国盟信息安全通报

2019 年 10 月 14 日第 203 期

国盟信息安全通报

（第 203 期）

国际信息安全学习联盟

2019 年 10 月 14 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 505 个，其中高危漏洞 126 个、中危漏洞 327 个、低危漏洞 52 个。漏洞平均分值为 5.62。本周收录的漏洞中，涉及 0day 漏洞 171 个（占 34%），其中互联网上出现“YzmCMS 跨站请求伪造漏洞（CNVD-2019-33085）、WordPress yawpp 插件跨站脚本漏洞”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 3148 个，与上周（2794 个）环比增长 13%。

主要内容

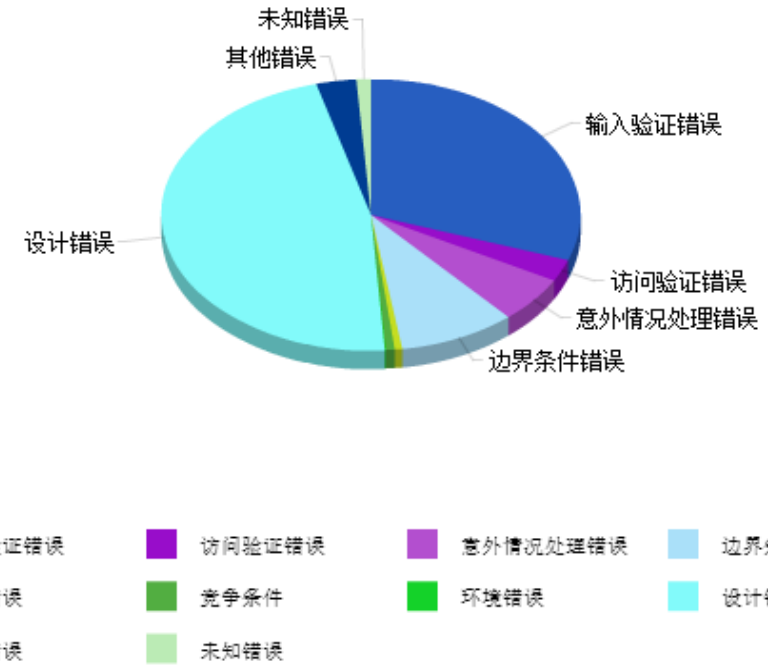
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

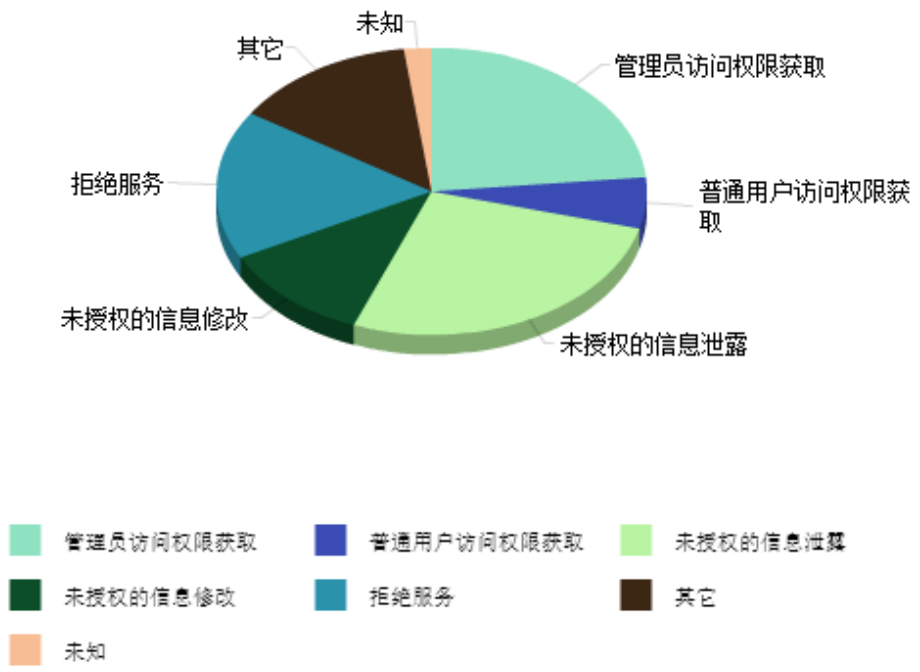
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 505 个，其中高危漏洞 126 个、中危漏洞 327 个、低危漏洞 52 个。漏洞平均分值为 5.62。本周收录的漏洞中，涉及 0day 漏洞 171 个（占 34%），其中互联网上出现“YzmCMS 跨站请求伪造漏洞（CNVD-2019-33085）、WordPress yawpp 插件跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3148 个，与上周（2794 个）环比增长 13%。

二、安全漏洞增长数量及种类分布情况

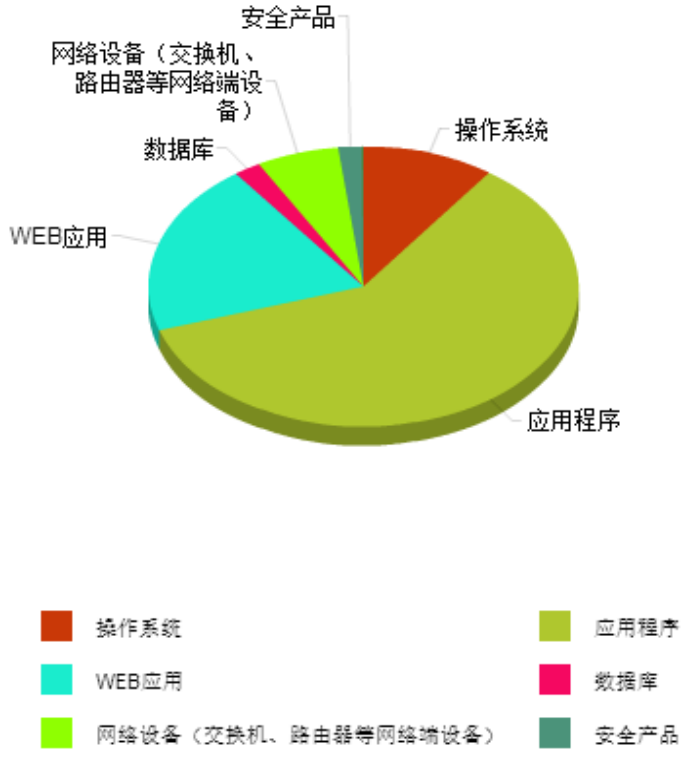
➢ 漏洞产生原因（2019 年 9 月 30 日—2019 年 10 月 14）



➢ 漏洞引发的威胁（2019 年 9 月 30 日—2019 年 10 月 14）



➢ 漏洞影响对象类型（2019 年 9 月 30 日—2019 年 10 月 14）



三、安全产业动态

➢ 确保“四个坚持”，让网络安全理念深入人心

前阶段，国家网络安全宣传周活动举行。习近平总书记强调，国家网络安全工作要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。这体现了我国网络强国战略“以人民为中心”的价值立场和实践原则，赋予了新时代网络安全观的重要内涵。

网信发展安全为要

确保网络安全是我国互联网发展的需要，是维护人民群众根本利益的需要，是推动信息化发展的需要。万物互联、实时相通，互联网科技正深刻影响着现代社会，给社会生活带来美好愿景。但互联网并非乐园净土，也引发了新的风险与挑战。网络技术普惠经济发展，也提高了人们掌握安全技术的难度；互联网+产业做大做强便利生活，也给不法分子提供了新的机会；网络社交拉近了人与人之间的距离，也造成了人际信任的新危机。当互联网深度融入到生活，从线下到线上，从实体场景到虚拟空间，风险发生的现实性、潜在性和预测难度明显增加，网络安全形势更加严峻。

“大安全时代”风险遍在，网络安全必须得到有效防控

近年来，网络攻击、诈骗等时有发生，网络暴力、网络谣言、网络侵权呈多发态势。安全风险从单位、个人手机、电脑信息渗透到国家、国防、基础设施、社会和个人安全等各个

领域，互联网进入“大安全”的时代。据《2018 年中国互联网网络安全报告》显示，当年国家互联网应急中心共协调处理网络安全事件 10.6 万起，包括网页仿冒、恶意程序、DDoS 攻击等多种类型，其中，云平台成为发生网络攻击的重灾区。勒索软件攻击变种数量不断攀升，移动应用网络诈骗尤为突出，个人信息数据泄露被恶意利用引起了国内外普遍关注。当前，大数据、人工智能、物联网等新技术涌现，全球正处于 5G 商用部署的关键期，网络战略博弈筹码加重。新一轮科技角逐和应用必然带来网络安全结构性改变，增加网络安全问题的复杂性，人类安全意识必须更上一层楼。

面对挑战，任何人任何国家都不能独善其身，唯有合舟共济共同应对。党的十八大以来，以习近平同志为核心的党中央系统部署和全面推进网络安全和信息化工作，不断完善依法治网法律体系，实现了制度规范从无到有、从原则到规则、从粗放到精细的重大转变。通过开展系列专项治理行动，建立起关键信息基础设施安全保护制度，形成网络安全总体战略布局和制度保障，我国网络安全产业发展和治理实力增强， 保障能力显著提升。

2017 年《网络安全法》正式实施，作为一项基础性法律，该法内容全面丰富，明确了掌握个人信息的平台和关键信息基础设施运营者的主体防护责任、主管部门的监管责任，涉及基础设施、技术系统、运营行为安全，以及个人信息保护各个层面，成为依法治网的系统方案，也为确保网络空间安全提供了行动指南。近年来，与鼓励互联网创新、产业融合发展同步，我国积极开展安全技术研发，构建安全技术体系，综合利用大数据、云计算、智能感知、区块链等新技术对高威胁进行持续性攻击鉴别、判断，防范网络攻击、网络违法犯罪掷地有声，也为国际社会提供了经验。每年一度的国家网络安全宣传周，让网络安全意识教育深入百姓生活， 越来越为社会熟知。

“以人民为中心”一直是我国网信事业发展的价值主线

我国网信事业以人民的基本利益为着力点，发挥广大人民群众的主人翁作用，最大限度地调动民众的积极性和主动性，激发人民群众主体意识，增强全民主动参与，发动群众、集民意、聚民心。网络安全为人民、网络安全靠人民。实践证明，这一理念和作为有利于促进全民牢固树立起正确的网络安全观，使人民群众在享受信息科技便利的同时，懂得如何通过安全技术守法经营、合理合法地保护自己，共同遵守网络空间活动规则，规避安全风险，防范黑客攻击、盗用数据、侵犯公民个人信息等网络违法犯罪活动，更好地趋利避害，确保互联网健康稳步的进展。

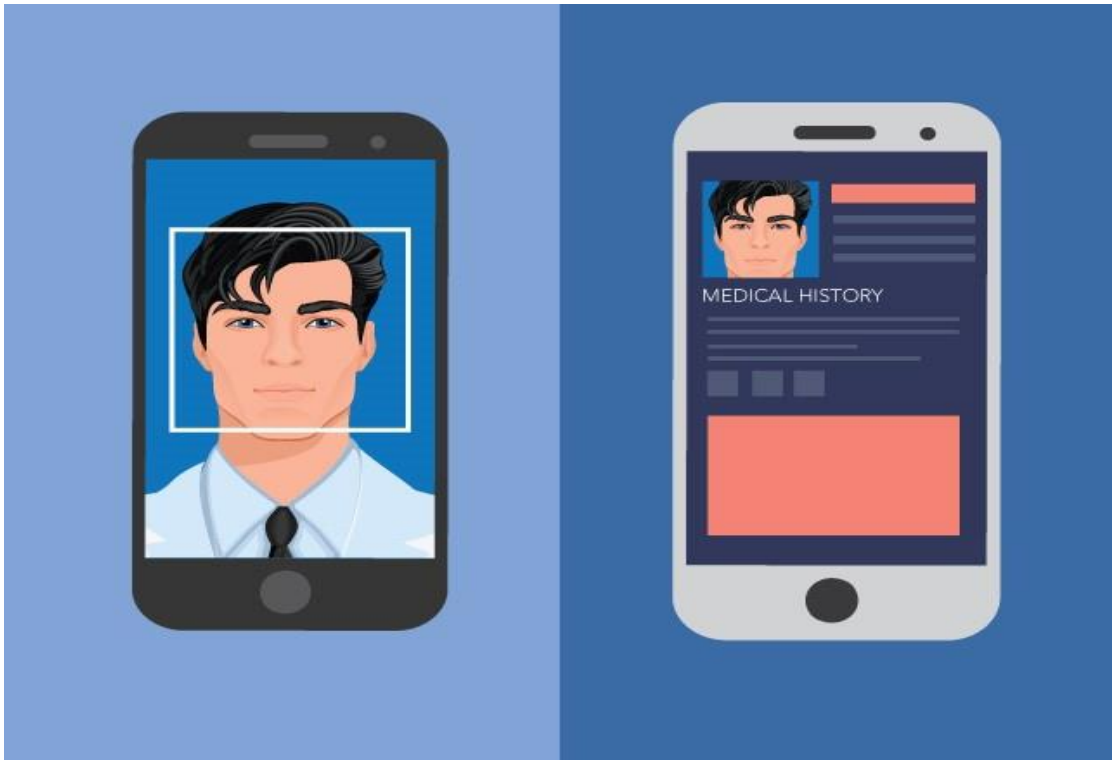
网络信息人人共享，网络安全人人有责

网络安全治理需要全社会共同参与，形成多主体、多效力的综合治网格局。一方面，这

有赖于国家网络安全立法保持动态发展、长效施力，加强安全保障制度建设，加强国际社会合作，随着安全形势变化不断升级治理方式、细化操作。有赖于网信部门进一步加强政策引导，提高信息基础设施网络安全防护能力和网络安全事件应急指挥能力，维护网络发展的良好生态；另一方面，信息媒体、网络企业、网络运营商等主体也要进一步提升遵纪守法、公共服务的责任义务， 深化技术创新与安全理念，将法律法规与行业自律相结合，守土有责、自我约束，落实好作为基础设施运营者和信息内容提供者应承担的防护责任。同时，广大网民也要提高网络安全防御主动性，更好地了解网络，更敏锐地感知风险，增强安全意识，提高防护技能，从基本应用做起，从身边点滴做起，防止违法行为发生，促进网络文明发展。当全社会牢牢树立起网络安全的“防火墙”，互联网必然将更好地造福社会。（来源：光明网）

➢ 人脸识别技术的法律规制研究初探

人脸识别技术为社会带来效益提升的同时，也隐含着因技术滥用对公民权益的风险与威胁。如何对技术失范问题加以规制成为使用人脸识别技术亟待解决的问题。本文将从三个维度，即现阶段法律发展情况、人脸识别技术的机遇与风险以及规制方式进行分析，从而为国内的人脸识别技术的规制提供借鉴。



一、现阶段法律发展情况

国际层面对人脸识别技术的规制主要通过数据保护法律法规进行的，其中最具代表性的是美国和欧盟，以下将结合具体法规对两种模式的特点进行分析。

（一）美国模式

美国在联邦层面没有统一的法律规制人脸识别数据的收集和使用，而是通过各州的独立立法进行管理。目前共有六个州或城市制定了与生物识别数据相关的法案，分别为伊利诺伊州、华盛顿州、德克萨斯州和俄勒冈州和新汉普郡以及加利福尼亚州旧金山市。其中，伊利诺伊州颁布的《生物信息隐私法案》（Biometric Information Privacy Act，简称“BIPA”）最具参考意义。该法案于 2008 年颁布，是美国境内第一部旨在规范“生物标识符和信息的收集，使用，保护，处理，存储，保留和销毁”的法律。

根据 BIPA 的定义，“生物标识符”（biometric identifier）包括对“脸部结构”的扫描，但明确排除了照片。与“生物标识符”相关的术语是“生物信息”（biometric information），该信息是指“通过用以识别特定自然人的生物标识符所获取的信息”。与欧盟保护模式不同（下文详述），BIPA 的规制的范围并不在于能否使用生物识别数据，而在于使用生物数据的方式，具体体现在以下三个方面：

1. 初次收集某自然人的生物标识符或生物识别信息时，须告知该自然人其生物数据被收集的情况、收集目的、数据的保留时间，并获得该自然人的书面授权。Facebook 的“面部印记”功能遭到起诉便是因为 Facebook 未经用户同意便收集了面部结构数据，进而违反了 BIPA。

2. 企业须制定书面政策设定生物识别数据的保留时间表，且当收集数据的目的已达到或距信息主体与企业最后一次联络已满三年时（以先发生者为准），应当摧毁该数据。

3. 生物识别数据不得出售，且除非获得相关自然人的同意或如法律规定的特定例外情况不得对他人披露。

（二）欧盟模式

欧盟保护人脸识别数据的核心法律是《通用数据保护法规》（General Data Protection Regulation，简称“GDPR”）。根据 GDPR 第 4(14)条的定义，生物识别数据明确包括面部图像，且与 BIPA 相同，GDPR 对面部识别数据和照片进行了区分。GDPR 叙文第 51 条指出，“处理照片并不当然地被认为是处理个人敏感数据。仅在通过特定技术方法对照片进行处理，使其能够识别或认证特定自然人时，照片才被认为是生物识别数据”。GDPR 并未提及视频影像，例如被监控摄像头收集的视频影像，但应当类推适用相同的原则进行处理。即如果使用“特

定技术手段”来识别或认证特定自然人，则通过照片或视频收集的任何图像均构成生物识别数据。

GDPR 第 9 条规定，生物特征数据属于个人数据的“特殊类别”，除非某些特殊情况外，不得处理该等数据。人脸识别技术的商业应用可适用的唯一例外是“数据主体已明确表示同意”，同意须“自由给予、明确、具体、不含混”，数据主体任何形式的被动同意均不符合 GDPR 的规定。

此外，GDPR 第 9(4)条允许欧盟各成员国规定在特定情况下不适用 GDPR 中对处理生物识别的数据的限制。例如，荷兰规定了为完成认证或安全需要时可以处理生物识别数据。克罗地亚的新数据保护法对生物识别数据的限制排除适用监控安全系统。

（三）小结

美国和欧盟对人脸识别数据的保护模式代表两种不同规制路径。第一种是欧盟采用的在整体上严格限制生物识别数据的使用，但同时赋予了欧盟成员国一定的自由裁量权，允许成员国规定在特定情况下不适用对生物识别数据的限制；第二种是美国采用的较为自由的方式，即不在联邦层面限制面部识别数据的使用，赋予各州各领域极大的规制权限。

二、面部识别技术的机遇与风险

（一）面部识别技术的机遇

人脸识别作为一项新技术，其应用领域多样，利用得当将为政府、企业和个人均带来新的机遇或便利。

对于政府而言，政府作为保障公民安全和打击犯罪的主要力量，人脸识别技术一方面有利于增强公共安全和监控警情，通过在公共场所使用人脸识别技术有助于警方建立人像库，从而为抓捕犯人、打击犯罪以及追踪、监控恐怖主义活动提供帮助；另一方面有利于寻找失踪人口，特别是儿童。例如，2018 年印度新德里警方利用人脸识别技术，在 4 天内发现了近 3000 名失踪儿童，人脸识别技术在此方面的推动是极具突破性的。

对于企业而言，人脸识别技术将为其在产品和服务的研发和推广过程中产生新的机遇。例如在医疗和技术的革新方面，研究人员使用人脸识别软件成功诊断出存在于非洲人、亚洲人和拉丁美洲人的一种罕见遗传疾病；此外，澳大利亚国民银行利用人脸识别技术设计了一个方案，可以让客户凭借人脸识别和个人密码从自动取款机中取款。

对于公众而言，之于上述人脸识别技术对于政府和企业在提高各自职能方面的促进，公民的人身安全和财产安全也将因此而获益。

（二）人脸识别技术带来的风险

这项技术带来显著的社会效益的同时，侵犯了公民的隐私权、民主自由和人权，并激发歧视问题。

不少西方学者认为：人脸识别技术的应用可能侵犯公民隐私权以及民主自由和人权。民主依赖于公民集会、公开讨论其观点，而这项权利的完满行使则要求人们自由行动而不受政府监督。然而，当无处不在的摄像头与强大计算能力和云存储相结合时，人脸识别技术能够帮助政府实现对每个地方的每一个人 24 小时不间断地监视，程度之深之广均为前所未有。这种被监视的状态进一步阻遏公民发表言论或参与公开抗议等民主活动，并从根本上改变公民在公共场合的存在方式。

此外，人脸识别技术可能导致歧视问题。目前的技术并不能保证人脸识别的准确性，数据识别结果的不准确将导致应用时产生偏见，进而引发歧视问题。麻省理工一工作组研究表明，人脸识别技术对非白人个体识别的准确率要低于白人个体，即意味着非白人个体更容易被打上“嫌疑人”标记。这种准确性上的差异将种族区分内置于技术本身，使得执法机关在判断某一犯罪或违法行为的犯罪嫌疑人身份时将种族特征列入考虑因素，从而对非白人群体造成歧视。

三、人脸识别技术的规制

人脸识别技术尚处发展初期，但其蕴含的风险可见一斑。如果不立即采取行动，很可能在该技术普及时产生更多的社会问题，到那时进行规制将更加困难。为享受该技术带来好处的同时降低对公民权利的风险，需要政府强制划定一条支撑良性市场竞争的责任底线，要求使用这项技术的企业或部门必须遵纪守法，同时企业也应在该底线的基础上制定政策进行自我规范。

（一）政府层面

本文第一节展示了现有的两种规制方式，即从使用数据源头严格监管的欧盟模式和赋予自由的美国模式。除这两种模式之外，两种模式的中间道路也值得考虑，即限制措施放置在处理人脸识别数据的方式上，同时对处理人脸识别数据的重要方面和基本原则进行统筹规制，如要求处理人脸识别数据的透明性、技术通过准确性和无偏见检验，并获取用户同意，从而保证企业人脸识别数据处理大方向上的正确性。具体应当采取何种规制方式，我国政府应当根据本国国情制定相适应的法律法规。

（二）行业自律

尽管从政府层面规制人脸识别技术更为有力，但是企业不应完全坐等政府采取行动。本文建议相关企业在使用并制定人脸识别技术和数据的相关政策时应当充分考虑以下七个原

则：用户同意；数据合规使用；透明性；数据安全保护措施；隐私设计；准确性和用户权利和问责制度。遵从上述七个原则不仅为收集、使用人脸识别数据提供保护，还可以赢得用户的信任。

1. 用户同意：企业使用人脸识别技术进行验证或识别特定用户和/或向第三人披露人时均应当获得用户的事先同意。“同意”的应当明确且肯定，且符合当地数据监管机构要求的标准和行业习惯做法。

2. 数据合规使用：企业应考虑收集人脸识别数据是否必要，在使用数据时应权衡隐私风险与消费者的可得利益，并向消费者提供减轻或避免风险的选择。

企业应充分考虑信息所对应的特殊群体（考虑因素包括年龄、社会地位、弱势程度），如儿童。在该群体的人脸识别数据时应提供额外的数据安全保护、更高透明性或更多的选择。此外，企业需注意当地法律是否对特殊群体有额外的要求。

企业业务范围可能发生改变，企业应时刻注意提供给用户的信息是否与收集、使用人脸识别数据相一致，如有重大变更应及时通知用户并获得新的同意。

3. 透明性：企业应制定并发布《隐私政策》，以清晰、明确、易懂的方式告知其使用人脸识别系统以及人脸识别数据收集目的、是否会被分享、数据分享的第三方清单、数据保留期、删除和去标识化手段、报告问题的途径、发生重大变更的措施、拒绝的方式等。

设计或研发人脸识别技术的企业应建议使用其技术的第三方告知消费者该技术的使用，促进人脸识别技术使用的透明性和隐私合规。

4. 数据安全保护措施：企业应依据当地法律规定、所涉人脸识别数据的敏感性、规模和使用环境，选择最适当的安全保护措施。除上述特别保护外，其他措施包括数据加密、病毒防护、访问控制、员工培训等。

5. 隐私保护设计：隐私保护设计应嵌入人脸识别产品和服务的设计和架构全阶段，并将该理念应用于公司实践中，包括任命人员负责监督隐私问题、培训员工隐私知识并定期进行隐私审查。

6. 准确性和用户权利：企业应当采取措施来确保人脸识别数据的准确性，并充分测试其系统以识别并消除缺陷，避免产生错误标记，特别是人脸识别数据涉及种族、年龄和性别方面的区分。

同时，企业应制定并发布相关政策，告知数据主体审查其个人数据的方法，数据有误时如何进行反馈修改。在可能的情况下，企业在收到执法请求时应通知相关自然人，告知将向政府相关部门披露。

7.问责制度：企业在使用人脸识别技术时应当保持政策、程序和措施的透明性，为对人脸识别数据提供充分的责任保障，应定期对人脸识别数据进行审计，对处理人脸识别数据的员工进行培训；设立内部隐私机构来评估、批准涉及人脸识别数据的新应用或服务；保证第三方服务提供者、商业伙伴在使用人脸识别技术或处理数据时符合本研究中提及的七大处理原则，一旦发现第三方企业违反要求，则拒绝其访问人脸识别数据。（来源《中国信息安全》杂志 2019 年第 8 期）

➢ 对 APP“强制索权”说不

打开手机的应用程序（以下称 APP），输入 18 位社会保障号、姓名、8 位查询密码、登录密码、手机号，你所有的个人信息有可能出现在别人的电脑后台上。这是曾发生在央视“3·15”晚会上的一幕，主持人通过一款名为“社保掌上通”的 APP 注册并进行社保查询，现场模拟了个人信息被远程截取的全过程。专家称，该社保查询 APP 暗含多项不合理条款，强制、过度索取用户隐私，比如“您同意并授权我们使用您的社保账户密码”以及“模拟您登录网站获取您的个人信息”等。但用户注册后，其个人信息却被发往某大数据公司的网站，并且这一切是发生在用户毫不知情的状况下。需要注意的是，类似“强制索权”、违法违规收集个人信息的 APP 并不少见。

没有电话业务，为何要电话权限？

国家互联网应急中心发布的《2019 年上半年我国互联网网络安全态势》显示，今年上

半年，国家互联网应急中心通过自主捕获和厂商交换获得移动互联网恶意程序 103 万余个，通过对恶意程序的恶意行为统计发现，排名前三的分别为资费消耗类、流氓行为类和恶意扣费类。

国家互联网应急中心监测分析发现，在目前下载量较大的千余款移动 APP 中，每款应用平均申请 25 项权限，其中不少 APP 与电话业务无关，却申请拨打电话权限，数量占比超过 30%。在个人隐私方面，每款应用平均收集 20 项个人信息和设备信息，涉及社交、出行、招聘、办公、影音等各方面。此外，大量 APP 有探测其他 APP 信息、读写用户设备文件等异常行为。

隐私的“钥匙”不要说给就给

当 APP 越界搜集用户的隐私信息时，这对用户个人信息安全造成的威胁不容小觑。因此，消费者应增强安全意识，加强对 APP 索权的重视程度，审慎对待 APP 索要的每一项授权。但不同类型授权的背后，究竟隐藏着怎样的风险？对此，记者做了简单的归纳整理。

如若授权 APP 读取位置信息，一旦位置信息被不法分子利用，或导致财产盗损甚至引发人身伤害；如若授权 APP 读取存储设备权限，重要文件、隐私照片有可能泄露；如若授权 APP 读取电话权限，就有可能被查看和修改通话记录、查看本机号码及设备 ID，APP 还可能获取通话状态和正在拨打的电话号码，甚至直接挂断电话；如若授权 APP 通讯录功能权限，APP 可能会读取、修改通讯录，这样联系人的信息可能泄露；如若授权 APP 短信功能权限，那么 APP 可能会收发、读取和删除短信，用户进行银行转账、网站登录的验证码也可能被读取，容易造成财产损失；如若授予获取摄像头、麦克风权限，那么用户打开设备的摄像、拍照、录音功能时，APP 可能会窥探用户生活隐私。

总之，对手机用户而言，一定要“长点心”，尽可能地保证个人隐私信息的安全，然后再享用 APP 带来的便捷。互联网企业要认识到，无底线的“强制索权”不仅有违商业道德，而且违法违规，应确保相关应用索取的权限与功能相匹配，并妥善使用这些权限，避免伤害用户权益。

举报信息近 8000 条，百余家企业须整改

一些网站和 APP 强制索权、过度索权、超范围收集个人信息，有的 APP 甚至向用户索要 70 余项权限，而一旦被拒绝，整个应用都将无法使用。某些软件开发者的“蛮横”行为激起用户的不满，也引起了有关部门的重视。

近日，由中央网信办等指导举办的“2019 年网络安全博览会”展示了今年 1 至 9 月中央网信办等 4 个部门开展 APP 个人信息保护专项治理工作的成果，其中就包括近 600 款 APP

的违法违规使用个人信息评估和处理情况。

中央网信办网安局一级巡视员兼副局长杨春艳提到，针对当前 APP 强制授权、过度索权，超范围收集个人信息、违法违规使用个人信息等数据安全问题，中央网信办起草了《APP 违法违规收集使用个人信息行为认定办法》、国家标准《移动互联网应用（APP）收集个人信息基本规范（草案）》等系列制度文件。

此外，就目前 APP 专项治理行动取得的阶段性成果，杨春艳表示，今年 1 月以来，中央网信办、工信部、公安部、市场监管总局联合开展了一系列综合治理活动：指导成立 APP 专项治理工作组；开发了举报平台，建立专门针对 APP 违法违规收集使用个人信息的举报渠道，至今已收到近 8000 条举报信息，其中实名举报占到近 1/3；并将 400 余款下载量大、用户常用的 APP 纳入了评估，向 100 多家 APP 运营企业发送了整改建议函，评估发现的问题得到整改落实；此外，通过微信、网站等渠道加大宣传普及力度，配合央视“3·15”晚会等对典型 APP 违法违规收集个人信息行为进行曝光，其目的是为了促进 APP 运营企业加紧整改。

“目前这项工作还在加紧推进，我们将继续完善相关文件标准，加大治理力度，不断提升 APP 个人信息保护水平。”杨春艳表示。（来源：人民网）

➢ 关于金融科技时代下银行网络安全运营的思考

在当今科技与金融发展深度融合的趋势下，党的十九大报告中提出了对“现代金融”的要求，现代金融的核心要义即是科技驱动的新金融。金融科技已不仅仅是金融行业本身的转型发展，更重要的是对社会经济发展具有重要促进意义。各家银行积极争夺金融科技主导权，纷纷将金融科技提升到战略高度。银行业发展已进入从传统科技“支撑”到金融科技“引领”的时代，金融科技也已是银行抢占未来主战场的重要利器。

随着金融科技时代的到来，网络安全“四化”趋势日益明显，即网络犯罪组织化、攻击方式定向化、攻击目标数据化、信息系统云化，网络安全运营已经走到变革的交叉路口。网络安全和信息化建设是相辅相成的，网络安全是信息化建设的前提，信息化建设是网络安全的保障，两者相互推进。金融科技所引领的网络化、数据化、智能化生活，对银行的网络安全运营工作既是机遇，同时也是巨大的挑战。银行应该充分认识到做好金融科技时代下网络安全运营工作的重要性和紧迫性，因势而谋、乘势而上、顺势而变，变被动防御为主动管理，

积极探索新的网络安全运营管理思路，才能与金融科技时代形成良好互动，赢得主动、赢得稳定、赢得未来。

一、直面金融科技时代下银行网络安全运营面临的新挑战

金融科技蓬勃发展，给银行的产品服务、商业模式、经营理念带来了深刻变革，为银行科技转型升级提供源源不断的动力。依托人工智能、区块链、云计算、大数据、物联网等技术在金融领域的应用，银行网络安全运营管理工作具有了全新的思路和手段，包括更全面的数据资源、更加智能的手段方法和更加高效的处理能力，进一步助推网络安全防御向着纵深化、智能化、快速化的方向发展。我们在看到金融科技时代下网络安全的巨大发展机遇的同时，必须承担越来越严峻的网络安全风险。

随着金融科技新技术在银行各业务领域的逐步渗透，网络安全与银行的各业务领域以及日常经营活动的关系愈加紧密，导致银行所面临的网络安全威胁更加复杂和多元化；与此同时，银行面临的网络攻击方式也日趋复杂，数据泄露、滥用问题更加严峻，窃密性攻击步入高发期，互联网面临的高级威胁不断加剧，金融科技安全运营复合型人才稀缺，业务流程与网络安全缺乏深度融合、协同联动，这无疑进一步增加了银行网络安全运营管理的难度。

（一）金融科技安全运营复合型人才稀缺，已成为银行网络安全运营发力的掣肘

人工智能、区块链、云计算、大数据等新技术面临快速迭代，银行业竞争日趋激烈，银行服务自动化、智能化的呼声越来越高，为客户带来极致体验的同时，银行必须充分预判和挖掘金融科技新技术应用存在的网络安全风险，方可做好网络安全运营工作。

金融科技时代下网络安全运营究其根本是人才工程，人才无疑是第一生产力。及时响应客户个性化、深层次的需求，打造银行特色化产品与服务，全面的安全感知、有效的安全防护、有力的应急响应均需要大量的人力投入，需要熟练掌握金融业务、深刻数字化思维以及

具备网络安全整体布局、顶层设计能力的复合型人才。但传统银行在这方面的人才少有积累，掌握传统技术架构的人才多但掌握金融科技新兴技术的人才匮乏，传统软件研发人员多但网络安全工程师紧缺，实施安全漏洞检测、评估、修复的人才多但兼有网络安全整体规划和顶层设计能力的人才很少或没有。

当前我们正处在银行转型的新时代，科技正在从底层基础设施跃升为顶层的创新先导，驱动着银行的流程再造和战略转型，催生出综合化、智慧化、生态化的新金融。而网络安全风险与金融科技应用创新相伴相生、如影相随，相较于资金、技术、场景研发能力等方面的不足，金融科技安全运营复合型人才的不足已成为银行转型升级的掣肘，这也是金融科技时代下银行网络安全发展的历史长河中必须直面的问题。

（二）网络攻击手段日趋多样，数据安全管控面临挑战

金融科技新技术的快速发展在为银行科技创新推波助澜的同时，也为不法分子提供了更多的犯罪渠道和手段。当前，银行已成为国内外敌对势力、黑客组织、不法分子实施网络攻击、电信诈骗和渗透窃密的重点目标。

过去两年，以盗取资金为目的的常规攻击手段不断衍变，除了传统的 SQL 注入、DDOS 攻击、病毒木马等常见攻击外，针对银行的 APT 攻击、精准式网络攻击等攻击手段也愈演愈烈，对银行网络安全，尤其是数据安全的保护提出了更高要求。一旦由于安全防控不足造成数据泄露或资金损失，银行声誉将遭受严重打击。但同时，由于银行技术实现方式的不断革新、网络互联互通、数据高度集中、系统日益复杂等现实情况，又使得银行难以将所有的风险敞口都提前覆盖并布局防御。因此数据安全管控将成为银行面临的严峻挑战。

（三）业务流程与网络安全缺乏深度融合、协同联动，业务创新与安全的矛盾凸显

随着大数据、人工智能等技术的持续渗透，银行的客户需求和行为发生了明显变化，对移动智能化、个性化、场景化提出了更高的要求。如何迎合客户需求的变化，将金融科技能力封装成标准化服务，有机融入银行各业务场景全流程，为客户带来智能高效的数字体验和智慧服务，已成为考验银行服务能力的关键，也是银行未来的核心竞争力之一。

在这个背景下，银行如果想保持核心竞争力，在激烈的市场竞争中占有一席之地，银行具备需要快速的反应能力和业务创新能力。为了快速响应市场需求变化，银行需要改变传统的系统研发模式，全力缩短系统研发流程和研发周期。在业务紧急上线的强压下，系统可能未经过充分的安全评估和测试便“带病”上线，难免在上线后出现各类安全漏洞，严重影响信息系统稳定运行。同时，业务创新必然有风险，业务环境的变化也会导致新的网络安全问题。随着大数据、人工智能在批量获客、销售支持、客户服务、运营管理、风险控制等领域

的深入应用，银行数据高度集中、系统日益复杂、网络互联互通，网络安全边界逐渐淡化，互联网资产暴露面持续变化，科技风险呈现集中化、复杂化趋势，风险传导更加迅速、蔓延范围更大、影响程度更深，单个系统或设备故障可能引发连锁反应。同时，银行可能遭遇大量勒索性质的网络攻击和各种针对应用程序新型未知漏洞攻击，防范和处置的时间窗口将会越来越短，对银行的网络防护和处置提出了更高要求。在此背景下，如何将业务流程与网络安全进行深度融合，做到事前预判防住风险，事中应急控制风险、事后追溯改进风险，也成为银行业面临的共同挑战。

二、用战争的思维和视角，打赢金融科技时代下的网络安全运营保卫战

在科技发展速度指数型攀上、新技术涌现速度不断加快、迭代成熟速度不断提升的今天，抓住新技术应用的发展机遇，主动防御，迎接金融科技时代的挑战，引领和推动银行进入全新的发展阶段，是银行必须做出的选择。面对紧迫的形势，面对复杂的环境，我们要打赢网络安全这场没有硝烟的战争，就要以战略思维及战争思维去部署准备。

（一）一套权责清晰、合力联动的指挥体系，是网络安全战争取胜的关键

这里说的指挥体系，就是指银行高级管理层的重视以及完善的网络安全治理架构。银行应当根据自身情况建立权责清晰、合理有效的网络安全治理架构，确定网络安全运营管理责任，合理划分职责是做好网络安全运营工作的基础。高级管理层的参与至关重要，银行应充分发挥领导的作用，银行高级管理层应参与到网络安全治理工作中来，实施“自上而下”的管理，是网络安全目标实现的催化器和倍增器。

同时，银行的网络安全治理架构要有弹性、要敏捷灵活，能够快速决策、快速响应、快速实践，打破传统银行业务、架构、研发、运营、测试、安全团队之间的壁垒，实现多部门、多职能的协调联动。科技应主动转变与业务部门的合作模式，从传统的研发支持、安全检测，转变为联合业务共同规划、设计、打造产品，加速孵化新业态和新模式，发挥科技引领作用。

（二）一支特别能战斗的队伍，是网络安全战争制胜的根本

金融科技与网络安全实现良性互动，复兴型人才是基础。银行应坚持以人为本的原则，坚持“以安全保发展、以发展促安全”原则，持续加强金融科技安全运营复合型人才队伍储备及建设。银行要重视复合型人才的培养，建立内部复合型人才培养体系，构建自身的“造血”系统。通过专业技术培训增强金融科技创新服务输出能力，通过技术平台建设为网络安全赋能，通过内部攻防对抗和联合外部开展攻防演练等方式锻炼队伍实战能力，逐步解决人才队伍能力短板，提升队伍的专业化能力和战斗力。同时，银行还要完善自身的薪酬和绩效考核机制，从外部吸纳更多复合型人才，形成自身的“活血”能力，从而保障金融科技的可

持续发展，夯实网络安全运营基础。正所谓“养兵千日、用兵一时”，自身能战斗的队伍，在关键时刻能起到非常关键的作用。

（三）一套智能联动的防御体系，是网络安全战争制胜的基础

银行网络安全防守重点通常集中在边界防护层面，但面对特种木马、0day 漏洞、钓鱼攻击、APT 攻击等不断更新的高级攻击手段，始终会有疏漏。一旦攻击者绕过了正面防御的边界防护手段，到达内网服务器实施异常操作，如：主动外连互联网传输数据，内网横向渗透，执行命令等，这些攻击行为与服务器正常操作行为混杂在一起，具有很高的隐蔽性和破坏性。

依托于大数据、人工智能等新技术的应用，通过综合运用流量检测、系统监控、大数据、机器学习等技术手段构建模型场景，关联分析各类安全设备监控信息、威胁情报和应用系统日志的历史数据，提取服务器日常主动行为中的典型特征，建立服务器行为基线，包括互联网外连、内网互访、内部运行三个基线组，设置异常行为匹配判别策略，甄别研判明显偏离日常基线的异常行为，做到第一时间采取访问限制或拦截等应急处置措施。

以安全大数据为基础，结合机器学习和人工智能等新技术，银行可构建威胁态势可感知、攻击态势可感知、流量态势可感知、行为态势可感知的四大核心能力，达到事态可评估、趋势可预测、风险可感应、知行可管控的感知效果。通过全方位的信息采集，深入挖掘各种攻击行为，融合用户、业务、关键链路和互联网访问等多个维护的流量信息，实现对风险的可视化呈现和趋势预测。通过关联用户“上下文”动作，实现第一时间发现异常行为，更精准地追踪溯源，快速提升银行网络安全风险感知能力和预警能力。

（四）一则精准、自动和智能的安全威胁情报，是网络安全战争制胜的有力支撑

网络安全威胁情报，是银行知己知彼的一个重要途径。关起门来做网络安全，是与时代背离的。随着外部攻击形势持续恶化，银行现有安全产品无法有效应对未知威胁，未知威胁或未修复的已知威胁已成为银行的风险防控短板，基于风险漏洞为中心的防御思路，已不能应对当前复杂和严峻的安全形势。威胁情报对运营层面的安全决策以及事件处理均起到了重要的支撑作用。通过采用机器学习、聚类、分类算法，从攻击规则、用户行为、业务场景出发，对互联网应用开展实时监控，增强系统的综合安全防护能力，提升对潜在安全威胁的预判能力。通过链条性的事件追踪和数据挖掘，深度挖掘安全威胁情报，根据异常行为直接实施自动化响应处置，大幅度提升应急响应决策效率。

（五）一条独立自主的道路，是网络安全战争长期制胜的核心战斗力

新时代下银行金融科技发展的迅猛，变化之迅速，要求银行具备强大的网络安全的反应速度和应变能力。“以不变应万变”显得尤为重要，而走独立自主，自力更生的道理，就是“以不变应万变”的根基。一是要有自己的队伍，安全团队的技术基础要求高，会接触到各种非常敏感的信息，自己的队伍尤为重要，是传承，也是对自身的保护。二是要有自己的技术，技术是我们自身与外部开展斗争的必须具备的，不能依赖外部的技术。三是要有自己的“武器”，也就是安全的工具，目前银行业务场景多，涉及的人员广，现代的安全战争不能单纯依靠“小米加步枪”，不能光靠人去判断，也不能光靠个人的努力，而是需要一批现代化的武器来武装安全团队，在网络安全、数据安全等挖掘、阻断、溯源等方面提供强有力的保障。

银行在抓住金融科技助力银行科技转型升级的同时，也应寻求其在银行网络安全风险管控的有效着陆点，这对提升银行网络安全运营管理水平有着重大意义。面对复杂多变的网络安全形势，银行应当加强安全整体设计，从组织架构、管理、机制等多方面入手，多管齐下、多措并举，真正做到“以安全保发展、以发展促安全”。（来源：广发银行信息科技部　刘远欢）

四、政府之声

➢ 教育部等十一部门发布关于促进在线教育健康发展的指导意见

2019 年 9 月 30 日，经国务院同意，教育部等十一部门联合印发《关于促进在线教育健康发展的指导意见》（以下简称《指导意见》）。

《指导意见》指出，在线教育是教育服务的重要组成部分，发展在线教育要以习近平新时代中国特色社会主义思想为指导，全面贯彻党的教育方针，落实立德树人根本任务，创新教育组织形态，丰富现代学习方式，为加快建设“人人皆学、处处能学、时时可学”的学习型社会服务。

《指导意见》明确，到 2020 年，大幅提升在线教育的基础设施建设水平，互联网、大数据、人工智能等现代信息技术在教育领域的应用更加广泛、在线教育模式更加完善，资源和服务更加丰富。到 2022 年，现代信息技术与教育实现深度融合，在线教育质量不断提升，资源和服务标准体系全面建立，学习型社会建设取得重要进展。

《指导意见》提出，要扩大优质在线教育资源供给。一是鼓励社会力量举办在线教育机构，支持互联网企业与在线教育机构充分挖掘新兴教育需求，满足多样化教育需求。二是推动学校加大在线教育资源的研发和共享力度，加快线上线下教育融通，扩大优质教育资源的

辐射面。三是实施“教育大资源共享计划”，建设一批高质量在线课程，培育优质在线教育资源。四是鼓励职业院校、普通高校、科研院所、企业等密切合作，推进在线教育产学研用一体化发展。五是鼓励职业院校、普通高校结合社会需要和办学特色，加强相关专业建设和在线教育人才培养力度，积蓄发展动力。

《指导意见》强调，要构建扶持在线教育发展的政策体系。一是完善在线教育准入制度，建立规范化准入体系。二是强化基础设施建设，推动现代信息技术在教育领域的规模化应用，加快建设教育专网，到 2022 年实现所有学校接入快速稳定的互联网。三是落实财政支持政策，指导各地完善政府购买优质在线教育资源与服务的相关制度。四是鼓励金融机构开发符合在线教育特点的金融产品，利用多种融资渠道，支持在线教育发展。五是完善在线教育知识产权服务体系，建立公平竞争的市场秩序。

《指导意见》要求，要形成多元的在线教育管理服务格局。一是保护消费者权益，明确在线教育服务提供规则，畅通消费投诉渠道。二是创新在线教育的管理服务方式，强化实时监测和风险预警。三是加强部门协同监管，加大对在线教育机构的信息归集和部门之间的数据共享力度。四是支持在线教育行业组织建设，强化行业自律，引导行业健康有序发展。（来源：教育部）

- **《教育部等十一部门关于促进在线教育健康发展的指导意见》全文：**
- http://www.moe.gov.cn/srcsite/A03/moe_1892/moe_630/201909/t20190930_401825.html

➢ 央行下发《个人金融信息（数据）保护试行办法（初稿）》征求意见

2019 年 10 月 9 日，获悉《个人金融信息（数据）保护试行办法（初稿）》已经出炉，央行已经下发到各家银行，目前正在征求意见中。

据了解到，《个人金融信息（数据）保护试行办法（初稿）》第十二条中规定：“（金融机构）不得从非法从事个人征信业务活动的第三方获取个人金融信息。”第十八条规定：“金融机构不得以“概括授权”的方式取得信息主体对收集、处理、使用和对外提供其个人金融信息的同意。”待到《办法》正式出台后，银行将根据该办法的要求，对提供业务数据的第三方机构进行摸排。对于不能保证数据来源合法的数据供应商，要停止合作。日前，已经有银行停止了与部分第三方数据提供商的合作。

2019 年 4 月，央行发布了《中国人民银行 2019 年规章制定工作计划》中，其中就包括制定《个人金融信息（数据）保护试行办法》。已经进入第四季度，从时间进度上看，离正式推出已经不远。

中国人民银行2019年规章制定工作计划

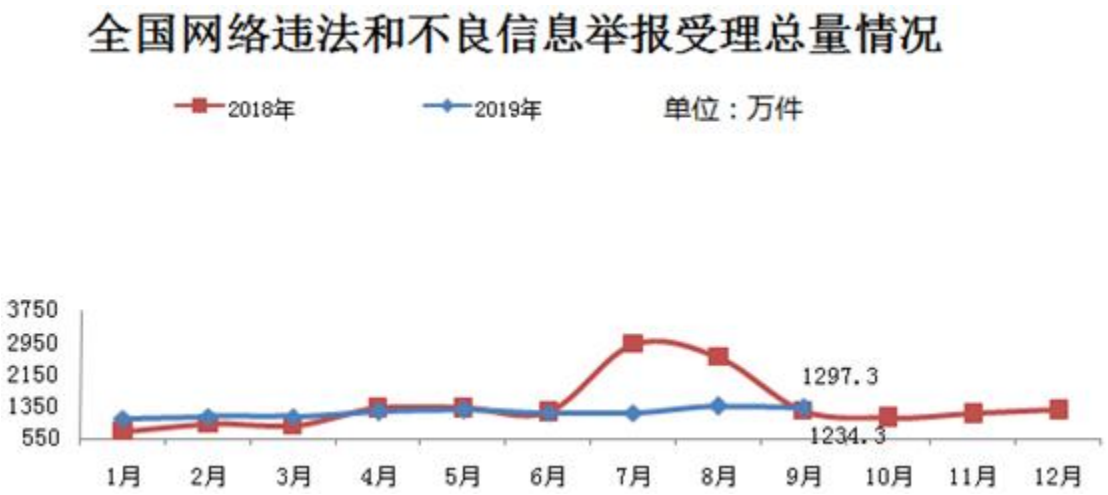
序号	项目名称	类型
1	中国人民银行行政许可实施办法	修订
2	准备金管理办法	制定
3	金融控股公司监督管理试行办法	制定
4	系统重要性银行监管规定	制定
5	人民币图样使用管理办法	修订
6	中国人民银行货币鉴别及假币收缴、鉴定管理办法	修订
7	储蓄国债（凭证式）管理办法	制定
8	个人金融信息（数据）保护试行办法	制定
9	信用评级业管理暂行办法	制定
10	金融机构反洗钱监督管理办法	修订
11	金融机构客户身份识别和客户身份资料及交易记录保存管理办法	修订
12	中国人民银行金融消费者权益保护实施办法	制定

据了解，央行对于个人信息，尤其是个人金融信息的保护工作，一直都很重视。据公开资料，央行已成立了“个人信息保护课题组”，由央行征信中心的王晓蕾副主任担任课题组的负责人，课题组成员由来自央行、信息研究领域、律所、法学院的专家组成。央行课题组就个人信息保护做了大量的比较研究。《个人金融信息（数据）保护试行办法》的推出，意味着央行在个人金融信息保护的监管方面，思路已经成熟。

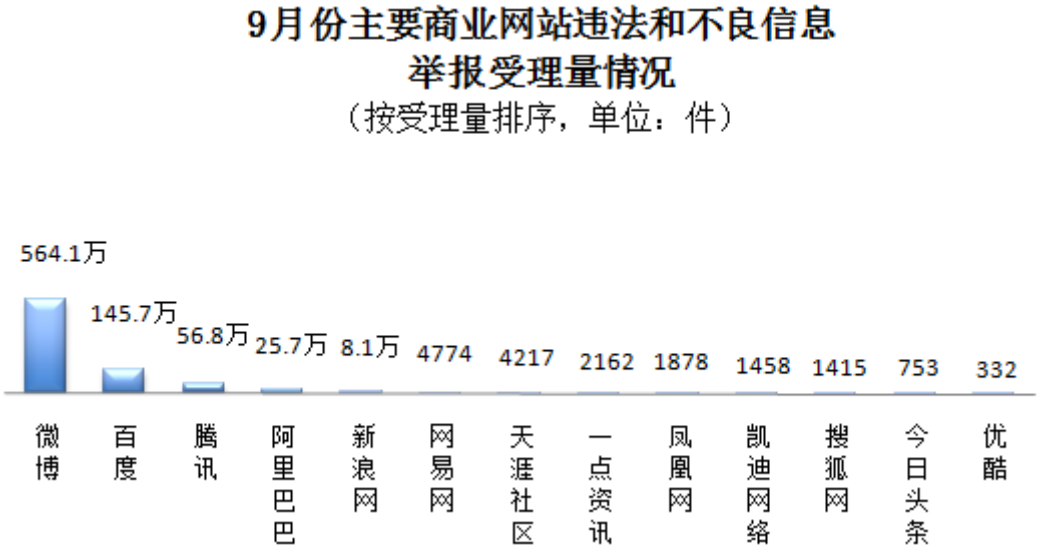
而近来监管对大数据行业的整顿，会随着即将来临的《个人金融信息（数据）保护试行办法》，进一步深入下去。大数据行业对数据来源一直“讳莫如深”。如今正本清源，第三方数据提供商与持牌金融机构做生意，双方都没法一个“装聋”，一个“作哑”了。（来源：消金界）

➢ 2019 年 9 月全国受理网络违法和不良信息举报 1297.3 万件

2019 年 10 月 11 日，国家网信办举报中心发布 2019 年 9 月，全国各级网络举报部门受理举报 1297.3 万件，环比下降 4.1%、同比增长 5.1%。其中，中央网信办(国家互联网信息办公室)违法和不良信息举报中心受理举报 18.3 万件，环比下降 20.8%、同比下降 38.2%；各地网信办举报部门受理 145.1 万件，环比下降 16.0%、同比下降 22.5%；全国主要网站受理 1133.9 万件，环比下降 2.0%，同比增长 10.5%。



在全国主要网站受理的举报中，微博、百度、腾讯、阿里巴巴、新浪网等主要商业网站受理量占 70.7%，达 802.1 万件。



在各级网信部门指导下，目前全国各主要网站不断畅通举报渠道、受理处置网民举报。欢迎广大网民积极参与网络综合治理，共同维护清朗网络空间。（来源：国家网信办举报中心）

➢ 工信部持续加强电话用户实名登记管理工作维护公民网络空间合法权益

2019 年 9 月 27 日，为依法推进电话用户实名登记管理，切实维护公民在网络空间的合法权益，有效适应防范治理电信网络诈骗等工作面临的新形势、应对新挑战，近期，工业和信息化部办公厅印发了《关于进一步做好电话用户实名登记管理有关工作的通知》（下称《通知》），指导电信企业扎实开展电话用户实名登记工作，夯实网络诚信体系建设基础。

近年来，工业和信息化部积极落实《反恐怖主义法》《网络安全法》等法律法规，在实现全部电话用户实名登记基础上，通过完善长效制度、组织联网核查、开展监督检查、加大考核问责，不断提升电话用户登记信息准确率。此次印发《通知》，从夯实基础管理、加大防范治理、强化技术监管等三方面提出了 11 项具体举措加强管理，进一步巩固工作成效。

一是为确保电话入网环节人证一致，创新运用人工智能等技术手段，要求电信企业自 2019 年 12 月 1 日起在实体渠道全面实施人像比对技术措施，人像比对一致后方可办理入网手续。

二是深入防范治理二次倒卖电话卡，各电信企业应于 2019 年 11 月底前，完善电信服务协议条款，明确用户不得二次转售、倒卖电话卡，并充分运用海报、广告、短信等多种方式积极开展宣传提醒，引导用户至正规营业场所购买电话卡。

三是积极防范用户名下不知情办卡，要求电信企业自 2019 年 12 月 1 日起通过自有营业厅向用户提供查询名下手机号码的服务，对用户提出存在异议的手机号码应立即组织核查和处理，切实维护群众合法权益。

下一步，工业和信息化部将坚持网络安全为人民、网络安全靠人民的工作理念，加大监督检查、强化考核问责、督促工作落实，持续从严推进电话用户实名登记管理，为推进网络诚信体系建设和网络空间综合治理奠定坚实基础。（来源：工业和信息化部 网络安全管理局 ）

五、本期重要漏洞实例

➢ Adobe Flash Player 信息泄露安全漏洞

发布日期：2019-09-26
更新日期：2019-09-30
受影响系统：
Adobe Flash Player <= 32.0.0.192
描述：

CVE(CAN) ID: CVE-2019-8075
Adobe Flash Player 是一款跨平台、基于浏览器的多媒体播放器产品。
Adobe Flash Player 32.0.0.192 及更早版本，在实现中存在同源策略绕过安全漏洞。攻击者可利用该漏洞获取当前用户上下文信息。

<*来源：vendor
*>

建议：

厂商补丁：
Adobe

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：
https://helpx.adobe.com/security/products/flash-player/apsb19-30.html
https://get.adobe.com/flashplayer/
https://chromereleases.googleblog.com/
https://portal.msrc.microsoft.com/en-US/security-guidance

➢ 多款 D-Link 产品远程代码执行漏洞

发布日期：2019-09-26
更新日期：2019-09-30
受影响系统：
D-Link DIR-655C
D-Link DIR-866L
D-Link DIR-652
D-Link DHP-1565
描述：

CVE(CAN) ID: CVE-2019-16920

D-Link DIR-655C 等都是一款无线路由器。
多款 D-Link 产品在实现中存在远程代码执行安全漏洞。通过发送任意输入到"PingTest"设备通用网关接口，攻击者可利用该漏洞注入命令，进而入侵系统。

<*来源：vendor
*>

建议：

厂商补丁：
D-Link

据厂商提供的信息，这些产品已于 2019 年 9 月 25 日停止更新，相关信息请随时关注厂商主页：
http://www.dlink.com/
参考：https://fortiguard.com/zeroday/FG-VD-19-117

➢ Linux kernel 信息泄露安全漏洞

发布日期：2019-09-26
更新日期：2019-09-30
受影响系统：
Linux kernel < 4.17
描述：

CVE(CAN) ID: CVE-2019-16921
Linux kernel 是开源操作系统 Linux 所使用的内核。
Linux kernel 4.17 之前版本，在实现中存在安全漏洞，该漏洞源于 drivers/infiniband/hw/hns/hns_roce_main.c 文件的 hns_roce_alloc_ucontext 没有初始化 resp 数据结构。攻击者可利用该漏洞从内核栈内存中获取敏感信息。

<*来源：vendor
*>
建议：

厂商补丁：
Linux

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：

https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=df7e40425813c50cd252e6f5e348a81ef1acae56
https://github.com/torvalds/linux/commit/df7e40425813c50cd252e6f5e348a81ef1acae56

➢ IBM Sterling B2B Integrator 信息泄露漏洞

发布日期：2019-09-26
更新日期：2019-09-30
受影响系统：
IBM Sterling File Gateway 2.2.0.0 - 6.0.1.0
描述：

CVE(CAN) ID: CVE-2019-4280

IBM Sterling File Gateway 是一套文件传输软件。
IBM Sterling B2B Integrator Standard Edition 在实现中存在信息泄露漏洞。攻击者可利用该漏洞获取 HTTP 请求内的敏感信息。

<*来源：vendor
*>

建议：

厂商补丁：
IBM

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：
https://www.ibm.com/support/pages/node/957207
https://exchange.xforce.ibmcloud.com/vulnerabilities/162769?_ga=2.15461558.108136552.1569830969-405391723.1569306263
https://exchange.xforce.ibmcloud.com/vulnerabilities/160503?_ga=2.208809746.108136552.1569830969-405391723.1569306263

六、本期网络安全事件

➢ 全球首例:苹果 Apple Card 用户遭盗刷，物理卡或被克隆

2019 年 10 月 10 日，苹果在春天正式推出了 Apple Card 信用卡，这一信用卡特色是隐去了很多关键信息，保证卡片足够的安全能防止盗刷。Apple Card 信用卡没有卡号也没有 CVV 码等信息，只保留有用户的名称，看似足够的安全，但情况并不是想象的那样美好。

据外媒 9to5mac 报道，美国网友 David 表示，自己的 Apple Card 最近被盗刷，Apple Card 在没有丢失的情况下，自己的信用卡却在几百英里的地方被盗刷。

他与苹果方面取得联系，但苹果并未给出答复，苹果称，这样一张 Apple Card 同时出现在两个地方的情况非常罕见，官方将继续调查这一问题。

虽然，Apple Card 上没有 CVV 和卡号信息，但是仍然保留有芯片和磁条，这名用户的 Apple Card 很有可能是被其他设备克隆，然后才被盗刷。（来源：IT 之家）

➢ “黑客”入侵网站获取公民信息 3 个月非法牟利近百万元

2019 年 10 月 10 日，记者从四川省绵阳市北川县公安局获悉，近日，北川县公安局破

获一起公安部督办的侵犯公民个人信息案件，3 名嫌疑人通过非法入侵贷款、购物、交易等网站，第一时间非法获取公民信息并整理出售，3 个月时间内获取并出售 20 余万条公民个人信息，非法获取利益近百万元。

据介绍，2018 年底，北川县公安局网络安全部门经过大量工作摸排梳理，发现绵阳辖区有一条由“黑客”和“中间商”搭档建立的贩卖公民个人信息的庞大的黑色产业链。通过侦查，北川县公安局发现该团伙利用“黑客”扫描、植入等攻击手段入侵各贷款、购物、交易等网站，盗取公民个人信息。在各个网站第一时间非法获取公民的信息后，该团伙又在第一时间进行整理出售，造成了很多人刚好办理了网贷、购车、购房等业务后，立刻就接到各类骚扰电话或是诈骗电话。

嫌疑人指认现场和作案工具（警方提供）

该案线索获取后，绵阳市公安局和北川县公安局高度重视，立即成立了市、县联合侦破专案组。公安部将此案挂牌为部督案件，指定北川县公安局办理。经过大量警力深入的研判、调查、摸排，四川绵阳、湖北孝感两处窝点浮现了出来。2019 年 3 月，在证据确凿、信息锁定后，在湖北省孝感市公安的支持下，北川公安专案侦办民警兵分两路，同时在两个城市实施抓捕。在孝感市抓捕了武某，在绵阳市抓捕了杨某和杨某某。抓获时，两处窝点人员正在家里实施网上“黑客”操作。

经突审，杨某等 3 人是一个犯罪团伙，均为网络“黑客”。据杨某交待，初中毕业后，他没有继续读书，也没有工作，平常喜欢打游戏玩电脑。由于没有工作，没有经济来源供自己玩游戏，就开始钻研“黑客”。2018 年底，他开始通过“黑客”入侵、植入等方式，盗取公民个人信息。杨某每日不同时段进入网站数据库对网民申请贷款时、购物时留下的姓名、身份证号码、手机、贷款用途、贷款金额等信息进行抄写，并整理成 50 或 100 条一个的 TXT 文档，然后第一时间将“鲜活”的公民个人信息大量贩卖给下游团伙。

杨某在从事非法侵犯公民信息过程中，在网上认识了湖北省孝感市的武某，与他一样从事“黑客”，二人于是联合起来共同实施犯罪。后来，在他认为工作量很大的时候，又动员同样无业的表弟杨某某前来帮忙。

杨某交待，他们每天出售公民个人信息几千条，收入上万元。3 个月时间，团伙非法获利近百万元。2019 年 6 月，北川县公安局对杨某等 3 名犯罪嫌疑人以侵犯公民个人信息罪依法提起公诉。近日，法院判处杨某和武某三年六个月和三年两个月的有期徒刑，杨某某被取保候审。（来源：中国新闻网）

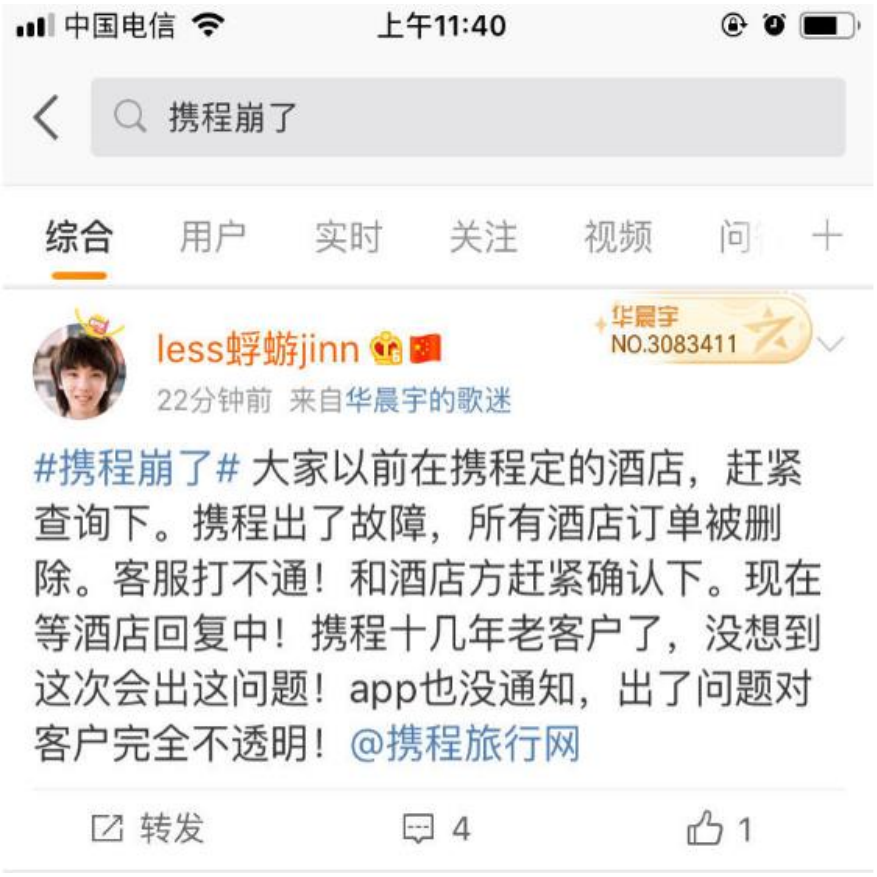
➢ 黄金周大量酒店订单系统突然崩溃 携程:预订故障已修复

2019 年 10 月 2 日，有微博平台大量网友爆料称，在携程预订的酒店住宿单无法确认，有人的已付款订单在携程 App 上显示未支付或订单不存在，有人入住时被告知酒店方面未收到订单，有人无法取消订单。在出现这些问题的同时，携程的客服电话又打不通。在国庆出行高峰期间，这些问题影响了他们的出行安排。

携程系统故障 旅客露宿街头

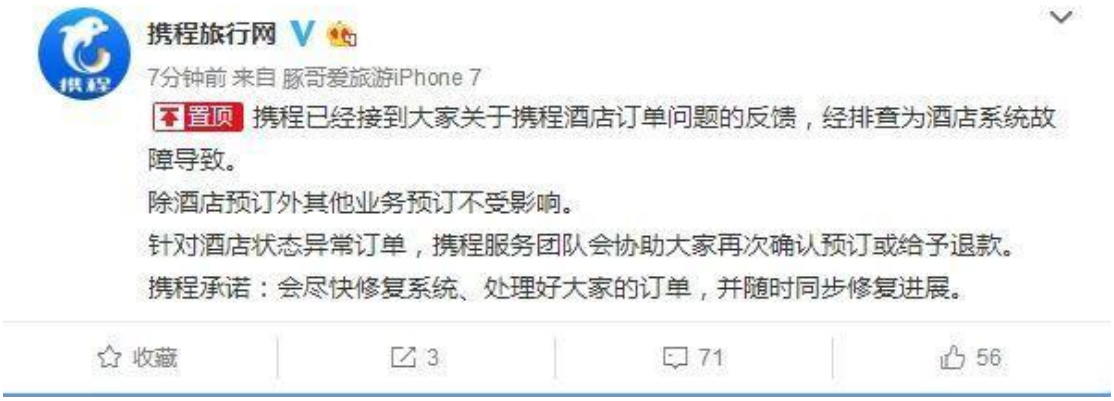
2019 年 10 月 2 日晚 11 时 16 分开始，微博网友开始在携程官方微博反映，自己在携程平台预订支付的酒店订单出问题，且客服电话打不通。

从网友留言来看，携程故障导致了多种问题，包括已付款却显示订单不存在或者已失效；到酒店前台办理入住时，被告知酒店方没有收到预定；扣款后未入住订单无法取消等问题。



预订的酒店无法入住，给在外的旅客平添不少麻烦，有转投其他酒店被狮子大开口的，有拖家带口在大堂苦等的。且旅客均反映携程平台故障时，客服电话无法拨通，APP 中客服为自动回复，旅客申诉无门。除给旅客入住带来麻烦外，多位旅客均反映，遭遇了故障期间付款预订酒店后，订单无法提交或确认，酒店无法入住的情况，在旅客更换酒店后，订单又自行确认不可退改，款项也无法退回。

对此，携程旅行网官微发布置顶公告，表示已经接到大家关于携程酒店订单问题的反馈，经排查为酒店系统故障导致。除酒店预订外其他业务预订不受影响。



针对酒店状态异常订单，携程服务团队会协助大家再次确认预订或给予退款。携程承诺：

会尽快修复系统、处理好大家的订单，并随时同步修复进展。（来源：互联网综合整理）

➢ “黑客”搞鬼？新西兰一运动商店播放色情片数小时

2019 年 9 月 29 日，运动品牌商店放色情片？还播放数小时？这一幕 29 日可“吓坏”了新西兰奥克兰市的一些路人和顾客，该品牌官方随后“澄清”：事件系黑客所为。目前，事件正在调查中。

路透社 29 日援引《新西兰先驱报》报道称，当天，奥克兰市一家运动服装零售商店亚瑟士（Asics）从清晨开始播放一段色情视频，播放时间持续数小时，直至上午 10 时左右才被店员关闭。

目击者坦尼娅•李（Tanya Lee）告诉《新西兰先驱报》，事发当时，她和自己 7 岁的儿子正在去吃早餐的路上。“我简直不敢相信我所看到的，”她说，“这简直不恰当且无礼，不是你想让孩子们接触到的东西，这也让奥克兰作为旅游胜地而蒙羞。”

这究竟是怎么一回事？

亚瑟士品牌的发言人随后发邮件向路透社证实，商店入口上方的屏幕因被黑客入侵，才播放了不当内容。发言人表示：“我们目前正在调查这一情况，并努力避免未来再次发生类似的事。”该公司还向当时看到视频内容的人致以歉意。警方向路透社表示，目前，尚未收到有关黑客入侵的任何消息。（来源：环球网）

➢ 黑客攻击事件被爆 100 万新西兰人的健康信息或处于危险之中！

2019 年 10 月 5 日，新西兰又现黑客攻击公众信息事件。黑客成功进入了 Tū Ora Compass Health 的系统，该卫生医疗机构为 Think Hauora 提供数据服务，为 Cosine，Te Awakairangi Health Network 和 Ora Toa 提供医疗服务。这些组织覆盖的地区大约有 64.8 万人，但如果算上死亡或迁移的人数，受影响的人数可能高达 100 万。

三年都没人注意 卫生部一无所知

这场危及 100 万人医疗信息的黑客攻击在三年内都没有引起人们的注意。卫生部对此次网络攻击的具体内容一无所知。

有消息称，这次将人们的医疗信息置于危险境地的黑客攻击仅仅是在一次检查中发现的。检查过程中，国家网络安全中心(National Cyber Security Centre)发现了其他入侵行为，包括 2016 年的一次“复杂”攻击，那次网络攻击窃取了人们 2002 年以来的个人数据。政府通讯安全局(GCSB)国家网络安全中心(NCSC)的分析表明，Tū Ora Compass Health 曾遭受了四次恶意网络攻击，利用众所周知的网络服务器漏洞。其中两次可以追溯到 2016 年。

共四起攻击 信息涉及 100 万人

卫生部健康主管 Dr Ashley Bloomfield 表示：自 8 月初发现这一黑客攻击以来，国家网络安全中心一直在与卫生当局合作。他说，他们当时决定，在检查系统脆弱性和尚未确定是否有数据被窃取时，不将此事告诉公众。他说，在检查卫生系统时发现，有三个地区卫生委员会容易受到网络攻击。他说，从 9 月中旬开始的检查旨在发现更多漏洞，目前检查仍在进行中。检查将包括所有卫生委员会和公共卫生组织。公共卫生组织不包括在内。

检查确定了四起黑客攻击：其中两起是由网络“黑客活动分子”发起的，如 Vanda The God，另外两起则更复杂。网络攻击通常分为国家支持、企业犯罪和个人行为三类。Bloomfield

没有透露有关这次“复杂”袭击的更多细节。

卫生部表示，存在风险的数据包括人们在哪个医疗中心登记、他们的国家健康指数(National Health Index Number)、姓名、出生日期、种族和地址。还可能包括促进健的的临床信息，如吸烟状况，糖尿病等慢性病的管理，或提供的服务。

被攻击医疗机构已道歉

Tū Ora Compass Health 首席执行官 Martin Hefford 表示：“我们不知道黑客攻击背后的动机。我们已经向警方正式报告，他们正在调查。“我们不能确定网络攻击是否导致了病人信息泄露。专家表示，我们可能永远都不会知道。然而，我们不得不做最坏的打算，这就是我们通知大家的原因。”“虽然这是网络罪犯的非法攻击，但我们有责任保护您的数据安全，我很抱歉，我们没有做好。”“虽然我们没有确切证据证明病人的数据是否被盗取，但我们建议大家对不寻常的网络请求保持警惕。”

国家党：这起攻击事件非常严重

黑客组织 Vanda the God 声称对 8 月份的事件负责，并表示：“是的，我有新西兰 100 万人的数据。”不过，国家网络安全中心表示，该黑客组织十有八九没什么信息可卖。国家党卫生发言人 Michael Woodhouse 表示，卫生部长 David Clark 必须向公众保证政府系统中信息的安全性。“这起网络安全事件可能导致人们隐私信息的泄露，包括心理健康和性健康等信息。涉及数千名过去和现在的患者。这些信息可能到达罪犯的手中。这起攻击非常严重，令人担忧。”（来源：新西兰先驱报中文网）

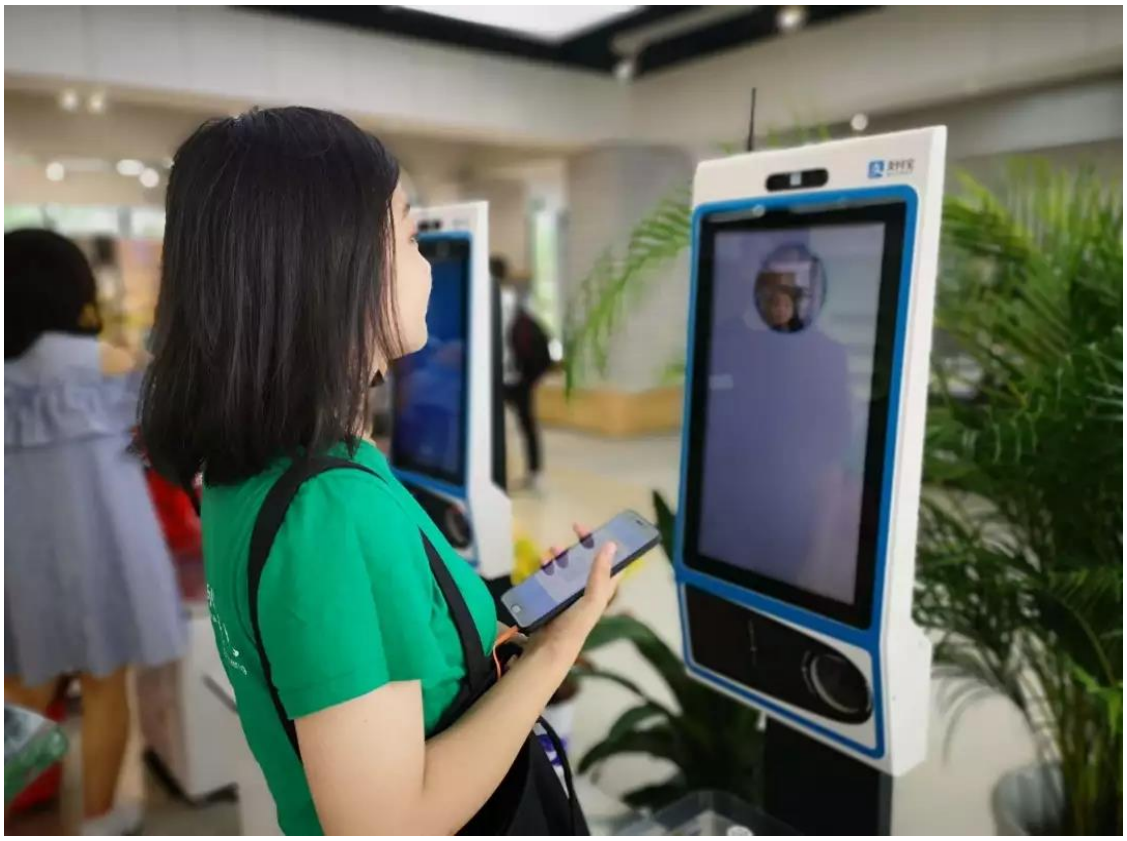
➢ 央视新闻：刷脸支付麻烦又不安全？

2019 年 10 月 9 日，央视新闻报道：随着二维码支付的普及，另一种支付方式——刷脸支付也在逐渐走进我们的生活。但当消费者和商家在对刷脸支付感到新鲜、好奇的同时，也出现了一些担忧……刷脸支付存在哪些问题，未来又能否普及？

刷脸支付鲜有人问津 消费者称麻烦又不安全

在北京的一家便利店，今年上半年安装的刷脸支付设备一直很少有人使用。便利店老板称：“顾客使用率不高，因为刷脸支付也得再去打开手机接收验证码，所以还不如直接扫二维码更方便。”

记者体验了整个支付过程：使用支付宝刷脸支付时，系统会自动关联支付宝帐号。第一次使用时，需要用户输入手机号码的后四位，下次在同一家商店使用，就可以直接完成支付。而使用微信刷脸支付时，每次都需要输入手机验证码才能完成支付。记者随机采访了几位消费者，大部分表示很少使用刷脸支付设备，并对刷脸支付的安全性表示担忧。



- 消费者：麻烦又不安全，人家一扫你的脸就支付出去了。所以你这个脸不就是一个行走的密码吗？
- 消费者：用过刷脸支付，但还是用二维码比较多。相比指纹来说，面部的抓取相对会没有技术门槛，感觉不是很安全。

北京一家数据科技公司的总裁张迎辉告诉记者，刷脸支付相较于二维码，优势在于去掉了手机这一介质。但介质的缺失，也意味着人脸信息的泄露变得更加容易。张迎辉：刷脸支付的基本原理就是将终端硬件采集到的信息，与云端存储的信息进行比对，看信息是否一致，然后解锁完成人脸支付。如果云端生物数据库发生信息泄露，那会对账户的安全带来一定风险。所以说个人信息外泄，是人脸支付可能面临的比较大的风险。

大多商家对刷脸支付不感兴趣 怕惹麻烦

去年底，支付宝推出刷脸支付产品“蜻蜓”。今年 3 月，微信刷脸支付设备“青蛙”正式上线，刷脸支付进入大规模应用阶段。除了大型超市、连锁餐厅，不少中小商户都收到了刷脸支付设备代理商的邀请。除此之外，为了鼓励商家安装，设备推销人员还会承诺，如果刷脸支付达到一定额度，可以有现金返还奖励。

尽管平台力推，还是有不少商家表示，对安装刷脸支付设备并不感兴趣。经营烟酒店的陈先生告诉记者，由于现在刷脸支付并不是很普及，考虑到成本和利用率，暂时没有安装的打算。

- 陈先生：目前我是还没计划，怕不够成熟，或者是推广度不够。一是它有设备押金，再者怕操作的过程中会失误，引起不必要的麻烦。

专家：刷脸支付隐患诸多 需加强监管

刷脸支付带来了全新的支付方式，但也有诸多隐患。中国人民大学法学院教授刘俊海对此表示，针对刷脸支付，监管部门应该尽快出台相应的法律法规，对其加强监管。除此之外，刘俊海认为，企业也应当自律，保障消费者的信息安全，减少刷脸支付的安全隐患。

央行科技司司长李伟近日也表示，线下刷脸支付技术已经较为成熟，具备了试点应用的基本条件；但在线上，开放的网络环境存在诸多风险，线上刷脸支付的应用条件并不成熟。而随着技术的发展，刷脸支付的技术中会增加指纹、掌纹、虹膜、声纹等生物信息作为辅助交叉验证。（来源：央视新闻）

信息安全意识产品年服务

021-33663299