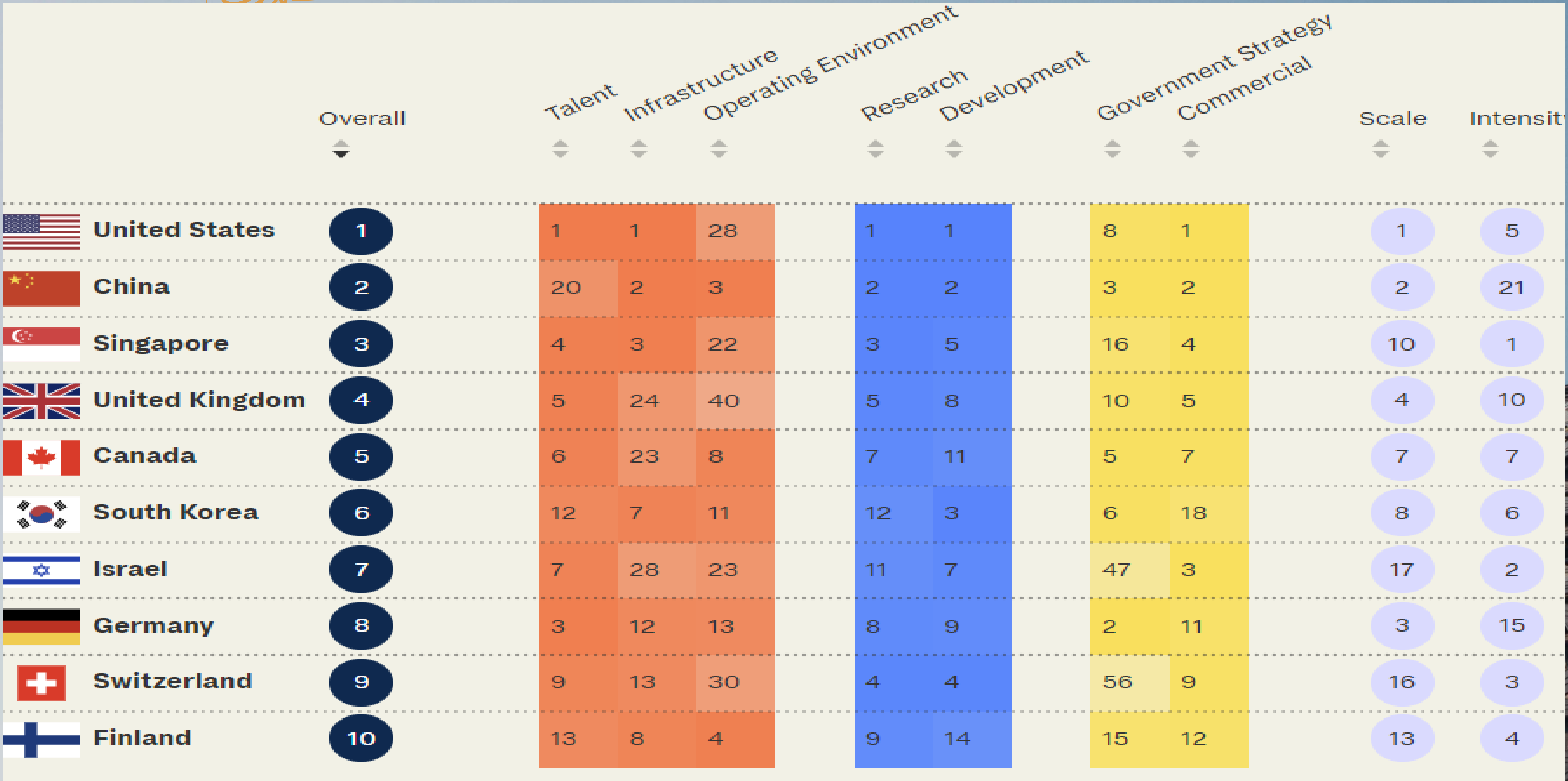
GALADARI
ADVOCATES & LEGAL CONSULTANTS
محامون ومستشـارون قانونيون

Navigating the Nexus of AI and Data Privacy: Insights from the UAE and Beyond

Raka Roy

Partner & Head of IP and Data Protection

Galadari Advocates & Legal Consultants



	Overall	Talent	Infrastructure	Operating Environment	Research	Development	Government Strategy	Commercial	Scale	Intensit
United States	1	1	1	28	1	1	8	1	1	5
China	2	20	2	3	2	2	3	2	2	21
Singapore	3	4	3	22	3	5	16	4	10	1
United Kingdom	4	5	24	40	5	8	10	5	4	10
Canada	5	6	23	8	7	11	5	7	7	7
South Korea	6	12	7	11	12	3	6	18	8	6
Israel	7	7	28	23	11	7	47	3	17	2
Germany	8	3	12	13	8	9	2	11	3	15
Switzerland	9	9	13	30	4	4	56	9	16	3
Finland	10	13	8	4	9	14	15	12	13	4

DATA SEMANTICS®
BETTER INSIGHTS SMARTER DECISIONS

“Machine intelligence is the last invention that humanity will ever need to make.”

- Nick Bostrom

www.datasemantics.co

TOPICS OF DISCUSSION

What is Artificial Intelligence

Data Privacy in the Digital Era

Current Challenges

Landmark Cases in the current time

Facial recognition, AI and Privacy rights

Relevant UAE legislations

UAE National Strategy for Artificial Intelligence 2031

Future Challenges and Recommendations

Artificial Intelligence –Few Facts!

- Mimicking human cognitive functions.
- Integrated into daily life ---voice assistants like Siri, Alexa, and customer service chatbots.
- By 2030, AI has the potential to contribute $15.7 trillion to the global economy,
- In the United Arab Emirates, 68% of companies allocate up to 50% of their tech budget to AI projects with well-defined strategies for the next five years.
- The rapid growth of AI is expected to boost global GDP by up to 14% by 2030.

Video: Dutch Telecom Agency

Data Privacy in the digital era.

- Digital age---- **personal data** ----valuable asset. **Empowered** businesses, governments, and organizations. However, sensitive information ----**organizations might misuse** without consent. **Rights to Privacy** becomes vital.

- Value of Personal Data
- Protection cyber harm
- Autonomy and Dignity
- Safeguarding free will

Challenges and Solutions in the Age of AI and Big Tech: Privacy, Ethics, Transparency, and Responsible Innovation

CHALLENGES

- Data-driven nature
- Extensive data collection
- Controversial technology
- Privacy and civil liberty concerns
- Lack of transparency
- Big Tech Influence
- Metaverse impact

SOLUTIONS

- Organizations using AI should **implement strong data security measures**.
- **Ethical AI system** design is essential for responsible data use.
- **Transparency is crucial**, allowing individuals to understand and control their data use, including opting out and requesting data deletion.
- The goal is to harness AI's benefits while **safeguarding privacy and data** protection.
- Ensure **AI respects individual privacy and adheres to ethical standards** in its development and application.
- **Big Tech firms** must prioritize transparency and ethical data use.
- **Responsible use of their power** is essential for the broader benefit of society.
- **Regulatory measures** may be necessary to enforce ethical practices and prevent abuses by Big Tech.

Legal and Ethical Challenges in the Age of Advanced AI

• OpenAI's ChatGPT and GPT-4 have revolutionized AI capabilities. Microsoft and Google have introduced AI-integrated tools for diverse applications. However, one cannot dodge the potential challenges brought about by such fast paced advancements.

BIAS AND FAIRNESS CHALLENGES

- AI models can perpetuate biases from training data, raising concerns about fairness.

TACKLING MISINFORMATION

- AI's potential to spread fake news necessitates stringent measures.
- Solutions include unbiased training data and public media literacy campaigns.

ACCOUNTABILITY FOR INTERMEDIARIES

- Growing calls to hold intermediaries responsible for harmful AI-generated content.
- Regulators scrutinize the role of intermediaries in content promotion.

INTELLECTUAL PROPERTY IN AI

- Complex IP issues arise from both data usage and AI-generated content.
- Ownership and commercialization challenges persist.

DATA PRIVACY AND PROTECTION

- AI models collect and process personal data, leading to privacy concerns.
- Robust data protection laws and ethical data practices are essential.

THE GLOBAL REGULATORY LANDSCAPE

- Governments worldwide are exploring AI regulation.
- Examples include the EU's AI Act and Canada's Artificial Intelligence and Data Act.

Google Location Tracking

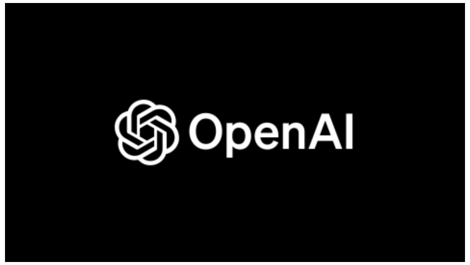
- **Faced intense scrutiny due to privacy concerns.**
- **In 2018, ----**tracked user locations **without explicit consent**, even when users opted out. This breach of trust **led to substantial backlash.**
- While Google **has since updated its policies and improved transparency**, worries persist about data misuse and third-party access.
- The **sensitive nature of location data underscores** the importance of robust security measures to protect user privacy and security.
- As one of the world's largest tech companies, Google's actions in this realm have far-reaching implications for individuals and society as a whole.

Class Action Lawsuit Filed by Microsoft Edge Users in California and Washington, USA

- On July 21, **a class action lawsuit was filed against Microsoft** by three individuals from California and Washington.
- **Saeedy et al v. Microsoft Corporation**,
- **Used by Microsoft to enhance its artificial intelligence and machine learning systems,** target advertising, and improve its software, services, and devices.
- The **plaintiffs have raised 13 distinct legal claims.**
- California plaintiffs in the case also assert that **their privacy rights under the state's constitution and other privacy laws were violated.**
- The lawsuit seeks **various remedies, including injunctive relief, restitution, disgorgement, and different forms of damages, such as statutory, actual, and punitive damages.**

P.M. v. OpenAI LP

- Anonymous plaintiffs filed a lawsuit **against OpenAI LP and Microsoft, alleging data theft.**
- OpenAI is accused of using **publicly-available Internet data to train AI tools like ChatGPT, Dall-E, and Vall-E.**
- **Allegations** include theft, misappropriation, and violation of privacy and property rights.
- Claims under Electronic Communications Privacy Act, state consumer protection laws, and common law.
- Plaintiffs emphasize AI's potential dangers, seeking human oversight and ethical protocols.
- Class-wide **damages and restitution for those whose data was used without permission.**



J.L. v. Alphabet Inc.

- Same plaintiffs' firm filed **a class action lawsuit** against Google.
- Accusations of **privacy and copyright law** violations.
- Google's generative AI products, including Bard, Imagen, Gemini, MusicLM, and Duet AI, **used Internet-collected data**.
- Plaintiffs argue Google should have **explored alternatives like purchasing commercial data.**
- Plaintiffs allege copyright infringement, **claiming AI products used copyrighted material.**
- Seeking **injunctive relief and specific remedies** for copyright claims.

Autopilot Accountability: Tesla's Landmark Trial Shaping the Future of Autonomous Driving

Imagine a Tesla on autopilot mode gets into an accident. Who do you think should be held responsible – the driver, the car manufacturer, or the AI system itself?

- **Tesla Autopilot Fatality in Florida (2016)**
- **Tesla Autopilot Class-Action Lawsuit (2017):**
- **Autopilot-Related Crashes and Investigations (Ongoing)**
- **National Transportation Safety Board (NTSB) Investigations: Regulatory Actions.**

Facial Recognition AI and Privacy Rights

Facial recognition technology **raises substantial concerns** surrounding privacy and consent.

Striking a balance between technological innovation and individual rights remains a formidable regulatory challenge.

The **outcome of these cases may significantly influence the trajectory of facial recognition AI** and the protection of privacy rights in the digital age.

Lawsuits targeting specific instances of harm caused by AI in facial recognition are crucial in setting legal precedents.

Courts and lawmakers are actively engaged in addressing the complexities of regulating facial recognition technology for responsible use.

Flora v. Prisma Labs, Inc.

- The lawsuit represents a putative class of internet users and **Prisma Labs, Inc., a software company specializing in AI applications.**
- The legal action alleges a violation **of Illinois' data privacy statute**.
- Plaintiffs claim that Prisma Labs' **portrait-generating application, Lensa**, scanned the facial information of internet users without obtaining their consent, thus infringing upon their data privacy rights.
- This case highlights the growing concerns surrounding the use of facial recognition AI and its impact on individual data privacy.

UAE Legislations concerning Data Privacy

Federal Decree-Law No. 45 of 2021 Personal Data Protection Law

- The UAE's inaugural federal-level data protection law, enacted on 20th September 2021.
- Designed to govern the processing of personal data and applies broadly unless explicitly exempted.
- Marks a significant step toward comprehensive data protection and privacy regulations in the UAE.

Telecommunications Law

- Regulates the telecommunications sector.
- Imposes penalties for intercepting telephone calls without permission.
- Requires licensed operators to protect the privacy of subscriber information.

Health Data Law

- Enacted to protect health data in the healthcare sector.
- Imposes obligations on healthcare providers, insurers, and IT providers.
- Aims to improve public health initiatives by enabling data collection and analysis.
- Supported by additional regulations, including Cabinet Resolution No. 32 of 2020 and Ministerial Decision No. 51/2021.

Consumer Protection Regulations

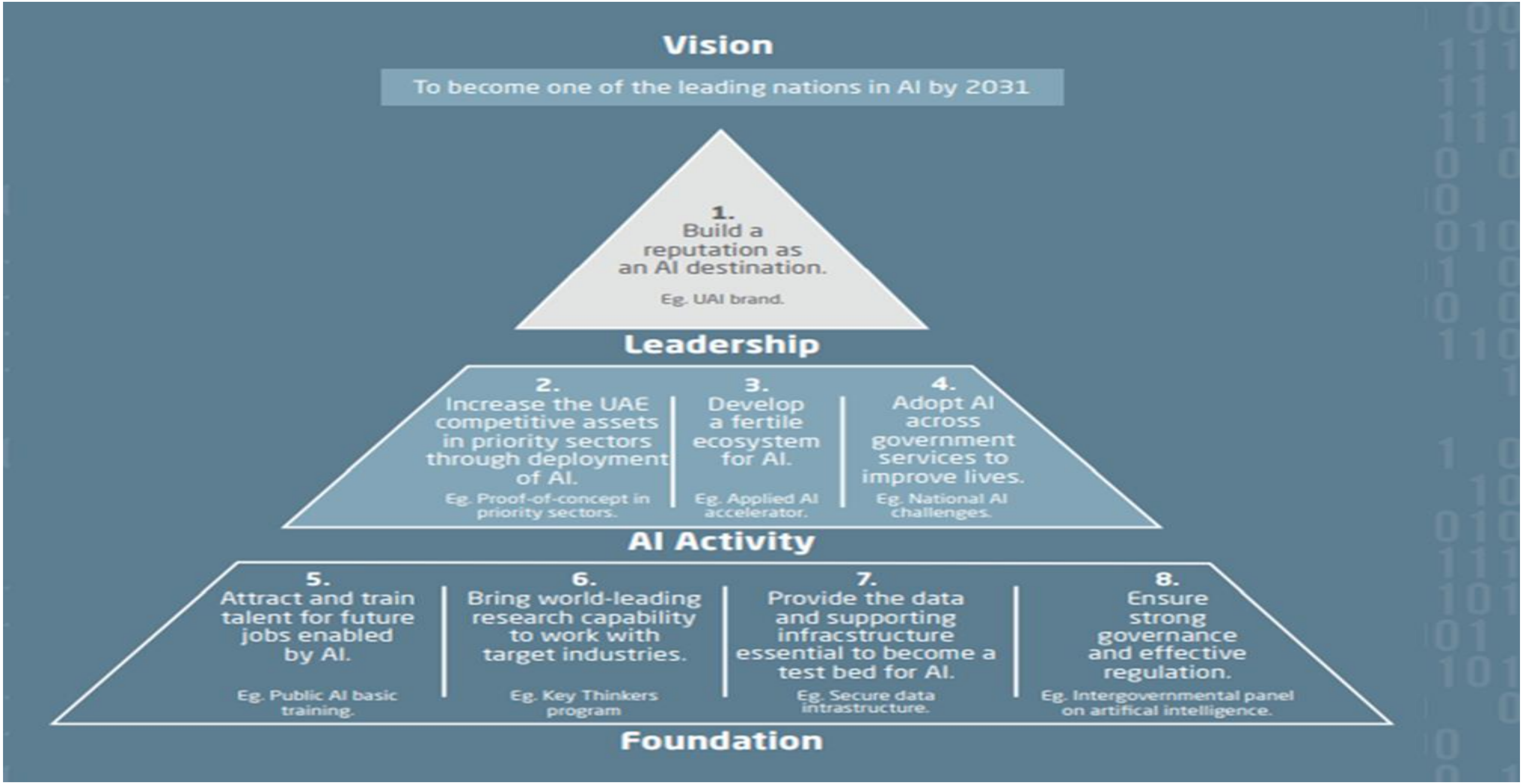
- Issued by the Telecommunications and Digital Government Regulatory Authority (TDRA).
- Obligates licensed operators to safeguard subscriber information.
- Limits the disclosure of subscriber information to third parties.

Cybercrime Law

- Penalizes hacking of websites, electronic systems, and information networks.
- Imposes fines and imprisonment for unauthorized data access, modification, or disclosure.
- Enhanced penalties for hacking with the intent to capture data for illegitimate purposes.

Constitution of UAE

- Provides citizens with a general right to privacy.
- Ensures the right to freedom and secrecy of communication.



Vision

To become one of the leading nations in AI by 2031

1. Build a reputation as an AI destination.

Eg. UAI brand.

Leadership

2. Increase the UAE competitive assets in priority sectors through deployment of AI.

Eg. Proof-of-concept in priority sectors.

3. Develop a fertile ecosystem for AI.

Eg. Applied AI accelerator.

4. Adopt AI across government services to improve lives.

Eg. National AI challenges.

AI Activity

5. Attract and train talent for future jobs enabled by AI.

Eg. Public AI basic training.

6. Bring world-leading research capability to work with target industries.

Eg. Key Thinkers program

7. Provide the data and supporting infracstructure essential to become a test bed for AI.

Eg. Secure data intrastructure.

8. Ensure strong governance and effective regulation.

Eg. Intergovernmental panel on artifical intelligence.

Foundation

UAE National Strategy for Artificial Intelligence 2031: A Roadmap to Innovation and Progress
UAE Strategy to a Data secure AI development

AI Governance Challenges:

- Rapid AI advancements
- Ethical and safe AI development
- Global governance challenges

Efforts to Address Challenges:

- Governments and AI experts involved
- Collaboration and learning from global leaders
- Establishing domestic and international AI regulations

UAE's Role in AI Governance:

- Promoting responsible AI
- Practical pilot projects
- Supportive legal environment & rapid regulatory changes
- Interconnected data systems
- Digital disruption susceptibility
- Importance of cybersecurity

UAE's Governance Review for Cybersecurity:

- Coherent national strategy
- Avoiding ad hoc approaches
- Considering cybersecurity importance

Objective 8 of the National Strategy: Ensuring strong governance and Effective regulations

Importance of Secure Data Infrastructure:

- Enable data sharing
- Address privacy concerns
- Unified AI data infrastructure
- Efficiency and access to data
- Data protection and authentication

UAE
WE WILL TRANSFORM THE UAE INTO A WORLD LEADER IN AI BY INVESTING IN PEOPLE AND INDUSTRIES THAT ARE KEY TO OUR SUCCESS.

Key Strategies for Companies

Prioritizing Data Privacy:

- Avoid **overlooking data privacy concerns** during the rush to adopt generative AI.
- Recognize that neglecting data privacy can result in **noncompliance and data breaches.**
- Emphasize the importance **of addressing data privacy early**, even if it slows down the adoption process.

Understanding the Compliance Landscape:

- The **global data privacy landscape** is intricate, with various regions and countries establishing their own regulations.
- Many jurisdictions **have implemented or are in the process** of adopting unique data privacy laws.
- **Establishing a diverse compliance team, including legal experts, DPOs**, data management specialists, privacy officers, and IT professionals, is crucial.
- This collaborative approach helps craft a **comprehensive compliance strategy adaptable to diverse regulatory environments**.

Employing AI Data Protection Best Practices:

- **Implement strict access controls to limit data access** to authorized team members.
- Utilize **secure data protection methods tailored to different stages** of the data life cycle (e.g., masking, tokenization, encryption).
- **Minimize data shared with generative AI platforms** to reduce the risk of exposing sensitive information.
- Develop and **continuously update AI data protection training standards within the compliance team**, keeping pace with evolving compliance regulations, threats, and technology trends.

Implementing the strategies

These implementing steps, guided by legal expertise, are crucial to ensuring data privacy compliance and safeguarding sensitive information in the era of generative AI technology.

- Legal Assessment
- Privacy Policies and Procedures
- Compliance Team Employment
- Contract Drafting and Reviewing
- Data Audits
- Access Control Agreements
- Compliance Monitoring
- Incident Response Plan
- Regular Legal Advises
- Litigation Support

Future Challenges

REQUIREMENT FOR MANDATORY REGULATIONS

- Potential requirements for individual prediction explanations **and detailed training record-keeping**.
- **Initiatives like the AI Bill of Rights** urge proactive company actions.
- Preparing for the **shift to mandatory regulations in regulated sectors.**
- Essential investment **in robust model governance** systems for compliance and innovation.

AI ACCOUNTABILITY

- AI algorithms, especially complex ones, can be opaque in decision-making.
- **Lack of transparency raises accountability concerns**, particularly when AI makes mistakes.
- The Tesla Autopilot incidents emphasized transparency and responsibility challenges.
- **Balancing proprietary tech protection with AI transparency** is vital for trust and accountability.

The way forward: Implementing Ethical AI

Beyond Compliance to Collaborative Solutions

Define Ethical Standards for AI:

- Ethical standards go beyond legal and regulatory compliance.
- Indentify industry-specifc ethical risks.
- Address challenging questions about what constitutes a discriminatory model and appropriate benchmarks.
- Develop frameworks and tools for ethical risk assessment and due diligence.

Identify Gaps in Ethical Standards:

- Technical Solutions alone cannot fully mitigate ethical risks.
- Collaboration among AI ethics team members is crucial.
- **Four key questions: risk identification, role of software/quantitative analysis, gap in analysis, and need for qualitative assessments**.
- Assess the technological maturity needed to meet ethical standards.

UAE DATA PROTECTION LAW ARE YOU COMPLIANT?

To win an exclusive Data Protection Assessment tailor made for your organization, Scan QR Code

- Half-day workshop to understand your readiness
- Our experts calculate a maturity score and gap analysis
- Prioritized list of recommendations to achieve compliance
- Ongoing guidance to achieve and maintain compliance

Q&A