NEWSLETTER 数据合规

2019 第十三期 /总第十三期

数据合规时事速递

北京市环球律师事务所

2019 年 12 月 17 日

目录

前 言

随着《网络安全法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。据时代的机遇与挑战。

环球律师事务所
GLOBAL LAW OFFICE

团队介绍：

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告法领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。

孟洁
合伙人律师
直线：86-10-6584-6768
总机：86-10-6584-6688
邮箱：
mengjie@glo.com.cn

一、新规速递

1. 《网络音视频信息服务管理规定》即将施行

国家互联网信息办公室、文化和旅游部、国家广播电视总局于 2019 年 11 月 29 日联合发布《网络音视频信息服务管理规定》(以下简称“《规定》”)，自 2020 年 1 月 1 日起施行。这是我国针对网络音视频信息服务领域的专门管理规定，及时回应了当前网络音视频信息服务及相关技术发展面临的问题，全面规定了从事网络音视频信息服务应当遵守的管理要求。《规定》创设了多项管理制度，以逐步探索的方式灵活地解决了技术创新应用中的相关问题，为促进网络音视频信息服务健康有序发展提供了重要指引，为保护公民、法人和其他组织的合法权益，维护国家安全和公共利益提供了有力保障。

《规定》及时回应网络音视频信息服务管理需求

网络音视频信息服务是指通过互联网站、应用程序等网络平台，向社会提供音视频信息制作、发布、传播的服务，在给企业发展带来机遇、给用户生活带来便利的同时，也带来了一定的安全风险。特别是在实践应用中，通过利用深度学习、虚拟现实等网络音视频信息服务相关技术，以及与传播领域的结合，可能被一些不法分子利用传播违法有害信息，实施网络违法犯罪活动，危害国家政治安全，损害公民、法人和其他组织合法权益。此外，部分网络音视频信息服务提供者的安全责任意识不强，管理措施和技术保障能力不健全，对网络信息安全提出了新的挑战。

“技术前进一小步，管理难度增加一大步”，新一代信息通信技术的快速发展、迭代更新和应用普及对立法机关和监管部门都提出了更高的要求。面对技术和应用发展的新情况、新问题，国家网信部门、国务院文化和旅游部门、广播电视部门把握网络音视频信息服务发展规律，立足经济社会发展管理需求，顺应广大人民群众迫切需要，本着急用先行的立法原则，及时制定出台《规定》，兼顾网络音视频信息服务健康有序发展和网络信息安全保障要求，完善监管手段措施，创新具体制度内容，是推进科学立法，实现良法促进发展、保障善治的重要体现。

《规定》立法技术的特点

相比传统领域立法，网络音视频信息服务具有较强的专业性，对立法技术也提出了更高的要求。从立法技术来看，《规定》体现了以下特点：

一是坚持问题导向，注重针对性。在人工智能、大数据等技术的推动下，网络音视频信息服务发展具有动态性，更新迭代速度快，相应带来了社会关系的快速变化，产生了换脸、深度伪造、虚假新闻等一系列问题。例如今年 8 月，一款名为“ZAO-逢脸造戏”的 APP 在社交网络上掀起了一阵“换脸”风潮，其引发的个人信息保护、侵犯知识产权和肖像权等法律问题受到社会广泛关注；再如 2018 年 4 月，一些利用深度伪造技术制作的关于美国总统特朗普的视频在网络公开传播，引起各国高度警惕。面对这些问题，《规定》及时出台，并有针对性地作了规定，明确要求不得利用网络音视频信息服务以及相关信息技术从事危害国家安全、破坏社会稳定、扰乱社会秩序、侵犯他人合法权益等法律法规禁止的活动，不得制作、发布、传播侵害他人名誉权、肖像权、隐私权、知识产权和其他合法权益等法律法规禁止的信息内容。

二是坚持统筹协调，注重系统性。网络音视频信息服务管理既涉及到提供者、使用者等多方主体，也涉及互联网信息服务、互联网新闻、互联网文化、互联网视听节目等多个领域，还涉及到多个管理部门，对此，《规定》作了较为系统的考虑和安排。其一，《规定》同时对网络音视频信息服务提供者和使用者作了界定，并要求任何组织和个人都不得利用网络音视频信息服务以及相关信息技术从事法律法规禁止的活动。其二，《规定》明确了网络音视频信息服务主管部门和监管职责，规定各级网信、文化和旅游、广播电视等部门依据各自职责开展网络音视频信息服务的监督管理工作。其三，《规定》与相关领域的法律法规作了衔接，即：网络音视频信息服务提供者和使用者违反《规定》的，由相关主管部门依照《网络安全法》《互联网信息服务管理办法》《互联网新闻信息服务管理规定》《互联网文化管理暂行规定》《互联网视听节目服务管理规定》等相关法律法规规定处理。

三是坚持把握规律，注重技术性。《规定》充分考虑到，只有着眼于技术发展规律，有前瞻性地为网络音视频信息服务的进一步发展把好方向、预留空间、提供法律制度环境，才能够充分发挥立法促进技术进步、规范产业发展、保障网络安全的作用。例如，《规定》对网络音视频信息服务提供者基于深度学习、虚拟现实等新技术新应用上线具有媒体属性或者社会动员能力的音视频信息服务并没有禁止，同时也规定应当按照国家有关规定开展安全评估的要求。此外，《规定》还要求，为网络音视频信息服务提供技术支持的主体，应当采取技术措施和其他必要措施，保障网络安全、稳定运行。

《规定》制度内容的亮点

《规定》共计十九条，明确界定了网络音视频信息服务以及服务提供者和使用者的概念，规定了网络音视频信息服务监督管理机制和相关主体责任。从具体制度内容来看，《规定》具有以下亮点：

一是压实信息内容安全管理主体责任。近年来，由于互联网行业竞争大大加剧，各类互联网企业不得不寻找新的增长点寻求转型。特别是在新技术新应用领域，一些企业在注重技术创新、产品创新的同时，并没有把信息内容安全合法合规放在同等重要的地位，导致引发各种问题。有鉴于此，《规定》对网络音视频信息服务提供者主体责任进行了明确规定，要求配备与服务规模相适应的专业人员，建立健全用户注册、信息发布审核、信息安全管理、应急处置、从业人员教育培训、未成年人保护、知识产权保护等制度，具有与新技术新应用发展相适应的安全可控的技术保障和防范措施，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、安全性和可用性。值得注意的是，与之前出台的《区块链信息服务管理规定》《微博客信息服务管理规定》等规定相比，《规定》首次增加了“未成年人保护、知识产权保护”等内容。

二是严格规范虚假新闻及非真实音视频信息管理。随着网络音视频信息服务及相关技术的不断进步，可达到高度逼真、难辨真伪的程度，特别是与传播领域应用结合，严重影响信息内容的真实性，对互联网传播秩序带来了新的挑战。对于这些风险隐患，《规定》积极谋划，作了严格规范。其一，《规定》明确禁止网络音视频信息服务提供者和使用者利用基于深度学习、虚拟现实等新技术新应用制作、发布、传播虚假新闻信息，并规定转载音视频新闻信息的，应当依法转载国家规定范围内的单位发布的音视频新闻信息。其二，《规定》强调了非真实音视频信息的标识义务，要求网络音视频信息服务提供者和使用者利用基于深度学习、虚拟现实等新技术新应用制作、发布、传播非真实音视频信息的，应当以显著方式予以标识。其三，《规定》强化了平台责任，要求网络音视频信息服务提供者加强对网络音视频信息服务使用者发布的音视频信息的管理，部署应用违法违规音视频以及非真实音视频鉴别技术。

三是建立健全网络音视频信息服务辟谣机制。网络音视频信息服务在给日常生活带来便利的同时，也为网络谣言的散播滋生了新的土壤，严重破坏网络生态环境。习近平总书记指出：“网络空间天朗气清、生态良好，符合人民利益。网络空间乌烟瘴气、生态恶化，不符合人民利益。”在 2018 年《微博客信息服务管理规定》有关要求的基础上，《规定》进一步将建立健全辟谣机制扩展到网络音视频信息服务领域，并规定网络音视频信息服务提供者发现网络音视频信息服务使用者利用基于深度学习、虚拟现实等的虚假图像、音视频生成技术制作、发布、传播谣言的，应当及时采取相应的辟谣措施，并将相关信息报网信、文化和旅游、广播电视等部门备案。

四是明确要求主管部门建立监督检查机制。在全面规定网络音视频信息服务提供者和使用者各项义务的同时，《规定》对相关主管部门监督管理职责提出了具体要求，规定各级网信、文化和旅游、广播电视等部门应当建立日常监督检查和定期检查相结合的监督管理制度，指导督促网络音视频信息服务提供者依据法律法

规和服务协议规范网络音视频信息服务行为。与此同时，为便于监管部门履行监督管理职能，《规定》也规定了网络音视频信息服务提供者的配合监督检查义务，依法留存网络日志，配合网信、文化和旅游、广播电视等部门开展监督管理执法工作，并提供必要的技术、数据支持和协助。[1]

2. 印度《个人数据保护法》几近通过，要求社交媒体平台执行用户验证

据外媒 MSPoweruser 报道，印度政府提出了一项新的隐私法案，以遏制错误信息和假新闻的传播。新法案旨在推动社交媒体网站进行用户验证，以确保减少虚假账户和假新闻。

假新闻问题目前已经成为印度政府面临的一个问题。据联系路透社的政府消息人士称，《个人数据保护法案》将迫使像 Facebook 和 Twitter 这样的社交媒体巨头设计一种方法来验证其平台上的用户。不仅如此，印度政府还希望社交媒体网站公开显示身份。其中一位消息人士表示："这个想法是为了减少假新闻和在线诱骗的传播。"

印度内阁已通过了该隐私法案，并将很快提交议会。但是，一位消息人士告诉路透社，该法案并不会很快通过，因为该法案可能会提交议会专家委员会或小组进行进一步审查。

虽然验证过程不是强制性的，但可以使公众将已验证的帐户与未验证的帐户区分开。此处的最终目标是确保用户知道该信息是由未经验证的帐户共享的，因此不能被信任。

今年早些时候，WhatsApp 添加了"转发"标签，以确保用户知道其消息已被转发。这是一种预防措施，可确保用户不会盲目转发信息。尽管该功能看上去很不错，但并没有真正发挥作用，因为用户仍在盲目地将消息转发给所有人，而没有花时间来决定新闻是否为假。对于提议的经过验证的系统，情况可能也是这样，因为用户仍将能够转发和共享来自未验证帐户的故事，而这将无法达到目的。[2]

[1] 国家互联网信息办公室。
[2] 新浪科技。

二、监管动态

1．公安部开展 App 违法违规采集个人信息集中整治，百款 App 下架整改

据国家网络安全通报中心通报，2019 年 11 月以来，100 款违法违规 App 被下架整改。

据介绍，2019 年 11 月以来，公安部加大打击整治侵犯公民个人信息违法犯罪力度，组织开展 App 违法违规采集个人信息集中整治。全国公安机关网安部门按照公安部网络安全保卫局的部署要求，集中查处整改了 100 款违法违规 App 及其运营的互联网企业。

此次集中整治，重点针对无隐私协议、收集使用个人信息范围描述不清、超范围采集个人信息和非必要采集个人信息等情形，责令限期整改 27 款，处以警告处罚 63 款，处以罚款处罚 10 款，另有 2 款被立为刑事案件开展侦查，相关案件正在侦查中。

今年以来，公安部组织开展“净网 2019”专项行动，已依法查处违法违规采集个人信息的 App 共 683 款。下一步，公安机关将坚持以打促管、以打促建，持续深入推进 App 违法违规采集使用个人信息的集中整治，发现一起，坚决查处整改一起，依法严厉打击侵犯公民个人信息的违法犯罪活动，全力铲除个人信息黑灰产乱象。[3]

2．国家标准《信息安全技术 关键信息基础设施网络安全保护基本要求》试点工作启动

2019 年 12 月 3 日，全国信息安全标准化技术委员会（以下简称信安标委）秘书处在北京组织召开了国家标准《信息安全技术 关键信息基础设施网络安全保护基本要求》（报批稿）（以下简称《基本要求》）试点工作启动会。本次试点工作旨在验证《基本要求》标准内容的合理性和可操作性，为标准推广实施积累经验，

[3] 央视新闻。

为关键信息基础设施安全保护工作提供技术支撑。

信安标委杨建军秘书长指出，关键信息基础设施网络安全标准在正式发布前进行试点，对标准指标的可行性、合理性、完备性和科学性进行综合验证，是提高标准质量的重要手段，也是推动标准应用实施的主要途径，需要试点单位、第三方测评机构在试点专家组的指导下共同合作实施。试点专家组组长冯燕春提出，标准要注重可操作性、可持续性和可发展性，标准试点工作是进行标准验证的很好的方式，具有重要意义。通过试点形成标准应用的过程文档和相应技术工具，为后续的标准推广和关键信息基础设施安全保护打好基础。

会上，信安标委秘书处介绍了去年开展的《信息安全技术 关键信息基础设施检查评估指南》（报批稿）国家标准项目试点情况，以及本次《基本要求》试点方案、标准基本内容及评价要点。试点专家组针对试点工作和标准应用提出了意见和建议，并对试点工作的开展进行了指导。试点单位分享了本单位相关系统的建设及安全防护情况，第三方测评机构针对标准试点工作介绍了测评实施的思路和建议。

本次试点工作在电信、广电、能源、交通、金融、卫生健康等重点行业和领域选取了 12 家单位作为标准应用试点单位。中国电子技术标准化研究院、中国信息安全测评中心、国家信息技术安全研究中心、国家计算机应急技术处理协调中心、公安部第三研究所、公安部第一研究所、国家工业信息安全发展研究中心、中国互联网络信息中心等 8 家标准编制单位作为第三方测评机构。来自关键信息基础设施安全防护相关领域的 12 位行业和地方专家组成标准试点专家组，指导试点工作开展。[4]

3. 最高法发布《中国法院的互联网司法》白皮书，五方面展示中国法院互联网司法制度优势和治理效能

12 月 4 日上午，最高人民法院发布《中国法院的互联网司法》白皮书（以下简称《白皮书》）。这是中国法院发布的首部互联网司法白皮书，也是世界范围内首部介绍互联网时代司法创新发展的白皮书。

《白皮书》为中英文双语版，中文全文约 1.6 万字，由前言、正文、结语、附录 4 个部分组成，从 5 个方面充分展示中国法院互联网司法的制度优势和治理效

[4] 澎湃号。

能。其中，正文包括总体发展、专业审判体系、便民利民机制、在线诉讼机制、智能化应用、司法协同治理及裁判规则体系 7 个版块；附录从第七部分裁判规则体系的案例中，精选了 10 个具有代表性和影响力的互联网司法典型案例。

《白皮书》从 5 个方面反映了人民法院推进互联网司法的核心举措和主要成效：在机构职能创新方面，中国设立三家互联网法院，开辟了互联网时代司法发展的全新路径，标志着我国互联网司法探索实践正式制度化、系统化；在司法裁判规则树立方面，互联网法院利用管辖集中化、案件类型化、审理专业化的优势，审理了一批具有广泛社会影响和规则示范意义的案件，促进了网络治理法治化；在诉讼规则探索方面，三家互联网法院和各地法院陆续制定出台各类规程、规范，推动建构现代化诉讼制度；在技术应用方面，各地法院广泛运用大数据、云计算、人工智能、区块链、物联网等前沿科技，推动诉讼模式深层变革；在司法便民方面，中国法院依托互联网，大力推进“互联网+诉讼服务”，着力打造一站式多元解纷机制和一站式诉讼服务中心，打造立体化诉讼服务。

《白皮书》图文并茂地反映了中国法院互联网司法发展的基本路径、价值取向、主要举措和重要成果。《白皮书》显示，互联网司法已从早期的单点突破、各自为战，转向顶层规划、整体推进。应用广度从单一领域向全方位拓展，探索主体从互联网法院向全国法院延伸，变革内容从数字化向网络化、智能化升级，工作重心从机制创新向规则确立演进。随着改革不断深入，互联网技术在司法领域的落地场景越来越多，与诉讼制度和审判模式实现了有机融合。

据介绍，《白皮书》附录中的 10 个典型案例，立足互联网审判，以期为同类型互联网纠纷提供可借鉴的审判思路，为社会公众依法维护自身合法权益、规范互联网从业者行为提供指引，推动网络空间治理法治化。[5]

最高人民法院副院长李少平介绍，这是中国法院发布的首部互联网司法白皮书，也是世界范围内首部介绍互联网时代司法创新发展的白皮书。

杭州、北京、广州三家互联网法院是探索在线诉讼规则和治理规则的“先锋”，目前已在大数据权属、虚假流量治理等类型案件中作出了创新性判决。然而，目前互联网法院受理的涉及互联网规则的案件比例较低，未来互联网司法的专业性如何提升仍待实践检验。

[5] 中国法院网。

区块链已落地司法场景

我国目前设立了三家互联网法院，对于其他普通法院，采用互联网技术开展审判工作的渠道将是“移动微法院”。李少平在 12 月 4 日的发布会上介绍，2019 年 3 月，12 个省（区、市）开展“移动微法院”试点，依托微信小程序打造电子诉讼平台，将部分诉讼环节迁移到手机移动端办理。截至 2019 年 10 月 31 日，移动微法院实名注册用户达 116 万人，注册律师 7.32 万人，在线开展诉讼活动达 314 万件。

相关人士告诉 21 世纪经济报道记者，目前，最高人民法院和全国 31 个省、自治区、直辖市及新疆生产建设兵团已全部上线统一标准的“移动微法院”小程序，并且实现总入口和分平台的全面连接。

最高人民法院司改办主任胡仕浩在发布会上介绍，未来“移动微法院”功能将高度集成整合，通过这一个平台全面实现在线诉讼服务、在线调解、在线审理、在线执行、在线公开等，丰富平台功能，优化使用体验。

上述相关人士认为，未来“移动微法院”可能增加区块链功能模块，用于电子证据存储。目前，区块链可谓最火的司法技术。李少平介绍，最高人民法院已建设“人民法院司法区块链统一平台”，完成超过 1.94 亿条数据上链存证固证，利用区块链技术分布式存储、防篡改的特点，有效保障证据的真实性，极大减轻法官认定证据的难度。

在大数据领域，李少平介绍，最高人民法院建设了人民法院大数据管理和服务平台，可以实时汇集全国 3507 个法院的审判执行、人事政务、研究信息等数据。2019 年 10 月 31 日，已汇集全国法院 1.925 亿案件数据，目前已成为全世界最大的审判信息资源库。

推动制定电子诉讼法

互联网司法并非仅仅将互联网技术应用于司法，而是要在采用互联网技术后，探索在线诉讼规则和互联网治理规则。

在线诉讼规则方面，李少平说，“例如，当事人不按时参加在线庭审的，根据规则如何处理；庭审中擅自退出的，对当事人会产生何种法律后果；电子送达适用范围、条件和效力等等。”

2018 年 9 月，最高人民法院制定印发《关于互联网法院审理案件的若干问题的规定》，有效明确了身份认证、在线立案、电子证据、在线庭审、电子送达、电子卷宗等在线诉讼规则，为完善在线诉讼程序和规则作出了有益探索。

三家互联网法院和各地法院也陆续制定出台了诉讼规程、诉讼指南、审判手册等文件，细化在线审理规程、明确在线诉讼规范。

北京大学法学院副院长薛军认为，互联网法院不是类似于知识产权法院、金融法院那样的审理专门类型案件，体现审判专业化分工的专门法院。互联网法院应该探索司法体制在互联网时代会呈现出何种特征，运用何种互联网技术，一方面保证程序的公正和有效，另一方面又能够便利当事人参与诉讼，极大地提高审判效率，降低司法制度运行的成本。

胡仕浩在发布会上介绍，最高法将积极研究在线诉讼新模式对诉讼理念、诉讼原则、诉讼规则带来的深刻影响。条件成熟时，推动立法机关制定专门的“电子诉讼法”，实现诉讼制度的创新与飞跃。

法院不要满足于调解结案

除了探索在线诉讼程序规则，互联网司法还需要探索互联网案件实体裁判规则，成为网络空间治理的重要一环。

目前，三家互联网法院均已审理了一些互联网行业新型案件，确立了相关的裁判规则。比如杭州互联网法院审理的淘宝诉美景公司案，对于确定互联网行业中大数据作为一种财产应该归谁所有具有重要意义。

“随着平台经济的兴起，互联网新型纠纷案例在不断出现，法院要把握住平台经济发展的新趋势，对于当事人起诉到法院的案件，要着力打造精品，不要满足于调解结案，通过法院的裁判为新类型的经济活动确立规则。”薛军告诉 21 世纪经济报道记者。[6]

白皮书的全文链接

http://wlf.court.gov.cn/upload/file/2019/12/03/11/40/20191203114024_87277.pdf

[6] 凤凰网。

4. 央行科技司司长李伟：做好数据资产、分级、共享管理

12 月 1 日，第四届中国新金融高峰论坛成功举办。此次会议以“新形势下的金融业变革与开放”为主题。会上，中国人民银行科技司司长李伟表示：

金融行业的数据治理存在这样四个问题：一是存在信息孤岛，有数不能用；二是数据质量不高，有数不好用；三是融合应用困难，有数不会用；四是治理体系缺失，有数不善用。

前不久召开的十九届四中全会，首次将“数据”列为生产要素参与分配，标志着以数据为关键要素的数字经济进入了新时代。当前，以人工智能、区块链等为代表的数字技术不断涌现，快速向经济社会各领域融合渗透。以数据为核心的数字化转型已是大势所趋。

首先，面临的数据治理困难，即数据治理之“困”。

第一，存在信息孤岛，有数不能用。当前，金融业数据治理过程中普遍存在“不愿、不敢、不能”共享的问题，导致海量数据散落在众多机构和信息系统中，形成一个个“数据烟囱”。

一是不愿共享，多数机构都将数据作为战略性资源，认为拥有数据就拥有客户资源和市场竞争力，主观上不愿意共享数据；与之类似，机构内部数据权属分割，数据所有权和事权密切相关，部门宁愿将数据“束之高阁”，也不愿轻易拿出来共享。

二是不敢共享，部分金融数据具有一定敏感性，涉及用户个人隐私、商业秘密甚至国家安全，数据共享可能存在法律风险，客观上给机构间共享数据带来障碍。

三是不能共享，由于各机构数据接口不统一，不同机构的数据难以互联互通，严重阻碍数据开放共享，导致数据资产相互割裂、自成体系。（数据孤岛的产生不能怪数据所有者，因为数据产生的初衷肯定是自己用，而并不是为了让别人用，以后也会如此）

第二，数据质量不高，有数不好用。金融科技背景下，高质量数据成为金融服务与创新的重要基础，也是大数据提升金融精准施策能力的关键前提。然而，当前金融业整体数据质量不高现象依然突出，给数据深入挖掘与高效应用带来困难。

在完整准确性方面，由于缺乏统一的数据治理体系，有些金融机构在数据采集、存储、处理等环节可能存在不科学、不规范等问题，导致错误数据、异常数据、缺失数据等脏数据产生，无法确保数据的完整性和准确性。

在一致性方面，由于业务条线繁杂、业务种类多样，多个部门往往数据采集标准不一、统计口径各异，同一数据源在不同部门的表述可能完全不同，看似相同的数据实际含义也可能大相径庭，数据一致性难以保障。这给全局数据建模、分析、运用造成障碍，数据挖掘效果大打折扣。

第三，融合应用困难，有数不会用。金融数据来源众多、体量庞大、结构各异、关系复杂。从如此繁杂的海量金融数据中挖掘高价值、关联性强的高质量数据，需要高效的信息技术支撑和可靠的基础设施保障。然而，部分金融机构科技研发投入相对不足、科技人员占比严重失调，利用数据建模分析解决实际问题的能力有待提高。

信息资源利用大多停留在表面，数据应用尚不深入、应用领域相对较窄、数据与场景融合不够，导致数据之“沙”难以汇聚成“塔”，海量数据资源无法盘活，数据潜力得不到充分释放。

第四，治理体系缺失，有数不善用。我们常说，技术本身是中性的，技术运用的善恶完全取决于人，我认为这一结论对数据同样适用。科技要向善，数据也同样要向善。然而，由于法律法规尚不健全、数据治理体系还不完善、机构合规意识不足，数据“不善用”的问题较为突出。

从业机构违法违规成本低，为谋求商业利益而置现有管理规定于不顾，过度采集数据、违规使用数据、非法交易数据等问题屡见不鲜。例如，某些 APP、网站，用户不授权提供手机号、通讯录、地理位置等信息，就无法继续使用和浏览，通过“服务胁迫”来达成“数据绑架”。

此外，部分机构数据保护意识、内部管理、技防能力薄弱，数据泄露事件时有发生，用户成为“透明人”，电信欺诈、骚扰电话、暴力催收等屡禁不止，严重侵害用户权益。

数据治理应遵循的基本原则，也就是数据治理之“道”。

一是依法合规，保障安全。数据作为重要的生产要素，确保数据安全应是始终

恪守的底线。金融业是对信息安全高度敏感的行业，应建立健全数据安全管理长效机制和防护措施，严防数据泄露、篡改、损毁与不当使用，依法依规保护数据主体隐私权在数据治理过程中不受侵害，不能因开展跨部门数据融合应用而突破现有法律法规与监管规则。

二是物理分散，逻辑集中。由于历史原因，很多机构往往存在“N”个数据中心（数据源），呈现出多个业务条线数据分散存储、分散运行的局面，若采用“推倒重来”的方式显然成本太高、阻力太大。

因此，应在保持现有数据中心职能不变的前提下，维持当前数据物理存放位置和运行主体不变，充分利用各数据中心 IT 设施和人财资源，构建“1 个数据交换管理平台+N 个数据中心（数据源）”的数据架构格局。在此基础上，制定实施统一的数据管理规则，实现数据的集中管理。

三是最小够用，用而不存。数据治理的一大难点就是如何在保障数据所有权基础上实现数据的融合应用。应消除数据所有方因信息“所有权让渡”造成“事权转移”的顾虑，规范数据使用行为，严控数据获取和应用范围，确保数据专事专用、最小够用、未经许可不得留存，杜绝数据被误用、滥用。在满足各方合理需求前提下，最大限度保障数据所有方权益，确保数据使用合规、范围可控。

四是一数一源，一源多用。当前，无论是金融管理部门还是金融机构，各业务条线数据分散现象或多或少存在，数据多头收集时有发生。这不但增加信息报送、采集、存储成本，也导致数据责任主体不明，数据安全、数据质量难以保障。应明确源数据管理的唯一主体，保障数据完整性、准确性和一致性，减少重复收集造成的资源浪费和数据冗余。同时，建立数据规范共享机制，提升数据利用效率和应用水平，实现数据多向赋能。

做好数据治理工作的意见，也就是数据治理之“术”。

第一，做好顶层设计，把数据规划好。数据治理是一项长期、复杂的系统工程，要在组织、机制和标准等方面加强统筹谋划。

一是优化组织架构。充分认识数据的重要战略意义，将数据治理纳入企业中长期发展规划，及时调整组织架构，明确内部数据管理职责，理清数据权属关系，自上而下推动数据治理工作。

二是完善应用机制。在保障各方数据所有权不变前提下，统筹规划全局数据架构，完善跨机构、跨领域数据融合应用机制，实现数据规范共享和高效应用。

三是构建标准体系。建立涵盖金融数据采集、处理、使用等全流程的标准体系，打造金融数据的“通用语言”，提升金融数据质量，为数据互通、信息共享和业务协同奠定坚实基础。

第二，健全治理体系，把数据管理好。

一是做好数据资产管理。根据统一的数据标准体系，建立全局数据模型和科学合理的数据架构。在此基础上，管理维护全局数据资产目录，实现对数据资产的全面梳理和有效管控，解决数据质量不高、数据利用不足等问题。

二是做好数据分级管理。综合国家安全、公众权益、个人隐私和企业合法利益等因素，制定数据分级标准，基于全局数据资产目录将数据进行分级。针对不同等级数据采取差异化的控制措施，实现数据精细化管理。

三是做好数据共享管理。规范数据共享流程，确保数据使用方在依法合规、保障安全前提下，根据业务需要申请使用数据。数据所有方按规则审核确定数据使用范围、共享方式等，通过数据交换机制实现数据有序流转和安全应用。

第三，加强安全管控，把数据保护好。要遵循“用户授权、最小够用、全程防护”原则，充分评估潜在风险，把好安全关口，加强数据全生命周期安全管理，严防用户数据的泄露、篡改和滥用。

在采集环节，要向被采集用户进行明示，明确告知采集和使用的目的、方式以及范围，在获取用户授权后方可采集。

在存储环节，通过特征提取、标记化等技术将原始信息进行脱敏，并与关联性较高的敏感信息进行安全隔离、分散存储，严控访问权限，降低数据泄露风险。

在使用环节，借助模型运算、多方安全计算等技术，在不归集、不共享原始数据前提下，仅向外提供脱敏后的计算结果。

第四，强化科技赋能，把数据应用好。数据治理的核心环节是数据应用，要从

算力、算法、存储、网络等维度加强技术支撑，切实增强数据应用能力。

在算力方面，加快分布式架构转型，充分发挥云计算等技术高性能、低成本、可扩展的优势，满足海量数据分析处理对计算资源的巨大需求。

在算法方面，基于深度学习、神经网络等技术设计数据模型和分析算法，提升数据洞察能力和基于场景的数据挖掘能力，为数据插上翅膀，让数据在金融领域展翼翱翔。

在存储方面，探索与互联网交易特征相适应、与金融信息安全要求相匹配的数据存储方案，稳步推动分布式数据库金融应用，实现数据高效存储和弹性扩展。

在网络方面，运用物联网技术丰富数据采集维度，利用 5G 技术带宽大、速度快、延时低等优势提升数据流转效率，打造金融数据“高速公路”。[7]

5. 央行 2019 中国金融稳定报告提及互金整治：网贷风险仍需关注

近日，中国人民银行发布了《中国金融稳定报告（2019）》，对 2018 年以来我国金融体系的稳健性状况进行了全面评估。报告认为，2018 年以来，全球经济政治格局仍处于深度调整过程中，中国经济金融发展面临的外部挑战明显增多。

报告指出，受内外部多重因素影响，中国经济中一些长期积累的深层次矛盾逐渐暴露，金融风险易发高发，经济增长面临的困难增多。从国际上看，世界经济增速“见顶回落”的可能性增加，全球范围内的单边主义和贸易保护主义情绪加剧，金融市场对贸易局势高度敏感，全球流动性状况的不确定性上升。国内方面，金融风险正在呈现一些新的特点和演进趋势，重点机构和各类非法金融活动的增量风险得到有效控制，但存量风险仍需进一步化解，金融市场对外部冲击高度敏感，市场异常波动风险不容忽视。

报告认为，过去的一年中，在国务院金融稳定发展委员会统一指挥协调下，人民银行会同相关部门，按照攻坚战总体要求，针对不同风险分类施策，对威胁金融稳定的重点领域风险，及时“精准拆弹”；对可能持续存在的潜在风险，采取主动措施进行逐步化解，实现“慢撒气、软着陆”；对于体制机制性不足，持续推动监管改

[7] 金融科技。

革，弥补监管短板；对于将来可能显现的“黑天鹅”和“灰犀牛”风险，强化日常风险监测与评估，做好各类风险处置预案。同时，在风险化解和处置过程中，把握政策节奏和力度，适时预调微调，防范“处置风险的风险”，有效保障了金融市场和金融机构的平稳运行。通过一年多的集中整治和多措并举，防范化解金融风险方面取得积极进展，有效稳住了宏观杠杆率；平稳有序处置了包商银行等高风险机构；大力整顿金融秩序，存量风险有序压降；稳妥化解中小银行局部性、结构性流动性风险，有序处置民营企业债券违约事件；出台资管新规、系统重要性金融机构监管相关指引文件，补齐监管制度短板。总体来看，我国金融风险由前几年的快速积累逐渐转向高位缓释，已经暴露的金融风险正得到有序处置，金融市场平稳运行，金融监管制度进一步完善，守住了不发生系统性金融风险的底线。

报告提到，重点机构和各类非法金融活动的增量风险得到有效控制，但存量风险仍然比较突出。个别金融控股集团、农村金融机构风险可能暴露，互联网金融特别是网络借贷风险仍需关注，非法集资形势仍然复杂。

关于互联网金融专项整治方面，报告披露：一是网络借贷机构从 5000 家减少到 1490 家，国内 173 家虚拟货币交易及代币发行融资平台已全部无风险退出；二是完成非银行支付服务市场专项整治工作，整顿市场秩序。从严监管持证机构，组建网联平台，开展“断直连”工作并按计划顺利完成支付机构客户备付金集中存管；持续打击无证经营支付业务行为，截至 2019 年 6 月，共清理处置 389 家无证机构，其中 69 家移送公安、工商等部门；三是继续严厉打击非法集资活动，及时查处大案要案。截至 2019 年 4 月末，共摸排发现互联网资产管理机构 282 家，其中，202 家机构存量清零，47 家停业失联机构已列入经营异常名录并提请市场监管部门吊销营业执照，31 家机构已移送公安部门、处置非法集资工作机制进行打击取缔。[8]

6. 金融 APP 备案开闸 首批 23 家机构试点

金融业移动金融客户端应用软件备案试点工作拉开大幕，关于移动金融 APP 的监管顶层设计也浮出水面。

12 月 9 日，首批 23 家机构试点备案名单出炉，包括 16 家银行类金融机构（含 5 家国有大行、5 家股份行、3 家城商行、2 家农商行和 1 家农信联社）、4 家证券基金保险类金融机构，以及 3 家非银支付机构。

[8] 腾讯网。

今年来，公安部已依法查处违法违规采集个人信息的 APP 共 683 款。记者获悉，央行此前已向部分金融机构定向下发《关于发布金融行业标准加强移动金融客户端应用软件安全管理通知》（简称“237 号文”）。通知显示，央行对移动金融 APP 安全问题进行管理规范，主要从提升安全防护、加强个人金融信息保护、提高风险监测能力、健全投诉处理机制、强化行业自律 5 个方面入手，并对备受关注的个人金融信息保护划定了四大红线。

备案流程明晰

12 月 3 日，中国互联网金融协会在京召开移动金融 APP 备案管理工作试点启动会议。会议明确，各试点机构应于 2019 年底前完成首批试点备案 APP 的材料提交和备案申请。

下一步，协会将会在全国范围内分批次组织开展 APP 备案推广，并逐步落实风险信息共享、投诉处置机制以及行业公约、黑白名单、自律检查、违规约束等自律管理工作。

上述知情人士告诉记者，这次试点工作的备案要点主要有三方面：“依托备案管理系统开展全线上的资料上传和审核；备案分为机构基本信息登记、APP 信息登记和 APP 软件上传三部分，系统所有项目均需填写；试点期间各试点单位至少提交一款有代表性的资金交易类或个人信息采集类 APP 进行备案。”

同时，按金融类 APP 首次发布、重大变更、一般变更或紧急变更、注销等不同情形，明晰了备案流程。“首次发布（申请备案提交材料）、重大变更（申请变更备案更新材料），经过受理审核，再完成备案/更新备案，才能实现公告和上架；对于已上架 APP，需要一般变更或紧急变更的，可提供变更备案更新材料，再受理审核，最后更新备案公告；对于注销 APP，需提交注销备案申请材料，受理审核，注销备案再公告及下架。”上述知情人士介绍。

安全规范四大红线

中国互金协会推动的移动金融 APP 备案试点背后，是央行“237 号文”明确中国互金协会需承担以下三大职责——风险监测（健全风险共享机制、加大联防联控）；投诉处理（通过机构核实、现场检查、技术检测、专家评议等方式查证，并督促整改）；加强自律管理，其中要求制定行业公约、建立健全行业黑名单管理，做好客户端软件实名备案等工作，同时，定期向央行报送相关情况。

“237 号文”显示，央行对移动金融 APP 安全问题进行管理规范，主要从提升安全防护、加强个人金融信息保护、提高风险监测能力、健全投诉处理机制、强化行业自律 5 个方面入手，并对备受关注的个人金融信息保护划定了四大红线。

首先，在收集、使用个人金融信息时，央行明确，各金融机构不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得收集与其提供金融服务无关的个人金融信息。第二，金融机构应采取数据加密、访问控制、安全传输、签名认证等措施，防止个人金融信息在传输、存储、使用等过程中被非法窃取、泄露或篡改。第三，在信息使用结束后，各金融机构应立即删除敏感信息，在客户端软件卸载后不得留存个人金融信息。最后，金融机构不得违反法律法规与用户约定，不得泄露、非法出售或非法向他人提供个人金融信息。

“关于数据使用的边界，不光是中国数字金融发展的问题，也是全世界都非常关注的重要问题。相对来说，在发达国家或者欧美市场，相关立法和政策规定会完善一点，特别是欧洲对这一块比较严格。”北京大学数字金融研究中心副主任黄卓分析，“对于大数据的使用和把数据作为资产进行交易，这是两个不同的层次。在符合一定授权的基础上，在合理范围内进行使用，这是一个层次；把数据作为一种资产进行交易，这是另外一个层次。到了第二个层次，需要更加严格的标准，这里还涉及数据的所有权，以及采集是不是合规、利益怎么分配等等。这方面是全世界都在探索的命题。”

与“237 号文”同步发出的《移动金融 APP 应用软件安全管理规范》，相比之前的金融行业标准，删除了应用场景、将人机交互安全改为身份证认证安全，增加了安全功能设计；修改了数据安全要求，在数据获取、数据访问控制、数据传输、数据存储、数据销毁等方面提出了具体安全要求。

该《规范》要求不同类型的软件的责任。其中，资金交易类软件应符合资金交易、信息保护等所有技术及管理安全要求；信息采集类软件应重点符合信息保护相关技术及管理安全要求；资讯查询类软件应符合相关客户端软件安全和管理要求。

客户端软件备案是什么？要做什么？为了什么？

客户端软件备案有法律依据

首先需要知道一个概念：互金协会是由中国人民银行会同银监会、证监会、保监会等国家有关部委组织建立的国家级互联网金融行业自律组织。

其主要职责包括：组织开展行业情况调查，制定行业标准、业务规范；收集、汇总、分析、定期发布行业基本数据，开展互联网金融领域综合统计监测和风险预警，并提供信息共享及咨询服务。

在《网络安全法》第十一条中明确规定：“ 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。”，这里的行业组织即为互金协会或类似组织。

该条规定为互金协会进行客户端软件备案提供了法律依据，后续的《金融科技（FinTech）发展规划（2019-2021 年）》、《关于发布金融行业标准加强移动金融客户端应用软件安全管理的通知》（即 237 号文）中的相关条款法律依据都来源于此。

据了解，各行业主管部门根据《网络安全法》相关要求都在制定客户端软件备案办法。今年 11 月，教育部发布教育 App 备案管理办法，要求相关互联网移动应用程序通过公共服务体系进行提供者备案，并将通过互联网信息服务（ICP）备案和网络安全等级保护定级备案设为前置条件。

可以预见，未来 App 备案将会成为监管常态手段，而各大行业组织、行业主管部门将会成为成为直接监管部门，行业自律或将成为监管重要组成部分。

备案是客户端软件安全管理的一部分

客户端软件对于互联网金融来说就像银行网点的业务柜台，大量的信息通过它流转与用户和金融机构之间，然而这个虚拟的柜台其实并不怎么安全。

央行科技司司长李伟在客户端软件备案管理工作试点启动会议上指出，当前一些金融机构客户端软件存在的安全防护能力参差不齐、超范围收集个人信息、仿冒钓鱼现象突出等问题。毫无疑问，这些问题是威胁金融信息安全与用户财产安全的重大威胁。

客户端软件安全管理就是为了解决这些问题。客户端软件备案只是客户端软件安全管理的一部分，甚至可以说是第一步。据了解，目前备案工作主要分为三部分：

1、依托备案管理系统开展全线上的资料上传和审核；

2、完成机构基本信息登记、App 信息登记和 App 软件上传等全部工作；

3、试点期间各试点单位至少提交 1 款有代表性的资金交易类或个人信息采集类 App 进行备案。

据媒体报道，备案流程包括首次发布、重大变更、一般变更或紧急变更、注销等不同情形。首次发布（申请备案提交材料）、重大变更（申请变更备案更新材料），经过受理审核，再完成备案/更新备案，才能实现公告和上架；对于已经上架 App，需要一般变更或紧急变更，可提供变更备案更新材料，再受理审核，最后更新备案公告；对于需注销 App，申请注销备案提交材料，受理审核，注销备案再公告及下架。

据了解，后续互金协会还会逐步落实风险信息共享、投诉处置机制以及行业公约、黑白名单、自律检查、违规约束等自律管理工作。

在 237 号文中，加强个人信息安全保护、提升安全防护能力、提高风险监测能力是文件的主要内容。文件中，央行明确提出了对个人金融信息保护的四点要求，被媒体称为“四大红线”：

第一、在收集、使用个人金融信息时，央行明确，各金融机构不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得收集与其提供金融服务无关的个人金融信息。

第二、同时金融机构应采取数据加密、访问控制、安全传输、签名认证等措施，防止个人金融信息在传输、存储、使用等过程被非法窃取、泄露或篡改。

第三、在信息使用结束后，各金融机构应立即删除敏感信息，在客户端软件卸载后不得留存个人金融信息。

第四、金融机构不得违反法律法规与用户约定，不得泄露、非法出售或非法向他人提供个人金融信息。

“实名制”提高门槛 保证安全

网络实名制在我国已经推行好多年了，这项制度有效增加了网络透明度，改善

了当时恶劣的网络环境，让互联网不再是法外之地，同时提升了网络准入门槛：只有真正的人才可以上网。

客户端软件备案可以说是 App 的“网络实名制”，对于监管来说服务提供者实名制和用户实名制同样重要；对于用户来说，则可以保证自己使用的软件是正品。

“实名制”可以预见的将会提高我国目前金融软件准入的门槛，就如同用户网络实名制一样：只有真正的金融 App 才可以提供软件服务。当然，具体操作还需要网信办、App 发布渠道等多方面协作，但是相信那一天很快会到来。[9]

[9] 新浪财经。

三、相关案例

1. 上海警方正式通报：以涉嫌非法吸收公众存款罪对麦子金服立案侦查

12 月 3 日，上海市公安局浦东分局发布通报显示，2019 年 11 月 23 日，麦子金服运营主体上海麦子资产管理有限公司（以下简称“麦子金服”）因涉嫌非法吸收公众存款被立案侦查。

根据通报，11 月 24 日，麦子金服法定代表人黄某容、联合创始人杨某敏等 16 名犯罪嫌疑人被依法采取刑事强制措施，查封相关涉案资产。

警方在通报中指出，经查，麦子金服未取得国家相关金融资质许可的情况下，通过“麦子金服财富”、“财神爷爷”等线上理财平台，向不特定社会公众非法吸收存款。目前，案件正在进一步侦查中。

警方表示，麦子金服所涉及的“麦子借款”、“白领贷”、“白领金库”、“麦芽分期”、“大房东”均系对外借款平台，涉及资金均属涉案资金，所涉借款人应依法履行还款义务。警方要求借款人将还款本息依法汇入公安机关指定账户；未及时还款的，警方将依法予以追缴。

融资存疑遭打脸

公开资料显示，麦子金服在资产端有名校贷（白领市场）、麦芽分期（消费分期）、大房东等业务，在资金端有诺诺镑客和财神爷爷业务。2015 年，麦子金服将名校贷、大房东、诺诺镑客、财神爷爷几家公司进行整合，形成了上海麦子资产管理有限公司（即“麦子金服”）。

资料显示，麦子金服成立于 2015 年 3 月，注册资本 5000 万元，法定代表人为麦子金服联合创始人兼 CEO 黄大容，杨淑敏为监事。大股东为上海爱曼商务咨询有限公司（黄大容个人持股 99%），持股比例 66.31%。第二大股东为上海诺明投资中心（有限合伙），持股比例 12.32%。

根据麦子金服官网，其运营时间超过 10 年，平台累计撮合成交 710.98 亿元，

2015 年曾获海通证券旗下海通创新战略投资。事实上，麦子金服一直负面缠身，曾曝出“获招行 B 轮融资”的乌龙事件，旗下诺诺镑客也是问题频频，接连爆出逾期、盗刷事件。

早前，招商银行曾声明表示“4 月 18 日，我行关注到有媒体发布关于招商银行参与麦子金服 B 轮融资的消息。经核实，招商银行及附属公司从未参与麦子金服融资，招商银行对以我行名义做不实宣传的行为保留追究法律责任的权利。”

而麦子金服则回应称，因其正谋求分拆上市，因此 B 轮资金需要在完成结构搭建完毕后才能入资，“目前麦子金服在搭结构进资金的过程中，故需等资金到账完毕，再向大家披露 B 轮的更详细的情况”。

值得一提的是，根据上海市第一中级人民法院此前发布的判决书，2017 年 5 月，麦子金服旗下上海诺诺镑客金融信息服务有限公司因使用“预期年化利率”与“预期年化利率最高 12%”等广告用语被上海市徐汇区市场监督管理局处以 18 万元的行政处罚。

法院经审理认为，麦子金服财富宣传“预期年化利率”、“预期年化利率最高 12%”用语，并无科学、合理的测算依据和测算方式，易误导投资者产生该金融产品保本、无风险或者保收益的误解，使投资者不能全面了解其所投资的项目可能存在的风险，而仅预期可能获得的收益，构成违法。

借壳失败打官司

2017 年，麦子金服曾计划借壳在美股上市，但最终未果。据柒财经了解，麦子金服早前借壳的上市公司为鲈乡小贷（NASDAQ：CCCR），并计划将公司名称改为“Wheat Fi－nance Service Group”（麦子金服）。

2018 年 1 月 2 日，麦子金服与鲈乡小贷股权互换交易告吹。麦子金服曾称，其已于 2017 年 12 月 29 日致函鲈乡小贷，终止了与鲈乡小贷的股权互换协议。而后，麦子金服相关负责人对柒财经表示，“未来可以期待在资本市场上的进一步动作”。

但截至目前，麦子金服并未有公开 IPO 的计划。而交易对手方——鲈乡小贷也在 2019 年 1 月更名为蝙蝠集团（China Bat Group, Inc.），而其前身为中国商业信贷有限公司（China Commercial Credit, Inc. ），在中国对应的实体公司全称为吴

江市鲈乡农村小额贷款股份有限公司。

不过，双方仍在持续对撕，并直接开打了官司。2017 年 9 月，麦子金服在美国特拉华州衡平法院就股权交换协议向鲈乡小贷提起诉讼（案件号 2017-0633-JTL）。最终不了了之，双方终止交换协议。

2018 年 7 月 30 日，仲裁员 Mentz 签署了一份合理的裁决，麦子金服败诉，被仲裁要求向鲈乡小贷（蝙蝠集团）支付 144 万美元赔偿金。由于不服判决，麦子金服计划提交一份请愿书来撤销仲裁裁决，以撤销纽约州最高法院的仲裁裁决。据了解，法院已安排举行听证会。

而今，已完成更名后的蝙蝠集团（NASDAQ:GLG）多次发布公告称，其收到纳斯达克交易所发来的退市或未能满足持续上市规则或标准的通知。此前，蝙蝠集团也曾因未达到纳斯达克挂牌的最低标准，被警告存在退市风险。

待还余额超 24 亿

值得一提的是，麦子金服还通过收购方式获得了一张小贷牌照。2018 年年底，麦子金服收购南宁市钜鑫小额贷款有限责任公司（下称“钜鑫小贷”）的 99%股权，并更名为南宁市麦子小额贷款有限公司。不过，钜鑫小贷的经营范围中并不包含网络小贷业务。

事实上，广西金融办也曾表示，麦子金服旗下诺诺镑客为互联网金融公司，目前国家互联网金融风险专项整治工作尚未结束，根据有关规定在整治期间凡是涉及互联网金融业务均暂时停止审批。随后，麦子金服以集团名义收购，并获得批准。

回到麦子金服本身，今年 10 月 16 日，麦子金服 CEO 黄大容在用户直播会上宣布，麦子金服暂停发布新标，出借人按照原借款协议正常回收对应债权。黄大容还表示，截至 2019 年 10 月 15 日，麦子经营一切正常。

据了解，截至 2019 年 8 月 31 日，麦子金服借贷余额约 24.38 亿元。黄大容称，麦子金服出借人待支付充值本金总额预计约 18 亿元，平台出借人预计约 1.6 万人，借款人预计约 19 万人，未兑付金额为 0，“麦子所撮合的每笔资金资产均一一对应, 不涉及资金池，不涉及自融”。

而在 11 月 25 日，多家媒体报道称，麦子金服的办公地点被上海市公安局浦

东分局查封，查封时间显示为 11 月 24 日。相关人士表示，麦子金服正配合警方调查。据 21 世纪经济报道报道，麦子金服创始人黄大容等高管接受警方调查，且“兑付存在困难”。

但宣称“资金资产一一对应，没有自融，没有资金池，没有碰触客户资金”的麦子金服结局已成为定局，涉嫌非法吸收公众存款被警方立案侦查。同时，黄大容等 16 名犯罪嫌疑人被依法采取刑事强制措施。[10]

2. 媒体曝光 5000 多张人脸照片 10 元兜售

五千多张人脸照片 网上 10 元被售

随着人工智能和大数据的发展，人脸信息成为越来越重要的个人信息。但经记者调查发现，就是这样对于每个人如此关键的数据信息，却在网上被公开兜售，而且价格低廉。记者在互联网平台“转转”上以关键词“人脸数据集”搜索相关信息，迅速弹出了一件名为“人脸相关算法训练数据集”的商品，标价 10 元。记者打开商品介绍后看到，这个数据集包含五千多张人脸照片。很多还是一个人不同表情的脸部照片。

照片没有经过所有者授权 被非法交易

记者通过平台的聊天功能和销售者取得了联系。当记者询问销售者是否经过照片所有者的授权时，销售者表示，“经过授权的肯定不是这个价了”。就这样，没有经过照片所有人授权的人脸照片在互联网平台被公开兜售。

中国人民大学法学院副院长杨东表示：非法交易的话对我们个人的隐私数据的侵犯是非常严重的。而且没有经过我们的允许，它会跟其它的一些个人的一些数据信息进行整合以后，非常精准地能够对人画像，从而从事非法的各种交易。

一份照片要价五毛至四毛不等

记者在百度一个名为“快眼”的贴吧，也发现有销售者在兜售人脸数据。记者联系到这位 qq 网名为“泯灭”的销售者，他告诉记者，不带身份证的大头照五毛钱一

[10] 新浪财经。

张，高清；还有一种是姓名、身份证照片、银行卡和手机号都有的，号称“四要素”，四块钱一份。记者了解到，这些数据可能被用于申请信用贷款，甚至注册公司，给泄露信息的用户带来巨大损失。

多款 APP 无协议采集人脸数据信息

不仅仅是非法兜售，记者在调查中还发现，多款 App 还存在着随意收集人脸数据信息的情况。

一款名为“人脸打分”的 App，需要用户上传照片后，方能对用户的外表进行评价。但记者发现，这款 App 却没有任何协议来确保用户上传的人脸照片不被滥用。而这款名为“证件照随拍”的 App 同样如此。就这样，在没有任何使用协议的情况下，多款此种类型的 App 在随意采集用户的人脸数据信息。

有的 App 对于用户的人脸数据信息采集过程中存在过度索取权利的问题。这款名为“颜值排行”的 App 在使用条款里就明确要求：“用户在任何时间段在 App 发表的任何内容，包括自拍的著作财产权，用户许可 App 开发者在全世界范围内免费地、长期性地、不可撤销地、可分许可地和非首批地使用的权利。”使用的权利也包括多个方面，包括但不限于复制权、发行权、出租权、展览权等。

危害个人信息安全 多家企业被约谈

在 App 中加入过度索取人脸数据信息权利的条款，本身已经触犯了法律。除此之外，还有另一个问题，就是这些采集人脸数据信息的 App 是否能够保证他们采集的人脸数据不被泄露呢？

以今年 8 月一款火爆网络的软件“ZAO”为例，这款 App 就因为用户隐私协议不规范、存在数据泄露风险等网络数据安全问题——比如人脸照片上传后不能撤销、默认授权“ZAO”及其关联公司有永久使用权等问题——被工信部约谈。而除了这家公司，工信部还曾以“存在用户个人信息收集使用规则、使用目的告知不充分的情况”约谈其它多家互联网企业。

人脸识别第一案：谁有权收集人脸信息

其实，随着人脸信息应用越来越多，人们对于它的安全意识也在逐渐提升。在浙江杭州，浙江理工大学副教授郭兵就由于不愿使用人脸识别，将杭州野生动物世

界告上了法庭。这起国内消费者起诉商家“人脸识别使用”领域“第一案”，案件的焦点就集中在：究竟谁有权收集我们的人脸信息。

人脸信息 怎样保护好又使用好？

在当下的信息社会背景下，怎样既促进人脸识别产业长远健康发展，又确保消费者的人脸信息等个人信息不被非法采集使用甚至交易？

多位专家表示，每一个消费者都亟需提高个人信息安全意识，这是确保自身个人信息安全的第一步。

我们每一个用户和消费者都应该提高我们保护个人隐私，个人数据信息的自觉意识和安全维护意识，我们接受任何服务的时候都要也认识到一个必要的原则，不能无限制的被商家对方采集我们的数据和信息。

互联网企业也要加强自律，要从企业责任出发，主动地通过行业的协会，或者是企业自身产品生产过程中，他们要制订相应的伦理的一些规约，或者是运用这些产品的准则或者是标准。

在法学专家看来，则要把人脸信息使用的种种行为都纳入法律的监管范围内，尤其是要把处理人脸信息等个人信息的算法纳入到法律的监管范围。[11]

3. 《2019 个人信息安全年度报告》发布，超七成 App 超范围获取权限

12 月 5 日，由南方都市报大数据研究院·南都个人信息保护研究中心主办的“2019 啄木鸟数据治理论坛”在北京举行。在“个人信息保护”专场，南都个人信息保护研究中心发布《2019 个人信息安全年度报告》（简称《报告》）。

《报告》指出，为实际考察 App 在个人信息收集使用方面的情况，南都个人信息保护研究中心从隐私政策透明度、移动金融类 App 权限获取情况等 3 方面展开测评。结果显示，在移动金融类 App 测评中，设备识别码被严重频繁调取，“招

[11] 新浪网。

联金融”一分钟内调用了 6109 次，而“拍拍贷借款”一分钟调用 1468 次定位权限。

针对公众关注度较高的移动金融类 App，南都个人信息保护研究中心选取 100 款下载量较高的 App，从是否超范围获取权限，尤其是危险权限、用户拒绝某权限后是否频繁申请等方面展开测评。《报告》显示，超七成 App 得分不及格，过半分数集中在 40 分和 50 分。

《信息安全技术移动互联网应用（App）收集个人信息基本规范》（草案）指出，金融借贷类 App 保障服务正常运行所需要的最少权限范围只涉及存储权限。而《报告》显示，22 款 App 强制要求获取设备识别码、定位、相机等权限，用户不同意就不能使用 App。

除了上述问题，默认获取隐私权限也是监督者重点关注的问题。2018 年 11 月，上海市消保委测评 18 款 App 并邀请企业进行沟通，多款 App 被曝存在默认获取权限问题。

在南都个人信息保护研究中心测评的 100 款移动金融类 App 中，68 款 App 存在默认获取非必要权限的行为。所谓默认获取，是指用户安装以后，打开权限设置面板，发现一些权限已经默认打开。。

在中国金融认证中心（CFCA）的技术支持下，此次测评还对移动金融类 App 一段时间调用危险权限的次数进行监测。《报告》显示，设备识别码被严重频繁调取，有 59 款 App 每分钟调用超过 100 次。

仅次于设备识别码、被频繁调用的是定位权限。共有 44 款 App 调用频率超过 50 次/分钟。

很长时间以来，App 注销难一直被用户诟病。相比之下，注册时一个手机号、一条验证码即可完成，而注销时，有的 App 要求用户提供历史登录地点等信息，有的还要求消费完代金券，甚至需要提供手持身份证照片。

《信息安全技术个人信息安全规范》规定，注销过程进行身份核验时，用户重新提供的个人信息不应多于注册、使用等环节收集的个人信息。

针对注销问题，南都个人信息保护研究中心选取了 20 款头部 App 进行测评，涉及“滴滴出行”、“QQ”、“淘宝”等。值得肯定的是，注销时身份核验的体验感显著

提升，要求用户上传有效身份证件或手持身份证照的现象完全消失。《报告》显示，19 款 App 得分在 70 分或以上，且大部分支持在线注销，需满足的条件也控制在 5 条以内。

《信息安全技术个人信息安全规范》指出，个人信息控制者宜为个人信息主题提供获取其基本资料、身份信息等个人信息副本的方法。

在隐私政策透明度方面，南都个人信息保护研究中心共检测 100 款 App，涉及购物导购、移动金融、教育文化等十个行业。《报告》显示，100 款 App 中，有 13 款达到隐私政策透明度高的层级，其中“京东金融”以 95 分位居第一，“美团”和“饿了么”以一分之差并列第二，其他透明度高的包括“百度”、“淘宝”等。。

《信息安全技术个人信息安全规范》规定，企业保存个人信息的期限为实现目的所必须的最短时间，超出期限应对个人信息进行删除或匿名化处理。然而，只有 29%的 App 有上述表示，27%的 App 没有提到保存期限，其余则表达含糊。[12]

4. 净网 2019 微信发图片原图会泄露隐私信息

近日，有消息称微信发照片时选择“发送原图”，可能会泄露拍摄定位，有专家表示的确如此，但需同时满足 3 个条件：1.手机 GPS 定位已打开；2.拍照设置保存了地理位置；3.发送原图。

实际上这其实是一个老生常谈的常识——图片所包含的信息，本来就不仅仅是视觉元素，其附带的 Exif 信息，往往能挖出很多颇具价值的信息。

用手机拍摄照片，照片会附带 Exif 信息，其中包含了手机型号、拍摄时间、其他各种拍摄参数等信息；而如果手机拍照的时候开启了记录 GPS 位置的选项，那么照片还会附带有地理位置信息。

利用微信发送原图，微信不会对这张图片有任何处理，Exif 信息自然也就原封不动地传输给了对方。而如果用微信发送的不是原图，那图片就会被压缩，从而丢失大量 Exif 信息，再也无法获知图片的原始拍摄参数，查看 GPS 定位信息也无从谈起。因此，如果想要保护隐私，就尽量不要在微信发送原图了，其他聊天工具也

[12] 南方都市报。

是一样的道理。另外，有的朋友担心朋友圈发送图片会泄露隐私，其实朋友圈发送的图片都经过压缩，Exif 信息并不完整，不会附带地理位置之类的信息，因此不必太过担心。

现在手机拍照默认会生成 Exif 信息，那么我们是否有必要对这信息进行处理、乃至删除呢？

这个看情况而论。如果你对隐私比较注重，不想让别人知道照片拍摄时的时间地点，那么发图前可以先把 Exif 删掉。另外，由于 Exif 可以记录各类摄影参数，因此有些摄影师将图片发布到影像社区的时候，也会先删除 Exif，以免他人知道自己设定的快门、光圈等信息，从而偷师。

要如何才能删掉 Exif 信息？在电脑上，最简单的方法，自然是利用 Windows 自带的功能。开启图片文件的“属性”后，找到“详细信息”，就可以在窗口左下角看到“删除属性和个人信息”的字样，点击即可进行 Exif 删除操作——既可以直接删除源文件的 Exif，也可以生成删除 Exif 后的图片文件，非常便利。

另一种比较简单的方法，就是图片压缩。前面提到过，图片压缩是导致 Exif 丢失的一大原因，为数不少的图片压缩方法都不支持 Exif 回写，因此将图片压一次，往往就能将 Exif 删除掉了。

例如微信发图片选择不发送原图，微信就会帮你压缩图片，Exif 信息就此丢失大半。又例如在 Windows 系统中用“画图”开启图片，然后将图片文件另存为另一个文件，Exif 也会丢失。但要注意，Photoshop 这样的专业图像处理软件是可以回写 Exif 信息的，不要用 Photoshop 压缩图片的方法，来删除 Exif。[13]

5. 某鞋类品牌沦为诈骗重灾区 消费者隐私泄露谁有责任

近日，有消费者投诉表示，自己于 11 月在北京某百货购买了一双某集团旗下 A 品牌长靴，时隔两天，有人自称是该集团旗下 B 品牌生产商要求给消费者退款，结果自己损失两万多人民币。除此之外，记者在调查中发现，多位消费者均接到过“B 品牌生产商”的电话，以及该集团旗下 C 品牌的消费者也接到过类似电话。面对个人信息泄露，商家有着不可推卸的责任，但对于已经造成经济损失的消费者，

[13] 环球网。

个人及品牌该如何处理？

精准诈骗 防不胜防

购买信息被泄露，精准诈骗让消费者放松警惕。近日，一位刘姓的消费者向记者表示，自己于 11 月 9 日在北京某百货二层的 B 品牌购买了一双 1295 元的长靴，时隔两天后的晚上，一个自称“B 品牌生产商”的客服人员向刘女士在电话中表示，刘女士购买该批次的鞋存在质量问题，需要召回并赔偿鞋款。同时，该“B 品牌生产商”能够准确的报出刘女士消费日期、金额及对应款式，从而让刘女士放松警惕。

利用消费者对于网上借贷功能的认知盲区进行诈骗。客服在退款过程中让刘女士通过网站链接开通某借贷通道，并声称可以通过该通道给刘女士退款。然而没过多久，该客服称，由于工作人员的失误，给刘女士的银行卡里多转入了两万多人民币，希望刘女士能退还。于是，便在对方一步步地“指导”下，向对方的微信账户转入了两万多人民币。

事发之后，刘女士才醒悟发现骗子是利用自己使用的借贷平台取现，导致自己造成了严重的经济损失。“为何自己的消费信息会被骗子利用”，刘女士对该品牌专柜的信息安全提出了质疑。在了解清楚事实真相后，记者走访了该百货的 B 品牌专柜，该专柜人员表示，可能是黑客进入后台盗取了信息，并非品牌人员故意泄露。此外，专柜人员表示，生产商不会直接接触消费者，如有召回事件也是品牌客服以“400”开头的电话联系消费者。

该集团事故频出

在走访过程中，上述 B 品牌专柜的员工表示，除了刘女士之外，也有其他消费者接到了类似的诈骗电话，但因为其他顾客与专柜人员反复确认，才避免了经济损失。同时，紧邻 B 品牌的 C 品牌专柜人员也透露，这种情况在 C 品牌也有发生，个别消费者反映接到了自称“C 品牌客服”的诈骗电话，但目前还未出现经济受损的情况。

对于上述两大品牌及刘女士受骗事件，记者以消费者的名义致电该集团售后中心得知，针对刘女士在百货诈骗事件，该集团已报警立案，但后续追踪情况并不知晓，该集团也并未设立相关部门或者具体岗位人员来负责此类事件的监督。当记者再次以记者身份向该集团联络时，客服表示，后续将对接高层领导对此进行回复。但截止发稿前，该集团并未回复。

此类案例不只是在今年频频发生，记者查阅网络资料看到，在 2015 年 5 月，该集团旗下一款的购物网站遭用户信息泄露，诈骗者以此为工具向 140 余人实施诈骗，获利上百万元。不少首次在该网站购物的用户质疑个人信息遭网站内部员工出卖，而网站官方回应是信息丢失是由于黑客“撞库攻击”，但对于未受害者赔偿事宜，该集团并未作出答复。

据了解，该集团自主经营 10 个鞋类品牌。

品牌商责无旁贷

对于客户信息的泄露，《中国名牌》杂志创始人、商务部品牌专家顾环宇在接受采访时表示，如果购买过程中商家详细登记了顾客个人信息，那么所有的商家都应对这些资料进行加密保护。一旦出现问题，企业也应担负相当部分的责任。“例如这起 2 万元的顾客损失案件，企业除了给予消费者相应的情感慰问外，还应该有一定程度的经济补偿。”顾环宇表示。

顾环宇还表示，如果该企业过去也出现过类似情况，从而说明企业本身管理有比较大的疏漏。“本质上来说，就是对于消费者的权益关心和重视程度不够。同时后续没有跟进措施、也没有相应的负责人去管理这个事件，说明企业在这方面没有制度保障。”

至于品牌如何减少、杜绝顾客信息的泄露，顾环宇表示，第一毫无疑问就是制度建设，管理层一定要从管理制度方面对顾客信息保密工作重视，具体到实际操作层面，在硬件和软件上都要落实到位，例如系统的及时防护、售后部门人员的完善等；另一方面就是企业文化方面着手，对于消费者权益的保护和重视，一定是要在意识层面进行建设。

大数据时代之下，自建线上平台来抓取客户数据来定位消费者画像已经成为不少企业、品牌的经营方式之一。随之而来的则是个人信息的频繁泄密，对于这点，顾环宇认为重视线上平台和后台数据值得肯定，但对于自检系统的检测、加固、安全工作一定要做到位。“因为不少企业就是因为多次顾客信息的泄密，最终因为多米诺骨牌效应导致口碑下降、股价下滑。”[14]

[14] 北京商报。

6. 买卖个人信息牟利，一人被起诉，三家教育培训机构受罚

因赌博欠债，就利用工作便利，目无国法，铤而走险，进行公民个人信息的买卖活动。近日，椒江警方对张某涉嫌侵犯公民个人信息罪一案移送检察机关审查起诉。

今年 8 月 1 日，市公安局椒江分局前所派出所接到椒江区市场监督管理局移交“有人涉嫌侵犯公民个人信息”的线索。接到线索后，前所派出所立即开展调查，并于当天将涉嫌侵犯公民个人信息的张某抓获。张某对其买卖公民个人信息的作案事实供认不讳。

经查，临海人张某从事教育培训行业。由于工作需要，他除了掌握大量的学生信息，还从同行业的女友电脑中，盗取了包含学生姓名、学校、生日、联系方式的公民信息 3 万余条。今年 3 月，他在椒江某教育培训机构离职时，以交换的方式，从该教育培训机构负责人处获得包含学生姓名、学校、生日、联系方式的学生信息文件 1 个，包含公民个人信息 1556 条。在此期间，张某因赌博欠了一笔债，便萌生了倒卖个人信息牟利的想法。

今年 4 月，张某应聘至椒江城区某教育培训机构万达校区。为证明自己有能力胜任工作，他以 700 元的价格向该教育培训机构负责人王某出售了公民个人信息 33123 条。与此同时，张某还在人力网、58 同城等网站，发布包含“出售公民个人信息”内容的招聘资料。6 月 14 日，张某将包含姓名、联系方式等内容的学生信息 3 万余条，以 1200 元的价格出售给另一教育机构负责人李某。

相关当事人触碰了侵犯公民个人信息这根高压线。8 月 2 日，涉嫌侵犯公民个人信息罪的张某被椒江警方依法刑事拘留。10 月 22 日，椒江区市场监督管理局对涉及买卖公民个人信息的三家教育培训机构，分别处以罚款 10 万元的处罚。

办案民警介绍，依据《刑法》第二百五十三条规定，向他人出售或者提供公民个人信息，情节严重的，处 3 年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处 3 年以上 7 年以下有期徒刑，并处罚金。泄露公民个人信息会造成恶劣的社会影响和严重后果，张某的案例给相关从业人员上了深刻的一课，希望大家引以为戒。[15]

[15] 中国台州网-台洲日报。

7. 某海外视频网站火速达成儿童在线隐私侵权诉讼的和解

12 月 4 日，某海外视频网站与一群家长达成了和解。此前，原告指控该公司违反了《儿童在线隐私保护法案》，收集并暴露了未成年人的数据和个人信息。该案原告律师 Gary Klinger 向外媒 The Verge 证实了此事，但拒绝发表评论和披露更多细节。该公司发言人在一份声明中称：尽管对投诉中的大多数内容提出了异议，但还是达成了某种“和解方案”。

该网站发言人向 The Verge 表示：“网站致力于保护其用户，尤其是年轻用户的数据。尽管我们不同意投诉中所述的大部分内容，但一直在与有关各方合作，并很高兴能解决这些问题”。

该公司拒绝披露和解条款的细节，不过由原告的投诉可知：网站未能提供适当的保护措施，以防止儿童使用该应用程序。若未满 13 周岁的未成年人创建了账户，该 App 会要求其填写个人识别信息，包括姓名、电话、邮件地址、照片等个人资料，且会向其它用户公开。

投诉还称：2015 年 12 月～2016 年 10 月间，该 App 收集了包括位置信息在内的未成年人数据。此举涉嫌违反《儿童在线隐私保护法案》。

涉嫌收集的内容将违反《儿童在线隐私保护法》（COPPA），其中明令禁止 Facebook 等社交媒体在未经父母或监护人明确同意的情况下、而收集 13 岁以下儿童的数据。[16]

8. FTC 正式裁定 Cambridge Analytica 欺骗 Facebook 用户谷歌将限制与广告商的数据共享 以保护用户隐私

7 月，FTC 指责该咨询公司以及 CEO Alexander Nix 和应用程序开发人员 Aleksandr Kogan 通过性格测试应用程序收集了数千万 Facebook 用户的数据。该消息于 2018 年首次披露，颠覆了 Facebook，并导致马克·扎克伯格在国会露面。FTC 先前与 Nix 和 Kogan 达成和解，12 月 9 日投票一致，正式称该公司的做法具有欺

[16] cnBeta.COM。

骗性。

在某些方面，投票在很大程度上是象征性的。丑闻首次被发现后不久，Cambridge Analytica 申请破产。正如美国联邦贸易委员会(FTC)在 12 月 9 日的公告中指出的那样，该公司从未对该机构的法律投诉或法院判决做出回应。

根据 12 月 9 日发布的联邦贸易委员会命令的条款，Cambridge Analytica 必须删除其在 Facebook 用户上收集的任何数据，并且今后不得对其收集数据的方式作出虚假陈述。

由于该公司已经解散，法院的这些要求似乎没有意义。尽管如此，尽管该机构的命令标志着剑桥分析公司的故事的终结，但丑闻的影响在今天仍可感受到，因为议员们在努力解决有关 Facebook 的权力以及如何保护用户隐私的问题。[17]

9. 欧盟正调查谷歌的数据收集规范

欧盟（EU）反托拉斯监管机构似乎尚未完成对 Google 商业实践的调查。据路透社报道，欧盟委员会已对 Google 的数据收集做法进行了“初步调查”。根据路透社看到的文件，欧盟委员会正在向多家公司寻求有关 Google 如何以及为什么从其服务中收集数据的详细信息。这些公司已经得到一个月的答复。

欧盟监管机构在一封电子邮件中告诉路透社：“作为对 Google 与 Google 收集和使用数据有关的做法的初步调查的一部分,欧盟委员会已发出了调查表。初步调查正在进行中。”

谷歌同时表示,它使用数据来改善其服务。“我们使用数据来提高我们的服务的实用性并展示相关的广告,并为人们提供管理,删除或转移其数据的控制权。我们将继续与委员会和其他机构就这一对我们行业的重要讨论进行接触。”谷歌在一封电子邮件中告诉路透社。

Google 的反托拉斯困境可能加剧

对于 Google 来说,这是一个新的打击,现在欧盟委员会已将目光转向了这家网

[17] 爱科技网。

络巨头的合作伙伴公司,以寻求有关其数据收集做法的详细信息。除其他外,委员会正在寻找与本地搜索、在线广告、在线广告定位、登录服务和 Web 浏览器有关的数据。简而言之,欧洲反托拉斯监管机构正在调查 Google 的核心业务。

要求这些公司提供有关“近年来向 Google 提供数据或允许其通过其服务收集数据的协议”的详细信息。监管机构想知道 Google 收集的数据类型以及是否为此获得补偿。此外,他们正在寻求有关 Google 如何使用收集到的数据以及公司对此类数据的重视程度的详细信息。

他们还想知道双方是否受“禁止或限制数据使用”的合同条款的约束。两家公司还被问到谷歌是否曾经拒绝提供数据以及这如何影响了他们。不过,委员会没有透露已向哪些公司发送了调查表。

在过去两年中,Google 因多项反托拉斯指控被欧盟处以超过 80 亿欧元的罚款。还要求该公司改变其商业惯例。尽管调查并不一定能保证这次也要提起诉讼,但 Google 的商业惯例使得这种情况往往会多半出现在接收方。因此,如果这项调查还给 Mountain view 公司带来了一些严重问题,也就不足为奇了。[18]

10. iPhone 11 Pro 被曝收集用户位置数据，苹果回应符合预期且没有安全隐患

12 月 5 日消息，据外媒报道，安全记者布莱恩·克雷布斯(Brian Krebs)日前发布报告，声称苹果 iPhone 11 Pro 存在持续收集用户位置数据的行为，此举可能会构成潜在安全风险。

克雷布斯在运行苹果最新 ios 13.2.3 软件的 iPhone 11 Pro 上做了演示，尽管在 iPhone 设置中手动禁用了个人定位服务，但该软件仍在继续收集某些应用程序和系统服务的 GPS 数据。更令人担忧的是，即使应用程序的定位服务设置为“从不”请求上述信息，iPhone 11 Pro 依然会主动寻找 GPS 数据。

苹果在 iPhone 定位服务设置的隐私政策中称，手机会定期以匿名和加密形式将附近 Wi-Fi 热点和蜂窝网络的地理标记位置发送给苹果，用来扩充这个包括 Wi-Fi 热点和蜂窝塔位置数据库。该公司表示，基于位置的系统服务可以在设置中被

[18] 威智网。

禁用，但克雷布斯发现事实并非如此。

他解释说："显然，这款机型(可能还有其他 iPhone 11 机型)上有些系统服务请求定位数据，如果不完全关闭定位服务，用户就无法禁用这些服务，因为即使单独禁用了所有使用定位的系统服务，箭头图标仍会定期出现。"

在 ios 中，用户可以通过设置用户界面启用和禁用系统定位服务，并提供对第一方和第三方应用程序、基本 ios 服务和其他苹果功能的控制。这些工具在 ios 13 中得到了支持，大大增强了用户对数据共享功能的控制，降低了无意中出现位置跟踪功能的可能性。

以前，第三方应用程序可以在初始设置时请求持续收集设备位置数据，但 ios 13 删除了这个功能。此外，当在设置菜单中手动启用始终在线跟踪功能时，会定期出现弹出窗口提醒用户，并提供关闭该配置的选项。

苹果工程师回应称："我们没有看到任何实际的安全隐患。启用定位服务时，在状态栏中显示定位服务图标是预期的行为。对于在设置中没有禁用的系统服务，将显示该图标。"

克雷布斯认为，苹果新款手机的这种情况可能与为支持 Wi-Fi 6 而引入的新 iPhone 硬件有关，不过这种说法仍未得到证实。[19]

11. Twitter 遵循加州法律 明年 1 月 1 日更新其全球隐私政策

Twitter 在 12 月 2 日表示，该公司正在更新其全球隐私政策，让用户更好地了解广告主可能收到哪些数据，该公司还将启动一个网站以澄清其数据保护工作。此次政策更新将于 2020 年 1 月 1 日生效，将符合《加州消费者隐私法》（CCPA）。

加州法律要求大型企业针对用户的个人信息提高消费者的透明度，并提供其个人信息的控制权。例如，消费者有权要求删除其数据，并选择不将其数据出售给第三方。

在 Facebook"剑桥分析"丑闻曝光后，包括 Facebook 和谷歌在内的社交媒体公

[19] 网易科技。

司在数据隐私方面遭遇广泛审查。该丑闻未经用户同意就收集了数千万人的个人数据。

Twitter 于 2 日还宣布，它将把先前与爱尔兰都柏林的 Twitter International Company 签约的美国和欧盟以外的用户帐户，都转移到总部位于旧金山的 Twitter Inc.。

该公司表示，此举将使其能够灵活地针对这些用户一起测试不同的设置和控件，例如附加的选择加入或选择退出隐私首选项，而这可能会受到欧洲具有里程碑意义的通用数据保护条例（GDPR）的限制。

Twitter 的数据保护负责人达米恩·基兰（Damien Kieran）在电话采访中说："我们希望能够在不立即违反 GDPR 规定的情况下进行试验。"他补充道："我们的目标是从这些试验中学习，然后向世界各地的人们提供相同的体验。"

该公司表示，它已经在过去两年加强了跟数据和安全问题有关的沟通。他们还在博客文章中强调说，该公司正在努力升级系统并将隐私权纳入新产品中。

今年 10 月，Twitter 宣布发现用于双重身份验证的电话号码和电子邮件地址可能无意中被用于广告目的。

Twitter 的新隐私站点被称为"Twitter 隐私中心"，目的是展示该公司数据保护工作，还将为用户提供另一种访问和下载其数据的途径。

包括 Twitter 在内的各大互联网公司最近都在 CCPA 生效之前表明了立场。微软上个月表示将遵守美国的法律。谷歌则告诉客户，为了遵守 CCPA，该公司将允许网站和应用使用其广告工具屏蔽个性化广告。[20]

12. 美法官：Facebook 必须面对数据泄露案非索偿集体诉讼

11 月 28 日，美国的一名联邦法官表示，2018 年 9 月数据泄露案中多达 2900 万名个人信息被盗的 Facebook 用户不能作为一个群体提起索偿诉讼，但在经历了

[20] 新浪科技。

一系列隐私泄露后，他们可以寻求让这家社交媒体公司向其提供更好的安全性。

在美国当地时间周二深夜（北京时间周三凌晨）作出的一项裁决中，旧金山的美国地区法官威廉·阿尔苏普（William Alsup）表示，不管是信用监控成本，还是被盗个人信息的价值减损，都不是可以支持受影响用户发起集体诉讼的“可认知损害”。

阿尔苏普还称，就用户花时间减轻伤害并因此而受到的损害而言，需要因人而异地做出决定，而不是进行单一的集体评估。受影响用户可以作为一个团体提出起诉，要求 Facebook 采用自动化的安全监控、改进员工培训以及更好地就黑客威胁的问题对用户做普及教育。Facebook 此前对此抗辩称其已经修复了导致数据泄露案发生的漏洞，因此没必要采取这些措施，但阿尔苏普驳回了这种抗辩。

“Facebook 屡次给用户隐私带来了损失，这意味着有必要对其进行长期监督”，至少在当前的诉讼阶段是这样，阿尔苏普在判决书中写道。

如果阿尔苏普此次的判决是允许 Facebook 用户发起集体诉讼以索求赔偿，则 Facebook 原本将会面临更高的总支出。

Facebook 用户的律师尚未对相关置评请求作出回应，Facebook 也尚未回复类似请求。

在 2018 年 9 月 28 日，Facebook 称黑客利用软件漏洞访问了 5000 万名用户的账号，这在当时被认为是该公司 14 年历史上最大的一次黑客入侵事件。两周以后，Facebook 缩小了受影响用户的规模，称有 3000 万用户的访问令牌被盗，而 2900 万用户的个人信息（如性别、宗教信仰、电子邮件地址、电话号码和搜索历史等）被盗。

Facebook 面临着诸多隐私相关诉讼，例如该公司允许英国政治咨询公司剑桥分析（Cambridge Analytica）获取了 8700 万名用户的数据，这桩数据泄露丑闻引发了用户诉讼。

今年 9 月，旧金山的美国地区法官文斯·查布里亚（Vince Chhabria）表示，Facebook 必须面对跟剑桥分析等第三方获取用户数据有关的大部分索偿诉讼，并指出就用户对隐私权作何期望的问题而言，Facebook 的观点是“大错特错的”。

Facebook CEO 马克·扎克伯格（Mark Zuckerberg）在 3 月 6 日发表博文，概述

了他对社交媒体“以隐私为中心的愿景”。他在文中写道：“隐私权能给人们以做自己的自由，并可更加自然地进行联系，而这正是我们打造社交网络的原因所在。”[21]

13. 美国联邦调查局警告:智能电视存隐私泄露风险

近日，美国 FBI（联邦调查局）波特兰总部发布公告，对智能电视可能带来的风险进行警告。公告称，智能电视可以连接互联网，提供流媒体服务和其他应用程序，并配备相机和麦克风。但是比起电脑手机，智能电视的安全问题却经常被忽略。

由于智能电视的设计特性，电视制造商、应用开发人员和黑客都有可能通过智能电视获取隐私信息。同时 FBI 警告称黑客可以控制智能电视，甚至可能控制摄像机和麦克风以监控用户的生活，细思极恐。

此外，在今年早些时候，《华盛顿邮报》也曾报道过类似新闻，一些智能电视制造商会回收用户的观看信息来提供定位广告，而大部分用户对此是不知情的，不知不觉中隐私就泄露了。

最后，FBI 给出了解决方案，在不使用时用黑胶布贴上电视的摄像头，并及时更新智能电视固件，仔细阅读隐私政策，以便更安全地使用智能电视。[22]

四、环球评论

1. 政府应该如何收脸？

上周参加了南方都市报一年一度的啄木鸟安全大会，其中专门有一个话题关于人脸识别技术的安全与规制，并且南都还发布了《人脸识别落地场景观察报告》[23]。另外，洪延青博士也特别写文关于《人脸识别技术的规制框架（PPT+讲稿）》[24]。可以看出，大家现在对人脸影像在收集使用环节，普遍认同需要分场景分析并

[21] 新浪科技。
[22] 中关村在线。
[23] 南方都市报：《人脸识别落地场景观察报告》，
https://m.mp.oeeee.com/show.php?m=Thinktank&a=reportDetail#/?id=224
[24] 洪延青：《人脸识别技术的规制框架（PPT+讲稿）》，
https://mp.weixin.qq.com/s/pyFxmnuAbtygttkoZExCdA

匹配不同的法律目的作为框架进行相关的规则。

但是不知大家有否发现，无论是南都的报告还是洪博士文章对场景的分析与梳理中，获取及使用人脸最多的场景还是政府（或者准政府机构/事业单位，以下统称政府部门）所控制的场所范围内，比如火车站的扫脸进闸机、街头大屏拍摄闯红灯者、公共厕所扫人脸取手纸、摄像头走进了学校教室还进入了动物园（被堪称“人脸诉讼第一案”）……特别近日，又有多家媒体报道，北京地铁即将推出“刷脸”通过安检的服务，一时间引起广泛争议。人脸识别技术近年来在国内一直热度不减，各行各业、包括各类各级政府部门都纷纷试水。随着互联网+以及人工智能技术的进一步发展，政府部门收集和使用公众人脸的目的，已经不纯粹是为了安全监控了，他们有的开始进行统计流量，有的为了识别会员，有的用人脸进行个体或者群体画像进行信息推送（包括精准推送），还有诸如用于进门打卡考勤，甚至还有跟踪相关人员或者智能公交或者地铁……

人脸识别技术越发达，可能发生的场景就越丰富。目前已经有许多学者写了很多篇关于人脸与隐私保护方面非常有价值的文章，给隐私合规与安全界提供了诸多思路与参考。M 姐曾经也接受过一些媒体关于对此话题的采访，例如上海市政府启动小区人脸识别进门（人脸钥匙取代了传统的普通钥匙进门）、公厕扫人脸取纸（用人脸来限制多次取纸），M 姐自己也曾在朋友圈发过一些牢骚例如只要进入北京火车站的大门，就需要掏身份证由站在门口的工作人员拿手机进行拍摄，不但没有任何告知还使得进闸人群排起长队等。以上这些事件基本上还在与政府部门采用人脸识别技术收集公众的人脸影像有关。

事实上，我国政府部门使用人脸识别技术起步很早，例如，中央政法委、公安部 2005 年起联合主导的“平安城市”以及后来的“天网工程”就是利用人脸识别技术的典型例子。然而，尽管实践先行，我国迄今尚未建立专门规制政府部门使用该技术的相关规范。

政府是具有超强职能的一方民事主体，同时他又是监管方。如果政府收集个人信息，甚至如人脸这种个人敏感信息，并不是为了公共利益、社会安全、第三方利益或者其他可以豁免同意的这种理由以外，是否可以利用自己的行政权力任意获取用户的人脸数据？一旦海量数据聚集以后，政府手上的数据是否会形成一定的垄断优势，而使同类其他企业的竞争优势失灵？政府收集了这些人脸数据以后，都存在了哪儿？是否有采取更高要求的网络安全保护机制与措施？公民以后在政府部门管辖的活动范围中，是否更加真空没有个人的隐私了?以上种种的疑问，导致我们团队，特别想写写关于政府部门采集人脸信息应该如何合理规制的问题。究竟应该采取一刀切来进行规制，还是也应该如规则同私营部门的行为一样分收集人脸的不同场景来进行管理？由于政府部门拥有公权力色彩的背景，其在收集人脸

时是否还应该与普通的私营部门在采集人脸信息的合规要求上有所不同？如有不同，在哪些点上应当有所区分而在哪些点上又应该一视同仁，甚至作为国家权力的代表机关在规制其行为时需以更加严格的标准对待呢？

下文拟对政府部门应该如何使用人脸识别技术收集使用人脸影像作简要的探讨，以供学者与实务界参考后做更加深入与细致的分析与研究。

一、政府能否使用人脸识别技术背后的利益平衡

世界范围内，规制政府使用人脸识别技术的立法不多。从现有的立法例来看，不同法域大多采取严格限制、或者原则禁止政府使用该技术的态度。探究背后的立法意图，立法者一直在政府履行职能的公共目的、与个人信息主体的权利与自由之间进行衡量，并试图作出较为合理的选择。

具体而言，一方面，政府使用人脸识别技术是为了履行政府职能，例如警察对大型集会的安保、对犯罪嫌疑人的追踪等，具有保护公共利益的特征。另一方面，由于人脸数据具有唯一性、与个人信息主体高度相关的敏感性，政府对该技术的使用极易侵扰个人信息主体的基本权利与自由，破坏个人信息主体对隐私保护的合理期待。

目前，正是由于人脸识别技术还不够完善，对有色人种、女性等的识别错误率远高于其他群体，导致种族歧视、性别歧视等严重侵犯个人权利的问题泛滥，各国才对政府使用该技术持非常谨慎的态度。

二、规制政府使用人脸识别技术的域外法经验

人脸数据是人脸识别技术的基础，一般而言，属于生物识别信息的一种。根据我国《信息安全技术 个人信息安全规范（征求意见稿）》（2019.10.22）（以下简称“《个人信息安全规范》”）第 3.2 条，“个人生物识别信息”属于一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇的个人敏感信息。

综合考虑人脸数据的敏感性等因素，如政府能够合法获取人脸数据，其作为数据控制者在处理人脸数据过程中，除了应当遵守个人信息保护合法、正当、必要原则外，很可能还需遵守其他更严格的条件。我国目前无专门规制政府使用人脸技术的规则，我们不妨先对目前世界上已有的立法进行调研与剖析。

- **欧盟 2016 年《通用数据保护条例》**

欧盟《通用数据保护条例》（GDPR）对人脸数据未作特别的规定。根据 GDPR 第 4 条定义，人脸数据属于生物识别数据的一种，在 GDPR 下作为“特殊类别的数据”进行统一规制。根据 GDPR 第 9 条，欧盟原则上禁止处理特殊类别的数据，除非具有法定的正当事由。

GDPR 第 9 条列举的正当事由包括：

（1） 征得个人信息主体明示同意；

（2） 政府在劳动、社会保障等方面履行义务以及行使自身或个人信息主体权利所必须；

（3） 保护个人信息主体或其他个人重大利益所必须；

（4） 非盈利机构处理其成员信息；

（5） 个人信息已经向公众公开；

（6） 司法程序中提出、行使或抗辩法律主张所必须，或法庭行使司法权力；

（7） 保护重大公共利益所必须；

（8） 保护公共卫生领域的重大利益所必须；或者

（9） 实现公共领域存档等目的。

同时，GDPR 第 9 条还在政府处理生物识别信息的问题上，赋予成员国进一步立法限制政府处理生物识别信息的权力。例如，英国《数据保护法》就在政府处理该问题方面做了较为细致的规定。

- **英国 2018 年《数据保护法》**

英国 2018 年《数据保护法》（以下简称“《数据保护法》”）对政府使用人脸识别技术的规制主要体现于第 3 部分“与执法相关的信息处理”（Law Enforcement Processing）中。该部分专门规制政府在防止、调查、侦查或起诉刑事犯罪或执行刑事处罚（包括防止对公共安全造成威胁）过程中的执法行为，不涉及其他类型的政府行为。

《数据保护法》第 34 条规定，政府在执法过程中处理个人信息应遵守六项原则：

（1） 行为合法公平原则；

（2） 目的合法清晰原则；

（3） 收集个人信息最小化原则；

（4） 保证个人信息准确性原则；

（5） 个人信息及时删除原则；

（6） 采取措施保护个人信息原则。

《数据保护法》第 35 条对第 34 条第（1）项行为合法性原则进行了阐释。其中，政府处理个人敏感信息（包括以识别个人为目的，对生物识别信息的处理）只在以下两种情形下具有合法性：

（1）政府征得个人信息主体的同意，并且政府在处理敏感信息时具有完备的细则文件。[25]或者

（2）政府的处理行为是为执法目的所必须的，处理行为至少满足附件 8 规定正当事由的一项，[26]并且政府在处理敏感信息时具有完备的细则文件。

[25] 《法案》第 42 条：政府处理敏感信息时遵循的细则文件应包含：（1）政府保证行为合法（要求征得信息主体同意或满足其他条件）的程序；（2）政府保留、销毁信息的政策，载明信息可能被保留的时间等。

[26] 《法案》附件 8 规定的例外目的有：法定目的、司法行政、保护个人信息主体或其他个人的重要利益、保护处于风险的儿童和个人、个人信息已经被公开、法律诉求、司法行为、防止诈骗、公共存档等。

其中，附件 8 列举的正当事由概括如下：

（1） 执行法定目的（Statutory etc purposes）；

（2） 执行司法的要求（Administration of justice）；

（3） 保护个人重大利益（Protecting individual's vital interests）；

（4） 保护儿童及处于风险的个人（Safeguarding of children and of individuals at risk）；

（5） 个人数据已经公之于众（Personal data already in the public domain）；

（6） 法律主张所要求（Legal claims）；

（7） 司法行为所要求（Judicial acts）；

（8） 为了阻止诈骗（Preventing fraud）；

（9） 为了归档事由等（Archiving etc）。

以上规则在 2019 年 9 月 4 日，英格兰和威尔士高等法院行政庭就 R (Bridges) v CCSWP and SSHD 一案作出的判决中得到引述。南威尔士警方自 2017 年起开始试点使用自动人脸识别技术（Automated Facial Recognition technology），对从闭路电视中获取的公众人脸进行实时处理，抽取面部生物识别信息后，将该信息与监视名单上的人的面部生物识别信息进行对比。[27]据此，原告对此提出三项主张，其中第二项认为警方利用人脸识别技术的执法行为违反了英国的《数据保护法》。

法院认为，公众的面部生物识别信息符合法条规定的"生物识别信息"的定义，构成个人敏感信息，且公众的生物识别信息被处理是为了进行对比，满足"为识别特定个体目的"。由于警方在人脸识别前未征得公众的同意（第 35 条第（1）款规

[27] 南威尔士警方自 2017 年起开始试点使用自动人脸识别技术（Automated Facial Recognition technology），对从闭路电视中获取的公众人脸进行实时处理，抽取面部生物识别信息，并将该信息与监视名单上的人的面部生物识别信息进行对比。若匹配未成功，抽取的面部生物识别数据和相关人员的照片不会被存储；与成功匹配相关的数据则最多会被保留 24 个小时；闭路电视记录根据相关标准保存 31 天。

定的情形），所以，在进行人脸识别时，警方只有满足《数据保护法》第 35 条第（2）款规定的三个要件，行为才具有合法性。

具体而言，首先，原告对“绝对必要”的诉讼请求基于前述《欧洲人权公约》下的合比例诉讼请求，满足绝对必要的要求；其次，警方的执法行为为警方根据法律或法律授权履行职能所必需，且为保护重大公共利益所必需，满足附件 8 中的正当性事由；再次，警方出具的 2018 年 11 月的细则文件《为执法目的进行的敏感处理政策》满足《法案》第 42（2）条细则文件的要求，但内容较为简短、缺乏细节，没有对相关政策进行系统性的认定和陈述，是否满足《数据保护法》要求仍存在疑问，建议信息官（Commission Officer）进一步提供指导。

此外，法院对《数据保护法》附件 8 中的多项正当性事由之一“实现法律法规规定的目的”（Statutory etc purposes）进行了阐释，认为：分析相关法律框架需要的条件时，应根据不同类型的生物识别信息本身的情况进行评估。本案政府使用该技术的法律框架充分，由三个层次构成：（1）初始立法，即《数据保护法》；（2）二级立法文件，关于《法案》的实践准则，即根据 2012 年《保护自由法》出台的《监控摄像机实践准则》；（3）三级立法文件，即警方自己出具的细则文件。总体上，以上法律文件组成的法律框架能够为警方的执行行为起到指引作用，因此较为充分。

《数据保护法》第 36-42 条对第 34 条列举的第（2）至（6）项原则的内涵进行了阐释。不难发现，《数据保护法》强调的六项原则与 GDPR、我国《个人信息保护规范》中对个人信息处理提出的原则总体上一致，是为各界广泛接受的处理个人信息的原则。

此外，英国 2012 年《保护自由法》还对《数据保护法》进行了补充，规定了政府处理儿童生物识别信息的要求。《保护自由法》第 26 条规定，原则上需要书面通知并获得监护人的书面同意，且监护人可随时撤回该同意。儿童拒绝被处理生物信息时，政府亦不得进行处理其生物识别信息，而应当使用替代性的方式。第 27 条规定了例外无需通知监护人的情形，如监护人无法找到，监护人缺乏监护能力，为保护儿童利益需要不通知监护人的，或者通知监护人不现实可行时。

GDPR 规定任何个人数据的处理必须获取数据主体“自由给予、明确、具体、不含混”的同意，数据主体任何形式的被动同意均不符合 GDPR 的规定。因此，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”。当然，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。但

是，限制排除的仍然

- **美国 2019 年《停止秘密监控法案》及一系列面部识别技术的法案**

截止 2019 年，美国目前已有多个州、市通过关于规制政府使用生物识别技术（包括人脸识别技术）的法案，大多都禁止政府部门使用该类技术，并且没有能够豁免的正当事由。例如，加州旧金山市《停止秘密监控法案》规定【可参考阅读原文中我们对相关段落的翻译】，禁止政府部门获取、保存、访问、使用人脸识别技术和使用人脸识别技术获取的信息。马萨诸塞州萨默维尔市《众议院/参议院第 1358 号法案》规定【可参考阅读原文中我们对法案全文的翻译】，除法律授权外，禁止市政府部门和官员获取、保存、访问、使用人脸监控系统和人脸监控系统获得的信息。加州奥克兰市亦禁止政府部门和工作人员获取、保存、访问、使用人脸识别技术和使用人脸识别技术获取的信息。

但是，也有一些州未直接禁止政府使用该类技术，而是对政府的使用行为进行了有条件的限制。例如，俄勒冈州华盛顿县警局《使用面部识别技术的规定》就从人脸数据的采集、使用、存储、销毁等生命周期，对警方使用人脸识别技术做了较为细致的指引：警方可以在宪法、法律以及华盛顿县警长办公室政策的范围内使用人脸识别技术。警方在使用该技术前，须获得个人信息主体的同意。警方仅能限于执法目的使用该技术，不能用于大规模监视。除非例外情形（如核实被捕人员犯罪记录），人脸识别结果不能单独作为证据，只能作为潜在的线索。此外，人脸数据只能存储在警局控制的服务器上，如不涉及刑事犯罪，定期将会删除。警方会对上传照片进行脱敏处理，照片不会存在任何标识或个人信息等。

此外，新罕布什尔州的《新罕布什尔州修订法》第 105 章 D 随身摄像机（Body-worn cameras），对州内警察和执法机构在执法时，如何使用摄像机收集人脸的相关信息也作出了较为细致的规定。

- **印度 2018 年《个人数据保护法草案》**

印度《个人数据保护法草案》（以下简称“《草案》”）规定，人脸数据属于生物识别信息 [28]，但《法案》未对生物识别信息作特别的规定，而是作为个人敏感信息进行统一规制。根据《草案》第 7（2）条，个人敏感数据原则上禁止处理，仅得

[28] 印度 2018 年《个人数据保护法草案》第一章 引 言（8）“生物数据”系指面部图像、指纹、虹膜扫描或者任何其他类似的源自对数据主体物理、生理或者行为特征进行测量或者技术处理而产生的个人数据，这些数据允许或者确认该自然人的唯一身份。

基于第四章规定的一项或几项结合的条件才能被处理。

《草案》第四章第 18-21 条列举可以处理人脸数据的条件有：

（1） 征得个人信息主体明示同意；

（2） 履行邦的某些职能所必须；

（3） 根据法律或法院、法庭的命令处理；或者

（4） 为迅速采取某些行动，如涉及对个人信息主体生活或健康构成严重威胁的医疗紧急情况，在公共卫生威胁期间为个人提供医疗健康服务，发生灾害或公共秩序崩溃期间为确保个人安全或向个人提供帮助或服务。

同时，《草案》第 23 条还规定了处理儿童个人（敏感）信息的相关规定，强调处理儿童个人（敏感）信息需要征得监护人的同意，除非服务数据处理者是专门为儿童提供咨询或者儿童保护服务的主体等。

- **澳大利亚 1988 年《隐私法案》**

澳大利亚《隐私法案》对人脸数据未作特别的规定，也通过归属于生物识别信息来进行保护。根据《隐私法案》定义 [29]，由于生物识别数据属于个人敏感信息，所以人脸数据作为个人敏感信息进行统一规制。根据《隐私法案》附件第二部分第 3.3 条，澳大利亚原则上禁止收集个人敏感信息，除非具有法定的正当事由。

对于政府收集个人敏感信息的正当事由，《隐私法案》第 3.3 条规定：

（1） 需要征得个人信息主体明示同意，并且，如果收集主体为相关机构（Agency/Organization），该个人信息为该机构实现其作用或开展活动所必须或直接相关联；

（2） 收集个人敏感信息有澳大利亚法律、法院/法庭命令所要求或授权；或

[29] 澳大利亚 1988 年《隐私法案》第一部分第六条规定，个人敏感信息包括用于生物身份验证的生物识别信息或生物特征模板。

者

（3） 如果收集主体是政府执法机构（Enforcement Body），该政府执法机构合理认为，收集个人敏感信息为履行执法机构职能或开展活动所必须或直接相关联。

此外，《隐私法案》附件第三部分第 6.3 条规定，如果使用或披露生物识别信息或生物特征模板（biometric templates），原则上只能在收集时的特定目的范围内进行使用或披露，除非是信息收集者（Agency）是面向政府执法机构（Enforcement Body）进行披露，且已经按照委员会的指引进行操作。

- **巴西 2018 年《通用数据保护法》**

如上，巴西《通用数据保护法》也未对人脸数据未作特别的规定，人脸数据归属于生物识别信息的一种。根据《通用数据保护法》定义，由于生物识别数据属于个人敏感信息，所以人脸数据也同样作为个人敏感信息进行统一规制。

根据《隐私法案》第 11 条，个人敏感信息可以在以下情形被处理：

（1） 当数据主体或其法定授权代表为特定目的而特别且重点地对处理表示同意时；

（2） 在数据主体没有给予同意的情况下，以下条件必不可少：

a. 控制者遵守法律或监管义务；

b. 公共行政机构为执行法律法规中的公共政策而共享处理所必需的数据；

c. 研究机构开展研究，并尽可能确保对个人敏感数据进行匿名化；

d. 定期行使包括协议、诉讼，行政程序或仲裁程序中的权利（最后一点是根据 1996 年 9 月 23 日第 9,307 号法律（《巴西仲裁法》）做出的规定）；

e. 保护数据主体或第三方的生命或人身安全；

f. 按医护人员或医疗机构执行的程序保护健康；或者

g. 除数据主体普适性的基本权利和自由需要保护个人数据的情况外，为遵守本法第 9 条所述的权利，在电子系统中记录识别和认证的过程，确保防止欺诈和数据主体的安全。

此外，《通用数据保护法》第 14 条规定，儿童个人数据的处理，应在至少其一位父母或法定监护人的特定和明确同意下进行。

三、政府使用人脸识别技术应当遵循的基本原则

总结以上域外法经验，针对政府是否能够使用人脸识别技术，目前大致呈现以下两种立法模式：

（1） 原则上禁止，例外有法定正当事由时可以使用。一般情况下，法定的正当事由包括两种，即用户的明示同意，以及其他法定正当事由；

（2） 原则上禁止，且无法定的正当事由。此时立法态度较为严格，不支持政府使用人脸识别技术。

立法不同态度由各法域不同的社会文化环境、价值衡量标准来决定。但可以观察到，不同的法域的立法其实呈现出很大程度的共性，例如，对政府使用人脸识别技术持原则禁止的态度；例外的正当事由始终包括用户的明示同意；例外的其他正当事由中，大多要求政府有法律的合法授权、为履行职能所必须、或为了保护公共利益及其他重大的法益等。

我们理解，对于政府使用人脸技术的规则，始终离不开以下个人信息保护的普适性原则，但是在这些原则具体解释上，可能需要更为严格：

- **合法授权原则**

政府处理人脸数据应当有宪法、法律等规范的明确授权。实践中，可能存在某些法域通过政府规范性文件授权并规制政府使用人脸数据的情况，但我们理解，授权政府使用人脸应当比技术性法律规范或者标准层级更高。这是因为人脸数据高度敏感，与个人信息主体人身和人格权具有密切的联系和重大利害关系，公权力的

行使在某种程度上必然会处分、甚至剥夺个人信息主体的相关权利，因此，需要立法机关更为慎重地对待授权行为、将授权性法律规范位阶上移。

同时，参考英国《数据保护法》第 42 条、英格兰和威尔士高等法院行政庭在 R (Bridges) v CCSWP and SSHD 一案中对法律框架的阐释，政府需要分层级地形成完整的法律框架，从上位法、实施细则、具体执行规范等层面，为政府在使用该技术提供完整、细致的指引。

- **目的明确原则**

政府处理人脸数据应当具有明确、清晰、具体的目的，且该目的应限制在履行职能所必需的范围内。从严格限制公权力的角度出发，一般不同法域都规定，处理个人敏感信息的正当事由仅包括为履行职能所必须，超出履行职能范围的都属于违法，政府应当承担相应的责任。

但是，参考澳大利亚《隐私法案》附件第三部分第 6.3 条规定，如果能够征得个人信息主体同意，政府仍有超出范围处理个人敏感信息的空间。是否允许超目的处理个人敏感信息，有赖于不同法域的价值衡量。当然，笔者建议，同一场景同一处理目的与手段的，可以在同一期限内再次授权一次；如果上述任何一个情况发生变化的或者采集人脸信息的场景非常复杂的，也应该做到请个人信息主体 case by case 的授权。

- **知情同意原则**

从上述世界各国相关法律看，获得个人信息主体同意通常是政府处理人脸数据的正当事由之一。但是，政府使用人脸数据是否一定需要通知用户并征得其同意，可能需要视具体应用场景而定。例如，政府为履行职能处理人脸数据就是无需征得个人信息主体同意正当化事由之一。实践中，警方为安保的目的使用人脸识别技术，也未必对公众进行了充分告知。如果此时仍要求政府获取公众同意才能使用该技术，未免会使政府履行职能的效果大打折扣。

当然，在政府主动征得个人信息主体同意的情形下，政府在获取人脸数据前，应当向个人信息主体明示个人信息处理目的、方式、范围、规则等，充分保证个人信息主体的知情权（比如北京火车站入口扫身份证场景，虽然说的不是人脸），并征得其对政府处理其人脸数据的同意。否则，相关执法、司法机关在此过程中获取的证据将不具有合法性，也不应当被采用。此外，如果个人信息主体同意政府的处理人脸数据，其仍应享有随时撤回同意的权利。

对于处理儿童人脸数据的问题，很多法域的规定都十分严格。政府应书面通知监护人，征得监护人的书面明示同意，并且监护人可以随时撤回其同意。根据英国《数据保护法》，及时获得监护人同意，但是如果儿童表示拒绝的，政府也应当立即停止处理行为，采用替代性的方式。

- **最小必要原则**

政府只应当处理满足履行政府职能所需的最少人脸数据数量。政府不应笼统、概括地说明履行职能的目的，相反，应当尽可能将行政行为的目的限缩至最小范围。政府应当证明，除使用脸识别技术外，无其他可行的替代方式、或其他替代方式的成本过高。此外，职能目的达成后，政府应及时删除人脸数据。此外，未经宪法、法律等规范的授权，政府不应对收集的人脸数据进行委托处理、转让、共享、公开披露等处分行为。当然，如征得个人信息主体的同意，是否还不得为之可进行进一步的讨论。

部分公共性质的其他组织，如学校、医院、商业银行、轨道交通运营公司等，有时会在政府授权范围内履行一定的公共职能。例如，中国人民银行、银保监会要求商业银行、证券公司等对进行金融交易的用户进行身份验证、地铁运营公司为履行安全保障职能对乘客进行安检等都属于这个范畴。从最小必要的原则出发，这类公共组织可能并不适宜直接类比政府，在履行其职能时直接享有处理人脸数据的权力。我们理解，如需处理人脸数据，此类场景可能仍以征得个人信息主体同意为宜。

- **比例原则**

在 GDPR 项下，比例性原则的意思是要求控制者为实现某一目的而实施的措施应与数据处理的风险合乎比例，包括相对与所追求的目的，数据控制者需要对数据处理活动的必要性和比例性开展评估，除非数据控制者做出该行为是为了社会公共利益、科学或研究目的、统计目的而处理数据。在日常生活中，我们通常都喜欢拿大炮打苍蝇来作比方形成做某件事情的花费与收益不成比例。这里是说，获取人脸对个人信息主体造成的损害是很大的，包括有可能存在泄露的风险，但为的是一个很不等比的目的，比如为了限制人们重复获取七公分的厕所纸。又比如说最近瑞典 DPA 处罚的一个案例，学校教室里安装摄像头获取人脸信息，为的却只是考勤打卡。如果为了限制获取厕所纸那就干脆别提供，或者设计一种厕纸盒每次只能出七公分（为了等待出 N 个七公分厕纸的赶火车乘客毕竟哪有几个），记考勤可以用另外一种方式，如传统的手动签到来执行，为何一定需要获取人脸呢？

- **公开透明原则**

除非为了社会公共安全与保护社会重大利益等例外情况，政府部门应当以明确、易懂和合理的方式公开处理人脸数据的范围、目的、规则等，并且需要让公众知道收集后的数据会使用在什么场景，会存储在什么地方。是政府自己履行数据安全保护义务还是委托第三方代为履行。政府是否存在与第三方进行数据共享，这些第三方都是哪些机构，这些机构的安全防护能力如何。政府收集数据的公开透明，也是对人权的尊重，对社会公平价值的体现以及不做失信政府短视政府。公开透明还需要接受外部监督。在利用人脸识别技术进行执法时，应保证人为的审查与干预，矫正利用该技术作出的判断所可能存在的错误，防止侵犯个人信息主体的基本权利。

- **确保安全原则**

清华大学法学院的劳东燕教授曾指出，人脸识别技术应用广泛，但如果人脸数据如何收集、保管和使用法律并没有严格规制，一旦发生数据泄露事件，所引发的风险将难以评估。由于大规模的人脸影像信息的收集，政府应当具备与担当与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护人脸数据的保密性、完整性、可用性。由于新的业务形态需要获得人脸的，最好在开展前组织内部相关部门进行个人信息安全影响评估，考虑某此场景下使用人脸技术获得信息是否会对个人信息主体造成权益影响，这类评估在适当时候，还可以邀请一些中立的机构一起参与，比如各行业的代表、学者、律师等。

- **权责一致原则**

目前，在中国个人信息主体通常较难追究侵害其个人信息权益主体的责任。例如，在刑事、行政责任方面，我国尚未有执法机构对人脸识别侵权事件进行处罚；在民法侵权责任方面，个人信息主体，常常无法得知侵权人读取的数据内容及使用方式，甚至找不到侵权主体，也无法举证自己的损失；此外，我国目前也缺乏类似美国联邦贸易委员会（Federal Trade Commission）的强势执法机构等。

政府应当采取技术和其他必要的措施保障人脸数据的安全，对人脸数据处理活动对个人信息主体合法权益造成的损害承担责任。关于责任承担形式，除了对受到侵害的个人信息主体承担民事责任外，政府部门以及其相关负责人是否需要为其不当使用公民人脸信息的行为承担行政、刑事等其他形式的责任，此处有待进一步商榷。

四、政府在不同场景下使用人脸识别技术的分析

目前，政府使用人脸识别技术的场景主要集中在公共安全、金融业务、社会保障系统等对身份验证有着高度要求的场景中。如前所述，政府处理人脸数据如果为履行职能所必须时（无可行的替代性方法），政府的处理行为无需征得个人信息主体同意。但对于政府非必须的履行职能的行为，或其他不具有正当事由的行为可能都需要征得个人信息主体的同意。举几个例子进行适当分析：

例如，警方利用人脸识别技术在交通执法、追寻逃犯等情形中对闯红灯个人进行拍照，通过识别面部特征匹配数据库中的个人身份信息，确认违反交通规则人员的身份，是为履公共安全保障职能所必须，因此无需征得个人信息主体同意。但是，如果警方将识别出个人身份的主体身份信息，如姓氏、照片、以往闯红灯记录或者其他不良信用信息等且直接在街口的屏幕上公示，是否合适可能就存在疑问，因为警方可以有其他替代性的惩戒措施。此处可能需要考虑比例性问题。

政府在公共厕所中向市民提供免费的纸巾，通过人脸识别的方式来验证身份，以防止滥用纸张。虽然该方案对遏制浪费可能具有良好效果，但是在该场景下处理人脸信息可能有违合理性原则，政府很可能找到其他替代性技术方案来限制取纸量，为何一定需要获取人脸信息呢。由于不具有其他可能的正当事由，如果政府一定要推行人脸识别提供纸张，不但需要征得使用者的同意并告知目的与信息后续的使用与存储情况，而且最好还提供一种替代性方案（可以比扫人脸取纸慢一点点但也不能太复杂了）供消费者选择。

又如，政府积极推行建立的“智慧城市”同样离不开人脸识别技术，楼宇门禁、社区管理、办税认证系统、养老金领取管理、驾驶学员身份信息认证、安全驾驶管理系统、商业智能分析等场景下，人脸数据被更广泛地运用。但是，这其中很多功能可能并非政府履行职能所必须推行的，在具体推广过程中需要我们仔细甄别。例如，如前所述，人脸门禁可以供选择，如果有业主在被充分告知后愿意使用则可以，如果不愿意被收集人脸的还应该允许继续让其用门禁卡来替代。政府不能打着“履行政府职能”的旗号，一揽子直接处理所有场景下的人脸数据。

办理银行金融业务中，银行需要进行人脸识别来验证身份。考虑到金融安全的重要性，银行按照《中国人民银行关于印发《金融科技(FinTech)发展规划(2019—2021 年)》的通知》等法律规定，对交易身份的验证要求极为严格。此时，银行的人脸数据处理行为可能因落入实现法律规定监管要求的正当事由而得到承认。

对于受政府委托的公共机构履行部分政府职能的情形下，如上文提及，可能并不适宜直接类比适用政府的相关规则，此类场景仍可能需要以征得个人信息主体同意为宜。近日，北京地铁 2 号线阜成门站开始试点人脸识别安检。在该场景下，地铁运营公司部分承担着政府进行安全检查的行政职能，但是仍然也应该通过征得用户同意的方式来处理用户人脸数据，体现着被授权公共机构与政府本身的区别。而且同意需要在被充分知悉所有数据处理情况后，由乘客自由地给出，而不是利用高峰时段让乘客扫码同意让其不得不做出一种“被迫式”的同意。当然，本次试点的另外一个问题是，地铁公司在进行人脸摄入同时还会匹配人脸信息与其掌握的用户个人历史行为、信用记录，而后者数据作为地铁运营公司又是怎么来的呢？这就有可能存在超出人脸数据的使用目的和违反必要性原则的风险；以及，地铁公司如果选择存储用户人脸数据、建立大型人脸数据库可能也存在违反必要性的合规风险等等。

五、我国未来可能的发展方向

我国目前没有专门针对人脸识别技术的专门规范，对人脸数据的保护大多通过个人敏感信息来实现。鉴于，目前我国正在大力推进“智慧城市”等的建设，从立法态度的来看也有不断有推进人脸识别等生物识别技术应用于各行业的趋势，我们理解，我国未来对政府处理人脸数据的立法态度也不宜像英国等国家比较严苛。但是，政府仍应当以上文提及的具有共性的基本原则蓝本，规范自己的处理行为，尽可能利用好人脸识别技术的优点同时，避免过分侵扰个人信息主体的基本权利、破坏公民对隐私保护的期待。[30]

[30] 作者：孟洁律师团队，https://mp.weixin.qq.com/s/jBnDt657Jr1q-Ucbc4A8YA

中国首家律师事务所

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层 邮编: 100025
15 & 20/F Tower 1, China Central Place,
No. 81 Jianguo Road Chaoyang District,
Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市黄浦区湖滨路150号企业天地
5号楼26层 邮编: 200021
26F, 5 Corporate Avenue,
No. 150 Hubin Road, Huangpu District,
Shanghai 200021, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区铜鼓路39号大冲国际中心
5号楼26层B/C单元 邮编: 518055
Units B/C, 26F, Tower 5,
Dachong International Center, No. 39 Tonggu Road,
Nanshan District, Shenzhen 518055, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987