

生物特征信息采集必须取之有道

□ 陆强华

近期，一个换脸软件——“ZAO”，上线后即刻火爆。“ZAO”除了采集一般个人信息之外，要求用户上传照片，用以采集人脸信息。网络平台和各类移动APP日益成为采集个人信息的主渠道。随着人工智能等产业发展，刷脸支付普及以及短视频产业的繁荣，采集的个人信息种类逐步转向指纹、人脸等生物特征信息，消费者信息保护再一次成为了大众的焦点。

生物特征信息与一般的个人信息的不同

一般来说，生物特征信息包括指纹、声纹、人脸、虹膜、掌纹等生理和行为特征信息。生物特征信息多用于身份识别，当前较为常见的使用场景有机场、门禁以及支付等。在进行身份识别前，需要先采集个人生物特征信息，便于在后续身份认证时进行比对和验证。那么，与身份证号、账号以及手机号等个人身份信息相比，生物特征信息有哪些不同呢？

生物特征信息具有唯一性和不变性。银行账户、移动手机号等个人身份信息有一定的生命周期。对个人来说，换个银行卡或者密码、换个手机号等比较容易。但是指纹、人脸等生物特征信息是和人的生理或者行为特征一一对应的。因此，生物特征信息最大的问题是一旦信息被泄露后，无法像密码、银行卡一样进行快速修改或者更换。个人生物特征信息在互联网上可无限复制、难以消灭，危害性难以预测和估量。

部分生物特征信息被非法采集的风险比较高。最为典型的就是人脸信息，人脸普遍暴露在商场、旅馆、饭店、街道等各种公共场所，不法分子通过远程、非接触方式，在用户本人毫无察觉的情况下“无声无息”地非法批量采集生物特征信息。

生物特征信息关乎身体、生理和行为特征，隐私性更强。生物特征信息与个人行为强相关，容易泄露个人行为、位置行踪等信息。如人脸信息被采集后，一旦被不当使用，行走在有摄像头的区域，摄像头可以随时捕捉和识别到你，你根本就无所遁形，个人隐私无法得到有效保障。

生物特征信息的识别体系还不完善，被冒用的风险依然存在。以人脸识别为例，当前人脸识别技术已经达到商用级别，但是面临的挑战依然很多，如对双胞胎的识别还是一个难点；对于假体识别的疏漏依然存在；线上远程人脸识别还没有建立一个可信的环境来支持，如网上曾流传一则视频，显示当事人用一个3D打印的人脸远程破解刷脸支付，用别人的脸为自己在线购买了一张高铁票。

生物特征信息采集在数字经济时代会越来越普遍

生物特征信息日益成为个人信息中的“金矿”。随着人工智能和大数据的发展，数据已经成为互联网产业发展的重要原料。由于生物特征信息识别更加便捷，不再需要携带手机、银行卡、钥匙或者身份证等介质，未来将成为网络经济中个人身份验证的新兴入口，成为大部分互联网商业模式成立和发展的基础设施。另一方面，各类机构通过多维度收集用户数据，能够更精准地为用户“画像”，从而实现精准营销和风险管理，生物特征信息可以直接“锁定”个人身份和行为，因此，从大数据分析的信息序列中，生物特征信息排位靠前，具有重要的商业价值，日益成为数据领域的必争之地。

生物特征信息采集呈现规模化和产业化态势。从2013年指纹识别技术应用在手机上开始，生物特征识别技术大规模进入我们的日常生活。除了指纹识别外，近几年，人脸识别技术发展迅速，刷脸支付已经逐渐普及。消费者通过“刷脸”进行支付，更加便捷高效，而且体验上更快捷，尤其受到年轻人的喜爱。另一方面，人脸识别可用在追捕逃犯、重要场合快速安检等方面，有利于社会安全管理。目前我国法律对哪些机构或个人可进行人面部等信息采集以及如何采集使用等还没有全面、明确的规定。部分商业机构利用这个“时间差”，不断加快生物特征信息的采集工作，支持后端的身份识别和数据分析，拓宽数据竞争的“护城河”。特别是随着刷

脸支付、刷脸辅助开户等服务的进一步推广，对于生物特征信息的采集将越来越普遍。

生物特征信息采集管理亟待加快推进

政府部门加快推进个人信息保护的立法立规。今年以来，网信办、工信部、信息安全标准化技术委员会等部门接连发布文件。正在公开征求意见的《数据安全保护法》要求收集个人信息使用规则应当明确具体、简单通俗、易于访问，并重点明确：一是收集使用个人信息的目的、种类、数量、频度、方式、范围等；二是向他人提供个人信息的规则；三是个人信息主体撤销同意，以及查询、更正、删除个人信息的途径和方法；四是仅当用户知悉收集使用规则并明确同意后，网络运营方可收集个人信息。针对当前移动互联网应用中存在的超范围收集、强制授权、过度索权等个人信息收集安全问题，《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）》明确了个人信息收集必须要用户同意和最小化原则。可见，政府部门对个人信息保护的原则和底线都是明确和一致的。

与其他个人信息相比，生物特征信息收集更加敏感。生物特征信息无疑属于个人信息当中最具争议、最受关注的部分。如前面提到的ZAO的人脸信息收集。另外一个事件也比较典型，据报道，某大学“试水”教室安装人脸识别系统，“上课发呆、玩手机都能被感知”，引发了社会公众对于隐私保护的担忧。教育部对此做出回应，“希望学校慎重使用生物特征识别等技术，对于学生的个人信息，能不采集就不采，能少采集就少采集，尤其涉及到个人生物信息的”。在国外，对于生物特征信息的保护更加严格。由于担心侵犯公众隐私权，从而产生法律风险，微软删除了其最大的公开人脸识别数据库——MS Celeb。MS Celeb数据库拥有超过1000万张图像，将近10万人的面部信息。

我国还没有专门针对收集和使用生物特征信息做出规定。不同于一般的个人信息，对于生物特征信息应实

行更加严格的管理，对实行人脸识别、录入的单位及相关人员应严格限制。对于新出现的一些生物特征识别技术，类似虹膜、指纹、刷脸、声音等辨别认证技术必须“特许经营”，凡此类技术公司设立必须“先证后照”，必须有较高的进入门槛。

增强消费者对生物特征信息采集的辨别力

对于个人信息的保护，需要政府加快立法，加强管理，设定底线，严厉打击侵害个人隐私的违法行为。作为消费者，尽管出于便捷性和政策性的要求，我们不可能完全不使用自己的生物特征信息，但是具备一定的辨识力和自我保护的意识，不能仅图一时便捷。

消费者要进一步提升个人信息保护的意识。在互联网和信息大爆炸的时代，各类机构过度收集、非法使用甚至泄露个人信息的行为屡见不鲜。这些泄露的信息，很可能会成为侵害个人权益的突破口。个人信息泄露导致的网络暴力、网络欺诈、恶意骚扰、传播个人隐私信息等违法行为时有发生。个人生物特征信息泄露的危害性更大。因此，消费者要有个人信息权的概念，培养个人信息保护的意识和能力，强化自身权益的保护。

消费者对生物特征信息采集要保持谨慎态度。消费者在网上办理相关事项时，遇到收集个人信息的情况，要提高警惕，要坚持“最小必要原则”，谨慎提供生物特征信息，特别是在移动APP中弹出的涉及生物特征信息采集的用户协议和隐私政策不要为了使用软件的功能直接点“同意”按钮，最好先浏览一下协议的隐私政策，对那些明显对消费者不利或者涉嫌过度采集的条款可以进行投诉。对于陌生或不常用的APP，不要轻易开启其自带的生物特征识别功能，从而避免提供生物特征信息。



算法价格歧视的市场解决机制

□ 王延川

目前，“大数据杀熟”已被大众广为诟病。“大数据杀熟”其实就是算法价格歧视，也称为差别化定价，即算法收集网络用户的交易历史记录，为其勾勒消费“画像”，经过评估让这些“老用户”支付比市场价格更高的价格。作为严重损害消费者利益的反竞争行为，算法价格歧视出现在网络订票、订房、购物、旅游、约车等多种场合，其已经成为一种较为普遍的社会现象。

大数据背景下的算法价格歧视

传统实体交易市场条件下也存在价格歧视，只是为消费者勾勒“画像”的工作都由自然人来承担，但人工勾勒“画像”很难促成价格歧视，数字市场则给价格歧视创造了很好的条件。首先，消费者使用各种APP购买商品和服务，留下各种浏览网页信息的“痕迹”，这些数据为商家捕捉消费者的消费偏好提供了很好的机会。其次，数字市场不再局限于特定的区域，而是扩展至全国乃至全球范围，陌生的消费者之间互通价格消息几乎不可能，价格歧视难以被发现。

伴随着计算机的强大计算力与大数据处理，商家开始大量使用定价算法，这为价格歧视创造了更好的条件。商家通过算法更容易和高速地捕捉消费者的消费偏好、购买习惯、搜索历史等方面的数据，且可以借助上述数据计算出消费者可以支付的最大化价格。

另外，算法还会利用消费者的消费偏见来引导消费者，或者向消费者固定推介某一类产品或者服务，其目的在于“迫使”消费者习惯并依赖某一类产品或者服务，最终将消费者“锁定”在算法所设定的生活方式之中，任由其“摆布”，进而获取额外利润。

市场解决机制：消费者算法

针对算法价格歧视，学界提出了一些应对方法。譬如，禁止商家使用算法，建立举报人制度，强制要求商家披露算法，运用算法事前监管商家算法。这些方法要么损害市场自由原则，要么难以实行，要么成本很高，均非可取的方法。还有人从合同法角度，提出消费者可以拒绝签订某些合同或者撤销合同，但这些措施涉及司法程序，给消费者带来一定的时间成本。

算法是一把双刃剑，它一方面促进了算法价格歧视，另一方面也极大地促进了数字市场的交易透明度，让消费者在线比较商品及其供应，享受价格更低的商品或找到更符合他们偏好的商品。而过度干涉算法使用会出现相背离的效果。有人提出以消费者算法来对抗商家算法的方法，这样既可以缓解算法价格歧视，又可以保全算法带来的社会福利。被称为“算法管家”的消费者算法在实践中已经出现，主要用于消费者与在线商家互动。消费者算法不仅可以满足消费者单纯的购物需求，还可以用来对抗商家算法。

消费者算法的运行是众多消费者借助相同APP选择自己想要购买的商品和服务，APP将这些选择集合在一起，进行分类后交由其算法在数字市场上匹配，消费者算法通过网络搜索或比较价格帮助消费者收集信息，然后进行比对和决策，并向商家算法发出交易要约。

对抗算法的策略

消费者算法可以模糊消费者的消费“画像”，消解算法价格歧视的生成条件。算法价格歧视建立在算法掌握消费者的选择偏好、购买习惯、搜索历史方面数据的基础之上，消费者算法可以将众多消费者的偏好选择聚

合为一个虚拟买家，由于消费者算法通过聚合实现了消费者的“匿名化”，消费者个人需求曲线被模糊化，商家算法无法收集消费者的消费信息，其价格歧视的企图被“粉碎”。

消费者算法与商家算法进行价格博弈，缓解或瓦解算法价格歧视。消费者可以在算法中设定自己可以接受的最高交易价格，如果商家的价格超出设定的价格，算法就会停止交易，迫使商家调整价格，否则消费者算法会在市场中继续寻找别的商家，以匹配消费者设定好的价格。

市场解决机制的构建

消费者算法具有强大的保护消费者功能，但其开发和运行存在以下几个问题：第一，消费者人数众多，存在集体行动的困境问题，自发去组织和使用者消费者算法的协商成本巨大。第二，消费者算法的使用，使得在消费者与商家信息不对称之外，又增加了消费者与消费者算法之间的信息不对称。第三，消费者算法在消费者之间进行价格协调，也可能被认定为具有“反竞争”嫌疑。第四，商家可以开发更先进的算法，用来击败消费者算法。商家还可以买通算法开发商，在提供给消费者的算法中设置对消费者不利的程序，或者雇佣黑客来破坏消费者算法的功能，使其难以发挥应有的效果。

解决上述问题的过程也就是构建消费者算法的过程：第一，针对消费者集体行动问题，解决方法是让消费者保护机构牵头组建消费者算法平台，再由消费者对平台实行集体共治。消费者人数众多，可以成立消费者算法发展委员会，委员会和消费者之间是委托关系，应该对使用交易平台消费者负注意义务和忠实义务。委员会的成员应该多元化，除了消费者和消费者保护机构的代表之外，还应该包括计算机专家和数据科学家等专业人士。第二，消费者算法应该被设计为不能“背叛”消费者的算法，以化解消费者与算法之间的信息不对称，保证消费者利益最大化。在程序设计中，用该表明其目的在于对抗商家算法，避免其被认定为具有“反竞争”嫌疑。第三，通过对算法进行训练，建立模式检测程序，识别黑客攻击行为，进而构建自己的识别模型，当识别出攻击行为时进行自我保护或者进行必要的反击。第四，委员会专家可以深入理解消费者算法的运行机理，时刻关注技术发展，并在必要时更新消费者算法技术，以有效地对抗商家算法。

消费者算法虽然不会彻底消灭算法价格歧视，却可以通过统一行动化解消费者的谈判能力，缓解或者化解算法价格歧视，这种市场治理方法，既避免了对算法使用的过度干预，又可以对抗商家算法，最终实现保护消费者利益以及提升数字市场竞争力的效果。



□ 刘海军 李 晴

习近平总书记对国家网络安全宣传周作出重要指示，强调要坚持安全可控和开放创新并重，坚持促进发展和依法管理相统一，提升广大人民群众在网络空间的获得感幸福感安全感，这是对当前网络安全工作提出的具体要求和行动指南。贯彻落实总书记重要指示精神，做好网络安全工作要瞄准一个总体目标，理清两个主要关系，把握三个通用原则，聚焦四项重点任务，统一五个标准规范。

瞄准一个总体目标。聚焦于党的领导下网络强国建设的统一目标，实现从网络大国到网络强国跃升。正如习近平总书记所强调的，“要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国”。具体来讲，就是要建设网络强国、数字中国、智慧社会，推动互联网、大数据、人工智能和实体经济深度融合，发展数字经济、共享经济，培育新增增长点、形成新动能。

理清两个主要关系。理清网络安全与信息化发展、网络使用与网络监管的关系，牢牢把握网络安全的战略地位。一是处理好网络安全与信息化发展的关系。习近平总书记强调，“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进”“网络安全和信息化要同步推进，网络安全和信息化是一体之两翼、驱动之双轮”“没有网络安全就没有国家安全，没有信息化就没有现代化”。二是处理好网络使用与网络监管的关

系。网络空间不是法外之地，有使用就要有监管，要进一步加强监督管理力度。国家层面有《网络安全法》，以“法”的形式对网络运行、信息安全和网络行为作出了明确规定。企业层面有《互联网新闻信息服务管理规定》《微信公众平台运营规范》等一系列规定，做到了有法可依。无论是网络使用者，还是平台建设者，都要遵守国家法律法规和社会道德规范。

把握三个通用原则。就是要理解好三个“对统一”，处理好促进发展与依法管理的矛盾。一是既要齐抓共管，又要百花齐放。无论是网络管理者，还是服务提供者，在思想认识上都必须与党和国家的要求高度统一，在具体网络应用领域可以各有特色，鼓励个性化发展，满足个性化需求。在资源整合和网络监管等方面，要统一标准，共治共治，共同维护信息安全和网络清明。二是既要自上到下，又要自下而上。无论是国家层面，还是地方层面，在网络建设和信息化发展的顶层设计、规划制定时，可以采取自上到下的方式，便于统一标准和贯彻执行。在具体项目和系统开发时，可以采取自下而上的方式，积极鼓励试点和经验推广。三是既要安全保底，又要加快发展。在网络和信息化发展方面，各地情况不同，应当结合实际因地制宜开展工作。要将网络安全摆在首位，牢牢守住安全底线，但又不可因噎废食成为约束，要边建设边防护，将制度约束和技术措施结合起来，正确处理好网络安全和

信息化发展之间的关系。

聚焦四项重点任务。就是要坚持安全可控和开放创新并重，做好网络的“管”“防”“建”“用”。一是加强互联网管理。在已有法律法规和管理规范的基础上，建立健全与互联网有关的管理制度，细化相关实施细则，做到有章可循，明确政府、企业、个人在维护网络安全和网络清明等方面的职责义务。二是加强网络安全防护。建立健全网络风险评估、网络安全预警、情况通报等制度，努力建设高素质的网络安全和信息化人才队伍，确保人员、技术双到位。三是加快网络建设和推广。从网络大国到网络强国是国家战略，不同主体、不同个人应有不同职责。网络服务提供者要结合实际，从用户需求出发，提供安全稳定的网络环境和方便快捷的应用体验。网络管理者要加强对网络和信息系统开发的指导和监督，提升信息化的应用效果。四是加快互联网成果应用。加快互联网知识普及，加快网络基础设施建设，加快数据资源建设共享，加快最新信息技术转化，使互联网更加“接地气”，提高人民群众在网络空间的获得感幸福感安全感。

统一五个标准规范。就是要规范“制度”“技术”“数据”“安全”“考核”五类标准。一是完善规章制度。建章立制，规范管理，建立统一的使用管理机制，是确保网络安全、加快互联网成果转化的前提。目前来看，法律条款、行为规范已经很多，但具体的管理办法、有效的网络安全机制

等操作层面的内容还较为紧缺。二是统一技术规范。按照国家信息系统整合共享的基本要求，加强信息部门的统一规划能力，建立信息系统先评估、后建设、再使用制度。在方案设计、网络和信息系统开发等方面，应当遵循国家标准、行业规定或国际惯例，采用最新最成熟的信息化技术手段。三是统一数据格式。从互联网应用的角度看，数据资源共享等方面还缺少统一的规范标准，不利于国家提倡的信息资源整合共享的总体思路，应当尽快研究制定国家层面的数据资源建设、应用的规范标准并加快推广。四是统筹安全规划。互联网发展过快，安全防护未能及时跟上。整体来看，符合国情民情的网络安全评估规划较少，且各自为政尚未统一。不同类型的网络建设者应当结合各自实际，拟制网络安全长期或短期规划，作为开展网络安全工作的依据。五是完善考评标准。加强对网络建设者和网络服务商的管理迫在眉睫，应当尽快引入考核评估和督查手段，将网络安全摆在首位，先防护、再建设，边建设、边规范，利用技术手段加强技术治理，从建设源头和使用末端同时发力，共同保护好网络安全，维护好网络清明。

