DOI:10. 13766/j. bhsk. 1008-2204. 2020. 0111

人工智能时代中国个人信息保护法的选择

李海英[1], 徐小露[2]

(1. 蚂蚁金融服务集团, 浙江 杭州 310007; 2. 对外经济贸易大学 法学院, 北京 100020)

摘　要: 个人信息保护立法的发展与所处的时代背景密切相关,从互联网商用到大数据的广泛应用,人工智能时代的技术和产业变革对个人信息来源、目的、存储及处理之要求产生的巨大变化使得个人信息保护之挑战日益严峻,传统的个人信息保护规范难以应对当下的需求。为应对"百年未有之大变局",创新地制定面向未来技术、经济、社会发展的个人信息保护规则,中国未来的《个人信息保护法》应充分回应新兴技术之发展需要;顺应个人信息保护重点从收集向使用转移、个人信息保护责任从信息主体向信息控制者转移之国际趋势;有针对性地借鉴 GDPR、CCPA 等前沿立法之理论与实践得失;对生物特征识别技术、自动化决策等具体制度作出前瞻性制度设计,在关注个人隐私保护之同时,充分利用人工智能之产业优势为社会经济发展开辟道路。

关键词: 人工智能; 隐私保护; 生物特征识别; 自动化决策; 个人信息保护法

中图分类号:D913　　**文献标志码**: A　　**文章编号**:1008-2204(2020)03-0017-08

Choice of Chinese Personal Information Protection Law in the Age of Artificial Intelligence

LI Haiying[1], *XU Xiaolu*[2]

(1. Ant Financial Services Group, Hangzhou Zhejiang 310007, China;
2. School of Law, University of International Business and Economics, Beijing 100020, China)

Abstract: The personal data protection legislation is closely related to the background of the era in which it is located. The widespread use of Internet, the application of big data and the technological and industrial changes in the artificial intelligence era has made tremendous changes in the requirements for the source, purpose, storage and processing of personal data. The challenges of personal data protection are becoming increasingly severe, and traditional norms are difficult to meet current protection needs. To cope with the big changes and creatively formulate personal data protection rules for future technological, economic, and social development, China's future Personal Information Protection Law should take the following actions: It should fully respond to the development needs of emerging technologies; it should comply with the international trend of data protection, with the point shifting from collection to use, with the protection responsibility shifting from data subject to data controller; it should purposefully draw on the theoretical and practical gains and losses of cutting-edge legislation such as GDPR and CCPA. In view of biometric identification technology and automated decision-making system, while paying attention to the protection of personal privacy, it should also make full use of the industrial advantages of artificial intelligence to open the way for social and economic development.

Keywords: artificial intelligence; privacy protection; biometric identification; automated decision-making; Personal Information Protection Law

收稿日期: 2020-03-23

作者简介: 李海英(1976—),女,吉林舒兰人,高级工程师,硕士,研究方向为网络法、数字贸易国际规则.

一、个人信息保护法与所处的时代背景

(一)互联网商用之前

个人信息保护法是在个人信息被“自动化处理”(Automatic Data Processing)的背景下发展起来的,1980 年经济合作与发展组织(Organization for Economic Co-operation and Development, OECD)《关于隐私保护与个人数据和跨境流动的建议与指南》(以下简称“OECD《隐私指南》”)开篇即指出:“自动化数据处理的发展,使得大量数据能够在几秒钟之内跨越国家甚至大洲传输,因此有必要考虑与个人数据有关的隐私保护问题。” 1981 年欧洲理事会(Council of Europe)发布《关于个人数据自动化处理的个人保护公约》(Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data),即著名的 108 公约,以“自动化处理”作为公约名称。

但是,当时的“自动化处理”是在互联网尚未商用,个人电脑刚刚开始走入家庭的背景之下,所谓的“自动化处理”主要是指纸质文档的电子化。也是在该背景下,除 OECD《隐私指南》外,各国纷纷开始就个人数据进行立法,瑞典 1973 年制定的《数据法》(The Data Act)、美国 1974 年通过的《1974 年隐私法》(Privacy Act 1974)及德国 1977 年颁布的《联邦个人数据保护法》(BDSG)都关注公共机构对个人数据的滥用[1]。国际社会也形成了以欧盟和美国为代表的两种主要立法模式:欧盟注重个人信息的人权特性与社会价值,以人格保护为重点,采取全方位的国家立法模式;美国则展现出对个人信息积极利用的态度,更关注个人数据的经济特性和个人价值,其个人信息保护立法体系主要由《1974 年隐私法》以及特殊领域的专门法构成①,采取分散立法的形式对其权利进行保护[2]。

(二)从互联网商用到移动互联网、大数据的发展

互联网在 1994 年实现商用。欧盟于 1995 年 10 月通过《欧洲议会和理事会关于个人数据处理和自由流通的指令》(Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 以下简称《数据保护指令》),作为互联网商用后世界范围内的第一部个人数据保护立法,该指令建立在 OECD《隐私指南》确定的数据保护原则之上,并设置了个人数据保护的双重目的:指令不仅要求成员国保护自然人的基本权利和自由,尤其是在处理个人数据方面的隐私问题,且不可限制或禁止与该种保护有关的个人数据在成员国间的自由流动。此后,欧盟的 27 个成员国以及挪威和列支敦士登(作为欧洲经济区国家)都已分别将该指令转化为本国的数据保护立法,奠定了欧盟数据保护法规的框架。《数据保护指令》适用范围广泛,包括自动化或非自动化的数据处理;赋予数据主体查阅权、拒绝权、基于自动化处理决策的否定权及获得救济的权利;规定数据保护监管机构的相关职权;并对跨国数据流通作出限制,提出第三国对个人数据充分保护作为数据转移之前提,旨在为所有成员国提供同等的高水平保护,以期实现欧盟内部市场的平衡发展。

2007 年,第一代 iPhone 问世,采用触控界面和全屏设计,奠定了后来的智能机设计基础,开启了移动互联网时代。移动互联网的发展加之云计算的助力,使个人信息的收集使用更加便捷并“尽在掌握”,而云计算的发展则使数据跨境流动的问题更加凸显,2012 年开始,个人信息保护立法也进入第一个高潮。2012 年 1 月,欧盟提出《有关“95 年个人数据保护指令”的立法建议》,为《一般数据保护条例》(General Data Protection Regulation, GDPR)奠定基础;美国 2012 年提出《消费者隐私权利法案(草案)》,虽然最后尚未正式通过,但是其保护消费者隐私的理念得到广泛传播;韩国修改《信息通信网络的促进利用与信息保护法》《位置信息保护与使用法》;新加坡通过《个人信息保护法》等。

随着云计算、大数据、人工智能的发展,如今“自动化处理”的内涵已经发生了翻天覆地的变化,不再仅仅是文档的电子化,而是基于海量应用、海量数据和复杂算法进行。美国白宫 2014 年的一份报告将大数据描述为一种“获取、聚合和处理更大规模、更快速度和更多种类数据”的技术能力[3]。在这一背景下,数据逐渐被视作最重要的生产要素和战略性资源,渗透到各个行业和业务领域,对社会生活、经济运行方式、公共治理等产生了根本性的影响,对个人信息保护规则也带来新的挑战。随着大数据分析能力、人工智能和机器学习的进步,“自动化决策”得到越来越多的应用。“自动化决策”是指在无人干预的前提下通过技术手段做出决策的能力。可以把“自动化处理”看作是“自动化决策”的

过程，“自动化决策”作为“自动化处理”的结果。但是需要注意的是，无论是自动化处理还是自动化决策，都不是全部需要依赖于“个人信息”，也存在完全不需要个人信息的自动化处理和决策。

（三）人工智能时代对个人信息保护的挑战

自 21 世纪初至今的二十年里，机器学习和大型数据集的融合导致公共机构和私营部门中产品和服务的数量不断增加、应用不断拓宽，人工智能产品的运用使得人工智能正在成为现实，经济和社会需求成为人工智能产业发展的驱动力。人工智能充分释放了大数据的价值，而机器学习则成为支撑和促进人工智能的技术机制之一，这三个概念的组合可以称为“大数据分析”[4]。人工智能时代，个人信息的来源、目的和存储要求均较之前发生巨大变化，传统的信息保护规范已不足以应对当下的需求：①人工智能对数据的需求量剧增，且来源从信息主体主动提供逐渐向由网络和设备自动记录产生发展。人工智能技术的应用质量会因缺乏足够的数据而恶化，从而导致交易效率低下并减少消费者福利。此外，足够的数据基础有利于防止人工智能在作出决策时出现偏差或歧视，收集“尽可能多的数据”才能够进一步学习和分析，而该种分析需求使个人信息的收集、处理与个人信息保护的“最小化原则”产生冲突②。②个人信息的重新利用或多重用途对“目的限制原则”产生冲击。算法环境下信息处理“结果的不可预测性”使得收集、使用个人信息的最初目的难以遵守，以机器学习为动力的大数据分析与个人信息保护的“目的限制原则”仿佛已然背道而驰。③个人信息的存储期限限制使得个人信息的效用无法充分发挥，数据红利难以释放。在达到数据收集、使用的原始目的或应个人信息主体要求删除或限制数据使用后，企业及公共管理部门将失去使用个人信息进行人工智能开发、部署和监督的潜在利益[5]。

二、人工智能时代个人信息保护的立法与反思

（一）从 2010 年起国际组织的讨论

2010 年，世界经济论坛（World Economic Forum，WEF）发起了一个“反思个人信息”的项目，认为“原来的数据保护这些原则在当今社会已经没用，尤其是告知与同意，根本没有赋予个人真实有效的选择权”。该项目倡导个人信息保护重心从收集转向使用，增加个人的管理能力，使个人能够管理与谁分享数据，什么目的分享，但是不采用事先同意的方式。OECD《隐私指南》修订过程中，2012 年牛津大学互联网研究院牵头的工作组建议，OECD 确立的基本原则应将数据保护责任从数据主体一方转移到数据控制者一方，且更加注重数据使用环节而非收集环节。因为事前机制已经逐渐失去了实质意义，不应当再对其投入过高的关注，事前的同意只能是作为保障的一种手段而不是数据行为合法性的所有依据。

这表明，以 WEF、OECD 为代表的国际组织早在 2012 年左右就已经注意到个人信息保护传统原则难以适应时代发展这一问题，并提出了新的解决方案。但由于政治、社会发展等历史原因，这些新的方案没有得到推行。时至今日，人工智能和算法技术的发展又使个人信息收集处理的背景与 2012 年左右又有了很大的变化。中国在这样一个新的历史时期制定《个人信息保护法》，理应反思这些四十年未变的原则，顺应“百年未有之大变局”，创新地思考面向未来技术、经济、社会发展的个人信息保护规则。

（二）欧盟 GDPR 对人工智能的影响

全球对于人工智能时代个人信息保护规则的制定还在探索阶段，欧盟 GDPR 事实上并未很好回应人工智能带来的数据保护问题，虽然其试图在保护个人信息基本权利的同时实现非个人信息的自由流动，从而跟上技术和社会经济发展的步伐，但却反而对人工智能甚至整个数字经济的发展形成了障碍。一方面，欧盟成员国正在测试或计划将人脸识别（Face Recognition）等生物特征信息识别技术用于执法目的③[6]。人脸识别技术可以对社会公众提供更及时的保护（如通过帮助寻找失踪儿童）及帮助发现欺诈和识别盗窃行为；但另一方面，因该技术对个人隐私的侵犯性以及存在人脸匹配错误导致歧视的风险，同样引发了各国关于基本权利问题的讨论[7]。此前，法国、瑞典等国的数据保护机构均认定在高中使用面部识别技术的行为违法，如法国数据保护监管机构国家信息与自由委员会（CNIL）认定该面部识别计划与数据最小化原则不符，将以轻易的手段实现对隐私和个人自由方面的入侵。可见，欧盟对于人脸识别技术的应用尚持相对谨慎的态度。而 2019 年 5 月美国数据创新中心发布的《欧盟需改革 GDPR 以在算法经济时代保持竞争力》报告指出：“欧盟在加速人工智能技术应用方面做了

许多努力,但 GDPR 从数据保护的层面对人工智能系统做出了限制。如不改革,欧盟在人工智能的全球竞争中将处于结构性劣势。"

此外,GDPR 对于自动化个人决策(Automated Individual Decision-making)也有所限制,赋予数据控制者更多的义务。根据 GDPR 第 22 条,"基于单独地"自动化处理意味着在决策制定过程中没有人为干预、在进行自动化个人决策时应获得数据主体的明示同意(同意必须经过特别地、具体地确认,如通过明示声明形式而非其他表示赞成的行为来确认)等[8],并对自动化个人决策的一般禁令赋予了例外情况,且对于用户画像(Profiling)作出了特别规定④,用户画像作为对自然人特定条件的评估,与自动化个人决策的范围有不同之处,但也可能会有部分重叠,自动化个人决策可以基于任何形式的数据,并非必须经过用户画像这一过程,而用户画像的发生可以无需作出决策。但是,由于算法本身的复杂与不透明以及单独的自动化个人决策可能产生的"法律或类似重大影响"之含义不明,GDPR 相关条款在适用上仍存在问题,实践中也对自动化个人决策的可解释性设置了比较高的门槛。欧盟委员会数据保护专员在处理金融信贷公司 Svea Ekonomi 投诉时遵循这样的审查逻辑,即首先指出应将公司的在线信用决策服务视为GDPR第 22 条中规定的自动个人决策,而后在数据处理阶段,公司必须向投诉者提供有关自动个人决策所采用的算法逻辑、其在评估决策中的作用以及对信用评估申请人可能产生的后果,并且以充分的通知确保信贷申请人可以理解作出决策的理由[9]。可见,算法可解释性要求对大数据背景下的分析活动带来了极大的影响,可能损害"人工智能最有价值的用途之一:自动化决策和预测"[10]。

(三)美国《2018 年加州消费者隐私法案》对人工智能的回应

已经颁布并于 2020 年 1 月 1 日生效的《2018 年加州消费者隐私法案》(California Consumer Privacy Act of 2018, CCPA)赋予消费者与企业收集消费者个人信息有关的多项权利,包括访问权、删除权、知情权、选择退出权、享有平等服务与价格的权利,同样关注消费者的隐私保护权利,消费者可合法地获知个人信息如何被收集、存储、使用、出售或共享,避免个人信息在不知情的情况下被收集并货币化。与欧盟 GDPR 相比,CCPA 更侧重考虑个人信息的价值利用,不再试图追求信息主体对个人信息的绝对控制权,赋予新型商业模式对信息的利用空间。首先,CCPA 确定了更加宽泛的个人信息定义:包括生物特征信息与互联网或其他电子网络活动信息、从已识别信息中得出的可创建用户画像之推论⑤,并从"个人信息"的定义中排除了公开可获取的信息,且"公开可获取"信息不包括去识别化的消费者信息以及聚合的消费者信息。其次,关注个人信息的流通价值与隐私权益的平衡:第一,区别于 GDPR 采用"选择加入"(Opt-in)的机制,CCPA 赋予消费者"选择退出"的权利(Opt-out),即在企业进行充分披露后,消费者可在任何时间指示出售消费者个人信息给第三方的企业不得出售该消费者的个人信息;第二,有条件地豁免数据控制企业合规负担,如通过考察经营者相关行为来降低信息去识别化的相关要求,在特定情况下使用"去识别化"信息的经营者可主张免责⑥;第三,允许企业根据隐私授权多寡实行差异化定价而不构成歧视(如果该等区分对待与消费者数据提供给消费者的价值合理相关,则该企业可向消费者提供不同价格、费率、水平或质量的商品或服务)及企业可以为个人信息的收集、出售或者删除提供财务激励,包括向消费者支付赔偿金;第四,CCPA 采取消费者民事保护之进路,消费者有权通过个人诉讼(或集体诉讼)对企业提出法定赔偿的要求,但仍需履行前置之提前三十天给予企业书面通知之义务,若企业三十天内改正并提供明确通知声明,诉讼即可避免[11-12]。

新法规正在改变很多企业的隐私政策,同时不断有讨论指出,人工智能技术同样可以作为 CCPA 合规性的可行解决方案。文章观点认为,人工智能不仅带来隐私挑战,也可以作为一种技术助力来促进隐私保护。作为全面落实 CCPA 项下消费者权利的实现机制,人工智能反将成为保护消费者个人信息权利的工具:当消费者根据 CCPA 请求企业作为信息控制者披露其收集的可识别个人身份的信息时,借助人脸识别技术,数据请求才可能高效且精确地完成,进而提高消费者对企业的信任和信心[13];通过在线身份验证技术,企业在满足个人数据删除请求之前识别其真实身份,可以防止企业或信息主体因身份盗窃而遭受经济损失;智能数据管理、人工智能客服等多种技术手段不仅可以更好地保护消费者信息,更可以作为企业合规运营的保护机制。

可见,作为美国史上最全面、最彻底的隐私法

案，CCPA 为个人信息的自由流动创造了更大的空间，有利于促进数字经济的发展，且基于合规性要求，人工智能技术作为隐私保护工具也正扮演着不可或缺的角色。同时，正如 CNIL 指出，人工智能和大数据是不可分割的，事实上人工智能与大数据之间的关系是双向的：通过机器学习，人工智能需要大数据领域的海量数据作为基础；同时，大数据则使用人工智能技术从大型数据集中提炼价值[14]。

三、中国人工智能时代个人信息保护立法

（一）中国人工智能相关产业发展趋势

近年来，中国陆续出台多项政策，在国家战略上多角度促进人工智能与经济社会深度融合发展。工业和信息化部印发了《促进新一代人工智能产业发展三年行动计划（2018—2020 年）》（以下简称《人工智能三年行动计划》），中央全面深化改革委员会会议审议通过了《关于促进人工智能和实体经济深度融合的指导意见》，科学技术部印发了《国家新一代人工智能创新发展试验区建设工作指引》。截至 2019 年，全国已建立十五个国家级人工智能开放平台，二十一个省市地区政府出台了人工智能产业相关政策，在安防、金融、零售、医疗、政务、交通、制造、家居等多行业领域均有不同程度的应用⑦。

其中，生物特征识别是人工智能的关键技术。目前，国内外均已在多个领域和行业广泛应用。中国相关产业政策大力支持生物特征识别技术发展，《人工智能三年行动计划》具体规划“到 2020 年，复杂动态场景下人脸识别有效检出率超过 97%，正确识别率超过 90%”，中央银行、发展和改革委员会、交通运输部、商务部等多个行业主管部门出台政策推进生物特征识别技术在金融服务、不动产登记、在线支付等多个领域的发展⑧。但因人脸识别等生物识别信息的高度敏感性，该技术依旧存在争议，如杭州一动物园因启用人脸识别技术，在未经消费者同意的情况下，通过升级年卡系统强制收集个人生物识别信息而被诉至法院，该案被称为“中国人脸识别第一案”，这也暴露了社会对人脸识别技术安全的担忧与质疑。同样，自动化决策因其效率及预测价值被广泛应用于社会各领域。自 2016 年以来，尤其在与日常生活密切相关的商业领域，注重实时数据分析的商品推荐、图书推荐、情境推荐等应用的研究引领自动化研究向个性化服务方向迈进[15]。在中国电子商务蓬勃发展的当下，自动化决策的应用，一方面，提高了交易效率，但“大数据杀熟”现象也相伴而生；另一方面，由于企业与用户之信息不对等，用户数据被多次整合和分析，隐私信息的保护也成为难题。

（二）现行立法分析

近年来，中国不断丰富个人信息保护立法之实践。自 2012 年全国人民代表大会常务委员会出台《关于加强网络信息保护的决定》以来，民法领域逐步关注个人信息的范围、保护原则及具体制度安排，消费者保护、征信业务等具体领域也对个人信息保护提出了新的要求。2016 年出台的《网络安全法》、2017 年施行的《民法总则》第 111 条等在法律层面体现了个人信息保护的重要性。但同样需要注意，针对人工智能带来的挑战，中国立法当前难以及时、全面地予以回应。如关于自动化决策之限制规定主要集中在电子商务领域，企业在现有商业模式下不可避免地收集和使用个人数据，商品和服务的提供以数据的定向分析为前提。《电子商务法》第 18 条规定，电子商务经营者“应当同时向该消费者提供不针对其个人特征的选项”，即明确提出平台经营者需要向消费者提供明确的退出机制。也有学者称之为电商平台的平台算法责任条款，恪以平台以算法的自然结果提供义务，在承认电商平台个性化推荐算法之合法性基础上，加诸提供一般搜索结果的义务，以纠正平台与消费者之间的信息不对称[16]。此外，《网络交易监督管理办法（征求意见稿）》等多项文件同样要求，网络交易经营者提供商品或者服务的搜索结果或者展示商业性信息时，同时以显著方式向消费者提供不针对其个人特征的选项⑨。现有规制方案主要依据个性化推荐之退出条款赋予消费者之自主选择权，以保护个人信息。但同样，在医疗、征信、保险等各行业逐步涌现的自动化决策应用，因各领域涉及用户个人信息之范围、敏感度的区别，难以根据电子商务领域之规定做普遍适用。

而在生物特征信息应用领域，中国将生物识别信息纳入个人信息的范围予以保护，并在《反恐怖主义法》《出境入境管理法》等特定情况下对于生物识别信息的收集、使用作出规定⑩。此外，即将于 2020 年 10 月 1 日施行的《信息安全技术 个人信息安全规范》（GB/T 35273—2020，以下简称《规范》）对个人生物识别信息收集、使用的告知同意方式、存

储标准及具体措施等作出了具体要求⑪[17]。中国目前在法律层面尚未对生物识别信息保护作出明确进行强化规定,该《规范》的颁布将对个人信息保护工作的落地产生重大意义,降低生物识别信息滥用和泄露风险的同时促进产业健康有序发展。

有学者认为,未来是"移动互联网 + 大数据 + 机器智能"三者叠加的时代,人类社会将进入一个透明的、没有隐私的时代[18]。在"互联网 + 电子商务"领域,个人信息流转链条长,数据保护难度大;新零售业态深度收集、使用个人敏感信息等都使个人信息的全面保护面临挑战⑫。为妥善应对个人信息保护这一人工智能时代的新课题,《民法典(草案)》之"人格权编"在第六章"隐私权和个人信息保护"中,对隐私权保护、个人信息的收集、使用、删除、更正和保护等问题作出了较为详细的规定⑬,第十三届全国人民代表大会常务委员会决定将该草案提请第十三届全国人民代表大会第三次会议审议,加快推进个人信息保护相关立法进程已经成为了全社会的共识[19]。

四、中国《个人信息保护法》的制度选择

人工智能的发展带给人们无限的可能,面向未来,中国有机会站在巨人的肩膀上,与欧美共同面对新技术新业务带来的冲击。在制度建设方面,中国面临前所未有的机遇,有机会引领未来的规则体系。

(一)体现人工智能时代的前瞻性

在算法经济时代,人工智能预示着显著的社会经济效益。首先要明确人工智能技术在个人信息保护中的中立性,对人工智能技术的合理利用可以为更快速便捷地获取公民个人信息提供技术支持,将作为实现公民信息权利最有效的执行者。面对人工智能技术带来的挑战,过于保守谨慎的全面禁止同样有可能对技术以及相关应用的发展带来极大阻碍。

因此,新时期的《个人信息保护法》要清楚地认识到数据在未来数字经济发展中的重要作用,既要为个人信息保护做出清晰指引,也要为人工智能时代的产业变革留下空间。《个人信息保护法》是一个多元利益的平衡,从个人的角度看,既要看到权利保护,也要看到服务提升带来的福利提升;从行业的角度看,既要看到个体的权利保护和权益实现,也要看到行业发展企业创新给群体带来的收益;从国家的角度看,既要看到用户个体价值和安全,也要看到国家经济发展和安全保障。用户福利不仅包括个人信息受到保护,也包括以更低的价格获得更好的服务,以及享受由于互联网产业的发展带来的总体福利提升。人工智能等新技术发展给个人信息保护带来挑战,但未来还要依靠技术来提升个人信息保护的水平,技术发展带来的新问题交由技术的发展来解决。人们既要应对数字经济时代人工智能等新技术给数据保护带来的新挑战,如数据无时无刻的收集、个人信息边界的进一步模糊、数据使用的目的无法事先明确等,也要看到以人工智能为基础的新技术在隐私保护、风险控制等领域会发挥越来越大的作用,用技术来解决技术发展带来的问题将是数字经济时代数据治理的重要手段。

(二)借鉴国际经验的同时汲取教训

更多国家开始重视并利用个人信息资源,通过国家和地区战略和激励措施来推进人工智能的发展是大势所趋。欧盟委员会此前曾表示考虑实施史上最严的人工智能监管措施,公共或私人机构在公共场所使用人脸识别技术将被禁止 3 ~ 5 年的时间。但 2020 年 2 月欧盟发布的《人工智能白皮书》(White Paper: On Artificial Intelligence — A European Approach to Excellence and Trust)对此限制已经有所缓和,根据欧盟 GDPR 和基本权利宪章,将人工智能用于远程生物识别只能基于正当和相称的目的,并应具备足够的保障。欧盟基本人权和消费者保护等特定行业的规定仍可适用于人工智能的场景,但需予以补充规定。并进一步提出通过新的监管框架来增强人们对人工智能的信任,如人工智能产品投入使用后将进行安全风险评估等。2020 年 3 月2 日,WEF 发布《人脸识别用例的责任限制框架——流程管理》(A Framework for Responsible Limits on Facial Recognition Use Case: Flow Management)白皮书,提出第一版人脸识别应用的十一项行动原则以建立人脸识别的监管框架,并希望通过分析人脸识别不同应用场景(包括准入系统、公共场所的安全保障、市场及客户服务、医疗保健服务)的案例,更好地权衡技术风险与监管,检验人脸识别监管框架[20]。GDPR 作为欧盟建立的数据保护领域的规则体系仍将发挥巨大的作用,但同样要警惕"一刀切"的严格立法与执法方式阻碍技术创新。如建立自动化决策之(事后)透明性原则和"算法责任制",要求数据控制者必须以数据主体能够理解结

果并行使其权利的方式解释自动化决策之结果[21]。将面部信息作为敏感个人信息加强保护，原则上禁止处理此类个人敏感数据，但仍确立了包括数据主体明确同意或处理对实质性的公共利益所必要等例外情况。

此外，美国伊利诺伊州 2008 年通过的《生物信息隐私法》(Biometric Information Privacy Act，BIPA)作为对生物识别信息保护规定最为严格的立法，其很多规定已经不适应发展的当下生物识别相关产业的实际发展，增加了企业的合规成本，甚至引发了消费者滥诉的风险。刚刚施行的 CCPA“以数据自由流动和便捷交易为价值取向”，在消费者隐私保护领域更加主动。因此，基于人工智能产业快速发展的现状，在中国《个人信息保护法》的制订过程中，借鉴国外立法之得失，顺应当下时代潮流，对于生物特征信息保护、自动化决策等制度的立法设计不宜过于严格，有条件地借鉴国外具体规则及场景化应用模式，为技术和产业发展留下充分的空间。

(三)具体制度考量

人工智能时代的《个人信息保护法》作为个人信息领域的统领性法律，蕴含着产业利益竞争、国家安全控制的内核，需要对当下已经产生实际争议的新兴技术做出回应，并对个人信息保护和自由高效发展技术产业作出权衡[2]。

《个人信息保护法》除赋予个人信息主体权利、制定个人信息收集使用的规则等传统制度外，如何回应人工智能的发展，目前主要体现在对于自动化决策、生物特征识别信息等的规制方面。大数据和机器学习从新的定性和定量维度对个人信息进行剖析，数据挖掘能力成倍增加，并有助于从大型数据库中发现有价值的信息(如设备维护记录、贷款申请、财务交易甚至医疗记录)并据此作出预测或建议。自动化决策在商业领域的合理运用可以提高经济效率，降低双向搜寻成本，有利于消费者的个性化定制与边缘创新，因此，肯定自动化决策在商业环境中的价值，赋予信息主体知情权与选择退出的权利，使其预测功能得到最大价值的发挥利用。在商业领域应用生物特征识别技术的情况下，除了认识到技术发展趋势及其带来的便捷和效率外，关键在于不能将生物特征识别作为唯一选项，而是应该给予用户是否使用此方式的选择权。更重要的是，加强对生物特征识别信息的数据安全保护，确保数据安全。

人工智能和数字经济的发展正在向世人展开未来的巨幅图景，数据价值将伴随着信息技术的进步而不断被挖掘和释放，科技创新也在为个人信息保护和数据安全带来新的动力支持。面向未来，中国需要制度创新的勇气和智慧！

注释：

① 如儿童信息保护领域的《儿童网络隐私保护法》(Children's Online Privacy Protection Act，COPPA)、电子通信领域的《电子通信隐私法》(Electronic Communications Privacy Act，ECPA)、金融领域的《公平信用报告法》(Fair Credit Reporting Act，FCRA)、《金融服务现代化法》(Financial Modernization Act/Gramm - Leach-Bliley Act，GLBA)及消费者保护领域的《联邦贸易委员会法》(Federal Trade Commission Act)。

② 挪威数据保护局认为“大多数人工智能的应用都需要大量数据才能学习和做出明智的决策”，因此尤其重视对数据的更大需求。

③ 根据 29 条数据保护工作组意见，人脸识别是指对包含个人面孔的数字图像进行自动处理，以进行识别、验证或分类的目的。

④ GDPR 第 22 条规定了数据主体有权反对完全依靠自动化处理(包括用户画像)对数据主体做出具有法律影响或类似严重影响的决策，且数据控制者应当采取适当措施保障数据主体的权利、自由、正当利益，以及数据主体对控制者进行人为干涉，以便表达其观点和对决策进行异议的基本权利。GDPR 第 4 条定义中“用户画像”指的是为了评估自然人的某些条件而对个人数据进行的任何自动化处理，特别是为了评估自然人的工作表现、经济状况、健康、个人偏好、兴趣、可靠性、行为方式、位置或行踪而进行的处理。

⑤ 根据 CCPA 相关定义，生物特征信息指指个人的生理、生物或行为特征，包括个人的脱氧核糖核酸(DNA)，这些可以单独或组合使用或与其他识别数据一起使用，以建立个人身份。生物特征信息包括但不限于虹膜、视网膜、指纹、脸部、手掌、静脉图案和语音记录的图像，从其识别模板(例如面部印记、细节模板或声纹)可以被提取，以及包含识别信息的点击模式或节奏、步态模式或节奏以及睡眠、健康或运动数据；互联网或其他电子网络活动信息，包括但不限于浏览历史、搜索历史和关于消费者与互联网网站、应用程序或广告交互的信息；个人信息还包括从该条定义中已识别的任何信息中得出的推论，以创建反映消费者偏好、特征、心理倾向、偏好、倾向、行为、态度、智力、能力和资质的画像。

⑥ 该特定情况指：a. 经营者采取了防止再次识别的技术保护措施；b. 经营者采取了专门防止再次识别的经营流程；c. 经营者采取了防止去识别化信息因疏忽而被泄露的经营流程；d. 经营者未试图重新识别去识别化信息。

⑦ 在国家和地方政策扶持、数据资源丰富等多因素的驱动下，中国广阔的人工智能应用市场成为发展优势。参见：《人工智能安全标准化白皮书(2019 版)》，第 4—6 页。

⑧ 中央银行上海总部发布《关于促进金融科技发展 支持上海建设金融科技中心的指导意见》，鼓励金融机构创新思维与经营理念、顺应智能发展态势，借助云计算、区块链、人工智能、生物识别等技术，依托金融大数据平台，找准突破口和主攻方向，在智慧网点、智能客服、智能投顾、智能风控等金融产品和服务方面进行创新。发展和改革委员会、交通运输部提出，“铁路要推广

自助实名制核验通道,实现'刷脸'进站。"商务部《关于推动便利店品牌化连锁化发展的工作通知》提出,"推广自助结算、扫码支付、刷脸支付等支付技术,鼓励采用数字货架、电子价签、无线射频等商品管理技术,提升服务智能化水平,优化消费体验。"

⑨ 公安部网络安全保卫局、北京网络行业协会、公安部第三研究所联合发布的《互联网个人信息安全保护指南》,国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、市场监管总局办公厅联合发布的《App 违法违规收集使用个人信息行为认定方法》等文件也要求确保用户有拒绝的权利,或需提供终止定向推送的选项等规定。

⑩ 《反恐怖主义法》第 50 条规定,公安机关调查恐怖活动嫌疑时可以依照有关法律规定对嫌疑人员采集肖像、指纹、虹膜图像等人体生物识别信息和血液、尿液、脱落细胞等生物样本,并留存其签名。《出境入境管理法》第 7 条规定,公安部、外交部根据出境入境管理的需要,可以对留存出境入境人员的指纹等人体生物识别信息作出规定。

⑪ 《规范》不仅加强了对个人生物信息的收集标准要求,还提升了个人生物信息的存储标准要求。个人生物识别信息的收集,应提前单独向信息主体告知收集、使用此类信息的目的、方式和范围,以及存储时间等规则,并征得个人信息主体的明示同意。存储方面,要求个人生物识别信息要与个人身份信息分开存储;原则上不应存储原始个人生物识别信息,可采取的措施包括但不限于:仅存储个人生别信息的摘要信息;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。

⑫ 2020 年 3 月 2 日,中国信息通信研究院以直播形式发布《"互联网 + 行业"个人信息保护研究报告》即建议加快推进个人信息保护相关立法进程;完善个人信息保护标准体系建设;严厉打击侵犯个人信息的违法违规行为;灵活适用个人信息保护原则;适应全球立法趋势,加强个人信息保护国际合作。

⑬ 《民法典(草案)》(2019 年 12 月 16 日稿)第 1032 ~ 1039 条。

参考文献:

[1] 高富平,王苑. 论个人数据保护制度的源流——域外立法的历史分析和启示[J]. 河南社会科学,2019,27(11):38—49.

[2] 张平. 大数据时代个人信息保护的立法选择[J]. 北京大学学报(哲学社会科学版),2017,54(3):143—151.

[3] Executive Office of the President. Big data: Seizing opportunities, preserving values [EB/OL]. (2014-05-01) [2020-03-16]. https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[4] MITROU L. Data protection, artificial intelligence and cognitive services: Is the General Data Protection Regulation (GDPR) "artificial intelligence-proof"? [EB/OL]. (2019-06-03) [2020-03-16]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914.

[5] KUNER C, CATE F H, LYNSKEY O, et al. Expanding the artificial intelligence-data protection debate[J]. International Data Privacy Law, 2018, 8(4):289—291.

[6] Article 29 Data Protection Working Party. Opinion 02/2012 on facial recognition in online and mobile services[EB/OL]. (2012-03-22)[2020-03-16]. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf.

[7] European Union Agency for Fundamental Rights. Facial recognition technology: Fundamental rights considerations in the context of law enforcement[EB/OL]. (2019-11-27)[2020-03-16]. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law.

[8] BURRELL J. How the machine "thinks": Understanding opacity in machine learning algorithms[J]. Big Data & Society, 2016, 6(1):1—12.

[9] European Data Protection Board. The Data Protection Ombudsman ordered Svea Ekonomi to correct its practices in the processing of personal data[EB/OL]. (2019-04-24)[2020-03-16]. https://edpb.europa.eu/news/national-news/2019/data-protection-ombudsman-ordered-svea-ekonomi-correct-its-practices_en.

[10] WALLACE N. EU's right to explanation: A harmful restriction on artificial intelligence[EB/OL]. (2017-01-25)[2020-03-16]. https://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm.

[11] 陈慧慧. 比较视角看 CCPA 的立法导向和借鉴意义[J]. 信息安全与通信保密,2019(12):26—36.

[12] 魏书音. 从 CCPA 和 GDPR 比对看美国个人信息保护立法趋势及路径[J]. 网络空间安全,2019,10(4):102—105.

[13] MOORE S. CCPA and face recognition to ensure personal privacy [EB/OL]. (2020-03-09)[2020-03-16]. https://www.biometricupdate.com/202003/ccpa-and-face-recognition-to-ensure-personal-privacy.

[14] 38th International Conference of Data Protection and Privacy Commissioners. Artificial intelligence, robotics, privacy and data protection[EB/OL]. (2016-10)[2020-03-16]. https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf.

[15] 陈军,谢卫红,陈扬森. 国内外大数据推荐算法领域前沿动态研究[J]. 中国科技论坛,2018(1):173—181.

[16] 张凌寒.《电子商务法》中的算法责任及其完善[J]. 北京航空航天大学学报(社会科学版),2018,31(6):16—21.

[17] 法制网. 新版个人信息安全规范发布 收集个人生物识别信息须用户明示同意[EB/OL]. (2020-03-13)[2020-03-16]. http://www.legaldaily.com.cn/IT/content/2020-03/13/content_8142754.htm.

[18] 吴汉东. 人工智能时代的冷思考[J]. 中国报业,2018(3):60—61.

[19] 程啸. 民法典编纂视野下的个人信息保护[J]. 中国法学,2019(4):26—43.

[20] 赛博研究院. 世界经济论坛:人脸识别用例的责任限制框架——流程管理[EB/OL]. (2020-03-13)[2020-03-16]. http://www.sicsi.org.cn/Home/index/look/id/368/type/产业研究.

[21] TANEJA H. The need for algorithmic accountability[EB/OL]. (2016-09-09)[2020-03-16]. http://dy.163.com/v2/article/detail/F7M59MU60511B355.html.