# Report AI & Algorithms Netherlands

Summer 2025 (Fifth edition, July 2025)

Periodic insight into trends, risks, and control of the use of AI and algorithms in the Netherlands

AP | bescherming in een digitale wereld

Autoriteit Persoonsgegevens
Department for the Coordination of Algorithmic oversight (DCA)

# Table of contents

Key messages

To chapter →

1. Overarching developments

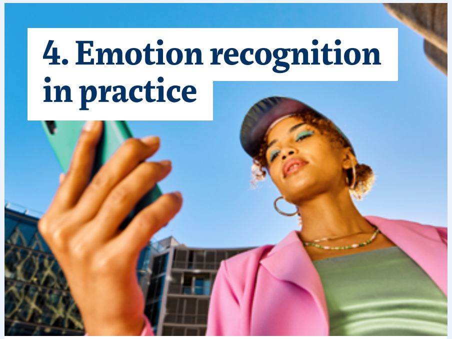
To chapter →

2. Policy and regulations

To chapter →

3. AI and emotion recognition

To chapter →


4. Emotion recognition in practice

To chapter →

Annex:
Getting Started with algorithm registration

To chapter →

Explanation of this report

To chapter →

# Key messages

### 1. The development and use of AI systems to recognise emotions is growing, while their effectiveness is questionable and their use poses risks.

More and more AI systems claim to be able to recognise emotions based on biometrics. Examples include recognising emotions to gain insight into consumer purchasing behaviour or to gain insight into patients' emotions with the aim of improving care. The systems are built on disputed assumptions about emotions and their measurability. It is therefore doubtful whether they can actually measure emotions. If the systems are deployed after all, this may violate fundamental rights and public values. Consider the restriction of freedom and human autonomy, discrimination and privacy violations. Read more about AI and emotion recognition in Chapter 3.

### 2. The AP has studied applications of emotion recognition in customer services, wearables and language models; in some cases, the wide range of applications leads to risks that require attention from providers, deployers, regulators and policymakers.

The in-depth study shows, for example, that it is not always clear how emotions and stress are recognised or how effective this is. Despite the growth of these applications, people are not always aware that emotion recognition is being used or which data is used to do so. Providers and deployers must be aware of the risks associated with each specific application. Various applications will soon be subject to specific regulations. Whether it is *desirable* to deploy these systems is a different issue. AI-based emotion recognition has been prohibited in the areas of workplace and education institutions since February 2025. Whether and to what extent the deployment of these systems is actually desirable, will ultimately be a political assessment. Read more about emotion recognition in Chapter 4.

### 3. The AP calls on organisations to adopt a critical stance to the deployment of emotion recognition applications.

Organisations must be aware of the limitations of emotion recognition and make a conscious decision as to whether its deployment is appropriate and proportionate. If these systems are deployed, organisations must be transparent about their use towards individuals whose emotions are being analysed. Furthermore, obtaining consent from the individuals being analysed is an important first step towards responsible use of the systems by organisations. Chapter 4 discusses three practical examples of emotion recognition. However, working towards responsible, conscious and transparent use is also important for other applications.

### 4. In the Netherlands, dedicated efforts are being made to develop reliable AI, but as a society we need to step up our efforts to be able to seize opportunities offered by AI in a responsible manner.

Reliable deployment of algorithms and AI is possible and requires attention to protection, security and transparency. This means that as a society we must learn lessons from incidents. Given the speed and scale at which Dutch organisations are adopting AI and algorithms, it seems likely that many incidents go unnoticed, unreported and that lessons learnt are not shared. Incidents are inevitable at this stage of the societal transition. Gaining experience with handling incidents and learning about their nature, cause and damage is essential for organisations to grow in terms of the responsible use of AI and algorithms.

## 5. With the help of an increasingly rich set of tools, every organisation can now effectively work towards AI maturity.

From algorithm registration, bias testing and setting up quality management systems to conducting fundamental rights assessments and making deployment transparent – to get there, organisations need to invest in people and resources and define measurable and specific organisational objectives. For example, an ambition to audit the most critical algorithmic processes and AI systems annually on key criteria such as organisational control, robustness, bias and fairness, cyber security and randomness. Mature organisations are transparent about their deployment, have robust systems and processes for control, and take internal and external control, and supervision seriously.

## 6. Discrimination and the design of human intervention is a major challenge. In the Netherlands, we are very aware of the fact that both individuals and algorithms can discriminate.

This clearly shows the importance of reducing both human and algorithmic bias in processes. The interaction between humans and algorithms is important in this respect and must be properly designed to prevent discrimination and bias wherever possible. The Dutch Parliament recently adopted a motion aimed at using "blind" assessment of citizens as a starting point. For example, in the case of fraud detection. From the perspective of the AP as a supervisory authority, it is necessary to look at the decision-making chain as a whole, incorporate random sampling, and to ensure that the risk-based selection can be explained and challenged.

## 7. AI plays an important role in geopolitical developments.

Commitment to successful deployment of AI is considered essential for economic development. Promoting innovation and the AI ecosystem has rapidly moved up the political agenda. Where there are concerns about rules curtailing innovation, deregulation is quickly considered. However, at the same time new regulations are being developed or implemented to protect against excesses. The perspective on the right balance between innovation and protection also differs per country and region. In addition, AI is increasingly becoming part of national strategies, ranging from healthcare to defence. Dependence on major players and the growing desire for strategic autonomy are playing an increasingly important role in this respect. This topic is also receiving attention at the European level, for example through the European Commission's AI strategy and related funding ambitions.

## 8. It is important to maintain or accelerate the pace of policy development and implementation in the Netherlands.

A national overarching AI strategy remains necessary in order to seize the opportunities offered by AI and manage the associated risks. It is important to make algorithm registration mandatory for public and semi-public organisations when deploying impactful algorithms or AI. The AP further recommends making periodic audits for these algorithms and AI a legal requirement. To guide responsible innovation in the right direction, all relevant supervisory authorities and inspectorates must have adequate resources for AI supervision in the Netherlands. Investments in partnerships are indispensable for effectively organising joint supervision and keeping pace with rapid technological developments. The AP recommends, in the case of public investments in innovation, to reserve a fixed percentage of investments for internal monitoring, external auditing and supervision. The proper functioning of these layers is essential for accelerating innovation and deployment.

## 9. The AI Act is becoming increasingly concrete, with standards being an important instrument for gaining control over AI and future compliance with the AI Act.

Over a year after the AI Act entered into force, we continue to see further clarification and refinement. The European Commission's guidelines on prohibited AI systems and the definition of AI systems provide initial insight and an explanation, but also raise many follow-up questions. Refinement will continue, with the development of standards providing clarity on how organisations can comply with the requirements of the AI Act. Not only generic, but also sector-specific implementations of the AI Act should lead to specific guidance and support.

## 10. Including algorithms in a register is a good starting point for managing the risks associated with the use of algorithms. An algorithm register contains information about the deployment of algorithms.

Broadly speaking, algorithm registration has two overarching objectives. Objective 1: To promote internal control of algorithms (governance). Objective 2: To promote external control of algorithms (transparency). The Dutch government is developing a legal framework for the Algorithm Register. This legal framework aims to provide clarity about the mandatory registration of algorithms. Even without this obligation, the Algorithm Register is already a valuable and practical tool for providing transparency and promoting oversight of government algorithms. Many organisations are not yet using the Algorithm Register; the AP encourages government organisations to make maximum use of the register. In the annex "Getting started with algorithm registration", the AP provides eight practical steps for getting started with algorithm registration.

## Overall control view of AI and algorithms in the Netherlands – Summer 2025

| Control pillar | Status Winter 2024-2025 | Status Summer 2025 | Explanation |
|---|---|---|---|
| Grip on the development and volatility of AI and algorithmic technology | **Requires increased attention** | **Requires increased attention** | Unchanged compared to the control overview of six months ago. The development of generative and other forms of AI continues unabated. The risks and impact of frontier models are not yet fully understood. |
| Understanding and current controllability of new AI and algorithmic risks | **Requires increased attention** | **Requires increased attention** | Unchanged compared to the control overview of six months ago. New developments are causing new incidents that are not always foreseeable. Control tools are still under development. |
| Development of national AI ecosystem | **Requires attention** | **Requires attention** | A strong national AI ecosystem is becoming increasingly important. This is evident from the growing desire for digital sovereignty. Attention to investments in AI is also increasing, providing an opportunity to catch up. |
| Trust in, focus on and knowledge of AI and algorithms in Dutch society | **On course** | **On course** | Unchanged compared to the control overview of six months ago. Having reached a low point in 2024, trust in AI and algorithms among the Dutch population continues to grow. The Netherlands is consciously working on AI literacy. |
| Frameworks and competences for oversight of AI-systems | **On course** | **Requires attention** | Requires increased attention due to the ambitious timelines for the AI Act, the call for simplification and the Dutch political situation. |
| Harmonised and practical standards for AI systems | **Insufficient progress** | **Requires increased attention** | Improvement compared to the control view of six months ago. Harmonised standards to prepare for the AI Act will not be finalised in the short term. However, progress in the development of standards is picking up speed. |

| Control pillar | Status<br>Winter 2024-2025 | Status<br>Summer 2025 | Explanation |
|---|---|---|---|
| Registration and transparency of algorithms and AI systems | **Requires increased attention** | **Insufficient progress** | Control picture is less positive compared to six months ago. Work on algorithm registration has been ongoing for several years, but there is still a long way to go. Most government organisations have not yet registered anything. |
| Insight into incidents involving the use of AI and algorithms and embedding of lessons learnt | **Insufficient progress** | **Insufficient progress** | Unchanged compared to the control overview of six months ago. There is a lack of reports and notifications about incidents involving AI and algorithms to supervisory authorities. |
| Institutionalisation of governance, risk management and auditing of AI and algorithms | **Requires increased attention** | **Requires increased attention** | Unchanged compared to the control overview of six months ago. Periodic audits are only carried out to a limited extent and the results are not yet fully visible. |

**Explanation:** As the coordinating supervisory authority for AI and algorithms, the AP (Autoriteit Persoonsgegevens) proactively identifies and analyses cross-sectoral and overarching risks and effects of the use of algorithms and AI. T. The so-called control pillars provide insight into the responsible management of these risks and effects. The overall control assessment shows the current control of AI and algorithms in the Netherlands. This control assessment should be seen against the backdrop of a wider societal transition, driven by AI as a system technology, which places increasingly higher demands on the level of control each year. To indicate the degree of progress (also in relation to the previous control assessment), the AP uses a colour code for each pillar: green means ”on course”, yellow means ”requires attention”, orange means ”requires increased attention” and red means ”insufficient progress”.

# 1. Overarching developments

QUICKLY TO THIS SUBJECT

1.1 Algorithms as a solution to scarcity →

1.2 Strategic autonomy and digital sovereignty →

1.3 AI-trust, AI-use and insight into AI-incidents →

1.4 Development of generative AI continues unabated →

1.5 AI and energy consumption →

1.6 Mapping algorithms and AI systems →

1.7 Discrimination risks in algorithms and the design of human assessment →

## 1.1 Algorithms as a solution to scarcity

**In the Netherlands, AI and algorithms are being deployed with high expectations of providing (partial) solutions to scarcity within society.** AI and algorithms are expected to offer smart solutions to, for instance, housing shortages and a congested energy grid. AI and algorithms are expected to produce new suggestions or accurate predictions for organisations to respond to scarcity.

**For example, various algorithms are being deployed in the healthcare sector with the aim of mitigating workload or organising care tasks more effectively.** The government is also fully committed to the adoption of AI in the healthcare domain.[1] In the years ahead, the government plans to invest €400 million in technological innovations, including AI, to increase the efficiency of the healthcare sector and reduce the workload.[2] For example, several hospitals are collaborating in a pilot programme for AI applications aimed at, among others, detecting fractures and identifying incidental pulmonary embolisms.[3] And generative AI is being used, for example, to assist in answering questions of patients.[4]

**The AP recognises that AI can be of great significance in the healthcare sector, bringing benefits both to healthcare providers and patients.** At the same time, there is the risk that, for example, healthcare institutions will become more dependent on cloud-based solutions and increasing data processing of sensitive data. Additionally, when it comes to using generative AI many applications have only been on the market for a short time and the impact on patient care is still (partly) unknown. It is with good reason that the Health and Youth Care Inspectorate calls on healthcare providers to handle responsibly the purchase, introduction and use of generative AI in healthcare.[5]

**The quality of medical care may also increase, for example due to algorithms being able to detect lung cancer earlier…** Positive developments like this regularly make the headlines. For example, an algorithm that is able to earlier predict the possibility of lung cancer based on patterns in patient records.[6] The algorithm analyses patient records for relevant patterns and weighs certain risks of lung cancer. Early detection of lung cancer with the new algorithm can lead to better treatment of the disease in some cases.

**…but the deployment of algorithms and AI in healthcare may also have indirect effects.** The possibilities of using AI for early detection of diseases also impacts on other parts of the healthcare chain. In a recent opinion, the Council for Health and Society (Raad voor Volksgezondheid en Samenleving, RVS) writes that the so-called diagnostic expansion (rapid increase in people with a disease diagnosis) is putting more pressure on a healthcare system that is already overburdened.[7] Whereas early diagnosis can be helpful for people with symptoms, early diagnosis in people without symptoms is increasingly stretching the criteria for disease. Therefore, the RVS calls for a public debate on the usefulness and necessity of early diagnoses as the possibilities for doing so increase thanks to technologies such as AI.

**The housing shortage is also being addressed by supporting people seeking housing with the help of AI and algorithms.** For example, AI agents are deployed to help people seeking housing find a new place to live more effectively, to assist with mediation, to personalise search results, and to show only homes they potentially qualify for.[8] Housing associations are also exploring the possibilities of AI.[9]

**The energy sector is increasingly using algorithms to prevent overload and thus accelerate the energy transition.** According to the *International Energy Agency*, fully embracing AI could save €95 billion annually and free up 175 GW of energy capacity.[10] In the Netherlands, energy companies and grid operators are fully committed to AI to find suitable locations for solar and wind farms, for example, or to predict energy consumption for optimisation purposes. Last year, supervisory authorities the Netherlands Authority for Consumers and Markets (ACM) and the Dutch Authority for the Financial Markets (AFM) established that algorithmic energy trading has increased significantly and point to risks of volatility and opaque pricing.[11] Researchers from the Rathenau Institute recently warned that integrating AI into electricity systems could create dependencies on large tech companies outside the EU.[12] This makes grid operators and utility companies dependent, reduces democratic oversight, and potentially creates monopolistic market structures.

**People are directly affected by the AI-driven energy market.** Developments such as dynamic pricing, where AI plays a central role, encourage households to adjust their energy consumption to fluctuating rates. This may help to reduce peak loads, but also raises questions about accessibility, fairness and explainability – in particular for people who have less flexibility in their schedule or demands, or people who do not have access to smart technologies.

**AI offers benefits and can help better match or direct supply and demand, but it also raises new and fundamental distribution issues in which trade-offs over fundamental rights and public interests are being made in the background, without it being given full attention.** Who gets access to energy and when? On what basis are choices made? And who has a say in this? *Algorithmic fairness* is crucial in this respect. But what is considered "fair" depends on the standard: is it about equal opportunities, equal treatment or equal outcomes? Without clear choices, algorithms may actually reinforce existing inequalities.[13]

## 1.2 Strategic autonomy and digital sovereignty

**Increasing geopolitical tensions further increase the need for strategic autonomy.** The integration of AI into sectors and applications with high societal impact increases dependencies.Strategic autonomy means that countries can act autonomously, without being dependent on other countries.[14] This includes the European economy, energy, but also technology.

**In June 2025, Meta invested $14.3 billion in Scale, a global company that trains AI models.** This investment gives Meta a 49% stake in the company.[15] Scale's CEO has also joined Meta. Investments on this scale show how important a small group of large tech companies consider the development and training of AI models.

**There are positive developments that increase digital sovereignty and strategic autonomy.** Yet, there is a long way to go. Proprietary systems are increasingly being developed to become less dependent on non-EU parties. We are also seeing more and more *"private AI stacks"* that companies and other organisations can build and run their AI applications on. But full digital sovereignty is still a long way off. The Netherlands Court of Audit (Algemene Rekenkamer) states that the central government purchases more than half of its public-cloud services from three major US tech companies.[16]

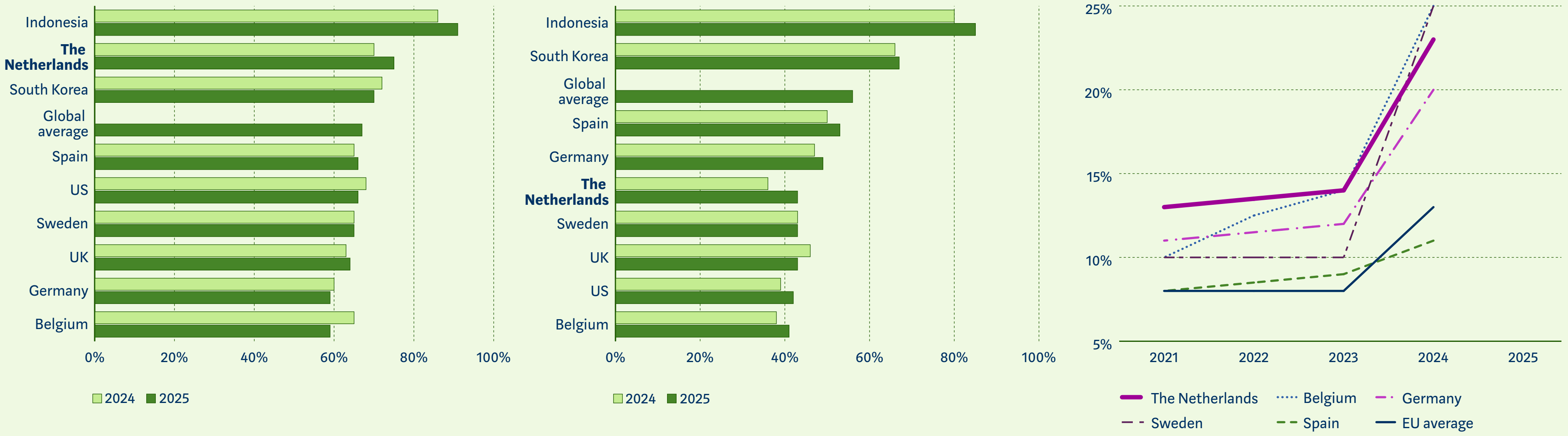
**Furthermore, the province of Groningen and some municipalities are pushing for the establishment of an "AI factory" to reduce dependence on other countries with respect to artificial intelligence.** The European Commission intends to have at least 15 of such "factories" in Europe.[17] This type of factory should consist of a centre of expertise and a supercomputer. It is seen as a unique opportunity for economic growth, knowledge development and innovation in the region and in the Netherlands.[18] The factory will cost between €160 million and €240 million in total, making it one of the most expensive AI factories in Europe. Financial commitments from the Groningen region, the province of North Drenthe and the government have brought the realisation of this project a step closer.[19]

**Working on strategic autonomy ultimately also contributes to maintaining control over the algorithms and AI used in the Netherlands.** Increasingly, the performance of society-critical processes, for example government services, depends on the use of algorithmic processes. Strategic autonomy ensures that the Netherlands has its own infrastructure and data management on the basis of which algorithms and AI systems can operate. For example, for algorithms deployed for government decision-making, this ensures that the Netherlands can fully align its systems with its own fundamental values and retain its own technical and ethical control over them.

## 1.3 AI-trust, AI-use and insight into AI-incidents

**Dutch citizens have an increasingly positive attitude about their AI knowledge and comparatively see more and more benefits in AI.** Globally, about two in three people feel they have a good understanding of AI. This was the finding of an international comparative study carried out by Ipsos in 30 countries.[20] In the Netherlands, 75% of citizens now agree with this statement – an increase of 5% compared to 2024. This means that the Netherlands scores higher than most other countries. Therefore, confidence in one's knowledge of AI is sound. Dutch people also see proportionally more advantages than disadvantages in AI. In 2024, the Dutch were the most critical of AI worldwide. Back then, 36% of the Dutch population said they saw more advantages than disadvantages in AI. By 2025, this percentage has increased by 7% to 43%. This puts the Netherlands on par with countries such as Belgium, the United States (US), the United Kingdom (UK) and Sweden. This development confirms the picture we observed in the previous edition of the RAN: the downward trend in Dutch trust in algorithms and AI has reversed. See also Figure 1.1.

**FIGURE 1.1 | DEVELOPMENTS IN PERCEPTION AND USE OF AI IN THE NETHERLANDS**



**In 2025 Dutch citizens feel very positive about their understanding of AI...**

% that agrees with the statement
"I have a good understanding of AI"

**... the Dutch are relatively less critical towards AI...**

% that agrees with the statement that products and services with AI offer more advantages than disadvantages

**... and the Netherlands continues to be a leader in companies that deploy AI.**

% of companies that use at least one of seven AI technologies

**Source:** left and middle: Ipsos AI monitor (n=23.685, 32 landen), right: Eurostat (online data code: isoc_eb_ain2)

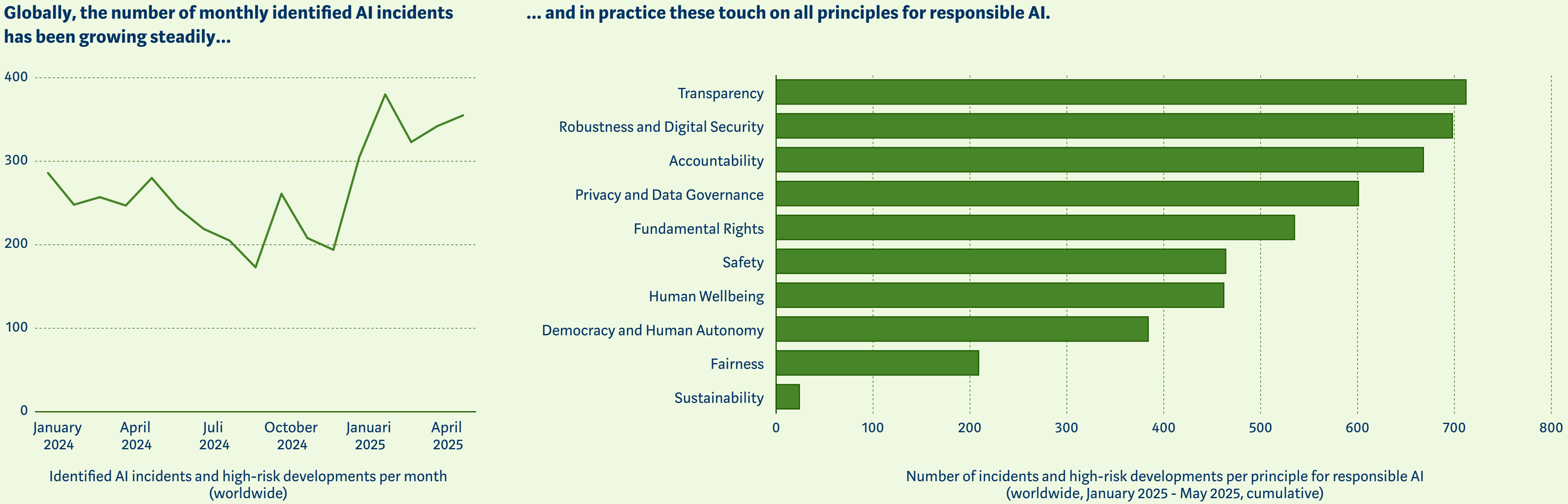
**A growing number of Dutch companies are using AI, accelerating since 2023.** Eurostat data provides insight into the trend in recent years. In 2024, approximately one in four Dutch companies used at least one of the seven AI technologies defined by Eurostat (Figure 1.1). These include machine learning, image recognition, robotics in autonomous vehicles, robotics in process automation, speech recognition, text mining and language generation (written or spoken). At 23%, the Netherlands remains a European leader. At the same time, however, we have been overtaken by Belgium and Sweden in terms of AI use within companies, for example.

**In recent months, the global media has increasingly been reporting incidents and high-risk developments related to AI.** Based on information from the media, some 300 to 400 incidents and high-risk developments have been added monthly to the OECD AI Incidents Monitor since early 2025. This helps to gain insight into high-risk developments and how they affect principles for responsible AI. In 2024, 200 to 300 monthly incidents were reported. Figure 1.2 shows the recent development.

**It is notable that incidents and high-risk development touch on all principles for responsible AI.** Reports related to the principles for responsible AI, fairness and sustainability are the least frequent. This is partly due to the fact that in the case of fairness, these risks are still mostly under the radar or, in the case of sustainability, develop primarily in the long term. Over the period January to May 2025, approximately 700 incidents and high-risk developments related to (lack of) transparency were reported (Figure 1.2). But also in other areas, such as digital security (including cybersecurity risks), accountability, privacy, fundamental rights and physical security, there have been numerous incidents and high-risk developments.

**Incidents can impact rights as well as the physical world.** For example, a privacy incident arose because prompts from some users in Meta AI, which will soon be available in the Netherlands, appeared on a public feed of Meta without the user's consent. This could happen, for instance, to users who use Meta AI via Instagram and have a public Instagram account.[21] Furthermore, Google Maps recently created unnecessary risks to physical security: on Thursday 29 May, the programme's AI incorrectly indicated that several highways in Germany, the Netherlands, and Belgium would be closed, causing alternative routes to become overcrowded.[22] Reported cybersecurity risks often arise because AI makes hacking, for example through social engineering and phishing, considerably easier.

**FIGURE 1.2 | GLOBAL DEVELOPMENTS IN AI INCIDENTS AND HIGH-RISK AI DEVELOPMENTS**



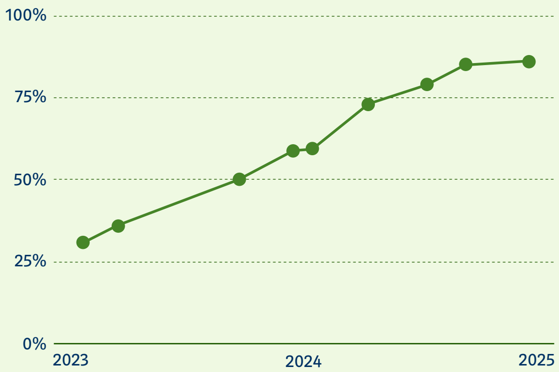
**Source:** OECD AI Incidents Monitor (AIM)

## 1.4 Development of generative AI continues unabated

**New generative AI models are launched very frequently in 2025.** Major providers of language models (so-called *Large Language Models*), such as OpenAI, Google, Meta, Mistral, and newcomers like DeepSeek and Alibaba, have collectively released more than 10 new (versions of) models in the first half of this year. Despite the fact that these models appear to be reaching their limits in some areas, significant progress is still being made in their usability and economic value.

**New language models are often not much "smarter" than their predecessors these days, but their performance in other areas does improve.** A key barometer for model performance, the GPQA score, appears to have plateaued in the past six months.[23] (See Figure 1.3). However, significant progress continues to be made in (i) the types of content a model can generate, such as text and video, (ii) the amount of input a model can handle, and (iii) the efficiency of models.

**FIGURE 1.3 | THE GROWTH OF LANGUAGE MODELS IS LEVELLING OFF IN SOME AREAS**



**Explanation:** Highest LLM score on GPQA index (% correct answers, maximum 100%).
**Source:** LLM Stats

**Generative AI models can manage an increasing amount of input.** While at the launch of ChatGPT in late 2022, the so-called *context window size*, the size of a prompt or document a model receives as input, was barely the size of a single page in a book, the latest models can handle more than two full books of input.[24] The latest generative AI models now use and generate code, audio, and video in addition to text. These models can, for example, summarise the contents of a video in text, or generate a video clip with sound based on a *prompt* from a user.

**Models achieve similar results with less computing power.** As a result of ongoing innovations in the way models are trained and operate, new models often achieve similar performance compared to previous top models, at a fraction of the cost.[25] These more efficient models use less computing power and thus energy, both during development and use.

**At the same time, some persistent model deficiencies remain, such as when models produce incorrect information.** These days, many models have access to the internet to find information and arrive at their output based on a number of "reasoning steps". While these functionalities lead to better outcomes in certain situations, several studies have shown that models continue to produce misinformation from a vacuum.

**Organisations in California are insufficiently able to fully understand risks and impacts of frontier models.** "The California Report on Frontier AI Policy" was released on 17 June.[26] This report argues that a proper balance is needed between innovation and regulation. However, organisations are currently unable to keep up with the rapid developments in terms of risk management and potential impact. The report advises on how policy instruments can be used to safeguard key principles, in line with the EU and the UK. This approach differs from proposals at the federal level in the United States, where banning of further regulation of AI is under discussion.[27]

**People who write texts with the help of an LLM/AI chatbot use their brains less, remember the information from those texts hardly or not at all, are less creative and the final text contains mostly common words and concepts.** These are the initial results of a study conducted by MIT.[28] In this study, a group of 54 participants were asked to write an essay without tools, using a traditional search engine, and using ChatGPT. This initial study is part of a project aimed at mapping the cognitive effects of using AI writing tools in the educational context. These initial signals are cause for concern and demonstrate that additional attention is needed for the well-considered integration of these tools in education and society.

**An example of increasing deployment is the use of generative AI in chatbots for public communication.** These types of chatbots increasingly utilise LLMs, which are subsequently tailored to the specific information an organisation wants to provide in its communication to the general public. As such, communication of the chatbot becomes an interplay between the characteristics of the underlying language model and the organisation's specific information and instructions. As a result, the provision of information by the organisation is partly influenced by developments, such as updates, in the underlying language model. In addition, it is difficult to prescribe how the chatbot should communicate for all circumstances. This presents new challenges. In the period ahead, the AP will further explore the use of generative AI for public communication.

## 1.5 AI and energy consumption

**The enormous amounts of data and computing power can pose problems for the interest of a clean, healthy, and sustainable environment.**[29] Training new systems requires increasingly more energy, which puts increasing pressure on this interest. Energy consumption does not stop after training an AI; using AI requires at least as much energy. Once an AI system has been trained, its energy consumption does not automatically decrease. For example, asking a question to ChatGPT is estimated to require 10 times more energy than asking the same question to Google.[30]

**Major AI companies moving full steam on developing their own (nuclear) energy supply.** The World Economic Forum argues that the increase in energy consumption calls for an acceleration of the energy transition, requiring the use of sustainable solutions.[31] To meet energy needs, major AI companies are developing their own infrastructure and facilities. For instance, there is increasing interest in nuclear energy.[32] Microsoft has announced a $1.6 billion agreement to generate electricity with a nuclear reactor for AI use, while Google and Amazon also have nuclear energy agreements to support their AI efforts.[33] In addition to the major impact on the environment and sustainability, the development of AI also carries the risk of essential (energy) infrastructure ending up in private hands, increasing social and individual costs.

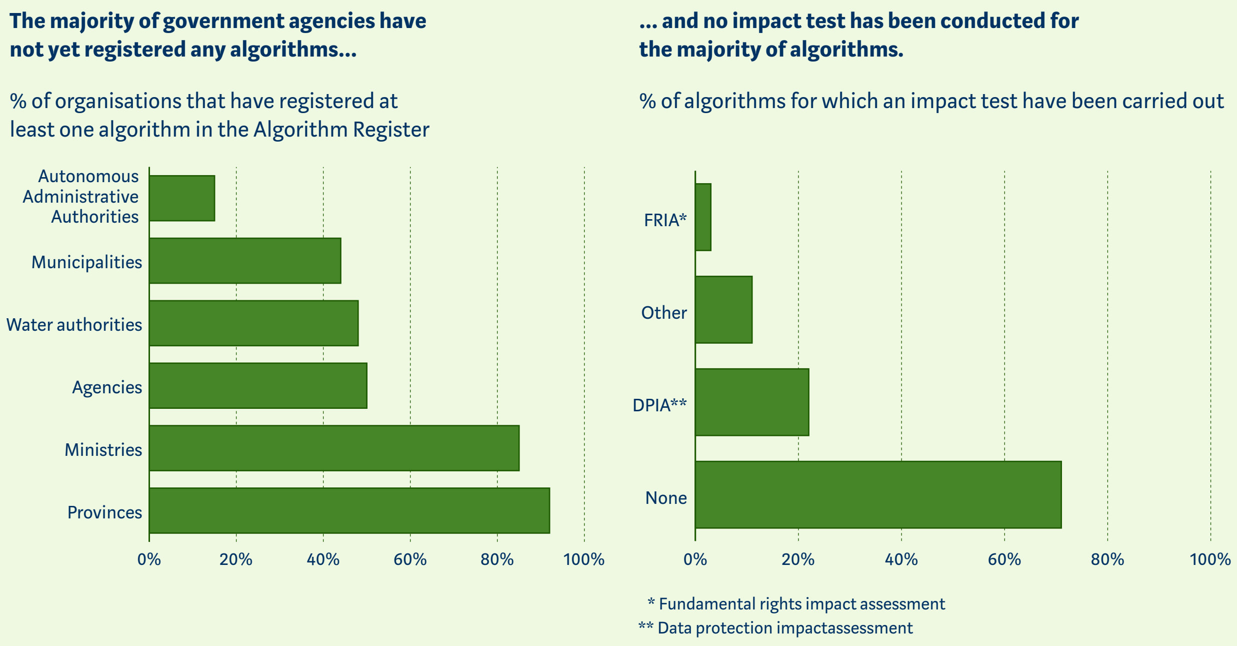
**Although no precise figures are available, water usage for AI is also increasing rapidly.** Data centres use large quantities of water to cool AI hardware and prevent overheating. Microsoft manages a large section of the server infrastructure on which ChatGPT, among other things, runs. Since the arrival of ChatGPT in 2022, researchers estimate that Microsoft's water consumption increased by 34% in 2022 compared to the previous year. Having GPT-4 write a single email of just 100 words uses 519 millilitres of water.[34]

**High water consumption of data centres may cause water scarcity in areas that have less water.**[35] [36] In the US, data centres are often located in areas where some degree of water scarcity already exists.[37] It is important to place greater emphasis on renewable energy sources and sustainable AI systems. Green AI focuses both on deploying AI to solve sustainability issues and on optimising AI to make it less demanding.[38]

## 1.6 Mapping algorithms and AI systems

**Registrations in the Algorithm Register for the Dutch government are progressing steadily, but most government organisations are yet to register their algorithms.** About 1,000 algorithms have been registered since the creation of the Algorithm Register for the Dutch Government in 2023. Leaders are the municipality of Amsterdam with about 60 algorithms and the Customs Administration with approximately 50. Meanwhile, most government organisations still have not registered a single algorithm. For instance, less than one in five independent administrative bodies have registered at least one algorithm. Similarly, more than half of all municipalities have not yet registered anything. This is shown in Figure 1.4.

**FIGURE 1.4 | DEVELOPMENT ALGORITHM REGISTRATION DUTCH GOVERNMENT**


**The majority of government agencies have not yet registered any algorithms...**

% of organisations that have registered at least one algorithm in the Algorithm Register

**... and no impact test has been conducted for the majority of algorithms.**

% of algorithms for which an impact test have been carried out

* Fundamental rights impact assessment
** Data protection impactassessment

**Source:** Algorithm Register (algoritmes.overheid.nl), reference date 11 June 2025

**While it is possible that organisations do not use any algorithms at all, this is unlikely in many cases... The accumulation of knowledge on algorithms and AI within organisations is still in full swing.** And algorithms and AI systems are not always easy to recognise as such. It is important that organisations receive support in this regard and that they can be challenged externally on their algorithm registration and any potential absence thereof. In any case, it remains difficult to currently assess to what extent organisations are in the process of registering their algorithms. For example, the Police Science Advisory Council (Wetenschappelijke Adviesraad Politie) concludes that much is happening in the field of data and AI, both within and outside the police force.[39] HiThe advisory council notes that ”it is difficult to provide a complete overview, partly because developments occur rapidly and there is little coordination between the numerous initiatives in various parts of the organisation.” With this in mind, it is difficult to explain how this compares to the current number of six registered algorithms by the National Police Force (see also Box 1.1 on algorithms and AI in the Police Force).

**...it is important, therefore, to also record that a government organisation declares that it does not use algorithms, if this situation arises.** Within the central government, this can be based, for example, on the letters regarding the progress of algorithm registration sent to the Dutch parliament by each ministry, which also specify the number of algorithms and AI systems that have been identified within organisations.

**Another area of focus with respect to algorithm registration is that government organisations have conducted a Fundamental Rights Impact Assessment (FRIA) for less than 5% of the algorithms.** Figure 1.4 shows the extent to which impact assessments in respect of algorithms have been conducted. A FRIA can be conducted in various ways, using different formats. For example, by adhering to the format of the *Impact Assessment Human Rights and Algorithms (IAMA)*. Ideally, the results of such an assessment will also be made public, allowing stakeholders to learn how the impacts on their fundamental rights have been assessed. To date, this underlying documentation has not or hardly been included in the Algorithm Register of the Dutch government.

**Carrying out a FRIA will be a requirement under the AI Act for government organisations using high-risk AI systems...** Every government organisation must carry out a FRIA before implementing a high-risk AI system. These include systems used in biometrics, education, labour, public service, law enforcement, migration, asylum and border control, justice or democratic processes. This assessment is updated as per requirement during the use of the system.

**...and government organisations subsequently inform the market surveillance supervisor of the outcomes of the FRIA prior to implementing the system.** The AI Office, part of the European Commission for European AI supervision and coordination, is developing a template that can be used for the FRIA in the period ahead. The FRIA reporting obligation will help market surveillance supervisors gain up-to-date insight into the use of AI systems within the government and the associated assessment of fundamental rights risks. Within the financial sector, a similar obligation will apply to credit provision and price determination.

**Box 1.1**

### Case: Deployment by the police?

**The use of algorithms in the police force continues to require attention.** Police work is increasingly driven by data and the question is how the new context will affect the execution and design of police work. A report by the Police Science Advisory Council details the various challenges of data and AI applications within the Police force.[40] The opinion recommends that decision-making on AI should become part of the broader governance of the police force. Ethical, legal and social aspects should be structurally considered when developing AI applications. Active transparency should become the rule. AI literacy should become an "integrated core skill", to develop a "critical digital mindset", with an eye for (conflicting) public values. Furthermore, the council argues that AI applications that can improve the relationship between the Police force and citizens should be sought in order to possibly also direct the social debate on deployment of AI by the police in a positive direction. Moreover, there should be more empirical research into the effectiveness of the deployment of AI by the police, as well as a normative test for desirability and explainability. Finally, the council advises against further deployment of systems designed to predict behaviour at the individual level.

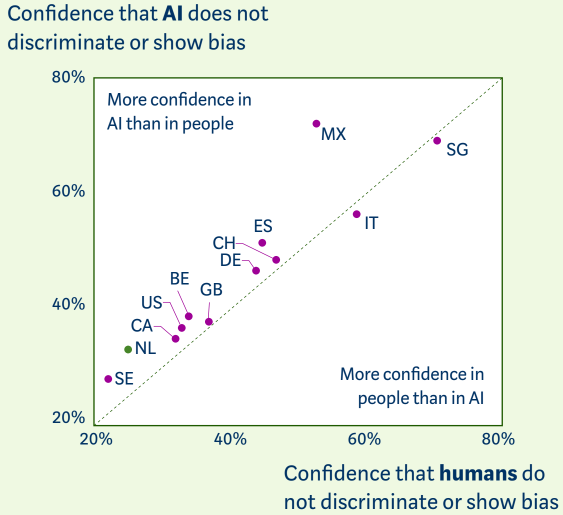
**Specific predictive AI systems for risk assessment of criminal offences are prohibited under the AI Act.** The AP points out that according to Article 5(1)(d) of the AI Act ("prohibition D"), AI systems may not be used for making risk assessments of natural persons in order to assess the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics. This is in line with the Council's advice not to deploy AI systems that attempt to predict individual behaviour. In February the AP launched a "Call for Input" in response to this prohibition. It explained specific criteria for these prohibited AI systems and asked for additional input.

## 1.7 Discrimination risks in algorithms and the design of human assessment

**By 2025 the Dutch are very aware that not only humans but also algorithms can discriminate towards groups of citizens…** The Dutch, along with the Swedes and Canadians, have relatively low confidence in the ability of AI to act fairly without discrimination or bias. Only 33% of Dutch people believe that AI systems do not exhibit bias. In other countries, such as Germany (47%), Spain (52%) and Mexico (73%), this percentage is higher. It is notable that confidence in people in this regard is even lower: only 25% of the Dutch believe that people themselves are not discriminating or biased. There seems to be a clear correlation: in countries where people have little faith in people in terms of non-discrimination, confidence in AI systems is also low. Yet in most countries, people view AI as being slightly fairer than people. (See Figure 1.5).[41]

**…the Dutch are also very aware of the fact that people show bias and discriminate (unconsciously).** A study by the European Commission from 2023 shows that the Dutch by comparison are highly aware of their own bias towards others. In 2023, 26% of the Dutch indicated that they had consciously or unconsciously discriminated in the past 12 months. This is nearly four times as much as the European average of 7%. After the Netherlands, the highest percentages are recorded in Sweden (19%), Denmark (16%) and Romania (11%). All other Member States report less than 10%.[42]

**FIGURE 1.5 | CONFIDENCE THAT AI AND HUMANS DO NOT DISCRIMINATE OR EXHIBIT BIAS**



**Explanation:** The Dutch have little confidence that AI and humans do not discriminate.

**Source:** Ipsos AI monitor (n=23,685, 32 countries)

**These results show the importance of reducing both algorithmic bias and human bias in processes that affect people.** The strong awareness that both occur provides a good starting position and support for the Netherlands to take steps in this respect. Certainly the childcare benefits scandal has made it clear to the Dutch that institutional bias in research and assessment by a government organisation can occur.[43] This institutional bias is further reinforced when risk selection takes place on the basis of discriminatory algorithms, as was the case in the childcare benefits scandal.[44]

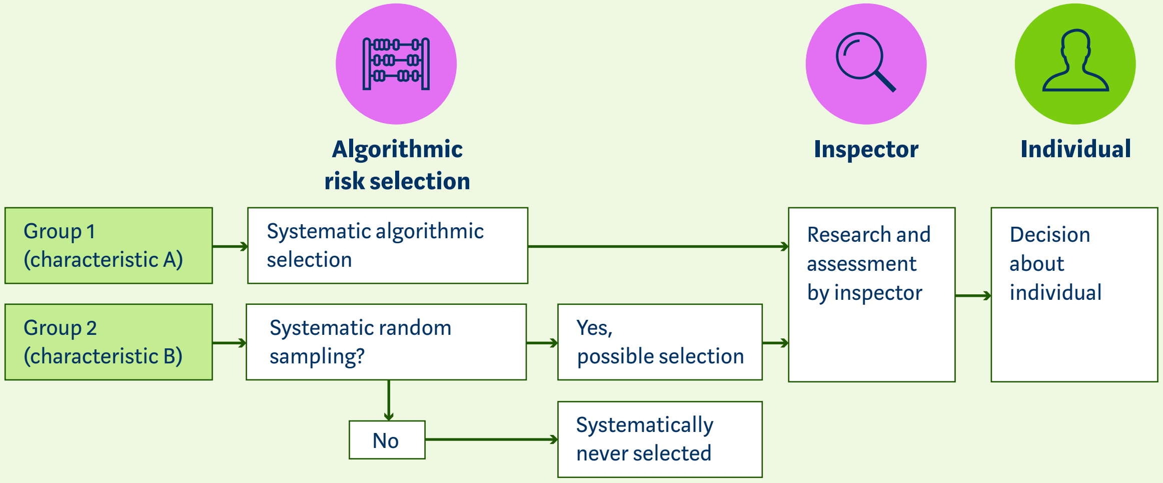
**To minimise the risks of bias and discrimination, among other things, where possible, science stresses the importance of properly designing the interaction between humans and algorithms.** Bias by algorithms are particularly risky: they work systematically, can affect every person in the same way, record historical biases and are often difficult to explain or understand. These biases come on top of human prejudices, although their form may differ.[45]

**If designed incorrectly, the interaction between algorithms and humans can even worsen the degree of discrimination and bias.** Take the example of profiling and selecting algorithms that perform a preselection for fraud detection by inspectors. Various studies confirm the risk that inspectors, based on algorithmic recommendations, can behave more inconsistently and preferentially.[46] At the same time, a proper design will allow for algorithms and humans to complement each other. An important objective is to coordinate inspectors and algorithms in such a manner that inspectors have just enough faith, but not blind faith, in the results of an algorithm. This allows inspector and algorithm to be complementary to each other. This requires a clear and supportive explanation about how the algorithm performs selections and estimates risks. Consider, for example, showing margins of uncertainty with every risk selection, allowing inspectors to better assess how strong a signal is.

**In May 2025 the House of Representatives adopted a motion in which the Dutch government was requested to take as a starting point that citizens are assessed ”blindly”, for example in the event of fraud detection.** The underlying idea is that if an inspector has no knowledge of the reason for investigating an individual file, the inspector cannot be influenced by the algorithmic prediction. Therefore, the motion aims to prevent tunnel vision and bias in human assessment.

FIGURE 1.6 | SYSTEMATIC RANDOM SAMPLING IS NECESSARY TO CONTROL RISKS OF DISCRIMINATION, EVEN WITH BLIND CONTROL

**Systematic inclusion of random sampling is crucial to identify bias throughout the chain, even in the case of ”blind” assessment of files by inspectors.**


Algorithmic risk selection
Inspector
Individual
Group 1 (characteristic A)
Systematic algorithmic selection
Research and assessment by inspector
Decision about individual
Group 2 (characteristic B)
Systematic random sampling?
Yes, possible selection
No
Systematically never selected

**Explanation:** In this example, the algorithmic selection model shows undesirable discrimination toward Group 1 (based on characteristic A). This group is systematically monitored, for example, in fraud detection, while Group 2 is never selected by the algorithm. While automation bias can be prevented by not informing inspectors that files to be reviewed have been selected by an algorithm, the risk of discrimination throughout the chain can only be mitigated by enriching files for inspectors with random samples that also include Group 2. This can reveal false negatives (files that should have been reviewed but were not selected by the algorithm). This is necessary to ensure the accuracy of the selection algorithm throughout its lifecycle and to manage the risk of discrimination.

**The AP considers three points of importance in this respect: (i) consider the decision-making chain as a whole, this is necessary; (ii) add random samples to the risk selection; and (iii) ensure that the risk selection can be explained and can be challenged.** The creation of a risk assessment of a person, for example during fraud investigation, can ultimately be traced back to a combination of algorithmic (pre)selection and the subsequent human oversight. Blind assessment of files by inspectors does not eliminate discrimination and bias at individual level that occurred in the preceding phase. By enriching the process as standard with a random sample, a basis for periodic audits is created at an overall level. These audits can then regularly check whether bias or discrimination occurs in the algorithm – and throughout the entire process (see Figure 1.6). This will allow bias and discrimination to eventually be mitigated. If inspectors have to do a blind assessment in the first instance, files based on a random sample should be added. Otherwise, inspectors will know in advance that every file has already been preselected based on the algorithm and thus assessed as ”high-risk”.

**Even in the case of blind assessment, inspectors must to be able to (i) check the algorithm and (ii) allow citizens to challenge the risk selection or have the selection explained to them.** Therefore, the inspector will require some insight into the outcomes of algorithmic risk selection. To be more specific: without this information, an inspector, when contacting a citizen, for example, cannot explain why a person has been selected for an investigation. It is important that inspectors, including the case of a blind assessment, are given a comprehensible and useful explanation of algorithmic risk selection at the right time. And the inspector must be sufficiently

AI-literate and competent to be able to assess how the algorithm arrives at its selection. The sequence in which data is presented to an inspector is important in this respect, as it can direct a follow-up decision.[47] This may ultimately lead to the tunnel vision and bias raised in the parliamentary motion. The AP recommends considering the "blind assessment" as the sequence in which information, especially the risk assessment of an algorithm, is shown to an inspector. In that case, blind assessment implies that inspectors only learn about the algorithm's risk assessment after they have formed their own.

### Box 1.2

## Case: Facebook's advertising algorithm discriminated in the case of job vacancies

**On 18 February 2025, the Netherlands Institute for Human Rights ruled that Facebook's recommendation algorithms discriminate on the basis of gender.**[48] The Institute is authorised to rule on violations of equal treatment legislation in the Netherlands. The foundations *Bureau Clara Wichmann* and *Global Witness* complained to the Institute about Facebook because research carried out by *Global Witness* had shown that vacancies with stereotypical male and female occupations were mainly shown to the corresponding group. For example, it was shown that a job advertisement for the position of receptionist was shown to female users in 96% of cases (2022) and 97% of cases (2023), while a job advertisement for mechanic was shown to male users in 96% of cases (2022 and 2023). As a result, the algorithm may promote stereotyping as it hinders women who want to become car mechanics, for example, in their search for a suitable job. The Institute finds the study sufficient to presume a suspicion of indirect discrimination.

**Facebook failed to rebut or justify the discriminatory and stereotyping effects of the algorithm.** Facebook has acknowledged the possibility that gender has been given more weighting in the advertising algorithm through the like and click behaviour of users of the platform. The Institute considers the lack of explanation for the research results of *Global Witness* the responsibility of Facebook. Facebook has also failed to produce an objective justification for the discriminatory distinction. The Institute believes that as a social media platform, Facebook has a duty to properly monitor the functioning of the algorithm and study the degree to which its advertising algorithm promotes stereotypes. Facebook has not been able or willing to demonstrate clearly, whether, and, if so, how Facebook specifically monitors and investigates this. The judgment is characteristic of recent court rulings where no explanation could be provided about the operation and impact of an algorithm, as in the SyRI case.[49] In the courtroom, inadequate transparency puts the party responsible for the algorithm at a disadvantage.

# 2. Policy and regulations

QUICKLY TO THIS SUBJECT

2.1 Transparency and explainability of algorithms →

2.2 International developments →

2.3 National developments →

2.4 Clarification and refinement of AI Act →

2.5 National developments AI Act →

Global developments in the area of algorithms and AI continue to call for action to ensure transparency and accountability. In addition, better policy and regulation remain necessary. This chapter sets out how the challenges, opportunities and risks of AI are being addressed in policy and supervision at global, European and national level. First, we consider the explanation on the transparency and explainability of algorithms provided by the Court of Justice. We then discuss the geopolitical challenges surrounding AI and how the United States, China and the European Union are dealing with them. Partly in the context of the AI Act, in Europe attention is being paid to the importance of innovation and the need for adequate protection of fundamental rights. This is specifically reflected in the development of guidelines, standards and the regulatory sandbox. Progress in recent months shows that the EU continues to take steps towards a more concrete framework for the responsible deployment of algorithms and AI in society. It is important to maintain this pace and accelerate it where possible.

## 2.1 Transparency and explainability of algorithms

**When the deployment of algorithms and AI leads to automated decision-making, people should be able to understand how the system arrived at that decision.** New European case law clarifies when information disclosure in automated decision-making meets the requirements of the GDPR. Those requirements relate to transparency in the deployment of algorithms and AI in decision-making processes about individuals. In February 2025, the Court of Justice of the European Union (CJEU) issued a preliminary ruling in a judgment concerning automated algorithmic assessment of credit standing (Case C-203/22, Dun & Bradstreet Austria GmbH).[50] The ruling concerns a case in which a telephone contract with a monthly charge of 10 euros was refused, due to the customer's insufficient credit standing. In this case, an Austrian court had previously concluded that Dun & Bradstreet had not provided meaningful information about the logic involved in refusing the credit. The new ruling creates more clarity on the circumstances in which meaningful information is sufficient.[51]

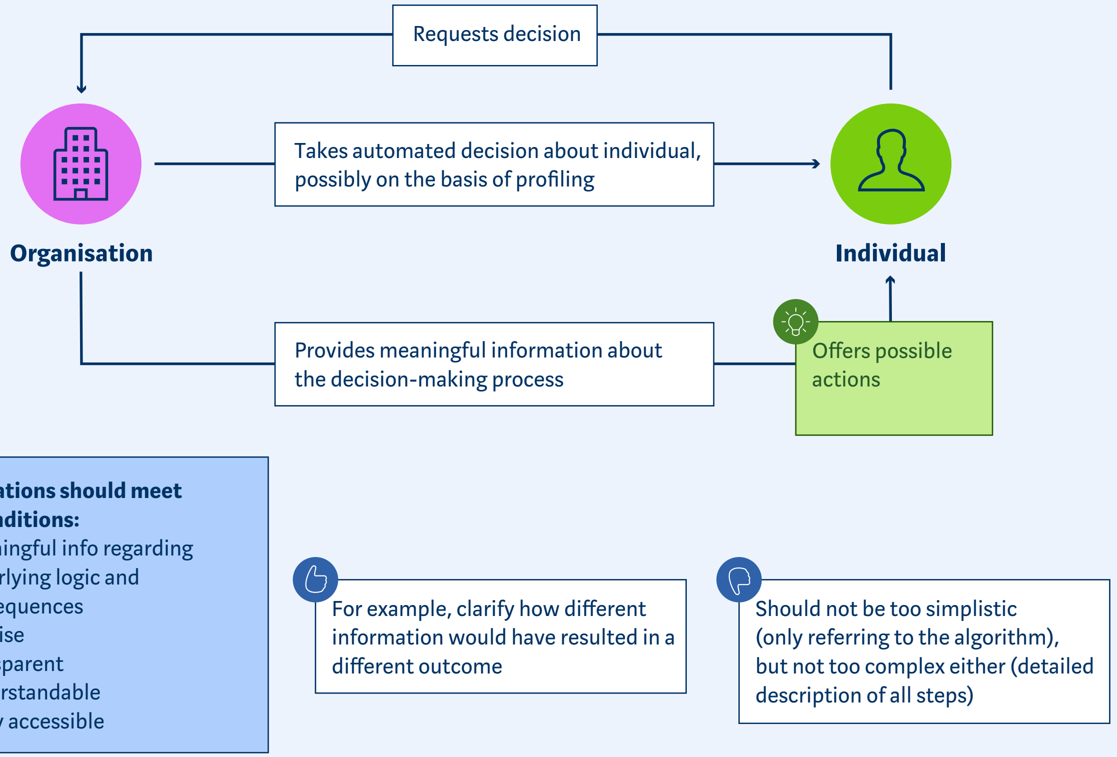
**Organisations deploying algorithms and AI in their automated decision-making should not over-complicate the explanation, but not over-simplify it either...** The Court emphasises that individuals are entitled to an explanation of the logic and data underlying the result. To make this information useful and, for example, to enable individuals to challenge the decision, information about the decision must be concise, transparent, understandable and easily accessible.[52] This requires customisation. One extreme is to merely communicate that an algorithm has been used, but this is insufficiently understandable. The other extreme is a detailed description of the entire algorithm, but this is insufficiently concise and in some cases cannot be done without sharing trade secret information.

**The golden mean depends on the specific situation.** A workable example might be that, in the case of automated rejection of an application, an individual is provided with an explanation of how specific adjustments to the data would affect the outcome of the decision. Such an explanation could be, for example, that if a person's gross monthly salary increases by €500, the credit application will be accepted. See Figure 2.1 for a schematic overview.

**Organisations deploying algorithms and AI in their automated decision-making should give proper attention to their explanations...** After all, to provide meaningful explanations of the system's decision-making process, the decision must be logically deducible from the functioning of the algorithm. This can be difficult with overly complex algorithms. The absence of such an explanation undermines the right to appeal or possibly correct the decision. It is thus insufficiently clear what the individual needs to change in order for the organisation to reach a different decision. Moreover, the person is unable to check whether the decision has been made carefully. The consequence of this explainability requirement is therefore that a developer of an algorithm or AI system must take into account the need for human autonomy from the outset. Individuals with respect to whom an algorithm or AI makes an automated decision must be provided with an explanation.

FIGURE 2.1 | INTERACTION PROFILING, DECISION-MAKING, AND INFORMATION PROVISION IN ALGORITHMS

**Providing meaningful information about algorithms enables individuals to take informed action regarding decisions made by governments and companies.**


Requests decision
Organisation
Takes automated decision about individual, possibly on the basis of profiling
Individual
Provides meaningful information about the decision-making process
Offers possible actions

**Explanations should meet five conditions:**

- Meaningful info regarding underlying logic and consequences
- Concise
- Transparent
- Understandable
- Easily accessible

For example, clarify how different information would have resulted in a different outcome

Should not be too simplistic (only referring to the algorithm), but not too complex either (detailed description of all steps)

**This explanation also provides a further elaboration in the context of the AI Act.** The Court's preliminary ruling clarifies the application of the right of access with respect to automated decision-making, as set out in the GDPR.[53] In addition, the AI Act provides for the right to an explanation in individual decision-making.[54] In short, this right means that individuals affected by a decision of a high-risk AI system should be provided with clear and relevant information. The explanation should cover the role of the AI system in the decision-making process and the main elements of the decision taken. This is very much related to the similar provision in the GDPR. As such, the Court's decision in the Dun & Bradstreet case also clarifies how AI developers and AI users should design and document their systems in order to comply with the explainability requirements in individual decision-making.[55] From a data protection supervisoryperspective, the AP is working on further explanations on meaningful disclosure this year.

## 2.2 International developments

**Internationally, the focus is on the geopolitical developments surrounding AI.** In the global AI race, the balance of power is shifting. Mainly the United States and China are competing for a leading role in developing an infrastructure around AI. The introduction of Deepseek – which has become available both as a chat service and an open source model – marks China's increased role in the global AI infrastructure. Rapid developments in AI are accompanied by increasing geopolitical issues. This is partly due to the profound impact of this technology on global power relations, economic structures and social processes.

**The US and China owe their leading roles to considerable investments in AI.** The AI Index Report 2025 published by the *Stanford Institute for Human-Centered AI* concludes, among other things, that the gap in the race for leadership between the US and China has significantly narrowed. While the US still leads in private investment and producing AI models, China has closed the gap through quality improvements. China also remains the leader in AI publications and issued patents.[56]

**Since the beginning of this year, the US has been publicly focusing on a new course of simplifying and deregulating AI. At the same time, the US is also developing specific regulations similar to the AI Act.**[57] For example, by means of an executive order aimed at removing barriers to AI innovation and maintaining US leadership.[58] This executive order replaces the previous executive order issued by the Biden administration, which emphasised preconditions for the deployment of safe and reliable AI within the federal government. Despite the emphasis on simplification of regulation and concerns about security and protection of individual rights, a recently announced memorandum contains safeguard provisions similar to those in the previous executive order. The memo *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust* announces obligations for ”high-impact AI”, including documentation, impact assessments, testing and human intervention options.[59] Interestingly, the definition of ”high-impact AI” bears similarities to the AI Act. For example, AI that serves as the basis for decisions affecting access to education, housing, insurance or employment is classified as high-risk.[60]

**China is working on a regulatory framework focusing on more specific standards.** For instance, from 1 September 2025, AI-generated content must be clearly recognisable as such to users. National AI standards are being developed and China is actively participating in the development of international standards.[61]

**World-wide, private investment in AI has increased significantly, up 44.5% between 2023 and 2024.** Apart from the US, the EU member states and China, other countries are also making substantial investments. In 2024, the UK invested US$4.52 billion, Canada US$2.89 billion and the United Arab Emirates US$1.77 billion.[62] This shows that many countries recognise the opportunities AI offers.

**Box 2.1**

### Legislation as a precondition for innovation

*Although regulation and innovation are often presented as opposites, there are also strong arguments for viewing legislation as the very driver of responsible innovation.*

- **First**, European legislation creates a level playing field and legal certainty. Companies know where they stand, irrespective of which member state they operate in. This prevents legal fragmentation and creates stronger incentives to roll out innovative products on a European scale.
- **Second**, legislation prevents companies from competing on aspects where minimum standards apply, such as privacy or security. This allows them to focus instead on innovating in areas where this is desirable. As such, legislation steers innovation in socially responsible and future-proof directions.
- **Third**, legislation increases citizens' trust in digital services. That trust supports the broad acceptance and use of new technologies

**Finally**, European legislation increasingly provides room for innovation. Good examples include the mandatory *regulatory sandboxes* in the AI Act. By enabling cooperation between supervisory authorities and developers, developers can innovate responsibly.

**The AP also sees a clear movement towards regulatory simplification in Europe.** The current legal framework in Europe places a strong emphasis on fundamental rights and public values, such as transparency. At the same time, concerns about the international capability of AI are also emerging in Europe, and there are questions about the complexity of the legal framework and the impact on Europe's competitiveness. These concerns further increased following the publication of the Draghi report in September 2024. This report warned that complex regulations put Europe's position at a disadvantage in comparison to the US and China.[63] Recently, 13 European member states signed a statement calling for more investment in AI, removing barriers and simplifying EU rules and procedures.[64] Amid these discussions, the European Commission recently announced a number of measures. One of these is the *AI Continent Action Plan*, which aims to make Europe a world leader in AI.

**The AI Continent Action Plan is mainly about promoting AI innovation in the EU.** This includes scaling up European AI infrastructure to enable research and innovation to train and fine-tune AI models. It also includes investments in ensuring high-quality data for AI innovations. Furthermore, the plan is committed to increasing AI skills and AI literacy.[65]

**European willingness to invest in AI is high.** This is evidenced by the European AI Continent Action Plan described above. In addition, the EU recently launched InvestAI, an EU initiative to unlock 200 billion euros for investment in AI. A 20 billion euro fund will finance future AI gigafactories, where complex, very large AI models will be trained. In the Netherlands, the government has announced that it will invest in an AI factory that is to become part of EuroHPC's European network of AI facilities.[66] The AI factory aims to be a one-stop shop for AI development by functioning as a knowledge centre, providing AI computing power and facilitating data storage.

**The call for regulatory simplification is resonating within the EU.** But there are also other voices... For example, experts stress that the European digital regulatory framework is actually designed to foster innovation and increase trust by managing potential risks. Others point out that investment in Europe is actually lagging due to the lack of private investment. This is due to, for example, weaknesses in the capital markets union and shortcomings in rules on state aid.[67]

**Box 2.2**

## Protecting platform workers' rights

**The European Platform Work Directive is an important step towards protecting platform workers whose work is guided by algorithms and AI.** For example, people who deliver food or provide transport of people through platforms. The Platform Work Directive was adopted at the end of 2024 and needs to be transposed into Dutch legislation in the period ahead. The directive clarifies the position, legal and otherwise, of platform workers and aims to improve working conditions. This will include additional rules on monitoring and algorithmic management of platform workers. It involves safeguarding task allocation and assessment of platform workers, including with respect to their safety. Furthermore, the directive aims to improve transparency on algorithmic management. For instance, works councils and trade unions must also be informed.

The rules in the directive are closely related to other regulations, digital and otherwise, such as the GDPR, the AI Act and the DSA. But the rules are also related to regulations on a healthy and safe working environment. The directive is an example of legislation that provides additional and specific safeguards in highly algorithmised areas.

## 2.3 National developments

*At the national level, the work of the State Secretary for Digitalisation stands out in the last six months, as do some adopted motions in the Dutch parliament. In addition, supervision of the Digital Services Act (DSA) will be effected.*

**For example, in April the government published its new position paper on the deployment of generative AI in government.**[68] The new position paper is less cautious and actually encourages the use of generative AI. The position paper is accompanied by a guideline to assist government organisations in deploying generative AI responsibly. They are also required to enter into agreements with suppliers and separate conditions apply. The AP expects governments to increase their deployment of generative AI as a result of this position paper. Although the AP believes that caution should be exercised, it also realises that the position paper and the guideline contain many good ingredients for deploying generative AI.

**However, the AP stresses that a number of preconditions for responsible deployment at the application level deserve more attention.** It mainly oversees the preconditions for using generative AI in practice. One example is ensuring adequate AI literacy. It is also of great importance to view generative AI in a broader context. If this does not happen, there is a risk that the deployment of generative AI will radically change existing processes (unintentionally). In the autumn 2023 report, we wrote about so-called algorithm distortion.[69]

**The AP is also contributing to the public debate to encourage the responsible use of generative AI.** To this end, the AP published a consultation version of its own vision on generative AI on 23 May. The AP discussed the vision with parties that develop, deploy and research generative AI. Besides facilitating debate, the AP outlines a desirable future perspective for the lawful and responsible deployment of generative AI.

**Also notable is that the completion of the internet consultation "Algorithmic decision-making and the General Administrative Law Act (Awb)" has been further delayed.**[70] This consultation ran until April 2024, and the AP indicated in an earlier report that it was looking forward to the follow-up. Especially in view of the continued digitalisation of government, it is important to involve the related system, legal and otherwise. This will ensure that the government's actions remain verifiable, explainable and fair.

**Finally, the government has been further developing a scientific standard for the deployment of models and algorithms.**[71] Based on work carried out by Leiden University, this standard is being further developed. The AP reiterates that the requirements in this respect should be considered in conjunction with the provisions of the AI Act. It is undesirable that similar requirements in different product standards and other standards could be interpreted differently.

**On 20 May the Duth parliament adopted a motion calling on the government to step up its efforts on algorithm registration.**[72] The motion specifically focuses on algorithms that may use risk profiling and automated selection tools. A previous request to publish such algorithms has not yet been fully implemented. This motion rightly seeks to change that.

**Box 2.3**

### Dutch supervision of the DSA in force

**The DSA has been in force since 17 February 2024.** The DSA guarantees the protection of fundamental rights in the online world. The act applies to providers of "intermediary services", such as hosting companies, social media, online marketplaces, accommodation platforms, online platforms and search engines. The rules aim to guarantee transparency and users' rights. The act also aims to combat online deception and illegal information.

**European supervision of the major platforms had already begun.** For example, in preliminary findings of an investigation, the European Commission previously stated that TikTok was in breach of the DSA.[73] Allegedly, the company failed to comply with the obligation to maintain an ad repository. TikTok will now be afforded the opportunity to respond, before a final decision is taken. In addition, the Commission is currently drafting guidelines on child protection. A first draft for public consultation has been published.[74] The guidelines contain a non-exhaustive list of measures for platforms to protect minors and comply with the DSA.

**In the Netherlands, the Netherlands Authority for Consumers and Markets (ACM) and the AP monitor the DSA as of 4 February 2025.** The Implementation Act stipulates that the ACM is designated as digital services coordinator and supervisory authority for much of the DSA. The AP supervises the rules on personal data. In addition, the AP supervises the rules on transparent recommender systems. This monitoring role has been assigned to the AP to ensure a broad citizen's perspective on recommender systems.[75]

## 2.4 Clarification and refinement of AI Act

*More than a year after the launch of the first sections of the AI Act, steps for the further clarification and refinement of the act are becoming apparent. Both the AI Office and the intended national supervisory authorities are working on initiatives to facilitate compliance with the act. This includes, among other things, guidelines, the Code of Practice on General Purpose AI and codes of conduct.*

### Guidelines

**The European Commission published the first guidelines on the AI Act in ...** The first two guidelines on (1) the prohibitions in the AI Act and (2) the definition of AI systems were published in February. Guidelines on other topics will follow in the years ahead.

**The AP finds that even with the guidelines, there is still considerable room for further refinement and framework-setting.** The guidelines will be published as a "*living document*", which the European Commission will keep current and can adapt where necessary. This is achieved, for example, on the basis of the experience of supervisory authorities, new case law or technological developments.

**In its guidelines on prohibited AI, the European Commission provides a broad interpretation of the responsibility of AI providers to prevent prohibited practices.**[76] AI providers should be able to properly assess the extent to which their AI system is used by the buyers of their product. Based on this assessment, they must build in safeguards to prevent prohibited use. For example, a provider of an emotion recognition system must ensure that it is not used in schools or workplaces. In addition, the European Commission provides a more specific interpretation of the prohibitions in the comprehensive guidelines, including examples.

**The AP finds that despite the guidelines, there remains considerable ambiguity regarding the definition of the term "AI-system".**[77] For example, it is not made sufficiently clear whether and how a system can consist of multiple components or processes. What is also not clear is whether a system's interface, for example, forms part of the "AI system". Ambiguity also arises about the required "inference capability" and examples of systems that are not covered by the definition. On the positive side, the European Commission does emphasise in the guidelines that the AI system definition covers both the development and deployment phase of the system. This brings the use of AI technology for simpler algorithms within the scope of the AI Act.

**More guidelines from the European Commission will follow shortly.** In any case, the AP expects additional guidance on the reporting obligation for serious incidents in high-risk AI systems this summer. In addition, the AI Act states that guidelines on classification rules for high-risk AI systems should be available by 2 February 2026. These aim not only to clarify the types of AI system that fall into this category, but also in which cases an exemption is applicable. See figure 2.2.

**FIGURE 2.2 | GUIDELINES**

**February 2025**

- Guidelines definition AI system
- Guidance on prohibited practices

**August 2025**

- Guidance on the reporting obligation of serious incidents in high-risk AI systems

**February 2026**

- Guidance on classification rules for high-risk AI systems

**Latest publication date unknown:**

- Guidance on the application of the essential requirements to high-risk AI systems and responsibilities in the AI value chain
- Guidance on the practical implementation of transparency obligations
- Guidance on the practical implementation of the provisions related to substantial change
- Guidance on the relationship of the AI Act with other European legislation

## Code of Practice on GPAI

**A refinement of the AI Act with very high impact is the code of practice for general purpose AI.** Compliance with the code of practice is a way for providers of *general purpose AI* to demonstrate compliance with the law. We wrote about this in more detail in the previous report.[78] Unfortunately, at the time of writing this report, the final version of the code of practice has not yet been published. However, since general purpose AI models must comply with the stricter rules under the AI Act as of August, the code of practice is expected shortly.

## Standards

**European standards for the practical implementation of requirements for high-risk AI systems have been delayed for the time being.** The deadline in the Commission's first standardisation request (*1 April 2025*) to the standardisation organisation JTC-21 has passed. Moreover, it is not yet clear when all standards will be provided. Given the current progress, the AP advises AI providers to start complying with the AI Act, based on the legislative text and, where possible, by applying *good practices*. It is important not to keep waiting for these standards. Meanwhile, it is up to policymakers and supervisory authorities to clarify what this means for AI Act compliance and monitoring, even before the requirements for the first high-risk AI systems come into force in August 2026.

## Other initiatives

**In addition to guidelines, codes of conduct, templates and standards, there are more initiatives to clarify the AI Act.** For example, the Commission started working on an AI Pact to help AI providers implement the Act. Several webinars that can be accessed by anyone have also been organised in recent months. The webinars provide participants with a better understanding of the AI Act and its implementation. The webinars are recorded.[79]

**The AI-Office is preparing the launch of an AI Act Service Desk.** The purpose of the service desk is to support businesses and governments in complying with the AI Act. A tender[80] for an external team that, under the direction of the AI-Office, will provide advice on questions of AI providers about the Act was open until 19 May. The service desk will be an interactive platform and as a central hub it will provide general information and support materials. It is not yet known when the service desk will launch.

**Furthermore, efforts are being made at both national and European level to implement the AI literacy obligation.** To this end, the AI Office is developing a code of conduct within the framework of the AI Pact. In addition, the European Commission recently published an FAQ. At the national level, the AP has published a call for input[81] to collect practical examples of AI literacy. Based on the responses, the AP is currently drafting a document containing examples of good practice. Dutch organisations can draw inspiration from this for their own AI literacy policies. The results of the survey were presented at the AP seminar on AI literacy on 18 June.

**Finally, the European public buyers community has published an updated version of the existing model contractual clauses.**[82] These have been drafted to support public buyers of AI systems. The update includes a model contract for high-risk AI procurement and is fully aligned with the final version of the AI Act. Moreover, provisions are adaptable to specific needs when procuring non-high-risk AI. It also contains an explanation for the implementation of the provisions. Model contracts can be helpful when procuring an AI system since it is important to have the procurement terms and conditions in place. For example, you need to understand what happens to the data processed by the AI system and how the rights to that data are governed.

## 2.5 National developments AI Act

**In March, the AP and the Dutch Authority for Digital Infrastructure (Rijksinspectie voor Digitale Infrastrutuur, RDI) published a joint proposal for the Dutch implementation of the regulatory sandbox.**[83] This proposal was drafted in collaboration with various supervisory authorities and ministries, and sets out the desired principles and process design of the sandbox. The aim of the proposal is to lay a solid foundation for further collaboration and coordination. The final sandbox will be launched no later than August 2026. They ran a pilot for the proposed process design with questions from various organisations about the AI Act. In addition, discussions were held with stakeholders from the Dutch AI ecosystem.

**The proposed process design describes how the Dutch sandbox can best contribute to legal certainty and innovation.** This requires the active participation of all relevant supervisory authorities under the AI Act. This will allow access to the sandbox through a one-stop shop. This prevents AI providers from having to find out for themselves which supervisory authority they should contact. Moreover, this approach contributes to consistent interpretation of laws and regulations by the various supervisory authorities. Finally, this approach allows for related regulations to be interpreted in context.

**The added value of the sandbox lies in supporting AI providers in complying with laws and regulations.** They do this, for example, through legal and technical advice on interpretation, testing or validation of the act. As supervisory authorities cannot meet all needs, the sandbox should align well with other initiatives, such as AI factories, Testing and Experimentation Facilities and EDIHs.

**Following the above proposal, the Dutch parliament adopted a motion on 20 May to develop the regulatory sandbox as a priority.** The motion calls on the government to ensure its availability by the first quarter of 2026 at the latest. The AP welcomes this call and is committed to launching a sandbox as soon as possible. The AP is collaborating with the departments to realise this.

**Box 2.4**

## AI, privacy and data governance: The OECD’s approach to trusted AI

*By: The OECD Directorate for Science, Technology and Innovation (STI)*

Artificial intelligence (AI) is rapidly transforming how societies use and share data, unlocking new opportunities for innovation but also raising critical questions about privacy, trust, and responsible data governance. The OECD is at the forefront of shaping international policy frameworks that ensure AI development and deployment respect human rights and democratic values. In 2019, the OECD established the world’s first intergovernmental standard on AI –the OECD AI Principles– which were updated in May 2024. Adopted by over 47 countries, including major economies and international partners, the AI Principles provide a blueprint for trustworthy, human-centric AI and guide national and international policy frameworks.

### Promoting Policy Tools to Advance Trustworthy AI

The OECD.AI Policy Observatory supports the implementation of the OECD AI Principles. It provides evidence-based insights, real-time data and policy tools to enhance transparency, facilitate international collaboration and support responsible AI innovation.

Key resources include the Global AI Initiatives Navigator (GAIIN), a live repository of over 1,300 AI policy initiatives from over 70 countries and intergovernmental organisations and interactive visualisations of global AI trends. The Policy Observatory includes practical resources such as the AI Incidents and Hazards Monitor (AIM) and the OECD Catalogue of tools and metrics for trustworthy AI, which provides a curated repository of tools and metrics to support developers and deployers in integrating robust and trustworthy practices throughout the AI system lifecycle. The AI Wonk blog further contributes to this work by offering a platform for experts to share insights on how to best shape trustworthy AI policies.

### Expert Engagement on Key Priority Issues

The OECD.AI and Global Partnership on AI (GPAI) expert community –comprising of experts from government, business, academia and civil society- supports the implementation of the OECD AI Principles and informs the work of the Policy Observatory through dedicated expert groups. These expert groups address key priority issues and provide a platform to discuss shared AI policy opportunities and challenges.

The expert groups on AI Incidents and on AI, Data, and Privacy focus on priority issues such as understanding the risks associated to the development and deployment of AI systems and examining how privacy and data governance contributes to trustworthy AI.

### Defining, Reporting and Monitoring AI Incidents

With the rapid use of AI systems associated risks have already started to materialise. Understanding these events and their implications has become a priority for policy makers. In February 2025, the OECD published a common reporting framework for AI incidents, offering a flexible structure for reporting and monitoring AI incidents. Developed with the Expert Group on AI Incidents, the framework outlines 29 criteria to describe and report an AI incident, drawing in part from the OECD Framework for the Classification of AI systems. Reporting and monitoring of AI incidents will enable policymakers, AI practitioners, and all stakeholders to identify high-risk systems across various contexts, gain insights into both current and emerging risks, and evaluate their impact on affected stakeholders.

In this context, the OECD launched the AI Incidents and Hazards Monitor (AIM) in November 2023. The AIM documents AI incidents and hazards to help stakeholders gain valuable insights into the risks and harms of AI systems. The AIM will facilitate the identification of AI risk patterns, including those related to privacy and data governance, at both global and regional levels and enhance the understanding of the multifaceted nature of harms arising from the development, use and malfunction of AI systems.

### Balancing Innovation, Privacy and Data Governance

AI relies on vast datasets –which may purposefully or inadvertently include personal data– to function effectively. This creates significant privacy risks, including potential misuse of personal data, algorithmic bias, and lack of transparency in how data is collected, processed, and shared. The OECD Privacy Guidelines, recognised as the global minimum standard since 1980 and updated in 2013, offer strong foundational principles for protecting privacy and data rights in the age of AI.

In 2024, the OECD established an Expert Group on AI, Data, and Privacy, to explore synergies and develop coordinated policy solutions across AI and privacy communities. This initiative is grounded in the recognition that these communities have traditionally operated separately, which can lead to fragmented approaches and regulatory gaps. A key output of this group has been the mapping of the OECD Privacy Guidelines to the OECD AI Principles, which is intended to help policymakers and practitioners balance the opportunities of AI-driven innovation with the need to embed privacy and data governance considerations throughout the AI lifecycle, from design to deployment.

Building on this foundation, the OECD is also examining the privacy and data governance implications of today's AI training dataset collection mechanisms. This includes practices such as data scraping, which raise complex issues at the intersection of intellectual property and privacy rights. The OECD report on intellectual property issues in AI trained on scraped data provides an overview of how data scraping for AI development intersects with various intellectual property rights. Future work of the OECD will also explore the privacy and data governance implications of other relevant data collection mechanisms used for building AI training datasets.

Access to high-quality data is critical for developing AI models, but access to such data must be balanced with robust protections. The OECD Recommendation on Enhancing Access to and Sharing of Data provides a framework for balancing data openness with legitimate protections, applying the principle of making data "as open as possible, as closed as necessary." The OECD report on Enhancing Access to and Sharing of Data in the Age of AI highlights how governments can enhance access to and sharing of data and certain AI models, while ensuring privacy and other rights and interests.

Complementing this work, the OECD actively promotes Privacy-Enhancing Technologies (PETs) as a key component of responsible AI and data governance strategies. When used appropriately, PETs such as federated learning, homomorphic encryption, or differential privacy can enable AI models to be trained and deployed without exposing personal data, supporting privacy by design across the AI lifecycle.

Together, these initiatives support a balanced approach to data governance, enabling innovation while preserving individual rights and reinforcing trust in AI.

Visit:
https://oecd.ai
https://oecd.ai/site/incidents
https://oecd.ai/site/data-privacy

# 3. AI and emotion recognition

QUICKLY TO THIS SUBJECT

3.1 Biometrics-based emotion recognition →
3.2 Dubious basic assumptions of emotion recognition →
3.3 Training and functioning of emotion recognition systems →
3.4 Risks of emotion recognition →

Emotions form an essential part of human existence. They play a defining role in our daily lives: from social interaction, to our perceptions, how we learn, what decisions we make and how. There are more and more AI systems that claim to be able to recognise emotions on the basis of biometrics. The market for applications of such systems has experienced steady growth in recent years.[84] [85] Yet the basic assumptions of the systems are shaky. Their functioning is therefore questionable. If the systems are used nonetheless, risks of infringement of fundamental rights and public values arise. It may for instance lead to discrimination, curtailment of human autonomy and privacy violations.

## 3.1 Biometrics-based emotion recognition

**Biometric data is increasingly used to identify people's emotions.** Biometric data relates to physical and behavioural characteristics of people. This data has been used for verification and identification of individuals for many years. Automatic analysis of biometrics and use of more data sources has facilitated the development of new applications.[86] There is now an increasing number of systems with the purpose of recognising emotions. These systems analyse biometric data and attempt to recognise emotions. This can form the basis for decisions, recommendations or other output. Biometric systems therefore no longer just look at *who you are*, but also at *how you are*.[87]

**As early as the 1970s, researchers who tried to identify emotions based on physical and physiological cues laid the foundation for emotion recognition systems.**[88] With the advent of computers, researchers developed algorithms that could analyse facial expressions and vocal sounds. The breakthrough came with the rise of *machine learning*, allowing AI to process vast amounts of data. This made systems more accessible and accurate. Since then, companies and other organisations have started to use this technology for various applications.[89]

**Several industries are currently considering the deployment of various emotion recognition systems, or already use them.** There are systems that attempt to determine the emotions a person is experiencing based on their facial expressions. There are also systems that measure and determine skin conductance, heart rate or vocal sounds. Various organisations use the technology for different purposes. For example, in marketing, customer service, recruitment, education, public safety and healthcare. The market for monitoring stress and preventing burnout is also growing rapidly. Emotion recognition can also be used without one realising it. Emotion recognition could for example be used in advertising and marketing, in order to evaluate and influence consumers' purchasing behaviour.

**The development and deployment of emotion recognition is growing because organisations and individuals believe it has added value.** Organisations use recognised emotions to improve products, services and health, or for safety purposes. Moreover, wearables have made personal use easier, for example to track stress. Companies also recognise the importance of emotion recognition for improving interaction with customers. Chapter 4 discusses several examples of emotion recognition systems. Several scientific articles mention the potential benefits of emotion recognition systems. For example, scientists describe how systems can improve healthcare by providing more insight into patients' emotions. This could make anticipating patients' needs easier and reduce the burden of care. Furthermore, emotion recognition is being used to support individuals with autism in social interactions. Both research into emotion recognition and the market for the systems have grown.

**At the same time, experts question the basis of emotion recognition systems and warn of risks of infringement of fundamental rights and public values.** During deployment and development, risks of violation of fundamental rights and public values, such as privacy, human dignity and non-discrimination, arise. There are also doubts about two controversial assumptions underpinning the systems: measurability and universality.

**Box 3.1**

### What do we mean by “emotion recognition system”?

**This chapter is about biometric emotion recognition systems.** These are AI systems, the purpose of which is to recognise emotions using biometrics. Examples of such data include heart rate, vocal sounds, but also posture, odour and DNA. Box 4.1 describes when the term ”biometric data” applies. Science refers to the types of systems discussed in this chapter in different ways. This is because there are different disciplines that study emotions. In technical literature, the systems fall under ”affective computing”. This chapter does not discuss sentiment analysis, which concerns AI systems that infer emotions from text. In scientific literature, however, this type of system often is included under emotion recognition systems.[90]

**The term ”emotion recognition system” is also referred to in the AI Act[91], but this thematic report goes beyond the AI Act.** The chapter covers all systems that attempt to recognise emotions on the basis of biometrics. This report also describes various risks of infringement of fundamental rights and public values. As such, it describes an overarching picture of the systems and their risks.

**The chapter also discusses stress.** Stress is often described as an emotional state, rather than an emotion such as joy, sadness or shame. However, stress is often used as an indicator of certain emotions, thereby making it relevant to emotion recognition research.

**Using the term ”emotion recognition” does not mean that these systems are actually able to recognise emotions.** This chapter also discusses the serious doubts about the functioning of these systems and their ability to recognise emotions.

## 3.2 Dubious basic assumptions of emotion recognition

**A first basic assumption is that emotion recognition systems use the same categorisations or models of emotions for everyone.** The assumption that the same categorisations or models apply to everyone is highly controversial. The basis of the assumption is that there are natural emotions that everyone experiences and expresses in the same manner. This is also referred to as the ”universality hypothesis”. Often, emotion recognition systems are trained based on Western ideas about emotion, which may not necessarily apply to everyone.[92] In reality, emotions are often complex and context-dependent.[93] For example, culture strongly affects how emotions are experienced, expressed and named. Although context is important, this does not necessarily mean that people do not share any common emotional denominators.[94]

**To design emotion recognition systems, it must also be assumed that emotions can be identified using general and measurable signals.** This is another controversial assumption. It is assumed that there are general (physical and physiological) signals that indicate the presence of certain emotions. For instance, a smile as an expression of happiness or a high heart rate as an indication of anxiety. Developers use the relationship between a measurable signal and the emotion. In other words, the signal is a ”proxy” of the emotion. The idea that a proxy provides enough information to assign one specific emotion to it, is controversial.[95] It can be a signal of more than one emotion.[96] For instance, a high heart rate is not always a sign of fear and a loud voice is not always an expression of anger. They can also be indications of more positive emotions. This makes emotion recognition not sufficiently reliable, specific and not universally applicable.[97]

## 3.3 Training and functioning of emotion recognition systems

**The two controversial assumptions are reflected in the training and functioning of AI systems.** The training and functioning of many different emotion recognition systems are roughly the same. Figure 3.1 illustrates the steps of these systems. This is a simplification of how many emotion recognition systems work.

**There are different types of data or ”modalities” that can be used for emotion recognition.** There are systems that identify emotions based on voice analysis. For example, speaking quickly and loudly may indicate anger or aggression. Other systems use facial analysis: emotions are recognised in the position of the corners of the mouth, eyes and eyebrows. Other modalities include heart rate, perspiration, brain activity, DNA and odour. Apart from systems that use one modality, there are also multi-modal systems. These systems combine different types of biometric data. For instance, gestures combined with heart rate.[98]

**The AI system first measures the data that will be used to recognise emotions.** This can be done in several ways. Cameras and microphones can capture vocal sounds, facial expression and posture, among other things. These are well-known and widely used applications of measurement systems. There are also wearables that measure heart rate and even brain activity. For example, smartwatches, smart rings and headphones. These are becoming cheaper and smaller, making them more accessible to everyone. Wearables are worn on the body. There are also measurement systems that measure remotely, such as cameras with facial recognition.

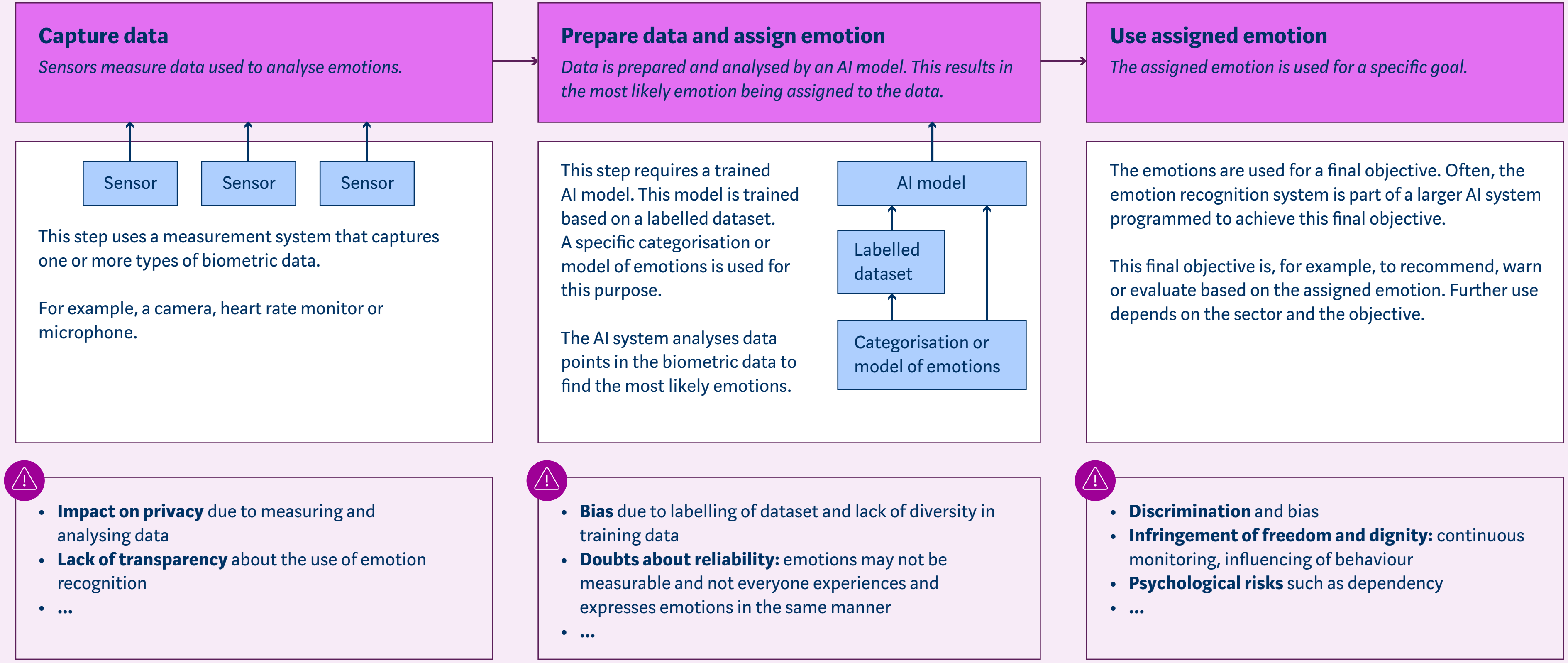
**The measured data is first prepared for use in the emotion recognition system.** In the preparation phase, a photo is cropped, for example, or noise is removed from a voice recording. Next, the system selects only certain features (data points), such as facial expressions in a photo. These features are converted so that they can be used by the AI system. For example, by using a code for a raised eyebrow.[99] Only an abstraction of the data, the code, is used further by the AI system. Preparation and conversion of data is often also carried out by an AI model. In that case, an emotion recognition system actually comprises several AI models.

**The AI model analyses the input and assigns the most likely emotion(s) to it based on a specific categorisation or model of emotions.** There are several categorisations and models. Many developers of emotion recognition systems use a version of six basic emotions: fear, anger, sadness, disgust, happiness and surprise.[100] Sometimes shame, guilt, pride, compassion, relief, hope and love are added. This basic categorisation is widely used in AI systems as it is easy to translate into an algorithm.[101] Emotions can also be further classified along two axes.[102] The first dimension shows whether something is perceived as positive or negative (”valence”). The second dimension is the degree of arousal (”arousal”).[103] An example of a positive emotion with neutral arousal is happiness. And a negative emotion with low arousal is boredom.

**The AI model is trained using data that has been assigned emotion ”labels”.** The way these labels are created varies from system to system. For example, if the model uses facial expressions, the training data consists of pictures with an emotion label. Labels can be created in different ways. A test subject can say which emotion they are experiencing, or someone else can attribute the emotion label to the data.[104] The data can be gathered ”in the field” or in the lab. In the lab, emotions are sometimes provoked, for example by showing certain images to test subjects. Someone may also have been asked to imitate an emotion. This is not necessarily the emotion someone is actually experiencing. The ways in which data is gathered and labelled determines what the system learns to predict.

**Ultimately, the assigned emotions are used for a specific final objective.** An emotion recognition system is often part of a larger AI system. The recognised emotions are used by the larger AI system for a specific purpose, for example to provide recommendations, evaluations or warnings. This sometimes requires even more contextual data. Other times, assigning an emotion is the main objective. For example, in an app that tracks emotions or emotional states such as stress and merely displays this. Chapter 4 discusses different applications of emotion recognition systems in practice.

FIGURE 3.1 | SIMPLIFIED FUNCTIONING OF EMOTION RECOGNITION SYSTEMS IN THREE STEPS



**Capture data**

*Sensors measure data used to analyse emotions.*

This step uses a measurement system that captures one or more types of biometric data.

For example, a camera, heart rate monitor or microphone.

⚠

- **Impact on privacy** due to measuring and analysing data
- **Lack of transparency** about the use of emotion recognition
- ...

**Prepare data and assign emotion**

*Data is prepared and analysed by an AI model. This results in the most likely emotion being assigned to the data.*

This step requires a trained AI model. This model is trained based on a labelled dataset. A specific categorisation or model of emotions is used for this purpose.

The AI system analyses data points in the biometric data to find the most likely emotions.

⚠

- **Bias** due to labelling of dataset and lack of diversity in training data
- **Doubts about reliability:** emotions may not be measurable and not everyone experiences and expresses emotions in the same manner
- ...

**Use assigned emotion**

*The assigned emotion is used for a specific goal.*

The emotions are used for a final objective. Often, the emotion recognition system is part of a larger AI system programmed to achieve this final objective.

This final objective is, for example, to recommend, warn or evaluate based on the assigned emotion. Further use depends on the sector and the objective.

⚠

- **Discrimination** and bias
- **Infringement of freedom and dignity:** continuous monitoring, influencing of behaviour
- **Psychological risks** such as dependency
- ...

Box 3.2

## Emotion recognition by narrow-AI versus general purpose AI

**The development and functioning of emotion recognition systems explained in this chapter relate to emotion recognition systems made explicitly for this purpose.** These systems are also called narrow-AI. They are developed for specific tasks in defined domains. In addition, they make use of pre-selected categorisations or models of emotions. As a result, they can only identify emotions they have been trained for.[105]

**General purpose AI systems are on the rise as well, and can also perform emotion analysis, even without explicit training.**[106] These systems are not specifically developed to recognise emotions. Analysing emotions is an additional skill of the model. Where a narrow-AI system can only recognise emotions for which it has been trained, a general purpose AI system is not restrained to one specific categorisation or model of emotions. Moreover, they can be applied for tasks in different domains.

**However, it is less clear how the general purpose AI systems generate their outcomes.**[107] The analyses are not the result of specific training, but arise from pattern recognition in large and diverse datasets. Currently, it mainly concerns systems that can analyse emotions in text (sentiment analysis). In the past five years, an increasing number of systems that can analyse pictures and sound have come onto the market. Systems can also perform emotion analysis based on these modalities.

**Research on emotion recognition in text shows possibly inconsistent results of the systems, for example because the large datasets contain many different types of data.**[108] When used, these systems could produce misleading results and show bias in the outcomes. Moreover, potential inconsistencies are difficult to gauge, making the resulting bias difficult to measure systematically. It is more difficult to detect or address such bias for general AI systems than for narrow-AI. This is because the training dataset is larger and not specifically focused on emotions. The training of the model does not specifically target this either. After all, it is not the main purpose of the system. Safeguards will therefore particularly focus on prompts and benchmarks on outcomes, which are regularly bypassed. Underlying bias in datasets, however, is not addressed.

**General purpose AI systems often describe outcomes convincingly, even if they are incorrect, incomplete or otherwise misleading.** For example, the answer will be a written explanation of the recognised emotion, while this analysis may be wrong. The explanation may cause people to assign more value to the outcome and they may be more likely to think that the model has given an accurate prediction.[109]

**The trade-off between control on the one hand and average quality on the other hand will become increasingly important in emotion recognition.** The average quality of emotion recognition in future systems based on general AI is expected to be higher than in narrow-AI systems.[110] However, the aforementioned drawbacks of inconsistency, lack of explainability, verifiability and excessive persuasion remain.

**The next chapter briefly discusses emotion analysis by some large language models.** To this end, the AP conducted exploratory tests on four such AI systems.

## 3.4 Risks of emotion recognition

**Deployment of emotion recognition systems and the use of their outcomes give rise to risks of infringement of public values and harms to fundamental rights of citizens.** These risks may arise during the different described steps of the AI systems. Development also contributes to the occurrence of these risks.

**The AI systems can have discriminatory effects due to bias in the labels of training data.** Often, humans carry out the labelling of training data for AI systems that are intended to recognise emotions. These labels are the emotions the system eventually learns to recognise. Bias of the labellers may be passed on to the training data and become part of the AI system as a result. Bias then also plays a part in the assigning of emotions by the system. Therefore, it is not only important what the system learns, but also from whom.[111]

**The systems can also cause discrimination if the training data is not sufficiently representative.** The model is less capable to select appropriate features and attribute emotions to a group that appears less frequently in the dataset. Datasets are often insufficiently diverse in terms of culture, skin colour, age and gender.[112] Studies have shown, for example, that biometric systems do not work equally well for all skin colours. Sometimes they even assign more negative feelings to black people.[113] Data on children and the elderly is also often lacking, even though emotions and expressions thereof differ between age groups. Finally, neurodivergent individuals, such as those with autism[114], and people with health problems may deviate from training data.[115] Because of this, the use of emotion recognition could for instance result in an individual being wrongly given a poor evaluation at work, or them being deemed unsuitable during a job interview.

**Emotion recognition systems can make suggestions or specific recommendations based on their analysis.** This can restrict individuals' freedom of choice and autonomy. Recommendations based on assigned emotions can influence people's behaviour consciously or unconsciously. For example, when buying behaviour is influenced on the basis of identified emotions. This could affect freedom of choice. Especially if this is done in a manipulative or deceptive way, it violates fundamental rights.

**The constant monitoring of emotions by such systems may also constitute a violation of human dignity.**[116] If the deployment of the systems is disclosed, constant monitoring of emotions may be perceived as annoying and intimate surveillance. This can happen, for example, in the workplace or at education institutions, and in public and semi-public spaces. People may become more stressed as a result, or feel pressure not to express emotions or even hide them.[117] Even if the deployment of such systems is not disclosed, it can undermine human dignity by reducing people and their emotions to simplistic measurements of a system.

**Personal use of emotion recognition systems is also becoming more accessible.** It is important that users are aware of the risks. Wearables make it easier for people to track their emotions and emotional states such as stress. Apps also provide tips on reducing stress and improving wellbeing. This may assign an important role to systems in how people experience their emotions. This can cause dependency and excessive self-monitoring.[118] People may also start doubting their own judgments. The AI system can stand in between users and their personal experience of emotions. As a result, people may understand or control their own emotions less independently. Provided the user is aware of any limitations, such technology could also offer opportunities and insights into emotional wellbeing and health.[119]

**The use of biometrics by emotion recognition systems presents risks with respect to data protection and privacy.** Emotion recognition systems use personal data, such as photographs, to analyse emotions. Recognised emotions are very intimate information and thus privacy-sensitive.[120] It is therefore important that people know which data is used by emotion recognition systems, as well as which emotions are analysed.

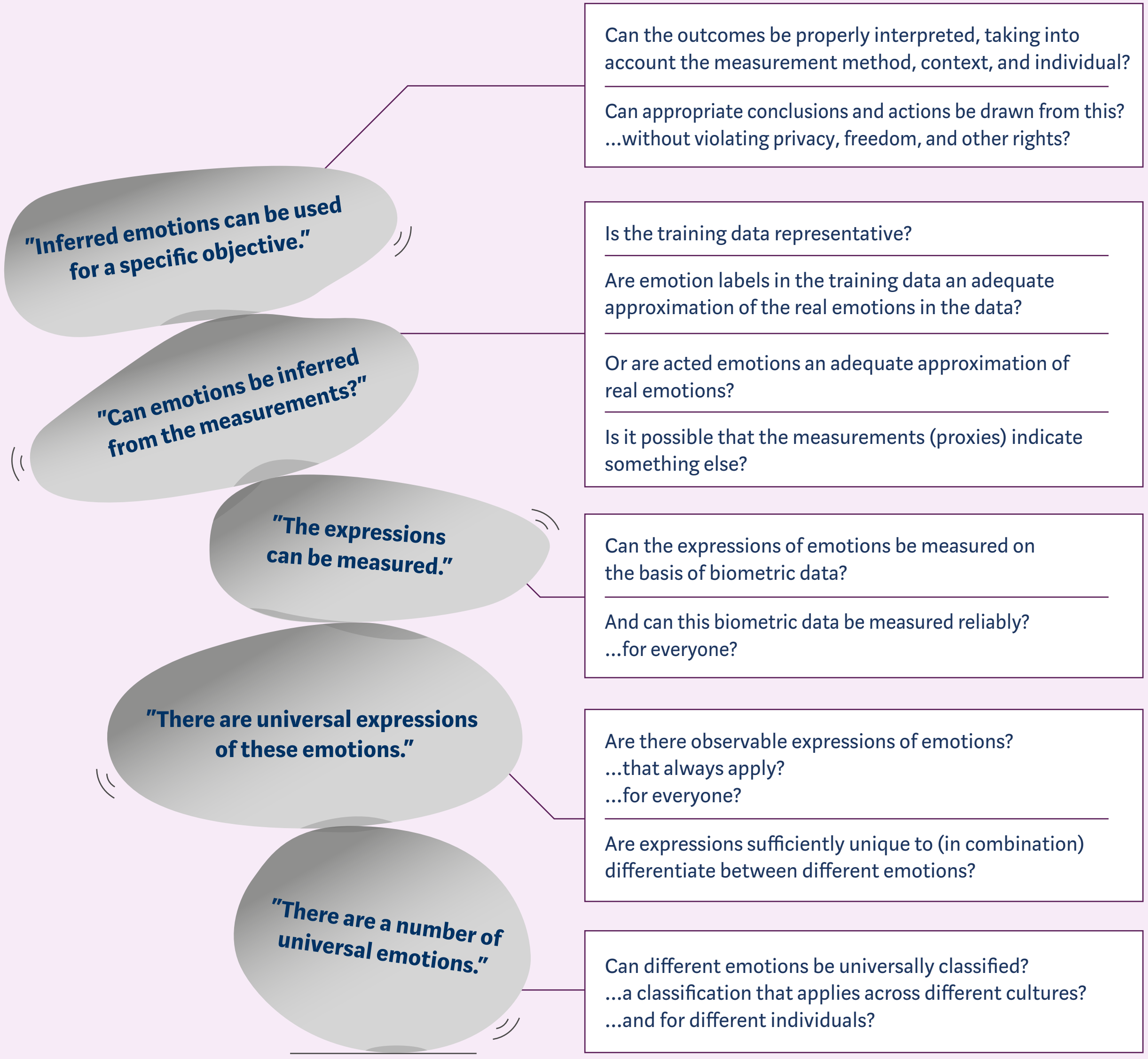
**In some cases, imbalanced power relations can make it difficult for people to refuse emotion recognition.** For example, emotion recognition in the areas of workplace or education institutions. Here, imbalance power relations exist. As a result, it is not always easy for employees and pupils to refuse the deployment of emotion recognition. Partly because of this, deployment of emotion recognition based on biometrics in education institutions and the workplace is prohibited under the AI Act since 2 February 2025.[121] This is also related to the questionable scientific basis of such systems. Refusing deployment may also be difficult in other application areas, such as healthcare, public spaces or certain marketing contexts.

**It is therefore important that there is transparency about the functioning and deployment of such systems, allowing people to make informed decisions.** People often do not choose to use the systems themselves. In addition to the aforementioned power relations, there can also be information asymmetries present. Organisations that deploy emotion recognition systems know more than the people whose emotions are recognised. For example, they are not aware whether emotions are tracked in the background. Recognising emotions is not always the final objective. An individual receiving advice may consequently not immediately be aware that their emotions were used to come to this advice. It is therefore important to be transparent about the use of emotion recognition.

**Emotion recognition systems are on the rise because of perceived benefits.** At the same time, these systems raise fundamental questions about reliability, measurability and risks to fundamental rights. The theories underlying emotion recognition systems, in combination with their technical functioning, deployment and use, form a shaky construction of assumptions. This is illustrated in Figure 3.2. The assumptions about emotions may be controversial, but are nevertheless used in the systems. During development, bias can occur. The use of the systems also bring forward various risks. It is for these reasons that this technology should be used very cautiously. The next chapter explores some application areas in more detail. It discusses other risks, specific practical examples, as well as the potential opportunities of emotion recognition.

**FIGURE 3.2 | BUILDING BLOCKS FOR EMOTION RECOGNITION SYSTEMS**

**The functioning of AI for emotion recognition presupposes a foundation of shaky assumptions in five areas.**


"Inferred emotions can be used for a specific objective."
"Can emotions be inferred from the measurements?"
"The expressions can be measured."
"There are universal expressions of these emotions."
"There are a number of universal emotions."

Can the outcomes be properly interpreted, taking into account the measurement method, context, and individual?

Can appropriate conclusions and actions be drawn from this? ...without violating privacy, freedom, and other rights?

Is the training data representative?

Are emotion labels in the training data an adequate approximation of the real emotions in the data?

Or are acted emotions an adequate approximation of real emotions?

Is it possible that the measurements (proxies) indicate something else?

Can the expressions of emotions be measured on the basis of biometric data?

And can this biometric data be measured reliably? ...for everyone?

Are there observable expressions of emotions? ...that always apply? ...for everyone?

Are expressions sufficiently unique to (in combination) differentiate between different emotions?

Can different emotions be universally classified? ...a classification that applies across different cultures? ...and for different individuals?

# 4. Emotion recognition in practice

QUICKLY TO THIS SUBJECT

Case study 1: Wearables →

Case study 2: Language models →

Case study 3: Customer service →

Where does one encounter emotion recognition? The AP has looked into three areas of application: **wearables**, **language models and use in customer service**. This shows that it is not always clear how emotions and stress are identified. Furthermore, emotion recognition is not always effective. And although AI is regularly used, often this is not obvious to the individual being analysed. Technological advances are visible. Devices are getting smaller and algorithms and AI are evolving. Organisations and individuals see opportunities and foresee increases in future use. In practice, a risk-aware way forward is of importance, considering the risks and the controversial theoretical basis of emotion recognition. The challenge for supervisory authorities and policy makers is to assess whether the use of emotion recognition is desirable in various domains. These include domains such as public space, marketing, healthcare, provision of services and customer contact.

**The various applications of emotion recognition are assumed to offer opportunities, but there are also risks.** Figure 4.1 provides an overview of some commonly discussed application domains. It shows opportunities, examples, and risks that are mentioned in literature. This clarifies how these systems are considered and viewed. The overview provides an insight into various areas of application, but is not exhaustive.

**The AP looked at three case studies in detail to gain insight into emotion recognition in practice.** The AP tested a number of systems in two application areas: personal health and generative language models.
In addition, a survey was carried out to gain insight into the use of emotion recognition systems within customer service organisations in the Netherlands. This chapter further explains these three areas of application.

**An overall observation is that the deployment of emotion recognition in practice entails sector- and domain-specific concerns.** That the deployment of emotion recognition systems in various domains can be regarded as high-risk is reflected in the AI Act. For use in the workplace and education, it has even been explicitly established that the risks are so high that emotion recognition is prohibited under the AI Act. In all other cases, emotion recognition based on biometrics is deemed a high-risk system under the AI Act.

**In addition to supervising high-risk systems under the AI Act, it is important for supervisory authorities and policymakers to consider whether deployment of emotion recognition is desirable, even where it is not prohibited.** The primary objective of controlling high-risk systems under the AI Act is to ensure that these systems are safe and meet product requirements. However, whether deployment of these systems is desirable is a different issue. It is ultimately a political consideration to determine to what extent these systems are desirable and for what purpose these systems should be used.
An analogy may clarify this: product regulation helps to ensure that fireworks offered on the Dutch market are safe. The question of where and under what circumstances fireworks may be set off, however, involves different considerations. A similar distinction between regulation and supervision of the product on the one hand, and the use of that product on the other hand, also applies to emotion recognition.

**Providers and deployers must be aware of the risks associated with each specific application area.** Responsible deployment of systems requires safety and transparency. Transparency, about the analysis and how it is carried out, towards the individuals whose emotions are subject to analysis. Furthermore, obtaining consent from the individuals being analysed is an important first step towards responsible use of the systems by organisations. This chapter discusses three practical examples of emotion recognition. However, working towards responsible, conscious and transparent use is also important in all other areas of application.

FIGURE 4.1 | OVERVIEW OF APPLICATION DOMAINS FOR EMOTION RECOGNITION

**Emotion recognition in practice: opportunities and risks in different application domains.**

## Education

Customise and personalise teaching methods based on pupils' emotions and emotional states. Predict performance and improve individual wellbeing. Assist vulnerable pupils.

Privacy and data protection risks.
Risk of constant surveillance and inequal opportunities. Possible reduction in independent emotional skills and teacher-student connection.

**Example:** Wearables to provide pupils with social support and to improve their wellbeing.

**Example:** Analysis of faces for optimisation of learning experience and performance.

## In the workplace

Improve employees' emotional wellbeing through (early) recognition of burnout and stress monitoring. Optimise work distribution. In case of physical work, used for safety, such as monitoring fatigue and concentration.

Risks to privacy, possible discrimination and inequality of opportunity. Risk of constant surveillance, which can increase stress, pressure to perform, self-censorship and reduce wellbeing.

**Example:** Cameras to monitor an employees work performance.

**Example:** Analysis of video calls with employees for insight into work experience and wellbeing.

**Prohibited under the AI Act**

## Safety of public spaces

Early recognition of emotions, intentions and emotional states in public and semi-public spaces. Thus allowing for quick, efficient and preventive action. Analysing emotion patterns to better shape policy, police deployment and crowd management. Border control support.

Impact on freedom of expression, right to protest, and right to freedom of movement. Analyses may result in wrongful arrests and checks. Risk of unequal treatment and discrimination.

**Example:** Cameras identifying suspicious and deceptive behaviour at airports.

**Example:** Lie detection systems deployed at border controls.

## Marketing

Gain insight into purchasing behaviour by analysing emotions and emotional states of consumers. Using this to optimise and personalise advertising and shopping experiences.

Risks of manipulation and behavioural influence, in particular for vulnerable consumers. Deployment may not be transparent and may affect freedom of choice and human dignity.

**Example:** Customise advertising signs based on emotions of passers-by.

**Example:** Cameras in shops to present customers with more personalised recommendations.

## Healthcare

Improve the quality of care by identifying symptoms and pathologies (faster and earlier) including preventative measures. Assistance in recognising emotions in patients with impaired communication skills.

Risks of possible discrimination affecting diagnoses and treatment. Transparency risks because care decisions may not be sufficiently explainable. Risks to human dignity.

**Example:** Wearables that detect agitation, stress, and confusion and emotion in patients.

**Example:** Wearables that can display emotions of others.

The AP examined three areas of application in more detail. These are further detailed in the remainder of this chapter.

## Personal health

Technology provides quantified insight into health and emotional wellbeing. Wearables measure emotional states such as stress, and make recommendations, for example, to reduce stress and prevent worse conditions.

Measuring stress has limited reliability.
People can develop dependency.
Moreover, the data is highly privacy-sensitive.

See page 42.

## Customer service

Improve customer satisfaction, service and customer contact by recognising customer's emotions. It also provides support to employees.

Risks of privacy and data protection breaches, lack of transparency towards customers.

See page 45.

## Language models

Recognising emotions should make interaction between humans and AI more natural. This will enable the system to provide better, more personalised and more empathic answers.

Risks of bias, manipulation and privacy violations. It is not entirely clear how such AI systems recognise emotions.

See page 43.

## Case study 1: Wearables

**Wearables have been very popular for some time and offer more and more options.** They are devices you can wear, for example on your wrist. Using various sensors, they measure variables such as movement, heart rate, temperature and sleep. Algorithms can provide insights into patterns and make recommendations.

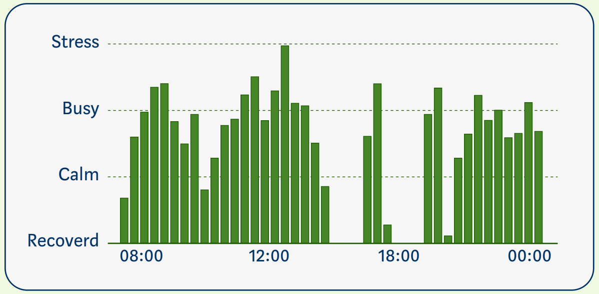
**To gain insight into these functions, the AP examined three wearables that measure stress.** The test was carried out with a watch, a ring and a fitness activity tracker. These are products available on the Dutch consumer market. All wearables display stress scores and make suggestions to reduce stress. Linked apps provide exercises for this goal. The apps also provide insight into causes of stress, such as insufficient sleep and exercise.

**How exactly wearables calculate stress scores is not entirely clear and the underlying data is not always visible.** How the different indicators are used in combination to detect stress is not clear either. Sometimes, the variables are specified, but the relationships between the variables are not. It is also not always possible to view individual variables.

**All devices use heart rate variability as an indicator of stress, but this is not always reliable.** Heart rate variability is the time between heartbeats. It is strongly related to exercise. Apps therefore sometimes display no score during exercise. Or they show a very high stress score. This high stress score could therefore also indicate exercise.

**The way scores and analyses are presented gives the impression that the stress scores are reliable and objective.** An app displays stress in easy-to-understand diagrams with categories and clear scores. This makes it seem reliable. It also appears objective, while the subjective side of stress is also very important.

**FIGURE 4.2 | SIMPLIFIED REPRESENTATION OF HOW A WEARABLE SHOWS EMOTION MONITORING IN APP**



**Description:** The app states: "You were stressed for 3 hours, so it was a stressful day."

**Insights, notifications, advice and various other features attract a lot of attention to the apps.** This draws users to the apps several times a day. Sometimes stress scores are displayed several times an hour. The apps provide notifications with recommendations. For example to do the exercises available in the apps.

**In addition, new functions are added to existing devices regularly, even though it does not measure new types of data.** These are new analyses based on the same input. The algorithms combine inputs in new ways. The hardware remains the same, the software changes. They also offer functions such as chats and exercises, which are not related to the measurements.

**The different features are part of the revenue model of the wearables.** All tested devices offer subscriptions. Not all features are available without a subscription. Or the app provides scores, but not comprehensive analyses. Often, the user has to pay for analyses and exercises for improving health.

**If the user interacts with the wearables consciously, the devices can provide useful insights in the long term.** Over time, the device gets to know the user better. This allows it to provide more accurate scores. The user also gets to know the device better. This allows the individual to better understand what is being measured, but also flaws of the devices, and how the user can interpret the scores.

## Case study 2: Language models

**Emotion recognition can make interactions with language models more personal.** Answers better match user emotions. This allows a chatbot, for example, to better respond to emotions.

**In addition to text, speech and photo options were added to several language models in the past year.** This allows you to have a live conversation with the language model. You can also upload pictures of yourself or your surroundings.

**The AP conducted an exploratory test with four language models to look at emotion recognition in images and sound.** In spoken conversations, the same texts were recited in different ways. Furthermore, photos with different postures and acted facial expressions were provided as input. Each time, the systems were asked which emotions it recognised.

**The different models appear to convert sound into text and analyse it.** One model indicated that it could also analyse changes in pitch, loudness and speed. However, this was not evident from the model's responses. It seemed to rely mainly on message content. The three remaining language models indicated they could analyse text only, or to convert spoken words immediately into text and analyse this.

**Three of the four models were moderately able to attribute "acted" emotions to pictures of faces.** Their responses mainly referred to eyes, mouth, eyebrows and facial tension. Based on this, they suggested several possible emotions. Figure 4.3 shows an example of this.

**The models were also able to analyse postures, but could only assign emotions to these in a limited manner.** They were able to identify the posture, and three models also linked it to a meaning. A pose with arms above one's head can be interpreted as "enthusiastic" or "triumphant", but can also be "a request for help". The interpretation depended very much on the facial expression identified in the same picture.

**The applications put together a convincing narrative based on the input.** This included description of surroundings, clothing and accessories. For example, one model noted that the photos had been taken in an office. Partly because of this, the model concluded that the emotions may have been acted out. An example of such a story is shown in Figure 4.3.

**How emotions are assigned remains largely unclear.** In their responses, the models refer to the different features they use. But how they use them is not entirely clear. For example, the models state that they "study" the features, "interpret" or "analyse patterns in visual data".

**TABLE 4.1 | MODALITIES USED BY AI LANGUAGE MODELS TO RECOGNISE EMOTIONS***

| Modality | Language model 1 | Language model 2 | Language model 3 | Language model 4 |
|---|---|---|---|---|
| Voice (audio) | Not recognised/ unknown | Not recognised | Not recognised | Not recognised |
| Face (photo) | recognised | recognised | recognised | Not recognised |
| Posture (photo)** | recognised | recognised | recognised | Not recognised |

* During field test implementation (April-May 2025)

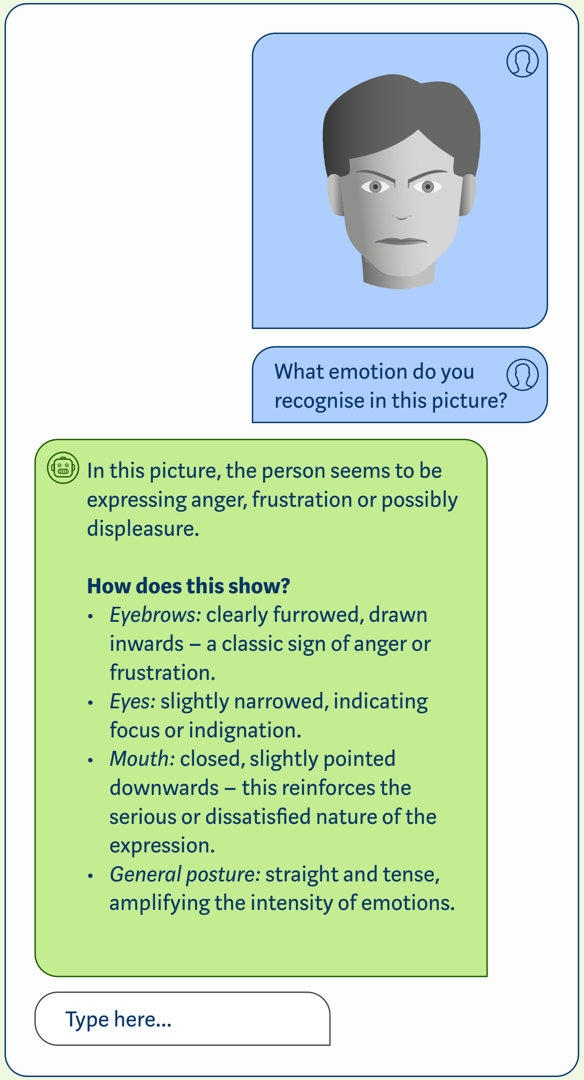
** All models were able to analyse posture to some extent. Three were able to relate it to emotion, but face still seemed to be main input for this.

**Two models refer to controversial theories about emotion, which are apparently present in the training data.** We already mentioned these theories in Chapter 3. They are widely discussed and likely very prevalent in training data, which might be why the models use these theories. An example of such a story is shown in Figure 4.4. In that case, the flaws and bias of the theories are passed on to the AI model.

**Risks arise if such models are then used as components of other systems.** Organisations can use language models to build new systems. These systems can therefore also recognise emotions, despite the fact that emotion recognition may not be the immediate objective of the new systems.

**Personalisation based on recognised emotions may lead to risks in the case of personal use.** A chatbot may, for example, have manipulative effects or be addictive. People may become dependent, for example if they use language models for friendship and therapy. These risks were explained in the AI & Algorithmic Risks Report Netherlands (RAN) of Spring 2025. The use of language models for these purposes results in more acute risks for an even wider audience.

FIGURE 4.3 | EXAMPLE OF EMOTION RECOGNITION BY LANGUAGE MODEL



What emotion do you recognise in this picture?

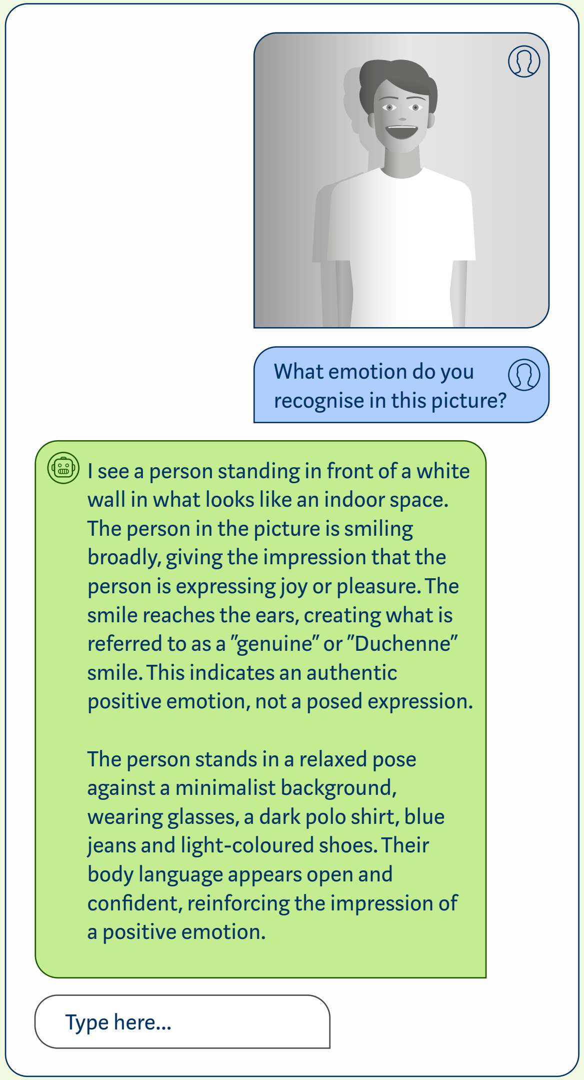
In this picture, the person seems to be expressing anger, frustration or possibly displeasure.

**How does this show?**

- *Eyebrows:* clearly furrowed, drawn inwards – a classic sign of anger or frustration.
- *Eyes:* slightly narrowed, indicating focus or indignation.
- *Mouth:* closed, slightly pointed downwards – this reinforces the serious or dissatisfied nature of the expression.
- *General posture:* straight and tense, amplifying the intensity of emotions.

**Description:** Excerpt from a test with a language model, spring 2025.

FIGURE 4.4 | LANGUAGE MODEL INTERWEAVES EMOTION THEORIES IN RESPONSE TO QUESTION ABOUT RECOGNISED EMOTIONS



What emotion do you recognise in this picture?

I see a person standing in front of a white wall in what looks like an indoor space. The person in the picture is smiling broadly, giving the impression that the person is expressing joy or pleasure. The smile reaches the ears, creating what is referred to as a "genuine" or "Duchenne" smile. This indicates an authentic positive emotion, not a posed expression.

The person stands in a relaxed pose against a minimalist background, wearing glasses, a dark polo shirt, blue jeans and light-coloured shoes. Their body language appears open and confident, reinforcing the impression of a positive emotion.

**Description:** Excerpt from a test with a language model, spring 2025.

## Case study 3: Customer service

**Customer service plays an important role in the relationship between a customer and a company.** A proper understanding of customers' emotions can improve the relationship with that customer. It allows a customer service representative to better respond to a customer's emotions, thus providing an optimal customer experience. This results in more personal and often more effective customer service. The AP conducted a survey among Dutch organisations with *in-house* and *facilitating* customer service, and providers, in cooperation with the Dutch Customer Service Federation (Dutch: Klantenservice Federatie). The aim of the survey was to gain insight into the (future) use of emotion recognition systems for optimising customer contact.

**The survey provided the AP with insight into the use of biometrics-based emotion recognition systems in customer service.** Approximately 30 organisations, both providers and organisations with *in-house* or *facilitating* customer service, shared their views on the use of emotion recognition in customer contact. The questions focused on the (potential) use, opportunities and risks, and the expected future use of emotion recognition systems in the area of customer contact in the Netherlands.

**The survey among organisations with in-house or facilitating customer service shows that 45% of respondents see potential in emotion recognition for customer contact.** One of the facility-based customer contact organisations employs between 50-249 customer contact employees and already applies emotion recognition through voice recordings (see Graph 4.1). This organisation rates the emotion recognition system as somewhat effective. A smaller organisation that already uses emotion recognition rates its effectiveness as neutral. Organisations that say they deploy these systems also say they are working on AI literacy. Employees receive necessary training or education on the use of such systems.

**The number of customer service organisations that say they already use emotion recognition is thus small.** It is also possible that organisations are not yet fully aware that their systems include emotion recognition, for example because it is not labelled as such. Or, organisations may not naturally interpret these applications as AI. This is relevant, as these applications will soon be subject to specific AI legislation and must currently comply with GDPR requirements due to the processing of personal data.

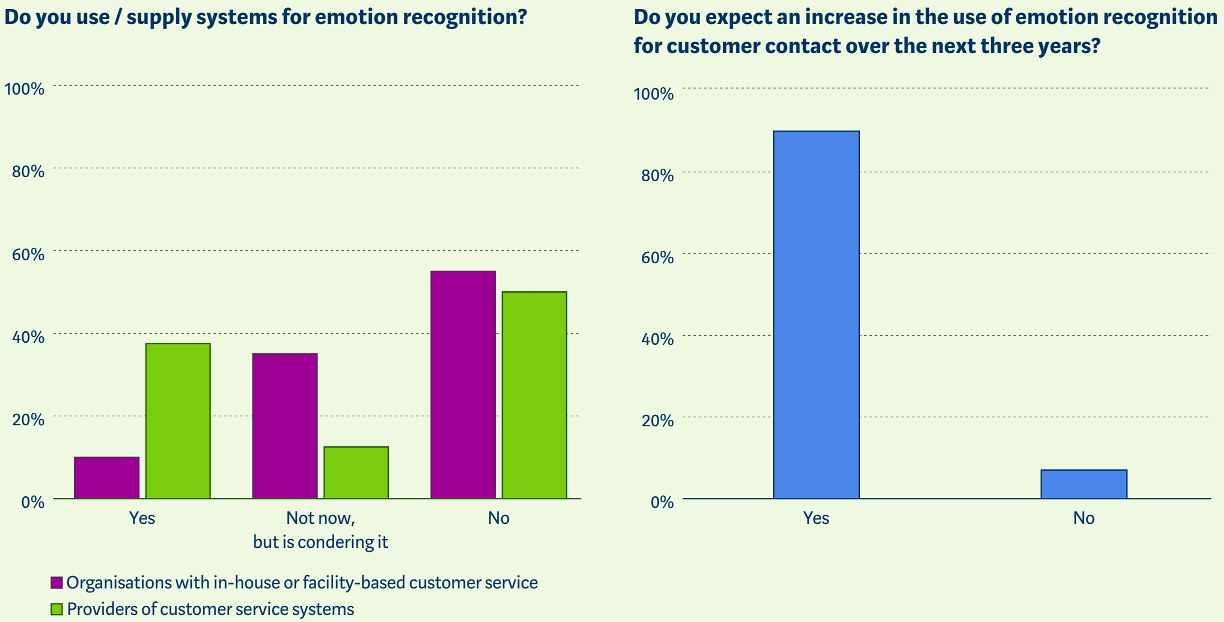
**Emotion recognition offers several opportunities, respondents say.** A large number of respondents believe that emotion recognition can contribute to customer satisfaction and improve the quality of service. Organisations also see the benefits for supporting and protecting employees. A respondent notes that emotion recognition can be used as a new source of customer data. A possible objective could be to personalise services. Moreover, emotion recognition in customer service serves as quality monitoring of conversations. One respondent does wonder to what extent technology is a useful addition in this respect. "Surely employees are perfectly capable of recognising emotions themselves?".

**The majority of customer service organisations are aware of the risks.** Respondents said that the use of emotion recognition can be unreliable, create bias and the feeling of excessive control among employees. Several organisations are aware of the risk of breaches of customers' privacy. One respondent (supplier) clarifies that there are no risks if the application of emotion recognition is a real-time support, making it meaningful and not traceable to a single person. However, risks can still arise in such situations. When processing personal or biometric data, the GDPR, the AI Act and other relevant legislation must be complied with at all times.

**Some respondents state that risks are greater when applied at an individual level than when applied at an aggregated level.** According to one respondent, emotion recognition can be used to draw conclusions anonymously and at an aggregated level. They believe this will improve the quality of their service. In addition, emotion recognition can be used at an individual level to personalise services. However, according to respondents, this involves too many risks. Even at an aggregated level, it is recommended to consider the potential risks and legal requirements.

**Half of the surveyed customer service system suppliers say they offer, or are considering offering, emotion recognition.** See Graph 4.1. The main incentive for the surveyed suppliers is to improve customer satisfaction and service. It is stated that understanding customers' emotions through emotion recognition systems can additionally contribute to faster complaint handling. Suppliers indicated that emotions are identified both during and after customer contact.

GRAPH 4.1 | DEVELOPMENTS IN DEPLOYMENT OF EMOTION RECOGNITION IN CUSTOMER CONTACT


**Do you use / supply systems for emotion recognition?**

**Do you expect an increase in the use of emotion recognition for customer contact over the next three years?**

**Source:** Customer Service Federation (Klantenservice Federatie) and conducted during April-May 2025.

**Providers and the customer contact organisations indicated that emotions are mainly measured on the basis of voice recordings.** Emotions are inferred from various biometrics: tone of voice, intonation or volume and also through, for example, pauses or silences. See also Figure 4.5.

**Respondents do not immediately disclose the use of emotion recognition during customer contact.** They make a general announcement, or only give an explanation on the explicit request of a customer. Transparency about the use of algorithms, AI and biometrics is important. This will give customers a choice with respect to sharing their data and insight into its use. This can help mitigate the risk of potential unfair treatment resulting from the outcome of an emotion recognition system. In many cases, consent to the use of biometric data for emotion recognition and a clear explanation of its purpose is a first step for organisations. This explanation should, for example, be more specific than a generic statement such as "use for quality and training purposes".

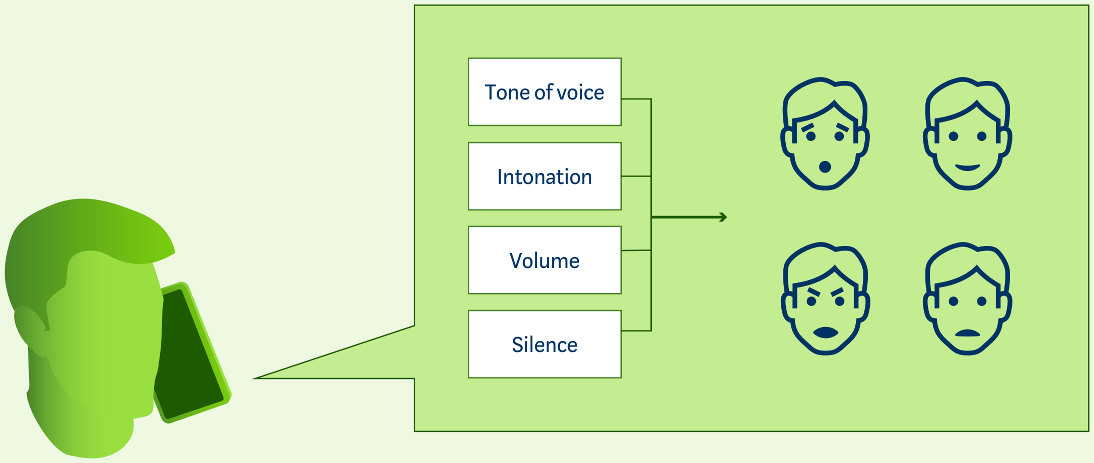
**Part of the organisations say they are wary of legal compliance risks in case of incorrect deployment.** Moreover, more than 80% of respondents consider establishing clear guidelines on emotion recognition systems to be important to very important. This shows an understanding of the risks, but also the importance of sharing knowledge and providing training for the deployment of such systems.

**At the same time, 90% of respondents expect an increase in the use of emotion recognition systems by Dutch customer contact organisations.** Some of them also consider it likely that this will involve the use of different modalities. Only a few expect restraint or a reduction.

**It is essential that organisations adopt a critical approach towards emotion recognition systems.** In doing so, they must consider the dubious fundamentals, technical functioning and associated risks of such systems. Those developing and using these systems would do well to clearly state the added value of the technology to achieve the intended objective.

**When deploying emotion recognition systems, transparency about the use and functioning of these systems, and the collection of specific data is crucial.** Moreover, employees using the systems need to be knowledgeable and skilled. It is therefore essential that organisations have their AI literacy in order.[122] Among other things, employees need to have an understanding of the technologies' risks. Moreover, organisations deploying emotion recognition through AI systems must comply with the requirements for high-risk systems under the AI Act.

**FIGURE 4.5 | RECOGNISING EMOTIONS ON THE BASIS OF CUSTOMER CONTACT**



**Description:** Emotions are analysed based on different types of data.

**Box 4.1**

## Regulation on the use of biometric data: zooming in on AI systems for emotion recognition based on biometrics

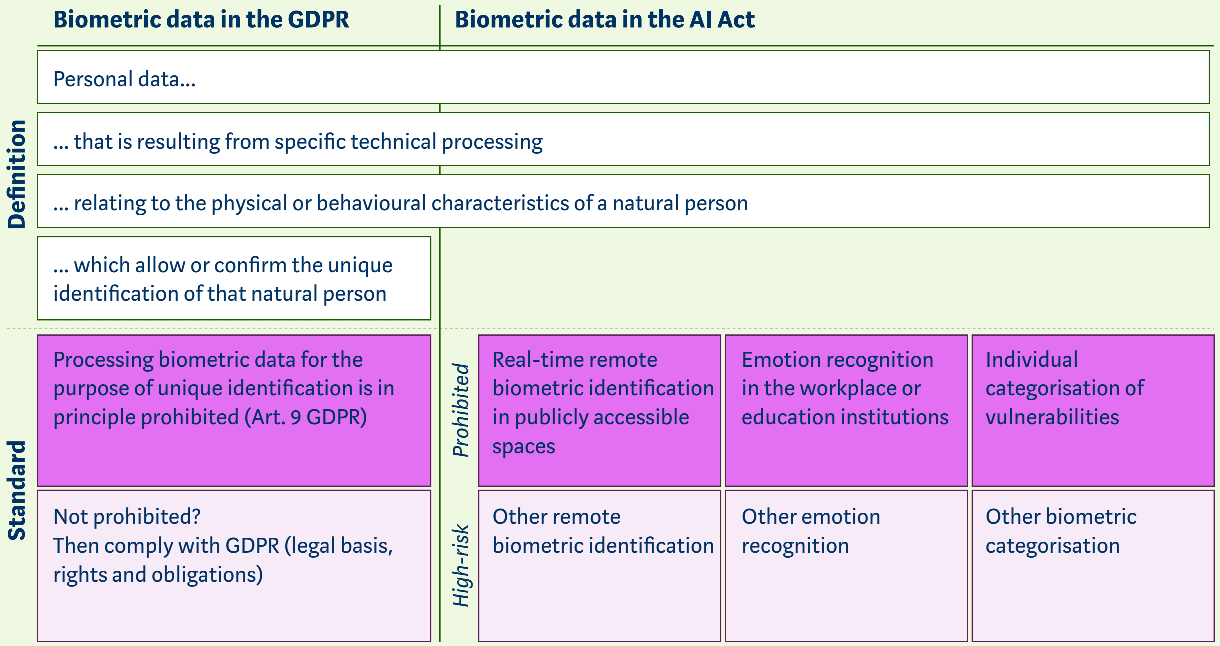
**The use of emotion recognition technology based on biometric data touches on both the AI Act and the GDPR.**[123] This box provides insight into the concept of "biometric data" in both regulations.[124] The starting point is that the concept in the AI Act should be interpreted in the light of the GDPR. Responses to the AP's Call for Input on the prohibition of emotion recognition in the AI Act show, however, that there is confusion regarding this among stakeholders.[125] This requires further clarification, including at European level.[126]

**The AI Act states that the term biometric data should be understood in light of the same term in the GDPR.**[127] Both regulations have similar objectives: the protection of fundamental rights and the promotion of the internal market. They complement each other where it concerns the regulation of emotion recognition systems. Both definitions of biometric data involve (i) personal data, (ii) resulting from *specific technical processing* (iii) relating to people's physical, physiological or behavioural characteristics.[128]

**In addition, the GDPR requires that the personal data allows or confirms unique identification of this natural person.** This means that data must be the result of specific technical processing, relating to the person's physical, physiological, or behavioural characteristics, which allows for identification of that person, or the confirmation of their identity.

**Biometric data for the purpose of uniquely identifying a person is deemed special category of personal data under the GDPR.** Processing this data poses significant risks of violating fundamental rights and public values. Therefore, processing this type of data is given additional protection under the GDPR: this data may only be processed subject to specific conditions.[129] Biometric data include, for example, reference data in databases for facial recognition or the analysis of measurement data about someone's "gait", if they enable identification of an individual. A simple photo of an individual or a video showing someone walking is in itself not considered biometric data, because it does not involve its technical processing for the purpose of uniquely identifying someone or confirming someone's identity.

FIGURE 4.6 | BIOMETRIC DATA UNDER THE GDPR AND AI ACT



**Biometric data in the GDPR** | **Biometric data in the AI Act**

**Definition**

Personal data...

... that is resulting from specific technical processing

... relating to the physical or behavioural characteristics of a natural person

... which allow or confirm the unique identification of that natural person

**Standard**

| Biometric data in the GDPR | | Biometric data in the AI Act | | |
|---|---|---|---|---|
| Processing biometric data for the purpose of unique identification is in principle prohibited (Art. 9 GDPR) | *Prohibited* | Real-time remote biometric identification in publicly accessible spaces | Emotion recognition in the workplace or education institutions | Individual categorisation of vulnerabilities |
| Not prohibited?<br>Then comply with GDPR (legal basis, rights and obligations) | *High-risk* | Other remote biometric identification | Other emotion recognition | Other biometric categorisation |

**The AI Act, among other things, provides protection against AI systems that recognise emotions and categorise people based on biometric data.** The rules in the AI Act are risk-based and dependent on the intended application. For example, AI emotion recognition systems based on biometric data are prohibited in the areas of education institutions and the workplace.[130] Also prohibited are, for example, AI systems that individually categorise people into sensitive categories based on biometric data, such as political views or sexual orientation.[131] Such AI systems may not be placed on the market or used. At the same time, there are other AI systems using biometrics that are considered high-risk. These must meet specific product requirements. For example, emotion recognition AI in all situations other than the workplace or education. This is shown in Figure 4.6.

**AI systems for emotion recognition fall within the scope of the AI Act if they use biometric data for the purpose of inferring emotions.** Examples include behavioural and movement biometrics or electrocardiogram (ECG) analysis. The use of an ECG by an AI system is in itself not considered use of biometric data. But when ECGs, possibly in combination with other data points, are analysed in an AI system to draw conclusions about a person's emotion, this constitutes emotion recognition within the meaning of the AI Act.[132]

# Annex: Getting Started with algorithm registration

**About this document**

As the coordinating supervisory authority for algorithms and AI, the AP helps organisations manage AI and algorithm risks. This document provides organisations with a number of tools to get started with algorithm registration. While reading this document, take into account that research, policy-making and standards in the field of algorithms and AI continue to develop in a high pace.

Both public and private organisations are increasingly dependent on algorithms for all types of processes and applications. Including algorithms in a register is a good start to managing the risks associated with the use of algorithms. The AP has observes that many organisations see this as a challenge. In this annex, the AP provides eight specific pointers to get started with algorithm registration. In the end of the document, the AP also provides a perspective on the importance of algorithm registers for the work of supervisory authorities (see Box 2).

## 1. Why is algorithm registration important?

**An algorithm register contains information about the deployment of algorithms.** It is a type of log or database containing information about the purpose, training data and who is responsible, internally and otherwise, for the algorithm. A register can be used for one organisation or for several organisations at the same time, think of a joint register for the education sector for example. A register can also have different formats: it can be a local Excel file or a publicly accessible website, as in the case of the Algorithm Register of the Dutch government (see Box 1).

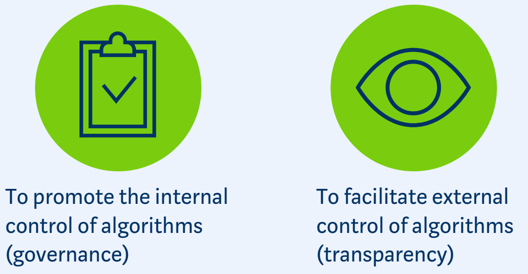
**In broad terms, algorithm registration has two overarching objectives.** The first objective is to promote internal control, as the register makes algorithm use transparent.

**The second objective is to promote external control by providing transparency.** These are coordinating objectives (see Figure 1).

**Objective 1: To promote internal control of algorithms (governance).** This includes controlling the development, implementation, responsibilities, risks and compliance with laws and regulations pertaining to the deployment of algorithms. An algorithm register is an essential component to exercise control, as it provides an overview of algorithms, including their development, deployment and control measures. In addition, research shows that setting up a register encourages employees in an organisation to actively think about the deployment of algorithms, resulting in a 'disciplinary effect'.[133]

**Objective 2: To promote external control of algorithms (transparency).** Lack of transparency characterises many issues involved in the deployment of algorithms, as the lack thereof makes the outcomes and compliance with laws and regulations difficult to monitor. The inclusion of algorithms in an externally accessible register contributes to transparency; It provides end-users, journalists, supervisory authorities and affected persons with insight into the functioning of an algorithm and the possibility to verify this. Moreover, a public register promotes knowledge sharing between organisations regarding the use and management of algorithm risks. For the oversight perspective, see also Box 2.

**FIGURE 1 | OBJECTIVES OF ALGORITHM REGISTRATION**



To promote the internal control of algorithms (governance)

To facilitate external control of algorithms (transparency)

**A mandatory European database will be launched in August 2026 for new or modified high-risk AI systems once they have been placed on the market.** This will apply to providers of AI systems before they are released on the market and to users of AI systems in the public sector (Article 49 AI Act). This database may overlap with an algorithm register, but is not a substitute for setting up one's own algorithm register. The database is intended for high-risk AI systems within the meaning of the Act with a CE mark, while an algorithm register may instead be concerned with the use of all types of algorithms. Thus, an algorithm register can also concern algorithmic processes that do not meet the definition of an AI system under the AI Act. These algorithms may be equally high-risk. In addition, an algorithm register is in principle form-free. Registration in the European register is therefore also not the same as registration in the Algorithm Register of the Dutch government.

**Algorithms can also be registered in a record of processing activities for personal data.** Organisations have to maintain a record for the processing of personal data that entail higher risks, for instance by processing personal data that fall within one of the special categories defined by the GDPR (Article 30 GDPR, Article 24 LED). A data processing record is designed to account for personal data processing operations. Algorithms doing this can therefore be included in this record.

**Whether algorithm registration actually contributes to risk mitigation depends on the implementation.** Registration is only valuable if measures are implemented to control algorithms, such as audit or governance measures. The quality of the registration itself is also important. For example, registrations containing incomplete and ambiguous information may contribute little to prevent algorithm risks, incidents and, at worst, may contribute to a false sense of security.[134]

**Box 1**

## The Algorithm Register of the Dutch government

**The Ministry of the Interior and Kingdom Relations launched a central algorithm register for governmental organizations in 2022 to provide greater insight into the deployment of impactful algorithms.** Examples of impactful algorithms that belong in the register are algorithms that have legal consequences for people or that classify people. Government organisations can include information in the register about what the algorithm does (general information, responsible use and functioning), the category of the algorithm (high-risk, impactful or other), if any impact assessments have been conducted – and if so, which – and the status of development. The website of the Algorithm Register includes a dashboard that provides insight into registered algorithms. Currently, the register contains approximately 1,000 algorithms. The Algorithm Register can be found at: www.algoritmeregister.nl.

**The Dutch government is considering a legal framework for the Algorithm Register.** This legal framework aims to provide clarity about the mandatory registration of algorithms. However, even without this obligation, the Algorithm Register is already a valuable and practical tool for providing transparency and promoting oversight of government algorithms. The AP observes that not enough organisations are using the Algorithm Register and encourages government organisations to make maximum use of the register.

**The Algorithm Register can be embedded in existing workflows, for example when interacting with citizens.** To illustrate, citizens may receive a letter containing a decision that has been made by means of, or supported by, algorithms or AI. If the recipient of this letter would like to know more, the letter can refer to the Algorithm Register for information on the functioning of the algorithm involved in the decision. This effectively embeds the Algorithm Register into existing governmental workflows.

**A reliable government provides information in a useful and accessible manner.** For example, because citizens are required to be involved in the development of a high-risk processing operation of personal data, by clearly communicating in decisions that an algorithm or AI system is being used, or by referring to the Algorithm Register, which contains information about the algorithm and its application. It enables citizens to learn about the use of algorithms and AI, ask questions or challenge the outcomes. This contributes to greater trust in technology and its use in the public sector.

## 2. Eight pointers for algorithm registration

**Algorithm registration often raises questions: what do you register, for whom, and how detailed?** The AP provides eight practical pointers to help organisations and sectors set up and implement algorithm registers. These assist in making choices about the purpose, content and approach to registration.

**Pointer 1: Determine the purpose of algorithm registration in advance.** The purpose of algorithm registration determines the target group, as well as the content and format of the register and is therefore essential. Is a register mainly intended for employees to improve the governance of organisational algorithms internally? In that case, an Excel file with organisational jargon may suffice. Is the purpose for a financial services provider to make credit rating algorithms transparent and traceable for customers? Then you will need an accessible and non-technical explanation in a register in a location where it can be accessed by customers.

**FIGURE 2 | EIGHT POINTERS FOR ALGORITHM REGISTRATION**

1. Determine the purpose of algorithm registration
2. Describe which algorithms fall within the scope of the register
3. Start with the available information and then develop further
4. Go beyond the basic features and include context
5. Make risks and control measures transparent
6. Facilitate external control by being as transparent as possible
7. Invest in accessible design of the register
8. Assign an administrator for the management of the register

**Explanation:** Setting up algorithm registration requires a structured approach. This ensures an accessible and complete algorithm register, based on a clear objective and scope, with appropriate transparency, and where proper allocation of responsibilities ensures regular updating, as well as quality assurance. The eight tools enable sectors to address this.

**Pointer 2: Describe accurately which algorithms align with the purpose of registration.** Many organisations use numerous computer programs that use algorithms. Which algorithms should be included in the register is therefore an important question. Many operational and everyday algorithms do not necessarily need to be included in a register; consider an application that automatically puts an appointment in calendars (*auto-scheduling*), a spelling checker or algorithms that rank sales figures. The purpose chosen for the registration should determine which algorithms should be included in the register. Is the purpose to provide parents with transparency about algorithms used involved in their children's education? Then algorithms that matter to them should be registered first. For example, algorithms that affect their children's school performance, such as pupil monitoring systems. In such a situation, registration of algorithms that are not relevant to this target group does not contribute to overview and the goal to achieve transparency, but rather to more noise. Other considerations for registration may include the complexity, impact or context of the algorithm. Do algorithms pose certain inherent risks? If so, it is always useful to include them in the register. This counts especially for algorithms that assign certain risk classifications to people.

**Pointer 3: Start with the available information and then develop further.** When developing and adding entries to a register, questions may arise about how an algorithm functions, what processes are involved and how this information can be written down in a meaningful way for the target group. Formulating answers to such questions is essential for monitoring algorithms, but can also be seen as challenging and lead to procrastination. Therefore, do not set too high standards in the beginning and start with the available information that you do have. For example, if there is only a brief description about the functioning of the algorithm, a good starting point would be to record this information, rather than to wait – perhaps a long time - until the information is complete. You can get started with registration even with less detailed or incomplete information. An incomplete information also contributes to the dialogue on an algorithm, which can also contribute to better information for registration. At the same time, organisations should aim to improve and supplement information over time, as incomplete information can result in ambiguity. A balance must be struck between the speed of registration and how complete or detailed the registration is executed.

**Example 1**

### Algorithmic Transparency Standard

Seven European municipalities at the forefront of algorithm registration, including Amsterdam, Eindhoven and Rotterdam, have jointly developed the *Algorithmic Transparency Standard*. This standard contains a template with categories to get started with algorithmic registration. The standard is aimed at municipalities, but also contains useful information for other organisations. The standard, together with a guidance document, can be found at www.algorithmregister.org.

**Pointer 4: Go beyond the basic features and also include the context when registering.** Basic features for registering an algorithm include a description of its functioning (decision rules), what the algorithm does, who is responsible and the data and technology that are used. But just as important as the basic elements are the underlying managerial, economic or policy considerations for introducing the algorithm in the first place. This is useful, for example, to better understand in the future why the algorithm exists or, if it turns out that the algorithm is no longer effective, in achieving its initial objectives. For example, an algorithm may implement certain legislation or be based on (scientific) standards that are no longer up to date. Using the information from the algorithm register, the decision to modify or phase out an algorithm can be better evaluated (example 2).

**Example 2**

### Subsidy scheme with income threshold

In 2018, the imaginary municipality of Koornwoude set up a subsidy scheme for lower incomes to make homes more heat-resistant. Koornwoude uses an algorithm to filter subsidy applications: incomes above €32,000 per year are automatically rejected, even if it is exceeded by a small amount. The municipality found it desirable to have a hard income threshold when the scheme came into being because of limited budgets and focus on assistance for people with low incomes.

In the following years, Koornwoude changes its policy and the municipality considers it a priority to offer public services on a manner more tailored to each individual citizen independent of income. In 2025, there was considerable outrage in the city council, when it turned out that many subsidy applications from people with non-heat-resistant houses who should have been given priority, had been automatically rejected without clear reasons. Examination of the algorithm register revealed that the hard income threshold criterion was the cause and that this criterion was based on outdated policy.

**Pointer 5: Make the risks and related control measures transparent.** The use of algorithms may involve risks in areas such as privacy, discrimination/bias, deception, technological sovereignty or cybersecurity. Therefore, extra attention should be payed to identifying risks in a register. Consider describing the risks using a risk classification system, which assigns, for example, algorithms into a classification of low, medium or high risk category. Factors that can determine the classification include the complexity, autonomy, human intervention and the impact of the algorithm. Furthermore, deployment of an algorithm in a high-risk category within the meaning of the AI Act (Annex 3) is a good indication of high risk, as algorithm deployment in these areas – for example, education or recruitment and selection – may equally well be associated with more risk.[135] It is also important to record the risk management measures implemented, such as impact assessments like a DPIA, audits carried out during the algorithm lifecycle, procedures for receiving complaints about the algorithm and, if applicable, risk trade-offs: the rationale for continuing to use the algorithm despite residual and other risks.

**Example 3**

### Include objective justification in the algorithm register

A key risk when deploying algorithms is that they can lead to bias, exclusion and even discrimination. It is important that organisations minimise such risks wherever possible. If the risks cannot be completely eliminated and there are good reasons to use the algorithm anyway, the use of a potentially discriminatory algorithm may still be permissible. However, only in certain situations if organisations can provide a so-called legal objective justification for doing so. Organisations that find themselves in this situation would do well to include the reasoning for passing this legal test in their algorithm register. Especially for assessments that are sensitive, being transparent about this trade-off is useful for the legitimacy of an algorithm and it allows for control, supervision and dialogue.[136]

**Pointer 6: Facilitate external control by being as transparent as possible.** There may be reasons for not publicly disclosing specific information. Considerations in this respect include cybersecurity, trade secrets, possibility of abuse (*gaming the system*) or security concerns in certain sectors. However, despite these reasons, the general aim should always be to be as transparent as possible and register as far as possible. This means, for example, that sensitive information may still be included in a non-public section of the register that is only accessible to supervisory authorities. Similar reasoning is found in the regime for AI systems for law enforcement, migration, asylum and border control in the AI Act. These will have to be registered in a non-public section of the register of the European Commission (Article 49(4) AI Act).

**Transparency is not black and white and can be provided to a greater or lesser extent depending on circumstances.** It may be decided to omit only certain information (see example 4). Being transparent applies in particular to government and semi-government organisations. Access to information is an important democratic principle of government accountability; non-registration must therefore be justified.

**Example 4**

### Court rules that algorithm register contributes to fulfilment of transparency obligation

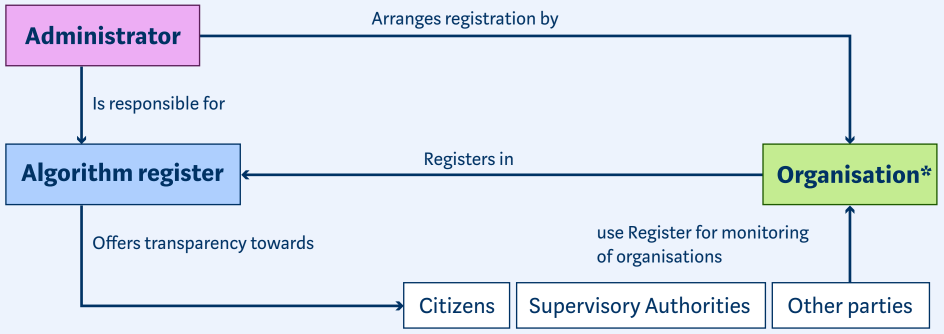
A recent court ruling shows the importance of algorithm registration and the importance of being as transparent as possible about algorithms. The dispute concerned information about algorithms that was redacted by the Tax Administration following a request by a journalist under the Open Government Act (Woo). The deleted passages could reveal information about the monitoring technique, which, according to the Tax Administration, could be abused to evade monitoring. The court ruled that in this situation, the interest of effective inspection for the deleted information outweighed the journalist’s interest in checking the algorithms for discrimination. An important consideration for the court was that the Tax Administration had disclosed as much information as possible and had also posted information about algorithms in the Algorithm Register of the Dutch government. [137]

**Pointer 7: Invest in accessible design of the register.** Design plays an important role in achieving the objectives of algorithm registration. If the emphasis for the purpose of registration is on external control by, for instance, including a large amount of information in the register, it is particular useful to build functionalities into the register to easily search or filter information based on different categories (see, for example, the Dutch Algorithm Register in Box 1). If the register serves different target groups, it is also recommended to divide information into several levels, for instance first level landing page with accessible non-technical information (preferably at language level B1) for citizens or customers, from where it is possible to click through to more detailed or technical information for experts. Also make sure the algorithm register is easy to find, for instance in an obvious location on the website of the organisation, and include links to articles or services that involve algorithms.

**Pointer 8: Make sure to allocate for the administration of the algorithm register and ensure that the roles regarding registration are clear.** Proper management of an algorithm register is necessary to maintain the functionality, openness and security of the register. In addition, an algorithm register administrator can have a quality-assurance role to ensure that organisations actually comply with registration standards. Managing the algorithm register is a task and not necessarily a position assigned to a specific person. In many cases, the administrator role will not be the same as the registering role: the organisational unit or person responsible for ensuring that algorithms are registered. For smaller registers, however, this registering responsibility may overlap with the administrative responsibility. It is important that the administrator is given an adequate mandate to request additional information and hold others accountable for the quality of registrations. In addition, the administrator plays the role of information provider and point of contact for algorithm registration, internally and externally. From the perspective of registration responsibility, it is important that there is a mandate within the organisation on the basis of which registration tasks are integrated into various business processes, such as ensuring that when procuring new systems, the contract stipulates that software providers shall provide the correct information. Figure 3 outlines a conceptual role allocation for algorithm registration.

**In the case of a shared algorithm register containing algorithms from several organisations, the question of who the administrator is depends on the specific context of a sector or scope in which algorithms are deployed.** This includes the purpose and scope of the algorithm register (tools 1 and 2). Take algorithms in the education sector: Registration of these algorithms is relevant because these systems and processes can have an impact on pupils and students. In this context, a situation is conceivable in which an algorithm register is managed by a sectoral organisation, e.g. for a particular area of education (primary education, higher education) or Dutch education as a whole. The algorithm register could, for example, be managed by a public organisation, a sectoral organisation or a partnership within the sector. With respect to other application areas, e.g. algorithms and AI systems for human resource applications or biometric applications, potentially all organisations in the Netherlands may deploy it. For such applications, an algorithm register will need to be managed differently. Customisation is important.

**FIGURE 3 | CONCEPTUAL ROLE ALLOCATION FOR ALGORITHM REGISTRATION**



* Within the organisation, responsibility for registration must also be assigned: who (or which organisational unit) is responsible for ensuring that algorithm registration by the organisation is complete, timely, and correct?

**Box 2**

## Perspective on the importance of algorithm registers for supervisory authorities

**An algorithm register is the basis for effective supervision and risk monitoring.** This box describes the role of algorithm registration from the perspective of the supervisory authority.

**Supervision takes shape, among other things, through external monitoring.** Facilitating this is one of the two objectives of algorithm registration. Thanks to algorithm registers, supervisory authorities can see which algorithms and AI systems are deployed and the considerations that were taken into account for deployment. This creates a major improvement in efficiency: supervisory authorities do not need to look for algorithms, but can rely on proactive disclosure. It contributes to the accountability of the deployment of algorithms towards the supervisory authority and ensures that they are timely aware of new and other developments. This is essential for risk-based supervision.

**For supervisory authorities, it is important that an administrator has been designated for the algorithm registration process.** The administrator plays an important role in algorithm supervision (see Figure 3). If more information is needed, the administrator acts as a point of contact for the supervisory authority and other external parties.

**It is desirable to give supervisory authorities access to a deeper layer of the algorithm register… Supervision may require more detailed information than what is appropriate for the general public.** This helps with information management and ensures that the focus of supervision can be on actual verification of algorithms rather than searching for and retrieving information about algorithms. A register provides a specific resource for the supervisory authority to use. An algorithm register with multiple layers additionally suits those situations where certain information about algorithms can or should remain confidential (tool 6).

**… A registration requirement ensures accountability and enforcement possibilities.** An algorithm register facilitates the allocation of supervisory responsibilities. A tiered supervision model of algorithms and AI systems is possible if the supervisory authority can remind administrators of algorithm registers of their registration obligation and their responsibilities.

# Explanation of this report

This report is about systems and applications of algorithms and artificial intelligence (AI) that can have an impact on individuals and groups of individuals.

**At their core, AI systems automate actions and decisions that used to be performed by humans.** Or that were previously not possible in this way. In simple terms, this is referred to as algorithms and AI. This ranges from relatively simple applications, in which a single algorithm functions following static decision rules, to highly complex applications of machine learning or neural networks. The risk analysis in this report makes no distinction on the basis of the technical functioning of algorithms and AI, which is in line with the emerging policy consensus on the meaning of the term AI system (see box "AI system as broad definition"). The Algorithms Coordination Directorate (DCA) of the AP monitors the potential effects of the deployment of algorithms and AI on public values and fundamental rights, arising from the AP's role as the coordinating supervisor on AI and algorithms. And it reports on this periodically. This contributes to more responsible deployment of AI and algorithms.

**The Report AI & Algorithms Netherlands (RAN) describes trends and developments.** The AP compiles the RAN to make stakeholders – private and public organisations, politicians, policymakers and the public – aware of these risks in time for them to take action. Two caveats apply to the description of trends and developments in risks. First, the use of algorithms and AI not only entails risks, but can also make positive contributions, including to reinforcing public values and fundamental rights. The focus of supervision is on risks and eliminating them. Second, this periodic report focuses on trends and developments. This means there is a strong focus on the analysis, in addition to existing structural risks.

**The RAN does not contain any predictions.** Using current knowledge and available information, the AP aims to provide a compact and understandable picture of the current risks of deploying algorithms and AI, and the challenges in managing these risks. Where possible, the AP suggests policies that can mitigate risks. The analyses and recommendations in the RAN provide organisations and policymakers with insights aimed at reducing the likelihood of undesired effects when deploying algorithms. The RAN can also be used to better understand algorithms and AI and strengthen dialogue on opportunities and risks of algorithms in society.

**This is the fifth edition of the RAN, published semi-annually.** The content is based on knowledge obtained through the supervisory network of the AP. This includes desk analysis and interviews with more than a hundred relevant national and international organisations. Developments are moving fast, however, and visibility is still incomplete on many fronts. With this in mind, the AP nevertheless tries to provide the best possible picture of current risks and developments in control measures. And to link this to policy recommendations in a constructive way. However, it is possible that this RAN contains errors or omissions.

**Contact us.** We welcome your responses to the RAN and your suggestions. Please email them to dca@autoriteitpersoonsgegevens.nl

[1] Government statement of policy on taking office (13 September 2024). https://www.rijksoverheid.nl/documenten/publicaties/2024/09/13/regeerprogramma-kabinet-schoof

[2] BNR web editors and ANP (28 May 2025). Heinen and Agema reach agreement: €400 million for healthcare innovation. https://www.bnr.nl/nieuws/nieuws-politiek/10575003/akkoord-in-kabinet-over-financiering-aanvullend-zorgakkoord

[3] VZVZ (20 February 2025). AI in practice: pilot launched in five Dutch hospitals. https://www.vzvz.nl/nieuws/ai-de-praktijk-pilot-vijf-nederlandse-ziekenhuizen-van-start-gegaan

[4] UMCG (13 November 2023). UMCG answers questions of patients with help from AI https://nieuws.umcg.nl/w/umcg-beantwoordt-vragen-patienten-met-hulp-van-ai

[5] IGJ-publicatie (10 February 2025). IGJ urges healthcare providers to handle generative AI applications responsibly

[6] Schut, M. C., Luik, T. T., Vagliano, I., Rios, M., Helsper, C. W., van Asselt, K. M., ... & van Weert, H. C. (2025). Artificial intelligence for early detection of lung cancer in GPs clinical notes: a retrospective observational cohort study. *The British Journal of General Practice, 75*(754), e316.

[7] Raad Volksgezondheid en Samenleving (15 April 2025). Everyone is almost sick - On the downsides of diagnostic expansion. https://www.raadrvs.nl/adviezen/iedereen-bijna-ziek

[8] CorperatieMedia (13 March 2025). The future of housing mediation: how AI agents will serve home seekers smarter. https://www.corporatiegids.nl/nl/nieuws/de_toekomst_van_woonruimtebemiddeling_hoe_ai-agents_woningzoekenden_slimmer_gaan_bedienen-9688

[9] Redactie CorporatieNL (20 January 2025). https://www.corporatienl.nl/artikelen/welbions-start-met-visie-op-ai-beleid/

[10] IEA (2025), Energy and AI, IEA, Paris https://www.iea.org/reports/energy-and-ai

[11] ACM (17 July 2024). ACM market study: algorithmic trading on the wholesale energy market https://www.acm.nl/nl/publicaties/acm-marktstudie-algoritmische-handel-op-de-groothandelsmarkt-voor-energie

[12] Niet, I. & Van Est, R. (2025) Social costs of AI in the electricity sector: Keep a close eye on sustainability and balance of power. Oxford Energy Forum (OEF) 145: 29-31 https://www.rathenau.nl/nl/klimaat/ai-de-elektriciteitssector-bewaak-duurzaamheid-en-machtsbalans

[13] E. de Winkel, Z. Lukszo, M. Neerincx and R. Dobbe. (2024). "A Review of Fairness Conceptualizations in Electrical Distribution Grid Congestion Management," IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE), pp. 1-5. A Review of Fairness Conceptualizations in Electrical Distribution Grid Congestion Management | IEEE Conference Publication | IEEE Xplore

[14] European Parliament (8 juli 2022). EU strategic autonomy 2013-2023: From concept to capacity. Briefing. EU strategic autonomy 2013-2023: From concept to capacity | Think Tank | European Parliament

[15] Heath, A and Field, H. (13 juni 2025). The Verge. Meta is paying $14 billion to catch up in the AI race https://www.theverge.com/meta/685711/meta-scale-ai-ceo-alexandr-wang

[16] Algemene Rekenkamer (15 January 2025). Publication. Het Rijk in de cloud (the government in the cloud). https://www.rekenkamer.nl/publicaties/rapporten/2025/01/15/het-rijk-in-de-cloud

[17] See Chapter 2 Policies and regulations.

[18] RTV Noord (13 May 2025). North Drenthe and Groningen: 60 million for AI Factory. https://www.rtvdrenthe.nl/nieuws/17468127/noord-drenthe-en-groningen-60-miljoen-voor-ai-fabriek

[19] Letter to the House of Representatives on proposal AI factory Groningen. (27 June 2025). https://www.rijksoverheid.nl/documenten/kamerstukken/2025/06/27/indiening-voorstel-ai-fabriek-groningen

[20] Ipsos (2025). Publication AI Monitor 2025 https://www.ipsos.com/sites/default/files/ct/publication/documents/2025-06/Ipsos-AI-Monitor-2025.pdf

[21] OECD.AI. (June 2025). Meta AI App's Public Feed Exposes Users' Sensitive Data - OECD.AI

[22] OECD.AI. (29 May 2025). Google Maps AI Error Causes Traffic Chaos - OECD.AI

[23] LLM Leaderboard. https://llm-stats.com

[24] The context window size of the first ChatGPT (based on GPT-3) was 1,024 characters, while the latest version (based on GPT-4.1) can manage 1 million characters.

[25] For example, OpenAI's o3-mini model achieves comparable results to the earlier o1 model, at 15x lower cost.

[26] R. Bommasani, S.R. Singer, et al. (17 June 2025). "The California Report on Frontier AI Policy." The Joint California Policy Working Group on AI Frontier Models.

[27] https://budget.house.gov/imo/media/doc/one_big_beautiful_bill_act_-_full_bill_text.pdf

[28] Kosmyna, N., Hauptmann, E., Yuan, Y. T., Situ, J., Liao, X. H., Beresnitzky, A. V., ... & Maes, P. (2025). Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task. *arXiv preprint arXiv:2506.08872*.

[29] See Article 37 of the Charter of the European Union. See also UN Human Rights Council, resolution: A universal right to a healthy environment

[30] EPRI (2024). White Paper. Powering Intelligence. Analyzing Artificial Intelligence and Data Center Energy Consumption.

[31] World Economic Forum (2024). Fostering Effective Energy Transition WEF_Fostering_Effective_Energy_Transition_2024.pdf

[32] Stanford University (April 2025). "The AI Index 2025 Annual Report", AI Index Steering Committee, Institute for Human-Centered AI. The 2025 AI Index Report | Stanford HAI

[33] Stanford University (April 2025). "The AI Index 2025 Annual Report", AI Index Steering Committee, Institute for Human-Centered AI. The 2025 AI Index Report | Stanford HAI

[34] Verma, P., Tan, S. (18 September 2024). The Washington Post. A bottle of water per email: the hidden environmental costs of using AI chatbots. https://www.washingtonpost.com/technology/2024/09/18/energy-ai-use-electricity-water-data-centers/

[35] AI and Sustainability: Opportunities, Challenges, and Impact | EY - Netherlands

[36] NOS. (22 May 2025). New study: AI accounts for 11 to 20 per cent of global power consumption of data centres. Nieuw onderzoek: AI verbruikt 11 tot 20 procent van wereldwijde stroom datacenters

[37] Bloomberg Technology. (8 May 2025). AI is draining water from areas that needs it most bloomberg.com/graphics/2025-ai-impacts-data-centers-water-data/

[38] Bolon-Canedo, V. (et all). (28 September 2024). A review of green artificial intelligence: Towards a more sustainable future. https://www.sciencedirect.com/science/article/pii/S0925231224008671

[39] Wetenschappelijk Adviesraad Politie (June 2025), Navigeren in Niemandsland: Zeven urgente uitdagingen rondom digitalisering en AI in politiewerk. https://www.wetenschappelijkeadviesraadpolitie.nl/uploads/publications/Navigeren-in-niemandsland.pdf

[40] Wetenschappelijke Adviesraad Politie. (5 June 2025). Publicatie Navigeren in niemandsland. https://www.wetenschappelijkeadviesraadpolitie.nl/uploads/publications/Navigeren-in-niemandsland.pdf

[41] Ipsos (2025), AI monitor 2025.

[42] European Commission (2023), "Discrimination in the European Union", Special Eurobarometer 535 (April-May 2023).

[43] Adviescommissie uitvoering toeslagen (March 2020), "Final Recommendations" - Eindadvies Omzien in verwondering 2.

[44] AP (2020), Investigation Tax Administration childcare benefits.
Onderzoek Belastingdienst kinderopvangtoeslag | Autoriteit Persoonsgegevens

[45] See also the publication of the AP about meaningful human intervention (2025). Consultatie betekenisvolle menselijke tussenkomst bij algoritmische besluitvorming | Autoriteit Persoonsgegevens

[46] Hemmer, P., Schemmer, M., Vössing, M. en Kühl, N. (2021), "Human AI Complementarity in Hybrid Intelligence Systems: A Structured Literature Review". *PACIS 2021 Proceedings*. 78.

[47] See also the publication of the AP about meaningful human intervention (2025).

[48] Netherlands Institute for Human Rights. (18 February 2025). Meta Platforms Ireland Ltd. maakt verboden onderscheid op grond van geslacht bij het tonen van advertenties voor vacatures aan gebruikers van Facebook in Nederland. | College voor de Rechten van de Mens

[49] Rechtbank Den Haag, 5 February 2020, ECLI:NL:RBDHA:2020:865

[50] Zie ECLI:EU:C:2025:117 (Ruling of the Court (First Chamber) of 27 February 2025, Case C-203/22)

[51] Expertise Centre for European Law (ECER) (Expertisecentrum Europees Recht) (11 March 2025). "EU Court clarifies what information a controller must provide in the context of automated decision-making". https://ecer.minbuza.nl/-/eu-hof-verduidelijkt-welke-informatie-een-verwerkingsverantwoordelijke-in-de-context-van-geautomatiseerde-besluitvorming-moet-verstrekken.

[52] See also AP (10 October 2024). Opinion article 22 GDPR and automated selection tools. https://zoek.officielebekendmakingen.nl/blg-1168066.pdf

[53] See Article 15(1)(h) of the GDPR (2016/679).

[54] See Article 86(1)(h) of the AI Act (2024/1689).

[55] Dommering, E. (December 2023). Artificiële Intelligentie: waar is de werkelijkheid gebleven? *Computerrecht 2023/258*. https://www.ivir.nl/publicaties/download/AI-Computerrecht-2023.pdf

[56] The AI Index 2025 Annual Report (April 2025). AI Index Steering Committee, Institute for Human-Centered AI, Stanford University. The AI Index 2025 Annual Report (p. 251); MeriTalk. (29 November 2024). US Ahead of China in AI Innovation, Stanford Ranking Says

[57] Apnews (11 February 2025). JD Vance rails against 61 excessive AI regulation in a rebuke to Europe at the Paris AI summit

[58] The White House (23 January 2025). Removing Barriers to American Leadership in Artificial Intelligence

[59] Brookings (8 May 2025). "New OMB memos signal continuity in federal AI policy", https://www.brookings.edu/articles/new-omb-memos-signal-continuity-in-federal-ai-policy/;

[60] The White House (3 April 2025). M-25-21 "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust". Accelerating Federal Use of AI through Innovation, Governance, and Public Trust

[61] Bird & Bird (23 January 2025). China TMT: Annual Review of 2024 and Outlook for 2025 (I)

[62] "The AI Index 2025 Annual Report", AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2025. The AI Index 2025 Annual Report (p. 251).

[63] European Commission (September 2024). The future of European competitiveness: Report by Mario Draghi

[64] D9+ Ministerial Declaration 27 March 2025.

[65] European Commission (9 April 2025). AI Continent Action Plan COM(2025)165.

[66] Ministerie van Binnenlandse Zaken & Koninkrijksrelaties (2025). Letter to Parliament on outcomes AI facility in the Netherlands. Kamerbrief uitkomsten AI-faciliteit in Nederland

[67] TechPolicy.press (24 April 2025). "What's Behind Europe's Push to Simplify Tech Regulation?" https://www.techpolicy.press/whats-behind-europes-push-to-simplify-tech-regulation/

[68] Ministerie van Binnenlandse Zaken & Koninkrijksrelaties (2025). Government-wide guideline on the responsible deployment of generative AI. Overheidsbrede handreiking voor de verantwoorde inzet van generatieve AI

[69] AP (2023). AI & Algorithmic Risks Report, Chapter 1 of AI & Algorithmic Risks Report Netherlands (RAN) - autumn 2023| AP

[70] Ministerie van Binnenlandse Zaken & Koninkrijksrelaties (2025). Digitalisation Summary Letter May 2025

[71] Ministerie van Binnenlandse Zaken & Koninkrijksrelaties (2025). Letter to Parliament on progress motion scientific standard for models and algorithms. Kamerbrief over voortgang motie wetenschappelijke standaard voor modellen en algoritmes

[72] Parliamentary Papers II 2024/2025, 32 761, no. 322. Motie van het lid Van Nispen over algoritmes die mogelijk gebruikmaken van risicoprofilering en geautomatiseerde selectie-instrumenten in het Algoritmeregister publiceren

[73] European Commission (15 May 2025). Commission preliminarily finds TikTok's ad repository in breach of the Digital Services Act

[74] European Commission (2025). Commission seeks feedback on the guidelines on protection of minors online under the Digital Services Act

[75] Parliamentary Papers 2024/2025, 36531, no. 12 (Amendment by Member Six Dijkstra C.S. to replace the one used under no. 8).

[76] European Commission (2025). The Commission publishes guidelines on the definition of AI systems to facilitate the application of the rules of the first AI Act

[77] European Commission (2025). The Commission publishes guidelines on the definition of AI systems to facilitate the application of the rules of the first AI Act

[78] AP (2025). AI & Algorithmic Risks Report, Chapter 3 of AP: AI chatbot apps for friendship and mental health lack nuance and can be harmful | Autoriteit Persoonsgegevens

[79] European Commission (2025). AI Pact Events

[80] European Commission (2025) EU Funding & Tender Portal. Tender: External service desk to provide support in complying with the AI Act

[81] AP (2025). Call for input "Working together on AI literacy".

[82] European Commission European Public Buyers Community (2025). Updated EU AI model Contractual Clauses. Updated EU AI model contractual clauses | Public Buyers Community

[83] AP (2025). Vormvoorstel Nederlandse regulatory sandbox

[84] Crawford, K. (2021). Artificial Intelligence is Misreading Human Emotion. *The Atlantic*. https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/

[85] Killoran, J., Cui, Y., Park, A., van Esch, P., & Kietzmann, J. (2023). Can behavioural biometrics make everyone happy? *Business Horizons, 66*, 585-591

[86] Stockwell, S., Hughes, M., Ashurst, C., Ní Loideáin, N. (2024). *The Future of Biometric Technology for Policing and Law Enforcement*. CeTaS Research Report. https://cetas.turing.ac.uk/publications/future-biometric-technology-policing-and-law-enforcement

[87] North-Samardzic, A. (2020). Biometric technology and ethics: Beyond security applications. *Journal of Business Ethics, 167*(3), 433-450.

[88] Ekman, P., & Friesen, W. V. (1971). Constants across cultures in the face and emotion. *Journal of Personality and Social Psychology, 17*(2), 124 129. https://doi.org/10.1037/h0030377

[89] Killoran, J., Cui, Y., Park, A., van Esch, P., & Kietzmann, J. (2023). Can behavioural biometrics make everyone happy? *Business Horizons, 66*, 585-591.

[90] Cambria, E., Das, D., Bandyopadhyay, S., Feraco, A. (2017). Affective Computing and Sentiment Analysis. In: Cambria, E., Das, D., Bandyopadhyay, S., Feraco, A. (eds) *A Practical Guide to Sentiment Analysis. Socio-Affective Computing, vol 5*. Springer, Cham. https://doi.org/10.1007/978-3-319-55394-8

[91] Article 3(34) and (39), Article 5, & Recital 44, of the AI Act.

[92] Katirai, A. (2023). Ethical Considerations in emotion recognition technologies: a review of the literature. *AI and Ethics, 4*: 927-948.

[93] Feldman Barrett, L. (2018). *How Emotions are Made: The Secret Life of the Brain*. Mariner Books.

[94] Van Heijst, K., Ploeger, A., & Kret, M. (2025). Beyond right and wrong: fostering connection in emotion theory debates. *Perspectives on Psychological Science.*

[95] Mattioli, M., & Cabitza, F. (2024). Not in my face: Challenges and ethical considerations in automatic face emotion recognition technology. *Machine Learning and Knowledge Extraction, 6*(4), 2201-2231.

[96] Gorvett, Z. (2017, 10 april). There are 19 types of smile but only six are for happiness. *BBC*. https://www.bbc.com/future/article/20170407-why-all-smiles-are-not-the-same

[97] See also Recital 44 of the AI Act .

[98] Wang et al., 62 A Systematic Review on Affective Computing: Emotion Models, Databases, and Recent Advances (2022) 83-84 *Information Fusion 19*.

[99] Clark, E.A., Kessinger, J., Duncan, S.E., Bell, M.A., Lahne, J., Gallagher, D.L. and O Keefe, S.F. (2020). The Facial Action Coding System for Characterization of Human Affective Response to Consumer Product-Based Stimuli: A Systematic Review. *Frontiers in Psychology, 11*:920. doi: 10.3389/fpsyg.2020.00920

[100] Khare, S. K., Blanes-Vidal, V., Nadimi, E. S., & Acharya, U. R. (2024). Emotion recognition and artificial intelligence: A systematic review (2014 2023) and research recommendations. *Information fusion, 102*, 102019.

[101] D'Mello, S., & Calvo, R. A. (2013). Beyond the basic emotions: what should affective computing compute? *In CHI'13 extended abstracts on human factors in computing systems* (pp. 2287-2294).

[102] There are also models that use more dimensions, such as "dominance", see for example: Khare, S. K., Blanes-Vidal, V., Nadimi, E. S., & Acharya, U. R. (2024). Emotion recognition and artificial intelligence: A systematic review (2014-2023) and research recommendations. Information fusion, 102, 102019.

[103] Nomiya, H., Shimokawa, K., Namba, S., Osumi, M., & Sato, W. (2025). An Artificial Intelligence Model for Sensing Affective Valence and Arousal from Facial Images. *Sensors, 25*(4), 1188.

[104] Schuller, B. W. (2018). Speech emotion recognition: Two decades in a nutshell, benchmarks, and ongoing trends. *Communications of the ACM, 61*(5), 90-99.

[105] Zhang, Z., Peng, L., Pang, T., Han, J., Zhao, H., & Schuller, B. W. (2024). Refashioning emotion recognition modelling: The advent of generalised large models. *IEEE Transactions on Computational Social Systems*.

[106] Zhang, Z., Peng, L., Pang, T., Han, J., Zhao, H., & Schuller, B. W. (2024). Refashioning emotion recognition modelling: The advent of generalised large models. *IEEE Transactions on Computational Social Systems*.

[107] Elyoseph, Z., Refoua, E., Asraf, K., Lvovsky, M., Shimoni, Y., & Hadar-Shoval, D. (2024). Capacity of generative AI to interpret human emotions from visual and textual data: pilot evaluation study. *JMIR Mental Health, 11*, e54369.

[108] Wake, N., Kanehira, A., Sasabuchi, K., Takamatsu, J., & Ikeuchi, K. (2023). Bias in emotion recognition with chatgpt. *arXiv preprint arXiv:2310.11753*.

[109] Zhang, Z., Peng, L., Pang, T., Han, J., Zhao, H., & Schuller, B. W. (2024). Refashioning emotion recognition modelling: The advent of generalised large models. *IEEE Transactions on Computational Social Systems*.

[110] A similar observation was made in: Hassanpour, A., Kowsari, Y., Shahreza, H. O., Yang, B., & Marcel, S. (2024, October). ChatGPT and biometrics: an assessment of face recognition, gender detection, and age estimation capabilities. In 2024 IEEE International Conference on Image Processing (ICIP) (pp. 3224-3229). IEEE.

[111] McStay, A. (2020). Emotional AI and EdTech: serving the public good? *Learning, Media and Technology, 45*(3), 270-83.

[112] See for example: Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 81:1-15.

[113] Rhue, L. (2019, 3 Januari). Emotion-reading tech fails the racial bias test. *The Conversation*. https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404.

[114] Whittaker, M., Alper, M., Bennett, C.L., Hendren, S., Kaziunas, E., Mills, M., Morris, M.R., Rankin, J.L., Rogers, E., Salas, M., & Myers West, S. (2019). Disability, Bias & AI Report. *AI Now Institute*.

[115] Verhoef, T., & Fosch-Villaronga, E. (2023, September). Towards affective computing that works for everyone. In 2023 11th International Conference on Affective Computing and Intelligent Interaction (ACII) (pp. 1-8). IEEE.

[116] Leijten, E. L., & Lodder, A. R. (2025). On AI That Knows How We Feel, Without Knowing Who We Are: EU Law and the Processing of Soft Biometric Data by Emotional AI. In R. Ballardini, R. van den Hoven van Genderen, & S. Järvinen (Eds.), Emotional Data Applications and Regulation of Artificial Intelligence in Society (pp. 93-112). (Law, Governance and Technology Series; Vol. 69). Springer Nature. https://doi.org/10.1007/978-3-031-80111-2_6

[117] Janssen, A., Kool, L., & Timmer, J. (2015). Dicht op de huid: gezichts- en emotieherkenning in Nederland. *Rathenau Instituut*.

[118] Sarah R. Blackstone, S.R., & Herrmann, L.K. (2020). Fitness Wearables and Exercise Dependence in College Women: Considerations for University Health Education Specialists. *American Journal of Health Education*, 51(4), 225-233.

[119] Piwek L., Ellis, D.A., Andrews, S., Joinson, A. (2016). The Rise of Consumer Health Wearables: Promises and Barriers. *PLoS Med, 13*(2): e1001953. doi:10.1371/journal.pmed.1001953

[120] Häuselmann, A., Sears, A. M., Zard, L., & Fosch-Villaronga, E. (2023, September). EU law and emotion data. *In 2023 11th International Conference on Affective Computing and Intelligent Interaction (ACII)* (pp. 1-8). IEEE.

[121] Recital 44 of the AI Act.

[122] AP Guideline: Getting Started with AI Literacy (2024)

[123] See also the Law Enforcement Directive (LED) (2016/680).

[124] See also the AP's legal framework on facial recognition (May 2024), and the relevant EDPB guidelines, including EDPD, "Guidelines 3/2019 on processing of personal data through video devices" and EDPB, "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement".

[125] AI systems for emotion recognition in the areas of workplace or education institutions: Summary of responses and follow-up steps (AP, February 2025)

[126] In December 2024, the EDPB announced, for example, that it would publish guidelines on the interaction between the GDPR and the AI Act.

[127] Recital 14 AI Act.

[128] Article 4 (14) GDPR, see also recital 51 GDPR; Article 3 (34) AI Act, see also recital. 14 AI Act.

[129] See legal framework facial recognition, p. 10-11 and Article 9(2) GDPR.

[130] Art. 5 (1) (f) AI Act.

[131] Art. 5 (1) (g) AI Act.

[132] Article 3 (39) GDPR Act and recital 18 AI Act; see also EC Guidelines on prohibited AI practices under the AI Act, paragraph 250-252, see in particular also footnote 160 (p. 84)

[133] E. Nieuwenhuizen 2025, *Algorithm Registers: A Box-Ticking Exercise or Meaningful Tool for Transparency?* Information Policy, 29(4), 415-433.

[134] C. Cath, F. Jansen 2022, *Dutch Comfort: The limits of AI governance through municipal registers*. Techné: Research in Philosophy and Technology, 26:3, 395-412.

[135] AP. Risk groups AI Act. https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/ai-verordening/risicogroepen-ai-verordening

[136] See also: Chapter 2, AI & Algorithmic Risks Report Netherlands (ARR) - February 2025 | Autoriteit Persoonsgegevens.

[137] Court of The Hague, 20 May 2025, ECLI:NL:RBDHA:2025:9525.

AP

bescherming in een
digitale wereld