SOUTH AFRICAN
Intellectual Property
Law Journal

Articles

The inadequacy of copyright-related provisions in economic partnership agreements between the European Union and the African, Caribbean and Pacific regional groups from an educational perspective
James David

Shifting digital media ecologies and how copyright law should adjust and adapt to journalism
Brian Hungwe

Navigating the complexities of the adaptation right in copyright law: Addressing ambiguities, gaps and the need for reforms in South Africa
Lucinda Kok

One (innovation) flew over the law's head: The intersection of artificial intelligence and copyright
Razeen Khan and Ngonidzaishe Gotora

Opinion

Artificial intelligence facial recognition surveillance and the breach of privacy rights: The 'Clearview AI' and 'Rite Aid' case studies
Ifeoma E. Nwafor

VOLUME ELEVEN 2023

SOUTH AFRICAN INTELLECTUAL PROPERTY LAW JOURNAL

Volume 11 2023

juta

Published in association with the Faculty of Law, University of Cape Town.

ISSN: 2309-4532

Cover design: Drag and Drop
Typesetting: Peter Howe
Printed by:

Publishers:
Juta and Company (Pty) Ltd
1st Floor Sunclare Building
21 Dreyer Street
Claremont
www.juta.co.za

EDITORIAL POLICY

The *IPLJ* is a peer-reviewed journal that publishes contributions in the area of intellectual property law. The *IPLJ* aims to be essential reading for intellectual property academics and for those seeking perspectives from Africa generally and South Africa specifically. The *IPLJ* is published once a year.

CITATION

This journal should be cited as (2023) 11 *IPLJ*.

INFORMATION FOR CONTRIBUTORS AND REFEREES

For information about publishing in *IPLJ* contact the Editor at:
Email: Editoriplj@uct.ac.za

CONTENTS

Articles

The inadequacy of copyright-related provisions in economic partnership agreements between the European Union and the African, Caribbean and Pacific regional groups from an educational perspective
James David 1

Shifting digital media ecologies and how copyright law should adjust and adapt to journalism
Brian Hungwe 16

Navigating the complexities of the adaptation right in copyright law: Addressing ambiguities, gaps and the need for reforms in South Africa
Lucinda Kok 42

One (innovation) flew over the law's head: The intersection of artificial intelligence and copyright
Razeen Khan and Ngonidzaishe Gotora 72

Opinion

Artificial intelligence facial recognition surveillance and the breach of privacy rights: The 'Clearview AI' and 'Rite Aid' case studies
Ifeoma E. Nwafor 88

ARTIFICIAL INTELLIGENCE FACIAL RECOGNITION SURVEILLANCE AND THE BREACH OF PRIVACY RIGHTS: THE 'CLEARVIEW AI' AND 'RITE AID' CASE STUDIES

Ifeoma E. Nwafor*
Senior Lecturer, Godfrey Okoye University (Nigeria); Visiting Scholar, Faculty of Law and Criminology, KU Leuven, Belgium; Member, United Nations Development Programme AI4Dev Reference Group; Research Member, Centre for Artificial Intelligence Digital Policy

1. Introduction

The increasing sophistication of artificial intelligence (AI) facial recognition models and the accessibility of photos online by companies and governments have amounted to the excessive misuse of facial surveillance systems. The government, the police and organisations have a long history of using AI facial recognition technologies to gather data on citizens without respecting their data and privacy rights. The government relies on national security and public safety to justify such gathering of data. Marginalised groups and people of colour are disproportionately affected by such surveillance. Data protection and privacy rights activists have called on governments to regulate facial recognition systems. It is also essential to establish AI oversight agencies with the responsibility to monitor the use of AI models and to ban such use when it breaches citizens' data and privacy rights, and any other human rights.

The European Union's AI Act is the first comprehensive regulation on AI. It provides a risk management framework with different rules for different risk levels: unacceptable risks, high risks, and limited or low-risk applications. In June 2023, the European Parliament voted in favour of a total ban on live facial recognition in public spaces. Although the new Act did not stipulate a full ban on live facial recognition surveillance, it provides that all high-risk AI systems will be assessed before being put on the market and throughout their lifecycle.

African governments have caught the AI bug but only a few African countries have an existing AI strategy; these include Mauritius, Egypt and Rwanda. It has been argued that international AI technologies and ethical

* LLB (NAU) LLM PhD (UNN).

https://doi.org/10.47348/SAIPLJ/v11/a5

deliberations are modelled without Africa in mind.[1] Against this backdrop, it is more likely that Africans as people of colour will be subjected to AI ethical bias, privacy and data protection concerns, risks and harms. It is essential that African countries develop AI policies. Additionally, Africa should also take a strategic place in the ongoing debate on global AI regulation.

2. Facial Recognition Surveillance and Data and Privacy Rights Issues

Facial recognition involves the use of technology to collect and process an individual's face from a digital image or video frame against a massive database or watchlist to confirm their identity. These digital images and videos may have been collected without the individual's explicit permission. The digital representation of physical features that identify humans in the Internet of Everything environment is known as personal physiological data. Such data includes identification, characteristics of uniqueness, relevance of information, irreversibility of damage and replicability; this data is easily collected, shared and deployed in multiple applications.[2] Significant data and privacy breach concerns exist regarding the use of AI recognition surveillance. Such surveillance tools have been criticised for raising ethical, technical and legal concerns and for unfairly or inaccurately profiling people of colour and marginalised groups.[3]

Tech companies such as Facebook, Google, Microsoft, IBM, Apple and Amazon had projects that either internally developed or purchased facial recognition systems. Some of these companies have shut down their facial recognition projects because of the backlash against such projects and the clamour for their restriction. Clearview AI, a tech start-up, developed a facial recognition app that was widely adopted by police departments across the United States. However, Clearview AI's facial recognition system was on the news for years for data breaches, such as stealing customers' data and infringing on consumers' privacy rights. The Clearview app and its data scraping practice go far beyond traditional facial recognition tools by combining its technology with a database of over three billion images circulated online.[4] It has been argued that Clearview, now a market leader, has amassed over 30 billion images.

1 DO Eke, K Wakunuma & S Akintoye 'Introducing responsible AI in Africa' in DO Eke, K Wakunuma & S Akintoye (eds) *Responsible AI in Africa: Challenges and Opportunities* (2023) 6.

2 M Wang, Y Qin & W Li 'Identifying personal physiological data risks to the Internet of Everything: The case of facial data breach risks' (2023) 10(1) *Humanities and Social Sciences Communications*.

3 IE Nwafor 'AI ethical bias: A case for AI vigilantism (AIlantism) in shaping the regulation of AI' (2021) *International Journal of Law and Information Technology*, available at https://doi.org/10.1093/ijlit/eaab008.

4 IN Rezende 'Facial recognition in police hands: Assessing the "Clearview case" from a European perspective' (2020) 11(3) *New Journal of European Criminal Law* 375–389.

https://doi.org/10.47348/SAIPLJ/v11/a5

In May 2022, Clearview AI was fined £7.5 million by the United Kingdom (UK) privacy watchdog, the Information Commissioner's Office (ICO), for breaching several provisions of the UK's General Data Protection Regulation; one such breach was collecting and processing images without individuals' consent. The ICO also ordered the company to delete the data of UK residents in its database. However, in October 2023, Clearview AI won its appeal against the sanction. In its ruling, the Tribunal stated that 'although the processing undertaken by the ICO was related to the monitoring of data subjects' behaviour in the United Kingdom, the processing is beyond the material scope of the General Data Protection Regulation'.[5] The Tribunal ruled that the ICO did not have jurisdiction because foreign governments used the Clearview AI system, which is beyond the ICO's remit.

It is submitted that data and privacy rights should be equated with human rights without limitations. National or foreign government and law enforcement authorities should not be able to avoid sanctions for invading the sacred precincts of privacy.

On 22 November 2023, the United States (US) Federal Trade Commission (FTC) banned a US pharmacy chain, Rite Aid, from using facial recognition systems for surveillance purposes for five years. From 2012 to 2020, Rite Aid had recklessly employed facial recognition technologies to identify shoplifters and inaccurately flagged some customers, especially people of colour and women, as matching previous shoplifters. The pharmacy used the facial recognition software in neighbourhoods largely populated by Blacks, Latinos and Asians. These customers were subjected to unnecessary searches and humiliation and their sensitive information was placed at risk. The Director of the FTC stated that the ground-breaking order elucidated the FTC's vigilance in protecting citizens from unfair biometric surveillance and data breaches.

Two cases were described in the FTC's complaint against Rite Aid pharmacy. They were:

1. An employee searched for an 11-year-old girl after a false match. The girl's mother said that she missed work because her daughter was 'so distraught by the incident'.
2. Employees called the police on a black woman after a false alert. The person in the image that triggered the alert was described as 'a white lady with blonde hair'.[6]

The Rite Aid pharmacy violated some customers' sensitive data and subjected them to unwarranted searches due to inaccurate flagging provided by the facial recognition software. The database was developed from thousands of low-quality pictures from store cameras, etc, labelling specific individuals as criminals.

Marginalised or minority groups, especially people of colour, suffer extreme discrimination, risks and harms from AI facial or biometric surveillance technologies. It has been argued that 'the low testing or selection

5 *Clearview AI Inc v The Information Commissioner* [2023] UKFTT 819 (GRC).

6 B Schulz 'FTC bans Rite Aid from AI facial recognition use after unfair searches' (2023) available at https://www.usatoday.com (accessed 22 December 2023).

https://doi.org/10.47348/SAIPLJ/v11/a5

of marginalised groups in data that shapes AI has resulted in technological inventions based on a small-scale fragment of the world. These inventions do not represent a thorough analysis of different groups across the globe.'[7] In other words, bias, discrimination or the lack of representativity of people of colour, women and minority groups in the data sets used to train an AI model will exacerbate pre-existing prejudices. Until stakeholders, including people of colour, women, seniors, youths, people with disabilities and other minority groups, are involved in the designing, development, deployment and governance of AI, the issues surrounding AI technologies will continue.

From the preceding case studies, it is evident that people of colour and minority groups are more likely to be disproportionately criminalised by facial recognition systems that perpetuate racial discrimination. Africans as people of colour fall within the loop of AI ethical and racial bias.

The UK's ICO and the US' FTC have exhibited the independence expected of a data protection and privacy oversight agency by the quality and breadth of their oversight mechanisms. The relevance of an independent agency or mechanism for data protection and privacy oversight cannot be over-emphasised. Since AI technologies such as facial recognition software raise concerns of fairness, accountability, privacy and data protection, and equity, the key responsibility of such oversight agency would be to protect the fundamental rights of the public against AI risks and harms.

The African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) is the continent's legal framework for data protection, electronic commerce, cybercrime and cybersecurity. The Convention came into force on 8 June 2023, nine years after its adoption on 27 June 2023, after receiving the minimum required number of ratifications by AU Member States (as provided in Art 36 of the Convention). The Convention is overly broad in scope, combining data protection, cybersecurity, cybercrime and electronic commerce. It is the first of its kind globally.

Article 11 of the Malabo Convention requires each State Party to establish an independent data protection authority (DPA) to protect personal data. This authority is responsible for overseeing the implementation of the Convention and ensuring compliance with its provisions. Article 12 of the Convention lists the duties of DPAs. It empowers such authorities to mete out the temporary or permanent withdrawal of authorisation or monetary sanctions on data controllers who fail to comply with the Convention's provisions.

Several African countries have national data protection laws or regulations. Thirty-six out of 54 African countries have a data protection legal and regulatory framework. However, most of these countries do not have an independent agency or mechanism for data protection and privacy oversight, such as Egypt does. According to the country evaluation of the Centre for Artificial Intelligence Policy's 'Artificial Intelligence and Democratic Values of 2022', countries such as Malaysia, Mauritius, Rwanda and Uganda have

7 Nwafor (n3).

https://doi.org/10.47348/SAIPLJ/v11/a5

a partial data protection and privacy oversight agency.[8] The existence of an agency or mechanism for data protection and privacy oversight does not suffice. The effectiveness of the agency is measured by its independence and the quality and breadth of its oversight mechanisms.

3. Conclusion

The drawbacks of facial recognition technologies currently outweigh their positive aspects. Such technologies violate the data and privacy rights of the public. Facial recognition technologies, in most cases, misidentify people of colour, women, and other marginalised or minority groups.

This opinion makes a case for developing ethical and legal frameworks with prescriptive regulations to mitigate the drawbacks associated with such systems. Governments in all countries should abide by such regulations except in critical public safety situations. Particularly on the African continent, AI oversight agencies should be established and empowered to conduct holistic audits of AI facial recognition software to determine its fairness, accountability, transparency and compliance with fundamental rights and the rule of law. African states' DPAs should also exhibit the independence expected of a data protection and privacy oversight agency through the quality and breadth of their oversight mechanisms.

8 Centre for Artificial Intelligence Policy 'Artificial Intelligence and Democratic Values of 2022' (2023) available at https:/www.caidp.org.

https://doi.org/10.47348/SAIPLJ/v11/a5