个人生物信息安全的法律保护

——以人脸识别为例

张勇[1]

【摘 要】：随着人脸识别等生物识别技术的广泛应用，个人生物识别信息作为一种特殊的个人敏感信息，所蕴含的个人信息权利应受到法律保护。在此基础上，应当确立风险预防及利益平衡原则以保障个人生物信息安全。在生物信息安全法律领域，我国现有的私法和公法保护模式都难以实现体系化保护。我国应以网络安全法、生物安全法、个人信息保护法、数据安全法等综合性立法为契机，通过相关行政法与刑法的衔接协调，构建个人生物信息安全的法律法规体系。

【关键词】：人脸识别 个人生物识别信息 生物信息安全

【中图分类号】D92**【文献标识码】**A**【文章编号】**1004-518X（2021）05-0157-12

个人生物识别信息，即自然人可识别的生理或行为特征，从中提取可识别、可重复的生物特征样本、模板、模型等识别数据或数据的聚合。随着生物、医学与信息技术的不断发展，个人的面部、指纹、视虹膜、基因（DNA）等生物信息识别技术被广泛应用到治安防控、政府治理、医疗卫生、轨道交通等社会生活领域。

生物识别技术发展所带来的身份验证、人体试验、器官移植、辅助生殖技术、基因编辑及重组等问题，都可能会侵犯个人信息数据权利，危及生物信息安全甚至国家安全。如何防范生物识别技术应用的安全风险，构建个人生物信息安全的法律法规体系，成为法学理论界和司法实务界共同关注的问题。

除了国家立法机关已颁布实施的《网络安全法》《民法典》《生物安全法》之外，《个人信息保护法（草案）》《数据安全法（草案）》已经向社会征求意见。这些重要立法都与个人生物信息安全保护密切相关。

2020 年 12 月 7 日，中共中央印发《法治社会建设实施纲要（2020—2025 年）》，提出要完善网络信息服务方面的法律法规，完善网络安全法配套规定和标准体系，研究制定个人信息保护法等。如何依法规范个人生物识别技术的研发和应用，确定侵犯个人生物识别信息权利的法律责任，构建危害生物信息安全行为的制裁体系，本文将对此展开讨论。

一、人脸识别：个人生物信息的安全隐忧

人脸识别（Face Recognition）又称面部识别，作为一种识别个人身份信息的新型技术，其主要特征是非接触性、主体唯一性和不易复制性，同时也具有无须携带、易于采集、成本低廉等特点。信息采集者只要通过设置普通摄像头等传感器，加上面部识别的软件和算法的运用，无须接触自然人个体便可实现面部信息的抓取与存储。

在不同的动态场景中，可以自动检测定位、跟踪采集、比对提取、分离存储个体的脸部特征信息，通过与数据库中已登记

[1]**作者简介**：张勇，华东政法大学刑事法学院教授、博士生导师。（上海 200042）
基金项目：国家社会科学基金一般项目“大数据背景下公民个人信息刑法保护体系研究”（19BFX074）

的面貌进行核实以确认自然人身份，或在数据库中搜索是否存在指定人像的完整流程。

目前，从出入境识别、违法行为曝光到刑事案件中的身份核查，从直销银行的人脸识别客户身份验证、3D 人脸识别解锁智能手机到移动端刷脸支付，人脸识别的应用范围越来越广。手机厂商推出的新一代手机中，刷脸解锁已经替代了指纹解锁，许多支付系统也纷纷采用人脸识别技术。

运用海量数据挖掘和神经网络技术的人脸识别系统已成为人工智能、区块链商业应用的新领域。我国工业与信息化部于 2019 年 9 月 27 日发布的《关于促进网络安全产业发展的指导意见(征求意见稿)》指出，国家支持构建基于人脸识别等识别技术的网络身份认证体系。

应当看到，个人生物识别信息需要结合信息网络技术才能形成，由此改变了个人生物信息的不可复制和不可变更的基本属性。人脸识别的非接触性特征也更容易产生个人信息侵权问题。人脸可以被模仿，“变脸”和“换脸”不存在什么技术困难。相对于其他个人信息，人脸识别应用的数据存储、传输流程存在严重的隐私侵权和安全受损风险；而一旦人脸识别信息被泄露或冒用，就可能会对信息主体造成永久性伤害和难以弥补的损失。

2018 年 4 月，美国 Facebook 公司因其开发使用的“面部印记”功能遭到消费者团体起诉，起诉书指控 Facebook 在未经同意的情况下定期进行照片扫描和生物特征匹配。同时，Facebook 还提供访问接口，允许微软、亚马逊和 Apple 等合作机构读取、发送和删除用户个人信息。[1]又如，当下新冠肺炎疫情肆虐全球，很多人居家隔离或工作，对 Zoom 和其他数字通信工具的需求剧增。但据媒体报道，美国公司 SpaceX 和 NASA 已禁止员工使用 Zoom 的视频会议应用程序，因其存在“严重的隐私和安全问题”。

在我国，个人生物识别信息数据被盗或过度滥用的问题层出不穷，引人关注的“刷屏”级换脸 APP“ZAO”经历了从爆红到爆黑的“昙花一现”。这一应用项目所采用的格式化用户协议存在过度攫取用户授权和单方强加用户义务的嫌疑，从而引起社会公众的普遍担忧。

又如，在设置了人脸识别摄像头的商场、车站等公共场所，消费者甚至不知道自己会被拍摄。公民个人的相关隐私权益无法得到有效保障。以人脸识别厕纸机为例，用户进入摄像头范围后就被“刷脸”，仅仅是为了防止其多用厕纸，至于人脸数据怎样被存储、是否能被删除、是否被用于其他用途等问题，该机器并没有进行任何说明，明显存在过度收集个人生物识别信息的问题。

从司法实践来看，国内涉及人脸识别侵权诉讼或刑事犯罪的案件也屡屡发生。例如，2019 年 10 月，浙江理工大学副教授郭兵因不同意杭州野生动物世界使用人脸识别对其进行用户认证而提起侵权诉讼，被称为“人脸识别第一案”；2020 年 11 月 20 日法院判决野生动物世界赔偿郭兵合同利益损失及交通费一千余元，删除原告办理指纹年卡时提交的包括照片在内的面部特征信息。[1]

又如，张某、余某等侵犯公民个人信息案，被告人张某等购买 2000 万条公民身份信息，使用软件将他人头像照片制作成 3D 头像，用以支付宝人脸识别认证、注册支付宝账号从而获取红包奖励，共获利 4 万元。[2]近年来，我国相关部门和机构颁布实施了诸多个人信息保护的国家行业标准，对于个人生物识别信息的收集和使用提出了具体合规标准。

2019 年 6 月 25 日，全国信息安全标准化技术委员会公布《信息技术安全技术生物特征识别信息的保护要求（征求意见稿）》（以下简称《生物识别信息保护要求（征求意见稿）》）；2020 年 3 月 6 日出台《信息安全技术个人信息安全规范》（以下简称《个人信息安全规范》），在 2017 年该规范文件旧版本的基础上，细化与完善了个人生物识别信息在收集、存储和共享三个方面的保护要求，对于人脸识别技术的合规使用具有重要的指引作用。

2020 年 11 月 27 日，工信部组织发布了《APP 收集使用个人信息最小必要评估规范人脸信息》团体标准（以下简称《APP 人脸信息规范》），明确了 APP 收集使用个人信息的“最小必要”原则，并对收集、存储、使用、删除人脸信息的行为进行了具体规范。须指出，作为国家行业标准的《个人信息安全规范》不是强制性法律标准，而是推荐性行业标准，因而对个人信息保护的要求也更加严格。

总的来看，我国有关个人信息安全的法律法规和行业规范多头迭出，但能够起到提纲挈领和体系协调作用的“个人信息保护法”尚未出台。相对于网络信息安全保障，在公民个人信息权益保护方面的立法显得尤为不足。上述行业规范能否作为认定侵犯公民个人信息犯罪的前置性规范，也是值得探讨的问题。

二、个人生物信息安全法益的法律保护

随着计算机科学与基因组技术的融合，个人生物识别信息从传统的“基因信息”和“遗传资源信息”脱离出来，已具有人体生物特征的计算机数据库、数据处理、基因序列信息、生物系统的计算机分析与软件设计等内涵。个人信息保护原则是个人生物识别信息利用的最起码规则，而对个人生物识别信息的权利属性和法益内容进行界定，是对其实施法律保护的逻辑前提。面对个人生物识别技术风险增大、违法犯罪趋于严重的态势，我国立法与司法应当在保护个人生物识别信息权利的基础上，以风险预防及利益平衡理念和原则为引导，对个人生物信息安全法益实行多层次、等级化和体系化的法律保护。

（一）个人生物识别信息的权利属性

《APP 人脸信息规范》第 3.1 条规定，“人脸识别”即基于个体的人脸特征，对个体进行识别的过程；第 3.3 条规定，“人脸信息”即对自然人的人脸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。

《生物识别信息保护要求（征求意见稿）》第 3.1.3 条规定，个人生物识别信息基本特征在于，可检测到的个体生理或行为特征，可以从其中提取可识别的、可重复的生物特征。第 3.1.9 条规定，生物特征识别属性即由生物测定样本估计或导出的生物特征数据对象的描述性属性。同时，第 4.1 条规定，个体生理特征包括但不限于指纹、人脸、虹膜、声纹、手型、指静脉/掌静脉、视网膜、DNA、掌纹等，个体行为特征则包括步态、签名、语音等。

个人生物特征识别系统包括数据采集、存储、注册、辨识、验证五个子系统，通常将个人生物特征识别的关联信息与其他个人信息绑定在一起，以保证包含生物识别信息记录在内的信息安全性。因此，所谓“生物识别”并非仅是对自然人生理特征的识别，而且将生物识别信息与个人身份、金融、行为、位置、偏好等信息对接，使得个人生物识别信息的法律属性具有更强的多元化、复杂化的特点。

从国外立法来看，欧盟《一般数据保护条例》（GDPR）、英国《数据保护法案》、日本《个人信息保护法》等法律法规都对“生物识别数据”做出专门规定。我国《网络安全法》规定，个人生物识别信息属于“直接可识别”到个人身份的隐私敏感信息，其必须经过计算机的相关生物识别程序的识别才能生成相关信息数据。

《个人信息安全规范》第 3.2 条规定，个人生物识别信息属于个人敏感信息，在收集信息授权同意、隐私政策制定、传输与存储、访问控制措施、目的限制、共享与转让、公开披露、应急处置和报告、数据控制者的义务与责任等方面，须以个人敏感信息的严格标准加以保护。

根据《生物识别信息保护要求（征求意见稿）》第 3.1.7 条的规定，个人生物识别信息所涉及的权利包括其在整个生命周期的收集、转移、使用、存储、归档、处置和更新的权利。从权利内容来看，个人生物识别信息权利包括知情权、同意权、查询权、更正权、删除权、利用权和公开权等权利。

我们将个人生物识别信息进一步分为可识别个体生物特征的个人隐私信息、一般个人信息和个人数据三种，其权利属性也有所差别。首先，一般个人信息具有人格权属性，可谓“信息主体人格的外在标志”。[2]但个人信息所蕴含的权利并不限于隐私权，后者则是其最重要、最核心的内容。

个人信息权的法律保护属于弱保护，而隐私权的法律保护则属于强保护，大多数一般个人信息不需要权利主体明示同意也可收集，但对于个人私密敏感信息不能仅仅通过知情同意权加以保护，对于个人生物识别信息应优先适用更为积极的隐私权保护。其次，个人隐私信息属于人格利益但不包含财产属性，不具有任何财产属性的交易价值，不可利用且受法律绝对保护。“人的自由与尊严价值不可动摇，互联网络时代亦如是。”[3]

再次，一般个人信息亦属于人格利益但可包含财产属性，这种人格利益基于信息主体的同意，转化为具体财产利益后，可以进行交易。不少数据企业采用“去识别化”或匿名化技术手段，对个人信息进行“脱敏”或“漂白”，使其成为普通的数据。

同样，个人生物识别信息经过去识别化技术处理之后，仅具有个人信息数据的财产属性，可以自由使用、转让，而为其他数据主体所利用。然而，随着再识别技术的发展，“匿名化”已变成一个相对的概念，完全不能复原的匿名化个人信息是比较少见的。[4]不过，通过去识别化信息技术，结合再识别的风险管理，“去识别化”仍然是数据企业合规收集、使用个人生物识别信息的有效途径。

（二）个人生物识别信息的安全法益

个人生物识别信息属于自然人固有的生理特征或行为特征，生物识别身份验证技术本身具有客观性、中立性，一般不具有违法性和可罚性；但正因为如此，反而更容易被不法分子利用法律漏洞进行不当收集或滥用。概括起来，生物识别技术带来的个人信息安全风险包括以下情形：未经授权的或不必要的收集；未经授权之使用或披露；不当比对；错误匹配；不当储存或不当传输；功能蠕变（creepfunction）等。[5]

在大数据背景下，个人生物信息安全越来越依赖技术保障，然而目前个人生物特征识别技术尚不够成熟，存在一定的技术缺陷和管理风险。同时，随着国际上生物资源数字序列信息的提取、跨境转移和利用，许多国家面临着所谓“生物数字盗版”的生物信息跨国传输问题。

一些发达国家通过多种途径集聚各类生物信息，进行生物信息资源的控制与争夺，而输出国遗传信息资源流失的风险不断增大，已经上升到公共安全和国家安全层面，人类遗传基因的生物信息资源已成为国际战略博弈的新领域。面对国际上愈加激烈的遗传基因资源控制与争夺态势，我国必须运用法律强制手段保障生物信息安全，防止生物信息资源流失。

从个人生物信息安全的法益属性来看，生物识别技术虽然以自然人为对象，但其涉及的社会利益关系不限于公民个体，而是包括与个人生物识别活动相关的技术服务者、经营者、使用者和管理者。即使是从公民个人权利角度，个人生物信息事关个人身份、隐私、人身、财产等各方面的利益与安全，已经不能仅仅用传统民法上的某种单一权利加以限定。

个人生物识别信息所蕴含的保护法益内容逐渐呈现出复合性、多元化特征，从个体的人格权扩展至公共利益、社会秩序和国家安全。对此，有学者提倡法律应着力保护“数据安全法益”，即数据的保密性、完整性和可用性的保护，维护数据在社会往来中的安全性和可信赖性。[6]

《数据安全法（草案）》第 3 条规定：“数据安全,是指通过采取必要措施,保障数据得到有效保护和合法利用,并持续处于安全状态的能力。”我国现行的《网络安全法》中有关个人信息保护的内容，也是着重从保障信息网络安全的角度做出的规定，该法对网络运营者提出的义务要求，就不仅仅是从个人信息权利保护的角度考虑的，而《网络安全法》作为《刑法》中侵犯公

民个人信息罪等相关罪名的前置性法律规范，其法益保护价值取向也必然反映在这些罪名的构成要件要素当中。

三、个人生物信息安全风险预防及利益平衡

个人生物识别信息的权利保护和价值利用是一枚硬币的两面，自由与安全的价值取向既是对立的，又统一于个人生物识别信息权利保护和价值利用的关系当中，两者缺一不可。在风险社会背景下，需要确立风险预防的理念，并以利益平衡原则为补充，作为构建个人生物信息安全保护法律体系的观念基础。

（一）个人生物信息安全的风险预防法律原则

作为一种法律理念，“风险预防”较早地出现在生态环境保护领域。当生态环境遇到严重的或不可逆转的损害或威胁时，即使不能在科学上找到明确证据证明某种行为必将产生实际危害，也应当采取法律防范措施以避免该行为的发生。[7]“风险预防”是相对于“损害预防”而言的，前者针对的“危害”具有不确定性、未然性，而后者的“损害”是指已现实存在或已产生客观损害结果，“不确定性”是风险预防的核心概念。

将风险预防原则确立为生物安全立法的基本原则，是由生物技术发展所带来的高风险性和严重危害性所决定的。就像 SARS、新冠病毒性肺炎疫情一样，一旦生物安全潜在风险转化为现实损害，与生态环境灾难一样无法逆转且危害严重。生物安全风险的不确定性、突发性及不可预测性要求相关法律法规要采取具有相对灵活性、开放性的立法模式，在预防和控制风险时留有法律操作的空间。确立生物安全保护的风险预防原则，用以指导生物安全立法和司法实践，是十分必要的，这也符合人类命运共同体的价值理念。

《生物识别信息保护要求（征求意见稿）》第 5.1 条针对“生物特征识别系统信息安全保护要求”提出了以下原则：

其一，保密性原则。在生物特征数据的存储和传输过程中，生物特征识别系统各部件之间的通信通道可能会被窃听、读取、插入或修改，而用户并不知道已建立的链接遭受了攻击。对此，应当使用 SM2 或 SM4 加密算法对信息数据进行保密处理，未经信息主体授权不得访问或披露；可以通过将生物特征参考存储在个人令牌或卡上进行数据分离，或使用仅身份管理系统的操作人员或数据主体可知的密钥对生物特征参考进行加密。

其二，完整性原则。生物特征识别系统应通过访问控制来实现数据的完整性保护，防止未经授权访问生物特征数据，或通过使用加密技术进行完整性检查。

其三，可更新性与可撤销性原则。根据该《生物识别信息保护要求（征求意见稿）》第 3.1.10 条规定，如果攻击者非法获取、泄露或未经授权访问生物特征参考样本、模板或模型，如护照上的面部图像、居民身份证上的指纹细节模板、数据库中用于识别说话人的高斯混合模型，就需要撤销和更新受侵害者的参考样本，并将合法的数据主体与新的生物特征参考样本联系起来。

在个人生物信息安全领域，生物识别技术的研发者、服务者、经营者和利用者违法违规收集和使用个人生物识别信息的行为，主要涉及侵犯公民个人信息罪及其他关联罪名。究竟是将法益性质界定为个人法益、公共法益还是国家法益，将直接决定或影响着刑法中相关罪名的认定和处刑轻重。

同时，对刑法中相关罪名的构成要件设置和司法认定，也需要依托前置性行政法律规范及行业标准，针对不同安全等级的个人生物信息识别行为，设定生物信息安全法益保护的命令性义务、禁止性规范及刑事责任，设置刑事风险防范的法律底线，侧重体现对于生物信息安全保护的特殊要求。

例如，个人生物识别信息的收集者、使用者在向信息主体征求授权同意时，应向其明确告知收集目的、处理方式、使用范围、再度披露规则等，并且在后续的二次使用中，仍需再次征求用户的明确授权。用户可以随时行使更正、删除和注销生物特征识别信息的权利，不需要任何前置条件即可当场实现与即时生效。

对于这些较为严格的生物信息安全保护的义务要求，司法机关在认定侵犯公民个人信息罪、拒不履行信息网络安全管理义务罪的时候，就可以作为认定前置性法律规范、进行刑事违法性判断的参考依据，这样才能够尽可能地防范生物信息安全风险，从根本上避免阻碍生物信息识别技术的创新发展。

（二）个人生物信息安全保护的利益平衡

在风险社会背景下，保障公共安全与保护个人隐私之间不是非此即彼的利益衡量问题，而是如何共生共存的利益协调问题。其实，公共安全与个人隐私之间并不存在实质冲突，个人隐私保护没有必要让步于公共安全保障，公共安全保障也不能以牺牲个人隐私为代价。[8]

有学者指出，在应用与开发个人信息数据过程中不仅应追求个体利益最大化，还要保证社会利益的最大化，为追求个体利益而牺牲社会利益的做法是无法持续发展的，这就需要在社会利益和个体利益之间创建一种利益平衡机制。确定个人信息数据的权利归属、实行权利与义务相匹配是实现个体利益与社会利益之间协调的前提基础。[9]

对于个人生物识别信息来说，法律同样面临着如何在保护和利用、自由与安全之间进行利益平衡和价值选择的问题。比较来说，在个人生物识别信息的商业使用方面，大多数欧美国家持谨慎态度。欧盟保护人脸识别数据的核心法律是《通用数据保护法规》（GDPR）。

根据 GDPR 的规定人脸识别技术的商业应用可适用的例外情形是数据主体已明确表示同意，“同意”的方式须“自由给予、明确、具体、不含混”，数据主体任何形式的被动同意均不符合规定。比较而言，我国对于个人生物识别技术的开发和应用持较为积极的态度。

然而，从利益平衡角度，应当分类分层地明确个人生物信息权利主体、生物识别技术的研发者、个人生物信息的收集者和使用者、生物信息安全的管理者等各方利益主体的权责关系，避免个人生物识别信息数据滥用。

对于人脸识别来说，其商业性应用与公共性应用应该有所区别，公共利益目的是隐私个体权利的抗辩事由之一，在一定情况下可以超越个体隐私权利以维护社会整体效率与安全，但人脸识别的商业应用则必须以个体隐私权利保护为前提。对于人脸识别信息来说，一般情况下不允许搜集者以“共享”或“开放平台”等方式进行利用，更不得未经用户事先授权和再次授权就进行转让使用。[10]

人脸识别技术应用同样涉及多个主体之间的合意以及权责分配等问题，需要受到公平正义价值的评价与约束。[11]个人生物识别信息的收集者、利用者和数据系统的管理者，也是借助个人生物信息安全风险的获利群体，应当作为风险义务和责任的主要承担者，法律应当对个人信息权利主体予以适当的倾斜保护，从实质上实现公正和利益平衡。

值得关注的是，区块链技术逐渐应用于生物信息商业领域，实现与生物识别技术的融合。如科创公司 Nebula Genomics 公司推出基于区块链技术的匿名 DNA 测序隐私功能，用户可以用加密货币购买全基因组测序并提交其样本，并允许用户自行处理测序信息。

有学者指出，区块链的核心价值在于“私密性、准确性和可验证性”[12]，与个人生物信息识别技术属性具有内在共通性。

因此，生物识别技术也被应用于区块链产品，以提高对用户的数字货币、私钥以及身份信息存储的安全性。如，HYPR 公司与比特币交易安全平台 BitGo 联合开发生物认证与区块链融合的新技术，客户通过 HYPR 的生物识别进行安全登陆，加上 BitGo 的多重签名技术，实现用户信息安全的双重保障。

不少国家政府机构开展了区块链身份验证项目，采用基于生物识别技术的认证机制，建立自主身份管理系统。须指出，区块链“去中心化”的特点天然排斥监管，但是如果缺乏必要的法律规范和政府监管，也会增加市场交易的风险。[13]在区块链产业化过程中，往往通过加密算法对账本的数据进行“哈希化”处理，将包含在交易记录中的个人信息以哈希值的形式体现，从而在区块链背景下实现了个人信息的匿名化，使其成为不具有可识别性的数据。

哈希函数具有单向和不可逆的特点，但哈希化技术含量和程度仍然存在逆转风险，并非不可破解，区块链业者面临着违规陷阱甚至刑事风险。为了避免给区块链产业发展带来不必要的障碍和困难，如果区块链业者在将个人信息记录到区块链上时运用匿名化技术手段，并切实履行了保护个人信息安全的合理义务，尽最大努力采取技术措施确保哈希化信息的匿名化，则该哈希化信息就不再属于法律意义上的个人信息。[14]

这样既保护了区块链背景下的个人信息安全，又避免给区块链产业带来过高的发展门槛和应用成本。对个人生物信息来说，这同样能够在个人生物信息权利保护和价值利用、生物信息安全风险防范和区块链产业发展之间取得利益平衡，值得肯定。

四、个人生物信息安全保护的立法模式

在生物安全领域，个人生物信息安全的法律保护一直受到国际社会的关注和重视，相关的专门性国际条约及行业标准主要是《生物多样性公约》《生物多样性公约卡塔赫纳生物安全议定书》《信息技术—安全技术—生物测定信息保护标准》等，其中也包含着人类基因信息保护和利用的规制内容。

在个人生物信息安全保护方面，美国和欧盟等发达国家立法相对比较完善。我国虽然制定实施了不少与个人生物信息有关的法律法规、部门规章以及行业标准等规范性文件，但仍缺少综合性、专门性立法，法律法规体系并不完善。以下予以比较研究。

（一）个人生物信息安全的私法保护

从国外立法来看，美国和欧盟等发达国家和地区出于保护本国遗传资源以及本国利益的考虑，对人体基因信息能否获得专利问题普遍持肯定态度，专利制度在生物信息法律保护方面居于很重要的地位。然而，因掣肘于专利权保护所造成的垄断，其立法首要目标并不在于安全价值的考虑，其所能发挥的作用当然也是有限的。

对于个人生物识别信息安全的保护仍然主要体现在个人隐私权、信息数据权利的民事法律保护方面。在我国，对个人生物识别信息的保护来自于民法、消费者权益保护法等法律法规中有关隐私权、名誉权的保护规定，以及个人信息保护的法律法规、行业规范。如《侵权责任法》第 2 条只是原则性、概括性地确认了隐私权的存在，对于生物识别信息的隐私法律保护而言显得尤为不足。

由于个人信息的财产价值难以估算，且以人格权为基础的财产赔偿数额也比较有限，侵犯个人生物识别信息的行为也很难通过《侵权责任法》的现有规定获得有效的赔偿。2020 年 5 月颁布的《中华人民共和国民法典》（以下简称《民法典》）人格权编第 799 条第 1 款对个人生物识别信息也提供了多重保护：一是可以受到肖像权的保护；二是采取偷拍偷录等方式采集个人生物识别信息构成对隐私权的侵害；三是除了肖像权、隐私权保护之外，还可以适用个人信息保护的规定。

值得注意的是，根据《民法典》第1036条的规定，合理处理自然人自行公开的或其他已经合法公开的信息，除该自然人明确拒绝或者处理该信息侵害其重大利益的之外，行为人不承担民事责任。据此，个人信息分为公开的个人信息和非公开的个人信息，公开的个人信息限于“合法公开”的个人信息，而不包括非法公开的个人信息。

而对于个人信息是否属于“合法公开”，行为人主观上是很难认识到的，在无法证明的情况下，只能按有利于被告的原则处理。[15]可见，即使在现有民法典框架之下，对个人生物识别信息的民事权利保护仍然是不足的，对于个人生物信息安全更难以直接给予保障和救济。

总体上，我国个人生物识别信息的民事权利保护模式主要有三种路径：人格权模式、财产权模式、人格权与财产权的复合模式。其一，人格权保护模式主张将个人生物识别信息视为具有人格权的基本属性，将其作为个人私密敏感信息进行保护。

其二，财产权保护模式认为，个人生物识别信息具备财产性质，应赋予其财产权保护，但其又不是完全的财产，因为它不能被继承、赠予、遗赠等，保护隐私最容易的途径是将个人信息的控制作为数据主体拥有的财产权。

其三，复合保护模式主张，将人体基因视为人格和财产的复合体，即把人体基因视为知识产品。还有学者提出，将人体基因及基因信息视为人格性财产权。[16]比较来看，首先，单纯的人格权模式无法对个人生物识别信息专利及商业化所带来的可分享的财产利益予以充分保护。

与传统的隐私权保护方法相比，隐私权是强调“不干涉”的权利，财产权则是一种积极的权利。通过财产权保护，个人生物识别信息所有权人能够拥有一系列权利包括控制、占有、转让。其次，对个人生物识别信息财产权益的承认并不与相关的人格权相矛盾。

承认个人生物识别信息的财产权属性，更有利于保护合法的相关信息交易，解决纠纷，保护信息主体的合法权益。再次，如果单纯采用财产权模式来界定个人基因信息的法律属性，则可能造成对人体基因信息的人格权属性的忽略，在否定其主体地位的同时，还可能会带来物化人格的风险。

须指出，相对于美国与欧盟来说，我国目前尚未形成具体明确的个人信息权利保护模式。无论对个人生物识别信息采取何种保护模式，现行民事立法都是从基本民事权利角度作出的粗线条规定，无法为特定场景下个人信息权利的保护确定具体规则。例如，在个人隐私政策中，相关企业机构在取得收集或使用公民个人信息的授权时，对于取得用户授权的行为方式是否妥当，能否产生取得授权的效力等，民事立法无法提供具体的判断标准。

笔者主张，我国应以人格权和财产权的双重机制对其予以保护，为平衡人格价值和科技进步、经济发展之间的冲突提供可行的通道。以人格权的保护机制确保供体对个人生物识别信息使用情况的控制和支配，以财产权的保护机制维护其对生物信息技术进步利益的合理分享。[17]

未来的个人生物信息保护立法应考虑到其商业性使用价值财产权的正当诉求，建立个人生物信息权利损害的民事诉讼救济机制，明确侵害个人生物识别信息权利的“损害”认定与赔偿标准，完善相关民事诉讼损害赔偿的举证原则与责任制度等。

（二）个人生物信息安全的公法保护

首先，在行政法领域，我国与个人生物信息安全相关的法律规范多散见于《网络安全法》《传染病防治法》《人类遗传资源管理条例》《基因工程安全管理办法》《人类辅助生殖技术管理办法》《涉及人的生物医学研究伦理审查办法》等法律法规、部委规章及专门规范文件。如《人类遗传资源管理条例》规定采集人类遗传资源信息须符合个人信息收集的一般法律要求，但并未

建立起与其敏感隐私特征相适应的特殊保护制度。

《个人信息安全规范》较为详细地规定了个人生物识别信息在收集、存储和共享等环节的安全保护要求。在涉及人脸识别、声纹识别等生物识别信息的项目，网络运营者须专门设计获得用户同意的环节，这也意味着当用户提起争议时，信息业者负有更多的举证责任。

《生物特征识别信息保护要求（征求意见稿）》第 5.1 条提出了生物特征识别系统的保密性、完整性、可更新性与可撤销性等方面的原则和具体要求；第 6.4 条也提出在生物特征识别信息生命周期管理中有关采集、传输、使用、存储、归档与数据备份、废弃阶段的义务要求，除非法律法规另有规定，否则在收集、访问、处理或修改、使用生物特征识别信息之前，有关组织应获得主体的同意；系统安全与隐私政策应保证存储、控制和处理过程中生物特征识别信息的安全等。

《APP 人脸信息规范》第 6.1 至 6.4 条详细规定了收集、存储、使用、删除个人信息过程中的“最小必要规范”。例如，其第 6.1.c）规定，收集人脸信息应遵循“最小必要”原则，收集前应通过隐私协议等方式向人脸信息主体告知相关信息，不应超过人脸信息主体“告知同意”的范围。上述国家行业标准和规范虽不具有法律效力，但能起到生物识别技术风险防范和合规性指导作用，也能为将来生物信息安全立法提供经验基础。

其次，在刑事法领域，由于个人基因信息技术发展所带来的人体试验、器官移植、辅助生殖技术、基因编辑及重组等问题日趋严重，不少国家对上述行为规定相关罪名予以刑事惩处。如，1994 年《法国刑法典》第六章明确规定了处罚基因泄露行为，对于 DNA 鉴定中侵犯他人个人基因隐私的行为进行刑事惩处。

在刑法典之外，不少国家的专门性立法中规定了刑事责任条款，如德国 1990 年的《胚胎保护法》、澳大利亚的《禁止克隆人法案 2002》和《基因技术法案 2000》、韩国的《生物安全与技术法》、日本的《克隆技术限制法》等。法国《公共卫生法典》中的《人体尊重法》规定人体及其生成物的不可转让性，禁止他们成为商业交易的对象，禁止代理胎儿，包括基因检查规则等。

如果违反了这些规则，将被判处 1 年至 7 年的监禁刑及 10 万法郎到 70 万法郎的罚金。德国《胚胎保护法》第 5 条第 1、2 项规定：“改变人类生殖系细胞遗传信息的，处以 5 年以下的自由刑或者罚金。将人为改变了的遗传信息的人体生殖细胞用于受精的，处相同刑罚。”美国 1998 年《防止身份盗窃及假冒法》规定，故意转移、使用生物识别信息用于违法活动的行为构成“身份盗窃”罪。

2003 年美国的《身份盗窃处罚增强法》进一步将非法“占有”识别他人的方法规定为“身份盗窃”罪。须指出，上述附属刑法规范均发挥着与刑法基本规范同样重要的定罪量刑作用，且更具灵活性、协调性，值得我国立法借鉴。我国于 2019 年制定出台了《人类遗传资源管理条例》，在“法律责任”一章规定了非法采集、保藏、利用、对外提供人类遗传资源的行政责任和刑事责任。

根据现行《刑法》的规定，我国可以将违反该条例规定的行为认定为犯罪，如将故意或过失泄露被列为国家秘密的基因资源、资料的行为认定为故意或过失泄露国家秘密罪，为境外窃取、刺探、售卖、非法提供国家秘密、情报罪等，但也有不少行为是刑法典中现有罪名无法涵盖的。从立法完善角度，我们可考虑以当前生物安全立法或修法为契机，通过制定或修订相关行政法律法规中的刑事责任条款，设置“非法利用胚胎罪”等罪名[18]，实现刑法与行政法规范的有效衔接，本文在此不赘述。

（三）个人生物信息安全的综合法律保护

目前，我国《个人信息保护法（草案）》在《民法典》基础上，建构了我国个人信息保护的单行法律框架。草案第 5 条、第 6 条分别规定了个人信息处理的方式和目的。第 5 条规定“处理个人信息应当采用合法、正当的方式”；第 6 条规定“处理个人

信息应当具有明确、合理的目的”。同时，该草案将“告知—同意”确立为信息处理的核心规则，告知义务是信息主体的主要义务。[3]

《数据安全法（草案）》第四章规定了数据安全保护义务，其中第 29 条规定，“任何组织、个人收集数据,必须采取合法、正当的方式,不得窃取或者以其他非法方式获取数据”，“应当在法律、行政法规规定的目的和范围内收集、使用数据,不得超过必要的限度”。然而，与国外立法相比，我国个人信息保护的法律法规相互之间有机协调不够，实施起来难免出现立法空白、规范冲突和不衔接等问题。[19]

个人生物信息保护法益的复合性、多元化，决定了仅靠私法保护模式或是公法保护模式均无法有效保障其安全，因而有必要对我国生物安全法律保护作出系统性的制度安排。从立法完善的角度，应当设定企业生物识别技术及其应用的行业标准、认证评价机制、安防制度以及许可制度，明确规定个人生物信息识别的禁止性与限定性规范、个人生物信息权的基本内容，以及互联网企业在采集、存储、使用、传输、保管、披露、销毁个人生物识别信息中的法律义务和责任等。

同时，我国还需要通过立法设置国家层面的数据保护监管机构，并于地方设置下级机构，明确监管机构对各种实体数据处理行为的审查权、许可权、调查权、检查权、命令权和司法介入权，以及纠纷调处权，受理控诉、申诉权，以保证实现个人生物信息安全管理的目标。

在此方面，2020 年 10 月颁布的《中华人民共和国生物安全法》作为一部综合性立法，应当能够适应我国生物多样性保护和生物安全保障的制度需求。[20]在该法的统领和协调下，其他各专门法、单行法具体设置应对生物信息安全风险的法律规则，处理好行政法、民法、刑法等相关法律法规之间的关系，从公法和私法的不同层面进行法律保护，构建个人生物信息安全保护的法律体系。

五、个人生物信息安全法律保护的体系化

在个人生物信息安全保护的法律法规体系中，刑法规范也是其中的重要的子系统。由于生物信息安全法益属性具有复合性、复杂性、间接性和多变性的特点，刑法不可能靠一己之力遏制危害生物安全的违法犯罪。刑法作为法律体系中的保障法，其与民法和行政法之间具有紧密的关联性和从属性。

因此，立法机关应当将相关违法犯罪行为放置在整个生物信息安全保护的法律体系之中加以考量，保证刑法规范适用的统一性和协调性。以下主要讨论个人生物信息安全领域的刑法前置规范、附属刑法规范两个问题，从中寻求相关行政立法、行业规范与刑法规范之间的衔接，协调问题的解决路径。

首先，在我国刑法中，与个人生物信息安全保护相关的罪名包括：侵犯公民个人信息罪、拒不履行信息安全管理义务罪、非法侵入和破坏计算机系统罪、假冒专利罪、非法经营罪、妨害传染病防治罪、非法行医罪、故意或过失泄露国家秘密罪等。上述罪名或多或少、直接或间接地涉及个人生物信息安全法益的保护。同时，在上述罪名中，存在大量的“违反国家规定”“违反……管理规定”“违反……法规”等空白罪状，对此，行政法律法规、部门规章及行业规范文件成为填补空白罪状的根据。

判断行为刑事违法性以行为人违反前置性法律法规为前提，对于行政法律法规及行业规范中的违法违规行为，需要进行违法性的层次性判断，即“出行入刑”，形成刑行关系的衔接协调。然而，我国行政法律法规带有很强的部门立法特点，存在委托立法和行业立法现象和问题，不少行政法律法规关注部门利益和行业保护，法律体系的观念意识不强；加上各部门法的立法修法时间不一致，立法过程往往比较仓促，欠缺系统性的通盘考虑；在制定行政立法中的刑事责任条款时缺乏对既有刑法规范的充分研究，没有顾及或疏忽了刑法的相关规定，缺乏整体立法的协调性，导致刑法与行政法之间出现不衔接，甚至互相冲突的问题，因而需要通过构建和完善刑法前置性行政法律规范这个制度链接点加以解决。

其次，根据《网络安全法》的规定，网络服务经营者在运用生物识别技术收集个人信息时，原则上应经过被收集者同意，并遵循合法、正当、必要的原则。在此情况下，我国《个人信息安全规范》等相关行业标准指南提供了立法框架样本。

（1）个人生物识别信息的收集。《个人信息安全规范》第 5.4 条规定，网络运营者收集个人生物识别信息应征得个人信息主体的明示同意。即使已取得个人信息主体的同意，网络运营者仍应仅收集达到目的所需的最少个人生物识别信息，以最大限度降低损害风险。

（2）个人生物识别信息的存储。2020 年《个人信息安全规范》第 6.3 条规定，可采取的存储措施包括但不限于：仅存储个人生物识别信息的摘要信息，且该摘要信息应具备不可逆性，即无法回溯至原始信息；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；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。网络运营者应将个人生物识别信息与个人身份信息分开存储，同时，还需将这两者的控制权限分配给不同的操作人员，以实现分隔效果。

（3）对个人金融信息特定类别的特殊要求。根据《个人信息安全规范》第 9.2 条规定，网络运营者确因业务需要，确需共享、转让的，应单独向个人信息主体告知目的并征得其明示同意、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等。可见，《个人信息安全规范》以“不应共享、转让”为原则，只有当出现业务需要或满足“告知同意”要求的例外情形时，网络运营者方可进行个人生物识别信息的共享或转让，且应当采取加密安全措施或进行安全评估。

上述推荐性国家标准，在立法过程中均可有选择性地纳入法律规制中。另须指出，行业规范并不具有法律效力，对个人生物识别信息的规制范围更广，安全义务要求更高；而刑法是从惩治犯罪活动角度出发，所规制的入罪门槛必须是个人生物识别信息保护的“最低安全基线”。为了避免刑事打击范围过大，刑法应将个人生物信息安全行业规范作为前置性规范的参考依据，但不宜直接将其作为判断刑事违法性、认定犯罪的法律根据。

六、结语

个人生物信息法益的多元属性涵盖了其对隐私权、人格权、财产权及安全法益的保护，决定了其合理使用和权利保护的多元价值。在生物安全风险因素和潜在威胁因素突发、增升的情况下，追求公共安全成为国家和社会公众的普遍心态和立法目标选择。应当看到，我国个人信息安全保护立法存在“碎片化”和规范冲突问题，这是由于对个人生物识别信息的权利属性界定模糊不清，加上不同部门法的立法价值目标存在差异所致。

可以说，“碎片化”是一种立法常态，虽然会对法律体系造成一定冲突，但没有破坏法律体系的整体性及适用效力。不同的部门法各有其调整对象和范围，相互之间存在交叉竞合、冲突矛盾的情况在所难免。单一的民法、行政法或刑法无法完成多元化价值目标的实现，特别是刑法居于后盾法、保障法地位，若将其作为“急先锋”和“主力军”来抗制生物识别技术带来的安全风险，非但不能实现个人生物信息安全法益保护，反而会丧失个体权利的保障功能。

总之，我国需要以网络安全法、生物安全法、个人信息保护法、数据安全法等综合性立法为契机，构建个人生物识别信息安全保护的法律体系，发挥各个部门法在保护权利和保障安全方面的功能，实现行政立法与刑法规范的良性互动、附属刑法规范的实质化，以促进个人生物信息安全法律法规内外部的衔接协调。

参考文献：

[1]张欢,文铭,汪友海.从 Facebook 数据滥用事件谈个人信息法律保护[J].重庆邮电大学学报 2018,(6).

[2]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).

[3]彭诚信.数据利用的根本矛盾何以消除——基于隐私、信息与数据的法理厘清[J].探索与争鸣,2020,(2).

[4]Paul Ohm.Broken Promises of Privacy.UCLA Law Review,2010,Vol.57.

[5]朱工宇.生物识别与隐私权保护之法律冲突及其协调[J].科技与法律,2009,(6).

[6]杨志琼.我国数据犯罪的司法困境与出路:以数据安全法益为中心[J].环球法律评论 2019,(6).

[7]柯坚.论生物安全法律保护的风险防范原则[J].法学杂志,2001,(3).

[8]刘艳红.公共空间运用大规模监控的法理逻辑及限度——基于个人信息有序共享之视角[J].法学论坛,2020,(2).

[9]李爱君.论数据权利归属与取得[J].西北工业大学学报(社会科学版),2020,(1).

[10]朱巍.人脸识别的法律性质认定[N].检察日报,2019-11-06(7).

[11]李怀瑾.人脸识别技术风险的法律防范[N].中国社会科学报,2019-03-06(5).

[12]郑戈.区块链与未来法治[J].东方法学,2018,(3).

[13]赵磊,石佳.依法治链:区块链的技术应用与法律监管[J].法律适用,2020,(3).

[14]罗勇.特定识别与容易比照:区块链背景下的个人信息法律界定[J].学习与探索,2020,(3).

[15]喻海松.民法典视域下侵犯公民个人信息罪的司法适用[J].北京航空航天大学学报(社会科学版),2020,(6).

[16]刘红臻.人体基因财产权研究——“人格性财产权”的证成与施用[J].法制与社会发展 2010,(2).

[17]刘越.论生物识别信息的财产权保护[J].法商研究,2016,(6).

[18]刘长秋.生命科技犯罪的发展趋向及其法律对策研究[J].北京政法职业学院学报,2012(1).

[19]程啸.加强个人生物识别信息法律保护[N].光明日报,2020-01-04(07).

[20]常纪文.加快构建国家生物安全法律法规体系[N].学习时报,2020-02-17(01).

注释:

1 参见浙江省杭州市富阳区人民法院（2019）浙 0111 民初 6971 号民事判决书。

2 参见浙江省衢州市中级人民法院（2019）浙 08 刑终 333 号刑事判决书。类似案例还有福建省厦门市思明区人民法院（2019）

闽 0203 刑初 890 号刑事判决书、福建省厦门市中级人民法院（2019）闽 02 刑终 749 号刑事裁定书。

3 参见《关于〈中华人民共和国个人信息保护法（草案）〉的说明》（2020 年 10 月 13 日）。