# 国盟信息安全通报

2020 年 9 月 27 日第 225 期

全国售后服务中心

# 国盟信息安全通报

（第 225 期）

国际信息安全学习联盟

2020 年 09 月 27 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 395 个，其中高危漏洞 94 个、中危漏洞 231 个、低危漏洞 70 个。漏洞平均分值为 5.43。本周收录的漏洞中，涉及 0day 漏洞 51 个（占 13%），其中互联网上出现“Linux expand_downwards()竞争条件漏洞、Open Solutions for Education openSIS SQL 注入漏洞（CNVD-2020-52193）”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 2152 个，与上周（4632 个）环比增加 54%。

# 主要内容



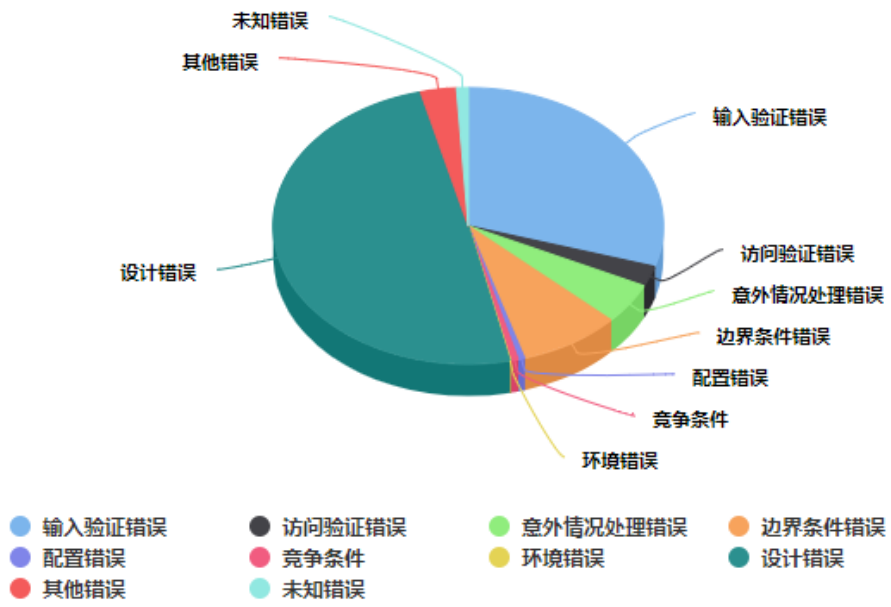
**注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。**

# 一、概述

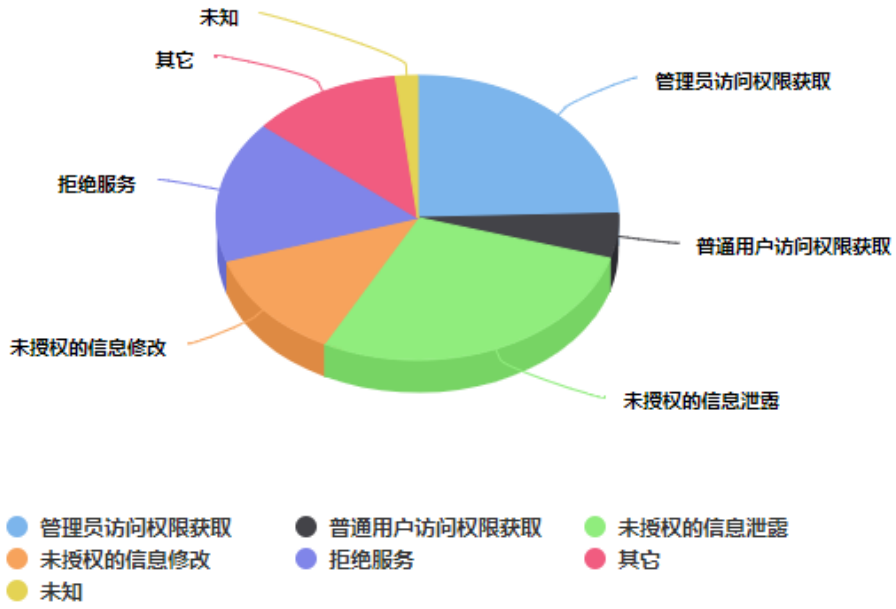
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 395 个，其中高危漏洞 94 个、中危漏洞 231 个、低危漏洞 70 个。漏洞平均分值为 5.43。本周收录的漏洞中，涉及 0day 漏洞 51 个（占 13%），其中互联网上出现“Linux expand_downwards()竞争条件漏洞、Open Solutions for Education openSIS SQL 注入漏洞（CNVD-2020-52193）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 2152 个，与上周（4632 个）环比增加 54%。

# 二、安全漏洞增长数量及种类分布情况

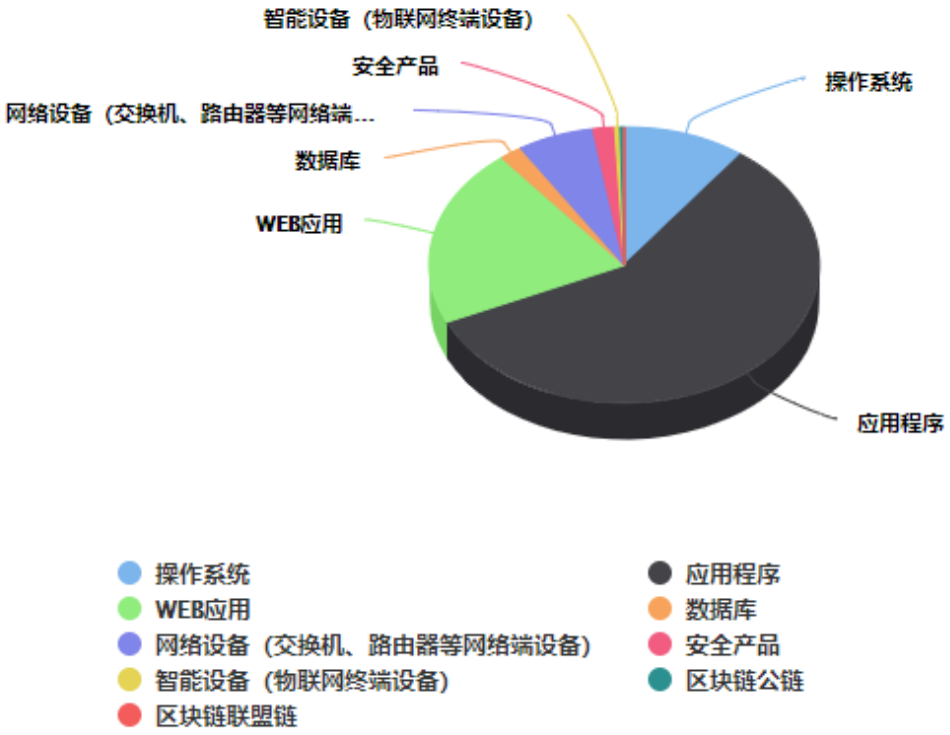
➢ **漏洞产生原因（2020 年 09 月 13 日—2020 年 09 月 27）**



## ➢ 漏洞引发的威胁（2020 年 09 月 13 日—2020 年 09 月 27）




## ➢ 漏洞影响对象类型（2020 年 09 月 13 日—2020 年 09 月 27）



# 三、安全产业动态

## ➢ 筑牢网络安全之基 保护人民群众信息安全

### ——新时代我国网络安全发展成就综述

以“网络安全为人民，网络安全靠人民”为主题的 2020 年国家网络安全宣传周将于 9 月 14 日至 20 日在全国范围内开展，注重提高全民网络安全意识和能力。

“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”习近平总书记高瞻远瞩的话语，为推动我国网络安全体系的建立，树立正确的网络安全观指明了方向。党的十八大以来，在中央网络安全和信息化领导小组领导下，我国不断完善网络安全工作顶层设计，有效治理网络空间乱象，为保卫人民群众信息安全筑牢防线，取得了一系列瞩目成就。


**网络安全“四梁八柱”基本确立**

进入新时代以来，法治思维贯穿于网信事业发展的始终，依法管网、依法办网、依法上网成为政府、企业和社会各界的共识。以《网络安全法》为核心的网络安全法律法规和政策标准体系基本形成，网络安全“四梁八柱”基本确立。

——体制机制确立。2014 年，中央网络安全和信息化领导小组成立，集中统一领导全国互联网工作。中央网信办统筹协调，各地网信机构逐渐建立，网络安全管理工作格局逐步成熟。

——战略先行、有法可依。2016 年 12 月，《国家网络空间安全战略》发布，确立了网络安全的战略目标、战略原则、战略任务；2017 年 6 月 1 日起，《网络安全法》正式施行，是我国网络安全领域首部基础性、框架性、综合性法律。

——应急响应能力提升。《国家网络安全事件应急预案》发布实施，网络安全应急响应和处置能力有效提升；发布《网络安全审查办法》，有效防范化解供应链网络安全风险；制定《云计算服务安全评估办法》，提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平。

——强化网络安全统一标准。对网络安全国家标准进行统一技术归口，统一组织申报、送审和报批，国家网络安全标准体系日益健全。截至目前，已发布个人信息安全规范等国家标准 263 项，正在研究制定 79 项，39 项国家标准和技术提案被国际标准化组织吸纳。……

为网络安全织密防护网，多措并举、多管齐下、多方参与。党的十八大以来，我国互联网治理能力的法治化、科学化水平不断提升。

**加强个人信息保护 构建清朗网上家园**

整治网络生态、保护个人信息安全，网络安全事业必须贯彻以人民为中心的发展思想，让人民群众在信息化发展中有更多获得感、幸福感和安全感。

近年来，我国多部门联动，在持续整治网络谣言、打击网络犯罪、整治违法违规“自媒体”等方面成效显著。2019 年，中央网信办、工信部、公安部、市场监管总局联合行动，在全国范围内开展 App 违法违规收集使用个人信息专项治理。

一年来，用户量大、与生活关系密切、问题反映集中的千余款 App 得到有效整改，260 款问题严重的 App 被约谈、曝光、下架；App 强制索权、超范围收集、账号注销难等问题明显改善，全社会关注和重视个人信息安全的氛围基本形成。

在法律层面，去年 11 月 1 日起实施的“两高”司法解释明确，网络平台拒不履行信息网络安全管理义务，具有泄露用户通信内容 500 条以上等 8 种情形的，可入罪追究刑事责任。

“00 后”作为第一代“网络原住民”，从小就接触各种各样的电子产品和网络内容，引导他们安全用网、保护他们的合法权益，对培养社会主义事业接班人至关重要。

由中央网信办发布的《儿童个人信息网络保护规定》已于 2019 年 10 月 1 日起施行，规定网络运营者应设置专门的儿童个人信息保护规则和用户协议，并明确任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的内容。

同时，开展“护苗行动”集中清理网上涉未成年人有害信息，通过给 App 设置“青少年

模式”上线防沉迷系统，为青少年健康成长营造清朗的网络空间。

自 2014 年起连续多年举办的国家网络安全宣传周，通过开展网络安全进社区、进校园、进军营等活动，有效提升了全民网络安全意识和防护技能，“网络安全为人民，网络安全靠人民”的理念深入人心。

**做大做强网安产业 培养更多网安人才**

近年来，我国网络安全产业已进入高速增长的全面发展时期。

2017 年底，工信部和北京市签署共同打造国家网络安全产业园区的协议，拉开网络安全产业创新发展序幕。2019 年底，工信部复函湖南省工信厅，支持湖南建设国家网络安全产业园区，成为继北京之后全国第二个获批国家网络安全产业园区的省市，目前网络安全产业规模突破 100 亿元，形成了涵盖基础硬件、应用系统、商业密码、信息安全服务、工业互联网安全等多领域的产业链条。

中国网络安全产业联盟统计数据显示，2019 年我国网络安全产业规模已达 480 亿元，同比增长 21.52%，预计未来几年产业整体市场依然会保持 20%左右的高速增长。

**网络空间的竞争，归根结底是人才竞争。**

我国高度重视网络安全人才培养，抢占国际战略竞争制高点。新时代以来，有关部门与时俱进，探索人才培养新思路、新机制，推动加快网络安全学科建设和人才培养。

2016 年 6 月，中央网信办、教育部等 6 部门联合印发《关于加强网络安全学科建设和人才培养的意见》，推动开展网络安全学科专业和院系建设，创新网络安全人才培养机制。

2017 年，中央网信办、教育部实施一流网络安全学院建设示范项目，西安电子科技大学、东南大学、北京航空航天大学等 11 所高校入选。

示范项目高校在相关部门和地方的支持下，出台特殊政策，加强院企合作，扩大招生规模，深入推进网络空间安全学院建设，网络安全人才培养取得明显进展。

位于武汉市东西湖区的国家网安基地规划面积 40 平方公里，国内网络安全企业 50 强中已有大约三分之二落户该地，联合武汉大学、华中科技大学等发展一批重点项目，网络安全人才、技术、产业融合发展的生态环境正逐步确立。（来源：新华社）

## ➢ 我国网络安全产业规模 2020 年将达 1702 亿元

近年来，基于政策扶持、需求扩张、应用升级等方面的驱动，我国网络安全产业发展进

入“快车道”。在第七届国家网络安全宣传周上，中国信息通信研究院发布的《中国网络安全产业白皮书（2020 年）》（以下简称《白皮书》）显示，2019 年我国网络安全产业规模达到 1563.59 亿元，同比增长 17.1%，企业发展态势总体良好，产品体系日益完善，技术创新高度活跃，综合实力显著增强，为保障国家网络空间安全发挥基石作用、作出重要贡献。

**产业规模快速增长政策环境不断向好**

《白皮书》显示，2019 年全球网络安全产业规模达到 1244.01 亿美元，预计 2020 年增长至 1278.27 亿美元。从增速上看，2019 年全球网络安全产业规模增速为 9.11%，是自 2014 年以来的最低值；受疫情影响，2020 年最新预期增速远低于 2019 年 12 月的预测值，约为 2.75%。

在全球网络安全产业规模增速放缓的情况下，我国网络安全产业规模却保持持续快速增长势头，2019 年我国网络安全产业规模达到 1563.59 亿元，较 2018 年增长 17.1%，预计 2020 年产业规模约为 1702 亿元，增速约为 8.85%。

近年来，我国网络安全相关政策布局不断提速，网络安全及相关政策密集出台，为产业发展营造了良好的政策环境。一方面，网络安全法律及配套政策密集落地，网络法制建设继续稳步推进。2020 年 1 月，《中华人民共和国密码法》正式施行，为我国商用密码技术和产业的发展开放平台。《个人信息保护法》《数据安全法》正在加快制定，《关键信息基础设施安全保护条例》已纳入国务院 2020 年立法工作计划。

另一方面，新兴领域政策举措密集落地。2020 年以来，工业和信息化部会同有关部门印发《国家车联网产业标准体系建设指南（车辆智能管理）》《关于推动 5G 加快发展的通知》《关于推动工业互联网加快发展的通知》等政策指引，聚焦新一代前瞻性技术创新，加快完

善新兴技术的网络安全产品和服务支撑体系。

**产品体系逐步完善企业发展总体向好**

随着网络安全行业的迅猛发展，现有网络安全产品和服务基本从传统网络安全领域延伸到了云、大数据、物联网、工业互联网、5G 和移动互联网等不同的应用场景。基于安全产品和服务的应用场景、保护对象和安全能力，我国网络安全产品和服务已覆盖基础安全、基础技术、安全系统、安全服务等多个维度，网络安全产品体系日益完备，产业活力日益增强。

与此同时，《白皮书》也指出，随着我国网络安全产业近年来高速增长，目前，产业链已经逐步完善，供需关系也相对明朗。网络安全产品和服务整体发展较为稳定，技术布局相对完整。然而在产业链上游，我国在芯片、操作系统、数据库等基础硬件和软件系统方面的技术基础仍然较为薄弱。

此外，《白皮书》显示，我国网络安全企业发展总体良好。在营收规模方面，上市企业营收规模总体呈稳定增长态势。10 家上市网络安全企业 2019 年平均营收规模为 16.82 亿元，较 2018 年的 13.23 亿元增长了 27.08%。在营业收入构成方面，10 家上市网络安全企业的营业收入主要由网络安全软硬件产品及服务组成，其中，网络安全软硬件产品营收占比较高，平均占比达到企业营业收入的七成。尽管今年以来，新冠肺炎疫情对网络安全产业发展造成一定冲击，但云化、远程化等需求激增，为产业带来商机。随着云化、远程化办公需求的增长，疫情防控支撑系统、在线教育、远程办公、远程会议等系统和应用大规模推出，网络安全产品和解决方案需求相应增加，智能化、远程化的安全运维需求也逐步提升。

《白皮书》对我国网络安全产业的前景进行了展望。在我国对技术创新支持力度不断加大的大背景下，产业链各环节相关主体将持续加大在关键核心技术方面的研发投入，安全厂商将与产业链各环节进行深度融合。而随着国家级产业园区建设的逐步提速，政策、技术、产业和人才等要素之间互动紧密，为产业合作构建良好的生态体系。与此同时，通过开展在线的网络安全培训、竞赛，线上或线上与线下结合的网络安全会议等方式，为网络安全人才培养找到了新的路径。此外，新基建与信息化建设的持续推进，也将对网络安全保障提出更高要求，从而进一步推动相关支撑政策加快落地。（来源：中国信息产业网）

- **《中国网络安全产业白皮书 2020》全文**
- http://www.caict.ac.cn/kxyj/qwfb/bps/202009/P020200916482039993423.pdf

## ➢ 从国际标准 ISO/IEC27701 视角评析 2020 版《个人信息安全规范》

2020 年 3 月 6 日，全国信息安全标准化技术委员会归口的 GB/T35273-2020《信息安全技术个人信息安全规范》国家标准正式发布，代替 GB/T35273-2017。新版《个人信息安全规范》在“用户画像的使用限制”、“第三方接入管理”、“个人信息安全工程”等方面扩展了原有标准的内容，并对“征得授权同意的例外”、“个人信息主体注销账户”等方面进行了一定的修改。

2019 年 8 月 6 日，国际标准化组织(ISO)和国际电工委员会(IEC)发布了 ISO/IEC27701（安全技术-针对 ISO/IEC27001 和 ISO/IEC27002 在隐私信息管理的扩展-要求和指南），对建立、实施、维护和持续改进隐私信息管理系统（PIMS）的各项要求做出了规定。在个人可识别信息（PII）处理情境中的隐私保护是一种社会需求，也是全世界专门立法和/或监管的主题。ISO/IEC27701 是第一部 PIMS 国际标准，为 PII 控制者和 PII 处理者如何做好 PII 保护和控制指明了方向，且可能会被用于证明包括《通用数据保护条例》(EU)2016/679(GDPR)在内的全球隐私合规实践。


GB/T35273-2020《个人信息安全规范》和 ISO/IEC27701 的发布时间只差半年，可以说两者在国内和国际上均引起了广泛的关注。本文从 ISO/IEC27701 国际标准角度，解读我国国家标准 GB/T35273-2020《个人信息安全规范》在个人信息保护方面与国际标准的耦合性。

**一、《个人信息安全规范》多维度全方位保护个人信息主体的权利**

不同于 ISO/IEC27018、ISO/IEC29151 的控制措施全都属于“指南 should”，ISO/IEC27701 同时扩展了 ISO/IEC27001 和 ISO/IEC27002 中有关信息安全的控制要求，变成了“要求 shall+指南 should”模式，成为第一部扩充了信息安全管理体系（ISMS）的隐私保护“认证”性质

的标准，而同时又整合了“指南”性质的条款，让其具有“双重身份”。《个人信息安全规范》制定的目的是“规范”个人信息控制者在收集、存储、使用、共享、转让、公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄漏等乱象，最大程度地保障个人的合法权益和社会公共利益。相较于 ISO/IEC27701，《个人信息安全规范》“要求”的属性更加明显，也在个人信息主体权利保障层面提出了更加具体、明确的规定，比如：

（1）收集规则-多项业务功能的自主选择同意。《个人信息安全规范》5.3a)不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求。此处的“业务功能”可以理解为“服务类型”。针对当下 App 集合多个服务类型的现状，《个人信息安全规范》针对性的提出“区分业务功能“，不得捆绑个人信息来强迫用户接受的要求，并要求同时提供关闭或退出特定业务功能的方式，相比 ISO/IEC27701 中关于具体征得用户同意的要求要更加具体和有指导性。

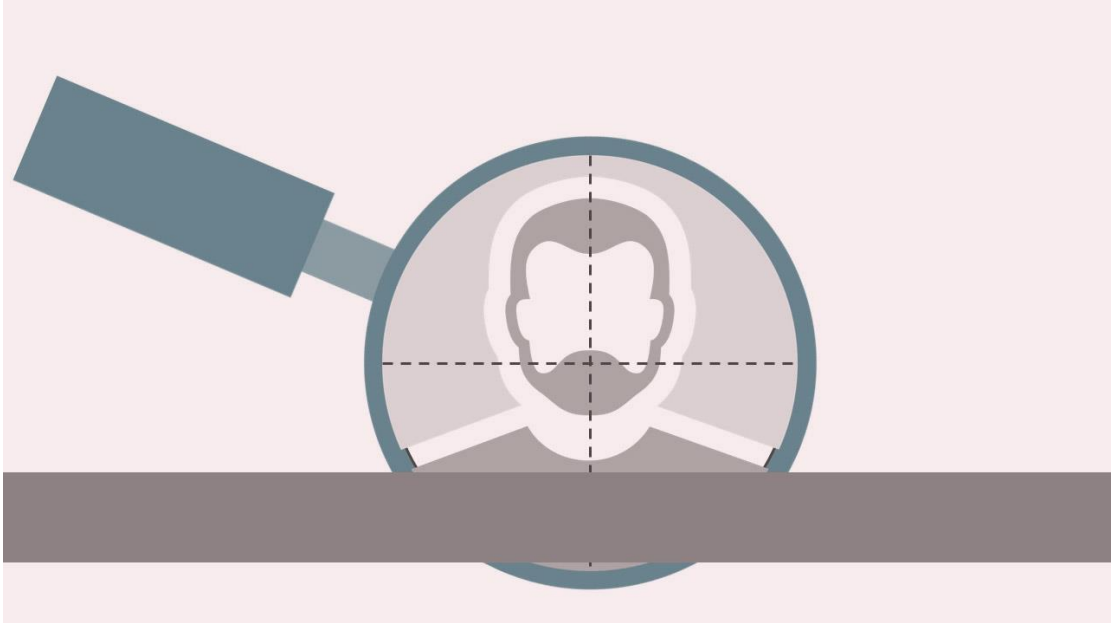
（2）保存规则-个人控制者停止运营。ISO/IEC27701 在 7.4.7 组织应制定并维护保留信息的留存时间规划，并考虑到 PII 留存期限不得超过必要的时间。PII 留存时间规划应考虑法律、法规和业务要求。《个人信息安全规范》更加明确的指出个人控制者停止运营，是个人信息不得留存的场景之一，并把这种场景单独列出，以防止个人信息倒卖、黑灰产运作等不良个人信息用途的发生。

（3）使用规则-基于不同业务目的所收集个人信息的汇聚融合。《个人信息安全规范》7.6b)应根据汇聚融合后个人信息所用于的目的，开展个人信息安全影响评估，采取有效的个人信息保护措施。大数据时代下，各个大平台厂商可能会收购、并购一些小的不同业务类型的企业，它们收集的个人信息类型也不完全相同；有些还可能会涉及线上平台与线下门店个人信息的汇聚融合。这些汇聚融合后的个人信息如何使用，是否会做大数据分析，相比于单个已经征得用户同意的个人信息对个人信息主体的影响是不一样的。《个人信息安全规范》对于基于不同业务目的所收集个人信息的汇聚融合做出了规定，ISO/IEC27701 对此没有进行具体展开。

**二、《个人信息安全规范》紧密结合了中国互联网行业发展的实情，秉承了行业规制与个人信息保护平衡发展的思路**

（1）个性化展示的使用区分了不同场景的要求。电子商务服务有更大的需求根据消费者的兴趣爱好、消费习惯向个人信息主体提供商品或服务搜索结果的个性化展示，消费者群体对个性化展示也更加易于接受，因此《个人信息安全规范》提出了“提供不针对其个人特征选项”的要求。对于推送新闻信息服务，个人信息主体的需求小，主观更加不希望自己的

阅读偏好被知晓，因此《个人信息安全规范》提出了“简单直观退出或关闭个性化展示模式的选项”以及“向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项”。对于标签、画像维度等的自主控制机制，考虑到当下的行业发展水平、技术能力，以及实现的成本情况，《个人信息安全规范》采用鼓励引导的方式，提倡企业“宜”保障个人信息主体调控个性化展示相关性程度的能力。我国个人信息保护总体情况较为复杂，涵盖范围大、涉及环节多，一方面要提升能力，解决公民关切的问题，另一方面也要考虑当前技术和监管的能力限制。个性化展示的使用要求兼顾了行业的发展现状以及用户对个人信息保护在不同行业领域的需求来区分，是对行业规制与个人信息保护的平衡发展的有益探索。相比而言，ISO/IEC27701 在个性化展示方面没有进行具体展开。



（2）总体规范与不同行业标准指南相结合。ISO/IEC27701 采用的是“要求+指南”的模式，既扩充了信息安全管理体系（ISMS）的隐私保护“认证”性质的标准，而同时又整合了“指南”性质的条款，因此在 ISO/IEC27701 的“指南”的条款较多，虽然给出了一些具体的指导，但是国际标准需要兼顾通用性，无法囊括各个行业的特点，也使得在行业针对性方面略显不足，。《个人信息安全规范》旨在规范各行业在个人信息处理过程中的相关行为，给出了原则和方向性的规范。同时，通过制定指南性质的国家标准来作为《个人信息安全规范》的配套标准，进一步将《个人信息安全规范》的要求在各个具体行业落地。全国信息安全标准化技术委员会于 2020 年 3 月 7 日发布的“《关于印发<2020 年网络安全国家标准项目申报>指南》的通知”中指出重点标准制定项目“拟支持网络平台数据安全（网络预约汽车、网络支付、网上购物、即时通信、快递物流、网路广播等）”。规范标准与指南标准相结合的

方式更加契合中国互联网行业快速发展的现状，个人信息保护方式在具体行业领域的落地更加具有针对性和可操作性。

**三、《个人信息安全规范》与国际接轨，总体要求与 ISO/IEC27701 一致**

（1）个人敏感信息的重要性。ISO/IEC27701 的特殊类型 PII 对应《个人信息安全规范》中的个人敏感信息。ISO/IEC277017.2.2 中提到特殊类别 PII 的使用应进行更严格的控制，也指出特殊类别的 PII 的定义可以依据 PII 的性质（如医疗健康信息）或相关 PII 主体（如与儿童有关的 PII）。属于特殊类别 PII 的分类可能因不同地区而异，也可能因适用于不同类型业务的监管制度而异，因此组织需要清楚适用于 PII 处理的分类。ISO/IEC27701 对特殊类型的 PII 注意到了要根据不同地域以及不同类型业务的监管制度来考虑更加严格的保护，但对于保护的方式并没有详细规定。《个人信息安全规范》对个人敏感信息在传输和存储方面特别提出对个人信息控制者的要求。传输和存储个人敏感信息时，应采用加密等安全措施。对于个人生物识别信息，提出了应与个人身份信息分开存储、原则上不应存储原始个人生物识别信息(如样本、图像等)的明确要求，把个人生物识别信息提高到了更加突出的保护地位。

（2）个人信息处理目的。ISO/IEC277017.2.1 与 7.2.3 指出组织应确保 PII 主体了解处理其 PII 的目的；组织除非有其他合法理由，否则处理 PII 都需要征得同意，并要将处理目的和如何获得同意的相关信息关联起来。ISO/IEC27701 注意到了征得同意的时机与处理目的的关联性。相比，《个人信息安全规范》更加明确的指出，使用个人信息时不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围，因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。《个人信息安全规范》的规定更加明确征得同意的时机与业务目的的关联性关系，给企业更强的指导。

总的来看，相比于 ISO/IEC27701，《个人信息安全规范》更注重以国内个人信息保护领域的重点问题为导向，延续国内法律法规关于个人信息保护的规定和管理原则。ISO/IEC27701 则更注重于国际通用性，它对当下世界各国法律制度中有关个人信息保护的主要要求进行了实践层面的指导。两者虽然侧重点有所不同，但对于在个人信息保护方面所提的要求体现出来的方向性、前瞻性均值得参考。（来源：中国电子技术标准化研究院）

## ➢ 人才队伍建设是国家网络安全事业的关键

随着信息技术的飞速发展与网络边界的逐渐模糊，关键信息基础设施、重要数据和个人

隐私都面临新的威胁和风险，网络安全逐步呈现出“以人为本、以数据为中心”的新特点。其中，“以人为本”意味着，要筑牢网络安全新防线，教育是基础，人才是关键。

**一、我国网络安全人才队伍建设成效显著**

近些年，党中央、国务院高度重视信息安全学科、专业建设和人才培养工作，围绕网络安全人才队伍建设作出一系列重要战略部署：

2007 年，教育部成立高等学校信息安全类专业教学指导委员会，专门负责对我国高等学校信息安全类专业建设进行指导。

2012 年，国家出台《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23 号），大力支持信息安全学科师资队伍、专业院系、学科体系、重点实验室建设，为高校信息安全学科专业建设给予政策支持。

2014 年，中央成立网络安全与信息化领导小组，习近平总书记亲自担任组长，着力加强网络信息安全人才队伍建设，把造就世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队作为国家的战略任务来抓，切实把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍，将网络安全人才队伍建设提升到一个前所未有的高度。

2015 年，为加快网络安全高层次人才培养，国务院学位委员会决定在工学门类下增设网络空间安全一级学科，学科代码为“0839”，授予“工学”学位。2016 年，国务院学位委员会正式下发《国务院学位委员会关于同意增列网络空间安全一级学科博士学位授权点的通知》，清华大学、北京交通大学、山东大学等 27 所高校获批增列网络空间安全一级学科博士学位授权点，解放军电子工程学院和空军工程大学获批对应调整网络空间安全一级学科博士

学位授权点，共 29 所高校获得首批网络空间安全一级学科博士学位授予资格。

2016 年，中央网信办联合相关部门出台《关于加强网络安全学科建设和人才培养的意见》（中网办〔2016〕4 号），明确了网络安全学科建设和人才培养方向。同年，中国互联网发展基金会成立了网络安全专项基金，专门用于人才培养和激励。2016-2019 年，网络安全专项基金按程序公开评选出 1 名网络安全杰出人才、40 名网络安全优秀人才、38 名网络安全优秀教师、301 名优秀本科生和 303 名优秀研究生、6 本网络安全优秀教材、5 项优秀网络安全标准。根据偏远地区实际情况，设立新疆和西藏网络安全人才奖，各评选出 5 名网络安全优秀人才，其中含 1 名突出贡献奖。专项基金为上述获奖者发放免税奖金。其中，三届网络安全人才奖和四届优秀教师奖获奖代表在国家网络安全宣传周上受到表彰。此外，网络安全专项基金还支持了网络安全人才培养基地建设、网络安全万人培训、网络安全宣传周及其他相关工作，对于加快网络安全人才培养、吸引更多人才投身网络安全事业发挥了重要作用。

2017 年，中央网信办、教育部印发《一流网络安全学院建设示范项目管理办法》，明确我国将在 2017 年-2027 年期间实施一流网络安全学院建设示范项目，形成 4-6 所世界一流的网络安全学院。根据管理办法，评选出西安电子科技大学、东南大学、武汉大学、北京航空航天大学、四川大学、中国科学技术大学、战略支援部队信息工程大学为首批一流网络安全学院建设示范项目高校。2019 年，华中科技大学、北京邮电大学、上海交通大学、山东大学入选第二批一流网络安全学院建设示范项目高校。两批一流网络安全学院建设示范项目高校均在国家网络安全宣传周上由中央领导同志亲自授牌，受到广泛关注。

总体来看，近年来我国网络安全人才队伍建设取得显著进展，人才队伍规模不断壮大，人才队伍质量明显提升。

**二、当前网络安全人才队伍建设面临的主要问题**

尽管如此，也必须看到我国网络安全人才队伍建设还存在一些突出问题：

一是网络安全人才总量不足。高等院校毕业生是我国网络安全人才的主要来源。目前，我国网络安全人才年培养规模在 3 万人左右。据专业机构测算，我国网络安全从业人员需求数量为：2020 年为 1550026 人、2027 年为 3267099 人、2035 年为 7841866 人。当前培养的人才数量远远不能适应社会发展对网络安全人才的需求。

二是缺乏世界一流的网络安全学院。没有一流的网络安全学院，很难培养出世界一流的网络安全人才。我国目前已有的网络安全学院，距离国际一流水平仍有较大差距，这已成为我国网络安全人才培养乃至整个网络安全工作的突出问题。

三是教育、技术、产业良性生态还要健全完善。近年来，有关部门从人才培养、技术创新、产业发展等环节加大对网络安全的支持力度，但很多工作往往是各有各的目标，各有独自考核标准，自成体系，没有从产业链、生态链上进行统筹和设计，难以形成系统性能力。

四是企业作用没有得到充分发挥。网络安全是实操性和技能性非常强的行业，企业处于网络安全一线，在网络安全人才培养和培训方面具有得天独厚的优势。但是多年来，国家的网络安全项目往往是政府出题目、出资金、管检查、管验收，通过政府验收已经成为企业承担项目的最重要目标，客观上形成了企业围着政府转的局面，企业在很多方面的积极性创造性没有得到充分发挥。

五是社会大众网络安全意识和技能仍需提高。随着互联网的普及，人们对网络依赖程度越来越高，但是对个人信息的保护意识还没跟上，特别是青少年、老年人的网络安全技能和应用安全意识亟待加强。

**三、加强网络安全人才队伍建设的几个方向**

一是确保合理的网络安全学院数量和规模。鼓励高等院校通过整合、新建等方式成立网络安全学院，保持全国网络安全学院数量和规模适量增长，增加网络安全学科专业招生指标和生均费用，为培养更多数量的学生提供基础条件。

二是推动一流网络安全学院建设。探索网络安全人才培养新思路、新体制、新机制，强化网络安全师资队伍建设，改革创新，通过开展一流网络安全学院建设示范项目等多种方式，推动我国网络安全学院向世界一流的方向发展。

三是推动高等院校与企业行业协同创新。鼓励企业深度参与高等院校网络安全人才培养工作，推动高等院校与科研院所、行业企业协同育人。鼓励学生在校阶段积极参与创新创业，形成网络安全人才培养、技术创新、产业发展的良性生态。

四是加强全民网络安全意识与技能培养。办好国家网络安全宣传周活动，面向大众宣传普及网络安全知识。网络安全教育从孩子抓起，加强青少年网络素养教育。同时加强针对老年人的网络安全知识推广和普及。（来源：网信中国）

# 四、政府之声

## ➢ 商务部发布《不可靠实体清单规定》

2020 年 9 月 19 日，中华人民共和国商务部发布令二〇二〇年第 4 号《不可靠实体清单规定》已经国务院批准，现予公布，自公布之日起施行。


**以下为全文：**

第一条 为了维护国家主权、安全、发展利益，维护公平、自由的国际经贸秩序，保护中国企业、其他组织或者个人的合法权益，根据《中华人民共和国对外贸易法》、《中华人民共和国国家安全法》等有关法律，制定本规定。

第二条 国家建立不可靠实体清单制度，对外国实体在国际经贸及相关活动中的下列行为采取相应措施：

（一）危害中国国家主权、安全、发展利益；

（二）违反正常的市场交易原则，中断与中国企业、其他组织或者个人的正常交易，或者对中国企业、其他组织或者个人采取歧视性措施，严重损害中国企业、其他组织或者个人合法权益。

本规定所称外国实体，包括外国企业、其他组织或者个人。

第三条 中国政府坚持独立自主的对外政策，坚持互相尊重主权、互不干涉内政和平等

互利等国际关系基本准则，反对单边主义和保护主义，坚决维护国家核心利益，维护多边贸易体制，推动建设开放型世界经济。

第四条 国家建立中央国家机关有关部门参加的工作机制（以下简称工作机制），负责不可靠实体清单制度的组织实施。工作机制办公室设在国务院商务主管部门。

第五条 工作机制依职权或者根据有关方面的建议、举报，决定是否对有关外国实体的行为进行调查；决定进行调查的，予以公告。

第六条 工作机制对有关外国实体的行为进行调查，可以采取询问有关当事人、查阅或者复制相关文件、资料以及其他必要的方式。调查期间，有关外国实体可以陈述、申辩。

工作机制可以根据实际情况决定中止或者终止调查；中止调查决定所依据的事实发生重大变化的，可以恢复调查。

第七条 工作机制根据调查结果，综合考虑以下因素，作出是否将有关外国实体列入不可靠实体清单的决定，并予以公告：

（一）对中国国家主权、安全、发展利益的危害程度；

（二）对中国企业、其他组织或者个人合法权益的损害程度；

（三）是否符合国际通行经贸规则；

（四）其他应当考虑的因素。

第八条 有关外国实体的行为事实清楚的，工作机制可以直接综合考虑本规定第七条规定的因素，作出是否将其列入不可靠实体清单的决定；决定列入的，予以公告。

第九条 将有关外国实体列入不可靠实体清单的公告中可以提示与该外国实体进行交易的风险，并可以根据实际情况，明确该外国实体改正其行为的期限。

第十条 对列入不可靠实体清单的外国实体，工作机制根据实际情况，可以决定采取下列一项或者多项措施（以下称处理措施），并予以公告：

（一）限制或者禁止其从事与中国有关的进出口活动；

（二）限制或者禁止其在中国境内投资；

（三）限制或者禁止其相关人员、交通运输工具等入境；

（四）限制或者取消其相关人员在中国境内工作许可、停留或者居留资格；

（五）根据情节轻重给予相应数额的罚款；

（六）其他必要的措施。

前款规定的处理措施，由有关部门按照职责分工依法实施，其他有关单位和个人应当配合实施。

第十一条 将有关外国实体列入不可靠实体清单的公告中明确有关外国实体改正期限的，在期限内不对其采取本规定第十条规定的处理措施；有关外国实体逾期不改正其行为的，依照本规定第十条的规定对其采取处理措施。

第十二条 有关外国实体被限制或者禁止从事与中国有关的进出口活动，中国企业、其他组织或者个人在特殊情况下确需与该外国实体进行交易的，应当向工作机制办公室提出申请，经同意可以与该外国实体进行相应的交易。

第十三条 工作机制根据实际情况，可以决定将有关外国实体移出不可靠实体清单；有关外国实体在公告明确的改正期限内改正其行为并采取措施消除行为后果的，工作机制应当作出决定，将其移出不可靠实体清单。

有关外国实体可以申请将其移出不可靠实体清单，工作机制根据实际情况决定是否将其移出。将有关外国实体移出不可靠实体清单的决定应当公告；自公告发布之日起，依照本规定第十条规定采取的处理措施停止实施。

第十四条 本规定自公布之日起施行。（来源：中华人民共和国商务部）

## ➢ 中国人民银行发布《中国人民银行金融消费者权益保护实施办法》

2020 年 9 月 15 日，为加快建立完善有利于保护金融消费者权益的机制，保护金融消费者长远和根本利益，人民银行发布《中国人民银行金融消费者权益保护实施办法》（中国人民银行令〔2020〕第 5 号，以下简称《办法》）,并由有关部门负责人就相关问题回答了记者提问。

**一、《办法》出台的背景是什么？**

为贯彻党的十九大和十九届二中、三中、四中全会精神，进一步落实习近平总书记在中共中央政治局第十三次集体学习时的重要指示，根据党中央、国务院《关于新时代加快完善社会主义市场经济体制的意见》中提出“要建立健全金融消费者保护基本制度”的决策部署，加快建立完善有利于保护金融消费者权益的金融监管体系，保护金融消费者长远和根本利益，中国人民银行金融消费权益保护局在《中国人民银行金融消费者权益保护实施办法》（银发〔2016〕314 号文印发）的基础上，结合新需求、新情况、新问题和人民银行新“三定”方案，修订、增补相关条款后，将《中国人民银行金融消费者权益保护实施办法》升格为部门规章，以人民银行令形式发布实施。

**二、制定《办法》的目的是什么？**

一是坚持金融监管问题导向的客观需要，把主动防范化解系统性金融风险放在更加重要的位置，发挥好金融消费者权益保护工作金融领域“减震器”和“舒压阀”的基础性作用。二是保护金融消费者长远和根本利益的现实需要，提升保护金融消费者权益专门文件的法律效力位阶，进一步规范银行、支付机构的经营行为。三是完善人民银行金融消费者权益保护法律体系的履职需要，更好地履行新“三定”方案赋予的职责。四是打击侵犯金融消费者合法权益的违法违规行为、合理提升违法违规成本的迫切需要，解决金融领域违法违规成本过低的问题。五是更好回应基层呼声和社会关切的实际需要，对“两会”全国人大代表、政协委员及金融消费者、金融机构、人民银行分支机构等提出要加快金融消费者权益保护立法进程的期望作出回应。

**三、《办法》主要解决了哪些问题？**

一是细化、落实上位法要求的问题。金融消费者权益保护机制与一般消费领域的消费者权益保护机制存在差异，《中华人民共和国消费者权益保护法》中的相关内容在金融领域应当进行更为细致的规定。二是人民银行履职依据的问题。原规范性文件效力层级较低，结合新“三定”方案提升《办法》的法律效力层级将更有利于人民银行金融消费者权益保护工作的开展。三是原有规定的适应性问题。原规范性文件实施三年多以来，金融消费领域出现了许多新情况、新问题，党中央、国务院对于金融消费者权益保护也提出了新的要求，因此，需要在原有规范性文件基础上出台部门规章，及时调整监管手段和策略。四是合理提升违法违规成本的问题。原规范性文件没有配置相应罚则，对侵害金融消费者合法权益的违法违规行为震慑力有限。《办法》专章设置了法律责任，解决了金融消费者权益保护领域违法违规成本较低的问题。

**四、《办法》主要从哪些方面对金融消费者合法权益进行保护？**

《办法》坚持问题导向，对实践中反映强烈的问题，尤其是与金融消费者息息相关的八项权利进行了重点突出、有的放矢的规范。例如，规章新增了受尊重权的内容；为适应金融市场发展，在公平交易权与自主选择权方面提出更为明确的要求；吸收了“一行两会一局”联合发布的《关于进一步规范金融营销宣传行为的通知》的相关内容，对营销宣传进行了针对性规范；在延续原有的金融信息保护专章的基础上，以实现保护金融消费者信息安全权为目的，从信息收集、披露和告知、使用、管理、存储与保密等方面进行了优化。（来源：中国人民银行办公厅）

- **《中国人民银行金融消费者权益保护实施办法》**
- **全文：**http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4098472/index.html

## ➢ 人社部发布《网络招聘服务管理规定（征求意见稿）》

2020 年 9 月 17 日，为了规范网络招聘服务，进一步促进网络招聘服务业态健康有序发展，发挥其在促进就业方面的作用，人力资源和社会保障部研究起草了《网络招聘服务管理规定（征求意见稿）》（简称“征求意见稿”），近日向社会公开征求意见。


征求意见稿明确了从事网络招聘服务活动应具备的资质条件，包括取得营业执照、取得人力资源服务许可证和电信业务经营许可证等。

征求意见稿还围绕招聘信息的真实性、合法性和安全性，明确招聘信息审核规范、网络

安全规范、信息保护规范、收费管理等；主要规定了网络招聘服务机构、用人单位和劳动者在网络招聘活动中的权利和义务；明确网络招聘服务机构应当履行资质公开、信息核查、网络安全、建立信息安全保护制度等义务。

同时，征求意见稿对用人单位招聘、求职者求职过程中发布合法真实信息进行了规定，其中明确，用人单位向网络招聘服务机构提供的单位基本情况、招聘人数、招聘条件、用工类型、工作内容、工作条件、工作地点、劳动报酬等招聘信息，应当合法、真实，不得含有民族、种族、性别、宗教信仰等方面的歧视性内容。

征求意见稿还强调，网络招聘服务机构应当对提供的网络招聘服务收费实行明码标价，公布其服务项目、服务内容、计费方式、收费标准、收费对象等内容。网络招聘服务机构不得向劳动者收取押金，不得以欺诈、暴力、胁迫或者其他不正当手段，牟取不正当利益。

如果违规向劳动者收取押金的，由人力资源和社会保障行政部门责令限期退还劳动者，并以每人 500 元以上 2000 元以下的标准处以罚款。

违规牟取不正当利益的，由人力资源和社会保障行政部门责令改正；有违法所得的，没收违法所得；拒不改正的，处 1 万元以上 5 万元以下的罚款；情节严重的，吊销人力资源服务许可证。（来源：中华人民共和国人力资源和社会保障部）

- **《网络招聘服务管理规定（征求意见稿）》公开征求意见的通知全文：**
- http://www.mohrss.gov.cn/SYrlzyhshbzb/zcfg/SYzhengqiuyijian/202009/t20200917_386032.html

## ➢ 中办国办印发《关于加快推进媒体深度融合发展的意见》

2020 年 9 月 26，近日，中共中央办公厅、国务院办公厅印发了《关于加快推进媒体深度融合发展的意见》，并发出通知，要求各地各部门结合实际认真贯彻落实。

《意见》从重要意义、目标任务、工作原则三个方面明确了媒体深度融合发展的总体要求，要求深刻认识全媒体时代推进这项工作的重要性紧迫性，坚持正能量是总要求、管得住是硬道理、用得好是真本事，坚持正确方向，坚持一体发展，坚持移动优先，坚持科学布局，坚持改革创新，推动传统媒体和新兴媒体在体制机制、政策措施、流程管理、人才技术等方面加快融合步伐，尽快建成一批具有强大影响力和竞争力的新型主流媒体，逐步构建网上网下一体、内宣外宣联动的主流舆论格局，建立以内容建设为根本、先进技术为支撑、创新管

理为保障的全媒体传播体系。

《意见》指出，要推动主力军全面挺进主战场，以互联网思维优化资源配置，把更多优质内容、先进技术、专业人才、项目资金向互联网主阵地汇集、向移动端倾斜，让分散在网下的力量尽快进军网上、深入网上，做大做强网络平台，占领新兴传播阵地。

《意见》指出，要走好全媒体时代群众路线，坚持以人民为中心的工作导向，坚持贴近群众服务群众，创新实践党的群众路线，大兴“开门办报”之风，把党的优良传统和新技术新手段结合起来，强化媒体与受众的连接，以开放平台吸引广大用户参与信息生产传播，生产群众更喜爱的内容，建构群众离不开的渠道。

《意见》指出，要以先进技术引领驱动融合发展，用好 5G、大数据、云计算、物联网、区块链、人工智能等信息技术革命成果，加强新技术在新闻传播领域的前瞻性研究和应用，推动关键核心技术自主创新。要推进内容生产供给侧结构性改革，更加注重网络内容建设，始终保持内容定力，专注内容质量，扩大优质内容产能，创新内容表现形式，提升内容传播效果。要深化主流媒体体制机制改革，建立适应全媒体生产传播的一体化组织架构，构建新型采编流程，形成集约高效的内容生产体系和传播链条。要发挥市场机制作用，增强主流媒体的市场竞争意识和能力，探索建立“新闻+政务服务商务”的运营模式，创新媒体投融资政策，增强自我造血机能。

《意见》指出，要按照资源集约、结构合理、差异发展、协同高效的原则，完善中央媒体、省级媒体、市级媒体和县级融媒体中心四级融合发展布局。努力打造全媒体对外传播格局，讲好中国故事，传播中华文化。

《意见》强调，要大力培养全媒体人才，实行更加积极、开放、有效的人才引进政策，提高主流媒体人才吸引力和竞争力。要优化人才队伍结构，把更多熟悉新媒体的中青年优秀人才充实到关键岗位，充分释放人才活力。

《意见》强调，各级党委和政府要强化资金保障，加强政策支持，形成政策保障体系，支持媒体深度融合发展。要强化党的领导，把推进媒体深度融合发展作为本地区本部门本单位落实意识形态工作责任制的重要内容。要加强评估考核，加强督促检查，推动媒体深度融合发展各项任务落到实处。（来源：新华社）

# 五、本期重要漏洞实例

## ➢ Linux kernel 权限控制漏洞

**发布日期：**2020-09-16
**更新日期：**2020-09-16
**受影响系统：**Linux kernel 5.8.9
**描述：**

---

CVE(CAN) ID: CVE-2020-25284
Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。Linux kernel 5.8.9 中存在权限控制漏洞。该漏洞源于 driver /block/ rbdc 中的 rbd 块设备驱动程序使用了不完整的权限检查来访问 rbd 设备。攻击者可利用该漏洞提升权限。
**建议：**

---

厂商补丁：
Linux
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f44d04e696feaf13d192d942c4f14ad2e117065a

## ➢ Microsoft Windows Jet Database Engine 远程代码执行漏洞

**发布日期：**2020-09-15
**更新日期：**2020-09-15
**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 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
Microsoft Windows Server 2004
Microsoft Windows 10 2004
**描述：**

---

CVE(CAN) ID: CVE-2020-1557
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。
Microsoft Windows Jet Database Engine 存在远程代码执行漏洞，该漏洞源于 Windows Jet 数据库引擎未能正确处理内存中的对象，攻击者可通过特制文件利用该漏洞在目标系统上执行任意代码。
**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/en-US/security-guidance/advisory/CVE-2020-1557

## ➢ Apache Syncope 远程代码执行漏洞

**发布日期：**2020-09-17
**更新日期：**2020-09-17
**受影响系统：**
Apache Syncope 2.1.*;<2.1.7
**描述：**

---

CVE(CAN) ID: CVE-2020-11977
Apache Syncope 是美国阿帕奇（Apache）基金会的一套用于企业环境中的开源数字身份管理系统。该系统支持身份管理、角色配置等。
Apache Syncope 2.1.7 之前的 2.1.x 中存在安全漏洞。攻击者可利用该漏洞执行恶意操作，包括但不限于文件读取、文件写入和代码执行。
**建议：**

---

厂商补丁：
Apache
厂商已发布了漏洞修复程序，请及时关注更新：
https://syncope.apache.org/security#CVE-2020-11977:_Remote_Code_Execution_via_Flowable_workflow_definition

## ➢ Trend Micro Apex One 权限提升漏洞

**发布日期：**2020-09-16
**更新日期：**2020-09-16
**受影响系统：**
Trend Micro Apex One
**描述：**

---

CVE(CAN) ID: CVE-2020-24559
Trend Micro Apex One 是一个端点防护解决方案，可提供最广泛的防护功能，包括高准度机器学习与进阶勒索病毒防护。
Trend Micro Apex One 中的 ApexOne Security Agent 存在权限提升漏洞。攻击者可通过创建硬链接而滥用服务来覆盖所选文件的内容，从而可利用该漏洞提升权限并在 root 用户的上下文中执行代码。
**建议：**

---

厂商补丁：
趋势科技
厂商已发布了漏洞修复程序，请及时关注更新：
https://success.trendmicro.com/solution/000263632

# 六、本期网络安全事件

## ➢ 雷蛇为意外泄露 10 万余账户个人信息向所有用户致歉

2020 年 9 月 15 日，网络安全顾问 Volodymyr Diachenko 在领英网站发布的一份报告（现已删除）显示，自 8 月 18 日以来，约有 10 万个雷蛇账户的个人数据被泄露。Diachenko 表示，他立即通知了雷蛇这个漏洞，但是非专业技术人员处理了三个星期也没能解决问题，直到合适的技术人员在 9 月 9 日才真正将其解决。


**雷蛇官方向 PC Gamer 网站证实了 Diachenko 的报告，并发表了以下声明：**

“一位安全研究员发现了我们服务器的错误配置并告知了我们，这个漏洞可能会暴露订单细节、客户联系方式和物流信息。信用卡号或密码等敏感数据未被泄露。在该故障被公开之前，漏洞在 9 月 9 日已被修复。

我们对自己的疏忽深表歉意，并已采取一切必要措施解决问题，并对我们的信息安保人员及安保系统进行彻底检讨。我们将继续致力于确保所有客户的数据安全。

对此有疑问的客户可以联系 DPO@RAZER.com。”

虽然泄露的信息中没有敏感数据，但 Diachenko 认为，这些信息仍可能被用于未来的网络钓鱼诈骗，并建议警惕冒充雷蛇或相关公司的诈骗电子邮件。（来源：快科技）

## ➢ 医院信息科负责人辞职后 竟入侵医院系统篡改数据

2020 年 9 月 23 日报道， 医院信息科负责人辞职后竟又侵入医院信息管理系统、伪造医院充值小票、雇用朋友冒充患者等方式行骗。经山东省日照开发区检察院提起公诉，近日，法院以诈骗罪判处被告人张某有期徒刑一年零六个月，缓刑二年，并处罚金 6000 元;分别以诈骗罪判处李某、宋某有期徒刑一年，缓刑一年，各并处罚金 3000 元。

**一张“与众不同”的充值小票**

简爱医院是日照市开发区一家口碑不错、效益较好的私立医院，每天前来诊病的患者络绎不绝。2019 年 10 月 15 日上午，“林主任，您快看这张充值小票，咱医院小票的字体是蓝色打印的，可这张是黑色的，日期显示格式也不一样，咱是用横杠间隔的，这张是用斜杠间隔的……”细心的收款员小张发现一张办理退余额业务的充值小票有问题，让这位患者稍等一下，她急匆匆跑到主任办公室汇报自己发现的疑点。

林主任拿着这张小票仔细端详了半天，发现的确有猫腻，就同收款员一起来到缴费大厅想进一步了解一下情况，却发现刚才那名神色慌张的男子已悄悄离开。听其他同事说，那名

男子是边打电话边匆匆忙忙跑开的。

林主任赶紧让小张查一下卡内的个人信息情况，小张熟练地刷了一下手中的就诊卡，登录医院系统后顿时大吃一惊：刚才还有 300 多元余额的就诊卡，此时显示余额为零，而这张卡明明一直在她手里攥着啊……二人意识到这件事有蹊跷，向医院领导汇报后，院领导要求信息科工作人员从后台进行排查。

与此同时，在简爱医院旁边的一个小区里，一个“神秘”的男子在车上正在熟练地操作电脑。他叫张某，十几分钟前，他刚刚接到冒充患者办理退余额业务的李某的电话：“哥，不好了，医院发现充值小票有问题了……”张某一边嘱咐李某赶紧离开医院，一边打开车上的笔记本电脑，连接上简爱医院的无线网络，熟练登录了系统，找到了刚才办理退余额业务的那个账号，把里面的余额清零……一番操作后，张某长舒了一口气，轻轻合上了电脑，他觉得简爱医院发现余额为零，应该就不会再深究此事了，便给李某发出了一条信息：“兄弟，放心吧，我已处理好。”然后发动汽车，慢慢驶出了小区……

再说简爱医院这边。数据库工程师马上查阅后台数据，发现持卡人的信息显示：2019 年 10 月 11 日充值 500 元，10 月 15 日开了一份腹部彩超检查和两盒复方红衣补血口服液，药已经购买但检查没做，卡内余额 323 元，后台数据显示在当天 10 时 08 分余额已清退，而这恰好是收款员小张发现问题小票向林主任进行汇报的时间段。结合之前持卡男子的异常行为，大家得出了一个大胆推断：“有人侵入了医院的信息管理系统，篡改了后台数据。”

随后，工程师迅速对后台数据进行梳理，果然发现有异常账户存在多次充值、消费和退余额记录，同时，收款台工作人员也从近期的充值小票中又找到了 4 张用黑墨打印的问题充值小票，这进一步印证了大家的推断。

事关重大，简爱医院立刻报警。警方让医院工作人员仔细回忆了一下近期有没有发生可疑的人和事。工作人员想起来，该院原信息科负责人张某一直负责医院网络系统维护，但他已在当年 8 月辞职，辞职原因是张某曾盗窃收款员收取的现金，并通过修改系统后台数据将账目扯平，后被医院发现，因数额不大，医院就没再追究。

**与朋友“组团”发财，按比例提成**

张某有重大作案嫌疑。警方立刻电话通知张某到公安机关配合调查。到案后，心虚的张某低下了头，面对侦查人员摆出的相关证据，他承认利用医院系统漏洞，想方设法骗取医院钱财。

原来，2019 年 7 月，简爱医院更新了财务信息管理系统，此时新旧系统的表格是不兼容的，老系统内的数据需要由人工导入到新系统中，这个导入过程为张某提供了犯罪的机会。

张某发现这个漏洞后，利用职务之便进入计算机旧数据库，把多年不用且余额小于 10 元的患者账户筛选出来，并把这些钱转入到一个自己创建的账户上暂时隐藏起来。随后，他又利用在医院工作之便，从收款台窃取少量现金，再偷偷修改后台数据把账目扯平。然而，张某窃取现金的行为很快就被医院发现了，也因此丢了这份工作。

离职后，张某一时也没找到合适的工作，经济上日渐捉襟见肘。作为南京某重点大学计算机专业的毕业生，他曾经是父母的骄傲，也是他们的希望。可如今面对娇妻幼子，为了养家糊口，他甚至不得不去送外卖赚钱，风吹日晒，很是辛苦，而在农村的父母也已经年事已高，体弱多病。看看自己的大学同学，都混得风生水起，而自己却如此落魄。

张某很不甘心，又惦记起那些被自己藏在虚拟账户中的钱，一番冥思苦想后，想到了把这些钱转入他人就诊卡，再通过办理退费业务的方式把钱倒出来。早在离职前，他就私自留存了三四十张还未录入患者信息的空白就诊卡，还在笔记本电脑上私自安装了该医院的系统，此时正好可以派上用场。

那天午后，张某在医院附近搜索到了医院财务信息系统的无线网络信号，窃喜之余，迅速登录后往原在职期间私存的空白就诊卡内充值 300 元至 500 元不等。随后，他又在客户端登录医生账户冒充医生身份进行就诊操作，一次只开几十元药品。接下来，他又买了一个小票打印机，专门用来打印虚假充值小票。

这样一番“神”操作后，万事已俱备，张某明目张胆去医院办理了两次退余额业务，结果非常顺利，但因为怕被熟人认出来，他又雇用了好友李某、宋某扮演患者角色，并承诺给他们 30%的好处费，二人没有抵住诱惑，轮番出入该医院骗取药品和钱财。

为方便联系，张某还建立了一个名称为“外卖兼职”的微信群，把简爱医院附近的一个网吧作为秘密联络点，每次事成之后，张某会立刻给好朋友们按照 30%的比例发红包，这些微信里的红包转账记录，为后来诈骗案数额的认定起到了至关重要的作用。

张某等 3 人自以为如同“黑客”一般，神不知鬼不觉找到了一条不用费力的生财之道，却不知法网恢恢、疏而不漏，仅仅两个月，他们的行为就被简爱医院发现了。截至案发，他们共计骗取医院款项 4 万余元。

**是盗窃还是诈骗**

今年 5 月，日照开发区公安分局将此案侦查终结，以张某等 3 人涉嫌盗窃罪移送审查起诉。在该案的定性上，公安机关认为，张某通过后台操作系统，将一些小额账户资金转移到虚拟账户，符合使用秘密手段窃取他人财物的特征，其行为符合盗窃罪的构成要件。

**办案检察官则认为：**虽然盗窃罪和诈骗罪都是以非法占有为目的获取他人数额较大的

财物的行为，但盗窃罪的特点是行为人使用秘密手段窃取他人财物，被害人没有主动处分财产的行为;而诈骗罪的特点是行为人使用虚构事实、隐瞒真相的欺骗方法，使被害人陷入错误认识，从而主动处分财产给他人占有的行为。

该案中，张某前期通过后台操作的行为只是在为实施诈骗做前期准备，还不能实际控制这些财物，还未达到非法占有的目的，此时不能认定为盗窃罪;在完成后台操作后，在就诊卡里面完成了虚拟充值，张某又伪造了充值小票，让李某、宋某冒充患者去医院就诊取药并办理退款业务，这些行为使医院工作人员陷入了错误认识，误以为被告人就是来院就诊的真实患者，从而按照流程为他们办理了退款业务，把现金交到了被告人手中，这些行为完全符合诈骗罪构成要件，应当认定为诈骗罪。检察官对 3 人释法说理，他们均对当初的行为悔恨不已，自愿认罪认罚，积极退赔，争取从宽处理的机会。近日，日照开发区检察院对该案提起公诉，法院综合考虑三被告人的犯罪事实、性质、情节和对社会的危害程度及认罪态度，分别作出上述判决。（来源：检察日报）

## ➢ 黑客泄露了上千名白俄罗斯高级警察的个人信息

2020 年 9 月 22 日，近日，一群黑客泄露了 1000 多名白俄罗斯高级警官的姓名和个人信息，以回应警察对反政府示威的暴力镇压。据了解，此次泄露的数据包括姓名、出生日期、所在部门和职务头衔。1003 名警官的详细信息是通过谷歌电子表格泄露的，其中大多数记录的都是高级警官，比如中尉、少校和上尉。

黑客将数据提供给了独立的白俄罗斯新闻社 Nexta，还于上周六在其官方 Telegram 频

道上发布了未编辑的版本。该新闻机构在最近的反政府示威活动中曝光了警察的暴行后，在反卢卡申科的抗议者中颇受欢迎。该机构要求抗议者提供更多细节，帮助核实名单的准确性。

Nexta 说：*“如果你知道名单上某些人的犯罪事实，以及他们的个人信息(地址、电话、车牌号、生活习惯、情妇/情人)，给我们留言。”“如果继续拘留，我们将继续大规模发布数据，”* Nexta 补充说。*“没有人会在巴拉克拉法帽下保持匿名。”*

上周六，白俄罗斯内务部的一名发言人在其网站上发表了一份声明，证实了泄密事件，但同时警告说，他们计划找到并起诉黑客和泄密者。根据多名自称黑客在 Twitter 上发表的声明，该网站随后因 DDoS 攻击而瘫痪。

自 8 月 9 日总统选举结果公布以来，白俄罗斯一直处于近乎彻底的混乱之中。官员们说，现任总统卢卡申科以约 80%的选票赢得第六次连任。反对派候选人 Sviatlana Tsikhanouskaya 指责目前的政权存在大规模的舞弊行为，并声称获得了至少 60%的选票。由于担心自己的人身安全，她最终逃离了这个国家。（来源：互联网）

## ➢ 全国首例微信“清粉”案告破 警方作出郑重提醒

2020 年 9 月 17 日，微信上常看到这样的“清粉”消息：号称“极速清粉”“安全稳定”，但其实暗藏猫腻可能危害个人信息安全。日前，江苏省南通市公安局宣布侦破一起利用微信“清粉”软件非法获取计算机信息系统数据的案件，5 名犯罪嫌疑人落网，这也是全国首例破获的此类案件。据警方披露，仅 3 个月时间，该犯罪团伙以“清理僵尸粉”为名，非法获取用户的微信群聊二维码 2000 余万个，非法获利 200 余万元。

**号称官方“清粉”团队非法获取用户信息 5 人犯罪团伙被抓获**

南通市公安局网安支队三大队副大队长许平楠介绍，“清粉”软件的原理，就是通过应用集群控制软件控制微信账号，自动向所有好友群发消息，再由软件自动识别哪些是“僵尸粉”并予以删除。“但犯罪嫌疑人在取得微信账号的控制权限后，却借机非法获取用户微信群聊二维码信息，并将这些群聊二维码以图片形式保存在服务器上，再倒卖给下游的诈骗、赌博等犯罪团伙获利。”

7 月 3 日，南通市公安局成立由网安、法制、通州区公安局等部门组成的专案组，全力开展工作。专案组研判发现，今年 2 月以来，多个地区频繁出现陌生人扫码进群散布赌博、营销等非法广告，甚至实施诈骗，关联案件达 1500 余起，涉及 20 多个省市。

腾讯公司反馈，微信群聊二维码泄露现象发生后，他们依法配合多地公安机关抓获了多个出售和利用微信群聊二维码作案的犯罪团伙。


通过对大量“清粉”软件开展侦查实验，专案组最终锁定一款名为“微清”的软件有重大嫌疑。“精心制作了‘极速清粉’的广告图，号称官方认证，只需要 1 分钟检测完毕。”许平楠说，为吸引人使用，这款软件打着官方清粉团队的旗号，通过各种途径在微信用户群体中传播，一旦有人点击扫描登录检测，就可以通过后台服务器直接登录受害人的微信，并获取所有的用户权限。

警方梳理线索后，成功挖出团伙成员刘某、何某等人的真实身份。7 月 22 日，专案组民警兵分三路，在广东韶关、仁化，湖北天门等地公安机关的支持下，将涉案的 5 名犯罪嫌疑人全部抓获归案。

经查，该犯罪团伙分工明确，由张某、刘某、何某负责系统开发和维护，李某负责出售二维码牟利，谭某负责为微信公众号引流牟利。

据众人交代，所谓的官方认证、放心访问只是为了降低使用者的警惕心理，他们并没有获得官方授权，而是租用服务器自行搭建系统，在骗取用户授权登录后，通过这些外挂软件系统批量获取微信群聊二维码，批量关注、阅读、点赞等。

短短 3 个月时间，该犯罪团伙共非法获取用户微信群聊二维码 2000 余万个，均出售给了福建龙岩等地的诈骗、赌博犯罪团伙，同时还为他人批量关注微信公众号和刷阅读量、刷赞，先后获利 200 余万元。

**“平台化、专业化、精细化程度高，隐蔽性极强。”**

南通市公安局网安支队支队长张建说，从非法获取微信用户的相关个人信息，到下游的广告、营销和其他网络犯罪，相关的网络黑灰产已经形成一个各环节相互独立又紧密协作的产业链。这起案件系全国首例，没有经验借鉴，办案民警通过分析作案手法、犯罪事实，在腾讯公司和南京森林警官学院的支持配合下，最终案件得以成功告破。目前，上述 5 名涉案犯罪嫌疑人因涉嫌非法获取计算机信息系统数据罪均已被执行逮捕，案件仍在进一步办理中。

**警方提醒：**一旦同意使用这类“清粉”软件，就意味着自己的账号完全让人“接管”，不法分子将轻易获取相关个人信息，建议广大网友尽量不要使用破坏官方软件协议或具有外挂功能的插件和软件，有效规避可能遇到的安全风险。（来源：中国消费者报）

## ➢ 德医院遭遇勒索软件攻击：一名患者或因此死亡

2020 年 9 月 18 日，据报道，一名生命垂危的患者因勒索软件攻击被迫去了更远的医院，不幸的是，这位患者最终没能被救回来。当地时间 9 月 10 日，德国杜塞尔多夫大学医院遭遇勒索软件攻击，而正是因为这个攻击他们的 IT 系统中断进而导致门诊治疗和紧急护理无法正常进行。于是，那些寻求紧急护理的人只能被转移到更远的医院接受治疗。

德国媒体报道称，警方通过赎金说明联系了勒索软件运营商并解释说他们的目标是一家医院。据悉，留在医院加密服务器上的勒索信息显示，其原本的攻击对象是杜塞尔多夫大学而非杜塞尔多夫大学医院。

在警方联系了勒索软件攻击者并解释说他们加密了一家医院之后，攻击者撤回了赎金要求并提供了解密密钥。医院在收到钥匙后开始在缓慢地恢复系统，而调查得出的结论显示，数据应该没有被盗。

据 NTV 报道，杜塞尔多夫大学医院取消了紧急服务登记后，一名生命受到威胁的病人被转到了更远的医院。这种干扰导致病人在一小时后接受治疗很有可能导致了其最后的死亡。对此，德国检察官正在调查此次网络攻击是否犯下过失杀人罪。检方以涉嫌过失杀人罪对这两名身份不明的肇事者展开调查，原因是一名生命危险的病人被送到了伍珀塔尔的一家医院，而这家医院距离事发地约有 32 公里。

外媒 BleepingComputer 在新冠病毒大流行初期接触了不同的勒索软件公司看看他们是否会继续攻击医疗保健和医疗机构。对此，CLOP、DoppelPaymer、Maze 和 Nefilim 勒索软件的运营者表示，他们不会以医院为目标，如果有医院被错误加密他们会提供免费的解密密钥。不过 Netwalker 表示，他们虽然不是以医院为目标，但如果他们不小心加密了一家医院，后者仍需要支付赎金。（来源：cnBeta）

## ➢ 微盟“删库跑路”主角贺某被判 6 年有期徒刑

2020 年 9 月 20 日，今年 8 月 微盟集团（2013.HK）发布 2020 年上半年财报。其中，上半年营收 9.57 亿元，同比增长 45.7%；净亏损为 5.46 亿元，其中包含了香港财务报告准则下可换股债券确认的金融负债公平值变动引起的人民币 4.96 亿元亏损及 SaaS 破坏事件的赔付计划带来的预计赔付支出的损益影响人民币 0.87 亿元。公司经调整净利 5230 万元，同比增长 77.4%。2020 年 2 月份发生的微盟“删库”事件主角贺某被判处 6 年有期徒刑。

**上海市宝山区人民法院刑事判决书（一审）（8 月 26 日宣判）摘录内容：**

2020 年 2 月 23 日 18 时 56 分许，贺某酒后因生活不如意、无力偿还网贷等个人原因，在其暂住地上海市宝山区逸仙路 XXX 弄 XXX 号 XXX 室，通过电脑连接公司 VPN、登录公司服务器后执行删除任务，将微盟服务器内数据全部删除，导致微盟自 2020 年 2 月 23

日 19 时起瘫痪，300 余万用户（其中付费用户 7 万余户）无法正常使用该公司 SaaS 产品，经抢修于 3 月 3 日 9 时恢复运营（故障时间 8 天 14 个小时）。


截至 2020 年 4 月 30 日，造成微盟公司支付恢复数据服务费、商户赔付费及员工加班报酬等经济损失共计人民币 2260 余万元。2020 年 2 月 24 日，贺某在暂住地被公安人员抓获，到案后如实供述了上述犯罪事实。

**法院裁定：**上海市宝山区人民法院认为，贺某违反国家规定，删除计算机信息系统中存储的数据，造成特别严重的后果，其行为已构成破坏计算机信息系统罪，应当依法追究刑事责任。公诉机关指控的犯罪事实清楚，证据确实充分，罪名成立。

贺某如实供述自己的罪行，认罪认罚，可依法从轻处罚。辩护人的相关意见本院予以采纳。依照《中华人民共和国刑法》第二百八十六条第二款、第六十七条第三款、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、贺某犯破坏计算机信息系统罪，判处有期徒刑六年。（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 2020 年 2 月 24 日起至 2026 年 2 月 23 日止。）二、作案工具笔记本电脑一台依法没收。

**附：相关法律条文**

**一、《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。……第六十七条……犯罪嫌疑人虽不具有前两款规定的自首情节，但是如实供述自己罪行的，可以从轻处罚；因其如实供述自己罪行，避免特别严重后果发生的，可以减轻处罚。第六十四条犯罪分子违法所得的一切财物，应当予以追缴或者责令退赔；对被害人的合法财产，应当及时返还；违禁品和供犯罪所用的本人财物，应当予以没收。没收的财物和罚金，一律上缴国库，不得挪用和自行处理。

**二、《中华人民共和国刑事诉讼法》**

第十五条犯罪嫌疑人、被告人自愿如实供述自己的罪行,承认指控的犯罪事实,愿意接受处罚的,可以依法从宽处理。（来源：安全学习那些事）