重庆大学学报(社会科学版) 2023年第29卷第3期
JOURNAL OF CHONGQING UNIVERSITY(Social Science Edition) Vol. 29 No. 3 2023

Doi:10. 11835/j. issn. 1008-5831. fx. 2021. 12. 001

欢迎按以下格式引用:焦艳玲. 个人生物识别信息的界定[J]. 重庆大学学报(社会科学版),2023(3):200-211. Doi:10. 11835/j. issn. 1008-5831. fx. 2021. 12. 001.

Citation Format: JIAO Yanling. The definition of personal biometric information[J]. Journal of Chongqing University (Social Science Edition), 2023(3):200-211. Doi:10. 11835/ j. issn. 1008-5831. fx. 2021. 12. 001.

个人生物识别信息的界定

焦艳玲

(天津师范大学 法学院,天津 300387)

摘要:生物识别信息是对自然人的生物特征进行特定技术处理所形成的信息。个人生物特征具有不变性和唯一性的特点,这使生物识别能够一劳永逸地实现对个人身份的鉴别。经过特定技术处理所形成的生物识别信息也具有这些特点,因此任何对于生物识别信息的攻击都可能对个人产生不可逆转的影响。现实生活中,商业化收集的泛滥、限制行动自由、售卖和窃取、深度伪造以及诈骗已经成为侵害生物识别信息的重要表现。保护个人生物识别信息安全迫在眉睫,而准确界定生物识别信息是首要前提。综观国外立法经验,生物识别信息的构成应当聚焦三个要素:个人生物特征之反映、特定技术处理之环节、唯一性识别之功能。此三项要素也是认定生物识别信息的关键。生物识别信息可以通过含有个人生物特征的图像来采集,但是该图像仅仅是个人生物特征的反映。在没有进行特定技术处理之前,图像本身并不构成生物识别信息,无论该图像是电子图像抑或纸质照片。生物识别信息的本质是对个人生物特征进行的测量,即所谓的"特定技术处理",至于测量的方式则在所不问。无论进行面对面的真人测量抑或从含有个人生物特征的图像中测量,所得的信息都是生物识别信息。单纯对于个人生物特征的描述不构成生物识别信息,个人生物特征的样本也须与生物识别信息区分开来。目前我国法律文件对于生物识别信息定义的认识还存在许多偏差,概念混淆、内涵不明、外延短缺是主要问题。未来我国的生物识别信息定义应当遵循三个原则:揭示生物识别信息的本质、反映生物识别信息的要素、兼顾技术更新的速度。为此有必要从内涵和外延两方面着手:内涵规定本质与构成,从而为技术更迭可能出现的新情况提供解释的空间;外延进行开放式列举,以引导当下的理论与实践。就内涵而言,可概括为"对自然人的生物特征进行特定技术处理(测量)所形成的能够唯一性识别自然人身份的信息"。就外延而言,可以进行常态化列举,同时使用"包括但不限于"的表述使生物识别信息的范围不受列举的限制。

关键词:生物识别信息;个人生物特征;生物特征样本;生物特征测量;个人信息保护

中图分类号:TP391. 41;D923 **文献标志码**:A **文章编号**:1008-5831(2023)03-0200-12

基金项目:2021年度天津市哲学社会科学规划项目"个人生物识别信息的民法保护"(20BFX163)

作者简介:焦艳玲,天津师范大学法学院教授,Email:cn_lily@ 163. com。

一、缘起:数字时代的生物识别信息危机

生物识别普及化应用的速度令人惊叹。声纹控制、指纹解锁、人脸支付,一系列生物识别的应用以铺天盖地之势袭来,住宅小区、职场、图书馆、公园、机场、车站,一时间生物识别无处不在[1]。生物识别就像一个巨大的宝藏,其价值令人垂涎,其风险令人生畏。

生物识别是利用人体固有的生物特征对个人身份进行鉴别的技术。在以数字技术作为运算规则的当代,个人的生物特征经过计算机程序的处理变身为一串代码,这些代码成为生物识别信息最常见的形态。代码化的生物识别信息可以用来对个人的行为进行实时查询和验证,因此常被冠以“个人数字身份”的称谓[2]。个人的生物特征转变为有价值的社会资源正是通过这种数字化的进程实现的,而无论个人是否接受,这种趋势都不会改变[3]。有观点认为,生物识别将推动身份认证领域的一场革命[4]。因为生物识别信息安全、可靠又便捷,任何传统的身份认证方式都无法比拟[5]。但不容忽视的是,代码化了的生物识别信息极易遭受侵害,损害后果比其他个人信息严重得多。现实中生物识别的应用场景多种多样,诱发的个人信息保护风险形态各异。

第一,生物识别信息商业化收集的泛滥。目前我国尚无对生物识别信息收集和使用的禁止性规定,商业公司为了分得市场的一杯羹,对生物识别信息的收集和利用充满了热情。2019 年换脸软件“ZAO”受到手机用户的疯狂追捧,当用户享受与影视剧偶像同台飙戏的快乐时,其人脸信息已被软件公司永久性占有。软件公司在用户协议中载明“同意 ZAO 及其关联公司和用户对用户内容进行永久免费、不可撤销地修改与编辑”,这样的协议充斥着霸王条款的味道,即使形式上取得了用户的同意,又能在多大程度上反映用户的真意[6]?

第二,对抗生物识别的人格自由困境。生物识别已然成为信息社会下难以抗拒的洪流,以个人之力对抗这股洪流常常会遭遇人格自由的困境,乃至于在现实世界中寸步难行。一个典型的场景是将生物识别应用于门禁,当住宅小区、职场、公园等场所安装了生物识别系统,其结果是个人若不同意交出生物识别信息就无法正常生活。2019 年郭冰因杭州野生动物世界强制用户使用人脸识别入园诉至杭州富阳区法院,这个被称为“人脸识别第一案”的事件才第一次引起了国人对于生物识别应用边界的思考[7]。

第三,深度伪造。深度伪造(deepfake)俗称“换脸”,实质上是通过生物识别技术实现移花接木。在国外,利用人脸信息进行深度伪造进而嫁接于不雅视频以羞辱他人的行为已经拥有了专门的称谓“色情报复”[8]。由于受害人没有真实地出现在视频里,并且人脸信息多从受害人自愿上传到网络的照片中提取,深度伪造很难成立隐私侵权和肖像侵权,但是它对于受害人名誉的破坏却现实存在。

第四,生物识别信息的售卖和窃取。生物识别信息由于强大的身份识别功能而具有巨大的商业利用价值,对于饥渴寻找潜在客户的商家而言无疑是一笔巨大的财富,在此背景下买卖生物识别信息成为一桩生意就不难理解了。北京青年报曾曝出网络商城中有人售卖人脸信息,2 000 多人的 17 万条信息被公开叫卖,每个人都有 50 张以上的照片,每张照片配套一份数据文件,内容涵盖人脸的 106 处关键点[9]。除故意售卖以外,个人生物识别信息遭黑客窃取在国内外亦不罕见。

第五,生物识别信息泄露诱发财产诈骗。生物识别具有便携、保密、安全和不被遗忘的多重优势,随着技术成本的下降,生物识别的应用场景越来越多元化。目前手机应用、智能家居、智能安防

和互联网金融已成为生物识别技术应用的核心领域[10]。然而当人们不断让渡个人信息以换取生活的便利时,信息泄露和被滥用的风险亦成倍增加。2020年张富等人利用软件将他人照片制作成3D头像,进而通过人脸识别认证骗取他人支付宝钱财,被衢州市中级人民法院判决成立侵犯公民个人信息罪和诈骗罪①。在商业应用比较成熟的人脸识别领域,近年来发生的刑事案件逐年增多,就2017至2019年法院审结的案件有16件,其中仅2019年就有11件[11]。

不少学者认识到,生物识别信息的安全风险以自然人为对象,但涉及的利益关系涵盖了生物识别活动的服务者、经营者、管理者、使用者甚至国家[12]。党的二十大报告提出,加强个人信息保护是推进国家安全体系和能力现代化、维护国家安全和社会稳定的重要方面。而加强对生物识别信息的保护则是当前最突出的任务。随着《民法典》和《个人信息保护法》对个人生物识别信息的确认,主张建立民事、行政、刑事多元协调保护机制的建议获得广泛支持[13],而以专门法律或者在《个人信息保护法》中增设专章进行保护的建议也不在少数[14]。然而目前法律仅仅提到一个抽象的概念,什么是生物识别信息,其包括哪些类型,具体又该如何认定,这些问题尚不清晰。对于"生物识别信息"这个富含科技色彩的词汇,大众的理解仍然停留在感性层面。为避免认识偏差和法律适用的混乱,有必要对生物识别信息进行清晰界定,这是加强生物识别信息保护的首要前提。

二、生物识别信息的构成:域外立法的启示

(一)生物识别的基本原理

肖像权于照相机发明后始受重视,声音权因窃听器和录像机的使用而被认可[15]。个人生物信息作为人格标识受到关注,是基于生物识别技术的迅猛发展。生物识别又称生物特征识别,是利用人体固有的生物特征对个人身份进行鉴别,它有两种工作模式:其一为认证,即在有怀疑对象的前提下将某人与怀疑对象直接比对,从而回答"是他么"的疑问;其二为识别,即从庞大的数据库中找到与某人最为匹配的身份,以此解决"他是谁"的困惑[16]。从生物识别技术的发展历程看,早期生物识别的工作模式主要是认证,例如将指纹、签名的检材和样本进行比对和分析,以此来验证某人是否具有特定的身份。由于是一对一的比较,工作量小,针对性强,所以采用人工方式即可进行。可是随着计算机技术的发展,海量生物信息的收集和存储已成为可能,生物识别的工作模式渐渐转向了识别。特别是计算机技术与光学、声学、医学、生物传感器技术、生物统计学原理相结合之后,一系列新型的生物识别如人脸识别、视网膜识别、基因识别不断涌现,以往的人工识别也被计算机自动识别所取代。

生物识别之所以能够鉴别身份,与个人的生物特征密不可分。个人生物特征是个人所固有的生理特征和行为特征,其最显著的特点是具有不变性:要么难以改变,要么不能改变。恒久不变的特点实现了人工智能对生命体识别的一劳永逸,这正是生物识别能够鉴别个人身份的根源[17]。当然,并非所有的生物特征都能鉴别身份,可以在技术上推广使用的生物识别方法要求某项生物特征必须满足:(1)普遍性(每个人都有);(2)唯一性(至少在某一方面任何人都不同);(3)可测量性;(4)可收集性;(5)可重复性。目前可以用来鉴别身份的生物特征包括生理特征和行为特征,前者主要是指纹特征、人脸特征、虹膜特征、声纹特征、手型特征、指静脉和掌静脉特征、视网膜特征、DNA

①参见:衢州市中级人民法院(2019)浙08刑终333号刑事裁定书。

特征、掌纹特征等,后者则涉及签名特征、步态特征、语音特征和击键方式等。生物特征是生物识别的基石,它的不变性和唯一性为生物识别应用提供了坚实的保障,而在此基础上形成的生物识别信息也具有上述特性,故任何对于生物识别信息的攻击都可能对个人产生不可逆转的影响。

(二)生物识别信息的核心要素

在世界范围内,生物识别信息并没有统一的定义,各国采用的称谓也不尽相同,不过定义之间存在一些共性,从中或可尝试提取生物识别信息的核心要素。

欧盟的《通用数据保护条例》(简称 GDPR)将能够唯一识别自然人身份的生物特征数据列入"特殊类别的个人数据",原则上禁止对该信息进行任何形式的处理。根据 GDPR 的规定,"生物特征数据"是指自然人的身体、生理或者行为特征在经过特定技术处理后所产生的个人数据,该数据能够确认自然人的独特身份,例如面部图像的数据或者指纹数据。欧盟立法对许多国家产生了影响,英国的《数据保护法》采用了与 GDPR 相似的规定,该法第 205 条对"生物特征数据"的定义是:对个体的身体、生理或者行为特性进行特定技术处理所产生的个人数据,这些数据可以唯一地识别个人的身份,例如面部图像或者指纹数据。印度的《个人数据保护法》第 3 条也采用了"生物特征数据"的称谓,其定义是:对数据主体的身体、生理、行为特征进行测量或者技术处理所产生的面部图像、指纹、虹膜扫描或者任何其他类似的个人数据,这些数据能够唯一地确认自然人身份。

在美国,越来越多的民众意识到自己的生物识别信息正在遭受政府过度监控、黑客攻击和商业公司行为异化带来的风险[18]。尽管联邦政府尚未出台生物识别信息的专门立法,但是许多州加紧了对生物识别信息的保护。康涅狄格、爱荷华、内布拉斯加、北卡罗来纳等州已在数据安全通知的法律中通过扩大个人信息的范围实现了对生物特征数据收集行为的规范[19]。伊利诺伊、德克萨斯、华盛顿各州则制定了生物识别信息的专门立法来限制和规范私人实体收集、使用生物识别信息的行为。伊利诺伊州的《生物信息隐私法》(简称 BIPA)于 2008 年生效,该法对于"生物识别信息"的定义是:能够识别个人身份的生物特征标识的任何信息,无论它如何被取得、转换、存储或者共享。至于定义中的"生物特征标识",BIPA 的解释包括视网膜或虹膜扫描,指纹、声纹、手部或面部几何结构的扫描,但是书写样本、书面签名、照片、用于有效科学检测或筛选的人类生物样本、人口数据、纹身描述或诸如身高、体重、头发颜色或眼睛颜色等物理描述不在此列。根据 BIPA 的规定,生物特征标识与生物识别信息是两个高度关联的概念,被生物特征标识的定义所排除的项目将不构成生物识别信息。两个概念的外延高度一致,为什么还要区分它们呢?一个非常重要的理由是"防止规避法律"。生物特征标识与生物识别信息的根本区别在于,前者是对生物特征的测量,后者是将这些测量结果转换为可以使用的形式。如果单一使用生物特征标识的概念,难免私人实体会将生物特征标识转换为其他形式(例如数学表达式),从而规避 BIPA 法案的适用。有了生物识别信息的概念后,无论私人实体将生物特征标识转换为何种形式的信息,只要这些信息可用来识别个人身份,那么,它均可以受 BIPA 的保护②。此外,加利福尼亚州也从消费者保护法的角度对生物识别信息给予了关注。该州的《消费者隐私法》第 1798.140(b)条对"生物识别信息"的界定是:个人的生理、生物和行为特征包括个人脱氧核糖核酸(DNA)的数据,这些数据可以单独、合并或者与其他身份识别

②LINDABEHT RIVERA and JOSEPH WEISS, on behalf of themselves and all others similarly situated, Plaintiffs, v. Google Inc., Defendant. United States District Court, N. D. Illinois, Eastern Division. 238 F. Supp. 3d 1088.

数据一起使用以建立个人身份。生物识别信息包括但不限于从虹膜、视网膜、指纹、脸部、手掌、静脉的图像和语音记录中所提取的识别模板(例如面部印记、细节模板或者声纹),以及包含可以识别身份的点击模式或节奏、步态模式或节奏,以及睡眠、健康或运动数据。

综观各国立法上的定义,无论从个人信息的角度进行阐释(如欧盟、英国、印度),抑或从隐私的角度进行界定(如美国),各国对于生物识别信息本质的认识基本一致:(1)个人生物特征的反映。生物识别信息是个人生物特征的抽象表现形式,能够表征和反映个人生物特征的独有特点。(2)特定技术处理的环节。生物识别信息是对个人生物特征进行特定技术处理所获得的信息。常见的技术处理是借助计算机程序对个人生物特征进行几何扫描、计算和模板建构,即所谓的个人生物特征的测量。只有经过特定技术处理,才能形成反映个人生物特征的虚拟数据。因此,"特定技术处理"是连接个人生物特征与生物识别信息的纽带,其承担着转换器的功能,若没有经过这一环节则不会产生生物识别信息[20]。(3)唯一识别的功能。生物识别信息是可以唯一性识别个人身份的信息。表征个人生物特征的信息通常储存于数据库或者特定介质中,其中能够唯一性识别个人身份的信息才是生物识别信息。若不能做到唯一性识别,则此类信息便没有太多法律保护的必要。"唯一性识别"最能反映生物识别信息与其他个人信息的差别,也最能说明生物识别信息应受法律保护的根源——当该信息遭到泄露、盗用或者违反预期目的而使用时,不可能通过重新设置来更改,个人将永久性丧失自我身份,并间接引起人格和财产利益的重大损失。

三、生物识别信息的认定:美国司法审判的经验

生物识别信息的商业使用已成为当前各国重要的经济增长点,然而为了保护信息主体的自由与安全,法律为信息控制者设定了一系列禁止性义务③。为避免被划入信息控制者的范畴从而承担强制性义务,许多企业对生物识别信息作出新颖之解读。以常见的人脸识别案件为例,被诉侵权者最常提出的反驳是——被告仅仅收集了原告的面部图像,并未处理原告的生物识别信息,且图像为原告自愿公开披露。涵盖了生物特征的图像是否是生物识别信息?自愿公开披露该图像是否意味着同意他人收集和使用自己的生物识别信息?这些问题成为困扰法官的难题。美国伊利诺伊州作为世界上最早制定生物识别信息专门立法的地区,自BIPA颁布以来至少已有110起针对私人实体提出的违法诉讼[21]。这些私人实体大多是拥有尖端生物识别技术的科技公司或者是通过指纹识别等生物识别方式进行员工管理的雇主[22]。在这些诉讼中,私人实体是否涉及对个人生物识别信息的处理,更确切地说,生物识别信息应当如何认定,成为案件审理不得不跨越的障碍。

(一)图像是否构成生物识别信息的争论

生物识别信息可以通过含有生物特征的图像来采集,例如人脸、指纹、掌纹和虹膜的影像。不过获取图像只是信息采集的第一步,接下来还要进行许多维度的测量。以人脸识别为例,采集者在获取人脸的图像后需要测量面孔各个节点的特征,例如两眼之间的距离、鼻子的宽度、眼窝的深度、颧骨、下颌轮廓和下颚等,最后获得一串可以代表这些特征的数字代码,这串数字代码即为生物识别信息。由于识别系统的不同和测量节点的差异,人脸特征在不同数据库中呈现出的数字表达也

③美国伊利诺伊州规定私人实体处理生物识别信息必须负担书面告知的义务、取得书面同意的义务、禁止出售和出租以获取利益的义务、禁止披露和传播的义务,以及妥善储存和传输的义务(参见BIPA第15条)。

不相同,但是这些数字表达的源头——人脸图像可能是相同的。那么,收集、储存、使用人脸图像是否就是在处理生物识别信息?

2016 年,全球最大的社交网络公司脸书公司因使用面部识别软件在用户上传的照片中显示头像的人名引发用户集体诉讼。这项所谓"标签建议"服务的基本步骤是:首先扫描用户上传的照片,然后识别照片中出现的面孔,如果程序识别出面孔的主人,就会提示该人的名字或者自动为面孔添加姓名标签。三名用户对脸书公司提起了诉讼。他们主张,脸书公司利用先进的面部识别技术,在未经用户同意的情况下从用户上传的照片中秘密收集了用户的生物识别信息,其行为构成了对权利的侵犯。三用户认为,脸书公司至少在四个方面违反了 BIPA 的规定:(1)没有书面告知用户他们的生物识别信息正在被生成、收集和储存;(2)没有书面告知用户生物识别信息被收集、储存、使用的目的和时间;(3)没有公开提供保留生物识别信息的期限和销毁的期限;(4)没有获得用户的书面同意。面对以上指控,脸书公司从生物识别信息的定义入手提出了反驳。其援引了 BIPA 对"生物识别信息"的除外规定——"被生物特征标识的定义所排除的项目的信息不是生物识别信息",然后又援引了 BIPA 对"生物特征标识"的除外规定——"书写样本、书面签名、照片、用于有效的科学检测或筛选的人类生物样本、人口数据、纹身描述或者诸如身高、体重、头发颜色或眼睛颜色等物理描述不在此列",最后得出结论:照片和从照片中衍生的信息被明确排除在生物特征标识和生物识别信息之外,因此不受 BIPA 的保护④。

对照片性质的认定直接影响到案件的判决,但是解决这一问题着实棘手:照片的确不在 BIPA 的保护范围;但是,脸书公司取得的面部特征数据确实从照片中来。若对 BIPA 的规定进行纯粹字面上的解释,原告极有可能败诉,而这样的结果与 BIPA 的立法意图明显背离,因为伊利诺伊州制定 BIPA 的初衷就是为了解决新兴的生物识别技术对民众隐私的侵犯。审理该案的法院非常清醒地认识到这一点,于是放弃了单纯的文本解释,改采目的解释、体系解释、历史解释的多元方法以求对 BIPA 规定的深入理解。法院认为,法律条文必须置于整体背景下审读,对其含义的理解应当考察其他相关规定,并考虑条文在整个法律中的地位。就如 BIPA 将照片排除在外一样,这里的"照片"更应当被理解为纸质印刷品,而非储存于电脑文件或者上传到互联网的数字化图像。因为从体系上看,与照片一同被排除的还有"书写样本、书面签名、人类生物样本、人口统计数据、纹身描述和身体描述",它们与照片一样都是非数字化的物理标识。因此,将照片绝对排除在 BIPA 的保护范围之外是不恰当的,这样做只会削弱 BIPA 的效力④。

本案法院尽管驳回了被告提出的"照片不受保护"的主张,却没有承认从照片中衍生的信息就是生物识别信息。按照法院的逻辑,纸质印刷品的照片确实不涉及生物特征标识和生物识别信息,但是以数字化形式呈现的图像则可能是生物特征标识和生物识别信息的重要来源,所以一概将照片排除在 BIPA 的保护范围是不恰当的。美国法院超出法律文本之字面对"照片"一词重新解释的做法,深刻反映了生物识别技术快速发展给社会认识带来的变化。BIPA 颁布于 2008 年,当时的照片以纸质印刷品为主,即便储存了数字化图像,凭借当时刚刚起步的生物识别技术,也不足以从数字图像中提取生物特征标识。在伊利诺伊州,生物识别信息纠纷大多发生于 2015 年之后,被告则大

④185 F. Supp. 3d 1155, United States District Court, N. D. California. In Re Facebook Biometric Information Privacy Litigation. Case No. 15-cv-03747-JD, Signed May 5, 2016.

多是尖端的生物识别技术公司,这些事实表明生物识别信息纠纷是随着生物识别技术的发展产生的,而BIPA的规定一定会落后于快速变化的社会生活,因此对于BIPA条文的解释必须跟上现实需要。脸书案判决的意义在于澄清了“单纯的图像不能作为生物识别信息而受保护”,但是法院的说理仍然不能从根本上回答原告怎样的利益受到了侵害,尤其在当下纸质印刷品的照片与数字化的图像早已实现了相互的自由转换,以照片形式(无论是纸质化还是电子化)划分保护对象的方法终将没有说服力。因此,法院仍有必要在“照片”解释的基础上更近一步,才能使被告信服其行为确实与BIPA的规定相违背。

(二)对“几何结构扫描”真实含义的理解

在脸书案中,三原告围绕“照片是否受保护”的问题提出了许多有价值的主张,由此推动了案件真相的发现。原告提出,脸书公司的违法行为不在于收集、储存和使用了原告的照片,而在于收集、储存和使用了从原告的数字化图像中衍生的信息——根据原告独特的面部特征而创建的原告面部特征的数字表示,即所谓的“人脸模板”。这些面部特征的数字表示来源于对面部几何结构的测量,又称为“面部几何结构扫描”,例如一个人的眼睛、鼻子和耳朵之间的距离。脸书公司的“标签建议”服务必须依赖于面部几何结构扫描,而后者是BIPA明确保护的“生物特征标识”,所以脸书公司未经原告同意收集、储存和使用原告照片的行为就是对生物识别信息的侵犯。

原告的这一主张使案件变得更加复杂,而要解除困惑就必须从技术层面回答什么是“面部几何结构扫描”。脸书公司首先通过词语解释的方法对原告的主张进行了反驳,它认为BIPA虽然明确将“面部几何结构扫描”规定为生物特征标识,但是这一术语中的“扫描”一词应当作限制性解释,即应理解为“精确测量”,例如眼睛、鼻子和耳朵等在距离、深度和角度上的专门测量,而自己的行为仅仅是对照片进行了映射,所以不符合“扫描”的应有含义,不能被认为收集了原告的生物识别信息。

原被告就“面部几何结构扫描”形成的争论真正触及人脸识别纠纷的根本,对于“扫描”一词的理解甚至可以决定案件裁判的走向。对于法院而言,探究这一词汇的真意至关重要,而一个前提是必须结合立法的目的进行考察。基于这样的考虑,法院认为,BIPA作为专门应对生物识别技术的隐私保护法律,理应不对“扫描”一词作过多的限制;“扫描”一般是指通过观察来检测或者通过系统性数据尤其是储存的数据来检测,“几何”于日常生活中被理解为“结构”,“结构”则指各部分或各元素的相对排列,所有这些词汇都不要求实际和精确的测量;BIPA没有对“扫描”一词作出解释,也从未暗示专门的测量是必需的。

法院对于“扫描”一词的分析看似在解决一个事实问题,实际上却揭示了生物识别信息纠纷的实质——生物特征测量或言生物特征标识,才是生物识别信息纠纷诉争的关键。脸书案之后,美国法院已经可以非常熟练地把握该类诉讼的核心问题了。例如在2017年,因谷歌“云服务”而引发的针对谷歌公司的集体诉讼中,法院很快就锁定了争议的核心,并确认通过扫描照片中人物的面部特征而创建的“人脸模板”属于生物特征标识,而谷歌公司未经原告同意创建和使用“人脸模板”的行为违反了BIPA的规定。谷歌案判决再一次证明,在因生物识别技术而引发的纠纷中,生物特征测量以及生物特征测量数据才是法律需要保护的核心利益。

(三)测量方式是否影响生物识别信息认定之辨析

脸书案和谷歌案让法院明白,生物识别所涉及的核心利益是生物特征测量及其数据,然而面对快速发展的生物识别技术,法院在认定一项行为是否涉及对生物识别信息的处理时仍会出现许多

障碍。在谷歌案中,就生物特征测量的来源问题再一次引发了争论。这次争论的焦点是:生物识别信息的获得是否受到测量方式的影响?

谷歌公司认为,BIPA 规定了两个非常重要的定义:“生物特征标识”和“生物识别信息”。这两个定义是从来源上进行区分——由人派生的是生物特征标识,随后由生物特征标识派生的才是生物识别信息。“面部几何结构扫描”之所以是生物特征标识,是因为它只能从人而来。因此,对人面部的直接扫描才能形成生物特征标识,而扫描照片获得的生物特征测量不符合生物特征标识的定义。谷歌公司意图从生物特征标识的来源(即生物特征的测量方式)入手找寻胜诉的机会,但它的这一努力无法从法律文本中找到依据,也明显不符合 BIPA 的立法目的。“BIPA 关于生物特征标识的定义只是简单列举了生物特征标识的类型,却没有规定获取和存储它们的方法,事实上生物特征标识可以通过各种方式获得,只要生物特征的测量值不发生改变,它们就依然是生物特征标识。”⑤法院通过判决表明一种立场:生物特征标识就是对一个人的生物特征测量,与测量的方式无关。

生物特征测量及其数据的获得不受测量方式的影响,这一观点对后续案件的审判起到了相当重要的影响。在 Monroy v. Shutterfly, Inc. 案中,被告再一次提出“面部几何结构扫描”应被理解为只能从真人处获得,理由是:其一,生物特征标识既然不包括从图像或照片中获得的信息,那么生物特征标识定义中的“面部几何结构扫描”就只能是对人脸进行的面对面扫描;其二,在生物特征标识的定义中,与“面部几何结构扫描”一同列举的项目例如视网膜或虹膜的扫描,指纹、声纹、手部扫描等都暗示了面对面的过程。审理该案的法院从多个角度反驳了被告的观点:其一,认为“生物特征标识”定义所列出的生物特征标识只能通过面对面方式获得的观点是不正确的,例如指纹、视网膜扫描从技术的角度看完全可以从电子图像和照片中获得,即便某些生物特征测量无法通过影像获得,考虑到技术发展的速度,未来也有充分的可能性。其二,如果将“面部几何结构扫描”理解为面对面扫描,那么法律将在应对技术发展带来的新问题时捉襟见肘。正如谷歌案判决陈述的那样,“技术的进步是促使伊利诺伊州颁布 BIPA 的原因,因此该法不可能通过限定测量的方式来限制生物特征标识的定义。有谁知道将来还可能通过何种方式进行虹膜扫描、视网膜扫描、指纹、声纹以及面部和手部扫描”,最为重要的是,没有法律条文要求生物特征标识必须直接来源于人。如果立法者有意使“面部几何结构扫描”指代对人脸进行的实际扫描,那么它就应当作出更明确的表示,例如在定义中明确使用“来自人”或者“基于人”等词汇⑥。

(四)美国经验的总结与反思

美国生物识别信息的认定经历了一个由技术进步助推认知成长的过程。技术更迭所带来的认知困惑深刻地反映在法庭双方所进行的各种争辩中。这些争辩为深入理解生物识别信息的内涵提供了鲜活的素材,也为检验法律定义的适恰性提供了现实依据。

美国法院的审判经验可以概括为以下方面:(1)单纯对于个人生物特征的描述不构成生物识别信息。生物识别信息要从个人生物特征中提炼,但是个人生物特征不是生物识别信息。个人生物特征的描述即便以有形的方式呈现亦不构成生物识别信息,例如能够展现眼睛颜色的照片不是生

---

⑤Lindabeth Rivera and Joseph Weiss, on behalf of themselves and all others similarly situated, Plaintiffs, v. Google Inc., Defendant. United States District Court, N. D. Illinois, Eastern Division. 238 F. Supp. 3d 1088.

⑥Alejandro Monroy, on behalf of himself and all others similarly situated, Plaintiffs, v. Shutterfly, Inc., Defendant. United States District Court, N. D. Illinois, Eastern Division. 2017 WL 4099846.

物识别信息。(2)生物特征样本须与生物识别信息区分开来。生物特征样本是记录个人生物特征的载体,该载体若单纯以物理形式呈现(如纸质印刷品的照片)则不会产生与生物识别信息的交集。但是当生物特征样本经过特定技术处理后(如数字化的图像),它与生物识别信息的界限就可能变得模糊。美国法院的贡献就在于澄清了一个事实——无论生物特征样本的载体形式如何,都不能将它与生物识别信息相等同,因为生物识别信息的本质不在于形式,而在于是否对个人生物特征进行了测量。(3)生物识别信息的实质是对生物特征的测量(即对生物特征的特定技术处理)。由于BIPA对生物识别标识采用了表象性的描述——"视网膜或虹膜扫描,指纹、声纹、手部或面部几何结构的扫描",由此引发了争议双方的各类解读。法院审判的意义在于还原了法律文本中"扫描"一词的真实含义,揭示了生物识别标识的内核是生物特征测量。建立在这一认知的基础之上,生物识别信息的认定变得精准而简单——所有因生物特征测量所形成的数据就是生物识别信息,至于这些数据的取得方式则没有必要过多考虑。

从美国的审判经验得到启示:一个良好的定义可以避免许多不必要的纷争,而要塑造这样一个定义,就必须从问题的本质入手。以BIPA的定义来看,其最大的缺陷在于采用表象性的描述来界定生物特征标识,没有对生物特征标识的内核进行挖掘。这种表象性的描述极易引起认识上的偏差,同时表象性的列举也不可能做到周延。例如,当作为行为特征的步态经过特定程序的测量从而具备识别个人身份的功能时也会上升为生物识别信息,但是在BIPA的列举中却缺乏这种描述。由是观之,生物识别信息的定义更应当从"生物特征测量"的本质着手,才能避免技术更迭所带来的不断解释的问题。对比来看,较BIPA晚了近10年的欧盟定义尤其是印度的定义更具有合理性。

四、生物识别信息的中国语义:以生物特征测量为核心的开放型定义

生物识别的应用带来了权利侵害的新特点:从显性到隐性的安全风险[23]。然而,个人生物识别信息的法律保护现实地摆在面前。随着《个人信息保护法》立法的尘埃落定,生物识别信息的安全防护将获得极大提升。但不可否认的是,我国尚缺乏对生物识别信息的准确定义,而现有法律文件所使用的定义存在保护对象不统一、内涵和外延不明确等各种问题[24]。这实际上反映了对生物识别信息本质认识的欠缺。

目前一个普遍性的错误是,将生物识别信息与个人生物特征相混淆。例如,有观点认为人脸就是生物识别信息[25]。生物识别信息须由个人生物特征经过特定技术处理转化而来,这是生物识别信息与个人生物特征的联系,二者绝非同一内涵。个人生物特征与生俱来,具有天然的客观性,生物识别信息则是经过了人工干预而在后天形成的数据。譬如一个人的两眼距离过宽,此乃对个人生物特征的描述,而两眼之间距离的测量数据才是生物识别信息。事实上,我国理论界对于个人生物特征、生物特征样本、生物特征测量、生物识别信息等均未形成明确的认知,因此上述概念混用的现象时有发生。例如,《信息安全技术:个人信息安全规范》第6.3C条之3规定:"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。"根据该条语义,人脸图像究竟是生物特征样本抑或生物识别信息,概莫能辨。2022年实施的《信息安全技术 生物特征识别信息保护基本要求》对"生物特征识别信息"作出了最新定义:"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。"然

而在该定义的注解中我们看到,“生物特征识别信息”不仅包括面部识别特征、虹膜、指纹等,还包括样本和图像。这表明概念之间交叉重叠、边界不明的现象依然存在,个人生物特征、生物特征样本与生物识别信息之间的混淆认识没有消除。

笔者认为,个人生物识别信息的定义应当把握三个原则:第一,揭示生物识别信息的本质;第二,反映生物识别信息的构成;第三,兼顾技术更新的速度。在上述原则的指导下,生物识别信息的定义宜由内涵与外延两部分组成,前者规定生物识别信息的本质与构成,为未来所有可能的情况提供解释的基础,后者进行开放式列举,以引导当下的理论与实践。生物识别信息的实质是对生物特征的测量,个人生物特征的反映、特定技术处理的环节、唯一性识别的功能是识别生物识别信息的核心要素,在此基础可以勾勒出生物识别信息的内涵——对自然人的生物特征进行特定技术处理(测量)所形成的能够唯一性识别自然人身份的信息(数据)。生物识别信息的三个要素也是区分它与个人生物特征、生物特征样本、生物特征测量的依据。例如,人脸图像在未经技术处理之前仅仅作为生物特征样本而存在,所以单纯对于照片的处理例如收集、扫描、传输、公开他人的照片不涉及生物识别信息的问题。倘若通过特定的程序从人脸图像中将面部各代表性部位的相对位置和相对大小作为特征提取出来,所获得的特征向量就是生物特征测量。如果这些特征向量被储存于特定数据库中以便日后用于识别和认证个人身份,那么便形成了生物特征参考模板俗称“人脸模板”,与原始的人脸图像不同,人脸模板则是生物识别信息。

至于生物识别信息的外延,则应当在兼顾特别列举的同时保持开放。尽管出于产业保护的需要,一些地区出现了限缩生物识别信息种类的现象,例如美国华盛顿州的《生物信息隐私法》没有在生物特征标识的定义中列举“面部几何结构扫描”[26]。评论者多认为这是一种商业友好利用的表现[27]。但是从国际总体情况看,保持外延的开放性已经成为主流。欧盟、英国和印度对生物识别信息的定义采取“概括”立法模式,其外延多不加以限制,只要对自然人的生物特征进行特定程序处理所形成的唯一识别自然人身份的数据均是生物识别信息。美国伊利诺伊州采用“概括+排除”的立法模式,例如将遗传信息和健康信息排除在生物识别信息之外,但是作此排除的目的主要是为了避免与联邦法律已有涉及的生物识别信息的规定发生冲突,至于生物识别信息的范围依旧十分广泛。加利福尼亚州的定义则采用“概括+列举”的立法模式,一方面从正面列举从虹膜、视网膜、指纹、脸部、手掌、静脉、语音、步态、点击模式、睡眠模式、运动模式,以及健康状况中提取的数据是生物识别信息,另一方面又在定义中使用“包括但不限于”的表述使生物识别信息的范围不受列举的限制。我国《信息安全技术:个人信息安全规范》也曾罗列生物识别信息的种类——“个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等”,此种罗列明显只具有提示意义。伴随着生物识别技术的发展,生物识别信息的范围会不断扩大,故而,为实现保护和管理的目标,不宜对生物识别信息的种类加以限制。我国应当借鉴比较法上的经验,在生物识别信息的外延界定上保持涵摄性。

五、结语

生物识别信息是随着生物识别技术发展出现的个人信息的新类型。伴随着生物识别技术应用的不断深入,生物识别信息危机问题将愈发突出。然而生物识别信息除承载个体的人格价值外,还有重要的商业利用价值与公共管理价值,这就意味着生物识别信息的安全风险可能长期存在[28]。加强生物识别技术的合规化管理,建立企业、行业组织、监管机构在内的多方协同治理机制,对于预

防生物识别信息的安全风险具有重要意义。而从技术或者法律的层面建立生物识别系统的安全性能标准,使个人在了解生物识别系统的风险后再进行授权同意,是实现个人对生物识别信息控制权的真正途径[29]。不过上述所有措施都必须依赖一个共同的前提,即明确生物识别信息的范围和类别,而这必须借助于对生物识别信息的准确定义。

参考文献:

[1]王丹娜.生物识别:传统信息安全在新技术环境的创新应用[J].中国信息安全,2019(2):60-64.

[2]付微明.大数据时代个人生物识别信息法律保护的重要意义[J].研究生法学,2019(4):134-140.

[3]JAIN A K. Technology:Biometric recognition[J]. Nature,2007(7158):38-40.

[4]周正.生物识别技术助力信息惠民工程[J].中国信息界,2015(2):72.

[5]宋子晴.生物识别信息安全新主张[J].中国公共安全(综合版),2016(10):84-87.

[6]李尔静.软件可以窃取"脸",你将如何证明你是"你"[N].长江日报,2019-09-05(05).

[7]毛亚楠.人脸识别第一案:告的是什么[J].方圆,2019(24):14-17.

[8]ELIZABETH C. Reject the evidence of your eyes and ears:Deepfakes and the law of virtual replicants[J]. Seton Hall Law Review,2020(1):177-206.

[9]屈畅.17万"人脸数据公开售卖被下架"[N].北京青年报,2019-09-11(07).

[10]海通证券.信息服务:生物识别产业爆发在即[J].股市动态分析,2016(38):48.

[11]王德政.针对生物识别信息的刑法保护:现实境遇与完善路径:以四川"人脸识别案"为切入点[J].重庆大学学报(社会科学版),2021(2):133-143.

[12]张勇.个人生物信息安全的法律保护:以人脸识别为例[J].江西社会科学,2021(5):157-168,255-256.

[13]周行.人脸信息立法保护的规范体系建构[J].中南民族大学学报(人文社会科学版),2021(8):128-135.

[14]吴小帅.大数据背景下个人生物识别信息安全的法律规制[J].法学论坛,2021(2):152-160.

[15]王泽鉴.债法原理(三)侵权行为[M].北京:中国政法大学出版社,2001:138.

[16]赵秀萍.生物特征识别技术发展综述[J].刑事技术,2011(6):44-48.

[17]顾理平.身份识别与复制:智能生物识别技术应用中的隐私保护[J].湖南师范大学社会科学学报,2021(4):123-130.

[18]WILLOUGHBY A. Biometric surveillance and the right to privacy[J]. IEEE Technology and Society Magazine,2017(3):41-45.

[19]BINIMOW B J. State statutes regulating collection or disclosure of consumer biometric or genetic information[J]. American Law Reports 7th,2019(41):38.

[20]付微明.个人生物识别信息民事权利诉讼救济问题研究[J].法学杂志,2020(3):78-88.

[21]SCHWAB K. A landmark ruling gives new power to sue tech giants for privacy harms[EB/OL].(2019-01-26)[2021-12-05]. http://www.fastcompany.com/90297382/illinois-supreme-court-decision-marks-a-landmark-win-for-biometric-privacy-harm? position=7&campaign_date=11082020.

[22]STEPNEY C. Actual harm means it is too late:How Rosenbach v. Six Flags demonstrates effective biometric information privacy law[J]. Loyola of Los Angeles Entertainment Law Review,2019(1):51-87.

[23]顾理平.智能生物识别技术:从身份识别到身体操控:公民隐私保护的视角[J].上海师范大学学报(哲学社会科学版),2021(5):5-13.

[24]曾昌.分离困境与整合路径:大数据时代下个人生物识别信息保护制度之完善[J].云南社会科学,2021(5):114-122,187.

[25]郭春镇.数字人权时代人脸识别技术应用的治理[J].现代法学,2020(4):19-36.

[26]BENSON B. Fingerprint not recognized:Why The United States needs to protect biometric privacy[J]. North Carolina Journal of Law & Technology,2018(4):161-192.

[27]陆海娜,赵赓.个人生物识别信息商业利用的法律规制:美国州立法经验的比较与反思[J].人权研究,2021(2):86-105.

[28]冉克平.论个人生物识别信息及其法律保护[J].社会科学辑刊,2020(6):111-120.

[29]华国庆,陶园.论生物特征识别系统个人信息采集处理授权同意机制[J].江西社会科学,2021(5):169-178.

The definition of personal biometric information

JIAO Yanling

(*School of Law*, *Tianjin Normal University*, *Tianjin 300387*, *P. R. China*)

Abstract: Biometric information is a kind of data that comes from technical processing of personal biological characteristics. Personal biometric characters have the characteristics of invariance and uniqueness, which makes biometric identification identify individuals once and for all. Biometric information processed by a specific technology also has these characteristics, so any attacks on biometric information may have an irreversible impact on individuals. In real life, the information subject suffer loss from illegal commercial collection, freedom limitation, information sale and theft, deep fake and fraud. It' s urgent to protect biometric information security, while defining biometric information precisely is the primary prerequisite. Experiences from comparative law show that the biometric information has three essential elements: the reflection of biological characters, the processing by specific technology, and the function of unique recognition. They are the key to identify biometric information. Biometric information can be collected by an image containing personal biometric characteristics, but the image is only a reflection of personal biometric characteristics. The image is not biometric information unless it is processed by specific technology, whether the image is an electronic image or a paper photo. The essence of biometric information is the measurement of personal biometric, which is called "specific technology processing", but the measuring method itself doesn' t matter. Whether measurement from face to face on real-person or from image containing personal biometric characteristics, the information is both biometric information. The description of personal biometric characteristic does not constitute biometric information, and personal biometric samples should be distinguished from the personal biometric information. There are many deviations in understanding the definition of biometric information in the legal documents now, and concept confusion, unclear connotation and incomplete extension are the main problems. The definition of biometric information in China should follow three principles in future: revealing the nature of biometric information, reflecting the elements of biometric information, and taking into account the speed of technology progress. It is necessary to define the concept from two aspects: connotation and extension. The functions of connotation are defining essence and composition, so as to provide explanation rooms for possible technological revolution. The functions of extension are listing typical biometric information, so as to provide guide for the current theory and practice. As far as the connotation, "biometric information" can be described as a kind of information which can uniquely identify a natural person by the specific technical processing of his biological characteristics. In terms of extension, the ordinary kinds of biometric information can be listed, at the same time, using the expressing of "including but not limited" to keep the scope of biometric information open.

Key words: biometric information; biological characters; samples of biological characteristic; biometric measurement; personal information protection

(责任编辑　袁　虹)