人脸识别信息保护亟待专门立法

前沿观点

□ 杨华（上海政法学院人工智能法学院教授）

习近平总书记指出，“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”“要加强人工智能发展的潜在风险研判和防范，维护人民利益和国家安全，确保人工智能安全、可靠、可控”。由于人脸识别信息作为敏感数据保护的复杂性、人脸识别技术与法律的融合性、人脸识别技术应用的具体标准尚未完备，人脸识别技术应用的边界、如何避免人脸识别技术滥用、人脸识别信息受到侵害后如何救济，等等，亟待通过专门立法予以明确。

人脸识别信息保护法律规制的现状及其存在的问题

（一）对“人脸识别信息”缺乏明确的法律界定

什么是“人脸识别信息”，目前法律并没有统一的规定。从语义上讲，人脸识别信息，属于人脸信息的子类概念，但其具体的法律概念界定仍需要进一步明确。个人信息保护法并没有对“人脸识别信息”给出明确的界定。我国其他立法如民法典、数据安全法和网络安全法对“人脸识别信息”的法律界定更是缺乏。

（二）缺乏人脸识别信息保护的专门规定

与人脸识别信息保护密切相关的法律有个人信息保护法、数据安全法和网络安全法，三部法律通过对个人信息或数据保护的法律规范，对人脸识别信息保护起到了间接规范作用。此外，宪法、民法典、刑法、电子商务法、《全国人民代表大会常务委员会关于加强网络信息保护的决定》以及《关键信息基础设施安全保护条例》、电信条例、《征信业管理条例》等法律、行政法规，均无法直接适用于人脸识别信息保护。

（三）司法解释无法替代人脸识别信息保护的立法和执法问题

郭兵诉杭州野生动物世界有限公司滥用人脸识别案，在一定程度上推动了2021年7月《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》的出台。然而，司法解释解决不了人脸识别信息保护的立法问题和执法问题。一方面，全民守法的前提是“有法可依”。司法解释正是在立法缺失的情况下，在审判领域确立人脸识别信息保护纠纷解决依据的被动之举。另一方面，人脸识别信息保护的执法工作急剧增长，根据“依法行政”的执法原则，缺少人脸识别信息保护的立法，必然会给执法工作带来极大的不便。

（四）地方法规没有实质性推动人脸识别立法

很多地方政府或人大制定了人脸识别的立法规定。例如，《上海市数据条例》《广东省社会信用条例》《天津市社会信用条例》《深圳经济特区数据条例》等，体现了人脸识别在全国很多地方正在走向法治化道路。然而，这些地方立法大都是参照现有国家立法所做的简单重复，而且条文比较少，对人脸识别技术应用的过程规范性、对自然人人脸识别信息的保护及其受到侵害后的损害救济，均缺乏相应的规定。

完善人脸识别信息保护的实体法律规范

（一）法律规范应注重人脸识别技术应用的利益平衡

人脸识别过程中，有多方利益需要平衡。一是国家因对人脸信息数据的归集、整理和分析，提高了国家治理体系和治理能力现代化水平，实现了国家数字经济、技术经济的快速发展。二是行使国家管理权的机构或部门可以在提高效率、节省人力、强化权威等方面受益。三是行使公共管理职能的企事业单位、基层自治组织既完成了国家授权的职能，也实现了自身利益需求。四是营利性的私营企业可以精准排查客户、节省运营成本、提高运营效率，还可以对客户的信息数据进行加工、整理形成独具特色的商业模式。五是公众可以享受人脸支付、人脸乘车、人脸住宿等系列便利。在这五个方面的受益主体中，谁将享受到最大的利益？谁应当享受最大的利益？利益主体之间是否会存在此消彼长的关系？怎么保障各利益主体之间的平衡？这是人脸识别法律规范制定过程中需要考虑的问题。

（二）确立人脸识别信息保护的基本原则

属于敏感个人信息的人脸识别信息相较于一般个人信息而言，受到侵害时的后果更为严重，应受法律的特殊保护。我国在制定人脸识别信息保护规范时应当确立如下原则：一是使用人脸识别的合法、正当和必要原则。二是处理人脸识别信息应当遵循诚实信用、公开透明原则。三是保障自然人的知情同意权和选择权原则。四是严格人脸识别商业性技术应用标准原则。五是明确人脸识别信息的最小化收集、利用和事后删除原则。六是确立鼓励技术创新原则。

（三）厘定人脸识别信息权益的保护范围

人脸识别信息权益的保护范围至少包括如下几个方面：一是民法典中规定的权利。具体包括与人脸识别信息相关的人格权、肖像权、隐私权、人脸识别信息产生的财产权、个人信息权等。二是个人信息保护法中规定的与人脸识别信息保护有关的人格尊严与人身财产安全以及通信自由和通信秘密等利益，为实现个人信息权益保护的同意权、知情权、查阅权、复制权、转移权、更正权、补充权、删除权、请求解释说明权等权利。

（四）明确人脸识别技术商业应用规则

由于商业应用的风险较大，我国有必要为人脸识别技术商业应用的主体设定人脸识别的“告知-同意-限制使用-及时删除-损害赔偿”规则。告知是指使用人脸识别技术收集人脸信息时必须告知对方。同意是指在收集、使用、披露个人信息之前也必须征得个人明示或默示的同意。限制使用是指使用人脸识别信息必须有加密措施并获得相应许可后方可使用。及时删除是指将不必要保留的人脸识别信息按照法律规定的时间、方式和途径予以删除。损害赔偿是对于违反法律规定的人脸识别技术应用主体赔偿受害人的标准和方式。

（五）规范公权力机构人脸识别技术应用

为了防止公权力的滥用，要适当规范政府或公共机构安装使用人脸识别技术或设备的行为。一是要减少政府或公共机构安装、使用人脸识别设备的随意性。二是政府部门获取、保存、访问、使用人脸识别技术获取的信息，要经过严格的许可程序。三是人脸信息的主体有权向政府部门申请查看自己的人脸信息并有权要求政府部门或公共机构删除自己的人脸信息。四是行使公共职能的机构要严格履行政府的授权或审批程序后方可使用人脸识别技术或设备。

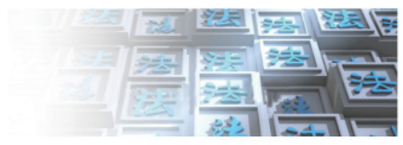
（六）明确人脸识别信息保护的违法责任

首先，界定人脸识别信息保护违法责任主体及法律责任。需要依法明确承担人脸识别信息保护违法责任的主体、方式和内容，明确违法责任的主观状态和客观行为表现。其次，严厉打击利用人脸识别技术的相关犯罪行为。由于违法犯罪分子使用数据的目的和手段不符合规定，应当施加严格责任。

（七）优化人脸识别信息保护的程序性规范

对人脸信息受侵权人的救济，除了通过实体规则确立其相应权利之外，还要通过程序法的规定确立或优化其权利的实现路径。优化人脸识别信息保护的程序规则，可以通过确立人脸信息侵权行为的举证责任倒置规则、建立人脸信息侵权行为的集团诉讼机制和完善司法救济机制等方式实现自然人人脸识别信息权益保护。

用法律净化网络环境



前沿话题

□ 李耀宇

党的二十大报告明确指出，良好的网络生态，是建设具有强大凝聚力和引领力的社会主义意识形态、增强文化自信的重要内容。

虽然近年来对网络环境的整治取得了较为显著的效果，但同时也要看到，网络秩序规范仍然存在不少问题，有必要进一步强化对网络环境的法律治理力度。笔者认为，目前，网络环境中有害因素的危害表现主要可以概括为两个方面：

其一是不法分子对守法公民的侵犯。在网络环境下，得益于空间距离的消解带来的接触成本大幅降低，不法分子可以轻易接近他人并实施违法犯罪行为。网络空间中不法分子侵犯他人的方式主要有以下几种：一是用语言对他人实施侮辱、诽谤、网络暴力等侵害行为，从而间接造成对方名誉权、健康权甚至生命权等权益的损害；二是利用网络提供的数据便利直接实施诈骗、盗窃、敲诈勒索等侵犯他人人身权和财产权的违法犯罪行为；三是引诱他人参与网络违法犯罪活动，一些不法分子以分享违法所得为诱饵，将部分思想意志不坚定的普通网民，特别是青少年网民拉进网络不法组织或黑灰色产业链中，继而使网络不法势力得以进一步扩张。

其二是有害信息对传播空间的挤占。网络的自由、开放、高速等特性，使其中汇聚了各种各样的信息，其中虽不乏有益信息，却也掺杂了不少有害信息。受制于人有限的信息处理能力和甄别能力，有益信息在与有害信息的竞争中往往是处于劣势的一方，使得传播空间更容易被有害信息占据。有害信息对传播空间的挤占主要有以下表现形式：一是色情、暴力、低俗的视听信息在网络上大肆传播，且形式愈发多样化，这是自现代媒体产生以来就有的痼疾，在网络中得到了进一步发展；二是极端反主流文化和不良网络亚文化在网络中的蔓延，这两种思想文化都是以思想自由、彰显个性等名义，否定社会主流价值观，否定多数人认可的基本道德准则；三是别有用心的人为达到自己的政治或者商业目的，散布夸大社会矛盾、煽动群体间仇恨的信息，在网民间制造焦虑，破坏社会和谐，阻碍社会主义社会的建设。

从中我们可以看出，不良网络环境的危害具有普遍性，小到个人道德水平，大到国家稳定社会和谐，都会不同程度受到不良网络环境中蔓延的“毒素”的袭扰。如不加以控制，其危害将不仅限于网络空间，也会影响现实生活的安定。在控制和治理网络环境的各种手段中，法治手段是最稳定最持久也是最根本的手段。加强对网络空间的法治力度、完善网络法治体系，可以让网民认识到网络空间也是法治社会的一部分而非逃避约束的灰色地带，进而形成主动抵制不法行为和有害信息的网络氛围，达成网络内部的良性生态循环，是解决网络环境问题的最优解。

加强网络空间法治力度，完整、明确的法律规则体系是基础。目前，网络安全法等相关法律仅对使用网络的行为规范作了原则性规定，对于不正当使用网络行为的表现形式几乎没有作出任何具体的划分。在技术手段日臻成熟且实践经验日益丰富的当今，对网络中的不法行为和有害信息进行精细化类型划分的时机已经成熟，应尽快制定更为详细的网络行为规范。同时，要进一步完善对违法行为的处置体系，对每一种类的网络不法行为都设置对应的处置措施。对于较为轻微的不良行为，可以通过网络平台的警告、封禁等措施配合普法教育使行为人认识到自身的错误；而对于危害较为严重的不法行为，需要法律的强制力介入，对其进行惩罚；对于危害特别严重的犯罪行为，应追究其刑事责任。在处罚方式上，除了传统的法律责任外，可以考虑增设限制或禁止行为人一定期限内使用网络的处罚，在预防再犯的同时也有助于行为人脱离网络不良环境、回归主流社会。

加强网络空间法治力度，司法的推动作用同样不容忽视。网络的发展千变万化，新事物、新技术不断出现，不能期待立法能概括当下所有的问题、预知将要出现的问题。因此，在采用相对灵活的立法方式的同时，应该充分发挥司法的能动性作用，填补立法留下的空白。司法工作者应当敢于适用法律、敢于提出问题，并及时总结经验，制定司法解释、指导案例等具有规范或指导作用的文件。

加强网络空间法治力度，同时要做好网络普法工作。网民的受教育程度和综合素质参差不齐，部分网民法治意识淡薄，在实施有害于网络环境的行为时缺乏羞耻感。对此，应当强化网络空间中的法治宣传和法治教育，让网络法治的观念深入每一位网民心中。为此，可以采取的措施有：定期开展网络普法宣传活动，并通过奖励等方式鼓励广大网民积极参与；在网站和网络平台中嵌入网络普法宣传文案；对特定人群（如未成年网民、上网时间较长的网民、经常被他人举报的网络平台用户）进行专门的网络普法教育等。

对网络环境的治理将是一项长期且艰巨的工程，但只要坚持走中国特色社会主义法治道路，必然能建成符合社会主义核心价值观的网络生态。

公共数据商业化服务中的合理利用

前沿关注

□ 苏剑

商业化服务中的公共数据合理利用需求

随着大数据的发展及商业模式的变革，数据已然成为新时代商业竞争的核心内容，而公共数据作为数字经济发展中的重要生产要素，电子商务法、网络安全法等法律均鼓励建立公共数据共享机制，促进公共数据资源开放。具体而言，公共数据是指政府部门、公益性事业单位以及涉及公共生活的企业，在依法履职或为社会提供公共服务的过程中收集与产生的各项数据及其衍生数据。为鼓励公共数据在更大范围的共享与流动，最大程度发挥公共数据的价值，应当赋予数据分析企业充分利用公共数据并享有基于公共数据利用而产生的相关数据权益。

从事企业征信等工作的互联网企业通过对公共数据的商业化利用，运用其自身大数据技术的优势，将本身处于碎片化的公共领域局部数据进行整合，使之能够较为完整地反映特定内容，实现了公共数据领域的市场信息共享，为解决市场中的信息不对称、信息滞后等困境提供了便利，有效降低了市场主体的信息收集成本，增加了市场交易的透明度。但也应当明确，公共数据同样与原始数据主体、公共数据消费者、公共数据提供者等主体的利益高度相关。例如，各地的政府数据开放平台就包含下属政府机关的信息公开、法人注册信息等内容，并涉及生活服务、城建住房、教育文化、财税金融等诸多场景。可见，公共数据的形成与内容决定其具有公共属性，其较之个人、企业等主体的数据，内容更为庞杂、范围更为宽广。是故，在公共数据商业化服务中，在保障社会整体利益的同时，亦应当兼顾各方主体的合法权益。因此，厘清公共数据在商业化服务中的合理利用边界，确保公共数据的来源、质量等方面符合法律规定，约束公共数据的使用行为，促进公共数据的正当使用，规范与改进算法技术，是实现数字经济良性发展的重要内容。

公共数据商业化服务中合理利用的责任与义务

公共数据具有极强的公益属性与可共享利用的经济价值，充分引导、发挥公共数据作为生产要素的功能与作用，是促进数字中国建设，助力中国式现代化实现的重要保障。但公共数据的形成本身是以个人数据等内容为前提，在使用公共数据中，通过数据抓取、分析等技术手段，难免会与个人数据、企业个体数据等其他信息形成交叉。应当明确，个人利益的实现不应以损害其他主体的利益为前提，民法典亦规定“自然人的个人信息受法律保护”“处理个人信息的，应当遵循合法、正当、必要原则”。申言之，公共数据的商业化服务应当做到利用的正当、合法，不得损害国家利益、公共利益以及他人的合法权益，特别是不能损害原始数据主体的正当权益。因此，在公共数据商业化服务中企业应当承担相应的社会责任，其本身是企业的无形资产之一，能够帮助企业在长期商业行为中树立良好的企业形象。并且，企业履行社会责任也是一种信号工具，亦能够降低投资者的信息搜寻成本，为企业创造积极的竞争环境。

一方面，为平衡公共数据商业化服务中的价值与风险，法律应当对涉及国家机密、商业秘密及个人隐私的敏感数据进行必要限制，从而避免其他机构与个人在使用公共数据时造成对国家利益、公共利益及个人正当权益的损害。根据公共数据的敏感程度不同，可以将公共数据划分为自由使用与申请使用两种，严格限制敏感数据的申请范围，并作出申请的利益衡量及损益审查。申请使用是对商业化手段的合理纠偏，从而实现公共数据公益属性与经济价值的平衡。但也需要防止部分管理部门为规避风险将公共数据均设置为申请使用，从而挤压自由使用空间，加大公共数据使用成本。同时也应当明确，公共数据的公益属性也要求经济价值的发挥以安全可控为前提，避免因小失大。政府作为公共利益的代表，需要承担起公共数据商业化服务中合理利用的监管职责，包括制定相应的数据使用细则、数据全生命周期监管以及对不当利用公共数据的主体予以惩戒等。此外，为了确保公共数据资源能被公众高效使用，管理部门还应当对影响公共数据使用的行为予以限制，如滥用爬虫技术抓取公共数据造成网络拥堵等，确保公共数据的合理使用。

另一方面，利用公共数据进行商业化服务的企业与个人亦应当在使用公共数据时坚持自我审查，尽到注意义务。一是确保数据来源的合法性，应当在官方公布的公共数据中进行采集与使用；二是确保数据使用程序正当，对需要申请使用的公共数据，需要向监管部门说明使用的相关性与合规性，并获得授权；三是注重对数据的时效进行检测，确保信息的及时性与有效性；四是保障数据公开的内容质量，避免无效或错误信息；五是做好敏感信息校验，对涉及国家利益、公共利益及个人正当权益的敏感信息进行筛除。然而，受公共数据使用的成本、技术等限制，不应对商业化利用企业或个人提出过高的注意义务，如普通的信息偏差应当允许其通过事后修正的方式予以救济。同时，公共数据商业化服务除政府监督与自我审查外，还应形成多渠道监督合力，如鼓励第三方主体在利益相关者之外开展独立性监督，通过设置数据专家委员会等机构对公共数据的使用行为进行数据安全审查、认证与评估，从而形成更广泛、更直接的多元数据主体治理格局。

观点新解

胡梦瑶谈行政处罚期间制度——

包括追究时效裁决时效执行时效

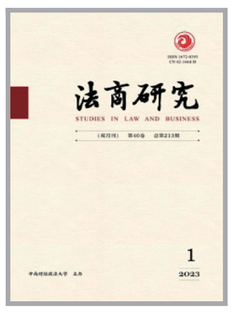
中国政法大学胡梦瑶在《政法论坛》2023年第1期上发表题为《行政处罚期间制度的规范检视与体系建构》的文章中指出：

完整的行政处罚期间制度包括追究时效、裁决时效和执行时效，这构成规范和限制行政处罚全过程和各阶段的期间制度体系。这三者处于行政处罚的不同程序节点，可以在时间上贯通到底、相互衔接，分别对应和限制着行政处罚的追究权、裁决权、执行权。具体来看，追究时效是行政机关对违法行为进行责任追究的期限，超过此期间就不得再追究责任。行政法上的追究时效对处罚权的限制，比刑法上的追诉时效对刑罚权的限制更为宽松；若尚未超过追究时效，行政机关发现违法行为就可以通过立案调查予以追究，但必须在裁决时效内作出处罚决定；行政处罚的执行时效就是强制执行的时效。在处罚决定作出后，若违法相对人在法定期限内不履行决定，则处罚机关必须在执行时效内强制执行或申请法院强制执行。

当前，行政处罚法规定的2年处罚时效是追究时效，它仅适用于违法行为的追究阶段；规定的90天办案期限并不发生实际法律效果，并非是规范意义上的裁决时效。同样，行政强制法规定的为期3个月申请法院强制执行的期限也缺乏刚性法律后果，不是真正限制处罚决定执行力的执行时效。经由理论检视，规范意义上的追究时效、裁决时效、执行时效在适用对象、起算时点、计算规则和期限经过的法律效果等方面存在显著差异，这三者在制度属性上分别对应权力期间、除斥期间和消灭时效，应当根据其制度属性展开立法建构和解释适用，才能发挥理想的规范效果，形成统一的期间秩序。具体来说，在立法论上，要注意这三者之间的内部衔接以及与刑法上追诉时效的外部衔接制度设计；在解释论上，要注意这三者之间的适用衔接以及执行“双轨制”模式下执行时效制度的内部一致性。完善的行政处罚期间制度经由立法论和解释论的合力体系化，最终方能实现规范和限制行政处罚权行使全流程的“时间法治”。

焦和平谈算法私人执法侵蚀版权公共领域的应对——

将版权公共领域考量植入算法设计中



西安交通大学法学院焦和平在《法商研究》2023年第1期上发表题为《算法私人执法对版权公共领域的侵蚀及其应对》的文章中指出：

在传统的版权法架构下，版权执法主要是指公权力机构对版权侵权纠纷的处理。20世纪末迅猛发展的互联网技术所带来的信息暴增、网络盗版泛滥使得在人力、财力和手段上都较为有限的公权力执法模式面临严峻挑战，由此出现了版权领域的“执法失灵”现象。为应对这一“执法失灵”现象给版权维权造成的不利影响，版权人开始在公权力执法之外寻求与网络服务商合作以共同打击网络侵害版权行为，并探索出遏制网络版权侵权的“通知-移除”机制。随着算法技术的应用，版权领域的私人执法模式从人工操作转向全程算法化，表现为查找侵权行为算法化、发送侵权通知算法化、处置侵权信息算法化、预防侵权发生算法化。

私人执法算法化在极大提高执法效率的同时，也造成了对版权公共领域的侵蚀，主要表现为压缩“个人使用”空间、剥夺“适当引用”机会、阻碍“科学研究”开展、架空用户“反通知”权利等。造成上述后果的根源在于侵权认定的复杂性与算法技术的局限性以及利益驱动下算法执法机制被滥用。

算法私人执法侵蚀版权公共领域的应对可从以下方面进行：(1)将版权公共领域考量植入算法设计中。这一建议在理论上具有正当性。即使在发现涉嫌侵权材料与版权作品具有“实质性相似”时，版权人尚不能立即向网络服务商发出移除通知，网络服务商亦不能立即处置涉嫌侵权材料，而应进一步审查该涉嫌侵权材料是否属于版权公共领域的信息。(2)在特殊情形下以人工审查辅助算法执法。在算法设计中植入包括合理使用在内的公共领域考量并不能完全避免算法执法对公共领域的误判，由此使得在算法执法主导下，辅之以人工审查提高算法执法的可信度便显得尤为必要。(3)完善过滤机制下的用户申诉程序。在算法过滤机制下，网络用户向互联网平台上传材料之前需要经过网络服务商的算法筛查，如果筛查结果被算法标记为涉嫌侵权信息那么无法上传至网络平台，此乃算法技术下版权私人执法的独有环节。(4)针对恶意通知行为规定惩罚性赔偿责任。在版权私人执法尚未算法化的人工操作时代，在实践中就经常发生版权人出于恶意竞争目的向网络服务商故意发出错误通知的情形，因此建议针对恶意通知行为规定惩罚性赔偿责任。

（赵珊珊 整理）