REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

2ND NATIONAL DATA PROTECTION MOOT COURT HYPOTHETICAL

THE HIGH COURT OF LUMORA AT CAPITAL CITY

CONSTITUTIONAL AND HUMAN RIGHTS DIVISION

CONSTITUTIONAL PETITION NO. E072 OF 2027

BETWEEN

ZAWADI LEMBA & DIGITAL RIGHTS WATCH LUMORA (suing on their own behalf and on behalf of approximately 200,000 affected voters) ..... PETITIONERS

AND

THE INDEPENDENT ELECTORAL COMMISSION

OF LUMORA (IECL) ..... 1ST RESPONDENT

UMOJA MBELE PARTY (UMP) ..... 2ND RESPONDENT

KURASENSE ANALYTICS LIMITED ..... 3RD RESPONDENT

Background:

The Republic of Lumora is implementing its national digital transformation agenda under the Lumora Digital Master Plan 2022–2032. As part of this strategy, the Independent Electoral Commission of Lumora (IECL) digitised voter registration, voter identification, voter verification and management of the national register of voters for the 2028 General Election.

IECL operates the Integrated Voter Management System (IVMS) containing names, identity numbers, phone numbers, addresses, polling station information, fingerprints and facial images of registered voters.

Pursuant to the Elections Act of Lumora, the IECL may provide extracts of the register to political parties and candidates for election-related purposes. In 2026, IECL supplied UMP with register extracts containing voters' names, identity numbers, telephone numbers and polling station details. No data-sharing agreement was concluded, IECL imposed no restrictions on onward disclosure or secondary use of the extracts, and it

conducted no subsequent audit of how they were used.

In 2026, Umoja Mbele Party (UMP), a registered political party and one of the leading contenders in the forthcoming general election, engaged KuraSense Analytics Limited, a data analytics and artificial intelligence company, to provide voter engagement and campaign optimisation services.

KuraSense developed and deployed Mwanga Insight, an AI-driven platform designed to predict political preferences, turnout likelihood, behavioural tendencies and responsiveness to political messaging.

The agreement between UMP and KuraSense did not expressly specify whether UMP, KuraSense, or both would determine the purposes and means of processing personal data, nor did it allocate responsibility for compliance with applicable data protection laws.

To build predictive voter profiles, Mwanga Insight integrated information obtained from multiple sources, including: voter register extracts obtained from IECL; mobile phone and location data purchased from data brokers; publicly accessible social media activity; online advertising and browsing metadata; demographic information; educational and employment information obtained from commercial data aggregators; and neighbourhood voting histories and socio-economic indicators.

The platform generated behavioural and psychographic profiles and assigned categories such as Ethnically Inclined, Economically Dissatisfied, Religious Conservative, Change-Seeker, and Persuadable Swing Voter.

It also generated a Voter Influence Score estimating susceptibility to political persuasion. The algorithms and weighting criteria were not publicly disclosed.

Different voter groups received tailored messages based on religion, ethnicity, economic circumstances and behavioural profiles. Internal documents indicated the system predicted emotional triggers, deployed dark advertisements, delivered contradictory campaign promises to different groups and, in some cases, targeted likely opposition supporters with messages designed to discourage electoral participation.

Civil society organisations, including Digital Rights Watch Lumora (DRWL), argued that these practices transformed political campaigning from public persuasion into individualised influence lacking transparency and accountability. DRWL is a registered non-governmental organisation whose mandate includes the protection of privacy and digital rights in Lumora.

UMP maintained that the activities constituted legitimate political communication protected by the Constitution.

UMP deployed facial recognition-enabled cameras at campaign rallies and party events. The technology compared attendees' facial images against information contained within voter datasets processed by KuraSense. This information was subsequently used to update voter profiles and assess campaign effectiveness. No signage or other notice of the cameras was displayed at any of the events.

KuraSense stored and processed substantial portions of the voter analytics database on cloud servers situated outside Lumora in a jurisdiction that lacked comprehensive data protection legislation.

To improve the performance of its machine learning models, KuraSense engaged foreign subcontractors and data scientists who were granted access to sections of the voter database.

Facts of the Case

Between January 2026 and May 2027, KuraSense processed personal data relating to approximately 4.5 million registered voters obtained directly and indirectly from IECL voter register extracts and other data sources. Using the Mwanga Insight platform, KuraSense generated behavioural profiles, psychographic classifications, turnout predictions, and Voter Influence Scores for individual voters across Lumora.

On 14 May 2027, an unauthorised third party gained access to a voter analytics database maintained by KuraSense and extracted records relating to approximately 200,000 registered voters from all regions of Lumora. The extracted records were subsequently published on an online file-sharing platform and remained publicly accessible for approximately three weeks before being removed.

Zawadi Lemba, a 30-year-old trader and registered voter whose information was included in the disclosed dataset, had received numerous political messages through SMS, WhatsApp, and social media platforms during the election period. Many of the messages referenced her religion, ethnic community, neighbourhood, economic circumstances, and perceived political interests.

Following media investigations conducted after the disclosure, Zawadi became aware that Mwanga Insight

had classified her as a "Persuadable Swing Voter" and assigned her a high Voter Influence Score.

She further discovered that the system had generated predictions concerning her political preferences, religious orientation, economic concerns, voting behaviour, likelihood of electoral participation, and susceptibility to particular forms of political messaging.

Independent forensic experts retained by Digital Rights Watch Lumora (DRWL) subsequently examined the publicly disclosed dataset and confirmed that every affected record contained, at a minimum, the individual's name, national identity number, telephone number, psychographic classification, and Voter Influence Score generated by Mwanga Insight.

The forensic analysis further established that the disclosed records contained personal and derived data relating to approximately 200,000 voters and included geolocation histories, inferred political preferences, behavioural classifications, and other analytics generated through automated processing. Approximately 35,000 records also contained facial images and facial recognition data obtained from campaign events organised by UMP.

Through media investigations and publicly released internal documents, it emerged that neither Zawadi nor any other affected voter had been informed that such detailed profiles were being created, updated, and used for political targeting. No affected voter had been given an opportunity to access, review, correct, challenge, restrict, or object to the profiles generated about them.

In April 2027, Zawadi attended a UMP political rally. Unknown to her and other attendees, facial recognition-enabled cameras deployed at the venue analysed and matched attendees against voter analytics datasets maintained by KuraSense. Similar systems were deployed at not fewer than forty UMP political events held across Lumora between January and May 2027.

Information derived from attendance at those events was incorporated into voter profiles maintained within Mwanga Insight and used to assess political engagement, campaign effectiveness, and responsiveness to campaign messaging.

Following publication of the dataset, affected individuals lost exclusive control over their personal information and became publicly associated with inferred political characteristics, behavioural classifications, and voter influence assessments regardless of whether those inferences were accurate.

After publication of the dataset, Zawadi received threatening and intimidating messages referring to her political profile and attendance at political events. Within six weeks of the disclosure, DRWL received more than 3,000 complaints from other affected voters reporting harassment, intimidation, unwanted political communications, attempted identity fraud, reputational concerns, and fear of reprisals arising from the disclosure of their information.

Subsequent media investigations revealed that KuraSense had commissioned internal security assessments before the breach which identified vulnerabilities within its voter analytics infrastructure and recommended additional safeguards, including encryption of biometric data, stricter access controls, and segregation of voter analytics datasets. Those recommendations had not been fully implemented prior to the incident.

The investigations further suggested that both UMP and KuraSense became aware of the breach shortly after its discovery. Neither UMP nor KuraSense notified affected individuals nor reported the breach to the Office of the Data Protection Commissioner of Lumora within the period prescribed by law.

DRWL subsequently conducted a nationwide review of complaints arising from the incident and concluded that all affected individuals whose records appeared in the disclosed dataset had been subjected to the same profiling system, automated scoring mechanisms, and unlawful disclosure of their personal information.

Zawadi Lemba and DRWL thereafter filed a constitutional petition before the High Court under Articles 22 and 258 of the Constitution on their own behalf and on behalf of approximately 200,000 individuals whose personal data, psychographic profiles, Voter Influence Scores, facial recognition data, and related analytics were contained in the dataset disclosed in May 2027 (the "Class").

The Petitioners contend that the Respondents' collection, profiling, scoring, targeting, facial recognition practices, cross-border transfers, security failures, and subsequent disclosure of the Class members' personal data give rise to questions of constitutional and statutory interpretation affecting all members of the Class.

Issues for Determination

Participants shall address, among others, the following issues:

1. Whether the use of artificial intelligence, behavioural profiling, psychographic segmentation, voter influence scoring, and personalised political advertising to influence voting behaviour is compatible with the constitutional right to privacy.
2. Whether political microtargeting messaging based on inferred personal characteristics, emotional vulnerabilities, religion, ethnicity, socio-economic status, and predicted political preferences constitutes a lawful exercise of the freedom of expression.
3. Whether the processing of psychographic and behavioural voter profiles, ethnicity, religion, political opinions, facial recognition data, location data, and socio-economic information for electoral profiling constitutes lawful processing of personal data and sensitive personal data.
4. Whether the deployment of facial recognition technology at political events without adequate notice, transparency, or lawful basis violates constitutional and statutory privacy protections.
5. Whether the transfer and processing of voter data outside Lumora contravenes the Data Protection Act.
6. Whether the Respondents' security measures were adequate and whether their failure to notify affected individuals and the Office of the Data Protection Commissioner following the data breach was unlawful.

Reliefs Sought

The Petitioners, on their own behalf and on behalf of the Class, seek:

1. A Declaration that the use of behavioural profiling, psychographic segmentation, voter influence scoring, emotion-based targeting, and algorithmic political persuasion designed to influence electoral behaviour is inconsistent with the constitutional right to privacy.
2. A Declaration that the creation and use of psychographic, behavioural, and predictive profiles of members of the Class without adequate transparency, accountability, or lawful basis violated the Constitution of Lumora and the Data Protection Act.
3. A Declaration that the processing of ethnicity, religion, facial recognition data, location data, and socio-economic information of members of the Class for electoral profiling constituted unlawful processing of sensitive personal data.
4. A Declaration that the generation of Voter Influence Scores and predictive political profiles through automated processing without appropriate safeguards violated the constitutional rights of members of the Class.
5. A Declaration that the development and deployment of Mwanga Insight without a Data Protection Impact Assessment violated the right to privacy under the Constitution and the Data Protection Act.
6. A Declaration that the use of facial recognition technology for voter monitoring, tracking, and political engagement without adequate notice or transparency violated the right to privacy.
7. A Declaration that the transfer of personal data of members of the Class outside Lumora without appropriate safeguards contravened the Data Protection Act.
8. A Declaration that the Respondents failed to implement appropriate technical and organisational measures to secure personal data.
9. A Declaration that the failure to notify the Office of the Data Protection Commissioner and members of the Class of the personal data breach constituted a violation of the Data Protection Act.
10. An Order compelling the Respondents to disclose the logic, significance, principal parameters, and consequences of any automated systems used to profile, classify, score, or target voters.
11. An Order directing the Respondents to delete all unlawfully generated profiles, Voter Influence Scores, facial images, and related derived data of members of the Class, and to file an affidavit of

compliance.

12. General damages, compensation for members of the Class, and such further relief as the Court may deem just and appropriate under the Constitution and the Data Protection Act.

Guidance on Positioning

Participating teams are required to submit both applicant and respondent Memorials.

The laws of Lumora are materially identical to the Constitution of Kenya, 2010, the Data Protection Act, 2019, the Elections Act, 2011, and subsidiary legislation thereunder, unless otherwise stated. Participants may rely on comparative jurisprudence and international legal instruments where relevant.

The Moot Court Committee expects that all participants will adhere to the principle of fair play. Any severe violation of this principle may be sanctioned with disqualification.

For correspondence and more information, please contact: Email: **mootcourt@odpc.go.ke**