国盟信息安全通报

2020 年 7 月 05 日第 219 期

全国售后服务中心

国盟信息安全通报

（第 219 期）

国际信息安全学习联盟

2020 年 07 月 05 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 259 个，其中高危漏洞 104 个、中危漏洞 130 个、低危漏洞 25 个。漏洞平均分值为 5.97。本周收录的漏洞中，涉及 0day 漏洞 83 个（占 32%），其中互联网上出现“Savant Web Server 拒绝服务漏洞、vCloud Director 远程代码执行漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3522 个，与上周（3718 个）环比减少 5%。

主要内容

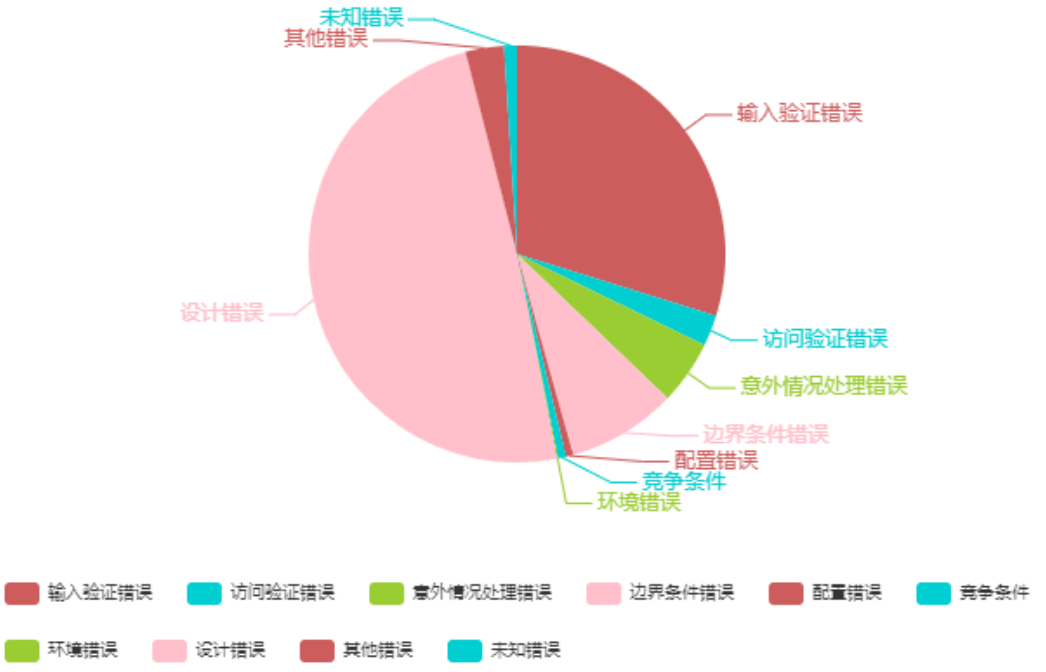
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

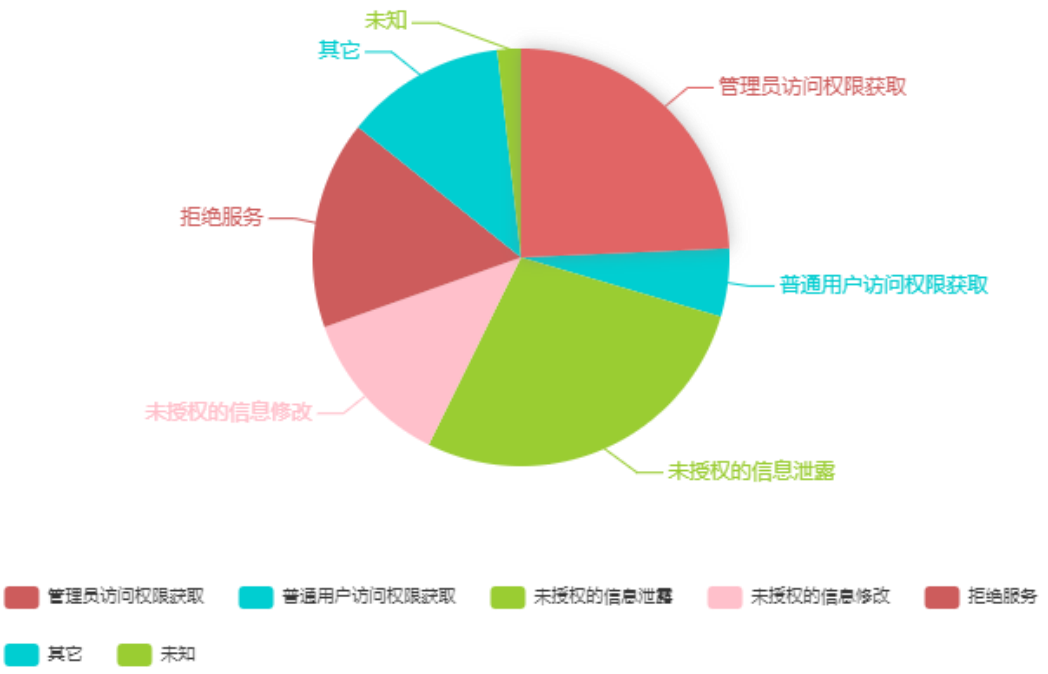
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 259 个，其中高危漏洞 104 个、中危漏洞 130 个、低危漏洞 25 个。漏洞平均分值为 5.97。本周收录的漏洞中，涉及 0day 漏洞 83 个（占 32%），其中互联网上出现“Savant Web Server 拒绝服务漏洞、vCloud Director 远程代码执行漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3522 个，与上周（3718 个）环比减少 5%。

二、安全漏洞增长数量及种类分布情况

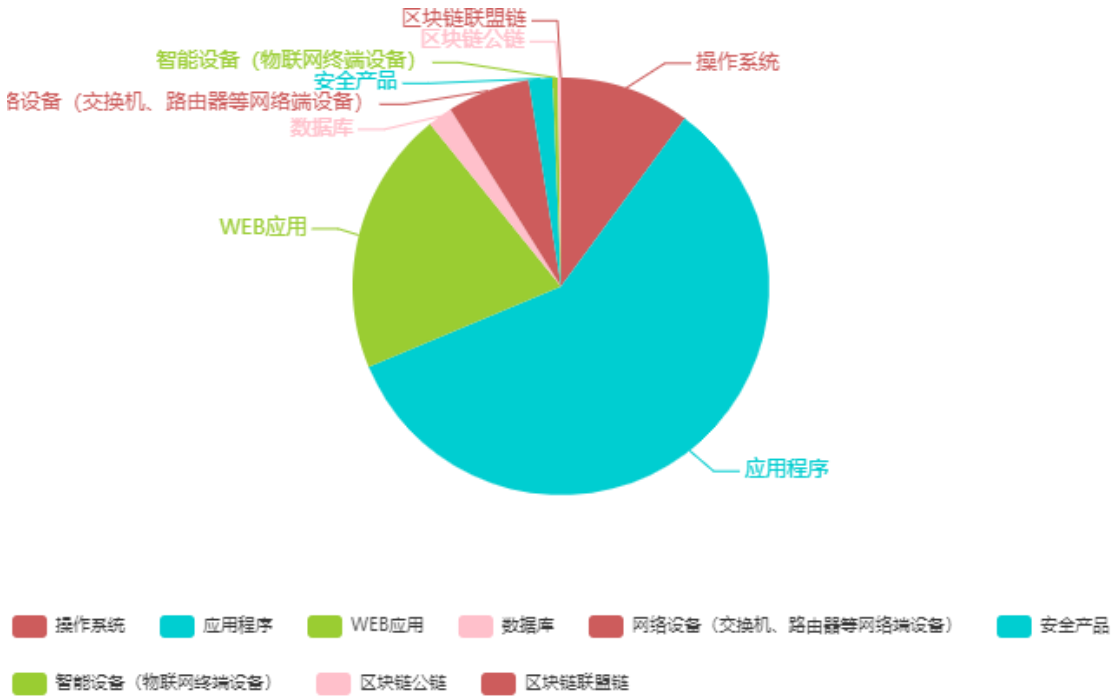
➢ 漏洞产生原因（2020 年 06 月 21 日—2020 年 07 月 05）



➢ 漏洞引发的威胁（2020 年 06 月 21 日—2020 年 07 月 05）



➢ 漏洞影响对象类型（2020 年 06 月 21 日—2020 年 07 月 05）



三、安全产业动态

➢ 我国拟立法确立数据安全保护管理基本制度

2020 年 6 月 28 日，数据安全法草案提请十三届全国人大常委会第二十次会议初次审议。随着信息技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对经济发展、社会治理、人民生活都产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。制定一部数据安全领域的基础性法律十分必要。

《数据安全法（草案）》起草说明

一、关于制定本法的必要性

随着信息技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对经济发展、社会治理、人民生活都产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。党中央对此高度重视，习近平总书记多次作出重要指示批示，提出加快法规制度建设、切实保障国家数据安全等明确要求。党的十九大报告提出，推动互联网、大数据、人工智能和实体经济深度融合。党的十九届四中全会决定明确将数据作为新的生产要素。按照党中央部署和贯彻落实总体国家安全观的要求，制定一部数据安全领域的基础性法律十分必要：一是，数据是国家基础性战略资源，没有数据安全就没有国家安全。因此，应当按照总体国家安全观的要求，通过立法加强数据安全保护，提升国家数据安全保障能力，有效应对数据这一非传统领域的国家安全风险与挑战，切实维护国家主权、安全和发展利益。二是，当前，各类数据的拥有主体多样，处理活动复杂，安全风险加大，必须通过立法建立健

全各项制度措施，切实加强数据安全保护，维护公民、组织的合法权益。三是，发挥数据的基础资源作用和创新引擎作用，加快形成以创新为主要引领和支撑的数字经济，更好服务我国经济社会发展，必须通过立法规范数据活动，完善数据安全治理体系，以安全保发展、以发展促安全。四是，为适应电子政务发展的需要，提升政府决策、管理、服务的科学性和效率，应当通过立法明确政务数据安全管理制度和开放利用规则，大力推进政务数据资源开放和开发利用。

二、关于起草工作和把握的几点

按照党中央部署，制定数据安全法列入了十三届全国人大常委会立法规划和年度立法工作计划。2018 年 10 月，全国人大常委会法工委会同有关方面成立工作专班，抓紧草案研究起草工作。在起草过程中，多次召开座谈会，认真听取有关部门、企业和专家学者的意见；整理国内外有关立法资料，开展专题研究；并到有关地方和部门调研，深入了解数据安全领域存在的突出问题，听取立法意见建议。形成数据安全法草案稿后，又征求了中央有关部门和部分企业、专家的意见，经反复修改完善后，形成了《中华人民共和国数据安全法（草案）》。

起草工作注意把握以下几点：一是，把握正确政治方向，贯彻落实总体国家安全观，坚持党对数据安全工作的领导。二是，立足数据安全工作实际，着力解决数据安全领域突出问题，同时坚持包容审慎原则，鼓励和促进数据依法合理有效利用。三是，数据安全法作为数据领域的基础性法律，重点是确立数据安全保护管理各项基本制度，并与网络安全法、正在制定的个人信息保护法等做好衔接。

需要说明的是，按照全国人大常委会立法规划和年度立法工作计划的安排，全国人大常委会法工委会同中央网信办正在抓紧个人信息保护法草案起草工作，争取尽早提请全国人大常委会审议。

三、关于草案的主要内容

草案共七章五十一条，主要内容包括：

（一）关于本法的适用范围

草案明确在我国境内开展的数据活动适用本法，其中数据是任何以电子或者非电子形式对信息的记录，数据活动是指数据的收集、存储、加工、使用、提供、交易、公开等行为。同时，草案赋予本法必要的域外适用效力，规定：中华人民共和国境外的组织、个人开展数据活动，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。（草案第二条、第三条）

（二）关于支持、促进数据安全与发展的措施

草案坚持安全与发展并重，设专章对支持促进数据安全与发展的措施作了规定，保护个人、组织与数据有关的权益，提升数据安全治理和数据开发利用水平，促进以数据为关键要素的数字经济发展。包括：实施大数据战略，制定数字经济发展规划；支持数据相关技术研发和商业创新；推进数据相关标准体系建设，促进数据安全检测评估、认证等服务的发展；培育数据交易市场；支持采取多种方式培养专业人才等。（草案第十二条至第十八条）

（三）关于数据安全制度

为有效应对境内外数据安全风险，有必要建立健全国家数据安全管理制度，完善国家数据安全治理体系。对此，草案主要作了以下规定：一是，建立数据分级分类管理制度，确定重要数据保护目录，对列入目录的数据进行重点保护（草案第十九条）。二是，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，加强数据安全风险信息的获取、分析、研判、预警工作（草案第二十条）。三是，建立数据安全应急处置机制，有效应对和处置数据安全事件（草案第二十一条）。四是，与相关法律相衔接，确立数据安全审查制度和出口管制制度（草案第二十二条、第二十三条）。五是，针对一些国家对我国的相关投资和贸易采取歧视性等不合理措施的做法，明确我国可以根据实际情况采取相应的措施（草案第二十四条）。

（四）关于数据安全保护义务

保障数据安全，关键是要落实开展数据活动的组织、个人的主体责任。对此，草案主要作了以下规定：一是，开展数据活动必须遵守法律法规，尊重社会公德和伦理，有利于促进经济社会发展，增进人民福祉，不得违法收集、使用数据，不得危害国家安全、公共利益，不得损害公民、组织的合法权益（草案第八条、第二十六条、第二十九条）。二是，开展数据活动应当按照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（草案第二十五条）。三是，开展数据活动应当加强数据安全风险监测、定期开展风险评估，及时处置数据安全事件，并履行相应的报告义务（草案第二十七条、第二十八条）。四是，对数据交易中介服务和在线数据处理服务等作出规范（草案第三十条、第三十一条）。五是，对公安机关和国家安全机关因依法履行职责需要调取数据以及境外执法机构调取境内数据时，有关组织和个人的相关义务作了规定（草案第三十二条、第三十三条）。

（五）关于政务数据安全与开放

为保障政务数据安全，并推动政务数据开放利用，草案主要作了以下规定：一是，对推进电子政务建设，提升运用数据服务经济社会发展的能力提出要求（草案第三十四条）。二

是，规定国家机关收集、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，并落实数据安全保护责任，保障政务数据安全（草案第三十五条、第三十六条）。三是，对国家机关委托他人存储、加工或者向他人提供政务数据的审批要求和监督义务作出规定（草案第三十七条）。四是，要求国家机关按照规定及时准确公开政务数据，制定政务数据开放目录，构建政务数据开放平台，推动政务数据开放利用（草案第三十八条、第三十九条）。

（六）关于数据安全工作职责

数据安全涉及各行业各领域，涉及多个部门的职责，草案明确中央国家安全领导机构对数据安全工作的决策和统筹协调等职责，加强对数据安全工作的组织领导；同时对有关行业部门和有关主管部门的数据安全监管职责作了规定。（草案第六条、第七条）此外，草案还对违反本法规定的法律责任等作了规定。（来源：中国人大网）

- **中华人民共和国数据安全法（草案） 全文：**
- http://www.npc.gov.cn/flcaw/flca/ff80808172b5fee801731385d3e429dd/attachment.pdf

➢ 2019 年我国网络安全市场规模达 523 亿元

2020 年 6 月 29 日，中国网络空间安全协会发布了《2020 年中国网络安全产业统计报告》(以下简称“《报告》”)。《报告》指出，2019 年国内网络安全技术、产品与服务总收入约为 523.09 亿元，同比增长 25.37%，网络安全企业从业人员约为 10 万人。到 2023 年底，中国网络安全市场规模将突破千亿元。

《报告》将网络安全产业市场规模分为四个统计口径，从“行业总收入”“业务总收入”“技术、产品与服务总收入”“技术、产品与服务纯收入”四个维度分别进行统计，为客观清晰地反映我国网络安全产业的真实状况提供参考。

报告指出，2019 年国内网络安全技术、产品与服务总收入约为 523.09 亿元，同比增长 25.37%。在 2017 年至 2019 年期间，2018 年网络安全市场规模年复合增长率为 28.98%，达到历史最高。到 2023 年底，中国网络安全市场规模将突破千亿元。

报告显示，2019 年，软件及硬件产品收入约占安全业务总收入的 66%，安全服务收入约占安全业务总收入的 24%，安全集成收入约占安全业务总收入的 10%。

国内三大类网络安全业务，硬件产品占比较大，软件第二，安全服务第三。但随着合规驱动走向需求驱动的转变趋势，硬件占比逐年减少。预计未来两年，软件和服务的占比将与硬件持平。

据统计，全球网络安全业务年收入超过 10 亿美元的企业不到 20 家，其网络安全业务收入总和还未达到全球市场的 40%。值得关注的是，安全咨询业务占全球网络安全市场的 20%左右，而国内第三方安全咨询服务的收入占比极低。

2019 年，我国有 13 家企业网络安全业务年收入超过 10 亿元，占网络安全业务总收入的 48.82%，平均收入为 22.31 亿元;收入 1 亿元以上的共 94 家，占比 40.52%，平均收入为 2.56 亿元;收入 1 亿元以下的企业近 400 家，占比 10.66%。

同时，从各企业收入水平的占比情况来看，网络安全市场“没有寡头，只有诸侯”的格局明显，同时碎片化现象非常突出。这种情况也与全球网络安全市场的格局相似。

从区域分布来看，北京作为全国政治、文化、国际交往、科技创新中心，安全企业数量和安全收入水平居显著领先地位，此外，广东、浙江、四川、福建、上海、山东和江苏等经济发达地区也位列前茅。

据不完全统计，目前国内网络安全上市企业共计 62 家，其中，深交所和上交所上市企业 23 家(含安全业务收入少于 50%的上市企业 8 家)，新三板上市企业 39 家。

2015 年至 2017 年国内大量网络安全企业在新三板上市，2017 年达到高峰。到 2019 年，共有 66 家企业在新三板上市。但是，近年来由于投资资产门槛较高，企业达不到融资目的，截至 2019 年底，已有 26 家网络安全企业从新三板退市。目前，在新三板尚有 39 家网络安全企业。

统计显示，2019 年网络安全企业从业人员约为 10 万人(含主板和新三板企业从业人员 4.51 万人)，其中研发/技术人员约占 58.45%，从业人员同比增长 16.04%。

报告同时指出，一方面，从投融资金额和数量可以看出，云安全、数据安全、移动安全、身份安全和工控安全均为近几年来的市场投融资热点。

网络安全风险与战略投资金额呈逐年上升趋势，即使在 2018 年下半年至 2019 年上半年的资本市场“寒冬期”，也未受明显影响。2017 年至 2019 年是融资高峰期，每年的融资企业数量均在 50 家以上。

另一方面，2019 年上交所科创板的成立，四家网络安全企业完成 IPO，募集资金净额近 30 亿元，给网络安全企业的发展增添了强劲信心，并为网络安全领域资本退出提供了良好的通道。值得期待的是，2020 年深交所创业板注册制的落地，无疑将在网络安全企业的成长与发展方面给予有力的支撑。

中国网络空间安全协会秘书长李欲晓表示，促进行业的发展和技术的进步是行业协会的初心和使命。任何领域、行业或产业的发展都离不开对历史、现状的准确把握和判断，并以此作为产业健康发展的风向标和指南，此为中国网络空间安全协会发布《2020 中国网络安全产业统计报告》的核心立意所在。由于网络安全技术与产业的碎片化和复杂性，报告对国家网络安全产业做出的调研统计分析还很有限。今后协会将在机制和能力上逐步完善，扩大调研对象，形成常态调研统计，深入研究分析产业发展特点和规律，为政府宏观决策、产业发展和技术进步提供有力支撑。（来源：人民网）

- **《2020 年中国网络安全产业统计报告》**
- **全文：**https://www.cybersac.cn/News/getNewsDetail/id/1545

➢ 从执法实践看《网络安全法》三周年实施成效

《中华人民共和国网络安全法》（下文简称《网络安全法》）自 2017 年 6 月 1 日颁布实施以来，在我国网络空间治理、信息安全保护等方面发挥了积极的作用，成为我国网络安全治理历程上的一个里程碑事件。就实施过程来看，《网络安全法》在打击网络犯罪、保护公民个人隐私、规范网络运营者主体责任、维护国家安全等方面发挥了不可替代的作用，但部分内容以原则性规定为主，相关规定在执行层面相对宽泛，不利于具体实施落实，有待在后续立法过程中逐步完善。

一、对《网络安全法》实施三周年的总体看法

《网络安全法》对网络运行、信息安全、检测和响应、监管处罚等方面进行了详细规定，

围绕网络空间主权原则、网络空间安全与信息化发展并重原则、共同治理原则等进行了顶层设计，在数据安全保护方面按照数据安全、个人数据保护及国家层面数据保护三个层次进行了递进式的要求和规定。

（一）对网络安全防护各个环节进行详细规定

《网络安全法》针对网络安全防护中涉及的网络运行、信息安全、检测和响应以及监管处罚等方面，均按照网络运营者和关键信息基础设施运营者两个维度，进行了一般规定和特殊规定，明确不同主体的职责和任务，以及相应的处罚规定。比如在网络运行方面，对网络运营者“留存相关网络日志不少于六个月”“应当要求用户提供真实身份信息”“应当制定网络安全事件应急预案”等进行了明确的规定，进一步明确了网络运营者应当适用的一般规定，要求所有网络运营者都必须遵守和执行；而对关键信息基础设施运营者一方面进行了清晰的界定，并对“设置专门安全管理机构和安全管理负责人”、“制定网络安全事件应急预案，并定期进行演练”、“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”等内容进行了明确规定，要求关键信息基础设施运营者履行不同于一般网络运营者的更高责任要求。

（二）对基本原则进行了明确和进一步阐述

在《网络安全法》颁布之前，我国关于网络空间治理和信息安全防护的要求散见于各类法规、政策和文件要求中，在执行过程中既不利于统筹把握，也存在法律位阶不高的现实掣肘。随着《网络安全法》的颁布实施，对网络空间主权原则、网络空间安全与信息化发展并重原则、共同治理原则等进行了明确的阐述，不仅对网络安全的理念与指导思想从法律层面

予以了确认，更是对习近平总书记关于网络安全方面的理论思想的具体贯彻和集中体现，是中国特色社会主义法治建设中的重要一环。

（三）在具体措施上有明显的创新

《网络安全法》的颁布实施，解决了我国一段时间以来网络空间安全治理主管责任不清晰，存在“九龙治水、责权不清”等现象的弊端，同时在网络实名制、数据跨境流动等方面的明确规定，为管理执法层面提供了切实可行的法规支撑，保证了监管力度和执行效率。有关研究指出，《网络安全法》对“1+X”监管制度的明确，进一步强化了对互联网市场的监管，一定程度上解决了曾经存在的互相推诿、协作不力等问题，兼具“自上而下”及“自下而上”的监管模式，提升了管理部门执行效率，降低了监管部门相关人员出现玩忽职守、滥用职权等现象的发生。而在网络实名制和数据跨境流动等方面的具体规定，为监管部门在实践过程中提供了切实可靠的法律依据，有力解决了原有网络实名制立法等级较低的问题，同时从国家安全的高度对数据安全的重要性进行了明确，为国家实施数据安全保护提供了强而有力的法律依据。

二、积极实践应用,加大执法力度

（一）强化学习宣贯，营造浓厚氛围。《网络安全法》实施以来，我们采取多种措施，多种形式，从多层面，多角度，多领域，加强学习宣贯。一是内部，先后邀请公安部领导、网络安全专家、执法办案民警对《网络安全法》进行讲座授课，从网络安全的发展过程以及立法过程全面理解。二是外部，受社会各界邀请，民警分行业、分领域，结合案例，谈体会、讲意义，先后组织教育、卫生、国资等行业的讲座 12 次，在整个社会层面大力宣讲，使《网络安全法》深入民心。三是借鉴经验。多次组织领导和民警参加公安部及相关省市的交流和座谈，先后到昆明、杭州等地学习先进经验，确保法律法规形成实践。

（二）积极实践应用，加大执法力度。通过对全市范围内风险隐患较多的重点网站开展集中执法检查，围绕管制刀具、弩、剧毒化学品、招嫖、赌博、毒品等违法信息，指导互联网企业全面深化网上清理整治。按照《公安机关互联网安全监督检查规定》,针对未落实网络安全措施、存在严重安全隐患的互联网企业，依据《网络安全法》等法律法规，依法给予行政处罚，维护网上安全秩序。一是依法处罚违法信息高发的互联网企业。针对“JJ”网络游戏 App 用户账号、互动百科网、“猫途鹰”、“名师屋”等网站存在招嫖、赌博等违法信息，依据《网络安全法》给予限期改正、罚款等行政处罚。二是依法处罚超范围采集公民个人信息的互联网企业。针对牛股王 App 存在超范围采集用户个人信息及手机权限的情况，依据《网络安全法》对该公司给予行政警告处罚。此案例为北京市公安局网安部门首次适用《网

络安全法》对涉嫌超范围采集用户个人信息的互联网企业开展行政执法。三是依法处罚未落实实名登记信息的互联网企业。针对互联网应用分发企业（北京奇客创想科技股份有限公司），以及运营商（北京千秋大业信息科技有限公司），存在未按要求留存接入用户真实身份信息的情况，分别给予两家公司限期改正及罚款的行政处罚。

（三）坚持标本兼治，强化综合治理。我总队广泛调动各方积极性，特别是落实互联网企业主体责任，建立网络社会群防群治力量，提升网络社会治理能力和水平。一是注重部门联动，建立网络安全联合执法机制。总队多次会同市网信办、市工商局、市卫健委等部门约谈企业主要负责人，加大联合执法力度，形成我市网络安全执法合力。二是注重教育培训，建立网络风险防范化解机制。专门邀请部局领导，为全局网安系统业务骨干及全市 100 家重点互联网企业共 300 余人开展专题部署和培训，进一步提高了网站管理人员的法律意识和工作的主观能动性。

（四）制定工作指引，强化建章立制。按照《公安机关互联网安全监督检查规定》的要求，我总队组织专业技术支撑单位召开专门会议，结合互联网运营商各业务类型技术特点，从备案数据上报、等保测评、网络与信息安全技术防范措施、远程漏洞扫描等方面，创新制定了《运营商检查工作指引》，规范运营商现场检查工作流程。同时，按照从实际出发，突出检查重点、抓准问题要害的整体思路，研究制定《运营商安全监督检查表》，细化现场检查及远程技术检查的标准和方法，形成指导分局运营商检查工作的依据和抓手，推进全市运营商执法检查工作向前发展。

三、问题与思考

《网络安全法》的颁布实施，既是我国网络空间安全防护方面的一项开创性举措，同时也是互联网立法层面的一次探索和尝试，相关内容仍然存在完善和提高的空间。同时，互联网的快速发展，新业态、新技术的层出不穷，也要求我们不断地提升治理水平，不断完善立法和司法的各个环节。

（一）在执行层面迫切需要更具可操作性的实施细则。《网络安全法》在网络安全保护的各环节均作出了具体而明确的规定，特别是在监管处罚方面明确了具体的标准，但在具体执行层面依然存在标准模糊、模棱两可的情况，亟需配套的司法解释予以进一步明确和界定。比如，《网络安全法》中没有对网络信息系统停机整顿的处罚，且在法条论述上比较粗犷笼统，操作性不强，执行困难，需要“两高”、公安部等尽快出台实施细则或司法解释，对相关法条进一步细化分解。再比如，在网络实名制方面，《网络安全法》虽然提出了明确的要求，但在具体执行方面往往存在认识不统一、执行标准不一致的情况，不同的企业、不同的

应用对于实名认证的落实程度不一，特别是实名制在与游戏、金融等特殊应用领域的具体要求配套落实过程中，还需要探索具体的操作办法，需要从司法解释、实施细则以及行业标准等方面进一步予以完善支撑。

（二）重视监管职权而信息安全保护有待提升。《网络安全法》在明确网络运营者应尽的义务和责任方面着墨较多，对监管主体的监管责任都进行了详尽的规定，但同时应该看到，在网络安全防护和信息安全保护方面，对公权力和私权利保护程度的平衡，对法律秩序价值和自由价值之间的取舍，是需要加以考量的部分。如何在保证网络实名制等具体措施，在预防网络诈骗、减少网络暴力，整治低俗有害信息层出乱象的过程中发挥实际作用，又能做到充分保障公民的信息安全，确保公民个人隐私信息不受过度采集和不法侵犯，是立法者需要进一步探索和研究的内容。

（三）应对突发事件相关制度需进一步明晰。对于突发重大社会事件的处置，各国因维护国家安全和公共秩序的需要，均确立了对网络通信进行临时管制的制度措施。但随着互联网的高速发展，物联网、云计算、大数据等应用不断深入社会各个方面，网络通信的管制已不再局限于原有的限制公民个人通信自由的范畴，而可能扩展到对公民人身权和财产权产生重要影响。因此，有必要从法律层面对采取网络安全方面的应急管理措施予以明晰，对于国家、省市等不同层级的突发公共安全事件的界定、措施发布和应对方案予以明确，才能更好地确保网络安全应急管理制度的完善。

（四）裁量标准不统一。从行政处罚的结果看，不同区域的裁量标准也不一致。表现为：同样性质的案件，不同分局做出不同的行政处罚；如同样被黑客攻击的案件，有的分局做出了罚款的处罚，有的分局做出了警告的处罚。

（五）司法鉴定存在一定困难。目前，对于处罚证据中的司法鉴定，由哪个鉴定机构鉴定，出具什么样的报告，哪些专家的意见，鉴定程序和鉴定结论等，没有具体规定和具体样本，需要进一步研究和探讨。

四、意见和建议

一是建议继续加快《网络安全法》配套法规的立法。《网络安全法》作为网络安全领域的基础法，其内容大多为基础性、原则性的规定，需要制定配套的法规来实现其立法目的。为适应快速变化的网络发展，我们应当不断改进网络治理手段，提升网络治理能力，加快《网络安全法》的配套法规立法。同时，要让法律法规在实践中不断完善，尽快将前期试行和征求意见稿的法规转正。

二是建议加强各相关主管部门统筹，形成真正意义上的网络监管合力。从《网络安全法》

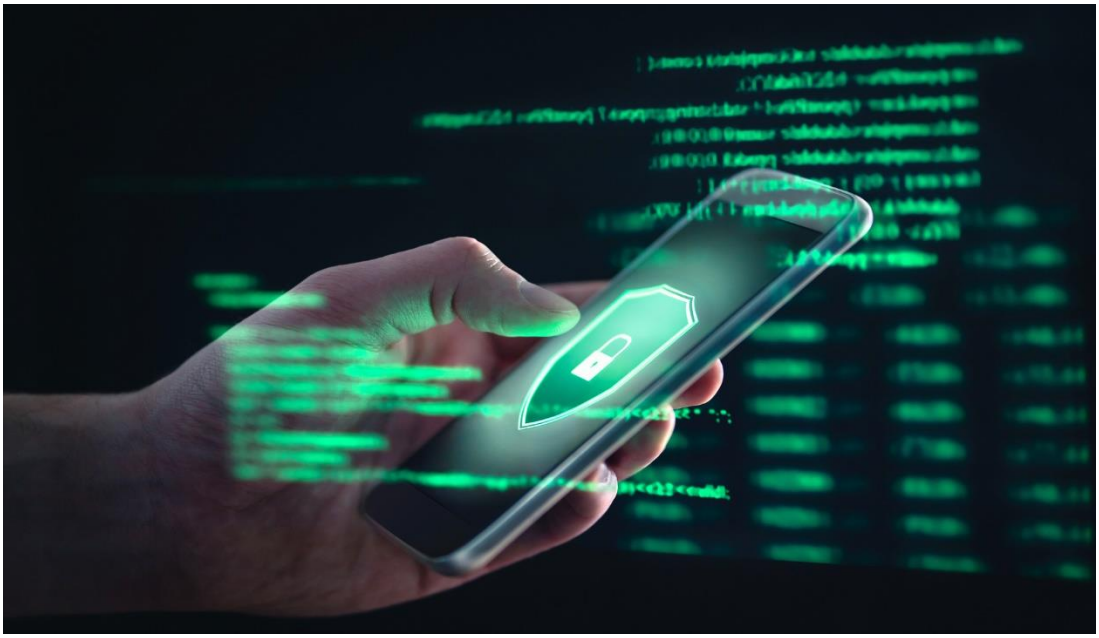
的实践层面来看，各相关主管部门为了保证各自工作顺利开展，纷纷从自身角度出台大量行政法规和地方政府规章来规范网络空间。这些部门间本身就存在职能上的交叉，加之各部门在制定部门规章时缺乏横向沟通，仅局限于自身工作需要，造成制定的规章内容重复，甚至相抵触，无法形成对网络监管的合力。建议相关部门在出台部门规章时，要加强部门间的统筹协调，明确各部门监管职责，形成有效互补，共同担负起维护网络安全的责任。

三是建议加强社会推动，大力宣传提升震慑力度。要加强对执法案例的宣传力度，通过电视、广播、网络等新闻媒体，宣传重要信息系统安全保卫执法的经典案例。让社会公众提升责任单位安全意识，扩大网安影响力，提升震慑力度，产生更广泛的社会效应，来推动重要信息系统安保工作的开展。（来源：《中国信息安全》杂志 2020 年第 6 期）

➢ 如何依法织密个人信息保护网

以大数据、云计算为代表的信息技术的快速发展，不仅为经济社会发展提供巨大动力、为人民生活带来更多便利，也给个人信息保护、个人隐私安全带来更多挑战。十三届全国人大三次会议审议通过的民法典在现行有关法律规定的基础上，进一步强化对隐私权和个人信息的保护，并为下一步制定个人信息保护法留下空间。

如何更好实现技术应用与隐私保护的统筹兼顾？疫情防控中的个人信息安全问题应如何破解？生物识别技术运用中暗藏的隐私泄露风险应如何规避？这都需要从法律和实践中寻找答案。



民法典提供更广泛的个人信息保护

前不久，哈尔滨市民王先生发现，在使用某应用程序时，该应用程序会自动获取其好友信息并推送好友发布的视频。据此，王先生以侵犯隐私权为由提起诉讼。法院裁定，要求该应用程序立即停止使用王先生的好友信息，停止将王先生信息推荐给其他用户。

“这起案件的判决将个人信息纳入到了隐私权保护的范围内，但并没有对个人信息和隐私权作出更清晰的区分。”在北京互联网法院审管办主任孙铭溪看来，这一判例是司法实践的常态，“民法总则虽然明确自然人享有隐私权，但并未对个人信息和隐私权的概念作出界定。”不过，前不久十三届全国人大三次会议通过的民法典中的人格权编，则给出了隐私的明确定义：既包括“私人生活安宁”，也包含“不愿意让他人知晓的私密空间、私密活动、私密信息”，任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权，不得实施可能破坏他人隐私和隐私权的行为。

“民法典对隐私权的强化保护，体现出在数字时代，更加重视数字人格的立法取向。”孙铭溪说，隐私权更多侧重于精神利益，个人信息则兼具人格和财产利益；隐私偏重于消极防御权，个人信息则强调个人信息的自决和控制；个人信息更多关注的是客观风险，隐私权所包含的“私密信息”则更关注主观意愿。

“民法典事实上提供了比隐私权更广泛的个人信息保护。”清华大学法学院院长申卫星表示，民法典在总则部分规定，自然人的个人信息受法律保护，任何组织或者个人应当依法取得并确保信息安全，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，“这意味着，即使是不属于隐私权中‘私密信息’的个人信息，也依然能得到相应的法律保护”。

“民法典强化对个人信息的保护，还体现在维护个人对其信息的控制权上。这种控制权包括控制个人信息流出、更正或撤回，维护个人信息的安全环境。”申卫星说，知情同意正是控制个人信息流出的关键措施。根据民法典规定，处理自然人个人信息的，一般都必须征得该自然人或者其监护人同意，即便是获得了个人同意，在处理个人信息过程中还需要明示处理信息的目的、方式和范围，不得违反法律、行政法规的规定和双方的约定，并按照合理的方式处理信息。

查询、复制并行使删除权是确保个人信息主体控制权的具体措施。根据民法典规定，自然人可以依法向信息处理者查阅或者复制其个人信息；发现信息有错误的，有权提出异议并请求及时采取更正等必要措施。此外，自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。“通过这些具体措

施的赋权，公民可以掌控其个人信息的使用状态，并且对相关状态进行调整，甚至提出删除的要求，个人信息的处理者都需要对这些权利主张予以满足。”申卫星说。

在疫情防控中要做好个人信息保护工作

2020 年 6 月 17 日，河北燕郊一街道办工作人员贾某某，因在微信群传播疫情防控传真文件照片，内容涉及居民张某等人的隐私信息，被公安机关依法行政拘留 10 日。

这一事件并非孤例。4 月 19 日，青岛公安发布通报称，因造成胶州中心医院出入人员名单在社会上被转发传播，3 人被依法行政拘留。名单涉及 6000 余人的姓名、身份证号码等个人信息，侵犯了公民个人隐私权。公安部统计数据显示，截至 4 月 15 日，全国公安机关共处罚网上传播涉疫情公民个人信息违法人员 1522 名。

在疫情防控常态化的大背景下，利用大数据开展联防联控已成工作常态。如何平衡公共利益与公民个人信息保护，兼顾社会治理安全与效率，确保公民个人信息安全，成为令人关注的社会话题。

“电信运营商和各大互联网平台掌握了公民大量的地理位置、行踪轨迹等个人信息，这是利用大数据助力疫情防控最显著的优势。”由全国信息安全标准化技术委员会牵头成立的 APP 专项治理工作组副组长洪延青表示，相较于传统的走访、摸排、登记，信息技术和大数据分析更加及时、准确、有效，成为疫情防控和监测的重要手段。此外，大数据不断学习、更迭、完善的特点，也有利于更好分析掌握疾病传播规律，消除防疫“盲区”和不确定性。

将大数据应用于疫情防控，要防止个人信息泄露的现象发生。在中国社会科学院大学互联网法治研究中心执行主任刘晓春看来，造成个人信息泄露的原因主要有以下几个方面：未经被收集者同意，随意收集、存贮、使用个人信息；收集的个人信息明显超过正当和必要范围；收集和控制的个人信息，未经被收集者同意，用于其他用途；未经被收集者同意，公开其个人信息，尤其是敏感信息；个人信息的收集和控制者，没有尽到个人信息安全保护主体责任。

事实上，早在今年 2 月，中央网信办就发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》，对疫情防控期间的个人信息安全保障作出规定。《通知》明确规定，为疫情防控、疾病防治收集的个人信息，不得用于其他用途，任何单位和个人未经被收集者同意，不得公开其姓名、年龄、身份证号码、电话号码、家庭住址等个人信息。

“疫情防控与个人信息保护，需要统筹兼顾、做好平衡。”在洪延青看来，涉及个人信息的采集、汇总、共享、披露等各个环节都应当注意做好个人信息保护工作，以防出现数

据泄露、丢失、滥用等情形。比如，以纸质填表方式开展的走访调查需要妥善保管，并在适当时候统一回收；以电子方式记录或汇总相关信息，则需要责任落实到人，并将数据保存在特定终端并加密存储。

“在汇总存储环节，尽可能相对集中管理和处理个人信息，采用严密的访问控制、审计、加密等安全措施；在向疫情防控工作相关方共享、传输相关数据时，应确认对方是有权获取数据的机构或个人，并采取加密传输的措施。”刘晓春说，在个人信息使用过程中，需要做到专采专用，严格限制于疫情防控目的，不得用于其他用途，并且在疫情防控结束后按照规定予以妥善处置。

生物识别信息保护要更加细化

“我的‘脸’我能做主吗？”为讨个说法，杭州市民郭兵打了场官司。2019 年 4 月，郭兵在某野生动物园办理了一张年卡，通过验证年卡和指纹，可在一年内不限次数入园游玩。当年 10 月，该野生动物园通过短信告知郭兵：园区年卡系统已升级为人脸识别入园，原指纹识别已取消，即日起，未注册人脸识别的用户将无法正常入园。郭兵认为，面部特征等个人生物识别信息属于个人敏感信息，一旦泄露、非法提供或者滥用，将极易危害包括原告在内的消费者的人身和财产安全。

在协商不成的情况下，郭兵以服务合同违约为由，将该野生动物园告上法庭。6 月 15 日，该案在杭州开庭审理。庭审中，双方辩论焦点集中于搜集的人脸等生物特征信息，是否符合法律法规要求；有无做到充分告知，及征得用户同意等。

郭兵认为，人脸属于敏感个人信息，搜集需要符合相应条件，即合法性、正当性、必

要性，而且即使符合这些原则，也应当告知用户使用目的并征得用户同意。“收到短信时，我还以为是要求采集人脸信息。但没想到这只是告知我已经升级为刷脸入园，要求激活而已。也就是说，被告之前已经收集了我的人脸信息，但此前从没有告诉用户需要采集面部信息。”郭兵说。此次庭审，法院未当庭宣判。

这起官司因涉及过度采集公民生物特征信息、个人隐私安全等，引起了社会公众的广泛关注。近年来，随着人工智能、信息技术快速发展，面部特征、指纹、虹膜、声音、步态等“个人生物识别信息”得以广泛运用，一方面给经济社会发展提供巨大助力、为公民日常生活带来更多便利，但另一方面，也存在着泄露个人信息、侵害个人隐私安全的隐患。

“在我国，包括生物识别信息在内的个人信息的法律保护，经历了一个从无到有、从刑法保护为主到公法私法并重的发展历程。”清华大学法学院副院长程啸表示，2009 年，刑法修正案（七）首次将窃取或以其他方式非法获取公民个人信息情节严重的行为规定为犯罪。2017 年施行的网络安全法，不仅明确界定了个人信息的含义，把个人生物识别信息纳入个人信息范畴，同时还对个人信息的收集、存储、保管和使用进行了更详细、全面的规范。

“在新出台的民法典人格权编中，对个人生物识别信息也提供了多重保护。”程啸说，在一定载体上所反映的特定自然人可以被识别的外部形象属于肖像，应当受到肖像权的保护，任何组织或者个人不得以利用信息技术手段伪造等方式侵害他人的肖像权，“采取偷拍偷录等方式采集自然人人脸等生物识别信息的行为，将构成对隐私权的侵害。对既不属于肖像，也不属于隐私的生物识别信息，还可以适用民法典人格权编个人信息保护的规定”。

“手机号码、邮箱、银行账号等个人信息，比较容易进行更改，但个人生物识别信息要更改则非常困难。这意味着个人生物识别信息一旦被非法收集、泄露，不仅会对自然人的人身财产安全产生威胁或现实损害，而且无法以修改、重置等方式预防后续损害。”程啸认为，人脸信息等个人生物识别的特殊性还在于容易在未经自然人主动配合的情形下进行收集，“在这种情况下，网络安全法等法律规定的告知同意原则实际上难以落实，这就要求法律对哪些组织或者个人在哪些场合可以收集人脸等生物识别信息，作出更明确的规定”。

在庭审中，郭兵说：“我并不是一个技术上的‘保守者’，但是面对类似人脸识别等技术创新时，也要同时绷紧个人信息保护这根‘弦’。希望这起案件的审理能够成为一堂普法课，让更多人关注和思考如何更好实现技术应用与个人信息保护的统筹兼顾。”（来源：人民日报）

四、政府之声

➢ 工信部部署推进 2020 年电信和互联网行业网络数据安全管理工作

2020 年 6 月 22 日，近日，为切实做好 2020 年电信和互联网行业网络数据安全管理工作，工业和信息化部印发《关于做好 2020 年电信和互联网行业网络数据安全管理工作的通知》（以下简称《通知》），提出深化行业网络数据安全专项治理、深入开展网络数据安全合规性评估、加快推进网络数据安全制度标准建设、提升网络数据安全技术保障能力等年度行业网络数据安全管理重点工作要求。

2020 年 6 月 18 日，工业和信息化部网络安全管理局召开全国视频会议，宣贯部署《通知》要求，解读《电信和互联网企业网络数据安全合规性评估要点（2020 年版）》。湖北、广东、青海通信管理局、中国移动、中国电信、中国联通、阿里巴巴、腾讯、滴滴出行、字节跳动、小米、中国信息通信研究院、国家工业信息安全发展研究中心、中国互联网协会等 14 家单位相关负责人作了交流发言，介绍了各自数据安全工作开展情况及后续贯彻落实《通知》的有关考虑。

会议指出，当前数据作为新型生产要素，已成为信息时代国家重要战略资源，数据安全关系到经济社会发展的方方面面，全行业要以习近平新时代中国特色社会主义思想为指导，进一步提高站位，充分认识加强数据安全工作的极端重要性与紧迫性，结合新形势新任务新要求，切实落实企业主体责任，聚焦重点难点，狠抓能力提升，确保《通知》各项任务措施落实落细，促进行业网络数据安全管理工作迈上新台阶。

各省、自治区、直辖市通信管理局相关负责人，各部属支撑单位相关负责人，各基础电信企业集团公司、省公司及 100 余家互联网企业相关负责人通过视频系统远程参会。（来源：工业和信息化部网络安全管理局）

➢ 中国广告协会发布《网络直播营销行为规范》7 月 1 日起施行

2020 年 6 月 30 日，中国广告协会发布了《网络直播营销行为规范》自 2020 年 7 月 1 日起施行。这也是是国内第一个关于网络视频营销活动的专门自律规范，于今日起正式实施。

规范指出，网络直播营销主体不得利用刷单、炒信等流量造假方式虚构或篡改交易数据和用户评价；不得进行虚假或者引人误解的商业宣传，欺骗、误导消费者。在网络直播营销中发布商业广告的，应当严格遵守《中华人民共和国广告法》的各项规定。此外，网络直播营销主体应当依法履行网络安全与个人信息保护等方面的义务，收集、使用用户个人信息时应当遵守法律、行政法规等相关规定。

规范同时明确，网络直播营销活动应当全面、真实、准确地披露商品或者服务信息，依法保障消费者的知情权和选择权；严格履行产品责任，严把直播产品和服务质量关；依法依约积极兑现售后承诺，建立健全消费者保护机制，保护消费者的合法权益。（来源：中国广告协会）

- **中国广告协会《网络直播营销行为规范》**
- **全文：**http://www.china-caa.org/cnaa/newsdetail/369

➢ 银保监会：规范互联网保险销售行为维护消费者合法权益

2020 年 6 月 30 日，为规范互联网保险销售行为，维护消费者合法权益，银保监会发布《关于规范互联网保险销售行为可回溯管理的通知》（以下简称《通知》）。《通知》全文共 26 条，主要包括以下五方面内容:

一是明确互联网保险销售行为可回溯管理的定义和范围。明确互联网保险销售行为可回溯，是指保险机构通过销售页面管理和销售过程记录等方式，对在自营网络平台上销售保险产品的交易行为进行记录和保存，使其可供查验。管理范围是投保人为自然人的商业保险产品。

二是明确销售页面和销售页面管理的定义。对销售页面管理主体、互联网保险销售行为的边界和销售风险点管控作出要求。特别强调销售页面只能设置在保险机构自营网络平台，且需要与非销售页面进行分隔。对于重要条款内容，要求单独设置页面展示，且由投保人自主确认，保护消费者知情权。

三是对保险机构互联网销售过程管理作出要求。包括保护投保人自主选择权、明确保险机构实名验证职责、细化销售过程记录标准、制定信息收集原则等内容。对于收集、使用消费者个人信息，《通知》特别强调保险机构应遵循合法、正当、必要的原则，并采取有效措施保护信息，保护消费者信息安全权。

四是明确可回溯内控管理。主要对可回溯资料内容、保管、安全防护及相关内控制度作出规定，要求保险机构建立全面、系统、规范的内部控制体系。特别强调互联网保险销售行为可回溯资料应当可以还原为可供查验的有效文件，销售页面应当可以还原为可供查验的有效图片或视频，以便调查检查使用。

五是明确对融合业务和自助终端业务的管理要求，以及相关法律责任和实施时间。

《通知》的发布有利于维护市场秩序、防范操作风险，进一步保障金融消费者知情权、自主选择权和公平交易权等基本权利。下一步，银保监会将加大督促指导，压实保险机构主体责任，规范互联网保险销售行为，推动互联网保险业务的持续健康发展。（来源：中国银行保险监督管理委员会）

- **中国银保监会关于规范互联网保险销售行为可回溯管理的通知 银保监发〔2020〕26 号**
- **全文：**http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=912732&itemId=926

➢ 国家卫健委办公厅发布关于做好信息化支撑常态化疫情防控工作的通知

2020 年 6 月 29 日，为充分发挥信息化在支撑疫情监测分析、创新诊疗模式、提升服务效率、促进人员安全有序流动等方面的作用，国家卫生健康委办公厅印发《关于做好信息化支撑常态化疫情防控工作的通知》(以下简称《通知》)，指导各地利用信息化手段支撑常态化疫情防控工作。

《通知》从六个方面提出了相关要求：

一是强化疫情监测预警，支撑疫情防控工作。加强区域统筹，完善中国疾病预防控制信息系统，强化疫情信息监测预警。完善预警指挥系统。

二是完善健康通行码政策标准，推动人员安全有序流动。优化防疫健康服务，完善健康通行码“一码通行”，推进多“码”融合。

三是推广疫情期间线上服务经验，大力发展“互联网+医疗健康”。鼓励“互联网+医疗健康”规范有序发展，发挥平台作用，强化数据共享，完善标准规范，扩大创新试点。

四是拓展“互联网+政务”服务，推动政务信息共享和“一网通办”。推进“互联网+政务”服务，统筹推进医疗机构、医师、护士电子证照建设应用，积极推广“出生一件事”，推动政务信息系统整合。

五是推进信息化新型基础设施建设，加快建立应急指挥系统。持续完善平台功能，建立基础数据库，建立应急指挥系统，开展大数据综合分析。

六是强化网络安全工作，切实保障个人信息和网络安全。落实网络安全责任，加大网络安全投入，加强网络安全防护和保障能力，组织网络安全宣传教育和培训。（来源：国家卫生健康委办公厅）

- **国家卫生健康委办公厅关于做好信息化支撑常态化疫情防控工作的通知 全文：**
- http://www.nhc.gov.cn/guihuaxxs/s10743/202006/5a2bc24e181a43a6b242a86706c361a3.shtml

五、本期重要漏洞实例

➢ Apache Dubbo Provider 远程代码执行漏洞

发布日期：2020-06-24
更新日期：2020-06-24
受影响系统：
Apache Dubbo 2.7.0 ~ 2.7.6
Apache Dubbo 2.6.0 ~ 2.6.7
Apache Dubbo 2.5.x 所有版本（官方不再提供支持）
描述：

CVE(CAN) ID: CVE-2020-1948
Apache Dubbo 是一种基于 Java 的高性能 RPC 框架。
Apache Dubbo Provider 存在远程代码执行漏洞。攻击者可以发送未经验证的服务名或方法名的 RPC 请求，同时配合附加恶意的参数负载。当恶意参数被反序列化时，将执行恶意代码。

建议：

厂商补丁：
Apache

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
升级至 Apache Dubbo 2.7.7 或更高版本，同时不要对外开启 telnet 功能，CNVD 建议用户立即升级至最新版本：

https://www.apache.org/

➢ Microsoft Windows Win32k 提权漏洞

发布日期：2020-06-22
更新日期：2020-06-22
受影响系统：
Microsoft Windows Server 2008 R2 SP1
Microsoft Windows Server 2008 SP2
Microsoft Windows 7 SP1
Microsoft Windows Windows Server 2012
Microsoft Windows 8.1
Microsoft Windows RT 8.1 SP0
Microsoft Windows Server 2012 R2
Microsoft Windows 10
Microsoft Windows 10 1607

Microsoft Windows Server 2016
Microsoft Windows Server 2019
Microsoft Microsoft Windows Server 1803
Microsoft Microsoft Windows Server 1903
Microsoft Windows 10 1709
Microsoft Windows 10 1803
Microsoft Windows 10 1809
Microsoft Windows 10 1903
Microsoft Microsoft Windows Server 1909
Microsoft Windows 10 1909

描述：

CVE(CAN) ID: CVE-2020-1143

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。win32k 是其中的一个 Windows 子系统的内核部分，是一个内核模式设备驱动程序，它包含有窗口管理器、后台控制窗口和屏幕输出管理等。

Microsoft Windows 和 Windows Server 中存在提权漏洞，该漏洞源于内核模式驱动程序未能正确处理内存中的对象，攻击者可借助特制应用程序利用该漏洞运行任意代码。

建议：

厂商补丁：

Microsoft

厂商已发布了漏洞修复程序，请及时关注更新：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1143

➢ Cisco Webex Meetings Desktop App 信任管理问题漏洞

发布日期：2020-06-23

更新日期：2020-06-23

受影响系统：

ICisco Webex Meetings Desktop App <39.5.11

描述：

CVE(CAN) ID: CVE-2020-3342

Cisco Webex Meetings Desktop App 是美国思科（Cisco）公司的一款使用在桌面环境上的视频会议控制应用程序。

Cisco Webex Meetings Desktop App 39.5.11 之前版本（Mac）中的软件更新功能存在信任管理问题漏洞，该漏洞源于程序未能正确验证下载文件的加密保护。远程攻击者可借助特制网站利用该漏洞在系统上

执行任意代码。

建议：

厂商补丁：
Cisco
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-mac-X7vp65BL

➢ 多款 Apple 产品 Audio 组件缓冲区溢出漏洞

发布日期：2020-06-28
更新日期：2020-06-28
受影响系统：
Apple macOS Catalina <10.15.5
Apple iOS <13.5
Apple iPadOS <13.5
Apple tvOS <13.4.5
Apple watchOS <6.2.5
描述：

CVE(CAN) ID: CVE-2020-9791
Apple iOS 等都是美国苹果（Apple）公司的产品。Apple iOS 是一套为移动设备所开发的操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。Apple macOS Catalina 是一套专为 Mac 计算机所开发的专用操作系统。Audio 是其中的一个音频组件。
多款 Apple 产品中的 Audio 组件存在缓冲区溢出漏洞。攻击者可借助恶意的音频文件利用该漏洞执行任意代码。

建议：

厂商补丁：
Apple
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://support.apple.com/zh-cn/HT211170
https://support.apple.com/zh-cn/HT211168
https://support.apple.com/zh-cn/HT211171
https://support.apple.com/zh-cn/HT211175

六、本期网络安全事件

➢ 收集 14 万余条学生个人信息 江苏省一培训机构被罚

2020 年 6 月 26 日，针对个人信息被非法收集、屡遭泄露这一严重的社会问题，刚刚通过的《民法典》从法律层面为消费者个人信息安全扎紧了防护网。近日，记者从江苏省江阴市市场监管局获悉，该局在“守护消费”暨打击侵害消费者个人信息违法行为专项行动中，查获一起 14 万余条个人信息遭非法收集的案件。

据江阴市市场监管局相关负责人介绍

执法人员在对辖区某教育培训机构进行监督检查时，在其营业场所办公室的电脑中发现了一个取名叫“江阴”的文件夹，执法人员点开后发现文件夹里是几十个标注了江阴各个中小学名称的 EXCEL 表，涵盖了江阴市绝大部分中小学学生和家长的信息资料。经初步清点，里面有“学校、学生姓名、性别、年级、班级、学生家庭地址、家长姓名及电话”内容的个人信息 14 万余条。此外，执法人员还在该办公室内找到上述 EXCEL 表打印后用水笔做过代号标记的电脑打印资料 500 余张以及众多登记了学生家长信息的“薄弱科目统计表”。

对此，江阴市市场监管局执法人员立即开始立案调查。执法人员通过电信部门调取了该教育培训机构办公场所 6 部固定电话 6 个月内的通话记录，随机拨打了记录中的电话及电脑中已做过标记的部分学生家长电话。经查，该教育培训机构主要面向小学初中学生提供非学历文化教育培训，当事人通过不明渠道获得涉及全市 97 所各类学校学生的个人信息 14 万余条。当事人打印了收集到的部分学校的学生信息，在未取得学生家长同意的情况下，以拨

打电话的方式推销商业性教育培训服务业务，在部分学生家长明确答复不需要表示拒绝后，后续仍多次拨打电话推销商业性教育培训服务业务，拨打后，当事人以代号的方式在电脑打印资料上记录了拨打学生家长电话推销教育培训业务的结果以及拨打的次数。此外，当事人还以在学校门口发放小礼品的方式通过学生家长或学生本人登记采集学生姓名、家长电话等个人信息，进而通过电话方式推销商业性教育培训服务业务，部分未事先征得学生家长同意。

当事人的行为违反了《消费者权益保护法》《江苏省消保条例》相关规定，依据《江苏省消保条例》第六十二条的规定，江阴市市场监管局对当事人处以罚款 30 万元。此外，因涉案公民个人信息数量巨大，江阴市市场监管局依法将此案件线索移交当地公安局。

随着互联网的飞速发展，消费者个人信息逐渐成为一种重要资源，由此产生行业中的恶性竞争，“得信息者得客户”成为不少商家不良竞争手段。江阴市市场监管局通过该案件的查办，对不法商家起到了强大的震慑作用，对消费者起到了教育和引导作用，有效遏制了热点行业中侵害消费者权益行为的蔓延势头，全力营造安全放心的消费环境。（来源：央视新闻）

➢ 上市公司京投发展子公司遭电信诈骗近 3000 万,已报案

2020 年 6 月 23 日晚间，京投发展股份有限公司（京投发展，600683）公告称：子公司北京京投银泰置业有限公司（以下简称“银泰置业”）遭遇犯罪团伙电信诈骗，导致银泰置业银行账户内 2670 万元于 2020 年 6 月 22 日通过网络被骗取。

证券代码：600683　　证券简称：京投发展　　编号：临2020-037

京投发展股份有限公司
关于子公司重大事项的公告

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性承担个别及连带责任。

公司接到持股 50%、由合作方负责操盘的子公司北京京投银泰置业有限公司（以下简称“银泰置业”）报告，其财务人员遭遇犯罪团伙电信诈骗，导致银泰置业银行账户内 2670 万元人民币于 2020 年 6 月 22 日通过网络被骗取。案发后银泰置业财务人员已第一时间向公安机关报案并于 2020 年 6 月 23 日收到了公安机关出具的《受案回执》（京公房（长阳）受案字（2020）51984 号）。

目前，公安机关正在积极侦办，已经冻结了部分被骗取资金。由于案件正处于侦办阶段，最终影响尚不能确定。公司将积极配合公安机关侦办此案，并密切关注该案件的侦办情况，及时履行信息披露义务，敬请广大投资者注意投资风险。

特此公告。

京投发展股份有限公司董事会
2020 年 6 月 23 日

据称，银泰置业为京投发展持股 50%、由合作方负责操盘的子公司，其财务人员遭遇犯罪团伙电信诈骗。案发后，银泰置业财务人员已第一时间向公安机关报案，并于 2020 年 6 月 23 日收到了公安机关出具的《受案回执》（京公房（长阳）受案字（2020）51984 号）。

公告称，目前，公安机关正在积极侦办，已经冻结了部分被骗取资金。由于案件正处于侦办阶段，最终影响尚不能确定。公司将积极配合公安机关侦办此案，并密切关注该案件的侦办情况，及时履行信息披露义务，敬请广大投资者注意投资风险。

还有哪些上市公司遭遇电信诈骗

就在一周之前的 6 月 16 日，世龙实业发布公告称，近期因财务主管人员遭遇电信诈骗，导致公司银行账户内的 298 万元人民币通过网络被盗取。经公司报案，江西省乐平市公安局已经采取立案侦查措施。

更早以前的 2014 年 9 月，惠天热电发布公告称，其全资子公司沈阳热力工业安装工程公司于当年 8 月 27 日遭遇电信诈骗，涉案金额为 385 万元。

另据报道，2016 年，深圳能源也遭遇了一起电信诈骗。相关裁判文书显示，骗子通过“高仿”QQ，冒充公司党委副书记兼纪委书记，将财务总监拉入所谓的“公司高管对话群”，以董事长亟需“支付投标保证金”的名义，合计骗取 3500 万元。（来源：互联网综合整理）

➢ 美加州旧金山大学向勒索软件支付 114 万美元赎金

2020 年 6 月 29 日，加州大学旧金山分校(UCSF)一所致力于治疗新冠肺炎的医学研究机构承认，该机构向黑客支付了 114 万美元的赎金。黑客是一个名叫 Netwalker 的网络犯罪团伙。在过去两个月里，该犯罪团伙至少与另外两起针对大学的勒索软件攻击案有关。

通过勒索软件对事主进行敲诈，近来在网络世界相当猖獗。乍一看，黑客的暗网主页看起来像一个标准的客服网站，它有一个常见问题(FAQ)标签，并提供软件的“免费”样本和一个实时聊天选项。但真正让人触目惊心的是，它有一个倒计时的计时器，一旦到了某一个时点，要么赎金被黑客翻倍，要么被他们用恶意软件加密的受害者数据就会被删除。

据了解，加州大学旧金山分校被勒索的经过是这样的

2020 年 6 月 5 日，黑客通过电子邮件或在被黑的电脑屏幕上留下的赎金通知，要求加州大学旧金山分校支付赎金。原来，黑客注意到该校一年赚了数十亿美元，于是要求 300 万美元，否则就会删除被他们加密劫持的数据。

代表加州大学谈判的代表表示，由于新冠肺炎肆虐全美，给学校造成了严重的经济损失，因此学校只能支付 78 万美元。经过一天的反复谈判，加州大学旧金山分校表示，它已经筹集了所有可用的资金，可以支付 102 万美元——但犯罪分子拒绝低于 150 万美元。几个小时后，双方谈妥了最终的价格——11140895 美元。第二天，116.4 个比特币被转移到 Netwalker 的电子钱包，解密软件也被送到了加州大学旧金山分校。

当被问及作为一所服务于公众利益的大学，为什么要向黑客组织支付赎金时，加州大学旧金山分校表示，加密的数据对于他们所从事的一些学术工作非常重要。因此，学校被迫做出了一个艰难的决定，决定向实施恶意软件攻击黑客支付巨额赎金，以换取解锁加密数据的工具，并拿回黑客获取的数据。

目前，加州大学旧金山分校正在协助 FBI 进行调查，同时努力恢复所有受影响的系统。事情远未结束，加州大学旧金山分校支付赎金的做法是否妥当，引起了广泛争议。网络安全专家表示，这种谈判现在在世界各地都在进行，有时涉及的金额甚至更大，但是这明显违背了包括美国联邦调查局、欧洲刑警组织和英国国家网络安全中心在内的执法机构的建议。

来自欧洲刑警组织的 Jan Op Gen Oorth 说：“受害者不应该支付赎金，因为这会资助犯罪分子并鼓励他们继续其非法活动。相反，他们应该向警方报告，这样执法部门就可以瓦解犯罪团伙。”

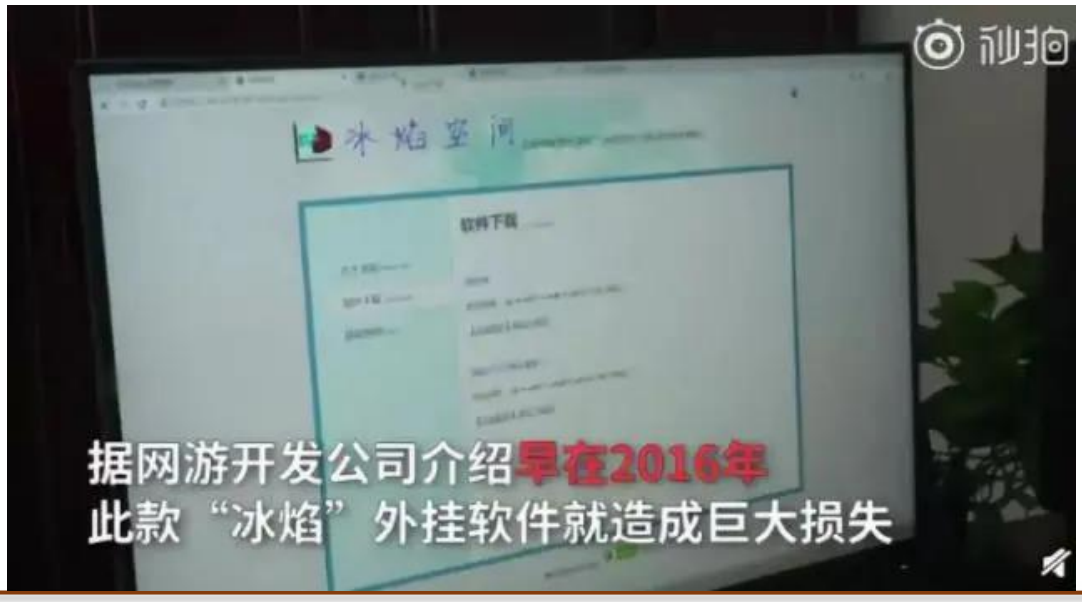
网络专家提醒大家：大多数勒索软件攻击始于 email 陷阱。研究表明，犯罪团伙越来越多地使用可以通过一次下载就进入系统的工具。仅在本月的第一周，Proofpoint 公司的网络安全分析人员就观察到了 100 多万封发送到美国、法国、德国、希腊和意大利的电子邮件，邮件中使用了各种钓鱼诱饵，包括虚假的 Covid-19 检测结果。Proofpoint 公司表示，对于 IT 管理员来说，大学确实是一个具有挑战性的环境。因为不断变化的学生人数，加上开放和信息共享的文化，与有效保护用户和系统免受攻击所需的规则和控制会经常发生冲突。因此，学校、公司等各类组织要经常备份自己的关键数据，以防万一。（来源：财以经世）

➢ 博士做游戏外挂赚 12 万获刑 被抓才知道帮人赚 300 万

2020 年 7 月 3 日报道，近日，因犯侵入、非法控制计算机信息系统程序罪，博士毕业生申某被判处有期徒刑一年缓刑一年，并处罚金两万元。在这起警方破获的案件中，申某还是一名中科大的博士，写代码是他的兴趣爱好，为赚外快，他参与编写游戏外挂程序，并由团伙其他成员通过网络进行销售。

在“净网 2019”行动中，扬州广陵警方成功侦破这起非法制售“冰焰”外挂的案件，抓获犯罪嫌疑人 4 人，涉案金额达 300 多万。

2019 年，北京某公司到扬州广陵公安分局网络安全保卫大队报案称，从 2016 年 6 月份以来，该公司发现大量游戏用户在一款游戏中使用一款名为“冰焰”的游戏外挂。这款外挂具有自动打怪、自动刷副本、自动与其他游戏玩家 PK 等功能。该公司表示，这款外挂软件导致公司大量在线用户迅速流失，给公司造成了巨大损失。



自己每月仅分 4000 多元报酬 总共获利 12 万余元

接到报案后，网安大队立即成立专案组。民警经过调查发现，该外挂软件主要通过犯罪嫌疑人自己搭建的网站进行销售。经过缜密侦查，民警在河南、四川、安徽和福建将犯罪嫌疑人魏某、段某、申某和傅某 4 人抓获归案，当场查扣计算机 6 台。

警方调查，该犯罪团伙分工明确，魏某是该团伙协调组织和销售者，段某是网站的客服，主要负责解答游戏玩家使用过程中的问题，而申某则是该外挂软件主要程序的编写者，傅某提供外挂软件的答题功能。自 2016 年 6 月起，该团伙累计销售该外挂软件 60 余万人次，销售金额达 300 余万元。

而申某案发前在合肥某能源公司上班，每个月工资收入近万元。为了赚取外快，申某为魏某编写外挂程序，并负责平时软件更新。魏某平时每个月付给申某 4000 多元的报酬，至案发时申某非法获利 12 万余元。被警方抓获归案后，申某也将丢掉工作。（来源：每日经济新闻）

➢ 上海某物流公司数据泄露 在暗网上被买卖群发赌博短信

2020 年 6 月 30 日报道，通过暗网论坛、telegram 等社交平台非法获取、买卖公民个人信息，指使他人群发包含赌博等违法内容的短信，致使全国各地不特定公众的利益受到损害。近日，上海市青浦区检察院对被告人熊某提起刑事附带民事公益诉讼，建议法院判令熊某在国家级媒体上公开向社会赔礼道歉，注销涉案账户，并永久删除其中存储的相关数据信息。

2018 年 9 月，熊某通过 QQ 群认识了游某(另案处理)。后来，熊某做起了暗网生意，他安排游某在暗网论坛和即时通讯软件 telegram 上发布买卖数据的广告：出售棋牌、彩票、股票、信用卡、网贷、区块链、业主、车主、母婴、网购数据。熊某承诺，若有人通过游某发布的广告达成交易，游某可获得 20%的提成。

2019 年 10 月，熊某开始让游某帮忙整理买来的 200 多万条数据。这些数据分为棋牌类、网贷类、网购类等不同类型，内容涵盖姓名、手机号、验证码、借款金额、地址、快递单号、商品名称以及购物平台名称等信息。游某通过软件对熊某提供的手机号先进行空号检测，确保可以接收短信，再根据手机号的地区、运营商进行分类。游某从这 200 多万条数据中整理出有效数据后发送给熊某，熊某再将其出售给他人。

熊某提供给游某的这些数据，一部分是直接从他人处购买的，另一部分则是租用后台调取的。据称，网络上有人通过提供后台服务器地址、账号和密码，出租棋牌、博彩、网购等平台的后台权限，使租用者能够通过网页或者远程桌面连接的方式登录后台，调取后台数据记录。

除了买卖个人信息牟取不法利益，熊某还利用这些信息推广赌博网站。2019 年 10 月，熊某找到王某(另案处理)，向其提供了一批买来的手机号码以及编辑好的短信内容，让其帮忙群发。短信内容为繁体字广告以及赌博网站的网址链接。

2019 年 11 月，上海某物流公司发现数据在 telegram 上泄露后报警。警方根据公司提供的线索，抓获了熊某。经查，2019 年 7 月至 11 月，熊某通过暗网论坛、telegram 等社交平台非法获取、买卖公民个人信息 40 万余条;2019 年 10 月至 11 月，熊某指使他人群发包含赌博等违法内容的短信至 3 万多名手机用户。

青浦区检察院审查后认为：熊某违反国家有关规定，非法获取、出售公民个人信息，情节特别严重;又伙同他人利用信息网络发布违法犯罪信息，情节严重，应当以侵犯公民个人信息罪、非法利用信息网络罪追究其刑事责任。今年 3 月 24 日，该院对被告人熊某以侵犯公民个人信息罪、非法利用信息网络罪提起公诉。

基于熊某的行为致使社会公共利益受损，应当依法承担相应的民事侵权责任，4 月 1 日，该院决定立案审查，并依法刊登诉前公告，后未收到有关机关或组织就该案向法院提起公益诉讼的回复，该院遂对其提起刑事附带民事公益诉讼。（来源：检察日报）

➢ 一男子在网上贩卖大量微信号 被南京警方刑事拘留

2020 年 7 月 2 日报道，6 月 23 日上午，南京江宁警方抓获一名涉嫌帮助信息网络犯罪活动的嫌疑人王某。王某自去年 4 月份以来，一年多的时间内，通过网络贩卖微信号 6000 多个，非法获利 5 万余元。

经警方调查，王某是偶然的机会在网上了解到有人在做倒卖“微信号”的生意，在利益的驱使下发展成为其销售代理，以每个微信号 38 元的批发价格，从上家处购买。购买后再以发广告的形式招募下家购买。每个微信号再以 42——45 元的价格售出，从中获利。

据王某自己交代，这些被售出的微信号都是境外手机号注册，买家拿到微信号和密码需要验证码才能登录。因此在售卖微信号的同时王某还会发给对方一个数据文档，买家通过相关破解软件破解该数据文档后就可以免验证码登录。这样的操作方式登录后的微信号不仅是不法分子违法犯罪的“工具”，同样还是他们强有力的“保护伞”。卖家王某自己也非常清楚他贩卖出去的微信号将用作赌博、诈骗等违法行为。

经查，嫌疑人王某的行为已经触犯了《中华人民共和国刑法》第 287 条之二的规定，涉嫌帮助信息网络犯罪活动罪。目前，王某已经被警方刑事拘留，此案正在进一步办理中。（来源：中国法院网）

信息安全意识产品服务

021-33663299