身体指示符号传播与其法律风险

杨小凤

摘　要：身体指示符号的广泛运用，可能衍生出技术符号取代个人的文化风险，以及身体指示符号失序泄漏、深度伪造、技术异化等法律风险。这些不断扩张的风险主要来源于符号传播结构的异化，包括受众需求的扩张、传播模式的裂变、“把关人”的缺位等。对身体指示符号传播的法律风险进行规制，需要结合行政向度和刑事向度，明确身体指示符号处理环节的规范标准，强化主体监管和权利救济，并重塑其刑事规制。

关键词：身体指示符号，传播风险，法律规制

Communication of Body Indices and the Legal Risks

Yang Xiaofeng

Abstract: The extensive use of body indices may entail cultural risks, such as technical signs replacing individuals, and legal risks, such as the disorder leakage of body indicators, deep forgery, and technical alienation. These new risks arise from the alienation of the structure of sign communication, including the expansion of audience demand, the fission of transmission modes and the absence of gatekeepers. The regulation of the legal risks inherent in the communication of body indices requires practitioners to consider both the administrative and criminal dimensions, to clarify the normative standards for dealing with body indices, to strengthen subject supervision and right relief and to remodel the criminal regulation system.

Keywords: body indices, communication risk, legal regulation

DOI: 10. 13760/ b. cnki. sam. 202301017

皮尔斯曾根据符号所指称的对象将符号划分为图像符号、指示符号和象征符号三种类型，图像符号是通过模仿相似形象或相似图形，借用原已具有意义之事物来表达意义；指示符号是通过因果逻辑，在时间、空间和逻辑上构成指涉关系以表达意义；象征符号与其指示对象之间既无因果相承的关系，也无必然或内在的联系，其表征方式建立在社会约定或习惯的基础之上，是通过约定俗成来代表某一事物的符号（赵星植，2014，p. 56）。这三种符号指示性的强度有所不同，呈现出递减趋势。个人身份符号是能够关联个人身份的符号，该符号能够指向个人的鲜明特征，使人能够区别于他人。传统个人身份符号中的性别、出生日期、婚姻状态、住址、职位等都属于指示性符号，符号与个人可能构成 1 ∶ N 的关系，是一种弱标识符。传统个人身份符号中的姓名、身份证、护照、邮箱地址、银行账号等也属于指示性符号，但部分地增加了图像性符号，符号与个人可以构成 1 ∶ 1 的关系，标识符的指示性有所增强，成为强标识符。但这些全部个人符号组合或相加，也未必能绝对准确地识别某个具体个人，即使是身份证这种集图像性符号与指示性符号于一体的强标识符，也常常由于人的发展性而变得不够准确。数字时代的来临，增加了个人身份符号的类型，也增强了个人身份符号的指示性，如通过生物识别技术获得的面部、虹膜、基因、指纹、步态等身体指示符号，是对个人形象的数字化描摹，与识别对象绝对构成 1 ∶ 1 的关系，是一种强标识符。数字身份符号与传统身份符号共同形成了个人身份符号集群，并能够通过符号的共同运用与相互验证，准确识别具体个人。

身体指示符号作为一种“独属于公民自身的标识符”（蔡士林，2021），以其专属性、便捷性、安全性、精准性等特征，使相关技术在电子政务、教育服务、移动支付等各个领域备受青睐。然则风险与收益并存，身体指示符号在数字社会的广泛运用为公众带来便捷的同时，也带来多种风险，如技术符号取代个人的文化风险，身份符号泄露、伪造的法律风险、数字技术的异化风险等，种种风险都导致学界对身体指示符号运用的隐忧。因此，有必要对身体指示符号的传播及其法律风险进行类型化分析，探讨其传播风险的内在动因，以期形成有效的法律规制。

一、身体指示符号的界定与应用

（一）身体指示符号的概念界定

身体指示符号，主要是生物识别信息，2022 年 5 月 1 日实施的《信息安全技术生物特征识别信息保护基本要求》采取“定义 + 列举”的方式对生物特征识别信息进行了界定：“对自然人的物理、生物或行为特征进行技术处理得到的、能够单独或者与其他信息结合识别该自然人身份的个人信息。”该要求还以“注”的方式解释了其包括个人面部识别特征、虹膜、指纹、基因、声纹、步态、掌纹、耳廓、眼纹等，这些生物识别信息都是身体指示符号。身体指示符号具有区别于其他个人身份符号的独特性：人身唯一性、高度敏感性、侵害后果严重性、侵害方式隐蔽性等（蓝寿荣，罗静，2022），这种独特性决定了其一旦发生泄露或者滥用，将给个人带来难以弥补的永久性损害。我国 2021 年 11 月 1 日施行的《中华人民共和国个人信息保护法》将生物识别信息纳入了敏感个人信息的范畴，并明确了生物识别信息的收集、存储、使用、加工、传输、提供、公开、删除等处理行为应当遵循严格必要原则和知情同意原则。当前，对生物识别信息这种身体指示符号的处理主要基于两种目的：一种是公共目的，用于犯罪侦查、电子政务等；一种是非公共目的，用于电子支付、门禁系统、考勤管理等（林梓瀚，游祎，史渊，2022）。

（二）身体指示符号识别技术的主要应用场景

身体指示符号的识别技术，即生物识别技术，主要通过计算机与声学、光学、生物传感器等科学技术相结合，识别人体固有的生物特征和行为特征，如指纹、人脸、虹膜、声音、步态等，进行个人身份的识别与鉴定（吴彩霞，2018）。目前，广泛应用的生物识别技术主要是指纹识别技术和面部识别技术，包括人脸识别、虹膜识别和视网膜识别等技术，其在市场交易、社区管理、公司考勤等多个领域都具有重要价值。以高校为例，通过生物识别技术可以获取多种校园基础数据，不仅包括校园人员的基本信息，还包括校园实时数据，如视频、图像数据，时间序列监测数据等实时数据，辅助高校管理，主要应用场景如表 1 所示：

表 1　高校场域生物识别技术的应用场景

序号	场景	实例	信息主体	信息用途
1	校门口	人脸识别安防系统	教师、学生、学校其他工作人员、外来访问人员	入学身份核验、身份认证、出入校园记录、定位记录、校园人流量监测等
2	图书馆	图书馆门禁系统、自助借还书系统	教师、学生、图书馆管理人员	图书借阅、图书归还、图书分拣、图书馆人流量控制等
3	实验室	实验室门禁系统	教师、学生	考勤、考试身份验证等
4	教学楼	考场指纹校验、自助打印机	教师、学生	上课考勤、监测上课状态、远程考试、考试监管、教务管理、电子支付、定位记录等
5	宿舍	人脸识别智慧公寓系统	学生、宿舍管理人员	进出宿舍授权、通行信息记录、定位记录等
6	超市	自助收银、无人超市、自动售卖机	校内所有人员	身份认证、电子支付等
7	餐厅	校园卡充值、无人餐厅	教师、学生、其他学校工作人员	电子支付等
8	快递柜	人脸识别存取快递系统	校内所有人员	身份验证、快递存取等

二、身体指示符号的传播风险样态

身体指示符号作为公民专属的身份识别认证数据，蕴藏着巨大的社会价值和商业利益，借助数据挖掘、编辑、整合等技术，身体指示符号的非法传播衍生出大量下游黑灰产业，在民事、刑事、行政领域对公民个人权益、社会公共秩序、国家安全等造成侵害，其社会危害性已不容忽视。

（一）身体指示符号失序泄漏风险

身体指示符号识别技术不断地发展和更新迭代，在公私领域迅速走红并被广泛接受和应用。如警方利用面部数据、指纹、DNA 等身体指示符号进行数据库比对，帮助侦破线索、鉴定证据和指证犯罪嫌疑人等；政务机关、教育金融行业、私营企业利用指纹识别、人脸识别、声纹识别等进行身份认证、

电子支付、门禁安全、行程追踪等。与此同时，大量采集、存储和使用公民身体指示符号的行为，伴生了网络安全漏洞、技术缺陷和管理漏洞等引发的信息泄露风险。高校师生员工人员庞杂，所涉身体指示符号量大面广，信息泄露风险激增。

1. 因网络安全漏洞产生的信息泄露风险

技术的更新升级伴随着网络安全漏洞的增加，存储于网络数据库中的身体指示符号可能受到黑客攻击导致信息泄露风险。“2014 年，美国人事管理办公室（U. S. Office of Personnel Management）政府数据库遭到黑客攻击导致约2200 万人的个人数据被盗，其中包括大约560 万人的指纹；2016 年，菲律宾选举委员会被黑客攻击，菲律宾 5500 万选民的数据库被侵入，其中1580 万份指纹记录被盗取。”（张溪璠，王晓丽，2022）身体指示符号作为密切关联个人身份认证的要素信息，在各种利益需求的诱因下极易成为黑客的盗取目标。身体指示符号的处理一般依托于第三方平台公司，其系统的网络安全认证级别相较于政府网络安全等级更低，更易被黑客攻击导致信息泄露。

2. 因技术缺陷产生的信息泄露风险

新兴技术囿于其研发阶段的社会背景、功能需求、技术水平等，实践应用中往往存在一定的技术缺陷。身体指示符号的识别技术在应用中存在着安全性、准确性等方面的技术缺陷，由此产生的信息泄露风险在学术界和实务界已然受到关注。在高校，大量师生员工的身体指示符号经由第三方平台公司采集、存储并应用到校园门禁、校内信息管理系统中，如果该平台公司的数据库因系统软件缺陷、上市公司信息披露等原因被公开，将导致其所获取的身体指示符号暴露在互联网上。2019 年，荷兰安全研究员 Victor Gevers 在社交网站上表示，我国深圳市某科技有限公司的数据库暴露在网上且无密码保护，超过 250 万人的数据可被获取，其中包括身份证信息，人脸识别图像及捕捉地点等，共计 680 万条记录泄露。（张溪璠，王晓丽，2022）

3. 因信息管理漏洞产生的泄露风险

身体指示符号的处理包括符号的采集、存储、应用、加工、流转等环节，各环节管理失序都会引起信息泄露风险。高校在校园进出口、教室、图书馆、食堂等公共场所安装的用以统计人流量的摄像装置，以及用于安全防控的校园天网监控设备等，都在无感知的情况下获取了所处场域中人们的人脸、体态信息；存储环节管理漏洞造成身体指示符号被管理主体因故意或过失泄密，或是被他人利用非法手段获取导致泄露；使用环节中某些系统应用或小程序

通过使用时的捆绑授权，访问设备传感器或身体指示符号数据库获取数据信息，导致符号泄露。浙江大学研究人员发现，利用其特制的软件可以通过收集手机加速度计的震动频率还原扬声器播放的语音，从而实现窃听（宋祎晨，2022）。

（二）身体指示符号深度伪造风险

随着网络信息技术的优化升级及大数据、人工智能算法的不断发展，不法分子可能利用新兴技术对图像、声纹等身体指示符号进行活化、合成、动态融合、编辑改造等，以实施下游犯罪行为。以“人脸识别”+“刑事案件”作为关键词在中国裁判文书网中检索可以看到，利用新兴技术将目标人物照片进行活化处理，制作人脸识别动态视频图，骗取网络购物平台、金融平台、移动支付等系统认证以实施盗窃、诈骗等犯罪已不是个案。如，湖北省巴东县人民法院（2021）鄂2823刑初48号刑事判决书中，被告人利用被害人生物识别照片制作人脸识别动态视频图，解除被害人微信支付限制从而盗取其微信绑定的银行卡内资金，实施盗窃行为（王文娟，2022）；广东省广州市海珠区人民法院（2021）粤0105刑初292号刑事判决书中，被告人购买京东用户的人脸照片和账户信息，将照片进行技术处理制作成人脸动图，登录该账户后利用人脸动图通过人脸识别认证，修改原用户的电话、地址、密码等信息后以其名义申请开通白条支付功能，利用白条支付购买商品并倒卖获利（王文娟，2022）。利用身体指示符号实施犯罪行为，已从初始的直接利用获取的身体指示符号进行物理识别，向利用新兴技术对身体指示原始符号进行动态融合、编辑改造等深度伪造的技术性识别转化。

（三）身体指示符号技术异化风险

信息网络社会的运转以个人信息为基础，这促使个人身体指示符号在数字社会被广泛运用，随着数据挖掘技术的发展，这些信息“被转化成0和1的数字编码，成为可以追踪、检索、汇编、计量和运算的信息，个人的行为偏好、价值观，就可以被清晰刻画出来”（罗琳，2020）。“个人画像”结合挖掘出来的财产信息、行动轨迹等社会性信息，能够“勾勒一个人的所有社会性要素，形成天然的‘记事本’”（蔡士林，2021），再利用数字挖掘技术进行反向挖掘，就能形成完整的个人追踪链条，异化为更恶劣的侵害他人人身权益、财产权益的行为。身体指示符号的技术异化风险可能体现在商业化利用（如售楼部利用人脸识别对新老来访客户给予不同优惠政策），或其他

黑灰产业及下游犯罪，通过画像对个人生活轨迹、经济状况、习惯偏好、政治立场、心理状态等进行描绘，从而侵犯个人隐私。如高校通常出于门禁识别或是日常管理之目的，抑或是为了测评教师教学质量、监管学生课堂学习专注程度，采集身体指示符号，并进一步进行信息处理、分析，描绘出个人或群体画像。相较其他个人信息而言，这种通过身体指示符号做描摹的画像更加直观精准，也更易产生无监管、无限制的特殊风险，被采集者将承受来自信息处理主体的凝视，承担身体指示符号的技术异化风险。

三、动因：价值需求与传播方式的风险扩张

从身体现象所获得的身体指示符号通常具有两个辨别性作用，即基础符号学功能的作用和生成行程的作用（丰塔尼耶，2021，p. 3）。通过对生物特征和行程的描述，可以生成用户画像，从而反向挖掘和塑造用户，甚至洞悉用户那些私密的、情绪性的现实需求和潜在需求。身体指示符号这种潜藏的功能使其具备更大的流通价值，也导致更大的传播风险。这种传播风险一方面来源于身体指示符号本身，另一方面来源于信息传播结构的异化。身体指示符号经历了信息采集、解码、比对和匹配等数字化处理过程，可以保证符号的精准性和唯一性，也导致符号遭遇侵害的程度加重并且不可消除。传播结构的异化则导致符号传播风险的进一步扩张，具体表现为受众需求的扩张、传播模式的裂变以及“把关人”的缺位。

（一）受众需求的扩张

伴随信息技术和全球化的加速发展，受众对身体指示符号的需求呈现出扩大化增长的趋势。这种需求不仅在于通过直接出售、加工制作身体指示符号来获取经济利益，还在于通过分析、研判身体指示符号来掌握公、私主体的运转状况等，再对其进行非法传播，从而谋求政治利益。第一种需求在电信网络诈骗类案件中得到了充分体现。以高校为例，以三种诈骗类案件为甚。第一，虚假贷款类诈骗，如“张某等诈骗案”，诈骗行为人在取得学生身体指示符号，并关联身份证、银行卡、电话号码等个人信息后，有针对性地诱导学生利用“名校贷”“优分期”等贷款平台进行贷款，并使用其身份信息造成贷款信息被屏蔽、不用还款的假象，利用大学生社会阅历浅、家庭具有实际困难急需用钱等特点，骗取贷款超 125 万元［吉林省长春市中级人民法院（2020）吉 01 刑终 390 号二审刑事裁定书］。第二，冒充老师、熟人类诈

骗，诈骗行为人可能通过对学生身体指示符号的获取与比对，取得高校办理助学贷款的学生名单，直接冒充学校教务处、财务处工作人员，要求学生向指定账户缴纳学费；也可能利用师生关系等校园人际关系进行诈骗。在“梁某诈骗案”中，梁某作为武汉某健康管理有限公司创业街分公司的总经理，唆使公司销售人员冒充教授的学生、医生助理，使用电话、微信等问诊并夸大病情，以诱骗被害人购买其公司产品，骗取他人财物［湖北省汉江中级人民法院（2021）鄂 96 刑终 53 号二审刑事裁定书］。第三，网络游戏产品虚假交易类诈骗，如“王某诈骗案”，诈骗行为人获取了某高校学生李某的身份信息并与其取得了联系，通过伪造自己的身份信息为大四女生，取得李某信任，再以谈恋爱为由，骗取李某游戏充值超 13 万元［福建省三明市中级人民法院（2019）闽 04 刑终 180 号二审刑事判决书］。这些涉大学生电信网络诈骗类案件都是在诈骗行为人掌握高校人员身份信息的基础上实施的。

第二种需求往往更为隐蔽，基于这种需求的身体指示符号传播后果也更为严重，甚至危害国家安全。例如，高校场域的身体指示符号常常能够与专业领域发展水平、科研状况、教育教学水平、保密性技术等发生关联，由此，受众对身体指示符号的获取和进一步传播，对身体指示符号的分析与加工，将可能被用作舆论战的武器，以制造社会混乱。某高校曾于 2022 年 6 月份发布声明，称有来自境外的黑客组织和不法分子向学校师生发送包含木马程序的钓鱼软件，企图盗取师生邮件数据和个人信息。可见，受众对高校场域身体指示符号的需求正在不断扩张，不断扩张的需求将带来一系列针对高校身体指示符号的挖掘、盗取、加工和非法传播行为，导致符号的传播风险扩大化。

（二）传播模式的裂变

伊尼斯（2018，p. 17）曾指出，“传播媒介的性质往往在文明中产生一种偏向，这种偏向或有利于时间观念，或有利于空间观念”。网络文明时期的数字传播媒介则同时在时间和空间上拓展了传播行为，使得作为传播内容的信息既可以不经历时间上的遗忘，又可以不受地域空间上的限制。数字传播媒介还增强了与信息的黏合性，成为一种符号表意系统，统一了传播技术物质载体与传播内容。传播媒介形态的变革直接导致信息传播模式发生了裂变，主要表现为：第一，传播速度的超速化，信息的最小单位由原子变成了无色、无重、能以光速传播的比特，光纤通信线路又为信息传播提供了超大容量的传输通道，并且每秒可达 30 万公里，信息瞬间可以到达世界的任何地

方；第二，传受关系的交互化，传播者和受众处于双向互动中，并能够适时地根据对方的反馈调整自己的信息传播行为，这意味着受众也可能成为新的传播者，信息传播可以采取一对一、一对多、多对一甚至多对多等各种形式；第三，传受范围的全球化，数字信息常常突破“领域疆界”，在虚拟空间无限传播，并且不可撤回。就高校场域身体指示符号的传播而言，传播者在获取高校人员的身体指示符号之后，首先可能将其整理为文字、图像、视频等不同的符号进行储存、售卖；其次可能根据不同的传播目的，对数据信息进行清洗、加工、编辑、打包等，将编码后的信息重新进行组合再解码，并有针对性地传递给不同的受众。受众再根据自身需求对信息进行解码，并反馈给传播者，也可能拒绝接收该信息，但各种反应都能让传播者对其传播行为进行调整，或继续，或矫正，或改变。这一循环传播的过程可以在很短的时间内完成，并裂变为无数的循环传播过程，且由于身体指示符号的高度人身附着性，这种传播将导致信息永久性泄露的严重后果。

（三）“把关人”的缺位

美国社会学家卢因曾提出“信息的传播网络中布满了把关人”（张国良，2009，p. 156），传播学者怀特又将“把关人”理论引入新闻传播领域，认为记者、编辑、编导等信息传播职业者应当对要传递给受众的信息进行把关。伴随信息传播模式从一对多到多对多的裂变，掌握信息资源、参与信息传播环节的任一节点都成了信息传播的“把关人”，导致“把关人”泛化，以及把关功能的实质性缺失。以高校场域为例，在身体指示符号的传播扩散过程中，高校合作的信息采集平台便是信息传播的第一个“把关人”。但实际上，信息采集平台权利义务不明确的立法状况常常导致其“把关人”角色的缺位，许多信息采集平台及其工作人员并没有意识到自己对信息资源的必要管理责任，如为多所高校提供生物识别技术的某科技有限公司曾 58 次被列为失信被执行人（据“天眼查”数据）；“林某侵犯公民个人信息案”中，林某作为温州市某数码科技有限公司的客服人员，在履行职责过程中将获得的学生信息出售给他人用以牟利［浙江省温州市中级人民法院（2017）浙 03 刑终 1560 号刑事裁定书］。高校信息管理部门作为信息传播的主体之一，也是重要的把关人，但为了获得一定的经济利益，也不乏高校信息管理人员贩卖高校人员信息的情形。2021 年开始施行的《天津市社会信用条例》规定了“企业事业单位可以依法记录自身业务活动中产生的市场信用信息；市场信用信息提供单位采集自然人信息的，应当经本人同意并约定用途；市场信用

信息提供单位不得采集自然人的宗教信仰、血型、疾病和病史、生物识别信息以及法律、行政法规规定禁止采集的其他个人信息”，企业事业单位作为信息传播“把关人”的角色已经逐渐失去民众信任。各种数字平台作为信息传播的载体同样也是重要的“把关人”，但其本身就已经在信息垄断的运作机制下饱受流量至上、资本导向、算法歧视等诟病（姬德强，李蕾，2022），更别提为个人信息传播把关了。受众也常常成为新的传播者，并且可能仅仅因为猎奇心理就将获得的生物识别信息进一步传播，更不用说还可能获得经济或政治上的收益，其“把关人”角色几乎被消解。可以看到，在高校身体指示符号传播过程中的各个节点，传播者都可能收获利益，这就鼓励其更大可能地背叛信息“把关人”的身份，转向对身体指示符号的深度挖掘，促进身体指示符号的加速流通，从而扩大身体指示符号的传播风险。

四、法律规制：行政向度与刑事向度的多元结合

身体指示符号作为数字时代个人身份识别和认证的重要基础资源，密切关系着信息主体的人身和财产权益。然则身体指示符号在网络空间的传播呈现快速蔓延、急剧裂变的扩张风险，一些非法传播行为又具有隐蔽性与潜在性，故而对传播风险的法律规制也需同步紧跟新生事物和新兴技术的发展。“由算法支撑的智能社会依然是‘人的’社会而不是‘物的’社会。具体而言，构建以人为本的智能社会法律秩序，就是以人的权利为本，把权利保护和人权保障作为智能社会法律秩序的核心要义。”（张文显，2020）公权力主体基于日常管理对身体指示符号进行处理的行为，兼具行政行为与民事行为的双重属性，其行为过程所产生的个人身体指示符号失序泄露、深度伪造、技术异化等传播风险，当秉持“以人为本”的权利保障核心要义，行政向度与刑事向度相结合予以法律规制。

（一）明确身体指示符号处理环节的行为规范标准

身体指示符号的采集、存储、使用、传输、加工、公开和删除等处理环节，均应有明确的行为规范标准，并严格遵循必要性和充分性原则。必要性层面，即对身体指示符号的处理行为划分权限等级。对取得信息主体同意的处理行为，出于身份识别认证的基础目的和用途，作为一般风险等级允许进行处理，但应同时提供替代性方案以防止公权力主体利用其优势地位强迫被管理者同意；对于滥用处理权、严重侵犯个人隐私的行为，作为高风险等级

予以绝对禁止，如出于营利性目的对身体指示符号的加工或对个人画像的深度挖掘等。此外，面对国家公共安全、刑事犯罪预防与侦查等特殊情形，应当允许公权力主体在紧急情况下的非必要处理行为，如为保障公共安全时出于追踪与识别目的，配合其他公权力机关的紧急处理行为，无须事先取得信息主体的同意，但需确保在必要的限度内，事后及时删除以防止衍生信息泄露风险。

充分性层面，即根据《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第十三、十四条规定，一般情况下个人信息处理应当取得个人同意，并应由个人在“充分知情”的前提下自愿、明确作出。此处“充分知情”应当具化，在对身体指示符号进行采集时应当充分告知采集的目的、类别、范围、使用用途、存储方式及时间、信息主体同意处理后所需面临的风险等。在公共场所基于安防等目的进行身体指示符号采集的行为，当以醒目标识提示进入信息采集区域，并以适当方式告知信息主体权利和风险。在存储、使用、传输、加工等环节，应当充分告知身体指示符号的存储介质及数据平台，确保不被用于营利性的加工、挖掘，并根据《个人信息保护法》第四十七条规定，在信息主体撤回同意或离开相应场所的情形下，应赋予其充分的“被遗忘权”。

（二）强化身体指示符号处理的主体监管和权利救济

行政向度应强化行政部门对身体指示符号处理过程中的主体监管职责，对侵害或可能侵害信息主体权益的行为予以规制，畅通权利救济途径。

一方面，各级行政部门应当承担身体指示符号处理行为的主体监督职责。可以聘请法律、信息技术等相关专家与教育行政管理专家共同组建专门机构，针对各单位对身体指示符号的处理行为进行评估、管理和监督，以加强个人信息的保护力度。应当明确，公权力主体在必要性限度内处理身体指示符号时，需提前向主管行政部门专门机构报备，全面说明其处理行为的目的、方式、所采用的设备技术标准等，由专门机构进行必要性和风险评估，并在必要时组织听证。

另一方面，应当畅通身体指示符号的权利救济途径。我国遵循大陆法系“有侵害必有救济”的原则，对权利侵害的救济是维护社会秩序的根本保证。当公权力主体对身体指示符号的处理行为存在侵害权益的风险时，信息主体有权依法提起权利救济，作为监管主体的行政部门应当畅通权利救济途径，保障信息主体的信息处置权益及针对侵权行为获得救济的权利。申言之，当

信息主体对其身体指示符号的处理行为存在异议时，有权向作出处理行为的主管部门提出异议，并向作为监管责任主体的行政部门提起行政复议。主管行政部门作为监管主体，应当作为行政复议机关对公权力主体的相关身体指示符号处理行为分别从形式层面和实质层面进行合法性审查。此外，信息主体也可选择司法救济途径，对公权力主体作为行政主体实施的对其身体指示符号的处理行为提起行政诉讼，亦可对其遭受的权益侵害提起民事诉讼。

（三）刑事向度重塑身体指示符号非法传播的法律规制

不法分子非法传播身体指示符号衍生出大量下游黑灰产业及犯罪行为，当前刑事立法的滞后性尚不能对其形成有效的法律规制。从刑事向度重塑身体指示符号非法传播的法律规制，可从以下几个方面进行着手：

1．将生物识别信息作为敏感个人信息纳入刑法规制

《中华人民共和国刑法》第二百五十三条“侵犯公民个人信息罪”对“向他人出售或者提供公民个人信息”“窃取或者以其他方法非法获取公民个人信息”作出了规定，《最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》对该条的“公民个人信息”进行了界定：“是指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身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。”可以看出，身体指示符号作为专属公民的特殊的、敏感的个人信息符号，并未纳入相应规制中。而事实上，通过非法传播的身体指示符号可以完整勾勒出公民个人画像，包括其财产状况、行踪轨迹等个人信息。身体指示符号扩张化的传播风险异化为下游犯罪，而上述刑事法律规范尚未将身体指示符号的非法传播行为与其他侵害公民个人信息的行为等同视之，利用非法传播的身体指示符号加以处理、深度伪造、挖掘分析个人关联信息并借此实施犯罪行为理应纳入刑事法律规制。

2．重构身体指示符号非法传播的入罪标准

犯罪构成要件的主观方面和客观方面是认定一个行为罪与非罪的重要标准和评价要素。信息网络犯罪具有跨地域、跨时空的特点，不再囿于传统犯罪构成理论的“一人对一人”“一人对少数人”。利用非法传播的身体指示符号为实施下游黑灰产业犯罪提供的技术帮助，实际可能是该类信息网络犯罪的诱发性因素或关键性决定性条件，具有明显的犯罪产业链行为特征，其社

会危害性不容忽视。对于身体指示符号非法传播行为若仍以传统犯罪构成要件主观方面的“知道或应当知道”为认定标准，已不符合当代网络数字社会背景下的风险预防理念和原则，不利于全面有效遏制利用非法传播的身体指示符号实施下游犯罪的行为，我国刑法应当对此作出适应性调整。

对身体指示符号非法传播行为犯罪构成客观方面的认定标准亦是如此。《最高人民法院 最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第一条规定，“获取支付结算、证券交易、期货交易等网络金融服务的身份认证信息十组以上的；获取其他身份认证信息五百组以上的”才属于《刑法》第二百八十五条第二款非法获取计算机信息系统数据罪规定的“情节严重”，构成犯罪。然而当下随着物联网、人工智能技术在人们社会生产生活中的广泛普及应用，很多即时通信类、社交类、旅游类、购物类、娱乐类小程序都已呈现功能的重叠交叉，诸如微信、去哪儿、美团、京东、抖音等，都已开设了网络金融服务功能。上述司法解释针对网络金融服务平台身份认证信息作了特殊保护，但对同样具备网络金融服务功能的其他网络平台的身份认证信息则只能按照第二项规定的“五百组以上”来作定罪依据，这与信息时代各类生活 App 普及化推广和交互发展的现实样态及未来趋势相冲突。故而，应当充分认识到身体指示符号在个人身份识别认证中的特殊性，不以是否属于网络金融服务的身份认证信息为区分，对非法获取身体指示符号十组以上的，即可认定为非法获取计算机信息系统数据罪。

3．增设“滥用生物识别信息罪”

对于身体指示符号非法传播行为的刑事规制，应当引入风险预防理论及原则，针对身体指示符号传播风险的弥散性特征和技术异化风险，增设“滥用生物识别信息罪”。预防刑法当以法益侵害为前提，将“危险行为”或是可能转化为“危险行为”的“风险行为”纳入犯罪行为认定中（蔡士林，2021）。具体到身体指示符号非法传播场景下，对“危险”的衡量标准除了充分观照“质”和“量”的要求，还应考虑到数字社会个人身份信息的特殊性。即使行为人滥用身体指示符号对信息主体个人的法益侵害可能较小，但信息网络使用者众多且数据量庞大，也可以认为其滥用行为造成的整体损害重大。故此，以盗取、截获、深度伪造等非法手段获取身体指示符号供自己使用或提供给他人使用的行为，应当纳入滥用生物识别信息罪的认定范围予以法律规制。

结 语

身体指示符号的应用呈现出多样化、扩张性的传播风险，其法律规制是广泛性、时代性的问题。基于公权力、私权利之间特殊的法律关系，对身体指示符号传播风险的法律规制应当依据双方特殊主体地位，兼顾行政向度和刑事向度。在此意义上，我国当前在行政监管、刑事立法和司法实践层面都尚待进一步推进，尤其要拓宽思路，引入风险防范理论，在技术赋能管理质效提升的基础上，不断完善身体指示符号法律保护的理论架构。

引用文献：

蔡士林（2021）. 生物信息识别：原理、风险与协同治理模式. 中国矿业大学学报（社会科学版），1－14.

丰塔尼耶，雅克（2021）. 身体与意义（怀宇，译）. 天津：南开大学出版社.

姬德强，李蕾（2022）. 信息疫情与数字平台语境下公共信息传播的新把关人建设——以新型主流媒体为例. 中国编辑，6，33－37.

蓝寿荣，罗静（2022）. 商业活动中个人身体指示符号的属性与保护. 陕西师范大学学报（哲学社会科学版），2，73－86.

林梓瀚，游祎，史渊（2022）. 基于生物识别技术的全球个人信息安全治理研究. 世界科技研究于发展，1－18.

罗琳（2020）. 信息技术的负效应及其消解对策研究. 科学技术哲学研究，4，124－128.

宋祎晨（2022）. 身体指示符号的安全风险及法律规制. 河南牧业经济学院学报，194，56－61.

王文娟（2022）. 身体指示符号传播风险的刑事规制向度——基于525份刑事裁判文书的内容分析. 新闻与传播研究，7，75－88.

吴彩霞（2018）. 金融领域生物识别技术应用探析. 金融理论与实践，12，61－66.

伊尼斯，哈罗德（2018）. 传播的偏向（何道宽，译）. 北京：中国传媒大学出版社.

张国良（2009）. 传播学原理. 上海：复旦大学出版社.

张文显（2020）. 构建智能社会的法律秩序. 东方法学，5，4－19.

张溪璠，王晓丽（2022）. 人脸识别技术与应用的风险及治理研究. 科学学研究，1－20.

赵星植（2014）. 论社交媒体的符号构成及其功能. 编辑之友，12，56－60.

作者简介：

杨小凤，博士研究生，四川大学法学院讲师，研究方向为法学、思想政治教育。

Author:

Yang Xiaofeng, Ph. D. candidate, lecturer of law college of Sichuan University. Her research interests include law and ideological political education.

Email: yangxiaofeng@ scu. edu. cn