国盟信息安全通报

2022 年 2 月 28 日第 248 期

国盟信息安全通报

（第 248 期）

国际信息安全学习联盟

2022 年 02 月 28 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 497 个，其中高危漏洞 153 个、中危漏洞 320 个、低危漏洞 24 个。漏洞平均分值为 6.07。本周收录的漏洞中，涉及 0day 漏洞 195 个（占 39%），其中互联网上出现“Saraban 文件上传漏洞、Saraban 访问控制错误漏洞”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 4976 个，与上周（2382 个）环比增加 109%。

主要内容

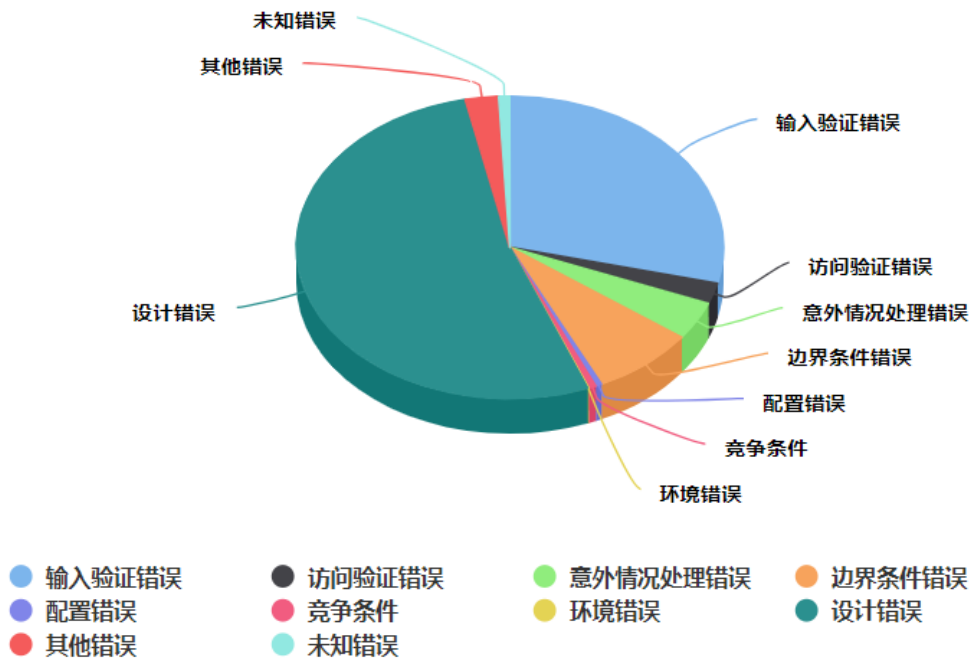
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

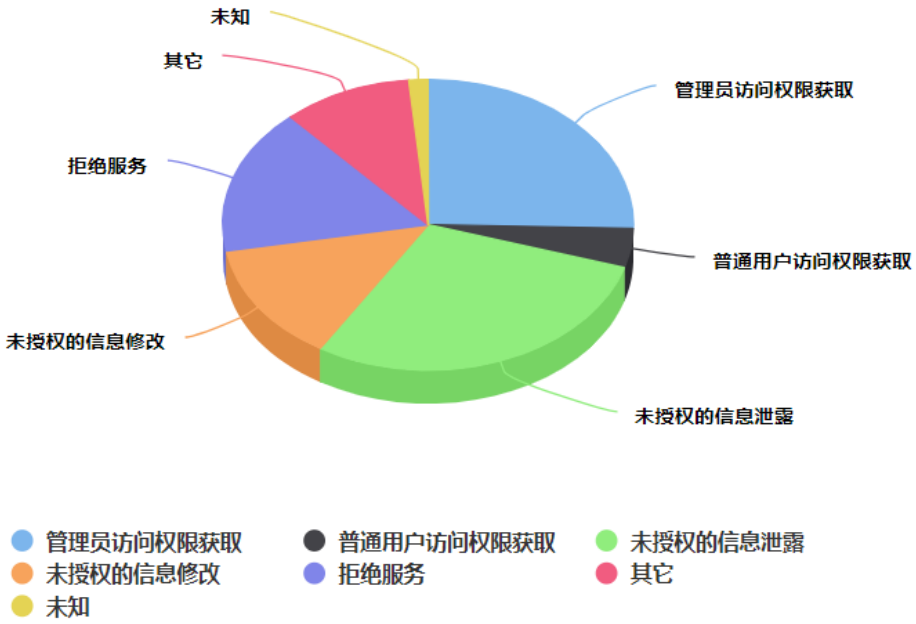
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 497 个，其中高危漏洞 153 个、中危漏洞 320 个、低危漏洞 24 个。漏洞平均分值为 6.07。本周收录的漏洞中，涉及 0day 漏洞 195 个（占 39%），其中互联网上出现“Saraban 文件上传漏洞、Saraban 访问控制错误漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4976 个，与上周（2382 个）环比增加 109%。

二、安全漏洞增长数量及种类分布情况

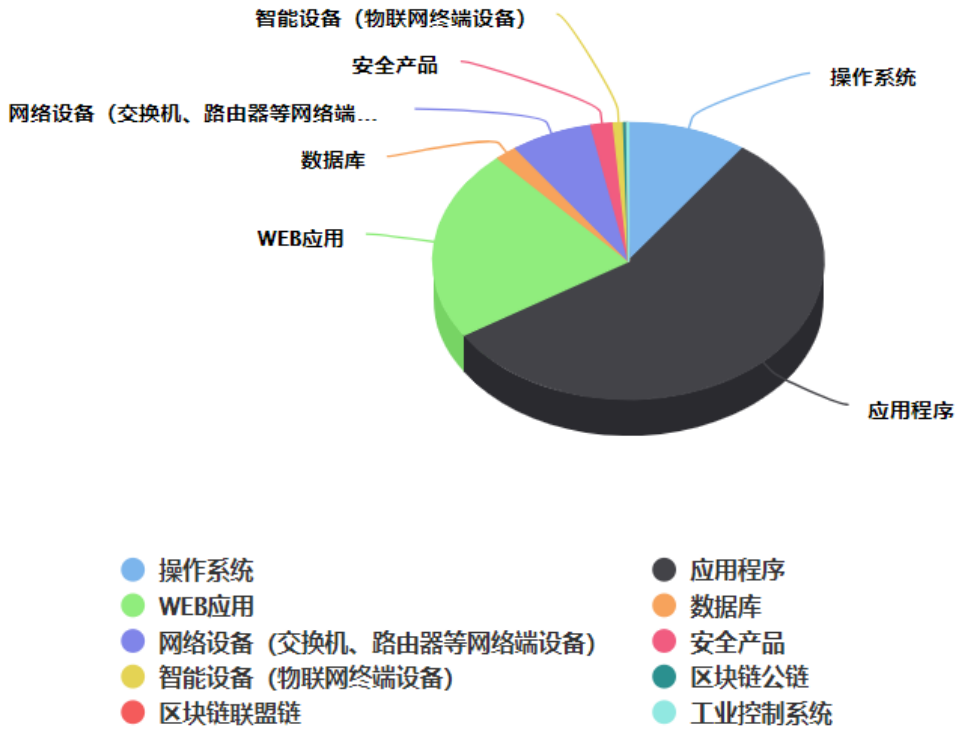
➢ 漏洞产生原因（2022 年 2 月 1 日—2022 年 2 月 28）



➢ 漏洞引发的威胁（2022 年 2 月 1 日—2022 年 2 月 28）



➢ 漏洞影响对象类型（2022 年 2 月 1 日—2022 年 2 月 28）



三、安全产业动态

➢ 汇聚向上向善力量 加快网络文明建设

网络文明与信息时代相伴而生，集中反映了互联网发展、治理、运用中形成的文明成果。加强网络文明建设，是顺应信息时代潮流、提高社会文明程度的必然要求，是坚持以人民为中心、满足亿万网民对美好生活向往的迫切需要，是加快建设网络强国、全面建设社会主义现代化国家的重要任务。

党的十八大以来，以习近平同志为核心的党中央高度重视网络文明建设，党的十九届五中全会对加强网络文明建设作出明确部署，中央制定实施《关于加强网络文明建设的意见》，成功举办首届中国网络文明大会，各地区各部门结合实际、勇于实践、锐意创新，我国网络文明建设日益深入人心、取得明显成效。

>> 首届中国网络文明大会发布新时代网络文明建设十件大事。

习近平总书记在致首届中国网络文明大会的贺信中指出：“要坚持发展和治理相统一、网上和网下相融合，广泛汇聚向上向善力量。各级党委和政府要担当责任，网络平台、社会组织、广大网民等要发挥积极作用，共同推进文明办网、文明用网、文明上网，以时代新风塑造和净化网络空间，共建网上美好精神家园。”习近平总书记的重要论述，登高望远、视野宏阔、内涵丰富、思想深邃，站在人类社会进入信息时代的战略高度，深刻回答了加强新时代网络文明建设的重大理论和实践问题，为我们做好工作指明了前进方向、提供了根本遵循。

立足新起点、奋进新征程，我们要深入学习贯彻习近平总书记关于加强网络文明建设的重要论述，坚持正能量是总要求、管得住是硬道理、用得好是真本事，大力培育和弘扬社会主义核心价值观，推动网络文明蔚然成风，为全面建设社会主义现代化国家、实现第二个百年奋斗目标提供坚强思想保证、强大精神动力、有力舆论支持、良好文化条件。

坚持举旗铸魂，以党的创新理论引领网络空间

党的十九届六中全会指出：“党确立习近平同志党中央的核心、全党的核心地位，确立习近平新时代中国特色社会主义思想的指导地位，反映了全党全军全国各族人民共同心愿，对新时代党和国家事业发展、对推进中华民族伟大复兴历史进程具有决定性意义。”习近平新时代中国特色社会主义思想是当代中国马克思主义、二十一世纪马克思主义，是中华文化和中国精神的时代精华，实现了马克思主义中国化新的飞跃，具有强大的思想引领力、实践指导力、精神感召力。

要高举思想旗帜。坚持以习近平新时代中国特色社会主义思想统领互联网内容建设，牢牢把握正确政治方向、舆论导向、价值取向，发挥网络传播优势，做好重大主题策划，加强个性化、可视化、互动化传播，阐释好习近平新时代中国特色社会主义思想蕴含的深刻道理学理哲理，推动网上理想信念教育常态化制度化。

要建强理论阵地。深入推进媒体融合发展，实施移动优先战略，加快推进各类理论资源数字化、网络化、智能化传播和应用，加强重点理论网站、公众账号、客户端建设，构建网上理论传播矩阵，让党的创新理论通过互联网“飞入寻常百姓家”。

要创新手段载体。广泛开展大众化理论传播，持续创新话语体系、宣传语态、表现形式、组织方式，打造内容鲜活、形式新颖、可亲可感的“现象级”传播产品，引导广大网民特别是青少年网民进一步坚定听党话、跟党走的信心和决心，努力建设具有强大凝聚力和引领力的社会主义意识形态，不断巩固全党全国人民团结奋斗的共同思想基础。

坚持成风化人，以健康向上文化塑造网络空间

文化是一个国家和民族的精神血脉。培育健康向上的网络文化，是加强网络文明建设的重要内容，也是推动互联网健康有序发展的内在要求。近年来，伴随互联网的快速发展，网络文化蓬勃兴起，极大地丰富了人民群众的精神文化生活，为推动我国文化建设高质量发展发挥了积极作用。同时也要看到，一些与社会主义核心价值观相违背的错误思潮、低俗文化、落后观念等在网上仍时有传播，干扰网络秩序、污染社会风气，尤其是对青少年的健康成长产生不良影响。这就要求我们必须厚植文化土壤、弘扬新风正气，让健康向上的网络文化充盈网络空间。

要弘扬主流价值。把社会主义核心价值观体现到互联网信息服务和网络文化产品生产全过程，引导广大网民特别是青少年网民自觉用中华优秀传统文化、革命文化、社会主义先进文化培根铸魂、启智润心。

要赓续红色血脉。加强党史、新中国史、改革开放史、社会主义发展史网上宣传，精心打造有创意、接地气的图解、动漫、微视频等融媒体产品，旗帜鲜明反对历史虚无主义，弘扬伟大建党精神，进一步传承红色基因、凝聚网民力量。

要饱含人民情怀。始终坚持以人民为中心的发展思想，努力创作出更多思想精深、艺术精湛、制作精良的网络文艺精品，不断提高网络公共文化服务供给的普惠性和便捷性，更好满足人民群众日益增长的精神文化需求。

坚持崇德向善，以良好道德风尚滋养网络空间

人无德不立，网无德则乱。崇德向善是中华民族的优良传统，也是网络文明建设的基本价值追求和重要行为准则。近年来，在社会各界共同努力下，网络空间道德建设水平不断提升，爱国主义、集体主义广为弘扬，崇尚英雄、学习先进成为风尚，整体呈现向上向善的良好态势。同时，受不良思想文化侵蚀和网络有害信息影响，一些领域和个人仍不同程度存在着道德失范现象，道德观念缺失、违背公序良俗等事件仍时有发生。这就要求我们必须在网络空间全面推进社会公德、职业道德、家庭美德、个人品德建设，持续强化教育引导、实践养成、制度保障，用道德滋养人心、凝聚力量。

要强化示范引领。广泛开展时代楷模、道德模范、最美人物、身边好人和优秀志愿者等典型案例和事迹网上宣传，推动形成崇德向善、见贤思齐的网络环境，让讲道德、尊道德、守道德在网络空间蔚然成风。

要坚持科技向善。深化网络诚信建设，大力传播诚信文化，鼓励支持互联网企业和平台完善内部诚信规范与机制，营造诚信办网、诚信用网的良好氛围。深入实施网络公益工程，拓展“互联网+公益”模式，广泛开展形式多样的网络文明志愿服务和网络公益活动。

要提高网络素养。深入开展争做中国好网民工程，引导网民培育正确的道德判断、道德责任，特别是聚焦青少年网民群体，引导青少年从自身做起，强化道德认同、投身文明实践，涵养高尚的道德追求，培育良好的文明习惯。

坚持激浊扬清，以综合治网管网净化网络空间

营造天朗气清的网络生态，是推动网络文明建设高质量发展的重要标志。没有良好的网络生态，就没有繁荣的网络文明。近年来，网信系统加快建立完善网络综合治理体系，集中整治“饭圈”乱象、恶意营销、流量造假、网络“黑公关”等群众反映强烈的问题，推动网

络生态持续向好。同时也要清醒地看到，网络谣言、网络诈骗、网络暴力、网络信息泄露等违法违规问题突出，需要综合多种手段、采取多重举措，激浊扬清、扶正祛邪，为广大网民营造良好的网络生态环境。

要深化专项整治。持续推进“清朗”“净网”系列专项行动，紧盯视频直播、公众账号、互动社区、知识问答等重点领域开展清理整治，规范网络传播秩序，强化辟谣联动和举报处置，坚决惩治各类网络不文明行为，引导广大网民自觉弘扬真善美、抵制假丑恶。

要强化依法治网。加快制定修订未成年人网络保护条例、互联网信息服务管理办法等法规制度，增强网络执法震慑威力，依法严厉打击网络违法违规行为，创新开展网络普法系列活动，着力实现依法治网和以德润网的有机统一。

要压实平台责任。引导督促网站平台充分发挥信息内容管理第一责任人作用，把社会效益摆在突出位置，加强自身规范建设，完善社区规则、健全审核机制、提升内容质量，加强榜单排行、算法推荐、弹窗推送等重点功能管理，提高网络从业人员政治素质和业务能力，严防违法违规信息生产传播。

坚持强基固本，以社会共同参与守护网络空间

社会各界的关心支持和积极参与，是深化网络文明建设的坚实基础和不竭动力。网络空间是亿万民众共同的精神家园，把网络空间发展好、守护好，是全社会的共同责任。这就要求我们必须充分发挥各地区各部门的积极性主动性创造性，坚持方方面面齐动手，构建网上网下同心圆，汇聚起网络文明建设的磅礴力量。

要加强组织领导。各级党委和政府要把网络文明建设摆上重要议事日程、纳入全局谋划推进，各级网信办要与本级文明办配合做好网络文明建设的组织指导和协调服务，着力形成党委统一领导、党政齐抓共管、有关部门各负其责、全社会积极参与的良好局面。

要夯实工作基础。进一步完善网络文明建设有关制度规定，在各类文明创建中鼓励制定出台有针对性的网络文明准则，有力推进群众性精神文明创建活动向网上延伸，推动基层深入开展网络文明建设活动。

要广泛汇聚合力。鼓励支持互联网企业、各级网络社会组织、广大网民积极主动参与网络文明建设，深化拓展中国正能量“五个一百”网络精品征集评选展播工程、网络中国节、阳光跟帖等品牌活动，持续办好中国网络文明大会，深入凝聚社会共识和行业力量，实现网上网下文明建设互促共进、融合发展。（来源：2022 年第 1 期《旗帜》杂志刊发中央宣传部副部长、中央网络安全和信息化委员会办公室主任、国家互联网信息办公室主任庄荣文署名文章。）

➢ 新修订的《网络安全审查办法》为网络安全做“加法”

2022 年 2 月 15 日，由国家互联网信息办公室等十三部门联合修订发布的《网络安全审查办法》（以下简称《办法》）正式施行。“此次修订以维护数据安全为中心，要求超过 100 万用户个人信息的网络平台运营者赴国外上市时必须申报网络安全审查，以做‘加法’的方式，新增了不少亮点。”北京航空航天大学工业和信息化法治研究院研究员雷震文在接受采访时表示。

在扎根实践中不断完善

互联网产品与服务在为日常生活带来巨大便利的同时，也带来了安全漏洞、数据泄露等网络安全威胁。《2020 年中国互联网网络安全报告》指出，近年来网络产品和服务供应链安全形势愈加严峻，针对关键信息基础设施的信息窃取、攻击破坏等恶意活动持续增加，针对数据的网络攻击以及数据滥用问题日趋严重，数据安全风险在未来将更加突出。

“网络安全审查是网络安全领域的重要法律制度。”国家网信办有关负责人在介绍《办法》修订背景时表示，2021 年 9 月 1 日，《数据安全法》正式施行，明确规定国家建立数据安全审查制度，据此对《办法》进行修订，主要目的是进一步保障网络安全和数据安全，维护国家安全。

在雷震文看来，再次修订《办法》可以从两个方面理解：一是应对网络安全新形势、新挑战的需要，多国网络空间博弈不断激烈，网络对抗与商业竞争和金融竞争逐渐融合，这给我国的网络安全维护带来了很多新问题；二是修订原《办法》能够为《数据安全法》相关规

范的落实提供进一步的依据。

为维护数据安全做“加法”

“此次修订以维护数据安全为中心，以做‘加法’的方式，新增了不少亮点。”雷震文认为，扩大网络安全审查适用的范围是本次修订的首要亮点。

《办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查范围，并明确要求掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须申报网络安全审查。“作为社会数字基础设施的网络平台往往聚集着海量数据，其数据处理行为可能会对国家安全和社会公共利益产生直接的影响。”雷震文解释称，《办法》对网络平台运营者的安全审查主要集中在两个方面：一是对平台运营者开展数据处理活动的审查，二是就特定网络平台运营者赴国外上市进行安全审查。

“此外，《办法》对审查工作机制成员、审查重点评估的国家安全风险因素也进行了扩充。”雷震文介绍，《办法》增加了中国证券监督管理委员会作为国家网络安全审查工作机制成员，新增了网络安全审查重点评估中的国家安全风险因素。

“《办法》对审查程序相关的部分规范也作出了必要调整，一是延长了特别审查程序的期限，即由原来的 45 个工作日延长至 90 个工作日；二是新增关于当事人在审查期间的义务的规定。”雷震文强调，这对于进一步发挥网络安全审查制度的实际功能，切实防范和控制网络安全风险具有十分积极的意义。

化解风险需要关口前移

“推行网络安全审查，加强风险识别和控制，是当前世界各主要国家防范网络安全风险的通行做法。”雷震文表示，此次《办法》的修订对于进一步扎实“篱笆”，有效应对数字社会、平台经济发展中出现的各类新型网络安全风险，对切实维护我国国家网络主权和安全具有积极的现实意义。

第 48 次《中国互联网络发展状况统计报告》显示，2021 年上半年，工业和信息化部网络安全威胁和漏洞信息共享平台接报网络安全事件 49605 件。“网络安全审查的主旨在于网络风险的识别与防范，是国家安全审查的重要组成部分。网络平台运营者是维护网络安全、国家安全的重要责任主体。”雷震文表示，保障数据安全与网络安全，要防患于未然。

对此，雷震文建议，网络平台运营者化解网络安全风险、国家安全风险，应该注意以下三个方面：首先，应提高安全意识、法治意识，尤其应正确理解和处理维护网络安全与促进自身发展之间的关系，坚持安全发展理念，筑牢网络安全的基石；其次，应不断增强对自身运营安全的管理和评估，积极对照《网络安全法》和《数据安全法》的相关规定以及《办法》

第 10 条列出的安全风险因素，做好安全风险的预判和评估、管理工作；最后，积极主动申报和配合网络安全审查，凡符合《办法》规定的审查条件的当事人都应负有主动申报并配合审查办公室做好安全审查工作的义务。（来源：人民网-强国论坛）

➢ 拥抱个人信息保护“法时代”

在信息化时代，个人信息保护已成为广大人民群众最关心最直接最现实的利益问题之一。2021 年 8 月发布的《中国互联网络发展状况统计报告》显示，截至 2021 年 6 月，我国网民规模达 10.11 亿，互联网普及率达 71.6%，个人信息的收集、使用更为广泛。

“安装手电筒程序，要提供地理位置信息”“下载文字编辑 APP，却需获取通讯录权限”“家里孩子刚出生，每天就有应接不暇的母婴用品广告推送”……人们享受着数据带来的便利的同时，随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全等问题仍十分突出。

2021 年 8 月 20 日，《中华人民共和国个人信息保护法》（以下简称个人信息保护法）经十三届全国人大常委会第三十次会议表决通过，于 2021 年 11 月 1 日起施行。个人信息保护法共八章七十四条，坚持和贯彻以人民为中心的法治理念，牢牢把握保护人民群众个人信息权益的立法定位，聚焦个人信息保护领域的突出问题和人民群众的重大关切，全方位构筑个人信息“保护网”，最大限度保护公民的个人信息权益。

个人信息保护法强调，处理个人信息应当遵循合法、正当、必要和诚信原则，具有明确、

合理的目的并与处理目的直接相关，采取对个人权益影响最小的方式，为个体权利在个人信息保护领域举起新旗帜。

“我的权利我做主”在个人信息保护法中得到了体现。“告知——同意”是法律确立的个人信息保护核心规则。个人信息处理者在取得个人同意的情形下方可处理个人信息，个人信息处理的重要事项发生变更，应当重新向个人告知并取得同意。

针对群众反映强烈的“一揽子授权”“强制同意”等问题，个人信息处理者在处理敏感个人信息、向他人提供或公开个人信息、跨境转移个人信息等环节应取得个人的单独同意，明确个人信息处理者不得过度收集个人信息，不得以个人不同意为由拒绝提供产品或者服务，并赋予个人撤回同意的权利。

同一平台上的同一款产品或服务，对“熟客”的报价可能要比新用户更高。面对饱受诟病的互联网平台“大数据杀熟”现象，个人信息保护法规定，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的公平、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。

超大型互联网平台掌握了海量用户数据，一旦发生信息泄露或者滥用，可能导致极为严重的后果。个人信息保护法特别规定了这类平台需要履行的义务，包括建立健全个人信息保护合规制度体系，定期发布个人信息保护社会责任报告，接受社会监督等。

网络空间是亿万民众共同的精神家园。全国人大常委会法工委经济法室副主任杨合庆表示，个人信息保护法以严密的制度、严格的标准、严厉的责任，构建了权责明确、保护有效、利用规范的个人信息处理和保护制度规则。社会各方面应当加强个人信息保护宣传教育，提升个人信息保护法治意识，推动个人信息保护法落地实施，助力网络强国、数字中国、智慧社会建设。

我们可以期待，随着个人信息保护法的实施、司法和执法的不懈推进、多方参与共治的持续发力，广大人民群众将长久拥抱个人信息合法权益受保护、个人信息处理活动受规范、个人信息合理利用受促进的数字治理新时代。（来源：全国人大）

➢ 微信办公泄密的四个高风险环节

近年来，机关单位工作人员违规通过微信等移动应用发布、传输、处理涉密文件材料的泄密行为多发易发、禁而不绝。这是移动互联网普及给保密管理带来的风险挑战。究其根源，

主要还是由于机关单位保密制度执行不严、保密管理不到位，工作人员保密意识、保密常识欠缺等问题导致的。全面加强微信使用的保密管理，规范工作人员特别是日常工作中接触、知悉国家秘密人员的移动办公行为，已刻不容缓。从用微信办公的各环节上看，绝大多数失泄密问题发生在以下四个环节，必须引起高度警惕。

材料起草

材料起草阶段是微信泄密最为高发的环节。目前来看，主要有两类泄密行为：一是通过微信群对涉密材料征求意见。例如，某市政府办公室干部小张，为市领导起草发言材料时，引用了涉密文件内容，但主观臆断“引用一两句话不至于涉密”，便将材料发送至微信群征求意见。经鉴定，该材料属于秘密级国家秘密。案件发生后，小张被给予政务警告处分。反思这起案件，小张的保密意识不强、对文件的涉密属性没有正确认识是案件发生的根本原因。

二是利用图文识别微信小程序转换涉密文件。许多工作人员在起草材料时，为方便摘抄、引用文件资料，经常利用图文识别类移动应用对文件拍照、转换，形成电子文档以减少敲键盘之累。对可以公开的文件资料进行转换无可厚非，但有些人为偷一时之懒，对涉密文件竟铤而走险，按此法处理，自认为无人知晓，实际是掩耳盗铃。相关涉密文件已经被上传到互联网服务器上，对国家秘密安全造成危害。

例如，某县公安局办公室干部小赵，为图便利，利用某款图文识别小程序转换一份机密级文件，文件随即被该小程序运营公司工作人员从服务器中获取并公开发布，造成恶劣影响。案件发生后，小赵被给予党内警告、政务警告处分。

传达部署

通过微信群传达文件、部署工作，是当下许多机关单位的工作常态。然而，一些工作人员养成“依赖症”，贪图方便，将涉密文件、涉密工作也通过微信群传达部署，造成了大量泄密案件发生。

例如，某市教育体育局办公室干部小黄，为尽快开展工作，将该市印发的一份秘密级文件拍照并发到校长联络群，部分群成员进而转发到本校微信工作群，造成文件在 40 多个微信群中传播。案件发生后，小黄被给予政务记过处分。

又如，某涉密单位办公室工作人员小张，为省时省力，同时又怕被发现，将一份机密级文件的红头和密级标志遮盖后拍照，发到下属单位微信群。案件发生后，小张被给予党内严重警告处分并扣发绩效奖金。

再如，某市住建局办公室干部小王，根据一份机密级通知起草该局相关文件时，为方便从非涉密内网传达，不依法派生定密，擅自将文件降为工作秘密。该局下属单位小孙收到文件后，也为图方便，将本单位相应文件擅自降为不涉密，在微信群传达部署。案件发生后，小王、小孙均被给予政务记过处分。

密件阅知

这一环节，大多数责任人员往往是为了工作方便，对涉密文件进行拍照，通过微信进行传递。例如，某市海洋与渔业局办公室干部小金，在市机要局阅知一份机密级密码电报时，因事情较为紧急，担心抄录字迹潦草，便偷拍电报主体内容，并通过微信“点对点”发给该局多名领导。案件发生后，小金被给予行政记过处分。

又如，某区公安分局交通巡逻警察支队几名辅警在阅知一份涉密安保方案时，为节省传阅时间，便于后续查看，将安保任务安排内容拍照并发至微信群。案件发生后，责任人员被给予辞退处理。

宣传报道

目前，微信公众号已是许多机关单位的重要宣传窗口。一些单位在微信公众号发布信息保密审查不严，导致将涉密内容发布至官方微信公众号的案件时有发生。微信公众号受众范围广、转发方便，一旦发布涉密信息，往往容易引发大范围泄密。

例如，某涉密单位宣传部门工作人员小胡，根据有关涉密文件内容起草了该单位开展相关工作的新闻宣传稿，自以为已脱密处理，经部门分管领导简单审核后，在单位微信公众号公开发布，迅速被多个微信公众号转载、解读，造成不良影响，经鉴定，发布内容涉及机密级国家秘密。案件发生后，小胡及相关领导责任人均被给予党内严重警告、行政记大过处分。

总的来看，绝大多数微信泄密的责任人员，主观上都属于过失状态，或是缺乏常识，不知不惧，不知其不可为；或是意识欠缺，明知其不可为，却因麻痹大意或者侥幸心理而仍为之。但无论故意还是过失，通过微信发布、传输、处理涉密文件材料，都将对国家安全和利益造成严重风险甚至危害。对此，保密意识、保密常识的“两识”普及教育还需久久为功、不断深入开展。各机关单位及其工作人员要高度警惕、紧紧扭住上述四个高风险环节，绷紧保密之弦，布好保密防线，时刻防范失泄密事件发生。

第一，材料起草要履行定密程序。在材料起草环节，应当认真考虑、核实是否可能涉及国家秘密、工作秘密，对于内容较为敏感、可能涉密特别是引用涉密文件的，要在涉密计算机中起草，并标注国家秘密、工作秘密标志，起草完成后，必须严格履行定密审核程序，明确可以公开的，才能通过互联网传输、处理。保密工作机构要加强对材料起草人员的监督，督促其严格履行定密程序、落实保密要求，禁止通过互联网应用识别、转换涉密材料。

第二，传达部署要脱密处理。传达文件、部署工作前，务必认真核实涉密属性，涉密文件传达、工作部署，应当按照保密规定、采取保密措施进行。特殊情况需要通过互联网渠道传达部署的，必须事先进行全面彻底的脱密脱敏处理。是否已脱密脱敏，绝不能任凭个人主观臆断，应当逐级请示文件产生的机关、单位，按程序审慎处理。

第三，密件阅知要做好监督提醒。涉密文件管理人员要做好对阅文人员的监督提醒，严格办理登记并明确告知禁止手机拍摄、微信传输等行为。密件传阅过程中，工作人员相互间要做好监督提醒，一层提醒一层、层层抓落实，严防不知不惧者、铤而走险者，发现微信泄密行为的，要立即向保密工作机构报告，保密工作机构要果断采取补救措施，并及时向保密行政管理部门报告。

第四，宣传报道要加强保密审查。对于官方微信公众号，要严格做好信息发布保密审查，审查人员和相关运营人员要充分认识到自己所担负的保密责任，杜绝粗放式审核、走过场审批。涉密程度高的机关单位，要审慎设立微信公众号、微博等新媒体账号，慎之又慎发布信息，增设审核审批“关卡”，压实审查人员责任，避免失泄密事件发生。（来源：秘书工作）

四、政府之声

➢ 国务院：加强电子证照应用安全管理，严格保护信息安全

2022 年 2 月 22 日，国务院办公厅印发《关于加快推进电子证照扩大应用领域和全国互通互认的意见》(以下简称《意见》)，指出，着力破解电子证照应用中的难点堵点问题，积极拓展电子证照应用和服务领域，推动实现全国互通互认。


中华人民共和国中央人民政府
www.gov.cn
简 | 繁 | EN | 注册 | 登录
国务院 总理 新闻 政策 互动 服务 数据 国情 国家政务服务平台
首页 > 信息公开 > 国务院文件 > 综合政务 > 电子政务
收藏 留言
索 引 号： 000014349/2022-00016 主题分类： 综合政务\电子政务
发文机关： 国务院办公厅 成文日期： 2022年01月20日
标 题： 国务院办公厅关于加快推进电子证照扩大应用领域和全国互通互认的意见
发文字号： 国办发〔2022〕3号 发布日期： 2022年02月22日
主 题 词：
国务院办公厅关于加快推进
电子证照扩大应用领域和全国互通互认的意见
国办发〔2022〕3号
各省、自治区、直辖市人民政府，国务院各部委、各直属机构：
近年来，随着“互联网+政务服务”深入推进，各地区各部门依托全国一体化政务服务平台，积极推进电子证照应用，持续优化政务服务，在支撑政务服务事项办理减环节、减材料、减时限、减费用等方面取得了初步成效，政务服务便捷度、企业和群众获得感明显提升。但从全国层面看，电子证照还存在标准规范不健全、互通互认机制不完善、共享服务体系不完备、应用场景不丰富等突出问题。为加快推进电子证照扩大应用领域和全国互通互
相关报道
• 国务院办公厅印发《关于加快推进电子证照扩大应用领域和全国互通互认的意见》

《意见》强调，统筹发展和安全，加强电子证照应用全过程规范管理，严格保护商业秘密和个人信息安全，切实筑牢电子证照应用安全防线。意见》强调，加强电子证照应用安全管理和监管。加强电子证照签发、归集、存储、使用等各环节安全管理，严格落实网络安全等级保护制度等要求，强化密码应用安全性评估，探索运用区块链、新兴密码技术、隐私计算等手段提升电子证照安全防护、追踪溯源和精准授权等能力。按照信息采集最小化原则归集数据，对共享的电子证照进行分类分级管理，避免信息泄露。

加快推进国家网络身份认证公共服务基础设施建设和应用，加强对电子证照持证主体、用证人员的身份认证、授权管理和个人信息保护。强化企业和群众身份认证支撑，增强电子证照签发和使用等环节的统一身份认证能力。

建立健全严格的责任追究制度，依法严厉打击电子证照制作生成过程中的造假行为，杜绝未经授权擅自调用、留存电子证照信息，切实保障电子证照及相关信息合法合规使用，保护持证主体的商业秘密和个人信息。（来源：中国政府网）

- **《国务院办公厅关于加快推进电子证照扩大应用领域和全国互通互认的意见》**
- **全文：**http://www.gov.cn/zhengce/content/2022-02/22/content_5674998.htm

➢ 最高法发布《人民法院在线运行规则》

2022 年 2 月 22 日，最高人民法院召开发布会，发布《人民法院在线运行规则》（以下简称“《规则》”）。据最高人民法院信息中心主任许建峰介绍，这是继《人民法院在线诉讼规则》《人民法院在线调解规则》之后，最高法出台的又一份重要文件，将在世界范围内首次构建全方位、系统化的互联网司法规则体系。


中华人民共和国最高人民法院
The Supreme People's Court of The People's Republic of China
关注：
手机客户端
首页 学习新时代 机构设置 法院资讯 执行时讯 权威发布 公报 审判业务 法院建设 办事服务 公众互动 巡回法庭 驻院纪检监察组 关于我们
所在位置：首页 > 权威发布 > 通知(司法文件)
人民法院在线运行规则
来源：最高人民法院 发布时间：2022-02-22 11:08:37 字号： 打印本页
法发〔2022〕8号
最高人民法院
关于印发《人民法院在线运行规则》的通知
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：
《人民法院在线运行规则》已于2021年12月30日经最高人民法院审判委员会第1861次会议通过，现予以印发，自2022年3月1日起施行。
最高人民法院
2022年1月26日
人民法院在线运行规则
为支持和推进在线诉讼、在线调解等司法活动，完善人民法院在线运行机制，方便当事人及其他参与人在线参与诉讼、调解等活动，提升审

《人民法院在线运行规则》将于 2022 年 3 月 1 日起正式施行，共包括 5 个部分 45 条内容，涵盖人民法院在线运行的基本原则、适用范围，确定了人民法院用以支持在线司法活动的信息系统建设、应用、运行和管理要求。值得注意的是，该规则明确了人民法院在线运行网络安全、数据安全、个人信息保护等要求，并特别强调了关于用户信息保护的相关要求。

《规则》总则第二条人民法院在线运行遵循的原则第五小条“安全可靠”中指出，要“依法采集、存储、处理和使用数据，保护国家秘密、商业秘密、个人隐私和个人信息，保障人民法院在线运行信息安全。”《规则》第十二条规定，各级人民法院应当建设安全保障系统，包括身份认证平台、边界防护系统、安全隔离交换系统等，为各类信息基础设施、应用系统

和数据资源提供主机安全、身份认证、访问控制、分类分级等安全服务。

第三十四条规定，各级人民法院应当按照信息安全等级保护要求，确定智慧法院信息系统的安全保护等级，制定安全管理制度和操作规程，确定网络安全责任人，落实网络安全保护责任。

个人信息保护方面，《规则》第三十五条规定，各级人民法院应当确保智慧法院信息系统相关数据全生命周期安全，制定数据分类分级保护、数据安全应急处理和数据安全审查等制度；遵循“安全、必要、最小范围”原则实现数据共享和安全管控，保证在线诉讼、在线调解等司法活动中的个人隐私、个人信息、商业秘密、保密商务信息、审判执行工作秘密等数据依法予以保密，不被随意泄露或非法向他人提供。

第三十六条要求，各级人民法院应当指导、监督智慧法院信息系统建设、运行和管理中的个人信息保护工作；加强司法公开工作中的个人信息保护，严格执行法律规定的公开范围，依法公开相关信息，运用信息化手段支持个人敏感信息屏蔽、司法公开质量管控。（来源：最高人民法院）

- **《人民法院在线运行规则》全文：**
- https://www.court.gov.cn/fabu-xiangqing-346471.html

➢ 人行市场监管总局银保监会证监会印发《金融标准化“十四五”发展规划》

2022 年 2 月 8 日，中国人民银行会同市场监管总局、银保监会、证监会联合印发《金融标准化“十四五”发展规划》（以下简称《规划》）。《规划》依据《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》《国家标准化发展纲要》制定，明确“十四五”时期统筹推进金融标准化发展的指导思想、基本原则、主要目标、重点任务和保障措施。

《规划》以习近平新时代中国特色社会主义思想为指导，深入贯彻党的十九大和十九届历次全会精神，坚持以人民为中心，坚定不移贯彻新发展理念，以支撑金融业高质量发展为主题，以深化金融供给侧结构性改革为主线，以维护国家金融安全为底线，推动标准化与金融业重点领域深度融合，支持健全现代金融体系，融入和服务以国内大循环为主体、国内国际双循环相互促进的新发展格局。

《规划》提出，到 2025 年，与现代金融体系相适应的标准体系基本建成，金融标准化

的经济效益、社会效益、质量效益和生态效益充分显现，标准化支撑金融业高质量发展的地位和作用更加凸显。展望 2035 年，科学适用、结构合理、开放兼容、国际接轨的金融标准体系更加健全，市场驱动、政府引导、企业为主、社会参与、开放融合的金融标准化工作格局全面形成，标准化成为支撑金融业高质量发展的重要力量。

《规划》明确七个方面的重点。一是标准化辅助现代金融管理。完善金融风险防控标准，健全金融业综合统计标准，推进金融消费者保护标准建设，加强标准对金融监管的支持。二是标准化助力健全金融市场体系。完善金融基础设施标准，深入推进证券期货标准建设，加大黄金市场标准供给，拓展升级保险市场标准。三是标准化支撑金融产品和服务创新。加快完善绿色金融标准体系，有效推进普惠金融标准建设，加强产业链供应链金融标准保障。四是标准化引领金融业数字生态建设。稳步推进金融科技标准建设，系统完善金融数据要素标准，健全金融信息基础设施标准，强化金融网络安全标准防护，推进金融业信息化核心技术安全可控标准建设。五是深化金融标准化高水平开放。加快先进金融国际标准转化应用，积极参与金融国际标准化活动。六是推动金融标准化改革创新。优化金融标准供给结构，强化金融标准实施应用，培育金融标准化服务业，推动金融标准检测认证协同发展。七是夯实金融标准化发展基础。优化金融标准化运行机制，提升金融机构标准化能力，推动金融标准化工作数字化转型，加强金融标准化人才队伍建设。（来源：人民银行）

- **《金融标准化“十四五”发展规划》全文：**
- http://www.pbc.gov.cn/zhengwugongkai/4081330/4081344/4081395/4081686/4466286/in

dex.html

➢ 上海发布《企业数据合规指引》

2022 年 2 月 7 日，上海市杨浦区检察院发布首份《企业数据合规指引》(下称《指引》)。《指引》明确，一般由董事会直接设立企业合规部门，不建议由法务部门履行合规管理职能。企业最高管理者作为数据合规的第一责任人，需确保将数据合规落实情况和效果纳入企业内部人员绩效考核体系。

《指引》全文共 38 条，按照合规架构与风险识别处理的逻辑划分为六章，从数据合规管理体系、数据风险识别、数据风险评估与处置、数据合规运行与保障等方面引导企业加强数据合规管理。（来源：上海市杨浦区人民检察院）

- **《 企业数据合规指引》**
- **全文：**http://www.shyangpu.jcy.gov.cn/ypjc/jcdt/79471.jhtml

五、本期重要漏洞实例

➢ Microsoft 发布 2022 年 2 月安全更新

发布日期：2022-2-8

更新日期：2022-2-8

描述：2022 年 2 月 8 日，微软发布了 2022 年 2 月份的月度例行安全公告，修复了多款产品存在的 49 个安全漏洞。受影响的产品包括：Windows 11（22 个）、Windows Server 2022（21 个）、Windows 10 21H2（21 个）、Windows 10 21H1（21 个）、Windows 10 20H2 & Windows Server v20H2（21 个）、Windows 8.1 & Server 2012 R2（13 个）、Windows Server 2012（13 个）、Windows RT 8.1（13 个）和 Microsoft Office-related software（8 个）。利用上述漏洞，攻击者可以绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题	最高严重等级和漏洞影响	受影响的软件
CVE-2022-21984	Windows DNS Server 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Windows 10
CVE-2022-21989	Windows Kernel 权限提升漏洞	重要 特权提升	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-22005	Microsoft SharePoint Server 远程代码执行漏洞	重要 远程代码执行	SharePoint Server 2019 SharePoint Server Subscription Edition SharePoint Enterprise Server 2016 SharePoint Enterprise Server 2013
CVE-2022-22003	Microsoft Office Graphics 远程代码执行漏洞	重要 远程代码执行	Office LTSC 2021 Office 2016 Office 2013 Office LTSC for Mac 2021 Office 2019 Office 2019 for Mac 365 Apps Enterprise

来源：https://msrc.microsoft.com/update-guide/releaseNote/2022-Feb

➢ Oracle MySQL Cluster 输入验证错误漏洞

发布日期：2022-01-18
更新日期：2022-02-24
受影响系统：
Oracle Oracle MySQL Cluster <= 8.0.27
Oracle Oracle MySQL Cluster <= 7.6.20
Oracle Oracle MySQL Cluster <= 7.5.24
Oracle Oracle MySQL Cluster <= 7.4.34
描述：

CVE(CAN) ID: CVE-2022-21280
Oracle MySQL Server 是美国甲骨文（Oracle）公司的一款关系型数据库。
Oracle MySQL 的 MySQL Cluster (组件: Cluster: General) 7.4.34 及之前版本、7.5.24 及之前版本、7.6.20 及之前版本以及 8.0.27 及之前版本存在输入验证错误漏洞。攻击者可利用该漏洞破坏 MySQL Cluster，并导致 MySQL Cluster 被接管。
链接：https://www.oracle.com/security-alerts/cpujan2022.html
建议：

厂商补丁：
Oracle

Oracle 已经为此发布了一个安全公告（cpujan2022）以及相应补丁:
cpujan2022：Oracle Critical Patch Update Advisory - January 2022
链接：https://www.oracle.com/security-alerts/cpujan2022.html

➢ Cisco NX-OS Software 命令注入漏洞

发布日期：2022-02-23
更新日期：2022-02-24
受影响系统：
Cisco Cisco NX-OS Software
描述：

CVE(CAN) ID: CVE-2022-20650
Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。
Cisco NX-OS Software 的 NX-API 特性存在命令注入漏洞，该漏洞源于程序未对输入数据进行正确验证。经过身份认证的远程攻击者可利用该漏洞在底层操作系统上使用根权限执行任意命令。
链接：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-nxapi-cmdinject-

建议：

厂商补丁：
Cisco

Cisco 已经为此发布了一个安全公告（cisco-sa-nxos-nxapi-cmdinject-ULukNMZ2）以及相应补丁：
cisco-sa-nxos-nxapi-cmdinject-ULukNMZ2：Cisco NX-OS Software NX-API Command Injection Vulnerability
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-nxapi-cmdinject-ULukNMZ2

➢ Adobe Illustrator 越界读取漏洞

发布日期：2022-02-08
更新日期：2022-02-18
受影响系统：
Adobe Adobe Illustrator <= 26.0.2
Adobe Adobe Illustrator <= 25.4.3
描述：

CVE(CAN) ID: CVE-2022-23196
Adobe Illustrator 是美国奥多比（Adobe）公司的一套基于向量的图像制作软件。
Adobe Illustrator 25.4.3 及之前版本和 26.0.2 及之前版本存在越界读取漏洞。攻击者可利用该漏洞导致敏感内存泄露并绕过缓解措施（如 ASLR）。
<*来源：Yonghui Han （Fortinet's FortiGuard Labs ）
链接：https://helpx.adobe.com/security/products/illustrator/apsb22-07.html
建议：

厂商补丁：
Adobe

Adobe 已经为此发布了一个安全公告（APSB22-07）以及相应补丁：
APSB22-07：Security Updates Available for Adobe Illustrator | APSB22-07
链接：https://helpx.adobe.com/security/products/illustrator/apsb22-07.html

六、本期网络安全事件

➢ 沃达丰 5G 网络遭黑客攻击，导致葡萄牙全国断网

2022 年 2 月 8 日，国际电信巨头沃达丰的葡萄牙公司表示，由于遭受了一大波“以损害与破坏为目的的蓄意网络攻击”，其大部分客户数据服务被迫下线。该公司的 4G 与 5G 移动网络、固话语音、电视、短信及语音/数字应答服务目前仍处于离线状态。

沃达丰发布声明称：“我们已经恢复了移动语音服务，目前葡萄牙国内的 3G 移动数据服务也基本恢复可用。但不幸的是，由于此次遭遇犯罪行为的规模和严重性都很高，其他各项服务恢复仍需努力。”

这是沃达丰葡萄牙公司迄今为止处理过的最大规模网络安全事件。沃达丰在葡萄牙拥有超过 400 万手机用户、340 万家庭和企业互联网用户，此次网络攻击造成了大规模的网络中断问题。

该公司表示：他们正在与政府当局合作对事件开展调查。根据目前搜集到的证据，客户数据似乎并未泄露或遭到攻击者访问。尽管网上出现一些传言，但沃达丰葡萄牙公司尚未将事件定性为勒索软件攻击。

网上之所以传言四起，是因为在过去一个月内，有勒索软件团伙攻击了葡萄牙国内最大的两家新闻媒体 Impresa 与 Cofina。相关团伙名为 Lapsus$，目前尚无法确定沃达丰葡萄牙公司遇袭事件与他们有关。一位沃达丰葡萄牙公司员工透露，他们只知道发生了技术中断、但并未听说公司将事件归结为网络攻击的消息。从这个角度来看，这波发生在 2 月 7 号晚间到 8 号的突发袭击还没有在公司内部进行披露或者通报。（来源：安全学习那些事儿）

➢ 程序员“删库跑路”删除零售平台代码，被判刑 10 个月

2022 年 2 月 10 日，上海市杨浦区检察院业务科室证实，被告人录某在从一互联网公司代码研发岗位离职当天，删除相关代码，被以破坏计算机信息系统罪起诉，获刑有期徒刑十个月。据上海市杨浦区检察院介绍，被告人录某 1992 年出生，原系北京一信息技术有限公司员工，2021 年 3 月起，录某入职上海一公司，负责某生鲜配送平台的代码研发工作。同年 6 月 18 日，录某离职。当日，录某未经许可用本人账户登录服务器位于上海市杨浦区某地的代码控制平台，将其在职期间所写某平台优惠券、预算系统以及补贴规则等代码删除，导致原定按期上线项目延后。经审计，为保证系统运行通畅，该公司聘请第三方公司恢复数据库等，共计支出人民币约 3 万元。

法院裁定，录某违反国家规定，对计算机信息系统中存储数据进行删除，后果严重，其行为已构成破坏计算机信息系统罪。公诉机关指控的罪名成立，对录某依法应予处罚。录某到案后能如实供述自己的罪行，赔偿被害单位并取得谅解，依法可以从轻处罚。录某自愿认

罪认罚，依法可以从宽处理。公诉机关量刑建议适当，予以采纳。

根据我国刑法第二百八十六条第一、二款，第六十七条第三款以及我国刑事诉讼法第十五条之规定，法院判决录某犯破坏计算机信息系统罪，判处有期徒刑十个月。

近来程序员删除数据库被公诉非个案：据公开报道，近年来影响较大的一起“删库跑路”案件，系微盟遭内部程序员删库，导致该司市值一度缩水 21.5 亿元。

2020 年 2 月 24 日晚，微盟的 SaaS 业务服务宕机，旗下 300 万商户的线上业务停止，商铺后台所有数据被清零。微盟集团同年 2 月 25 日公告称，数据库遭运维人员贺某人为破坏，公司已报案，通过登录账号及 IP 地址追踪，定位并找到了犯罪嫌疑人，其迅速承认了犯罪事实，被刑事拘留。微盟创始人事后回应称，涉事员工深陷网络贷，删库事件一度导致微盟集团股价缩水 21.5 亿元，涉事程序员最终被判处 6 年有期徒刑。（来源：南方都市报）

➢ 知乎否认使用“行为感知系统”监测员工，称坚决反对违规收集个人信息

2022 年 2 月 14 日，对于部分媒体报道“公司监测员工行为感知系统”，以及有部分消息认为知乎使用了该系统，**知乎相关负责人表示：**我们就此声明，知乎从未安装使用过网上所说的行为感知系统，今后也不会启用类似软件工具。对于网上该系统的截图，我们从未接触过，因此也不清楚其真实性。对于违规收集个人信息安全的行为，本身严重背离知乎价值观，对这类系统我们一向持坚决反对态度。

近日，有网友爆料称，知乎的视频部门正在裁员，几乎裁掉一半员工，之后知乎官方对此进行了辟谣。与上述消息几乎同时曝出的，是知乎安装了行为感知系统，可以通过监控员

工的上网行为获悉其浏览招聘网站、投简历等行为，以此了解员工是否想离职。

据了解，该监控系统页面与 A 股上市公司深信服科技股份有限公司 2017 年开发的一款软件“深信服行为感知系统 BA”产品介绍页面一致上述产品均为按年付费的，费用与网络带宽、终端数量有关。

此前深信服官网罗列出的该监控系统与光大银行深圳分行、新浪以及华东师范大学合作的成功案例，目前已搜索不到，或被删除。此外，在百度搜索、头条搜索中还能搜到“光大银行深圳分行采用深信服上网行为管理方案”等网页标题，但进入网页却没有任何内容，只显示“404”的字样。

深信服客服此前表示：该系统“主要是对员工在单位网络内的网站访问记录进行分析，支持做离职 (倾向) 分析”，并向记者提供了离职倾向分析的相关页面。图片显示，管理者可以限定一段时间，查看该期间内访问招聘网站的用户、访问时长、访问次数。目前，引发争议的相关行为感知系统在深信服官网已经检索不到产品。（来源：互联网综合整理）

➢ 350 余万名学生为“冰墩墩”上网答题比赛，结果居然被骗千万

2022 年 2 月 18 日，记者从江苏南通市公安局获悉，南通、如东两级公安机关破获一起特大假冒冬奥知识传播诈骗案，诱骗全国 350 余万名大中专院校学生参与并非法搜集个人信息。抓获涉案人员 19 名，案值逾千万元。同时还查获该犯罪团伙，非法获取到的 350 余万名大中专院校学生的个人信息数据。

“在公众号‘校园实践’回复：冬奥或微信扫码二维码，一起来报名参与吧！你将获得荣誉证书和冬奥纪念礼品。”2 月 8 日，有热心网友向南通市公安局网安支队举报，一场名为“‘魅力冬奥’冬奥知识传播助力大使活动”的线上答题在本地微信群、朋友圈内传播开来，吸引众多网友报名参加，涉嫌非法搜集公民个人信息和诈骗。

经初查，江苏南通网警发现，这个活动主办单位名为“中国管理科学研究院国际人才技能培训基地”，主要针对大中专院校在校学生开展，活动实行“冬奥值”积分制度，报名后首先在 10 分钟内答 10 道冬奥的常识题，答对 6 道即可加冬奥值 10 分。答题后，还要求填报所在学校、姓名、身份证号、手机号等个人信息。参与过程中，需通过学习签到、邀请报名等方式获取“冬奥值”，达到一定分值可获得一星至五星不同等级的冬奥大使称号，在全国排名靠前的还可获得定制手办“冰墩墩”等限量奖品。

2 月 9 日，南通市公安局网安支队会同如东县公安局成立专案组开展破案攻坚。经进一步侦查，专案组很快查明背后隐藏着一个以李某辉（男，38 岁，内蒙古人）、汤某峰（男，40 岁，江西人）等人为首的，专门针对大中专院校在校学生设计各类在线答题活动，从而非法获取公民个人信息、诈骗钱财的犯罪团伙。2 月 16 日，南通、如东两级公安机关抽调 20 余名精干警力，兵分两路，分别在重庆、北京将 19 名涉案人员全部抓获归案，现场查获作案用手机 38 部、电脑 57 台、U 盘 16 个，以及非法获取的 350 余万条公民个人信息，均为全国各大中院校在校学生为参加答题活动在线自主填报的。

经查，2022 年 1 月，犯罪嫌疑人李某辉伙同汤某峰等人在没有取得冬奥组委会官方授权的情况下，依托互联网开发了一个“竞赛平台”，精心设计了积分规则和活动海报，以多种形式推广，在全国范围内发起“‘魅力冬奥’冬奥知识传播助力大使活动”，以发放虚假“冬奥大使荣誉证书”、冬奥纪念礼品等为奖品，并宣称所颁发的荣誉证书可作为大学生社会实践加分、评奖学金等依据，诱骗各大中专院校在校学生进入“竞赛平台”，填写姓名、手机号码、身份证号码、联系地址等个人信息，并收取 28 元至 36 元不等的证书工本费牟利。截至案发，该犯罪团伙依托这一“竞赛平台”，已非法获取全国大中专院校在校学生的个人信息 350 余万条，骗取部分参与者缴纳证书工本费总计 1000 万余元。

南通市公安局网安支队副支队长张达经透露，在侦查过程中，南通警方还发现该犯罪

团伙此前多次利用非正规行业协会、学会等开展此类线上答题活动。目前，该案正在进一步侦办中。

警方提醒：目前的网络答题和抽奖活动，参与者大都要填写一些基本的个人信息，活动主办方可借机营销、吸粉引流、收集个人信息等。面对各类网络活动，广大网友要擦亮双眼，对活动主办方要仔细甄别，特别是涉及填写身份证号码、手机号码、联系地址等重要的个人信息时，一定要慎重。中奖后，主办方要求领奖前缴纳各类费用的更应提高警惕，谨防上当受骗。（来源：法制日报）

➢ 非法买卖 30 余万条业主房源信息，男子获利 150 余万元判刑并处罚金!

2022 年 2 月 21 日，最高检举行主题为“坚持以人民为中心 加强网络时代人格权刑事保护”的新闻发布会，公布了第三十四批指导性案例，其中披露了“柯某侵犯公民个人信息案”。

以现金激励非法获取大量公民个人信息牟利

1980 年出生的柯某，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。

因侵犯公民个人信息罪男子获刑并处罚金

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检察院提请批准逮捕。11 月 24 日，金山区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。

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，金山区检察院以柯某涉嫌侵犯公民个人信息罪提起公诉。

2019 年 1 月 16 日，上海市金山区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。

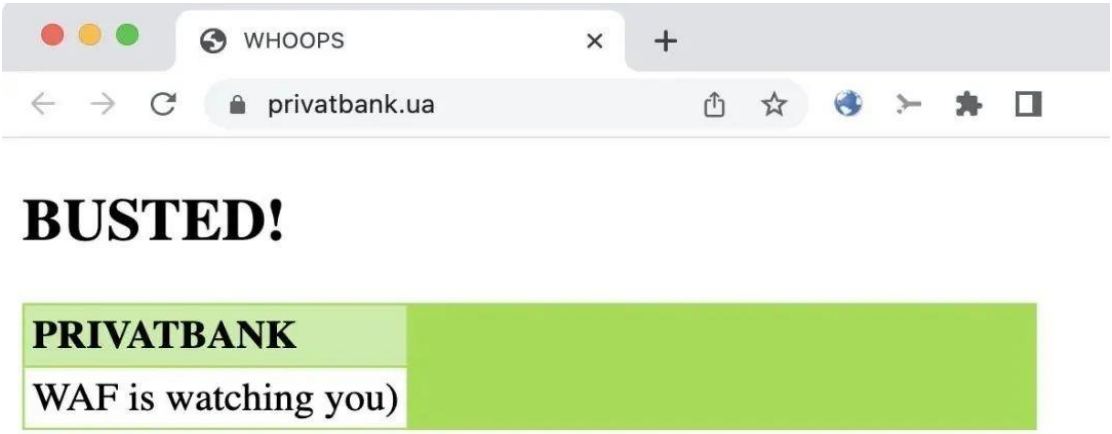
公诉人答辩指出，柯某的行为依法构成犯罪。第一，业主房源信息中的门牌号码、业主电话，组合后足以识别特定自然人，且部分信息有业主姓名，符合刑法对公民个人信息的界

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。

2019 年 12 月 31 日，金山区法院作出判决，采纳金山区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。（来源：检察日报正义网）

➢ 乌克兰政府和银行网站又遭大规模网络攻击被迫关闭

2022 年 2 月 23 日，乌克兰境内多个政府机构（包括外交部、国防部、内政部、安全局及内阁等）以及两家大型银行的网站再次沦为 DDoS 攻击的受害者。专注监测国际互联网状态的民间组织 NetBlocks 还证实，乌克兰最大银行 Privatbank、国家储蓄银行（Oschadbank）的网站也在攻击中遭受重创，目前与政府网站一同陷入瘫痪状态。



乌克兰国家特殊通信与信息保护局（SSCIP）表示：“部分政府与银行机构网站再度遭受大规模 DDoS 攻击，部分受到攻击的信息系统已经宕机，或处于间歇性不可用状态。”目前，该部门与他国家网络安全机构“正在努力应对攻击，收集并分析相关信息。”

上周已遭遇大规模 DDoS 攻击

而就在上周（2 月 15 日），已经出现过一波针对乌克兰政府及银行网站的 DDoS 攻击，并导致国防部、武装部队等网站被迫下线。三天后（2 月 18 日），乌克兰计算机应急响应小组（CERT-UA）在一份报告中表示，在这轮攻击中，攻击者曾动用到多种 DDoS 即服务平台，以及包括 Mirai 与 Meris 在内的多个僵尸网络。

美国政府已经认定这波 DDoS 攻击与俄罗斯武装部队总参谋部情报总局（GRU/格鲁乌）有关。美国国家安全副顾问 Anne Neuberger 表示，“我们已经掌握了俄情报总局与此次事件有关的技术信息，发现已知的 GRU 基础设施曾向乌克兰方面的 IP 地址和域名传输大量通信内容。”Neuberger 补充道，尽管这些攻击“影响有限”，但这也许是在“为更具破坏性的后续攻势奠定基础”。届时，可能还将有针对乌克兰领土的入侵行动与线上攻击协同推进。

英国政府也指责俄罗斯格鲁乌黑客在上周针对乌克兰军方和国有银行网站的在线服务发动了 DDoS 攻击。就在第一波 DooS 攻击的前一天，乌克兰安全局（SSU）发布新闻稿，称该国正成为“大规模混合战”的打击目标。发出不久，安全局网站也在此次攻击中受到影响。乌克兰安全局在 2 月初还曾经提到，他们已经在 2022 年 1 月期间阻止过 120 多次指向乌克兰国家机构的网络攻击。（来源：互联网综合整理）