适用推定规则的案件中，公诉方对作为推定前提的基础事实承担了证明责任，使得推定事实初步成立，被告人为推翻推定事实，需要承担证明责任。[78]即这些推定从一个事实的存在推定另一事实的存在，该推定不仅在诉讼开始对案件事实起到一种表见证明[79]的作用，而且会相应导致对方当事人承担证明责任，这就导致了证明责任的转移。[80]

需要注意的是：辩护方对推定事实的反驳属于他的证明责任，因此需要达到一定的证明标准，但基于保障被告人权利的价值考量，适用于辩护方的证明标准应低于适用于

公诉方的证明标准，只需达到“优势证据”的标准。[81]换言之，关于辩护方所承担的证明责任，法律并未确立明确的证明标准，学理上不要求达到最高的证明标准。[82]对此，有论者指出：司法实践中的理性证明模式应当是辩护方自由证明模式以及“合情确信”标准，即被告人通过提供某一证据（线索）或口头说明诸如“刷单”过程都可以影响法官的内心确信，且这种内心确信无须达到完全客观的保证，而仅需在情理上具有可接受性即可。[83]

五、公诉方对反驳进一步承担证明责任

在当辩护方针对网络黑灰产犯罪罪量的推定数量承担证明责任，提供证据证明推定事实不成立后，证明责任再次转移给公诉方。对于辩护方证明推定事实不成立的反驳，公诉方需要进一步承担证明其不成立的责任，且要达到事实清楚，证据确实、充分的程度。[84]该方法也得到了指导性案例等典型案例的落实。

在王某琼等侵犯个人信息案中，被告人王某琼的辩护人通过随机抽取涉案信息的方式进行的实验确实能够证实公诉方指控的涉案信息存在重复计算的情况，公诉方对此也予以认可。但鉴于数据海量，无法精准认定重复计算的条数，而实验所得结论（重复率）是客观的，将该实验所得结论推定适用于全部数据在总数中予以扣除，亦具有合理性。[85]该案中，公诉方对于辩护方的反驳予以认可，放弃了继续承担证明责任。

在最高检第 67 号指导性案例的庭审中，50 名被告人对指控的罪名均未提出异议，部分被告人及其辩护人主要提出以下辩解及辩护意见：检察机关指控的犯罪金额证据不足，没有形成完整的证据链条，不能证明被害人是被告人所骗。针对上述辩护意见，公诉人答辩如下：本案认定诈骗犯罪集团与被害人之间关联性的证据主要有：犯罪集团使用网络电话与被害人电话联系的通话记录；犯罪集团的 Skype 聊天记录中提到了被害人姓名、公民身份号码等个人信息；被害人向被告人指定银行账户转账汇款的记录。起诉书认定的 75 名被害人至少包含上述一种关联方式，实施诈骗与被骗的证据能够形成印证关系，足以认定 75 名被害人被本案诈骗犯罪组织所骗。对此，最高检指出：办理电信网络诈骗犯罪案件，认定被害人数量及诈骗资金数额的相关证据，应当紧紧围绕电话卡和银行卡等证据的关联性来认定犯罪事实。一是通过电话卡建立被害人与诈骗犯罪组织间的关联。二是通过银行卡建立被害人与诈骗犯罪组织间的关联。三是将电话卡和银行卡结合起来认定被害人及诈骗数额。[86]该案中，公诉方对于反驳进一步承担了证明责任并达到了法定的最高证明标准，成功地完成了指控。

随后，辩护方可以继续针对公诉方的指控进行反驳。如此进行第二轮、第三轮等环节的抗辩。这里需要再次强调的是，对网络黑灰产犯罪罪量的司法证明，如果公诉方是基于综合认定得出了推定数量，那么这个推定数量属于一个事实推定，而事实推定的效力具有一定的假定性，辩护方反驳的不存在或不成立是认定这一事实推定生效的必备因素。[87]所以，公诉方需要继续对辩护方反驳的不存在或不成立进行证明，否则就要承担败诉风险。

结论

通过对有关两高指导性案例、《最高人民法院公报》、《刑事审判参考》及相关典型案例的系统梳理，我们发现，对于网络黑灰产犯罪罪量的司法证明，我国司法机关业已形成了一套证明方法，其分为三个环节：首先，公诉方基于综合认定得出推定数量；

接着，辩护方针对推定数量承担证明责任；最后，公诉方对反驳进一步承担证明责任。区别于上述学界现有三种应对方案的“应然进路”制度设计之思路，该套证明方法关注中国司法实践中对网络黑灰产犯罪罪量司法证明的经验事实，尤其重视两高相关指导性案例及典型案例。当然这一关于经验事实的研究，并非旨在与上述三种应对方案进行优劣比较，笔者也并非对其进行一味的肯定，我们想要尝试的是洞悉当前司法实践对网络黑灰产犯罪罪量的司法证明问题的现状究竟是什么模样，其中涉及的关键性理论争点有哪些，进而为下一步从经验到理论的深入研究提供基础性参考与借鉴。

“21 世纪我们面临的重大挑战是如何把信息和技术风险维持在控制层次，以及战胜网络犯罪。”88 在网络黑灰产犯罪中，其罪量的证明对象呈现出海量化的特征，使得公诉方在证明罪量时困难重重，甚至是客观不能，超出了传统司法证明的极限。与此同时，在案证据与网络黑灰产犯罪罪量的证明关系发生了变化，我们需要根据多个证据共同拼凑、整合才有可能综合认定罪量。此外，随着网络黑灰产犯罪的发展，网络黑灰产犯罪的被害人教义学也出现了新的课题：一是网络黑灰产犯罪被害人的公共化，与传统犯罪被害人遭受的单一、巨大损害不同，网络黑灰产犯罪的被害人遭受的往往是群体性的、分散化的损害，呈现“海量行为”“微量损失”的特征。89 二是网络黑灰产犯罪被害人行为的虚无化，在电信网络诈骗案件中，行为人从被害人处骗取了网络银行帐号与密码、第三方支付平台帐号、密码或验证码，被害人并未直接处分财产，处分事实缺失；在调换二维码案件中，行为人偷换二维码进行收款，被害人的损失是应得财产，而没有对既有财产进行处分，缺乏处分意思。90 这些新课题的诞生，无疑又增加了网络黑灰产犯罪罪量司法证明的难度。除了上开从指导性案例中读解出的网络黑灰产犯罪罪量的司法证明方法，我们有些基层法院、检察院自生自发地进行摸索和改革，尝试运用社会科学方法，如抽样取证、等约计量与计量模型，对网络黑灰产犯罪的罪量进行证明。91 对此，我们要持开放的态度，但又要秉持刑事法学骨子里的“谦抑”与“保守”，对之进行审慎地观察、读解与反思。

总之，面对日益猖獗的网络黑灰产犯罪，我们在惩罚犯罪的同时，勿忘坚守保障人权的程序正义理念。但对网络黑灰产犯罪的罪量进行计量、核实与认定存在着客观不能时，运用上述指导性案例所揭示的证明方法不啻为一种最不坏的选择。毕竟，“就像蝴蝶飞不过沧海，没有谁忍心责怪”92。

注释

[1]百度时代网络技术(北京)有限公司：《2020 网络黑灰产犯罪研究报告》，百度网 https://baijiahao.baidu.com/s?id=1682519628280453846&wfr=spider&for=pc，最后访问日期：2020 年 11 月 5 日。

[2]同前注[1]。

[3]罗猛、邓超：《从精确计量到等约计量：犯罪对象海量化下数额认定的困境及因应》，《预防青少年犯罪研究》2016 年第 2 期。

[4]参见最高人民检察院法律政策研究室编：《网络犯罪指导性案例实务指引》，中国检察出版社 2018 年版，第 21 页。

[5]徐然等：《网络犯罪刑事政策的取舍与重构》，中国检察出版社 2017 年版，第 122 页。

[6]参见[美]Marjie T.Britz：《计算机取证与网络犯罪导论》，戴鹏等译，电子工业出版社 2016 年版，第 5 页。

[7]参见胡云腾主编：《网络犯罪刑事诉讼程序意见暨相关司法解释理解与适用》,人民法院出版社 2014 年版,第 9 页。
[8]参见喻海松：《网络犯罪二十讲》,法律出版社 2018 年版,第 10-11 页。
[9]陈兴良：《规范刑法学》(教学版),中国人民大学出版社 2018 年版,第 91 页。
[10]同前注[9],第 91-95 页。
[11]参见马忠红：《论网络犯罪案件中的抽样取证--以电信诈骗犯罪为切入点》,《中国人民公安大学学报》(社会科学版)2018 年第 6 期。
[12]同前注[8],第 186 页。
[13]参见高艳东：《网络犯罪定量证明标准的优化路径：从印证论到综合认定》,《中国刑事法杂志》2019 年第 1 期。
[14]张平寿：《网络犯罪计量对象海量化的刑事规制》,《政治与法律》2020 年第 1 期。
[15]同前注[3]。
[16]参见陈瑞华：《刑事证据法的理论问题》,法律出版社 2018 年版,第 228 页。
[17]参见陈瑞华：《刑事证据法》,北京大学出版社 2018 年版,第 156 页。
[18]同前注[14]。
[19]同前注[14]。
[20]参见刘品新：《网络犯罪证明简化论》,《中国刑事法杂志》2017 年第 6 期。
[21]同前注[13]。
[22]参见何邦武：《小额多笔网络电信售假和诈骗犯罪取证问题研究》,《政治与法律》2016 年第 8 期。
[23]参见何邦武：《“综合认定”的应然解读与实践进路》,《河北法学》2019 年第 8 期。
[24]参见白建军：《少一点“我认为”,多一点“我发现”》,《北京大学学报》(哲学社会科学版)2008 年第 1 期。
[25]参见陈瑞华：《从经验到理论的法学研究方法》,《中国法律评论》2019 年第 2 期。
[26]同前注[4],第 21 页。
[27]参见李荣耕：《数位时代中的搜索扣押》,元照出版公司 2020 年版,序言。
[28]第 20 条：“对针对或者组织、教唆、帮助不特定多数人实施的网络犯罪案件,确因客观条件限制无法逐一收集相关言词证据的,可以根据记录被害人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实的电子数据、书证等证据材料,在慎重审查被告人及其辩护人所提辩解、辩护意见的基础上,综合全案证据材料,对相关犯罪事实作出认定。”
[29]同前注[8],第 187 页。
[30]第 2 条第 4 项：“因犯罪嫌疑人、被告人故意隐匿、毁灭证据等原因,致拨打电话次数、发送信息条数的证据难以收集的,可以根据经查证属实的日拨打人次数、日发送信息条数,结合犯罪嫌疑人、被告人实施犯罪的时间、犯罪嫌疑人、被告人的供述等相关证据,综合予以认定。”
[31]第 6 条第 1 项：“办理电信网络诈骗案件,确因被害人人数众多等客观条件的限制,无法逐一收集被害人陈述的,可以结合已收集的被害人陈述,以及经查证属实的银行账户交易记录、第三方支付结算账户交易记录、通话记录、电子数据等证据,综合认定被害人人数及诈骗资金数额等犯罪事实。”
[32]公诉方指控：2013 年 11 月底至 2014 年 6 月间,被告人郭明升为谋取非法利益,伙同被告人孙淑标、郭明锋在未经三星(中国)投资有限公司授权许可的情况下,从他人处批发假冒三星手机裸机及配件进行组装,利用其在淘宝网上开设的“三星数码专柜”网

店进行“正品行货”宣传,并以明显低于市场价格公开对外销售,共计销售假冒的三星手机 20000 余部,销售金额 2000 余万元,非法获利 200 余万元,应当以假冒注册商标罪追究其刑事责任。

[33]郭明升、郭明锋、孙淑标假冒注册商标案,最高人民法院指导案例 87 号(2017 年)。

[34]参见姜瀛:《网络假冒注册商标犯罪中被告人“刷单”辩解的证明模式和证明标准--以第 87 号指导案例及相关案例为分析对象》,《政治与法律》2017 年第 9 期。

[35]被告人张凯闵等 52 人于 2015 年 6 月至 2016 年 4 月间,先后在印度尼西亚和肯尼亚参加对中国大陆居民进行电信网络诈骗的犯罪集团。在实施电信网络诈骗过程中,各被告人分工合作,其中部分被告人负责利用电信网络技术手段对大陆居民的手机和座机电话进行语音群呼,群呼的主要内容为“有快递未签收,经查询还有护照签证即将过期,将被限制出境管制,身份信息可能遭泄露”等。当被害人按照语音内容操作后,电话会自动接通冒充快递公司客服人员的一线话务员。一线话务员以帮助被害人报案为由,在被害人不挂断电话时,将电话转接至冒充公安局办案人员的二线话务员。二线话务员向被害人谎称“因泄露的个人信息被用于犯罪活动,需对被害人资金流向进行调查”,欺骗被害人转账、汇款至指定账户。如果被害人对二线话务员的说法仍有怀疑,二线话务员会将电话转给冒充检察官的三线话务员继续实施诈骗。至案发,张凯闵等被告人骗取 75 名被害人钱款共计人民币 2300 余万元。参见最高人民检察院第一检察厅编:《最高人民检察院第十八批指导性案例适用指引(电信网络犯罪)》,中国检察出版社 2020 年版,第 99 页。

[36]参见张凯闵等 52 人电信网络诈骗案,最高人民检察院指导性案例第 67 号(2020 年)。

[37]区别于普通电信网络诈骗通常是点对点的打款方式,“杀鱼盘”被害人的钱款并非直接打入被告人的账户中,而是购买了电商平台的电子购物卡。在这类案件中,被告人提供的钓鱼网站链接打开后,与真实的二手购物平台网站极其相似,被害人难以分辨。但点击付款后,钓鱼网站则会通过事先抓取的接口链接到某购物平台,被害人的付款会被用于购买该购物平台的购物卡。通过核查被告人与被害人的聊天记录、诈骗团伙上下线之间的聊天记录、被拉黑的被害人账号以及被告人的购物平台账号的订单等信息,承办检察官核实到 400 余名被害人。

[38]参见王伟:《不要落入二手交易平台“杀鱼盘”陷阱》,中国法院网 https://www.chinacourt.org/article/detail/2020/07/id/5376222.shtml,最后访问日期:2020 年 11 月 5 日。

[39]起诉书指控:2014 年 4 月,被告人董志超为谋取市场竞争优势,雇佣被告人谢文浩,多次以同一账号大量购买北京智齿数汇科技有限公司南京分公司淘宝网店铺的商品,致使该公司店铺被淘宝公司认定为虚假交易刷销量,并对其搜索降权。因消费者在数日内无法通过淘宝网搜索栏搜索到智齿科技南京公司淘宝网店铺的商品,严重影响该公司正常经营。经审计,智齿科技南京公司因被搜索降权,影响经营而产生的经济损失为人民币 159844.29 元。

[40]江苏省南京市雨花台区人民检察院诉董志超、谢文浩破坏生产经营案,《最高人民法院公报》2018 年第 8 期。

[41]2014 年 10 月 20 日,被告人李丙龙冒充某知名网站工作人员,采取伪造该网站公司营业执照等方式,骗取该网站注册服务提供商信任,获取网站域名解析服务管理权限。10 月 21 日,李丙龙通过其在域名解析服务网站平台注册的账号,利用该平台相关功能自动生成了该知名网站二级子域名部分 DNS 解析列表,修改该网站子域名的 IP 指向,使其连接至自己租用境外虚拟服务器建立的赌博网站广告发布页面。当日 19 时许,李丙龙

对该网站域名解析服务器指向的修改生效,致使该网站不能正常运行。23 时许,该知名网站经技术排查恢复了网站正常运行。
[42]同前注[4],第 24 页。
[43]李丙龙破坏计算机信息系统案,最高人民检察院指导性案例第 33 号(2017 年)。
[44]被害人陈某于 2009 年 5 月在大连市西岗区登录网络域名注册网站,以人民币 11.85 万元竞拍取得“www.8.cc”域名,并交由域名维护公司维护。被告人张四毛预谋窃取陈某拥有的域名“www.8.cc”,其先利用技术手段破解该域名所绑定的邮箱密码,后将该网络域名转移绑定到自己的邮箱上。2010 年 8 月 6 日,张四毛将该域名从原有的维护公司转移到自己在另一网络公司申请的 ID 上,又于 2011 年 3 月 16 日将该网络域名再次转移到张四毛冒用“龙嫦”身份申请的 ID 上,并更换绑定邮箱。2011 年 6 月,张四毛在网上域名交易平台将网络域名“www.8.cc”以人民币 12.5 万元出售给李某。
[45]张四毛盗窃案,最高人民检察院指导性案例第 37 号(2017 年)。
[46]参见杨勇传播淫秽物品牟利案,载最高人民法院刑事审判第一、二、三、四、五庭主办:《刑事审判参考》(总第 81 集),法律出版社 2011 年版,第 723 号。
[47]2016 年 10 月至 2018 年 5 月期间,被告人王某琼利用能够通过二级密码登陆进入辽宁省工商行政管理一体化办公系统的便利条件,使用抓取软件,从该系统中批量获取企业工商登记信息共计 219124 条,扣除重复信息及无电话信息后约为 206701 条。王某琼将其中 10 万余条信息经过处理后通过 QQ、微信等网络形式贩卖给被告人张某,获利 16300 元。2017 年 4 月至 2018 年 5 月 3 日间,张某将从王某琼等处购得的工商登记信息中的 131732 条通过 QQ 网络平台贩卖给被告人孙某桓,被告人张某从中获利 12270 元。被告人孙某桓将从被告人张某处购买的上述信息除用作自己 POSS 机销售联系使用外,于 2018 年 2 月 23 日、2018 年 5 月 2 日两次将上述信息中的两万余条卖给于某,获利 600 元。参见王某琼等侵犯个人信息案,辽宁省沈阳经济技术开发区人民法院刑事判决书,(2018)辽 0191 刑初 418 号。
[48]参见蔡云:《公民个人信息的司法内涵》,《人民司法》2020 年第 2 期。
[49]同前注[16],第 476-479 页。
[50]参见褚福民:《刑事推定的基本理论--以中国问题为中心的理论阐释》,中国人民大学出版社 2012 年版,第 13 页。
[51]一般又将法律推定区分为可以反驳的法律推定与不可反驳的法律推定。参见张海燕:《实体与程序双重视角下的民事推定》,法律出版社 2020 年版,第 23-31 页。
[52]参见黄永:《证明责任分配基本理论:以刑事诉讼为参照的研究》,中国法制出版社 2019 年版,第 288-294 页。
[53]参见[德]莱奥·罗森贝克:《证明责任论》,庄敬华译,中国法制出版社 2018 年版,第 253-254 页。
[54]参见何家弘:《司法证明方法与推定规则》,法律出版社 2018 年版,第 208 页。
[55]同前注[17],第 504-505 页。
[56]同前注[54],第 286 页。
[57]同前注[52],第 295 页。
[58]同前注[53],第 254 页。
[59]同前注[50],第 83-85 页。
[60]同前注[54],第 268 页。
[61]同前注[17],第 443-448 页。

[62]第 7 条第 2 项：“确因客观原因无法查实全部被害人,但有证据证明该账户系用于电信网络诈骗犯罪,且被告人无法说明款项合法来源的,根据《刑法》第六十四条的规定,应认定为违法所得,予以追缴。”
[63]同前注[33]。
[64]同前注[20]。
[65]同前注[34]。
[66]董志超的辩护人在一审时提出,对被害单位损失数额的审计结果过高。在上诉时提出,案件尚未达到此罪刑事立案标准；涉案损失鉴定意见依据审计报告不属于鉴定意见,属于书证,且存在取材错误、论证混乱等问题,无其他证据印证,应不予认定。
[67]同前注[40]。
[68]北京市西城区检察院以被告人罗刚等犯传播淫秽物品牟利罪,向西城区法院提起公诉,指控四名被告人在北京轻点万维电信技术有限公司工作期间于 2007 年 1 月 1 日至 5 月 9 日共上传 28 张淫秽图片,点击率达 253335 次,情节特别严重,应处 10 年以上有期徒刑或无期徒刑,并处罚金或没收财产。
[69]参见罗刚等传播淫秽物品牟利案,载最高人民法院刑事审判第一、二、三、四、五庭主办：《刑事审判参考》(总第 78 集),法律出版社 2011 年版,第 669 页。
[70]同前注[46]。
[71]公诉方指控王某琼非法获取个人信息 219124 条；电子证据检查笔录显示侦查机关从王某琼处扣押的台式机电脑 E 盘共提取涉企业及法人信息 219124 条。
[72]第 11 条第 3 款：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。
[73]同前注[20]。
[74]同前注[47]。
[75]同前注[17],第 517-521 页。
[76]同前注[52],第 262 页。
[77]参见姜世明：《举证责任与证明度》,厦门大学出版社 2017 年版,第 40 页。
[78]同前注[17],第 441-443 页。
[79]所谓“表见证明”,是指法院基于由一般生活经验而推得的典型事象经过,由某一定客观存在事实(不争执或已得完全确信者),而推断另一于裁判具重要性待证事实的证据提出过程。同前注[77],第 207-208 页。
[80]同前注[52],第 306 页。
[81]同前注[54],第 287-288 页。
[82]同前注[17],第 522-523 页。
[83]同前注[34]。
[84]同前注[17],第 521-523 页。
[85]同前注[48]。
[86]同前注[36]。
[87]同前注[50],第 85 页。
[88][瑞士]索朗热·戈尔纳奥提：《网络的力量：网络空间中的犯罪、冲突与安全》,王标等译,北京大学出版社 2018 年版,第 14 页。
[89]参见皮勇：《论新型网络犯罪立法及其适用》,《中国社会科学》2018 年第 10 期。
[90]参见王肃之：《网络犯罪原理》,人民法院出版社 2019 年版,第 253-270 页。

[91]参见万毅、纵博：《论刑事诉讼中的抽样取证》,《江苏行政学院学报》2014 年第 4 期；刘品新：《印证与概率：电子证据的客观化采信》,《环球法律评论》2017 年第 4 期。
[92]林夕：《蝴蝶》,王菲演唱,Adrian Chan 作曲,1999 年。

3.网络黑灰产上游犯罪的刑法规制

刘宪权华东政法大学
来源《国家检察官学院学报》
摘　要：
网络黑灰产业链中常见的上游行为主要有侵犯信息与虚假流量两类。利用能够规避或突破网络安全防护系统的软件技术侵犯公民个人信息的行为可能构成非法获取计算机信息系统数据罪与侵犯公民个人信息罪的想象竞合,而利用破坏性程序软件虚假注册的行为则可能构成破坏计算机信息系统罪。现行刑法无法对恶意注册行为进行有效规制,应通过刑事立法增设“妨害信息网络管理秩序罪”,以保护包括互联网实名制在内的信息网络管理秩序。实践中可以以“大于半数规则”作为量化标准推定网络中立业务平台在帮助信息网络犯罪活动行为中“明知”的成立。刑法应当密切关注人工智能技术与网络黑灰产犯罪结合带来的破坏。
关键词：网络黑灰产;上游犯罪;网络爬虫;恶意注册;中立平台;人工智能;
一、网络黑灰产的产生与研究的展开
“这是最好的时代，也是最坏的时代”，如今我们所处的网络信息时代或大数据时代、人工智能时代，可以用狄更斯在《双城记》开篇的第一句话加以完美诠释。所谓“最好的时代”，集中体现在网络信息技术给人类的生产生活带来了前所未有的便利与飞跃；所谓“最坏的时代”，则主要说明信息智能革命可能使一部分不法分子有机会利用网络的虚拟性和先进技术的不易察觉性实施违法犯罪活动。应该看到，近年来随着互联网新技术的不断进步，新型网络犯罪层出不穷，犯罪手段不断升级，犯罪行为人之间的分工逐渐细化，形成了上、下游相互协作的链条化模式，“网络黑灰产”应运而生。
（一）网络黑灰产的界定
网络黑灰产源于网络犯罪，但又不同于传统网络犯罪。这是由于黑灰产中既有“黑”的部分也有“灰”的部分。我们经常将“黑”理解为违法犯罪行为，将“灰”理解为游走于违法犯罪边缘但在立法上却没有明确规定的一些行为。在互联网技术层出不穷的背景下，将合法的技术运用在非法的目标上，或者为配合下游犯罪而准备工具、制造条件的一些尚不能以犯罪追究的上游行为则构成了网络黑灰产的主要表现形式。“黑灰”可以理解为处于罪与非罪交界的行为性质，而“网络黑灰产”也可以理解为互联网技术和网络违法犯罪相结合的相关产业。
应该看到，网络黑灰产的发展和互联网行业的发展方向密不可分，而网络黑灰产的模式则是由互联网经济模式决定的。互联网经济的发展经历了三个重要阶段，即从重视服务器和硬件的生产到对电脑的普及，再从对电脑的普及到对网站、系统和软件的推广，最后从网站、系统和软件的推广到对点击和流量的重视。1 而正因如此，当今互联网发展已经从开始的计算机巨头的一对多服务模式发展到了如今人人参与、互通共享的模式。个体的参与构成了当今互联网经济的主要标志，这也给网络黑灰产的滋生创造了环境条件。

当今互联网经济模式可以总结归纳为两点，第一是对流量的重视，即任何一个软件、网站、搜索引擎或者系统，对其使用或者浏览的人越多，经济价值便越大；第二是对精准需求的重视，一个产品或者网站光有流量还不够，还需要进一步明白什么人需要什么，这样便可以顺利将用户需求和产品进行直接对接，大大提高了交易的可能性。这是当前所有互联网公司发展的两个共同目标趋向，但是，怎样才能提升知名度增加用户数量，怎样做到对于用户需求的精准对接则无规则和习惯的定数，市场在这方面将永远走在法律的前面。因此围绕着这两大核心需求的争夺必将导致不正当竞争行为的出现，而当今网络黑灰产的主要产业链也正是在这两点基础上形成的。

至此，我们可以将“网络黑灰产”定义为：以虚拟网络空间为场所，以中立性技术为依靠，以谋取不正当利益为动机，以非犯罪技术或行为为表象，以实施违法犯罪行为为实质的社会分工组织形式。

（二）网络黑灰产相关刑法理论的展开

根据 2018 年南都大数据研究院和阿里巴巴集团安全部联合发布的《2018 网络黑灰产治理研究报告》、2019 年百度与公安部第三研究所网络安全法律研究中心联合发布的《网络犯罪防范治理研究报告》以及 2020 年百度时代网络技术有限公司和公安部第三研究所网络安全法律研究中心联合发布的《2020 网络黑灰产犯罪研究报告》，实践中普遍认为网络黑灰产中存在上、中、下游犯罪，其中上游是为相关犯罪提供或准备工具，中游是针对网络系统和软件的直接破坏以及对公民个人信息的侵犯，下游则是对上中游行为的结果实施如诈骗、赌博、洗钱等相关传统犯罪。通过对比分析，笔者认为网络黑灰产上游和中游行为本质上都是准备行为或手段行为，下游行为才是最终目的行为。因此，网络黑灰产的产业链或者说网络黑灰产犯罪链的结构可以归纳为两条，即上游的手段链和下游的目的链，上下游的结合构成了网络黑灰产业链。

不难看出，现有上游网络黑灰产技术及其作用范围准确对应者互联网市场经济的价值导向，即所有网络黑灰产主要都是针对流量提升和用户需求精准对接而衍生的。以上游网络黑灰产对刑法所保护法益的直接侵犯作为区分标准，笔者将网络黑灰产上游犯罪活动分为信息类网络黑灰产和流量类（包括账号类）网络黑灰产。其中信息类网络黑灰产（包括非法买卖个人信息、涉物联网犯罪、盗号类等产业）直接侵犯的是公民的个人信息权，即它们都是通过非法掌握用户详细信息，以更加精准实施产品推销或违法犯罪活动的相关产业。流量类网络黑灰产（包括恶意注册、虚假注册、网络水军、恶意点击、DDo S 攻击、黑 SEO、暗网等产业）直接侵犯的是网络市场经济管理秩序，即为了增加自身用户流量或减少竞争对手的用户流量而衍生的相关产业。而下游目的链行为则是上游手段链行为的对应目标，是对上游行为“成果”经济价值的转化，既可以是正当的市场经营行为，也可以是诈骗、赌博、洗钱等违法犯罪行为。

就此看来，网络黑灰产之所以有别于网络犯罪而被称为“黑灰”产业，主要原因在于我们重点关注的是其上游行为，而并非其下游行为。这一方面是因为下游目的链既可表现为传统的违法犯罪行为也可表现为合法的市场经济行为，而上游的手段链则普遍是以“黑灰”等违法犯罪技术对公民个人信息侵犯和对网络市场经济管理秩序进行破坏为行为模式的。另一方面，不可否认的一个基本事实是，网络犯罪因为链条长，上、下游勾结隐蔽，发现和斩断整个网络黑灰产业利益和共同犯罪链条是非常困难的，因此通过共同犯罪的方法打击上游犯罪行为本身存在相当大的挑战。2 正因为上游的网络黑灰产手段链是网络黑灰产的关键性环节，且在司法实务中通过认定共同犯罪对网络黑灰产上游犯罪予以刑事规制具有一定的困难性，所以其理应成为新业态下网络黑灰产研究的重点。

二、网络黑灰产上游犯罪的刑法适用

随着互联网新技术在经济活动和社会生活中的不断渗透，诈骗、盗窃、赌博等诸多传统犯罪成为网络黑灰产业链中的下游犯罪，并在互联网平台的助力下呈现爆发式增长。需要指出的是，为了更有效且隐蔽地为上述网络黑灰产中的下游犯罪提供帮助，网络黑灰产中的上游犯罪手段也在持续升级，即诸多新类型的上游犯罪形式层出不穷、屡见不鲜。如前文所述，信息和账号是网络用户赖以生存的基础，为精准对接用户需求而衍生的网络黑灰产上游犯罪本质上是对个人信息的侵害，以提升流量为核心的网络黑灰产上游犯罪则是对网络账号的滥用。笔者将网络犯罪上游黑灰产犯罪总结为信息类黑灰产和流量类黑灰产两类，由此，我们完全有必要针对这两类黑灰产业中相关行为的刑事规制问题展开研究。

（一）网络信息类黑灰产相关行为的刑法适用

大数据时代下，个人信息数据的泄露随处可见，无论是快递、外卖包装上的姓名、联系电话、家庭住址等，还是各类网站以及电脑、手机软件强制个人授权信息的登录认证，都在无形中助长个人信息数据的泄漏势头，而垃圾短信、骚扰电话的泛滥更是让人们对于信息的泄漏司空见惯，却又无能为力。根据中国互联网络信息中心 2020 年 9 月发布的第 46 次《中国互联网络发展状况统计报告》的数据显示，截止至 2020 年 6 月，遭遇个人信息泄漏的网民占比高达 20.4%，并且有 17%的网民表示曾经遭遇过网络诈骗。

在涉及非法使用个人信息的黑灰产业链的上游，犯罪分子对个人信息数据进行非法收集、处理与加工，并进行违规买卖与交换；在黑灰产业链的下游，犯罪分子利用非法获取的个人信息数据进行“精准”网络诈骗、敲诈勒索以及冒用信用卡的信用卡诈骗等诸多犯罪活动。从中我们不难看出，个人信息的泄漏正是黑灰产业链中从事诸多后续犯罪行为的源头，甚至可谓是网络黑灰产业结构的核心。

2014 年“京东撞库事件”正是由于不法分子通过部分具有信息安全隐患的网站获取用户信息，使用“撞库”方式在其他具有交易属性的电商、互联网金融等网站尝试登录并获取了用户的商品购买信息。32020 年 4 月公安部公布了 10 起关于侵犯公民个人信息的违法犯罪案例典型，其中就有 1 例涉及“黑客”入侵的技术攻击，行为人利用暴力破解手段非法获取了涉案网站的后台管理权限，从而盗取大规模公民个人信息并予以出售。4 所有这些都足以说明，随着网络技术的蓬勃发展，黑灰产上游犯罪中针对个人信息的窃取手段也在不断升级，不再局限于传统的人为泄漏与盗卖，而是发展为包括“撞库”软件、木马病毒程序、“网络爬虫”技术等在内的诸多系统性的技术攻击手段。

实践中，通过“撞库”技术侵入计算机信息系统并获取相关信息的犯罪行为时有发生。2016 年，被告人曹某开办“精品客栈”网站，将其开发的“冻结分类查询助手”与“无保回收查询助手”等验密软件置于该网站供他人免费下载。上述软件可通过批量导入 QQ 账号与密码数据，绕过腾讯系统的安全策略，实施“撞库”验密。同年，被告人曾某购买大量 QQ 账号和密码，使用上述软件辨别购买所得的账号是否被腾讯公司冻结，并出售没有被冻结、具备正常使用功能的账号，法院判决曹某与曾某分别构成提供侵入、非法控制计算机信息系统程序、工具罪与侵犯公民个人信息罪。52018 年 11 月至 2019 年 3 月间，被告人沈某编写名为“群发助手”的恶意“撞库”验密系列软件，并出租给他人使用，法院判决沈某构成提供侵入、非法控制计算机信息系统程序、工具罪。6 依笔者所见，从上述“撞库”、木马病毒等程序软件的使用功能来看，这些程序软件包含一定的规避或突破网络安全防护系统的技术，即通过绕过或破解计算机系统的安全防护措施，从而获取计算机系统数据。由于这些软件均“具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权获取计算机信息系统数据的功能”7，

所以我们可以将它们归入刑法第 285 条第 3 款规定“专门用于侵入、非法控制计算机信息系统的程序、工具”范围之中。就此而言，行为人开发上述软件，并提供给他人的行为，情节严重的，应当构成提供侵入、非法控制计算机信息系统程序、工具罪。根据 2011 年 8 月 1 日“两高”《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《信息系统安全解释》）第 3 条的规定，该罪的入罪标准为提供专门性程序、工具 5 人次或 20 人次以上，8 或违法所得 5000 元以上，或造成经济损失 1 万元以上，或其他情节严重的情形。由此可知，即使行为人开发上述软件后免费供人下载使用，只要其提供的人次达到 5 人次或 20 人次以上的，即可构成该罪；若行为人出租或出售其开发的相关软件或向软件使用人收取任何其他名义的费用，违法所得 5000 元以上的，即可构成该罪。

“网络爬虫”技术则与前述“撞库”软件、木马病毒程序稍有不同。“网络爬虫”（web crawler）是一项常见的数据抓取技术，常用于搜索引擎领域对站点进行爬取收录，如谷歌、百度、必应等搜索引擎通常都使用“网络”爬虫技术获取数据资源。该数据抓取技术按照一定的规则，自动抓取万维网的信息或者脚本。“网络爬虫”技术的有效使用有利于数据的共享和分析，也就是说“网络爬虫”技术本质上是一项中立技术，与前述的木马病毒、“撞库”软件不同的是，其一般不具有天然的违法性。一项中立的技术最终是被用于合法抑或是非法途径，无法被技术的开发者预见或控制。因此，开发并提供“网络爬虫”技术程序的行为也并不像开发“撞库”软件、木马病毒等程序软件的行为一样，当然构成提供侵入计算机信息系统程序、工具罪。但是，作为一项中立技术，“网络爬虫”技术应当在法律框架里有其使用边界，如果突破这一边界就可能存在刑事风险。

在全国首例“网络爬虫案”中，被告单位与被告人破解了北京字节跳动网络技术有限公司的防抓取措施，使用名为“tt__spider”文件的一种网络数据抓取工具，对涉案网站服务器实施数据抓取行为，最终法院判决以非法获取计算机信息系统数据罪对被告单位及被告人定罪处罚。9 理论上，有学者认为，网络数据爬取行为只有在对方设置的 Robots 协议或被爬取的数据用于不正当竞争的情形下，造成对方实际损失的，才具备刑事可罚性。10 也有学者认为，数据的访问权限和开发程度这两个维度形成了网络爬虫的归责体系，只有在网络爬虫行为同时具备行为不法（故意避开或强行突破网站技术措施）与对象不法（抓取限制访问、获取的数据）的情况下，才需承担刑事责任。11

可见，对中立性技术的使用有其不可触碰或逾越的法律红线。在“网络爬虫”技术的数据抓取过程中，如果其采取的技术手段规避或突破了计算机信息系统有关反“爬虫”的安防措施，未经许可进入计算机信息系统，从而抓取限制访问的计算机信息系统数据，那么该“爬虫”技术的中立性已经消失殆尽，丧失了因技术中立而豁免责任的可能性。此时的“网络爬虫”技术同前述“撞库”软件一样，均“具有避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权获取计算机信息系统数据的功能”，对其刑法规制应当与对“撞库软件”、木马病毒程序等程序、软件的刑法规制一致。

同时，在行为人使用上述软件程序窃取个人信息的犯罪行为中，利用相关软件程序获取数据的手段不法行为可能构成非法获取计算机信息系统数据罪，非法获取公民个人信息（《信息系统安全解释》第 1 条第 1、2 款所称“身份认证信息”，包括账号、口令、密码、数字证书等，属于公民个人信息范畴）的结果不法行为则可能构成侵犯公民个人信息罪。有学者认为，《刑法》第 253 条之一的侵犯公民个人信息罪和第 285 条第 2 款的非法获取计算机信息系统数据罪是法条竞合关系，公民个人信息也是数据

的一种，只不过我国《刑法》第 253 条之一对个人信息数据予以特别保护。12 笔者对此不能苟同。诚然，仅从犯罪对象的层面看，由于公民个人信息是数据的一种，侵犯公民个人信息罪的对象范围可以被非法获取计算机信息系统数据罪包含。但因犯罪对象形成的法条竞合的适用前提应当是两罪的手段行为保持范围一致，或者侵犯公民个人信息罪的手段行为同样可以为非法获取计算机信息系统罪所包含。然而，侵犯公民个人信息罪的犯罪手段显然较非法获取计算机信息系统数据罪范围更广，因此两罪的构成要件并不存在包含与被包含的关系，两罪属于部分重合的交叉关系，当然不能构成法条竞合。如果将这种所谓的“交叉式”型法条竞合同样认定为法条竞合，将会模糊法条竞合（单纯的一罪）同想象竞合犯（科处的一罪）之间的界限。此时，仅适用一个法条要么不能全面保护法益（两个法条的保护法益不同），要么不能全面评价行为的不法内容（虽然侵害相同法益，但不法内容存在区别）。13 依笔者之见，行为人使用上述软件程序，避开或者突破计算机信息系统安全保护措施，未经授权或者超越授权获取计算机信息系统数据中公民个人信息的行为，同时触犯了非法获取计算机信息系统数据罪与侵犯公民个人信息罪，属于一行为触犯数罪名的想象竞合犯，对其应当以“从一重罪处断”的处罚原则处理。由于刑法中对两罪的法定刑规定完全一致，笔者认为，以更能体现行为结果不法与犯罪最终目的的侵犯公民个人信息罪定罪处罚最为合适。

（二）网络流量类黑灰产相关行为的刑法适用

近年来，网络直播、短视频行业的异军突起使流量具备了巨大的商业利益。包括“小红书”“阿里本地生活”在内的诸多内容平台都对虚假流量问题进行过大规模整治。根据“小红书”反作弊中心公布的数据，仅 2019 年该平台就封禁了涉黑产账号 2182 万，拦截了黑产作弊行为超过 14 亿次。14 与此同时，电商平台的兴起也催生了包括网络正向刷单（虚构交易量以提高商户信誉）与网络反向炒信刷单（恶意交易与差评以损害商户信誉）在内的电商刷单产业。上述新兴的有关虚假流量的网络黑灰产业无一不以行为人掌握大量网络账号为前提，因而均离不开网络黑灰产的源头之一——互联网账号的恶意注册。

2018 年 12 月，腾讯公司于“互联网账号恶意注册黑产治理”论坛发布了首份定向剖析黑产源头的《互联网账号恶意注册黑色产业治理报告》，指出互联网账号恶意注册是指不以正常使用为目的，违反国家规定和平台注册规则，使用虚假或非法取得的身份信息，以手动方式或通过程序、工具自动进行，批量创设网络账号的行为。15 应当看到，根据注册时所使用身份信息的真实与否，恶意注册可以分为使用虚假身份信息创设账号的以及使用非法获取的真实身份信息创设账号的两类，笔者将前者称为虚假注册，将后者称为假冒注册。

在涉及假冒注册的黑灰产业链中，其上游的犯罪行为主要是收集（窃取或其他非法方法获取）后续账号注册所需的真实身份信息，同前文阐述的“侵犯信息类”上游犯罪具有一致性，在此不再赘述。笔者对恶意注册黑灰产业链的探讨主要集中在使用虚假身份信息创设网络账号的虚假注册。以虚假注册为源头或核心的黑灰产业链之下游行为，主要包括“广撒网”式网络诈骗行为，囤积大量账号以采集商家为刺激消费而发放的小额优惠或现金返利的“薅羊毛”诈骗行为，内容平台数据刷量和电商平台刷单炒信等虚假流量行为，以及诸如“黑公关”“网络水军”等的流量明星营销行为等。这些下游行为以高流量为核心、以高盈利为驱动，驱动上游虚假注册行为的肆意发展；上游的虚假注册行为同样为下游的黑灰色产业链提供了源头性的技术支持，助力下游的违法犯罪行为。

实践中，由于虚假注册涉及的账号注册量巨大，行为人通常利用自动化的运行工具以及能够突破相关平台安全保护措施的技术工具进行大批量、自动化的网络账号注册。2018 年 10 月，浙江省兰溪市人民法院对“首例恶意注册账号案”进行了判决。被告人汤某通过网络购买了注册机及 E 语言源代码，改写成名为“畅游注册机.exe”的注册机。经改写后的注册机软件通过设置相应配置，可以实现批量注册程序。具体流程如下：注册机软件可以实现自动产生注册信息并通过第三方平台获取手机号，继而将注册信息及获取的手机号通过数据包方式发送给“畅游”注册平台服务器，借助第三方平台自动将获取的手机验证码发送回“畅游”注册平台，据此完成批量注册程序。法院经审理认为该软件对“畅游”注册平台的正常操作流程和正常运行方式造成了干扰，属于“破坏性程序”，最终判决汤某构成提供侵入、非法控制计算机信息系统、工具罪。16 该案被称为“首例恶意注册账号入刑案”，法院判决认定该案中的犯罪行为是有关恶意注册的手段行为，即通过特定的程序和工具对相关注册平台的正常操作流程和正常运行方式造成干扰的破坏行为。有学者将此类网络攻击的手段行为称为“真正的网络犯罪”，包括非法侵入计算机信息系统罪，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，提供侵入、非法控制计算机信息系统的程序、工具罪，破坏计算机信息系统罪，网络攻击往往被用作实施其他类型网络犯罪的手段行为。17 换言之，该案最终对该恶意程序的开发者、提供人是以提供侵入、非法控制计算机信息系统、工具罪定罪处罚，这就意味着，该案判决似乎认为，当前刑法能够处罚的是网络攻击的手段行为，而非实现行为人最终目的的恶意注册行为，如果没有对相关注册平台的正常操作流程和正常运行方式造成干扰的恶意注册行为则不能入罪。

依笔者所见，开发并提供用以恶意注册的软件是否可以构成提供侵入、非法控制计算机信息系统、工具罪是有待商榷的。实践中，互联网平台为执行《网络安全法》所规定的实名制规则，也为维护用户的账户安全，大多采取了一系列反自动化批量注册与反虚假注册的安全策略和安全防护措施。行为人要想绕过或破解平台的防护措施以达到虚假注册的目的，势必需要通过一定的技术手段对其进行干扰。在司法实务中，包括前述“首例恶意注册账号案”在内的批量注册案中，大多将虚假注册所倚赖的破解技术认定为“破坏性程序”，即该程序会对计算机信息系统功能进行删除或干扰等，造成计算机信息系统不能正常运行。笔者认为这种认定是符合此类虚假注册软件的运行机制的。然而，提供破坏性程序的行为是否可以以提供侵入、非法控制计算机信息系统的程序、工具罪定罪处罚？换言之，提供侵入、非法控制计算机信息系统的程序、工具罪是否可以同时理解为将《刑法》第 286 条破坏计算机信息系统罪的帮助行为正犯化？

笔者认为，刑法中提供侵入计算机信息系统程序、工具罪并不规制提供破坏计算机信息系统的程序、工具的帮助行为，即提供破坏性程序的行为不应当以提供侵入、非法控制计算机信息系统的程序、工具罪定罪处罚。理由是：

首先，提供侵入、非法控制计算机信息系统数据程序、工具罪与破坏计算机信息系统罪所保护的法益有着不同的侧重。《刑法》第 285 条第 2 款的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以及第 3 款的提供侵入、非法控制计算机信息系统程序、工具罪是 2009 年《刑法修正案（七）》新增设的罪名。后罪行为实际上是前者行为的帮助行为，理论上将其称为“帮助行为的正犯化”。前罪重点规制的是侵入计算机系统或采用其他技术手段获取相关数据，或者非法控制计算机信息系统的行为，即强调的是对相关数据的非法获取与对系统的非法控制；后罪中“专门用于侵入、非法控制计算机信息系统的程序、工具”应当是用于对数据的非法获取或者对计算机信息系统的非法控制，而不仅仅是用于对计算机信息系统的侵入。与之不同的是《刑法》

第 286 条第 1 款规定的破坏计算机信息系统罪，该罪强调的是包括删除、修改、增加、干扰计算机信息系统功能在内的、影响计算机系统正常运行的破坏行为。

其次，从《刑法》第 285 条第 3 款提供侵入、非法控制计算机信息系统的程序、工具罪该条文所处的具体位置来看，其位于同条第 2 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之后，与第 286 条破坏计算机信息系统罪分属两个法条，理论上将该条理解为破坏计算机信息系统罪的“帮助行为正犯化”规定实为牵强。

需要指出的是，《刑法》第 286 条第 3 款规定了“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”，而相关司法解释并未将刑法这一款规定设置为独立罪名。这就充分表明，刑法实际上将制作、传播用于破坏计算机信息系统的破坏性程序的准备行为归入破坏计算机信息系统罪之中，以区别于前述有关提供侵入、非法控制计算机信息系统程序、工具的帮助行为正犯化的立法方式。因此，对于故意制作、传播此类破坏性程序行为应当以破坏计算机信息系统罪追究其刑事责任。当然如果这些程序、软件仅以自动化注册技术取代人为的手动注册方式，行为人为提高注册效率，通过模拟人工点击一次性批量注册，而未对计算机信息系统产生干扰且不可能影响到计算机信息系统的正常运行，对行为人的行为则不能以侵害计算机信息系统的相关犯罪认定。

此外，有学者认为，在网络账号恶意注册的黑色产业中，黑产人员利用伪造、变造的居民身份证、护照、社会保障卡、驾驶证等依法可以用于证明身份的证件进行虚假注册，可以构成《刑法》第 280 条之一规定的使用虚假身份证件、盗用身份证件罪 18。笔者对此观点表示质疑。在网络账号虚假注册的过程中，黑灰产上游人员为规避注册平台对于实名制账号的要求，所利用的并非是伪造、变造的身份证件，而只能是虚假的身份信息。刑法中使用虚假身份证件中“身份证件”应当是伪造、变造的居民身份证、护照等虚假实体证件，不应当包括虚假的身份信息。特别是在我国有关电子身份证、“网证 CTID”19 等电子或网络证件的技术尚未全面普及的当下，生活中人们仍然需要通过实物的载体使用相关的身份证件。而且相关司法解释也并未对该概念作任何扩张解释，因此目前从实然的角度，我们不应该随意将“身份证件”的涵义拓展至“身份证件信息”，使用虚假身份证件的行为应当是在现实生活中使用伪造、变造的实体身份证件，而不包括通过互联网等使用虚假的身份信息进行虚假注册账号等行为。

三、网络黑灰产上游犯罪刑法规制的完善

应当看到，新业态下网络黑灰产上游犯罪通过我国现行刑法的相关规定可以在一定程度上进行有效规制，但随着网络信息技术的持续更新与上游犯罪手段的不断更迭，传统刑法已逐渐显露出力有不逮之势。我们有必要对刑法规制黑灰产上游犯罪时存在的难题予以明确，并通过解释论或立法论探寻其应对路径。

（一）增设对恶意注册行为的刑法规制

如前所述，实践中通常以计算机信息系统相关罪名对网络黑色产业链上游中侵犯个人信息与恶意注册的技术手段进行规制。对于侵犯公民个人信息这一目的行为（包括出售、提供、窃取、非法获取等），我国刑法可以通过侵犯公民个人信息罪进行规制，但对于恶意注册这一目的行为或者说核心行为，是否构成犯罪以及构成何种犯罪，刑法理论与实务界皆尚无定论。

在解释论层面，有学者认为，网络恶意注册行为不具备“违反国家规定”的规范构成要素，因而不能构成《刑法》第 255 条非法经营罪，同时认为恶意注册黑产行为具有帮助性质，如果其帮助的对象属于信息网络犯罪活动，则可以构成帮助信息网络犯罪活动罪。20 有学者进一步指出应当对帮助信息网络犯罪活动罪作“去中心化”的解释，以适用网络社会特点。21 还有学者主张通过对破坏生产经营罪进行与时俱进的客观解

释，以涵盖日本刑法中妨害业务罪的内容，并以该罪对恶意注册行为进行规制。22 在立法论层面，则有学者建议在《刑法》第 287 条之一的非法利用信息网络罪中增加一项作为第 4 项，将恶意注册行为纳入其中。23

应当看到，刑法学界普遍认识到了网络黑灰产业链上游的恶意注册行为对网络实名制管理秩序与互联网诚信体系造成的巨大威胁，具有严重的社会危害性和刑法规制的必要性。然而，在我国目前的刑法体系下，恶意注册行为难以受到刑事层面的有效治理。一方面，在目前的刑法体系下，传统罪名如非法经营罪、破坏生产经营罪等罪并不能对恶意注册行为进行合理有效的规制。另一方面，从恶意行为作为帮助行为的角度出发，纵然恶意注册的上游行为客观上为下游犯罪提供了帮助，但在网络黑灰产业链结构中，上下游人员之间关联性极低，通常互不相识，甚至上游人员对下游行为毫不知情，因此无论是试图将恶意注册行为认定为下游网络犯罪的共同犯罪，或是意图以帮助信息网络犯罪活动罪进行定罪处罚，在具体适用上都存在一定的困难。正因为如此，司法实践中通常以计算机信息系统方面的犯罪对恶意注册的手段行为进行惩治，但本质上这种处罚并不是基于侵犯了网络管理秩序的恶意注册行为，而仅仅是对恶意注册相关技术手段的惩治。

因此，在传统罪名打击靠后、新型罪名打击有限的规制困境下，笔者建议在立法层面针对恶意注册行为增设相关罪名，主要可以有以下两条规制路径。其一，由于恶意注册行为的前提与基础在于假冒他人真实的身份信息与创设虚假的身份信息，因此可以从侵犯身份信息的角度对恶意注册行为进行规制。如前所述，我国《刑法》分则第六章第一节扰乱公共秩序所规定的“伪造、变造、买卖身份证件罪”“使用虚假身份证件、盗用身份证件罪”中的“身份证件”在实然层面是指居民身份证、护照等载有身份信息的实体证件。而在“去实体化”的大背景下，身份证件电子化已是大势所趋，是否可以从应然层面，考虑通过立法解释将“身份证件”的涵义拓展为“身份信息”，进而对恶意注册过程中买卖他人真实的身份信息、使用虚假的身份信息、盗用他人的身份信息的行为进行规制。其二，则是可以比照我国刑法对信用卡管理秩序的保护，通过增设全新的“妨害信息网络管理秩序罪”对恶意注册等一系列危害网络实名制管理秩序、侵害网络诚信体系的行为进行规制。两相比较，笔者认为，第二种规制路径更契合恶意注册行为所侵害的法益。尽管目前包括互联网实名制管理秩序在内的信息网络管理秩序还未受到刑事立法者的重视，但随着网络黑灰产业链的不断扩张与信息类、流量类犯罪的持续高发态势，对危害信息网络秩序这一种重要法益的刑事治理工作势在必行。通过增设“妨害信息网络管理秩序罪”不仅可以对一系列新业态下的网络黑灰产犯罪行为进行规制，还可以对未来可能出现的危害网络管理秩序的新型犯罪手段进行前瞻性的规定。当然，如何避免该罪沦为互联网信息时代的“口袋罪”也是立法者在罪名设置时不得不考量的问题。

（二）明确网络中立业务服务平台的刑事责任边界

网络黑灰产业链中上游源头行为的开展与进行离不开互联网平台的助力，如前述恶意注册过程中用以提供短信验证码或语音验证码的接码（接收验证码）平台，非法获取的他人个人信息、黑账号等的流转售卖平台，以及黑灰产业链中各环节人员用以互相联络的通讯群组与隐蔽论坛等，都在网络黑灰产业链中起着无可取代的重要作用。

在刑法规制上，对于专门设立用于实施违法犯罪活动的通讯群组、隐蔽论坛、网站等行为，以《刑法修正案（九）》新增的非法利用信息网络罪进行规制应当在实践与理论上均没有任何障碍。然而对于并非设立专门用于违法犯罪活动，但客观上为犯罪行为提供了技术支持与帮助的中立业务服务平台，在没有明确证据证明技术支持提供者在主观上与犯罪实行人存在共谋或放任，还是在不知情的情况下被犯罪实行人所滥用，

此时的帮助行为只能属于法律属性不明的灰色地带。如何兼顾对网络犯罪活动的严厉打击与对信息网络中立技术进行刑事处罚的谨慎克制，明确网络中立业务服务平台的刑事责任边界，是刑法目前亟需解决的问题。

在 2015 年《刑法修正案（九）》增设拒不履行信息网络安全管理义务罪、帮助信息网络犯罪活动罪等罪之前，著名的“快播案”经由北京市海淀区人民法院初审、北京市第一中级人民法院二审，最终以传播淫秽物品牟利罪这一传统犯罪对快播公司及吴某等主管人员定罪处罚。二审过程中，辩护人曾提出辩护意见，称“快播公司只是提供了一种技术模式，法院审判的不应是技术，而应是行为”。对此，法院认为，一方面，快播公司可通过积极作为的方式由自主选择如何设定技术服务规则。正是由于平台向所有用户免费提供资源服务器程序及快播播放器程序，并对上传视频资源的用户及视频内容均不做任何限制，才造成大量淫秽视频存储于快播缓存服务器中并通过其更快速地在网络上传播。另一方面，其怠于履行网络安全义务的消极不作为导致了淫秽视频在快播网络上长时间的大量传播。24 学界有相当一部分学者对该案的判决结果表示质疑，当时的争论焦点主要集中在将拒不履行网络管理义务的不作为评判为传播淫秽物品牟利罪的作为犯合理与否以及中立技术可否作为法律责任的豁免事由。25

依笔者之见，网络业务平台具有中立特性毋庸置疑，“法院审判的不应是技术”同样无可厚非。由于网络中立业务服务平台无差别地向不特定的社会大众提供技术服务，信息网络技术又天然地具有被犯罪分子利用从事犯罪行为的风险，因此网络平台提供的技术服务很有可能在客观上为犯罪行为提供了信息网络支持，帮助了犯罪的实行行为。譬如“快播”平台免费提供的资源服务器程序客观上帮助了淫秽视频的广泛传播；“暗网”平台 26 客观上为网络黑灰产上游犯罪中公民个人信息的出售与买卖行为提供了交易场所；有关技术论坛客观上对影响计算机系统正常运行的破坏性程序或是专门用于侵入计算机信息系统的程序等工具软件进行了传播。由于网络中立业务服务平台客观上帮助了犯罪实行行为，在此前提下，认定网络中立业务服务平台是否需要承担刑事责任的关键不在于其提供的服务技术本身，而在于网络服务平台的开发者与使用者的主观意图。在传统的共犯结构中，实行犯与帮助犯之间通常需要具备意思联络，或者至少帮助者在主观上具有通过本人的帮助行为促进实行者实施犯罪的意思。实务上认定中性业务活动者成立帮助犯，通常需要考其有无故意；反过来，在中性业务活动中连未必的认识都不存在的场合，就能够否定其故意，不认为其成立帮助犯。27 但由于网络中立业务的特殊性，在网络服务平台的日常业务过程中，鲜有证据可以证明平台提供技术支持具有促进他人犯罪的主观意思，更遑论网络服务提供者与犯罪实行行为人之间的意思联络。

正因为如此，2015 年《刑法修正案（九）》增设了《刑法》第 287 条之二的帮助信息网络犯罪活动罪，明确了只要在主观上“明知他人利用信息网络犯罪实施犯罪”，在客观上又提供技术支持、帮助的，即可以构成该罪。该条规定理论上被认为是有关“中立帮助行为正犯化”的规定。笔者认为，帮助信息网络犯罪活动罪主观构成要件中的“明知”应当包括“确知”与“应当知道”，其中“应当知道”是一种推定的“明知”。28 事实上，“明知”的直接证明一直是司法实践中的一大难题，尤其是对于中立业务服务平台而言，其所提供服务的中立属性决定了其作为帮助犯的帮助行为与日常经营活动中的服务提供行为并无二致、难以辨清。在缺乏合法有效的被告人供述或是能够直接证明帮助者“确知”的证据时，应当以“大于半数规则”作为量化标准推定中立业务服务平台“明知”的成立是有效合理的方案。“大于半数规则”是指，中立业务平台在帮助犯罪活动与提供合法服务之间的分配比例大于 1∶1。具体而言，若从网络服务平台后台收集得到的客观电子数据可以表明网络中立业务服务平台所服务的对

象中，利用信息网络实施犯罪活动的占全部服务对象的比重超过半数以上，便可以据此推定中立业务服务提供者为“明知”，即“应当知道”其业务行为所支持的对象利用信息网络实施犯罪还仍然为其提供技术支持与帮助。

（三）关注人工智能技术与网络黑灰产犯罪结合带来的破坏

根据《2019 年网络犯罪防范治理研究报告》，2018 年因网络犯罪而导致的每分钟全球经济损失高达 290 万美元，新技术、新业态网络黑灰产犯罪数量更是呈上升趋势。其中以人工智能技术为代表的新技术在网络黑灰产犯罪中的应用范围也越来越广。笔者认为，人工智能新技术在网络黑灰产中的运用，可能对我国现行刑事法律规范产生以下两方面的冲击：

其一，受程序完全或主要支配的人工智能技术在网络黑灰产中的运用，对现行刑事法律规范的冲击。应该看到，受程序完全或主要支配的人工智能技术可能被应用于网络黑灰产下游的传统犯罪中。例如，行为人借用人工智能换声技术（采集目标人物的原始音频文件，通过深度学习模仿目标人物的发音特点，最后使用 AI 技术合成语音片段，将语音片段与目标人物的视频相结合进行剪辑）使对目标人物的模仿更可以以假乱真，从而实施电信诈骗、敲诈勒索、侵犯著作权等犯罪行为。又如，行为人通过换脸技术（通过使用源人物和目标人物图片和视频训练模型进行分别识别，还原两人的核心面部特征，最后用源人物的图片及视频搭配目标人物的解码器完成转换，将源人物的人脸替换目标人物的人脸）实施诈骗、敲诈勒索、传播淫秽物品等犯罪行为。对此，我们应该追究人工智能软件的使用者的刑事责任。这是因为时下换脸、换声等人工智能技术的研发并未违反国家规定，也即该技术具有中立性，对该技术的研发者不能追究刑事责任，而对以违法犯罪为目的的使用者则应按其具体实施的相关犯罪追究相应的刑事责任。当然如果相关软件的研发者对使用者犯罪目的知情仍提供为其技术支持的，对此研发者就可能构成帮助信息网络犯罪活动罪。

受程序完全或主要支配的人工智能技术也同样可被应用于尚未被刑法所规范的网络灰色产业。例如，在恶意注册产业链中，行为人可借用人工智能技术，在不破坏、不控制、不侵入计算机系统的前提下，以薅羊毛为目标实施恶意注册行为，或通过人工智能技术实施虚假注册账号及养小号等行为。29 在黑公关和恶刷流量产业链中，行为人为了提升或打压相关人物、话题、产品、网站的热度，可在不侵犯他人人格权且不干扰计算机系统的前提下，通过人工智能技术实施控评、刷评等恶意公关行为，或通过人工智能技术实施恶意挂机刷流量等行为。30 如前文所述，在对信息网络系统不产生干扰和破坏的前提下，薅羊毛、养小号、刷流量等行为本身并不构成犯罪。应该看到，这种中立性的人工智能技术虽可能未对计算机系统造成干扰和破坏，但却足以给相关互联网行业带来恶意的市场竞争并造成难以估量的破坏。对此，我们只能以《反不正当竞争法》为据追究行为人的行政违法责任。笔者认为，应该适时将这些行为纳入刑法调整的范围之中。

此外，通过人工智能等技术手段将个人所有已公开的信息资料进行全面整合的“电子人肉”的技术也有可能成为新型网络黑灰产业的内容。虽然人肉检索行为有侵犯公民隐私之可能，但是，由于收集公开的信息本身及行为人利用人工智能技术整合这些收集的公开信息，均不违反国家的法律规定；同时，行为人既没有利用自身履行职责或者提供服务过程的便利，也没有以窃取或其他方式为手段，因此其行为不构成《刑法》第 253 条之一的侵犯公民个人信息罪。但不可否认的是，“电子人肉”技术的出现可能给公民的隐私权保护带来破坏，对于人工智能技术整合他人公开信息等不合理运用的行为，有必要从刑事层面上加以规制。

其二，拥有自我学习和深度学习的弱人工智能技术在网络黑灰产中的运用，对现行刑事法律规范的冲击。拥有自我学习和深度学习的弱人工智能技术将有极大几率被动地成为网络黑灰产相关讯息的传播媒介。我们完全可以预见，随着人工智能技术的飞速发展，不远的将来势必会出现超出生产者和研发者的预见且不完全受其支配控制的人工智能产品。该类产品可以通过自我学习和深度学习能力，对网络平台的信息进行全方位的浏览和掌握，并以用户的浏览信息种类、网络检索内容、购买记录等为依据，智能推送网络黑灰产相关网站或产品链接，进而引诱他人接触或者从事网络黑灰产违法犯罪活动。例如，具有深度学习算法的人工智能聊天机器人，在自我学习过程中掌握用户需求，并向用户推送黄色网站和赌博平台等链接。由于聊天机器人推送违法网站的行为并非研发者和生产者可以预见，且深度学习和自我学习算法作为弱人工智能最为核心功能之一，该算法本身不具有违法性，因此，研发者和生产者不应承担刑事责任。同时，由于使用者的浏览、检索、购买等习惯行为亦不属于犯罪行为，当然也不应承担刑事责任。但是，这种人工智能技术在客观上对于网络黑灰产蔓延产生了推波助澜的效果，同时对社会管理秩序也可能造成破坏，刑法有必要提前加以规制。

注释

[1]参见吴军：《浪潮之巅》,人民邮电出版社 2016 年版,第 600-606 页。

[2]周光权：《刑法软性解释的限制与增设妨害业务罪》,《中外法学》2019 年第 4 期。

[3]“撞库”,又称“扫存”,是指黑客通过收集互联网已泄漏的用户和密码等账号信息,生成对应的数据字典表,尝试批量在其他网站或平台登录系统进行匹配登录,一旦用户基于习惯在多个不同的网站或平台登录时使用了相同的注册用户名和密码,就能匹配成功,黑客可以据此登录用户的其他所有同名账户。目前市场上有 STORM、Black Bullet 等多款免费或收费工具软件可用于实施“撞库”。

[4]参见江苏南京公安机关侦破“4·12”“暗网”侵犯公民个人信息案(公安部 2020 年 4 月公布的十起关于侵犯公民个人信息的违法犯罪典型案件之一),参见中华人民共和国中央人民政府网站 http://www.gov.cn/xinwen/2020-04/16/content_5502912.htm,最后访问日期：2021 年 1 月 6 日。

[5]参见四川省南充市中级人民法院刑事判决书,(2018)川 13 刑终 174 号。

[6]参见江苏省新沂市人民法院刑事判决书,(2020)苏 0381 刑初 83 号。

[7]参见 2011 年 8 月 1 日“两高”《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 2 条第 1 款有关“专门用于侵入、非法控制计算机信息系统的程序、工具”的认定。

[8]“两高”《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 3 条规定：“提供侵入、非法控制计算机信息系统的程序、工具,具有下列情形之一的,应当认定为刑法第二百八十五条第三款规定的“情节严重”：(一)提供能够用于非法获取支付结算、证券交易、期货交易等网络金融服务身份认证信息的专门性程序、工具五人次以上的；(二)提供第(一)项以外的专门用于侵入、非法控制计算机信息系统的程序、工具二十人次以上的；……”

[9]“tt_spider”文件工作原理是：通过分类视频列表、相关视频及评论等接口对网站服务器进行数据抓取,并将结果存入到数据库中。在数据抓取的过程中使用伪造 device_id 绕过服务器的身份校验,使用伪造 UA 及 IP 绕过服务器的访问频率限制。参见北京市海淀区人民法院刑事判决书,(2017)京 0108 刑初 2384 号。

[10]郭玮：《网络数据爬取行为的刑法规制研究--以非法获取计算机信息系统数据罪为视角》,《新疆社会科学》2020 年第 3 期。

[11]杨志琼：《数据时代网络爬虫的刑法规制》,《比较法研究》2020 年第 4 期。

[12]刘艳红：《网络爬虫行为的刑事规制研究--以侵犯公民个人信息犯罪为视角》,《政治与法律》2019 年第 11 期。
[13]张明楷：《刑法学》(上),法律出版社 2016 年版,第 486 页。
[14]《重刑严惩“刷流量”黑产,才能让口碑成为真正的流量》,中国经济网 http：//www.ce.cn/xwzx/gnsz/gdxw/202001/10/t20200110_34094752.shtml,最后访问日期：2020 年 11 月 25 日。
[15]腾讯安全战略研究公众号：《聚焦网络黑产源头首份〈互联网账号恶意注册黑色产业治理报告〉在京发布》,参见腾讯网 https：//mp.weixin.qq.com/s/hi K3gubw S m Qe1v GCY3VQSQ,最后访问日期：2020 年 11 月 25 日。
[16]参见浙江省兰溪市人民法院刑事判决书,(2018)浙 0781 刑初 300 号。
[17]时延安：《个人信息保护与网络诈骗治理》,《国家检察官学院学报》2017 年第 6 期。
[18]陈兴良：《互联网账号恶意注册黑色产业的刑法思考》,《清华法学》2019 年第 6 期。
[19]身份证“网证”(CTID)是身份证电子版与网络版的简称,是以居民身份证制证数据为基础,通过国家“互联网+可信身份认证平台”签发,与实体身份证芯片唯一对应的电子映射文件。2017 年 12 月 25 日,全国首张微信身份证“网证”于广州南沙签发。李喆等：《广州签发首张“微信身份证”》,中国警察网 http：//news.cpd.com.cn/n3559/c40120110/content.html,最后访问日期：2020 年 11 月 25 日。
[20]同前注[18]。
[21]郭玮：《累积犯视域下网络账号恶意注册行为的规制》,《法学杂志》2020 年第 1 期。
[22]高艳东：《破坏生产经营罪包括妨害业务行为--批量恶意注册账号的处理》,《预防青少年犯罪研究》2016 年第 2 期。
[23]刘仁文、杨学文：《用刑法规制电子商务失范行为》,《检察日报》2015 年 8 月 26 日。
[24]参见北京市第一中级人民法院刑事裁定书,(2016)京 01 刑终 592 号。
[25]参见王华伟：《网络服务提供者刑事责任的认定路径--兼评快播案的相关争议》,《国家检察官学院学报》2017 年第 5 期；高艳东：《不纯正不作为犯的中国命运：从快播案说起》,《中外法学》2017 年第 1 期；陈洪兵：《网络服务商的刑事责任边界--以“快播案”判决为切入点》,《武汉大学学报》(哲学社会科学版)2019 年第 2 期。
[26]“暗网”是指无法直接通过超链接访问、无法被标准搜索引擎索引到的资源合集,通常使用动态网页技术进行访问。
[27]周光权：《中性业务活动与帮助犯的限定》,《比较法研究》2019 年第 5 期。
[28]刘宪权：《论信息网络技术滥用行为的刑事责任--〈刑法修正案(九)〉相关条款的理解与适用》,《政法论坛》2015 年第 6 期。
[29]参见前注[18]。
[30]参见高艳东、李莹：《数据信用的刑法保护--以“流量黑灰产”为例》,《浙江大学学报》(人文社会科学版)2020 年第 5 期。

4.网络黑灰产刑法规制实证研究

皮勇：同济大学上海国际知识产权学院

摘要：网络黑灰产活动通常指称具有一定独立性、常业性的非法牟利型网络违法犯罪。利用对传统犯罪立法进行合理扩张解释的方法,能解决相当多网络黑灰产犯罪案件的法律适用问题,但也不应过度依赖扩张解释方法,对相关构成要件的解释应在合理限度内。当传统犯罪和侵犯公民个人信息罪不能规制网络黑灰产犯罪时,可以按手段行为入罪,适用侵犯计算机信息系统安全或妨害信息网络管理秩序相关罪名,后者对惩治新型网络黑灰产犯罪发挥了重要作用。当前侵犯计算机信息系统安全犯罪立法有不足之处,司法实践中存在泛化适用问题。妨害信息网络安全管理秩序犯罪是具有积量构罪构造的独立犯罪,不应以共犯或预备犯的构成条件来限制其适用。同时,为了避免司法实践中对其泛化适用,对相关构成要件的解释应当限制在合理范围内。
关键词：
网络黑灰产;合理扩张解释;手段行为;积量构罪;实证研究;
网络黑灰产活动通常指称具有一定独立性、常业性的非法牟利型网络违法犯罪活动，网络社会的高度发展为其提供了“肥沃的土壤”和“广阔的天地”。当前网络黑灰产活动呈现出泛滥之势，产生了严重的社会危害。刑法是网络社会良性治理的重要保障，对遏制网络黑灰产犯罪发挥了关键作用。由于该类犯罪演变迅速，相关犯罪立法难以及时跟进其发展，司法机关在处理该类犯罪案件时遇到不少适用难题。本文通过分析 1211 份网络犯罪刑事判决书，研究司法实践中的典型问题，探索网络黑灰产犯罪立法及其司法规制的完善路径。

一、以传统犯罪立法规制的刑法问题

在过去 20 多年，我国网络犯罪经历了由计算机犯罪（Computer-Crime）到网络犯罪（Cyber-Crime）再到网络空间犯罪（Crimes in Cyberspace）的三次样态转变，立法机关随之及时修改刑法，建立了“四位一体”的网络空间犯罪立法体系，侵犯计算机信息系统安全犯罪、传统犯罪网络化的刑事责任确认、妨害信息网络管理秩序犯罪、侵犯个人信息犯罪立法相互补充、配合，组成了惩治网络空间犯罪的严密法网。1 大部分网络黑灰产犯罪属于传统犯罪的网络化，由于我国刑法规定的大多数犯罪不限定特殊犯罪目的、犯罪方法、手段、对象、后果形式等，多数网络黑灰产犯罪可以按传统犯罪定罪处罚。例如，通过“撞库”获取他人网银、支付宝账号、密码后通过信息网络转走他人资金的，关于该行为的性质属于盗窃还是诈骗行为存在争议，但是，将其按照一定的理论解释为成立盗窃罪或诈骗罪等传统犯罪，并不存在异议。2 换言之，许多网络黑灰产犯罪只是犯罪手段、方法和犯罪场域不同于传统犯罪形式，这些改变一般不超出传统犯罪立法的“张力范围”，通过对传统犯罪立法进行合理扩张解释，能解决相当多网络黑灰产犯罪案件的法律适用问题。

但是，教义学解释方法不是“解开”所有网络黑灰产犯罪定罪“难题”的“万能钥匙”，对传统犯罪立法中构成要件的扩张解释应当有一定的限度。以下通过评述 2 件典型网络黑灰产犯罪案件判决书来讨论这一限度问题。

（一）犯罪地点

网络“水军”或“推手”活动在网络空间有巨大影响力，表现为通过散布夸大事实或编造的虚假信息，吸引网络用户关注，从而获取非法利益，严重扰乱网络空间秩序。在惩治此类网络黑灰产犯罪时，关于传统犯罪立法规定的犯罪地点能否扩张解释为网络空间，理论和实务界对此存在严重分歧，以“秦火火”网络寻衅滋事案判决书对行为的定性为争论焦点。3《刑法》第 293 条第 4 项规定的寻衅滋事行为是“在公共场所起哄闹事，造成公共场所秩序严重混乱的”行为，将其犯罪地点限定为“公共场所”。2013 年 9 月颁布的《最高人民法院最高人民检察院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》第 5 条第 2 款规定，“编造虚假信息，或者明知

是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照《刑法》第 293 条第 1 款第 4 项的规定，以寻衅滋事罪定罪处罚。”该款将《刑法》第 293 条规定中的“公共场所秩序”换为“公共秩序”，将信息网络认定为公共场所。对于此案判决及前述司法解释的规定，有的学者予以支持，认为“尽管在信息网络公共空间‘起哄闹事’行为，没有造成网络空间‘公共场所秩序’的混乱，但是，造成社会秩序严重混乱，而且危害往往更大的，完全符合第 293 条规定的“破坏社会秩序”的要求。如此解释……没有超出第 293 条规定的范围……不存在类推刑法而违反罪刑法定原则的问题。”4 然而，多数学者认为，该解释并不合理，认为是“以解释之名，行立法之实”。5

信息网络包括非公共信息网络和公共信息网络，6 与刑法规定的“公共场所”性质不同。7 信息网络是传播信息类犯罪的新环境，信息的数字化和网络化传播方式不改变该类犯罪的犯罪对象、危害行为、危害后果等构成要件性质，也不影响不限定犯罪场所的犯罪立法的适用，如利用信息网络空间可以实施诽谤、煽动型犯罪、传播淫秽物品犯罪等。对于以公共场所为犯罪地点的犯罪，如聚众扰乱公共场所秩序、交通秩序罪和寻衅滋事罪等，公共信息网络空间能否认定为相关犯罪条款中的“公共场所”，影响到刑法是否认可这类行为。《刑法》共有 7 条使用了“公共场所”的表述，8 从相关犯罪的立法时间、社会环境以及罪状描述来看，以上“公共场所”都必须是有人身、财物在场，相关犯罪对人身、财产安全有直接侵害的危险，才使寻衅滋事行为达到应受刑罚处罚的严重危害程度，即公共场所不仅具有公共性，还必须具有人身、财物的在场性。前述解释对传统物态社会环境下设立的、由原流氓罪分解出来的寻衅滋事罪进行扩大解释，将其物态“公共场所”扩大到纯粹信息交流、无侵害人身、财产危险的信息网络，违反了罪刑法定原则，实质上是创设了“扰乱公共信息网络秩序罪”。

将“公共场所秩序”解释为“社会秩序”不合理。如果前述学者的解释，《刑法》第 237 条（强制猥亵、侮辱罪、猥亵儿童罪）、第 291 条第 1 款（聚众扰乱公共场所秩序、交通秩序罪）、第 292 条（聚众斗殴罪）乃至第 120 条之五（强制穿戴宣扬恐怖主义、极端主义服饰、标志罪）、第 130 条（非法携带枪支、弹药、管制刀具、危险物品危及公共安全罪）、第 236 条（强奸罪）中的“公共场所”都可以作此类比解释，因其都破坏了社会秩序而可以在信息网络上实施，如此解释会使构成要件的限定功能不复存在。因此，有学者提出，“《刑法修正案（九）》生效后利用信息网络或者其他媒体造谣、传谣的行为，原则上即不得再根据司法解释以寻衅滋事罪论处。”9

从社会效果看，以上解释使寻衅滋事罪成为管制网络空间信息的“口袋罪”。按照该解释的规定，认定该罪的关键是判断信息是否虚假，当信息真假难辨时，谁掌握信息真实性的认定权力，谁就掌握着处罚信息发布者、传播者的决定权，其中险恶不言自明。揭穿谎言的最佳武器是事实真相，及时调查和公布事实真相，更能消除虚假信息的危害。在紧急情况下，需要及时控制虚假信息传播时，可以依法管制互联网，事后追究虚假信息传播者的民事或者行政法律责任，足以消除虚假信息网络传播的危害，而采取刑法手段反而会造成“以刑封口”“弄假成真”的恶劣社会影响。如果确有必要对故意在信息网络上散布虚假信息、情节严重的行为追究刑事责任，也应当通过修改故意传播虚假险情、疫情、灾情、警情信息罪立法，将其犯罪对象扩展为扰乱社会公共秩序的其他虚假信息，而不应进行以上越权解释。对其他网络黑灰产犯罪适用其他传统犯罪立法时，如果涉及犯罪地要件的认定，应遵守以上文义限度原则，避免为了处理具体案件而破坏我国刑事法治。

（二）犯罪对象

计算机数据是网络社会活动的重要资源，是网络黑灰产犯罪侵犯的新对象，如何运用刑法手段规制侵犯计算机数据行为，成为司法实践中经常遇到的疑难问题。其中，关于网络虚拟财产能否解释为盗窃罪立法中的财物，刑法理论界和司法实务界存在争议。2017 年 10 月 12 日最高人民检察院发布的第九批指导性案例中，检例第 37 号张四毛盗窃案的判决书将网络域名认定为盗窃罪的犯罪对象，“行为人利用技术手段，通过变更网络域名绑定邮箱及注册 ID，实现了对域名的非法占有，并使原所有人丧失了对网络域名的合法占有和控制，其目的是为了非法获取网络域名的财产价值，其行为给网络域名的所有人带来直接的经济损失。该行为符合以非法占有为目的窃取他人财产利益的盗窃罪本质属性，应以盗窃罪论处。”该指导性案例并没有平息前述理论界的纷争。

持肯定说的学者认为，“具备财物特征的虚拟财产，才是刑法上的财物”，财产特征是指“管理可能性、转移可能性与价值性”，其中的价值性是“具有一定客观价值或者一定使用价值”。10 笔者认为，该观点对“价值性”的界定不明，未讨论“价值性”是否具有普遍性，即对社会所有人或者多数人具有客观价值或主观价值。如果认为只对特殊人或者少数群体具有客观价值或主观价值的虚拟财产具有价值性，那么，只被特定网络游戏的少数用户群体认为具有使用价值和交换价值的网络虚拟财产就具有刑法上财物的“价值性”，进而可以被认定为盗窃罪中的财物。按此观点推导，在其他非网络游戏如大富翁纸牌游戏中，幸运卡等游戏道具在部分游戏者及相关人之间进行财与物的交换，盗窃该游戏道具的行为也应认定为盗窃罪，这种处理明显违反常理常识，不会得到司法实务和刑法理论的支持。反之，如果认为“价值性”应当具有普遍性，则应当否定不具有兑现或者合法交易条件的网络虚拟财产的财产性，如网络游戏装备、腾讯公司的 Q 币和 QQ 号等。

持否定论的学者将其划归为计算机数据，回避讨论网络虚拟财产的法律属性。有学者认为，除非有特殊规定，无体物和“财产性利益不是我国刑法中盗窃罪的对象”，因此，即使将虚拟财产的本质界定为无体物和财产性权利，也不能成为盗窃罪的犯罪对象。而“将侵犯虚拟财产的行为认定为破坏计算机信息系统罪，在不违背罪刑法定原则的同时，避免了对虚拟财产法律属性的争议。”11 还有学者认为，“网络游戏中的虚拟财产，不属于盗窃罪所能侵害的‘财物’；窃取网络游戏中的虚拟财产，侵犯的也主要不是财产所有权，不符合盗窃罪的构成要件”，12 由于刑法修正案（九）设立了非法获取计算机信息系统数据罪，“窃取网络虚拟财产行为符合非法获取计算机信息系统数据罪的构成要件”，应按该罪而不是盗窃罪认定，而网络游戏运营企业的工作人员实施前述行为的，应认定为侵犯著作权罪。

笔者赞同否定说对网络虚拟财产的定性，但认为其对相关行为的定性不妥当，理由详述如下：（1）“将侵犯虚拟财产的行为认定为破坏计算机信息系统罪”不当。破坏计算机信息系统罪是指违反国家规定，删除、修改、增加、干扰计算机信息系统功能，或者删除、修改、增加计算机信息系统中的数据和应用程序，或者故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行且后果严重的行为。而盗号活动通过侵入网络游戏服务器，获取大量用户的账号密码数据并出售给下游犯罪人，其行为没有影响计算机信息系统正常运行，计算机信息系统核实账号密码并执行相关指令的功能并未被干扰，不符合破坏计算机信息系统罪的结果要件，不应当认定为破坏计算机信息系统罪。（2）非法获取计算机信息系统数据罪保护的是计算机信息系统数据的保密性，对其删除、修改、增加操作属于破坏计算机信息系统行为。有学者认为，“将玩家拥有的游戏装备、宝物等电子数据从其游戏账户中注销，尔后添加到自己控制的游戏账户中或转给第三者；也有的是侵入网络游戏系统采用技术手段复制某种虚

拟财产（即电子数据）后转卖给他人。对这后一种情形也应该与前一种情形同等看待，即认定行为人‘获取’了电子数据。”13 前者行为是修改数据而不是非法获取数据，如果将修改解释为获取，违反罪刑法定原则。（3）将网络游戏运营企业的工作人员“获取自己管理的公司存储在网络系统中的虚拟货币等虚拟物品，并转卖给他人，换取大量现金的”行为认定为侵犯著作权罪不妥。侵犯著作权罪是复制发行、出版、制作、出售他人作品的行为，对运行中计算机程序中的数据进行修改，不属于以上危害行为，计算机程序作为作品整体也没有被侵犯。如果网络游戏公司设定的规则是该公司可以交易前述虚拟物品，代表该虚拟物品的计算机数据是财物的电子形式，通过修改数据获取虚拟物品属于职务侵占行为；如果以上虚拟物品不允许交易或者转让的，该虚拟物品只是网络公司服务协议规定的债务形式之一，其行为属于非法控制计算机信息系统，应认定为非法控制计算机信息系统罪。

笔者认为，“网络虚拟财产”不是一个法律概念，将其认定为盗窃罪等侵犯财产罪的“财物”，既不合法也缺乏有力的理论支撑。网站域名是依法登记使用的网络服务入口代码，虽然具有类似于财物的价值性，但不同于财物的所有权性质，将其认定为盗窃罪的“财物”没有法律依据，在解释逻辑上也不严谨：按此逻辑，商业秘密、商标、专利等也具有价值性，可以成为盗窃罪和诈骗罪的犯罪对象，行为人窃取或者骗取前述对象的，至少会构成盗窃罪或诈骗罪与侵犯知识产权犯罪的竞合，这与侵犯知识产权犯罪立法和司法实践相悖。对于侵犯网络虚拟财产的有害行为，如果其行为对象不能依法认定为相关犯罪的犯罪对象，应当根据网络虚拟财产的具体形式分析其法律性质，从行为的违法性、后果的严重性等方面来研究刑法规制的路径。当现行刑法对其无法规制，却有必要追究刑事责任的，应当通过立法途径来解决。14

综上所述，对网络黑灰产犯罪适用传统罪名时，不应过度依赖扩张解释方法，对相关构成要件解释应在合理限度范围内，不应超出立法规定和语义范围作出越权解释。

二、以侵犯计算机信息系统安全犯罪规制的刑法问题

当传统犯罪和侵犯公民个人信息罪不能有效规制网络黑灰产犯罪时，还可以按手段行为入罪，适用侵犯计算机信息系统安全犯罪或妨害信息网络管理秩序犯罪立法。相比于妨害信息网络安全管理秩序的三种新网络犯罪立法，侵犯计算机信息系统安全犯罪立法较早，在以传统罪名处罚网络黑灰产犯罪遇到困难时，司法机关多考虑适用后者。侵犯计算机信息系统安全犯罪立法是指《刑法》第 285 条和第 286 条规定的 5 种犯罪，这五罪都不要求特定的犯罪目的，网络黑灰产犯罪齐备某一罪构成要件的，就可以适用相应犯罪立法。以下对侵犯计算机信息系统安全犯罪适用于网络黑灰产犯罪的判决情况及存在的问题进行分析。

（一）非法侵入计算机信息系统罪

笔者在裁判文书网、无讼网和北大法意上搜索到 2011 年至 2020 年期间以非法侵入计算机信息系统罪定罪的刑事判决书共 250 份，各年判决书数量如图 1 所示。

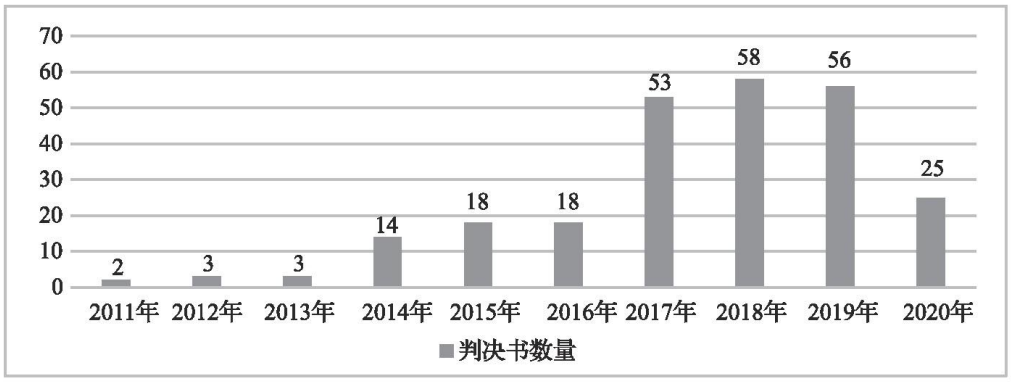


图 1 非法侵入计算机信息系统罪判决书数量　　下载原图

对以上判决书进行分析，发现以该罪判决的犯罪具有如下特征：（1）犯罪目的多样化。在以上判决认定的犯罪中，犯罪人的犯罪目的多种多样，其中，62.3%的案件中的犯罪人是出于以非法牟利为常业目的。（2）侵犯的对象全部是较低层级的国家事务领域计算机信息系统。这一方面可能是因为这些计算机信息系统的安全保护程度不高，另一方面也可能是非法侵入国防建设、尖端科学技术领域计算机信息系统犯罪因涉密而没有公布。受攻击的国家事务计算机信息系统多为与国计民生密切相关的计算机信息系统，其中，以交警警务平台系统受攻击的案件最多，其次是向电子政务系统植入广告推广。（3）非法侵入计算机信息系统罪成为侵犯国家事务、国防建设、尖端科学技术领域计算机信息系统安全犯罪的兜底罪名。不少判决书查明的犯罪事实不只是非法侵入国家事务领域计算机信息系统，还有后续的破坏行为，但是由于破坏行为导致的危害后果不能全部查明，达不到认定为破坏计算机信息系统罪的要求，只能退而求其次认定为该罪。15(4）非法侵入国家事务领域计算机信息系统获取计算机数据犯罪只能以非法侵入计算机信息系统罪定罪处罚。相当多判决书认定的网络黑灰产犯罪人非法侵入国家事务领域计算机信息系统后，获取大量计算机数据，16 可以认为达到情节严重的程度，但由于《刑法》第 285 条第 2 款规定的非法获取计算机信息系统数据罪的犯罪对象不包括前述三类特殊计算机信息系统，只能按照该罪定罪处罚。

以上情况说明《刑法》第 285 条的规定存在不足。非法侵入计算机信息系统罪是最早设立的计算机犯罪之一，本意是对前述三类特殊领域计算机信息系统给予更有力的刑法保护，当前立法状况却做得相反，具体分析如下：（1）根据《刑法》第 285 条第 2 款的规定，前述三类特殊计算机信息系统不受第 2 款保护，如果以上系统中的数据不属于国家秘密、商业秘密、公民个人信息和通信信息，则落入刑法保护的“真空”，即非法获取前述三类计算机信息系统的行为没有受到刑法的评价，只能按其前行为——非法侵入行为认定为该罪。（2）非法获取计算机信息系统数据罪重罪的法定刑为 7 年有期徒刑并处罚金，而非法侵入计算机信息系统罪的最高法定刑为 3 年有期徒刑，且无罚金刑。当前网络黑灰产犯罪侵犯国家事务计算机信息系统是为了非法获取其中的国家事务相关计算机数据，按照该罪论处没有反映其重要的主客观特征，加之法定刑比非法获取计算机信息系统数据罪低，又不能按后罪处罚，导致轻纵了这类犯罪活动。笔者建议，应当完善《刑法》第 285 条第 2 款的规定，使该款的保护对象涵盖前述三类特殊领域计算机信息系统，同时，将该罪的行为对象由“数据”扩展为“数据和程序”，可以在第 2 款最后增加一段：“对第一款规定的计算机信息系统犯本款规定的犯罪的，依照本款规定从重处罚。”

（二）非法获取计算机信息系统数据罪

笔者在裁判文书网、无讼网和北大法意上搜集到 2010 年至 2020 年期间以非法侵入计算机信息系统罪定罪的刑事判决书共 889 份，各年判决书数量如图 2 所示。

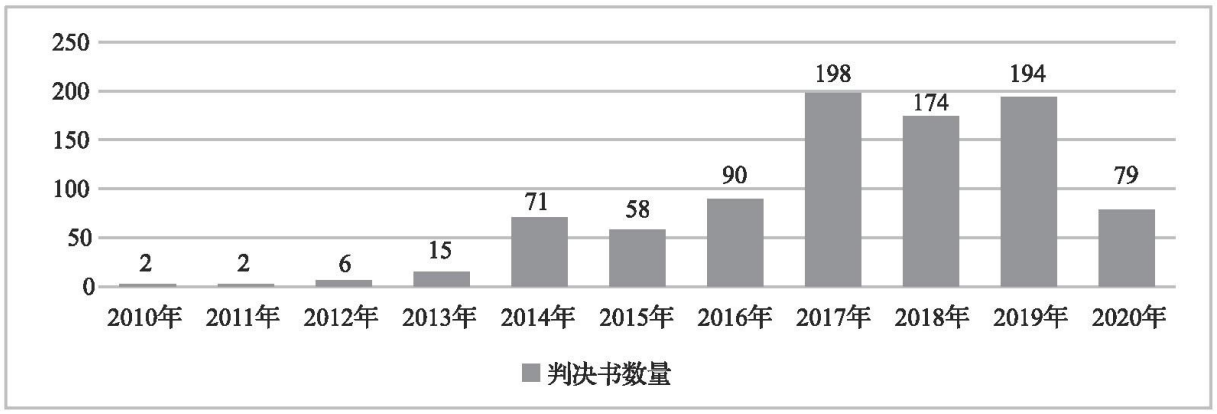


图 2 非法获取计算机信息系统数据罪判决书数量　　下载原图

由于以上判决书数量巨大，笔者对以上判决书以 11%的比例对各年判决书进行随机抽样，同时，保证每年至少有 1 件判决书，共抽取到 103 份判决书。17 对以上判决书进行分析，发现以该罪判决的犯罪具有如下特征：（1）犯罪目的高度趋向于非法牟利。在以上判决书查明的犯罪事实中，不以非法牟利为目的的案件仅 11 件，以非法牟利为目的的案件占比为 89.3%，其中，对特定单个或少数被害人实施 3 次以下该罪行为的案件仅有 5 件，其余 87 件案件中的犯罪人是以非法牟利为常业目的。（2）各类计算机数据都对该类犯罪都有利用价值，包括 QQ 号、电子邮箱信息、网络游戏账号、网络游戏装备数据、二维码、用户信息、比特币数据、医院处方数据、快递单号等，各应用阶段中的计算机数据都可以成为非法获取并与下游违法犯罪进行交易的对象，18 其中，游戏账号及其中的游戏装备数据占大部分。（3）该罪的危害行为是复合性行为。该罪行为包括两部分组成，非法获取计算机信息系统数据是后行为、目的行为，而非法侵入计算机信息系统或利用其他技术手段是前行为、手段行为，前者手段行为占绝大多数，在前述抽样判决书中，仅有 2 件判决书查明的犯罪是通过“劫持”传输中的数据，19 或者避绕保护措施，20 这说明非法侵入计算机信息系统对该罪的实施起关键作用。但是，关于如何认定非法侵入行为，部分判决书的认定值得商榷，如有判决书将内部人员对外提供授权范围内获取的计算机数据行为认定为非法侵入行为。21(4）少数判决书将前述三类特殊计算机信息系统认定为该罪的犯罪对象。根据《刑法》第 285 条第 2 款的规定，非法获取计算机信息系统罪的犯罪对象不包括前述三类特殊计算机信息系统，有少数判决书将公安内网计算机信息系统及其中的计算机数据纳入该罪的保护对象。22

根据以上特征，司法机关对网络黑灰产犯罪适用该罪时，要注意以下几点：

1. 非法获取计算机信息系统数据罪能够较好地规制多数侵犯计算机数据的犯罪。在立法构造上，该罪与《美国联邦法典》第 1030 条（a)(2）规定的侵入计算机信息系统并获取计算机数据罪相似，23 且适用范围更宽。关于计算机数据是否属于财产存在争议，前文提到的部分学者将各种计算机数据不加区分地认定为法律上的财产，并按照传统的侵犯财产犯罪定罪处罚，在实践中是行不通的，如将快递单号、医生处方信息等计算机数据认定为财产，只会引起更多的法律问题，如快递公司每天都在发行此类“数据财产”、该类“财产”的财产性质及其权属问题等。该罪立法避开了以上法律困境，只要行为人以该罪规定的手段非法获取了计算机数据，就可以按该罪追究刑事责任，同时，针对该类犯罪大多出于非法牟利目的特征，规定了罚金刑，实现了罪责刑相适

应。不过，该罪不能规制非法获取前述三类特殊领域计算机信息系统数据的行为，需要按照前文所述完善立法。

2. 根据非法获取计算机信息系统数据行为与下游犯罪的关系，行为人可以构成不同犯罪。如果非法获取的计算机数据属于公民个人信息、国家秘密、商业秘密等特定信息，并且齐备相应犯罪的构成要件的，构成侵犯公民个人信息罪、非法获取国家秘密罪、侵犯商业秘密罪等犯罪，不以本罪处罚。如果行为人与下游犯罪人存在共同犯罪关系，如利用非法获取的快递单号实施诈骗犯罪，应当认定为共同犯罪并从一重罪定罪；当下游行为不构成犯罪，如快递单号出售牟利的，应当按照非法获取计算机信息系统数据罪的共同犯罪定罪处罚；如果二者只是上下家违法交易关系，则分别按照非法获取计算机信息系统数据罪和掩饰、隐瞒犯罪所得罪定罪处罚。

（三）非法控制计算机信息系统罪

笔者在裁判文书网、无讼网和北大法意上搜集到 2012 年至 2020 年期间以非法侵入计算机信息系统罪定罪的刑事判决书共 596 份，各年判决书数量如图 3 所示。

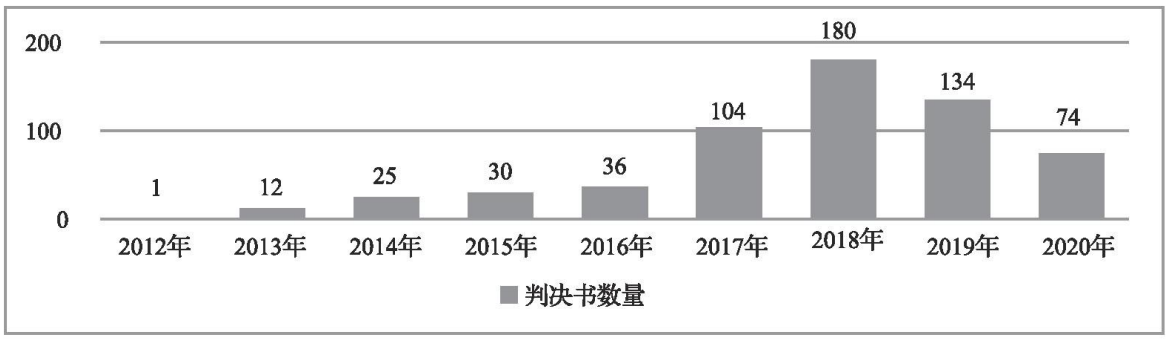


图 3 非法控制计算机信息系统罪判决书数量　　下载原图

笔者按分析前罪的方法抽取到 103 份判决书，通过分析以上判决书，发现以该罪判决的犯罪具有如下特征：（1）大部分案件中的犯罪是以非法牟利为目的。前述判决书中，只有 17 件案件中的犯罪不以非法牟利为目的，83.5%的判决书认定的犯罪以非法牟利为常业目的。（2）犯罪人在非法控制计算机信息系统之后实施了多种行为，包括用于刷单、出售计算机信息系统的控制权、发布非法广告、24 比特币“挖矿”、25 对被控制的计算机信息系统的权利人进行敲诈勒索以及电信网络诈骗活动等，26 下游行为是实现非法牟利的关键，但往往不能单独成立犯罪，或者难以定罪处罚，或者以下游犯罪定罪不能客观体现其危害性，27 故而按照其犯罪过程中的手段行为定罪处罚。（3）少数判决书将非法控制国家事务领域计算机信息系统的行为认定为该罪，包括非法控制国家事务领域计算机信息系统并修改其中数据、28 非法侵入国家事务领域计算机信息系统并删除其中数据，导致系统不能正常运行且后果严重。29

根据以上特征，司法机关在对网络黑灰产犯罪适用该罪时要注意以下几点：

1. 该罪仅能适用于侵犯前述特殊领域计算机信息系统之外的计算机信息系统的行为，该款的缺陷应当通过修改立法来弥补，不能违反法律规定来惩治网络黑灰产犯罪。

根据《刑法》第 285 条第 1、2 款的规定，非法控制国家事务领域计算机信息系统并修改其数据的，只能认定为非法侵入计算机信息系统罪。根据《刑法》第 286 条的规定，非法侵入国家事务领域计算机信息系统并删除其中数据，导致系统不能正常运行且后果严重的，30 应认定为破坏计算机信息系统罪；如果未造成严重后果的，应当按照非法侵入计算机信息系统罪定罪处罚，而不是适用该罪。

2. 该罪规制的犯罪行为有特定的范围。

该罪行为应当限定于以下两类：第一类是未造成严重后果、但属于情节严重的行为，如控制计算机信息系统数量、非法牟利数额、用于非法活动的次数较大等；第二类是虽然造成严重后果，但不属于影响计算机信息系统正常运行的严重后果。在最高人民检察院第九批指导性案例中，“李俊杰等破坏计算机信息系统案”的犯罪行为没有造成购物网站系统不能正常运行，没有引起破坏计算机信息系统罪立法规定的严重后果，不应认定为破坏计算机信息系统罪；其行为性质是非法控制购物网站系统并用于非法牟利，虽然其非法牟利行为不能单独定罪处罚，但是，其非法牟利 9 万元可以被评价为非法控制计算机信息系统罪的“情节严重”，按照该罪认定更符合法律规定。这样认定不仅能避免对以上行为适用过重的刑罚，还能防止将破坏计算机信息系统罪变成新的重“口袋罪”。31

3. 该罪是非法控制前述特殊领域之外计算机信息系统的“兜底”犯罪。

行为人非法侵入计算机信息系统后，就实现了对系统的非法控制，非法获取其中计算机数据只是其中被独立规定的非法控制行为，因此，《刑法》第 285 条第 2 款规定的“实施非法控制”涵盖了非法获取数据之外的各种非法控制情形，起到防止该款立法挂一漏万的兜底作用，这一点在司法实践中要注意掌握运用。

（四）提供侵入、非法控制计算机信息系统程序、工具罪

笔者在裁判文书网、无讼网和北大法意上搜集到 2013 年至 2020 年期间以提供侵入、非法提供计算机信息系统程序、工具罪定罪的刑事判决书共 470 份，各年判决书数量如图表 4 所示。

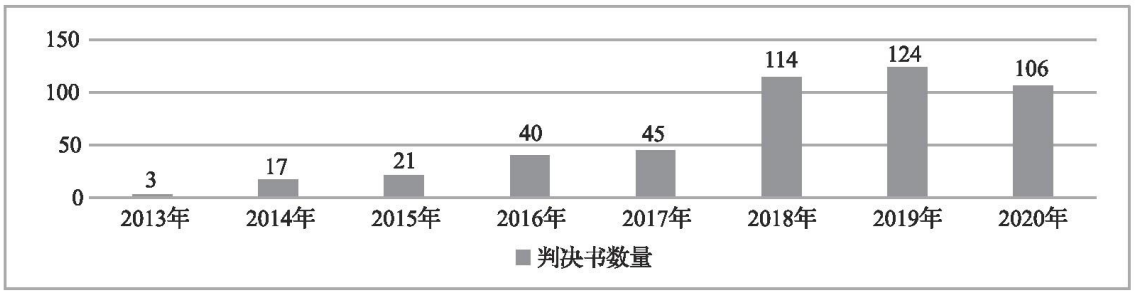


图 4 提供侵入、非法控制计算机信息系统程序、工具罪判决书数量　　下载原图

笔者按分析前罪的方法抽取到 101 份判决书，通过分析以上判决书，发现以该罪判决的犯罪具有如下特征：（1）前述判决书查明的犯罪绝大部分以非法牟利为常业目的。只有 1 件案件中的犯罪不以非法牟利为目的，超过 99%的犯罪是网络黑灰产犯罪，其非法牟利的方式主要是出租或出售（97 件），或者用于发布广告（2 件）或进行违法经营活动（2 件）。（2）多数犯罪行为是非法交易前述程序、工具，表现为三种行为：买进并转手卖出或出租、自己编写并出售或出租、买进后自行修改然后出售或出租。后二者制造或强化了有害程序、工具，社会危害性较之于前者更严重。（3）前述程序绝大多数是网络游戏的外挂程序，其次是翻墙软件，32 再次是用于非法控制计算机信息系统的其他程序、工具，前述工具包括无线路由器、33 钓鱼网站、34 征信密码等。35 司法机关对工具的理解较为宽泛，不仅包括避绕电子商务网站监管措施的程序，36 也包括翻墙软件、虚拟机服务，后者不能用于对他人的计算机信息系统实施侵入或非法控制，只能避绕我国互联网监管的“防火长城”系统的监管，将其认定为该罪的犯罪对象与事实不符。（4）部分判决书将出售具有远程控制功能的计算机程序认定为该罪，没有查明行为人是否明知购买者用于违法犯罪活动。37

根据以上特征，对网络黑灰产犯罪适用该罪时要注意以下几点：

1. 该罪的犯罪对象限于计算机程序和工具，司法实践不应随意扩大范围，立法机关有必要明确将密码、深度链接等纳入犯罪对象的范围。

前文提到，有判决书将出售他人计算机信息系统登录密码行为认定为该罪，笔者认为，登录密码、深度链接等都能够避绕计算机信息系统安全保护措施、非法获取计算机信息系统控制权的功能，其作用与侵入、非法控制计算机信息系统的程序没有差别，理应将上述行为纳入该罪规制的范围。但是，密码和深度链接毕竟不同于计算机程序，如果按照“工具”认定，将使“工具”的范围过于宽泛，可以包含一切能实现以上功能的手段，如果作此理解，将使该罪对象不具有类型性。欧洲理事会《网络犯罪公约》第 6 条规定的滥用设备罪将提供密码规定为该罪的基本危害行为，38《美国联邦法典》第 1030(a)(6)规定的提供密码类设备罪的犯罪对象是密码以及与密码具有相同防护作用的、能指引获取计算机信息系统访问权的信息，39 都明确将密码明确规定为该罪对象，以上立法值得我国借鉴。但是，假网站不应被认定为该罪的工具，理由是，假网站的作用是使被害人上当受骗，而不是使计算机信息系统被非法侵入，不具有“两高”《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 2 条规定的“用于侵入、非法控制计算机信息系统、非法获取计算机信息系统数据”功能，用假网站骗取被害人个人信息或实施诈骗的，应当按照侵犯公民个人信息罪、诈骗罪等犯罪定罪处罚。

2. 该罪的下游犯罪应当扩大，使之包括破坏计算机信息系统、对抗《网络安全法》等法律法规规定的网络安全管理措施和其他严重违法犯罪行为。

在当前网络黑灰产犯罪生态中，提供犯罪程序、工具是犯罪“去高技术化”的关键，如果不能有效遏制该类行为，就无法控制网络犯罪生态的“野蛮生长”。应当看到，以上程序、工具等不仅对侵入、非法控制计算机信息系统犯罪发挥了关键作用，对破坏计算机信息系统犯罪同样不可或缺，刑法举轻以明重，将前者行为犯罪化，没有理由去放纵后者行为。加之，破坏计算机信息系统罪或其他犯罪立法都无法规制后者行为，只能通过扩展该罪的下游违法犯罪范围来规制。40 需要特别指出的是，我国网络安全管理措施是国家网络主权的重要保障，“防火长城”等互联网管理措施对拦截境外违法犯罪信息起到重要作用，浏览、下载境外网站上的违法内容信息是违反《网络安全法》的违法行为，提供翻墙软件、虚拟机服务等对抗法律法规规定的网络安全管理措施，对我国网络安全乃至国家安全构成威胁，理应通过立法修改纳入该罪规制的范围，而不应采取违反法律规定扩张该罪适用的方式。

3. 将提供双用途程序、工具的行为认定为该罪时，应当查实行为人明知他人将其用于法定违法犯罪活动。

远程控制计算机信息系统的程序、工具是网络产业的重要产品，不能因其具有以上功能，就一律认定为专用于侵入、非法控制计算机信息系统，应当从具体案情出发，考察其是否可能用于其他合法用途，如果可以肯定，则应认定为双用途程序、工具。如果需要将相关行为认定为该罪，应当查实行为人明知他人用于侵入、非法控制计算机信息系统，防止该罪适用范围不当扩大。

（五）破坏计算机信息系统罪

笔者在裁判文书网、无讼网和北大法意上搜集到 2011 年至 2020 年期间以破坏计算机信息系统罪定罪的刑事判决书共 1159 份，各年判决书数量如图 5 所示。

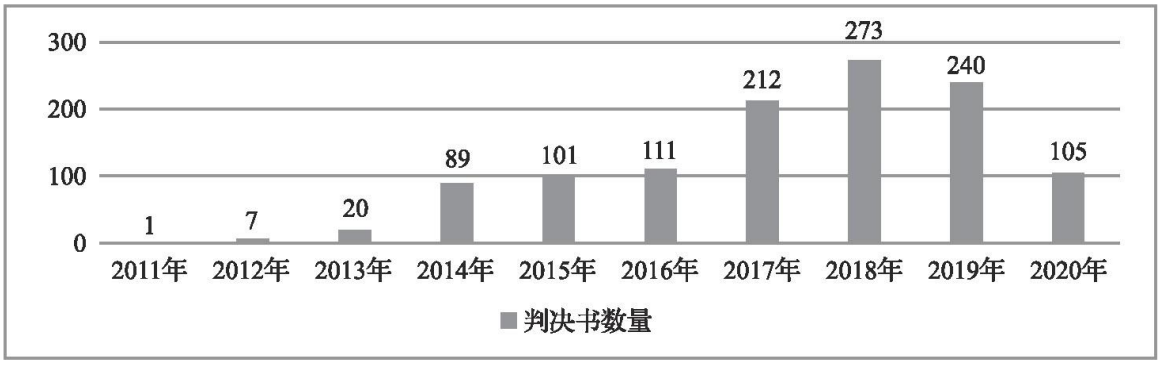


图 5 破坏计算机信息系统罪判决书数量　　下载原图

笔者按分析前罪的方法抽取到 116 份判决书，通过分析以上判决书，发现以该罪判决的犯罪具有如下特征：（1）在前述判决书查明的犯罪中，网络黑灰产犯罪占 82.7%，不以非法牟利为目的的仅有 20 件，主要表现为干扰环境污染检测设备的正常运行，41 以及出于报复目的的破坏计算机信息系统。42 由于破坏计算机信息系统本身不能带来非法利益，犯罪人往往是通过该行为配合其他非法牟利行为的实施，如流量变现、收取广告费等。（2）较多犯罪行为是重置他人苹果手机密码，致使被害人的手机不能正常使用，然后以帮其找回密码为名索取财物，43 也有判决书将为以上犯罪人提供重置手机账号密码链接的行为认定为该罪。44(3）部分判决书将出售干扰应用程序正常运行的程序行为认定为该罪，这类程序有的是干扰、破坏“YY 语音”应用程序正常功能的程序，45 更多的是避绕网吧实名登记监管措施的程序；46 有的犯罪人自己编写或修改程序并出售或出租，有的是从网上买入转手倒卖。（4）部分判决书将内部人员违规修改计算机信息系统数据的行为认定为该罪，其行为并未造成计算机信息系统不能正常运行，如内部人员违规为他人修改交通违章记录。47(5）部分犯罪人删除计算机信息系统数据是为了配合盗窃犯罪的实施，48 按照破坏计算机信息系统罪定罪存在疑问。根据以上特征，对网络黑灰产犯罪适用该罪时要注意以下几点：

1. 如果行为没有直接影响他人计算机信息系统的正常运行不宜认定为该罪。

部分判决书将修改计算机信息系统数据、非法获利较大的行为认定为该罪，49 似乎符合《刑法》第 286 条第 2 款的规定，因为该款并未像第 1 款、第 3 款那样要求危害行为“影响计算机系统正常运行”。笔者认为，如果按此理解该款，会导致对该罪保护法益的混淆，理由是：首先，该罪保护的是公共秩序，具体表现为保护承载各种社会活动的计算机信息系统安全。如果危害行为没有影响计算机信息系统的正常运行，就没有侵害该罪的保护法益，如前述内部人员违规修改交通违章数据的，其侵犯的法益是交通管理机关的行政管理活动，而非计算机信息系统安全管理秩序，没有危害计算机信息系统安全；其次，当前社会各领域活动通过计算机信息系统管理，如果将以上行为认定为该罪，由于该罪的最高法定刑为 15 年有期徒刑，凡是修改计算机信息系统数据且有相关严重后果的，都可能按照从一重罪处罚原则，认定为该罪，导致该罪的泛化适用。因此，该罪行为应当限于能够直接影响计算机信息系统的正常运行，该罪的严重后果与该行为应当具有“二次因果关系”，即，由该行为引起计算机信息系统不能正常运行，因系统不能正常运行导致的严重后果。

2. 出售破坏性程序行为不属于该罪的故意制作、传播行为。

部分判决书将出售避绕网吧实名管理措施的程序认定为该罪，50 认为只要该程序能够用于干扰应用程序正常运行，出售该程序的行为就属于《刑法》第 286 条第 3 款规定的故意传播行为。笔者认为，以上出售行为不直接影响计算机信息系统的正常运行，

不同于向计算机信息系统施放的行为，后者才属于该罪所要求的传播行为。《刑法》第 286 条第 3 款规定的故意、传播计算机病毒等破坏性程序，是指将其投入运行并发挥出破坏计算机信息系统的作用，而非包括向他人（非计算机信息系统）提供该程序。前述行为应当结合其与下游行为人是否具有共同犯罪关系，考虑认定为破坏计算机信息系统罪的共犯或者帮助信息网络犯罪活动罪，而不能单独构成该罪。

3. 没有利用计算机信息系统特性干扰计算机信息系统正常运行的，不应认定为该罪。有判决书将“对需要排放的污水进行稀释的方式，干扰 COD 在线监控设备的采样”的行为认定为该罪。51 笔者认为，该案中的行为不应认定为该罪，原因是：首先，该案中的行为是对检测对象进行稀释，只是影响了检测结果，而没有造成在线监控设备不能正常运行，其后果也不是因检测系统不能正常运行所致；其次，该案中的行为并未利用计算机信息系统的技术特性，不属于该罪的危害行为。对计算机信息系统进行物理破坏、拔电源，也能造成计算机信息系统不能正常运行，这些行为只能构成故意毁坏财物罪或一般破坏行为，不应认定为该罪。

4. 为了实施盗窃、敲诈勒索犯罪而破坏计算机信息系统的，一般不认定为该罪。该类行为构成牵连犯，一般应当按照目的行为定罪，但是，如果按照破坏计算机信息系统罪处罚更重的，应当认定为该罪。

三、以妨害信息网络安全管理秩序犯罪立法规制的刑法问题

惩治网络黑灰产犯罪既可以按其目的行为适用传统犯罪立法，也可以按其手段行为适用侵犯计算机信息系统安全犯罪立法。近年来，网络黑灰产犯罪演变出独立的中间性犯罪，表现为利用计算机信息系统而不是侵犯计算机信息系统安全。同时，其既不满足传统犯罪实行犯的构成特征，也不同于传统犯罪的共犯或未完成犯罪形态，难以按前述两类犯罪定罪处罚。为了遏制新型网络犯罪，2015 年通过的《刑法修正案（九）》增设了三种妨害信息网络安全管理秩序犯罪，2019 年 6 月“两高”通过了《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》（以下简称《解释》），解决了前述三罪立法适用中的大部分问题，但是，司法适用中还存在一些问题，以下具体分析。

（一）拒不履行信息网络安全管理义务罪

笔者在裁判文书网、无讼网和北大法意上搜集以拒不履行信息网络安全管理义务罪定罪处罚的刑事判决书，截止 2020 年 11 月 1 日，只收集到以该罪判决的刑事判决书 2 份，一起是胡某非法提供 VPN 服务案，52 另一起是朱某销售翻墙软件和非法提供 VPN 服务案，53 另有 1 份刑事判决书认定何某某开设赌场成立该罪，但按其他罪名定罪处罚。54 该 3 件刑事判决书具有以下特点：（1）前述判决的时间都是 2018 年 9 月至 12 月之间，处于前述司法解释生效之前。2015 年 10 月 1 日《刑法修正案（九）》生效后，司法机关对如何适用该罪立法存在疑问，导致该罪适用率极低，即使在前述解释施行之后，以上疑问仍然没有消除，没有新的判决。（2）前述判决将违反禁止性规定的行为认定为拒不履行信息网络安全管理义务行为。胡某非法提供 VPN 服务案和朱某销售翻墙软件和非法提供 VPN 服务案中的提供非法搭建的国际联网通道行为，何某某开设赌场案中的不制止参赌人员违法标注和转移游戏币行为，被认定为该罪行为。

笔者认为，以上 3 份判决书对以上涉案行为定性错误，理由是：（1）网络服务提供者提供的必须是合法的网络服务，而以上涉案行为本身是违法行为。胡某、朱某的行为是违反《计算机信息网络国际联网管理暂行规定》第 6 条和第 13 条规定的行为，何某某的行为本身就是开设赌场罪行为，与不履行信息网络安全管理义务行为的性质不同。（2）胡某、朱某的行为不在刑法规制的范围内，如果确有必要追究刑事责任，应通过修改立法来实现，如前文提到的扩展《刑法》第 285 条第 3 款规定的处罚范围。何某

某在开设赌场过程中的不制止参赌人员违法标注和转移游戏币行为，属于刑法上不可期待的行为，不应单独认定为犯罪。

从前述判决书和以该罪判决的案件数量极低的情况看，拒不履行信息网络安全管理义务罪立法对网络黑灰产犯罪的适用表现出“滞胀化”特征，少数案件出现不当扩大适用，而空置化成为大趋势，这说明该罪立法及其司法适用仍有问题需要解决。

前述《解释》对拒不履行信息网络安全管理义务罪的构成要件要素进行解释，包括网络服务提供者的范围、监管机关责令改正的认定标准以及四种严重情节的认定，解决了该罪司法认定中的多数问题。笔者认为，还应注意以下两点：

1. 依法合理认定信息网络安全管理义务的范围。

首先，认定网络服务提供者的信息网络安全管理义务要遵守法律层级的限制。目前只有《网络安全法》《反恐怖主义法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《国务院互联网信息服务管理办法》是该义务的法律依据。其次，要根据该罪的成立条件，对义务内容进行实质限制。信息网络安全管理义务应限于能够产生《刑法》第 286 条之一规定的后果之义务，即造成“违法信息传播”“用户信息泄露”“刑事案件证据灭失”及相当的后果，不应对该条第 4 项规定的“其他严重情节”进行无限制的扩大解释。这是因为，“该罪是法定犯和不作为犯，不直接引起危害后果，虽有违法性但危害性程度低，只有在未防止他人违法行为或者系统危险导致严重后果，才具备了应受刑罚处罚的现实可能性和必要性，因此，应以造成严重结果作为评价情节严重的基础。对比作为同样违反管理义务的玩忽职守罪和消防责任事故罪，后二罪都以造成严重后果为构成要件，而该罪既不是危害公共安全罪，犯罪性质不如消防责任事故罪严重，其义务性质也低于国家机关工作人员的职责。如果没有发生严重后果，仅具有其他主观方面或者危害行为方面的严重情节，不足认定危害行为达到了应受刑罚处罚的严重程度。”55 违反网络用户身份实名验证和服务限制义务等，与以上后果不具有刑法上的因果关系，不能制造出刑法所不允许的风险，56 不应纳入该罪规定的义务范围。

2. 对情节要件进行合理评价。

前述《解释》对《刑法》第 286 条之一的第 1 项至第 3 项规定的情节进行了类型化、数量化解释，指导了该罪的正确适用。但是，该《解释》第 6 条对其第 4 项规定的“其他情节严重”有扩大解释之嫌。例如，该条规定的“其他严重情节”包括“对绝大多数用户日志未留存或者未落实真实身份信息认证义务的”“二年内经多次责令改正拒不改正的”，二者都属于对危害行为本身的评价，本身不引起危害后果或造成危害事实，与该条规定第 3 至 6 项规定的后果性情节不同。《网络安全法》等法律法规对违反实名认证、限制提供服务等义务规定了较严厉的行政法律责任，前述《解释》将二者其解释为违反刑法义务的严重情节，追究刑事责任，属于以刑代管，不合理地扩大了该罪的处罚范围。笔者认为，对“其他严重情节”的解释，应比照前三项情节规定进行同类解释，同时，对比相应行政违法行为进行体系性解释，57 从危害后果或危害事实方面确定评价标准，建立基本均衡的情节评价规则。

（二）非法利用信息网络罪

按照分析前罪的方法，笔者搜集到 2015 年 11 月 1 日到 2020 年 11 月 1 日期间以非法利用信息网络罪定罪的刑事判决书共 267 份，各年判决书数量如图 6 所示。以上判决书认定的犯罪行为中，绝大多数是以非法牟利为目的的网络黑灰产行为，少数为网络聚众滋事行为，表明该罪立法在惩治网络黑灰产犯罪中发挥了重要作用。

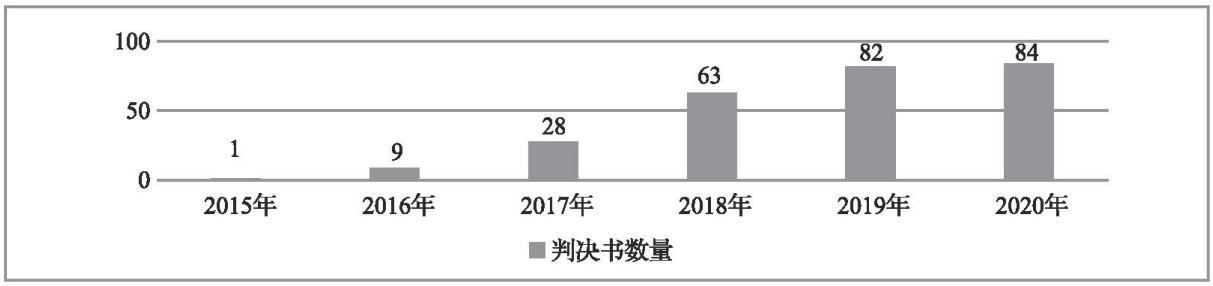


图 6 非法利用信息网络罪判决书数量　　下载原图

根据非法利用信息网络罪立法的规定，笔者将前述判决书中查明的犯罪行为分为四类，各类判决书数量如图表 7 所示，其中，发布违法犯罪信息的案件数最高，有 3 件案件判决书对犯罪事实的描述不明，或者明显不属于前述三类危害行为。58

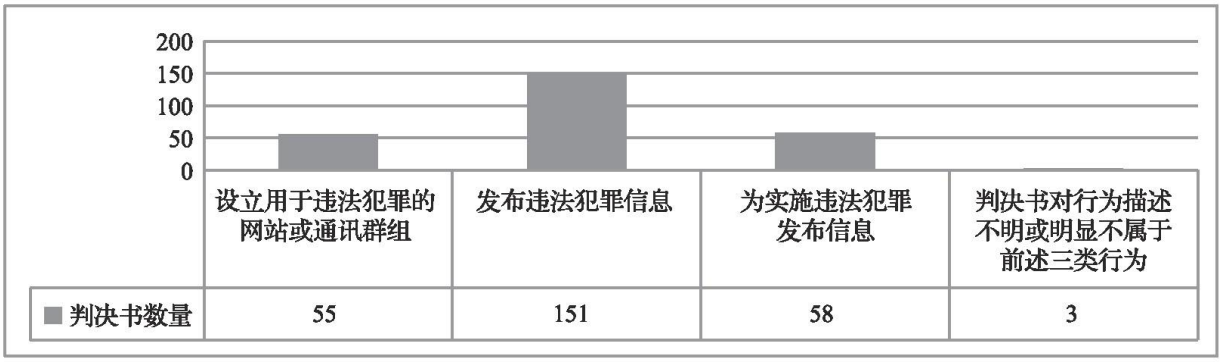


图 7 非法利用信息网络的典型行为类型　　下载原图

具体而言，最终以该罪判决的案件具有以下特点：

1. 下游违法犯罪类型较为集中，极少数判决书有扩大处罚范围的倾向。

该罪行为指向的下游违法犯罪类型较为集中，主要是介绍卖淫嫖娼、销售违禁管制物品、网络赌博、诈骗等四类违法犯罪行为。其中，介绍卖淫嫖娼占大部分，发布违法犯罪信息的 151 件案件主要是发布招嫖信息案件，59 设立用于违法犯罪的网站或通信群组的 55 件案件也主要是建立通信群组供他人发布招嫖信息或介绍卖淫嫖娼。60 在该罪立法适用初期，有个别判决书将该罪的下游违法犯罪放得过宽。61

2. 该罪行为的积量构罪特征明显，与司法解释规定不完全相符。

该罪行为不直接侵犯下游违法犯罪侵害的法益，社会危害性比后者更低，是在较长时间内大量实施该罪行为，累积危害达到情节严重的程度，具有积量构罪特征。以上判决书认定犯罪成立时，依据的事实证据大多是发布违法犯罪信息数量达到几千条以上，或者向几千个以上群组成员账号的通信群组中发布违法犯罪信息，62 仅有极少数案件认定的犯罪行为是设立假冒中央司法机关网站的行为。63 如果行为人仅设立 3 个用于违法犯罪的网站或 5 个通信群组，注册账号或群组成员账号数量未达较大的，尚无判决书将此类行为认定为犯罪，这与《解释》第 10 条的规定不一致。

3. 该罪行为是兼有预备行为和帮助行为性质。

在以上判决书查明的犯罪事实中，部分犯罪人是帮助他人实施下游违法犯罪并从中牟取非法利益，如为他人发布网络赌博信息并收取所谓推广费，64 或者是设立用于卖淫嫖娼活动的通信群组并向加入者收取入群费，65 也有部分犯罪人是为了自己实施下游违法犯罪，如建立用于违法犯罪的通信群组并发布违法犯罪信息。66 因此，将该罪解读为预备犯、帮助犯或其正犯化与司法实践状况不相符。67

4. 该罪行为随着信息技术的发展应用而有所扩展。

该罪行为之一是设立用于违法犯罪的网站或通信群组，行为对象限定为网站和通信群组。随着信息技术的发展应用，App 和小程序也能发挥出类似于设立网站和通信群组的发布信息和联络用户群体的作用，由于它们依托后台网络服务系统，因此，虽然行为人没有设立传统意义的网站和通信群组，但是，其行为效果实际上与之没有区别。针对非法利用信息网络犯罪的这种发展趋势，已有判决将犯罪人制作并提供 App 认定为该罪，从而在司法实践中扩展了该罪危害行为范围。68 笔者认为，该判决具有一定的合理性，需要反思我国网络犯罪立法设定的罪状过于具体，在未来修改立法时应当考虑信息技术的发展规律，采用兼有列举和定性描述的罪状表述。

根据以上特征，司法机关办理该罪案件时要注意以下几点：

1.如果单次危害行为的社会危害性达到应受刑罚处罚程度，出现该罪与下游犯罪或其预备犯、未遂犯或帮助犯的竞合时，不宜以非法利用信息网络罪定罪处罚。有部分判决书将以牟利为目的传播淫秽电子信息行为认定为该罪，在构成传播淫秽物品牟利罪与该罪的竞合时，选择以该罪定罪处罚。69 该罪是传播违法犯罪信息类犯罪，与传播淫秽电子信息犯罪之间存在一般犯罪与特殊犯罪的关系，后者入罪门槛更低，法定刑更重，在案件证据查实的情况下，一般应以后罪定罪处罚。基于前述相同的理由，在出现该罪与其他犯罪及其共犯或未完成形态犯罪竞合时，如果符合从一重罪处罚原则，一般应以后者犯罪定罪处罚。70 只有在按后者犯罪认定存在证据等方面障碍时，才以非法利用信息网络罪定罪处罚，但不宜将入罪标准放得太低。前述《解释》第 10 条第 1 项规定，“假冒国家机关、金融机构名义，设立用于实施违法犯罪活动的网站的”，属于非法利用信息网络罪的“情节严重”，将认定标准放得过松。建议在司法实务中，将国家机关按照县级以上国家机关、金融机构按照分行级以上金融机构的标准来把握。

2.低量损害行为范围不应太宽。在该罪的罪刑构造中，低量损害行为是倍增危害量的基础，如果单次危害行为的危害基本量过低，不仅要求更高的积数才能使行为整体达到应受刑罚处罚的程度，而且，会使该罪的适用过分扩张，错误地处罚本应由民事、行政法律调整的一般违法行为。前述《解释》第 7 条规定，“刑法第二百八十七条之一规定的‘违法犯罪’，包括犯罪行为和属于刑法分则规定的行为类型但尚未构成犯罪的违法行为”，合理地限定了下游违法行为的范围，避免了该罪的下游违法行为不构成犯罪，而较之危害性更低的相关帮助、未完成性质行为因为“触网”而致罪。这一解释规定符合刑法教义学理论，71 在司法实践中应当遵照执行，防止该罪泛化适用。

3.入罪的积数标准不应定得太低。积数作为评价“情节严重”的客观因素，在危害行为“质变”中发挥着重要作用，如果将积数标准定得太低，对于较低危害程度的危害行为而言，就难以实现行为整体的犯罪化，导致该罪的不当适用。前述《解释》第 10 条第 2 项、第 3 项规定，“设立用于实施违法犯罪活动的网站，数量达到三个以上或者注册账号数累计达到二千以上的”和“设立用于实施违法犯罪活动的通讯群组，数量达到五个以上或者群组成员账号数累计达到一千以上的”属于情节严重。该规定的合理性值得商榷：以上规定对违法犯罪活动的范围不作限制，可以涵盖刑法分则中轻罪行为，也不限定发布信息行为影响的人员账户数量，只要设立的网站数达到 3 个或者通信群组数达到 5 个，就可以认定该罪成立。笔者认为，以上情节并非都达到了应受刑罚处罚的严重程度，如设立用于侮辱他人的通信群组 5 个，但群组成员账号数累积只有十几人的，就不适合作为犯罪处理。建议在司法实务中，根据违法犯罪的严重性质进行区别对待：如果是用于实施最高法定刑在五年有期徒刑以上的犯罪行为的，按前述《解释》第 10 条的规定认定“情节严重”；如果是用于其他违法犯罪的，应当

同时要求“注册账号数累计达到二千以上”“群组成员账号数累计达到一千以上”，才能认定情节严重，以避免打击面过宽。

（三）帮助信息网络安全管理秩序罪

按照分析前罪的方法，笔者搜集到 2015 年 11 月 1 日到 2020 年 11 月 1 日期间以帮助信息网络犯罪活动罪定罪的刑事判决书共 265 份，各年判决书数量如图 8 所示。2018 年后以该罪判决的案件数量增长迅速，其查明的犯罪行为全部是以非法牟利为目的的网络黑灰产行为。

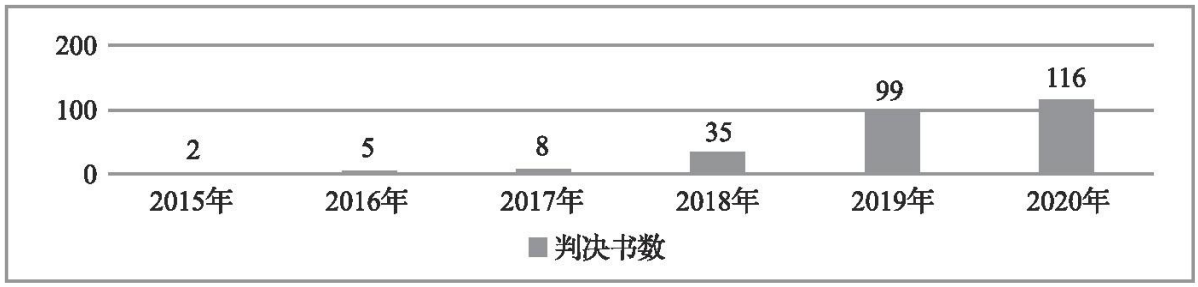


图 8 帮助信息网络安全管理秩序罪判决书数量　　下载原图

以上黑灰产犯罪都是与电信网络诈骗犯罪互生互利的支持行为。其中，为下游犯罪提供银行卡、微信或支付宝收款账户、对公账户等支付结算工具的案件数为 92 件，提供广告推广的案件为 33 件，提供网络技术支持的案件为 28 件，运行多卡宝、GOIP 等卡池的案件为 27 件，如下图 9 所示。以上行为对电信网络诈骗犯罪的实施起关键作用，不只是增加后者犯罪的隐蔽性和反侦查能力，没有以上行为的支持，电信网络诈骗犯罪就不能实施或完成，因此，遏制以上犯罪行为对有效控制电信网络诈骗犯罪至关重要。换言之，该罪立法对遏制电信网络诈骗等牟利型网络犯罪发挥了重要作用。

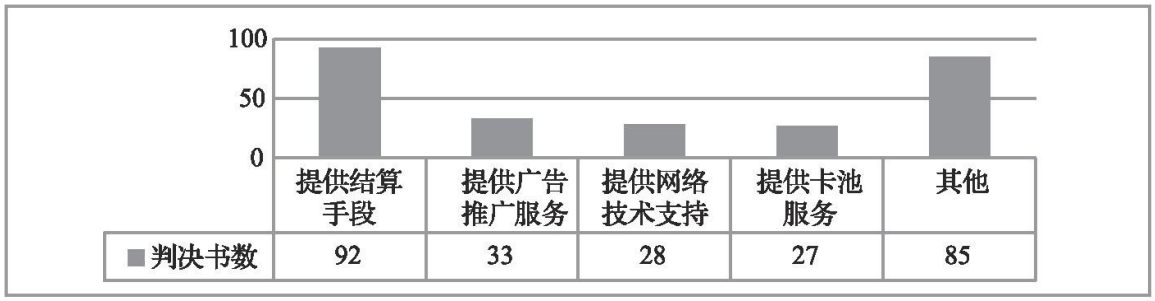


图 9 帮助信息网络的典型行为类型　　下载原图

为了分析以上犯罪行为的构造特征，笔者将以上案件分为 4 类：1.行为人明知下游犯罪的具体情况，并与下游犯罪人有双向意思联络的；2.行为人仅概括认识下游犯罪是严重违法犯罪行为，但对其行为的具体性质没有认识，对下游犯罪人的责任能力状况及其是否实施实施没有确定的认识；3.下游犯罪人为相互无联系的多人或多个群体，行为人对其认识情况与第二类案件相同，至少有 1 个下游犯罪人的罪行严重，对其单次帮助行为成立犯罪；4.下游犯罪人为相互无联系的多人，各下游犯罪只能构成轻罪或无证据证明达到犯罪的严重程度，行为人对其认识情况与第二类案件相同，对其单次帮助行为不成立犯罪。分类统计结果如下图 10 所示。

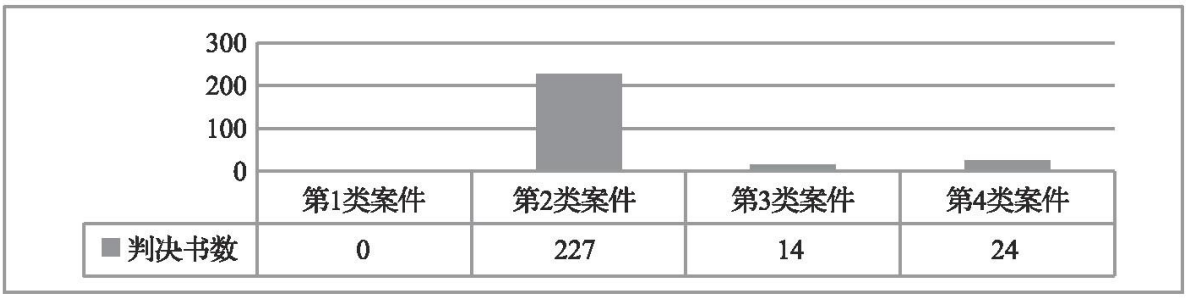


图 1 0 帮助信息网络罪的上下游意思联络类型　　下载原图

分析以上判决书的统计结果，可得出如下结论：

1. 第一类案件数量为零，说明以上判决将该罪行为与典型的帮助犯相区别。

2. 第二类案件数量最大，说明该罪立法主要解决行为人概括认识下游犯罪情形下帮助他人犯罪的定罪问题。按照帮助犯的理论解释，行为人概括、片面认识他人实施具体犯罪行为的，也可以成立帮助犯。但是，如果行为人对下游犯罪人的行为性质缺乏具体的认识，如提供的银行卡被下游犯罪人用于何种犯罪没有认识、也不关心，仅查到该银行卡被用于非法转账部分涉案资金，72 将其按照下游犯罪的共犯定罪会遇到困难，这是前述判决书选择以该罪定罪的主要原因。但是，以上案件中，也有一些判决书将行为人明知下游犯罪的具体性质向其提供帮助的行为按照该罪处罚，73 表明以该罪判决的案件中存在着下游犯罪的帮助犯和该罪的竞合，可能是审判机关认为按照下游犯罪的帮助犯处罚太重，选择以该罪定罪处罚，例如帮助行为在客观上是可以独立存在的合法行为，如网站维护和技术支持等，或者犯罪所得较少，如仅比正常业务收费略高等。

3. 第三类案件数量不大，代表了实际操作中的一种定罪模式。在帮助特定人或多人的犯罪案件中，有可能只能查实某一次下游犯罪的严重危害后果，而更多的后果无法查明或者达不到追究刑事责任的程度。74 此种情形下，如果按照下游犯罪的帮助犯处罚，除了因认识因素不确定而难以认定存在共同犯罪故意，行为人实际帮助的下游犯罪引起的危害后果远不止查明的结果，按照该罪定罪处罚则可以将其他帮助行为纳入量刑考虑因素。

4. 第四类案件的数量也不大，代表了积量构罪的定罪模式。75 行为人帮助了多个相互无关联的下游犯罪，但所有下游犯罪都未查明，或者未查实造成严重危害后果，按照其帮助犯难以定罪处罚，76 该类案件的判决书选择按照该罪定罪。该类案件的数量并不小，表明司法机关已经接受了按积量构罪的定罪方式处理“海量行为×低量损害”式的犯罪活动。

结合以上特征，司法机关办理该罪案件时要注意以下几点：

第一，帮助信息网络犯罪活动罪是独立的犯罪，“明知他人利用信息网络实施犯罪”是其主观构成要件要素，不应将其按照帮助犯认定。持帮助犯论的学者认为，“明知他人利用信息网络实施犯罪”是共同犯罪故意（片面帮助犯的犯罪故意）的构成要素，将该罪解释为帮助犯或者帮助犯的正犯化，该种观点与《解释》相关规定不一致：（1）下游违法行为人可以不是刑法意义上的犯罪主体。前述《解释》第 13 条规定，“被帮助对象实施的犯罪行为可以确认，但尚未到案、尚未依法裁判或者因未达到刑事责任年龄等原因依法未予追究刑事责任的，不影响帮助信息网络犯罪活动罪的认定。”该条明确将该罪的下游违法犯罪行为人包括不负刑事责任的自然人，行为人帮助这些人时，依据我国刑法的规定和共犯从属性理论，不能成立帮助犯，而只可能成立独立的犯罪，要么构成该罪，要么构成所帮助之罪的间接正犯。（2）无需证明下游行为成立

犯罪。前述《解释》第 12 条第 2 款规定，“实施前款规定的行为，确因客观条件限制无法查证被帮助对象是否达到犯罪的程度，但相关数额总计达到前款第二项至第四项规定标准五倍以上，或者造成特别严重后果的，应当以帮助信息网络犯罪活动罪追究行为人的刑事责任。”该款取消了司法机关查证被帮助的行为成立犯罪的法律义务。虽然采取不法论立场的共犯理论认为可以成立无实行犯的帮助犯，但该观点与我国刑法的规定不符。笔者认为，帮助信息网络犯罪活动罪立法的目的是打击独立的网络帮助行为犯罪，按照帮助犯定罪处罚将使其失去存在意义。“明知他人利用信息网络实施犯罪”是该罪的主观构成要件要素，只要行为人认识到他人利用信息网络实施的是刑法分则规定的行为类型，并且已经达到严重危害社会的程度，在此认识因素基础上，仍然故意向其提供技术支持和帮助，表明其具有严重的主观恶性，结合其客观方面的行为及严重情节，应当认为达到了应受刑罚处罚的严重程度，无需从被帮助者行为侵犯法益的因果性上证成犯罪成立。

第二，“他人利用信息网络实施犯罪”中的“犯罪”应当解释为犯罪行为和属于刑法分则规定的行为类型的严重违法行为。非法利用信息网络罪和帮助信息网络犯罪活动罪属于相同性质的独立犯罪，法定刑也相同，前者规定的“违法犯罪”和后者中的“犯罪”所起作用都是对其主观违法要件要素的限制，二者的内涵应当一致。前述《解释》第 7 条将非法利用信息网络罪中“违法犯罪”解释为“犯罪行为和属于刑法分则规定的行为类型但尚未构成犯罪的违法行为”，该罪中的“犯罪”可以作此相同解释。考虑到二者对下游行为表述上的区别，可以将该罪中的“犯罪”解释为“犯罪行为和属于刑法分则规定的行为类型的严重违法行为”。

第三，该罪包括单次构罪和积量构罪两种定罪模式，对前者情形应当优先考虑认定为下游犯罪的帮助犯。《解释》第 12 条规定了该罪的“情节严重”的 7 种情形，其第 1 款第 1 项规定的情节是“为三个以上对象提供帮助的”，这显然是积量构罪的犯罪成立模式，原因是，帮助犯从属于实行犯，帮助行为指向的必然是某个特定犯罪人及其特定实行行为，对不同对象的不同性质犯罪提供帮助，不可能从整体上评价为帮助犯。因此，前述《解释》设置该项严重情节否定了该罪的帮助犯性质。不过，在单次构罪的情形下，行为人可以同时构成帮助犯和帮助信息网络犯罪活动罪，考虑到行为人的行为指向特定犯罪，除非违反该条第 3 款的规定，一般应当认定为帮助犯。当被帮助者因不具有刑事责任能力等原因不承担刑事责任，或者客观上无法追究其刑事责任，仍应按照帮助信息网络犯罪活动罪定罪处罚。

结语

网络黑灰产活动是具有一定独立性、常业性的非法牟利型网络违法犯罪，通过传统犯罪立法进行合理扩张解释，能解决相当多网络黑灰产犯罪案件的法律适用问题，但是，也不应过度依赖扩张解释方法，对相关构成要件的解释应在合理限度内。

当传统犯罪和侵犯公民个人信息罪不能规制网络黑灰产犯罪时，可以按手段行为入罪，适用侵犯计算机信息系统安全犯罪。当适用前述两类犯罪立法遇到困难时，还可以按照妨害信息网络安全管理秩序犯罪定罪处罚。侵犯计算机信息系统安全犯罪立法和妨害信息网络安全管理秩序犯罪立法不是“象征性立法”，77 与传统犯罪立法一样，它们对惩治网络黑灰产犯罪发挥了重要作用。

侵犯计算机信息系统安全犯罪立法存在缺陷，主要有保护范围狭窄、立法逻辑错误和罪状描述不完整、规制的行为范围不合理等问题，导致司法实践中遇到较多困难，需要及时完善相关立法，不应置之不理或以司法解释、指导性案例替代。妨害信息网络安全管理秩序罪是独立的犯罪，不应以帮助犯、预备犯的构成条件来限制其适用。同

时，该类犯罪具有特殊罪行构造，司法实践中应合理解释其构成要件，避免该类犯罪处罚范围的不当扩张。

注释

[1]以上四方面网络犯罪立法在惩治网络黑灰产犯罪中都发挥了重要作用,由于打击侵犯公民个人信息的黑灰产犯罪有专门的侵犯公民个人信息犯罪立法,以下只讨论其他网络黑灰产犯罪相关法律适用问题。

[2]参见王安异、许姣姣：《诈骗罪中利用信息网络的财产交付--基于最高人民法院指导案例 27 号的分析》,《法学》2015 年第 2 期。

[3]参见北京市朝阳区人民法院刑事判决书,(2013)朝刑初 2584 号。

[4]曲新久：《一个较为科学合理的刑法解释》,《法制日报》2013 年 9 月 13 日。

[5]参见孙万怀、卢恒飞：《刑法应当理性应对网络谣言--对网络造谋司法解释的实证评估》,《法学》2013 年第 11 期。

[6]2013 年 9 月 21 日最高人民法院、最高人民检察院颁布的《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》第 10 条规定：“本解释所称信息网络,包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络,以及向公众开放的局域网络。”

[7]2013 年 7 月 15 日最高人民法院、最高人民检察院颁布的《关于办理寻衅滋事刑事案件适用法律若干问题的解释》第 5 条的规定,“在车站、码头、机场、医院、商场、公园、影剧院、展览会、运动场或者其他公共场所起哄闹事,应当根据公共场所的性质、公共活动的重要程度、公共场所的人数、起哄闹事的时间、公共场所受影响的范围与程度等因素,综合判断是否‘造成公共场所秩序严重混乱’”。对公共场所的种类、特性和范围进行限定,有自然人在场是公共场所的基本特性。

[8]《刑法》第 120 条之五(强制穿戴宣扬恐怖主义、极端主义服饰、标志罪)、第 130 条(非法携带枪支、弹药、管制刀具、危险物品危及公共安全罪)、第 236 条(强奸罪)、第 237 条(强制猥亵、侮辱罪、猥亵儿童罪)、第 291 条第 1 款(聚众扰乱公共场所秩序、交通秩序罪)、第 292 条(聚众斗殴罪)、第 293 条(寻衅滋事罪)规定中都使用了“公共场所”。

[9]梁根林：《传统犯罪网络化：归责障碍、刑法应对与教义限缩》,《中国法学》2017 年第 2 期。

[10]张明楷：《非法获取虚拟财产的行为性质》,《法学》2015 年第 3 期。

[11]陈云良、周新：《虚拟财产刑法保护路径之选择》,《法学评论》2009 年第 2 期。

[12]刘明祥：《窃取网络虚拟财产行为定性探究》,《法学》2016 年第 1 期。

[13]同前注[12]。

[14]参见皮勇：《论中国网络空间犯罪立法的本土化与国际化》,《比较法研究》2020 年第 1 期。

[15]参见内蒙古自治区呼和浩特市新城区人民法院刑事判决书,(2017)内 0102 刑初 269 号。

[16]参见安徽省亳州市谯城区人民法院刑事判决书,(2018)皖 1602 刑初 481 号。

[17]后文分析其他网络犯罪立法时,如果搜集到的判决书数量超过 300 份,则按照与这里相同的做法随机抽取 100-200 份判决书进行分析。

[18]参见广东省深圳市福田区人民法院刑事判决书,(2018)粤 0304 刑初 925 号

[19]参见重庆市沙坪坝区人民法院刑事判决书,(2016)渝 0106 刑初 1393 号。

[20]参见广东省深圳市南山区人民法院刑事判决书,(2015)深南法刑初 1014 号。

[21]参见上海市静安区人民法院刑事判决书,(2019)沪 0106 刑初 1793 号。

[22]参见湖南省湘潭市岳塘区人民法院刑事判决书,(2010)岳刑初第 62 号
[23]参见皮勇：《〈网络犯罪公约〉框架下的美国网络犯罪立法：特立与趋同》,《国外社会科学》2020 年第 5 期。
[24]参见重庆市万州区人民法院刑事判决书,(2018)渝 0101 刑初 396 号。
[25]参见广东省河源市源城区人民法院刑事判决书,(2018)粤 1602 刑初 441 号。
[26]参见江苏省南京市栖霞区人民法院刑事判决书,(2017)苏 0113 刑初 32 号。
[27]参见江苏省新沂市人民法院刑事判决书,(2018)苏 0381 刑初 211 号。
[28]参见湖北省宜昌市西陵区人民法院刑事判决书,(2020)鄂 0502 刑初 2 号。
[29]参见安徽省池州市贵池区人民法院刑事判决书,(2015)贵刑初 00346 号。
[30]同前注[29]。
[31]参见于志刚：《口袋罪的时代变迁、当前乱象与消减思路》,《法学家》2013 年第 3 期。
[32]参见福建省大田县人民法院刑事判决书,(2019)闽 0425 刑初 150 号。
[33]参见天津市宝坻区人民法院刑事判决书,(2020)津 0115 刑初 245 号。
[34]参见江苏省涟水县人民法院刑事判决书,(2015)涟刑初 00570 号。
[35]参见黑龙江省哈尔滨市呼兰区人民法院刑事判决书,(2016)黑 0111 刑初 63 号。
[36]参见山西省太原市迎泽区人民法院刑事判决书,(2017)晋 0106 刑初 583 号。
[37]参见江苏省淮安市清河区人民法院刑事判决书,(2015)河刑初 00098 号。
[38]See Explanatory Report of Convention on Cybercrime,Paragraph 71-78.
[39]See S.Rep.No.99-432,at 13(1986),reprinted in 1986 U.S.C.C.A.N.2479,2491.
[40]同前注[14]。
[41]参见辽宁省朝阳市龙城区人民法院刑事判决书,(2018)辽 1303 刑初 94 号。
[42]参见杭州市余杭区人民法院刑事判决书,(2014)杭余刑初 38 号。
[43]参见江苏省徐州市云龙区人民法院刑事判决书,(2017)苏 0303 刑初 134 号。
[44]参见江苏省江阴市人民法院刑事判决书,(2017)苏 0281 刑初 2612 号。
[45]参见江苏省南京市雨花台区人民法院刑事判决书,(2016)苏 0114 刑初 332 号。
[46]参见湖北省钟祥市人民法院刑事判决书,(2015)鄂钟祥刑初 00147 号。
[47]参见福建省福清市人民法院刑事判决书,(2016)闽 0181 刑初 513 号。
[48]参见浙江省瑞安市人民法院刑事判决书,(2013)温瑞刑初 2008 号。
[49]参见山东省临沂市兰山区人民法院刑事判决书,(2016)鲁 1302 刑初 839 号。
[50]参见河南省内乡县人民法院刑事判决书,(2014)内刑初 186 号。
[51]参见江苏省盐城市大丰区人民法院刑事判决书,(2019)苏 0982 刑初 46 号。
[52]参见上海市浦东新区人民法院刑事判决书,(2018)沪 0115 刑初 2974 号。
[53]参见荆州市荆州区人民法院刑事判决书,(2018)鄂 1003 刑初 150 号。
[54]参见南昌市东湖区人民法院刑事判决书,(2018)赣 0102 刑初 585 号。
[55]皮勇：《论新型网络犯罪立法及其适用》,《中国社会科学》2018 年第 10 期。
[56]参见陈兴良：《从归因到归责：客观归责理论研究》,《法学研究》2006 年第 2 期。
[57]参见柏浪涛：《罪量要素的性质与评价》,《上海政法学院学报》2017 年第 1 期。
[58]参见北京市海淀区人民法院刑事判决书,(2019)京 0108 刑初 157 号。该案查明的犯罪行为是向他人出售破坏性计算机程序,不属于非法利用信息网络罪的规制范围,也不能适用《刑法》第 285 条第 3 款的规定。
[59]参见上海市宝山区人民法院刑事判决书,(2020)沪 0113 刑初 885 号。
[60]参见上海市金山区人民法院刑事判决书,(2020)沪 0116 刑初 911 号。

[61]参见新疆维吾尔自治区高级人民法院伊犁哈萨克自治州分院刑事判决书,(2017)新 40 刑终 78 号。
[62]参见上海市金山区人民法院刑事判决书,(2020)沪 0116 刑初 768 号。
[63]参见北京市海淀区人民法院刑事判决书,(2016)京 0108 刑初 2019 号。
[64]参见广东省湛江市霞山区人民法院刑事判决书,(2020)粤 0803 刑初 368 号。
[65]参见辽宁省葫芦岛市连山区人民法院刑事判决书,(2020)辽 1402 刑初 160 号。
[66]参见吉林省梅河口市人民法院刑事判决书,(2020)吉 0581 刑初 134 号。
[67]于志刚：《网络空间中犯罪预备行为的制裁思路与体系完善---截至〈刑法修正案(九)〉》的网络预备行为规制体系的反思》,《法学家》2017 年第 6 期。
[68]参见北京市大兴区人民法院刑事判决书,(2020)京 0115 刑初 123 号。
[69]参见江苏省盐城市盐都区人民法院刑事判决书,(2018)苏 0903 刑初 252 号。
[70]同前注[55]。
[71]参见欧阳本祺、王倩：《〈刑法修正案(九)〉新增网络犯罪的法律适用》,《江苏行政学院学报》2016 年第 4 期。
[72]参见湖北省南漳县人民法院刑事判决书,(2020)鄂 0624 刑初 17 号。
[73]参见江苏省淮安市淮阴区人民法院刑事判决书,(2019)苏 0804 刑初 503 号
[74]参见河南省商水县人民法院刑事判决书,(2020)豫 1623 刑初 151 号。
[75]同前注[55]。
[76]参见安徽省明光市人民法院刑事判决书,(2019)皖 1182 刑初 212 号。
[77]参见刘艳红：《象征性立法对刑法功能的损害--二十年来中国刑事立法总置评》,《政治与法律》2017 年第 3 期。

5.公安部公布涉网络账号黑色产业链十大典型案例

近年来，公安机关持续加大对电信网络诈骗、网络赌博、网络色情以及从事网络水军、“薅羊毛”、刷单炒信等网络黑产违法犯罪活动的打击整治力度。然而一些不法人员为逃避网络安全监管和公安机关侦查打击，通过非法获取、使用大量网络账号实施网络违法犯罪。对网络账号的非正常需求催生了由恶意注册账号、养号、盗号以及使用非正常手段解除对违规网络账号封禁、非法交易等节点组成的网络账号黑色产业链。

去年，公安部推进“净网 2021” 专项行动，并在专项行动中发起“断号”行动，对网络账号黑色产业链予以依法严厉打击，取得显著战果。2021 年，共抓获行业“内鬼”6000 余名，打掉关停接码、打码、解封、养号、非法交易网络平台 80 余个，收缴“猫池”、卡池设备 1 万余台，查获关停涉案网络账号 1000 余万个。24 日，公安部公布 “断号”行动十大典型案例：

一、广东公安机关破获陈某等人帮助信息网络犯罪活动案。广东网安部门侦查查明，某电信运营商 5 名“内鬼”勾结社会不法人员，为恶意注册、贩卖网络账号牟利的“号商”提供未对外发行的 188 万个手机号和短信网关,涉案金额 8550 余万元,非法获利 3000 余万元。

二、山东公安机关破获徐某等人帮助信息网络犯罪活动案。山东网安部门侦查查明，徐某等人搭建打码平台，为“号商”提供批量识别验证码服务，自动识别网络账号恶意注册、换绑、解封等过程中的验证码，涉案金额 2520 余万元，非法获利 1680 余万元。

三、江苏公安机关破获蒋某等人非法获取计算机信息系统数据案。江苏网安部门侦查查明，蒋某等人搭建提供手机卡、短信验证码交易服务的某接码平台，招揽非法提供手机卡、物联网卡的“卡商”入驻，为“号商”提供用于恶意注册网络账号的手机号和验证码 400 余万组，涉案金额 2000 余万元，蒋某等人非法获利 140 余万元。

四、陕西公安机关破获余某等人侵犯公民个人信息案。陕西网安部门侦查查明，余某等

人搭建某接码平台，招揽“卡商”入驻，为“号商”提供用于恶意注册网络账号的手机号和验证码 85 万组，涉案金额 230 万元，非法获利 140 万元。

五、北京公安机关破获某公司帮助信息网络犯罪活动案。北京网安部门侦查查明，某公司开发一款用于管理网络账号的“云控”平台，在明知客户将网络账号用于赌博和诈骗等违法犯罪活动的情况下，仍为客户提供“养号”服务，涉案金额 550 余万元，非法获利 360 余万元。

六、辽宁公安机关破获杨某等人帮助信息网络犯罪活动案。辽宁网安部门侦查查明，杨某等人搭建“猫池”窝点和网络平台，提供网络账号恶意注册、换绑、解封服务，涉案网络账号 40 余万个，涉案金额 200 余万元，非法获利 40 余万元。

七、湖北公安机关破获李某等人帮助信息网络犯罪活动案。湖北网安部门侦查查明，李某等人搭建 9 个“猫池”窝点和 1 个接码平台，为“号商”提供用于恶意注册网络账号的手机号和验证码，涉案金额 250 余万元，非法获利 110 余万元。

八、陕西公安机关破获訾某等人侵犯公民个人信息案。陕西网安部门侦查查明，訾某等人开发所谓网络账号找回申诉软件，董某等人提供境外手机号和验证码，为骗取他人网络账号的诈骗人员提供所谓“保号”服务（利用所谓申诉软件耗尽被骗网络账号原主人可使用的找回申诉次数，以使原主人无法通过正常申诉找回被骗网络账号），涉案金额 130 余万元，非法获利 80 余万元。

九、广西公安机关破获谢某等人侵犯公民个人信息案。广西网安部门侦查查明，以谢某为首的犯罪团伙流窜至 20 余个村庄，借为村民激活“医保电子凭证”之机，在村民不知情的情况下，非法获取 1.5 万名村民的手机号及验证码 10 万余组，贩卖给“号商”，涉案金额 60 余万元，非法获利 21 万余元。

十、江苏公安机关破获杨某等人侵犯公民个人信息案。江苏网安部门侦查查明，杨某等 41 名电信营业厅、通讯店、银行工作人员利用工作便利，在客户不知情的情况下，非法获取客户的手机号及验证码 4.2 万余组，贩卖给“号商”，涉案金额 150 余万元，非法获利 44 万余元。

公安机关正告不法人员，实施网络黑产违法犯罪，必将受到法律的严惩。接下来，公安机关网安部门将继续加大“断号”行动工作力度，保持对网络黑产违法犯罪的高压严打态势。同时，公安机关提醒大家，一旦发现网络黑产违法犯罪线索，请及时向公安机关报案。

（十七）依法惩治涉未成年人电信网络犯罪 共建清朗网络空间

来源：最高人民检察院网上发布厅 发布时间：2021 年 10 月 18 日

2021 年 1 至 9 月，全国检察机关起诉涉及未成年人的电信网络犯罪 4822 人。其中，利用电信网络实施的诈骗罪 2066 人，占 42.8%；帮助信息网络犯罪活动罪 1205 人，占 25%。涉及未成年人电信网络犯罪既包括未成年人利用电信网络实施犯罪，也包括利用电信网络侵害未成年人犯罪，主要呈现三方面特点，需引起高度重视。

一、未成年人利用电信网络实施犯罪同比增长三成。2021 年 1 至 9 月，检察机关起诉未成年人利用电信网络实施犯罪 2467 人，同比增长 32.6%。由于未成年人易沉迷网络、受到各类不良信息诱导，在遇到问题时，易与网络因素叠加，诱发实施网络犯罪。除虚假交友、骗买游戏装备、骗取客户保证金、信用卡提额诈骗、刷单诈骗等诈骗手法外，还出现了利用网络平台监管漏洞虚假充值、骗取运费险及退货款、诈骗未成年追星族等新型犯罪手段和作案方式。

二、诈骗团伙组织、胁迫、教唆、利诱未成年人实施犯罪问题突出。一些诈骗团伙利用未成年人心智发育不成熟、识别风险能力和自我保护能力弱等特点，以及法律对未成年人从轻、减轻处罚的特殊政策，胁迫、教唆、利诱未成年人参与、实施电信网络诈骗犯罪，甚至利用公司化运作，裹挟未成年人加入跨境诈骗集团。如，利用未成年人涉世未深、急于赚快钱的心理，设置“高薪”“兼职”等诱人入职条件，使未成年人成为诈骗集团业务员；发布租借网络账号、银行卡、电话卡、收款二维码信息，让未成年人在不知不觉中为网络诈骗犯罪提供帮助；发布支付转租中介酬劳等广告信息，使部分未成年人成为收售“两卡”的职业卡商等，严重损害未成年人健康成长，危害社会和谐稳定。

三、未成年在校学生、低龄未成年人受害问题值得关注。随着手机和电脑使用的低龄化，未成年人进行网络游戏、网课、网络购物等时间长、频率高，加之未成年人防骗意识薄弱，遭受网络违法犯罪侵害的风险日益加剧。尤其在新冠肺炎疫情期间，一些不法分子利用未成年学生网上学习、社交之机诈骗钱财。有的在班级群冒充班主任骗取学费、收取爱心捐款。有的以低价出售电子产品、扫码领取虚拟礼物、游戏充值等方式，诱骗未成年人通过网络支付费用。江苏、山东、广东等多地发现，一些不法分子以不满 14 周岁的未成年追星族为诈骗对象，在网络平台发布“明星感谢粉丝”“领取任务”“明星生日回馈”等消息，以充值返现等手段，诱骗未成年人用手机多次扫码，低龄受害人数量大，社会影响恶劣。

针对办案中发现的问题，各级检察机关深入学习贯彻习近平法治思想，认真贯彻落实新修订的未成年人保护法、预防未成年人犯罪法相关规定，依法惩治涉未成年人电信网络犯罪，积极保护未成年人合法权益。**一是**严格落实最高人民法院、最高人民检察院、公安部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》相关规定，对利用未成年人、在校学生、老年人、残疾人实施电信网络诈骗的，依法从严惩处，重点惩治成年人胁迫、教唆、引诱、欺骗未成年人参与电信网络诈骗犯罪组织、帮助信息网络犯罪活动等违法犯罪行为。**二是**在办理此类案件时，特别注意对未成年人主观明知和主从犯认定的审查。检察机关在办理案件时，深入贯彻“少捕慎诉慎押”刑事司法政策，准确甄别未成年人在共同犯罪中的层级地位及作用大小，对于主观恶性不大、犯罪情节较轻，属于初犯、偶犯的未成年人，特别是其中参与时间相对较短、诈骗数额相对较低或者从事辅助性工作并领取少量报酬的，结合其认罪态度和悔罪表现，依法不捕不诉或提出轻缓量刑建议，为他们回归社会预留通道；对于积极主动策划、参加，主观恶性较大的未成年人依法惩治，加强警示教育，体现“宽容不纵容”的工作理念。**三是**严格落实刑事诉讼法特别程序，重点关注涉电信网络诈骗未成年犯罪人融入回归社会以及预防再犯。针对未成年人心智不成熟、在网络空间缺乏辨别力等特点，坚持“教育为主、惩罚为辅”的原则，做到依法少捕、慎诉、少监禁，积极适用附条件不起诉、家庭教育指导等制度。支持和引导专业力量，为网络犯罪未成年人提供网络安全教育、心理疏导、法律咨询等社会化服务，引导未成年人正确使用互联网，自觉抵制不良网络信息。**四是**全面履行刑事、民事、行政、公益诉讼检察职能，深入梳理未成年人网络保护领域存在的问题，依法督促有关部门切实履职，为未成年人健康成长创造良好环境。**五是**根据未成年人法治需要，开展“菜单式”法治教育，为网络诈骗套路“画像”，分析套路、拆解套路，让未成年人提高警惕，建立防犯罪和防被骗的经验防线和心理防线。

下一步，检察机关将进一步加强与相关部门协作配合，全面履行检察职能，依法惩治涉未成年人电信网络犯罪，积极推动完善相关制度机制，对涉罪未成年人依法惩戒和精准帮教，为未成年人健康成长营造良好环境。