



20 YEARS OF

Business & Human Rights
Resource Centre

MARCH 2024

Big tech in Africa: Insights for investors

Investors may not expect there to be serious legal, operational or reputational risks outside of the United States or the European Union, assuming that there has been little progress on litigation and corporate accountability in other jurisdictions. This assumption, however, is becoming outdated, as evidenced by the [increasing number of lawsuits, operational disruptions and moral quandaries](#) executives are facing in relation to alleged human rights abuses by technology companies doing business in Africa.

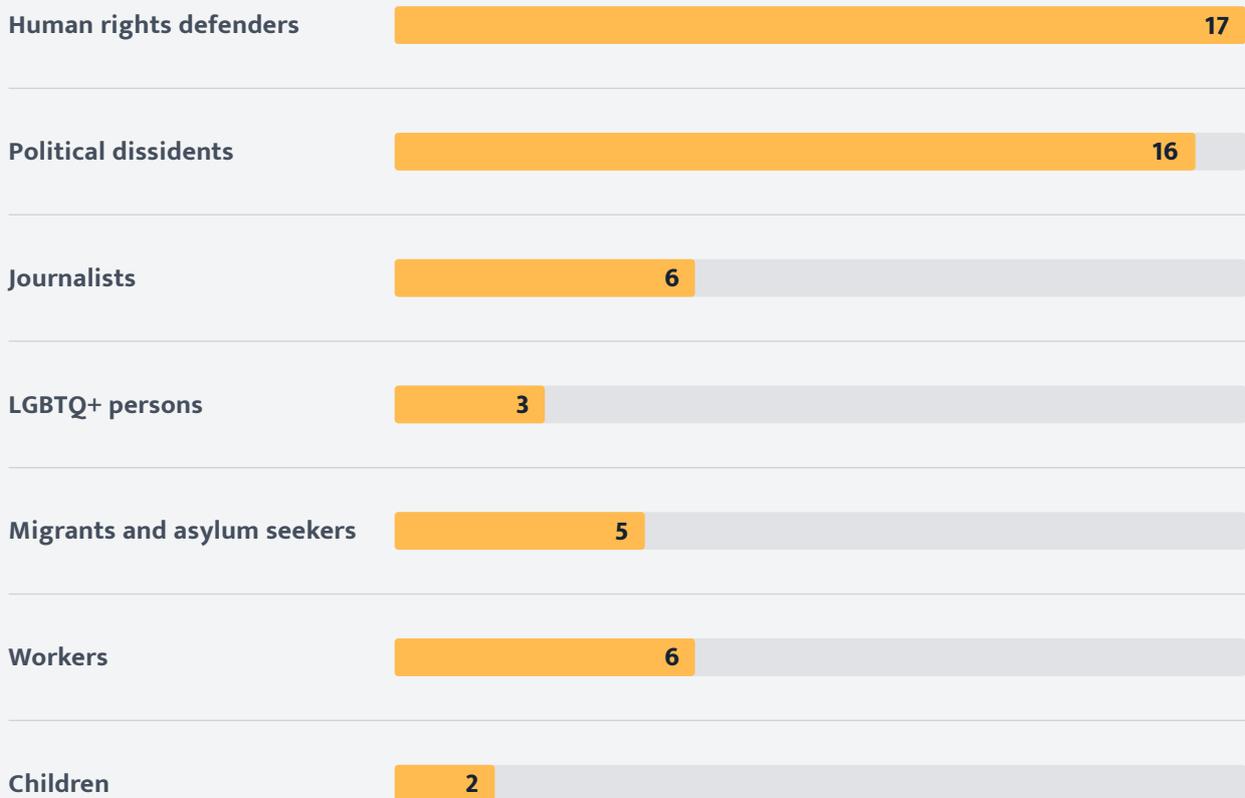
As outlined in the UN Guiding Principles on Business and Human Rights, investors should be using their leverage to improve company conduct and promote human rights due diligence processes to identify, prevent and mitigate salient human rights risks from materialising. The tech sector is no exception. Several key cases, including those outlined below, have the potential to change how “rights” are discussed within corporate decision-making spaces. Investor action is needed to protect people and portfolios from undue risk.

Salient human rights risks for the tech sector in Africa

The Business & Human Rights Resource Centre (the Resource Centre) has been [monitoring allegations of human rights abuse related to the tech sector](#) globally, with [1,577 articles, briefings and civil society reports](#) related to the tech sector in Africa added to our online database up to March 2024. We have recorded numerous allegations of human rights harms, including incidents of [child labour](#) in extracting minerals crucial to the tech sector, [internet shutdowns](#) and [censorship, data privacy breaches](#) and incidents of [online violence](#) against female content creators, among others. Using our [Company Response Mechanism](#) (CRM), the Resource Centre has contacted 34 tech companies¹ about allegations of human rights harm on the African continent a total of 48 times. Of the company response requests sent, almost half (19 out of 48) concerned harms experienced by African human rights defenders, political dissidents and journalists.

WHO IS AFFECTED?

Across the 48 approaches we made to companies about specific cases of alleged abuse, human rights defenders were most frequently affected. Note: some CRMs involve multiple affected groups.



¹ Airtel, Alcatel One Touch (part of TCL Communication), Cellebrite (part of Sun Corporation), Congo Telecom, Elaman, Elettronica Mangione (Elman), Ercom, Etisalat, FinFisher, Gamma Group, GE Health (part of General Electric), GEM Security Services Ltd., Globacom, Grindr, IDEMIA (formerly Morpho), Jumia, Meta (formerly Facebook), Millicom, MTN, Nexa Technologies (formerly Amesys), NSO Group, Orange, Sagemcom, Sinovatio, Telkom Kenya, Trovicor, Uber, Verint, Vivacell, Vodafone, X Corp. (formerly Twitter), Zain, ZTE

Data breaches and hyper surveillance

As African societies [increasingly digitise](#), data is often cited as having economic and developmental importance. But the growing value of data, paired with an increase in data breaches, [raises concerns](#) about whether governments and companies are doing enough to protect people's privacy and safeguard them from harm and manipulation, particularly in electoral contexts (see case studies in [Kenya](#) and [Nigeria](#)). Failure to do so has resulted in improper surveillance and targeting, threatening democracy and putting [human rights defenders](#), dissidents and journalists in danger.

In the name of public safety, many governments are [deploying surveillance](#) hardware and software (including [spyware](#)) that facilitates undue interceptions of private communications, social media monitoring and geo-location tracking. Using surveillance tech for repression has a negative ripple effect on numerous rights – such as the right to privacy, freedom of expression, freedom of assembly and freedom from arbitrary detention. Increasingly pervasive and invasive surveillance technologies are complicating human rights activists' efforts to organise, as unwarranted surveillance has a chilling effect on civil society. All companies within the surveillance tech ecosystem – including [telecommunications](#), [biometric software](#) and [hardware providers](#) – [have a responsibility](#) to mitigate human rights harms.

Translating rights to material risk:

Privacy

🔗 Kenya: [Government suspends WorldCoin's operations due to data privacy concerns](#)

Risks: **Legal** **Operational**

WorldCoin, a [crypto-project created by OpenAI](#), had its operations suspended in Kenya due to concerns over data and privacy risks. Scrutiny by Kenya, along with [several other countries](#) including the United Kingdom, Argentina, Portugal, Germany and France, has led to [slowed growth](#) in the technology's adoption.

🔗 South Africa's [information regulator issues enforcement notice to protect consumer privacy](#)

Risks: **Legal** **Financial**

At the start of 2024, South Africa's information regulator [began investigating](#) marketing companies, technology consultancies and data brokers under the Protection of Personal Information Act (POPI Act) to prevent companies from contacting consumers without proper consent. On 27 February 2024, the regulator issued its first enforcement notice, directing technology consultancy FR Ram Consulting to modify its practices within 90 days to ensure obtention of informed user consent or pay a fine of up to ZAR 10 million.

🔗 Kenya: [Data protection regulator fines businesses for breach of data privacy](#)

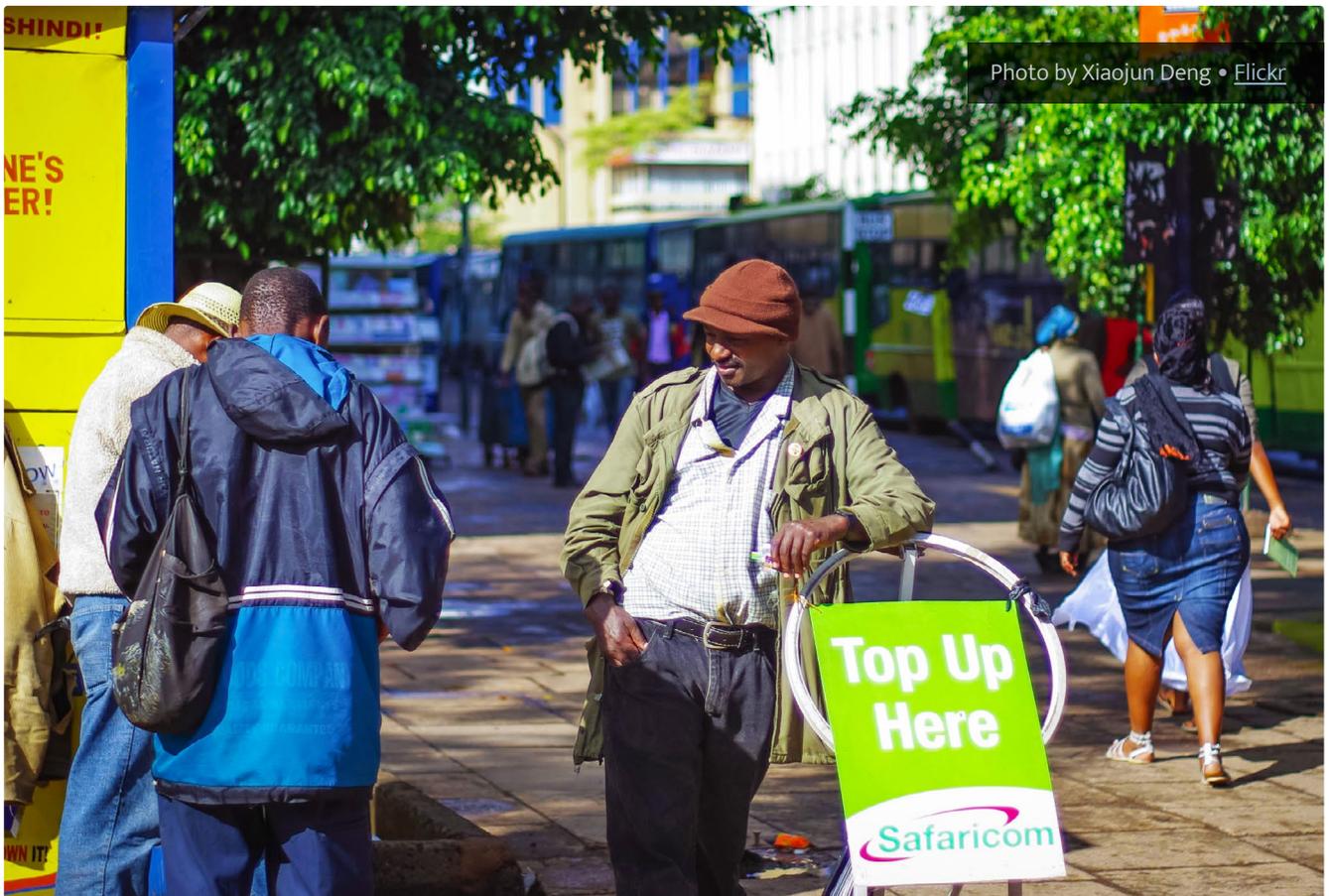
Risks: **Legal** **Financial**

Kenya is one of 35 African countries with data protection legislation. In 2023, Kenya's data protection agency fined three businesses, including a digital credit provider linked to threatening messages and calls; a school which posted children's photos without consent; and a restaurant for posting photos of patrons without consent over breaches of data privacy.

🔗 Kenya: [Court allows Safaricom subscribers to join suit challenging company's rules that allegedly breach privacy](#)

Risks: **Legal** **Reputational**

The High Court of Kenya has given approval for millions of Safaricom subscribers to engage in a class action lawsuit against the telecommunications company regarding a clause in SIM card registration rules. This clause, found in the data privacy statement, permits Safaricom to collect and store users' bank details, including credit or debit card information, sparking a legal challenge by subscribers who argued that the company's dominance in the Kenyan mobile market leaves users with little choice but to accept the controversial clause.



Labour rights abuses

Big tech's investments in Africa can be attributed to a number of factors, including a [growing base](#) of young consumers, lower labour costs and government incentives for foreign direct investment. Irresponsible business conduct in addressing risks linked to the [gig economy](#), [training artificial intelligence systems](#), and other types of outsourcing have resulted in a number of labour rights violations, such as [tech-facilitated human trafficking](#), [child labour](#), [unfair wages](#) and [poor working conditions](#). Many ride-sharing and food delivery companies [do not meet basic standards](#) for protecting workers, as evidenced in reported lack of clarity around contracts and non-payment of wages. Call centre workers have allegedly experienced [union busting](#) by multinational corporations which curtail unionisation efforts by firing workers or by intimidating and bribing them to resign. The limits of responsibility, namely concerning accountability for the global supply chain, are being tested and potentially re-drawn.

Translating rights to material risk:

Labour rights

🕒 **DRC: [Big tech companies named in lawsuit over child deaths in Congolese cobalt mines](#)**

Risks: **Legal** **Reputational**

Apple, Google, Alphabet, Microsoft, Dell and Tesla were recently sued by IRAdvocates, a US NGO which filed a federal class action lawsuit on behalf of 14 plaintiffs connected to children affected by mining cobalt in the DRC. The plaintiffs alleged forced child labour violations and seek relief for unjust enrichment, negligent supervision and intentional infliction of emotional distress. The case was eventually dismissed after lengthy court proceedings stretching over four years.

🕒 **Kenya: [Legal battles against Meta unite content moderators across borders in the fight for fair working conditions](#)**

Risks: **Operational** **Legal** **Reputational**

In 2022, Daniel Motaung, an ex-content moderator from South Africa, filed a suit against Sama and Meta in Kenya. He alleged [unreasonable working conditions including irregular pay](#), inadequate mental health support, union busting, and violations of workers' privacy and dignity. Sama [denied](#) the allegations while Meta claimed that it was not responsible for Mr. Motaung's working conditions since [he was not its employee](#). The court has ruled that it has jurisdiction to hear the case. In another case, 43 content moderators employed by Meta subcontractors Samasource Kenya EPZ and Majorel Kenya sued the three entities alleging unfair dismissal. The High Court of Kenya [issued interim orders](#) compelling the companies to provide *"proper medical, psychiatric and psychological care for the petitioners and other Facebook Content Moderators..."* The case is still ongoing, and it has inspired employees of social media giants based in Africa to unionise for better working conditions. A notable example is the [coalition of Meta, TikTok and YouTube content moderators in Kenya](#).

Discrimination

For the tech sector in particular, diversity in management as well as technical positions is critical for ensuring products and services are usable in and reflective of our diverse societies. [Data gaps](#) and [biases](#) in artificial intelligence (AI) systems impact Africans both online and offline. For example, inaccuracies in facial recognition systems have led to wrongful arrests of [Black women](#) and [men](#). Generative AI chatbots have peddled [false or misleading medical information](#) about Black people. An increase in automated gender recognition systems in Africa is fuelling [discriminatory impacts](#) on women and gender non-conforming individuals. And, as [explained by Paradigm Initiative](#), “*language inequalities risk excluding certain members of society.*” For example, Facebook’s AI-powered hate speech detection systems only operate in [40 languages](#), and Africa is home to over 2,000 languages. This ultimately and disproportionately impacts persons speaking minority languages who are also part of historically marginalised groups, including the proliferation of hate speech against [LGBTQ persons](#) and [women](#).

Translating rights to material risk:

Non-discrimination

🕒 Ghana: [Twitter Africa employees accuse Elon Musk of discrimination over severance terms](#)

Risks: **Legal** **Reputational** **Financial**

X, formerly known as Twitter, has [compensated the employees](#) it dismissed from its African headquarters in Ghana more than a year after their layoffs, following threats of legal action for unpaid redundancy payments. The company’s significant global reduction of its workforce, during which over 6,000 employees lost their jobs in a process initiated by owner Elon Musk, was met with criticism and legal challenges worldwide, including a lawsuit in California for not fulfilling severance package promises.

🕒 Facebook accused of gender discrimination as research finds bias in advertising algorithm

Risks: **Operational** **Reputational**

A group of NGOs filed a complaint against Meta in the Netherlands and France after conducting research on gender bias in the algorithms used by Facebook to recommend job advertisements. The NGOs analysed the reach of job ads in six countries, including South Africa, and found that across the studied jurisdictions “*90.9% of ads for a mechanic [were] seen by men, whilst 78.6% of ads for preschool teachers were seen by women.*” The organisations filed complaints to the French *Defenseur des Droits* and the Dutch Institute of Human Rights to launch investigations.

Internet shutdowns and censorship

According to [Business Insider Africa](#), in 2023, “Sub-Saharan Africa witnessed a financial setback of \$1.74 billion during 30,785 hours of internet downtime, affecting 84.8 million people.” Internet shutdowns restrict [digital freedoms](#), including the right to access information, the right to organise online and freedom of speech. Tech companies should have contingency plans on how to respond to requests by governments to shut down the internet, ideally prior to operating in markets that have a history of shutdowns. The Resource Centre has examined the [human rights responsibilities of telecoms companies for internet shutdowns in Africa](#) and provided recommendations for companies, including open and transparent communication with users before and after internet cut-offs.

Translating rights to material risk:

Access to information & consumer rights

- ➔ **Sudan: [Following a six day communication blackout, internet access is “gradually returning” amid devastating war](#)**

Risks: **Operational** **Reputational**

The Sudanese Government has been known to use [internet shutdowns](#) as a response to protests and criticisms since 2019, when service disruption lasted 37 days and over 100 protesters were allegedly killed. In 2019, the [court ordered MTN, Zain and Sudani](#) to restore internet services after a lawsuit was filed to challenge the cut-off.

- ➔ **[TikTok bans in several African nations deemed “undemocratic”](#)**

Risks: **Operational**

Somalia and Senegal banned TikTok in August 2023 over claims of human rights concerns, but activists say the bans are politically motivated and ultimately aim to reduce government criticism. According to Rest of World, “*In Senegal, the government blocked several popular social media apps like Facebook, Instagram, Telegram, WhatsApp, and YouTube in early June, amid nationwide demonstrations after the [sentencing](#) of opposition leader Ousmane Sonko. A subsequent increase in the number of videos criticizing the government on TikTok led to the app being blocked on August 2.*”

- ➔ **South Africa: [Regulatory body fines Vodacom over violation of consumer rights](#)**

Risks: **Legal** **Financial**

South Africa’s National Consumer Tribunal fined Vodacom ZAR 1 million for requiring a 75% payment from customers terminating fixed-term contracts early, citing a violation of consumer rights. The National Consumer Commissioner sees the ruling as a crucial victory against unscrupulous practices in the telecommunications industry.

Exacerbating conflict

For some time, headlines have revealed that tech companies sourcing coltan, tin, tungsten and other minerals [without sufficient due diligence](#) has funded illegal mining activities that directly or indirectly support armed groups in conflict affected areas. More recently, investigations are demonstrating the impact of social media platforms' policies and practices in [exacerbating conflict](#) by failing to prevent incitement to violence. Online platforms have been used to spread hate and misinformation that escalates tensions and contributes to the polarisation of communities. For example, given the rise of violence and xenophobia in South Africa, Global Witness and the Legal Resources Centre [collaborated on an investigation](#) assessing Facebook, TikTok and YouTube's effectiveness in detecting and removing hate speech against refugees and migrants. The investigation involved submitting real-world examples of hate speech as scheduled advertisements; all three platforms approved every ad, except for one rejected by Facebook in English and Afrikaans but accepted in Xhosa and Zulu. These types of gaps leave ample room for hate and violence to fester.

Translating rights to material risk:

Safety & security of person and right to life

👉 Kenya: [Ethiopians & Kenyan rights groups sue Meta for posts inciting violence in Tigray war](#)

Risks: **Legal** **Reputational** **Financial**

Meta was sued in Kenya by victims of ethnic violence in Ethiopia for allegedly failing to conduct proper content moderation on the platform and fuelling violence and hate speech during the Tigray war in which over 500,000 Ethiopians reportedly died. Two Ethiopian researchers claimed that their father was killed during the Tigray conflict due to hateful posts against him on Facebook. They are seeking the creation of a USD 1.6 billion fund for victims.