Issue #14

INTEL WATCH

July 2026

Watching the watchers. Guarding the guardians.

THE WATCHER

Monthly

DEFENDING HUMAN RIGHTS, PROTECTING CIVIC SPACE

DO YOU KNOW WHO'S WATCHING YOU? WE'RE HERE TO HELP YOU FIND OUT

EXCLUSIVE INTELWATCH REPORT

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

THIS MONTH UNDER THE MICROSCOPE

WELCOME TO ISSUE #14 OF THE WATCHER

In this Issue #14 of The Watcher, we shine light on a must read exclusive report by Intelwatch titled ***Biometrics, Border Control and Surveillance in Angola*** - a report that is based on field research conducted in Angola and on documentary analysis and maps the systems, vendors and rights risks along Angola's borders with the Democratic Republic of the Congo and Namibia, and their implications for the 2027 elections.

In this Issue #14 we ask: What happens when the technologies designed to protect us become the very tools that expose us? as we examine a rapidly evolving digital landscape where cyber threats, artificial intelligence and surveillance technologies are becoming increasingly intertwined with everyday life. From South Africa's escalating wave of cyberattacks and costly data breaches to growing concerns over ransomware, hidden smartphone data collection and AI-powered phishing campaigns, this issue reveals how individuals, businesses and governments are confronting an increasingly complex and relentless digital threat environment.

This edition also explores the accelerating expansion of surveillance technologies across Africa and beyond. We investigate South Africa's intensifying debate over facial recognition, new efforts to regulate surveillance in estates and shopping centres, and growing concerns over biometric data collection, spyware and zero-click mobile attacks. Beyond the technology itself, we examine how digital monitoring is reshaping democratic freedoms—from allegations of surveillance targeting journalists and activists in Kenya, Nigeria and Uganda, to spyware operations, internet restrictions and AI-enabled monitoring that are increasingly being used to influence, intimidate and suppress dissent around the world.

Issue #14 further highlights the growing convergence of artificial intelligence, cybersecurity and human rights. As AI transforms both cyber defence and cybercrime, governments, technology companies and civil society are confronting urgent questions about privacy, accountability and the future of digital freedom. Through investigations, regional developments and global case studies, The Watcher uncovers the systems quietly shaping our digital lives—reminding us that cybersecurity is no longer just about protecting data, but about safeguarding democracy, human rights and the freedoms that depend on them.

THIS MONTH'S FOCUS

A report by Intelwatch, mapping the systems, vendors and rights risks along Angola's borders with the Democratic Republic of the Congo and Namibia, and their implications for the 2027 elections

This section examines the rapidly evolving surveillance and cybersecurity landscape, highlighting the technologies, policies and incidents shaping digital security across South Africa and the world. Readers will find coverage of major cyberattacks targeting critical infrastructure, businesses and public institutions, alongside analyses of ransomware trends, large-scale data breaches, mobile malware and supply-chain compromises. The section also explores the expansion of facial recognition systems, biometric surveillance, spyware, smartphone data collection, AI-enabled cyber threats, online privacy debates and emerging digital governance frameworks. Beyond reporting on individual incidents, these stories reveal how governments, corporations and cybercriminals are transforming the digital environment, exposing new vulnerabilities while redefining the relationship between security, technology and privacy.

This section tracks the growing use of surveillance technologies, spyware and digital controls to monitor, intimidate and suppress journalists, activists, opposition figures and civil society around the world. The stories investigate allegations of state surveillance in countries including Kenya, Nigeria, Uganda, Morocco, Russia and India, while also examining how digital monitoring, biometric systems, internet restrictions and commercial spyware are increasingly intersecting with electoral politics, media freedom, freedom of expression and civic space. The section further explores the broader human rights implications of pervasive surveillance, including its psychological effects, its impact on democratic participation and peaceful assembly, and the expanding role of digital technologies in enabling repression beyond traditional forms of state control.

This section explores the expanding capabilities, operations and oversight challenges surrounding intelligence agencies and state security institutions in an increasingly digital world. Readers will encounter investigations into the deployment of advanced surveillance technologies, cyber-espionage operations, intelligence gathering, digital forensics and the growing convergence of artificial intelligence with national security. The section examines how governments are strengthening their intelligence capabilities through biometrics, cyber operations, communications interception and AI-assisted analysis, while also highlighting the legal, ethical and human rights concerns that arise when these powers operate with limited transparency or accountability. Collectively, these articles provide insight into how intelligence services are adapting to emerging technological threats and the implications these developments hold for privacy, democratic governance and international security.

EXCLUSIVE INTELWATCH REPORT

BIOMETRICS, BORDER CONTROL AND SURVEILLANCE IN ANGOLA

BY INTELWATCH

DOWNLOAD REPORT

Executive summary

More than 50 years after independence from Portugal in November 1975, Angola's development stands at a decisive crossroads. Confronted by porous and poorly governed borders, endemic cross-border crime and unregulated trading, and seemingly unending instability in the neighbouring Democratic Republic of Congo (DRC), the Angolan government has embarked on one of the most ambitious technological transformation programmes in its post-independence history: the mass deployment of biometric surveillance systems at its land border posts.
The legitimacy of this effort is not in dispute, given that Angola's borders are extremely porous, with associated economic and security implications. Illicit diamond smuggling, human trafficking, arms movements, and irregular migration are highlighted as serious threats to national security. Hence, the case for a modern, technology-enabled border governance system has merit.

What this report demonstrates, however, is that the conditions under which these systems are being introduced — the opacity of procurement, the weakness of legal safeguards, the historical patterns of state repression, and the proximity of a pivotal electoral cycle (national elections are due in 2027) — transform an otherwise legitimate security management project into a potential
instrument of surveillance overreach and accompanying authoritarian entrenchment.

Key findings:

1. There is no operational biometric system at the Angola–DRC border.
2. Santa Clara (Namibia border) is the sole functioning biometric post — and it is degraded
3. The projects build a centralised identity infrastructure, not merely border tools.
4. Procurement is opaque, vendor-driven and tied to political interests.
5. Intelligence services can reach biometricdata with no judicial oversight.
6. The legal framework exists on paper but is unenforced against the state
7. The 2027 elections are the real stakes.
8. A 50 per cent documentation deficit makes the system exclusionary by design.
9. Counterterrorism and foreign interference narratives are being instrumentalised to justify surveillance expansion and chill dissent.
10. Foreign vendor dependency raises data-sovereignty concerns
11. Border surveillance in the diamond rich northeastern Lundas provinces sits under presidential, not ministerial, control.
12. The securitisation case for biometrics is unproven

SURVEILLANCE UPDATES

52% OF SOUTH AFRICANS RISK HAVING THEIR IDS OR PASSPORTS STOLEN FROM THEIR SMARTPHONES

IMAGE SOURCE: MY BROADBAND

More than half of South Africans (52%) are storing sensitive identity documents—including ID books, smart ID cards and passports—as easily accessible images on their smartphones, significantly increasing their risk of identity theft if their devices are lost, stolen or compromised by malware. According to a new Kaspersky survey, smartphones have become the primary internet device for 48% of South Africans—and 67% of those aged 18 to 28—leading users to store an increasing amount of sensitive personal and financial information on a single device. Beyond identity documents, the survey found that 73% of users keep personal photos and videos on their phones, 67% store contact information, 66% retain messages and chat histories, while 55% save financial credentials and login details. Cybersecurity experts warn that this concentration of sensitive information makes smartphones highly attractive targets for cybercriminals, particularly as mobile banking Trojans and credential-stealing malware continue to surge globally. Kaspersky advises users to avoid storing critical documents as unprotected images in their photo galleries, recommending instead the use of encrypted document vaults, secure password managers, cloud backups and multi-factor authentication to reduce the impact of device theft or malware infections. The findings underscore how smartphones have become central repositories of digital identity, making stronger mobile security practices essential to protecting both personal privacy and financial security (22 July 2026). My Broadband

SOUTH AFRICAN DATA CENTRE BUILDER ALLEGEDLY HIT BY CYBERATTACK

IMAGE SOURCE: MY BROADBAND

A South African engineering and technology infrastructure company involved in the development of major national facilities—including data centres for Liquid Intelligent Technologies, the Johannesburg Stock Exchange (JSE), Eskom, and high-profile entertainment developments such as Sun City and Montecasino—has reportedly been targeted in a cyberattack by Payload ransomware group. The incident highlights growing concerns around the vulnerability of companies operating within critical digital infrastructure supply chains, where a compromise of one contractor can potentially expose multiple organisations and sectors. While details of the attack remain limited, cybersecurity experts warn that infrastructure providers are increasingly attractive targets because they possess privileged access to networks, systems and technical environments belonging to major clients. Supply-chain attacks have become a growing global threat, with cybercriminals often targeting service providers, contractors and technology partners rather than directly attacking larger organisations with stronger security controls. The reported incident reinforces concerns about South Africa's expanding digital ecosystem, where data centres and technology service providers have become essential components of financial markets, energy systems and public services. Experts emphasise the need for stronger third-party risk management, continuous monitoring, robust access controls and improved cybersecurity standards across the technology supply chain to prevent a single compromised provider from creating widespread disruption (25 July 2026). My broadband

SOUTH AFRICAN TECH DISTRIBUTOR HIT BY MAJOR CYBERATTACK

IMAGE SOURCE: MY BROADBAND

One of South Africa's largest technology distributors has suffered a major network outage allegedly caused by a cyberattack, disrupting business operations and raising concerns about the vulnerability of critical technology supply chains. The affected company, which provides hardware, software and IT services to organisations across the country, reportedly experienced widespread system disruptions that impacted internal operations, customer services and digital platforms. While details of the incident remain limited, the attack highlights the growing risks facing technology distributors, which often represent attractive targets because they sit at the centre of multiple business networks and maintain access to large volumes of customer, supplier and infrastructure data. Cybersecurity experts warn that attackers increasingly target third-party providers as a pathway into larger ecosystems, exploiting weaker security controls in supply chains rather than directly attacking high-value organisations. The incident reinforces concerns that South Africa's expanding digital economy remains exposed to ransomware, network intrusions and supply-chain attacks, emphasising the need for stronger cyber resilience measures, including improved vendor security assessments, multi-factor authentication, incident response planning and continuous monitoring of interconnected systems (19 July 2026). My Broadband

CYBERCRIMINALS ARE COMING FOR SOUTH AFRICA'S SPORTS CLUBS

IMAGE SOURCE: FA NEWS

South Africa's sports clubs are becoming attractive targets for cybercriminals as growing digitalisation leaves many community organisations holding valuable personal data but lacking adequate cybersecurity defences. From running clubs and cycling groups to school teams and provincial federations, sporting organisations increasingly rely on online membership portals, payment platforms and event registration systems that store identity numbers, medical information, contact details and financial records—making them prime targets for ransomware, business email compromise (BEC), WhatsApp impersonation scams and identity theft. Cybersecurity experts warn that attackers are not targeting clubs because of their size, but because they often rely on outdated websites, weak passwords, shared volunteer accounts and unpatched systems that are easy to exploit. The consequences can be severe, ranging from stolen member data and financial fraud to ransomware attacks that disrupt sporting events and threaten to leak sensitive information. Beyond the immediate financial losses, a cyberattack can erode member trust, damage sponsorship relationships and expose clubs to significant legal obligations under South Africa's Protection of Personal Information Act (POPIA), including mandatory breach notifications and potential regulatory fines. The growing threat underscores that even volunteer-driven sports organisations must adopt basic cyber hygiene measures—such as multi-factor authentication, regular backups, phishing awareness training and secure cloud storage—to protect both their members and their long-term reputation (13 July 2026). FA News

DATA BREACHES COST SOUTH AFRICA AN ESTIMATED R142 BILLION ANNUALLY

IMAGE SOURCE: IOL

South Africa's escalating data breach crisis is costing the economy an estimated R142 billion annually, equivalent to roughly 1.8% of the country's GDP, according to new analysis based on more than 3,200 reported data breaches during the 2025/26 financial year. Using IBM's Cost of a Data Breach Report 2025, cybersecurity firm Cube ICT Solutions estimates that the average breach now costs South African organisations R44.1 million, with financial losses extending far beyond system recovery to include reputational damage, customer attrition, legal costs and lost productivity. Experts argue that many of these incidents stem not from sophisticated cyberattacks but from preventable human errors such as misconfigured databases, phishing attacks, lost devices and accidental data disclosures. The report calls for organisations to prioritise cybersecurity awareness training and cultivate a "human firewall" by equipping employees to recognise and report cyber threats before they escalate. As cyber incidents continue to rise across both the public and private sectors, the findings highlight that improving cyber resilience is not only a security imperative but also an economic necessity, with stronger cyber hygiene capable of protecting businesses, consumers and South Africa's long-term digital growth (July 2026). IOL

SA HUMAN RIGHTS COMMISSION WEBSITE BREACHED BY MALWARE ATTACK

IMAGE SOURCE: MY BROADBAND

The South African Human Rights Commission (SAHRC) has confirmed that its website was compromised after attackers exploited a vulnerability in a third-party Joomla extension to inject malicious code capable of infecting visitors' devices. The breach involved a ClickFix social engineering attack, in which users were presented with a fake reCAPTCHA verification prompt instructing them to open Windows Run and execute malicious PowerShell commands. Security researchers identified the attack as a delivery mechanism for information-stealing malware, including variants such as Lumma Stealer, Vidar, StealC and ACR Stealer, all designed to harvest passwords, browser data and other sensitive information. The compromise was detected on 7 July 2026, after a cybersecurity researcher flagged the malicious activity, prompting the SAHRC and its IT service provider to remove the infected files, patch the vulnerable extension, change system credentials and implement additional security measures. The Commission stated that there is no evidence its database or user information was compromised, attributing the incident solely to the compromised web pages. The attack highlights the growing exploitation of trusted public sector websites to distribute malware through social engineering, demonstrating how even reputable institutions can become unwitting vectors for cybercriminal campaigns when third-party software vulnerabilities go unpatched (15 July 2026). My Broadband

SOUTH AFRICA'S FACIAL RECOGNITION DEBATE INTENSIFIES

IMAGE SOURCE: MODERN TREATISE

South Africa's growing adoption of facial recognition technology is fuelling a national debate over whether expanding biometric surveillance risks reinforcing historical patterns of inequality under the guise of crime prevention. As governments and private security firms roll out thousands of AI-enabled CCTV cameras across cities such as Cape Town and Gauteng, supporters argue the systems strengthen policing by identifying suspects, tracing stolen vehicles and improving public safety. However, critics warn that weak regulation under the Protection of Personal Information Act (POPIA), extensive data sharing between public authorities and private surveillance companies, and limited independent oversight create significant risks for privacy and civil liberties. The article also highlights longstanding concerns that facial recognition algorithms can exhibit racial bias, increasing the likelihood of misidentification among Black South Africans, while surveillance infrastructure remains disproportionately concentrated in wealthier, historically white neighbourhoods. These concerns have prompted comparisons with apartheid-era systems of monitoring and control, with digital rights advocates arguing that stronger legal safeguards, greater transparency and rigorous oversight are essential to prevent emerging surveillance technologies from entrenching existing inequalities under the banner of public security (10 July 2026). Modern treatise

SOUTH AFRICA TIGHTENS RULES ON ESTATE AND MALL SURVEILLANCE

IMAGE SOURCE: DAILY INVESTOR

South Africa is moving to introduce stricter privacy rules governing how residential estates, shopping malls, office parks and other controlled-access environments collect and process personal information from visitors. The proposed Protection of Personal Information Act (POPIA) Code of Conduct for Gated Access Areas seeks to address growing concerns over excessive collection of identity documents, driver's licence scans, biometric information, facial recognition data and visitor records by private security systems. Under the new framework, organisations operating gated access points would be required to justify what information they collect, limit data collection to what is necessary, establish retention and deletion policies, improve security safeguards and ensure greater transparency about how personal data is processed. The move follows concerns that many estates and commercial properties have adopted intrusive surveillance practices, including copying IDs and storing visitor information indefinitely, without adequate safeguards against misuse or breaches. While the regulations are intended to balance security needs with privacy rights, they also highlight the growing tension between expanding private surveillance infrastructure and individual data protection in South Africa. As biometric technologies and digital access-control systems become increasingly common, the new rules represent a significant shift towards greater accountability for organisations responsible for managing personal information in everyday spaces (26 July 2026). Daily investor

RANSOMWARE EMERGES AS SOUTH AFRICA'S FASTEST-GROWING CYBER THREAT

IMAGE SOURCE: MY BROADBAND

Ransomware has become one of the most significant cybersecurity threats facing South African organisations, with at least 21 major institutions—including the ANC, Anglo American, Mediclinic, South African Airways, Pick n Pay, Netstar and several government departments—reportedly targeted since the beginning of 2025. According to data from Ransomware.live, cybercriminal groups are increasingly using double extortion tactics, in which they not only encrypt an organisation's systems but also steal sensitive data and threaten to publish it unless a ransom is paid. Unlike traditional ransomware, these attacks exploit phishing emails, stolen credentials and other social engineering techniques to gain initial access before moving laterally through networks and exfiltrating confidential information. Researchers note that groups such as The Gentlemen, INC Ransom and other ransomware-as-a-service (RaaS) operators have become particularly active in South Africa, reflecting a broader trend of increasingly organised, collaborative cybercrime. Beyond operational disruption, victims also face significant legal and reputational consequences under South Africa's Protection of Personal Information Act (POPIA) if personal information is compromised. The growing wave of attacks highlights the urgent need for organisations to strengthen phishing awareness, implement multi-factor authentication, maintain secure backups and adopt proactive threat detection to counter increasingly sophisticated ransomware campaigns (20 July 2026). My Broadband

RANSOMWARE ALLIANCE TARGETS SOUTH AFRICA'S INVESTMENT BOOM

IMAGE SOURCE: CYBERSPACE CHRONICLES

Cybersecurity experts are warning that a newly formed alliance between the Vect ransomware group and the TeamPCP cybercriminal collective signals a dangerous evolution in ransomware operations, with South Africa's rapidly growing investment and financial sectors emerging as attractive targets. By combining Vect's ransomware-as-a-service (RaaS) infrastructure with TeamPCP's expertise in software supply chain compromises, credential theft and large-scale intrusion campaigns, the partnership enables attackers to infiltrate organisations more efficiently before deploying ransomware and stealing sensitive data. Analysts warn that sectors handling high-value financial transactions, investor information and critical business services are particularly vulnerable, especially where third-party software dependencies and weak cybersecurity practices create exploitable entry points. The alliance reflects a broader trend towards increasingly industrialised cybercrime, in which specialised threat actors collaborate to maximise operational efficiency, expand victim pools and increase extortion profits. Security experts urge organisations to strengthen supply chain security, implement multi-factor authentication, continuously monitor for compromised credentials and improve incident response capabilities, warning that ransomware groups are increasingly targeting the weakest link in interconnected digital ecosystems rather than attacking organisations directly (6 July 2026). Cyberspace chronicles

CRIMINALS HAVE A NEW TARGET IN SOUTH AFRICA

IMAGE SOURCE: BUSINESS TECH

Cybersecurity experts are warning South Africans that cybercriminals are increasingly targeting consumers during major sporting events, particularly the Springboks' Nations Championship campaign, by exploiting the expected surge in online shopping, takeaways, and courier deliveries. Fraudsters are sending convincing phishing messages via SMS, WhatsApp, and email that impersonate trusted retailers and delivery companies, falsely claiming there is an issue with a package or that an urgent payment is required to complete a delivery. These messages often contain malicious links designed to steal banking credentials, personal information, or install malware on victims' devices. Security specialists note that these scams rely on creating a sense of urgency and legitimacy, making them increasingly difficult to distinguish from genuine communications. Consumers are therefore urged to verify delivery updates only through official retailer or courier websites or apps, avoid clicking on unsolicited links, enable multi-factor authentication on their accounts, and remain vigilant against unexpected requests for personal or financial information, particularly during periods of increased online shopping activity (26 July 2026). Business Tech

MOZAMBIQUE JOINS NEW GLOBAL ARTIFICIAL INTELLIGENCE ORGANIZATION

IMAGE SOURCE: 360 MOZAMBIQUE

Mozambique has become one of the 29 founding members of the newly established World Artificial Intelligence Cooperation Organization (WAICO), an intergovernmental initiative launched in Shanghai to strengthen international cooperation on artificial intelligence development and governance. By joining the organisation, Mozambique aims to accelerate its digital transformation by gaining access to AI expertise, emerging technologies, investment opportunities, and international research partnerships. Membership is expected to support the country's efforts to modernise key sectors such as public administration, healthcare, education, agriculture, and economic development while promoting the ethical, inclusive, and responsible use of AI. The move also positions Mozambique to collaborate more closely with other developing nations in shaping global AI standards, reducing the technological divide between developed and developing countries, and ensuring that AI contributes to sustainable development, innovation, and long-term economic growth (27 July 2026). 360 mozambique

KENYA'S PRESIDENTIAL WEBSITE BREACHED IN BITCOIN RANSOM ATTACK

IMAGE SOURCE: TECHPOINT

Kenya's official presidential website was compromised by hackers who briefly seized control of the platform, replacing its homepage with hostile messages targeting President William Ruto and demanding a ransom payment of five Bitcoin in exchange for withholding the release of unspecified information. The attackers displayed a cryptocurrency wallet address and threatened to leak alleged sensitive material if the payment was not made, turning the breach into both a financial extortion attempt and a highly visible political statement. Kenya's government confirmed the cybersecurity incident, stating that response teams had activated containment measures and that there was no evidence of unauthorised access to sensitive government data, data exfiltration or information loss. The website was temporarily restricted while forensic investigations and restoration efforts were conducted before being brought back online. The attack highlights the growing vulnerability of government digital infrastructure across Africa, where public websites have become attractive targets for cybercriminals and hacktivists because of their symbolic importance, public visibility and potential impact on public trust. Cybersecurity experts argue that government platforms are often compromised not because of advanced hacking techniques, but due to weaknesses such as outdated content management systems, poor access controls, insufficient monitoring and limited long-term cybersecurity investment. The incident also follows previous attacks against Kenyan government systems, reinforcing concerns that as states digitise public services, government websites must be treated as critical infrastructure requiring continuous security investment rather than one-off technology projects (29 July 2026). TechPoint

MILLIONS OF AFRICAN SMARTPHONES ALLEGEDLY SENDING HIDDEN DATA OVERSEAS

IMAGE SOURCE: MY BROADBAND

Security researchers have raised concerns over the discovery of pre-installed software on millions of smartphones widely used across Africa that allegedly collects and transmits sensitive user data without clear user awareness. The investigation claims that devices manufactured by Transsion Holdings—including popular brands such as Tecno, Infinix and itel—contain system-level applications capable of gathering information such as device identifiers, location data, app activity and network information. Researchers argue that because the software is embedded into the operating system, ordinary users have limited ability to remove or disable these data-collection mechanisms. The concerns are particularly significant in African markets, where Transsion dominates the affordable smartphone sector and millions of users rely on its devices as their primary gateway to digital services. Privacy advocates warn that opaque data practices by major technology manufacturers could expose users to surveillance risks, identity threats and unauthorised profiling, especially in regions where consumer protections and data governance frameworks remain uneven. The allegations have renewed debate around digital sovereignty, transparency in smartphone supply chains and the responsibility of technology companies to clearly disclose what personal information is collected, where it is stored and how it is used. The controversy reflects wider concerns across Africa regarding the rapid expansion of digital technologies without equivalent investment in privacy protections and regulatory oversight (24 July 2026). Streamline

EU CHAT CONTROL REIGNITES GLOBAL ENCRYPTION DEBATE

IMAGE SOURCE: STREAMLINE FEED

The European Union's decision to extend its controversial Chat Control framework has intensified global concerns over the future of private digital communication and end-to-end encryption. The regulation allows online platforms to continue voluntarily scanning user communications for child sexual abuse material (CSAM) while EU lawmakers negotiate a permanent framework, prompting cybersecurity experts and privacy advocates to warn that expanded message scanning could undermine the security foundations of encrypted communication. Supporters argue that the measures are necessary to combat online child exploitation and prevent criminals from abusing encrypted platforms to hide illegal activity. However, critics contend that technologies capable of scanning private messages could create new vulnerabilities, weaken encryption protections and establish surveillance mechanisms that may later be expanded beyond their original purpose. The debate has become particularly significant for services such as secure messaging platforms, with digital rights groups warning that any weakening of encryption standards in one major market could have global consequences because technology companies typically operate unified systems worldwide. The controversy highlights a growing tension between online safety and digital privacy, raising fundamental questions about whether governments can combat serious online crimes without creating systems that compromise the confidentiality and security of all users (27 July 2026). Streamline feed

CHINA-LINKED HACKERS EXPAND GLOBAL PHISHING CAMPAIGNS

IMAGE SOURCE: THE HACKER NEWS

A suspected China-linked cybercrime group known as TA4922 has significantly expanded its phishing operations beyond East Asia, launching sophisticated campaigns targeting organisations in the United Kingdom, Germany, Italy, South Africa and other regions using highly localised social engineering tactics. According to cybersecurity researchers, the financially motivated group disguises phishing emails as legitimate tax notices, payroll updates, HR documents, invoices and government communications tailored to each country's language and institutions, increasing the likelihood that victims will engage with malicious attachments or links. The campaigns deploy an evolving arsenal of malware—including Atlas RAT, RomulusLoader, SilentRunLoader and ValleyRAT (Winos 4.0)—to establish persistent access, steal credentials, exfiltrate sensitive data and facilitate financial fraud or the resale of compromised network access. Researchers note that TA4922 operates at an unusually high tempo, frequently rotating malware families, phishing themes and delivery techniques to evade detection. The expansion underscores the growing sophistication of modern phishing operations, demonstrating how cybercriminal groups are increasingly leveraging localisation, adaptive malware and rapid campaign changes to target organisations across multiple continents with greater effectiveness (4 June 2026). The Hacker News

HIDDEN SYSTEM SOFTWARE RAISES PRIVACY CONCERNS FOR AFRICA'S BIGGEST PHONE BRANDS

IMAGE SOURCE: KORBEN

New security research has raised concerns that millions of Tecno, Infinix and itel smartphones—manufactured by Transsion, Africa's largest smartphone vendor—contain deeply embedded system software capable of collecting extensive user data that cannot easily be removed by device owners. According to reverse engineering conducted by independent researcher Buchodi, the proprietary Athena framework and oneID tracking system operate with elevated system privileges, enabling the collection of precise GPS location, nearby cell tower information, app usage across dozens of applications, foreground activity and notifications when apps access a device's camera. Researchers claim the telemetry is transmitted to servers operated by Transsion's software subsidiary, raising concerns about the scale of data collection, the lack of meaningful user consent and the difficulty of disabling the software without modifying the operating system. Given Transsion's dominant market share across Africa, privacy advocates warn that the findings could have significant implications for millions of users, particularly in countries with limited data protection enforcement. The case has renewed calls for greater transparency from smartphone manufacturers, stronger regulatory oversight and clearer disclosure of what data is collected by pre-installed system services before devices reach consumer (9 July 2026). Korben

AFRICAN STARTUP TACKLES THE CONTINENT'S DIGITAL TRUST GAP

IMAGE SOURCE: BUSINESS INSIDER AFRICA

As cyber threats continue to rise across Africa, Nigerian cybersecurity startup Cybervergent is positioning itself to address what experts estimate is a US$3.5 billion digital trust gap by helping organizations strengthen cybersecurity, regulatory compliance and operational resilience through a single AI-powered platform. Founded by Adetokunbo Omotosho, the company aims to simplify governance, risk and compliance (GRC) by replacing fragmented security tools with an integrated system that enables businesses to continuously monitor cyber risks, demonstrate compliance and build customer trust. The platform responds to growing regulatory requirements such as South Africa's POPIA and Nigeria's Data Protection Act, while addressing the shortage of cybersecurity expertise that leaves many African organisations vulnerable to attacks. As digital transformation accelerates across the continent, Cybervergent's founders argue that trust has become a critical component of economic growth, with secure and compliant digital infrastructure serving as the foundation for resilient financial systems, e-commerce and cross-border digital services. Their approach highlights a broader shift in Africa's cybersecurity landscape—from reacting to cyber incidents to proactively building trusted digital ecosystems that support long-term economic development (25 June 2026). Business Insider Africa

FIVE EYES WARNS: AI CYBER ATTACKS COULD CRIPPLE GOVERNMENTS “WITHIN MONTHS”

IMAGE SOURCE: NATURAL NEWS

Five Eyes intelligence agencies are warning that rapidly advancing AI could soon supercharge cyberattacks, making them faster to launch, harder to stop, and more damaging to government systems, businesses, and critical infrastructure. The core concern is not simply that AI can help hackers write better phishing emails or malware, but that frontier models may reduce the skill and time needed to find vulnerabilities, automate reconnaissance, and scale attacks in ways that overwhelm existing defences. That shifts cyber risk from a slow-moving technical problem into a strategic national security issue, because defenders may have only a short window to adapt before attackers start using AI to exploit systems at machine speed. For governments, the warning also points to a broader governance challenge: cybersecurity teams, policymakers, and national leaders now need to treat AI safety, access controls, and digital resilience as urgent priorities rather than future concerns (24 June 2026). Natural News

'HALLUSQUATTING' TURNS AI HALLUCINATIONS INTO A MALWARE THREAT

IMAGE SOURCE: DIGITAL SHIELD

Cybersecurity researchers have uncovered a new attack technique known as HalluSquatting, which exploits AI assistants' tendency to invent—or "hallucinate"—non-existent software repositories, packages and online resources, potentially tricking users into installing malware. Unlike traditional typosquatting, which relies on human typing mistakes, HalluSquatting targets AI coding assistants such as GitHub Copilot, Cursor, Gemini CLI and other agentic AI tools by predicting the fake repository names they are likely to generate. Attackers can then register these hallucinated names, embed malicious code or hidden prompts within them, and wait for an AI assistant to automatically retrieve and execute the compromised resource. Researchers found that AI models hallucinated repository names in up to 85% of testing scenarios—and up to 100% for certain AI skills—raising concerns that a single malicious repository could compromise thousands of developer systems, facilitate remote code execution and even contribute to large-scale botnets. The discovery highlights a new frontier in software supply chain attacks, demonstrating that as AI agents gain greater autonomy, organisations will need stronger safeguards, including repository verification, restricted AI permissions and human oversight, to prevent attackers from exploiting AI-generated errors as an entry point into critical systems (10 July 2026). Digital shield

GLOBAL CYBER FRAUD CRACKDOWN NETS 5,800 ARRESTS

IMAGE SOURCE: CYBER SCOOP

A coordinated INTERPOL operation spanning 97 countries and territories has delivered one of the largest global crackdowns on cyber-enabled financial crime, resulting in 5,811 arrests, the identification of more than 15,600 suspects and the interception of US$293 million in illicit assets. Operation First Light 2026, which ran from January to April, targeted a wide range of social engineering scams—including business email compromise, investment fraud, romance scams, sextortion and impersonation schemes—while disrupting the money laundering networks used to move criminal proceeds. Investigators analysed more than 152,000 cases, blocked over 31,000 bank accounts and identified 142,000 victims worldwide, highlighting the industrial scale of cyber-enabled fraud. Notable operations included the dismantling of a criminal syndicate in Eswatini that operated a fake Brazilian police station to deceive victims during video calls, as well as investigations in Thailand and Palau that uncovered sophisticated cryptocurrency laundering networks and scam centres. The operation demonstrates the growing importance of international intelligence sharing, rapid financial intervention mechanisms and cross-border law enforcement cooperation in combating increasingly organised cybercriminal networks operating across multiple jurisdictions (9 July 2026). Cyber scoop

ZERO-CLICK SPYWARE BECOMES THE NEW MOBILE THREAT

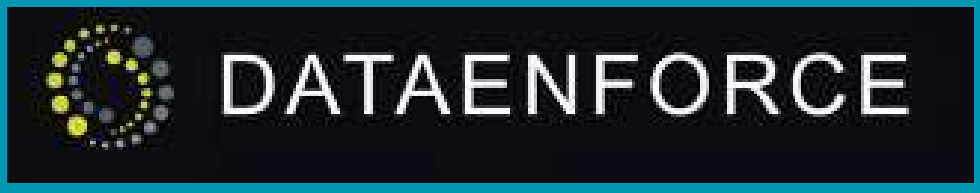

IMAGE SOURCE: DATA ENFORCE

Mercenary spyware has entered a new phase in which zero-click attacks—requiring no interaction from the victim—have become the preferred method for compromising high-profile targets, according to a new cybersecurity analysis by DataEnforce. Unlike traditional phishing campaigns, these attacks exploit vulnerabilities in messaging applications, media processing services and communication protocols, allowing attackers to silently infect smartphones through malicious images, voice call packets, document previews or other content processed automatically by the device. Once deployed, the spyware operates entirely in memory, enabling operators to access messages, emails, microphones, cameras and location data while evading conventional mobile device management (MDM) and app-based security tools. The report warns that sophisticated surveillance capabilities once reserved for intelligence agencies are now commercially available through mercenary spyware vendors, making advanced cyber espionage increasingly accessible to state and non-state actors alike. As a result, organisations are being urged to move beyond traditional endpoint protection by adopting behavioural monitoring, forensic analysis and operating system-level threat detection to defend against a new generation of stealthy mobile surveillance attacks (1 July 2026). Data enforce

BIOMETRIC DATA IS BECOMING THE NEW FRONTIER OF CONTROL

IMAGE SOURCE: HUMAN RIGHTS INSTITUTE

As biometric technologies become embedded in everyday life, scholars are warning that the collection of facial scans, fingerprints, iris patterns and behavioural data is transforming the human body into a source of digital control and economic value. The article argues that biometric systems now extend far beyond identity verification, enabling governments and technology companies to continuously monitor, classify and influence individuals through AI-driven surveillance networks. Drawing on the theories of Michel Foucault, Gilles Deleuze and Shoshana Zuboff, the author contends that society is shifting from traditional surveillance toward a "society of control," where access to public spaces, financial services and digital platforms is increasingly governed by biometric data. Rather than viewing privacy as the primary concern, the article warns that the deeper threat lies in the erosion of individual autonomy, political agency and anonymity, as biometric information becomes a tool for behavioural prediction, social exclusion and commercial exploitation. The analysis concludes that stronger legal safeguards, democratic oversight and rights-based governance are essential to prevent biometric technologies from entrenching new forms of digital authoritarianism and turning the human body itself into an instrument of algorithmic control (12 July 2026). Human Rights Institute

WARFARE IN THE DIGITAL AGE TESTS THE RIGHT TO PRIVACY

IMAGE SOURCE: VOX LEGIS

As armed conflicts become increasingly driven by digital technologies, legal experts warn that existing constitutional and international laws are struggling to keep pace with the growing use of AI, cyber operations, mass surveillance and digital intelligence gathering in warfare. The article argues that governments are increasingly relying on advanced surveillance technologies—including communications interception, biometric databases, facial recognition and AI-assisted intelligence—to identify threats and protect national security, often at the expense of individual privacy rights. While international human rights law and constitutional protections recognise privacy as a fundamental right, these safeguards are frequently challenged by broad national security powers, particularly during periods of conflict or emergency. The article highlights the need for clearer legal standards to ensure that digital surveillance remains lawful, necessary and proportionate, warning that unchecked technological capabilities risk eroding civil liberties and normalising mass surveillance long after conflicts end. As AI and cyber warfare continue to redefine modern security operations, policymakers face mounting pressure to develop legal frameworks that effectively balance national security imperatives with the protection of fundamental human rights in an increasingly digitised battlefield (1 July 2026). Vox Legis

AI SURVEILLANCE THREATENS DEMOCRATIC FREEDOMS

IMAGE SOURCE: THE GUARDIAN

As artificial intelligence rapidly enhances surveillance capabilities, experts warn that the greatest danger extends beyond privacy violations to the gradual erosion of democratic participation and social progress. Writing in The Guardian, the authors argue that AI-powered technologies—including facial recognition, real-time behavioural analysis, predictive analytics and large-scale data integration—are enabling governments to monitor populations with unprecedented speed, scale and precision. Unlike traditional surveillance, AI systems can automatically identify, profile and track individuals across multiple data sources, creating a pervasive environment in which people may self-censor, avoid protests or limit lawful political activity for fear of being watched. The article highlights growing concerns over the deployment of these technologies in countries such as China and the United States, where AI-assisted surveillance is increasingly being used to monitor immigrants, protesters and other groups under the banner of security. Calling for urgent policy intervention, the authors advocate stronger privacy protections, tighter regulation of AI-driven surveillance and restrictions on facial recognition technologies to prevent the normalisation of mass digital monitoring that could fundamentally undermine civil liberties, democratic accountability and the freedom to challenge those in power (6 July 2026). The Guardian

FAKE CLAUDE AI APP DELIVERS MALWARE THROUGH SEARCH ADS

IMAGE SOURCE: INTERNATIONAL BUSINESS TIMES

Cybercriminals are exploiting the growing popularity of artificial intelligence tools by creating a fake version of Anthropic's Claude AI assistant and promoting it through malicious online advertisements to distribute malware. According to cybersecurity researchers, attackers used Bing search advertisements to direct users searching for Claude AI to a fraudulent website designed to appear legitimate. Instead of providing access to the AI service, the fake platform delivered SectopRAT malware, a remote access trojan capable of allowing attackers to control infected devices, steal sensitive information and conduct further malicious activity. The campaign highlights how threat actors are increasingly abusing public interest in generative AI platforms to exploit user trust, particularly as millions of people turn to AI tools for professional, educational and personal tasks. Researchers warn that malicious advertising has become an increasingly effective delivery method because sponsored search results can appear alongside legitimate services, making it harder for users to distinguish genuine platforms from fraudulent copies. The incident underscores the importance of verifying AI services through official channels, avoiding suspicious downloads and recognising that the rapid growth of AI adoption has created new opportunities for cybercriminals to conduct malware distribution and social engineering campaigns (24 July 2026). International Business Times

HOW FRAUDSTERS BYPASS FACIAL RECOGNITION AND STAY HIDDEN IN 2026

IMAGE SOURCE: SUMSUBER

As facial recognition becomes a cornerstone of digital identity verification, cybercriminals are developing increasingly sophisticated methods to evade biometric security, forcing organisations to strengthen their fraud detection capabilities. According to identity verification company Sumsub, attackers are no longer relying solely on simple spoofing techniques such as photographs or pre-recorded videos, but are increasingly using AI-generated deepfakes, face-swapping technology, 3D masks, injected video feeds and synthetic identities to deceive facial recognition systems. Fraudsters are also exploiting compromised devices and manipulating the transmission of biometric data to bypass identity verification processes without physically appearing in front of a camera. Experts warn that facial matching alone is no longer sufficient to verify a person's identity, as modern attacks increasingly combine multiple techniques to imitate legitimate users. To counter these evolving threats, organisations are adopting liveness detection, behavioural analysis, device intelligence and multi-layered identity verification systems that confirm not only whether a face matches an identity document but also whether the individual is physically present and the biometric data has not been manipulated. The report highlights the escalating technological arms race between cybercriminals and security providers, demonstrating that as AI makes biometric fraud more accessible and convincing, businesses must continuously evolve their identity verification systems to stay ahead of increasingly sophisticated digital deception (2 June 2026). Sumsuber

HACKED FOOTBALL FEDERATION SPREADS WORLD CUP DISINFORMATION

IMAGE SOURCE: AFRICA TOP SPORTS

A cyberattack targeting the Argentine Football Association (AFA) demonstrates how major sporting events are becoming prime targets for hacktivism and disinformation campaigns. Following Argentina's controversial 2026 FIFA World Cup victory over Egypt, attackers believed to be linked to an Egyptian hacking group compromised an official AFA email account and distributed fraudulent messages falsely claiming that Argentina's victory had been secured through biased refereeing and corrupt officiating. The AFA quickly confirmed that one of its institutional email accounts had been breached, stressing that the messages were unauthorised and that security protocols had been activated to contain the incident while investigations continued. The hack came amid intense online controversy over disputed VAR decisions and referee bias allegations, allowing the attackers to exploit an already polarised information environment to amplify misinformation and undermine trust in official communications. The incident illustrates how cyberattacks are increasingly being used not only to steal data or disrupt systems, but also to manipulate public narratives, fuel disinformation and exploit emotionally charged global events, highlighting the growing intersection between cybersecurity, information warfare and digital trust (11 July 2026). Africa Top Sports

THE SILENT WINNERS OF THE WORLD CUP: COMPANIES EXPANDING SURVEILLANCE

IMAGE SOURCE: TECH POLICY

The 2026 FIFA World Cup has created a lucrative opportunity for technology companies involved in building and expanding global surveillance infrastructure, with digital rights researchers warning that the tournament has normalised the use of AI-powered monitoring systems far beyond the stadiums. According to an investigation by Ranking Digital Rights, at least 21 companies contributed to the surveillance ecosystem deployed across World Cup host cities in the United States, Mexico and Canada, providing technologies including facial recognition, automated licence plate readers, predictive policing tools, data integration platforms, drones and large-scale data collection systems. While these technologies were introduced under the justification of improving fan safety and preventing security threats, critics argue that the infrastructure risks becoming a permanent feature of urban policing after the tournament ends. The investigation highlights concerns that surveillance systems developed for major events often remain in place indefinitely, expanding government and corporate abilities to track, profile and analyse individuals with limited transparency or accountability. Companies including major technology and security providers have benefited from increased demand for AI-driven security solutions, while civil society groups warn that the normalisation of mass surveillance threatens privacy, freedom of expression and peaceful assembly—particularly for marginalised communities that are often disproportionately affected by monitoring technologies. The report argues that mega-events such as the World Cup have become testing grounds for surveillance expansion, where temporary security measures can evolve into permanent digital monitoring infrastructures without sufficient public oversight or human rights protections (19 July 2026). Tech Policy

GLOBAL PUSH GROWS FOR CHILD-SAFE AI REGULATION

IMAGE SOURCE: BIOMETRIC UPDATE

Pressure is mounting on governments and technology companies to place children's safety at the centre of AI regulation, as more than 100 organisations worldwide have called for stronger safeguards against the growing risks posed by artificial intelligence. The coalition argues that existing approaches are too reactive, addressing harm only after it occurs rather than requiring AI systems to be designed with child protection built in from the outset. Key recommendations include mandatory safety testing before deployment, child rights impact assessments, age-appropriate design standards, stronger transparency and accountability requirements, and meaningful oversight of AI systems that collect biometric data or influence children's online experiences. The initiative follows the UN's first Global Dialogue on AI Governance and reflects growing international concern that AI-powered recommendation systems, generative AI tools and biometric technologies are exposing children to new risks ranging from manipulation and exploitation to privacy violations and harmful content. Advocates warn that without stronger regulation, commercial incentives will continue to outpace child protection, urging policymakers to move beyond voluntary principles and implement enforceable rules that ensure AI innovation does not come at the expense of children's rights, safety and wellbeing (11 July 2026). Biometric Update

META'S AI PHOTO FEATURES SPARK FRESH PRIVACY CONCERNS

IMAGE SOURCE: KFI

Meta is facing renewed scrutiny over privacy after the launch of new AI-powered photo features that allow users to upload, analyse and transform personal images through the Meta AI app. Privacy advocates have raised concerns over how uploaded photos are stored, processed and potentially used to improve the company's AI models, particularly as many users remain unaware of the extent to which their images may contribute to AI training. Experts warn that photographs often contain sensitive information—including faces, locations and metadata—that can reveal far more than users intend to share. The controversy comes amid broader criticism of Meta's AI data practices, with consumer groups calling for clearer consent mechanisms, greater transparency and stronger user control over how personal images are collected and used. The debate underscores a wider challenge facing generative AI platforms: balancing rapid innovation with robust privacy protections, informed consent and public trust in an era where personal photos have become valuable training data for increasingly sophisticated AI systems (8 July 2026). KFI

IRAN-LINKED HACKERS ARE USING AI TO SUPERCHARGE CYBERATTACKS

IMAGE SOURCE: CYBERSECURITY DRIVE

Iran-linked state-sponsored and hacktivist groups are increasingly incorporating generative AI tools, including large language models such as ChatGPT, into their cyber operations to improve the speed, scale and sophistication of malicious campaigns. According to new threat intelligence, these actors are using AI to write and refine malware code, generate convincing phishing emails in multiple languages, translate communications, automate reconnaissance and analyse publicly available information to identify potential targets, including industrial facilities and critical infrastructure. Researchers stress that AI is not replacing traditional hacking techniques but is acting as a force multiplier, enabling threat actors to conduct more efficient social engineering campaigns, accelerate malware development and reduce the technical expertise required to launch complex cyber operations. While many AI-generated outputs still require human refinement, the technology is lowering barriers to entry and increasing operational efficiency for both state-backed groups and cybercriminals. The findings highlight a broader shift in the cyber threat landscape, where artificial intelligence is becoming an integral component of offensive cyber capabilities, prompting calls for stronger AI safeguards, enhanced threat intelligence sharing and improved organisational resilience against increasingly AI-assisted attacks (16 July 2026). Cybersecurity Dive

GOSERPENT MALWARE STEALS GOVERNMENT SECRETS THROUGH MULTI-STAGE CYBER ESPIONAGE

IMAGE SOURCE: BIOMETRIC UPDATE

Cybersecurity researchers have uncovered a sophisticated cyber-espionage campaign dubbed GoSerpent, which used a carefully coordinated chain of malware to infiltrate government and diplomatic organisations across Southeast Asia, remaining undetected for months while quietly harvesting sensitive information. According to Kaspersky, the operation began with the GoSerpent Remote Access Trojan (RAT), which established long-term access to compromised systems before deploying additional tools—including ThumbcacheService to collect Word, Excel and PDF documents, Mimikatz and QuarksDumpLocalHash to steal credentials, and Stowaway with TmcLoader to exfiltrate the stolen data through encrypted network tunnels. Researchers noted that the attackers deliberately delayed each stage of the operation, allowing malware to remain dormant for weeks before activating secondary payloads, a tactic designed to evade routine security monitoring and log retention policies. The malware also masqueraded as legitimate Windows processes and used encrypted communications, proxy capabilities and remote shell functions to maintain stealth and move laterally across compromised networks. Although attribution remains unconfirmed, researchers identified similarities with the TetrisPhantom threat actor, highlighting the campaign as an example of increasingly patient and highly coordinated cyber-espionage operations targeting government institutions. The discovery underscores the growing sophistication of advanced persistent threats (APTs), where multiple specialised tools are combined into a single, long-term intelligence-gathering campaign capable of stealing highly sensitive government information while avoiding detection (19 July 2026). Biometric Update

REPRESSION MONITOR

KENYA'S MEDIA FACES GROWING SURVEILLANCE FEARS

IMAGE SOURCE: EASTLEIGH VOICE

Fresh allegations of state surveillance have intensified concerns over press freedom in Kenya after former Deputy President Rigathi Gachagua claimed that journalists critical of President William Ruto's administration are being monitored, intimidated and targeted ahead of the 2027 general elections. Speaking at a press briefing, Gachagua alleged that senior journalists and editors—including personnel from Standard Media Group—had been placed under surveillance and "marked" for a wider crackdown, warning that investigative reporters covering corruption and government misconduct were operating under constant threats from state agencies. He further claimed that the government intends to financially weaken independent media through reduced state advertising and could interfere with internet access during the election period, allegations the government has not substantiated or acknowledged. While no evidence has been publicly presented to verify the surveillance claims, the allegations have fuelled broader concerns over the use of digital monitoring and political pressure to silence independent journalism, highlighting the growing intersection of cybersecurity, surveillance and media freedom in East Africa (30 June 2026). Eastleigh voice

SPYWARE ALLEGATIONS RAISE ALARM OVER DIGITAL REPRESSION IN NIGERIA

IMAGE SOURCE: ICIR NIGERIA

An investigation by the International Centre for Investigative Reporting (ICIR) alleges that authorities in Nigeria's Kogi State have deployed sophisticated surveillance technologies and security operatives to monitor, intimidate and detain journalists, activists and political critics under the guise of maintaining security. The report traces procurement records linking the state to surveillance equipment supplied through international vendors, including technology reportedly capable of intercepting communications and tracking mobile devices. Victims described being lured into arrests through deceptive phone calls, followed by prolonged surveillance, harassment and detention after criticising government officials online. While security experts warn that the growing use of spyware without robust legal oversight poses serious risks to privacy, freedom of expression and democratic accountability, Nigerian security officials have rejected the allegations, insisting that surveillance activities comply with legal procedures and standard operating protocols. The investigation underscores broader concerns over the rapid expansion of state surveillance capabilities across Africa and the increasing use of cyber-enabled monitoring tools to suppress dissent and shrink civic space (28 June 2026). ICIR Nigeria

UGANDA'S EXPANDING SURVEILLANCE SYSTEM RAISES RIGHTS CONCERNS

IMAGE SOURCE: USAA

Uganda is facing growing criticism over the expansion of state surveillance capabilities and restrictions on digital freedoms, with human rights organisations warning that new technologies are being deployed in ways that threaten privacy, political participation and freedom of expression. The country has expanded its surveillance infrastructure through the installation of public-space monitoring systems, collection of biometric information—including names, photographs, signatures and fingerprints—and the use of communication interception powers justified on national security grounds. Authorities have also introduced digital vehicle number plates designed to enable location tracking, raising concerns about the scale of government data collection and the lack of sufficient safeguards governing how information is stored, accessed and used. Critics argue that these surveillance tools have been introduced within a broader environment of restrictions on journalists, activists, opposition figures and civil society organisations, where digital monitoring can contribute to self-censorship and discourage political engagement. Digital rights advocates warn that Uganda's experience reflects a wider trend across Africa, where governments are increasingly adopting biometric systems, AI-enabled monitoring and data-driven policing without equivalent investment in transparency, accountability and privacy protections. The debate highlights the growing challenge facing governments across the continent: ensuring that cybersecurity and public safety measures do not become mechanisms for expanding state control over citizens' digital lives (24 July 2026). USAA

WHISTLEBLOWER EXPOSES MOROCCO'S EXTENSIVE PEGASUS SPYWARE OPERATIONS

IMAGE SOURCE: THE GUARDIAN

A former officer from Morocco's domestic intelligence agency has provided the most detailed insider account to date of the country's alleged use of Pegasus spyware, revealing a sophisticated surveillance apparatus that targeted journalists, human rights defenders, political dissidents and foreign government officials. According to a joint investigation led by The Guardian, Forbidden Stories and media partners, the whistleblower—identified only as "Safir"—confirmed that Morocco's Directorate General for Territorial Surveillance (DGST) began deploying the Israeli-made spyware in 2017 after receiving training from NSO Group, initially relying on phishing links before adopting advanced zero-click exploits capable of infecting devices without user interaction. Safir alleged that Pegasus formed only one part of a broader surveillance ecosystem that included IMSI catchers, network interception tools, hidden cameras and other spyware used to monitor communications, track targets and gather intelligence on domestic critics and foreign officials, including senior French and Spanish politicians. The investigation also claims that Moroccan authorities worked closely with telecommunications providers to facilitate covert data extraction, while using the intelligence gathered to intimidate critics and suppress dissent. Although Moroccan authorities have consistently denied using Pegasus and NSO Group has maintained that its products are intended solely for legitimate law enforcement and counterterrorism purposes, the whistleblower's testimony provides unprecedented insight into how commercial spyware can become a cornerstone of state surveillance, reinforcing global concerns over the lack of oversight governing the cyber-mercenary industry (16 July 2026). The Guardian

POLICE SURVEILLANCE SHADOWS AI DATA CENTRE PROTESTS

IMAGE SOURCE: THE INTERCEPT

An investigation by The Intercept reveals that local law enforcement agencies in the United States are increasingly deploying advanced surveillance technologies to monitor communities protesting the construction of AI data centres. Internal police records obtained through public records requests show authorities using drones, automated licence plate readers, social media monitoring and intelligence-sharing networks to track activists opposing large-scale data centre developments over concerns about environmental damage, water consumption and energy use. In several cases, peaceful protesters were reportedly categorised as potential security threats, with information shared across regional law enforcement agencies despite little evidence of criminal activity. Civil liberties advocates argue that these tactics reflect a growing trend of using sophisticated surveillance tools to monitor lawful civic activism, raising concerns that critical infrastructure projects linked to the AI industry are becoming increasingly intertwined with expansive policing and intelligence practices. The investigation underscores how the rapid growth of AI infrastructure is not only reshaping digital economies but also expanding the surveillance capabilities used to monitor public dissent, reigniting debates over privacy, transparency and the right to peaceful protest (1 June 2026). The Intercept

MODI FACES CHALLENGE FROM ACTIVISTS OVER SURVEILLANCE AT INDIA YOUTH PROTEST

IMAGE SOURCE: DAWN

Indian Prime Minister Narendra Modi's government is facing growing criticism from activists over allegations of expanded surveillance during youth-led protests, raising concerns about the use of digital monitoring tools to track political dissent. The controversy centres on claims that authorities have used advanced surveillance capabilities, including facial recognition, digital monitoring systems and other data-driven policing methods, to identify and monitor protesters participating in demonstrations. Civil society groups argue that the deployment of such technologies without clear transparency, independent oversight or strong privacy safeguards risks creating a chilling effect on freedom of expression and peaceful assembly. Activists warn that mass surveillance systems can transform ordinary political participation into a monitored activity, discouraging citizens—particularly young people—from engaging in public debate or opposing government policies. The dispute reflects broader concerns across India regarding the rapid expansion of surveillance infrastructure, including facial recognition networks and digital identity systems, amid limited legal protections governing biometric data collection and state access to personal information. As governments worldwide increasingly adopt AI-enabled policing tools, rights advocates argue that security measures must be balanced with constitutional protections for privacy, democratic participation and civil liberties (27 July 2026). Dawn

RUSSIA USED CELLEBRITE TOOL TO JAIL ACTIVIST AFTER COMPANY CLAIMED TO HAVE ENDED CONTRACT

IMAGE SOURCE: ACCESS NOW

Russia used Cellebrite's phone-extraction tools to access the iPhone of prominent activist Andrey Pivovarov after the company said it had stopped selling to Russia, raising fresh concerns about surveillance technology being used for political repression. The case highlights a wider problem in cybersecurity and digital forensics: tools designed to extract data from seized devices can become instruments of abuse when used against dissidents, especially if vendor restrictions are weak or unenforced. It also underscores the vulnerability of activists once a phone is physically in state hands, since investigators can recover messages, contacts, app data, and other sensitive information that may expose networks of supporters and broader opposition activity. The broader takeaway is that spyware and forensic tools are not neutral technologies; their impact depends on who controls them, how tightly they are regulated, and whether companies can actually prevent misuse across borders (25 June 2026). Access Now

KREMLIN TIGHTENS GRIP ON RUSSIA'S INTERNET

IMAGE SOURCE: CEPA

Russia is intensifying its control over the internet as the Kremlin deliberately throttles mobile internet access and restricts online communications to curb the spread of information that could undermine the government. According to the Center for European Policy Analysis (CEPA), mobile internet usage has fallen significantly in some regions due to state-imposed restrictions aimed at limiting citizens' ability to share videos of drone strikes, protests and other politically sensitive events. The measures form part of Russia's broader "sovereign internet" strategy, which enables authorities to isolate regions from the wider internet and tighten control over online information during periods of unrest. Analysts warn that the growing restrictions are accelerating Russia's shift toward a state-controlled digital ecosystem, raising concerns over censorship, surveillance and the erosion of digital freedoms as authorities prioritise political control over open internet access (24 July 2026). CEPA

RUSSIA ACCUSES TELEGRAM FOUNDER OF AIDING TERRORISM IN ITS LATEST ONLINE CRACKDOWN

IMAGE SOURCE: THE GUARDIAN

Russia has formally accused Telegram founder Pavel Durov of aiding terrorism and placed him on an international wanted list, alleging that the messaging platform failed to remove channels, bots, and content used by Ukrainian intelligence, extremist groups, and terrorist organisations to coordinate sabotage, recruit individuals, commit cyber fraud, and facilitate attacks inside Russia. The charges, brought by the Federal Security Service (FSB), carry the possibility of a life sentence if Durov is convicted. Durov, who lives in Dubai and holds French and UAE citizenship, has not publicly responded to the latest allegations, although he has previously argued that similar actions are politically motivated attempts to undermine online privacy and freedom of expression. The case represents a significant escalation in Russia's long-running efforts to tighten control over digital communications, with authorities increasingly restricting foreign platforms while promoting state-backed alternatives. Critics have also highlighted the apparent contradiction that Telegram continues to be widely used by Russian officials, military personnel, and pro-Kremlin channels despite the government's claims that the platform facilitates terrorism (29 July 2026). The Guardian

DIGITAL SURVEILLANCE IS BREAKING ACTIVIST MENTAL HEALTH

IMAGE SOURCE: GLOBAL VOICES

A new report by United Nations Special Rapporteur Gina Romero warns that pervasive digital surveillance is having a profound psychological impact on activists, journalists, human rights defenders, and civil society organisations worldwide. The report argues that constant monitoring through facial recognition, spyware, biometric systems, social media tracking, and other digital technologies has created a climate of fear and hypervigilance, leading to chronic stress, anxiety, burnout, depression, and trauma among those engaged in advocacy and dissent. Beyond its mental health consequences, surveillance is also producing a significant "chilling effect," discouraging individuals from participating in protests, joining organisations, communicating freely, or expressing dissent due to fears of being identified, monitored, or targeted. The report urges governments to adopt stronger legal safeguards, ensure surveillance measures are lawful, necessary and proportionate, and recognise the long-term psychological harm that unchecked digital surveillance inflicts on civic participation and fundamental human rights (23 June 2026). Global voices

SPYWARE TURNED ON EU LAWMAKER INVESTIGATING SPYWARE

IMAGE SOURCE: CITIZEN LAB

A new investigation by Citizen Lab has revealed that Stelios Kouloglou, a former Member of the European Parliament and investigative journalist, was repeatedly infected with NSO Group's Pegasus spyware while serving on the European Parliament's PEGA Committee, which was established to investigate the abuse of commercial spyware across Europe. Forensic analysis found that Kouloglou's iPhone was compromised during critical phases of the committee's work in 2022 and 2023, potentially giving attackers access to confidential parliamentary discussions, investigative findings and sensitive communications. Although researchers could not definitively identify the government responsible for the attacks, the timing suggests the surveillance was closely linked to the committee's investigations into spyware misuse. The case marks the first publicly confirmed instance of a PEGA committee member being targeted while actively investigating Pegasus, highlighting the growing threat posed by mercenary spyware to democratic institutions and legislative oversight. The findings have renewed calls for stronger regulation of the commercial spyware industry and enhanced protections for public officials, journalists and human rights defenders against unlawful digital surveillance (3 July 2026). Citizen Lab

DIGITAL SURVEILLANCE IS QUIETLY SILENCING COLLECTIVE ACTION

IMAGE SOURCE: LAWFARE

As governments and private companies expand their use of digital surveillance technologies, experts warn that the greatest threat may not be the collection of personal data itself, but the gradual erosion of citizens' willingness to organise, protest and participate in democratic life. Writing for Tech Policy Press, UN Special Rapporteur Gina Romero argues that pervasive surveillance—including facial recognition, biometric monitoring, AI-powered analytics and social media tracking—creates a "chilling effect" that discourages people from exercising their rights to freedom of peaceful assembly and association. Even when surveillance is not actively used to prosecute individuals, the perception of being watched can foster fear, self-censorship and distrust, making it harder for civil society organisations to recruit members, mobilise supporters and advocate for social change. Romero warns that these long-term psychological and societal impacts threaten the foundations of democratic participation, urging governments to embed human rights safeguards, transparency and accountability into digital governance before surveillance technologies permanently undermine collective civic action (23 June 2026). Tech Policy

EVERYDAY TECHNOLOGY BECOMES A TOOL FOR DOMESTIC SURVEILLANCE

IMAGE SOURCE: THE NEW ZEALAND HERALD

Affordable consumer technologies are increasingly being weaponised by domestic abusers to stalk, monitor and control victims, prompting renewed calls for stronger safeguards against technology-facilitated abuse. The New Zealand Herald reports that devices such as Apple AirTags, Bluetooth trackers, hidden cameras, spyware applications, smart home systems and GPS-enabled wearables are being misused to secretly track victims' movements, monitor communications and maintain coercive control long after relationships have ended. Specialists warn that these tools have lowered the cost and complexity of digital surveillance, allowing perpetrators to exploit everyday technologies that are often difficult to detect. Victims frequently remain unaware they are being monitored until unusual patterns emerge, while experts stress that technology companies and policymakers have been slow to implement safeguards against misuse. Digital safety organisations are urging individuals experiencing abuse to seek specialist support before removing suspected tracking devices, as doing so can sometimes escalate the risk of harm. The growing misuse of consumer technology highlights how cybersecurity is no longer limited to protecting systems and data but has become a critical issue for personal safety, privacy and the prevention of technology-enabled coercive control (6 July 2026). The New Zealand Herald

ACTIVISTS FIGHT BACK AGAINST ICE'S EXPANDING SURVEILLANCE NETWORK

IMAGE SOURCE: THE CONVERSATION

As US immigration authorities expand their use of artificial intelligence, data analytics and digital tracking tools, activists and civil rights groups are developing their own technology-driven strategies to monitor and challenge government surveillance practices. The article examines how Immigration and Customs Enforcement (ICE) has built a vast technology-enabled enforcement system by combining government databases, private-sector data brokers, facial recognition tools, location data and automated analytics to identify, track and investigate migrants and communities. Critics argue that this surveillance infrastructure operates with limited transparency and oversight, allowing authorities to access extensive personal information that can affect individuals who have not committed crimes. In response, privacy advocates and activist networks are using publicly available data, digital research tools and community-based monitoring initiatives to document government surveillance activities, expose potential abuses and demand greater accountability. The growing confrontation reflects a broader struggle over who controls data in modern society: governments and corporations that increasingly rely on predictive technologies for enforcement, or communities seeking to protect privacy, civil rights and democratic participation. The debate surrounding ICE's surveillance expansion highlights wider global concerns about the normalisation of algorithmic policing and the risks posed when powerful data systems operate without sufficient legal safeguards or public oversight (23 July 2026). The Conversation

ITALY'S MEDIA FREEDOM CONTINUES TO SLIDE

IMAGE SOURCE: EUROPEAN FEDERATION OF JOURNALISTS

Italy's media freedom environment continues to deteriorate, according to a new Media Freedom Rapid Response (MFRR) report, which warns that political pressure, spyware targeting journalists and weakening institutional safeguards are placing independent journalism under increasing strain. Following a fact-finding mission to Rome, the MFRR found that the country has experienced further backsliding since 2024, citing concerns over political interference in the public broadcaster RAI, insufficient implementation of EU anti-SLAPP protections, legal harassment of journalists and continued threats to media pluralism. The report also highlights serious safety concerns, including spyware attacks against journalists and the attempted car bomb assassination of prominent investigative journalist Sigfrido Ranucci, arguing that these incidents reflect a hostile environment for independent reporting. While the European Union has raised concerns through its Rule of Law monitoring, the MFRR contends that stronger enforcement is needed to ensure compliance with the European Media Freedom Act (EMFA) and other press freedom standards. The findings underscore a broader trend across Europe in which surveillance technologies, political influence and legal pressure are increasingly converging to undermine journalistic independence and the public's right to access independent information (13 July 2026). European Federation of Journalists

ACTIVISTS FIGHT BACK AGAINST ICE'S EXPANDING SURVEILLANCE NETWORK

IMAGE SOURCE: EUOBSERVER

Although Budapest Pride has been officially reinstated under Hungary's new government, digital rights advocates warn that the surveillance framework created under former Prime Minister Viktor Orbán remains firmly intact. Legislation introduced in 2025 expanded police powers to use facial recognition technology to identify participants at public gatherings by classifying Pride attendance as a minor offence, creating what experts describe as a chilling effect on freedom of assembly. While authorities ultimately refrained from prosecuting participants after massive public turnout, biometric surveillance vehicles were still deployed around the event, demonstrating that the technology was intended as a deterrent rather than solely an enforcement tool. Civil society organisations argue that Hungary's continued use of remote biometric identification may violate the EU Artificial Intelligence Act, which largely prohibits real-time biometric surveillance in public spaces for law enforcement purposes. Despite calls for legal reform and European Commission intervention, the surveillance legislation remains in force, raising broader concerns that governments can retain intrusive digital monitoring capabilities even after political leadership changes, leaving fundamental rights vulnerable to future abuse (25 June 2026). Euobserver

RIGHTS GROUPS CHALLENGE PARAGUAY'S SECRET FACIAL RECOGNITION PROGRAMME

IMAGE SOURCE: EUROPEAN FEDERATION OF JOURNALISTS

Digital rights organisations Electronic Frontier Foundation (EFF), TEDIC and the Center for Justice and International Law (CEJIL) have filed a petition before the Inter-American Commission on Human Rights, accusing Paraguay of unlawfully concealing information about its use of facial recognition technology in public surveillance. The case stems from a six-year legal battle after Paraguayan authorities repeatedly refused to disclose key details about the procurement, operation and oversight of facial recognition systems installed by the Ministry of the Interior and National Police, citing national security concerns. The petition argues that this secrecy violates the public's right to access information and prevents meaningful scrutiny of technologies capable of enabling mass biometric surveillance. The organisations are urging the Commission to establish regional standards requiring governments to disclose how facial recognition systems operate, conduct human rights impact assessments before deployment and ensure transparency around data collection, storage and oversight. If successful, the case could set a landmark legal precedent for Latin America by reinforcing that governments cannot deploy powerful AI-driven surveillance technologies behind a veil of secrecy and without adequate public accountability (25 June 2026). EFF

RUSSIAN-MADE FACIAL RECOGNITION FUELS CRACKDOWN IN GEORGIA

IMAGE SOURCE: ALGORITHM WATCH

A new investigation by AlgorithmWatch alleges that Georgia has rapidly expanded an AI-powered facial recognition network using Polyface, surveillance software supplied by Moscow-based company Papillon AO, which has reported ties to Russia's Federal Security Service (FSB). According to the investigation, the system has been used extensively to identify participants in pro-European demonstrations, allowing authorities to issue fines and pursue protesters weeks or even months after rallies have ended. The report details how an extensive network of CCTV cameras integrated with facial recognition software has transformed public surveillance, enabling authorities to remotely identify demonstrators without direct police interaction. Civil society groups argue that the technology has become a powerful instrument for suppressing dissent, with many targeted individuals facing financial hardship after receiving substantial penalties or having bank accounts frozen for unpaid fines. The findings have intensified concerns over the growing export of Russian surveillance technologies beyond its borders and the use of AI-driven biometric monitoring to erode privacy, intimidate political opposition and restrict the right to peaceful assembly in countries experiencing democratic backsliding (27 June 2026). Algorithm Watch

HACK EXPOSES SURVEILLANCE OF FACIAL RECOGNITION CRITICS

IMAGE SOURCE:SOFX

A sophisticated phone-based social engineering attack against Madison Square Garden (MSG) reportedly led to a major cyber breach that exposed internal documents revealing how the company monitored and profiled critics of its facial recognition programme. Among the leaked files was a document titled "Facial Recognition Activists.docx", which compiled the names, public statements, social media activity and online profiles of prominent privacy advocates and civil society figures who had publicly criticised MSG's use of biometric surveillance. The breach also exposed broader security records, highlighting concerns that facial recognition systems were being used not only for venue security but also to monitor and potentially retaliate against lawful criticism. Privacy advocates argue that the revelations reinforce longstanding fears that organisations deploying biometric surveillance may use the technology to suppress dissent, while the incident also underscores the cybersecurity risks of storing sensitive surveillance data without adequate safeguards. The case has reignited debate over corporate accountability, transparency and the ethical limits of facial recognition technologies, particularly when surveillance extends beyond security objectives to include the monitoring of activists and critics (26 June 2026). Sofx

HACKERS EXPLOIT REAL BOOKING DATA IN SOPHISTICATED TRAVEL SCAM

IMAGE SOURCE: TOURISM UPDATE

Cybercriminals are increasingly exploiting genuine travel reservation data to launch highly convincing phishing campaigns against tour operators, travel agencies and accommodation providers, marking a dangerous evolution in social engineering attacks. According to Tourism Update, attackers are sending fraudulent emails that impersonate hotels and lodges with which operators have legitimate bookings, using authentic reservation details to make the messages appear credible. Recipients are urged to click links to "confirm" bookings or resolve reservation issues, but the links instead harvest login credentials or install malware, potentially giving attackers access to booking systems, customer information and financial accounts. Security experts warn that the use of real booking data makes these attacks significantly harder to detect than traditional phishing emails, as victims are far more likely to trust messages containing accurate reservation information. The campaign follows a broader wave of cyberattacks targeting the global travel industry, where compromised booking data has become a valuable tool for spear-phishing, fraud and credential theft. Experts urge travel businesses to verify booking requests through trusted channels, strengthen multi-factor authentication and train staff to recognise increasingly sophisticated phishing attempts that exploit trusted customer and reservation data (16 July 2026). Tourism Update

CRASHSTEALER MALWARE DISGUISES ITSELF AS APPLE'S CRASH REPORTER

IMAGE SOURCE: THE TECH BUZZ

Cybersecurity researchers have uncovered a sophisticated new macOS infostealer, CrashStealer, that masquerades as Apple's legitimate crash-reporting utility to trick users into surrendering sensitive credentials and financial data. First observed in development in May before becoming active in July, the malware is distributed through a signed and Apple-notarised installer, allowing it to bypass Gatekeeper, Apple's built-in security feature, and appear trustworthy to unsuspecting users. Once installed, CrashStealer displays a convincing fake macOS password prompt that captures the victim's login credentials, granting attackers access to Apple Keychain passwords, browser credentials, cookies, cryptocurrency wallets, password managers and locally stored files. Researchers found the malware also establishes persistence on infected devices and encrypts stolen information before transmitting it to attacker-controlled servers, making detection more difficult. The campaign demonstrates the growing sophistication of macOS-targeted malware, with threat actors increasingly abusing legitimate code-signing processes and trusted system interfaces to evade security protections. Experts urge users to install software only from trusted sources such as the Mac App Store, remain cautious of unexpected password prompts and use reputable endpoint security tools to detect threats that can slip past native operating system defences (15 July 2026). The Tech buzz

UK RETAIL FACIAL RECOGNITION LINKED TO CONTROVERSIAL CLOUD INFRASTRUCTURE

IMAGE SOURCE: THE NEWRAB

The rapid expansion of facial recognition technology across UK supermarkets is raising fresh concerns over privacy, corporate accountability and the wider human rights implications of biometric surveillance. Retailer Sainsbury's is expanding its use of Facewatch facial recognition systems to as many as 200 stores by the end of 2026 to combat shoplifting, with the technology processing data through Amazon Web Services (AWS). Critics have drawn attention to AWS's separate involvement in Project Nimbus, a US$1.2 billion cloud and AI contract with the Israeli government that supports multiple state agencies, including the military and security services. Campaigners argue that the connection raises ethical concerns about how commercial facial recognition infrastructure may intersect with broader systems of state surveillance, although Facewatch maintains that it has no involvement in or visibility of Amazon's other commercial relationships and says its technology is deployed under UK legal and governance requirements. Supporters of the rollout point to Sainsbury's reported 46% reduction in recorded theft, aggression and anti-social behaviour during trials, while privacy advocates continue to warn about biometric data security, potential demographic bias and the normalisation of facial recognition in everyday public spaces (10 July 2026). The Newarab

FAKE VPN APPS SPREAD IRANIAN STATE SPYWARE

IMAGE SOURCE: TECH TIMES

Cybersecurity researchers have uncovered a sophisticated Iranian state-linked cyber espionage campaign that disguises spyware as fake VPN applications to target Persian-speaking users inside Iran and abroad. The operation, attributed to the threat group TAG-182, distributes malicious Android applications—including fraudulent VPN and media player apps promoted through Instagram and other online channels—to exploit users seeking to bypass internet censorship. Once installed, the malware, known as MarkiRAT, grants attackers extensive access to infected devices, enabling them to steal messages, contacts, files, location data and other sensitive information while maintaining persistent remote control. Researchers believe the campaign primarily targets journalists, activists, dissidents and members of the Iranian diaspora, weaponising the very tools people rely on to protect their privacy from state surveillance. The operation forms part of a broader ecosystem of Iranian state-aligned spyware campaigns that use social engineering, fake applications and malware to monitor perceived opponents both domestically and internationally. The findings highlight the growing trend of governments exploiting trusted privacy tools as delivery mechanisms for surveillance software, underscoring the importance of downloading VPN applications only from verified sources and remaining cautious of software promoted through social media or unofficial websites (23 July 2026). Tech times

INTELLIGENCE AGENCIES

INVESTIGATION ALLEGES DSS SPYWARE ENABLED ILLEGAL WIRETAPS

IMAGE SOURCE: ICIR

An investigation by the International Centre for Investigative Reporting (ICIR) alleges that Nigeria's Department of State Services (DSS) has acquired sophisticated surveillance technologies that have been used to conduct warrantless wiretaps, track mobile devices and facilitate the arrest and prolonged detention of activists, government critics and suspected security threats. Drawing on court records, victim testimonies and public procurement documents, the investigation claims the agency has deployed tools including Pegasus, FinSpy and Athena Forensic Solutions, alongside IMEI tracking, cell tower triangulation and telecommunications interception technologies, to monitor targets and extract data from seized devices. Legal experts argue that while Nigerian law permits surveillance under certain national security circumstances, interception of private communications generally requires judicial authorisation and independent oversight—safeguards they say are frequently bypassed in practice. The report also highlights Nigeria's substantial investment in surveillance technologies over the past decade, warning that weak accountability mechanisms have enabled intrusive digital monitoring with limited transparency or legal recourse for those affected. The DSS rejects allegations of unlawful surveillance, maintaining that its operations comply with standard operating procedures and applicable legal authorities, while insisting that its primary mandate remains the protection of national security (6 July 2026). ICIR

FOREIGN INFLUENCE THREATENS AFRICA'S DIGITAL RIGHTS LANDSCAPE

IMAGE SOURCE: CIPESA

A new report by CIPESA warns that Africa's digital rights are increasingly being shaped by foreign geopolitical influence, as global powers leverage economic partnerships, digital infrastructure investments and information operations to expand their strategic interests across the continent. The report points to the abrupt cancellation of RightsCon 2026 in Zambia—following reported diplomatic pressure linked to Taiwan's participation—as a stark example of how external actors can influence major digital rights events and policymaking. Beyond diplomacy, the report argues that many African governments have become increasingly dependent on foreign-funded digital infrastructure, particularly surveillance technologies, cloud services and AI systems, often supplied by China and Russia with limited transparency or independent oversight. It also highlights the growing use of foreign-backed disinformation campaigns to influence elections, public opinion and political stability, citing documented Russian information operations across more than 20 African countries. CIPESA cautions that these developments are accelerating digital authoritarianism by enabling mass surveillance, restricting civic space and weakening internet freedoms. The organisation calls for stronger digital sovereignty, greater transparency in technology procurement, robust human rights safeguards and regional cooperation to ensure Africa's digital transformation is guided by democratic values rather than external geopolitical interests (1 July 2026). CIPESA

ZAMBIA AND SOUTH SUDAN EXPAND CYBERCRIME POWERS AMID FREE EXPRESSION CONCERNS

IMAGE SOURCE: DEVELOPING TELECOMS

Zambia and South Sudan have begun enforcing new cybercrime laws that human rights organisations and digital rights advocates warn could expand government powers to monitor online activity and restrict freedom of expression. The legislation, introduced as part of broader efforts to combat online fraud, cyberattacks, misinformation and digital abuse, gives authorities greater authority to investigate online offences and prosecute individuals accused of misusing digital platforms. However, critics argue that several provisions are overly broad and could be used to criminalise legitimate online speech, silence government critics and increase surveillance of journalists, activists and ordinary internet users. Digital rights groups have raised concerns that vague definitions of cyber offences, insufficient judicial oversight and limited transparency around enforcement could enable authorities to misuse cybersecurity frameworks for political purposes rather than focusing solely on genuine cyber threats. The developments reflect a wider trend across Africa, where governments are increasingly introducing cybercrime legislation while facing pressure to balance cybersecurity needs with constitutional protections for privacy, access to information and freedom of expression. As digital adoption accelerates across the continent, experts stress that effective cyber governance requires laws that protect citizens from cyber threats without creating tools for censorship, surveillance or repression (22 July 2026). Developing telecoms

CHINA'S AI SURVEILLANCE IS SHIFTING FROM MONITORING TO PREDICTION

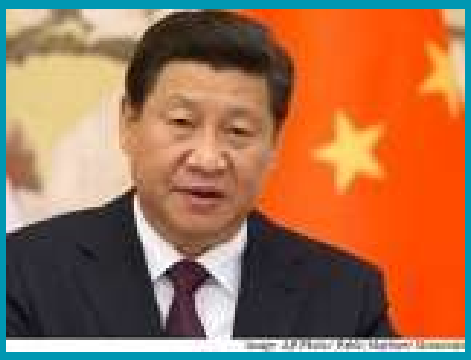

IMAGE SOURCE: NDTV

China is entering a new phase of AI-driven surveillance in which authorities are seeking not only to monitor citizens' behaviour but also to predict potential dissent before it occurs, raising fresh concerns over digital authoritarianism and pre-emptive policing. According to the analysis, Chinese technology firms are developing artificial intelligence systems capable of analysing vast amounts of personal data—including travel patterns, online activity, social networks, financial records and behavioural histories—to generate risk profiles that identify individuals deemed likely to participate in protests or challenge state authority. These predictive tools build on China's already extensive surveillance ecosystem of facial recognition cameras, biometric databases and online censorship, transforming AI from a reactive monitoring tool into one designed to anticipate and prevent perceived threats before any crime has been committed. Critics warn that such systems risk criminalising intent rather than actions, reinforcing political repression through opaque algorithms that lack transparency, accountability and legal oversight. The development highlights the growing convergence of artificial intelligence, predictive analytics and state surveillance, illustrating how emerging technologies are reshaping authoritarian governance and intensifying global concerns over the future of privacy, civil liberties and digital human rights (30 June 2026). NDTV

TECH GIANTS ACCUSED OF POWERING AMERICA'S EXPANDING SURVEILLANCE STATE

IMAGE SOURCE: PRISM

A new investigation by Prism Reports argues that leading technology companies are playing an increasingly influential role in expanding the United States' surveillance infrastructure through close partnerships with the Department of Homeland Security (DHS) and immigration enforcement agencies. The report alleges that firms specialising in artificial intelligence, data analytics, cloud computing, facial recognition and digital identity verification have secured lucrative government contracts to develop technologies that enhance migrant tracking, biometric identification, predictive analytics and large-scale data integration. Civil liberties advocates warn that surveillance capabilities initially justified for immigration enforcement are increasingly spilling over into broader domestic policing and public monitoring, raising concerns that technologies developed to monitor border populations could become normalised across wider society. The investigation also highlights the growing political and commercial influence of major technology executives, arguing that private sector interests are increasingly shaping public security policy while outpacing democratic oversight and accountability. The report adds to mounting concerns that the convergence of AI, big data and government surveillance is creating an increasingly powerful digital monitoring ecosystem, underscoring calls for stronger transparency, procurement oversight and legal safeguards to prevent the erosion of privacy and civil liberties (7 July 2026). Prism

NATIONAL SECURITY INCREASINGLY USED TO SILENCE JOURNALISTS

IMAGE SOURCE: RSF

A new report by Reporters Without Borders (RSF) warns that governments around the world are increasingly exploiting national security as a pretext to suppress independent journalism, transforming laws intended to protect citizens into powerful tools for censorship, surveillance and repression. According to the report, journalists are being prosecuted under counterterrorism, espionage and national security legislation, while others face digital surveillance, arbitrary detention, forced exile and even assassination for reporting on issues deemed politically sensitive. RSF argues that vague and overly broad national security laws have enabled authorities to criminalise investigative reporting, restrict access to information and intimidate media organisations under the guise of protecting state interests. The report highlights a growing reliance on spyware, communications interception and online surveillance to identify journalistic sources and monitor reporters, warning that these practices undermine press freedom and democratic accountability. Calling for stronger legal safeguards and greater international oversight, RSF cautions that the expanding use of national security as a justification for restricting journalism poses one of the most significant threats to media freedom in the digital age, with profound implications for privacy, transparency and the public's right to information (July 2026). RSF

CHINESE AI SURVEILLANCE EXPANDS ACROSS AFRICAN CITIES

IMAGE SOURCE: INSTITUTE OF DEVELOPMENT STUDIES

A landmark report by the Institute of Development Studies (IDS) reveals the rapid expansion of Chinese-backed AI surveillance infrastructure across 11 African countries, documenting more than US$2 billion in investments in "smart city" technologies that include facial recognition, AI-enabled CCTV cameras, automated number plate recognition and centralised command centres. Chinese companies—including Huawei, Hikvision and ZTE—have emerged as the dominant suppliers, often supported by Chinese state financing under the Digital Silk Road initiative. While governments argue these systems improve public safety, combat crime and modernise urban management, the report finds little evidence that large-scale surveillance has significantly reduced crime. Instead, researchers warn that the technologies are increasingly being used to monitor political opposition, journalists, activists and peaceful protesters in countries such as Kenya, Uganda, Zimbabwe and Nigeria. The report concludes that weak legal safeguards, limited transparency and inadequate independent oversight have created conditions for widespread violations of privacy, freedom of expression and the right to peaceful assembly, raising urgent questions about the long-term human rights implications of AI-powered surveillance across the continent (11 March 2026). Institute of development studies

EGYPT STRUGGLES TO BALANCE PRIVACY AND STATE SURVEILLANCE

IMAGE SOURCE: RECORD OF LAW

As Egypt continues to modernise its digital governance framework, tensions persist between strengthening data protection and preserving expansive national security powers. The country's Personal Data Protection Law (PDPL) represents Egypt's first comprehensive privacy legislation, introducing safeguards for the collection and processing of personal data. However, critics argue that broad exemptions granted to national security agencies, combined with cybercrime and counterterrorism laws that permit extensive access to user data, significantly weaken these protections. Security authorities retain wide-ranging surveillance powers, including the ability to monitor digital communications and require service providers to retain user data, often with limited independent oversight. Human rights advocates contend that these legal loopholes risk enabling mass surveillance and undermine citizens' rights to privacy, freedom of expression and due process, while the government maintains that such measures are essential to combat terrorism, cybercrime and other national security threats. Egypt's evolving legal landscape therefore reflects a broader global challenge: finding an effective balance between protecting digital privacy and equipping governments with the tools they argue are necessary to safeguard national security in an increasingly connected world (30 June 2026). Record of Law

EUROPE'S BANNED FACIAL RECOGNITION FINDS A MARKET IN INDIA

IMAGE SOURCE: THE REPORTERS COLLECTIVE

A cross-border investigation has revealed that Herta Security, a Spanish company whose facial recognition technology would be largely prohibited for law enforcement use under the EU AI Act, has deployed its software across thousands of surveillance cameras in India, exposing what critics describe as a troubling double standard in global surveillance exports. The investigation estimates that more than 4,000 cameras across railway stations, prisons, temples and "safe city" projects are powered by Herta's technology, with some systems capable of scanning crowds in real time against watchlists containing up to 100 million individuals. While the EU's AI Act largely bans real-time biometric identification in public spaces except under narrowly defined circumstances with judicial authorisation, India lacks equivalent legal safeguards or oversight governing the widespread deployment of facial recognition technologies. Digital rights advocates warn that the systems are being integrated with vast government-held databases while operating with minimal transparency regarding who is being monitored, how data is stored or how long biometric information is retained. The investigation also raises ethical concerns over the export of surveillance technologies that are increasingly restricted within Europe but continue to be marketed abroad, fuelling calls for stronger international controls on the sale of high-risk AI surveillance systems and greater accountability for companies supplying biometric technologies to countries with weaker privacy protections (15 July 2026). The reporters collective

BRAZIL'S SMART CITIES RAISE SURVEILLANCE CONCERNS

IMAGE SOURCE: THE ECONOMIST

Brazilian cities are rapidly expanding large-scale surveillance networks that combine artificial intelligence, facial recognition and data-sharing systems in an effort to combat crime and improve public safety. The most prominent example is São Paulo's Smart Sampa programme, which uses tens of thousands of cameras equipped with facial recognition technology to identify wanted suspects, locate missing persons, detect stolen vehicles and support police investigations. The system is part of a wider national trend, with hundreds of facial recognition projects reportedly operating across Brazilian states and increasingly integrating cameras from public spaces, transport systems and private networks. While authorities argue that these technologies provide valuable tools for reducing crime and improving emergency responses, privacy advocates and digital rights groups warn that the rapid expansion of biometric surveillance risks creating systems of mass monitoring without sufficient transparency, oversight or protections against misuse. Concerns include potential violations of privacy rights, algorithmic bias and the possibility that surveillance infrastructure built for security purposes could later be used for broader social control. Brazil's surveillance expansion reflects a growing global debate over whether AI-powered security systems can balance public safety objectives with the protection of civil liberties in increasingly digital societies (8 July 2026). The Economist

SÃO PAULO'S AI SURVEILLANCE FACES RACIAL BIAS ALLEGATIONS

IMAGE SOURCE: FRANCE24

São Paulo's Smart Sampa programme—the world's largest municipally operated facial recognition network—is facing mounting criticism over allegations that its AI-powered surveillance system disproportionately targets Black Brazilians and reinforces racial profiling in policing. The system, which integrates tens of thousands of CCTV cameras with facial recognition software to identify suspects, locate missing persons and support law enforcement, has been promoted by city authorities as a vital crime-fighting tool. However, human rights advocates, researchers and members of Brazil's newly established Parliamentary Front Against Racist Technologies argue that the technology lacks transparency and may replicate existing racial biases embedded in policing practices. Critics warn that inaccurate facial recognition matches and algorithmic bias could lead to wrongful police stops, arrests and increased surveillance of predominantly Black and low-income communities, while also raising concerns over the absence of robust oversight and independent auditing of the system. The controversy has intensified the broader debate over whether AI-driven surveillance can genuinely improve public safety without exacerbating discrimination, highlighting the urgent need for stronger governance, transparency and accountability in the deployment of biometric technologies (10 July 2026). France24

INDIA'S AI SURVEILLANCE BUILT ON FLAWED DATA, EXPERTS WARN

IMAGE SOURCE: TECH POLICY

India's rapid expansion of AI-powered policing and surveillance is raising concerns that advanced technologies are being layered onto unreliable data systems and long-standing deficiencies in law enforcement, potentially amplifying existing injustices rather than improving public safety. According to Tech Policy Press, police agencies are increasingly adopting facial recognition, predictive policing tools and interconnected surveillance databases despite persistent problems with inaccurate criminal records, outdated databases, inconsistent data collection and documented patterns of discriminatory policing. Experts warn that AI systems are only as reliable as the data on which they are trained, meaning flawed or biased records can lead to wrongful identification, disproportionate targeting of marginalised communities and the automation of policing errors at scale. The article argues that without comprehensive police reform, stronger data governance, independent oversight and clear legal safeguards, India's growing surveillance infrastructure risks embedding systemic bias into digital policing while creating an illusion of technological objectivity. The analysis serves as a broader warning that deploying artificial intelligence without first addressing institutional weaknesses may ultimately undermine both public trust and fundamental rights. (9 July 2026) Tech policy

FRANCE PUSHES DIGITAL SURVEILLANCE LAWS THREATENING ONLINE FREEDOM

IMAGE SOURCE: THE STAR

France is facing growing criticism from digital rights advocates over proposed surveillance measures that could expand state access to online communications and increase monitoring capabilities in the name of national security and public safety. The measures form part of a wider European debate over the balance between combating cybercrime, terrorism and online harms while protecting privacy, encryption and freedom of expression. Critics argue that expanded surveillance powers—including potential access to encrypted communications, increased digital monitoring and broader data collection—risk creating systems that could be misused beyond their original security objectives. Privacy advocates warn that weakening encryption or increasing state oversight of private communications could undermine the security of ordinary users, journalists, activists and businesses by creating new vulnerabilities in digital infrastructure. Supporters of stronger surveillance powers argue that law enforcement requires updated tools to investigate serious crimes in an increasingly digital environment. The controversy reflects a broader global tension between cybersecurity and civil liberties, as governments seek greater visibility into online activity while citizens and rights groups demand stronger safeguards, transparency and judicial oversight to prevent excessive monitoring and protect fundamental digital freedoms (27 July 2026). Newsfire

HAVE YOUR SAY!
LETTER TO THE EDITOR

Dear Readers:

Welcome to the "Letter to the Editor" section of our newsletter - a safe space dedicated to your voice and your views. As an organisation rooted in the Global South but whose work extends across borders, our mission is to promote democratic oversight of intelligence and surveillance activities worldwide. We monitor, report, educate, and advocate to ensure that surveillance laws and practices respect human rights and democratic principles.

We strongly believe that meaningful change begins with dialogue, and that's where you come in. We invite you to share your thoughts about the issues we cover, your concerns, and experiences related to surveillance in your community or country and suggest topics or questions you want us to explore. Your insights help shape the conversation and strengthen our shared commitment to Defending Human Rights, Protecting Civic Space in the digital age, amplifying the need for transparency and accountability and holding power accountable.

Send your letters, stories, or feedback to us at advocacy@intelwatch.org.za, and together, let's strengthen the global movement for democratic oversight.

We look forward to hearing from you and building a Intelwatch-out community where everyone's voice matters.

Warm regards
The Intelwatch Team

INTEL WATCH

Watching the watchers. Guarding the guardians.

GET INVOLED!

Sign up to get occasional news and briefings on intelligence oversight and surveillance reform in Southern Africa and beyond

FIND US ON SOCIAL MEDIA

@IntewatchNews

@IntewatchNpc

Intewatch website

@IntewatchNpc

@IntewatchNpc

HAVE ANY QUESTIONS?

Email: info@intelwatch.org.za

The Reynolds Foundation Now for tomorrow

Global Dialogue

Luminate

Funded by the European Union

We are grateful for the support of our donors!