Advances in Social Science, Education and Humanities Research, volume 554
Proceedings of the 7th International Conference on Humanities and Social Science Research (ICHSSR 2021)

Research on the Legal Issues of Personal Information Protection Under the Background of Normal Epidemic Prevention
------Take the Application of Face Recognition Technology for Example

ZHOU Wan-yang[1,*]

[1]*Department of Law, Southwest Minzu University, Chengdu, Sichuan, China*

**wsww0226@163.com*

ABSTRACT
Facial recognition technology, known as "body code", is the latest application of biometric recognition. In the process of epidemic prevention and control, China's digital anti epidemic effect is remarkable. Scientific and technological means represented by face recognition technology can effectively save labor costs and improve the efficiency of epidemic prevention and control. However, as its application becomes more and more widespread, the risk of putting the public in the "dilemma" between public interest protection and personal information protection still cannot be underestimated. Face recognition technology has four major dilemmas: cognitive risk, imbalance risk, subject risk and damage risk. In this regard, the next step should be to fully grasp the application scenarios and take the "transition period" of the normalization of epidemic prevention and control. Refine the measurement standard of subject responsibility, clarify the legal boundary between data utilization and personal information protection; Standardize the collection of personal information, establish a security responsibility system throughout the whole process of face recognition application, and avoid the abuse of personal information by taking advantage of epidemic prevention and control.

Keywords: *Post-epidemic era, personal information protection, balance of interest, risk prevention*

疫情防控常态化背景下个人信息保护的法律问题研究
——以人脸识别技术应用为例

周宛央[1,*]

[1] *西南民族大学法学院，成都，四川，中国*

**wsww0226@163.com*

摘要
人脸识别技术被称为“人体密码”，是生物特征识别的最新应用。疫情防控过程中，我国数字化抗疫成效显著，以人脸识别技术为代表的科技手段能有效节省人力成本，提高疫情防控效率。然随其应用愈广，将公众置于公共利益维护与个人信息保护“两难”困境的风险仍不可小觑。人脸识别技术存有认知风险、失衡风险、主体风险、损害风险四重主要困境。对此，下一步应充分把握应用场景，走好疫情防控常态化的“过渡期”；细化主体责任衡量标准，厘清数据利用与个人信息保护的法律界限；规范个人信息收集，建立贯穿人脸识别应用全流程的安全责任体系，规避借疫情防控之由开个人信息滥用之口。

关键词：*后疫情时代，个人信息保护，利益平衡，风险预防*

1. 引言

自我国新冠疫情抗击工作开展以来，基于防控需求，大数据运用与信息化手段成为对抗疫情的有力武器，如病例行动轨迹分析、重点人群监测、疑似病例排查等，将海量信息与精准“狙击”巧妙对接，在抗疫历程中发挥了重要作用。情虽趋于平稳，其“后遗症”却并未消除。大数据运用于疫情防控便捷高效的背后，却是个人信息急剧“透明化”，隐私权限频受侵

扰的尴尬处境，疫情虽已得到控制，但个人信息的四散泄露确如洪水溃堤难以短期收回。其中，人脸识别技术又以其直接识别性、个人生物信息的唯一性、不可更改性、泄露后的无法逆转性等显著特征成为个人信息保护不可忽视的一部分，事实上，从多地小区、商场、校园陆续开通人脸识别，到人脸识别小程序、门禁系统、测温识别一体机的依次推出，庞大的安防市场也随之打开，其应用面之广、推广度之高也由此可见，背后的潜在风险与隐性问题不容小觑。

后疫情时代，对人脸识别技术的合理规制与科学运用是时代所需。因此，本文试以人脸识别技术为切入点，分析人脸识别技术推广运用所存在的认知、失衡、主体、误差四重风险，寻求疫情防控常态化背景下公共利益维护与个人信息保护的平衡点，力求从法律法规、责任矫正、技术制衡三维度提出针对性建议，对潜在风险予以回应，探索规范收集使用个人信息、更好保护个人信息的有效举措，这对于人脸识别技术长远、科学、合法、规范的发展，社会公益与公民个体利益的平衡具有重要意义。

2. 人脸识别技术应用状况概述

大数据的运用便利了疫情实时监控，也更好管控个人行程。从企业门禁考勤，到校园安全防控，再至社区、门店、交通站台、旅游景点等多种应用场景，但凡人流密集度高的区域，随处可见人脸识别技术的“身影”。就人脸识别用途而言，大体可分为公权力机关的公共应用、满足生活便利需求的日常应用、商业机构的商业应用及非营利性组织的公益运用四类应用方式。如公安机关的天眼系统，疫情防控的人脸信息监测等，能有效节省人力成本，也为逃犯追捕、防疫信息更新和公共秩序维护提供助益。又如公益机构的失物招领、寻亲平台，通过 “多方合一”的合作机制，更好协助失亲家庭寻找走失亲人。而日常应用及商业应用的部分则更为广泛，可以说渗透进公众日常生活的方方面面。然与之相对的是，我国迄今仍无明确的人脸识别法律规制，而仅作为一般个人信息保护的子项条款加以笼统规定，这对于解决我国目前人脸识别技术几近“滥用”而风险却缺乏把控的问题，无疑是杯水车薪。

3. 疫情防控中个人信息保护范围厘清

3.1. 个人信息定义溯源

追溯我国立法关于个人信息的定义，初次出现于《中华人民共和国网络安全法》（下文简称“网络安全法”）附则部分第 76 条第 5 款“个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。”但概念相对孤立，随后《中华人民共和国民法典》（下文简称“民法典”）在第 1034 条再次予以明确规定“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。”应对疫情情况，针对性地增补了“健康信息、行踪信息”两项，并将隐私权纳入并行保护轨道，对个人信息的处理条件、权利救济等也予以宏观规定，2020 年 10 月发布的《中华人民共和国个人信息保护法（草案）》（下文简称“个人信息保护法（草案）”），基于先前基础再次细化，且针对疫情类公共卫生事件中的个人信息保护的具体情形作出更详尽的回应。

综上，通过几部法律的定义比对，笔者认为，上述内容规定的共性在于个人信息具有显著的身份识别性与紧密的人身关联性，即对个人信息的自由支配和自主决定。其囊括范围或许会随信息技术的发展而不断调整，种类无法穷尽，但变化的多为形式，其主要特征却不会改变。事实上，《民法典》《中华人民共和国刑法》《网络安全法》《中华人民共和国数据安全法（草案）》《个人信息保护法（草案）》及诸多行业管理办法，已初步形成对个人信息保护的“全护航”。

随立法进程推进，学界关于如何保护个人信息的讨论也日趋热烈。如就法理层面的个人信息权，已有“宪法人权说、一般人格权说、隐私权说、财产权说、新型权利说、独立人格权说”[1]六种主要学说观点；而自划分角度观之，有的学者认为，个人信息权利作为一项与信息数据时代相伴相生的新兴权利，范围远超个人不愿为人所知、披露后会导致社会评价降低的私密信息，应属于一项独立自主的公法权利[2]；亦有学者认为，大数据时代下个人信息权具有鲜明的私法属性，是本人依法对其个人信息所享有的支配、控制并排除他人侵害的权利，作为一项独立人格权独有其价值与内涵[3]。观点虽有分异，但学界至少在一个层面达成了共识：个人信息需与一般信息、隐私权等概念相区别，需脱离传统民事权利体系的固化思维加以创新，理应加强对个人信息的保护，进而赋予新时代背景下个人信息全新的保护模式。

3.2. 人脸识别信息的独特地位

个人信息保护的立法保护脉络是逐渐明晰、日渐周密的过程，但面对大数据时代的波诡云谲与科技手段的更新迭代，“防患于未然”的愿景仍显力不从心，个人信息与隐私权界定概念含混、个人生物识别信息缺乏特殊保护等问题不容忽视。笔者认为最为重要的恰是人脸识别信息的特殊性。

我国目前立法对个人生物识别信息的法律定位不够明晰。虽《民法典》已于第 1034 条中说明“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定”。但具体如何区分一般信息、敏感信息、隐私信息却仍显模糊。此种表述方式，既不利于隐私权和个人信息保护的边界理清，也并未给予生物识别信息特殊的保护地位及保护方式，从而只能将其作为一般个人信息处理。若

说其他一般个人信息尚可以利用数据脱敏的手段加以保护，而生物识别信息尤其是人脸信息所具备的不可更换性与明显识别性，显然无法通过该途径保护。而《个人信息保护法（草案）》中虽已对该问题有所回应，将敏感个人信息作为专节设置，且也将“个人生物特征”纳入“敏感个人信息”，但依笔者之见，人脸识别信息相较于条文中所指的其他敏感个人信息（如宗教、种族、医疗信息），乃至在个人生物识别信息的范畴中又更具特殊性，其独有的直接识别性、侵入性、非接触性的显著特征，与现有较为笼统的立法规制手段、人脸信息及人脸识别技术特殊风险并不契合。因此，理应正视其差异，给予其更为严密周延的单独立法保护。

4. “人脸危机”与个人信息保护的四重风险

4.1. 认知风险

结合前文可知，我国当前的个人信息处理多以“知情同意”作为信息使用的主要正当性基础。但面对人脸识别技术，这一理念的落实难免流于形式。首先，人脸识别技术作为一项新兴科学技术，显然具有认知门槛，以多数公众获取信息的途径，极有可能仅观察到“硬币的一面”，难以发现所谓方便快捷的背后所潜藏的巨大信息泄露风险。信息储存的位置或时效、谁能为储存的安全性“背书”、信息的私密性如何确保等通通缺少明晰的答案。哪怕征得公众同意，其同意适用范围权限与实际适用范围是否能始终保持一致不得而知，又如有些协议以“包含但不限于”的条款无限降低对用户人脸信息的使用底线。如若依据该条款任意使用和处理人脸识别信息，显然会突破收集面部信息是为服务用户亦或维护公共利益的初衷[4]。公众在缺乏充分知悉情况的前提下，所做出的同意意思表示难说属于实质意义上的“授权”，若侵权行为发生后意图寻求权利救济，曾经的“同意”甚至会成为阻碍维权之路的绊脚石。再退一步说，人脸识别技术相区别于指纹录入等其他生物信息，需要切实交互方可做到，其可直接识别性和易采集性的明显特征决定了信息采集的隐蔽、迅速、快捷，公民的面部信息完全可能在不知情的状况下处于“裸奔状态”，连“表面同意”也被抛却，让本身即处于弱势一方的公众尤为恐慌。

4.2. 失衡风险

个人信息本身具备公私利益交织的属性，因公众作为社会构成的一份子，其个人信息本身也是公共利益维护的重要一环。相区别于隐私权的个人性、私密性，与国家安全有着更为紧密的联系，并有必要情况下个人利益需适度让渡于公共利益的显著特征。疫情防控期间，公众很难对提供个人信息的要求说“不”，诚然，缺乏个人信息与相关数据的收集分析，公权力机关就很难在短时间内制定有效的防控方案，也不排除如果执法机构获取个人信息都需要获得个人同意，那么个人就会有足够的时间与机会藏匿或删除执法所需信息，滥用权利破坏执法所需要的信息与证据，造成信息失真，进而严重破坏国家的执法能力与社会公共利益[5]。若信息大数据的价值被充分利用，合理发掘，于国计民生、安全防控、科学研究等自然有益，但在现实情况下，收集主体繁杂不清，个体授权以信赖为要旨，商业利益主体的营利性质注定难以交付个人信息信任，相应立法框架又边界模糊，正如疫情期间，大量个人信息被非法收集买卖，运用于商业营销、广告推销，网络上亦有因未经脱敏的病例信息曝光而遭受“人肉搜索”等网络暴力，还有甚者通过个人信息盗窃财物走向犯罪。面部信息作为当前电子支付的主要方式之一，一经利用后果不堪设想。在多数人沉默之时，公私利益保护走向失衡，个人信息面临被滥用的巨大风险。质言之，要求信息不对等的弱势方反向承担信息泄露最严峻的后果，显失公平。

4.3. 主体风险

关于主体风险，不仅包括个人信息所有者，随信息技术发展的愈发成熟，信息收集者、信息处理者及信息者主体等更多主体均可能参与信息“流通链”。换言之，参与主体越多，个人信息所有者面临的侵权风险可能性便越大，信息主体对个人信息的控制权也愈见削弱，相应寻求权利救济的可能也愈困难。从公权力机关观之，国家的个人信息治理成效一定程度上可以反映个人信息保护的走向，若执法过程中未能掌控好公私利益的界限，其后果将更为恶劣。

换言之，疫情防控时期人脸识别技术的运用推广乃至强制推广是否确有必要？其运用当真不可取代吗？其有益之处足以弥补潜在风险吗？谁能为这些风险买单？如许多企业并不具备相应的风险防控能力与安全保障举措，也难以妥善充当数据收集者的角色，在以疫情防控需求收集个人面部信息后，或不尽妥善存储义务，或将海量面部数据整体泄露。加之个人信息本就有流动性强的特征，而以电子形式存储的面部数据更加剧了网络空间中流动的风险性，如此便是将公民个人信息安全视若无物。即便公民想寻求权利救济，往往也是陷入面临举证困难、无从追责的尴尬处境——所有接触过信息的主体都将成为潜在的侵犯者，但受害人往往难以查清个人信息的真实“脱节”与泄露情况，只能接受利益受损。

4.4. 损害风险

人脸识别技术虽已发展较为成熟，但难免受制于天气、温度、色差甚至种族等诸多要素的影响，也会因人脸间的相似程度、数据样本集的缺乏、数据规模度的大小、脸部特征提取难易程度有所偏差，进而存在识别错误的可能性。不当利用人脸识别技术会侵犯隐私利益，可能给信息主体带来社会评价降低、信誉受损、歧视等损害，人脸识别技术的算法偏差性也间

接导致了损害发生[6]。这种误差的发生轻则影响正常生活秩序，重则可能导致错误逮捕无辜者，令其遭受难以弥补的心理障碍与精神创伤。这种风险并非危言耸听，据《纽约时报》2018 年 2 月 9 日发表 MIT 媒体实验室研究员研究文章《Facial Recognition Is Accurate,if You're a White Guy》称，人脸识别技术针对不同种族的准确率差异极大。其中，针对黑人女性的错误率高达 35%，而针对白人男性的错误率则低于 1%，并得出“微软、IBM 和 Face++ 所做的面部识别算法，相比白人男性更容易混淆黑人女性的性别”的结论，而这一缺陷后续也获得了 IBM、旷世等相关机构的承认，且是“在业内普遍存在”的一类问题。

除此之外，以保护公共利益为由，随意允准各式组织收集公民面部信息，不仅危及主体的信息安全、财产安全，可能被二次出售、非法应用。面部信息的唯一性与不可更改性两项特征甚至会危及主体的身份安全，导致身份被冒用的巨大风险。

综上所述，相较于财产损害，信息主体在面部信息泄露后更可能蒙受精神损害，即对个人正常生活秩序造成侵扰。但由于侵权对象难以确定，财产损失往往并不明显，而精神损失的法定标准又难以达到，个人想要寻求合适的救济方式非常困难。遗憾的是，现有《民法典》中匮乏对相关损害后果的明确救济路径，《个人信息保护法（草案）》的敏感个人信息专节也缺少相关内容。

5. 个人信息保护困境相关解决建议

5.1. 加强差异化立法规制，厘清个人信息适用边界

邢会强曾引入风险预防理论与场景理论的概念，并指出以同一与差异相结合的规制原理以应对个人信息保护未来的不确定性，通过不同的适用场景、不同的使用用途，进而采取差异化的应对策略。[7]对此，笔者予以认同，我们既应正视人脸信息识别技术在各种适用场景使用的共性特征，并围绕此建立贯彻人脸识别信息保护全流程的责任安全体系，也应明确不同应用场景、应用方式的内容区别，采取差异化的手段予以规制。不能基于特殊缘由而持续降低准入门槛，直至面部信息数据滥用的严重后果酿成再反向予以救济，也不能“一刀切”地全盘否定，仅为规避风险而错失大数据时代的信息红利，而应有的放矢，基于数据利用优势最大化的价值理念，针对性区分信息在不同场景使用中的敏感性层级划分，进而确定相应的数据利用规则、相关保护举措、适格主体以及责任划分，力求在有所分异的使用场景中满足各方主体的期待预期。

此外仍需注意的是，尽管可以采取差异化的方式灵活应对不同的使用场景和实际用途，但过于零散的应对模式也不利于人脸识别技术的大规模应用展开，因此仍需注意体系化的区分应用场景大类，并注意在各类场景中留有发展空间。其次，“存异”方需“求同”，差异化运用的前提是共同的准则与底线，让用户对个人面部信息识别的安全性抱有合理期待。而不能以特殊情况开“特权”之口，致使衡量标准参差不齐，同时可以考虑以典例发布、新闻宣传等模式让公众及相关主体具象化了解相关信息的含义及不同场景模式下的适用边界，进而为个人数据信息的合理使用与个人信息的有效保护提供明确引导。

5.2. 矫正信息主体失衡状态，提高公众信息自决权

结合上文关于脸部信息保护的内容分析，我们可以发现，在前有知情权流于形式，中有“同意”往往被多种意志裹挟，后有信息滥用风险不可估量的严峻情况，传统的“知情同意”作为正当性基础的个人信息保护模式对人脸信息的保护作用早已名存实亡。相较于一般个人信息而言，脸部信息保护显然需要结合其技术发展态势予以独立的规制体系，无论自何角度出发，以牺牲个人信息支配自由所换取的数据利益显然有悖公序良俗，个人信息都是人格尊严的象征符号，当疫情防控步入常态化阶段，公民虽仍存有不同程度的个人信息公开责任，但个人信息自决权作为准则决不能突破。信息主体与信息收集者处于天然不对等的状态，尤其是个人与商主体间的地位严重失衡，依靠个人力量难以实现有效对抗。

正如王利明认为“对于个人信息权的保护,应采取注重预防的方式,主要原因还在于应在法律上实现信息主体和信息控制者之间的地位平衡”[8]，天平的两端，需要制度发挥矫正地位的作用。

为更好实现制度的矫正功能，一方面，需要在制度安排中对弱势方予以倾斜保护，提高公民个人信息自决权，不再以形式上的“告知同意”成为数据滥用与数据风险的“免死金牌”，为自决权的实质有效行使添砖加瓦。同时，公众也应加强个人信息保护意识，尤其是面部信息等敏感生物识别信息，更应深入了解信息的来源，努力将风险扼杀于源头。

另一方面，也要提高信息收集者的准入门槛，尤其是具有营利性的商业机构，在收集利用个人面部信息的过程中需有更严格的资质审查，强化企业风险承担责任，要求“享受利益者承担风险”，促使信息收集者与信息主体共担风险，借此方能让相关信息收集者不再以信息主体的“知情同意”作为唯一目标，进而让个人信息泄露与滥用的风险不再由信息主体“自咽苦果”，而是成为信息控制者的关注点。其次，需以获取授权为起点，尤其是面对疫情此类公共卫生突发事件，信息流动性大，收集量多，更需加强信息使用监督要求，避免有不良商家假借疫情防控之名行滥用个人信息之实。在此期间，商业机构的人脸识别技术运用应以维护公共秩序及服务消费者作为首要任务，并要及时制定完备利用方案，报请政府机构备案登记。最后，政府机构也应严格对自身的要求，未经有权机

关批准同意，不得自行安装、使用人脸识别技术。网信等相关部门应主动承担起责任，加强控制非必要的个人面部信息收集设施使用，实时监管信息使用的合法合规情况，并要求商业机构在后疫情阶段及时、定期、批量删除非必要储存的个人信息内容，明确规定违规收集个人信息将面临的处罚内容，同时，先进的制度设计与切实有效的行动力是良好生态的风向标，所以，公权力机关也应在信息的收集上保证公开透明，确保信息收集流程的规范化。从立法、执法两个维度矫正信息主体失衡状态，更好保证个人信息权益。

除此之外，虽个人信息保护理应以事先预防为主，但事后救济的路径同样应以立法明确。继前文所述的考虑加强立法针对性，可考虑于《个人信息保护法》中另设“个人生物识别信息”专节，对人脸信息识别予以特别规制，还需对完整救济路径予以明确，以弥补《民法典》中相关规定模糊适用困难的缺憾。笔者认为：

第一，可考虑降低精神损害在个人信息保护领域的适用门槛，亦或适度扩大“信息损害”的涵盖范围以降低救济难度；第二，针对侵权主体的强势地位引用“集合诉讼”模式，以规模化的集合规避个人面对复杂侵权主体“单打独斗”的窘境；第三，给予公民更有力的发声权与自我信息捍卫途径，如充分告知、书面同意、不得以不同意为由拒绝信息服务等，以“实质同意”规范取代“形式规范”，第四，结合不同主体，不同场景对过错责任、无过错责任以及过错推定责任原则灵活适用，让权利救济有径可循。

5.3. 加强新兴技术制衡，增强信息交互信任度

追溯个人信息保护的本质问题，其实是“信任危机”，公权力天然具有的强势性、商业主体以盈利为目的的天然属性、日趋复杂的信息主体彼此博弈、层层叠叠的信息中间环节时刻面临脱节风险、信息主体处于信息不对等的最弱端……诸多要素相互作用，无不将公众时时置于信息泄露的恐慌中。而区块链技术因其链式存储、加密算法、分布式架构、共识机制和智能合约技术特征[9]，既能有效提高个人信息自决权，又以“去中心化”的方式促使用户个人信息主权重新得到技术承认巩固，更好保证多元主体利益平衡，并能充分挖掘数据信息价值，推动个人信息可信共享，化“个人信息孤岛”为联动的大数据网络，发掘背后隐藏的商业价值与公共性价值，为个人信息治理困境的破解提供全新可能。而且区块链技术具有不可篡改性，使用非对称加密技术，能够对侵权行为进行溯源抓取记录，做到“全程留痕”，具有高度的信任背书，再次，区块链技术还能有效解决个人信息侵权寻求救济困难的问题，在个人信息保护中，区块链证据的法律效力已于司法实践中获得认可。同时，区块链技术结合爬虫、大数据等技术，能对侵权行为进行抓取分析和识别，并能对用户因侵权致使的损失进行动态分析，精准确定侵权赔偿额[10]。因此，以区块链为代表的新兴技术引进无疑能为现阶段的个人信息保护提供了一种可行性极高的新思路。

6. 结论

人脸识别技术的运用“牵一发而动全身”，不仅关乎每个人的切身利益，同时也涉及社区、政府机关、商业机构、公益组织等多元主体，将其纳入合法规制的轨道需要各方协作配合、共同发力。后疫情时代，走稳走好个人信息保卫战的过渡期至关重要。科技是一把双刃剑，数字化抗疫不仅是一次在突发性公共卫生事件中的有效尝试，也为我国个人信息保护法律框架的构筑提供了完善的发展新思路，个人信息的收集和使用理应以社会共同利益作为核心出发点，找准公私利益、数据信息利用与个人信息保护的平衡位置，也应考虑新兴科学技术的合作治理、互利共赢，让科技智慧为我国的法律宏图造血赋能。

REFERENCES

[1] Zhang, L, Han, X.(2016). The property of personal information right in private law in the era of big data. Law Forum, 31(03):119-129.

[2] Zhou, H.(2020). The legal positioning of personal information protection. Law and Business Studies,37(03):44-56.

[3] Ding, X. (2018). The Predictions and Solutions of Personal Information Protection in Private Law. Legal Studies, 40(06):194-206

[4] Lin，L, He，X. (2020). The legal regulation path of face recognition [J]. Chinese Journal of Law, 41(07):68-75.

[5] Ding, X. (2020). The right to personal information: a case study of the United States of America [J]. Chinese and Foreign Law, ,32(02):346-347.

[6] Yan, S. (2020). Tort Relief of Biometric Technology such as Face Recognition -- From the Perspective of Personal Information Protection. Journal of Henan Institute of Technology, 28(06):74-80.

[7] Xing, H.(2020). Legal Regulation of Face Recognition. Comparative Law Research,5:51-63.

[8] Wang, L.(2013). On the Legal Protection of Personal Information Right -- Focusing on the Division of Personal Information Right and Privacy Right. Modern Law, 35(04):62-72.

[9] Wang, L, Wang, S.(2020). Dilemma Traceability and Pattern Innovation: Research on Personal Information Cooperative Governance Based on Blockchain. Chinese Administration, 12:56-61.

[10] Wu, J.(2020). Research on Application of Blockchain Technology in Personal Information Protection. Internet World, 11:38-43.