

【比较与借鉴】

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

陆海娜 赵 赓

【摘 要】随着生物识别技术在商业领域迅速推广,其伦理风险和安全问题也日益凸显,但我国法律对生物识别信息商业利用的规范存在严重不足。目前,美国共有三个州通过了对个人生物识别信息的专门立法,并采取了不同进路,其各自的优点和缺陷及不同的实践效果都对我国颇具参考意义。伊利诺伊州通过了《生物识别信息隐私法》,对生物识别信息采用严格的保护标准;德克萨斯州通过了内容非常相似的《生物特征符获取或使用法》。这两个州采取了严格保护的进路。但是,过于严格的保护产生了限制表达自由、阻碍信息利用的问题。华盛顿州的《生物识别隐私法》则采取了对商业利用比较友好的进路,但存在着对生物识别信息保护不足的风险。美国法的经验反映了生物识别信息具有高度的敏感性和一定的公共性特征。我国在立法时,需充分考虑到生物识别信息的双重属性,既要保护好信息主体的隐私权,也要照顾到个人信息所具有的公共性以及正当的商业利用需求。本文建议可以通过完善信息区分、场景化行为主义规制以及公私结合的救济途径来实现对生物识别信息双重属性的兼顾。

【关键词】生物识别信息;隐私权;商业利用;个人信息保护

【作者简介】陆海娜,中国人民大学法学院副教授、中国人民大学人权研究中心执行主任;赵赓,云南省财政厅(试用期)公务员。

【原文出处】《人权研究》(京),2021.2.86~105

【基金项目】本文为教育部人文社科项目基地重大项目《全球发展权的理论创新与平权机制研究》(20JJD820001)的阶段性成果。

引言

生物识别技术,是一种通过自动技术对人体固有的生物特性和行为特征进行识别,然后与数据库的模板数据进行比较,从而确定个人身份的技术。^①相比于其他身份鉴定方法,生物识别技术具有安全、便捷的优势。近几年,我国生物识别产业迅速发展,商业利用人脸、指纹等生物识别信息的范围越来越广,使用方式也越来越多样化。^②但是,我国对生物识别信息的保护现状却不容乐观,实践中在信息收集和披露、损害救济等方面存在不少问题。^③诸如商业滥用个人生物识别信息的问题,主要反映出我国

现行法律对生物识别信息商业利用规范的不足。我国现行法律中仅有《中华人民共和国民法典》和《中华人民共和国网络安全法》在“个人信息”的定义中提到了“生物识别信息”^④,尚未针对生物识别信息保护作出专门规定。《信息安全技术公共及商用服务信息系统个人信息保护指南》(以下简称“《个人信息保护指南》”)、《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》”)以及《个人金融信息保护技术规范》等规范性文件虽然区分了“个人信息”和“个人敏感信息”,将生物识别信息列入“个人敏感信息”,规定了更严格的保护措施,但

它们均为非强制性的国家标准或行业标准。^⑤立法的缺失使得个人在强势企业收集利用其生物信息时显得软弱无力。

个人生物识别信息涉及隐私权等基本权利,其性质与其他敏感信息不同:个人生物识别信息涉及人的身体,对个人身体自主控制的权利是隐私权最核心的内涵。尤其是人脸识别技术,具有非接触性、侵入性强等特点,一旦被滥用可能会对个人生活造成难以恢复的灾难性影响。而且即便没有被滥用等后果,一个人如何处理关于自身身体的信息,本质上也是个人自主权的一部分,是个人尊严的体现。因此,对个人生物识别信息的法律保护,需要从信息收集、储存、披露以及损害救济等方面作出相比其他个人信息更为严格的规定。

《中华人民共和国个人信息保护法(草案二次审议稿)》(以下简称“《个人信息保护法(草案二次审议稿)》”)从立法层面区分了一般个人信息和敏感个人信息,规定了处理敏感个人信息应当向个人告知处理的必要性和对个人的影响,并指出法律、行政法规可以对处理敏感个人信息作出更严格的限制。^⑥对于生物识别信息,《个人信息保护法(草案二次审议稿)》将“个人生物特征”列入“敏感个人信息”中,并规定“在公共场所安装图像采集、个人身份识别设备,应当为维护公共安全所必需,遵守国家有关规定,并设置显著的提示标识。所收集的个人图像、个人身份特征信息只能用于维护公共安全的目的,不得公开或者向他人提供,取得个人单独同意的除外”^⑦。尽管《个人信息保护法(草案二次审议稿)》已在生物识别信息保护专门规定上迈进一步,但目前仍存在许多未决的问题。

我国学术界对个人信息保护的研究成果已经非常丰富,但对于个人生物识别信息保护方面的研究还较少。本文尝试从比较法的角度,从已有的他国法律经验出发,为我国进一步完善这方面的法律提出建议。

比较各国实践,美国较早地对生物识别技术进行商业利用,也较早地面临生物识别信息法律保护的问题。

伊利诺伊州、德克萨斯州和华盛顿州都先后对生物识别信息进行了专门立法保护。前两个州的立法基本采取了严格保护生物信息的进路,而华盛顿州则采取了对商业利用更为友好的进路。两种进路是不同立法理念和利益方博弈的结果,也展现了不同进路对各种权利和利益平衡的考量。中国和美国法律制度虽然有很大差异,但是同样面临着大数据时代个人信息保护的法律难题。因此,从功能主义的角度,美国生物识别信息商业利用的立法和实践经验对我国相关法律制度的完善也有参考价值。

一、伊利诺伊州《生物识别信息隐私法》和德克萨斯州《生物特征符获取或使用法》

2008年,美国伊利诺伊州通过了《生物识别信息隐私法》(Biometric Information Privacy Act,以下简称“BIPA”)。作为美国第一部对商业利用生物识别信息进行专门保护的法律,BIPA对“私营实体”在个人生物识别信息的收集、保护、使用和销毁以及个人信息主体的救济手段等方面作出了较为详尽的规定,并经过判例法不断发展。^⑧BIPA通过后一年,德克萨斯州通过了《生物特征符获取或使用法》(Capture or Use of Biometric Identifier Act,以下简称“CUBI”),该法在规范内容上与BIPA非常相似。BIPA和CUBI被认为是“美国第一代生物识别信息隐私法”^⑨,其特点是对生物识别信息进行严格的保护。

(一)严格保护的进路

1.立法目的与概念定义

伊利诺伊州BIPA的出台具有偶然性。由于伊利诺伊州一家运营指纹识别系统的公司破产,大量被收集了指纹的用户开始担心他们的生物识别信息会被任意处理。^⑩生物特征具有独特性和不可变更性,一旦泄露便是终身泄露,会有极大的身份被盗窃的风险,并且难以恢复原状。在此背景下,伊利诺伊州议会注意到了人们对生物识别信息安全性的焦虑、公众对新技术的警惕以及生物识别技术商用化潜在的未知风险。^⑪出于这种对生物识别技术商业利用高度警惕的态度,BIPA的规范内容对生物识别信息的保护作出了严格的规定。同时,由于BIPA在

文本中明确了其立法目的,使得法院在具体判例中也倾向于采取严格保护个人信息主体权益的态度。

美国生物识别隐私法在概念上区分了“生物特征符”(biometric identifier)和“生物识别信息”(biometric information)。BIPA将“生物特征符”定义为“视网膜或虹膜的扫描、指纹、声纹、手或脸的几何扫描”^⑫。CUBI的定义与之相似。^⑬BIPA进一步规定该法所称的“生物特征符”不包括笔迹、签名、照片以及用于科学和医疗的人体数据等。^⑭“生物识别信息”的定义则是建构在对“生物特征符”的定义之上的。根据BIPA,“生物识别信息”是指基于“生物特征符”产生的信息(无论该信息是如何获得、转换、储存或者共享的);基于“生物特征符”定义所排除的项目或过程所产生的信息都不属于“生物识别信息”。^⑮

判例法对“生物特征符”和“生物识别信息”的概念做了进一步的明确。在里维拉等诉谷歌案(Rivera et al.v.Google Inc.)中,原被告针对通过对用户上传到云服务中的照片进行人脸扫描所获得的人脸模板是否属于BIPA所规定的“生物特征符”产生争议。由于BIPA规定照片不属于该法所称的“生物特征符”,被告认为对照片进行的人脸识别不受BIPA的保护。对此,法院认定,BIPA没有对获取生物特征符的方式作出限制,以不同方式收集到的生物特征符并不会因其收集方式的不同而导致性质上的不同;无论收集者将生物特征符转换成何种形式,只要所得到的信息可以用来对个人进行识别,就受到BIPA的保护。对本人面部进行扫描得到的人脸模板,和从照片或视频中生成的人脸模板都属于BIPA所规定的“生物特征符”。^⑯法院指出,“生物特征符”和“生物识别信息”区分的意义在于,前者是生物特征测量的集合,后者是将这些测量转换成不同的可用的形式;前者只是用于识别一个人的、特定的、基于生物学的测量,并不涉及测量是如何进行的,而后者确保收集者不能通过将生物特征符转换成某种其他形式来规避法律。^⑰

2. 数据收集、保护、使用和销毁规则

在数据收集上,BIPA要求私营实体在收集生物

特征数据(biometric data)之前,必须通知个人(或者其合法的代理人)其生物特征符或生物识别信息正在被收集,并告知收集和储存这些数据的目的和时间长短;这些告知必须是书面形式,并且个人(或者其合法的代理人)必须提供同意的书面声明。^⑱CUBI同样要求收集者在收集生物特征数据前对被收集者进行通知并获得同意。^⑲但与BIPA不同,CUBI在通知和同意的具体形式上并没有作出要求。

在生物特征数据的保护标准上,BIPA要求私营实体必须将生物识别信息作为机密和敏感的信息对待,并给予与其他敏感和机密信息相同或更高的保护,以“该私营实体行业内的合理注意标准”来储存、传输和保护这些信息。^⑳而CUBI规定,出于商业目的而获取的个人生物特征符的拥有者,应当以与该人储存、传输和保护其拥有的任何其他机密信息相同或更具保护性的方式,合理谨慎地储存、传输和保护生物特征符,防止其被披露。^㉑因此,与BIPA相似,CUBI的保护标准同样可以分为两个部分:第一个标准是要求生物特征数据的拥有者采用与其他机密信息相同或更高的标准进行保护,这一点与BIPA的规定相同;第二个标准是“合理谨慎”,其仅是一种“常规的客观标准”^㉒,这一点与BIPA规定的“行业内合理注意标准”略有不同。

对于生物特征数据的使用,BIPA要求私营实体不得向第三方出售、出租、交换生物特征符和生物识别信息,或以其他方式从保有的生物特征符和生物识别信息中牟利。^㉓私营实体仅能在以下4种情况下,才能披露其所保有的生物特征符或生物识别信息:(1)信息主体同意披露;(2)信息主体授权或要求的金融交易需要披露;(3)联邦法律、州的法律或者市政条例要求披露;(4)有合法管辖权的法院发出令状或传票要求披露。^㉔CUBI原则上禁止出租、出售或以其他方式披露生物特征数据,仅有4种例外情形:(1)信息主体同意在其失踪或死亡的情况下,为识别目的而披露;(2)为完成信息主体所要求或授权的金融交易;(3)联邦法或州法要求或允许披露;(4)为了执行搜查令,由执法机构或向执法机构进行披露。^㉕因

此,BIPA对利用生物特征数据牟利的行为采取绝对禁止的态度,仅允许在4种法定例外情形下披露数据。相比之下,CUBI将例外情形的适用范围扩大到了出售、出租等牟利行为。

关于生物特征数据的销毁规则,BIPA要求私营实体必须制定一项书面政策,并向公众公开;建立一个数据保留时间表和准则,在最初收集和保存生物特征符或生物识别信息的目的已经被满足的情况下,或者个人与私营实体最后一次互动后的三年内(以先发生者为准),永久销毁这些信息;除非有具有合法管辖权的法院发出有效的令状或传票,否则拥有生物特征符或生物识别信息的私营实体必须遵守其制定的数据保留时间表和准则。^⑤CUBI规定,个人生物特征符的拥有者,应当在合理时间内销毁生物特征符,并且不得迟于收集该生物特征符的目的实现之日起的一年内。^⑥此外,如果雇主出于安全目的收集雇员的生物特征符,当雇佣关系终止时,生物特征符的收集目的推定为终止,将适用该法规定的目的实现后一年内销毁数据的规定。^⑦可见,CUBI规定的数据保存期限更短,更为严格。并且,对雇员的生物特征数据保存时间作出了创新性的规定。但是,BIPA的规定更为全面,还要求收集者在与信息主体最后一次互动后的三年内必须销毁数据。此外,BIPA要求私营实体制定并公开书面政策,能“激励私营实体在收集生物特征数据时进行合规的考虑,理想情况下,有助于防止今后出现诉讼;并且,可以帮助消费者作出更好的选择”^⑧。

3. 救济规则

BIPA规定,任何因违反该法的行为而受到损害的人,胜诉后可就每一侵权行为要求赔偿:因过失违法而造成损害的,赔偿数额为实际损失额或1,000美元;因故意或者重大过失违法而造成损害的,赔偿数额为实际损失额或5,000美元。此外,被受害人胜诉后可以获得律师费用和其他合理费用的赔偿,以及禁止令等其他救济。^⑨

然而,对于“损害”的判断标准,一直存在着较大的争议,不同的法院也在实践中作出过不同的判

决。^⑩最终,伊利诺伊州最高法院在罗森巴赫诉六旗娱乐公司案(Rosenbach v. Six Flags Entertainment)中确定,BIPA所规定的“损害”指合法权利遭到侵犯、剥夺或者其他不利影响;信息主体无需证明其受到的实际损失,信息收集者和控制者对BIPA程序性要求的违反即构成对信息主体的“损害”。^⑪法院还进一步指出,BIPA规定的“程序性的保护”,在当今数字时代具有重要的意义。个人独特的生物特征符在被泄露或滥用后是无法更改的,一旦私营实体未遵守法定程序,个人的生物信息隐私权就立刻烟消云散了。BIPA使得收集生物特征数据的企业必须谨慎行事,这是法律本身的合理意图,因为,无论企业为满足法律要求而可能产生多高的费用,与生物识别信息得不到适当保护可能造成的重大的、不可逆转的损害相比,这些费用显得微不足道;公共利益与安全必须放在优先地位。^⑫

在救济方式上,CUBI与BIPA有较大的不同,CUBI并未赋予个人提起民事诉讼的权利。根据CUBI的规定,违反该法的人,对于每次违反将受到不超过25,000美元的民事处罚。州总检察长(State Attorney General)可以提起诉讼以获得民事罚款。^⑬相比较而言,CUBI不论是在救济方式的种类还是幅度上均弱于BIPA。CUBI的救济规则给了数据收集和控制者一个最高赔偿额度的保护。并且,由于未赋予个人诉讼权利,数据收集和拥有者也免于应对大量的个人诉讼。此外,CUBI也未像BIPA一样,赋予信息主体金钱赔偿之外的救济手段(如申请禁止令)。

有学者指出,BIPA关于私人诉讼的救济模式也许是该法“最独特和最重要的一个方面”^⑭。在美国有关数据保护的法律法规中,很少有明确规定个人诉讼权利的。赋予个人诉讼权,既给予了信息主体一个有力的救济途径,也有利于督促信息收集者和控制者严格遵守法律。此外,通过大量判例法的发展,生物识别信息保护的法律法规和法理也能得到进一步的丰富。

(二) 严格保护进路产生的问题

从信息主体的角度看,BIPA和CUBI的严格保

护进路较好地保护了信息主体的隐私权;但是从权利和利益平衡的角度看,这种相当严格的保护也会产生一些负面影响,主要体现在对表达自由的限制和影响对个人生物识别信息的正当商业利用。

1. 对表达自由的限制

有学者认为,BIPA等生物识别隐私法对个人生物识别信息的严格保护限制了表达自由,违反了美国宪法第一修正案。谷歌、脸书等公司都在从用户照片中创建人脸模板的那一刻起触犯了BIPA。但是,创建人脸模板属于创造信息,而BIPA对这种信息创造的限制实际上是对表达自由的限制。由于从照片中获取的数据并没有用于广告或市场营销,因此,这种观点认为BIPA和与它相似的生物识别隐私法构成了基于内容的、对非商业性表达的歧视性限制。^⑨

表达自由是美国信息理论的一个重要基础理论。言论表达常常需要通过一定的信息来实现,因此在美国,信息被认定为表达自由所保护的对象。例如,在《纽约时报》诉沙利文案(New York Times Co. v. Sullivan)中,美国联邦最高法院认为,对公共人物个人信息的使用受到言论自由的保护。^⑩早期,美国联邦最高法院曾经认为,美国宪法并不保护商业言论。但这一立场在弗吉尼亚州药事管理局诉弗吉尼亚州消费者委员会案(Va. Pharmacy Bd. v. Va. Consumer Council)中得到了转变。在该案中,联邦最高法院认定,广告商对药品价格信息的传播受言论自由条款的保护,弗吉尼亚州立法对其进行的限制无效。联邦最高法院指出,商业信息的自由流动对自由企业体系的合理资源配置具有不可或缺的意义,因为它能对大量的企业决策提供信息,从而驱动商业体系的有效运行。^⑪由此,出于商业目的,对信息各种形式的创造和使用也常常被视为商业言论表达,从而受到美国宪法言论自由条款的保护。

在索雷尔诉艾美仕健康公司案(Sorrell v. IMS Health Inc.)中,美国联邦最高法院认定,对个人处方信息的获取和使用受宪法言论自由条款的保护。药店将其接收的个人处方信息卖给数据挖掘者,数据挖掘者生成关于处方行为的报告,并将其出售给制

药商,制药商则依此来改变其营销策略。佛蒙特州《处方保密法》规定,除非获得信息主体的同意,否则药店不得销售或出于营销目的披露处方信息,制药商也不能将处方信息用于营销。但该法也规定了一些例外情形,如用于医疗研究等。在该案中,联邦最高法院认为:佛蒙特州《处方保密法》的规定构成了基于内容(禁止药店销售和披露,以及禁止制药商用于营销,但是允许医疗研究等例外情形对处方信息的使用)和言论者(药店和制药商)歧视性的限制,因此违反了美国宪法对言论自由的保护。^⑫

综上所述,美国联邦最高法院已经在一系列的判例中,将商业领域中各种形式的信息创造、获取和传播认定为受宪法保护的言论表达。表达自由的权利保护人们在公共场所交流的权利。而“交流”包括任何意图被公众理解或部分理解的象征性的表达行为。^⑬信息创造、获取和传播之所以能成为言论或表达自由保护的对象,原因在于信息具有公共性,进而具有非竞争性和非排他性,是一种处于公共领域的资源。^⑭人类社会的不断进步,正是通过信息的公开、流动以及对思想成果的使用来实现的。

2. 对个人生物识别信息的合理商业利用造成阻碍

对于美国第一代生物识别信息隐私法的另一个批评是,为了保护个人隐私而进行过于严格的规制,这会阻碍许多依赖生物识别来提供安全的新技术的应用,妨碍信息行业的发展,最终导致“企业和消费者都被剥夺了使用生物识别技术来提高安全性的权利”^⑮。

例如,美国奈斯特公司(Nest)生产了一种门铃,配有人脸识别技术的摄像头,可以区分已知的和未知的面部,从而为房主提供更大的安全性。但是奈斯特公司在伊利诺伊州销售该门铃时,门铃的人脸识别功能被禁用,因为BIPA要求在收集生物特征数据之前,必须进行书面的通知并获得书面的同意。然而,每次有访客出现在房主门前时,向访客发出书面通知并要求获得书面同意是不现实的。^⑯

此外,BIPA的损害救济规则也会对生物识别产

业的发展带来阻碍。伊利诺伊州最高法院在前述罗森巴赫案中确定,信息收集和控制者违反程序性义务,即使未对个人信息主体造成实际损害,也需要承担BIPA规定的赔偿责任。仅违反程序性义务即需承担赔偿责任,固然有利于降低个人信息主体在侵权损害赔偿中的证明责任,促进信息收集者、控制者遵守程序性义务,从而强化对个人信息主体的保护力度。但是,对信息业者而言,这样的判决结果无疑会使信息业者面临巨大的赔偿风险。^④

同时,由于BIPA规定了个人诉讼权,导致近年来基于BIPA的诉讼激增,这给信息业者造成了相当大的诉讼负担。仅2018年和2019年上半年,就有213起BIPA诉讼案件提交到法院。^⑤不仅案件数量增加,案件所需时长也往往因案件本身的复杂性而大大延长。2015年提起的针对脸书公司的诉讼案件经历了长达五年的漫长诉讼过程才得到最终判决。^⑥

此外,BIPA法定的赔偿数额过高,以至于在实践中并不能得到实现。BIPA规定每一个因私营实体过失违法而受到损害的人可以获得至少1,000美元的赔偿(如因故意或重大过失违法则为5,000美元),另外还有诉讼费等赔偿;而集体诉讼的形式又会进一步成倍放大赔偿数额。以2016年12月伊利诺伊州库克县法院批准的第一份BIPA和解协议为例。由于是针对L.A.Tan公司提出的集体诉讼,该和解协议最终确定的金额为150万美元(其中包括60万美元的律师费),每个提出索赔的原告获得125-150美元的赔偿。^⑦在针对脸书公司的集体诉讼案件中,法院也认为BIPA法定赔偿数额过高,因此,案件最终以达成和解协议而结束。脸书公司将向一项基金支付6.5亿美元,但据测算,每一个个人只能获得200-400美元。^⑧

二、华盛顿州《生物识别隐私法》

BIPA和CUBI通过后,美国各州生物识别隐私保护立法在一段时间内陷入了停滞。多个州试图通过保护消费者生物特征数据的立法,^⑨但直到2017年,华盛顿州才通过了《生物识别隐私法》(Washington Biometric Privacy Act,以下简称“WBPA”),成为美

国第三个进行生物识别隐私专门立法的州。在WBPA的制定过程中,BIPA和CUBI的严格保护所引发的争议日益凸显。同时,脸书和谷歌之类的大型高科技企业也雇佣了游说团体去积极影响该法案的制定,使得WBPA在规范内容上更多地考虑了生物识别信息商业利用的利益,对商业利用比较友好。^⑩

(一)对生物识别信息商业利用的友好进路

1.立法目的与概念定义

立法目的上,WBPA指出,立法机关发现,出于商业、安全和便利的目的,华盛顿州的公民越来越多地被要求公开其敏感的生物信息,这些生物信息被用于识别特定、唯一的个人。在未经信息主体的同意或其不知情的情况下,收集和出售个人生物特征数据的情况令人担忧。因此,立法机关要求生物特征数据收集者披露其如何使用这些数据,并在将个人的生物特征数据录入数据库或在数据库中进行更改、使用之前向该个人发出通知并获得其同意。^⑪

与BIPA在立法目的中体现的对生物识别技术的警惕和严格保护态度不同,WBPA在立法目的上,仅仅是为了规范数据收集者和控制者对生物特征数据的收集和使用行为。

根据WBPA,“生物特征符”是指“通过自动测量个人生物特征(如指纹、声纹、视网膜、虹膜或其他用于识别特定个体的独特生物特征)而产生的数据”。^⑫与BIPA相似,WBPA还进一步对定义所不包括的内容进行了列举。根据该法,“生物特征符”不包括物理或数字照片、视频或音频记录或由此产生的数据,也不包括医疗方面的信息。^⑬

此外,WBPA还对一些新的概念进行了定义。“录入”(enroll)是指获取个人生物特征符后,将其转换为无法重建为原始输出图像的参照模板,并将其存储在用于与特定个人生物特征符相匹配的数据库中。WBPA还区分了“商业目的”和“安全目的”。“商业目的”是指为销售商品或服务而向第三方出售或披露生物特征符的目的,这种商品或服务并不涉及首次获得个人生物特征符的初始交易;“安全目的”指防止行窃、欺诈或任何其他盗用或盗窃有价值的

东西(包括有形和无形的物品、服务)的目的,以及其他保护软件、账户、应用程序、在线服务等安全或完整性的目的。^⑤

2. 数据收集、保存、使用和销毁规则

在具体的数据保护规则上,WPBA明确区分了“商业目的”与“安全目的”,并在此基础上作出了不同的规定。根据该法,为了实现安全目的而收集、获取或录入并储存生物特征符,并不要求私营实体提供通知并获得同意。^⑥这一规定免除了私营实体将生物识别技术用于安全目的时,通知被收集者并获得同意的义务。比较而言,尽管CUBI也包含“商业目的”的限制,但由于其并未对商业目的作出定义,并且“是否包含了安全目的也尚不明确”^⑦,因此CUBI并未在其规范内容上体现出在商业利用中因为生物特征数据使用目的的不同而导致的规则不同。

在生物特征数据的收集上,与BIPA和CUBI不同,WPBA只对数据收集者将生物特征数据录入数据库的行为进行规制。根据WPBA,收集者需要事先通知被收集者,取得同意,或者提供一种机制防止生物特征符被用于商业目的,否则,不能将生物特征符录入到数据库中。^⑧这种规制方法具有以下优点:第一,有利于提高生物特征数据的安全性。WPBA对“录入”的定义明确了生物特征数据应当被存储的特点格式,要求将生物特征符转换为不能从数据重建为原始图像的模板。由于这种模板可以使得窃取生物特征数据的黑客无法轻松地数据重建原始的识别符,这将导致生物特征符更难被窃取。第二,更为灵活。WPBA只要求私营实体满足发出通知并获得同意,或者提供一种防止数据被用于商业目的的机制,符合这两个条件中的一个即可。第三,收集者负担更轻。可以避免仅短暂收集生物特征数据而不将其储存在数据库的私营实体受到各种严格的限制。第四,可以避免对表达自由造成限制的问题。与BIPA不同,WPBA并未对通知和同意的具体形式作出规定,只要求通知是“通过合理设计为受影响的人可随时获得的程序”作出的;对于通知和同意的内容也仅规定“确切的告知和同意类型视情况而定”。^⑨

在生物特征数据的保护标准上,与BIPA和CUBI的两个要求不同,WPBA只要求生物特征数据的控制者“采取合理谨慎的措施,防止未经授权的人对生物特征数据的访问和获取”^⑩。WPBA的保护标准仅仅是一个客观的合理谨慎标准,类似于CUBI的第二个标准。因此,WPBA的保护标准低于BIPA和CUBI。

对于生物特征数据的使用,与BIPA和CUBI相同,WPBA原则上禁止出售、出租或者以其他方式披露生物特征符。同时,WPBA也规定了与BIPA和CUBI相似的4个数据披露的例外情形:(1)获得信息主体的同意;(2)法律要求披露;(3)法院指令要求披露;(4)披露是为完成主体授权的金融交易所必需的。其中,WPBA在完成金融交易所必需的披露中,增加了对数据接收方的要求:数据接收方必须维护数据机密性,并且除非依据该法获得允许,否则不可再次披露生物特征符。此外,与BIPA和CUBI不同的是,WPBA进一步增加了数据披露的例外情形,具体包括:(1)符合该法通知、同意和数据保护要求的;(2)为提供信息主体订阅、请求或明确授权的产品或服务所必需的;(3)第三方以合同方式承诺不会出于商业目的而再次披露生物特征符,以及不会以与该法要求所不符合的方式,将生物特征符录入数据库以用于商业目的;(4)用于准备诉讼,或者回应或参加司法程序。与CUBI相同,WPBA也允许在例外情形下出售、出租生物特征符。^⑪由此可见,WPBA为生物特征数据的出售、出租和披露留出了较大的空间。另外,WPBA规定,如果没有获得同意,生物特征符不得以实质上不同于最初所规定的条款的方式使用或披露。^⑫

对于生物特征数据的保存时间,WPBA只要求生物特征数据的控制者保留数据的时间不得超过为实现其目的所必需且合理的时间。这些目的包括遵守法律规定的保留时间、安全目的以及为已经录入了的生物特征数据提供服务。^⑬因此,相对于BIPA和CUBI,WPBA对数据保存时间的规定更灵活,但也最不确定。

3. 救济规则

与CUBI相似, WBPA并未赋予个人提起民事诉讼的权利, 只能通过州总检察长来进行起诉。但与CUBI所规定的单独的执行机制不同, WBPA的执行机制是通过《华盛顿州消费者保护法》来进行的。根据WBPA, 违反该法的行为, 将被视为不公平或欺骗性的行为或者不公平的竞争方法而适用消费者保护法的相关规定。^⑤然而, 《华盛顿州消费者保护法》对每一个不公平或欺骗性的行为或者不公平竞争方法的最高民事处罚为2,000美元。^⑥因此, WBPA在救济力度上甚至还弱于CUBI。

(二)对个人生物识别信息保护的不足

1. 规范上的漏洞

在“生物特征符”的定义上, 与BIPA和CUBI相比, WBPA的一个明显的区别是其并未明确将“脸部的几何扫描”放入定义中。同时, 其还明确将“物理或数字照片”排除在定义之外。这可能会导致法院在司法实践中将从照片中产生的人脸几何模板排除在该法的保护范围外。但另一方面, WBPA在其定义中还有“或其他用于识别特定个体的独特生物特征”的兜底规定, 并且该法排除了“视频或音频记录或由此产生的数据”, 却没有在“物理或数字照片”后加上“或由此产生的数据”。这又使得从WBPA定义的文本中, 有解释出包含照片中产生的人脸几何模板的可能。WBPA这种立法上的模糊与其立法时的背景有关。从2015年起, 不少企业因为对用户上传的照片进行人脸识别而遭到起诉。其中的一个重要争议就是从照片中获取的人脸数据是否受BIPA的保护。^⑦然而, 从实践中来看, 爬虫工具爬取网络上的人脸照片已经成为人脸数据的重要来源之一^⑧, 而这些公开的数据倘若与个人身份信息相匹配, 将会侵犯到个人隐私。WBPA的这种模糊态度无疑会使得个人生物识别信息的安全处于严重的危险之中。

此外, WBPA对“生物特征符”是否包括从视频或音频记录中产生的声纹也不确定。该法在其定义中明确提到了声纹, 但随后又将“视频或音频记录或由此产生的数据”排除在外。然而, 在现实中一些声

纹实际上可能是从视频或音频记录中产生的数据。

WBPA关于“安全目的”的规定也存在漏洞。该法对“安全目的”的定义过于广泛, 同时, 定义中的“其他目的”也容易被扩大解释。因此, 该规定会减损WBPA的实际效力。^⑨从生物识别技术在现实生活中的应用来看, 虽然生物识别并不仅仅被用作一种安全手段, 但安全手段确实占了生物识别用途的大部分。^⑩在对生物识别信息的商业利用中, 很多利用形式都可以被解释为具有保护有形或无形的物品、服务或空间的安全和完整性的目的。而根据WBPA的规定, 为了实现“安全目的”而收集并储存生物特征数据的, 可以免除通知和获得同意的义务。这将使得在生物识别信息商业利用的大部分场景中, 收集者可以在不通知信息主体并获得同意的情况下, 收集并储存生物特征数据, 进而产生收集者过度收集, 造成个人生物识别信息安全风险的问题。

在规制范围上, WBPA由于“商业目的”的定义使其在对数据收集者的规制上出现漏洞。由于该法仅适用于向第三方销售或披露的行为, 数据收集者对生物特征符内部的使用行为便不受规制。^⑪此外, “商业目的”的定义将获得个人生物特征符的初始交易排除在外, 因此, WBPA也仅仅是对部分出于销售目的而使用生物特征符的行为进行规制。

在信息披露上, WBPA扩大了允许披露的情形。只要披露是为提供信息主体订阅、请求或明确授权的产品或服务所必需的, 甚至只要求第三方以合同方式承诺不会再次披露并且遵守该法即可。这就增加了信息泄露的风险。而在保护标准上, WBPA仅要求采取合理谨慎的措施以防止未经授权的访问和获取, 并未规定相比一般个人信息更高的保护标准。在信息保存期限上, WBPA仅规定不得超过实现目的所必需且合理的时间。该法所规定的“合理谨慎”和“必需且合理”都是相对不确定的, 这在实践中并不利于对个人生物识别信息的保护。

2. 救济手段的不足

CUBI和WBPA都没有赋予个人提起诉讼的权利, 只能由州总检察长进行起诉。州总检察长诉讼

的模式源于美国消费者保护法的诉讼机制。20世纪60-70年代,在美国联邦贸易委员会的推动下,美国各州陆续采用了“不公平和欺骗性行为”(Unfair and Deceptive Practices,以下简称“UDAP”)法规,并在州总检察长办公室下设立了消费者保护司。由于对于隐私和数据安全的调查往往涉及较为复杂的技术性问题,消费者在查清案件事实上存在困难。20世纪90年代后,州总检察长办公室开始通过UDAP法规来保护消费者免受商业行为对其隐私的侵害。此外,州总检察长诉讼的模式也可以避免消费者滥诉。^①

然而,这种模式也受到质疑。由于总检察长办公室对是否提起诉讼拥有最终的决定权,因此,受到侵害的消费者无法控制自己的追索权。并且,由于州总检察长是民选官员,因此,难免会受到利益团体游说,被选举政治所影响。^②在个人信息的侵权案件中,州总检察长诉讼模式下,由于诉讼的最终决定权并不掌握在消费者手中,生物识别信息的主体很有可能无法获得充分救济。

从救济方式看,WBPA对违法者每次违法行为的最高处罚金额仅为2,000美元。相对于利用生物识别信息所获得的利益而言,这样的处罚数额难以产生足够的震慑力。而对于信息主体因生物识别信息泄露或滥用而可能遭受的损害而言,这样的救济是不充分的。因此,WBPA救济规则可能导致法律实施效果不理想。

三、美国州立法经验的启示与反思

从BIPA到WBPA,美国三部州一级的立法形成了两种立法倾向:严格保护进路和商业友好进路,二者均有各自的优缺点。两种不同进路背后的立法理念及其各自的法律实践和社会后果值得参考。在考量立法进路时需要充分考虑到生物识别信息的双重属性,既要保护好信息主体的隐私权,也要照顾到个人信息所具有的公共性、正当的商业利用需求和表达自由。在进行具体规制时,可以通过完善信息区分、场景化行为主义规制模式以及公私结合的救济途径来实现对生物识别信息双重属性的兼顾。

(一)充分考量生物识别信息的双重属性

美国的法律实践展示了个人生物识别信息的双重属性。从人权保护的角度看,个人生物识别信息也涉及隐私权(right to a private life)和表达自由(freedom of expression)这两个相互关联并常常冲突的权利。

1948年《世界人权宣言》将隐私权作为一项基本人权加以保护。1950年《欧洲人权公约》紧随其后,保护尊重私人生活的权利。1966年联合国通过的《公民权利和政治权利国际公约》也明确保护隐私权。1981年,欧洲理事会发布了《个人数据自动化处理中的个人保护公约》。^③2000年《欧盟基本权利宪章》将个人数据保护确定为一项基本权利。^④在美国,学者沃伦(Samuel Warren)和布兰德斯(Louis Brandeis)在著名的《论隐私权》中,首次提出“隐私权”的概念,并将其定义为“个人独处的权利”。^⑤进入信息时代,学者威斯汀(Alan F. Westin)将“隐私权”定义为“个人、群体或者机构自主决定什么时候、如何以及在多大程度上将有关自身的信息披露给他人的权利”,^⑥由此形成了“信息隐私权”。美国联邦最高法院在1977年惠伦诉罗(Whalen v. Roe)案的判决中指出,受宪法保护的隐私领域的利益包括“防止披露个人事务中所体现出的个人利益”^⑦,从而从法律层面正式确立了信息隐私权。

但是信息主体对个人信息的权利不是一项绝对权利。《欧洲人权公约》第10条和《公民权利和政治权利国际公约》第19条保护表达自由,其中包括接受和传播信息和思想的自由。《个人数据处理中的个人保护公约》在其序言中指出,“个人数据保护的利益应当就其社会作用加以考虑,并且应当与包括表达自由在内的其他人权和基本自由相协调”,要将“查阅官方文件权利的原则考虑在内”,认识到“促进人与人之间信息的自由流通之必要性”。欧盟《一般数据保护条例》的声明(Recital)条款第4条也明确指出“保护个人数据的权利不是绝对权利,必须根据比例原则,考虑其社会中的作用,并且与其他权利进行权衡”。在美国,信息隐私权在理论和法律层面的确

立,使得个人获得了对个人信息控制权利。但这种权利也不是绝对的,如前文所述,美国联邦最高法院在一系列的判例中确定了言论自由包括信息创造、获取和传播的自由。信息隐私权必须与信息表达自由相平衡。

从理论上,个人信息具有公共性。施瓦茨(Paul M.Schwartz)教授认为,个人信息的交换会形成“隐私公共空间”(privacy commons)。“信息隐私像干净的空气或国防一样,发挥着作为一种公共物品的功能”,因此,信息隐私可以被看作是一种需要一定程度的社会和法律控制来构建和维护的公共空间。^⑦费尔菲尔德(Joshua A.T.Fairfield)和恩格尔(Christoph Engel)教授也认为信息隐私具有公共性,并指出,“对隐私公共物品性质的忽视将导致隐私政策误入歧途”。他们解释了过度重视个人隐私保护实际上会导致对他人隐私和社会利益的损害,因此,需要通过促进社会在隐私方面的集体行动(collective action),才能避免或补救这一“社会困境”。^⑧

作为特殊的一类个人信息,生物识别信息同样具有双重属性。一方面,生物识别信息承载着信息主体人格尊严、隐私权等基本权利。并且,由于具有专属、唯一以及不可变更等特性,生物识别信息具有更高的敏感度。生物识别信息能更好地标识个人,一旦和其他信息相结合,便能精准地勾勒信息主体的社交网络、行为偏好等,形成数字画像。脸书、谷歌等公司推出的引发大量BIPA诉讼的人脸识别功能就是这样的例子。对用户照片进行人脸识别,并做出标签,会使得个人生活更多地暴露给其他人。大数据时代,“这种在海量数据中进行筛选的能力,有可能抹去人们在公共生活和私人生活之间精心构建的界限”^⑨,进而对个人隐私造成侵害。对个人隐私的侵害还可能对个人声誉产生负面影响,进而侵害个人的人格尊严。一个明显的例子是,美国俄亥俄州的新闻主播凯瑟琳·博斯利(Catherine Bosley)到佛罗里达州度假,由于她认为周围都是陌生人,因此参加了“湿T恤”比赛。但随后照片和视频被传到网上,她也因此被电视台解雇。^⑩对此,有学者指出,

“由于人脸搜索引擎,发生在博斯利身上的事很可能会更频繁地发生在其他人身上”^⑪。

但另一方面,生物识别信息也具有公共性,涉及公共利益,而非完全处于个人领域内。现代社会个人很难完全独立于世。例如,人总是生活在一定的社群之内,人脸、声纹、步态等个人生物识别信息不可避免地会在一定的公共领域内被收集、储存并进行一定程度的流通。当个人出现在商店、餐馆等公共场所时,其生物识别信息也必然会被同一场所内的其他人获取和识别。在这样的场景下,个人不可能主张对自己生物识别信息的绝对控制权。同时,生物识别信息的利用也有着促进社会公共利益的方面。生物识别技术在安全认证领域的应用,对于保护个人人身和财产安全有着重要的作用,有利于维护社会治安。此外,生物识别技术还能运用于社会治理领域,提升社会管理水平,例如打击“号贩子”、便利养老金发放等。^⑫因此,在生物识别信息的保护中,也应当注意到个人信息的公共性,从而避免过度保护导致的对其他权利的损害。

(二)完善商业利用生物识别信息法律规则的路径

个人生物识别信息的双重属性,使得立法者必须不同权利和利益之间进行平衡。本文提出,可以通过完善信息区分、场景化行为主义的规制以及公私结合的救济路径来构建商业利用生物识别信息的法律规则。

1. 完善信息区分

不同的个人信息有着不同的敏感度,不同信息的处理对个人隐私造成的风险也不相同。^⑬个人一般信息(如手机号码、家庭住址等)被泄露或滥用的损害后果较为轻微(例如垃圾信息对私人生活安宁的干扰),达不到严重损害的程度。^⑭相比较而言,生物特征具有唯一、不可更改的特性,生物识别信息一旦被泄露或滥用,极有可能发生身份被窃取等情况,严重威胁信息主体的人格权、财产权等基本权利,并且,这样的损害难以获得完全的恢复。因此,在对个人信息的法律保护上,需要对生物识别信息的储存

和利用进行相比一般个人信息更严格的规制。

从域外立法上看,不少国家和地区已经在立法中对个人信息的类型进行了区分,进而提供不同的保护。《个人数据处理中的个人保护公约》最早区分了个人一般信息和个人敏感信息。欧盟《一般数据保护条例》第4条和第9条将基因数据和经处理可识别特定个人的生物特征数据纳入个人敏感数据当中,原则上禁止处理。从BIPA到WBPA,美国现行的三部生物识别隐私法都将生物识别信息与其他个人信息相区别,规定了专门的保护规则。特别是,BIPA和CUBI分别定义了生物识别信息和敏感信息;在生物识别信息的保护标准上,明确规定要采用比其他敏感和机密信息相同或更高的标准。

信息区分在我国已经有着一定的基础。如前文所述,《个人信息保护指南》《个人信息安全规范》《个人金融信息保护技术规范》都明确区分了个人一般信息和个人敏感信息。在学界,也有不少学者提出对个人信息进行分类保护或者对敏感的个人信息进行特别规定。^⑤还有学者进一步提出,应当在各类个人信息单行法律法规中对敏感的个人信息进行特别规定。^⑥《个人信息保护法(草案二次审议稿)》已经初步确立了信息区分。因此,我国可在未来的立法中结合国内外立法和理论经验,在法律、行政法规中进一步完善信息区分,对生物识别信息等敏感信息规定信息收集、储存、处理等不同环节的更为严格的保护规则。

2. 场景化行为主义的规制方式

生物识别信息的敏感性要求更高的保护,但并不意味着绝对的保护。实际上,生物识别技术在不同的场景下和不同的信息处理环节中,对生物识别信息安全所带来的风险程度是不同的。因此,可以通过场景化行为主义的规制方式来实现生物识别信息的高度敏感性与一定的公共性之间的平衡。

个人信息保护应当根据信息收集、储存、处理等不同环节所可能侵犯个人与社会的权益而进行不同程度的规制,以确保个人信息流通的各个环节都能得到法律的合理介入。^⑦对于生物识别信息,本文认

为,生物特征数据仅仅是对个人生物特征的数字化表述,并不直接与具体个人身份信息相关联,对生物特征数据的采集并不会直接对个人信息主体的权利造成损害,只有当数据经过一定的处理,才有侵害个人信息主体权利的可能。因此,在生物识别信息的法律规制中,可以根据场景的不同采取不同的收集规则,一定程度上采取相对宽松的规制方式,以利于生物识别信息公共价值的实现。对于信息的储存和披露,由于生物识别信息的高度敏感性,应当采取比一般个人信息更严格的规则。具体而言,可以借鉴BIPA和CUBI,规定信息控制者必须以和其他敏感信息相同或更高的标准储存、传输和保护生物识别信息,并通过强制性国家标准等规范,确定加密、分段等储存和传输方式;要求信息收集者、控制者在保存一定的期限后必须删除;此外,应当严格禁止信息出租、出售或者其他披露行为,并将例外情形严格限制在法律要求、主体同意或授权的金融交易需要等范围内。

个人信息是高度场景化的,不同场景下的个人信息可能需要不同程度的规制。^⑧生物识别信息也是如此。生物识别主要有两种应用方式:“验证”(Verification)和“辨识”(Identification)。前者是“1对1”的验证,即通过比较被识别对象的生物特征数据和数据库的模板数据,判断被识别对象和数据库模板数据的主体是否为同一个人;后者是“1对N”的辨识,即通过将个人的生物特征数据与数据库中存储的所有记录进行比较来确定被识别对象的身份。^⑨“1对1”的验证广泛应用于门禁系统、手机解锁、微信和支付宝的支付程序等。而线下零售中,商店通过摄像头记录顾客行为轨迹和面部表情等,来分析顾客对商品的需求,则属于生物识别技术辨识身份的应用场景。相比较而言,生物识别技术的风险主要集中于“1对N”辨识的应用场景中。

对于“1对1”的验证场景,本文认为,可在数据收集规则上降低规制力度,以实现生物识别信息的公共性和利用价值。在门禁系统等应用场景中,收集数据时,向被识别对象发出通知并获得明示的同意,

既不现实也无必要。因此,可以在身份验证的场景中,推定进入一定识别范围内的被识别对象同意;或者借鉴WBPA的模式,仅在需要将数据储存在数据库时,要求通知并获得同意。对于“1对N”辨识的应用场景,由于其具有辨识个人的功能,因此需要在数据收集规则上加以更严格规制,要求收集者明确告知并获得同意,数据用途也应当受到严格的限制。

3.公私结合的救济途径

在救济途径上,BIPA采用了私人诉讼模式,而CUBI和WBPA则采用了州总检察长诉讼模式,但如前文所述,这两种救济模式均存在不足。伊利诺伊州通过罗森巴赫案确立了对BIPA程序性规定的违反即构成侵权的规则,但这样的判决是否合宪仍存在着争议。^⑨在我国,信息收集者、控制者仅违反程序性规定是否构成侵权,同样也并无定论。^⑩在损害的认定、因果关系等信息侵权理论问题还没有解决的情况下,如果广泛赋予个人诉讼权,可能导致与伊利诺伊州相似的过度诉讼的情况出现,进而降低救济效率。此外,由于技术的专业性,对信息侵权案件的事实调查也需要专业机构的介入。而CUBI和WBPA的州总检察长诉讼模式虽有助于查清事实、提高救济效率,但也面临着剥夺了信息主体诉讼权利的问题。

从域外立法趋势上看,由于个人信息的公共属性越来越明显,近年来,美欧主要的数据保护法都采取公法保护为主、有限赋予个人诉讼权的路径。^⑪2018年颁布、2020年生效的美国《加州消费者隐私法》(California Consumer Protection Regulations)在救济途径上,规定了州总检察长具有广泛的规制权力,同时,也赋予了个人对于“未加密和未经授权的个人信息”在信息收集者、控制者违反程序义务而“受到未经授权的访问和过滤、盗窃或泄露的影响”的情况下提起诉讼的权利。^⑫由于英美法律传统并不严格区分公法和私法,行政执行的程序也通过民事诉讼程序来实现。^⑬因此,美国州总检察长诉讼的模式本质上是行政处罚的程序。行政规制为主有利于提高救济效率,同时,有限地赋予个人诉讼权,有利于保

障个人信息主体在因数据泄露等特定类型的信息侵权案件中获得充分救济的权利。

我国在未来生物识别信息商业利用的立法规制中,可以借鉴公法保护为主、有限赋予个人诉讼权的模式。相比美国的州总检察长是民选职位、更易受到选举政治的影响,我国的检察机关更易从公共利益平衡的角度起诉滥用个人生物识别信息的商业行为;还可以通过专门的信息监管机构、强化对监管机构的授权等方式,对信息收集者、控制者进行有效的监管,及时纠正违法违规行为,并通过行政责任乃至刑事责任对违法违规行为形成震慑效应。同时,有限地赋予个人在生物识别信息泄露等特定类型的信息侵权案件中的诉讼权,以实现对个人权利的保障。

结语

美国法的两种不同立法倾向及其相应的问题,反映了生物识别信息具有高度敏感性和一定的公共性。生物识别信息的高度敏感性要求在立法上采取区别于其他个人信息的更严格的保护规则。但是,过度的保护会妨碍生物识别信息公共性价值的实现,损害社会利益,因此,需要根据场景和信息处理环节的不同作出场景化行为主义的规制。此外,在救济规则上,应该通过公法保护为主、有限保障个人诉讼权的模式,以实现生物识别信息的有效规制。

注释:

①参见张铎:《生物识别技术基础》,武汉大学出版社2009年版,第1页。

②根据前瞻产业研究院的报告,预计到2023年,我国生物识别行业市场规模将达到379亿元。参见前瞻产业研究院:《2021-2026年中国生物识别技术行业市场调研与投资预测分析报告》。

③例如,有报告显示,我国一些应用软件存在着过度收集个人生物识别信息的问题。参见中国消费者协会:《100款App个人信息收集与隐私政策测评报告》,载中国消费者协会网,http://www.cca.org.cn/jmx/f/detail/28310.html。有报道称,有商家公开出售大量“人脸数据”。参见《17万条“人脸数据”遭公开售卖,覆盖超2000人!》,载搜狐网,http://www.sohu.com/a/

343495053_100017041。此外,“人脸识别第一案”也引出了生物识别信息救济方面的问题。参见《人脸识别第一案:技术滥用下的隐私之殇》,载《三联生活周刊》2019年第46期,第108-113页。

④参见《中华人民共和国民法典》第1034条、《中华人民共和国网络安全法》第76条。

⑤参见《信息安全技术公共及商用服务信息系统个人信息保护指南》(GB/Z 28828-2012),5.2-5.5;《信息安全技术个人信息安全规范》(GB/T 35273-2020),5-7;《个人金融信息保护技术规范》(JR/T 0171-2020),6。

⑥参见《个人信息保护法(草案二次审议稿)》第31条、第32条。

⑦参见《个人信息保护法(草案二次审议稿)》第27条。

⑧BIPA所规制的“私营实体”指个人、合伙企业、公司(corporation)、有限责任公司(limited liability company)、协会或者其他组织。其中,与中国的“有限责任公司”不同,美国的“有限责任公司”(limited liability company)实际上是一种股份公司与合伙相结合的公司组织形式。See Illinois Compiled Statutes Chapter 740 §14/10(2008); Robert B. Taylor, Limited Liability Company, 26 Maryland Bar Journal 48, 48-50(1993)。

⑨Michelle J. Anderson & Jim Halpert, Washington Become the Third State with a Biometric Privacy Law: Five Key Differences, 1 RAIL: The Journal of Robotics, Artificial Intelligence & Law 41, 41-46(2018)。

⑩See Charles N. Insler, How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act, 43 Southern Illinois University Law Journal 819(2019)。

⑪See Illinois Compiled Statutes Chapter 740 §14/5(2008)。

⑫See Illinois Compiled Statutes Chapter 740 §14/10(2008)。

⑬See Texas Business and Commerce Code §503.001(a)(2009)。

⑭See Illinois Compiled Statutes Chapter 740 §14/10(2008)。

⑮See Illinois Compiled Statutes Chapter 740 §14/10(2008)。

⑯See Rivera v. Google Inc., 238 F.Supp.3d 1093-1095(N.D. Ill. 2017)。

⑰See Rivera v. Google Inc., 238 F.Supp.3d 1096(N.D. Ill. 2017)。

⑱See Illinois Compiled Statutes Chapter 740 §14/15(b)(2008)。

⑲See Texas Business and Commerce Code §503.001(b)(2009)。

⑳See Illinois Compiled Statutes Chapter 740 §14/15(e)(2008)。

㉑See Texas Business and Commerce Code §503.001(c)(2009)。

㉒Michael A. Rivera, Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies, 29 Fordham Intellectual Property, Media & Entertainment Law Journal 571, 591(2019)。

㉓See Illinois Compiled Statutes Chapter 740 §14/15(c)(2008)。

㉔See Illinois Compiled Statutes Chapter 740 §14/15(d)(2008)。

㉕See Texas Business and Commerce Code §503.001(c)(2009)。

㉖See Illinois Compiled Statutes Chapter 740 §14/15(a)(2008)。

㉗See Texas Business and Commerce Code §503.001(c)(2009)。

㉘See Texas Business and Commerce Code §503.001(c- 2)(2009)。

㉙Michael A. Rivera, Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies, 29 Fordham Intellectual Property, Media & Entertainment Law Journal 571, 603(2019)。

㉚See Illinois Compiled Statutes Chapter 740 §14/20(2008)。

㉛See e.g. Mc Collough v. Smarte Carte, Inc., No.16- cv- 3777, 2016 WL 4077108(N.D. Ill. 2016); Sekura v. Krishna Schaumberg Tan, Inc., No.2016 CH 4945(Ill. Cir. Ct.2017)。

㉜See Rosenbach v. Six Flags, 2019 IL 123186, p.10-11。

㉝See Rosenbach v. Six Flags, 2019 IL 123186, p.11-13。

㉞See Texas Business and Commerce Code §503.001(d)(2009)。

㉟Michael A. Rivera, Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies, 29 Fordham Intellectual Property, Media & Entertainment Law Journal 571, 603(2019)。

㊱See Jane Bambauer & James E. Rogers, Biometric Privacy Laws: How a Little-Known Illinois Law Made Facebook Illegal, Program on Economics & Privacy(21 June 2017), <https://pep.gmu.edu/2017/06/21/new-paper-biometric-privacy-laws-how-a-little-known-illinois-law-made-facebook-illegal/>。

㊲See New York Times Co. v. Sullivan, 376 U.S. 254(1964)。

㊳See Va. Pharmacy Bd. v. Va. Consumer Council, 425 U.S. 748(1976)。

㊴See Sorrell v. IMS Health Inc., 131 S. Ct.2653(2011)。

㊵Joseph Raz, Free Expression and Personal Identification, 11 Oxford Journal of Legal Studies 303(1991)。

㊶See Charlotte Hess & Elinor Ostrom, Ideas, Artifacts, and

Facilities: Information as a Common-Pool Resource, 66 Law and Contemporary Problems 111, 111-145(2003).

⑫See Lauren Stewart, Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security, 60 Boston College Law Review 349, 380(2019).

⑬Learn More about Familiar Face Detection and Managing Your Library, Nest Support, <https://nest.com/support/article/Familiar-face-alerts>.

⑭See Boyd Garriott, How Patel v. Facebook Might Tee up a Privacy Battle at the Supreme Court, Wiley Connect(16 October 2019), <https://www.wileyconnect.com/home/2019/10/16/how-patel-v-facebook-might-tee-up-a-privacy-battle-at-the-supreme-court>.

⑮See BIPA Update: Class Actions on the Rise in Illinois Courts, Holland & Knight(22 July 2019), <https://www.hklaw.com/en/insights/publications/2019/07/bipa-update-class-actions-on-the-rise-in-illinois-courts#:~:text=According%20to%20Court%20house%20News%20Service%2C%202013%20BIPA%20cases,at%20employers%20utilizing%20fingerprint%20technology%20for%20timekeeping%20purposes>.

⑯See In re Facebook Biometric Information Privacy Litig., No.15-cv-03747(N.D. Cal.).

⑰See Jonathan Bilyk, L.A. Tan Settles Fingerprint Scan Privacy Class Action for \$ 1.5M; Attorneys Get \$ 600K, Cook County Report(9 December 2016), <https://cookcountyrecord.com/stories/511056103-1-a-tan-settles-fingerprint-scan-privacy-class-action-for-1-5m-attorneys-get-600k>.

⑱See Lorraine Swanson, Illinois Facebook Users Can Claim up to \$ 400 in Class Action Suit, MSN(23 September 2020), <https://www.msn.com/en-us/lifestyle/lifestyle-buzz/illinois-facebook-users-can-claim-up-to-dollar400-in-class-action-suit/ar-BB19kuiN>.

⑲华盛顿州、阿拉斯加州、蒙大拿州、新罕布什尔州、康涅狄格州以及纽约州都提出综合性生物识别保护立法。See Jared Bennett, Saving Face: Facebook Wants Access without Limits, The Center for Public Integrity(31 July 2017), <https://www.publicintegrity.org/2017/07/31/21027/saving-face-facebook-wants-access-without-limits>.

⑳ Kartikay Mehrotra, Tech Companies Are Pushing back

against Biometric Privacy Laws, Bloomberg(20 July 2017), <https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws>.

㉑See Washington Revised Code §19.375.900(2017).

㉒See Washington Revised Code §19.375.010(1)(2017).

㉓See Washington Revised Code §19.375.010(5)(2017).

㉔See Washington Revised Code §19.375.010(4),(8)(2017).

㉕See Washington Revised Code §19.375.020(7)(2017).

㉖Lauren Stewart, Big Data Discrimination: Maintaining Protection of Individual Privacy without Disincentivizing Businesses' Use of Biometric Data to Enhance Security, 60 Boston College Law Review 349, 378(2019).

㉗See Washington Revised Code §19.375.020(1)(2017).

㉘See Washington Revised Code §19.375.020(2)(2017).

㉙See Washington Revised Code §19.375.010(4)(2017).

㉚See Washington Revised Code §19.375.020(3)(2017).

㉛See Washington Revised Code §19.375.020(5)(2017).

㉜See Washington Revised Code §19.375.020(4)(2017).

㉝See Washington Revised Code §19.375.030(2017).

㉞See Washington Revised Code §19.86.140(2012).

㉟See e.g. Norberg v. Shutterfly, Inc., 152 F.Supp.3d 1103 (2015); In re Facebook Biometric Info. Privacy Litig., 185 F. Supp.3d 1155(N.D. Cal.2016); Rivera v. Google Inc., 238 F. Supp.3d 1093-1095(N.D. Ill.2017).

㊱See Louise Matsakis, Scraping the Web Is a Powerful Tool. Clearview AI Abused It, WIRED(25 January 2020), <https://www.wired.com/story/clearview-ai-scraping-web/>.

㊲See Michael A. Rivera, Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies, 29 Fordham Intellectual Property, Media & Entertainment Law Journal 571, 603(2019).

㊳See Alexandro Pando, Beyond Security: Biometrics Integration into Everyday Life, Forbes(4 August 2017), <https://www.forbes.com/sites/forbestechcouncil/2017/08/04/beyond-security-biometrics-integration-into-everyday-life/#38724d81431f>.

㊴See Lara Tumbel, Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law, Bloomberg Law(13 October 2017), <https://news.bloomberglaw.com/privacy-and-data-security/washingtons-new-biometric-privacy-statute-and-how-it-compares-to-illinois-and-texas-law>.

⑦⑩ See Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 *Notre Dame Law Review* 747, 753–754 (2016).

⑦⑪ See Emily Myers & Ayeisha Cox, *The Authority of State Attorneys General and Their Efforts on 21st Century Policing*, *The Book of the States* 2016, http://www.knowledgecenter.csg.org/kc/system/files/Myers_Cox_2016.pdf.

⑦⑫ 2012年欧洲委员会通过公约修正案,删除了“自动化”,改名为《个人数据处理中的个人保护公约》。

⑦⑬ 《欧盟基本权利宪章》第8条第1款规定:“每个人都有权保护涉及自身的个人数据。”

⑦⑭ See Samuel D. Warren & Louis D. Brandeis, *Right to Privacy*, 4 *Harvard Law Review* 193, 193–220(1890–1891).

⑦⑮ See Alan F. Westin, *Privacy and Freedom*, Atheneum, 1967, p.7.

⑦⑯ *Whalen v. Roe*, 433 U.S. 425(1977), p.599–600.

⑦⑰ See Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 *Harvard Law Review* 2056, 2084–2090(2004).

⑦⑱ See Joshua A. T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 *Duke Law Journal* 385, 385–458(2015).

⑦⑲ See A. J. McClurg, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 *Harvard Law Review* 1870, 1874(2007).

⑦⑳ See Connie Schultz, *Bare Facts Don't Tell Whole Story*, *PLAIN DEALER*(Cleveland), 29 January 2004, at Fi, LEXIS, News Library, Clevpd File.

⑦㉑ Jim Barr Coleman, *Digital Photography and the Internet*, *Rethinking Privacy Law*, 13 *Journal of Intellectual Property Law* 205, 205–207(2005).

⑦㉒ 参见王丹娜:《生物识别:传统信息安全在新技术环境的创新应用》,载《中国信息安全》2019年第2期,第60–64页。

⑦㉓ 参见孔令杰:《个人资料隐私的法律保护》,武汉大学出版社2009年版,第213页。

⑦㉔ 参见吴标兵、许和隆:《个人信息的边界、敏感度与中心度研究——基于专家和公众认知的数据分析》,载《南京邮电大学学报(社会科学版)》2018年第5期,第44–53页。

⑦㉕ 参见张新宝:《从隐私到个人信息:利益再衡量的理论与制度安排》,载《中国法学》2015年第3期,第38–59页;鞠晔、王平:《云计算背景下欧盟消费者个人敏感数据的法律保护》,载《法学杂志》2014年第8期,第79–85页;胡文涛:《我国个人敏感信息界定之构想》,载《中国法学》2018年第5期,第235–254页;田野、张晨辉:《论敏感个人信息的法律保护》,载《河南社会科学》2019年第7期,第43–49页。

⑦㉖ 参见张鹏:《论敏感个人信息在个人征信中的运用》,载《苏州大学学报》2012年第3期,第97–103页。

⑦㉗ 参见丁晓东:《个人信息的双重属性与行为主义规制》,载《法学家》2020年第1期,第64–76页。

⑦㉘ See Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 *UCLA Law Review* 1701, 1701–1778(2010); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 *New York University Law Review* 1814, 1814–1894(2011).

⑦㉙ See Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 *Hastings Communications and Entertainment Law Journal* 653, 655–656(2003).

⑦㉚ 美国联邦最高法院在斯波基奥公司诉罗宾斯(*Spokeo Inc.v.Robins*)案中认为,根据美国《宪法》第3条,原告必须受到实际损害才有资格提起诉讼,不能“仅仅主张一个没有任何具体损害的、纯粹程序上的违法”。因此,伊利诺伊州最高法院对罗森巴赫案的判决存在着是否违反美国联邦最高法院斯波基奥公司案判决的争议。See *Spokeo Inc.v.Robins*, 136 S. Ct.1540(2016).

⑦㉛ 参见高富平:《个人信息保护:从个人控制到社会控制》,载《法学研究》2018年第3期,第84–101页。

⑦㉜ 参见王融、黄致韬:《迈向行政规制的个人信息保护:GDPR与CCPA处罚制度比较》,载搜狐网, https://www.sohu.com/a/381134650_455313。

⑦㉝ See California Consumer Protection Regulations 1798.150 (a),(c).

⑦㉞ See Robert A. Kagan, *Adversarial Legalism: The American Way of Law*, Harvard University Press, 2001, p.3–15.