

DNS-RELATED DIGITAL RIGHTS LINKED TO ECONOMIC DEVELOPMENT IN SOUTH AFRICA

Busisiwe Mathonsi¹, Hlologelo Ngobeni², and Adv. Lerato Seema³

¹ Busisiwe Mathonsi, Compliance and Regulatory Manager - Policy, Licensing, and Regulations, ZA Domain Name Authority, Johannesburg, South Africa (*Contributor*)

² Hlologelo Ngobeni, Public Administration Graduate - Policy, Licensing, and Regulations ZA Domain Name Authority, Johannesburg, South Africa (*Contributor*)

³ Advocate Lerato Seema, Executive Manager – Policy, Licensing, and Regulations, ZA Domain Name Authority, Johannesburg, South Africa (*Peer-Reviewer*)

Abstract

Internet use expansion in South Africa has significantly increased over the past decade, with 89% of households that have mobile phones in 2011. Currently, 68.2% of the population—or 41 million, use the Internet. In this context, digital rights associated with Domain Name Systems (DNS) and their protection are significant concerns with a global effect on people, groups, and enterprises. This study explores the digital rights linked to DNS in South Africa, including the right to access the Internet, to control an owned domain name, and Internet use privacy and security. International laws, agreements, and the South African Constitution protect these rights. The study examined relevant cases linking digital rights to the Constitution, such as the right to access information, freedom of expression, privacy, equality, and property rights. Understanding the importance of DNS-linked digital rights is crucial for individuals, organisations, and businesses to participate fully in the digital economy, access information and knowledge, and express themselves online.

Keywords: Internet use; digital rights; DNS protection; personal data; intellectual property rights; Universal Declaration of Human Rights; South African Constitution; and economic development

1 Introduction

Internet use has significantly expanded, with much of this occurring over 10 years (2001 to 2011). According to the national census estimates, South African households with mobile phones increased from 32% to 89% between 2001 and 2011. In 2020, of the 59 million people living in South Africa, 36.54 million used the Internet—34.93 million with Internet access on a mobile device. In the absence of universal broadband, access increased regarding the expansion of mobile Internet.

As of January 2022, there were 41 million Internet users in South Africa. South Africa's penetration in 2022 stood at 68.2%. Between 2021 and 2022, Internet users increased by 494 000, translating to a 1.2% increase.¹

2 Background

Digital rights associated with Domain Name Systems (DNS) and their protection are significant concerns with a global effect on people, groups, and enterprises. For economic growth—freedom of speech, and information access, are essential to maintain the Internet's stability, security, and accessibility.

An essential component of DNS-related digital rights is the protection of personal data, the encouragement of competition and innovation in the domain name market, and the fair and open operation of domain name registries and registrars. These rights are safeguarded by international laws and agreements, including the European Union General Data Protection Regulation, the International Covenant on Civil and Political Rights, the Convention on Cybercrime, the World Intellectual Property Organization Copyright Treaty, the Universal Declaration of Human Rights, and the Internet Governance Forum (IGF) of the United Nations.

DNS converts domain names (like www.example.com) into IP addresses for computers to access websites and other Internet resources.² Economic progress in South Africa is highly correlated with access to the Internet and control over DNS. For instance, businesses and organisations constructing and managing websites with ease, holding domain name ownership, hold a clear advantage. Access to the Internet and DNS control may help South Africa's small business development and entrepreneurship.³

3 Digital rights linked to DNS

Digital rights linked to DNS include the right to Internet access and control over an owned domain name. This includes the right to register, renew, and transfer domain names without

interference or censorship and the right to accurate and up-to-date DNS information. Digital rights linked to DNS also include the right to privacy and security when using the Internet and the right to free expression and the free flow of information. These rights are crucial for individuals, organisations, and businesses to participate in the digital economy fully and access information and knowledge while freely expressing themselves online.⁴

4 Linking rights to the South African Constitution

The South African Constitution provides several provisions relating to DNS-linked digital rights. Interpreting and implementing these rights may vary in practice; there may be limitations to these rights in certain circumstances.

The right to access information and freedom of expression, as protected by Section 16 of the Constitution, guarantees the citizens' right to access and receive information while expressing themselves freely. It is essential to exercise several other rights, including Internet access. In the *Independent Newspapers v Minister of Home Affairs and Another [2018] ZAGPPHC 117*, the court emphasised the importance of freedom of expression in a democratic society while recognising that information access is essential to exercise this right. The court also remarked that Section 16 of the Constitution protects the right to receive and impart information, including through Internet use.

Another case would be the *National Coalition for Gay and Lesbian Equality and Others v Minister of Home Affairs and Others (1999) (1) SA 6 (CC)*, where the Constitutional Court held that the right to freedom of expression includes the right to receive and impart information. The restriction of such rights must be justified under the Constitution.

The right to privacy protected by Section 14 of the Constitution guarantees citizens' right to privacy, including protecting personal information. It is important to ensure that individuals can use the Internet and control their domain names without fear of surveillance or interference. In the pre-dated case of *H v W [2012] ZAGPJHC 208*, the court recognised the importance of privacy in a democratic society, affirming that Section 14 of the Constitution protects the right to privacy. The court also remarked that this right extends to protecting personal information, particularly in modern technology.

Another relevant case is the case of *R v Morris [2003] ZACC 18*, where the Constitutional Court of South Africa recognised that the right to privacy includes the right to control owned personal information and data. The court emphasised that the right to privacy is crucial for protecting human dignity and exercising other fundamental rights.

The right to equality protected by Section 9 of the Constitution guarantees that all citizens are treated equally, including the right to Internet access, which can help to reduce digital inequality and promote economic development in South Africa. In the case of *Minister of Home Affairs v NICRO [2004] ZACC 7*, the Constitutional Court held that the right to equality is a foundational value of the South African Constitution; measures to promote equality may be necessary to discourse historical imbalances.

The right to property protection by Section 25 of the Constitution also guarantees the citizens' rights to own and control their property, which includes domain names and other digital assets. In the case of *Mvelaphanda Holdings (Pty) Ltd and Others v Registrar of Companies and Others*,⁵ the High Court of South Africa ruled that the registrar of companies had the power to cancel a company's registration had the company been dormant for an extended period, but that this power had to be exercised fairly and reasonably and should not be used to deprive the company of its property without compensation. This case demonstrates the importance of the right to property in protecting domain names and other digital assets.

5 The difference between rights and interests

Rights and interests are closely related concepts, but they have distinct meanings. A right is a legal or moral entitlement to do or not do something. It is a claim or privilege recognised and protected by law or moral principles. Rights are usually positive, meaning they present individuals with the power to do something or to demand that something be done for them. Examples of rights include the right to freedom of speech, a fair trial, and to own property.⁶

Interests refer to something an individual is concerned about or has a stake in. Interests are often negative, indicating they offer individuals the power to prevent something from happening or to demand that something not be done. Interests can be economic, social, political, and personal. Examples of interests include economic interests, such as the interest in a stable and growing economy; social interests, such as the interest in a strong and cohesive society; or personal interests, such as the interest in maintaining personal health and well-being.⁷

6 DNS-related digital rights interests

DNS-related digital rights interests include the interest in protecting personal information, the interest in ensuring the security and stability of the Internet, the interest in promoting competition and innovation in the domain name market, and the interest in ensuring that domain name registries and registrars are operated fairly and transparently.

- Interests in protecting personal information include ensuring that personal information is not collected, used, or disclosed without the individual's consent and that it is protected from unauthorised access, use or disclosure.
- Interest in ensuring the security and stability of the Internet includes the protection of the Internet infrastructure from cyberattacks and ensuring that the DNS system is dependable and resilient.
- Interest in promoting competition and innovation in the domain name market includes promoting competition among domain name registries and registrars and protecting intellectual property rights in domain names.
- Interest in ensuring that domain name registries and registrars are operated fairly and transparently includes protecting the rights of registrants, providing accurate and up-to-date WHOIS information, and protecting the rights of intellectual property holders in domain names.

All these interests are important to ensure a fair and stable Internet ecosystem where individuals, companies, and organisations can fully participate, express themselves, and conduct business online.

7 Economic development

Digitisation in any form and sector offers new opportunities that include domain names.⁸ Studies demonstrate that Internet access and using more advanced digital technology help lower-income, lower-skilled individuals find further and better employment, therefore, reducing poverty. After three years, localities with Internet access significantly outperformed those lacking access concerning labour force participation and employment.⁹ According to the Harvard Business Review, South Africa outperforms major developing market nations in the Latin American and Asian/Southeast Asian areas concerning the ease of creating digital jobs, supported by strong consumer demand for digital firms and a supportive institutional environment.¹⁰

8 International laws on DNS-related digital rights

Several international laws and agreements relating to DNS-related digital rights, including:

- **The Universal Declaration of Human Rights (UDHR):** This is a non-binding resolution adopted by the United Nations General Assembly in 1948, recognising the right to privacy, own property, freedom of expression, and fundamental human rights;¹¹ however, Article 29(2) provides that these rights are provisional; necessity and proportionality may be applied, specifically to the right to privacy.¹²
- **The International Covenant on Civil and Political Rights (ICCPR):** This treaty, adopted by the United

Nations General Assembly in 1966, recognises freedom of expression and privacy as protected human rights.¹³

- **The Convention on Cybercrime:** This treaty, adopted by the Council of Europe in 2001, provides for criminalising certain computer system-related Acts, such as unauthorised access, computer-related fraud, and distributing child pornography. The treaty includes measures for personal data protection and traffic data preservation.¹⁴
- **The World Intellectual Property Organization Copyright Treaty (WIPO Copyright Treaty):** This treaty, adopted by the World Intellectual Property Organization in 1996, protects copyright in the digital environment, including copyright protection in domain names.¹⁵
- **The European Union General Data Protection Regulation (GDPR):** This regulation, adopted by the European Union in 2016, governs the collection, use, and storage of personal data applying to any organisation that processes the personal data of EU citizens, regardless of the organisation's location.
- **The United Nations IGF:** This forum is a platform for international dialogue on Internet governance issues; it is open to all stakeholders, including governments and the private sector.

9 United Nations Internet Governance Forum

The United Nations IGF is a platform for international dialogue on Internet governance issues. It is open to all stakeholders, including governments, the private sector, civil society, the technical community, and academia. The United Nations Secretary-General established the IGF in 2006 because of the World Summit on the Information Society (WSIS); its mandate was renewed in 2015.

The IGF's mandate is to provide a forum for discussing Internet-related public policy issues and to promote stakeholder participation in the decision-making process. The IGF is not a decision-making body, and it does not have the authority to make binding decisions; it is a platform for dialogue, discussion, and exchange of information and best practices.

The IGF holds an annual meeting where representatives from diverse sectors and regions convene to discuss Internet governance concerns. The annual meeting includes a programme of workshops, main sessions, open fora, and other activities, such as dynamic coalitions and best practice fora. The IGF also conducts regional and national meetings to further its objectives.

The IGF's main objective is to foster inclusive and pluralistic dialogue on Internet governance concerns, promoting a shared

understanding of the Internet governance challenges and opportunities, and identifying and discussing ways to regulate these challenges. The IGF united stakeholders from diverse sectors and regions to discuss important Internet governance issues, such as cybersecurity, privacy, human rights, and online protection.

The United Nations IGF is vital in promoting stakeholder participation in the decision-making process. It fosters inclusive and pluralistic dialogue on Internet governance issues to ensure a free and open Internet for all.

10 Recommendations

- Ensuring universal broadband access in South Africa is crucial to provide equal Internet access to everyone, including those in rural areas. The government must take necessary measures to protect DNS-related digital rights. These rights include personal data protection, encouraging competition, innovation in the domain name market, and fair and open operation of domain name registries and registrars.
- The South African Constitution outlines various provisions regarding DNS-related digital rights; however, interpreting and implementing these rights may vary. Limitations may apply in certain situations.
- Individuals, organisations, and businesses need the right to access the Internet and control their domain names to participate in the digital economy, access knowledge fully, and freely express themselves online.
- The South African Constitution protects various rights, including access to information and freedom of expression, privacy, equality, and property rights, relating to DNS-linked digital rights.

References

- ¹ <https://www.statista.com/statistics/685134/south-africa-digital-population/>
- ² Wessels, D., Fomenkov, M., & Claffy, K. 2004. DNS Performance and the Effectiveness of Caching. *IEEE/ACM Transactions on Networking*, 12(2), 226-238. <https://doi.org/10.1109/TNET.2004.826281>
- ³ Nanjira, N. 2017. Digital equality: A necessary condition for inclusive internet. *Development*, 60(2-3), 93-99. <https://doi.org/10.1057/s41301-017-0115-9>
- Deibert, R. J. 2011). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. *The Political Quarterly*, 83(1), 34-42. <https://doi.org/10.1111/j.1467-923X.2012.02359.x>
- ⁴ Nanjira, N. 2017. Digital equality: A necessary condition for inclusive internet. *Development*, 60(2-3), 93-99. <https://doi.org/10.1057/s41301-017-0115-9>
- ⁵ (Mvelaphanda Holdings (Pty) Ltd and Another v JS and Others 2016 (2) SA 266 (GJ)).
- ⁶ Moore, A. D., & Bamberger, K. A. 2011. Rights and Interests: Two Sides of the Same Coin?. *Law and Philosophy*, 30(3), 255-285 doi:10.1007/s10982-011-9104-4.
- ⁷ Moore, A. D., & Bamberger, K. A. 2011. Rights and Interests: Two Sides of the Same Coin?. *Law and Philosophy*, 30(3), 255-285. doi:10.1007/s10982-011-9104-4
- ⁸ Seacom. (2022, May 12). *How Digital Innovation Tackles Socio-economic Challenges*. Retrieved from <https://seacom.co.za/business-insights/how-digital-innovation-tackles-socio-economic-challenges/>
- ⁹ The World Bank. 2021, September 24. *Narrowing the Digital Divide Can Foster Inclusion and Increase Jobs*. Retrieved from <https://www.worldbank.org/en/news/feature/2021/09/24/narrowing-the-digital-divide-can-foster-inclusion-and-increase-jobs>
- ¹⁰ Chakravorti, B., & Chaturvedi, R. S. 2019, December 04. Research: How Technology Could Promote Growth in 6 African Countries. *Harvard Business Review*. Retrieved from <https://hbr.org/2019/12/research-how-technology-could-promote-growth-in-6-african-countries>
- ¹¹ Universal Declaration of Human Rights. n.d.. Retrieved from <https://www.un.org/en/about-us/universal-declaration-of-human-rights> -Article 12, 17, 19.
- ¹² Ustaran, E. 2019. *European Data Protection : Law and Practice*. IAPP pg 15.
- ¹³ International Covenant on Civil and Political Rights, 1966 Article 19.
- ¹⁴ Cybercrime (Convention. (2001) Articles 2, 8,9.
- ¹⁵ Treaty, 1996.