

《个人信息保护法》实施中生物识别信息的特殊保护机制研究

王丹, 蒋倩, 江旭, 陈诗慧, 辛芳

江南大学法学院, 江苏 无锡

收稿日期: 2024年3月20日; 录用日期: 2024年4月7日; 发布日期: 2024年5月17日

摘要

在网络与数字技术不断发展的背景下, 生物识别信息保护领域所牵涉的各方主体应当被合理且正当的分配效益与风险, 《个人信息保护法》的颁布与实施为个人生物识别信息的保护拉开了序幕, 但司法实践仍面临重重阻碍。对此, 应当明晰信息处理所涉主体的权利义务关系、构建信息流通中监督反馈、司法适用、利益平衡并重的特殊保护机制, 以维护生物识别信息权利人的权益。

关键词

生物识别信息, 特殊保护机制, 利益衡量

Research on the Special Protection Mechanism of Biometric Information in the Implementation of the Personal Information Protection Law

Dan Wang, Qian Jiang, Xu Jiang, Shihui Chen, Fang Xin

Law School of Jiangnan University, Wuxi Jiangsu

Received: Mar. 20th, 2024; accepted: Apr. 7th, 2024; published: May 17th, 2024

Abstract

In the context of the continuous development of the network and digital technology, all parties involved in the field of biometric information protection should be reasonably and properly allo-

文章引用: 王丹, 蒋倩, 江旭, 陈诗慧, 辛芳. 《个人信息保护法》实施中生物识别信息的特殊保护机制研究[J]. 法学, 2024, 12(5): 2956-2963. DOI: 10.12677/ojls.2024.125421

cated benefits and risks. The promulgation and implementation of the Personal Information Protection Law has kicked off the protection of personal biometric information, but judicial practice still faces many obstacles. In this regard, it is necessary to clarify the rights and obligations of the subjects involved in information processing, and build a special protection mechanism that focuses on supervision and feedback, judicial application, and balance of interests in information circulation, so as to safeguard the rights and interests of biometric information holders.

Keywords

Biometric Information, Special Protection Mechanism, Interest Measurement

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 生物识别信息司法保护的现实困境

2021年11月1日,我国《个人信息保护法》正式实施,该法首次确立了“敏感个人信息”的法律概念,“生物识别信息”被列举为敏感个人信息进行特殊保护。但《个人信息保护法》实施以来,现有的救济途径仍未能有效的震慑生物识别信息侵权行为,对生物识别信息的司法保护仍不成熟。

1.1. 监管体制有待厘清

随着《个人信息保护法》的出台,生物识别信息应用的监管问题逐渐得到重视。但由于立法规范中监管主体不明确、部门分工不明晰,监管空缺、监管交叉、监管推诿等问题时常发生,现有规范中“国家网信部门及有关部门”的表述仍无法得出相关行政部门的具体分工。监管部门之间各自为政和碎片化的监管难以形成统一的标准,大大降低了生物识别信息的监管效能,也导致不能有效预防或及时遏制生物识别信息侵权行为。

1.2. 法律适用衔接有待加强

个人生物识别信息法益的多元属性涵盖了对隐私权、人格权、财产权的保护,决定了其合理使用和权利保护的多元价值。但个人信息保护法、民法典、行政法或刑法具有各自的立法价值目标,不同的部门法有各自的调整对象和适用范围,相互之间出现交叉竞合甚至冲突矛盾在所难免。因此,司法实践中应发挥各个部门法在权利保护方面的功能,实现不同法律之间的良性互动,以寻求促进个人生物识别信息相关法律法规衔接适用的有效路径[1]。

1.3. 企业、政府、个人间的利益冲突有待平衡

党的二十大强调加快发展数字经济,在“数字融合”的过程中,人体指纹、面容、虹膜等个人生物识别信息常常应用在主体识别、物联网等场景中,个人生物识别信息的商业应用处于高速发展期。商业化应用的快速扩张必然伴随着风险的增加,信息采集未授权、流动不透明、处理不合规等问题愈发凸显,例如,众多售楼处未经授权直接拍摄客户进行识别,用作中介佣金分配依据或客户喜爱倾向等信息的采集;《个人信息保护法》实施后,商家仍通过限制消费者选择权变相的收集、利用生物识别信息,如刷脸支付。若某些机构在收集个人生物识别信息后违法使用,不仅会造成个人生物识别信息权益受到损害,而且极易助长经济市场上的不正当竞争等乱象。

知微见著,基于个人生物识别信息的独特属性,信息被大量的收集、处理、利用是一种必然的趋势,随着个人的面部、指纹、视虹膜、基因(DNA)等生物信息识别信息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,相伴而生的是巨大的安全隐患和法律风险。政府部门有需求,公司要抢占市场,二者“合谋”,让存在大量风险隐患的人脸识别应用“遍地开花”,这一过程本质上是多元主体之间利益的角逐。

针对以上问题,唯有准确界定生物识别信息,阐明其特殊性,并构建相应的特殊保护机制,才能在充分保护个人生物识别信息的同时对此类信息进行限制性的开发利用,寻求双赢局面。

2. 生物识别信息特殊保护的必要性和实践经验

2.1. 生物识别信息的特殊性决定其保护的必要性

个人生物识别信息包括自然人的身体、生理特征的相关信息如指纹、声纹、掌纹、虹膜、面部特征、个人基因等。不同于一般个人信息,生物识别信息所蕴含的生物特征和人格特征是直接指向自然人本质的,并且是无法替换和更改的,一旦被泄露将会对被侵权人财产和精神造成极大的损害,难以弥补。

2.1.1. 唯一性与人身属性

生物识别信息与一般个人信息例如电话号码、电子邮箱地址、身份证号码等相比具有显著差异:前者直接反映信息主体内在的身体、生理和行为本质属性,无需和其他信息进行结合即可快速为生物识别信息匹配出对应的身份主体,而后者则以信息主体的社会性特征为基础外化于人本身,这种外在的社会属性决定了该类信息与人身不具有实质且唯一的绑定关系。生物识别信息具有高度人身属性,使其常与道德风险相挂钩,其承载的人格尊严与个人隐私天然需要特殊保护。

2.1.2. 高度敏感性与易识别性

与一般个人信息相比,生物识别信息属于个人敏感信息,一旦泄露或者非法使用,可能导致个人受到歧视或者人身、财产安全受到严重危害,这种具有高度敏感性的信息却又因现代科技的发展而具有易识别性,在未经信息权利主体授权的情况下,个人或者组织就可以收集、存储、处理个人的生物识别信息,例如,侵入式监视技术可以突破公共场所的匿名性,使得人们从“匿名”走向“显名”。由此观之,对生物识别信息进行特殊保护更具有必要性。

2.2. 生物识别信息保护模式的域外经验

2.2.1. 生物识别信息司法保护的价值取向

欧盟《一般数据保护条例》(简称 GDPR)是现代社会保护个人数据安全迈出的重要一步,其被称为“史上最严格的数据保护法案”。GDPR 是通过知情同意权、访问权、删除权等权利束意图加强信息主体对个人信息的支配和控制,其通过综合立法的模式将不同级别、种类、性质的个人信息纳入统一的个人信息保护法之下,将行政、民事以及刑事等法律的保护措施集为一体,明确“禁止处理”“明示同意”“法定必需”为包括个人生物识别信息在内的个人特殊敏感类型新数据处理的三大特定法律原则¹。

在 Facebook 人脸识别一案中,Facebook 公司在未经许可的情况下,从该州数百万用户的照片中获取面部数据用于标签建议,从而引发了一起集体诉讼[2]。该案中确立了“程序性违法”原则,即无论收集方收集、使用生物识别信息的行为对信息主体是否造成了实际损害后果,只要收集行为并未事前告知或与事前告知的情况不符,则依然构成侵权,且由于该行为将生物识别信息主体暴露在不确定的风险之中,收集方应承担相应赔偿责任[3]。

¹ 参见欧盟《一般数据保护条例》GDPR 第 14、15、16、17 条。

总体而言,欧美对生物识别信息的保护模式均秉持着个人权益保护优先于信息流通变现的价值取向,并通过制度设计对生物识别信息进行了较为体系化且有效的保护。在我国现有法律框架下,个人生物识别信息保护的价值取向仍存在模糊性,我国在司法实践中可借鉴域外经验以更好的维护公民个人信息安全,促进社会的和谐发展。

2.2.2. 生物识别信息流通的多元监管

美国主要采取分散立法、多元监管、行业自律的模式,没有成立专门的监管机构,而是将对个人信息的保护工作交给各行业或各领域的主管机关负责,以此更有针对性的对个人信息进行保护。此模式符合美国的国情,体现了其对个人信息所蕴含的经济效益的重视,可以兼顾各行业的特殊性进行个性化的保护,但该模式缺少统一的监管标准,且行业自律监督方式缺乏法律强制力,难以达到预期的监管效果。

不同于美国的分散式监管,欧盟采取了统一的监管模式:一方面,欧盟通过制定各种条例及指令,形成了统一的一般性原则;另一方面,各成员国所设置的监管机构在EDPB的统一领导下开展监管工作,“统分”结构对个人信息保护进行递进式的监管,辅以企业内部的保护监管制度,为欧盟个人信息保护监管机制建立起了有力的保障[4]。此种监管机制很大程度上保障了个人信息安全,对我国生物识别信息保护机制的构建具有巨大的参考价值。

我国在完善个人信息监管模式时应当综合考量实际情况,个人信息保护的监管既要发挥政府部门统筹监管的作用,也要发挥行业自律的优势;监管个人信息还应当权衡效益和安全之间的利弊,不能放松对个人信息安全保护,也不能过分抑制个人信息流动带来的经济效益。

3. 生物识别信息特殊保护机制构建的原则

3.1. 以保障人格权为根本原则

《民法典》第1034条将生物识别信息纳入个人信息范畴作为人格权的一项内容进行保护。《民法典》将之纳入人格权编,说明了生物识别信息具备人格属性,自然人与其具有人格属性的生物识别信息应当是一体的。《民法典》第991条规定:“民事主体的人格权受法律保护。任何组织或者个人不得侵害。”由于生物识别信息具有极强的人身属性,人格与人身不可分割,人格权是民事主体对其特定的人格利益享有的权利,关系到每个人的人格尊严,是民事主体最基本、最重要的权利。因此,尊重和保障人格权是个人生物识别信息使用和保护的**根本原则[5]。

3.2. 私法与公法双重保护原则

在信息数据社会中,大数据的体量计算及区块链、元宇宙等信息技术的快速发展为个人生物识别信息实现其丰富的商业价值和公共管理价值提供了可能性,赋予生物识别信息全新的价值性与经济性。基于此,生物识别信息将在一定程度上和一定范围内不可避免地由于社会秩序、公共目的、商业价值需要而被使用,信息主体对个人生物识别信息的保护需求与信息处理者对个人生物识别信息的利用需求之间的矛盾日益激化,生物识别信息保护的公力救济与私力救济都凸显出严重的问题,这意味着在个人生物识别信息的保护应当从私法和公法两方面入手同时进行保护。

生物识别信息在私法保护上应当主要倾向于生物识别信息基于财产属性的商业利用价值,规范生物识别信息权利人与信息处理者这一对平等私法主体之间的权利义务;公法保护上侧重于政府和公共机构对生物识别信息的收集和使用的限制问题,以便有力的规制生物识别信息在共享使用中的法律风险[6],另外,政府与司法部门还应当承担相应的监督管理与提供救济路径的责任。将私法保护与公法规范相统一,有利于在社会总体层面上降低生物识别信息侵权的概率与损害程度。

3.3. 比例原则

我国的《宪法》规定之中无论是关于权利的保障还是权力的限制等内容，都蕴含了比例原则的基本精神，其中体现出的均衡、公平等理念，具有普适性，是行政合理性原则的具体体现，在公法范围内具有其固有的适用空间，可以作为政府部门从事行政执法活动的指导性原则。客观而言，保护与利用的平衡实质上是个人利益与公共利益的平衡，比例原则是实现二者平衡的重要方式，因此在生物识别信息保护领域更应当加强贯彻落实。

比例原则包括适当性原则、必要性原则和狭义比例原则三个子原则。首先，明确的处理目的是适当处理的前提，宽泛、模糊的进行信息收集会给个人信息带来不确定的风险，《个人信息保护法》明确要求，处理个人信息应有明确且合理的目的，且以显著方式、清晰易懂的语言真实、准确、完整地告知个人；其次，必要性原则要求处理个人信息的活动应限定在必要的范围内，防止过度收集分析个人生物识别信息，不得过度处理个人信息，确保个人生物识别信息被合理收集和有效分析利用。尤其在处理敏感个人信息时，更需要遵循“充分的必要性”，现有许多特定机构对个人生物识别信息的处理并没有遵循必要性原则，而是利用优势地位使个人达成半强迫式的同意；最后，狭义比例原则又称均衡原则，其精髓在于对手段和目的进行价值和利益上的衡平，约束行政机关收集处理个人生物识别信息的范围和幅度，强调信息处理的目的是履行法定职责、维护社会稳定安全，有利于为法律原则发挥作用提供标准。

3.4. 预防与救济并重的原则

个人生物识别信息的处理活动中蕴藏着巨大的风险，风险一旦转化为现实损害，将会产生不可逆的严重后果。当前的事后救济模式无法填平信息权利人的损失，但只要预防措施实施得当，就可以大大降低现实损害发生的可能性，从根源上保护个人生物识别信息。

对于生物识别信息侵权的救济而言，生物识别信息的侵权后果远远比一般个人信息侵权严重，在这种情况下，《民法典》对个人信息的保护路径并不完全适用于生物识别信息，因此应对其保护措施进行单独、特殊的考量。笔者认为，对于个人生物识别信息侵权中较为轻微的违法行为，应当降低立案标准，从而达到对生物识别信息侵权以及其带来的危害应有的重视程度。当前，我国个人信息流通频繁，侵权案件频发的一个重要原因就是个人信息侵权行为的违法成本较低、不被相关信息处理者所重视。实践中，对于一些难以证明损失的案件，往往只能要求信息处理者承担停止侵害、排除妨碍、消除危险的侵权责任，此种处理结果对于信息处理者来说不痛不痒，难以形成威慑力。

综上所述，生物识别信息作为高度敏感的个人信息，其保护层级应显著高于一般个人信息，结合域外经验，以《个人信息保护法》等相关法律为着眼点，我国司法实践应准确把握生物识别信息保护的各項原则，以此为据进一步构建具体的特殊保护机制。

4. 生物识别信息特殊保护机制的具体构建

4.1. 生物识别信息保护的监督机制

完善的监督机制是生物识别信息风险预防的基础。只有多元主体参与构建监督机制，使个人信息的收集和流动在透明公开的环境下运行，才能平衡企业和个人之间由于技术和资本的巨大落差而形成的不平等地位。

《个人信息保护法》规定：履行个人信息保护职责的部门为国家网信部门、国务院有关部门及县级以上地方人民政府有关部门。笔者认为，一方面，应以国家网信部门这一信息监管机构为核心，对企业 and 政府等信息处理者进行技术监管，并在实践中不断细化对企业的监督权限；另一方面，国家网信部门

应加快完善个人信息保护投诉、举报等反馈机制,积极引导社会公众参与个人信息保护工作,从而畅通公众寻求救济的渠道。

当前,随着生物识别信息技术的不断发展,互联网平台凭借其便捷性、覆盖范围之广度在新一代非实体性公共基础设施中脱颖而出。毋庸置疑,互联网平台在治理生物识别信息(尤指采集、保存和利用中出现的乱象)过程中扮演的角色也愈发重要起来。故此,加强平台监控、落实互联网平台责任的必要性也逐渐彰显、加强。基于上述原因,笔者认为,结合现状及实践发展需要——在社会层面,较能展现出有益效用的做法应为对互联网平台进行社会监督,激发行业自律监督。只有形成行业自律、行政监管、公众参与的多方共治监督机制,才能使生物识别信息保护工作在监督下有序进行,真正做到防患于未然[7]。

4.2. 法律适用的灵活衔接

笔者认为,生物识别信息特殊保护机制的构建可以从私法保护路径和公法保护路径出发,充分考虑个人信息保护法律制度与其他相关法律的衔接与适用问题。

4.2.1. 《个人信息保护法》与《民法典》的协同适用

《民法典》区分个人信息与私密信息,将私密信息作为隐私的组成部分进行保护;《个人信息保护法》为避免个人人格尊严遭受侵害,特别规定敏感个人信息处理规则。具体而言,私密信息的规定强调在民事救济上适用隐私权的责任认定标准;敏感个人信息侧重于规范信息处理行为本身,对信息处理者提出了高标准要求。两者存在一定范围的重合,笔者认为,在具体案件中,应当根据个人信息处理的阶段和侵权责任发生的阶段,结合具体情况分别进行适用。

4.2.2. 《个人信息保护法》与相关行政法的互补

《个人信息保护法》与行政法的衔接主要体现在相关部门依法处罚信息处理者侵害个人信息合法权益的行为。当前,对应用软件中的隐私条款进行评估和审查是我国相关监管部门规范个人信息收集情况的重要内容之一,具体做法为:执法部门对不按照法律规定进行个人信息收集的应用软件发出限期整改通知,并对逾期未整改的应用软件予以下架处理。

《个人信息保护法》出台后,对相关案涉主体的行政责任进行了更为严格、全面的规定,但条文的设置仍较为抽象,整体而言,执法部门的监管工作并不能因而有效地推进、落实。基于上述原因,将《个人信息保护法》与《行政处罚法》、《行政许可法》等相关行政法内容进行合理、有效的衔接,细化各环节的监督工作并相应地规范监管程序,有利于实质有效的达到保护信息权利人之合法权益的目的[8]。

4.3. 生物识别信息利益相关者间的利益平衡

在数字化时代的大背景下,生物识别信息被大量采集、广泛运用于经济、社会管理活动中。基于此,一方面,以发展的眼光看待,对个人信息的采集、处理和利用客观上不可避免;另一方面,这种采集使用可能造成使个体人格权、财产权被侵害的巨大风险,其中牵涉至少公民个人、企业、政府三方利益主体,故此,对于生物识别信息的特殊保护必须充分考量对于三者间利益与需求的平衡。

4.3.1. 个人私益与商业利益间的平衡

基于上述分析,对生物识别信息的利用是存在风险的,但由此而“一刀切”式地杜绝对其加以利用显然是不合理的。生物识别信息的保护,取决于良好平衡商主体因营利而带来的信息流动与个人的信息保护之需求这两种利益。在侵权赔偿制度较为完善的前提下,笔者认为,不应不当抹杀其商业价值,

通过正向激励对生物识别信息的商业利用,鼓励商业化运作反而可能促进生物识别信息的权益保障向更良好的效益发展。

从权利救济的视角来看,在个人生物识别信息保护的场景下,相较于“违约之诉”以合同关系为基础,忽视企业和个人处理信息能力的悬殊,优化“侵权之诉”显然更有利于保护信息主体。

首先,应借鉴环境领域、医疗领域对于侵权损害的认定,可以将风险作为直接损害,即使生物识别信息泄露大多时候不会直接导致财产损失,但各项事实表明因信息处理不当造成未来遭受损害的风险是客观的、确定的,就应当认定为损害成立[9]。

其次,对生物识别信息侵权案件而言,个人在举证方面处于绝对劣势的地位,应赋予信息处理者更高的证明责任,具言之,可以适用《个人信息保护法》第六十九条第一款规定的过错推定责任,处理者应当证明自己履行了保护义务,或者证明被诉行为与损害结果之间没有因果关系,最大限度地减轻被侵权者的举证压力,有利于增强此类案件的救济可能性。

4.3.2. 个人私益与公共利益间的平衡

《个人信息保护法》第二十六条将公共场所图像设备收集个人信息的目的限缩在维护公共安全所必需的范围内,体现了个人信息权益与公共利益并重的立法价值取向。个人作为社会的一份子,在某种程度上必定需要让渡部分个人私益以实现社会的整体进步,这是法律设定的负担。但这一过程之正当性与合理性的关键在于,个人让渡出的权益能否得到法律、社会的有效保障。基于此,明晰个人生物识别信息被采集利用的边界的必要性则需要时刻加以强调。

以公共场所的视频监控为例,公共场所的视频监控设备收集个人信息在收集的区域、收集的内容、收集的强度等方面均呈现出逐渐泛化的趋势,身处公共场所的公民成为无处遁形的“透明人”,不恰当的监控无疑是对公民生活的过度介入,降低了公民在公共场所的安全感[10]。

因此,公安机关及相关部门应当严格按照比例原则对公共场所的视频监控进行规范管理。其一,监控设备的安装位置必须以维护公共安全的目的为导向;其二,个人信息的收集应当遵循最小化收集原则;其三,视频监控所拍摄的隐私等个人信息应严禁不当的传播。

5. 结语

当今,数据产业发展来势汹汹,个人信息侵权案件频发,个人信息被滥用的问题从长远来看矛盾也可能逐渐增多;作为更加敏感,涉及隐私的生物识别信息,为其构建特殊保护机制之重要性和紧迫性愈发彰显。因此,只有建立多元主体共同参与的监督机制、合理分配个人信息流动的风险、坚持知情同意原则的根本性地位、加强相关法律制度的衔接适用、并充分理顺公民个人、政府和企业之间的权责关系等,才能达成个人生物识别信息权益保护与信息流通、数据发展间的良性互动,进而构建安全、和谐,具有正当性的生物识别信息保护新局面。

参考文献

- [1] 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, 41(5): 157-168+255-256.
- [2] 张文韬, 伊莱扎·斯特里克兰. Facebook 人脸识别技术面临诉讼[J]. 世界科学, 2017(3): 33-34.
- [3] 王政, 石魏. 生物识别信息保护制度的检视、借鉴与完善——以“人脸识别案”比较研究为视角[J]. 北京警察学院学报, 2023(3): 16-24.
- [4] 蒋红珍. 《个人信息保护法》中的行政监管[J]. 中国法律评论, 2021(5): 48-58.
- [5] 杨安华. 个人生物识别信息及其法律保护问题探究[D]: [硕士学位论文]. 长春: 吉林大学, 2022.
- [6] 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.

- [7] 庞文, 纪来斌. 大数据时代个人信息法律保护的难点及解决路径[J]. 武汉公安干部学院学报, 2022, 36(4): 33-37.
- [8] 马赛楠. 在保护与流通之间: 我国数据权利法律制度建构路径反思[D]: [硕士学位论文]. 开封: 河南大学, 2023.
- [9] 于若兰. 个人生物识别信息商业化应用规制: 路径对比与规则补正[J]. 科技与法律(中英文), 2023(5): 128-137.
- [10] 董皞, 王裔莹. 论公共场所监控设备收集个人信息泛化的规制进路——兼评《个人信息保护法》第 26 条[J]. 法律适用, 2023(10): 9-16.