三维视阈下网络身份认证公共服务的发展路径探索

李佳强

（中国人民公安大学　研究生院，北京　100038）

摘　要：随着数字化手段对科技的革命与产业的升级，社会中也滋生了各种互联网平台乱象与违法犯罪行为。网络身份认证公共服务作为我国可信网络身份战略的重要推进，如何对网络身份认证公共服务进行全面优化是当前亟待解决的问题。通过梳理我国网络身份认证的提出与发展进程，围绕公民网络身份数据权利视阈、价值风险视阈、制度建设视阈三个维度，分析网络身份认证公共服务所形成公共数据的权利应然，聚焦公共数据的价值实然与网络身份认证公共服务的风险似然，探索网络身份认证公共服务在制度建设过程中的优化策略。

关键词：网络身份认证；网络身份认证公共服务；数据权利；价值风险；优化策略

中图分类号：D922. 17　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 02. 010

引用格式：李佳强. 三维视阈下网络身份认证公共服务的发展路径探索［J］. 网络安全与数据治理，2025，44(2)：62 - 66.

Exploring the development path of network identity authentication public service under three-dimensional perspective

Li Jiaqiang

(Graduate School, People's Public Security University of China, Beijing 100038, China)

Abstract: Accompanied by the digital means of the revolution in science and technology and industrial upgrading, society has also bred a variety of Internet platform chaos and illegal and criminal behavior. Network identity authentication public service is an important promotion of China's credible network identity strategy, but how to optimize the public service is an urgent problem to be solved. Through sorting out the proposal and development process of network identity authentication in China, we analyze the right contingency of public data formed by public services, focus on the value reality of public data and the risk likelihood of public services, and explore the optimization strategy of public services in the process of system construction by focusing on three dimensions, which are the right threshold of citizens' network identity data, the value risk threshold, and the system construction threshold.

Key words: network identity authentication; network identity authentication public services; data rights; value and risk; optimization strategies

0　引言

随着科技革命与产业升级的深入推进，近年来，人类社会的生活方式、生产方式和治理方式都依托于数字化网络手段进行了转型升级。在媒体推广和商业利益的推动下，信息网络技术迅速成为社会热点，受到社会各界的广泛关注。这也引发了犯罪人依靠其进行犯罪手段升级，包括但不限于“诈骗案中的假脸假声技术”“侵犯公民个人信息案中的数据滥用技术”“破坏网络信息安全案中的自动攻击技术”等[1]。在网络发展的过程中也出现部分自媒体账户在网络社交平台通过传播不实消息、炒作热点事件、制造群体对立、消费社会爱心等行为实现恶意流量变现。除此之外，网络上还存在“编造虚假人设引流”“利用伪科普传播不良消息”“软色情违规引流”“夸大商品功效欺骗消费者”等营商网络乱象。这些现状引发了网络可信身份战略的确立及推进国家网络身份认证公共服务建设的公众需求。

自 2002 年以来，李希光教授率先提出“应禁止任何人网上匿名”，自此网络实名制开始在学界展开探讨。2012 年，全国人大常委会通过《关于加强网络信息保护的决定》，明确了国内网络实名制治理的要求[2]。2015 年，国家网信办出于整顿互联网乱象的目的，发布的《互联网用户账号名称管理规定》中提出按照“后台实

名、前台自愿”的原则认证使用者真实身份信息[3]。2024年，公安部发布《国家网络身份认证公共服务管理办法（征求意见稿）》（以下简称《管理办法》），提出按照自愿原则推广互联网登记服务中应用网络身份认证公共服务管理。这使得网络可信身份战略以网络身份认证公共服务的形式进入应用阶段。

网络身份认证公共服务是指国家根据法定身份证件信息，依托国家统一建设的网络身份认证公共服务平台，为自然人提供申领网号、网证以及进行身份核验等服务[4]。网络身份认证公共服务的目的旨在保护公民的身份信息安全与促进国家数字经济发展。网号是指与公民自然人身份所对应的由字母与数字组成，不含个人身份信息的网络虚拟身份符号；网证是指承载网号及自然人非明文身份信息的网络身份认证凭证。依托于网号与网证，在互联网服务及相关行业管理中以非明文登记的方式核验自然人身份信息。

1 数据权利视阈下的网络身份认证公共服务应然

1.1 网络身份认证公共服务是对数据所有权的确权

网络身份认证公共服务的运行本质上是一种社会身份向网络身份的映射。由国家公安部门和国家网信部门所监督管理的公民网络虚拟身份数据，由于与自然人身份信息一一对应，可以看作是网络数据化的社会身份。从个人的视角，网络身份认证公共服务所提供给公民个人的网络虚拟身份是公民的个人身份隐私，隶属于自然人的人格权受到法律保护；立足国家和社会的层面，网络虚拟身份数据应具有公共属性且涉及国家安全、个人隐私，故按照《数据二十条》的分类，应属于用于公共治理、公共利益的国有公共数据。所谓国有公共数据，即由国家管理和控制，受全体国民自由利用公益目的制约，非经过技术手段和法定程序使其转化为可市场化流通利用的私用类公共数据，不得进行市场化流通和利用的公共数据[5]。对于其所有权的确权规则，当前学界已经形成共识，公共数据的所有权应当为公共主体所有[6]。理论上来说，在公共主体同时享有网络虚拟身份数据的支配权的情况下，整体性的所有权的内涵是个人所有权所变现出的管理权能。而在我国以公有制为主体的经济制度下，应由国家公安部门和网信部门通过监督管理这部分数据信息从而对其他机构的持有权做出部分限制与制约，传达来自人格权所有权人（全体公民）的约束并负责落实公民网络虚拟身份数据安全。

1.2 网络身份认证公共服务是收益权与隐私权的区隔

网络身份认证公共服务基于对网络虚拟身份的数据确权，回应公共数据公共财产属性，通过技术加密和法定程序将国有公共数据转化为可以进行市场化流通利用的私用类公共数据，进而区分涉及公民数据的衍生数据收益权和公民隐私权，最终实现公共数据利益的全民共享。传统公物理论认为，公物的自由利用遵循自由使用、免费或低费使用、平等使用三大原则[7]，国有的公共数据也应具有“公益性”和“公用性”的特点，但是由于没有经过公有化－许可－使用的流程，无法进行数据确权，导致这部分数据难以有效利用，甚至产生权利间的冲突。网络身份认证公共服务的过程正是对网络虚拟身份的公有化－许可－使用的流程体现，如图1所示。申领网号、网证与登记核验的过程是现实身份到网络虚拟身份公有化的路径体现；互联网平台的接入是政府公共平台批准许可的过程。只有经由网络身份认证公共服务平台的许可和用户同意后，互联网平台才可以对用户的网络虚拟身份信息进行留存和处理；只有经过用户本人授权或单独同意，互联网平台才可以获取、留存用户现实的法定身份证件信息。换而言之，网络身份认证公共服务的存在更像是一道由政府部门负责的阻隔公民社会身份和网络虚拟身份的防火墙，从而解决企业涉及公民衍生数据收益权和公民隐私权之间的权利冲突。

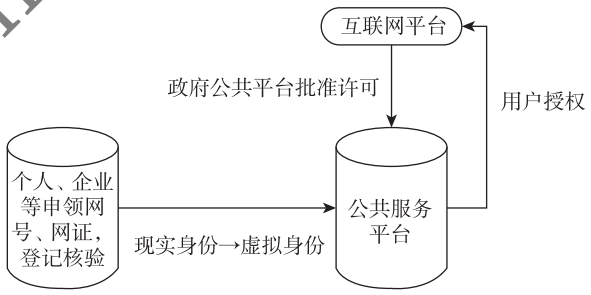

图1 网络身份认证公共服务过程

1.3 网络身份认证公共服务是持有权与经营权的配置

在企业的数据经济流通过程中存在两个问题难以解决，一个是企业数据持有权的确立，另一个是数据经营权的保障。网络身份认证公共服务的存在对公民网络身份数据背后的隐私权进行了一元论的权利配置，但是经由官方的加密工作对涉及公民在互联网平台的使用记录等衍生数据收益权做出了二元的权利配置，包括企业数据的持有权和企业数据经营权。互联网平台持有的衍生数据与用户的身份信息脱钩，不与公民的隐私权产生权利的冲突。这部分衍生数据的持有主体为互联网平台，且经营权仍隶属于平台。基于此，网络身份认证公共服务以一元论的所有权与二元论的收益权，采取一种围绕数据所有、管理与利用相兼容的权利构造。

2 价值风险视阈下网络身份认证公共服务的实然与似然

2.1 价值维度下网络身份认证公共服务的实然

2.1.1 网络身份认证公共服务落实网络可信身份战略

网络身份认证公共服务来源于《中华人民共和国个人信息保护法》，服务产生的前提是用户法定身份证件信息与网号、网证的关联，实现社会身份到网络虚拟身份的迁移。由于网络空间在物理上与现实的隔离，其用户身份、行为都具有不确定性，进而引发诸多乱象，给网络空间的安全管理与网络上的公民信息交互信任体系建设造成了巨大的打击，在一定程度上制约了我国网络应用的发展。实际上，网络空间的安全不仅影响公民个人的身份信息安全，大规模的公民个人身份信息的泄漏更会影响国家安全[8]。在原有的网络环境下，用户在不同互联网平台的使用过程中均需要提供不同的账户名和密码，且每申请一次账户都“软强迫式”向平台提供涉及自身社会身份信息的数据，存在严重的网络身份不实与个人信息泄露风险。网络身份认证公共服务的出现可以有效解决这一现象。由网络身份认证公共服务平台提供的网证、网号阻隔了社会身份与网络虚拟身份，一方面用户不必反复向互联网平台提交涉及自身社会身份信息，降低了在使用网络过程中的信息泄露风险，避免身份信息的盗取和滥用；另一方面由国家确立网络身份的可信性，打击自媒体野蛮发布信息的乱象或网络诈骗的猖獗，进一步保障我国网络空间的安全形势。

2.1.2 网络身份认证公共服务保障数据使用安全

网络公共数据的使用分为“信息生成”“数据处理”与“信息存储”三个阶段。首先在“信息生成”阶段，网络身份认证公共服务以保障公民身份信息安全为前提，网证、网号是网络身份认证公共服务平台对国有公共数据进行再加工所形成的可供私用的公共数据。网络身份认证公共服务在此也就保证了公共数据产出的安全前提。其次在“数据处理”阶段中，《管理办法》中明确网络身份认证公共服务平台在处理用户个人信息前，需要向用户告知涉及平台名称、信息处理目的、用户权利救济等相关信息，在互联网平台需要获取相关信息时既保障用户知情权，也以最小化原则提供相关信息。据此，网络身份认证公共服务保障了数据利用过程中的安全性。除此之外，在“信息存储”阶段，无论是公民身份信息形成的国有公共数据还是加工形成的私用类公共数据，《管理办法》中均明确了网络身份认证公共服务过程中的数据安全和信息保护的责任主体，并设立相关监督部门共同治理。在信息存储的过程中，国务院下属的民生相关部门，诸如铁路、邮政、文旅、民政等在各自职责范围内负责其数据安全。

2.1.3 网络身份认证公共服务保障数据经济流通

网络身份认证公共服务可以通过数据流动和配置、数据创新应用、数据安全保障三个方面赋能新质生产力，加快数字经济流通。首先，网络身份认证公共服务由于对网证、网号等公民网络虚拟身份进行确权，规定企业的二元论收益权，进而保障了企业数据持有权的排他性，让企业作为数据持有者依法享有对数据的自主管控，从而加速数据作为企业资产在市场上流通。通过网络身份认证公共服务对数据信息的保护，避免了企业对“不可用不可见”的国有公共数据的无法利用，促进国有公共数据向私用类公共数据的发展进程，形成推动公共数据流动的内在推力[9]。其次，网络身份认证公共服务对网证、网号的规定利于企业的数据创新应用。高质量的私用类公共数据依托于网络身份认证公共服务对网证、网号的数据确权与政府各个部门在网络身份认证公共服务环节上的共同参与、互相监督，可以在一定程度上缓和政府对企业数据的苛责监管，防止政府部门对企业数据创新的干预。最后，在数据安全保障方面，网络身份认证公共服务平台的统一身份认证体系，有效防止反复、多平台输入个人信息造成的信息泄漏。网络身份认证公共服务的建设基于策略、检测、防护和响应的安全模型，采用应用安全、数据安全、云平台安全、网络安全与边界安全的五维安全体系提供数据安全保障[10]。网络身份认证公共服务平台向社会释放五维安全体系过滤后的公共数据，提升数据利用的安全可控程度，数字经济安全与发展的平衡需求得以实现。

2.2 风险维度下网络身份认证公共服务的似然

2.2.1 公共数据泄密导致的网络安全隐患

网络身份认证公共服务身份建设在运营过程中可能存在的网络安全隐患包括数据隐患与技术出境泄密隐患。

首先，原始数据的存储媒介是在可信身份认证总体架构中属于内网下数据处理中心的多级云管，通过采用多地多中心架构设计导致数据并不会轻易泄露。但是互联网平台在调用公民社会身份信息并经过哈希算法等处理形成网证、网号等原始数据的过程中仍然存在信息泄露的隐患。以 2023 年 12 月 AI 平台 HF（Hugging Face）存在 API 令牌漏洞导致谷歌平台数据库被插入恶意代码为例，如果互联网平台后台存在漏洞，因平台间的关联性，在数据使用的过程中会导致网络身份认证公共服务平台存在数据泄露隐患。

其次，技术出境也可能导致泄密隐患。网络身份认证公共服务平台是由国务院下属的民政、文旅、传媒、

卫健、铁路、邮政等多个与民生相关部门共同推广应用，虽然我国目前已出台《数据安全管理办法》《个人信息安全规范》《个人信息出境安全评估办法》《政务信息共享数据安全技术要求》等部门规章和管理规定，但是很难全面覆盖形成精细化管理。由于法律对技术出境问题无法进行详尽有效的规定，导致技术人员对自己负责的网络身份认证公共服务部分信息不能依法进行严格保密，进而影响我国网络身份认证公共服务的进展。

2.2.2 公共数据使用过程中的不平权利用

公共数据使用过程中的不平权利用主要聚焦于两个问题，分别是使用许可问题与收益分享问题。在使用许可问题上，《管理办法》中网证、网号等形成的国有类公共数据的管理权能配置属于一元论，掌握在政府部门手中。但是需要注意的是即便管理权能是一元论配置，但其本质上是国家作为所有权人代表全部公民行使主体意志自由以保障社会数字经济的发展。最容易导致许可行为发生异化的是网络身份认证公共服务的成本问题。无论是公共数据的运行、维护、更新，抑或基础设施的建设，还是向企业提供数据产品服务都需要网络身份认证公共服务平台投入大量的经济成本。需要警惕网络身份认证公共服务在发展过程中面对这些经济成本，导致政府对国有类公共数据的“授权运营”向“审批许可”的异化，进而导致公共数据使用过程中的不平权利用。第二个可能导致公共数据使用过程不平权利用的是收益分享问题。我国数据发展尚处于摸索阶段，关于数据资产的收益还难以准确地衡量。但是网络身份认证公共服务所提供的无论是国有类公共数据还是私用类公共数据，都是网络身份认证公共服务平台在履职过程中所收集的数据。其来源是社会公众，其支出是公共财政资金，但是公共数据经由后续运营所产生的利润却归属于企业或互联网平台。虽然企业或互联网平台对数据进行了再加工，但是这也导致了由公共财政资金所承担的运营成本支出所得的后续利润并未向社会公众分享，仅由企业等少数运营主体获得。这种收益分享导致的问题如果不能得到妥善解决，也会对我国数字经济的发展形成严重的阻碍。

2.2.3 多政府主体参与数据治理责任风险

多政府主体参与数据治理的责任风险体现在组织内部的数据孤岛、治理责任边界不清与存在黑客的攻击。《管理办法》中按照《网络安全法》确定网络身份认证公共服务所产生数据的保护主体为公安与网信两个监督管理部门与多个涉及民生的推广应用部门，诸如民政、文旅、传媒、邮政等。由多个部门协同参与网络身份认证公共服务，一方面在发展初期确实可以形成合力互相监督网络身份认证公共服务的发展，但是另一方面由于各政务部门各自掌握其独特数据资源，在网络身份认证公共服务发展中后期可能也导致数据封闭，进而在组织内部形成数据孤岛[11]。另外，多个政府部门分别掌握各自数据，存在治理责任边界不清的问题。由于目前缺少数据在政府内部流动的规范流程和标准，各政务部门按照自身行业标准所形成的内外流动规范也莫衷一是，在数据安全治理的过程中缺乏统一流程。一旦发生数据泄密问题，溯源、追责、事后维护等机制难以有效启动，故存在数据治理的责任风险。最后，政府数据安全治理的网络技术发展动力主要来源于社会治理现实需求，在多部门共同参与的情况下必然会着眼于如何利用数据为自己所负责的政务产生更大的社会效益。这种出于公益的目的，无法与追求经济效益的互联网平台企业等同步数据治理技术的发展。由于国有类数据的原始性与稀缺性产生的巨大利益，存在激生黑客攻击的动机。

3 制度建设视阈下网络身份认证公共服务的优化策略

3.1 法律建设下的数据泄密风险优化策略

网络身份认证公共服务似然存在的风险中，有关数据泄密的问题主要是因为数据调用与技术出境两方面造成的。

数据调用过程涉及数据由内部向外部输出的过程，其风险调试优化重点在于法律有效性的建设。首先法律所赋予政府的职权概念发生改变。数据经济的出现使得社会生活中政府、企业、公民的法律角色在互联网虚拟空间中发生转变，政府的职能之一是实现对国家数据主权的维护，在法律建设中重点突出对数据的管理权能。这个管理权能不仅包括政府对数据的开放共享、调配归集权利，也包括对数据流向路径的追踪与持续保障数据安全的能力。其次，数据调用风险的优化还可以进行法律治理模式的优化。相比较于传统的社会空间，网络空间的治理在政府自上而下地主导制定政策的模式下，还可以引入多元化主体（包括企业、个人等）进行社会参与。以企业的技术优势与公民的数量优势，管理、利用数据，政府行使管理权能的过程中可以引导这部分社会优势力量应对数据调用过程中可能存在的风险。

技术出境问题的治理重点在于完善相关法律。《数据安全管理办法》《个人信息安全规范》《个人信息出境安全评估办法》《政务信息共享数据安全技术要求》等法律规定对技术出境问题仍不完善。针对法律法规要及时更新完善，可以根据政务工作人员参与数据网络身份认证公共服务的数据体量不同，设立不同的数据风险防范等级身份，以防技术出境导致的泄密。除此之外，在公安、网信两个监督部门可以设立“名录”，涵盖相关涉及网络身份认证公共服务的政府人员与企业代表，形成有效监督。

3.2 组织管理下数据不平权利用风险优化策略

对网络身份认证公共服务平台推进过程中可能存在的数据不平权的风险治理，重点在于形成内 + 外的组织管理模式。

网络身份认证公共服务对内的组织管理，可以按照网络身份认证公共服务平台的数据流程处理过程进行分工，形成收集 - 存储 - 管理 - 调用各级分工机制，以明确责任制来提高组织内部数据处理效能。对内的组织管理也可以从工作绩效的角度提升数据治理工作积极性。数字经济是现阶段中国的发展重点，因此涉及网络身份认证公共服务平台建设的政府部门可以围绕“干部任用”选拔标准与“按劳分配”薪酬体系实现内部的双向管理。结合政府部门的规章制度，保障国有类公共数据的收集存储、私用类公共数据的管理调用，确保公共数据可以发挥其本身的优势，实现企业对数据的有效利用，进而推动我国数字经济发展。

网络身份认证公共服务对外的组织管理，应当着重注意互联网平台以及公共数据运营企业的权责范围。网络身份认证公共服务所掌握的数据可以按照“公共数据分类分级”的管理要求，供给互联网平台与企业进行数据的再加工。一方面避免企业对私用类公共数据的收集不易、政府对公共数据供给不足的数据窘境，实现企业对数据的合法利用；另一方面也要避免企业从网络身份认证公共服务平台以“地下途径”拿到涉及公民身份的敏感数据，避免数据泄露。

3.3 流程优化下数据治理责任风险优化策略

网络身份认证公共服务数据治理风险隐患的治理重点是优化统筹各部门网络身份认证公共服务平台建设的完整性与规范性。镜鉴传统管理体制下政府数据的存储与管理，各部门、各地区之间的数据管理往往由于地区经费保障、技术发展的不一致，导致各个数据平台系统呈割裂状态发展，最终形成的数据信息格式不同、内容不同。这部分差异化信息如果想要综合利用就需要进行清洗处理，影响数据治理效能。因此，在网络身份认证公共服务平台建设过程中需要做到对数据的“书同文，车同轨”，形成统筹规划。除推广应用的政务部门外，更需要监督管理部门统筹规划出制式的数据存储、处理格式，完善数据在各平台流转的流程，实现国家范围的政府数据格式统一，标准化数据传输与准入流程。另外，多政务部门共同推广应用网络身份认证公共服务，需要监督管理部门划分清晰各政务部门的职责范围，避免责任不清的问题。监督部门还可以通过设立数据治理网站反馈板，通过引入第三方机构评估或引入其他社会主体参与以明确问题和改进方向，促进政务部门网络身份认证公共服务的流程优化，形成综合全面的网络身份认证公共服务平台，增强政府的数据治理能力。

4 结束语

现阶段，网络身份认证公共服务平台的建设目标是形成新型举国体制优势来保障我国数字经济的高速发展，支持我国网络虚拟空间治理，最终实现数字中国建设。为提升我国网络身份认证公共服务进程，本文分析了《国家网络身份认证公共服务管理办法（征求意见稿）》，在权利视阈下形成公共数据的确权，并进一步围绕价值风险，对网络身份认证公共服务与其产生数据进行价值分析与风险研判。最后从法律建设角度对网络身份认证公共服务提出一些可供借鉴的优化策略，以期推动我国网络身份认证公共服务进程。

参考文献

[1] 聂江波. AI 犯罪前瞻及人工智能侦查系统构建 [J]. 公安研究，2024（5）：86 - 91.

[2] 全国人民代表大会常务委员会. 全国人民代表大会常务委员会关于加强网络信息保护的决定 [R]. 北京：全国人大常委会办公厅，2013.

[3] 国家互联网信息办公室. 互联网用户账号名称管理规定 [Z]. 2015.

[4] 公安部，国家互联网信息办公室. 国家网络身份认证公共服务管理办法（征求意见稿）[Z]. 2024.

[5] 张素华，王年. 公共数据国家所有权的法理基础及实现路径 [J]. 甘肃社会科学，2023（4）：146 - 158.

[6] 叶宣含. 公共数据授权运营赋能新质生产力的逻辑展开与法治进路 [J]. 北京理工大学学报（社会科学版），2024，26（6）：28 - 40.

[7] 肖泽晟. 公物法研究 [M]. 北京：法律出版社，2009.

[8] 刘耀华. 国际网络可信身份战略研究及对我国的启示 [J]. 网络空间安全，2018，9（2）：1 - 5.

[9] 张素华. 数据资产入表的法律配置 [J]. 中国法学，2024（4）：229 - 249.

[10] 吴国英，杨林，邱旭华. 可信身份认证平台的构建 [J]. 信息安全研究，2022，8（9）：888 - 894.

[11] 王龙. 政府数据安全风险治理的机理逻辑与优化策略 [J/OL]. 科学学研究，1 - 13 [2024 - 09 - 01]. https://doi. org/10. 16192/j. cnki. 1003 - 2053. 20240705. 001.

（收稿日期：2024 - 09 - 29）

作者简介：

李佳强（2000 - ），男，硕士研究生，主要研究方向：刑事侦查学、侦查讯问学。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部