社会科学进展
2024 年 4 月第 6 卷第 2 期

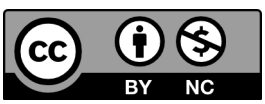
Web3.0 时代下生物识别信息法律保护研究

尹忠誉　杨子涵

上海政法学院，上海

摘　要 | 在近年来的科技发展中，人脸识别、指纹解锁和虹膜识别等生物识别技术已逐渐走入大众生活。这些技术基于个体的生物特征进行身份验证，这些与个体身体紧密相关的信息，被称之为生物识别信息。在Web3.0的背景下，生物识别信息的广泛应用为我们的生活带来了便利，但其在处理过程中的风险也不容忽视。因此，对生物识别信息的保护进行检视显得尤为重要。本文通过对生物识别信息定义的比较研究，明确其在中国的语境含义，重点探讨生物识别信息处理过程中的风险，以及我国当前法律对生物识别信息的保护现状与不足。最后，本文提出对生物识别信息法律保护的建议，要求建立体系化的生物识别信息法律，规范化生物识别信息知情规则，严格化生物识别信息的同意规则，以更有效地避免生物识别信息利用中的风险。

关键词 | 生物识别信息；《个人信息保护法》；同意规则



作者简介：尹忠誉，上海政法学院硕士研究生，研究方向：刑法学；杨子涵，上海政法学院硕士研究生，研究方向：刑法学。

文章引用：尹忠誉，杨子涵．Web3.0时代下生物识别信息法律保护研究［J］．社会科学进展，2024，6（2）：179–189.
https://doi.org/10.35534/pss.0602015

1 问题之提出

随着 Web3.0 的深入发展，大数据、物联网等技术革新正在深刻地改变着我们的生活。在这个数字化、数据驱动的时代，个人信息在各个场景中大量产生和流通，从日常网购到政府管理的公民信息，都基于个人信息的基础之上形成了一个庞大的数据网络。然而，这个过程中也容易出现个人信息被非法获取、分析、提供等违法行为，甚至可能涉及严重的数据犯罪。因此，制定相关的法律以规范和保护个人信息显得尤为迫切。特别是生物识别信息，这种兼具人格权和财产权的敏感个人信息，更应该成为法律保护的重点。在 Web3.0 时代，生物识别信息的应用越来越广泛，从常见的指纹解锁、人脸识别，到步态特征等，人类已经可以通过生物特征信息进行身份识别。然而，生物识别信息在处理和应用过程中面临的风险也是不容忽视的，包括私人信息泄露、技术误判、安全性问题以及道德和伦理问题等。在现行法律中，生物识别信息的保护还存在不足之处，主要表现在以下几个方面：首先，相关的法律法规比较分散，缺乏系统的保护框架；其次，生物识别信息的定义模糊不清，容易与其他个人信息混淆；最后，《个人信息保护法》等法律对于生物识别信息的具体处理规则不够明确，导致实际操作中难以有效保护个人生物识别信息。

2 生物识别信息具体含义之界定

在万物互联的今天，生物识别信息已然发展成为个人信息的重要组成部分，随着社会生物识别技术的不断发展，生物识别信息也将愈来愈普遍适用于日常生活。在生物识别信息发挥效用，便利生活的同时，其带来的安全风险易不容小觑。针对生物识别信息而建立一系列的规则要求和法律保护是紧迫且必要的。但建立安全标准的前提是基于对生物识别信息的准确界定，统一生物识别信息的内涵，明确生物识别信息的法律定义，是我国依法治国建设的题中应有之义。生物识别信息作为现代科技的产物，在全世界各地的界定并不相同。目前欧盟、美国等域外地区对生物识别信息的界定较为明晰，我国域内相关标准也对其有一定借鉴之处。

2.1 域外定义

2018 年欧盟发布的《通用数据保护条例》（又称 GDPR）关于个人的生物识别数据做出了明确的界定：“生物识别数据”指的是通过与自然人的身体、生理或行为特征相关的特定技术处理产生的个人数据，这种个人数据能够做到识别或确定自然人的唯一身份，例如面部图像或指纹数据。[1] 欧盟对于生物识别信息的界定对很多国家地区的立法产生了一定的启发，例如英国的《数据保护法》和印度的《个人数据保护法（草案）》，采用了和欧盟相同这种对生物识别信息“概括加列举”的定义模式。美国通过司法审判的经验将生物特征信息与生物识别信息相区别，比如头发的颜色并不是生物识别信息。生物识别信息的核心是对生物特征信息的特定技术处理而可以还原成个人身份的数据。基于此，美国各州对生物识别信息的界定也多为“概括加列举”。俄罗斯则是在《个人数据法》中进行专门规定：“表征一个人的生理和生物学信息的特征，在此基础上可以确定他的身份（生物特征个人数据），并且运营商使用它来识别个人数据的主体，只能处理经个人数据主体的书面同意。”俄罗斯《个人数据法》在此仅仅做了原则性的表述，同时规定生物识别信息的处理规则。

2.2 域内定义

我国现行法律中并没有明确规定生物识别信息的具体含义，仅仅是做原则性的规定。比如在《网络安全法》和《民法典》中，生物识别信息被包含进个人信息的概念中加以规定。而在作为专门保护个人信息的《个人信息保护法》中，其对于生物识别信息的概念也没有具体的界定，而是作为敏感个人信息的一部分进行规制，没有突出生物识别信息的独特性。立法中对生物识别信息概念含义的模糊，导致司法中的诸多问题，例如对生物识别信息和生物特征信息的混同，无法准确评价是否造成权利侵害。在法律之外，国家市场监督管理局和国家标准化管理委员会 2021 年 10 月 11 日发布了标准《信息安全技术 生物特征识别信息保护基本要求》，该《要求》区分了生物特征识别原始信息、生物特征对比信息和生物特征识别信息，并把生物识别信息定义为：“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

https://doi.org/10.35534/pss.0602015

然人身份的个人信息，保护个人的面部识别特征、虹膜、指纹、步态等。”[2] 该定义借鉴了欧盟 GDPR 的定义模式，具有科学性和合理性。但其作为行业标准并不能对生物识别信息的权利侵害行为进行有效的规制。

因此，《个人信息保护法》确有必要明确生物识别信息的具体含义，借鉴域外经验和《要求》的定义，采用“概括加列举”模式，根据生物识别信息的本质和特点，明文规定生物识别信息的内涵和外延。

3 生物识别信息法律风险及立法现状

生物识别技术是指根据自然人的生物特征对其个人身份进行识别的技术。在 Web3.0 时代下，随处可见生物识别技术的运用，指纹解锁、人脸支付、语音识别等时刻关系着人们的日常生活。据统计，在中国，随着生物识别技术的高速发展和多场景的应用增加，预估到 2024 年，中国生物识别行业市场规模将增长至 600 亿元。[3] 但在这巨大的“数字利益”后，随之而来的在生物识别信息处理全过程所产生的法律风险是不能忽视的。根据个人信息保护法的规定，生物识别信息属于敏感个人信息。事实上，基于生物识别信息的强人身性、唯一性、强识别性，其敏感程度明显高于其他敏感个人信息。［4］个人信息保护法并未对生物识别信息作特别规定，而是将其笼统的规定于敏感个人信息的处理规则中，导致现实中对生物识别信息保护的缺位。

3.1 生物识别信息处理过程中的法律风险

（1）收集、存储环节

个人生物识别信息在收集、存储环节易引发数据泄露的风险。近年来，个人信息被大量泄露的实例屡见不鲜。被称为“国内人脸识别第一案”的动物园入园案，要求游客必须指纹，“刷脸”进园，这类非法收集、存储个人生物识别信息的行为，不合规也不合法，导致了大量公民的生物识别信息被泄露。在许多公共场所，比如商城、酒店、餐厅等商业场所，摄像头已完全做到全覆盖，在消费者大多无知的情况下人脸信息已经泄露。生物识别信息一般用来识别个人身份，因此在存储环节，通常将生物识别信息于个人身份相连接，信息处理

者为了便利和经济往往不会做高度保密措施，例如分开处理生物识别信息。此时，一旦生物识别信息泄露，那么个人身份信息也就随之完全泄露。生物识别信息具有高经济效益，一旦泄露，很容易诱发侵害公民合法权益甚至是犯罪的现象发生。

（2）使用、加工环节

个人生物识别信息在使用、加工环节易产生技术误判和安全性的相关风险。生物识别技术是利用计算机系统与光学、声学、生物传感器和生物统计学原理等手段相结合，通过计算机算法分析个人生物特征信息并进行身份的识别认证。[5] 尽管相比于传统的身份认证，生物信息识别技术更加准确和便捷，但其在应用过程中仍然会不可避免地出现内外部风险即技术误判和受安全性攻击。生物识别技术存在对生物特征信息的误识别、漏识别等情况，直接导致对个人身份的错误授权或拒绝，造成不必要的困扰和损失。与此同时，生物识别信息系统面临着来自外部的各种安全威胁，例如生物识别信息的复制、盗窃和操作已注册的模板。[6] 2020 年，英国易捷航空遭黑客攻击，900 万用户个人信息遭窃取，其中不乏个人生物识别信息。生物识别技术尚未完全成熟，一旦遭遇内外部安全风险，将会造成无法挽回的损失。

（3）提供、公开环节

个人生物识别信息在提供、公开环节易引发财产犯罪，同时侵犯公民的隐私权和肖像权。在 Web3.0 背景下，只要行为人上传一张照片，AI 就能够通过生物识别技术实现“换脸”。以“换脸软件”为关键词在手机 App 商店进行搜索，不下数十款“换脸软件”可供下载。前段时间爆火的换脸软件 ZAO，引起了一波潮流，通过该软件可以将影视片段中的明星替换成自己的脸，让自己可以在影片中发挥演技。这听起来固然新奇有趣，但却隐藏着法律的风险，例如色情产业中利用 AI 换脸非法获利，行为人通过“色情报复”（即利用人脸识别信息深度伪造不雅视频以羞辱他人）侵犯他人权利。利用提供的和已公开的生物识别信息进行非法牟利或侵犯他人隐私权和肖像权的行为屡见不鲜。随着技术的不断发展，生物识别信息被应用于更广泛的领域，涉及道德和伦理问题也随之浮现，如个人自主权、隐私保护、公平竞争等方面的问题。需要制定相关规章

https://doi.org/10.35534/pss.0602015

制度和实践标准，确保生物识别技术的合理、公正和安全应用。

3.2 生物识别信息法律的立法现状

我国针对个人生物识别信息的立法目前主要存在于《中华人民共和国网络安全法》《中华人民共和国民法典》和《中华人民共和国个人信息保护法》中。在《民法典中》的人格权编中，明确地指出了生物识别信息属于个人信息的范畴，受到民法典关于个人信息的保护。在《网络安全法中》附则中指出个人信息包括个人生物识别信息。在《个人信息保护法》中则是进一步进行界定，在敏感个人信息的处理规则中将生物识别信息置于敏感个人信息下位进行保护。综合看来，我国对于个人生物识别信息的立法保护零散于各项法律，且都没有突出其特殊性。《民法典》和《网络安全法》仅仅只是把生物识别信息规定为个人信息加以保护，其与自然人的电话号码、出生日期、住址等普通个人信息相并列，缺乏对生物识别信息的针对性保护，导致法律保护力度不足。《个人信息法》虽然进一步将生物识别信息界定为敏感个人信息，但也并无专条专款对其进行明确规定。

生物识别信息有与其他敏感个人信息不同的独特性质，而且其会随着技术的革新不断产生新模式新样态。美国的专门立法模式和欧盟的综合立法模式值得借鉴，对于个人的生物保护信息应该在《个人信息保护法》中制定专门一章进行规制，以对生物识别信息提供更严格保护，且为信息主体和信息处理者提供更为清晰的引导。[7]

4 生物识别信息法律保护之完善

《个人信息保护法》将生物识别信息纳入敏感个人信息中进行保护，从法律层面明确了生物识别信息的敏感性和重要程度，这是立法层面的一大突破。但随着社会经济的快速发展，Web.3.0 时代的到来，生物识别信息技术被广泛使用，从收集到提供的全过程存在着不同的法律风险，《个人信息保护法》的泛化规定明显不足以对生物识别信息进行全面的保护，敏感个人信息的处理规则的要求始终是具体化，体系化，为此本文在结合现今生物识别信息存在的风险

上提出了对生物识别信息法律保护的建议，第一，生物识别信息法律保护体系化；第二，生物识别信息知情规则规范化；第三生物识别信息同意规则严格化。具体建议如下。

4.1 生物识别信息法律保护体系化

生物识别信息较其他个人信息隐私程度高，与人身关联性强，被侵害后所遭受的往往是财产利益和人格权益的双重损失。因此有必要构建完整的生物识别信息法律保护体系，明确界定生物识别信息的内涵和侵犯个人生物识别信息的责任。

目前《个人信息保护法》将生物识别信息纳入敏感个人信息中进行概括规定。实际上敏感个人信息存在不同的等级区分。在电信行业中，根据个人信息敏感程度的不同，生物识别信息属于第五级敏感个人信息。根据保护措施的程度不同，敏感个人信息分为低敏感级，较敏感级，敏感级和极敏感级，而生物识别信息属于极敏感级。而从敏感个人信息所遭受损失程度来看，对生物识别信息的侵害也属于经济和精神损害的最高等级。[8]《个人信息保护法》第二十八条对敏感个人信息作出了定义，把包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息都归为敏感个人信息来进行保护。生物识别信息不同于上述其他敏感个人信息，其兼具财产属性和人格属性的特点决定了对生物识别信息的保护应该严于对一般敏感个人信息的保护。《个人信息保护法》这样简单的概括列举易导致生物识别信息的法律定位不明，对此有必要借鉴域外立法的经验，在个人信息保护法敏感个人信息条款后单独设置生物识别信息保护条款，规定生物识别信息的内涵和处理规则，并出台司法解释确定生物识别信息的定罪量刑标准，做到前置法与刑法的有序衔接，以构建完整的生物识别信息法律保护体系。

4.2 生物识别信息知情规则规范化

Web3.0 时代下的个人信息高速流通利用，而生物识别信息的知情规则却并未得到充分遵循，一些信息处理者不告知或进行虚假告知使得信息所有权者的

https://doi.org/10.35534/pss.0602015

知情权形同虚设。由于信息的不对称，信息处理者和信息所有权者存在知情差异，个人信息自决权无法得到有效实施。由于信息处理的告知义务不规范，知情规则名存实亡，使得信息所有权者的知情权受到侵犯。

知情规则规范化要求信息主体在特定场景里对信息处理者所收集处理的信息目的能够做到完全的知晓。在生物识别信息的收集处理过程中，信息处理者往往采取的是一次性告知的形式，信息主体对信息的后续处理情况可以说是并没有做到充分知情。信息处理者应该将生物识别信息的收集和后续使用单独且充足的告知信息主体。为保护信息主体的合法权益，必须将生物识别信息的知情规则规范化，建立动态且连续的信息披露机制[9]，保障信息主体享有完整的知情权。除此之外，对于信息处理者收集生物识别信息的告知不规范问题，信息主体亦有权行使知情权，信息处理者有义务作出回应，与信息主体进行有效沟通，使其处理行为被信息主体完全知情，否则信息主体有权利撤回同意，要求信息处理者进行信息销毁和遗忘。信息处理者完全不遵守知情规则造成信息主体人格权益或财产权益受损时，信息主体有权诉诸法律，提起诉讼。

4.3 生物识别信息同意规则严格化

《个人信息保护法》要求在处理包括生物识别信息的敏感个人信息时，只有取得信息主体的单独同意时才能对个人生物识别信息进行处理。在数据高速流通利用的 Web3.0 时代，相对静态的知情同意往往逐渐演化为被动地接受，单独同意规则也不例外。[10]信息主体在被告知单独同意其生物识别信息的收集时，在不充分了解其同意内容后选择同意是否是意思表示的真实有待考量，由此若发生对个人生物识别信息的侵害行为时，信息主体无法通过单独同意这一项规则来进行维权。综合看来，没有充分的知情则难以实现真正的同意，[11]单独同意规则有时并不能有效地保护对生物识别信息的处理，从而沦为形式。

生物识别信息不同于一般的敏感个人信息，其唯一性，不可更改性等特征决定了其需要更高标准的处理规则，单独同意规则无法有效保护生物识别信息的处理全生命周期。信息处理者在收集环节取得信息主体的同意，而信息主体一般对信息处理者对生物识别信息的后续行为则做不到充分知情。静态的单独

同意需要转向动态的分别同意，个人信息处理者不仅在收集储存环节需要信息主体的单独同意，在后续二次使用或公开等环节也必须征得信息主体的明确同意，使信息主体清楚该处理行为的法律风险，并保障其撤回同意权，做到充分保障信息主体关于个人生物识别信息的自决权。由于生物识别信息的高度人身相关性，保障信息安全理应重于信息流通。

5 结语

步入 Web3.0 时代，每个人的生活都离不开数据，信息，甚至有学者提出“数据人”的概念以涵摄数据的重要性程度及其与个人的高度相关性。目前，与个人直接相关的生物识别信息已经充斥我们的日常生活，并日趋发展成熟。生物识别技术已然是蕴含巨大利益的经济宝库，在对个人生物识别信息的利用中如何做到严格的保护是当前社会面临的难题。为此，需要对生物识别信息的保护进行充分检视。通过上文的阐述，中国现今对于生物识别信息的保护需要明确在生物识别信息处理过程中出现的技术和法律风险，因而有针对性的加以完善和监管；准确界定生物识别信息的具体含义，做到法律法规的明确，同时与国际上的生物识别信息发展接轨；完善《个人信息保护法》关于生物识别信息的规定，区别生物识别信息与一般个人信息，建立体系化的生物识别信息法律，规范化生物识别信息的知情规则，调整生物识别信息的单独同意处理规则而转向分别同意规则，有效的法律保障是生物识别信息有效利用的基础和前提。

参考文献

[1] 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），2023，29（3）：200-211.

[2] GB/T 40660-2021，信息安全技术 生物特征识别信息保护基本要求[S/OL]. [2024-03-20]. https://www.softhome.cc/tuji/gbt40660-2021.html.

[3] 胡学慧. 多模态生物识别：茁壮成长 未来可期[J]. 中国安防，2022（12）：45-47.

[4] 郭锋，陈龙业，贾玉慧，等. 《关于审理使用人脸识别技术处理个人信

https://doi.org/10.35534/pss.0602015

息相关民事案件适用法律若干问题的规定》的理解与适用［J］. 人民司法，2021（25）：37–42.

［5］张淑娥，田成伟，李保罡. 基于区块链技术的身份认证研究综述［J］. 计算机科学，2023，50（5）：329–347.

［6］张淑娥，田成伟，李保罡. 基于区块链技术的身份认证研究综述［J］. 计算机科学，2023，50（5）：329–347.

［7］宋祎晨. 生物识别信息的安全风险及法律规制［J］. 河南牧业经济学院学报，2022，35（3）：56–61.

［8］唐迪，顾健，俞优， 等. 基于等级保护的个人信息安全分级方法研究［J］. 信息网络安全，2020（S2）：13–16.

［9］陈希. 我国敏感个人信息保护规则进路探析——以《个人信息保护法》第28～30条为基准［J］. 湖南社会科学，2023（6）：98–107.

［10］王冉冉. 已公开生物特征信息保护中单独同意规则的功能转向及实现［J］. 南京社会科学，2023（5）：94.

［11］姜野. 由静态到动态：人脸识别信息保护中的“同意”重构［J］. 河北法学，2022，40（8）：126–144.

Research on Legal Protection of Biometric Information in the Era of Web3.0

Yin Zhongyu Yang Zihan

Shanghai University of Political Science and Law,Shanghai

Abstract: In recent years' technological development, biometric technologies such as face recognition, fingerprint unlocking and iris recognition have gradually come into public life. These technologies are based on the individual's biometric characteristics for identity verification, and this information, which is closely related to the individual's body, is called biometric information. In the context of Web 3.0, the wide application of biometric information has brought convenience to our lives, but the risks in its processing should not be ignored. Therefore, it is particularly important to review the protection of biometric information. This paper clarifies the contextual meaning of biometric information in China through a comparative study of the definition of biometric information, focuses on the risks in the processing of biometric information, as well as the status quo and deficiencies in the protection of biometric information in China's current laws. Finally, this paper puts forward suggestions for the legal protection of biometric information, calling for the establishment of systematic laws on biometric information, standardisation of the rules for knowing biometric information, and strictness of the rules for consenting to biometric information, in order to more effectively avoid the risks in the use of biometric information.

Key words: Biometric information; *Personal Information Protection Law*; Consent rules

https://doi.org/10.35534/pss.0602015