

人脸识别法律规范初探： 权利属性、保护基础与法律对策

马俊军 王星宇

摘要：人脸识别技术作为图像识别领域的人工智能在近十年展开了大规模商用，传统的自然人隐私权、信息财产权已无法准确描述其法律属性。本文认为，人类社会的文明从农业文明转型到工商文明，再到今天的数字文明，人类最重要的资源也从土地、资本转向数字。在数字时代，数据刻画了自然人的数字属性，描绘了自然人的数字画像，包括人脸识别信息构成了数字人权的重要内容。人脸识别信息保护的理论基础包括个人信息自决权理论、权利救济理论，特别是利益平衡理论。保护的法律对策包括整合分散的法条细化处理规则、强化政府对人脸识别技术使用的监管、加大权利救济的司法保护力度、加强行业自律改进企业内部《隐私政策》设置等。

关键词：人脸识别信息；权利属性；理论基石；法律规范

中图分类号：D922.16 **文献标识码：**A **文章编号：**1673-5706（2023）03-0060-07

一、人脸信息权利属性

人脸信息是人脸识别技术的成果，是通过人脸识别设备对人脸进行信息采集，提取人脸特征点将人脸信息转化为数字形式，再与数据库存储的数以亿万记信息比对，以此完成确认身份的目的^[1]。人脸识别技术的特征，大都可以概括总结为三点：一是自然性，即每一个自然人都有区别于其他个体的自然特征，例如面部特征、指纹特征、声波以及虹膜特征等。社会主体区别不同自然人个体的依据就是此类自然特征，人脸识别技术正是利用了这些具有唯一性的生物特征来识别确认信息主体的身份。二是非接触性与隐蔽性，即人脸识别技术不同于指纹识别等技术，其不需要信息主体通过触碰按压识别系统的外接设备来采集个人信息，远程空间即可完成信息采集、处理、

储存等一系列行为动作。三是信息处理的自动性，即人脸识别技术与传统短信密码验证相比不需要手动输入密码或者验证码，与指纹识别相比不需要主动接触识别设备，与声波识别系统相比不需要主动发出声音，与虹膜识别系统相比不需要主动将眼睛对准识别器，人脸识别技术不需要信息主体主动配合，甚至可以在被采集对象“无意识”状态下完成个人面部识别信息的提取。

由于人脸识别技术的上述特征导致人脸信息拥有复杂的权利客体，是多种权利内容的集合，且从司法实践来看，人脸识别技术滥用给信息主体带来了包括个人隐私、个人尊严、财产权、生命权、健康权等权利在内的侵害结果，因此，厘清人脸信息的权利属性有助于我们在受到人脸识别技术侵害后找到对应的救济依据和相应的救济方式。

（一）隐私权说

《中华人民共和国民法典》第1034条^①将生物识别信息纳入人格权编中个人信息保护的相关内容并同时规定：个人信息中的私密信息，适用隐私权的规定；没有规定的适用个人信息保护的规定。从中可以窥见个人信息保护和隐私权的保护是并列的两项内容，个人信息保护并不必然等同于隐私权的保护，同时隐私权也无法给予个人私密信息的全面保护。根据《中华人民共和国民法典》第1032条^②的规定，传统隐私权保护的是自然人对个人信息诸如私密空间、私密信息等的被动防御权利，而不是个人对其私密信息的主动支配与控制权利；这与对生物识别技术发展的规制和对人脸识别信息保护的初衷并不契合。同时单就人脸识别信息而言，人脸信息是自然人个体公开于社会的外部特征信息，具有一定的社会身份属性，人脸信息是自然人在社会生存交往中必须展露和公开的信息，本身不具有私密性。理论通说认为人脸信息属性具有隐私权属性是因为随着人脸识别技术链条的延长，识别算法的进步，在识别设备比对相应人脸信息后会自动粘贴诸如性别、家庭住址、消费能力、活动轨迹等私密信息，因此，将人脸识别信息指代为隐私权，不管是在权利内涵还是外延上都有所欠缺。

（二）财产权说

随着数字中国战略贯彻发展，数字经济在国民经济发展中占比越来越重要，人脸识别背后携带的各项数据所蕴含的经济价值不容小觑，人脸识别信息财产化趋势愈加明显，包括信息主体在内的人脸识别技术参与主体都可以通过买卖、交易、二次挖掘等行为从人脸识别信息上获取经济效益。由于人脸识别信息既包括个人一般信息，例如人脸、性别、年龄等，也包括附带挖掘的其

他个人私密信息，例如收入水平、消费习惯、活动轨迹、心理状态等。在商业应用领域中，商业主体已经普遍达成共识：人脸识别信息是作为一种重要的社会资源而存在，商业主体可以利用采集、处理的人脸识别信息和数据算法进行自动化决策，制定符合不同消费水平和不同消费需求的个性化市场战略，从而达成精准投送，针对性营销的目的。

但是，将人脸识别信息的权利属性划归为财产权范畴，只注重其经济效益和商业价值，会带来个人信息过度消费的现象，商业主体逐利性会加剧人脸识别信息的非法流动，随之而来的是信息泄露和滥用风险的提升。人脸识别信息财产权说关注的重点是商业利用主体的财产利益，在实践应用中人脸识别信息主体往往难以发掘自身信息的财产价值，而且单一个体的人脸识别信息财产价值有限，商业主体收集汇拢的聚合式信息才能产生巨大的经济效益，因此过分强调人脸识别信息的财产属性会对价值平衡产生巨大冲击，更多地保护在商业应用中信息收集者或者信息处理者的利益而非信息主体的利益。另外，将人脸识别信息权利属性划归为财产权，不同自然人个体之间有经济能力之差异，反映到识别信息价值上难免会产生等级分类从而导致算法歧视和身份歧视，这与人脸识别信息背后蕴含的人格权应该被平等保护的基本原则不符。

除了海量人脸识别信息汇聚在一起成为“数据富矿”，我们还应该看到在公权力机关履行公共管理和提供社会服务职能过程中人脸识别信息所蕴含的社会治理效用，例如公安机关的天眼系统对于社会治安管理效率的提升。综上所述，人脸识别信息财产权说也有失偏颇。

（三）数字人权说

如果说农业文明时代最重要的战略资源是土

^① 《中华人民共和国民法典》第1034条：自然人的个人信息受法律保护。个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

^② 《中华人民共和国民法典》第1032条：自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

地，工商文明时代最重要的战略资源是资本，那么第四次产业革命即人工智能数字文明时代最重要的战略资源就是数字了。步入数字经济时代，社会朝着智能化方向发展，数字化、智能化、网络化深度融合构成了现代社会运行的基本框架，催生了一系列诸如人工智能、大数据、云计算等新时代产物，数字人权这一概念应运而生，并成为法理学和人权法学的最新学术热点，“数字人权”引领着新一代人权^[2]。数字经济时代，传统生产要素越来越多的以数字化形式发挥作用，生产生活中源源不断产生的数据资源已然成为驱动经济增长，转变经济发展模式的核心生产要素，伴随数字资源社会地位的提升，自然人也逐渐由物理空间的人向数字空间的人转变，物理人权观向数字人权观的转变也已迫在眉睫。

在当今数字时代，人们的每一个行为动作都将产生痕迹化数据，这些海量的信息既是日常生产生活的运行轨迹，也是个人身份数据、行为数据的具象展示，这些数据刻画了自然人的数字属性，描绘了自然人的数字画像，构成了数字人权的重要内容。现代社会自然人个体假如不具备基本的数字素质，将无法接受数字化产品和服务，无法与外界社会沟通链接。人脸识别技术通过采集信息主体的自然生物特征，提取特征点，将自然信息转化为数字信息，这些信息在历经存储、转移、应用等多项流程后，最终在基础的场景验证，高级的自动化决策等领域发挥作用。同时，人脸识别技术并非由一个孤立单一的系统构成，卷积神经网络、大数据算法应用等程序共同构成了完整的功能，这些功能运行的基础就是对面识别信息在内的个人信息的深度挖掘、开发、利用。鉴于人脸识别信息在内的个人信息对于现代社会公共管理、经济运行的重要作用，对于这些数字式生产要素的保护程度更要与其重要的社会地位相匹配，我国《中华人民共和国民法典》和《个人信息保护法》将人脸识别信息确定为敏感类个人信息，《中华人民共和国民法典》将个人信息保护放在人格权编中，同时对于个人信息的特征做了说明即可识别性，其直接体现了个人信息主体的人格特征，肯定了个人信息是作为一个自然

人天然拥有的权利，对其保护的重要性如同人格尊严、个人自由一样重要。人脸识别信息的可识别性与人格权所具有的主体附随性一样，都是对于权利主体客观存在的一种反应，这也说明人脸识别信息与人格权内涵是相契合的。因此，人脸识别信息在内涵和立法保护期待上都有诸多方面同人格权相一致，加之数字经济快速发展带来的传统物理界限的消解，肯定数字化人权是保护人脸识别信息的必然选择。

综上所述，笔者认为就人脸识别信息在内的个人信息内容、特征、客体讨论而言，将人脸识别信息表述为一项新兴的权利：数字人权，是具有合理性和可操作性的。除此之外，包括人脸识别信息在内的个人信息拥有广泛且丰富的客体，都不宜将其大而化之地划归为传统的诸如隐私权、财产权等权利范畴。在促进数字经济发展、建设数字政府的历史变革中，我们也需要在公共政策中注入“数字人权”价值，强化“数字人权”的权益平衡，确立公法与私法的双重保护机制，注重场景化的人权保护，促进空间上的国际合作，进而促进数字时代的人权保护^[3]。

二、人脸信息保护的理论基石

（一）个人信息自决权理论

个人信息自决权是指信息主体有独立自主不受他人干涉的占有、使用、收益、处分个人信息相关利益的权利，是信息主体实现自我发展、自我价值提升和获得社会认同的重要手段。“个人信息自决权”概念肇始于德国，在1971德国学者Wilhelm steinmuller和Bernd Lutterbeck受德国内政部委托研究而提出“关于个人或者团体形象之资讯自决权”，并且由1983年德国宪法法院在人口大普查中正式确认采用^[4]。信息自决权的概念在德国语法语境中是指“自然人个体在个人信息利用领域有权决定其个人信息是否被采集利用以及在何种界限上被收集利用”。“信息自决权”在德国法律体系中并不是一项新生的权利，是德国联邦宪法法院依据新的社会关系变化对《德意志联邦共和国基本法》中关于一般人格权的人格尊严进行的最新阐释，联邦宪法法院推导出在技术变革引起权利冲突的过程中需要引入“个人信

息自决权”来平衡信息主体相对弱势的地位，以此保证自然人个体能够获得足够的隐私空间，捍卫自身人格尊严不受侵犯。国家在宪法层面享有使用信息的权益，但是出于对国家权力运作规范的考量，国家需要赋予信息主体控制支配其个人信息的权利，这一权利诞生的先天基础是为一般人格权中关于人格尊严的描述：法律保护个人的人格尊严和人格平等。

个人信息自决权是对信息时代技术发展扩张的回应，在信息社会背景下，个人之于国家或者其他信息收集使用主体都是相对弱势的，实际上个人信息逐渐成长为代替本人履行社会职责的外化符号。在信息收集、存储、处理、流转等过程中信息主体的意思表示很容易被排除在外，个体也很容易丧失对自己信息完整、安全的控制权，特别是在网络信息化时代，对于个体信息的保护已经不仅局限于消极被动的防御，更在于信息主体积极主动的控制支配权。2021年11月1日生效的《中华人民共和国个人信息保护法》强调敏感个人信息的处理规则实际也贯彻了个人信息自决权的原则。

（二）权利救济理论

法谚有云“无救济，则无权利”，权利救济理论是指在公民个人权利遭受侵害的时候，被侵害人既有认定损害事实的权利，也有要求侵害人予以赔偿或者补偿的权利，它预示着权利主体和救济主体的统一。这一权利行使的内涵就是人人平等，权利行使的根据是受害人拥有获得救济的权利而非他主体拥有家长式的恩赐能力。我国历来遵从大陆法系法典法的传统，信奉有权利必有救济，且以存在损害事实为理由，人脸识别信息的规制与保护存在保护——损害——赔偿的完整法律行为链条，因此在这一完整法律行为链条下权利救济理论是绕不开的理论基础，这一理论既是符合信息主体人人平等的论调，也是符合权利保护的立法精神。

将保障公民权利以成文法的形式固定下来是现代宪法成熟的重要标志。《中华人民共和国宪法》第三十七条和第三十八条规定：中华人民共和国公民的人身自由和人格尊严不受侵犯。宪法

对于公民基本权利类型的例举总是不能穷尽的，如果只保护宪法例举规定的权利或者宪法权利具体化的法律权利，那么就存在违宪法立法原则和立法精神。虽然我国宪法目前还没有列举个人信息自决权，但数字经济的蓬勃发展，数字中国的加快建设，对个人人脸信息被滥用的权利救济是对国家尊重和保障人权的具体体现。根据立宪主义原理、权利救济理论和对人脸识别信息权利属性的分析可知，人脸识别信息背后蕴藏的人格权、财产权、隐私权等相关内容都属于宪法及其部门法的保护范围，在这些实体权利遭受损害的时候，个人及有关机构可以依据相关法律法规规定采取救济措施和获得赔偿。

（三）利益平衡理论

传统经济学中利益的概念是指各种能够满足人类需求的好处，以法学视角探究利益，利益则是一种欲望和要求，这种欲望和要求是人类社会在生产生活中产生的并且渴望得到的一种满足^[5]。人类社会资源的有限性和稀缺性决定了无法满足每一个人的需求，利益争夺无法避免，利益冲突就此产生。德国法学家赫克提出，法律不仅是一种逻辑结构，同时也是各种利益的平衡，法律通过界定、分配来达到权衡各种利益的效用，进而完成阶级统治和维持社会平稳运行的目的，利用价值判断的方法对各个社会参与主体的利益进行再衡量和再分配是法律规范的重要作用。

数字经济时代，随着人脸识别技术的长足发展，各种生物识别信息在不同信息收集主体的每一次收集、存储、流转、使用过程中都会不断被填充其他标识符号。人脸识别信息所蕴含的社会管理价值和商业经济价值不断提高，作为社会生产力重要组成部分的人脸识别信息数据就成为多方参与主体争夺的稀缺资源，经历了个人权利觉醒和人文主义的洗礼，个体开始产生对抗大众对于其私生活领域窥欲的权利诉求。人脸识别技术是把双刃剑，公权力使用主体可以借用方便快捷的技术设备提升公共服务的效率和社会管理的效能，私权力使用主体可以借用人脸识别技术达到自动化决策、精准化营销的目的，提升自己商业运营的经济效益。但是信息主体对于个人生物识

别信息在内的个人信息保护期待和保护需求被技术扩张所威胁，政府以及其他信息收集利用主体站在发展利用的角度对于人脸识别信息在内的个人信息依赖和利用需求度不断攀升，这与站在规制保护角度的信息控制支配主体产生了天然对立的矛盾冲突。从全世界范围来看，法律层面上处理个人信息，都要面对两个问题，一是基于个人信息自决权强化保护，二是基于社会公共利益优先，个人信息权利需要适度限缩，加强个人信息利用。如何在保护与利用之间找到最佳的平衡点，一直是各国制定个人信息保护法时需要精准拿捏的最大难题。目前学术界已达成基本共识，将人脸识别信息等生物敏感信息与一般的信息区分开来，在如何平衡“利用与保护”两者关系时，人脸识别等生物信息要坚持“保护”优先，而其他非敏感信息则是更多地强调“利用”。

三、我国人脸识别问题的法律对策研究

对于公民人脸识别信息在内的个人信息保护，其方式历经历了从消极的被动防御式向积极主动的具体确权式的演进，随着人脸识别技术应用的铺开和社会管理、经济发展的需求不断攀升，关于人脸识别信息保护的要求也逐渐朝着精细化、系统化方向发展。由前文论述可知，明确人脸识别信息的权利属性是确定人脸识别信息权利行使规则和确立人脸识别信息保护方式的前提和基础。在我国目前司法实践中对于人脸识别问题的规范和救济的法理依据是人格请求权和侵权责任法，人格请求权法是权利法，侵权责任法是救济法，上文中人脸识别法律问题研究的理论基石揭示了有权利必有救济的原则，而且权利要走在救济之前，而权利法最核心和最重要的诉求就是辨析人脸识别信息的权利属性，以成文法的形式确立人脸识别信息是一项具体明确的数字人权，本文将从权利法和救济法两个方面探求人脸识别的法律问题对策。

（一）规范整合现有法条，细化处理规则

梳理我国关于人脸识别法律问题的规定，发现其散见于《中华人民共和国宪法》《中华人民共和国民法典》《中华人民共和国个人信息保护法》和其他行政规范性文件、行业标准之中，比较零

散。我国更加适宜采取“一元多样式”的立法模式，参考我国《中华人民共和国民法典》编纂成立过程，在现有的《中华人民共和国个人信息保护法》框架体系及个人信息处理原则之下规范整合、系统集成专门适用于人脸识别行业的法律法规，细化对于人脸识别信息的采集、使用、处理规则，开辟专章，强化保障，方便适用。完善散见于《中华人民共和国民法典》《中华人民共和国刑法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国消费者权益保护法》等配套法律中关于人脸识别信息保护的法规条文设置，在民法领域厘清人脸识别信息权利属性问题，确定“个人信息权”乃至“人脸识别信息权”的权利概念表述，肯定其数字人权的基本权利属性，同时区分人脸识别信息与隐私权、肖像权、身份权的关系问题。在刑法上具体明确侵犯公民人脸识别信息的定罪量刑标准，综合考量不同信息处理主体、信息侵害后果，违法情节轻重等因素，形成不同处罚程度的措施，从而形成全方位、跨领域、多层级的法律规制保护体系，真正做到全方位无死角地实施个人信息完整生命周期的动态保护。

明确哪些主体有资格进入人脸识别技术应用的市场。市场主体具有多样性，不同主体处理、控制人脸识别信息规模的大小、使用人脸识别技术品质的高低和自身对于人脸识别信息保护能力的高低各有不同，设置人脸识别技术准入门槛有利于整合资源，促成资源的集中利用，避免没有使用资质的主体进入市场导致人脸识别技术的滥用，给信息主体带来权利损害。在准入门槛的设置上，可以参考借鉴美国立法模式中的“场景理论”，场景理论（又称“情境脉络完整性”理论），即指个人信息原始收集时的具体语境应得到尊重，其后续传播及利用不得超出原初的情境脉络；不同人脸识别信息收集利用的具体语境和需求都不同，针对不同应用等级的场景设置不同准入门槛，例如在支付转账的应用场景中对于人脸识别技术精准性要求和对识别信息的保护需求都很高，因此需要对此类应用场景设置较高的准入门槛，对于技术使用主体的合法性、专业性问题进行规范

审查。对于社区门禁、打卡签到之类应用场景其技术使用主体没有很高专业性要求，也不需要后台处理识别到的人脸信息，这种情况下就需要让更多市场主体参与竞争；通过区分不同使用需求来保持应用场景的判断和处理目的的一致性。

设立公私一体适用的安全与责任底线。无论是谁使用人脸识别技术，人们都有权拒绝“刷脸”，在人们拒绝“刷脸”时，服务商应该及时提供可替代的验证方式，并且不能以信息主体拒绝“刷脸”为由增加其责任承担或者拒绝提供服务和产品。无论是谁使用人脸识别技术，都要建立技术使用影响评估制度，在收集人脸识别信息前进行必要性、合法性、合目的性的审查判断，对信息保护实行事前预判。无论是谁使用人脸识别技术，都要在使用主体内部设置安全责任人，懂得人脸识别技术从上游的算法开发、芯片制造到下游的场景应用全链条知识，更要熟悉与人脸识别技术相关的法律法规，并且要求安全责任人职位要求和其他职位权益不相冲突，安全责任人独立自主地开展主体内部人脸识别技术应用的安全规范巡查与指导，发现问题时及时充当“吹哨人”的角色。无论是谁使用人脸识别技术，都要建立数据库安全保障机制，定期检查，修复漏洞，实行数据库专人负责制度，建立数据库与监管机构的沟通机制，完善信息披露制度。

（二）强化政府对人脸识别技术使用的监管

根据《中华人民共和国个人信息保护法》第60条之规定^①，建议在网信办下设置专门管理人脸识别技术使用的领导小组，人脸识别技术监管领导小组中可以选择有智能设备制造应用专门知识，熟悉《中华人民共和国个人信息保护法》在内的有关人脸识别信息保护的法律法规知识，以及具有公共管理知识的人员组成，形成从中央到地多层次专门监管部门的组织架构，实施垂直领导，独立履行对人脸识别技术应用的监管。公民作为

侵犯人脸识别信息权益的直接受害者，因为其处于信息链条的末端，信息获取渠道有限、获取能力不足、可获得信息范围狭窄等多种因素导致其话语权有限，侵权责任举证困难，在人脸识别技术应用过程中的所有信息主体中始终处于相对被动和弱势的地位。政府搭建直接联系信息主体和监管机构的互动桥梁可以最大程度和最真实地获取公民在面对人脸识别技术应用时的诉求，更加敏锐地发现人脸识别技术应用过程中存在的缺陷，避免侵权程度更加严重的行为发生，同时在沟通投诉的过程中还可以利用监管机构的法定职责获取侵权证据，缓解信息主体维权难的困境。

（三）加大权利救济的司法保护力度

全球人脸识别市场渗透率快速攀升，数字经济与数字政府正进入增长快车道，我国人脸识别市场复合年增长率超过全球平均水平，成为全球第一大人脸识别应用国家，在此大背景大环境下，必须提升司法对于人脸识别新技术发展的应对能力。人脸识别行业参与主体大概可以分为五类：产品制造者（在此将软硬件的制造者统归为产品制造者）、产品销售者、数据保管者、数据处理者、数据应用者，要通过司法解释细化这五类主体在诉讼的法律地位、举证责任（对于人脸识别技术滥用的案件要严格贯彻举证责任倒置原则）、归责原则、赔偿标准（加大惩罚性处罚力度），明确裁判标准，提高司法审判的效率。发挥公益诉讼在人脸信息保护中的独特作用，赋予消费者权益保护协会等社会组织原告主体资格，对社会影响大的案件，由检察院直接提起人脸识别信息的公益诉讼，有效解决人脸识别技术侵权中产业链环节冗长、侵权主体复杂的难点，可以扩大权利人救济渠道，破解维权难的问题。

提升司法应对能力协调行政执法与司法救济关系，行政执法具有执行能力强、针对性强、确定性高等特点，要充分发挥各自职能作用和自身

^① 《中华人民共和国个人信息保护法》第60条：国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

优势，共同协作加强人脸识别行业下个人信息的保护工作。在“保护为主，利用为辅”中加强行政执法和司法保护工作的对接，建立健全行政管理执法与司法审判保障的协作联动机制。建立人脸识别大案要案通报机制，构建人脸识别保护信息共享机制。在网信办下设的人脸识别技术使用领导小组与各级法院之间共同构建畅通的联系渠道。公民个人信息保护领域内产生重大舆情影响或者较为严重危害后果的，尤其是影响国家和社会公共利益的大案要案及时通报各自获得的重要线索或案件处理进展情况，共同研究制定处置办法，加强行政执法和司法保护工作的对接，回应社会关切和舆情关注。

（四）加强行业自律，优化企业内部《企业隐私政策》设置

“知情—同意”规则是处理人脸识别信息在内的个人信息的核心规则，企业完成这一核心规则的具体表现形式通常是通过《企业隐私政策》完成的。在《企业隐私政策》中，人脸识别信息处理者会告知权利人被采集信息的种类、范围、使用方式及目的、信息存储位置及期限等信息。《企业隐私政策》是人脸识别技术使用主体为了履行其处理行为的合规性义务而制定的专业性条款。在实践中我们不难发现，此类《企业隐私政策》具有三大特点：隐蔽性、抽象性、冗长性。

对于企业的隐私政策进行考察，其设置方式通常分为两种：其一将隐私政策的链接放入网站或者搜索端入口，位置通常是在客户端的最末端，而且设置用户默认同意其政策，该类隐私政策通常适用于搜索引擎、内容网站；其二是通过弹窗提醒用户注意其隐私政策，并通过倒计时的方式强迫用户注意该提醒事项，该类方式的设置主要适用于各类应用程序，并且将用户阅读——同意其隐私政策作为继续接受服务或者产品的前置程序，以此证明其获得了用户的知情同意和自己履行了法律规定的说明义务。第一种隐私政策的提醒方式极具隐蔽性，除非用户主动寻找，否则不能轻易发现，对于用户知情权和同意权的保护形同虚设。第二种隐私政策的设置方式看似保证了用户的知情权和同意权，同时自己也履行了说明

披露的义务。但是此种设置流于形式，其隐私政策内容本身是复杂冗长的，动辄几十上百条注意事项仅在“长度”上就“劝退”了大量用户，且在专业表述上非常抽象，不具备人脸识别和个人信息保护专门知识的人难以理解其通告内容。《中华人民共和国个人信息保护法》第17条规定信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；个人行使本法规定权利的方式和程序等事项；企业的隐私政策在形式上显然并不具备简洁明了、通俗易懂的特点，业内企业的《隐私政策》与《中华人民共和国个人信息保护法》第17条的规定有明显差距。因此，建议行业协会或者政府监管部门出台企业《隐私政策》的格式文本，对各企业《隐私政策》的文本进行指引，尽量做到字体大、字数少、语义明，避免“知情—同意”规则流于形式。

参考文献：

- [1] 邢会强. 人脸识别的法律规制 [J]. 比较法研究, 2020, (5): 51-63.
- [2] 张文显. “数字人权”这个概念有着坚实的法理基础、现实需要和重大意义——“无数字不人权” [N]. 北京日报, 2019-09-02 (15).
- [3] 马长山. 强化“数字人权”的权益平衡 [N]. 广州日报, 2020-10-01 (8).
- [4] 张娟. 德国信息自决权与宪法人性尊严关系述评——德国个人信息保护的法律基础解读 [J]. 安徽农业大学学报 (社会科学版), 2013, (6): 45-49.
- [5] [美] 庞德. 通过法律的社会控制——法律的任务 [M]. 沈宗灵、董世忠, 译. 商务印书馆 1984: 81-82.

作者：马俊军，广东行政学院法学教研部副主任、教授、博士

王星宇，广东行政学院硕士研究生

责任编辑：熊哲文