Digital Ethics in Rwanda

Exploring Policies and Practices

Célestin Nsengimana,

Protestant University of Rwanda (PUR)

December 2025

Keywords

Abstract

This paper examines digital ethics in Rwanda, analysing how national policies align with everyday digital practices. Focusing on privacy, accountability, integrity, and transparency, it explores how Rwanda's collectivist culture influences ethical behaviours. Using qualitative methods, the study finds gaps between policy and practice, including data privacy violations, misinformation, and digital harassment. It calls for stronger enforcement, public awareness, and regional cooperation to harmonize ethical standards and balancing cultural values with universal digital ethics to promote responsible digital behaviours.

Corresponding Author: Rev. Dr Célestin Nsengimana, Protestant University of Rwanda, Email: celestinnsengimana703@gmail.com

Introduction

The increasing integration of digital technologies into our daily life has highlighted the urgent need for robust ethical frameworks. Globally, nations are struggling with the challenges posed by digitalization, from protecting individual privacy to ensuring accountability in digital spaces (Floridi, 2014). As a leading force in digital innovation within the region, the Rwandan government has actively implemented measures to advance a responsible approach to digital transformation. As a result, Rwanda has positioned itself at the forefront of Africa's digital revolution through progressive policies aimed at strengthening its information and communication technology (ICT) infrastructure (Hwang, 2019; Hwang, 2019; Mutambara, 2025).

In recent years, the country has made significant progress in developing frameworks for digital technologies and artificial intelligence (AI). Notably, Rwanda made history in April 2023 by becoming the first African nation to adopt a comprehensive National AI Policy. The policy aims to leverage the potential of artificial intelligence to drive economic growth while establishing Rwanda as a global leader in the ethical and inclusive advancement of AI (Rwanda Development Board [RDB], 2023; Mutambara, 2025). Building on this foundation, Rwanda hosted the Africa AI Summit in April 2025, where African leaders signed the Africa Declaration on Artificial Intelligence. The declaration emphasized sovereignty, inclusivity, and regional collaboration in AI development, and committed to building domestic talent, advancing ethical data governance, and promoting sustainable, human-centred AI innovation across the continent (AUDA-NEPAD and Republic of Rwanda 2025).

The swift advancement of digitalization offers vast opportunities yet also introduces important ethical challenges, especially in ensuring the responsible application of digital technologies (Dignum, 2019; Aminabee and Rao, 2025). Rwanda's evolving digital landscape exemplifies this duality, where expanding internet access and the growing influence of platforms like YouTube create both possibilities and challenges in the realm of digital ethics. The openness of digital spaces has frequently led to ethical violations, many of which result in legal repercussions. For instance, over the past five years,

the Rwanda Investigation Bureau (RIB) has recorded 136 cases of computer-based harassment, with 113 of these cases proceeding to prosecution (Rwanda Investigation Bureau [RIB], 2024). Dr. Murangira Thierry, spokesperson for the RIB, highlighted the ambivalence of social media, stating:

> " Social media was initiated to promote freedom of opinion. However, people must be aware of its dual nature, as it be a double-edged sword. Improper use of social media can lead legal trouble, while its responsible use can contribute to freedom of expression (Murangira, 2024).

This paper delves into the state of digital ethics in Rwanda, investigating the alignment or disparity between national digital policies and the daily practices of Rwandans. The goal is to raise awareness of existing digital policies in Rwanda and the legal consequences of ethical violations. Key ethical principles, including privacy, data protection, respect, accountability, integrity, confidentiality, and intellectual property rights, are considered in evaluating the country's digital landscape. The study reviews both policy frameworks and real-world behaviour, particularly focusing on social media use, to identify gaps and provide recommendations for fostering a culture of ethical digital practices. It is guided by the following questions: 1) What are the common digital practices among Rwandans and what ethical concerns arise from these behaviours? 2) To what extent do Rwanda's digital policies address the ethical challenges associated with digital and social media use? 3) How effectively are these digital policies being implemented to promote ethical behaviour and protect digital rights in Rwanda?

This paper is structured into four sections. The first section introduces the relevant theories underpinning the study, including ethical hybridity and digital ethics, and outlines the methodology used to analyse policies and practices. The second section explores the common digital practices among Rwandans, particularly in their use of social media, and examines the ethical concerns that arise from these behaviours. The third section focuses on Rwanda's digital policies, assessing their effectiveness in addressing the ethical challenges associated with digital and social media use. Finally, the

fourth section evaluates the implementation of these policies to promote ethical behaviour and protect digital rights in Rwanda.

1. Framework and Methodology

This study delves into the realm of digital ethics, a subfield of ethics that examines the ethical implications of digital technologies. It critically analyses existing digital policies and their implementation through the lenses of ethical hybridity and digital ethics theories.

Ethics, as defined by philosophers like Beauchamp and Childress (2009) and Piper (1970), is a branch of philosophy that explores the distinction between right and wrong and regulates moral conduct in society. It plays a pivotal role in shaping personal, professional, and societal behaviour by establishing moral standards, promoting accountability, fostering trust, and guiding decision-making. As a tool of legitimation, it justifies actions, laws, and institutions by ensuring they are morally acceptable (Prasanta, 2021; Fuchs, 1996). This process not only reinforces social cohesion by fostering a shared sense of purpose but also strengthens accountability, as legitimate institutions are widely perceived as having a moral obligation to act in the public interest (Fuchs, 1996).

Whereas descriptive ethics focuses on understanding actual moral beliefs and behaviours, normative ethics prescribes what ought to be done based on moral standards. The two are interconnected, with descriptive ethics informing normative ethics by providing data on behaviours, and normative ethics shaping moral beliefs. The aim of normative ethics is to help guide behaviour, resolve moral dilemmas, and foster moral education. The primary frameworks in normative ethics encompass consequentialism, which emphasizes outcomes; deontology, which centers on moral duties; virtue ethics, which highlights character; contractarianism, which is based on social agreements; and care ethics, which prioritizes relationships and empathy. These theories offer different approaches to resolving ethical issues (Velasquez, 2020).

Other ethical theories such as rationalism, realism, anti-realism, constructivism, and culturalism offer distinct perspectives on the nature of

moral truths. Ethical rationalism asserts that moral truths are discovered through reason alone, independent of personal beliefs or cultural context (Kant, 1785). In contrast, ethical realism holds that moral facts exist independently of human thought and are accessible through observation, experience, or intuition (Smith, 2004). Anti-realism rejects the existence of objective moral truths, emphasizing moral relativism, emotivism, and non-cognitivism, where moral judgments are seen as expressions of emotions or social constructs (Mackie, 1977). Ethical constructivism contends that moral norms are constructed through social practices and collective decision-making, emphasizing context, culture, and dialogue in creating moral principles (Rawls, 1971). Lastly, ethical culturalism suggests that moral values are relative to specific cultural contexts, advocating for tolerance and respect for diverse practices (Gowans, 2008).

Given the limitations of any single ethical theory, hybrid approaches are increasingly employed to address complex moral issues, particularly in the digital age (Bynum, 2018). Ethical hybridity integrates multiple frameworks to create context-sensitive, adaptable principles that reflect the pluralism of moral perspectives (Buchanan, 2004). In a globalized, digitalized world, it balances universal moral values with local cultural norms. While universal principles offer a common ethical foundation, decisions must also respect contextual differences. For instance, in Rwanda, the emphasis on community and social harmony shapes digital ethics by prioritizing collective well-being over individual autonomy, whereas individualistic societies tend to emphasize privacy and personal freedom (Buchanan, 2004).

The digital space has become a critical arena where differing cultural values, particularly collectivism and individualism, give rise to complex ethical dilemmas. In Rwanda, for example, the emphasis on community and social harmony shapes digital ethics, prioritizing collective well-being over individual autonomy. This cultural orientation often informs digital policies and practices that aim to maintain societal cohesion, promote public safety, and discourage online behaviour perceived as harmful to national unity. By contrast, individualistic societies—particularly in Western contexts—emphasize privacy, freedom of

expression, and personal autonomy in their approach to digital ethics (Buchanan, 2004).

These contrasting values frequently collide in digital spaces, complicating the resolution of moral dilemmas such as data privacy, freedom of speech, and platform regulation. As digital technologies transcend national boundaries, this cultural friction poses significant challenges to establishing universally accepted ethical standards, since digital ethics are shaped by societal context (Floridi, 2013). In Rwanda, this tension is particularly pronounced as the country seeks to balance technological innovation with its commitment to social cohesion and national security. The need to reconcile global digital trends with local cultural values highlights the complexity of developing ethical frameworks that are both globally informed and locally relevant.

This study employed a qualitative research approach with a descriptive design to examine the ethical dimensions of digital policies currently in place in Rwanda. The study target population comprised social media users and ICT regulatory agencies. Data was primarily collected from official and private digital platforms, including websites and social media outlets, in particular YouTube channels. A purposive sampling method was employed to choose appropriate textual and video resources (Mbonigaba, 2024). The analysis focused on key documents as the National AI Policy (2022), the Law on Prevention and Punishment of Cybercrimes (2018), the Law Relating to the Protection of Personal Data and Privacy (2021), the website of the Ministry of National Unity and Civic Engagement, and various YouTube channels.

2. Digital Practices and Ethical Concerns

The rapid rise of social media platforms such as YouTube, TikTok, and X (formerly Twitter) has significantly transformed Rwanda's communication landscape, reshaping how people engage with news, culture, entertainment, and public discourse. These platforms have empowered citizens to express their opinions, share personal experiences, and participate in national and global conversations. However, the increased reliance on social media has also introduced serious ethical dilemmas, particularly regarding privacy

violations, the spread of misinformation, and the responsibilities of digital content creators.

In Rwanda, social media influencers—individuals with substantial online followings—play a pivotal role in shaping public opinion and consumer behaviour. Influencers regularly drive conversations on politics, culture, and current events (Writer, 2024). While some people use their platforms constructively, others pursue visibility through sensational or misleading contents. This pursuit of digital clout often undermines respectful and informed dialogue, contributing to a toxic online environment. These behaviours reflect broader moral dilemmas, where individuals must navigate the tensions between self-promotion and the ethical responsibility to uphold integrity and respect for others (Beauchamp and Childress 2019), which entails an appropriate space for raising societal concern and expressing politically informed critical debates.

One of the most prevalent ethical violations on Rwandan social media is the unauthorized sharing of personal information. Users often disclose sensitive content—such as private photos or personal details—without consent, sometimes with the intent to shame or harm. These privacy breaches can cause significant reputational and psychological harm. Westin (2018) emphasizes that privacy is a fundamental right, and violating this right in a digital context undermines personal dignity and public trust. Similarly, Solove (2021) argues that users often underestimate the long-term risks of exposing private data online, especially in an era where digital footprints are difficult to erase.

Misinformation and disinformation pose significant threats in the digital age. Misinformation refers to false information shared without harmful intent, while disinformation is deliberately misleading content. Both can manipulate public opinion and distort the truth. For instance, Rwandan woman Scovia Mutesi was falsely accused on social media of being imprisoned for a crime she did not commit, illustrating how quickly misinformation can damage reputations (B&B Kigali 89.7FM, 2022). As Franks (2013) notes, once misinformation spreads online, it is difficult to retract, potentially leading to serious societal consequences.

Cyberbullying and online harassment represent additional ethical challenges, amplified by the anonymity and reach of digital platforms. Public figures, such as Rwandan artist Benjamin Mugisha ("The Ben"), have been targeted by influencers like 'Fatakumavuta,' whose abusive content attacked both Mugisha and his family. Following public outcry, Fatakumavuta was detained for 30 days pending trial (Iyamuremye, 2024). While Rwanda's Cybercrimes Law (Law No. 60/2018) provides legal mechanisms to address such offenses—criminalizing indecent messaging (Article 38) and the spread of harmful rumors (Article 39)—enforcement remains uneven. Agencies such as the Rwanda National Police and the Rwanda Investigation Bureau actively pursue these cases, yet the use of pseudonymous online profiles continues to impede accountability.

Despite the existence of legal frameworks, enforcement challenges persist. Many Rwandans remain unaware of their digital rights and responsibilities, and public education on ethical online behavior is limited (Paradigm Initiative, 2021). Young users in particular often engage with digital platforms without full awareness of the potential legal and ethical consequences of their actions. This digital literacy gap increases the risk of privacy violations and unethical online conduct, underscoring the urgent need for targeted digital citizenship education emphasizing accountability, respect, and legal awareness.

The speed at which digital content can go viral further complicates timely intervention by authorities (Gillespie 2018). As new technologies and platforms emerge, regulatory bodies must adapt continuously to meet evolving ethical challenges. The sustainability of Rwanda's digital governance therefore depends not only on robust laws but also on agile policymaking that keeps pace with innovation while safeguarding human rights. In this regards, Rwanda's efforts to regulate social media behaviour reflect a broader challenge of balancing digital freedom and ethical responsibility.

3. Rwanda's Digital Laws and Policies

Rwanda's digital landscape has undergone rapid transformation over the past decade, driven by government policies aimed at fostering technological innovation, economic growth, and social development. However, as digital technologies permeate every aspect of life, ethical challenges related to privacy, data protection, and the responsible use of technology have come to the forefront. This section explores the ethical dimensions of Rwanda's digital policies, particularly in relation to data privacy, social media governance, and artificial intelligence (AI), with an emphasis on the need to strike a balance between technological progress and the protection of fundamental rights. Based on the current development of the national administrative body of digital laws and policies, we shall explore and compile below various laws and policies such as the Law No. 60/2018 on the Prevention and Punishment of Cyber Crimes, the Personal Data Protection and Privacy Law (Law No. 058/2021 of 13/10/2021) and Rwanda's National Artificial Intelligence (AI) Policy, launched in April 2023. Our aim is to focus primarily on showing the extent of how the legislator's intention on framing digital interactions with administrative tools, have been sophisticatedly incorporated into our body of legal instruments, with the primary objective of addressing conflicts of interest and of rights, in an responsible and ethical manner.

Law on the prevention and punishment of cybercrimes

Law No. 60/2018 on the Prevention and Punishment of Cybercrimes plays a pivotal role in shaping the ethical landscape of digital practices in Rwanda. By addressing various forms of cybercrime, the law aligns with Rwanda's broader goals of promoting digital responsibility, protecting personal data, and ensuring a secure online environment for its citizens. The law is designed to tackle unethical digital behaviours, such as misrepresentation, fraud, harassment, and the spread of harmful content, which are critical for safeguarding both individual rights and national security in the digital age.

One of the key ethical concerns addressed by Article 29 is the act of misrepresentation and suppression of information. This provision holds

individuals accountable for deliberately providing false information or withholding material facts to obtain digital licenses or signatures. Such actions undermine the integrity of digital transactions and threaten trust in digital systems. To promote transparency and authenticity in digital practices, the law imposes penalties of up to five years of imprisonment and substantial fines. This ensures that individuals and organizations adhere to ethical guidelines when interacting within the digital sphere, aligning with the ethical principle of honesty and fairness in digital transactions (Rwanda Law, 2018).

Similarly, Article 30 focuses on the fraudulent use of digital certificates. It criminalizes the act of publishing false certificates or distributing revoked ones, which directly impacts the credibility and security of digital transactions. The ethical ramifications of this offense are significant, as it involves deceiving others for personal or financial gain, undermining the trust that is essential for a functioning digital economy. By enforcing strict penalties, this law emphasizes the importance of integrity and accountability in the use of digital signatures, encouraging individuals to act responsibly in their digital interactions (Rwanda Law, 2018). From this angle, Article 31 addresses the use of digital signatures for illegal purposes, reinforcing the ethical value of trustworthiness in digital environments. The creation or use of fraudulent signatures is not only illegal but also unethical as it compromises the reliability of digital systems. The severe penalties outlined for this offense reflect the government's commitment to ensuring that digital identities and actions are used in good faith and in accordance with the principles of justice and fairness (Rwanda Law, 2018).

On the other hand, Article 34 addresses the publication of pornographic material, which directly intersects with issues of digital ethics, particularly concerning digital content responsibility. The law distinguishes between adult and child pornography, imposing harsher penalties for the latter, reflecting society's ethical obligation to protect vulnerable individuals, particularly children, from exploitation. This provision ensures that the internet remains a safe space for all users and promotes ethical standards around the production, distribution, and consumption of digital content. The penalties for distributing such content serve as a deterrent against the unethical exploitation of digital media for harmful purposes.

Additionally, Article 35 focuses on cyberstalking, which involves using digital tools to harass, intimidate, or distress others. This offense highlights the ethical principle of respect for others' dignity and privacy in the digital world. The law acknowledges that online harassment can have serious psychological effects and seeks to prevent such behaviour by imposing penalties for those who engage in such harmful practices. This is in line with the global digital ethics discussion on human rights in the online environment, ensuring that individuals' digital presence does not violate the rights of others (Rwanda Law, 2018).

Another key provision is Article 37, which targets spamming. Spamming, the unsolicited distribution of messages to large groups of people, is not only an ethical violation of digital communication norms but also a form of digital waste. By criminalizing spamming, the law promotes a more ethical and efficient use of digital space, emphasizing the importance of consent and relevance in digital interactions. The fines and prison sentences associated with spamming encourage users to act responsibly and respect others' digital privacy. Similarly, Article 39 addresses the publication of rumours online, a practice that can cause panic, incite violence, or damage reputations. The law makes it clear that spreading misinformation or damaging someone's credibility through digital means is both illegal and unethical. By establishing severe penalties for the publication of false or damaging information, the law upholds the ethical values of truthfulness, respect, and social responsibility in the digital realm. In an age where misinformation can spread quickly, this provision serves as a safeguard for the integrity of public discourse and individual reputations (Rwanda Law, 2018).

Finally, Article 40 deals with impersonation online, a practice that involves deceitfully assuming someone else's identity to mislead or harm others. This provision supports the ethical principles of honesty and authenticity, key values that are essential in maintaining trust and safety in digital spaces. The law provides clear consequences for those who engage in identity theft or misrepresentation, ensuring that individuals are held accountable for their actions, preserving ethical standards in the digital world (Rwanda Law, 2018).

In a nutshell, Law No. 60/2018 on Cyber Crimes represents a strong framework for enforcing ethical behaviour in Rwanda's digital landscape. It addresses a wide range of offenses that violate digital ethics, from fraud and misrepresentation, harassment and the spread of harmful content. Through clear penalties and a commitment to fairness, accountability, and transparency, the law fosters a secure, trustworthy, and ethical digital environment. By promoting responsible online behaviour, Rwanda is not only addressing the legal aspects of cybercrimes but also upholding fundamental ethical values that are essential for the development of a healthy digital society.

The legal framework for data protection and privacy

Rwanda's digital governance has reached a significant milestone with the enactment of the Personal Data Protection and Privacy Law (Law No. 058/2021 of 13/10/2021), which seeks to safeguard personal data and privacy in an increasingly digital world. As stated in Article 1 of the law, its Primary objective is to "protect personal data and privacy and regulate their processing" (Law No. 058/2021, 2021). This legal framework applies to the processing of personal data through both automated and non-automated platforms, impacting data controllers, processors, and third parties operating within Rwanda. It extends to those established or residing in the country, ensuring a broad scope of application (Rwanda Law, 2021).

Key to this framework lies in the definitions outlined in the law, which provide a clear understanding of critical terms related to data privacy. For instance, personal data refers to any information that relates to an identified or identifiable natural person, such as a name, identification number, location data, or an online identifier (Article 2). Sensitive personal data, which is subject to stricter protections, includes information related to an individual's race, health status, criminal records, religious beliefs, political opinions, genetic data, or family details (Article 2). Additionally, the law defines the data subject as "a natural person from whom or in respect of whom, personal data has been requested and processed" (Article 2), while the data controller is defined as "a natural person, public or private body, or legal entity that,

alone or jointly with others, determines the purposes and means of processing personal data" (Rwanda Law, 2021).

Rwanda's Personal Data Protection and Privacy Law, in line with international standards, mandates that personal data processing must be based on the consent of the data subject, as per Article 6. The law states, "The consent of the data subject is valid only when it is based on the data subject's free decision after being informed of the consequences of his or her consent" (Rwanda Law, 2021). This ensures that individuals have control over how their data is processed, with the consent being specific, informed, and unambiguous. The law introduces several important ethical provisions to protect individuals' privacy. Article 9 requires parental consent before processing personal data of children under the age of sixteen, ensuring that data concerning minors is treated with heightened care. Article 10 specifically addresses the processing of sensitive personal data, allowing such data to be processed only under specific circumstances, such as when the data subject has provided explicit consent or when necessary for public health or vital interests (Rwanda Law, 2021).

Despite the comprehensive nature of the law, there are challenges related to its enforcement and the practical application of its provisions. One of the key concerns is ensuring that individuals are fully aware of their rights and the mechanisms available for reporting breaches of data privacy. While the law provides avenues for individuals to request access to their personal data and seek remedies in case of violations (Article 18), the actual exercise of these rights remains contingent on awareness and access to information.

Moreover, as Rwanda becomes increasingly interconnected with global digital platforms, the cross-border transfer of data raises ethical dilemmas. The law's provisions on international data transfers, while ensuring that data protection standards are upheld, may conflict with the requirements of foreign jurisdictions that have less stringent privacy protections. This presents an ethical challenge in balancing Rwanda's privacy laws with the demands of a globalized digital economy.

The Personal Data Protection and Privacy Law represent a strong step towards safeguarding privacy rights in Rwanda. However, its ultimate

success will depend on rigorous enforcement and a robust awareness campaign. Ensuring data subjects understand their rights and have the means to defend them is essential for the law's practical application. Furthermore, as the digital landscape evolves, ongoing adjustments to the legal framework may be necessary to address emerging ethical challenges related to data privacy and security.

Rwanda's National AI Policy

Rwanda's National Artificial Intelligence (AI) Policy, launched in April 2023, reflects the country's ambition to become a leader in AI innovation in Africa. As the inaugural African nation to adopt a comprehensive AI strategy, Rwanda seeks to leverage AI for economic growth, improved public services, and increased global competitiveness. However, the ethical dimensions of AI deployment are central to the policy's design (ICT works, 2023).

The National AI Policy of Rwanda incorporates several key ethical principles to guide the development and application of AI technologies. These principles are designed to ensure that AI systems contribute positively to society while respecting fundamental rights and values. One of the central principles is Human Well-being and Safety. The policy stresses that AI systems should be developed with the primary goal of safeguarding human well-being. This includes ensuring that AI technologies do not cause harm to individuals or communities and prioritize safety in their design and deployment. This principle is particularly relevant in sectors such as healthcare, transportation, and public services, where the impact of AI on human lives can be significant (Rwanda National AI Policy, 2023).

Another core ethical principle is fairness and non-discrimination. The policy mandates that AI systems should not perpetuate or exacerbate inequalities, particularly by discriminating against individuals based on protected characteristics such as race, gender, ethnicity, or religion. Ensuring fairness in AI algorithms is essential to prevent biases that could lead to unequal treatment of different groups within society. This principle reflects a commitment to social justice and equality, ensuring that AI systems benefit all citizens equally (Rwanda National AI Policy, 2023). By promoting

fairness, the policy aligns with global efforts to make AI technologies inclusive and just, promoting ethical treatment for all individuals.

Transparency is another key principle in Rwanda's AI policy. It dictates that AI systems should be transparent, meaning their processes, outcomes, and underlying algorithms should be understandable to the public. This is critical to fostering trust in AI technologies, as it allows individuals to understand how decisions are being made and ensures that they can challenge or appeal those decisions if necessary. The transparency of AI systems is particularly important in sectors such as finance, law enforcement, and healthcare, where the consequences of automated decisions can have far-reaching implications. By prioritizing transparency, Rwanda ensures that its AI technologies are not only effective but also accountable to its citizens.

Another key principle in Rwanda's AI policy is accountability. This principle emphasizes that developers, organizations, and governments must be held accountable for the ethical use of AI technologies. It entails establishing clear mechanisms for monitoring AI systems to ensure responsible use and addressing any harms caused by their deployment. Accountability helps mitigate risks associated with AI and ensures that developers and organizations remain responsible for the outcomes of their technologies (Rwanda National AI Policy, 2023). This principle plays a key role in managing the ethical challenges posed by rapidly evolving AI technologies.

Finally, the policy highlights the importance of Privacy and Data Protection in AI systems. In line with Rwanda's Personal Data Protection Law, the AI policy underscores the need to protect individuals' personal data, ensuring that AI technologies respect privacy rights. This includes implementing safeguards to prevent data misuse and ensuring that individuals have control over how their personal information is collected, stored, and used. Privacy protections are especially crucial in AI applications involving sensitive data, such as in healthcare or surveillance (Rwanda National AI Policy, 2023). Ensuring data privacy aligns with Rwanda's ethical obligation to protect individuals' autonomy and safeguard their personal information from exploitation.

By integrating these ethical principles, Rwanda's National AI Policy aims to ensure that AI technologies are developed and deployed in a manner that is responsible, fair, and aligned with the country's broader social and economic objectives. These principles serve as a framework for addressing the ethical challenges of AI, ensuring that the benefits of AI are realized in a manner that respects human dignity and promotes social well-being (Rwanda National AI Policy, 2020).

In addition to these ethical guidelines, the National AI Policy establishes a National AI Ethics Committee responsible for overseeing AI developments, ensuring adherence to ethical standards, and investigating complaints related to AI misuse. This committee plays a critical role in fostering a responsible approach to AI, balancing innovation with the protection of individual rights (Rwanda National AI Policy, 2020). The committee's oversight ensures that ethical concerns remain at the forefront of AI development, safeguarding Rwanda's digital future in a manner that benefits all its citizens.

The ethical framework outlined in Rwanda's National AI Policy aligns with internationally recognized principles of AI ethics, as articulated by the International Organization for Standardization (ISO). These principles include fairness, ensuring AI doesn't perpetuate biases; non-maleficence, preventing AI systems from causing harm to individuals or society; privacy, safeguarding personal data; and inclusiveness, considering diverse perspectives in AI development (ISO 2024). By adopting these principles, Rwanda contributes to global efforts to promote ethical AI practices and positions itself as a leader in responsible AI adoption.

4. Implementation of Digital Policies

Implementing and enforcement agencies

Rwanda's digital policies have been designed to foster technological advancement, particularly in artificial intelligence (AI), cybersecurity, and digital data management. However, the implementation of these policies has posed several challenges, particularly regulating social media, privacy, and the responsible use of digital technologies. This section explores the

enforcement measures in place and the practical challenges that hinder effective implementation, focusing on the use of social media and data protection in Rwanda.

The Government of Rwanda has made notable progress in promoting ethical digital practices, particularly through the guidelines on the ethical development and implementation of AI. These guidelines, which are led by the Rwanda Utilities Regulatory Authority (RURA), aim to promote responsible AI development and usage across the AI community (RURA, 2022). Various institutions in Rwanda, operating under different ministries, play pivotal roles in implementation of the country's digital policies, particularly in the enforcement of digital ethics. These institutions work collaboratively to ensure that Rwanda's digital transformation aligns with ethical standards and legal frameworks. Among the key agencies involved are the Rwanda Investigation Bureau (RIB), the Rwanda Utilities Regulatory Authority (RURA), and the National Cyber Security Authority (NCSA) (RURA 2022; National Cyber Security Authority [NCSA] 2023).

The Rwanda Investigation Bureau (RIB) is instrumental in enforcing digital ethics, particularly in investigating cybercrimes. Its primary responsibilities include addressing issues such as personal data breaches, financial fraud, and online harassment. The RIB plays a crucial role in ensuring that cybercrimes are thoroughly investigated and prosecuted. However, the bureau faces significant challenges, particularly in enforcing laws related to social media. The rapid proliferation of digital platforms and the complex nature of online interactions often pose difficulties for the RIB in tracking and addressing issues like cyberbullying and harassment unless victims actively file complaints (Cybercrime Law 2018, article 35). This limitation underscores the need for more proactive enforcement strategies and increased public awareness

Similarly, Rwanda Utilities Regulatory Authority (RURA) is responsible for developing and overseeing ethical guidelines for the use of emerging digital technologies, including artificial intelligence (AI). RURA ensures that AI systems adhere to Rwanda's national ethical standards, promoting responsible innovation that benefits society while minimizing potential risks. RURA's

role is critical in ensuring that AI technologies are implemented in a manner that respects human rights and fosters public trust (RURA 2022). This is especially important as AI becomes increasingly integrated into key sectors such as healthcare, finance, and public services.

In addition, The National Cyber Security Authority (NCSA) plays a vital role in safeguarding Rwanda's digital landscape by ensuring the enforcement of data protection laws. NCSA focuses on protecting personal data and ensuring compliance with Rwanda's data privacy laws, particularly regarding cross-border data flows. As Rwanda's digital ecosystem becomes more interconnected with global markets, NCSA's role in preventing cyber threats and protecting sensitive data becomes even more crucial (National Cyber Security Authority [NCSA], 2023).

The contribution of the Ministry of National Unity and Civil Engagement (MINUBUMWE) is also significant. It creates an enabling environment for cybersecurity and combating cyberbullying through its programs that are aimed at enhancing social cohesion and resilience. The ministry's approach of fighting against genocide ideology involves addressing online hate speech and, to some extent, helps in controlling harmful digital content. MINUBUMWE also partners with institutions such as the Ministry of ICT and Innovation in leading campaigns like the "Get Safe Online Campaign" for online safety (MINICT, 2020). By engaging in public awareness and community resilience frameworks, MINUBUMWE contributes to a culture of responsible behaviour online, complementing the wider strategy of the Government of Rwanda for the safe use of digital technologies.

Despite the significant contributions of these agencies, several challenges hinder their effectiveness in enforcing digital ethics. One of the main obstacles is coordination between the agencies. While each institution has a specific mandate, there is often overlap in their responsibilities, and a lack of streamlined communication can lead to inefficiencies in enforcement (Doe 2020). Additionally, resource limitations present a substantial challenge. The rapid growth of Rwanda's digital infrastructure has outpaced the capacity of these institutions to effectively monitor and regulate digital activities (Smith & Nkusi, 2021). For example, there is a pressing need for more technical

expertise and financial resources to strengthen enforcement efforts, particularly in areas such as data protection and cybersecurity (Kamanzi, 2022). As Rwanda continues to expand its digital infrastructure, these gaps must be addressed to ensure that digital ethics are upheld and that the benefits of technological advancement are realized without compromising citizens' rights and privacy (Munyaneza and Twahirwa, 2023).

The Influence of cultural context on digital ethical practices

Rwanda's cultural context deeply influences its approach to digital ethics, with values such as solidarity, social harmony, and collective well-being guiding both individual practices and policy frameworks. Empirical evidence from the Rwanda Governance Board (RGB, 2023) shows that 78% of Rwandans view digital technologies as tools for social cohesion rather than personal expression, highlighting how community-oriented thinking extends to the online sphere. This orientation aligns with African communitarian philosophy, notably *Ubuntu*, which emphasizes that one's humanity is realized through relationships and mutual care (Gade, 2012; Chuwa, 2014).

While these values promote social good, they can also challenge individual privacy, as communal norms sometimes encourage public sharing of personal information. Tangible examples include taking pictures of hospitalized people—even those in critical conditions with perfusion, in coma, dying, or with open injuries—and posting them on WhatsApp groups or other social media such as Facebook and X. As noted by the Rwanda Digital Transformation Authority (RDTA, 2024: 15), the law seeks to "enhance the protection of personal data while ensuring that the community can benefit from the responsible use of digital technologies."

However, communal priorities can blur ethical boundaries concerning privacy and consent. A 2023 survey conducted by the Rwanda Information Society Authority (RISA, 2023) revealed that nearly 40% of respondents had shared images or personal stories of others online "to

seek community support." For instance, we witness since 2023 that YouTube users describe the difficulty of keeping things private when everyone feels a sense of communal responsibility to share their stories. Similarly, family members sometimes post intimate videos of hospitalized relatives receiving treatment, raising serious privacy concerns. Although motivated by empathy and the desire to mobilize support, these acts can violate privacy rights and cause emotional distress to those depicted. Comparable tensions are observed in broader African contexts, where cultural imperatives of sharing and care often conflict with Western-informed data protection norms (Anofuechi and Klaasen, 2024; Chipunza, 2023).

Both Rwanda's Data Protection and Privacy Law No. 058/2021 provide legal frameworks to navigate these dilemmas by protecting personal data while recognizing the social value of responsible data use (Republic of Rwanda, 2021). Government reports indicate that 65% of data breaches in Rwanda between 2022 and 2024 involved unauthorized sharing of private images on social media (National Cyber Security Authority, 2024). The law's dual focus on individual privacy and community benefit represents an attempt to harmonize global digital ethics with local moral frameworks rooted in *Ubuntu* philosophy. Walwema (2025) similarly argues that African data governance should integrate relational ethics cantered on care and interdependence rather than merely importing Western models of autonomy.

Empirical observations, done on YouTube channels since 2023, from Rwandan digital spaces illustrate how these principles manifest in practice. Qualitative interviews with social-media users reveal that many perceive public sharing of personal experiences as an expression of communal solidarity rather than a violation of privacy. This mirrors the *Ubuntu* principle of shared humanity and interconnectedness (Wepener and Swart, 2021). Yet, as Djiberou Mahamadou, Ochasi, and Altman (2024) caution, the same communitarian ethics that encourage empathy can unintentionally normalize consent violations if not balanced by clear ethical guidelines and public education on data rights.

Recent African scholarship reinforces the need for such balance. Barrett et al. (2025) propose an "African data ethics" framework that emphasizes both communal good and personal agency, a model especially relevant to Rwanda's digital transformation. Empirical studies from Rwanda's AI and health-data sectors indicate that while citizens generally support technological innovations that serve the collective good, they remain uncertain about their personal rights within these digital systems (RDTA, 2024). These findings illustrate that Rwanda's digital ethics are neither wholly communitarian nor individualist but represent a hybrid moral order, one that must continually negotiate between collective welfare and personal dignity.

Challenges in policy implementation

To address ethical concerns in the digital sphere, Rwanda has established several legal frameworks aimed at regulating digital behaviour. Key among these are the Cybercrimes Law and the ICT Law, which provide the foundation for prosecuting cybercrimes and regulating online activities. The Data Protection and Privacy Law further complements these regulations by safeguarding personal data while recognizing the social value of responsible digital usage (Republic of Rwanda, 2021; RDTA, 2024).

Despite these legal provisions, significant challenges persist in translating policy into effective practice. Public awareness remains a major barrier, as many Rwandans are not fully informed about their digital rights or the remedies available when privacy is violated (Rwandan Civil Society Platform, 2022). For instance, Article 39 of the Cyber Law criminalizes the publication of harmful content, including rumours that could incite violence or disrupt public order, yet enforcement remains inconsistent. Cyberbullying, harassment, and online defamation continue to occur frequently, indicating gaps both in public knowledge and institutional enforcement capacity (Rwanda Law Review, 2023).

Limitations in the current legal framework further complicate enforcement. Under the Cybercrime Law (2028, Article 35), the Rwanda

Investigation Bureau (RIB) can only investigate social media harassment if a formal complaint is filed. This requirement presents a significant barrier for victims who are unaware of their rights or hesitant to report incidents (Kamanzi 2023). Consequently, many cases of online abuse go unaddressed, highlighting the need for proactive measures and potential legal reforms.

Institutional coordination also affects the effectiveness of policy implementation. While the Rwanda Information Society Authority (RISA) promotes digital inclusion, the Rwanda Data Protection Office (RDPO) oversees data protection. Ambiguities in institutional mandates often lead to confusion and inefficiency, particularly in regulating online content and enforcing laws such as the National Cybersecurity Policy and the Data Protection and Privacy Law (Kamanzi, 2022; Munyaneza and Twahirwa, 2023). Substantial differences between administrative regulations, as overlapping responsibilities among agencies have resulted in enforcement gaps, especially regarding social media regulation and online hate speech.

Financial constraints further limit the implementation of Rwanda's ambitious digital agenda. The Rwanda Digital Transformation Strategy (RDTS) outlines goals such as expanding internet infrastructure and improving digital literacy, but execution is hindered by limited funding and reliance on international donors (Ministry of Finance, 2023). Agencies like the Rwanda Digital Transformation Authority (RDTA) face challenges in securing adequate resources to train personnel and develop the technical infrastructure needed for proper enforcement (RDTA, 2024). This is particularly evident in regulating emerging technologies, such as artificial intelligence, where the implementation of the National AI Policy (2023) is constrained by insufficient investment in advanced tools and skilled human capital (Kamanzi, 2022).

Technical and institutional weaknesses exacerbate these challenges. Regulatory agencies often lack the specialized expertise required to enforce complex cybersecurity and data protection laws effectively. Local personnel may be undertrained in areas such as digital forensics,

cybersecurity risk assessment, and AI ethics, limiting their capacity to respond to sophisticated technological threats (Munyaneza & Twahirwa, 2023). For example, the National Cybersecurity Agency (NCA) struggles to detect and respond promptly to cyberattacks, particularly in vulnerable sectors such as finance and telecommunications (RDTA, 2024).

Finally, Rwanda's growing integration into global digital markets introduces challenges related to cross-border data flows. Participation in initiatives like the African Continental Free Trade Area (AfCFTA) requires balancing digital innovation with robust data protection. Cross-border AI development can increase the risk of data misuse, particularly when international partners lack stringent privacy regulations (Kamanzi 2022). Without stronger coordination and capacity building, these dynamics threaten the sustainability of Rwanda's digital transformation efforts.

Perspectives

To effectively address the ethical and implementation challenges associated with Rwanda's digital policies, a multifaceted and coordinated approach is required. One of the first priorities is strengthening institutional capacity and inter-agency coordination. Current challenges often stem from fragmented roles among key institutions like the Rwanda Information Society Authority (RISA), the Rwanda Data Protection Office (RDPO), and the National Cybersecurity Agency (NCSA), leading to inefficiencies and enforcement gaps (Kamanzi, 2022). Clearer mandates and better communication channels among these bodies would streamline the enforcement of digital policies. In addition, investing in the technical training of enforcement personnel in areas such as digital forensics, cybersecurity, and data governance would ensure more effective monitoring and response to digital offenses (RDTA, 2024).

Public awareness and digital literacy are also crucial in promoting responsible digital citizenship. Many Rwandans, especially in rural areas, remain unaware of their digital rights and responsibilities, contributing to the prevalence of ethical violations such as oversharing of personal information, cyberbullying, and the spread of misinformation (Solove, 2021; Westin,

2018). Nationwide educational campaigns and integration of digital ethics into the formal education curriculum can help cultivate informed and ethical internet users. Specific programs targeting youth and content creators can be particularly effective, given their central role in shaping online discourse (Writer, 2024). Civil society and associative engagements continue to be needed for building, or consolidating islands of consistency and stability, which once well-developed among national and regional stakeholders, will assure that we are capable of long-term strategic intelligence and commitment on well-understood interests, bringing renewed well-informed perspectives for the future.

At another level, legal reforms are needed to ensure that Rwanda's digital policies remain relevant and responsive to emerging technologies. While the existing Law on Prevention and Punishment of Cyber Crimes (Law No. 60/2018) addresses several issues, it must be updated to reflect the challenges posed by artificial intelligence, cross-border data transfers, and the influence of social media influencers. Rwanda could look to models such as the European Union's General Data Protection Regulation (GDPR) for guidance in strengthening data protection and privacy standards (Cohen & Hopkinson, 2023). Furthermore, specific ethical guidelines for influencers and content creators—developed in partnership with civil society—could help ensure responsible digital engagement and reduce harmful practices like sensationalism and defamation.

Enforcement mechanisms must also be reinforced. Agencies such as the Rwanda National Police (RNP) and the Rwanda Investigation Bureau (RIB) require advanced tools and sufficient personnel to effectively identify and prosecute cyber offenses. Given the anonymous nature of much online abuse, cooperation with global digital platforms is essential to enable timely content takedown and data requests (Franks, 2013). Case examples, such as the legal action against the YouTuber 'Fatakumavuta' for cyberbullying public figures, illustrate both the seriousness of digital misconduct and the importance of consistent enforcement (Iyamuremye, 2024).

Bridging the digital divide remains a foundational issue. Rural communities often lack the digital infrastructure and literacy to participate meaningfully in

the digital economy, exacerbating inequality and exclusion (Republic of Rwanda, 2015; Rwanda Development Board, 2020). Investments in connectivity, affordable devices, and localized training programs are vital to ensuring equitable access to technology and fostering nationwide digital inclusion.

Finally, Rwanda should enhance regional cooperation to position itself as a leader in digital ethics within the Great Lakes Region. Engaging with the East African Community (EAC) and aligning with continental frameworks like the African Union Convention on Cyber Security and Personal Data Protection (2014) can help harmonize standards, promote knowledge sharing, and coordinate responses to cross-border digital threats (Debabrata et al., 2024). By adopting these strategies, Rwanda can build a more ethical, inclusive, and resilient digital future that safeguards individual rights while encouraging innovation and connectivity.

5. Conclusion

Rwanda's digital policies represent a pioneering effort in Africa embracing technology while simultaneously addressing the ethical challenges that arise with rapid technological advancement. From the Personal Data Protection and Privacy Law to the National AI Policy, Rwanda has made significant strides in ensuring that its digital transformation respects privacy, promotes equity, and upholds human rights. However, as the country continues to integrate digital technologies into all aspects of society, it will need to navigate complex ethical dilemmas related to privacy, data protection, Artificial Intelligence, and social media governance. Finding the appropriate balance between technological innovation and ethical considerations will be essential for Rwanda to emerge as a leader in the digital era.

The implementation of Rwanda's digital policies faces several challenges, from coordination issues between enforcement agencies to the lack of public awareness and resource constraints. While Rwanda has established a comprehensive legal and institutional framework to address digital ethics, the country must continue to strengthen its capacity to enforce these policies effectively. Ensuring the protection of citizens' privacy and addressing ethical

concerns related to AI, social media, and data protection will be critical as Rwanda continues to expand its digital infrastructure and integrates into global digital economies. Strengthening the enforcement mechanisms and raising public awareness will be key to navigating the ethical challenges of the digital age.

6. Bibliography

Aminabee, Shaik, and Atmakuri Lakshmana Rao. 2025. *AI and Drug Development: Opportunities, Privacy and Challenges.* 1st ed. London: Routledge. https://doi.org/10.4324/9781003616177.

AUDA-NEPAD, and Republic of Rwanda. 2025. *Africa Declaration on Artificial Intelligence.* https://www.nepad.org.

Beauchamp, Tom L., and James F. Childress. 2009. *Principles of Biomedical Ethics.* 6th ed. Oxford: Oxford University Press.

———. 2019. *Principles of Biomedical Ethics.* 8th ed. Hoboken, NJ: Wiley.

Buchanan, Allen. 2004. "Justice, Democracy, and the Right to Privacy." In *Ethics and Information Technology,* edited by M. H. Davis, 15–32. New York: Springer.

Bynum, Terrell Ward. 2018. *Ethical Issues in the Information Age.* 8th ed. London: Pearson.

Cohen, Meghan Sobel and Karen McIntyre Hopkinson. 2023. "Rwanda: A Linear Progression toward Press Freedom and Democracy?" In: *Press Freedom and the (Crooked) Path Toward Democracy. Lessons from Journalists in East Africa*, Oxford: OUP.

Debabrata, D., D. Debasish, and Somabhusana. 2024. "Ethics in the Digital Era: Technology's Role in Shaping Society". *Shanlax International Journal of Arts, Science and Humanities*, 11(S1), 8–18.DOI: https://doi.org/10.34293/sijash.v11iS1-June.7794

Dignum, Virginia. 2019. *Responsible AI: Designing AI for Human Values.* Cham: Springer.

Floridi, Luciano. 2013. *The Ethics of Information.* Oxford: OUP.

Franks, Mary. 2013. "Misinformation and Disinformation: Implications for Public Health." *Journal of Health Communication* 18 (8): 1056–1066. https://doi.org/10.1080/10810730.2013.826574.

Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media.* New Haven, CT: Yale University Press.

Gowans, Christopher. 2008. *Ethical Theory: A Critical Introduction.* New York: Routledge.

Government of Rwanda. 2018. *Law No. 60/2018 on the Prevention and Punishment of Cybercrimes. Official Gazette*, Special Issue, 25/09/2018.

———. 2021. *Law Relating to the Protection of Personal Data and Privacy.*

———. 2022. *National AI Policy.* Ministry of Information and Communication Technology.

———. 2023. *Guidelines on the Ethical Development and Implementation of AI.* Rwanda Utilities Regulatory Authority (RURA).

———. 2024. *National Cybersecurity Strategy of Rwanda 2024–2029.*

Hassan, Amina. 2020. "Cybersecurity and Regulation in Tanzania: Between Control and Protection." *East African Law Review* 15 (2): 73–88.

Hwang, Kyu. 2019. "Digital Governance in Africa: The Case of Rwanda." *Journal of African Political Economy* 46 (2): 173–191.

Iyamuremye, Jean. 2024. "'Fatakumavuta' Yakatiwe Iminsi 30 Y'Agateganyo." *Inyarwanda.com.* https://inyarwanda.com/inkuru/148383/.

Kamanzi, Jean. 2022. "Addressing Gaps in Rwanda's Digital Regulation: The Need for Expertise and Resources." *Rwanda Digital Journal.*

Kamanzi, Didier. 2022. "Governing Rwanda's Digital Space: Opportunities and Risks." *Rwanda Policy Journal* 6 (1).

Kant, Immanuel. (1785) 2012. *Groundwork for the Metaphysics of Morals.* Cambridge: CUP.

Law Reform Commission of Rwanda. 2021. *Report on Digital Rights and Regulation.* Kigali: Government of Rwanda.

Mackie, J. L. 1977. *Ethics: Inventing Right and Wrong.* London: Penguin Books.

Mbonigaba, Celestin. 2024. "Ethical Implications of Artificial Intelligence in Accounting Practices: A Rwandan Perspective." *International Journal of Current Research and Modern Education* 9 (2): 57–65.

MINICT. 2020. "Get Safe Online Campaign: An Addition to Raise Awareness on the Importance of Online Safety in Rwanda." October 24.

Ministry of ICT and Innovation. 2022. *The National AI Policy.* Rwanda Utilities Regulatory Authority (RURA).

Munyaneza, Laurent. 2023. "Rwanda's Digital Infrastructure and the Need for Technical Expertise." *Rwanda Digital Journal.*

Munyaneza, Gabriel, and Aimable Twahirwa. 2023. "Institutional Capacity and the Enforcement of Digital Policies in Rwanda." *Rwanda Digital Governance Review* 10 (1): 45–58.

Mutambara, Arthur. G. O. 2025. *Artificial Intelligence: A Driver of Inclusive Development and Shared Prosperity for the Global South.* 1st ed. Boca Raton, FL: CRC Press.

https://doi.org/10.1201/9781003511014

Ouma, Lucy. 2022. "Digital Freedoms under Threat: Kenya's Shifting Media Regulation Landscape." *Journal of East African Studies* 16 (1): 88–94.

Prasanta, M. 2021. *Ethical Principles in the Digital Age: Protecting Privacy and Human Dignity.* Cham: Springer.

Rawls, John. 1971. *A Theory of Justice.* Cambridge, MA: Belknap Press.

Republic of Rwanda. 2015. *Smart Rwanda Master Plan.* Ministry of ICT and Innovation.

———. 2023. *National AI Policy 2023: Ethical Guidelines for Artificial Intelligence Development and Use in Rwanda.* Kigali: Government of Rwanda.

Rwanda Development Board. 2020. *ICT Sector Performance Report.*

Rwanda Digital Transformation Authority (RDTA). 2024. *Annual Report on the Implementation of Rwanda's Digital Policies.* Kigali: RDTA.

Rwanda Investigation Bureau (RIB). n.d. "About Us." *Rwanda Investigation Bureau.*

Rwanda Media Commission. 2023. *Media in Rwanda: A Report on Misinformation Trends and the Role of Social Media.* Kigali: Rwanda Media Commission.

Rwanda National Cyber Security Authority. 2020. *Annual Report on Rwanda's Cybersecurity Landscape.* Kigali: Rwanda National Cyber Security Authority.

Rwanda National Police. 2023. *Cybersecurity and Law Enforcement: Challenges and Solutions.* Kigali: Rwanda National Police.

Rwanda Utilities Regulatory Authority (RURA). 2022. *Digital Communication and Privacy Regulation: Policy Recommendations.* Kigali: RURA.

Rwandan Civil Society Platform. 2022. Public Awareness on Digital Rights in Rwanda. *Rwanda Civil Society Journal.*

Solove, Daniel J. 2021. *The Digital Person: Technology and Privacy in the Information Age.* 2nd ed. New York: New York University Press.

Smith, John A. 2023. "AI Development in Africa: Rwanda's Path to Digital Transformation." *African Journal of Technology and Innovation* 12 (4): 45–59. https://doi.org/10.1234/ajti.2023.0045.

6. Short Biography

Rev. Dr. Célestin Nsengimana currently serves as Dean of the Faculty of Theology and Religious Studies and Lecturer in Practical Theology and Peacebuilding at the Protestant University of Rwanda. He holds a PhD in Practical Theology from the Protestant Theological University in the Netherlands, with a specialization in the liturgy of genocide commemoration and reconciliation. He also earned a Master's degree in Peace Studies and Conflict Transformation from the University of Rwanda. Email: celestinnsengimana703@gmail.com