北京理工大学学报社会科学版
Journal of Beijing Institute of Technology(Social Science Edition)

论个人生物识别信息保护的立法路径

杨铜铜

On Legislative Path of Personal Biometric Information Protection

YANG Tongtong

在线阅读 View online: https://doi.org/10.15918/j.jbitss1009-3370.2022.2469

您可能感兴趣的其他文章

Articles you may be interested in

论个人信用信息公开的私法规制

On the Private Law Regulation of Personal Credit Information Disclosure

北京理工大学学报（社会科学版）. 2020, 22(3): 144 https://doi.org/10.15918/j.jbitss1009-3370.2020.9462

个人信息权法益确证及其场景化实践规则

Confirmation of Legal Interests of Personal Information Right and Situational Practice Rules

北京理工大学学报（社会科学版）. 2021, 23(5): 169 https://doi.org/10.15918/j.jbitss1009-3370.2021.1489

税务信息管理权与保护权的冲突与平衡

The Conflict and Balance of Information Management Power of Tax and the Information Protection Right

北京理工大学学报（社会科学版）. 2018(4): 151 https://doi.org/10.15918/j.jbitss1009-3370.2018.2845

论数据保护法的域外效力

The Extraterritoriality of Data Protection Law

北京理工大学学报（社会科学版）. 2021, 23(5): 161 https://doi.org/10.15918/j.jbitss1009-3370.2021.9938

中国电力消费周期的路径演化识别——基于Markov区制转移模型

Path Evolution Identification of China's Electricity Consumption Cycle based on Markov-switching Model

北京理工大学学报（社会科学版）. 2018(5): 17 https://doi.org/10.15918/j.jbitss1009-3370.2018.3030

基于SAO语义分析的潜在技术合作伙伴识别

Potential Technology Partner Identification by Using SAO Semantic Analysis

北京理工大学学报（社会科学版）. 2017(4): 91 https://doi.org/10.15918/j.jbitss1009-3370.2017.6206

关注微信公众号，获得更多资讯信息

DOI: 10.15918/j.jbitss1009-3370.2022.2469

论个人生物识别信息保护的立法路径

杨铜铜

（华东政法大学　政治学与公共管理学院，上海 201620）

摘　要：个人生物识别信息具有高度的专属性与私密性，与个人隐秘的生理特征直接相关，彰显个人身份特质，因而需要特别保护。通过立法路径提供个人生物识别信息使用与保护的框架，是规制个人生物识别信息滥用、实现个人生物识别信息保护的关键。在立法模式上，结合中国的立法传统、现实需求以及法制发展现状，应当采用渐进式的综合立法模式。在立法理念上，为实现多元主体之间的利益平衡，在充分保护的基础上有限地利用个人生物识别信息，是立法应当秉持的核心理念。在立法内容上，需要界定个人生物识别信息的法律概念、类别、属性，确立特殊保护原则，明确信息主体的权利，细化信息处理者的行为规范，以及设置多元化保护机制等。

关键词：个人生物识别信息；生物识别技术；综合立法模式；保护机制

中图分类号：DF523.9; DF529　　**文献标志码：**A　　**文章编号：**1009-3307(2021)06–0140–11

伴随着人工智能的快速发展，以“人脸识别”“指纹验证”“声音解锁”“虹膜识别”为代表的生物识别技术蓬勃兴起，在刑侦、治安、金融、医疗、交通、学校、支付、社区、企业等场景大范围使用，其对网络科技、大数据，乃至数字经济的发展发挥着至关重要的作用，已经成为国民经济的重要组成部分。这种通过生物识别技术对自然人的物理、生理或行为特征进行特殊技术处理而得到的信息即为“个人生物识别信息”，比如指纹、虹膜、脸部特征、声音、步态、笔迹等。由于个人生物识别信息具有唯一性、不可更改性，一经泄露将永远不可索回，因而可能引发侵犯隐私、违法犯罪、种族歧视、危害国家安全等风险，亟待警觉。比如近来广受热议的 Facebook 因人脸识别技术引发集体诉讼赔偿 5.5 亿美元、郭某诉杭州市动物园强制收集人脸信息案、17 万人脸数据遭公开销售、“ZAO”网红换脸软件、“剪刀手”拍照泄露指纹信息等。因此，面对生物识别技术带来的挑战，如何保护个人生物识别信息已经成为全球关注的核心议题。

在保护个人生物识别信息的多种机制中，通过立法路径提供个人生物识别信息使用与保护的框架，是规制个人生物识别信息滥用，实现个人生物识别信息保护的前提与关键。“从法律原理上来说，一般性规则能够减少信息搜寻成本与认知成本，有利于个人尽快认知和利用法律进行维权，有利于数据收集者与处理者尽快地进行合规操作，也有利于执法主体尽快进行执法。”[1] 当前许多国家和地区已经开始制定相关立法①，然而中国尚未形成体系化的立法保护框架，致使个人生物识别信息的保护存在重大缺漏。

一、中国个人生物识别信息保护的立法现状与问题

（一）个人生物识别信息保护的立法现状

中国有关个人生物识别信息保护的规范相对较少，主要散见于《身份证法》《反恐怖主义法》《网络安全法》《出境入境管理法》《刑法》《刑事诉讼法》《民法典》《消费者权益保护法》等法律，《外

收稿日期：2020-07-13

基金项目：上海哲社青年项目“个人生物识别信息的多元保护机制研究”（2020EFX004）；第 66 批中国博士后科学基金资助项目“法律解释规则的实践运用及其效果提升”（2019M661446）

作者简介：杨铜铜（1990—），男，法学博士，特聘副研究员，E-mail：yangtongtongmy@sina.com

① 比如美国伊利诺伊州制定了《生物识别信息隐私法案》；马塞诸塞州萨摩维尔市制定了《暂停面部识别或其他远程生物识别监控系统的法案》；欧盟最新颁布的《一般数据保护条例》(General Data Protection Regulation, GDPR) 将“个人生物识别信息”作为敏感个人信息的一种，着重予以保护；印度《2019 年个人数据保护法》（Personal Data Protection Bill, PDPB 2019）对“生物特征数据”保护亦作出特别规定。

国人入境管理条例》《保安服务管理条例》《征信业管理条例》等行政法规，以及一些效力较低的规章、规范性文件之中[①]。多涉及个人生物识别信息保护原则、使用规则、监管机构与职能、法律责任、权利救济等内容。

一是有关公安机关在侦查案件、打击犯罪和治安管理等活动中收集、管理与保护“指纹信息”的相关规定。根据《居民身份证法》《反恐怖主义法》《刑事诉讼法》《外国人入境管理条例》《公安机关办理行政案件管理规定》等法律规定，公安机关可以在身份证管理、出入境管理、办理行政案件、刑事案件中利用指纹等个人生物识别信息，并负有保密义务，如果泄露将承担行政处分、追究刑事责任。

二是通过明确各方信息主体的权利义务、法律责任对个人生物识别信息进行保护。比如在民事领域，《民法典》第 111 条规定了个人信息保护的基本行为规范，信息处理者确保信息安全等基本义务。《民法典》人格权编更是着重从“隐私权”保护的维度，对个人信息处理的原则、个人信息主体的权利、信息处理者的安全义务和保密义务等进行了详细的规定。同时《消费者权益保护法》第 29 条规定了经营者收集、使用消费者个人信息的规则以及经营者的保护义务。在刑事领域，通过规定侵犯公民个人信息的刑事责任间接地对个人生物识别信息进行保护，较为典型的是《刑法》第 253 条之一侵犯公民个人信息罪的规定。

三是规定个人生物识别信息的收集、处理、使用等不同环节的规则。相对聚焦在信息管理领域，例如《网络安全法》规定了网络运行者收集、使用个人信息的规则，网络运行者、网络监管人员以及其他组织和个人不得非法获取、出售、向他人提供个人信息等义务，其中的“个人信息”便包括“个人生物识别信息”。与此同时，中国立法也已意识到“个人生物识别信息”有别于一般个人信息，对个人生物识别信息进行了特别规定，比如《互联网个人信息安全保护指南》在“个人信息安全保护的管理机制、安全技术措施和业务流程”中，对个人生物识别信息的“收集”“公开披露”环节作出了特殊规定。需要注意的是，2020 年 3 月 6 日修订的《信息安全技术个人信息安全规范》对个人生物识别信息的收集与存储进行了专门规定，明确规定“收集人脸信息需单独告知，不得存储原始图像”。此外，一些行业协会的自律规范也对其进行了规定，比如中国支付清算协会发布的《人脸识别线下支付行业自律公约（试行）》，从安全管理、终端管理、风险管理、用户权益保护等方面对人脸识别线下支付进行了规定。

（二）个人生物识别信息保护的立法问题

中国对个人生物识别信息的保护已经有部分规定，但立法仍较为分散，无法满足个人生物识别信息保护的需要。

第一，独特属性未突出，针对性规定缺失。现有立法未突出个人生物识别信息的独特属性，多将“个人生物识别信息”视为“个人信息”的一种类型加以规范，比如上述《民法典》《网络安全法》《消费者权益保护法》的规定。即使少数法律规范意识到个人生物识别信息属于“敏感个人信息”，但也只是在“收集”“披露”等环节简单地进行规定，缺乏系统的针对性规定，比如《信息安全技术个人信息安全规范》。

第二，立法理念不明确，表达不清晰。立法理念本质上是对不同利益的衡量，引导着立法的路径与价值选择。当前国内外均对收集、处理与利用个人生物识别信息的安全性、合法性存在质疑，但中国各行业却积极鼓励开发利用个人生物识别信息，甚至有愈演愈烈之势，因而如何确立立法理念、衡量个人生物识别信息保护与利用之间的利害，是个人生物识别信息保护立法的重点。当下中国立法理念并不明确，比如《网络安全法》《民法典》等仅将“个人生物识别信息”作为“个人信息”的一种类型进行规范，《互联网个人信息安全保护指南》《信息安全技术个人信息安全规范》也只是对个人生物识别信息收集、存储、公开披露环节作出特别规定，均没有明确地表明立法理念。

第三，立法碎片化，法律位阶较低。当前有关个人生物识别信息的技术标准与保护机制缺乏统一的规定，系统的专门立法付之阙如。同时，个人生物识别信息保护规范的法律位阶较低，大多为规章、规范性文件，甚至是行业协会与企业制定的行业规则。尽管当下对个人生物识别信息的权利属性存在隐私

① 比较具有代表性的规章、规范性文件为《公安机关办理行政案件程序规定》《普通护照和出入境通行证签发管理办法》《互联网个人信息安全保护指南》《信息安全技术个人信息安全规范》等。

权、新型人格权、财产权之争，但是毋庸置疑均属于公民的基本权利，因此应由效力等级较高的立法规范进行规定。

第四，具体内容不明确，尚未形成体系化的保护。当前有关个人生物识别信息保护的规定多以原则性、概括性条款为主，可操作性不强。比如《保安服务管理条例》仅规定了公安机关“应当保密”，但是对于如何保密等问题没有进行规定。同时，从内容上看集中于责任条款设置，并散见于不同的规范类型中，比如刑事领域规定侵犯公民个人信息罪；而关于个人生物识别信息的法律属性、保护的特有法律原则、权利义务关系、监管机构与职责等均没有规定，而上述内容正是个人生物识别信息保护的核心。

第五，保护对象比较狭窄，适用主体较为单一。由于受制于信息技术发展，当前立法多侧重于“指纹信息”的保护，对面部信息、虹膜信息、耳廓信息、静脉信息、声音信息等其他个人生物识别信息的保护规定较少。近来伴随着“人脸识别技术”的快速发展与广泛运用，才开始对“人脸识别信息”加以保护。与此同时，现有法律多集中于规制公权力机关，尤其是公安机关收集指纹信息的相关规定，针对私主体收集、处理与利用个人生物识别信息的保护规定相对较少。

二、立法模式：渐进式的综合立法模式

个人生物识别信息的立法模式是指国家在个人生物识别信息保护立法时所采取的、与调整范围有关的法律形式。立法模式在广度上深刻影响着个人生物识别信息保护的实现，是个人生物识别信息立法首先需要解决的问题。

（一）个人生物识别信息的双重立法模式

基于立法传统与背景等方面的不同，当前个人生物识别信息保护的立法模式主要存在专门立法模式与综合立法模式两种。

专门立法模式是指采用单独立法的形式对个人生物识别信息加以保护的模式。其中以美国的部分州为代表。美国对个人生物识别信息的保护大多建立在隐私权保护的基础上，自21世纪开始生物识别技术被规模化地应用到反恐、国家安全、刑事侦查等领域，并逐渐在伊利诺伊州、芝加哥州等开始民用化与商用化[2]78-88。当前美国大部分州均允许雇主或企业收集、分析个人生物识别信息，但是禁止通过生物识别信息获利。美国虽然未在联邦层面上对个人生物识别信息的收集与使用作出统一规定，但各州先后制定了专门规制私部门使用个人生物识别信息的保护法案，如2008年伊利诺伊州制定了美国首部《生物识别信息隐私法案》，2009年德克萨斯州制定了《生物特征信息隐私法》，2019年佛罗里达州制定了《生物信息隐私法案》等，此外阿拉斯加、新罕布什尔等州也逐渐将生物识别信息法列入立法议程。上述立法的适用对象仅为“私营主体”收集、处理、利用个人生物识别信息的行为，立法内容主要从法律概念、权责关系、行为规范、监管机构与职能、救济途径与方式等方面进行规定。自2019年开始，由于“人脸识别技术”的广泛应用，有关利用个人生物识别信息的合法性问题再次引发争议，无论是州层面还是联邦层面，均出台了专门针对“人脸识别信息”保护的法案。2019年5月加利福尼亚州旧金山市对《停止秘密监视》条例进行修订，认为人脸识别技术侵害了公民的隐私与自由，并可能引发种族不平等，由此成为美国第一个禁止官方机构使用人脸识别技术的城市。2019年6月马萨诸塞州萨默维尔市议会则通过《人脸识别全面禁止条例》，禁止警察和公共部门使用人脸识别软件，2019年7月加利福尼亚州的奥克兰市亦颁布《监视及社区安全法案》。在联邦层面上，2019年3月美国参议院通过了《商业面部识别隐私法案》；2020年2月12日有议员在参议院提出了《人脸识别道德使用法》草案，旨在委员会提出使用人脸识别技术的适当指南和限制之前，暂缓政府机构使用人脸识别技术[3]。

综合立法模式是指不区分个人生物识别信息与一般个人信息，将不同类型、性质的个人信息统一纳入到个人信息保护法之下，从行政、民事、刑法等不同方面进行统一的立法保护[2]80。当前大多数国家、地区采用综合立法模式。欧盟是综合立法模式的典型代表，其以人格权为基础建立了强化公共部门行政监管的保护方式。2018年生效的《通用数据保护条例》（亦称为《一般数据保护条例》），即GDPR，对处理个人数据中的自然人保护以及个人数据自由流动的规则进行了规定，将“生物识别数据”作为“特

殊类型个人数据”予以特殊保护，并“原则上禁止”为了“识别特定自然人”而收集处理生物特征数据，但是规定了 9 种例外情形[①]。同时 GDPR 允许成员国在国内立法作出额外的限制。需要注意的是，欧盟对于人脸识别技术的应用持有警惕态度，2019 年欧盟基本权利保护局发布了《面部识别技术：执法中的基本权利考虑》，分析了面部识别技术对基本权利带来的挑战，简要介绍了当公共当局部署实时面部识别技术来实现执法的目的时避免侵犯人权应采取的步骤[4]。亚洲对个人生物识别信息保护进行立法相对较晚，并深受欧盟立法的影响，亦主要采取综合立法模式。比如印度为了保护与个人数据有关的个人隐私，以及明确个人数据的流动和使用，于 2019 年颁布了第 373 号法案《2019 年个人数据保护法》，其在明确一般个人数据保护规则的同时，将“生物特征数据”作为一种特殊的个人数据类型予以特殊保护，明确规定“除非法律允许，任何数据受托者不得处理经中央政府通告的生物特征数据。”[②]

总体而言，两种立法模式均存在利弊。专门立法模式针对性、可操作性强，可以根据不同领域灵活制定，然而不同立法之间容易发生冲突；综合立法模式体系性较强，但灵活性却存在不足。从立法内容上看，无论采取何种模式，在保护个人生物识别信息的法律原则、保护规则、权责条款等方面趋于一致。

（二）中国个人生物识别信息保护的立法模式选择

个人生物识别信息保护的立法模式选择应在辨析不同立法模式的产生原因、历史演变与现实困境的情况下，结合中国的立法传统、现实需求，以及法制发展现状等进行综合判断，在个体权益保护与群体发展之间寻求最佳利益平衡点[5]。

从中国信息立法的传统与发展趋势看，均采用综合立法模式。在立法传统上，比如《网络安全法》即将个人生物识别信息纳入个人信息的范畴予以规范。其他的一些规范性文件，如《互联网个人信息安全保护指南》《信息安全技术个人信息安全规范》等也均在明确一般个人信息保护规则的同时，对个人生物识别信息的特殊保护规则进行规定。在立法趋势上，当前《数据安全法》与《个人信息保护法》的草案均已进入公开征求意见阶段，两者均呈现出综合立法的模式，比如《数据安全法》（草案）已经对重要数据与一般数据共同予以规范。

同时，相较于专门立法模式，综合立法模式更有助于解决中国分散立法存在的问题：一是综合立法模式层级清晰体系完整。个人生物识别信息的保护属于个人信息保护法律体系的一个分支，采用综合立法模式能够在明晰一般个人信息保护规则的前提下，规定个人生物识别信息保护的特殊规则，进而实现个人信息保护法律体系的完整性。二是综合立法模式的保护方法与保护措施全面。一方面综合立法模式不局限于单一领域，对个人生物识别信息的保护具有普遍的适用性。另一方面保护方法与保护措施更为全面，包括行政法保护、民事救济以及刑事制裁等领域。三是综合立法模式有利于法律适用。个人生物识别信息在体系上不仅要符合一般个人信息收集、处理、使用的基本原理与规定，而且要符合个人生物识别信息的特殊规则。综合立法模式有助于实现一般个人信息与特殊个人生物识别信息的体系协调，避免分散立法引发的体系违反，便于法律适用。

需要注意的是，一方面面对当下个人生物识别信息滥用的境地，亟待立法保护。特别是在中国生物识别技术安全性未得到充分证实，使用风险尚未得到全面评估，以及保护机制尚待系统化之前，个人生物识别信息已经被大范围使用，比如不仅局限于国家安全、治安管理等公用场景，而且包括金融、医疗、学校、支付、交通、社区、企业、小区物业管理、商场等私用场景。日益泛滥的生物识别技术运用，已经导致个人生物识别信息在实践中被贩卖、泄露，侵犯了信息主体的隐私权、财产权等合法权益，亟待进行立法规制。另一方面虽然《数据安全法》与《个人信息保护法》的草案已经开始公开征求意见，但是纵观世界，生物识别技术尚未成型，有关的技术标准也未达成共识，因而对个人生物识别信息进行系统性、明确性、完整性规定尚需时间。比如 2019 年 12 月，全国信标委生物特征识别分技术委员会才正式全面启动人脸识别国家标准的制定，系统化建设中国人脸识别国家标准体系。作为大数据时

① General Data Protection Regulation. Art. 9。

② Personal Data Protection Bill, Sec. 92。

代的新问题，在尚未探索出个人生物识别信息保护的成熟实践经验之前，贸然进行立法可能适得其反。可根据《立法法》第 9 条进行“授权立法”[①]，或者根据《立法法》第 73 条进行“地方先行立法”[②]，待时机成熟上升至全国统一立法。

综上所述，面对中国当前个人生物识别信息保护分散立法存在的问题，结合中国信息立法的现有情况与发展趋势，中国应该采用综合立法模式。但是为了解决当前个人生物识别信息亟待立法进行保护的迫切需求，可以采用“授权立法”“地方先行立法”的模式，为综合立法中个人生物识别信息保护条款的制定提供经验。因此，渐进式的综合立法模式更适合中国实践。

三、立法理念：充分信息保护基础上的有限开发利用

个人生物识别信息保护立法是一项系统的工程，立法理念是支撑立法的基石，指引着立法的制度设计。个人生物识别信息保护的立法本质上是多元主体之间利益的角逐，基于个人生物识别信息的独特属性，“充分信息保护基础上的有限开发利用”是立法的核心价值理念。

（一）个人生物识别信息承载人格尊严与个人隐私需要充分保护

相较于一般个人信息，个人生物识别信息具有独特的物理属性，属于敏感个人信息，承载着人格尊严与个人隐私利益，需要予以特殊、充分的保护。

1. 个人生物识别信息具有独特物理属性

生物识别是以人类独有的生理特征或行为表现，来辨识或者验证使用者的个人身份。生理特征是先天具有的，包括指纹、人脸、虹膜、视网膜、静脉等。行为表现是后天形成的，如走路的步态、按键的力度等。由此而获取的个人生物识别信息具有独特的物理属性，需要予以充分保护：

一是具有“独一无二性、难以更改性”，一旦被窃取或泄露，将不可索回，无法进行更改与撤销。与其他个人信息，比如身份证号、电话号码、银行卡密码、家庭住址等相比，个人生物识别信息具有生物学意义上的唯一性，其不可能因客观环境的变化而作出改变，如果使用不当，造成的损害将是不可逆的。

二是部分个人生物识别信息极易脱离信息主体的掌控，可以被轻而易举地获得与利用，加剧了滥用风险。以“人脸识别”信息为例，由于当下密集的摄像头布置，致使个体容易暴露在摄像头之下，因而在收集上可不经过信息主体主动配合而获得人脸图像，在使用上亦可以脱离信息主体而被利用。例如嘉兴上外秀洲外国语学校 402 班科学小队在做课外实验的时候，用一张打印照片就能代替真人刷脸，骗过小区里的丰巢智能柜，取出父母们的货件[6]。

三是由于个人生物识别信息需经由计算机的算法才能生成，因而可能存在算法错误，导致误判，由此引发种族歧视风险，加剧社会不平等等问题。美国国会经过调研发现，人脸识别技术的准确率历来不高，特别在识别女性、年轻人、非裔美国人和其他族裔群体。已有证据显示人脸识别对有色人种、活动家、移民和其他原因本就受到不公正对待的群体的不良影响更为显著[7]。

2. 个人生物识别信息属于“敏感个人信息”

个人生物识别信息的性质决定其保护的方式。根据泄露该信息导致重大伤害的可能、对信息主体带来伤害的大小、社会大多数人对某类信息敏感度的认知等因素，可以将个人信息划分为“一般个人信息”与“敏感个人信息”。敏感个人信息是指“一旦泄露或滥用，极易危及人身、财产安全或导致人格尊严受到损害、歧视性待遇的个人信息”，比如健康信息、金融信息、基因信息、关乎个人安全的信息等[8]。从性质上看，个人生物识别信息属于“敏感个人信息”的一种，应当予以特殊保护。

一方面，个人生物识别信息承载着人格尊严、隐私等重要价值。由于个人生物识别信息具有高度的专属性与私密性，与个人最隐秘的生理特征直接相关，具有表征和彰显个人身份的特质，因而构成了

---

①《立法法》第 9 条：本法第八条规定的事项尚未制定法律的，全国人民代表大会及其常务委员会有权作出决定，授权国务院可以根据实际需要，对其中的部分事项先制定行政法规，但是有关犯罪和刑罚、对公民政治权利的剥夺和限制人身自由的强制措施和处罚、司法制度等事项除外。

②《立法法》第 73 条：地方性法规可以就下列事项作出规定：……除本法第八条规定的事项外，其他事项国家尚未制定法律或者行政法规的，省、自治区、直辖市和设区的市、自治州根据本地方的具体情况和实际需要，可以先制定地方性法规。在国家制定的法律或者行政法规生效后，地方性法规同法律或者行政法规相抵触的规定无效，制定机关应当及时予以修改或者废止。

“数字化人格”的核心组成部分。“人格标识的完整性与真实性是主体受到他人尊重的基本条件。”[9] 只有保障数字化人格与信息主体相一致，并且不被非法侵犯，才能获得他人的尊重，实现自由与尊严。另一方面，个人生物识别信息的泄露将对公民权利造成更大的伤害。相较于其他个人信息，个人生物识别信息不仅能够识别自然人的身份，而且可以从事个性化服务，如利用指纹、面部开启手机、办理金融业务等。一经泄露或者公开，将对个人隐私、尊严等造成不可逆影响，乃至遭受歧视性待遇。正是由于个人生物识别信息与个人生理特征最为紧密，承载了人格尊严与个人因素等权益，属于敏感个人信息，理应予以充分、特殊保护。

当下将个人生物识别信息列入“敏感个人信息”并给予特殊保护，已经成为各地的普遍共识。比如欧盟的《通用数据保护条例》GDPR 第 9 条便将“生物性识别数据”纳入“特殊类型个人数据”；美国《2018 年加州消费者隐私法案》亦将包括虹膜、视网膜、指纹、脸部、手掌、静脉图案和语音记录的图像等在内的生物特征识别数据列为个人隐私信息[10]；印度颁布的《2019 年个人数据保护法》禁止在印度境外处理个人敏感数据和重要个人数据，禁止处理特定形式的生物特征数据，明确了输入个人敏感数据和关键个人数据的条件。事实上，中国《个人信息保护指南》已经采取了一般个人信息与敏感个人信息区分的理念，在收集时前者可以默许同意，后者必须明示同意。《信息安全技术个人信息安全规范》也在收集与存储等方面进行了细化与完善，明确规定“收集人脸信息需单独告知，不得存储原始图像”“用户拒绝授权扩展业务功能权限，App 不得反复征求授权”,并建议 App 支持用户对画像标签的自主控制机制。

（二）公私部门对个人生物识别信息具有强烈利用需求

个人生物识别信息具有公共性，能够促进社会公共福祉的实现。无论在商业领域还是公务领域，均具有对个人生物识别信息强烈的应用需求。

1. 基于政务价值的公共利用

在信息社会，数字政府已经成为现代政府的基本标志。特别是当下，个人生物识别信息的社会治理价值更为突出。比如个人生物识别信息在公共秩序、公共安全、公共福利的推进方面，均发挥着不可替代的作用。

一是进行公共管理，维护公共安全。基于个人生物识别信息独特的物理属性，个人生物识别信息无论在传统的行政管理领域，亦或是现代的风险社会治理领域均发挥着重要功能。在传统的治安防控、犯罪侦查领域，公安机关借助指纹信息、肖像、虹膜图像等，开展身份管理、打击刑事犯罪、维护国家安全，尤其在查找失踪儿童、犯罪分子等方面表现卓越。在现代风险社会，看似偶然、不确定的公共事件，其背后的行为规律仍有迹可循。“大数据的核心就是预测，是把数学算法运用到海量的数据上来预测事情发生的可能。”[11] 个人生物识别信息有助于提升预测的准确性，比如人脸识别能够实现数据的实时监控，提升风险防控的效率。

二是优化行政服务，增进公共福利。推行电子政务一直是中国信息化发展的的战略重点，当前中国已经运用生物识别信息推行高效便捷的“网上政务”，并在社会保障领域积极推广，提升了社会治理的效能。比如《国务院办公厅关于推进养老服务发展的意见》提出了实施“互联网+养老”行动，倡导通过运用互联网和生物识别技术，来探索建立老年人补贴远程申报审核机制。北京市为了加强公租房管理，规制违法转租等行为，规定纳入保障房建设计划的公租房，全面采用人脸识别等技术，以便于相关管理①。

2. 基于商业价值的市场利用

伴随着人工智能时代的来临，个人生物识别信息不再是简单地识别身份特征的标志，毋宁说其已成为重要的生产要素，推动着产业分工与经济结构调整，而且改变着人们的生活习惯。

首先，个人生物识别信息的收集与处理对人工智能、大数据，乃至整个数字经济的发展至关重要，具有重要的商业价值。在国家层面上，国务院 2015 年发布《促进大数据发展行动纲要》，积极鼓励与推进大数据产业的发展。据有关研究显示，2016 年国内生物识别的市场规模在 120 亿左右，而到 2021 年预测将达到 340 亿[12]。甚至有预测称，生物识别技术会先于人工智能步入大规模应用阶段[13]。与此同时，有

① 北京市住建委发布的《关于进一步加强公共租赁住房转租行为监督管理工作的通知》。

关个人生物识别信息的应用催生了大量的信息服务产业，比如信息查询平台、征信机构、数据处理公司等。

其次，个人生物识别信息有助于改变营销策略，提升个性化的服务。“营销建立在对消费者需求的准确把握之上。”[14] 运用个人生物识别信息有助于更为精确地了解消费者的需求与偏好，提升经营者决策的理性与效率，从而进行更具针对性的产品推介、引导，提供更为个性化的服务，促进服务升级与未来产品的研发。

最后，方便企业管理，提供更为安全、便捷的服务。基于个人生物识别信息的独特性，部分企业运用生物识别技术进行员工签到等日常管理。同时生物识别技术在提供安全管理、金融服务等领域具有独特的优势，比如物业设置人脸识别门禁系统防止外来人员进入，超市、商场等开设人脸识别支付系统实现自助结账等。

实现个人信息保护与利用的动态平衡是信息保护立法的关键。对于个人生物识别信息而言，其具有区别于一般个人信息的独特物理属性，关涉公民的人格尊严、隐私保护，一旦泄露，将对公民权利产生不可逆的影响，因而应当予以充分特殊的保护。尤其在生物识别技术的安全性尚未得到有效证实，生物识别技术使用标准尚未形成共识的情况下，对个人生物识别信息予以充分保护是立法应当明确的核心法益，这也是当前诸多国家和地区禁止收集、储存与利用个人生物识别信息的原因所在。个人生物识别技术在增进社会福祉方面发挥着不可替代的功能，既有助于维护公共秩序，增进公共福利，亦能推动信息产业、数字经济的发展。因此，在充分保护的基础上有限地利用个人生物识别信息，是立法应当秉持的核心理念，由此实现个人生物识别信息保护与利用之间的利益平衡。

四、个人生物识别信息保护立法的核心内容

个人生物识别信息的保护需要借助于具体的法律条文予以落实。个人生物识别信息保护涉及到诸多内容，在综合立法模式的前提下，需要结合中国的现实需要，制定较为完备、具有针对性、可操作性的法律规范。

（一）界定个人生物识别信息的法律概念、类别、属性条款

概念明确与否，直接关系到立法逻辑乃至法律体系构成。首先应当规定个人生物识别信息的法律概念。在此可以参照欧盟 GDPR[①]、伊利诺伊州[②]、印度[③]等国家或地区的立法经验，核心在于明确个人生物识别信息“单独”“识别个人身份”的“唯一标识性”、需要借助计算机程序等高科技手段予以特殊处理等核心法律内涵。其次，细化个人生物识别信息的类型，增强个人生物识别信息保护立法的可操作性。比如《信息安全技术个人信息安全规范》在附录中进行了例举，包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。然而个人生物识别信息并不限于上述“生理特征”的个人生物识别信息，还包括“行为特征”的个人生物识别信息，即“通过行为特征进行特定的技术处理而得到的可以辨识个人身份的信息”[④]，比如笔迹、步态等，均应在立法中加以明确。最后，明晰个人生物识别信息的法律属性，实现对个人生物识别信息的充分保护。对敏感个人信息与一般个人信息进行分类，并对敏感个人信息进行特殊保护已经成为世界各国的普遍共识。尽管“敏感个人信息”的认定方式与种类存在分歧，但并不影响个人生物识别信息属于敏感个人信息的性质定位。因而在未来的立法中应明确个人生物识别信息属于“个人敏感信息”的法律属性，为实现对其特殊保护奠定前提基础。

（二）确立个人生物识别信息保护的特殊法律原则

个人生物识别信息保护的法律原则，贯穿立法始终。个人生物识别信息保护属于新兴领域，涉及到

① 欧盟 GDPR 第 4 条第 14 款规定，“生物性识别数据”指的是基于特别技术处理自然人的相关身体、生理或行为特征而得出的个人数据，这种个人数据能够识别或确定自然人的独特标识，例如脸部形象或指纹数据。General Data Protection Regulation. Art. 4 (14)。

② 伊利诺伊州《生物识别信息隐私法案》中将生物识别信息界定为“基于个人生物标识而生成的任何信息，无论其如何被取得、转换、存储或共享”。Biometric Information Privacy Act。

③ 印度《2019 年个人数据保护法》（Personal Data Protection Bill, 2019）第 1 章第 3 条第 7 款规定，“生物特征数据”是指面部图像、指纹、虹膜扫描，或其他类似的能够通过物理、生理或行为特征测量或技术处理操作得到的，可以允许或完全能够确认一个自然人的唯一标识的个人数据。

④ General Data Protection Regulation. Art. 4 (14)。

多重利益关系，尚无成熟的立法经验，过于冒进或者退缩都可能带来负面影响，因此通过立法原则的规定不仅有助于引导个人生物识别信息的立法与适用，而且有助于弥补法律漏洞，增加法律条文的弹性与包容性。

在遵循个人信息保护一般法律原则的基础上①，基于个人生物识别信息的特性，还应规定个人生物识别信息保护的特殊原则。个人生物识别信息保护特殊原则的确立，尤其应当注重“充分信息保护基础上的有限开发利用”的立法理念，参考各国的经验，制定特殊原则：一是禁止原则。为充分保护个人生物识别信息安全，除非法律允许，原则上禁止“仅以识别自然人为目的”的收集、储存、传输、处理、使用或者披露个人生物识别信息。为了保护国家安全，尤为应当禁止向境外非法传输个人生物识别信息。二是明示同意原则。在法定范围内收集个人生物识别信息之前，应当单独向信息主体告知收集、使用生物识别信息的目的、方式与范围，以及存储的时间等，并获得信息主体的明示同意。三是法定必需原则。只有法律明确规定的情形下，才可以不经过信息主体的同意而处理个人生物识别信息。法定情形的设定，需要经过风险评估，并且符合“比例原则”的基本要求。纵观已有立法，大致包括：为履行工作职责必需；为实现实质性的公共利益与维护公共安全必需；对于数据处理主体或另一自然人的核心利益必需；基金、协会或其他非盈利组织已经采取了恰当的保护措施而进行的正当性活动必需；对于提起、行使或辩护法律性主张必需或者法院的司法活动必需；对于预防性医学或临床医学目的必需等②。

（三）明确个人生物识别信息主体的权利条款

法律以权利为关注焦点，“法律为客观的权利，权利为主观的法律。”[15] 在个人生物识别信息保护的立法中，对信息主体享有的权利予以明确是立法的核心宗旨，亦是引导相关保护措施设计、决定保护深度与质量的关键。

结合各国的立法经验，个人生物识别信息主体主要享有权利：其一信息决定权，即生物识别信息主体得以直接控制与支配其个人信息，并决定是否被收集、处理、利用的权利。“信息决定权是个人信息权的首要内容，它直接说明了个人信息的权利归属，决定了个人信息的命运。”[16]239 信息决定权是信息主体意思自治的体现，这便要求以充分的知情为基础。由于个人生物识别信息关联着个人基本权利，只有在获得信息主体明示同意的情况下，信息处理者才能在法定范围内处理个人生物识别信息。其二信息查询权，即个人生物识别信息主体具有查询其信息被收集、处理与利用的权利，包含信息处理者对信息主体的主动告知和信息主体提请查询两种方式。信息查询权是一项基本权利，但是也存有某些例外，比如在查询可能损害他人重大利益，扰乱公共秩序，危害公共安全等情况下，应该限制或者禁止查询[17]。其三信息更正权，即个人生物识别信息主体请求信息控制者对不正确的个人生物识别信息进行更正、补充的权利。其中“不正确”应当采用广义的理解，包括“不正确、不完整、不最新”三种情形。其四信息封锁权，即在法定或约定事由出现时，个人生物识别信息主体有权请求信息控制者以一定方式暂停处理和利用个人生物识别信息。“信息封锁权的行使对象是已经被收集的个人信息，行使事由有两个：一是个人信息的正确性处于不确定状态，二是个人信息的完整性处于不确定的状态。”[16]246由此可见，信息封锁权大多情况下是信息更正权的配套措施，在行使信息更正权之前，信息主体大多会行使信息封锁权，以防止不正确信息的利用给自身造成损害。其五信息删除权，即基于法定或约定的事由，信息主体要求信息控制者删除其个人信息的权利。行使此项权利的事由主要包括：收集、处理与利用之初没有得到明示同意、处理与利用的目的消失、处理与利用期限届满、处理与利用超出约定或法定的范围等[16]248。“删除”应当达到“不得复认”的状态，即不仅原信息无法被再次辨认使用，而且没有再次提供该信息的可能。其六信息收益权，即基于商业目的而被相关市场使用时，信息主体可以要求使用者支付相应对价，这是个人信息支配权的体现。

（四）细化个人生物识别信息处理者的行为规范

个人信息保护经历了从“积极确权模式”到“行为规范模式”的转变与融合，其中“行为规范模式”是指

① 即最小化收集原则、目的明确原则、信息质量原则、安全保障原则、限制利用原则、参与原则、公开原则、责任原则等。

② General Data Protection Regulation. Art. 9。

基于对个人信息运用可能带来的潜在风险与影响而为处理者设置相应的行为规范，以此为个人信息的收集、开发、持有以及泄露等阶段提供规范引导，进而实现个人信息的保护[18]。个人生物识别信息的保护以及上述信息主体权利的实现，需要信息处理者遵循立法设定的行为规范，事实上美国伊利诺伊州的《生物识别信息隐私法案》、欧盟的《通用数据保护条例》、印度的《2019 年个人数据保护法》等均采用此种模式。“从行为主义的进路出发，个人信息保护应当根据不同行为所可能侵犯个人和社会的权益而进行不同程度的规制。”[19] 在大数据时代，个人生物识别信息的应用场景纷繁复杂，并且受到多重因素的影响，僵化的、不变的措施可能难以展开有效的保护，因此在具体行为规范的制定中，要结合个人生物识别信息的不同应用“场景”，以及不同应用场景中个人生物识别信息的处理行为给信息主体带来的风险，进行综合考量。

事实上，《民法典》第 111 条①、《网络安全法》第 4 章以及《数据安全法（草案）》已经从信息的收集、利用、持有三个阶段大致设定了个人信息处理的一般规则，个人生物识别信息保护立法应在此基础上，结合个人生物识别信息的特殊属性进行规定。首先，信息收集阶段，收集者应当依法取得个人生物识别信息，并经信息主体的“明示同意”。为防止“明示同意”形同虚设，要求信息收集者应当进行清晰明确的告知与风险披露，以便个人生物识别信息主体自主作出选择。其次，信息开发利用阶段，不得非法买卖、传输、使用、加工个人生物识别信息。其中，“非法”应采取广义的理解，不仅包括不得违反法律、法规、规章等法律规范的规定，而且包含不得违反双方的约定。尤为注意的是，为防止僵化地审视是否符合当事人的同意，对个人生物识别信息的处理是否合理，应当综合考量所引发的风险是否符合信息主体的合理预期，是否可以为信息主体所接受。再次，信息持有阶段，确保个人生物识别信息安全。由于信息持有者的不当储存行为可能引发个人生物识别信息泄漏的风险，所以应当通过隐私设计政策、安全保障措施进行安全风险防范，消除因持有、储存等行为引发侵犯公民权利的风险。比如区别于一般个人信息的储存方式，原则上不储存个人生物识别信息，如果基于特殊需要进行储存，则仅储存摘要信息、与个人身份信息分开存储、采取加密措施等②。最后，信息泄露后的报告义务。为了降低个人生物识别信息泄露后的风险，信息处理者应当及时将泄露情况有效地告知信息主体，并应当向信息监管机关报告。

（五）设置个人生物识别信息的多元化保护机制

个人生物识别信息的保护不仅需要信息主体、信息控制者、信息处理者的自律，而且需要国家积极构建保护机制。为实现保护的充分性，应当从行政、民事和刑事三个方面构建。

相较于民事与刑事保护机制，行政保护机制具有事前预防、高效便捷等优势。在行政保护机制方面，首先应当设置独立的监管机构。美国伊利诺伊州设有“生物识别信息隐私调查委员会”，印度设有“数据保护局”，为解决分散化、多头化的监管机构带来的监管难题，中国应当明确网信办的独立监管地位，并在其内部设置“生物识别信息监管处”，实现统一监管。同时划清相关监管部门之间的机构职责，实现层级化、部门化政府机构的协同监管。其次，明确监管机构的法定职权，包括审查权、许可权、检查权、调查权、扣押权、处罚权、受理控诉权、纠纷解决权等。同时监管机构应当根据不同应用场景的风险设置不同的监管方式，以风险预防理念为指引，结合个人生物识别信息应用的不同环节，通过行政处罚、行政许可等强制性监管方式与行政约谈等非强制性监管方式的结合，实现贯穿个人生物识别信息处理生命周期的动态风险监管。最后，个人生物识别信息的保护需要专业能力与技术能力作支撑，因此应当配置具有行政专长的复合型监管人才，并通过聘请专家、顾问等方式弥补监管机构专业技术能力的不足，提升监管效能。

---

①《民法典》第 111 条：自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

② 2020 年《信息安全技术个人信息安全规范》（6.3）“个人敏感信息的传输与存储”已对此进行规定：对个人信息控制者的要求包括：（a）传输和存储个人敏感信息时，应采用加密等安全措施；（b）个人生物识别信息应与个人身份信息分开存储；（c）原则上不应存储原始个人生物识别信息（如样本、图像等），可采取的措施包括但不限于：（1）仅存储个人生物识别信息的摘要信息；（2）在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；（3）在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

在民事保护机制方面，核心在于建立个人生物识别信息的损害赔偿救济机制。在立法体系中应当明确个人生物识别信息不同处理阶段、不同信息处理主体的法律责任，结合“隐私风险”确定差异化的法律责任体系。由于个人生物识别信息的侵权行为大多属于“程序性违法”行为，比如在收集、使用个人生物识别信息之前没有履行告知义务、没有获得明确的同意，同时滥用、泄露个人生物识别信息的“损害”往往难以认定，所以“最大的问题是如何确认侵害知情权、民事同意权等程序性权利的损害事实和结果。”[2]85 对此可以借鉴域外国家的经验，即在规定过错责任原则的同时实行举证责任倒置，以化解程序性违法行为的损害赔偿难题。同时，根据《民法典》第 1034 条规定，个人生物识别信息属于个人信息的范畴，并属于私密信息，应当适用有关隐私权的规定。应以中国民法规范中隐私权损害赔偿条款为基础，结合损害的性质与程度、主观过错、信息处理者实施措施的透明度与问责性等因素，对损害赔偿责任进行综合考量。在此基础上，承担停止侵害、排除妨碍、消除危险、赔偿损失等侵权责任。

刑事保护机制是个人生物识别信息保护的最后防线，主要通过设置相应的刑罚进行保护。美国在 1989 年设置“身份盗窃”罪，其中非法故意转移、使用生物识别信息用于违法活动的行为就属于此种犯罪情形[20]，美国 2003 年制定《身份盗窃处罚增强法》；韩国《个人数据保护法》规定“非法处理唯一标识罪”。立足中国语境，基于罪刑法定与法律保留原则，刑事处罚只能由刑法进行规定，因而在严重侵害公民个人生物识别信息的问题上，可以采用“指引条款”的立法技术，规定“侵犯公民个人生物识别信息情节严重，构成犯罪的，依据《刑法》第 253 条之一侵犯公民个人信息罪追究刑事责任”。

参考文献：

[1] BEN-SHAHAR O, JACOB L S. Contracting over privacy: introduction[J]. Journal of Legal Studies，2016（2）：51–61.

[2] 付微明. 个人生物识别信息的法律保护模式与中国选择 [J]. 华东政法大学学报，2019（6）：78–88.

[3] CAICT 互联网法律研究中心. 美国参议员提出《道德使用人脸识别法案》概述 [EB/OL]. (2020-02-20)[2020-03-02]. https://www.secrss.com/articles/17249.

[4] CAICT 互联网法律研究中心. 欧盟发布《面部识别技术: 执法中的基本权利考虑》[EB/OL]. (2019-12-29)[2020-03-09]. http://kejixianfeng.blogchina.com/562126468.html.

[5] 张静. 个人信息保护立法模式选择 [J]. 法治社会，2019（3）：72–83.

[6] 金融虎. 丰巢刷脸取件被小学生“破解”刷脸支付还安全吗?[EB/OL]. (2019-10-17)[2021-01-09]. https://news.p2peye.com/article-552000-1.html.

[7] 林鑫, 王捷. 美国《人脸识别道德使用法案》全文翻译与评价 [EB/OL]. (2020-02-26)[2020-07-09]. http://www.hxxwzk.com/news/2020/shishi_0226/1142.html.

[8] 胡文涛. 中国个人敏感信息界定之构想 [J]. 中国法学，2018（5）：248–254.

[9] 王利明. 人格权法的新发展与我国民法典人格权编的完善 [J]. 浙江工商大学学报，2019（6）：6–19.

[10] 吴沈括, 孟洁. 美国《2018 年加州消费者隐私法案》中文译本 [EB/OL]. (2018-07-10)[2021-01-09]. http://www. http://www.yidianzixun.com/article/0JVEbyrg.

[11] 维克托·迈尔-施恩伯格, 肯尼斯·库克耶. 大数据时代: 生活、工作与思维的大变革 [M]. 盛杨燕, 周涛, 译. 杭州: 浙江人民出版社, 2013: 16.

[12] 前瞻产业研究院. 生物识别 2021 年国内市场规模有望突破 340 亿 技术突破是关键 [EB/OL]. (2018-04-13)[2020-03-12]. http://www.qianjia.com/html/2018-04/13_289445.html.

[13] 赵淑钰. 生物识别信息法律规制的国际经验与启示 [J]. 网络空间战略论坛，2019（11）：37–39.

[14] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排 [J]. 中国法学，2015（3）：38–59.

[15] 史尚宽. 民法总论 [M]. 北京: 中国政法大学出版社, 2000: 18.

[16] 齐爱民. 大数据时代个人信息保护法国际比较研究 [M]. 北京: 法律出版社, 2015: 239.

[17] 洪海林. 个人信息的民法保护研究 [M]. 北京: 法律出版社, 2010: 164.

[18] 宋亚辉. 个人信息的私法保护模式研究:《民法总则》第 111 条解释论 [J]. 比较法研究，2019（2）：86–103.

[19] 丁晓东. 个人信息的双重属性与行为主义规制 [J]. 法学家，2020（1）：64–76.

[20] KURT M S, BRUCE Z. Counteracting identity fraud in the information age: the identity theft and assumption deterrence act[J]. International Review of Law, Computers & Technology，1999，13（2）：183–192.

On Legislative Path of Personal Biometric Information Protection

YANG Tongtong

（School of Political Science and Public Administration, East China University of Political Science and Law, Shanghai 201620, China）

Abstract：Personal biometric information has a high degree of specificity and privacy, and is directly related to the physiological characteristics of personal privacy, highlighting personal identity characteristics, so it needs special protection. Providing a framework for the use and protection of personal biometric information through the legislative path is the key to the regulation of the abuse of personal biometric information and the protection of personal biometric information. In the legislative mode, combined with China's legislative tradition, realistic demand, and the current situation of the development of the legal system, the progressive comprehensive legislative model should be adopted. In the legislative concept, in order to achieve the balance of interests among multiple subjects, the limited use of personal biometric information on the basis of full protection is the core concept that legislation should uphold. In the legislative content, it is necessary to define the legal concepts, categories and attributes of personal biometric information, establish the unique protection principle, clarify the rights of information subjects, specify the behavior norms of information processors, set up diversified protection mechanisms, etc.

Keywords：personal biometric information; biological recognition technology; comprehensive legislative model; protection mechanism

[责任编辑：箫姚]

(上接第 139 页)

Normative Construction of the Administrative Order System of Ecological Environment Restoration

CHENG Yu

（School of law, Beijing Normal University, Beijing 100875, China）

Abstract：The "order for restoration" in China's natural resource law is a kind of administrative order for ecological environment restoration. The "order for governance" and "order for correction" in China's pollution prevention and control law cannot be interpreted as an administrative order for ecological environment restoration. In the case of directed behavior, it belongs to the order of rectification of illegal behaviors, while in the case of directed result, it belongs to the administrative order of elimination of immediate harmful consequences. Compared with judicial restoration, administrative restoration has institutional advantages. In the future, legislators should make clear the dominant position of the system of administrative orders for ecological environment restoration in Environmental Protection Law and separate environmental laws, and formulate a special procedure law. The core normative contents should include the notice procedure, the implementation procedure, the objection procedure, the recovery procedure of the restoration cost, and the sanction procedure. Administrative organs should start judicial restoration on the premise of exhaustion of administrative order system. The judicial restoration initiated by ENGOs and peoples' Procuratorates should be positioned as a supplementary system, and policy restoration should adhere to the principles of "Polluter Pay Principle" and "Unified Planning Principle".

Keywords：eco-environment restoration; administrative decision; administrative penalty; restoration by justice; restoration by governmental policy

[责任编辑：箫姚]