

论元宇宙数据安全风险的法律对策

唐欣奥^{*}

摘要:当前元宇宙技术蓬勃发展,为数据安全带来了新的挑战。元宇宙数据收集记录与当前数据收集记录相比,其范围突破了有限性,扩展到了用户自身及其行为习惯的各个方面,具有全方位性,因此具有更大的数据安全风险,亟待研究者以前瞻性眼光进行预测和防范。本文在探讨元宇宙数据、元宇宙数据安全概念的基础上,以元宇宙用户、元宇宙平台、国家三类主体为基础,探讨了不同层面的元宇宙数据安全风险,分析元宇宙去中心化管理办法在数据安全风险预防和应对上的不足与弊端,提出应以多元共治作为基本原则预防和应对元宇宙数据安全风险;分析我国当前元宇宙数据安全相关制度状况与缺陷,提出我国在多元共治原则下预防和应对元宇宙数据安全风险的具体建议。

关键词:元宇宙 数据安全风险 法律对策 多元共治

元宇宙得以产生和运转的枢纽之一就是海量的数据。数据不仅蕴含着丰富的商业价值,亦作为国家的基础性战略资源,与国家安全及利益息息相关(周若涵,2021)。大数据技术是元宇宙的技术基础之一,元宇宙的发展将推动大数据行业的更新和发展,但也会给数据安全带来新的风险和挑战。元宇宙的兴起,将不同程度地引发有关数据安全以及隐私保护的困境(高一乘、杨东,2022);并且在一定程度上,这一概念的火热与流行确实为进入信息化新阶段的全球各主要国家提出了如何通过构建生态化治理体系的方式,有效保障国家数据安全免受新型威胁的现实问题(沈逸,2022)。自2021年脸书(Facebook)母公司改名为Meta以来,“元宇宙”的概念在全球掀起了新的浪潮,各国纷纷制定元宇宙发展战略,力图在这一高新科技领域占得先机。

截至2022年9月,我国已有北京、上海、广州等30余个省市颁布了元宇宙相关支持性政策,其中11个省市出了19份元宇宙专项政策,力图突破关键技

^{*} 唐欣奥,北京林业大学人文社会科学学院。

术、扩大产业规模、构建产业生态,在全球范围内夺得先机。我国在大力发展元宇宙技术、产业的同时,也不能忽视其带来的数据安全风险,这需要研究者以前瞻性的眼光对元宇宙数据安全风险进行预测和防范。

一、元宇宙数据安全内涵

(一)何为“元宇宙”

一般认为,元宇宙概念最早出现于尼尔·斯蒂芬森(Neal Stephenson)1992年出版的小说《雪崩》之中,该书描述了一个由电脑和网络构成的虚拟空间。在之后的几十年里,人们从未停止对这样一个虚拟空间的想象。目前,Meta、微软、苹果等多家互联网巨头都相继布局元宇宙战略;2022年6月,Meta、微软、Epic、英伟达、高通、索尼、华为等36家公司组建了一个名为“元宇宙标准论坛”(Metaverse Standards Forum)的组织,拟为元宇宙、AR/VR等建立行业标准。

元宇宙大致是生活在现实物理世界的自然人以“化身”或者“数字人”的方式,通过计算机操作系统,与其他数字人即时互动的3D数字虚拟空间(程金华,2022)。作为热门概念的“元宇宙”目前尚未有一个获得普遍共识的定义,但根据当下的讨论与研究可知,各观点和学说都认为其有虚拟性和沉浸式的特点。在与元宇宙数据相关的方面,它还具有一定的独立性、封闭性,并由此具有会导致数据出现安全问题的隐蔽性。

(二)元宇宙数据

1. “元宇宙数据”定义

在元宇宙这样的虚拟世界中,一切都以数字化的形式存在,我们的每一个行为都可以被记录,成为元宇宙数据的一部分。未来的元宇宙数据并不会脱离当下人类对于数据的认识,只是在记录、储存形式等技术层面,伴随着技术的进步可能会有所更新和改变。我们可以通过当前对于数据的认识,总结出“元宇宙数据”的初步定义。

各国各地区的法律对数据的定义不尽相同。欧盟《数据治理法》(Data Governance Act)将数据定义为:“行为、事实或信息的任何数字表示以及此类行

为、事实或信息的任何汇编,包括声音、视觉或视听记录形式。”美国《政府数据开放法》(*Open Government Data Act*)将数据定义为:“被记录的信息,不论记录数据的形式或媒介。”我国《数据安全法》第三条规定,数据“是指任何以电子或者其他方式对信息的记录”。根据以上对数据的定义,可以尝试对元宇宙数据做出如下定义:元宇宙数据是指任何以电子或者其他方式对元宇宙世界中行为、事实或信息的记录,包括声音、视觉或听觉记录等生物识别信息和非生物识别信息。

2. 元宇宙数据主体

当前,数据主体主要有三类:其一是个人,个人信息及行为的记录产生零散的原始数据;其二是数据利用者,他们收集和整合海量零散的个人数据产生大数据,并对此继续开发利用,包括企业和国家相关部门;其三是国家,国家一方面为本国数据收集处理活动制定规则,另一方面在国际社会中保护本国大数据及其技术,维护国家安全。

可以预见,元宇宙数据涉及的主体主要也有三类。一是元宇宙用户,他们在元宇宙中进行社交、游戏、虚拟产品交易等活动,其生物信息和行为信息的直接记录构成了元宇宙用户数据,也是元宇宙的原始数据。二是元宇宙平台,平台为用户提供元宇宙服务,包括提供可供接入的元宇宙本身以及元宇宙内部的购物、游戏、学习等多类型服务,同时在提供元宇宙服务的过程中收集产生的数据。一方面,平台需要对用户数据进行分析以优化服务,吸引更多用户;另一方面,平台也可能直接将加工后的数据作为商品出售给别的元宇宙或是相关机构,以获得利益。平台是元宇宙衍生数据的主要创造者。三是国家,我国《数据安全法》第七条规定:“国家保护个人、组织与数据有关的权益,鼓励数据依法合理有效利用,保障数据依法有序自由流动,促进以数据为关键要素的数字经济发展。”在元宇宙视角下,国家自然也不会缺席元宇宙数据的管理。三种主体中,国家并不单独创造数据,即使创造数据也是以前两类主体的身份进行,“元宇宙国家数据”主要针对元宇宙数据中的个人信息、重要数据和核心数据等关乎国家安全的部分。

(三) 元宇宙数据安全风险

不论是元宇宙原始数据,还是元宇宙衍生数据,都可能受到数据安全风险的

威胁,例如原始数据的泄露可能侵犯用户隐私,衍生数据的泄露可能侵犯平台权益,等等。本文将对元宇宙数据整体的数据安全风险及应对措施进行讨论,而不再具体区分两类数据。

1. 元宇宙数据安全

基于元宇宙数据的定义,可以用类推的方法对元宇宙数据安全做出初步定义。国际化标准组织(ISO)对数据安全的定义是:“保护数据以保证可用性、机密性及数据完整性。”以科学数据为研究对象,李善青等学者将“科学数据安全”定义为通过必要的技术和管理措施,保护科学数据在其全生命周期中免受破坏性外力和非授权操作的侵害,保持科学数据的机密性、完整性和可用性(李善青、郑彦宁、邢晓昭等,2019)。《数据安全法》第三条规定:“数据安全,是指通过采取必要措施,确保数据处于有效保护和合法利用的状态,以及具备保障持续安全状态的能力。”综合以上定义,可以对“元宇宙数据安全”做如下定义:元宇宙数据安全是指通过采取必要措施,确保元宇宙数据在其全生命周期中,包括收集、利用、存储、传输等,始终处于有效保护和合法利用的状态,以及具备保障持续安全状态的能力。

2. 元宇宙数据安全风险

(1) 元宇宙数据安全风险的体现

根据工业和信息化部发布的《工业和信息化领域数据安全风险信息报送与共享工作指引(试行)(征求意见稿)》(以下简称《工作指引》),数据安全风险是指通过监测、评估、信息搜集、授权监测等手段获取的数据安全风险。根据实践经验,《工作指引》总结概括了六大类数据安全风险,分别是数据泄露、数据篡改、数据滥用、违规传输、非法访问、流量异常;但同时也认为数据安全风险包括但不限于上述类别,留下了增补的空间。实践中也还存在其他数据安全风险,如数据霸权、网络攻击等。

上述数据安全风险是长期以来从技术发展和实践经验中总结而来的,未来也可能会继续出现新的安全风险。就元宇宙而言,当前元宇宙技术尚在发展阶段,元宇宙数据安全风险并不会立刻显现出和当前数据安全风险完全相同的面貌,而将根据其技术发展和数据收集利用情况,在不同发展阶段呈现不同数据安全风险。对元宇宙数据安全风险的预防,应优先应对已经出现或很快就会出现的最紧迫部分。根据当前元宇宙数据安全案例,以及元宇宙技术发展带来的数

据收集利用情况,元宇宙数据安全风险将首先体现为元宇宙数据滥用、元宇宙数据泄露、元宇宙数据不当流通以及元宇宙数据垄断。

(2) 元宇宙数据安全风险的特点

元宇宙数据安全风险具有一般性和特殊性:一般性是说,元宇宙数据作为一种特殊的数据,它所产生的数据安全隐患和当下的数据安全隐患将会有交叉;特殊性是说,元宇宙本身具有独立性与封闭性,这样的独立性与封闭性导致外界难以全面地了解元宇宙内部的活动细节,同时也因为其中所有的活动都以数字化的形式被记录,数据安全隐患隐藏在庞大的数据海洋中,难以被察觉,所以元宇宙数据安全风险将更隐蔽。此外,由于元宇宙数据在采集范围、采集方式以及数据内容等方面的特殊性,其数据安全隐患的后果将更加严重,影响范围更广,弥补难度更大。

(3) 元宇宙数据安全风险分类应对

根据参与数据流动的主体和行为,数据安全风险将会在不同层面以不同的方式表现出来,引发不同的后果。例如 2022 年 2 月,Meta 公司因涉嫌非法采集用户面部信息被美国得克萨斯州总检察长起诉,指责其未经同意收集了数千万州民的面部识别数据,并将该部分数据披露给了第三方,涉案金额达数十亿美元。该案表明,即使虚拟世界的元宇宙还在发展成熟阶段,但是其技术发展过程中产生的数据收集处理活动就足以带来严重的隐私数据安全风险,造成严重后果,并且已经在个人、企业层面显现出来。对于元宇宙数据安全风险的分析和应对,应当和其技术的发展同步跟进,甚至需要前瞻性的预防;并且,应从元宇宙用户、元宇宙平台、国家三类主体的角度切入,对元宇宙数据安全风险展开多层次的应对。

二、元宇宙数据安全风险可能性分析: 基于三类数据主体

结合当前数据安全风险治理局势,以及对未来元宇宙数据所涉相关主体的预测,各个主体在元宇宙数据产生利用的过程中,扮演不尽相同的角色,拥有不尽相同的重要性。从规避元宇宙数据安全风险的角度看,应从主体入手,对元宇宙数据安全风险在元宇宙用户、元宇宙平台以及国家三类主体上的具体表现及

相应的应对措施进行可能性分析,以期提供有益意见。

(一)元宇宙用户的数据安全风险

数据驱动型经济是目前创新的蓝海,该模式需要对收集的海量数据进行开发利用,平台企业的业务如商业推广、精准营销等大都依赖于此(沈逸,2022)。可以预见到,在未来元宇宙经济环境下,收集、存储、利用用户数据仍将成为元宇宙平台经营发展的重要模式,而相比当下不同服务内容相互基本独立的点状互联网服务提供模式,作为沉浸式虚拟世界的元宇宙中的用户数据安全问题将更加严峻。元宇宙的技术原理和运行方式决定了即使在最小必要原则的约束下,它也必然会广泛地获取用户授权,全方位、实时地收集每一个用户信息(王德夫,2021)。这样的用户数据将不再局限于购物、社交等单一类型,而呈现出全方位记录的特点。换言之,元宇宙中的个人数据将是用户在一个虚拟世界中的全部痕迹,这是元宇宙用户数据与当下互联网用户数据的最大区别也是最主要区别,这样的全方位数据收集记录将为个人数据保护带来新的问题。具体而言,元宇宙用户个人数据安全问题将主要体现为元宇宙用户数据滥用、用户数据泄露和用户数据不当流通三个方面。

1. 元宇宙用户数据滥用

在元宇宙用户数据滥用方面,元宇宙平台过度收集或超范围、超用途、超时间地利用用户数据,将侵犯用户隐私。前文提到,收集、存储、利用用户数据仍将是元宇宙平台经营发展的重要模式,但是在元宇宙这样的环境下,即使平台是在最小范围内收集用户数据也依然会得到全方位的数据记录结果。算法帮助平台企业实现了深度挖掘个人信息,对于这样的全方位数据进行分析处理将得到比单一类型数据分析处理更加深入、更加立体的结果,这一过程极有可能突破用户个人隐私权边界。

2. 元宇宙用户数据泄露

在元宇宙用户数据泄露方面,元宇宙用户数据被恶意获取、转移或泄露至不安全环境,这将带来更大的安全风险。元宇宙中的用户数据呈现出全方位记录的特点,一旦出现数据泄露事件,就将是全方位的信息外泄。与金融信息泄露、用户注册信息泄露或者医疗信息泄露等单一类型数据泄露相比,元宇宙用户数据泄露负面影响的范围和程度将空前扩大(王德夫,2021)。这也对元宇宙环境

下的用户个人数据保障提出了更高的挑战。

3. 元宇宙用户数据不当流通

在元宇宙用户数据不当流通方面,用户个人数据具有人身性和财产性双重特点。信息控制者不但可以利用技术手段深入挖掘个人信息中潜藏的商业价值,使其服务于企业的经营、管理和决策,还可以将其直接打包出售以实现数据中的财产价值(王玉林,2016)。随着数据经济的发展,当下企业间的大数据交易流通已不是新鲜事。而在元宇宙环境下,如何界定可流通的大数据与用户个人数据的边界,如何防范元宇宙数据未按照有关规定就被擅自传输,如何防范尚未经过足够的脱敏加工以实现匿名化的用户个人数据“被流通”,甚至这样的全方位数据即使是脱敏加工后,是否依然存在被其他平台利用技术手段去匿名化,也将是值得关注的问题。

(二) 元宇宙平台的数据安全风险

经营者对可商品化数据使用价值的挖掘,是数据财产属性在大数据时代得以充分体现的关键,经营者据此应当对其所持有的可商品化数据享有财产利益(谢宜璋,2021)。平台除了将自己的元宇宙用户数据进行内部分析利用之外,还有可能对其进行分类、加工、脱敏以后放到数据交易市场进行交易,以实现财产价值。根据互联网企业的数据流动现状,这样的数据流通现象在未来元宇宙平台之间几乎必然存在,甚至未来的元宇宙平台很有可能就诞生于当下活跃在数据交易市场中的大型互联网企业里。但是,当下互联网平台大多只记录用户的单一类型数据,就已经引发了众多法律纠纷,诸如“上海汉涛信息咨询有限公司诉北京百度网讯科技有限公司等不正当竞争纠纷案”^①和“深圳谷米公司诉武汉元光公司不正当竞争纠纷案”^②等。因此,有必要对未来平台层面的元宇宙数据安全问题进行有前瞻性的探索与预防。把涉及用户个人隐私的部分归入用户数据安全问题,平台上的数据可能存在元宇宙平台数据不当流通以及数据垄断问题。

1. 元宇宙平台数据不当流通

当下互联网平台间的数据流通,主要有基于合同的大数据交易以及通过爬

① 上海知识产权法院(2016)沪73民终242号民事判决书。

② 广东省深圳市中级人民法院(2017)粤03民初822号民事判决书。

虫技术爬取他方平台数据两种方式。元宇宙本质上仍然是一种互联网服务,所以当下的两种数据流动模式仍将是未来元宇宙平台间数据流通的主要模式。大数据交易需要双方达成合意,对元宇宙平台数据利益的侵害可以得到经营者的有效防范,其中主要包含的是对元宇宙用户数据权利的侵犯,故此处主要讨论后者。

通过爬虫技术抽取他方平台数据,本质上是在未达成合意的情况下收集了大量的他方平台的数据,以形成新的具有商业价值的大数据集合,侵犯了他方平台的商业利益,引起了不正当竞争纠纷和平台数据泄露问题。这样的数据泄露问题在未来的元宇宙平台之间将依然存在。在未来的元宇宙环境下,元宇宙平台将记录的是用户行为各方面的全方位数据,平台收集数据的成本更高、内容更广,这可能导致非合意数据爬取行为更加严重。爬取方可能盯准被爬取方的某一类数据,也可能对其数据整体进行非法的收集爬取,对被爬取方的权益侵犯显然值得重视。

2. 元宇宙平台数据垄断

数据垄断即持有并控制海量数据的少数公司,通过占有大数据形成市场支配地位,滥用其市场支配地位以及利用数据实施不正当竞争行为(张菲、朱桐雨,2022)。元宇宙平台数据垄断问题是指大型元宇宙平台利用其在市场中的优势地位,不当排除其他平台对公域数据的收集利用,阻碍其他元宇宙平台的发展,形成自己在市场中的数据垄断地位。就此而言,元宇宙平台有范围地公布部分数据,合理的非合意的数据爬取行为也能为元宇宙数据流通、市场进步做出贡献。就此而言,如何妥当划定数据爬取正当性边界,不但关乎各方利益,更关乎网络空间数据流通的大局(许可,2021)。

(三) 元宇宙中的国家数据安全风险

从国家层面来说,元宇宙数据安全同样是不可忽视的问题。《数据安全法》第四条规定:“维护数据安全,应当坚持总体国家安全观,建立健全数据安全治理体系,提高数据安全保障能力。”这表明我国要建立健全数据安全治理体系,元宇宙数据安全的防范与治理自然应当包含于其中。具体而言,根据当前国家数据安全面临的风险,可以推测在未来元宇宙语境下,国家数据安全主要有元宇宙数据跨境流通中的泄露或不当流通风险。

数据跨境流通意指在一国内生成的电子化信息记录,被他国境内的私主体或公权力机关读取、存储、使用或加工,合称“处理”(何傲翹,2021)。在当前经济全球化和数字经济快速发展的局势下,数据跨境流通不仅是数字经济发展中面临的重要问题,也是开展数字贸易的基本前提(何波,2022)。元宇宙数据不同于一般大数据的信息全方位性,这意味着其跨境流通将带来更大的个人数据安全风险和国家数据主权风险,一旦发生泄露或者被不当流通,将对国家安全造成更大的危机。

三、当前我国元宇宙数据安全保护制度及缺陷

(一)我国元宇宙数据安全制度现状

当前,我国正在不断完善数据安全相关制度和规则,不断推动数据安全协同治理机制的形成(马忠法、胡玲,2021)。虽然还未针对元宇宙及元宇宙数据进行专门立法,而多是针对广义数据安全进行立法保护,但也有部分政策提到元宇宙。现主要有以三部法律、多个中央和地方政策为主的元宇宙数据安全保护格局,并形成以数据分类分级保护、数据安全风险评估和监测预警、数据安全应急处置为核心的数据安全制度及以告知同意为核心原则的个人信息保护制度。

1. 元宇宙数据安全相关法律

三部法律分别是《网络安全法》《数据安全法》《个人信息保护法》。其中,《网络安全法》提出了网络安全等级保护制度,并规定关键信息基础设施的运营者掌握的个人信息和重要数据应在境内保存,确需出境的需进行安全评估。《数据安全法》第九条提出数据安全协同治理体系,在第三章“数据安全制度”中规定了数据分类分级保护制度、数据安全风险评估和监测预警、数据安全应急处理机制,在第四章“数据安全保护义务”中规定了重要数据处理者的数据处理活动风险评估义务。《个人信息保护法》在敏感个人信息处理、国家机关处理个人信息、个人信息跨境提供、个人的权利、个人信息处理者的义务等方面构建了以告知同意为核心原则的个人信息保护制度框架,并在第七章规定了法律责任。另外,《民法典》也在第一千零三十四条规定了个人信息保护范围。目前尚未针对元宇宙进行专门立法,元宇宙数据安全相关问题应当参照并适用以上法律。

2. 元宇宙数据安全的中央及地方相关政策

中央政策是指国务院印发的《“十四五”市场监管现代化规划》中提出的,要“加快研究和完善国家数据安全标准与认证认可体系”。《要素市场化配置综合改革试点总体方案》进一步提出,要“加强数据安全保护”“推动完善数据分级分类安全保护制度”。二者虽然都未明确提及元宇宙,但是元宇宙数据安全作为国家总体数据安全下的重要部分,应当参照适用。

多个地方政策是指北京、上海、广州等地针对元宇宙发展制订的行动计划。多地把保障元宇宙数据安全作为工作要求之一,例如:《北京城市副中心元宇宙创新发展行动计划(2022—2024年)》明确提出,“提升覆盖云、网、端的数据安全服务与保障能力”;《上海市培育“元宇宙”新赛道行动方案(2022—2025年)》要求,“加强未来网络、云边计算、智能交互终端及数字基础设施的内生安全,保障海量数据的存储、传输和使用”;《厦门市元宇宙产业发展三年行动计划(2022—2024年)》规定,“提升元宇宙数据治理能力,加强数据安全管理和隐私保护”;《河南省元宇宙产业发展行动计划(2022—2025年)》也提出,要“深入研判元宇宙发展的伦理风险、数据安全风险、沉迷风险、知识产权风险等”。

(二) 元宇宙数据安全风险应对的现行制度之缺陷

首先,尚未出现针对元宇宙的法律法规。虽然《数据安全法》第九条规定了数据安全协同治理体系,但只是对保护主体做了明确说明,后文中也只是使用了“处理者”这样的词汇,并未真正建立起多元主体的数据安全保护制度。各省市的元宇宙行动计划中虽然有提到数据安全,但仅仅停留在原则层面,缺少具体的细化实施办法和规定。元宇宙数据安全保护制度应建立在一般数据安全保护制度之上,并具有针对元宇宙特点的专门规定,在目前这种缺少具体细化规定的情况下,仅凭原则性规定想要建立多元共治的元宇宙数据安全保护制度更是难上加难,不利于应对元宇宙数据安全风险。

其次,数据分级分类体系尚不完善。虽然我国确立了数据分级分类保护制度,确立了不同层级、不同领域的重要数据目录制定主体,并且全国信息安全标准化技术委员会发布的国家标准《信息安全技术 网络数据分类分级要求》(征求意见稿)已规定了较为详细的数据分级参考规则,但当下对核心数据、重要数据的识别脉络仍不够清晰,在行业数据分类以及重要数据目录制定方面仍在初

步阶段,数据管理制度和要求也缺乏细化规定,这些无疑都会影响元宇宙数据的分级分类保护、元宇宙数据管理和风险应对。

四、元宇宙数据安全风险的法律回应： 从去中心化到多元共治

(一)元宇宙的去中心化管理

1. 去中心化管理概念及现状

在元宇宙蓬勃发展的当下,有一部分声音认为元宇宙应该建立一个去中心化的成员自组织管理模式。去中心化(decentralization)在元宇宙语境下,即让每位元宇宙成员都能拥有该元宇宙的管理权,能参与到元宇宙的运营、管理和决策中,而不需要一个组织或特定的部分人集中对元宇宙进行管理。区块链技术也为这样的愿景提供了技术基础。区块链技术自问世以来,因其去中心化的分布式记账特征,被比喻为一种“信任机器”(程金华,2022)。当前已经存在这样的去中心化自治组织,例如成立于2016年11月的Aragon DAO,以及2020年8月上线的国内第一个基于区块链技术的自组织管理平台VoneD-AO(刘涛、袁毅,2022)。去中心化的观点主要从法律和理想两方面展开。元宇宙中行为的法律边界和效力处于待定状态,政府的干预又处于上位法真空状态,因此需要元宇宙成员自行达成定纷止争的治理规则并自立执行,以应对成员身份和行为发生的深刻变化(张钦昱,2022)。依靠区块链技术创造去信任、公开透明的网络环境,随着人工智能的应用,每个个体都将是具备感知、推理、决策功能的智能代理,参与组织的运营、管理和决策,真正发挥出群体智能的力量(刘涛、袁毅,2022)。

2. 去中心化管理的弊端

(1)元宇宙无法真正实现去中心化

元宇宙具备高度中心化的架构,并体现在相关系统搭建与运行、数据收集与处理、数字权益创设与处分等每一个“宇宙角落”(王德夫,2021)。元宇宙的产生和运营一定需要平台提供技术和资金支持,并且单个用户并不会只停留在一个元宇宙,也很难有精力参与到各个元宇宙的治理中去。从保证自身市场竞争力和保护用户隐私的角度来讲,有能力收集用户数据的也只有在技术上处于优

势地位的平台,用户一方面不能获取他人的数据或者只能获取公开的部分,另一方面在个人数据权利层面也未必能与平台处于对等地位。

(2) 过大的自治权和空间不利于保护元宇宙数据安全

元宇宙去中心化的管理方式赋予每一个元宇宙使用个体极大的主体自由,如果在数据安全风险治理问题上给予元宇宙过大的自治权和空间,将加大数据安全风险,有违我国建立健全数据安全治理体系的目标。关乎个人隐私和国家安全,不能放任元宇宙野蛮发展。虽然在元宇宙其他管理层面来说存在去中心化治理的实施空间,但是在元宇宙数据安全风险治理层面来说,我们应给予更多的关注,需要公权力的约束,由平台、用户与公权力主体共同参与,以多元共治的机制进行元宇宙数据安全风险的治理、防范和应对。

(二) 元宇宙数据安全风险回应的理想路径:多元共治

在传统意义上,多元共治是指以政府、市场与社会为主体,以法治、协商和自治为系统,以对话、竞争、妥协、合作和集体行动为机制的多元主体共同治理的社会共治模式。该治理模式是改革开放时期在制度转型、资源污染、资源约束等问题下我国实践探索的经验总结。其路径是政府职能转变和简政放权,将减少对微观经济事务的干预落到实处,采取更合理的方式消弭市场经济运行带来的各种负面影响(王名、蔡志鸿、王春婷,2014)。

1. 国家:把握底线、监督引导

在元宇宙数据安全风险应对的多元共治中,国家应主要承担把握底线、监督引导的作用。建立健全数据安全治理体系是保障数据安全的重要措施之一,元宇宙数据安全将是其中的重要部分,国家不应缺席其管理。并且,由于法律无法避免的滞后性,国家立法很难跟上技术快速进步的步伐。未来元宇宙的发展显然不会千篇一律,统一的元宇宙数据管理制度难以适配不同特点和类型的元宇宙产品,也难说适合具有全方位性的元宇宙数据。所以,相比于把元宇宙数据管理制度的细枝末节都收揽于国家手中,通过制定元宇宙数据分级分类保护的行业标准、拟定基本规范、确立应急情况的程序和责任承担等方式确立较为宽泛的元宇宙数据利用制度框架,重在把握元宇宙数据安全的底线和红线,把更细节的管理权放给直接支配和管理元宇宙的平台应是更好的选择。这样既可以减轻国家立法和执法压力,节约行政资源和司法资源,还可以通过审查平台制定的细化

的元宇宙数据管理规定,监督和引导企业建立符合基本规定的元宇宙数据管理制度,处理元宇宙用户与平台间的数据纠纷,实现对元宇宙数据安全的前端预防和应对。

2. 元宇宙平台:有限自治、接受监督

元宇宙平台应享有有限的自治权,接受国家和社会的监督。元宇宙平台直接控制、运营和管理自己的元宇宙产品,进行元宇宙数据的收集、处理活动,直接接触也最先接触到海量的元宇宙数据,是防范、发现和应对元宇宙数据安全风险的最前线。但因元宇宙平台本身的逐利性,不能将制定元宇宙数据分级分类保护标准等原则性和底线性规定的权力交予平台,而只能赋予其在底线框架之内进一步根据自己的元宇宙产品和元宇宙数据的特点,建立相应的有特色的元宇宙数据管理制度、元宇宙数据安全风险预防和应对机制的权力。换言之,在国家的监督和引导之下享有有限的自治空间,发挥其灵活性和前瞻性,适应迅速发展的技术和多变的现实情况。通过元宇宙数据风险预防、应对机制,以汇报情况、接受监督和引导、共同应对突发事件等方式和国家形成有机互动,形成权力互赖的伙伴关系,一方面能保障平台自身的利益不受非法侵害,另一方面也能共同达成建立健全元宇宙数据安全治理体系的目标。

3. 元宇宙用户:积极维权、反馈、举报

元宇宙用户作为国家和平台之间直接对接之外的另一条纽带,同样在预防和应对元宇宙数据安全风险中起到重要作用。由于个体力量较小、缺少技术能力、精力和经济有限等,元宇宙用户是相对于平台的弱势方,其数据权利容易受到平台的侵害。作为用户相对方的平台显然也难以保证公平公正,所以需要国家一定程度的介入。虽然用户之间通常难以形成合力,但其往往具有一定的规模性,单个用户的数据权利纠纷背后很可能隐藏着规模性侵犯用户元宇宙数据权利的行为,引发用户层面的元宇宙数据安全风险。这样的纠纷可以首先体现为少量用户数据的泄露、被滥用和被非法买卖传输等,而当少数用户发现自己的元宇宙数据权利受到侵害时,往往这一侵害行为已经波及更大范围的用户。用户层面的元宇宙数据安全风险可能进一步体现为平台甚至跨国的数据不当流通等,在这个意义上,通过国家主动关注元宇宙用户数据权利保护情况,再加上用户及时反馈和举报,有关部门能够及时发现潜在的元宇宙数据安全风险并加以控制。当然,除了可能引发更大规模的元宇宙数据安全事故,即使是不具备规模

性的个别用户的数据权利,也应当受到国家和平台的尊重与保护,这不仅仅是建立健全数据安全治理体系目标的要求,更是建设社会主义和谐社会的要求。

如此,以多元共治为基本原则,构建国家、元宇宙平台、元宇宙用户三方主体共同参与的立体多元主体共治制度,才能在各个层面有效防范和应对元宇宙数据安全风险。

五、元宇宙数据安全的制度建构

元宇宙数据安全风险回应需要以多元共治为基本原则,下文将从元宇宙用户、元宇宙平台、国家三主体的角度,论述各个主体应采取何种措施应对元宇宙数据安全问题。

(一)我国应尽快构建元宇宙制度

如前文所述,当前我国并未针对元宇宙进行专门立法,而各地的行动计划大部分也是论述如何鼓励发展元宇宙产业、元宇宙技术,对于元宇宙数据安全只在原则和目标部分略有提及。当前元宇宙数据安全还只能参照现有的数据相关法律适用,但元宇宙数据和传统数据的主要差异,以及元宇宙数据的全方位性,表明其数据安全风险的危害程度更在传统大数据的数据安全风险之上,只参照现有的数据制度显然不利于切实保护元宇宙数据安全风险。我国在重视推动发展元宇宙技术和产业的同时,也应重视在技术发展过程中以及技术发展成熟后所产生的数据安全风险,应尽快建立元宇宙基本制度、元宇宙数据安全风险应对制度,跟进技术发展的步伐,既要技术和产业发展,也要守住数据安全的红线。

(二)基于不同主体的元宇宙数据安全风险应对

1. 元宇宙用户应提升权利意识,遵守平台规范

就个人层面来说,个人用户在元宇宙中相较于平台处于技术上的弱势地位,个人的精力和所能发挥的作用也有限。元宇宙数据作为一种大数据,其一大特点就是来源海量性,所以不能苛求个人与平台抗衡以保障自身的权利。但是也不应完全剥夺个人保障自己数据权益的权利,而应当赋予用户在元宇宙视角下的元宇宙个人数据权,并通过普法教育、元宇宙进入页面告示等方式提高用户对

于自身数据权利的保障意识,并能积极主动保护自身合法的元宇宙数据权利。同时,要以公权力保障用户权利的实施,一旦用户难以以自身力量在与平台的纠纷中保障自身权益,公权力就可作为救济措施介入。当然,用户自身因为成本过高或其他原因而难以争取自身权益的时候,也应为用户提供向公权力求助的通道,甚至公权力也可主动介入保护用户个人的元宇宙数据权利,防范和应对元宇宙用户数据被平台滥采滥用、数据泄露和数据在未达到流通条件时被不当流通的风险。

用户在数据安全可能受到威胁的同时,也有可能反过来威胁元宇宙数据安全。例如现实中一些人以跟踪、人肉搜索等方式侵犯他人隐私,或是为境外势力拍摄机密设施、机密地区照片泄露国家机密等。为了预防该类事件在元宇宙中发生,一方面,需要平台充分提示用户在元宇宙中的权利义务,需要普法教育让用户了解元宇宙行为规范,让用户了解元宇宙不是法外之地,虚拟世界中同样有行为红线;另一方面,需要用户自觉遵守元宇宙行为规范,遵守行业规范,在接受公权力保护的同时也应当承担不去危害元宇宙数据安全的责任。

2. 元宇宙平台建立健全元宇宙数据安全管理制度,强化法律责任

元宇宙平台应建立健全元宇宙数据安全管理制度,承担元宇宙数据保护义务:一方面,平台在运营和发展过程中不可避免地会对用户数据进行采集和存储,所以在这个过程中平台自然应当承担对所采集的数据妥善保管保护的义务,以防止元宇宙数据泄露;另一方面,根据当前对大数据财产权的讨论和现实中对大数据的利用情况可以推知,平台对于所采集的原始数据进行适当的加工、脱敏以后形成的衍生数据,同样可以拥有财产权,可以进行流通以实现部分商业目的。不同于传统大数据财产权,元宇宙数据是用户在元宇宙中各类不同类型行为的集合,具有全方位性,所以在处理和流通阶段平台应当承担相较于传统大数据处理和流通过程中更大的数据保护义务。具体而言,平台对于元宇宙数据的脱敏程度应当更高,在流通过程中需要积极配合有关部门对处理后的元宇宙数据进行评估,以确保其满足市场流通标准,防止其被技术复原而恢复身份识别性,防止泄露用户个人隐私。此外,平台还应建立数据安全动态风险评估监测和突发情况应急制度,在元宇宙数据处理的全过程中有效防范风险,在发生元宇宙数据安全事故时有效组织力量减小损害、降低损失,及时向有关部门通报,有效应对紧急情况。平台还应明确元宇宙数据安全风险责任承担制度,明确责任分

配与责任承担,避免追责难的问题,督促相关责任人员做好数据安全防护工作。

平台应保障用户的元宇宙数据权利。个人信息分为一般个人信息与敏感个人信息(时明涛,2020),相应地,元宇宙数据也可以分为一般元宇宙数据和敏感元宇宙数据。元宇宙平台应充分保障元宇宙用户的数据权利,保障用户的知情同意权,即平台收集、存储、利用元宇宙数据等应让用户知晓并在取得用户同意以后进行,用户在元宇宙活动中产生的敏感个人数据更应如此。当用户希望在别的元宇宙世界中继续使用前一个元宇宙中的数据时,平台应当积极予以配合和协助,同时对于用户可以带走的数据范围进行协商。欧盟《通用数据保护条例》第20条创设了数据可携权这一新兴权利(汪庆华,2021),这一权利在未来元宇宙世界中或也有适用空间。不过,只要求单个企业自律或还有不足之处,笔者认为也有必要建立相应的行业规范和行业组织予以配套,督促元宇宙平台企业自觉自律承担责任、履行义务。

3. 国家建立元宇宙数据安全保障制度

用户和平台对于元宇宙数据安全风险的应对固然发挥着重要作用,但是就动力而言,更多需要的是用户和平台的自我驱动;缺少强制力的保障,对元宇宙数据安全的维护就难说完善。用户和平台更多是事前的防范,而难以在数据安全事故发生以后进行有效的止损和弥补,在追究责任方面更是捉襟见肘。元宇宙数据中必然包含诸如元宇宙系统数据、商业秘密数据、本国公民用户的个人信息及行为数据等关乎国家安全的保密数据,这就需要我国公权力的介入,建立更完善的制度并以强制力保障制度运行,同时能在数据安全发生问题之后统筹资源、弥补损失并追究相关人员责任。在最后这一部分,本文将探讨国家层面对于元宇宙数据安全风险的应对措施。

(1) 及时建立元宇宙数据分级分类目录

在我国数据分级分类保护的制度背景下,元宇宙数据管理也应采取相同路径。当前首先要尽快通过国家标准《信息安全技术 网络数据分类分级要求》,并建立元宇宙行业数据分类以及相关核心数据、重要数据、一般数据分类目录,如此才能和当前的数据保护制度有效衔接,以应对日渐严峻的元宇宙数据安全风险。随着元宇宙技术和产业的不断发展,各类数据的群体、区域、精度、规模等因素会产生变化,因此还应定期评估元宇宙数据分级分类目录的合理性并及时做出调整,防止部分数据重要性上升以后却未得到法律的有效保护,造成元宇宙

数据安全事故。

(2) 审查备案元宇宙平台资质及其产品

有关部门应严格审查元宇宙平台资质,审查备案元宇宙产品。可以预见到,未来元宇宙平台不会只有一家,而可能是来自不同国家的多家元宇宙企业同台共舞,这也导致了元宇宙数据安全问题可能在不同元宇宙平台上发生。元宇宙数据安全风险相较于传统单类型的大数据安全问题,后果更加严重,影响范围更加广泛。为了有效控制元宇宙数据安全风险,国家应建立元宇宙平台资质审查制度,提高元宇宙平台准入门槛,筛除明显没有能力应对和保障元宇宙数据安全的平台,例如审查元宇宙提供平台的数据安全保障技术能力、相关信用记录等方面的信息。同时,应建立元宇宙产品数据安全相关标准,对于平台所提供的各个元宇宙世界产品进行审查和备案,具体筛查各个元宇宙是否有数据安全漏洞,是否能够满足相应使用场景下的数据安全保障要求,对于不符合安全要求的元宇宙应不予批准对外开放。

(3) 构建元宇宙数据安全管理制度

有关部门应介入元宇宙内部数据管理,监督、引导平台制定元宇宙数据安全管理制度。虽然对于元宇宙内部社会性的管理目前有去中心化和非中心化两种不同观点,但是在元宇宙数据方面去中心化的管理显然不能满足防范数据安全风险的要求。为了防范平台自主制定的数据管理制度的漏洞和风险、平台怠于制定元宇宙数据安全保护制度、平台怠于履行元宇宙数据保护义务,国家应当介入元宇宙内部的数据管理,在确认元宇宙数据也应遵守当前《数据安全法》《个人信息保护法》等法律以外,针对元宇宙数据的特殊性,在元宇宙数据安全风险评估与监测预警、元宇宙数据安全风险应急管理措施、元宇宙数据安全管理制度备案等方面,为元宇宙的数据管理制定统一的基本管理规定。例如,在元宇宙个人信息收集和使用活动不得有所放宽的客观现实下,还需要更严格的数据分级分类管理制度、数据流动制度等予以配套(王德夫,2021);抑或要求平台在发生元宇宙数据安全事故时及时向有关部门通报,以及时控制局势、减少损害。国家层面既可以颁布统一的元宇宙数据管理办法,在现有法律法规中新增相关条文,也可以对元宇宙公司章程中涉及数据管理的内容单独进行审查,监督、引导各元宇宙平台切实建立健全元宇宙数据安全管理制度;同时,为平台留下一定的数据管理利用空间,在保障元宇宙数据安全和平台企业创新积极性与数据要素市场

活力之间达到平衡。

(4) 建立元宇宙平台数据安全管理的常态化审查监督制度

在审查和管理之外,还应建立元宇宙平台数据安全管理的常态化审查监督制度,及时排除风险;动态监测平台元宇宙数据安全管理的落实情况,定期进行元宇宙平台数据管理利用情况审查,及时发现平台安全漏洞并要求其整改,要求平台及时更新落后的元宇宙数据安全管理制度,避免真正造成数据安全事故;要求平台定期公布元宇宙数据安全报告,接受社会监督,帮助元宇宙用户更好地识别和筛选更有数据安全保障能力的元宇宙平台,促进平台良性竞争。做好元宇宙数据安全风险的事前防控,少发生、不发生元宇宙数据安全事故才是最终追求。

六、结语

当前元宇宙的发展距离实现其沉浸式虚拟世界的目标还有一段距离。在元宇宙技术不断发展的过程中,作为其核心技术之一的大数据技术也会随之发展,进行大量的数据采集、存储、利用等活动会一直持续到元宇宙的诞生和发展后,这将对数据安全保障提出新的挑战,而元宇宙数据和当前大数据不同的全方位性也预示着元宇宙数据安全更加需要我们重视和保护,并且将在用户、平台和国家三类主体上表现出不同的形态,引发不同的后果。为避免元宇宙数据安全问题引发严重后果,有必要对其风险来源进行前瞻性的分析并做好应对准备。我们通过对元宇宙治理模式的分析可知,去中心化的管理模式无法有效应对元宇宙数据安全风险,各主体共同参与的多元共治将是理想模式,但是我国当前尚未建立起元宇宙专门制度,元宇宙数据安全相关问题只能参照现行相关法律。要切实建立有效的多元共治的元宇宙数据安全风险治理制度,尽快建立元宇宙基本制度及元宇宙数据安全保护制度,在基本的数据制度之上为元宇宙数据安全上一把更有针对性、更有效的锁。

参考文献

程金华,2022,《元宇宙治理的法治原则》,《东方法学》第2期。

高一乘、杨东,2022,《应对元宇宙挑战——数据安全综合治理三维结构范式》,《行政管理改

革》第3期。

何傲翹,2021,《数据全球化与数据主权的对抗态势和中国应对——基于数据安全视角的分析》,《北京航空航天大学学报》(社会科学版)第3期。

何波,2022,《中国参与数据跨境流动国际规则的挑战与因应》,《行政法学研究》第4期。

李善青、郑彦宁、邢晓昭等,2019,《科学数据共享的安全管理问题研究》,《中国科技资源导刊》第3期。

刘涛、袁毅,2022,《去中心化自组织管理的形态、特征及差异性比较》,《河北学刊》第3期。

马忠法、胡玲,2021,《论我国数据安全保护法律制度的完善》,《科技与法律》第2期。

沈逸,2022,《元宇宙与国家数据安全——构建生态化治理体系的挑战与趋势》,《中国信息安全》第1期。

时明涛,2020,《大数据时代个人信息保护的困境与出路——基于当前研究现状的评论与反思》,《科技与法律》第5期。

汪庆华,2021,《数据可携带权的权利结构、法律效果与中国化》,《中国法律评论》第3期。

王德夫,2021,《元宇宙领域的个人信息保护新挑战与法律应对》,《中国市场监管研究》第11期。

王名、蔡志鸿、王春婷,2014,《社会共治——多元主体共同治理的实践探索与制度创新》,《中国行政管理》第12期。

王玉林,2016,《大数据中个人信息开发利用法律问题研究》,《情报理论与实践》第9期。

谢宜璋,2021,《可商品化数据的进一步厘清——概念、保护诉求及具体路径》,《知识产权》第8期。

许可,2021,《数据爬取的正当性及其边界》,《中国法学》第2期。

张菲、朱桐雨,2022,《互联网平台企业的数据垄断问题研究》,《国际经济合作》第5期。

张钦昱,2022,《元宇宙的规则之治》,《东方法学》第2期。

周若涵,2021,《数据安全风险对国家安全的挑战及法律应对》,《上海法学研究》第1卷。