【新闻与传播】

区块链与公民隐私保护的技术想象*

顾理平

摘　要:在中国传统文化中,隐私权作为一种人格权利在相当长的时间里并没有受到应有的重视。但是,中国法治现代化进程的快速推进和公民隐私权意识的不断增强,使我国在较短的时间里完善了公民隐私权保护的法律法规体系。随着大数据时代的到来和人工智能技术的普遍应用,公民的隐私权面临技术进步带来的严峻挑战,相对滞后的隐私权保护法律法规难以及时应对这种挑战。区块链中呈现出的去中心化、强加密和可追溯等技术特征,为公民隐私保护提供了一种可能的技术想象。

关键词:隐私;隐私权;区块链

中图分类号:G206.2　　**文献标识码**:A　　**文章编号**:1003-0751(2020)03-0166-07

隐私权是一项重要人格权利,但是中国公民对其认知过程和法律保护都比较滞后。绝大多数中国公民直到20世纪80年代,才开始从权利的层面接触隐私概念,在此之前只有少量的学术文章有所介绍,法律保护则更显滞后。尽管党的十一届三中全会以后,中国快速开启法治现代化进程,但在2009年《侵权责任法》首次正式从法律条文的角度确认隐私权为独立的人格权之前,公民隐私受到侵害一直以名誉权受损来适用法律条文的。随着中国社会的不断发展和公民个人自主意识的增强,这项权利近年受到普遍重视并开始从独立人格权的层面得到法律保护,也很快在《网络安全法》中得到了数字化时代的法律保护。最近公布的《民法典(草案)》讨论稿中,还对其进行了更加明确具体的规定。也就是说,从隐私权的概念共识形成到符合时代发展趋势的现代法律条文保护,其经历时间之短在世界范围内都是比较罕见的。

随着网络社会的到来,曾经行之有效的隐私权保护体系,却遭遇了前所未有的挑战。隐私之"隐"是因为其为一种私人生活、私人权利,需要与"公"区隔开来。前网络社会中,私与公的界限是比较分明的,隐私主体只要不向公共空间扩散隐私,其隐私权就可以得到比较好的保护。在网络社会,数字化生存中的人们私与公的边界开始消融,大数据技术的快速发展和人工智能的完善还导致数字化的整合型隐私形成,从而产生了无法被及时感知的"无感伤害"。换句话说,传播技术的进步令现代人的隐私无"私"可"隐",人们真正成为"透明人"。大数据和人工智能等技术导致的隐私困境,也许只能期待通过区块链技术寻求技术解决方案。

一、从广受漠视到渐趋完善的隐私保护体系

对于现代公民至关重要的隐私,在中国传统文化中并未受到足够的重视。家国的混杂长期影响着中国人对隐私的认知。在中国传统文化中,"家"最初是指大夫的封地,与诸侯的封地"国"相对应。两者虽然并不互属,但密切关联,并无本质差异。具体到"家",家是连接个人与国家的纽带。一个人在衣食住行及教育成长过程中,必须受到家的扶持和亲族的庇护。我们熟知的"修身、齐家、治国、平天下"

收稿日期:2020-02-15

*基金项目:国家社会科学基金重点项目"人工智能时代公民隐私保护研究"(19AXW009)。

作者简介:顾理平,男,中国新闻史学会媒介法规与伦理研究委员会会长,南京师范大学新闻与传播学院教授,博士生导师(南京　210097)。

的观念,表达的正是这种家国思想。就如《礼记》所述的“君子之道,造端乎夫妇;及其至也,察乎天地”,即个人在家庭中的私人行为最终折射着其未来的社会行动准则。具体到家国的治理上也体现彼此类推的特征:父亲在家庭中“君临一切”,君主在全国“君临天下”。这种互生关系是建立在对个人私人生活漠视的基础上的,也正是因为这样,“私”在中国传统文化中往往以负面形象出现。从词性上讲,“私”在绝大多数时候是以贬义词的词性出现的。尧舜禹无私禅让和为民尽心竭力的传说,很好地表明了先贤们对“公”与“私”的态度。《韩非子·饰邪》称:“公私不可不明,法禁不可不审。”《礼记·礼运》载:“大道之行也,天下为公。”……类似的言语很多,不仅确立了“公”“私”的严格分野,也在彼此地位的高低上进行了明确的判定。

传统文化中对“隐私”的漠视在相当长的时间里也令现代中国公民在日常生活中的隐私被漠视。打探、讨论他人隐私,长期以来是黎民百姓的一种生活日常,而刻意保护个人隐私却时常被视作“另类”——如果是光明正大的事,别人当然可以关注;如果需要藏着掖着,那一定是“见不得人”的事。回望那段中国公民隐私经历的不堪时期可以发现,隐私在相当长时间里是被作为“阴私”看待的。1984年,上海辞书出版社出版的《法学词典》还未有“隐私”或“隐私权”辞条,但有“隐私案件”的辞条——“亦称‘阴私案件’。内容涉及奸情、伤风败俗或其他私情私事方面的案件”。直到1994年,法学家王利明主编、吉林人民出版社出版的《新闻侵权法律辞典》中还这样写:“阴私(Privacy),参见‘隐私’。”这是当时公民隐私状况的一个缩影。在这种状态下,公民隐私当然不可能作为权利受法律保护,更多的时候是作为一种媒介、谈资被口口相传。即使在当下的中国社会,依然有很多人将知晓彼此隐私多寡作为衡量感情深浅的重要依据,且颇具验证效果。

党的十一届三中全会以后开启的中国法治进程,虽然没有在开始阶段给予公民隐私以应有的地位,但随着社会文明的推进和公民自主意识的不断提升,隐私很快上升到一种独立人格权的层面并开始受到法律的保护。我国1986年颁布的《民法通则》第101条规定:“公民、法人享有名誉权,公民的人格尊严受到保护。”《民法通则》没有直接规定对公民个人隐私权的保护,但由于一般性地规定了公民的人格尊严受到法律保护,这便为司法解释留下了较大的空间。人们的普遍认知是:隐私权应当属于人格尊严的一个部分。最高人民法院《关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见》第140条第一款规定:“以书面、口头等形式宣扬他人的隐私,或者捏造事实公然丑化他人人格,以及用侮辱、诽谤等方式损害他人名誉,造成一定影响的,应当认定为侵害公民名誉权的行为。”最高人民法院在《关于审理名誉权案件若干问题的解答》(1993年8月7日)中再次强调指出:“对未经他人同意,擅自公布他人的隐私材料或者以书面、口头形式宣扬他人隐私,致他人名誉受到损害的,按照侵害他人名誉权处理。”“文中有……披露隐私的内容,致其名誉受到损害的,应认定为侵害他人名誉权。”在这个阶段,隐私权虽然没有作为一项独立的权利受到法律明确的保护,但从20世纪80年代末到90年代初作为一个学术概念被讨论进而进入正式的法律解释、解答层面,其速度之快、效率之高,是令人鼓舞的。这也从一个侧面说明,隐私权之于现代公民而言有其特殊意义。2009年,我国正式颁布了《侵权责任法》,在这部法律中,第一次将“隐私权”作为一项独立的民事权利在法律中加以规定,标志着我国公民的隐私权保护真正进入到法律有效保护的阶段。

传播技术的发展和网络社会的到来,给隐私保护提出了新挑战。我国立法者对这种挑战的回应主要体现在《网络安全法》和《民法典(草案)》中。随着数字化时代的到来,数字化生存中人们的隐私更多是以信息、数据的形式出现,所以,立法者力图在法律条文中作出时代性的回应。《网络安全法》明确规定:“网络运营者收集、使用个人信息,应当遵循合法、正当、必要原则,公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意。”“网络运营者不得泄露、篡改、毁损其收集的个人信息;未经被收集者同意,不得向他人提供个人信息。”“个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用个人信息的,有权要求网络运营者删除其个人信息……”在2019年12月公布的《民法典(草案)》中,则进一步对隐私权进行了明确保护。在关于“隐私”的概念中规定“隐私是自然人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”。随后对上述权利侵害

的行为进行了明确规定:“(一)以短信、电话、即时通讯工具、电子邮件、传单等方式侵扰他人的私人生活安宁;(二)进入、窥视、拍摄他人的住宅、宾馆房间等私密空间;(三)拍摄、录制、公开、窥视、窃听他人的私密活动;(四)拍摄、窥视他人身体的私密部位;(五)收集、处理他人的私密信息;(六)以其他方式侵害他人的隐私权。”这些规定非常明显地体现出法律对数字化时代隐私保护问题的现实关切。除了权威的法律保护外,我国相关部门还从部门规章、政策层面等制定了一系列保护公民隐私的配套法规,并要求相关企业制定隐私政策、隐私条款或自律公约等,构建一个公民隐私保护的完整体系,这种多方面的努力正在不断发挥积极作用。

总而言之,在传统媒体时代,尽管中国公民的隐私曾经有过一段不受待见的经历,但随着对这项人格权利重要性的不断认知,隐私权在较短的时间里得到了有效保护,中国公民可以更好地享受到人格尊严。但是,即便如此,我们必须客观地承认这样一个事实:从我国公民当前隐私受到侵害的现实情况看,这种保护还存在亟须改变的薄弱环节。这是因为,一方面,法律规定和政策等的制定有一定的滞后性,出台后又具有相对长时间的稳定性,不可能对日新月异的隐私侵权形式作出即时回应;另一方面,大数据、人工智能等新技术的不断发展,除了对社会进步的诸多方面带来积极推动作用外,也对现代公民的隐私构成了新的挑战。现行保护体系已经较难有效地保护数字化时代的公民隐私。

二、大数据和人工智能技术令隐私保护面临困境

(一)数字化技术进展中的中国社会

在数字化时代,人们在现实生活中所有的言行全部被数字化,真正以数字化生存的方式存在,人们的社会联结方式也发生了巨大的变化。这种变化首先表现为社交空间借由网络得到无限扩展,“由于是否身处同样的地理位置已经不再是人们初次见面的先决条件了,人们潜在的关系范围比历史上任何时刻都要广阔”①。与此同时,人们在现实世界和虚拟世界的活动都会在公共空间留下大量数据,给个人隐私保护带来影响。大数据技术是以关系为纽带的一种数据挖掘技术,由于公共领域中的数据中包含了大量公民的隐私数据,所以这种挖掘极易侵入人们的隐私领域。鉴于此,一些学界和业界人士对公共空间数据的流动和处置持有比较保守的态度,强调应对这些数据进行强保护。从隐私权保护的角度看,这种观点有其合理性,但从推动大数据和人工智能技术发展的角度看,过度限制公共空间数据的流动显然并不合适。因为一旦对公共空间的数据流动作出更多限制,显然不利于数字化时代数据作为社会“能源”作用的发挥。

作为机器学习的人工智能技术的发展成熟,既借助信息传播技术的成熟,也借助数据挖掘技术的成熟和计算速度的快速提升。这种进展一定会对公民的隐私保护产生影响。2016 年,国务院印发《促进大数据发展行动纲要》,把大数据上升为国家战略。2017 年,国务院再次印发《新一代人工智能发展规划》,明确把人工智能上升为国家战略:2020 年,人工智能总体技术的应用与世界先进水平同步;2025 年,人工智能基础理论实现重大突破,部分技术与应用达到世界领先水平;2030 年,人工智能理论、技术与应用总体达到世界领先水平,成为世界主要人工智能创新中心。“人工智能是计算机科学的一个分支,现在无论其研究方法还是研究成果形态都离不开计算。”② 当然,随着人工智能技术的不断发展,其本身也正在不断拓展和融入更多的学科知识,从而开辟了更为广阔的天地。从大数据和人工智能技术本身的快速发展和中国政府颁布的一系列决策看,新技术将对中国社会的几乎所有领域都产生深刻影响,同时也会对公民的隐私保护产生深刻影响。智能技术的快速发展会不断提升智能机器的数据挖掘处理能力,被数字化的公民隐私正面临着深度精准处理的困境。

(二)数字化监控和数据挖掘中的公民隐私

大数据和人工智能技术首先在现代社会治理中被普遍应用——即无所不在的数字化监控。在数字化社会,人们的几乎所有行为都会留下数字化痕迹。所以,数字化监控是一种全方位的监控。密布于城乡的监控视频每天收集着人们的出行轨迹,这是一种可感知的有形数字监控;无处不在的数据采集中心则是功能更为强大的无形监控。现代人生活在由数据监控的“超级全景监狱”中,并且“超级全景监狱中的数据库给每一个人都构建了身份”③,这个被构建的“数字化身份”无时无刻不在影响着人们的现实生活。但是,社会治理过程中数字监控的普遍使用并未导致被监控者更多的逆反排斥,这是因为

数字监控会带来更多的安全感。“我们必须认识到社会作为一个整体,它的安全比监控更重要。”“通过优先考虑安全性,我们将保护这个世界的信息流,也包括我们自己的信息流,免于被窃听以及遭受更具破坏性的攻击,如盗窃和销毁。”④“9·11”事件发生后,许多曾经强烈排斥城市视频监控的美国公民,对此持有更加开放包容的态度。曾经长期困扰中国城市治理者的“摩抢”(骑着摩托车抢劫)案件因视频监控的普遍设置而极少发生。而在2020年初新冠肺炎疫情暴发后,疫情防控和流行病学调查更是通过对公民行踪数据的有效使用,为快速有效遏制疫情发挥了积极作用。从根本上说,社会治理者和全体公民在社会监控上看似存在矛盾,但实际上是“命运共同体”,社会治理者作为社会群体的一员,他们同样有对安全感的渴望。当然,对安全感的追求并不是滥用监控数据的理由,因为与监控行为相伴生的,一定是大量公民隐私数据被收集和存储,这就可能构成对公民隐私的潜在伤害。

电商企业对数据的挖掘有着本能般的冲动——资本推动的企业对数据以及由此可能带来的利益有着天然兴趣,因此,通过数据监控寻找商业机会的行为是一种“商业日常”。近年来,“精准广告”成为一种新兴的广告形态大行其道。精准广告主要通过对消费者相关数据的挖掘、计算、处理,分析其行为逻辑,借助人工智能对用户进行精准“画像”,从而实行个性化的广告投放,实现理想化的广告效果。“2014年的《中国互联网定向广告用户信息保护行业框架标准》中给出了这样的定义:‘通过收集一段时间内特定计算机或移动设备在互联网上的相关行为信息,例如浏览网页、使用在线服务或应用等,预测用户的偏好或兴趣,再基于此种预测,通过互联网对特定计算机或移动设备投放广告的行为。’我们可以发现,精准广告就是借助信息数字技术,通过搜集和分析用户个人数据对其需求和偏好进行预测,并据此投放具有针对性营销内容的行为。”⑤从“精准画像”到“精准广告”,这个过程可以让我们比较清晰地知晓电商企业的商业动因和商业实践。需要特别说明的是,在大数据时代,人们的商业行为已经基本实现了数字化,衣食住行等几乎所有的个人需求都可以“一机搞定”,如果采用现金支付手段,也会在网络中留下痕迹。即使不发生商业行为,但个人在网络使用行为中留下的痕迹,在大数据时代的电商眼中,也意味着“商机无限”。各种传感技术的普遍应用,正在造成这样的困惑:“传感器所收集的信息不仅仅局限于某一特定的时间或地点,还能扩展到更广泛的范畴。喻国明等学者曾指出传感器一方面可以扩宽信息的来源途径,例如利用传感器实时监测环境数据(包括温度、湿度等),甚至可以采集用户自发产生的生理数据(如脑电与心跳)。另一方面,传感器还扩宽了信息的采集维度,包括时间维度与空间维度。”⑥公民的隐私,就这样赤裸裸地被收集、利用着。

(三)技术导致新类型隐私和新形式伤害

自从隐私权被作为一种人格权开始受到保护后,其内涵虽然也在不断丰富,但其类型并无本质性的变化。换言之,公民的隐私在相当长的时期内主要表现为一种生物特征隐私,如生理特征、情感经历、个性癖好等。在传统媒体时代,传播技术的进步(从纸质媒体到电子媒体)并没有给隐私类型带来太多显性变化。基于隐私类型相对稳定这种现实,我们更多关注的是对隐私保护方式的多样化变化应对。随着大数据时代的到来,隐私类型相对稳定的特征发生了改变,技术导致的新类型隐私已经产生。

“在我们这个时代,美国国家安全局掌握的德国公民信息要比民主德国时期史塔西知道的还要多。美国情报部门能够掌握人们每次行动,得到每次电子交换信息,知晓个人日常生活的每个瞬间。如今人们清楚地意识到,有个看不见的间谍,在我们的口袋里和手机待在一起。它和史塔西的秘密警察一样,仔细地记录我们的出行,监视我们和什么人联系,窥探着我们的朋友,当我们在写记事本、发短信、收邮件、翻看相册照片或视频时,这个间谍趴在我们的肩头默默审视一切。它是我们生活的记录员,在它面前,我们什么也掩藏不了。”⑦这一段论述比较形象地呈现出现代公民隐私的现实困境,但这种“呈现”还是一种表层“呈现”,在大数据挖掘技术不断进步的深层,公民的数据可以被整合成新类型的隐私,从而被更“全面地”呈现。整合型隐私是指通过数据挖掘技术将人们在网络上留存的数字化痕迹进行有规律整合而成的隐私。与传统隐私表现出的生物特征不同,大数据时代的隐私表现为明确的数字化隐私特征,这是因为这种隐私的产生基于两个基本的前提:一是人们的言行被数字化,二是这种被数字化的数据可以通过数据挖掘技术进行有规律的

排列组合。大数据技术是以关系为纽带的数据挖掘技术,这里的关系正是形成整合型隐私的关键所在。一位研究者曾经在研究过程中收集到这样一个案例:一位新婚妻子感觉自己可能怀孕了,但没有告诉包括丈夫在内的其他任何人。但是不久,她就不断收到婴幼儿用品公司和保险公司的推销广告,这意味着她怀孕的隐私信息被泄露了。调查发现,她怀孕的信息是数据公司挖掘到了关于她生活中间的两个似乎微不足道的举动——浏览过两次育儿网站;购买化妆品时把以前习惯使用的刺激型化妆品改为温和型化妆品。数据公司把这两个举动关联到她身上,得出了她(可能)怀孕的结论并把此信息出售给相关商业公司。这是一种比较典型的整合型隐私形成的个案。人们每天都会在生活中或网络上留下无数个人活动的数据,这些数据在以前只是杂乱无章的数字,而在大数据挖掘的强大功能面前,就可能变成极具价值的整合型隐私。对隐私主体而言,隐私受伤害就会变得十分普遍。

整合型隐私的产生会导致无感伤害的出现,这是大数据时代隐私伤害的新特点。无感伤害并不是说大数据时代隐私侵权不存在伤害,而是指这种伤害不能被隐私主体及时感知,其伤害具有滞后性,且伤害程度伴随网络的高速传播迅速扩大。对于普遍的生物特征隐私,每个隐私主体都会小心翼翼地认真加以保护,而对于以数据信息为特征的整合型隐私,隐私主体却往往无从保护,留存于网络的涉及公民隐私的数据信息,除了少量是被他人不当上传外,绝大多数是由公民自己上传的(主动或被动),他们并不知道这些数据信息将会在何时何地被何人以何种方式整合成何种信息。如公民的网购信息可以整合成消费能力、消费癖好、身高体重等身体信息、社会关系网络信息等,也就是说,数据挖掘和人工智能的广泛使用,使公民真正成了“透明人”。尤其值得注意的是,对习惯于用隐私信息换取便捷(网购外卖)、优惠(打折)的许多公民而言,他们更难于想象这种潜在伤害会存在。数据构成了人们现实生活中的某种场景,而隐私伤害会以人们无法预计的多种方式发生并快速传播。当隐私主体感知这种伤害时,其范围与后果已经非常严重。

大数据时代,无论是新类型隐私的产生,还是隐私侵权无感伤害的出现,都给既有的公民隐私保护体系提出了挑战。如前所述,我国法律法规已经形成了对公民传统隐私进行保护的一整套体系,也产生了十分积极的作用。但是由于传播技术的快速发展和法律制定后的稳定性要求,对公民新类型隐私的保护相对滞后与无力——尽管立法者也努力对数字化环境积极应对并取得了一定效果,但在技术快速的进步面前常常显得亦步亦趋,所以,寻找更有效的新技术手段和法律相互配合,才有可能走出目前公民隐私保护的窘迫困境。

三、区块链为隐私保护提供新技术可能

(一)技术导致的问题应寻找技术解决之道

每一次传播技术的进步都会对公民权利产生影响,隐私权也不例外。布兰代斯和沃伦于 1890 年发表于《哈佛法学评论》上的《隐私权》一文中,首次提出了隐私权的概念。这项权利之所以在这样的时间节点被提出,与传播技术的进步关系密切。19 世纪末,美国新闻业的革命性发展带给私人空间极大的威胁和压力,“工业化促使大量农民移居城市,激烈的社会变动刺激着这些新移民对周遭事物尤其是上层社会的好奇。这种好奇心,伴随新的印刷技术的应用,推动了美国新闻业的迅速发展”⑧。与印刷技术进步相伴随的,还有这个阶段发明的照相技术及其在传媒业中的应用。作为生活在名门望族中的沃伦本身就深受当时盛行的“钥匙孔新闻”的伤害——他们家庭成员的一言一行不时成为当地媒体闲话专栏中的热门话题,这使沃伦及其家人倍感压力。“新近的发明以及商业手段引起了人们的注意:必需采取进一步的措施保障人格权,保障个人被库利(Cooley)法官所称的‘不受打扰’的权利。立拍即现的照相技术和报刊已经侵入了私人和家庭的神圣领域,不计其数的机器装置使人们可以准确做出预言,‘密室私语在屋顶上被公开宣告’。”⑨这是传统媒体传播技术进步对隐私影响的重要佐证,也触发了两位法律人从权利保护层面来关注这一问题。可以这样说,传播技术和隐私保护两个问题如影相随。所以,技术支撑是隐私保护有效性的重要基础。

网络社会到来之后,新媒体传播技术的发展气象万千、日新月异,而在传统媒体时代曾经行之有效的隐私保护规范,日渐显得捉襟见肘、力有不逮。伴随着大数据挖掘技术的进步和机器学习技术的成熟,传媒业已经进入智媒时代。就如习近平总书记在主持中央政治局第十二次集体学习时强调的那

样,“全媒体不断发展,出现了全程媒体、全息媒体、全员媒体、全效媒体,信息无处不存、无处不及、无人不用,导致舆论生态、媒体格局、传播方式发生深刻变化,新闻舆论工作面临新的挑战”。这种“新挑战”也包含了新的传播技术对公民隐私新的侵害形式。伴随大数据和人工智能传播技术而生的算法新闻和机器人新闻等新闻推送、写作形式的出现,公民隐私面临着由新技术带来的日益严峻的挑战。所以,我们不仅应该通过法律法规的及时修订加以应对,更应寻找可能的技术解决方案。

(二)区块链提供可能的技术解决方案

区块链作为一种新的技术系统,其运行的宏观框架和技术细节尚在不断完善中,所以,它在公民隐私保护的作用方式尚待不断跟进认知,但就其目前已经呈现的本质性特点而言,确实可以给我们思考隐私保护问题提供许多技术想象。

1.对隐私保护进行信任重建

区块链技术强调的是一种多方参与的加密分布式账本,最早是作为一种金融交易的解决方案来设计的,所以,其基因中的核心成分是“信任”。当然,如果信任只是作为一种类道德的要求来规范金融交易者,作为设计者和交易参与者所追求的信任、诚信目标显然会存在风险。所以,它是以去中心化的多方参与来推进的。这就意味着,在区块链中,所有的参与者成为彼此监督的对象,这对于建立有效信任无疑是至关重要的。“为了保障各节点的分类账本记录内容一致,各节点之间需要验证账本和更新账本,以此保证数据不可伪造或篡改,这构成了区块链的共防协议。如此,区块链分布式分类账技术通过去信任而达成信任,实现了‘不信之信’。”⑩“孤岛生存”状态中,讨论现代意义上的任何隐私都是没有意义的。从隐私的角度看,只有隐私主体与他人发生社会交往时,隐私的价值才会体现出来,从这个意义上说,“所有参与者”的“彼此监督”对信任建立和隐私保护就极具价值。

现实生活中,隐私经常是人们展开交往的一种介质,这种需要在一定范围内进行保护的介质在交往中之所以告知他人,其前提是信任,即相信对方会予以保密。遗憾的是,在大数据时代,随着大数据挖掘技术的快速发展和整合型隐私的产生,隐私主体和被告知隐私信息的对象已经无法对相应的隐私信息进行保护。也就是说,对于隐私信息保护的信任在数字化生存环境中无法真正建立起来。区块链通过所有参与者的彼此监督进行信任重建,这对隐私保护无疑是一种革命性的进步。

2.隐私信息自主可控

数字化环境中,隐私面临的最大困境是隐私主体对自己隐私信息的失控,亦即因为人们在生活中的一切言行均被数字化,均可以被可知的和不可知的第二方(如电商企业)、第三方(如数据公司)挖掘,所以隐私保护遭遇严峻挑战。“区块链技术以其分布式的特征,可以作为密码学中可信第三方的实现方案。区块链技术的防篡改特性能够为密码协议提供可信赖的激励机制,提高敌手在博弈中的作恶难度,降低作恶动机。”⑪区块链基于密码学的高加密技术而构建,这就意味着隐私信息更难被挖掘,可以得到更有效的保护。区块链的关键技术组成主要运用密码学中的哈希算法和非对称加密算法,与传统的密码相比较,这两种算法被解密的难度可以说是得到了几何级的提升,这就意味着公民需要保护的隐私信息更难被破解、挖掘。

区块链就其技术架构而言一般分为公有区块链、私有区块链和联盟链三种链。这三种链分别具备不同的功能。我们可以这样概括:公有区块链是开放式的链,其开放读写和去中心化的模式构成了共享共生的技术场景。这个链相当于传统媒体时代的公共空间,人们可以在这个空间自由地分享自己认为可以与他人共享的信息,也可以收集他人分享的信息。私有区块链则是闭合的链,其信息的输入和输出受相应权限的制约。区块链中私钥的设置可以比较好地控制信息的流向,私钥比较容易推导出公钥从而获得需要的信息,而公钥要反向推导出私钥几乎不可能。这就意味着私有链相当于传统媒体时代的私人空间,人们在这个空间分享的信息可以比较有效地控制在隐私主体认可的范围内。联盟链则是一个半开放的链,这个链相当于公共空间和私人空间的交叉地带,或者说是社会学家戈夫曼所称的连接“前台”和“后台”的“局外区域(中区)”⑫,在这里隐私主体需要适度管控自己的隐私信息。也就是说,隐私主体在联盟链内可以适度公开其认为可以公开的隐私信息,这种公开在联盟链范围内的信息尚不会导致其隐私权受到伤害。但基于区块链功能的特殊性,在这个范围内公布的隐私不会如网络世界那样被大规模扩散。这样的一种技术架构可

以令隐私主体较好地控制自己的隐私信息。

3.隐私痕迹不可更改和可追溯

区块链的不可更改和可追溯功能实际是对公民隐私的一种被动保护。区块链本质上是一个分散的数据库,而存储其中的数据就是一个个节点,这些数据借由网络被链接到分散于世界各地的计算机上。由于去中心化的特点,决定了这种数据的存储具有唯一性且是不可更改的,除非同时控制超过 51%的节点,否则单个节点上任何数据库的修改都是无效的。有人借用微信群的聊天记录做类比:区块链就像一个微信群的聊天记录,群中的所有人手中的手机都有聊天内容,单个人对聊天记录内容的修改都是无效的,都可以被他人进行虚假指证。与此同时,区块链还具有与不可更改功能相对应的可追溯功能。由于分散的数据库不受中心化服务器控制,所以其数据的存储都在区块链中存在印记且不可修改,所有数据的发布都可以追溯到最初的发布者,这就可以有效控制(威慑)他人上传隐私信息。

区块链的不可更改功能和可追溯功能可以有效增加区块链尤其是联盟链参加者的自律意识。任何人在作为“中区”的联盟链中公布相关的隐私信息后,一旦被隐私主体以外的其他人使用,都可以被发现,同时也可以被追溯到非法呈现的源头,成为非法泄露隐私信息的证据,这为隐私侵权救济、惩治提供了技术可能性。

四、结语

区块链的出现,给陷于困境和悖论中的公民隐私保护提供了一种技术想象。隐私的内涵随着社会的文明进步以及个人自主意识的不断觉醒而得到了极大的丰富,与此同时,隐私本身也随着传播技术的快速发展而面临诸多挑战,出现严重的“隐私悖论”。看似难于解决的技术导致的隐私保护问题,有可能因为区块链而出现转机。当然,区块链毕竟还没有真正成为成熟的应用场景,而区块链本身具备的不可更改、无法删除等功能特点,也许会产生新的隐私困境,但它的出现毕竟给隐私保护提供了一种新的技术可能性。我们理应本着科技向善的理念,期待隐私有效保护的理想状态。

注释

①[美]南希·K. 拜厄姆:《交往在云端》,董晨宇、唐悦哲译,中国人民大学出版社,2020 年,第 113 页。②陈钟:《从人工智能本质看未来的发展》,《探索与争鸣》2017 年第 10 期。③[美]马克·波斯特:《第二媒介时代》,范静哗译,南京大学出版社,2000 年,第 96 页。④[美]布鲁斯·施奈尔:《数据与监控:信息安全的隐形之战》,李先奇、黎秋玲译,金城出版社,2018 年,第 236 页。⑤于婷婷、杨蕴烙:《精准广告中的隐私关注及其影响因素研究》,《新闻大学》2019 年第 9 期。⑥喻国明、陈雪娇、卢文婕等:《边缘计算、5G 与传播的未来融合——试论场景视阈下新闻传播过程的重新构建》,《传媒观察》2019 年第 10 期。⑦[法]马尔克·杜甘、[法]克里斯托夫·拉贝:《赤裸裸的人:大数据,隐私和窥视》,杜燕译,上海科学技术出版社,2017 年,第 37 页。⑧冷霞:《隐私权的诞生》,《中国社会科学报》2010 年 3 月 30 日。⑨[美]路易斯·D. 布兰代斯:《隐私权》,宦胜奎译,北京大学出版社,2014 年,第 5 页。⑩陈吉栋:《播撒信任的技术幽灵——区块链法律研究述评》,《探索与争鸣》2019 年第 12 期。⑪刘明达等:《区块链在数据安全领域的研究进展》,《计算机学报》2020 年第 1 期。⑫[美]欧文·戈夫曼:《日常生活中的自我呈现》,黄爱华、冯钢译,北京大学出版社,2008 年,第 113—114 页。

责任编辑:沐　紫

Blockchain and the Technological Imagination of Citizen Privacy Protection

Gu Liping

Abstract: In traditional Chinese culture, privacy as a personality right has been underestimated for a long time. Later, with the rapid development of modernization under the rule of law and the continuous enhancement of citizens′ privacy awareness, China has improved the legal system of citizen privacy protection in a relatively short time. Nowadays, in the context of the big data era and the widespread application of AI technology, citizens′ privacy rights are facing severe challenges brought by the progress of communication technology, and it is difficult to get the timely protection from privacy law which is comparatively lagged behind. Therefore, the technological features of decentralization, strong encryption and traceability in blockchain, provide a possible technological imagination for the protection of citizens′ privacy.

Key words: privacy; right of privacy; blockchain