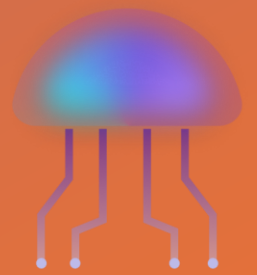
Ασφαλής Τεχνητή Νοημοσύνη: Προστασία Δεδομένων και Επιχειρηματικές Εφαρμογές

Dr. Georgios Feretzakis

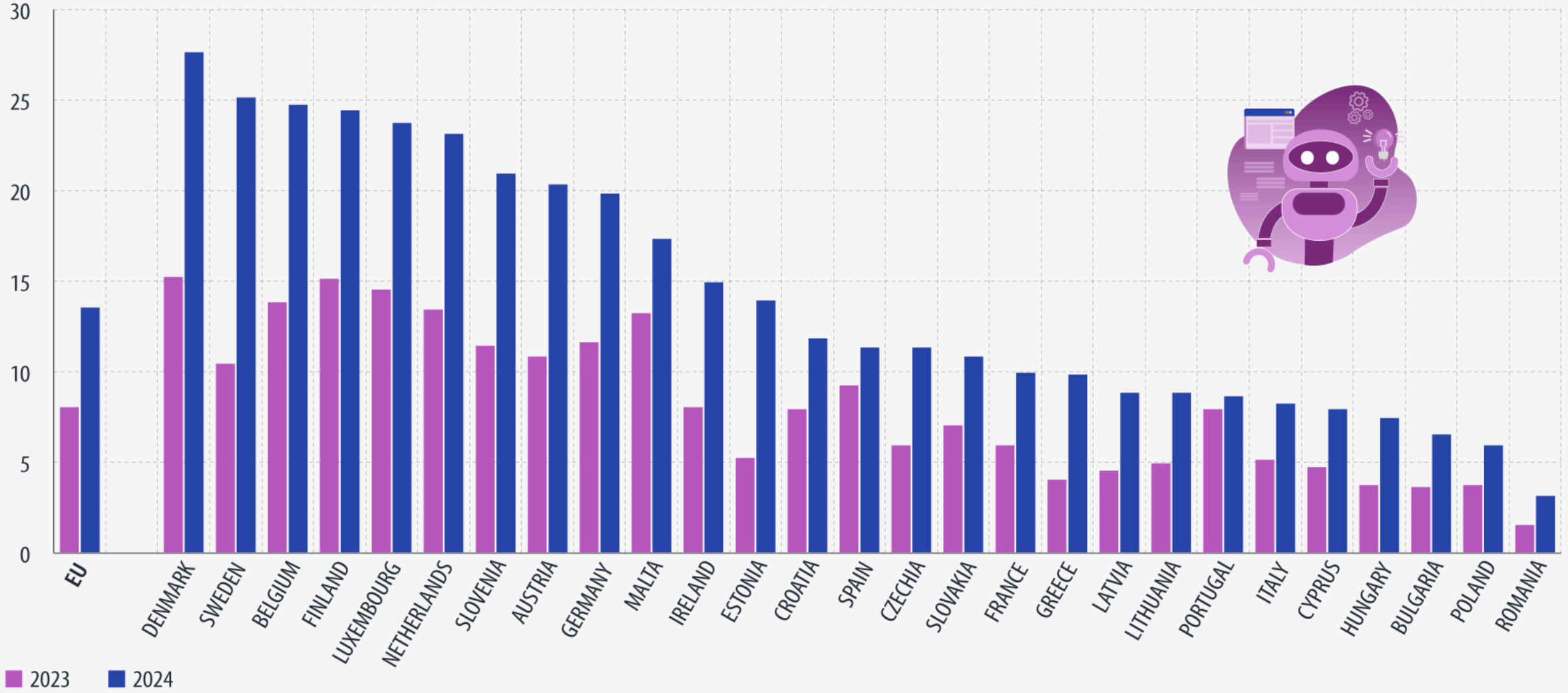
- CEO at securagen.ai
- Adjunct Lecturer & Researcher at Hellenic Open University
- Researcher at ReSEES, Athens University of Economics and Business



securagen.ai

Enterprises using AI technologies, EU, 2023 and 2024

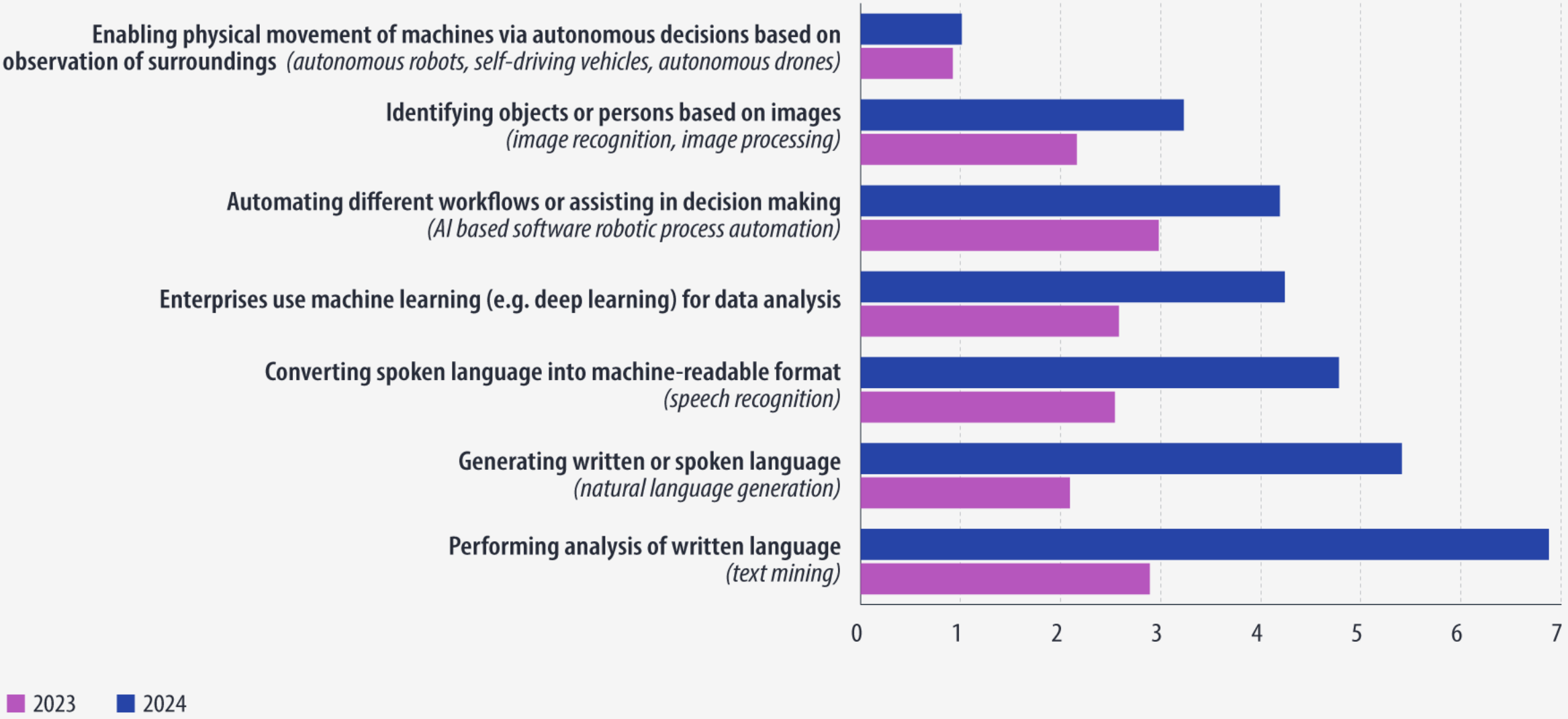
(% of enterprises)



France and Sweden: break in time series in 2023.

Type of AI technology used by enterprises, EU, 2023 and 2024

(% of enterprises)



Ασφαλής Τεχνητή Νοημοσύνη: Προστασία Δεδομένων & Επιχειρηματικές Ευκαιρίες

Κρίσιμο εργαλείο καινοτομίας για επιχειρήσεις

Απαραίτητη η προστασία ιδιωτικότητας & δικαιωμάτων

Πώς θωρακίζουμε την ΤΝ και τα δεδομένα μας;

Γιατί Είναι Σημαντικό για τις Επιχειρήσεις;

Διατήρηση & Ενίσχυση Φήμης

Υπεύθυνη διαχείριση ευαίσθητων πληροφοριών

Διασφάλιση Εμπιστοσύνης

Πελάτες & συνεργάτες απαιτούν σεβασμό της ιδιωτικότητας

Νομική Συμμόρφωση

Αποφυγή προστίμων (GDPR, EU AI Act, κ.λπ.)

Κίνδυνος με Δημόσια LLMs

“Απομνημόνευση” προσωπικών πληροφοριών

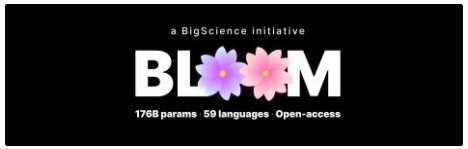
Αναπαραγωγή δεδομένων εκπαίδευσης

Συναγωγή ευαίσθητων στοιχείων

Ανάγκη αποφυγής κοινοποίησης προσωπικών δεδομένων σε δημόσιες πλατφόρμες

Κύριες Απειλές & Προκλήσεις

securagen.ai




Open Source & On-Premise

Έλεγχος Δεδομένων	• Τοπική επεξεργασία → ελαχιστοποίηση διαρροών
Προσαρμοσμένα Μέτρα Ασφαλείας	• Ευελιξία ρυθμίσεων & compliance
Διαφάνεια & Εμπιστοσύνη	• Επιθεώρηση κώδικα & μοντέλων
Ισχυρό Ανταγωνιστικό Πλεονέκτημα	• Καινοτομία με αποδοτική διαχείριση κόστους


securagen.ai

Υλοποίηση σε Cloud Platforms

Διαθεσιμότητα & Κλιμάκωση	• Pay-as-you-go, παγκόσμια υποστήριξη
Ενσωματωμένες Δυνατότητες Ασφαλείας	• Κρυπτογράφηση, διαχείριση ταυτοτήτων & πρόσβασης (IAM), παρακολούθηση σε πραγματικό χρόνο
Συμμόρφωση & Πιστοποιήσεις	• Συχνά συμμορφωμένες με GDPR, HIPAA, ISO 27001 κ.λπ.
Περιορισμοί & Εκτιμήσεις	• Σημαντική η προσεκτική επιλογή cloud provider για τοποθεσία δεδομένων (data residency) και πρόσθετες εγγυήσεις ασφάλειας

Κλειδιά Επιτυχίας στην Εφαρμογή

Στρατηγική Δέσμευση	• Διοίκηση & τμήματα στηρίζουν μέτρα ασφάλειας
Εκπαίδευση Προσωπικού	• Κυβερνοασφάλεια, νομικές πτυχές, ηθική
Ομαδική Προσέγγιση	• Data scientists, νομικοί, IT, leadership
Έλεγχος σε Όλο τον Κύκλο Ζωής	• Από τη συλλογή δεδομένων έως τη λειτουργία του μοντέλου
Διαφανής Επικοινωνία	• Τρόπος επεξεργασίας δεδομένων & δικαιώματα

Οφέλη Μιας “Ασφαλούς” ΤΝ

Ενδυνάμωση Φήμης: Προστασία ευαίσθητων δεδομένων → αξιοπιστία

Εμπιστοσύνη Πελατών: Σύγχρονοι καταναλωτές απαιτούν ιδιωτικότητα

Κινητήριος Δύναμη Καινοτομίας: Ασφαλή δεδομένα → νέες υπηρεσίες

Στρατηγικό Πλεονέκτημα: Προσέλκυση “έξυπνων” οικοσυστημάτων συνεργατών

securagen.ai

Τα Επόμενα Βήματα

- **Δημιουργία σαφούς Roadmap συμμόρφωσης**
- **Ενσωμάτωση Privacy-by-Design** σε όλα τα νέα έργα ΤΝ
- **Τακτικοί έλεγχοι & εκπαίδευση προσωπικού**
- **Παρακολούθηση νομοθετικών εξελίξεων** (EU AI Act κ.λπ.)

Τεχνητή Νοημοσύνη: Δύναμη και Υπευθυνότητα

Αξιοποίηση της ΤΝ με ασφαλή και ηθικό τρόπο

Επένδυση σε λύσεις

Απόλυτος έλεγχος δεδομένων και προστασία πελατών

Δημιουργία βιώσιμου δρόμου καινοτομίας

Ενίσχυση φήμης και οικοδόμηση εμπιστοσύνης

Πηγές

- Balancing Power and Privacy: Safeguarding Data in Generative AI and Large Language Models (Medium)
- Sharing with Caution — Protecting Your Personal Data When Using Public LLMs (Medium)
- How to Secure Generative AI Under the EU AI Act: Compliance, Risk Management, and Best Practices (Medium)

securagen.ai

Ερωτήσεις - Συζήτηση

g.feretzakis@securagen.ai

https://medium.com/@gferetzakis

https://www.linkedin.com/in/georgios-feretzakis-aab8b2249/

Google Scholar| Scopus| dblp| PubMed

securagen.ai