The Role of ICT in Advancing Freedom of Information, Innovation, and Market Dynamics: Balancing Rights, Access, and Regulation

Leah Kahunde, PhD in Communication, University of Nairobi
Collince Okumu, PhD in Communication, Multimedia University of Kenya
DOI: 10.5281/zenodo.21051394

Abstract

Information and Communication Technology (ICT) has fundamentally transformed the production, dissemination, and utilization of information, reshaping governance, economic development, education, communication, and innovation worldwide. While ICT has enhanced access to information, promoted freedom of expression, facilitated knowledge sharing, and stimulated technological innovation, it has also introduced complex challenges relating to digital censorship, misinformation, privacy, cybersecurity, intellectual property rights, market concentration, and ethical governance. This paper critically examines the multifaceted role of ICT in advancing freedom of information, media freedom, intellectual property protection, competition and antitrust regulation, privacy and security, and knowledge creation within the contemporary digital ecosystem. Drawing on global and Kenyan examples, the paper synthesizes existing literature to evaluate both the opportunities and risks associated with increasing ICT adoption. It argues that although ICT has become an indispensable driver of innovation, economic growth, civic participation, and social transformation, its benefits can only be fully realized through balanced regulatory frameworks that safeguard fundamental rights while promoting innovation, fair competition, and digital inclusion. The paper concludes that achieving sustainable digital development requires collaborative efforts among governments, the private sector, civil society, and international institutions to strengthen digital governance, bridge the digital divide, enhance cybersecurity, and promote the ethical development and deployment of emerging technologies such as artificial intelligence.

Keywords: Information and Communication Technology (ICT), Digital Governance, Intellectual Property Rights, Cybersecurity, Digital Privacy.

Introduction

Information and Communication Technology (ICT) refer to the diverse set of technological tools and resources used to communicate, create, disseminate, store, and manage information (Halich, 2023). Various aspects of human life have been revolutionized ranging from defying geographical, social and physical constraints to building social connections and relationships by facilitating social communication, connectivity, social inclusion, information sharing and civic engagement, as individuals can now access and share information more easily (Vasylchyshyn, 2023: Rizqi, 2023; Shtukareva, 2020).

ICT has also had a transformative impact on governance through use of e-government initiatives like e-citizen in Kenya through which governments can improve reach, service delivery and citizen participation in governance (Gojayeva et al., 2021). Mutisya (2020) also underscores the role ICT integration plays in economic growth and development as a modern and multifunctional infrastructure, enabling socio-economic progress and strengthening intellectual and human potential thereby increasing efficiency, productivity, and innovation. The education sector has also benefited from ICT as it has helped to narrow educational disparities through transforming teaching and learning experiences, fostering, student engagement and teacher professional development. (QUIMBO, 2023; Kumar, 2023)

This paper seeks to evaluate the role of ICT's role in Freedom of information, free expression, media freedom, intellectual property rights, competition and antitrust, privacy and security in advancement of knowledge and innovation;

Freedom of Information and ICT

Freedom of Information is the fundamental right of individuals to access information held by public authorities, promoting transparency, accountability, and public participation in governance. It allows people to seek, receive, and share information across media, as recognized by international instruments like the Universal Declaration of Human Rights (Sobel, 2020; Santy, 2024). While essential for democracy, this right is not absolute and can be restricted to safeguard national security, privacy, or commercial interests, provided such limitations are lawful, necessary, and proportionate (Šmigová, 2022).

ICT plays a vital role in facilitating the global flow of information by leveraging tools and platforms that connect individuals, organizations, and governments worldwide.
The internet, as a foundational component of ICT, has created a global network for instantaneous sharing of information, resources, and data across borders (Roland-Holst et al., 2022; Yang et al., 2020). Open data initiatives, which promote the free and unrestricted sharing of data, have further enhanced transparency and accessibility on a global scale (Clobridge, 2010; Roland-Holst et al., 2022).

ICT has also fostered global collaboration through tools such as video conferencing, cloud computing, and social media, enabling the exchange of knowledge and best practices across diverse fields (Yang et al., 2020; Iqbal et al., 2022). It has also increased access to educational resources and information, empowering individuals to engage in self-directed learning and research. Also supported global trade and commerce by streamlining supply chains, facilitating cross-border transactions, and contributing to economic growth (Billón et al., 2023; Juhász & Steinwender, 2018; Pérez-López et al., 2019).

However, the global flow of information facilitated by ICT faces several challenges, including digital censorship, unequal access, and the proliferation of misinformation.

Digital Censorship: Governments, both democratic and authoritarian, increasingly employ digital tools to control and restrict online information through methods such as website blocking, social media monitoring, and targeted surveillance (Franke, 2012; Meserve & Pemstein, 2020; Luo & Li, 2022). This censorship often creates a "chilling effect," discouraging users from freely expressing themselves due to fear of repercussions (Büchi et al., 2022). Interestingly, some studies suggest that censorship can have unintended consequences, as users often find ways to bypass restrictions, inadvertently increasing access to censored information (Hobbs & Roberts, 2017).

Unequal Access: The benefits of ICT remain unevenly distributed, favoring wealthier individuals and enterprises over marginalized groups. Infrastructure deficits, high costs, and limited digital literacy in developing regions exacerbate this disparity, hindering equitable access to ICT and the information it provides (Donner & Escobari, 2010).

Misinformation: ICT's capacity for rapid information sharing has also facilitated the spread of misinformation and disinformation, which can polarize societies and threaten democratic processes. Governments sometimes exploit the issue of misinformation as a pretext for imposing stricter digital censorship and surveillance measures (Vasist & Krishnan, 2022).

These challenges highlight the dual role of ICT as both a tool for enhancing access to information and a mechanism that can be misused to undermine democratic values and individual rights (Franke, 2012; Mirzoyan, 2023).

Free Expression and Media Freedom

Free expression is the principle that supports the freedom of an individual or a community to share their opinions, ideas, and information without fear of legal censorship. It is fundamental right that is intrinsically linked to freedom to information given that the ability to access information underpins the right to share ideas and opinions, while the free exchange of ideas ensures the circulation of information necessary for transparency and accountability in governance (Sobel, 2020; Momen, 2020)

Media freedom is implicitly defined by Leeson (2008) through its antithesis, government control or influence over the flow of information. As such, media freedom refers to the absence of direct or indirect governmental control

over media outlets, enabling them to operate independently and present information to the public without coercion or manipulation. Leeson cites examples such as monopolized media ownership and financial pressure, which suggest that media freedom entails the autonomy of media to disseminate diverse and unbiased information to citizens.

The role of Information and Communication Technology (ICT) in fostering free expression and citizen journalism can be explored through both global and Kenyan examples, highlighting its transformative impact on communication, activism, and accountability.

Globally, the Arab Spring uprisings (2010–2011) illustrate how ICTs, particularly social media platforms, enabled citizens to organize protests and share real-time news, images, and videos, drawing international attention to the events across the Middle East and North Africa (Blagojević & Šćekić, 2021). Similarly, during the Occupy Wall Street movement in 2011, ICTs facilitated "connective action" by allowing individuals to express dissent and rally around a unifying message such as "We are the 99 percent," using digital tools for self-mobilization and global outreach (Hopke, 2016).

In Kenya, ICTs have also played a critical role in empowering citizens. Mobile phones and social media platforms have facilitated citizen journalism, enabling individuals to report on issues like electoral violence and poor service delivery. Platforms such as Ushahidi have provided Kenyans with tools to crowdsource and disseminate information to a broader audience, fostering civic engagement and accountability (Ngwa, 2024). Moreover, civil society organizations in Kenya have leveraged ICTs to advocate for digital rights and freedom of expression, countering attempts to censor online content (Ngwa, 2024).

These examples underscore how ICTs have become indispensable in promoting free expression, amplifying citizen voices, and holding governments accountable, contributing to the advancement of democratic values and the global flow of information. The issues of digital surveillance, government crackdowns on online speech, and platform moderation represent significant challenges in the digital age, reflecting a delicate balance between security, free expression, and responsible regulation.

Digital Surveillance: Governments worldwide, regardless of their political systems, increasingly deploy digital tools to monitor online activities, often targeting dissidents and minority groups (Hargreaves, 2017; Marczak & Paxson, 2017). Such surveillance can create a "chilling effect," where individuals self-censor to avoid potential repercussions (Büchi et al., 2022). Interestingly, in some cases, abrupt censorship has led users to adopt alternative methods to access information, inadvertently boosting access rather than suppressing it (Hobbs & Roberts, 2017; King et al., 2013).

Government Crackdowns on Online Speech: Efforts to control online discourse include tactics like blocking websites, monitoring social media, and harassing activists and journalists (Hargreaves, 2017; Hashemi, 2020). While often justified as necessary for maintaining national security or public stability, such measures are frequently used to suppress dissent and silence criticism (King et al., 2013). Activists leveraging ICTs for organizing protests or mobilizing support have also faced government retaliation in the form of restrictive policies or repressive actions (Hashemi, 2020).

Platform Moderation: Social media platforms face growing pressure to combat disinformation, hate speech, and extremism, often through content moderation (Machado, 2023; Aaronson, 2018). However, overly aggressive moderation can raise concerns about censorship and the suppression of legitimate speech (Machado, 2023). Initiatives like the Global Network Initiative and Ranking Digital Rights aim to guide platforms in balancing content regulation with the protection of free expression and human rights (George, 2018).

These issues underscore the dual nature of ICTs: while they have empowered individuals to engage in activism and hold authorities accountable, they have also provided tools for digital repression. Addressing these challenges requires nuanced policies that safeguard digital rights while mitigating the misuse of online platforms.

Intellectual Property Rights (IPR)

Intellectual property (IP) rights refer to a set of legal protections granted to the creators of intellectual works,

such as inventions, literary and artistic works, designs, symbols, and trademarks used in commerce (Rout, 2018). These rights aim to incentivize innovation and creativity by allowing creators and inventors to benefit economically from their work while retaining control over its use (Kasmawati & Wiranata, 2023). The main categories of IP rights include patents, which protect new inventions; copyrights, which safeguard creative works like literature and software; trademarks, which distinguish goods and services; and trade secrets, which secure confidential business information (Rout, 2018; Brown, 2003). Recognized at both national and international levels, intellectual property rights promote economic growth and technological advancement, though they often spark debate due to potential conflicts with access to information and other fundamental human rights (Matthews, 2010; Bydoon, 2016).

ICT Influence on Intellectual Property Rights Enforcement and Innovation

The influence of Information and Communication Technology (ICT) on Intellectual Property Rights (IPR) enforcement and innovation can be understood through global and Kenyan contexts, demonstrating its dual role in both enhancing protection and fostering challenges.

Globally, the presence of Multinational Enterprises (MNEs) in developing countries has accelerated the adoption of stringent IPR frameworks, such as the TRIPS Agreement. MNEs often lobby for stronger IPR enforcement to lower transaction costs and safeguard their operations, thereby driving local governments to implement stricter regulations (Brandl et al., 2018). However, ICT has also facilitated software piracy, particularly in developing economies. While piracy remains a significant challenge, advancements in ICT and stronger IPR policies have been shown to reduce piracy rates and address broader socio-economic issues like inequality and poverty (Asongu, 2014).

In Kenya, ICT diffusion has contributed to the adoption and enforcement of IPR standards, influencing both legal frameworks and societal awareness (Gosebo & Rapea, 2015). Furthermore, the integration of ICT in education has been recognized as a key driver of innovation and creativity. The government's efforts to embed ICT in teaching and learning aim to equip students with the skills needed to develop new technologies and intellectual property. Despite challenges in infrastructure, teacher preparedness, and curriculum integration, ICT in education has significant potential to shape the future of innovation and IPR development in Kenya (Wambiri & Ndani, 2017; Pathak & Muralidharan, 2020).

These examples illustrate how ICT has become a critical factor in shaping IPR enforcement and innovation. While it has created challenges such as piracy, it also serves as a catalyst for adopting robust IPR frameworks and fostering technological creativity.

Balancing the Protection of Creators and Access to Knowledge

The interplay between protecting creators and enabling access to knowledge is a nuanced issue that demands careful consideration of competing interests. Intellectual property rights (IPRs), including copyrights, patents, and trademarks, are crucial for incentivizing creativity and innovation by granting creators exclusive rights to their works for a limited period (Kasmawati & Wiranata, 2023; Zhang & Ge, 2022). These rights allow creators to benefit economically from their efforts, encouraging further investment in creative and innovative pursuits.

However, overly stringent IPR frameworks can impede the free flow of information, which is vital for scientific progress, education, and cultural enrichment (Momen, 2020; Singh, 2017). Excessive protections may lead to monopolistic practices, inflated costs, and restricted access to knowledge, disproportionately affecting marginalized communities and developing nations (Kasmawati & Wiranata, 2023; Zhang & Ge, 2022).

Achieving a balance requires flexible IPR frameworks with provisions such as fair use, exceptions, and limitations that facilitate the legitimate use of protected works for public interest purposes, including education and research (Momen, 2020; Singh, 2017). Open-access models, such as Creative Commons licenses, offer additional pathways to share knowledge while preserving some rights for creators (Alnafrah & Bogdanova, 2019).

Media freedom and access to information further enhance this balance by promoting transparency and ensuring equitable engagement with creative works and knowledge. Conversely, restrictions on media freedom can stifle

public access and hinder societal progress (Momen, 2020; Singh, 2017; Solis & Waggoner, 2020).

The digital age has amplified both the opportunities and challenges associated with IPRs. While digital platforms enable widespread dissemination of knowledge, they also increase the risk of unauthorized use and distribution (Alnafrah & Bogdanova, 2019). Policymakers must address these challenges by crafting regulations that accommodate technological advancements while safeguarding the interests of creators and the public alike.

In summary, balancing the protection of creators with access to knowledge requires a multifaceted approach that includes adaptable IPR policies, support for open-access initiatives, and the promotion of media freedom. By striking this balance, societies can nurture innovation while ensuring that knowledge remains a shared resource for global progress.

Competition and Antitrust in ICT

Competition refers to the rivalry among firms or individuals in a market as they strive to attract customers and expand their market share (Lemley, 2016). Antitrust laws are regulatory frameworks designed to preserve and promote competition by preventing monopolistic or anti-competitive practices, such as price-fixing, market allocation, and mergers that hinder competition (McAfee et al., 2005).

These laws aim to protect consumer welfare by ensuring fair market conditions and curbing abuses of market power, thereby fostering innovation and economic growth (Buccirossi et al., 2009). However, the extraterritorial application of antitrust regulations, particularly involving multinational corporations, has sparked debate about balancing market competition with broader societal interests, such as consumer privacy and data protection (Sun, 2023).

Empirical studies underscore the complex interplay between antitrust enforcement such as merger approvals, entry barrier removal, and antitrust enforcement, on market competition and firm performance emphasizing the context-dependent nature of their outcomes (Scanlon et al., 2006; Kee & Hoekman, 2007; Giulietti et al., 2005; Lee et al., 2014).

The impact of Information and Communication Technology (ICT) on fostering competition and enabling the rise of tech monopolies can be assessed through both global and Kenyan examples, revealing its dual nature in shaping market dynamics.

Globally, ICT has facilitated the dominance of major tech companies like Google, Amazon, Facebook, and Apple, whose control over digital infrastructure and network effects has entrenched their market power. This dominance raises concerns about monopolistic practices that stifle competition and innovation. Efforts to address these challenges, such as antitrust enforcement, have been met with difficulty, as traditional legal frameworks often struggle to adapt to the complexities of platform-based business models in the digital economy.

In Kenya, ICT has driven the growth of a vibrant startup ecosystem, particularly through mobile technologies and increased internet access. However, local startups face significant barriers in competing with larger, well-established tech firms due to resource limitations and the network effects that favor dominant players. In response, the Kenyan government has introduced measures like the Digital Service Tax to regulate digital platforms and promote fair competition, aiming to level the playing field for local businesses.

These examples demonstrate that while ICT fosters innovation and competition by enabling new market entrants, it also facilitates the concentration of power in the hands of a few dominant players. Effective regulatory and antitrust measures are critical in ensuring that the digital economy remains dynamic and inclusive.

Implications for Innovation

The rise of tech monopolies, exemplified by companies like Google and Amazon, has raised concerns about their ability to suppress competition and limit market access for smaller firms. These companies leverage their dominance in digital infrastructure and network effects to maintain their market positions, often stifling innovation in the process (Décary-Hétu, 2023; Parks et al., 2017). Furthermore, the rapid evolution of platform-based business

models has exposed limitations in traditional antitrust frameworks, which often fail to account for the complexities of the digital economy (Neo, 2021). To address these issues, regulatory approaches must adapt to ensure a level playing field and encourage innovation.

Regulatory Interventions

Antitrust enforcement remains a key strategy in addressing the market power of tech giants, though its effectiveness depends on regulators' ability to keep pace with technological advancements (Blagojević & Šćekić, 2021). Targeted regulations, such as digital service taxes and policies aimed at content moderation, have emerged as complementary tools to balance competition with concerns about privacy, misinformation, and hate speech (Herwanto et al., 2021; Baltrusaitis et al., 2021). Additionally, fostering startup ecosystems through initiatives like regulatory sandboxes, financing support, and talent development can empower smaller firms to compete with larger players and drive innovation (Radu, 2019; Bello, 2023).

In summary, while ICT has significantly advanced innovation, it has also contributed to the emergence of tech monopolies, necessitating adaptive regulatory frameworks. Addressing these challenges is essential to promoting fair competition and sustaining a dynamic and inclusive digital economy.

Privacy and Security in the ICT Era

Privacy: Privacy means an individual's freedom to decide the extent to which others can have access to him or her, his or her ideas, conversations, and actions. It includes one's capacity to control information flow about an individual, and information gathering, processing, utilization, and transmission. Privacy has been accorded an international recognition as a basic human right in the Universal Declaration of Human Rights (UDHR, Article 12) and the International Covenant on Civil and Political Rights (ICCPR, Article 17).

Security is generally defined as the state of being free from danger or threat, as well as the measures implemented to prevent or mitigate such risks (Lucinescu, 2021). In the context of information and communication technologies (ICT), security specifically refers to the protection of information systems from unauthorized access, use, disclosure, disruption, or destruction, ensuring the confidentiality, integrity, and availability of information. As a multifaceted concept, security encompasses various dimensions, including cybersecurity, which has become increasingly critical with the growing reliance on ICT systems by individuals, organizations, and governments. A comprehensive approach to ICT security integrates technical measures, organizational strategies, and user awareness to safeguard information assets and mitigate risks effectively (Wang et al., 2012; Alzamil, 2018).

ICT has brought a dramatic change in the way people, companies, and governments deal with information. It has encouraged enhanced communication, exchange of information and information processing, thus promoting economic growth and development. But, these advantages have been accompanied with major problems of privacy and security. Individual and organizational privacy have become more vulnerable now that data is gathered, analyzed, and stored at a higher volume. Hacking, phishing, and ransomware attacks have become rampant, thus increasing the need for data security measures. In this section, we will evaluate the effect of ICT in privacy and security, review data protection laws, discuss cyber threats, and outline the relationship between security, freedom, and ICT innovation.

Impact of ICT on Personal and Institutional Privacy

ICT can be found almost everywhere and the way in which individuals and institutions gather, process and disseminate information has changed. Internet, social networks, applications, and e-services gather big amounts of user information to enhance target consumer experience. ICT systems are used by hospitals, financial organizations and educational institutions to handle the sensitive data.

Erosion of Personal Privacy: ICT gadgets like mobile phones, smart watches, and IoT devices are secretly collecting information from users. Technology firms and advertisers are able to monitor people's movements, search histories, buying behavior and social media usage (Zuboff, 2019). Facebook and X (previously Twitter) allegedly make money from selling user information, and search engines like Google gather users' activities on the

Internet in order to improve targeted advertisements. This triggers issues of consent, ownership of data, and privacy.

Institutional Privacy Challenges: Challenges to organizational privacy include, among others, cloud computing and working from home. Business data such as financial data, business and commercial secrets, and valuable customer information are now stored in cloud environments, which are at risk for data breaches. Hack attacks at Equifax and Yahoo revealed millions of user accounts leaving one to question the efficiency of institutional data security (Kshetri, 2018). There is always a challenge for institutions to achieve the efficiency in operations through the use of ICT and at the same time ensure they secure data from external threats.

Data Protection Laws and Cybersecurity Measures

In order to mitigate the identified privacy risks, different countries have introduced the laws on data protection and created the corresponding legal requirements for the processing and sharing of personal data. These regulations place requirements on organizations and attempt to provide people greater control over their data.

General Data Protection Regulation; GDPR: The GDPR is a general data protection regulation that applies to the member states of the European Union and these countries have set high standards for data processing, collection, and usage. It requires organizations to ask for clear consent for personal data collection and to explain rights to the individuals and to store the data securely (European Union, 2016). GDPR also applies extraterritorially, so any company worldwide has to act according to its rules in case it processes data of EU citizens. Failure to do so attracts penalties that can go up to 4% of the organization's revenues in the whole world.

The Data protection Act of Kenya 2019: The Data Protection Act of Kenya, which was developed to mirror the GDPR, regulates data processing in Kenya. It lays down standards like openness, responsibility, and using minimum data. The Act seeks to compel data controllers and processors to seek registration with the ODPC and grants data subjects' rights of access, erasure, and correction to their personal data (Kenya Data Protection Act, 2019). The Act is particularly useful to organizations such as banks, healthcare providers, and e-commerce businesses in Kenya.

Cybersecurity Measures: To address the issues of data protection, organizations have put in place cybersecurity measures like a firewall, encryption, and multi-factor authentication (MFA). Encryption for example helps prevent data interception during transmission hence it helps in issues to do with confidentiality. A firewall and IDS prevent the unauthorized network traffic from accessing the network. On the other hand, a program that requires the employees to undergo through training on how to safeguard themselves against social engineering such as phishing is also crucial.

Cyber Threats in the ICT Era

Having emerged from the ICT advancement, the new cybercrime is characterized by hackers employing new techniques in attacking networks and acquiring private details. Key threats include:

Ransomware Attacks: Ransomware is a type of malware that locks an organization's files and data making them unavailable until a ransom is paid. In 2021, ransomware attacks had a global impact of billions of dollars, and major industries including healthcare, education, and government services were targeted by the hackers (IBM X-Force, 2022).

Phishing Attacks: Phishing is a type of attack whereby the attacker pretends to be from a genuine organization in order to gain access to its target's passwords and any other financial details. New waves of phishing attacks are more complex, and many of them work based on social engineering that targets human weaknesses (Aleroud & Karie, 2017).

Distributed Denial of Service (DDoS) Attacks: DDoS attacks overload servers with fake traffic, rendering services inaccessible. They are directed towards big companies and some of them are financial institutions and government

websites. These attacks are usually performed by using other compromised devices, known as botnets to enhance the severity (Mirkovic & Reiher, 2004).

Insider Threats: People that are the employees, contractors, or insiders who have access to the data may deliberately or inadvertently leak information. Insider threats are usually hard to identify especially when the insiders exploit their lawful access privileges. Organizations can solve this through controlling users' activity, using role-based access control, and promoting whistleblowing.

Tension Between Security, Freedom, and Innovation

Privacy-security-innovation triad is one of the most heated topics in the ICT era. On the one hand, users expect anonymity and unrestricted access to information; on the other, governments stress security and control to fight terrorism, cybercrime, and child abuse.

Encryption Debates: Encryption helps to safeguard the privacy of a user by making his or her communication secure to the third party. Nonetheless, governments explain that encryption also protects the criminals from monitoring, which is why they cannot conduct investigations on criminal activities such as terrorism and drugs trafficking. This has stirred discussions on whether Apple and WhatsApp among other firms should develop 'backdoors' for use by police (Abomhara, 2015). Critics of the backdoors' approach insist that the presence of such openings decreases the level of protection for all users because hackers can take advantage of them.

Mass Surveillance: State agencies have implemented the large-scale spying of the population and its actions on the Internet. The surveillance was revealed by Edward Snowden, who leaked details of The U.S. National Security Agency's (NSA) PRISM program on how surveillance was being conducted across the globe (Greenwald, 2014). Some countries like China have put in place the facial recognition systems and social scoring that raise questions on privacy and freedom. While mass surveillance may enhance security, critics argue it violates civil liberties and fosters authoritarian control.

Balancing Innovation and Privacy: Solutions that are innovative ICT based like AI-based predictive analytics, need sample data. Nevertheless, getting and using such data causes privacy issues. Currently, organizations such as Google and Facebook are under criticism for relying on big data to feed AI systems. Balancing the need for innovation with privacy requires the adoption of privacy-preserving technologies such as federated learning and differential privacy (Dwork, 2008).

Advancement of Knowledge and Innovation through ICT

ICT is central to the advancement of knowledge and innovation., it is also central to knowledge and innovation. The emerging trends in the application of ICT has accelerated the production, dissemination and access to knowledge. ICT has thus led to the removal of geographic and time constraints in dissemination of knowledge in areas such as e-learning, digital libraries and collaborative research. In addition, ICT exercises influence over technology and social change by promoting creativity, providing information access and supporting new forms of business. This section explores ICT in enhancing the flow of knowledge and the function of technology and social change.

ICT and Knowledge Dissemination

ICT enables generation, acquisition, retrieval and dissemination of knowledge. The Internet and applications give users a chance to study, cooperate, and research further without stopping. Some of the important knowledge sharing areas supported by ICT are e-learning, digital libraries, and research.

E-Learning and Online Education: Online learning tools like Coursera, edX, and Khan Academy have brought education to the next level by making quality learning resources easily available to students irrespective of the part of the globe they come from. ICT enabled e-learning was the main means of education delivery to millions of learners during the COVID-19 outbreak (Bozkurt et al., 2020). Many Learning Management Systems (LMS) such

as Moodle and Blackboard help educational institutions in offering live group and individual classes through web conferences and recorded videos, and discussion forums. These platforms encourage continuous learning and retraining, which is very important in the developing world where literacy levels are low.

In the past few years, ICT has made it possible for learners to have individualized material depending on their choice and progress. AI and ML algorithms track students' learning behaviors, and with the result, adaptive learning applications can adjust the teaching approach to suit the learners (Holmes et al., 2019). This approach increases learner interaction and increases the effectiveness of the educational process.

Digital Libraries and Open Access Repositories: Digital libraries have dramatically changed the ways students get access to scholarly literature, research articles, and books. Web resources such as Google Scholar, PubMed, and ResearchGate offer the user a combination of the world's largest databases of academic works. Digital libraries give the researcher, students and the society at large an opportunity to access information at any one time and any part of the world. Open access projects like OpenAIRE and DOAJ share scientific information with the public so that researchers in low-income countries can access crucial research documents (Suber, 2012).

Digital libraries also preserve cultures as many libraries have an opportunity to scan historical documents, manuscripts and other artifacts. Some are the World Digital Library and the British Library's digitization projects. This enables the continuity of cultural aspects and at the same time making the cultural facets easily accessible to the outside world.

Research Collaboration and Virtual Laboratories: ICT has enabled international research collaboration through ResearchGate, Mendeley, Academia.edu and so on. Social media tools like Google Docs, Slack, Microsoft Teams, among others, help researchers to edit documents simultaneously, schedule virtual meetings and share knowledge in real-time. Social platforms such as GitHub enable researchers to share codes, data, and analysis scripts, enhance the practice of open science, and facilitate reproducibility.

Online simulations and remote access to instruments allows researchers to perform their experiments even if they are not physically in the lab. Virtual labs are being applied in physics, chemistry, and biology since students and researchers can carry out experiments practically without being physically present (De Jong et al., 2013). This has enhanced the research productivity and has also provided better access to the experimental resources.

ICT as a Driver of Technological Innovation

ICT is a facilitator of technological advancement since it promotes the creation of new technologies in products, services and procedures. Technological changes in artificial intelligence and machine learning have revolutionized industries and improved the technology frontier.

Development of Emerging Technologies: ICT has increased the pace of advancement and implementation of new technological trends like IoT, blockchain, and AI. Smart home appliances and health tracking gadgets are examples of IoT devices that gather and assess the data to give real-time information. Blockchain technology, earlier used in trading virtual currency known as bitcoins, is now utilized to create protected, distributed applications in finance, supply chain, and healthcare (Tapscott & Tapscott, 2016).

Cloud computing has evolved other types of models like Software-as-Service (SaaS) and Platform-as-Service (PaaS) that allow businesses to acquire computing resources ad hoc. AWS and Microsoft Azure present cloud architectures for scalable computing, enabling the new generation of startups and innovators to build and prototype new applications at a fraction of the cost.

Innovation in business models and Startups: ICT has given rise to new business models including; sharing economy, gig economy and platform economy. Other examples of ICT in the business environment include firms such as Uber, Airbnb, and Fiverr, who have used ICT to facilitate connection between sellers and buyers. This has given rise to some employment and business ventures. Entrepreneurs have also leveraged ICT to create solutions as health tech, edtech and fintech among others (Bock et al., 2012).

ICT has also helped in innovative products through crowdfunding sites such as Kickstarter and GoFundMe whereby innovative people seek funding from the public for their projects. They help in the process of new venture creation, turning ideas into actual businesses.

ICT as a Driver of Social Innovation

ICT is strategic to supporting and encouraging social innovation. Social innovation is defined as the processes for designing novel solutions to social problems of poverty, education, health and the environment. Social innovation is enabled by ICT in areas such as digital inclusion, e-governance and community enabling.

Digital Inclusion: ICT initiatives for digital inclusion intend to minimize the gap between developed and developing parts of the world. Mobile internet, affordable smartphones and Community Wi-Fi have enhanced ICT in hard-to-reach regions. Some examples are Google's Project Loon and SpaceX's Starlink that are trying to bring internet connection to hard-to-reach places. Digital inclusion is about facilitating fair use of technologies in accessing knowledge, learning, and employment for persons who are socially excluded (van Dijk, 2020).

E-Governance and Public Service Delivery: People's governments employ ICT to deliver e-governance services thereby making government services accessible through the internet. With e-governance, people can electronically file their taxes, register their businesses and seek medical care. For example, Kenya introduced an e-citizen platform that allows people to interact with public services electronically. This enhances the quality-of-service delivery, brings about transparency and minimizes bureaucratic encumbrances.

ICT-Driven Social Movements: The use of social sites such as Facebook, X (previously twitter) and WhatsApp has led to the emergence of digital activism. ICTs are employed to organize people for social issues, advocacy for human rights and for disaster relief. Social media campaigns like the #BlackLivesMatter and #RejectFinanceBill campaigns were common in the social media platforms in advocacy for change. ICT facilitates the speedy spread of information and brings awareness of social causes, and gives marginalized groups a platform to be heard (Tufekci, 2017).

Challenges and Ethical Considerations in ICT

Though ICT has made provisions of information, education, and innovation easier through the use of computers, telecommunication equipment and the internet, it comes with its fair share of difficulties and ethical issues. Policies and its limitations, systemization of digital divides, algorithmic injustice, ethical issues in AI, and privacy are the primary issues that may slow down the progress of freedoms and rights. Rather than encouraging equity, ICT may well reinforce inequality and support forms of monitoring, exclusion and regulation. This section outlines major issues regarding ICT and presents an analysis of how ICT may actually pose a threat to human freedoms and rights.

Digital Divide and Inequality

Digital divide is the break between those who use ICT and those who do not. This split is present in terms of device ownership, connectivity, and skills.

Socioeconomic Divide: Socioeconomic status is a major predictor of access to ICT resources. The high-income people and societies own smartphones, laptops, and broadband internet easily, but the low-income societies especially in developing countries have a high level of difficulty to access them (van Dijk, 2020). High-speed internet is also a scarce resource in the rural areas hence has a negative impact on education, employment and health. For instance, during the COVID-19 outbreak, students from low-income families have been disadvantaged by online learning because of poor internet connectivity and or no device (Bozkurt et al., 2020).

Gender Divide: Some women and girls are unable to access ICT due to the prevailing systems in their respective areas of residence. High levels of socio-cultural acceptance and gendered control of technology mean that women cannot own mobile devices or access the internet in patriarchal societies. Gender digital divide reduces women's

chances of engaging in digital schooling, working, and business (Webb et al., 2018).

Regional and Global Divide: There is a clear divide of ICT usage between the developed and the developing countries. Some of the issues associated with low-income countries especially those in the Sub-Saharan region include; high cost of data, poor infrastructure and lack of technical know-how. ITU says that by 2023 the Internet connection in Africa will be much lower than in Europe and North America. This regional division leads to disparities in education, health, and employment chances across the geographic region.

Critical Perspective: This results in a form of a 'digital exclusion' where the social groups in question does not get to benefit from ICT. ICT could be empowering as it could enhance equality, but the unequal access to ICT could accentuate inequalities social, gender and economical. To close the gap, we need to focus on the infrastructure for delivery, affordable broadband internet access and digital skills to ensure that the divide is closed.

Ethical Dilemmas in Artificial Intelligence (AI) and Automation

Automated systems and Artificial Intelligence are being integrated into various industries and so come with important ethical issues and concerns such as bias and accountability.

Algorithmic Discrimination: AI models are built based on historical data that may include biases and these biases are carried forward into the AI decision making. For example, algorithms used in recruitment such as the one that Amazon designed have been seen to favor males as the data used to train them was prejudiced (O'Neil, 2016). Likewise, facial recognition software has a higher error rate for people of color particularly black people which causes wrongful arrests and discrimination (Buolamwini & Gebru, 2018).

Loss of Jobs Due to Automation: AI and robotics have led to automation that in turn reduces the human workforce especially in areas that require low skills. Some industries such as manufacturing, logistics, and retail industries are already implementing AI-driven automation. Despite the fact that automation enhances efficiency and productivity, it results in job loss and aeration of insecurity among employees (Frey & Osborne, 2017). Examples include customer service chatbots powered by artificial intelligence, which replace human customer service personnel.

Lack of Accountability and Transparency: AI decision-making is usually concealed, and it may be quite challenging to explain why particular decisions are made. This is where the concept of a 'black box' tends to come into play and this is rather unethical when thinking about accountability. For example, in a case where an AI self-driving car is involved in an accident, it is not clear who is at fault, the manufacturer of the car, the designer of the software used in the car or the owner of the car (Floridi et al., 2018).

Critical Perspective: AI and automation are on one hand a boon but on the other hand they are a bane. Though claiming to improve productivity, they may further deepen prejudice, obscure decision-making, and lead to job loss. This can only be achieved if ethical AI principles are implemented and there is supervision by human beings. Organizations must carry out AI audits for them to uncover and address various forms of biases. The governments and policymakers should also set down standards on how AI should be developed.

Privacy, Surveillance and Data Protection

The increased use of ICT has raised many questions on data privacy, surveillance and data protection. People interact with the Internet, social networks, and applications, so they are creating the digital shadow; therefore, questions regarding the consent and rights to personal data occur.

Surveillance and violation of privacy: Most of the governments and corporations conduct mass surveillance through facial recognition, biometric scanners, and online tracking systems. In 2013, Edward Snowden leaked information to the public to show that the U.S government was monitoring its citizens under the NSA PRISM program (Greenwald, 2014). Technologies like China's 'social credit system' are considered authoritarian, they monitor people's behavior and punish them for such actions that a society considers improper.

Data Exploitation and Monetization: Silicon Valley companies, including Google, Facebook and Amazon, harvest users' data and sell it back to them through advertising. Consumers sign complicated terms of service without knowledge about use of their data thus losing control over personal information (Zuboff, 2019). Cyber-attacks like the Facebook and Cambridge Analytica show how personal data can be used for political machinations and fake news.

Weak Data Protection and Cybersecurity: Despite data protection laws like the General Data Protection Regulation (GDPR) and Kenya's Data Protection Act (2019), cybersecurity breaches remain a significant threat. Ransomware, data leaks, phishing attacks on individuals reveal their identity and lead to loss of money. Hospitals, banks, and government agencies are the most vulnerable to hackers' attacks, and this requires improvement of security.

Critical Perspective: Although ICT is a tool of communication, education, and business it has negative impacts on privacy and civil liberties. Technological tools of surveillance and data mining are capable of tracking and disciplining people. The governments and the corporations need to follow privacy by design and set out specific data protection policies. Should this not be done, Zuboff (2019) noted the emergence of "surveillance capitalism" where private data becomes a tradable asset.

Ethical Use of ICT in Research and Development

ICT R&D brings in some ethical issues mainly in the field of genetic research, military technology, and health diagnostic technology based on AI.

Ethical Use of Personal Data in Research: ICT based research work usually leads to the gathering and analysis of large data sets. One of the biggest concerns is ethical issues that may come up whenever an individual data is being used without his or her consent. For instance, health researchers who design wearable fitness trackers to track activity of the users of the device must make sure that the personal data being collected is not misused and used properly.

Dual-Use Dilemma in ICT Research: Some of the ICT innovations are dual use innovations, for instance, drone technology. As humanitarian drones are employed to assist in the delivery of medical supplies, the same drones are employed for attacks and reconnaissance. The dual-use issue raises the question of whether the R&D processes should persist if the obtained technology can be employed negatively (Joyce, 2022).

Critical Perspective: In ICT ethical research there is a need to establish ethical frameworks in matters concerning data collection, consent and dual-use technology. To this end, institutions have to set up review boards which are supposed to assess the ethical issues regarding the research activities.

Recommendations

Infrastructure Development: Governments and technology firms must come up with incentives like subsidies, tax exemptions and cheap cost structures based on the ICT gadgets including smart phones, tablets, laptops. They can bring in 'free browsing' to education and government owned websites so that people can access services without having to pay. For example, agreements between Meta (formerly Facebook) and telecom operators within the "Free Basics" project sought to offer free Internet connection for basic services.

Digital Literacy and Skills Development: To address this issue, national digital literacy programs should be put in place to educate the citizens on the use of the tools, and how to use the internet and other related issues. An effort should be made to adopt digital skills in school learning and adult education to prepare the people to take part in the new digital economy (van Dijk, 2020). Higher level of computer literacy guarantees that citizens can apply ICT in the spheres of learning, employment and interpersonal dealings. It opens the door for digital opportunities for the disadvantaged groups including women, people in the rural areas, and the disabled.

Fair and Inclusive AI Systems: Scholars and IT developers should consider the issue of fairness, explainability and reduction of bias in the use of AI. Government should implement check-points on AI ethics policies as seen with the EU's 'Ethics Guidelines for Trustworthy AI,' these guidelines make developers consider transparency, accountability and human supervision (Floridi et al., 2018). They can minimize prejudice in some sectors such as employment, law enforcement, and credit granting. For example, reimagining hiring processes to eliminate biases in the hiring software makes it easier for people of color to get a job.

AI Accountability and Explainability: Transparency and accountability policies for AI decision making especially in sensitive sectors such as law enforcement, health sector, and the financial sector can be introduced. Propose "algorithmic impact assessments" (AIAs) as a tool that will make companies evaluate and report the negative effects of its AI models on human rights and social justice (O'Neil, 2016). AI decision-making transparency makes it fairer and allows users to question the decisions made by the AI. This increases the level of acceptance of the new AI systems in the public domain and also makes sure that the new system is GDPR compliant.

Strengthening Data Protection Laws: National laws on data protection should be made to conform to international best practices, for example the GDPR of the EU. To ensure that compliance with data protection rules is achieved and violators penalized, governments should set up the Data Protection Authorities (DPAs). Kenya's Data Protection Act (2019) is a model that other countries can emulate. Better data protection legislation minimizes the threat of data breaches, safeguard user's data, and make organizations more accountable in their use of data.

Ethical Research Guidelines and Review Boards: For research and development of certain high-risk areas such as artificial intelligence, biotechnology, military developments, it is advisable to set up ethics review boards that will oversee such projects. There is also a need to make AI and ICT research to be ethical, like how there are ethical reviews before conducting research with human subjects. There is evidence that these boards enhance the possibility of the research being conducted under the guidelines of justice, equity and accountability ensuring that human rights violations are minimized as much as possible, for instance some AI applications in surveillance and warfare.

Multi-Stakeholder Governance: ICT policymaking must not only be left to governments, other players including civil society as well as other nonprofit organizations and businesses must also be integrated into the ICT policymaking processes through multi-stakeholder governance. Multi-stakeholder advisory boards at the national and international levels to provide guidance on ICT policy can be established. The Internet Governance Forum (IGF) is an example of a multi-stakeholder forum on the issues of ICT. The policies developed would be appreciated and accepted by the relevant stakeholders. More disadvantaged people are able to partake in the decision-making which really decides how and where ICTs are used. It also helps build confidence in the regulatory mechanisms.

Conclusion

To achieve productive use of ICT for the advancement of society, freedom, rights, and security must work hand in hand with policymakers, corporations and civil society. Governments should attempt to increase the overall levels of digital equity through purchasing affordable internet, reversible devices, and digital media literacy. Current guidelines and principles for the creation of AI must also ensure the balance and fairness, traceability and non-discrimination regarding application. Privacy should be protected by shared legislation on data protection, privacy integrated in products and services, and cyber security measures. Security initiatives such as mass surveillance and counter-terrorism have to be reasonable, warranted, open and accountable at the same time. ICT must be used to empower humans, create and liberate, and promote justice because ICT is a creation of human beings. By effectively handling ethical issues, diversity, and freedom, rights, and security, the societies shall fully benefit from ICT to support sustainable development for all.

References

Abomhara, M. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of Cyber Security and Mobility*.

Alzamil, Z. A. (2018). Information security practice in Saudi Arabia: Case study on Saudi organizations. *Information & Computer Security, 26*(5), 568-583. https://doi.org/10.1108/ics-01-2018-0006

Asongu, S. A. (2014). Software piracy, inequality and the poor: Evidence from Africa. *Journal of Economic Studies, 41*(4), 526-553. https://doi.org/10.1108/jes-10-2012-0141

Blagojević, J., & Šćekić, R. (2021). The Arab Spring a decade on: Information and communication technologies as a mass mobilization tool. *Kybernetes, 51*(9), 2833-2851. https://doi.org/10.1108/k-03-2021-0240

Billón, M., Andrés, A. R., & Rodríguez-Crespo, E. (2023). Broadband use and trade facilitation: Impacts on bilateral trade of Sub-Saharan countries. *African Development Review, 35*(2), 113-125. https://doi.org/10.1111/1467-8268.12698

Bozkurt, A., et al. (2020). A global outlook on the interruption of education due to the COVID-19 pandemic. *Asian Journal of Distance Education*.

Brandl, K., Darendeli, I. S., & Mudambi, R. (2018). Foreign actors and intellectual property protection regulations in developing countries. *Journal of International Business Studies, 50*(5), 826-846. https://doi.org/10.1057/s41267-018-0172-6

Brown, W. M. (2003). Intellectual property law: A primer for scientists. *Molecular Biotechnology, 23*(3), 213-224. https://doi.org/10.1385/mb:23:3:213

Buccirossi, P., Ciari, L., Duso, T., Spagnolo, G., & Vitale, C. (2009). Competition policy and productivity growth: An empirical assessment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1487489

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of the Conference on Fairness, Accountability, and Transparency*.

Bydoon, M. (2016). An overview of human rights and intellectual property protection. *Journal of Arts and Humanities, 5*(12), 58. https://doi.org/10.18533/journal.v5i12.1069

Clobridge, A. (2010). *Building a digital repository program with limited resources.* Chandos Information Professional Series. Chandos Publishing.

Dwork, C. (2008). Differential Privacy: A Survey of Results. *Proceedings of the 5th International Conference on Theory and Applications of Models of Computation*.

European Union. (2016). *General Data Protection Regulation (GDPR).*

Floridi, L., et al. (2018). AI4People—An ethical framework for a good AI society. *AI & Society*.

Franke, U. (2012). Disconnecting digital networks: A moral appraisal. *The International Review of Information Ethics, 18*, 23-29. https://doi.org/10.29173/irie300

Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerization? *Technological Forecasting and Social Change*.

Giulietti, M., Price, C. W., & Waterson, M. (2005). Consumer choice and competition policy: A study of UK energy markets. *The Economic Journal, 115*(506), 949-968. https://doi.org/10.1111/j.1468-0297.2005.01026.x

Gojayeva, E., Huseynova, S., Babayeva, S., Sadigova, U., & Azizova, R. (2021). Information platforms and the global network economy. *SHS Web of Conferences, 92*, 04007. https://doi.org/10.1051/shsconf/20219204007

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.*

Halich, A., Kutsevska, O., Korchagina, O., Kravchenko, O., & Fiedotova, N. (2023). The influence of social communications on the formation of public opinion of citizens during the war. *Social Legal Studios, 6*(3), 43-51. https://doi.org/10.32518/sals3.2023.43

Hargreaves, S. (2017). Online monitoring of 'localists' in Hong Kong: A return to political policing? *Surveillance & Society, 15*(3/4), 425-431. https://doi.org/10.24908/ss.v15i3/4.6619

Holmes, W., et al. (2019). *Artificial Intelligence in Education: Promises and Implications for Teaching and Learning.* OECD Publishing.

Hopke, J. E. (2016). Occupy is not a place. *Convergence: The International Journal of Research Into New Media Technologies, 22*(6), 596-615. https://doi.org/10.1177/1354856515601400

Juhász, R., & Steinwender, C. (2018). Spinning the web: The impact of ICT on trade in intermediates and technology diffusion. https://doi.org/10.3386/w24590Kshetri, N. (2018). *The Economics of Cybersecurity.* Cambridge University Press.

Leeson, P. T. (2008). Media freedom, political knowledge, and participation. *Journal of Economic Perspectives, 22*(2), 155-169.

Matthews, D. (2010). Intellectual property rights, human rights and the right to health. *Intellectual Property and Human Rights*. https://doi.org/10.4337/9781849802048.00014

Mutisya, S. M. (2020). Integration of information communication technology in teaching: The underpinning factors among Kenya's primary school teachers. *Journal of Learning for Development, 7*(2), 174-189. https://doi.org/10.56059/jl4d.v7i2.429

NORDITO S. QUIMBO (2023). Navigating the digital frontier: Exploring ICT integration in teaching for enhanced learning experiences. *World Journal of Advanced Research and Reviews, 19*(2), 776-778. https://doi.org/10.30574/wjarr.2023.19.2.1633

Suber, P. (2012). *Open Access.* MIT Press.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution.* Portfolio.

Tufekci, Z. (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protest.* Yale University Press.

van Dijk, J. (2020). *The Digital Divide: The Internet and Social Inequality in International Perspective.* Polity Press.Zuboff, S. (2019). *The Age of Surveillance Capitalism.* PublicAffairs.