国盟信息安全通报

2021 年 03 月 28 日第 236 期

全国售后服务中心

国盟信息安全通报

（第 236 期）

国际信息安全学习联盟

2021 年 3 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 679 个，其中高危漏洞 120 个、中危漏洞 299 个、低危漏洞 260 个。漏洞平均分值为 4.98。本周收录的漏洞中，涉及 0day 漏洞 427 个（占 63%），其中互联网上出现“CSZ CMS 跨站脚本漏洞（CNVD-2021-19691）、jsPDF 跨站脚本漏洞”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 4981 个，与上周（4752 个）环比增加 5%。

主要内容

一、概述 4
二、安全漏洞增长数量及种类分布情况 4
➢漏洞产生原因（2021 年 3 月 14 日—2021 年 3 月 28）.....4
➢漏洞引发的威胁（2021 年 3 月 14 日—2021 年 3 月 28）.....5
➢漏洞影响对象类型（2021 年 3 月 14 日—2021 年 3 月 28）.....5
三、安全产业动态 6
➢央视 3.15：你的脸、你的简历就这样被“偷了”.....6
➢从网络空间国际准则看国际关键信息基础设施保护及启示建议.....11
➢规范技术应用 保障信息安全.....16
➢商业银行数字化转型的数据治理问题.....17
四、政府之声 24
➢国家市场监督管理总局出台《网络交易监督管理办法》.....24
➢四部门联合发布《常见类型移动互联网应用程序必要个人信息范围规定》.....25
➢教育部发布关于加强新时代教育管理信息化工作的通知.....26
➢银保监会发布关于防范短信钓鱼诈骗的风险提示.....27
五、本期重要漏洞实例 29
➢Microsoft 发布 2021 年 3 月安全更新.....29
➢Cisco Aironet Access Points 文件覆盖漏洞.....30
➢Mozilla Firefox 越界读取漏洞.....31
➢Wordpress Contact Form Submissions SQL 注入漏洞.....31
六、本期网络安全事件 32
➢宏碁遭勒索软件攻击 要求支付高达 5000 万美元的赎金.....32
➢贩卖 50 多万条个人信息 警方抓获嫌疑人 16 名.....33
➢非法获取员工及用户敏感信息，法国宜家或将被罚 375 万欧元.....35
➢中信银行被罚 450 万元！曾泄露明星个人流水.....36
➢约 650 万以色列选民的详细信息在网上泄露.....37
➢江西首例区块链比特币特大盗窃案告破 6 名黑客被抓.....39

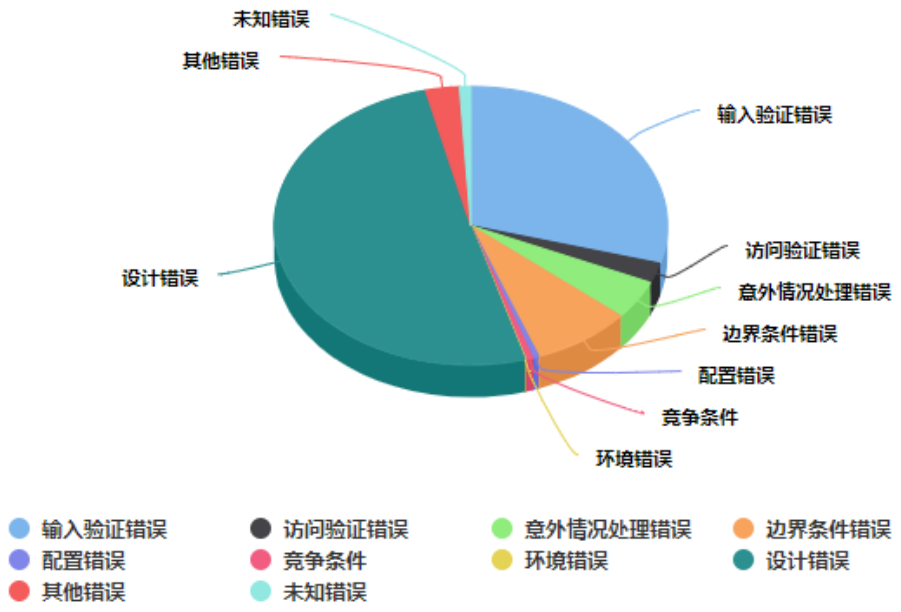
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

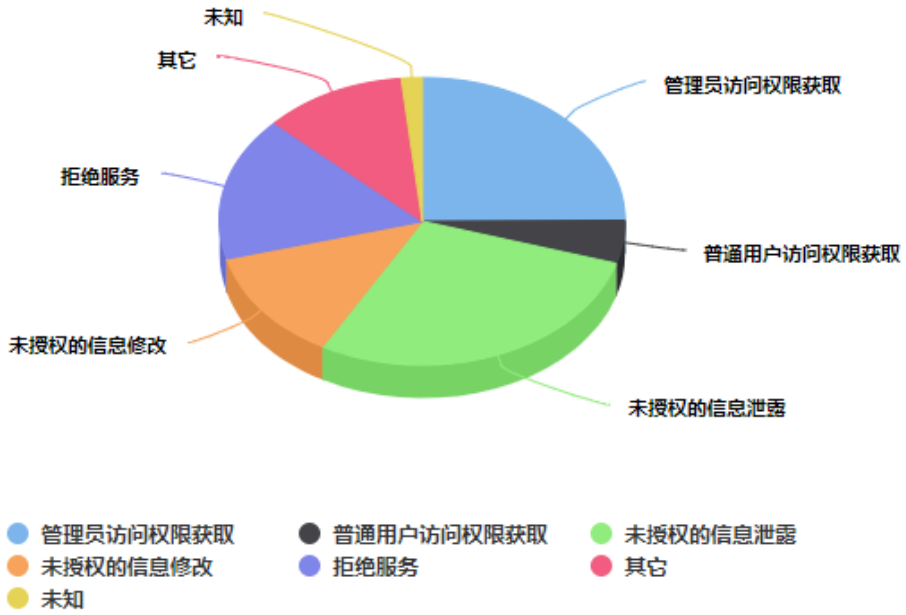
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 679 个，其中高危漏洞 120 个、中危漏洞 299 个、低危漏洞 260 个。漏洞平均分值为 4.98。本周收录的漏洞中，涉及 0day 漏洞 427 个（占 63%），其中互联网上出现“CSZ CMS 跨站脚本漏洞（CNVD-2021-19691）、jsPDF 跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4981 个，与上周（4752 个）环比增加 5%。

二、安全漏洞增长数量及种类分布情况

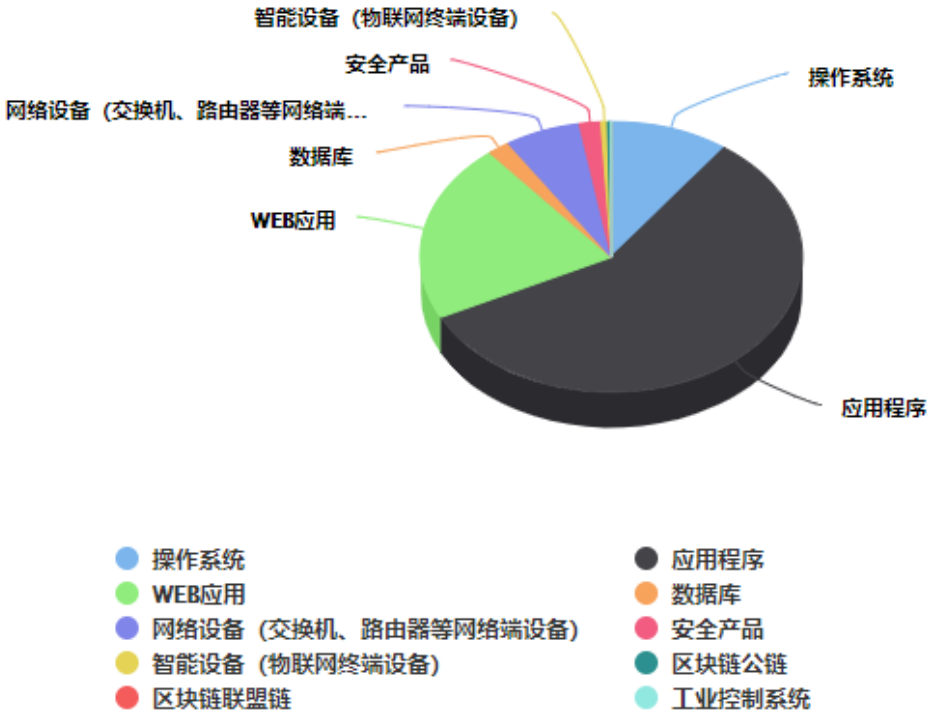
➢ 漏洞产生原因（2021 年 3 月 14 日—2021 年 3 月 28）



➢ 漏洞引发的威胁（2021 年 3 月 14 日—2021 年 3 月 28）



➢ 漏洞影响对象类型（2021 年 3 月 14 日—2021 年 3 月 28）



三、安全产业动态

➢ 央视 3.15：你的脸、你的简历就这样被“偷了”

2021 年 3 月 15 日，在央视 3.15 晚会的第三十个年头，互联网行业成为了上半场晚会的重灾区，前四个被曝光的案例，全部与互联网有关。央视 3.15 晚会重点把目光对准了互联网隐私黑产，其中包括摄像头抓取人脸信息，个人简历信息流入网络黑市，手机垃圾清理软件频繁读取手机信息，并向老年人强行推荐广告等。

一、监控摄像头暗藏玄机，人脸信息被企业利用

被曝光企业：科勒、万店掌、宝马 4S 店、悠络客、雅量科技、瑞为等

监控摄像头在生活中几乎无所不在，这些摄像头大多以保障公共安全为目的，但有些商家安装的摄像头暗藏玄机。据央视 3.15 晚会报道，科勒线下店的一位工作人员表示，他们的摄像头与众不同，具有人脸数据功能，而且不少门店都装有这个摄像头。一旦顾客进入科勒卫浴，人脸就会被捕捉记录，以后再去哪家店、去了几次，科勒卫浴都知道。对于科勒来说，就知道如何接待这个顾客，如何针对这个顾客去做报价，就都有心理准备了。央视 3.15 晚会报道称，记者走访了三家上海科勒卫浴门店，均看到了这种摄像头。但在记者进店一直到离开，都没有得到明确提示和告知，征得同意更是无从谈起。捕捉记录显示，不到两分钟，记者被摄像头的人脸识别功能抓拍了三次，角度不同，但是人脸编号是相同的。不仅如此，

去过的不同门店，人脸信息均被抓取，而且人脸信息编号是相同的，可见这个信息是被科勒卫浴掌握到的。

提供人脸识别服务的企业（如万店掌、悠络客、雅量科技、瑞为）的工作人员表示，只要进店，就能够获取顾客信息，它在不知情的情况下被动抓取，每一个后面会生成一个 ID。此外，摄像头不仅捕捉了人脸信息，还能分析出顾客的性别、年龄，甚至此时此刻的心情。据工作人员介绍，此外商家还可通过类似系统，手动为被抓拍的顾客添加各种信息，甚至还可以把某些特殊人员加入黑名单。

尽管法律明确规定：未经允许不得随意获取人脸识别信息。但央视 3.15 晚会显示，在我们周围偷偷获取我们隐私、财产安全的人脸识别摄像头数量惊人，甚至这些最核心的生物识别信息，已经被和我们毫无关系的第三方公司掌握。截至 21 点 30 分，科勒卫浴一名客服人员回应称，感谢关心，已知晓被央视 315 晚会曝光的情况，将会尽快反馈给相关部门。

央视总结：人脸识别这样的科技手段，本来应该是服务于美好生活的。但是在不法企业的手中，成为了盗取个人信息的工具。每个人的人脸特征、行动轨迹都是敏感的数据信息，企业可以运用大数据寻找商机，但不能在消费者没有知情权的场景下任意搜集、肆意滥用。

二、个人简历信息泄露，交钱就可以买到各种简历

被曝光企业：智联招聘、前程无忧、猎聘网等

央视 3.15 晚会报道称，在各类贴吧、论坛，出售招聘平台简历的信息比比皆是。有卖家表示，只需要支付 7 元就可以买到一份智联招聘最新的简历。卖家甚至可以根据用户的要求，对简历按照地域、毕业院校等信息进行精准筛选。央视 3.15 晚会揭秘称，招聘企业通

过上传营业执照和法人信息注册企业账号，就可以在智联招聘发布职位，查看求职者简历。点击简历，看到了求职者学历、工作经历等信息，但是关键信息却处于隐藏状态。点击下载简历，弹出了支付页面，原来需要支付 60 元才可以购买完整简历。支付后，无需征得同意就可以更新，所有关键信息全部显示出来。

从央视 3.15 晚会的报道可以看出，只要交钱办理会员，就可以不受数量限制，下载包含姓名、电话、邮件的信息。但是对于下载后的简历信息，却缺乏管理和监测，任其流入网络黑市。除了智联招聘，前程无忧、猎聘网也被央视 3.15 晚会点名。按照这样的操作逻辑，一个通过伪造资质申请下来的企业账户，只要支付费用，就可以随意下载信息详尽的个人简历。通过这样的途径，大量的个人简历信息源源不断地流入了不法分子的黑手。

截至 21 点 30 分，在央视 3.15 晚会曝光后，前程无忧在美股股价跌幅一度超过 4%。此外，据三言财经报道，OPPO、vivo 的应用商店中，已经将智联招聘、前程无忧等 App 下架。

央视总结：个人简历遭到了泄漏、买卖，以至于精准诈骗，这是形成了黑色产业链。这些网络求职平台在其中扮演了关键角色，给求职者和招聘企业带来了很大便利。但是作为专门的个人信息收集方，求职平台应该真正履行自己的责任和义务，严格保护着求职者的信息安全，不能仅仅把视用户信息安全与隐私的保护为自己生命线当作一句口号。

三、老年人手机垃圾清理软件骗局，手机越清理越慢

被曝光企业：内存优化大师、超强清理大师、智能清理大师、手机管家 PRO 等

央视 3.15 晚会报道称，老年人的手机里经常会自动蹦出一些安全提示，比如病毒、垃圾、内存严重不足等，老年人就赶快清理，但是用 A 软件清理完，B 软件又在提示需要清理。

与此同时，手机里开始频繁出现一些诱人的广告，比如红包领钱、金币赚钱、走路赚钱。

测试人员的测试结果显示，这类软件的功能非常简单初级，甚至没有清理效果的。除此之外，这类软件表面看起来是清理手机的逻辑，但背后不断获取手机的大量信息，几秒钟的时间，读取设备上的安装程序列表达 800 多次，读取地理位置定位达到 50 多次，读取手机号用户识别码 IMSI 行为 1300 多次，读取手机设备身份识别码 IMEI 号 900 多次。

据专家介绍，这类 APP 会收集很多信息，会频繁高频率上传，导致手机会更卡，用户再去下载清理，会形成恶性循环。测试人员进一步分析发现，这类 APP 十分活跃，他们通过在 APP 里发布广告诱导老人进行下载。这类 APP 驻扎在老人手机里，不断在后台发布用户数据信息，对老人们进行用户画像，打上了容易被误导的标签。于是各种低俗、劣质和欺骗套路的广告内容会源源不断推送到老人手机上。截至 21 点 30 分，在央视 3.15 晚会曝光后，“手机管家 PRO”已在苹果、OPPO 等手机应用商店下架。

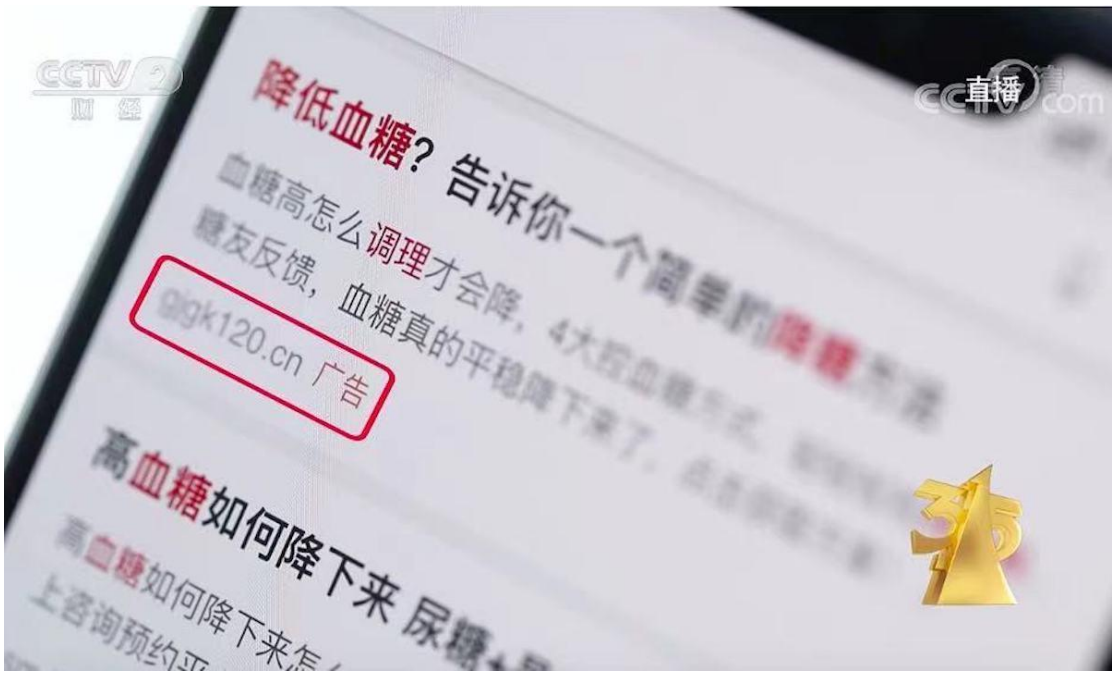
央视总结：这是一个老人很容易上当的连环套，这些手机 APP 打着安全提示的旗号，用夸大的危险去蒙骗老人不断下载安装。玩弄这样的花样，为的就是赚取点击量，获得广告流量，最后从广告商获得更多的广告分成。这是一种典型的商业落实，利用的就是老年人对智能手机不熟悉，对于网络知识相对缺乏的弱点。

四、互联网医疗广告乱象

被曝光企业：UC 浏览器、360 搜索及其代理公司等

央视 3.15 晚会报道称，在 UC 浏览器搜索减肥、降血糖等关键词，在最下方被标注着广告字样。点开这样的广告后，有一篇标题为《9 年的高血糖终于恢复正常了》的文章。网友自称 9 年里被高血糖折磨的生不如死，自从认识 XX 老师，按照老师给的方子服务用，胰岛素都停用了。多次推荐老师，并且醒目标红了联系方式。和所谓的老师联系上后，老师简单

询问病情后，就推荐了白背三七诺丽果粉，但其实这只是一款普通食品。不仅是 UC 浏览器，在 360 搜索也有不少类似的广告。根据《食品安全法》，食品广告的内容应当真实合法，不得含有虚假内容，不得涉及疾病预防、治疗功能。但在搜索过程中，以自述式文章屡见不鲜，患者都是被肥胖或各种疾病困扰多年，经老师治疗下解决困扰。



据 360 上海广告总代理经格网络科技有限公司的销售经理介绍，由于监管严格，这类宣传治疗效果的食品是不能进行直接投放的，是需要转换技巧的。在网站里不能有任何品牌，只有一个落地页，它就加微信、吸粉。加好微信之后，就会把微信推给人去聊，聊完之后去卖产品。据多家代理公司表示，如果公司没有资质，他们还会提供，页面也是帮着弄的，而且代理公司有大量的账号，随时应对被查封的风险。央视 3.15 晚会披露，只要提供了联系方式和产品类型，代理商很快就制作出了广告。专家子虚乌有，疗效神乎其神，连点赞数量也可以任意设定。

此外，在搜索引擎上，公立医院全称有相应保护机制，但是医院的简称可以作为关键词被其他医院用于投放广告：在成都通过 360 搜索，搜索成都市第二人民医院的简市市二医院，结果都是其他医院的广告；在太原通过 UC 浏览器搜索山西医科大学第一医院的简称山大一院，前三位也是其他医院的广告。除了利用简称，代理公司可为费尽心思，在公立医院中间打空格也可以搜其他医院。

央视总结：为了利益，互联网代理公司为虚假广告的发布推波助澜，相关搜索引擎也忽略了自己的监管责任。大数据、互联网+、人工智能这些新科技和新业态都代表着未来，但是并不代表着因此就可以坑蒙拐骗，或者打着新业态的旗号去侵害消费者的权益。（来源：互

联网综合整理）

➢ 从网络空间国际准则看国际关键信息基础设施保护及启示建议

为了应对关键信息基础设施面临的网络威胁，世界各大国和组织都相继制定了关于关键信息基础设施保护的一些法律和规范。《信息安全国际行为准则》和《塔林手册 2.0》是其中比较有代表性的规范。中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦提交的《信息安全国际行为准则》是目前国际上就信息和网络安全国际规则提出的首份较全面、系统的文件。北约卓越网络合作防卫中心发布的《塔林手册 2.0：适用于网络行动的国际法》是西方国家在网络空间国际规则理论研究的最新成果。它既是对《塔林手册 1.0：适用于网络战争的国际法》的延续和发展，也体现了各国网络空间博弈法治化和规则化的态势。对比二者的异同，有利于更好地保障各国国家利益，也有利于推动世界网络空间安全立法发展。

一、起草过程比较

1.《信息安全国际行为准则》

为推动国际社会建立一个和平、安全、公平、开放的信息和网络空间，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦常驻联合国代表于 2011 年 9 月 12 日联名致函联合国秘书长潘基文，请求将由上述国家共同起草的《信息安全国际行为准则》作为信息安全国际行为准则，该准则以第 66 届联大文件（A/66/359）分发，并呼吁各国在联合国框架内就此展开进一步讨论，以尽早就规范各国在信息和网络空间行为的国际准则和规则达成共识。

2015 年 1 月，中国、俄罗斯、塔吉克斯坦、乌兹别克斯坦、哈萨克斯坦、吉尔吉斯斯坦又创新性地对该准则进行了修改，再一次向联合国大会共同提交，其中的规则更为细化，更符合现代国际社会的利益。明确提出各国应遵守以《联合国宪章》为基础的国际法，致力于维护网络空间的和平与合作。

2.《塔林手册 2.0》

2009 年，北约合作网络防御卓越中心组织了 20 名来自不同国家的专家，开始编纂《塔林手册 1.0》并于 2013 年出版。2017 年 2 月，《塔林手册 2.0》出版。在《塔林手册 1.0》起草过程中，国际专家组的所有成员都承担了研究、准备拟议的规则和所附评注草案的任务。他们的初稿被分发给由小组协调员牵头的专家小组，并由专家小组完善初稿后供国际专家组全体会议审议。在《塔林手册 1.0》的起草过程中，各国都没有介入国际专家组的工作。然而，在《塔林手册 2.0》起草过程中，荷兰外交部举行了被称为“海牙进程”的活动，召集各国按照“查塔姆规则”对起草中手册草案做出非正式的评论。来自 50 多个国家和国际组织的代表团出席了在海牙举行的三次为期两天的会议。“海牙进程”在手册起草过程中的作用被证明是非常宝贵的，因为国际专家组一致认为，国际法是由国家制定并作出权威解释的。

二、内容结构比较

《信息安全国际行为准则》包含两部分。第一部分为目标与适用范围，第二部分为行为准则。初版行为准则有 11 条，修订版增加到了 13 条。主要增加的两条为：第七条，认识到人们在线时也必须享有离线时享有的相同权利和义务。第十条，各国应制订务实的建立信任措施，以帮助提高可预测性和减少误解，从而减少发生冲突的风险。《信息安全国际行为准则》内容结构如表 1 所示：

表 1 《信息安全国际行为准则》内容结构

《信息安全国际行为准则》	一、目标与适用范围		本行为准则旨在明确各国在信息空间的权利与责任，推动各国在信息空间采取建设性和负责任的行为，促进各国合作应对信息空间的共同威胁与挑战，以便构建一个和平、安全、开放、合作的信息空间，确保信息通信技术和信息通信网络的使用促进社会和经济全面发展及人民福祉的目的，并与维护国际和平与安全的目标相一致。本行为准则对所有国家开放，各国自愿遵守。
	二、行为准则	1	遵守《联合国宪章》和公认的国际关系基本原则与准则，包括尊重各国主权，领土完整和政治独立，尊重人权和基本自由，尊重各国历史、文化、社会制度的多样性等。
		2	不利用信息通信技术和信息通信网络实施有悖于维护国际和平与安全目标的活动。
		3	不利用信息通信技术和信息通信网络干涉他国内政，破坏他国政治、经济和社会稳定。
		4	合作打击利用信息通信技术和信息通信网络从事犯罪和恐怖活动，或传播宣扬恐怖主义、分裂主义、极端主义以及煽动民族、种族和宗教敌意的行为。
		5	努力确保信息技术产品和服务供应链的安全。
		6	重申各国有责任和权利依法保护本国信息空间及关键信息基础设施免受威胁、干扰和攻击破坏。
		7	认识到人们在线时也必须享有离线时享有的相同权利和义务。
		8	在国际互联网治理和确保互联网的安全性、连贯性和稳定性以及未来互联网的发展方面，各国政府应平等发挥作用并履行职责，以推动建立多边、透明和民主的互联网国际管理机制。
		9	各国政府应与各利益攸关方充分合作，并引导社会各方面理解他们在信息安全方面的作用和责任，包括私营部门和民间社会，促进创建信息安全文化及保护关键信息基础设施。
		10	各国应制订务实的建立信任措施，以帮助提高可预测性和减少误解，从而减少发生冲突的风险。
		11	为发展中国家提升信息安全能力建设水平提供资金和技术援助，以弥合数字鸿沟，全面落实“千年发展目标”。
		12	加强双边、区域和国际合作。推动联合国在促进制定信息安全国际法律规范、和平解决相关争端、促进各国合作等方面发挥重要作用。加强相关国际组织之间的协调。
		13	在涉及上述行为准则的活动时产生的任何争端，都以和平方式解决，不得使用武力或以武力相威胁。

《塔林手册 1.0》主要包括两部分：国际网络安全法和网络武装冲突法，共 7 章，95 条规则。《塔林手册 2.0》包括四部分：一般国际法与网络空间、特别领域的国际法和网络空间、国际和平安全与网络活动和网络武装冲突法，共 20 章，154 条规则。《塔林手册 2.0》内容结构如表 2 所示：

表 2 《塔林手册 2.0》内容结构

《塔林手册 2.0》	第一部分 一般国际法与网络空间	第一章 主权 第二章 审慎 第三章 管辖权 第四章 国际责任法 第五章 本身不受国际法约束的网络行动
	第二部分 特别领域的国际法和网络空间	第六章 国际人权法 第七章 外交和领事法 第八章 海洋法 第九章 航空法 第十章 外层空间法 第十一章 国际电信法
	第三部分 国际和平安全与网络活动	第十二章 和平解决争端 第十三章 禁止干涉 第十四章 使用武力 第十五章 集体安全
	第四部分 网络武装冲突法	第十六章 武装冲突法的一般规定 第十七章 敌对行动的开展 第十八章 特定人员、物体和活动 第十九章 占领 第二十章 中立

《塔林手册 2.0》比《信息安全国际行为准则》表述更加具体，内容更系统，涉及的范围更广泛。相比之下，《信息安全国际行为准则》则是针对不利用信息网络干涉他国内政、合作打击国际网络犯罪和恐怖活动、确保信息技术产品和服务供应链安全、保护本国关键信息基础设施免受攻击等方面提出了明确要求，并且要求以和平方式解决网络空间争端。而《塔林手册 2.0》则允许通过常规打击来反击造成人员伤亡和重大财产损失的网络攻击行为。近年来，中国的中兴、华为等企业在核心信息产品供应链安全方面就多次受到国外的制约与限制。

三、适用情况比较

《信息安全国际行为准则》是目前国际上就信息和网络安全国际规则提出的首份较全面、系统的文件。此准则作为联合国大会第六十六届会议大会文件（A/66/359）分发，国际社会予以高度重视，反响热烈。该准则对所有国家开放，各国自愿遵守。该草案目前尚处于建议阶段，但由于强调自愿，即便将来在联合国大会中获表决通过，也不具有法律约束力。

《塔林手册》是目前国际上对网络攻击问题规制最完整、最系统、最与时俱进的著作。它不仅促进了国际法学界对国际网络攻击的理论学习，与此同时也应当指导国际社会在法律

实务中对国际网络攻击问题的处理。北约高级协同网络安全中心的 11 个成员国已经将《塔林手册》作为北约国家的基本网络攻击法律咨询手册，其他国家或组织也逐渐开始认同《塔林手册》的法律地位。

总的来说，《信息安全国际行为准则》主要用于中国、俄罗斯等相关 6 国之间，但是随着中国在世界的影响力越来越大，使用该准则的国家也会越来越多。《塔林手册 2.0》更加成熟、主要用于美国等北约成员国之间，目前不少非北约的国家也开始认同其地位，使用的国家也越来越多。

四、关键信息基础设施保护内容比较

《塔林手册 2.0》第二部分特别领域的国际法和网络空间中，规则 39 网络基础设施所在馆舍不得侵犯，规则 40 保护网络基础设施的义务，规则 61 建立、维护和保护电信基础设施的义务；第四部分网络武装冲突法，规则 140 攻击堤坝和核电站时的注意义务，规则 150 中立国网络基础设施的保护。

新版《信息安全国际行为准则》第 9 条各国政府与各利益攸关方充分合作，并引导社会各方面理解他们在信息安全方面的作用和责任，包括私营部门和民间社会，促进创建信息安全文化及保护关键信息基础设施。《塔林手册 2.0》与新版《信息安全国际行为准则》两者都在内容上明确了关键信息基础设施的重要性以及要进行重点的保护。

2017 年 3 月，我国外交部和国家互联网信息办公室共同发布的《网络空间国际合作战略》在关键信息基础设施保护方面也做出了明确的规定，其中第四章第八条“加强全球信息基础设施建设和保护”提到“共同推动全球信息基础设施建设，铺就信息畅通之路”。该战略将与周边国家信息基础设施建设和“一带一路”建设相结合，推动各国就关键信息基础设施保护达成共识，制定相关的合作措施以及加强相关技术和经验交流。该战略首次提出网络空间国际合作的中国主张，为破解网络空间国际治理难题贡献中国方案。此外，本战略还将提升保护关键信息基础设施意识纳入其中。

2017 年 7 月 12 日，国家互联网信息办公室发布了《关键信息基础设施安全保护条例（征求意见稿）》，该部条例属于网络安全法的重要配套保护条例和下位法，规定了国家重要行业领域的网络安全保护要求。

2014 年由美国国家标准技术研究院(NIST)发布的《提升美国关键基础设施网络安全的框架规范》提出，美国的关键基础设施信息安全防护体系框架分为识别、保护、侦测、响应和恢复五个层面，是一种基于信息安全保护生命周期和风险防控流程体系，主要标准依据了国际风险评估系列标准 ISO/IEA27001 和美国联邦政府信息和组织的安全控制措施 NISTSP800-

53。

2020 年 9 月 8 日，澳大利亚战略政策研究所与英国外交、联邦和发展事务部以及澳大利亚外交贸易部合作，整理并提供联合国网络规范资源集合。联合国的 11 项负责任国家行为规范于 2015 年获得通过，列出了国家应采取的 8 项积极步骤和 3 项应避免的行动。上述规范是指导国家在网络空间实施网络活动的不具有约束力的行为规范集合，本质上属于“国际软法”。其中第 6 项规范明确指出“不应从事破坏其他国家关键基础设施的网络行为”。

五、启示和建议

1.联合国际上各国家和组织的力量，尤其是发展中国家，研究有利于发展中国家的网络空间规则，推动我国网络主权理论和网络空间规则获得更多的认可。发展中国家与我国在网络主权方面的目标与利益较为一致，容易达成共识，是我国主要联合的力量。通过联合各国家和组织，制定有利于国家的网络空间规则。

2.借鉴《塔林手册 2.0》编纂经验，学习其从学术观点到官方文件再到国际法律转变的实践经验。鼓励国内的相关专家积极参与国际交流，寻找国际共识，然后邀请国内外的专家学者以中立的视野，学术交流的形式,共同商讨适于网络主权的国际法规则。要先通过学术研究成果的形式，把现实中已经形成的体现网络主权平等的规则归纳出来，把应有的网络空间规则建立起来，争取达成国际共识，并最终获得国际承认。

3.借鉴《信息安全国际行为准则》中各国政府与各利益攸关方充分合作，引导社会各方面理解他们在信息安全方面的作用和责任，包括私营部门和民间社会，促进创建信息安全文化及保护关键信息基础设施。让政府主动引导社会积极因素参与网络安全相关工作。

4.积极参与网络空间国际学术会议，积极宣传我国的规则经验，提高网络空间规则制定的国际话语权。《塔林手册 2.0》的制定过程，已经有我国的一位学术代表获邀参与，这是一个很好的先例。未来我国如有更多学者参与，提出我们的主张和意见，宣传不同于西方意识形态的主张，将更有利于规避国际共识中不利于我国观点的形成。

5.在数据跨境传输保护方面，既要维护国家数据主权，又要逐步促进商贸普通数据的合法跨境流动；既要考虑数据输出国的因素，也要考虑数据输入国的因素，以及数据相关主体自身的因素。（来源:《中国信息安全》杂志 2021 年第 1 期）

➢ 规范技术应用 保障信息安全

随着互联网信息技术的发展，人脸识别技术应用场景日益广泛，大部分情况下比肉眼识别更准确，速度更快，能极大地节省成本。在社会治理、治安防控、疫情防控等领域，其精准性和高效性，既大大节约社会治理成本、提高治理效能，也对违法犯罪行为形成有效震慑；在商品交易和服务领域，其便利性和及时性也为消费者带来了良好的生活体验，节约了交易成本。

但是，随着“刷脸”成为人们进门、购物、游乐、签约、取款等日常生活的“不二”选择，网络上出现多款可以任意下载的 AI“换脸”软件，“换脸”导致案件频发……人脸识别技术及其应用可能引发的个人信息仿造、危害经济社会安全乃至国家安全等风险凸显，社会忧虑日渐加深，因此，一些人选择抵制使用。特别是浙江省杭州市富阳区人民法院“人脸识别第一案”宣判后，社会上更是出现了禁止人脸识别技术应用的声音。这种从一个极端走向另一个极端的状况，暴露了人脸识别技术应用、个人信息保护所面临的窘境。

从法律上看，处理好这个问题的核心在于妥当处理科技进步与个人隐私保护、技术运用与风险防范之间的关系。在鼓励发展大数据、人工智能技术及其应用的同时，对于“人脸”这种具有生物特征唯一性、不可再生性的重要信息，本着生物识别技术作为“最后手段”的原则，在数据采集、存储和应用方面做出更为严格的规范。

一是明确所有使用人脸识别技术主体的安全与责任底线，确立安全使用原则。所有人脸识别系统须经第三方独立机构定期检测其准确性与非歧视性，必要时向监管部门备案；所有通过公共网络收集、传输、存储的人脸信息都应采取加密措施，并对信息进行分片段单独存储；建立可追踪技术体系，保障对所有查询、使用、修改、下载人脸信息的行为可查证和可

追责。所有因被收集人脸信息而遭遇盗窃、泄露或者非法使用或出售等造成的损失，收集者应对受害人实际损失承担连带赔偿责任；实际损失难以证明的，应对每个受害者赔偿法定的定额赔偿金。任何人都有拒绝“刷脸”的权利，应在无竞争性服务领域（如民航、铁路、学校、社区等）设置替代性验证机制。

二是明确政府部门与非政府部门的不同规范重点。对政府部门以事前事中规制为主：设立审查批准机构，明确公开、透明、民主参与等审查原则与审查程序，对安装、使用人脸识别技术的必要性、正当性进行严格审查后批准使用。未经批准，政府任何部门不得安装、使用人脸识别技术；对非政府部门以事中事后规制为主：尽早制定个人信息保护法及其配套规章，明确执法部门及执法权限；降低受害人的举证负担，便利受害人维权。

三是采取严格的人脸信息采集知情同意措施。除了法定的例外情况，人脸信息采集者须书面告知被采集者信息类型、应用场景、保存时间及有关风险和权利。（作者：光明日报）

➢ 商业银行数字化转型的数据治理问题

近年来，数字经济的蓬勃发展推动了商业银行的数字化转型。突如其来的新冠疫情，给商业银行带来不同程度的影响，也成为商业银行数字化转型的助推器和催化剂。随着数字化转型步伐的加快，对数据治理提出了更高要求，商业银行数据质量、数据标准和数据安全问题面临的困境变得尤为突出。商业银行应当采取措施妥善应对，切实做好数据治理工作，提高数据治理水平，完善数据治理架构，提高数据质量，建立健全数据标准体系，切实保障数据安全，在业务经营、风险防控、内部管理与监管合规等方面充分发挥数据的作用，利用数据治理，实现数据驱动决策，为高质量发展夯实数据基础。商业银行应以数据治理为契机，加快推进数字化转型，全面提高数字化水平，实现由传统银行向更加数据化、自动化和智能化的数字化银行转变。

一、数据治理概述

根据银保监会 2018 年 5 月发布的《银行业金融机构数据治理指引》（以下简称《指引》），商业银行的数据治理是指通过建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求，制定和实施系统化的制度、流程和方法，确保数据管理高效运行，并在经营管理中充分发挥价值的动态过程。

目前，数据治理的相关定义并不一致。张绍华等从体系框架的角度，将大数据治理定义

为是对组织的大数据管理和利用进行评估、指导和监督的体系框架。郑大庆等从概念体系角度，认为数据治理需要从目标、权力层次、治理对象及解决的实际问题四个方面来解析数据治理概念。索罗斯从广义信息治理计划的角度，认为数据治理即制定与大数据相关的数据优化、隐私保护与数据变现的政策。Mohanapriya 等从部署及管理的角度，认为大数据治理是企业数据可获得性、可使用性、完整性、安全性的部署及全面管理。梅宏认为，数据治理是指在确保数据安全的前提下，建立健全规则体系，理顺各方参与者在数据流通的各个环节的权责关系，形成多方参与者良性互动、共建共享共治的数据流通模式。

国内数据治理的研究多集中在特定领域，包括金融领域、计算机科学、政府行政领域以及教育领域等。我国商业银行在数字化转型方面已进行了很多有益探索，部分银行的数字化转型取得良好进展，但总体仍处于发展阶段，商业银行数字化转型和高质量发展对数据治理提出了更高要求。银保监会于 2018 年 5 月发布的《指引》对商业银行的数据治理进行了规定，并将数据治理纳入监管范围。学者们也纷纷对商业银行的数据治理进行了研究。刘海飞等从 IT 层面、商业层面和管理层面分析了商业银行数据治理的目标，并据此阐述了商业银行如何建立健全数据治理体系。张军等人以支付清算数据为例，围绕数据治理的评估、指导、监督活动展开研究，构建了包括数据治理保障体系、数据管理体系、数据安全体系在内的数据治理框架。卞雨茗结合《指引》内容，阐述了商业银行数字化转型下的数据标准管理、元数据管理以及数据安全管理。

二、商业银行数字化转型中数据治理的困境

经过十几年的发展，商业银行的数据治理水平有所提高，但是数据治理涉及范围广、投入成本高、持续周期长、成效显现慢，特别是随着数字化转型的加快，对数据治理提出了更高要求，商业银行在数据质量、数据标准和数据安全方面面临困境。

2.1 数据质量有待进一步提高

商业银行虽然积累了海量数据，但数据质量仍有待进一步提高。2020 年，多家银行因存在违法违规行为被处罚。从监管部门公布的处罚信息可以看出，商业银行的数据报送存在不及时、不全面、不准确等问题，这从侧面可以反映出商业银行的数据质量不高，存在多种问题，有待规范提高。

商业银行的数据纷繁复杂，来源不一，且尚未进行有效整合，数据碎片化和数据孤岛问题突出，无法充分发挥数据价值。国有大型商业银行和股份制银行虽然已经建立了统一的平台，数据质量相对较高，数据治理水平也处于领先地位，但是对过去分散于不同系统、标准不一的数据进行整合仍需时日。中小银行的数据基础差、问题多，根据《中小银行数据治理调研报告》的调查结果，92.1%的受访银行经常遭遇数据质量问题。

2.2 数据标准问题突出

目前大部分商业银行已经开启了数据标准化工作，但是商业银行数字化转型对数据的要求进一步提高，导致了数据标准的提高。

商业银行的数据来源不一，既有商业银行在业务发展中积累的内部数据，也有从外部购买或者通过与第三方合作形成的数据，还有一些通过社交网络、购物平台等外部渠道获取的数据。这导致商业银行虽然形成了海量数据，但在数据标准问题上面临一些困境。部分银行缺少全行统一的数据标准，个别字段缺失或存在异常信息，部分失真，更新滞后，内、外部数据缺乏联系。部分银行虽已建立了数据标准，但贯彻执行不力，数据标准落实不到位，或者做不到及时、同步更新。数据标准不统一容易产生“数据孤岛”，给数据治理工作带来极大障碍，影响了数字化转型进程。

2.3 数据安全问题尤为突出

随着商业银行数字化转型的加快，数据安全的重要性日益凸显。商业银行面临着数据滥用、数据泄露、数据污染、数据非法使用等挑战。长期以来，商业银行的数据安全问题层出不穷，多家银行内部人士因数据泄露被处罚，有的甚至因构成犯罪被处以刑罚。2020 年 4 月，有监测机构发现，境外黑客网站出现多个出售国内银行客户信息的帖子，疑似是多家金融机构的百万客户数据资料被泄露所致。

随着金融科技的发展，数据已经成为商业银行数字化转型的核心竞争力，数据驱动商业是推动商业银行发展的重要动力。数据安全问题成为商业银行发展的前提和保障，是数据治理的关键。如果商业银行对数据保护力度不够，不仅会影响到商业银行自身，还有可能传染扩散，影响到国家安全、社会秩序、公众利益和金融市场稳定。

三、商业银行数据治理困境的原因分析

商业银行数字化转型对数据治理提出了更高要求。目前，推动数字化转型已成为我国商业银行提升服务质量、满足客户需求、提高自身竞争力的重要路径。在数字化转型过程中，数据作为数字经济时代的重要生产要素，已经成为商业银行的重要资产。高质量的数据是商业银行数字化转型的核心基础，商业银行的数字化转型也对数据治理提出了更高要求。商业银行在数字化转型过程中一直非常重视数据管理和数据治理工作，但直至今日，数据治理仍处于发展阶段。2019 年的一份关于中国商业银行数字化转型的调研报告显示，商业银行整体数据治理领域的得分仅为 3.03 分，商业银行数据治理仍存在很多问题和挑战，具有很大的提升空间。特别是中小银行，数据治理还处于起步阶段，绝大多数中小银行仍未能建立完善有效的数据治理体系。因此，数字化转型对商业银行的数据治理提出了更高要求，商业银行应进一步加强数据治理工作。

“以客户为中心的”发展理念对数据治理提出了更高要求。随着商业银行的竞争日趋激烈，客户逐渐成为未来商业银行发展的核心竞争力。商业银行“以客户为中心”的发展理念，对数据治理提出了更高要求。一方面，“以客户为中心”的发展理念，要求商业银行根据客户需求，提供高质量的金融产品和服务。这一要求应建立在对数据深度挖掘、分析和应用的基础之上。新冠疫情爆发以来，商业银行对 App 线上运营尤为重视，2020 年上半年，我国已有 7 家银行的手机用户突破亿户，其中用户最多的工商银行多达 3.85 亿户，数量巨大的用户产生了海量数据。商业银行如能进行有效的数据治理，形成高质量的数据，就能有效识别客户，对客户进行精准画像，分析客户潜在需求，以客户为中心提供金融产品和服务，从而可以全面提升客户体验，增强客户黏性。另一方面，“以客户为中心”的发展理念，要求商业银行加强消费者保护。商业银行既要防止因不同人群对信息、技术的拥有程度、应用程度的差异，而出现数字鸿沟和金融服务不平等现象，还要注重加强客户的个人信息保护。

数据治理架构不清晰。《指引》将数据治理纳入商业银行公司治理的范畴。商业银行的数据治理不是某一部门或者某几个部门的工作，而是涉及到全行的各个部门，如果没有健全的治理架构，数据治理仅是纸上谈兵，无法得到切实的落实和推进。目前，商业银行数据治理架构不健全主要体现在顶层设计、组织架构和人才队伍方面。在顶层设计方面，随着数字

化转型的发展，商业银行非常重视数据治理，但是仅有少数处于领先地位的商业银行制定了明晰清楚、具有全局性的数据战略，大多数商业银行缺乏数据治理的顶层设计和战略规划。在组织架构方面，我国商业银行的组织架构呈传统的金字塔型，管理以条线为主，各部门之间相对独立，已不能适应以科技为推动力的现代化流程，不利于全行“一盘棋”，一体化推进数据治理工作。比如根据《中国区域性银行数字化转型白皮书》调研，区域性中小银行在数字化转型中面临的重大挑战是部门沟通困难、权责不清，这也是其在数据治理中面临的问题。在人才队伍方面，商业银行数据治理人才短缺，亟须掌握金融、数据和技术知识的复合型人才。

四、商业银行数字化转型的数据治理建议

4.1 结合数字化转型特点，不断提高数据治理水平

商业银行数据治理水平差异较大，因而，对自身治理水平有清晰认知和准确定位，并选择适合自己的数据治理路径就更为重要。首先，建立数据治理能力成熟度等级评价机制。通过该机制建立和评价自身数据治理能力，对数据治理的现状、能力和发展路径等进行认知和定位，发现数据治理的问题和短板，不断提升数据治理水平。其次，探索并选择合适的数据治理路径。不同的商业银行数据治理水平不同，在数字化转型过程中，各银行应结合自身特点和短板，选择一条与自身定位、发展目标、经营环境相适应的数据治理路径。对处于数据治理起步阶段的商业银行，思想上要重视，要在总行层面建立全行数据治理体系；在战略上加强顶层设计，制定全行数据治理战略规划；积极推进各项数据治理工作，引进最新技术。对处于数据治理发展阶段的商业银行，要根据数字化转型要求，进一步完善数据治理体系，有步骤、按顺序地开展数据治理工作，对于发现的短板和出现的问题，要查缺补漏，补齐短板，解决问题。对在数据治理中处于领先的商业银行，要发挥数据驱动决策、数据引领业务发展的优势，巩固已有的数据治理成绩，继续探索引进最新技术，发挥数据在业务、产品、服务创新中的作用，将数据转化为成果。

4.2 完善数据治理架构

商业银行数据治理要做好顶层设计，提高统筹规划能力，制定符合监管要求和商业银行实际情况和各自特色的数据战略，设计阶段性的治理目标，将数据治理融入银行的公司治理、运行体系和业务流程，自上而下推动数据治理工作。

组织架构方面，商业银行应当加强组织领导，优化组织架构，建立由董事会、监事会、高级管理层、归口管理部门、业务部门各司其职、分工明确、职责清晰的数据治理组织体系，设置专门的数据中心或数据部门，负责数据治理工作，并可以适时设立首席数据官。例如：

工商银行于 2000 年正式成立数据中心，作为工行总行直属机构，负责全行信息系统的生产运维管理、基础架构技术研究，以及全集团信息安全防线等工作。建设银行成立了总行行领导挂帅的工作领导决策机构，强化总行数据管理部作为大数据建设牵头部门，与大数据指挥中心一体化协同运作，加强大数据工作的体系化统筹管理。

人才队伍方面，数据治理还需要一支专业化的团队。数据治理具有很强的专业性，商业银行要结合数据治理的实际需求，加强队伍建设，通过引进专业人才和加快内部数据治理人才培养相结合的方式，尽快配备一支专业化团队。各家银行都已认识到了人才的重要性，通过各种方式加强人才队伍建设。工商银行自 2014 年开始组建数据分析师队伍，截至 2020 年 9 月，已有数据分析师 5181 人，覆盖总分行多个主要部门及二级分行以上机构的 33 个业务条线。招商银行在总行各个业务部门均设立数据岗位，引进和培养复合型数据人才。浦发银行专门就科技数字化人才培养机制进行调研，结合自身实际建立人才培养机制。

4.3 持续提高数据质量

商业银行应当根据数字化转型的要求，加强数据质量管理，持续提升数据质量，秉持“以客户为中心”的发展理念，精准满足客户需求，实现数据价值最大化。

首先，建立一体化的数据平台，加强数据整合。一体化的数据平台是大数据基础架构的重中之重，不仅是数据整合的基础与数据治理的关键，也是数据价值得以实现的重要工具。建立一体化的数据平台，将分散设立的系统接入平台，使该平台能够覆盖商业银行全部数据的全生命周期，为数据整合和数据治理提供系统支撑。同时，在该平台上设置合理的数据质量检测标准和指标，对数据质量进行持续动态监测、评估和考核，针对发现的问题进行分析，查找原因，提供解决方案并进行反馈，由相关责任主体予以纠正，以确保数据质量。其次，在保障个人隐私的前提下，完善对客户个人信息、金融行为、账户特性等方面的数据采集。在客户授权下，商业银行可与征信、税务、社保等第三方机构合作，也可通过技术手段获取客户在社交平台上的信息。通过不断丰富客户数据来源，并进行交叉对比、分析和挖掘，提高数据质量，精准了解客户。最后，建立健全数据质量管理规章制度。商业银行应当确立数据质量管理目标，建立数据治理架构，制定全面、科学、有效的数据管理、数据应用和监管数据质量管控制度，通过数据质量管控、现场检查、考核评价以及整改等制度，全面提升数据质量。

4.4 进一步建立健全商业银行数据标准体系

商业银行应按照《指引》要求，适应数字化转型需要，站在全局角度，根据业务发展、风险防控、内部管理和监管合规的需要，设置全行统一的企业级数据标准。数据标准主要包

括业务定义、技术定义和管理信息。业务定义要让业务规则及标准达到“定义统一、口径统一、名称统一、来源统一、参照统一”的要求；技术定义要对数据类型、数据格式、数据长度等技术性要素统一数据标准；管理信息要求明确数据标准的制定者、管理者和使用者，确保各责任主体对数据标准进行管理和维护，以保障数据标准与业务实现同步更新。

标准建立后，商业银行内部各部门应加强联动，共同推进已经建立的数据标准落实到位。业务部门要与技术部门充分沟通，从业务经营、风险防控、内部管理以及监管合规的需求出发，推进数据标准化建设。技术部门应在系统设计和建立时将数据标准贯彻其中，用技术手段确保数据标准得到贯彻执行。监督部门应对数据标准的贯彻执行情况进行监督，如有落实不到位的情况，及时纠正。

另外，商业银行还要推动跨行业数据交互标准建立。随着商业银行数字化转型的发展，跨行业的数据交互与共享越来越多，交互标准的建立迫在眉睫。商业银行应当加强沟通，推动并积极参与跨行业数据交互标准体系建立，促进跨行业数据交互、共享及整合，实现数据价值的最大化。

4.5 切实保障数据安全

数据安全是数据应用和价值实现的前提，商业银行数据治理的主要目的是保障数据安全，推动数字化转型顺利进行。一方面，要构建覆盖数据全生命周期的安全防护体系，对数据进行全方位立体保护；不断升级技术安全防控系统，有效保障平台、数据和设备的安全。另一方面，要进行数据安全分类分级管理。商业银行应根据数据安全性遭受破坏后可能造成的影响，对数据安全定级。对不同类型、不同级别的数据制定不同的数据权限和管理审批流程，将数据安全融入到数据全生命周期管理中，并确保采用行之有效的保护手段。同时，还须加强个人数据保护。商业银行需提高个人信息采集、使用、处理等环节的合规性要求，在数据全生命周期的各个环节，综合利用加密存储、数据脱敏等技术，保护个人数据安全。（来源：银行家杂志）

四、政府之声

➢ 国家市场监督管理总局出台《网络交易监督管理办法》

2021 年 3 月 15 日，市场监管总局正式发布《网络交易监督管理办法》，办法自 2021 年 5 月 1 日起施行。近年来，我国网络交易蓬勃发展，“社交电商”“直播带货”等新业态新模式不断涌现、快速壮大，为网络经济增添了新的活力，为稳增长、促消费、扩就业发挥了重要作用。与此同时，也出现了不少问题，社会各界呼唤完善相应的监管规则。市场监管总局主动作为，积极回应社会关切，于 3 月 15 日制定出台《网络交易监督管理办法》（以下简称《办法》）。《办法》是贯彻落实《电子商务法》的重要部门规章，对相关法律规定进行细化完善，制定了一系列规范交易行为、压实平台主体责任、保障消费者权益的具体制度规则，对完善网络交易监管制度体系、持续净化网络交易空间、维护公平竞争的网络交易秩序、营造安全放心的网络消费环境具有重要现实意义。

《办法》共 5 章 56 条，包括总则、网络交易经营者、监督管理、法律责任和附则等内容。《办法》明确了网络交易监管坚持鼓励创新、包容审慎、严守底线、线上线下一体化监管原则，提出推动完善多元参与、有效协同、规范有序的网络交易市场治理体系，对网络经营主体登记、新业态监管、平台经营者主体责任、消费者权益保护、个人信息保护等重点问题作出了明确规定。

针对个人信息保护问题，《办法》规定了网络交易经营者应当明示收集、使用消费者个人信息的目的、方式和范围，并经消费者同意；不得强迫或者变相强迫消费者同意收集、使用与经营活动无直接关系的信息；在收集、使用个人敏感信息前，必须逐项取得消费者同意；未经被收集者授权同意，不得向包括关联方在内的任何第三方提供。

《办法》还针对虚构交易、误导性展示评价、虚构流量数据等新型不正当竞争行为进行了明确规制，禁止各类网络消费侵权行为。 《办法》的出台实施有利于指导督促网络交易经营者依法合规经营，更好规范网络交易秩序，保护网络消费者合法权益，促进我国数字经济持续健康发展。《办法》自 2021 年 5 月 1 日起施行，原《网络交易管理办法》同时废止。

（来源：国家市场监督管理总局）

- **《网络交易监督管理办法》**
- **全文：**http://gkml.samr.gov.cn/nsjg/fgs/202103/t20210315_326936.html

➢ 四部门联合发布《常见类型移动互联网应用程序必要个人信息范围规定》

2021 年 3 月 12 日，近日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局四部门联合发布《常见类型移动互联网应用程序必要个人信息范围规定》（以下简称《规定》），旨在落实《中华人民共和国网络安全法》关于个人信息收集合法、正当、必要的原则，规范移动互联网应用程序（App）个人信息收集行为，保障公民个人信息安全。

随着移动互联网快速发展，各类应用程序迅速普及应用，在促进经济社会发展、服务民生等方面发挥了重要作用。但同时，App 超范围收集用户个人信息问题十分突出。特别是大量 App 通过捆绑功能服务一揽子索取个人信息授权，用户拒绝授权就无法使用 App 基本功

能服务，变相强制用户授权。为聚焦解决 App 超范围收集个人信息问题，规范收集个人信息活动，国家互联网信息办公室会同工业和信息化部、公安部、国家市场监督管理总局联合制定实施该《规定》。

《规定》明确了地图导航、网络约车、即时通信、网络购物等 39 类常见类型移动应用程序必要个人信息范围，要求其运营者不得因用户不同意提供非必要个人信息，而拒绝用户使用 App 基本功能服务。

四部门要求，各省、自治区、直辖市及新疆生产建设兵团网信办、通信管理局、公安厅（局）、市场监管局（厅、委）指导督促本地区 App 运营者抓紧落实《规定》要求，加强监督检查，及时调查、处理违法违规收集使用个人信息行为，切实维护公民在网络空间的合法权益。（来源：国家互联网信息办公室）

- **关于印发《常见类型移动互联网应用程序必要个人信息范围规定》的通知**
- **全文：**http://www.cac.gov.cn/2021-03/22/c_1617990997054277.htm

➢ 教育部发布关于加强新时代教育管理信息化工作的通知

2021 年 3 月 25 日，据教育部官网信息显示，为有效解决系统整合不足、数据共享不畅、服务体验不佳、设施重复建设等突出问题，教育部印发《关于加强新时代教育管理信息化工作的通知》（以下简称 《通知》）。

《通知》要求，各地要加强教育管理信息化统筹协调，优化信息系统供给模式，以信息化支撑教育治理体系和治理能力现代化。同时，要利用新一代信息技术提升教育管理数字化、网络化、智能化水平，推动教育决策由经验驱动向数据驱动转变、教育管理由单向管理向协

同治理转变、教育服务由被动响应向主动服务转变。到 2025 年，要基本形成新时代教育管理信息化制度体系，促进教育决策科学化、管理精准化、服务个性化水平全面提升。

《通知》强调，各地还需加强教育管理信息化组织领导，构建教育管理信息化分工机制，完善教育管理信息化制度体系；加强信息系统规范管理，推进信息系统深度整合，促进应用服务创新发展；加强教育数据规范管理，促进教育数据开放共享，强化教育数据质量保障，提升教育数据管理效能；促进教育行政办公数字化，实现教育管理服务“一网通办”推进教育督导和监管信息化；加强网络环境建设，规范数据中心建设，构建数字认证体系，提升安全保障能力。此外，还要打造一支技术精湛、结构合理、精简高效的专业队伍，培养和吸引更多优秀人才，鼓励通过购买社会服务、实行岗位交流、健全产学融合等方式引入外部资源。加大教育管理信息化投入，为系统建设、运行维护、安全防护、应用培训、服务运营、队伍建设等提供必要保障。（来源：教育部）

- **教育部关于加强新时代教育管理信息化工作的通知**
- **全文：**http://www.moe.gov.cn/srcsite/A16/s3342/202103/t20210322_521669.html

➢ 银保监会发布关于防范短信钓鱼诈骗的风险提示

2021 年 3 月 16 日，中国银行保险监督管理委员发布关于防范短信钓鱼诈骗的风险提示。近日，一些不法分子通过群发短信，假冒多家银行名义发送服务信息，声称客户手机银行、银行卡、身份证等过期或失效，诱导客户点击短信中网站链接访问虚假手机银行系统,客户一旦受骗提供银行卡号或手机号、账户密码、短信验证码等信息，不法分子将迅速冒用客户身份进行转账，盗取银行卡内资金，使客户资金遭受损失。在此，中国银保监会消费者权益保护局发布 2021 年第一期风险提示：提醒消费者注意保护个人账户信息安全，从官方渠道办理手机银行或网上银行业务，谨防短信钓鱼诈骗侵害资金安全。

向消费者发送短信钓鱼链接是电信诈骗的常用手法之一。此次短信钓鱼诈骗在全国范围密集爆发，攻击目标和行为特征相对一致，受骗对象多为风险防范意识较弱、对手机银行或网上银行登录操作不熟悉的人群。此类诈骗一般是有组织的专业诈骗，目的主要是窃取消费者银行账户敏感信息或盗取账户资金。

中国银保监会消费者权益保护局提醒：广大消费者一定要对不明短信、不明网站链接和

页面、不明手机 APP 提高警惕，尤其是在被要求提供个人银行账户敏感信息时，要多看多思，防范被诈骗风险。

一看短信是否真实。诈骗短信假冒银行名义会降低消费者警惕性。消费者在收到署名为银行发送的信息时，要注意辨别真假，尤其不能盲目相信异常号码发送的短信。消费者若不确定短信是否真实，可以到银行营业网点或向其官方客服咨询。

二看网站链接和页面是否为官方渠道。诈骗短信提供的网页链接可能是假冒手机银行或网上银行网页的钓鱼链接，也可能是病毒木马，不应轻易点击和操作。建议广大消费者登录手机银行或网上银行时从银行官方手机 APP 或网站等正规渠道进入，尽量不要点击第三方提供的网站链接操作，以免被不法分子诱骗。

三看对方索要信息是否为个人重要敏感信息。消费者的身份证号、银行卡号、账户密码、短信验证码、付款码等均为个人重要且敏感信息，当有第三方要求提供或输入上述信息时，需提高警惕。不轻易提供重要敏感信息给他人，不点击来路不明的网站链接，不随意在除银行官方渠道之外的网页填写重要敏感信息。如发现自己上当受骗，请立即联系银行冻结银行账户，保存证据，及时报警。（来源：中国银行保险监督管理委员）

五、本期重要漏洞实例

➢ Microsoft 发布 2021 年 3 月安全更新

发布日期：2021-3-22
更新日期：2021-3-11
描述：

2021 年 3 月 11 日，微软发布了 2021 年 3 月份的月度例行安全公告，修复了其多款产品存在的 89 个安全漏洞。受影响的产品包括：Windows 10 20H2 & WindowsServer v20H2（48 个）、Windows 10 2004 &WindowsServer v2004（48 个）、Windows 10 1909 &WindowsServer v1909（47 个）、Windows 8.1 & Server 2012 R2（27 个）、Windows Server 2012（26 个）和 Microsoft Office-related software（9 个）。

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-2021-26867	**Windows Hyper-V 远程代码执行漏洞**	严重 远程代码执行	Windows 10 Server, version 1909 Server, version 2004 Server, version 20H2
CVE-2021-26897	**Windows DNS Server 远程代码执行漏洞**	严重 远程代码执行	Server 2016 Server 2019 Server, version 1909 Server, version 2004 Server, version 20H2 Server 2012 Server 2012 R2
CVE-2021-27077	**Windows Win32k 权限提升漏洞**	重要 特权提升	Windows 10 Server 2016 Server 2019 Server, version 1909 Server, version 2004 Server, version 20H2 Windows 8.1 Server 2012 Server 2012 R2
CVE-2021-24090	**Windows Error Reporting 权限提升漏洞**	重要 特权提升	Windows 10 Server, version 1909 Server, version 2004 Server, version 20H2
CVE-2021-24089	**HEVC Video Extensions 远程代码执行漏洞**	严重 远程代码执行	CHEVC Video Extensions
CVE-2021-26411	**Internet Explorer 内存破坏漏洞**	严重 远程代码执行	Internet Explorer 9 Internet Explorer 11

			Microsoft Edge(EdgeHTML-based)
CVE-2021-27085	**Internet Explorer 远程代码执行漏洞**	重要 远程代码执行	Internet Explorer 11
CVE-2021-27076	**Microsoft SharePoint Server 远程代码执行漏洞**	重要 远程代码执行	Business Productivity Servers 2010 SharePoint Foundation 2013 SharePoint Enterprise Server 2016 SharePoint Server 2019
CVE-2021-27053	**Microsoft Excel 远程代码执行漏洞**	重要 远程代码执行	Office 2019 Excel 2010/2013/2016 Office Online Server 365 Apps Enterprise Office Web Apps Server 2013

参考链接：https://msrc.microsoft.com/update-guide/releaseNote/2021-Mar

➢ Cisco Aironet Access Points 文件覆盖漏洞

发布日期：2021-3-25
更新日期：2021-3-26
受影响系统：
Cisco Aironet Access Points
描述：

CVE(CAN) ID: CVE-2021-1423
Cisco Aironet Access Points（aps）是美国思科（Cisco）公司的一款网络接入点设备。
Cisco Aironet Access Points 存在安全漏洞，该漏洞源于对特定命令的输入验证不足。攻击者可利用该漏洞覆盖设备闪存中的文件。
建议：

厂商补丁：
Cisco
厂商已发布了漏洞修复程序，请及时关注更新：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-foverwrt-HyVXvrtb

➢ Mozilla Firefox 越界读取漏洞

发布日期：2021-03-23
更新日期：2021-03-25
受影响系统：
Mozilla Firefox < 87
Mozilla Thunderbird < 78.9
Mozilla Firefox ESR < 78.9
描述：

CVE(CAN) ID: CVE-2021-23981
Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。Mozilla Firefox 存在越界读取漏洞。攻击者可通过上传像素缓冲区对象利用该漏洞导致内存损坏以及信息泄漏或崩溃。
链接：https://www.mozilla.org/en-US/security/advisories/mfsa2021-10/
建议：

厂商补丁：
Mozilla
Mozilla 已经为此发布了一个安全公告（mfsa2021-10）以及相应补丁：
链接：https://www.mozilla.org/en-US/security/advisories/mfsa2021-10/

➢ Wordpress Contact Form Submissions SQL 注入漏洞

发布日期：2021-03-18
更新日期：2021-03-23
受影响系统：
WordPress Contact Form Submissions <= 1.6.4
描述：

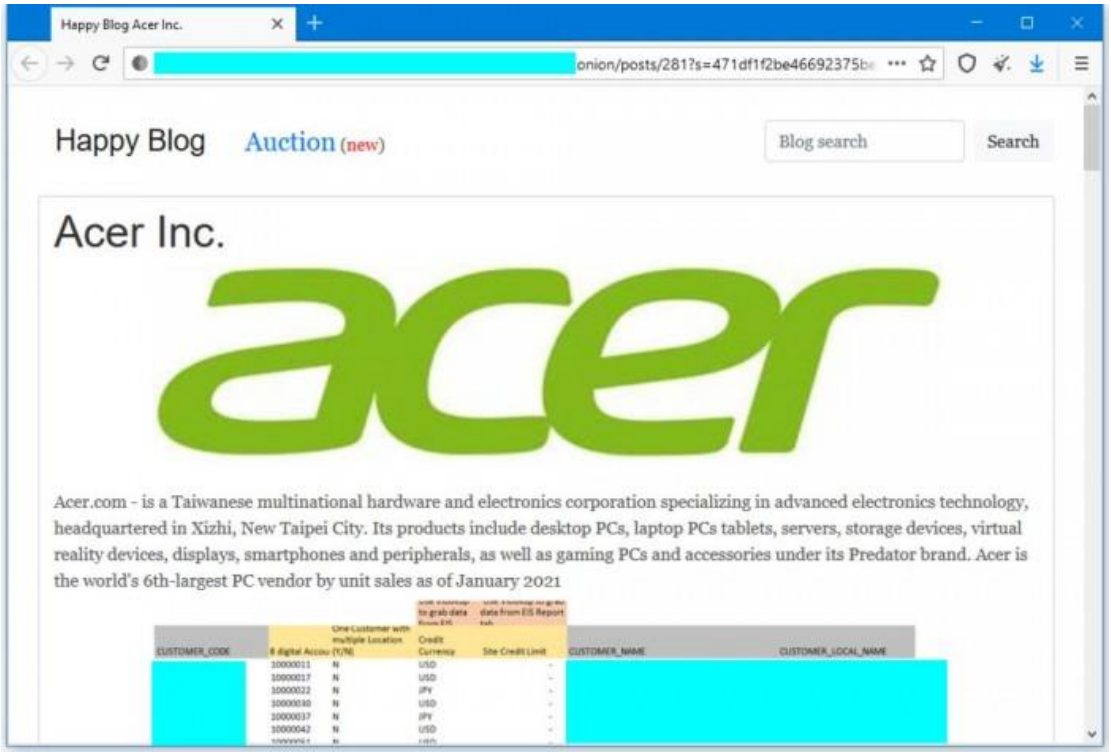
CVE(CAN) ID: CVE-2021-24125
Wordpress Contact Form Submissions 是（Wordpress）开源的一个应用插件。提供了以 csv 格式导出提交内容的功能。Contact Form Submissions WordPress plugin 1.6.4 及之前版本存在 SQL 注入漏洞。该漏洞源于程序未对输入进行正确验证。攻击者可利用该漏洞导致 wpcf7_contact_form GET 参数中的 SQL 注入。
建议：

厂商补丁：目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
http://wordpress.org/
https://wpscan.com/vulnerability/8591b3c9-b041-4ff5-b8d9-6f9f81041178

六、本期网络安全事件

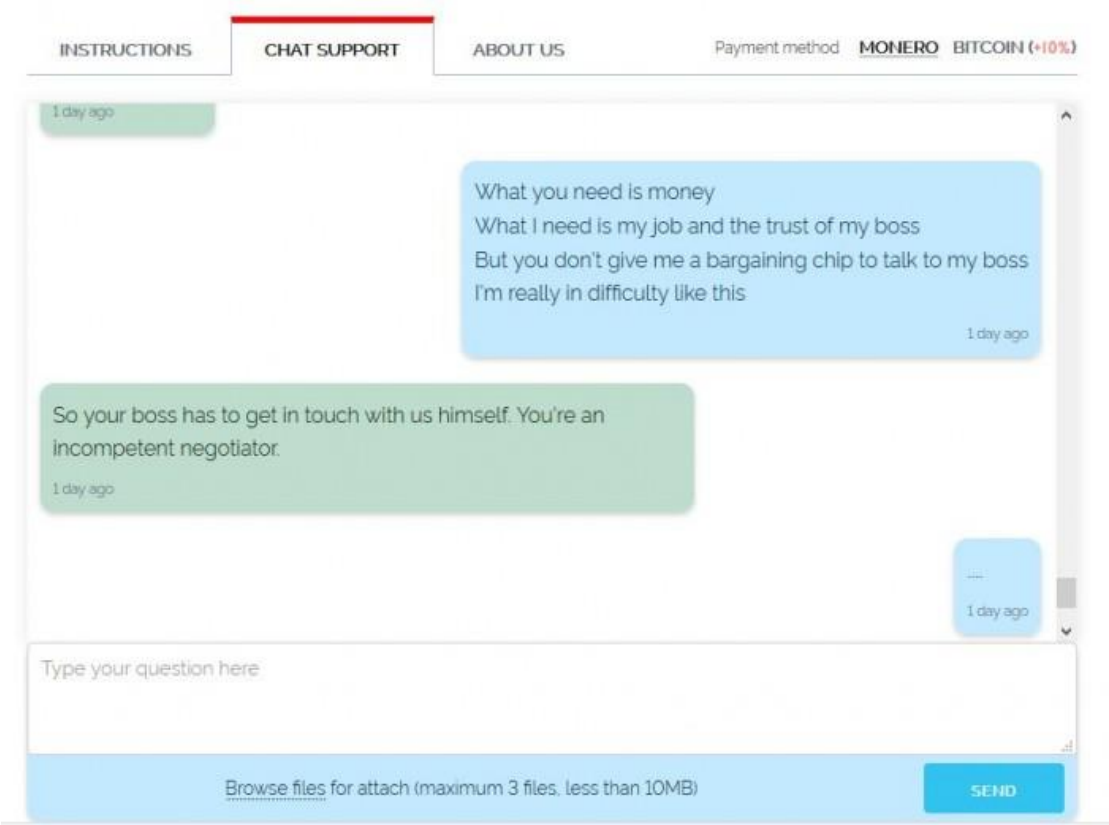
➢ 宏碁遭勒索软件攻击 要求支付高达 5000 万美元的赎金

2021 年 3 月 20 日，上周末，知名电脑厂商宏碁（Acer）遭遇勒索软件团伙 REvil 的攻击，要求支付高达 5000 万美元的赎金，以解密公司的电脑，并且不在暗网上泄露数据。本次攻击并未破坏生产系统，只是入侵了公司的后台网络。本次安全漏洞被认为破坏性不大，不足以阻止或推迟这家电脑制造商在周三公布 2020 年第 4 季度的财务业绩。



在外媒发出评论请求之后，宏碁发言人刻意淡化了这起勒索软件攻击事件，并避免承认遭到勒索软件攻击。The Record 在本周早些时候发现宏碁的名字出现在一个暗网上，REvil 勒索软件团伙通常会从那些不支付勒索费的公司泄露文件，之后该公司联系了评论。但 REvil 团伙还没有泄露宏基的文件。相反，它只分享了一些内部文件的截图，作为对这家电脑制造商管理团队的警告，并迫使其支付赎金。

在 Malwarebytes 的恶意软件情报分析师 Marcelo Rivero 的帮助下，The Record 能够追踪到 REvil 团伙运营的另一个暗网门户--受害者会被重定向到这里进行赎金支付谈判。在这里，勒索要求清晰可见，高达 5000 万美元的支付要求，这代表着勒索软件团伙有史以来最高的勒索要求。



这个页面还允许我们进入 REvil 团伙与宏碁代表沟通的在线聊天，这表明目前的谈判已经谈崩了。宏碁是全球第六大个人电脑制造商，市场份额约占全球总销售额的 6%。该公司在 2020 年第 4 季度的总收入约为 30 亿美元，因此，赎金需求创下了新纪录。（来源：cnBeta）

➢ 贩卖 50 多万条个人信息 警方抓获嫌疑人 16 名

2021 年 3 月 24 日，烟台市公安局开发区分局成功侦破了一起涉嫌重大侵犯公民个人信息案，抓获嫌疑人 16 名，刑拘 7 名，取保 1 名，扣 押涉案手机 23 部，笔记本电脑 3 台，电脑 6 台，查获公民个人信息 50 多万条，查明涉案人员二百余人，目前案件正在进一步侦办中。

为提升业绩 金融公司员工盯上个人信息

2021 年 2 月 26 日，烟台市公安局开发区网络安全大队民警在工作过程中发现，有人在网上大量买入公民个人信息，行为可疑。警方对此立即进行立案侦查。通过侦察，警方发现购买公民个人信息的张某在开发区某金融公司上班。据他交代，购买大量公民个人信息的目的是为了帮助征信有问题或者负债高的人办理贷款，提高业绩，这种做法在公司内部屡见不

鲜。

发现了大量的公民信息

警方顺藤摸瓜，对该金融公司 200 余名员工进行审查，发现 20 余人购买公民个人信息，其中 3 人因情节特别严重，被警方依法刑事拘留。据三人交代，不少人由于个人信用或者是经济收入无法达到大规模银行的放贷要求，通过金融公司从中小银行贷款，金融公司获取中介费用。为了拓展业务，三人动起了歪脑筋，陆续花 7 万元从济南一家网络科技公司购买个人信息。

为扭亏为盈 上线公司非法获取数据获利 40 余万

接到线索后，开发区警方立刻前往济南，经过精密布控，于 3 月 9 日在济南遥墙机场将准备前往外地的上线公司老板胡某某抓获。在办公室内，警方从手机、办公电脑中，发现该公司自去年 11 月到 3 月共出售公民个人信息 50 多万条，非法获利 40 余万元。据胡某某交代，公司去年经营不善。为了尽快止损，他打听到在网上贩卖个人信息数据来钱快，就带领部分员工瞄准“借贷”“买房”等关键词，通过通讯软件和技术手段非法获取数据，销售部门再广撒网，联系各地金融、销售等公司进行推销。

济南老板胡某某学计算机专业，计算机水平很高，通过非法手段精准获取公民信息。胡某某通过计算机编写程序，将相应的信息筛选出来，进行销售。为了发展客源，胡某某妻子负责销售，她亲自到烟台来考察客源，看是否是需求量大的和真实可靠的，并通过这种方式来进行公民信息的买卖。

为规避法律风险，胡某某还专门咨询律师，企图通过将数据和公民身份信息标识分割来

蒙混过关。为此，公司技术部门开发专用服务器和破译软件，把非法获取的个人信息数据做成乱码，客户登陆服务器后同时下载数据和软件，获取公民信息。胡某某以为这样就可万无一失，没想到法网恢恢、疏而不漏。目前，警方已刑事拘留包括胡某某在内的上线公司员工 4 人，取保 1 人。（来源：烟台日报）

➢ 非法获取员工及用户敏感信息，法国宜家或将被罚 375 万欧元

2021 年 3 月 22 日报道，法国宜家前高管被指控非法监视员工和客户一案于当日庭审。这场官司于当日起正式进入审判阶段，庭审将持续至下月 2 日。

据悉，2012 年宜家遭内部知情者举报，称法国宜家试图通过掌握警方内部数据库、雇私家侦探等方式，非法获取公司雇员以及宜家客户的个人资料和敏感信息，其中特别收集了工会活动人士和与宜家发生纠纷的客户信息。接到举报后，法国检方随即对宜家展开调查，最终法国宜家解雇了涉案的 4 名高管，并对内部政策做出修改。“宜家法国公司非常重视对员工和客户数据的保护。”宜家法国公司在一份声明中表示，并声称调查于 2012 年展开后，公司一直采取合规的培训程序，以防止非法活动的发生。

在周一凡尔赛法庭的审判中，法国宜家前首席执行官、前首席财务官以及多名前店长共计 15 人出庭受审，其中包括涉案的 4 名警务人员。如果罪名成立，涉嫌此案的两名前 CEO 将面临最多 10 年刑期以及 75 万欧元罚款，而宜家方面也有可能收到 375 万欧元的高额罚单。

宜家非法获取员工和用户信息的行为还面临着来自工会和 74 名员工提起的民事诉讼。据了解，一名宜家员工在庭审中表示，公司曾怀疑他是一名银行劫匪，因为他们在调查系统里发现了一名同名银行劫匪的犯罪记录。不仅如此，宜家法国公司还曾利用未经授权的数据试图抓获一名申请失业救济但驾驶保时捷的员工。“员工的隐私权应该是神圣的。”员工律师安妮·索伦布维尔认为。目前此案受到法国社会的普遍关注。（来源：互联网）

➢ 中信银行被罚 450 万元！曾泄露明星个人流水

2021 年 3 月 19 日，因客户信息保护体制机制不健全、对客户敏感信息管理不善等多项违规，中信银行被罚 450 万元。中国银保监会官网公布了上述针对中信银行股份有限公司的行政处罚信息公开表。此前的 2020 年 5 月，脱口秀演员池子曾控诉中信银行擅自泄露个人流水，中信银行也被银保监会立案调查。


中国银行保险监督管理委员会
China Banking and Insurance Regulatory Commission

机构概况 | 新闻资讯 | 政务信息 | 在线服务 | 互动交流 | 统计数据 | 专题专栏

当前位置：首页 > 政务信息 > 行政处罚 > 银保监会机关

发布时间：2021-03-19 来源：消保局 类型：原创

中国银行保险监督管理委员会行政处罚信息公开表
（银保监罚决字〔2021〕5号）

（中信银行股份有限公司）

行政处罚决定书文号			银保监罚决字〔2021〕5号
被处罚当事人	单位	名称	中信银行股份有限公司
		法定代表人姓名	李庆萍
主要违法违规事实（案由）			一、客户信息保护体制机制不健全；柜面非密查询客户账户明细缺乏规范、统一的业务操作流程与必要的内部控制措施，乱象整治自查不力 二、客户信息收集环节管理不规范；客户数据访问控制管理不符合业务“必须知道”和“最小授权”原则；查询客户账户明细事由不真实；未经客户本人授权查询并向第三方提供其个人银行账户交易信息

据行政处罚信息公开表，中信银行的违法违规案由包括：客户信息保护体制机制不健全;柜面非密查询客户账户明细缺乏规范、统一的业务操作流程与必要的内部控制措施，乱象整治自查不力;客户信息收集环节管理不规范;客户数据访问控制管理不符合业务“必须知

道”和“最小授权”原则;查询客户账户明细事由不真实;未经客户本人授权查询并向第三方提供其个人银行账户交易信息;对客户敏感信息管理不善，致其流出至互联网;违规存储客户敏感信息;系统权限管理存在漏洞，重要岗位及外包机构管理存在缺陷。3 月 17 日，银保监会依法作出对中信银行罚款 450 万元的行政处罚决定。

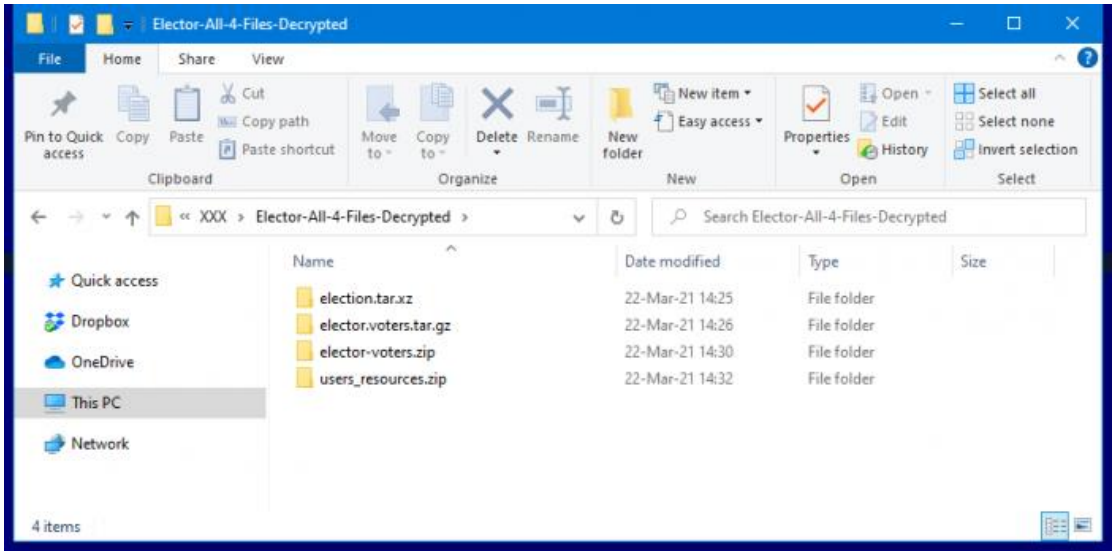
中信银行曾因员工泄露脱口秀演员银行流水被推上舆论风波

2020 年 5 月 6 日，笑果文化旗下脱口秀演员池子(原名王越池)发布一则长文和律师函，称中信银行未经授权将个人账户明细提供给笑果文化，诉其涉嫌“侵犯公民个人信息罪”。5 月 7 日凌晨，中信银行公开致歉，称对相关员工予以处分，并对支行行长予以撤职。

5 月 9 日，中国银保监会消费者权益保护局发出关于中信银行侵害消费者合法权益的通报。通报称，2020 年 3 月，中信银行在未经客户本人授权的情况下，向第三方提供个人银行账户交易明细，违背为存款人保密的原则，涉嫌违反《商业银行法》和银保监会关于个人信息保护的监管规定，严重侵害消费者信息安全权，损害了消费者合法权益。通报称，将按照相关法律法规，启动立案调查程序，严格依法依规进行查处。据官网介绍，中信银行成立于 1987 年，是中国最早成立的新兴商业银行之一，也是中国最早参与国内外金融市场融资的商业银行。2007 年 4 月，中信银行实现在上海证券交易所和香港联合交易所 A+H 股同步上市。（来源：南方都市报）

➢ 约 650 万以色列选民的详细信息在网上泄露

2021 年 3 月 25 日据外媒报道，当地时间周一，数百万名以色列公民的选民登记和个人信息在网上被泄露，两天之后，该国将举行一院制议会的大选。曝光的资料波及到 6528565 名以色列人的选民登记详细资料和以色列约 930 万总人口中 3179313 人的个人详细资料。后者包括了全名、电话号码、身份证号码、家庭住址、性别、年龄和政治倾向等细节。



据以色列媒体报道，一名自称为 The Israeli Autumn 的威胁分子称对此事负责

以色列威胁情报公司 KELA 的产品经理 Raveed Laeb 在周三媒体采访时表示，自周一以来，这些数据已经被多个电报频道广泛分享。此前，他在泄露的文件中发现了自己的个人信息。目前，数据泄露源头已被锁定为 Elector--一个为 Elector Software for Likud 公司开发的同名应用的网站。Likud（利库德集团）是以色列现任总理本雅明·内塔尼亚胡领导的政党。

2020 年 2 月，一位名叫 Ran Bar-Zik 的以色列网页开发者发现，该应用的网站暴露了一个 API 端点，该端点允许他获得该网站管理员及其帐户详细信息的列表，其中包括密码。

Bar-Zik 称，通过利用这些密码，他能访问一个包含以色列选民个人信息的数据库。Bar-Zik 在一篇博文中详细阐述了他的发现，这在 2020 年初引发了以色列的一场重大媒体丑闻，因为尽管出于政治竞选计划等原因政党可以访问以色列的全部选民数据库，但他们不应该跟第三方分享这些数据。当时，Bar-Zik 向该应用网站的开发公司报告了这一情况，但网站开发者警告称，目前尚不清楚其他各方是否在他之前发现了同样的问题，也不清楚他们是否利用 API 获取了以色列公民的选民登记数据。

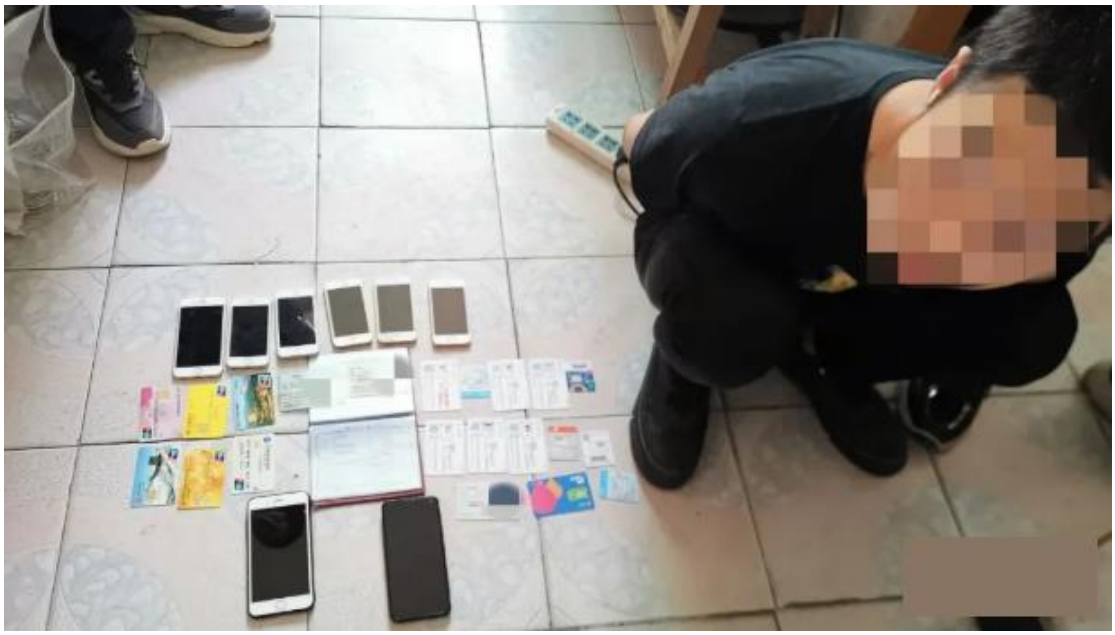
在该国最新一轮选举前几天公布的数据显示，Bar-Zik 的困境似乎在本周得到了解决。几位以色列政治专家本周提出的理论认为，泄露这些数据可能是为了损害利库德集团的公众形象和信任，然而，由于利库德集团有望在 2021 年 3 月的议会选举中获胜，所以此次的泄密似乎并没有产生任何的影响。（来源：互联网）

➢ 江西首例区块链比特币特大盗窃案告破 6 名黑客被抓

2021 年 3 月 25 日，南昌市公安局青云谱分局成功侦破了一起利用黑客网络技术盗取区块链货币的价值新型网络犯罪案件，实现了对案件上下游犯罪“全链条”的有力打击。截止目前，该案已抓获 6 名涉案犯罪嫌疑人。

虚拟货币不翼而飞受害者事前无操作

2021 年 2 月 26 日，辖区群众黄某到分局报案：其称 2 月 23 日 18 时许，突然发现手机号码被他人莫名挂失，继而发现与手机号码捆绑登录的“雷达网”账户中的区块链货币(雷达币和比特币)被人转走，被盗虚拟货币折合人民币价值近 1450 万元。。接警后民警迅速立案侦查，办案民警在侦查中初步发现——该案中涉及的“雷达网”，属于国外一雷达实验室开办，国内未发现有相应的公司或机构。受害人损失的是虚拟货币，且犯罪嫌疑人未与受害人发生任何实质性接触，也未留下电话、微信等任何联系方式。犯罪嫌疑人在受害人没有任何操作的情况下，盗取安全性较高的虚拟货币账户，而且几乎没有留下作案痕迹。



12 小时内锁定嫌疑人

专案组反诈民警通过摸排走访调查发现，案发前曾有 5 名江苏连云港籍男女开车流窜至南昌，持有伪造的受害人身份证件挂失、补办受害人手机卡的犯罪踪迹。获取初步线索后，专案组加班加点、连续攻坚，图侦、情报等警种联合作战，成功锁定涉案嫌疑人基本信息。经过办案民警不到 12 个小时的加班加点，案件侦查工作取得重大突破。

转战连云港抓获黑客 犯罪嫌疑人家中发现 140 余万现金

根据研判线索，专案组连夜奔袭上千公里到达江苏连云港，在当地转战 10 天，将嫌疑人轨迹逐一追踪到位。

直到 3 月 8 日，专案组在连云港市区、灌云县等地陆续抓获该 4 名嫌疑人——邓某(女，1991 年 2 月出生)、张某 1(男，1994 年 10 月出生)、王某苗(女，1981 年 4 月出生)、张某 2(女，1991 年 1 月出生)，并从邓某家中缴获了 140 余万现金，以及大量作案用手机、电脑以及各种伪造证件。3 月 15 日，专案组民警又赴广东中山、东莞分别抓获犯罪嫌疑人曾某(男，1997 年 12 月出生，湖南省耒阳市人)，张某某(男，1992 年 11 月出生，安徽省阜南县人)。

经查，犯罪嫌疑人邓某利用购买的黑客技术盗取虚拟货币交易平台“雷达网”后台用户信息，再雇佣犯罪嫌疑人王某、张某等伪造证件冒充受害人补办“雷达网”账户所捆绑手机号码，又通过补办的手机号由犯罪嫌疑人张某接受平台登录验证码，最后登陆受害人存有虚拟币的账户盗取账户内的虚拟货币。张某某负责查询相关信息，确认机主身份后发给曾某。曾某负责制作虚假证件和联系营业厅办理业务。专案组在前期侦查的基础上，逐步挖掘、固定该网络犯罪团伙的证据链条，斩断了该犯罪团伙盗取后台数据、制作假证、冒充受害人补办手机卡，利用手机验证码登录平台进行盗窃的犯罪链条。至此，利用黑客技术盗取虚拟货币的、江西首起特大新型网络犯罪案件实现全链条破案。目前， 6 名犯罪嫌疑人已依法刑事拘留，此案在进一步审理中。（来源：大江网）