Reporting AI & Algorithms

The Netherlands

Summer 2025 (Issue 5, July 2025)

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

AP | bescherming in een digitale wereld

Dutch Data Protection Authority
Directorate Coordination Algorithms (DCA)

Table of contents

Key messages

1. The development and deployment of AI systems to recognize emotions is growing, while their effectiveness is questionable and their deployment is risky.

A growing number of AI systems claim to be able to recognize emotional states, such as happiness, anger, or stress, based on biometrics. This could include emotion recognition for insights into consumer purchasing behavior, or patient emotions for improved healthcare.
The systems are built on controversial assumptions about emotions and indicators of emotional states, and their measurability. Therefore, it is doubtful whether they can actually measure emotions. If the systems are deployed anyway, they could violate fundamental rights and public values. Think of the restriction of freedom and human autonomy, discrimination, and privacy violations. Read more about AI and emotion recognition in Chapter 3.

2. The Dutch Data Protection Authority (AP) has examined applications of emotion recognition for customer services, wearables, and language models; the broad range of applications in certain cases leads to risks that require the attention of developers, users, regulators, and policymakers.

For example, the in-depth study reveals that it's not always clear how emotions and stress are recognized or how effective they are. Despite the growth of these applications, people still don't always know that emotion recognition is being used, or based on which data. Developers and users must be aware of the risks each specific application entails. Different applications will soon be subject to specific regulations. But whether it *desirable* is to deploy these systems. AI for emotion recognition has been banned in education and the workplace since February 2025, but where it is permitted under specific conditions, it will ultimately be a political decision to determine in which cases and to what extent the use of these systems is desirable. Read more about emotion recognition in practice in Chapter 4.

3. The AP calls on organizations to be critical about the use of emotion recognition applications.

Organizations must be aware of the limitations of emotion recognition and carefully consider whether their use is appropriate and proportionate. If these systems are deployed, organizations must be transparent about their use to the individuals whose emotions are being analyzed. Furthermore, obtaining consent from the individuals being analyzed is an important first step for organizations to deploy these systems responsibly.
Chapter 4 discusses three practical examples of emotion recognition. But working towards responsible, conscious, and transparent implementation is also important for other applications.

4. In the Netherlands, there is a strong commitment to reliable AI, but as a society we need to step up our efforts to responsibly utilize the opportunities of AI.

Reliable use of algorithms and AI is possible and requires attention to protection, safety, and transparency. This means that as a society, we must learn from incidents. Given the speed

Given the scale and extent to which Dutch organizations are adopting AI and algorithms, it seems likely that many incidents go unnoticed, unreported, and that lessons learned are not shared. Incidents are inevitable in this phase of societal transition. Dealing with incidents and learning from their nature, cause, and damage is essential for organizations to grow in responsible behavior. Supervisory authorities can work with legislators and the regulatory field to create a suitable environment in which this knowledge can be shared without revealing trade secrets.

5. It is now possible for every organization to work purposefully on AI maturity using the increasingly rich package of tools.

From algorithm registration, bias testing, and establishing quality management systems to conducting fundamental rights assessments and ensuring transparency of their use – to achieve this, organizations must invest in people and resources and establish measurable and concrete organizational goals. For example, an ambition to annually audit the most critical algorithmic processes and AI systems based on key criteria such as organizational control, robustness, bias and fairness, cybersecurity, and arbitrariness. This presents a challenge for organizations, demanding responsibility and their own judgment. Mature organizations are transparent about their use, have robust systems and processes for management, and take internal control, external audit, and oversight seriously.

6. Designing human review and combating discrimination remains a major challenge.

In the Netherlands, we are very aware that both individuals and algorithms can discriminate. This clearly demonstrates the importance of reducing both human and algorithmic bias in processes.
The interaction between humans and algorithms is crucial for this and must be properly designed to prevent discrimination and bias as much as possible. The House of Representatives recently adopted a motion aimed at making "blind" assessments of citizens a starting point, for example, in fraud detection. From the perspective of the Dutch Data Protection Authority (AP) as a supervisory authority, it is also necessary to consider the decision-making process as a whole, add random samples, and ensure the explainability and ability to challenge risk selection.

7. AI plays an important role in geopolitical developments.

Successful deployment of AI is seen as essential for economic development. Promoting innovation and the AI ecosystem has rapidly risen to the top of the political agenda. Where there are doubts about restricting innovation through regulations, people quickly turn to deregulation. However, to protect against excesses, new regulations are also being developed or implemented. The perspective on the right balance between innovation and protection also varies by country and region. Moreover, AI is increasingly becoming a key component of national strategies, ranging from healthcare to defense.

The dependence on major players and the growing desire for strategic autonomy are playing an increasingly important role. This topic is also being addressed at European level, for example through the European Commission's AI strategy and its accompanying financing ambitions.

8. It is important to maintain or accelerate the pace of developing and implementing AI policy.

To capitalize on the opportunities of AI and manage the risks, a national, overarching AI strategy remains essential. It is important to mandate algorithm registration for (semi-)public organizations when they deploy high-impact algorithms or AI. The Dutch Data Protection Authority (AP) also recommends requiring periodic audits for these algorithms and AI. To ensure responsible innovation, sufficient resources for AI oversight in the Netherlands must be available across all relevant supervisory bodies and inspectorates. To effectively organize oversight jointly and keep pace with rapid technological developments, investments in partnerships are essential. The AP recommends reserving a fixed percentage for internal control, external control, and oversight of public investments in innovation. It is also recommended to reserve a portion for risk management, including both internal and external control, for private investments.
The proper functioning of these layers is essential for accelerating innovation and deployment.

9. The AI Regulation is becoming increasingly concrete, with standards being an important instrument for gaining control over AI and complying with the AI Regulation in the future.

More than a year after the AI Regulation entered into force, we are seeing further clarification and elaboration. The European Commission's guidelines on prohibited AI systems and the definition of AI systems provide initial insights and explanations, but also raise many follow-up questions. Further elaboration will follow, with the development of standards providing clarity on how organizations can comply with the AI Regulation's requirements. Not only generic but also sector-specific adaptations of the AI Regulation should provide guidance and support.

10. Registering algorithms is a good start to managing the risks associated with algorithm use. An algorithm register contains information about the use of algorithms.

Broadly speaking, algorithm registration has two overarching goals. Goal 1: Promoting internal control of algorithms (governance). Goal 2: Promoting external control of algorithms (transparency). The Dutch government is developing a legal framework for the Algorithm Register. This legal framework should provide clarity regarding the mandatory registration of algorithms. Even without mandatory registration, the Algorithm Register is already a valuable and practical tool.

A tool for providing transparency and promoting oversight of government algorithms. Not all organizations are using the Algorithm Register yet; the Dutch Data Protection Authority (AP) encourages government organizations to use it as much as possible. In the appendix "Getting started with algorithm registration," the AP provides eight concrete tools for getting started with algorithm registration.

Overarching mastery image of AI and algorithms in the Netherlands – Summer 2025

Control pillar	Status Winter 2024-2025	Status Summer 2025	Explanation
Control over the development and volatility of algorithmic and AI technology	**Asks for increased attention**	**Asks for increased attention**	Unchanged from the mastery picture six months ago. Developments in (generative) AI continue unabated. The risks and impact of frontier models are not yet fully understood.
Understanding and manageability of emerging algorithmic and AI risks	**Asks for increased attention**	**Asks for increased attention**	Unchanged from the control picture 6 months ago. New developments are leading to new incidents that are not always anticipated. Controllability tools are still being developed.
Development of a national AI ecosystem	**Asks for attention**	**Asks for attention**	The importance of a strong national AI ecosystem is increasing. This is evident in the growing desire for digital sovereignty in the Netherlands and Europe. Attention to investment in AI is also increasing, enabling a catch-up effort.
Trust in, attention to and knowledge about algorithms and AI in Dutch society	**Is on track**	**Is on track**	Unchanged from the mastery profile 6 months ago. After a low point in 2024, Dutch public confidence in AI and algorithms is continuing to grow. The Netherlands is actively working on AI literacy.
Frameworks and powers for supervision of AI systems	**Is on track**	**Asks for attention**	Demands more attention due to the ambitious timelines for the AI Regulation, the call for simplification and the Dutch political situation.
Harmonized and practically applicable standards for AI systems	**Progress fail**	**Asks for increased attention**	An improvement compared to the control picture six months ago. Harmonized standards will not be ready in the short term to prepare for the AI Regulation. But progress in standard development is starting to accelerate.

Control pillar	Status Winter 2024-2025	Status Summer 2025	Explanation
Registration and transparency about algorithms and AI systems	**Asks for increased attention**	**Progress fail**	The overall picture is less positive than it was six months ago. Work on algorithm registration has been underway for several years, but there's still a long way to go. Within the government, most organizations haven't registered anything yet.
Insight into incidents involving the use of algorithms and AI and the embedding of lessons	**Progress fail**	**Progress fail**	Unchanged from the control picture six months ago. There is a lack of notifications and reports of incidents involving AI and algorithms to supervisory authorities.
Institutionalization of governance, risk management and auditing of algorithms and AI	**Asks for increased attention**	**Asks for increased attention**	Unchanged compared to the control picture six months ago. Periodic audits are now only being performed to a limited extent, and the results are only partially visible.

Explanation: As the coordinating supervisory authority for algorithms and AI, the Dutch Data Protection Authority (AP) proactively and comprehensively identifies and analyzes the most important, cross-sector risks and impacts. The so-called control pillars provide insight into how to responsibly address these risks. The overarching control picture shows the current state of control of algorithms and AI in the Netherlands. This control picture must be seen against the backdrop of a broad societal transition, driven by AI as a systems technology, which places higher demands on the level of control each year. To indicate progress (partly compared to the previous control picture), the AP uses a color code for each pillar: green means "on track," light pink means "requires attention," purple means "requires increased attention," and dark purple means "insufficient progress."

1. Umbrella developments

QUICK TO THIS PART

1.1 Algorithms as a solution to scarcity

In the Netherlands, AI and algorithms are often used with high expectations to (partly) solve scarcity in society.AI and algorithms are expected to offer smart solutions for issues like housing shortages and pressure on the energy grid. AI and algorithms are expected to generate new suggestions or accurate predictions that organizations can act on.

For example, various algorithms are used in healthcare to reduce workload or organise care tasks more effectively. The government is also fully committed to the adoption of AI in the healthcare sector.1 In the coming years, the government will invest 400 million euros in technological innovations, including AI, to make healthcare work more efficient and reduce workload.2
For example, a number of hospitals are collaborating in a pilot for AI applications for detecting fractures and identifying incidental pulmonary embolisms.3 And generative AI is being used to help answer patient questions.4

The AP believes that AI can be of great significance in healthcare and offers benefits for healthcare providers and patients. At the same time, there's a risk that healthcare institutions will become more dependent on cloud-based solutions and increasing processing of sensitive data. Furthermore, many applications of generative AI are still relatively new to the market, and their impact on patient care is still (partly) unknown. It's no wonder the Health and Youth Care Inspectorate urges healthcare providers to handle this carefully.
with the purchase, implementation and use of generative AI in healthcare.5

The quality of medical care can also improve, for example through algorithms that can detect lung cancer earlier... These kinds of positive developments regularly make the news. For example, an algorithm that can predict lung cancer earlier based on patterns in patient records. The algorithm analyzes patient records for relevant patterns and weighs certain risks for lung cancer. Early detection of lung cancer with the new algorithm can, in some cases, lead to better treatment.

...but the use of algorithms and AI in healthcare can lead to indirect effects. The potential of using AI for early disease detection also impacts other parts of the healthcare chain. The Council for Public Health and Society (RVS) recently wrote that the so-called diagnosis expansion (the rapid increase in the number of people diagnosed with a disease) is putting more pressure on an already overloaded healthcare system. While early diagnosis can be helpful for people with symptoms, early diagnosis for people without symptoms increasingly stretches the criteria for disease. The RVS therefore calls for a public debate on the usefulness and necessity of early diagnosis now that the possibilities are increasing thanks to technologies like AI.

The shortage on the housing market is also being addressed by supporting home seekers through AI and algorithms.AI agents are used to help home seekers search for a new place to live more effectively, to assist with mediation, and to improve search results.
personalize and show homes that they have a realistic chance of getting.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. If AI is fully deployed, then this can be achieved according to the*International Energy Agency* 95 billion euros in annual savings and 175 GW of energy capacity can be freed up.[10]In the Netherlands, energy companies and grid operators are fully committed to AI, for example, to find suitable locations for solar and wind farms or to predict energy consumption for optimization. Last year, regulators ACM and AFM noted a significant increase in algorithmic energy trading and highlighted 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 utilities dependent, reduces democratic oversight and may lead to the emergence of monopolistic market structures.

People are directly affected by the AI-driven energy market. Developments like dynamic pricing, in which AI plays a central role, encourage households to adjust their energy consumption to fluctuating rates. This can help reduce peak loads, but also raises questions about accessibility, fairness, and explainability – especially for people who are less flexible or lack access to smart technologies.

AI offers advantages and can help to better match or manage supply and demand, but it also raises new and fundamental distribution issues in which, in the background, considerations are actually made about fundamental rights and public interests, without receiving full attention.
Who gets access to energy and when? On what basis are choices made? And who has influence on that? *algorithmic fairness*Crucial. But what is "fair" depends on the standard: is it equal opportunities, equal treatment, or equal outcomes? Without clear choices on this, algorithms can actually reinforce existing inequalities.[13]

1.2 Strategic autonomy and digital sovereignty

With increasing geopolitical tensions, the need for strategic autonomy further increases. The integration of AI into socially relevant sectors and applications increases dependencies. Strategic autonomy means that countries have the ability to act autonomously, without being dependent on others.[14]This includes the European economy, energy, but also technology.

Meta invested $14.3 billion in global AI training company Scale in June 2025. With this investment, Meta will acquire 49% of the company.[15]
Scale's CEO has also joined Meta. Investments on this scale demonstrate the importance a small group of large tech companies attach to developing and training AI models.

There are positive developments that increase digital sovereignty and strategic autonomy. There's still a long way to go. Increasingly, proprietary systems are being developed to reduce dependence on parties outside the EU. We're also seeing more and more*private AI stacks*', where companies and other organizations can build and run their AI applications. But complete digital sovereignty is still a long way off. The Netherlands Court of Audit states that the Dutch government purchases more than half of its public cloud services from three major American tech companies.[16]

Furthermore, the province of Groningen and several municipalities are committed to the arrival of an 'AI factory' to reduce dependence on other countries in the field of artificial intelligence. The European Commission wants to have at least fifteen of these 'factories' in Europe.[17]
Such a factory would consist of a center of expertise and a supercomputer. It is seen as a unique opportunity for economic growth, knowledge development, and innovation in the region and the Netherlands.[18]
The factory will cost between €160 and €240 million, making it one of the most expensive AI factories in Europe. Thanks to financial commitments from the Groningen and North Drenthe regions, and the national government, its realization is moving closer.[19]

Working on strategic autonomy ultimately also contributes to maintaining control over the algorithms and AI used in the Netherlands. The execution of societally critical processes, such as government services, increasingly depends on the use of algorithmic processes. Strategic autonomy ensures that the Netherlands has its own infrastructure and data management, based on which Algorithms and AI systems can operate. For example, for algorithms used in government decision-making, this ensures that the Netherlands can fully align its systems with its own fundamental values and maintain technical and ethical control over them.

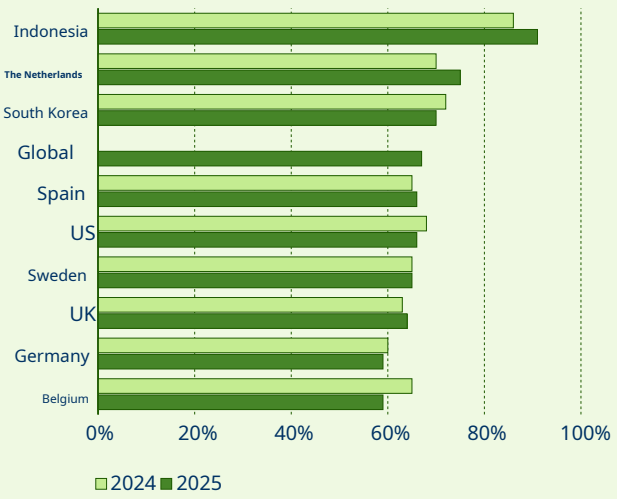
1.3 Trust, use and visibility into incidents

Dutch citizens are becoming increasingly positive about their own AI knowledge and see proportionally more advantages in AI. Globally, about two out of three people believe they have a good understanding of AI. This is according to an international comparative study conducted by Ipsos in 30 countries.[20]In the Netherlands, 75% of citizens now agree with this statement – a 5% increase compared to 2024. This puts the Netherlands higher than most other countries. Confidence in their own AI knowledge is therefore high. The Dutch also increasingly see proportionally more advantages than disadvantages in AI. In 2024, the Dutch were the most critical of AI worldwide. At that time, 36% of the Dutch population indicated they saw more advantages than disadvantages in AI. In 2025, this percentage will have increased by 7% to 43%. This brings the Netherlands to a level comparable to 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 been reversed. See also Figure 1.1.

FIGURE 1 . 1 | DEVELOPMENTS IN PERCEPTION AND USE OF AI IN THE NETHERLANDS

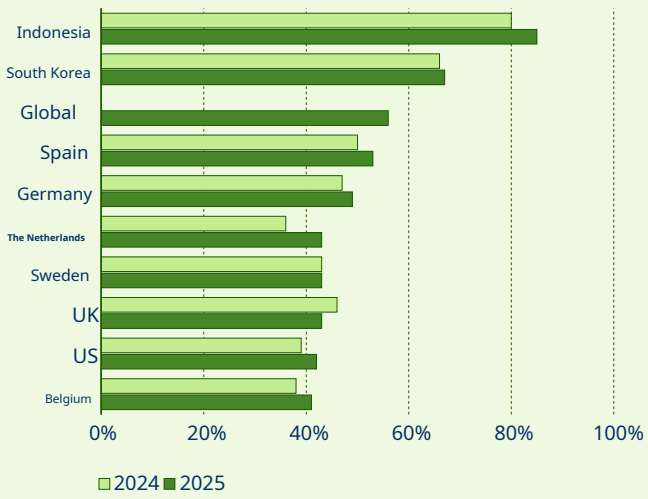
In 2025 zijn Nederlandse burgers zeer positief over hun begrip van AI...

% Eens met de stelling: "Ik heb een goed begrip van wat AI is"



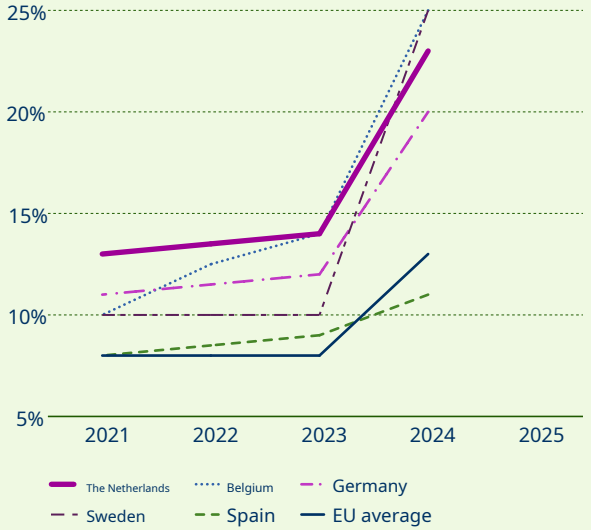
... staan Nederlanders relatief minder kritisch tegenover AI...

% Eens met de stelling: "Producenten en diensten met AI hebben meer voordelen dan nadelen"



... en met AI-gebruik door bedrijven blijft Nederland een koploper.

% Bedrijven dat gebruik maakt van minstens één van zeven AI-technologiën



Source: left and center: Ipsos AI monitor (n=23,685, 32 countries), right: Eurostat (online data code: isoc_eb_ain2)

More and more Dutch companies are using AI, with an acceleration in recent years. Eurostat data provides insight into recent developments. 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). With a percentage of 23%, the Netherlands remains a European leader. However, in terms of AI use in businesses, we have been overtaken by countries like Belgium and Sweden.

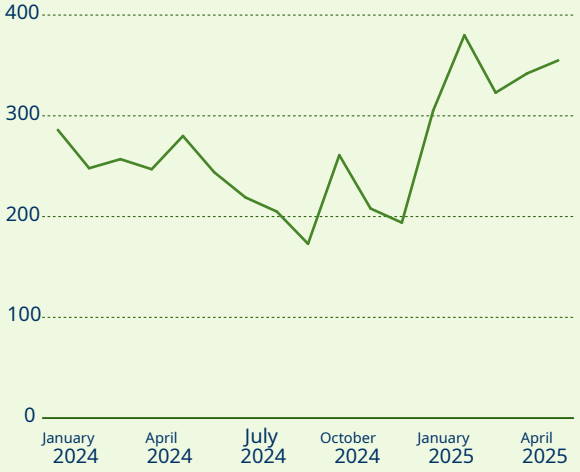
In recent months, the global media has increasingly reported on incidents and risky developments involving AI. Based on the information from Since early 2025, the media have been adding approximately 300 to 400 incidents and risky developments to the OECD AI Incidents Monitor each month. This helps provide insight into risky developments and how they impact principles for responsible AI. In 2024, this was 200 to 300 incidents per month. Figure 1.2 shows the recent trend.

It is striking that the incidents and risky developments affect all the principles for responsible AI. Reports related to responsible AI principles, fairness, and sustainability are the least common. This is partly because these risks often remain unnoticed in the area of fairness, or primarily play out in the long term in the area of sustainability. Between January and May 2025, approximately 700 incidents and risky developments related to (lack of) transparency occurred (Figure 1.2). But also in other areas. such as digital security (including cybersecurity risks), accountability, privacy, fundamental rights and physical security, the number of incidents and risky developments is numerous.

Incidents can impact rights and the physical world. This led to a privacy incident when prompts from some users in Meta AI, which will soon be available in the Netherlands, appeared on a public Meta feed without the user's consent. This can happen, for example, with users who use Meta AI via Instagram and have a public Instagram account.[21]Furthermore, Google Maps recently created unnecessary risks to physical safety: on day 1 of the Ascension weekend, the program'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 through social engineering and phishing much easier.

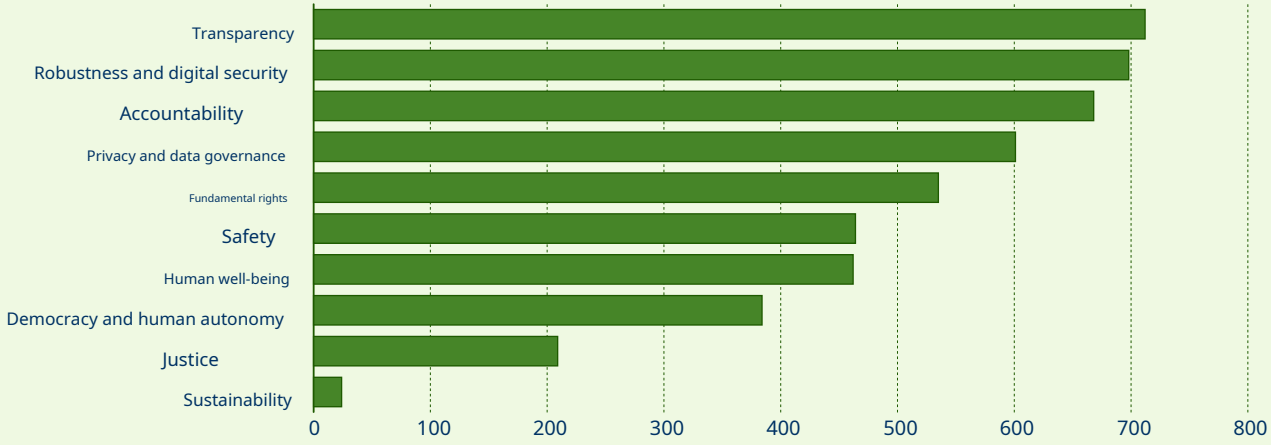
FIGURE 1.2 | GLOBAL DEVELOPMENTS IN AI - INCIDENTS AND RISKY AI DEVELOPMENTS

Wereldwijd is er een gestage toename van het maandelijkse aantal geïdentificeerde AI-incidenten...



Geïdentificeerde AI-incidenten en risicovolle ontwikkelingen per maand (wereldwijd)

... en deze raken in de praktijk aan alle principes voor verantwoorde AI.



Aantal incidenten en risicovolle ontwikkelingen per principe voor verantwoorde AI (wereldwijd, januari 2025 - mei 2025, cumulatief)

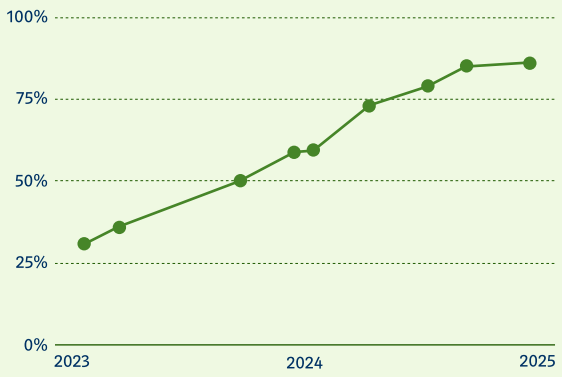
Source:OECD AI Incidents Monitor (AIM)

1.4 Development of generative AI continues unabated

New generative AI models will continue to be launched with great regularity in 2025. Major language model providers (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, but improve performance in other areas.A key indicator of 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 FLATTING OFF IN SOME AREAS



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

Generative AI models can handle more and more inputs. Where at the launch of ChatGPT at the end of 2022 the so-called*context window size*, the size of a prompt or document that a model receives as input was barely one page from 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, summarize what happens in 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. Due to continuous innovations in the way models are trained and work, new models often achieve performance comparable to previous top models, at a fraction of the cost.[25] These more efficient models use less computing power and therefore energy, both during development and use.

At the same time, some model shortcomings persist, such as when models fabricate false information. Many models today have access to the internet for information retrieval and arrive at their output based on a series of reasoning steps. While these functionalities lead to better outcomes in certain situations, various studies show that the problem persists: models continue to fabricate incorrect information out of thin air.

Organizations in California are not sufficiently equipped to fully understand the risks and impacts of frontier models. On June 17, 'The California Report on Frontier AI Policy' was published.[26]This report argues that a good balance between innovation and regulation is needed. However, organizations are currently unable to keep up with the rapid developments in 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 a ban on further regulation of AI is currently being discussed. [27]

People who write texts with the help of an LLM/AI chatbot use their brain less, hardly or not at all store the information from those texts, are less creative and the final text mainly uses

common words and concepts. This is evident from the initial results of a study conducted by MIT.[28]
In this study, a group of 54 participants was asked to write an essay without tools, using a traditional search engine, and using ChatGPT. This initial study is part of a study exploring the cognitive effects of using AI writing tools in education.
These initial indications are cause for concern and demonstrate the need for additional attention to the well-considered integration of these tools into education and society.

An example of increasing deployment is the use of generative AI in chatbots for public communication. These types of chatbots increasingly utilize large language models, which are then tailored to the specific information an organization wants to provide in its public communications. In this way, the chatbot's communication becomes an interplay between the characteristics of the underlying language model and the organization's specific information and instructions. The organization's provision of information is therefore partly influenced by developments, such as updates, in the underlying language model. It is also difficult to prescribe how the chatbot should communicate in all circumstances.
This presents new challenges. In the coming period, AP will further explore the use of generative AI for public communication.

1.5 AI and energy consumption

The huge amounts of data and computing power can pose problems for the importance of a clean, healthy and sustainable environment.[29]Training new systems requires increasingly more energy, which puts increasing pressure on this importance. Energy consumption doesn't stop after training an AI; using AI requires at least the same amount of energy. Training an AI system doesn't automatically mean its energy consumption decreases. 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 are fully committed to their own (nuclear) energy supply. The World Economic Forum states that the increase in energy consumption calls for an acceleration of the energy transition, in which we must use sustainable solutions.[31]To meet energy needs, large AI companies are developing their own infrastructure and facilities. For example, there is increasing interest in nuclear energy.[32]
Microsoft has announced a $1.6 billion agreement to generate power from a nuclear reactor for its AI applications, while Google and Amazon also have nuclear energy agreements to support their AI efforts.[33]
Besides the major impact on the environment and sustainability, the development of AI also carries the risk that essential (energy) infrastructure will end up in private hands, increasing social and individual costs.

Although precise figures are lacking, water use for AI is also increasing rapidly. Data centers use large amounts of water to cool AI hardware and prevent overheating. Microsoft manages a large part of the server infrastructure on which ChatGPT, among other things, runs. Since ChatGPT's arrival in In 2022, researchers estimated that Microsoft's water consumption increased by 34% in 2022 compared to the previous year. Writing a single 100-word email using GPT-4 uses 519 milliliters of water.[34]

Due to the high water consumption of data centers, water shortages may arise in areas with less water available.[35] [36]In the US, data centers are often located in areas where there is already some degree of water scarcity.[37]It's important to place more emphasis on renewable energy sources and sustainable AI systems. Green AI focuses on using AI to solve sustainability issues and on optimizing AI to make it less demanding.[38]

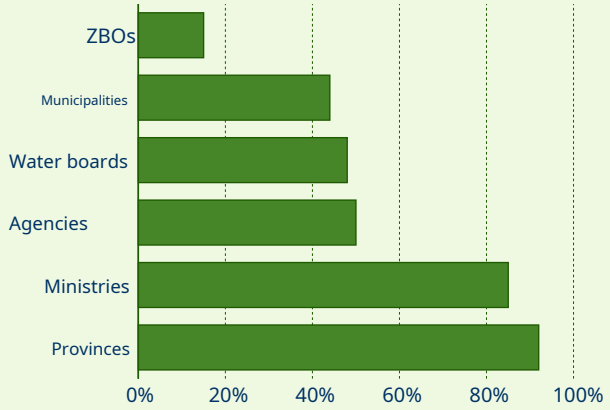
1.6 Mapping Algorithms and AI Systems

The completion of the Algorithm Register for the Dutch government is progressing steadily, but most government organizations have not yet registered any algorithms. Since the launch of the Algorithm Register for the Dutch government in 2023, approximately 1,000 algorithms have been registered. The municipality of Amsterdam leads the way with approximately 60 algorithms and the Dutch Customs Administration with around 50. At the same time, most government organizations still haven't registered a single algorithm. Fewer than one in five independent administrative bodies has included at least one algorithm in the register. More than half of all municipalities have not yet registered anything, as shown in Figure 1.4.

FIGURE 1.4 | DEVELOPING ING ALGORI TMERREGISTRAT I ON DUTCH GOVERNMENT

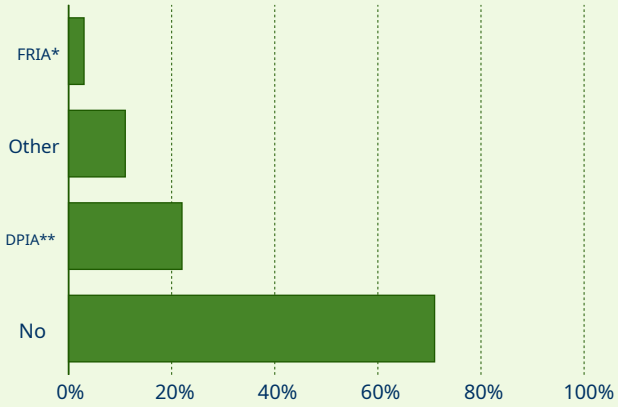
De meeste overheidsorganen hebben nog geen algoritmes geregistreerd...

% Organisaties met minimaal één registratie in algoritmeregister



... en voor de meeste algoritmes is nog geen impacttoets uitgevoerd.

% Algoritmes waarvoor wel of geen impacttoets is uitgevoerd



* Fundamental rights impact assessment (grondrechtenbeoordeling)
** Data protection impactassessment (gegevensbeschermingseffectbeoordeling)

Source: Algorithm register (algorithms.overheid.nl), reference date June 11, 2025

While it is possible for organizations to not use any algorithms at all, in many cases this is unlikely... Knowledge building about algorithms and AI within organizations is still in full swing. And algorithms and AI systems are not always easy to recognize as such. It is important that organizations receive support in this process and that they can be challenged externally on their algorithm registration and any potential lack thereof. In any case, it remains difficult to assess at this time how far organizations have progressed with their algorithm registration.

Algorithm registration. The Scientific Advisory Council for the Police concludes that much is happening in the field of data and AI, both within and outside the police organization.[39] The advisory board notes that "it is difficult to provide a complete overview of this, partly because developments are moving quickly and there is little coordination between the numerous initiatives in various places within the organization." With that in mind, it is difficult to indicate how this compares to the current number of six registered algorithms by the National Police (see also box 1.1 on algorithms and AI at the Police).

... It is therefore important, if this situation arises, to also record that a government organization declares that it does not use algorithms. Within the central government, this can be based, for example, on the letters sent to the House of Representatives by each ministry regarding the progress of algorithm registration, which also state how many algorithms and AI systems have been identified within organizations.

Another point of attention in the algorithm registration is that government organisations have carried out a Fundamental Rights Impact Assessment (FRIA) for less than 5% of the algorithms. Figure 1.4 shows the extent to which impact assessments have been conducted for algorithms. An FRIA can be conducted in various ways using different formats. For example, by changing the format of the *Impact Assessment Human Rights and Algorithms* (IAMA). Ideally, the results of such an assessment should also be made public, so that stakeholders can also read how the impacts on their fundamental rights have been assessed. This underlying documentation has so far been barely, if at all, included in the Dutch government's algorithm register.

Under the AI Regulation, conducting a FRIA will become mandatory for government organizations using high-risk AI systems... Every government organization must perform a FRIA before first deploying a high-risk AI system. This applies to systems used in biometrics, education, labor, public services, law enforcement, migration,

asylum and border control, justice, or democratic processes. This assessment is updated as needed during the use of such a high-risk system.

... And government organizations then inform the market supervisor of the results of the FRIA before deploying the system. The AI Office, part of the European Commission's European AI oversight and coordination team, will develop a template in the coming period that can be used for the FRIA (Finance Information Modelling Act). The FRIA reporting requirement will help market regulators gain up-to-date insight into the use of AI systems within government and the associated assessment of fundamental rights risks. A similar requirement will apply to lending and premium setting within the financial sector.

Box 1.1

Case: Use of algorithms and AI by the police

The use of algorithms in policing continues to require attention. Police work is increasingly driven by data, and the question is what this new context means for the implementation and organization of police work. A report from the Scientific Advisory Council for the Police examines the various challenges of data and AI applications in the police force.[40]
According to the advice, decision-making about AI should become part of the broader governance of the police organization. Ethical, legal and
Social aspects must be structurally incorporated into the development of AI applications. Active transparency must become the norm. AI literacy must be shaped as an "integral basic skill" to develop a "critical digital mindset," with an eye for (conflicting) public values. The council also states that AI applications that can improve the police's relationship with citizens should be explored, potentially also to steer the public debate surrounding the use of AI by the police in a positive direction.
Furthermore, more empirical research is needed on the effectiveness of AI deployment by police, as well as a normative assessment of its desirability and explainability. Finally, the council recommends discontinuing the use of systems that predict individual behavior.

Certain predictive AI systems for criminal risk assessment are prohibited under the AI Regulation. The Dutch Data Protection Authority (AP) points out that, according to Article 5, paragraph 1, subparagraph d, of the AI Regulation ("Prohibition D"), AI systems may not be used to assess a person's risk of criminal behavior if this is done solely on the basis of profiling or personal characteristics. This aligns with the Council's recommendation not to use AI systems that attempt to predict individual behavior. In February, the AP issued a "Call for Input" in response to this prohibition. This call explained specific criteria for these prohibited AI systems and posed questions for additional input.

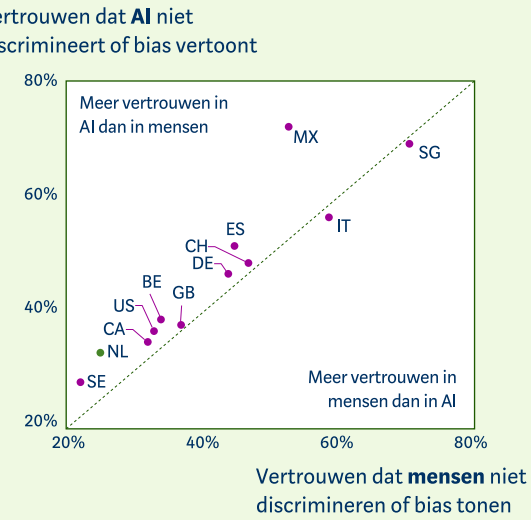
1.7 Discrimination risks in algorithms and the design of human testing

In 2025, the Dutch will be very aware that not only people but also algorithms can discriminate against groups of citizens... The Dutch, along with the Swedes and Canadians, have relatively little confidence in AI's ability to act fairly and without discrimination or bias. Only 33% of Dutch people believe that AI systems are free from bias. In other countries, such as Germany (47%), Spain (52%), and Mexico (73%), this percentage is higher. Strikingly, trust in humans in this regard is even lower: only 25% of Dutch people believe that humans themselves do not discriminate or exhibit bias.

There appears to be a clear correlation: in countries where people have little trust in people regarding non-discrimination, trust in AI systems is also low. Yet, in most countries, people consider AI to be slightly more fair than other people. (See Figure 1.5).[41]

... There is also a strong self-awareness among Dutch people that people show bias and (unconsciously) discriminate.A 2023 European Commission study shows that the Dutch are relatively highly aware of their own bias against others. In 2023, 26% of Dutch people reported having consciously or unconsciously discriminated against another person in the past 12 months. This is almost four times the European average of 7%. After the Netherlands, the highest percentages are achieved in Sweden (19%), Denmark (16%), and Romania (11%). All other Member States report below 10%.[42]

FIGURE 1.5 | TRUST THE GUIDE AND HUMANS AND SHOW NON-DISCRIMINATION AND BIAS



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

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

These findings demonstrate the importance of reducing both algorithmic bias and human bias in processes that affect people. The strong awareness of both these issues offers the Netherlands a good starting position and support for taking action in this area. The benefits scandal, in particular, has made it clear to the Dutch that institutional bias can occur in research and assessments by a government organization.[43]This institutional bias is further reinforced if risk selection takes place on the basis of discriminatory algorithms, as was also the case in the childcare benefits scandal.[44]

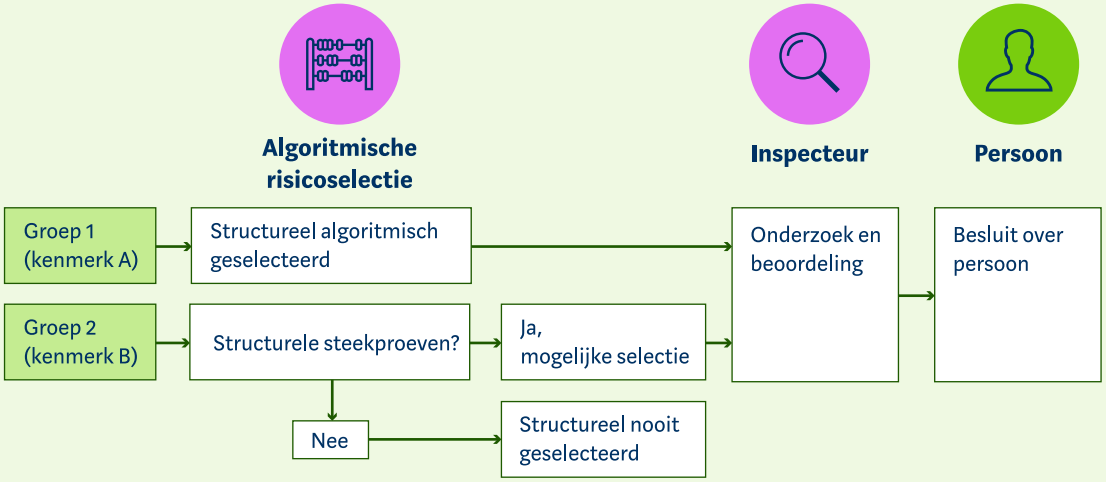
To minimize the risks of bias and discrimination, science points to the importance of properly designing the interaction between humans and algorithms. Algorithm biases pose an additional risk: they operate systematically, can affect everyone in the same way, enshrine historical prejudices, and are often difficult to explain or understand. These biases are in addition to human biases, although their forms can vary.[45]

When misdesigned, the interplay between algorithms and humans can actually exacerbate discrimination and bias. Consider the example of profiling and selection algorithms that pre-select fraud detection by inspectors. Several studies confirm the risk that inspectors, based on algorithmic recommendations, may act more inconsistently and biasedly.[46]
At the same time, algorithms and humans can actually complement each other when properly designed. A key goal is to align inspectors and algorithms so that inspectors have precise, yet not blind, confidence in an algorithm's output. This ensures that inspectors and algorithms complement each other. This requires clear, supporting explanations of how the algorithm selects cases and assesses risks. Consider, for example, displaying uncertainty margins for each risk selection, allowing inspectors to better assess the strength of a signal.

In May 2025, a motion was passed in the House of Representatives requesting the Dutch government to adopt the principle that citizens are assessed "blindly," for example, in fraud detection.
The idea here is that if an inspector has no knowledge The inspector cannot be influenced by the algorithmic prediction, given the reason why an individual file needs to be examined. The motion thus aims to prevent tunnel vision and bias in human assessments.

FIGURE 1.6 | STRUCTURAL STICKS AND RESISTANCE ARE NECESSARY TO PREVENT DISCRIMINATION AND RISK, ALSO BLIND CONTROL

Structurele toevoeging van steekproeven is cruciaal om bias in de gehele keten te detecteren, ook als inspecteurs "blind" dossiers beoordelen.



Explanation: In this example, the algorithmic selection model exhibits undesirable discrimination toward group 1 (based on characteristic A). This group is routinely checked, 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 examined have been selected by an algorithm, the risk of discrimination throughout the chain can only be reduced by enriching the files for inspectors with samples that also include group 2. This can reveal false negatives (files that should have been examined 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 important here: (i) also 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 is explainable and can be challenged. The creation of a risk assessment for an individual, for example, during a fraud investigation, ultimately comes down to a combination of algorithmic (pre)selection and subsequent human review. Blind file reviews by inspectors cannot eliminate discrimination and bias at the individual level that has occurred at the previous stage. By enriching the process with a random sample as standard, a basis for periodic audits is created at the overarching level. These audits can then regularly verify whether the algorithm—and the entire process—has

– bias or discrimination occurs (see Figure 1.6). This can ultimately reduce bias and discrimination. If inspectors initially have to perform a blind assessment, it is necessary to add files based on a random sample. Otherwise, inspectors know in advance that each file has already been pre-selected based on the algorithm and therefore assessed as "risky."

Even with a blind assessment, inspectors must be able to (i) check the algorithm and (ii) give citizens the opportunity to challenge the risk selection or to have the selection explained to them. Some insight for the inspector into the results of the algorithmic risk selection is therefore necessary. To put it concretely: without this information, an inspector, for example, if contacting a citizen, cannot explain why a person has been selected for an investigation. It is important that

Inspectors, even during blind inspections, receive a clear and useful explanation of the algorithmic risk selection process at the right time. Furthermore, inspectors must be sufficiently AI-literate and skilled to assess how the algorithm arrives at its selection. The order in which data is presented to an inspector is important, as this can influence subsequent decisions.[47]This could ultimately lead to the tunnel vision and biases addressed in the parliamentary motion. The Dutch Data Protection Authority (AP) recommends viewing "blind assessment" as the order in which information, particularly an algorithm's risk assessment, is presented to an inspector. Blind assessment means that inspectors only learn the algorithm's risk assessment after they have first formed their own opinion.

Box 1.2

Case: Facebook's advertising algorithm discriminated against job postings

On February 18, 2025, the Netherlands Institute for Human Rights ruled that Facebook's recommendation algorithms discriminate on the basis of gender.[48]
The Institute is authorized to rule on violations of equal treatment law in the Netherlands. The Clara Wichmann and Global Witness foundations filed a complaint with the Institute about Facebook because research by Global Witness itself showed that job postings featuring stereotypical male and female professions were primarily shown to the same group. For example, a job posting for a receptionist was shown to women 96% of the time in 2022 and 97% in 2023, while a job posting for a mechanic was shown to men 96% of the time in those same years. The algorithm can therefore promote stereotyping, hindering women who, for example, want to become car mechanics in their search for a suitable job. The Institute considers the research sufficient to establish a presumption of indirect discrimination.

Facebook has failed to refute or justify the discriminatory and stereotyping effects of its algorithm. Facebook has acknowledged the possibility that gender has been given more weight in the advertising algorithm due to the liking and clicking behavior of the platform's users. The Board considers the lack of an explanation for Global Witness's research findings to be Facebook's fault. Facebook also fails to provide an objective justification for the discriminatory distinction. The Board believes that Facebook, as a social media platform, is responsible for properly monitoring the algorithm's operation and must investigate stereotyping resulting from the use of the advertising algorithm. Facebook has been unable—or unwilling—to concretely demonstrate whether, and if so, how, it specifically monitors and investigates this. This ruling is typical of recent judicial decisions in which the operation and impact of an algorithm could not be explained, such as in the SyRI case.[49]Lack of transparency in court works against the person responsible for the algorithm.

2. Policy and regulations

QUICK TO THIS PART

Global developments in algorithms and AI continue to demand action for greater transparency and accountability. Furthermore, better policy and regulation remain necessary. This chapter describes how the challenges, opportunities, and risks of AI are being addressed in policy and oversight at the global, European, and national levels. First, we consider the Court of Justice's clarification regarding the transparency and explainability of algorithms. Next, we address the geopolitical challenges surrounding AI and how the United States, China, and the European Union are addressing them. Partly in the context of the AI Regulation, Europe is focusing on the importance of innovation and the need for adequate protection of fundamental rights. This is reflected in the development of guidelines, standards, and the regulatory sandbox. Progress in recent months demonstrates that the EU is continuing to take steps toward a more concrete framework for the responsible use 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 use of algorithms and AI leads to automated decision-making, people must be able to understand how the system reached that decision. New European case law clarifies when the provision of information in automated decision-making meets GDPR requirements.
These requirements concern transparency in the use of algorithms and AI in decision-making processes concerning individuals. In February 2025, the European Court of Justice issued a preliminary ruling in a judgment concerning automated (algorithmic) creditworthiness assessment (Case C-203/22, Dun & Bradstreet Austria GmbH).[50]The ruling concerns a case in which a phone subscription with a monthly fee of 10 euros was rejected on the grounds of insufficient creditworthiness. In this case, an Austrian court had previously concluded that Dun & Bradstreet had not provided meaningful information about the underlying logic of the credit rejection. The new ruling provides greater clarity on the circumstances in which meaningful information is sufficient.[51]

Organizations that use algorithms and AI in their automated decision-making should neither overcomplicate nor oversimplify the explanation. The Court emphasises that individuals have the right to an explanation of the logic and data underlying the result. To make this information useful and enable individuals, for example, to challenge the decision, the information about the decision must be concise, transparent, comprehensible, and easily accessible.[52]
This requires a tailored approach. One extreme is simply stating that an algorithm has been used, but this is insufficiently comprehensible. The other extreme is a detailed description of the entire algorithm, but this is insufficiently concise and, in some cases, impossible without sharing proprietary information.

The golden mean in explainability depends on the specific situation.A practical example could be that, in the case of automated rejection of an application, a person is given an explanation of how specific changes to the data would affect the outcome of the decision. Such an explanation could be, for example: if a person's gross monthly salary increases by 500 euros, the same loan application with the same terms will be approved. However, in practice, this presents a challenge: such an explanation can be time-bound (current explanations do not always guarantee future results) and, with some algorithms and AI systems, numerous parameters can have a decisive influence on the outcome. A question that policymakers and organizations with practical experience will therefore have to consider is whether in such a case insight should be provided into all possible ways to achieve approval, or whether a single method is sufficient. See Figure 2.1 for a schematic representation.

Organizations that use algorithms and AI in their automated decision-making must have sufficient

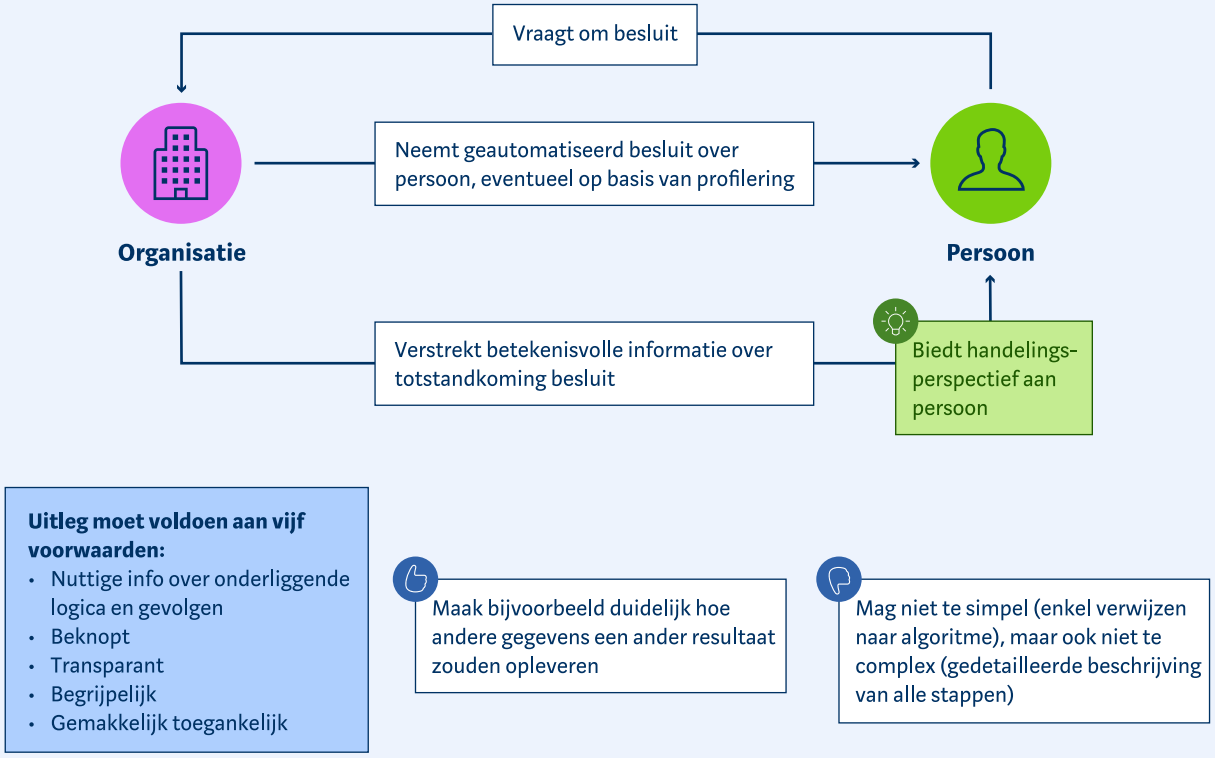
pay attention to their explanation. After all, to provide a meaningful explanation of the system's decision-making process, the decision must be logically deducible from the algorithm's operation. This can be difficult with overly complex algorithms. However, if this explanation is lacking, it also hinders the right to object or to Possible correction of the decision. It is then insufficiently clear what someone needs to change to get the organization to make a different decision. Moreover, the person cannot verify whether the decision was made carefully. The consequence of this explainability requirement is that a developer of An algorithm or AI system must consider the need for human autonomy from the outset. Individuals about whom an algorithm or AI makes an automated decision must be given an explanation.

This explanation also provides further clarification in light of the AI Regulation. The Court's preliminary ruling clarifies the application of the right of access to automated decision-making, as laid down in the GDPR.[53] In addition, the AI Regulation provides the right to explanation for individual decision-making.[54]In short, this right means that individuals affected by a decision made by a high-risk AI system must receive clear and relevant information. The explanation must address the role of the AI system in the decision-making process and the key elements of the decision taken. This closely resembles the similar provision stemming from the GDPR. The Court's decision in Dun & Bradstreet thus also clarifies how AI developers and users must design and document their systems to meet the explainability requirements for individual decision-making.[55]From the perspective of data protection supervision, the AP is working this year on further explanation of meaningful

provision of information.

FIGURE 2.1 | INTERACT I EPROF I LEARNING, DECISION MAKING AND INFORMATION PROVISION WITH J ALGORI TMES

Betekenisvolle informatieverstrekking over algoritmes biedt handelingsperspectief aan personen bij besluiten door overheid en bedrijven.



2.2 International developments

Internationally, attention is focused on geopolitical developments surrounding AI. In the global AI race, the balance of power is shifting. Primarily the United States and China are competing for a leading role in infrastructure development.

around AI. The introduction of Deepseek – which has become available as both a chat service and an open-source model - marks China's increasing 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 societal processes.

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

Since the beginning of this year, the US has publicly emphasized a new course of simplification and AI deregulation. At the same time, the US is also working on concrete regulations that resemble the AI regulation.[57] For example, through an executive order aimed at removing barriers to AI innovation and maintaining US leadership.[58] This executive order replaces the Biden administration's previous executive order, which emphasized the preconditions for deploying safe and reliable AI within the federal government. Despite the emphasis on simplifying regulations and concerns about security and protecting individual rights, a recently announced memorandum contains similar safeguards to the previous executive order. The memo *Accelerating Federal Use of AI through Innovation, Governance and Public Trust* announces requirements for 'high-impact AI', including documentation, impact assessments, testing, and human intervention capabilities.[59] It is striking that the definition of 'high impact AI' shows similarities with the AI Regulation. For example, AI that serves as the basis for decisions with consequences for access to education, housing, insurance or employment classified as high risk.[60]

China is working on a regulatory framework with a focus on more concrete standards. From September 1, 2025, AI-generated content must be clearly recognizable for users. National AI standards are being developed, and China is actively participating in the development of international standards.[61]

Globally, private investment in AI has increased significantly, up 44.5% between 2023 and 2024. Besides the US, EU member states, and China, other countries are also investing heavily. In 2024, the United Kingdom invested US$4.52 billion, Canada invested US$2.89 billion, and the United Arab Emirates invested US$1.2 billion. 1.77 billion.[62] This shows that many countries see the opportunities of AI.

Box 2.1

Legislation as a prerequisite for innovation

Although regulation and innovation are often presented as opposites, there are also strong arguments for seeing legislation as a driver of responsible innovation.

- **First of all** European legislation creates a level playing field and legal certainty. Companies know where they stand, regardless of which Member State they operate in. This prevents legal fragmentation and makes it more attractive to roll out innovative products on a European scale.
- **Secondly** Legislation prevents companies from competing on aspects where minimum standards apply, such as privacy or security. This allows them to focus on innovation in areas where it is desirable. Legislation thus steers innovation in socially responsible and future-proof directions.
- **Thirdly** Legislation increases citizens' trust in digital services. This trust supports the widespread acceptance and use of new technologies.

Finally European legislation increasingly offers scope for innovation. Good examples are the mandatory *regulatory sandboxes* in the AI Regulation. By enabling collaboration between regulators and developers, developers can innovate responsibly.

The AP also sees a clear movement towards simplification of regulations in Europe. The current European legal framework places a strong emphasis on fundamental rights and public values, such as transparency. At the same time, concerns are also emerging in Europe about the international AI landscape, and questions are being raised about the complexity of the legal framework and its impact on Europe's competitive position. This increased attention after the Draghi Report, published in September 2024. This report warned that the complex regulations disadvantage Europe compared to the US and China.[63] Recently, thirteen European Member States signed a declaration calling for increased investment in AI, the removal of barriers and the simplification of EU rules and procedures.[64]Amid these discussions, the European Commission has recently announced a number of measures. One of these is the*AI Continent Action Plan*, with the aim of making Europe a world leader in AI.

The AI Continent Action Plan focuses on promoting AI innovation in the EU. The European AI infrastructure must be scaled up to enable research and innovation for training and fine-tuning AI models. Investments are also being made to ensure high quality. Data for AI innovations. The plan also focuses on increasing AI skills and AI literacy.[65]

There is a high level of European willingness to invest in AI and algorithms. This is evident from the aforementioned European AI Continent Action Plan. In addition, the EU recently launched InvestAI, an initiative to mobilize €200 billion in investments for AI. A €20 billion fund will finance future AI gigafactories, where complex, very large AI models are trained. In the Netherlands, the government has announced its investment in an AI factory that will also become part of the EuroHPC European network of AI facilities.[66]The AI Factory aims to become a one-stop shop for AI development by functioning as a knowledge center, providing AI computing power, and facilitating data storage.

The call for regulatory simplification is resonating within the EU. But other voices are also being raised... Experts emphasize that the European digital regulatory framework is designed to foster innovation and increase trust by managing potential risks. Others point out that investment in Europe is lagging behind due to a lack of private investment. This is due, for example, to weaknesses in the Capital Markets Union and shortcomings in government support rules.[67]

Box 2.2

Platform workers better protected

The European Platform Workers Directive is an important step in protecting platform workers who are guided in their work by algorithms and AI. Consider, for example, people who deliver food or transport others via platforms. The Platform Work Directive was adopted at the end of 2024 and must be transposed into Dutch legislation in the coming period. The directive clarifies the (legal) position of platform workers and aims to improve working conditions. For example, additional rules will be introduced for the monitoring and algorithmic management of platform workers. This concerns ensuring task allocation and the assessment of platform workers, including their safety. Furthermore, the directive aims to improve transparency regarding algorithmic management. For example, works councils and trade unions must also be informed.

The rules in the directive are closely linked to other (digital) regulations, such as the GDPR, the AI Regulation, and the DSA. However, the rules also relate to regulations on a healthy and safe working environment. The directive is an example of regulations that offer additional and specific safeguards in a highly algorithmic area.

2.3 National developments

At the national level, the work of the State Secretary for Digitalization has been particularly noteworthy over the past six months, as have several motions adopted by the House of Representatives. Oversight of the Digital Services Regulation (DSA) will also begin.

In April, the cabinet published its new position on the use of generative AI in government.[68]The new position is less cautious and actually encourages the use of generative AI. The position is accompanied by guidelines designed to help government organizations deploy generative AI responsibly. They must also make agreements with suppliers, and separate terms and conditions apply. The Dutch Data Protection Authority (AP) expects this position to encourage government agencies to use generative AI more widely. While the AP believes caution is required, it also recognizes that the position and the guidelines contain many positive elements for deploying generative AI.

However, the AP emphasises that a number of preconditions for responsible use at the application level deserve more attention. This primarily concerns the preconditions for the practical use of generative AI. One example is ensuring sufficient AI literacy. It is also crucial that generative AI is viewed in a broader context. If this is not done, the use of generative AI risks (unintentionally) drastically changing existing processes. In our autumn 2023 report, we wrote more about so-called algorithm distortion.[69]

The AP also contributes to the social debate to stimulate the responsible use of generative AI. To this end, the Dutch Data Protection Authority (AP) published a consultation draft of its own vision on generative AI on May 23rd. The AP also discussed this vision with parties that develop, use, and research generative AI. In addition to facilitating the debate, the AP outlines the contours of a desired future perspective for the lawful and responsible use of generative AI.

It is also notable that the completion of the internet consultation 'Algorithmic decision-making and the General Administrative Law Act' has been further postponed.[70]This consultation ran until April 2024, and the Dutch Data Protection Authority (AP) already indicated in an earlier report that it was looking forward to the follow-up. Especially with the further digitalization of the government, it is crucial to involve the surrounding (legal) system. This way, government actions remain verifiable, explainable, and fair.

Finally, the government has recently continued to work on the development of a scientific standard for the use of models and algorithms.[71]This standard is being further developed based on work by Leiden University. The Dutch Data Protection Authority (AP) reiterates that the requirements for this must be considered in conjunction with the provisions of the AI Regulation. It is undesirable for similar requirements to be interpreted differently in different (product) standards.

On May 20, the House of Representatives adopted a motion calling on the government to do more to implement algorithm registration.[72]The motion specifically concerns the algorithms that may use risk profiling and Automated selection tools. An earlier request to publish these types of algorithms has not yet been fully implemented. This motion rightly attempts to change that.

Box 2.3

Dutch supervision of the DSA in force

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

European supervision of the largest platforms had already begun. The European Commission previously stated in preliminary findings of an investigation that TikTok violates the DSA.[73] The company allegedly failed to comply with the obligation to maintain an archive of advertisements. TikTok now has the opportunity to respond before a final decision is made. In addition, the Commission is currently Guidelines for the protection of children. An initial 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 will supervise the DSA as of February 4, 2025. The Implementation Act stipulates that the Netherlands Authority for Consumers and Markets (ACM) is designated as the digital services coordinator and supervisory authority for a large part of the DSA. The Dutch Data Protection Authority (AP) oversees the rules regarding personal data. In addition, the AP also oversees the rules regarding transparent recommendation algorithms. This supervisory task has been assigned to the AP to ensure a broad perspective for citizens on recommendation algorithms.[75]

2.4 Clarification and concretization of the AI Regulation

More than a year after the initial implementation of the AI Regulation, steps are also becoming visible towards further clarification and specification of the law. Both the AI Office and the proposed national supervisory bodies are working on initiatives to facilitate compliance with the regulation. This is being done through guidelines, the Code of Practice for General Purpose AI, and codes of conduct, among other things.

Guidelines

The European Commission published the first guidelines on the AI Regulation in 2025. The first two guidelines on (1) the prohibitions in the AI Regulation and (2) the definition of AI systems were published in February. Guidelines on other topics will follow in the coming years.

The AP recognises that the guidelines still leave ample room for further specification and framework setting. The guidelines are published as a '*living document*', which the European Commission will keep up to date and can adjust as needed. This is done, for example, based on 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 must be able to accurately assess the extent to which their AI system is used by the users of their product. Based on this assessment, they must implement safeguards to prevent prohibited use. For example, a provider of an emotion recognition system must ensure that it is not used in schools or the workplace. Furthermore, the European Commission provides more concrete interpretation of the prohibitions in its comprehensive guidelines, including examples.

The AP notes that, despite the guidelines, there is still considerable uncertainty surrounding the definition of the term "AI system".[77] This lacks clarity about whether and how a system can consist of multiple components or processes. It is also unclear whether, for example, the interface of a system also qualifies as an "AI system." There is also uncertainty about the required "inference capacity" and examples of systems that fall outside the definition. On a positive note, the European Commission does emphasize in its guidelines that the AI system definition covers both the development and operational phases of the system. This means that the use of AI technology for simpler algorithms also falls within the scope of the AI Regulation.

More guidelines from the European Commission will follow in the near future. The Dutch Data Protection Authority (AP) expects additional guidelines this summer regarding the reporting obligation for serious incidents involving high-risk AI systems. Furthermore, the AI Regulation stipulates that guidelines on the classification rules for high-risk AI systems must be available by February 2, 2026. This should not only clarify which types of AI systems fall into this category, but also in which cases an exemption applies. See Figure 2.2.

FIGURE 2.2 | TIJDLIJN PUBLICATIE GUIDELINES

Code of Practice on GPAI

A very impactful implementation of the AI Regulation is the Code of Practice for *general purpose AI*.Compliance with the code of practice is for providers of *general purpose AI* a way to demonstrate legal compliance. We discussed this in more detail in the previous risk report.[78]Unfortunately, at the time of writing this report, the final version of the Code of Practice has not yet been published. However, because general-purpose AI models will have to comply with the stricter rules of the regulation starting in August, the Code of Practice is expected soon.

Standards

European standards for the practical implementation of the requirements for high-risk AI systems are still pending. The deadline in the Commission's first standardization request (April 1, 2025) to the standardization organization JTC-21 has now passed. Furthermore, it is not yet clear when all standards will be delivered. Given the current progress, the AP recommends that AI providers begin complying with the regulation now. Based on the legal text and, where possible, with good practices. It is important not to wait for these standards. In the meantime, it is up to policymakers and supervisors to clarify what this means for compliance with the AI Regulation and its oversight, even before the requirements for the first high-risk AI systems take effect in August 2026.

Other initiatives

In addition to guidelines, codes of conduct, templates and standards, there are more initiatives to clarify the AI Regulation. The Commission has launched an AI Pact to help AI providers implement the regulation. Several webinars have also been organized over the past few months, open to everyone. These webinars provide participants with a better understanding of the regulation and its implementation. The webinars can be viewed on demand.[79]

The AI Office is working on establishing an AI Regulation Service Desk. The goal of the service desk is to support businesses and government agencies in complying with the regulation.A tender was open until May 19[80]Open to an external team that, under the guidance of the AI Office, will provide advice on questions from AI providers regarding the law. The service desk will be an interactive platform that, as a central hub, also

General information and support materials are provided. It is not yet known when the service desk will launch.

Furthermore, work is being done at both national and European level to fulfil the AI literacy obligation. The AI Office is working on a code of conduct for this purpose within the framework of the AI Pact. In addition, the European Commission recently published an FAQ. At the national level, the Dutch Data Protection Authority (AP) has issued a call for input.[81]
to collect best practices of AI literacy. Based on the responses, the AP is preparing a document with best practices. Dutch organizations can draw inspiration from this for their own AI literacy policies. The results of the survey were presented at the seminar of the
AP on June 18 on AI literacy.

Finally, the European *public buyers community* an updated version of the existing model contractual clauses has been published.[82]These have been developed to support purchasers of AI systems in the public sector. The update includes a model contract for the procurement of high-risk AI and is fully aligned with the final version of the AI Regulation. Furthermore, provisions can be adapted to meet specific needs when purchasing AI without high risk. An explanation of how to use the provisions is also provided. Model contracts are useful because it's important to have the purchasing conditions in order when purchasing an AI system. For example, you need to be clear about what happens to the data processed by the AI system and how rights to that data are regulated.

2.5 National developments AI regulation

In March, the AP, together with the National Inspectorate for Digital Infrastructure, published a proposal for the Dutch implementation of the *regulatory sandbox*.[83]
This proposal, developed in collaboration with various supervisory bodies and ministries, outlines the desired principles and process design of the sandbox. The goal of the proposal is to establish a solid foundation for further collaboration and coordination. The final sandbox will launch no later than August 2026. A pilot program was conducted to develop the proposal, which included questions from various organizations regarding the AI Regulation. Discussions were also held with stakeholders from the Dutch AI ecosystem.

The design proposal describes how the Dutch sandbox can contribute optimally to legal certainty and innovation. To this end, it is important that all relevant supervisory bodies under the AI Regulation actively participate. This allows access to the sandbox to be arranged through a single point of contact. This prevents AI providers from having to figure out which supervisory body to contact themselves. Moreover, this approach contributes to a consistent interpretation of legislation and regulations by the various supervisory bodies. Finally, this approach allows for the coherence of related regulations.

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 the interpretation, testing or validation of the law. Because supervisors are not in

To meet all needs, the sandbox must connect well with other initiatives, such as AI factories, Testing and Experimentation Facilities and EDIHs.

In response to the above proposal, a motion was adopted in the House of Representatives on 20 May to prioritise the development of the regulatory sandbox. The motion calls on the government to ensure that this is available by the first quarter of 2026. The Dutch Data Protection Authority (AP) welcomes this call and is committed to launching a sandbox as soon as possible. The AP is working with the various government departments to make this possible.

Box 2.4

AI, Privacy and Data Governance: The OECD Approach to Trustworthy AI

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

AI is rapidly changing how societies use and share data, unlocking new opportunities for innovation. But it also raises critical questions about privacy, trust, and responsible data management. The OECD (Organization for Economic Co-operation and Development) is leading the way in shaping international policy frameworks to ensure that human rights and democratic values are respected in the development and application of AI. In 2019, the OECD established the world's first intergovernmental standard for AI – the OECD AI Principles.
– which were updated in May 2024. The AI Principles have been adopted by more than 47 countries, including major economies and international partners. They provide a blueprint for trustworthy, human-centric AI and support national and international policy frameworks.

Policy instruments to promote trustworthy AI

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

Key tools include the Global AI Initiatives Navigator (GAIIN), a live repository of over 1,300 AI policy initiatives from more than 70 countries and intergovernmental organizations, featuring interactive visualizations of global AI trends. The Policy Observatory includes practical tools such as the AI Incident 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 providers in integrating robust and trustworthy practices throughout the AI system lifecycle. The AI Wonk blog further contributes to this work by providing a platform for experts to share insights on how to best shape trustworthy AI policies.

Expert involvement in priorities

The OECD.AI and Global Partnership on AI (GPAI) expert community comprises experts from government, industry, academia, and civil society. The community supports the implementation of the OECD AI Principles and informs the Policy Observatory through dedicated expert groups. These expert groups define key priorities and provide a platform for discussing opportunities and challenges in AI policy.

The expert groups for AI Incidents and for AI, Data & Privacy focus on key issues such as understanding the risks associated with the development and adoption of AI systems. They also investigate how privacy and data protection contribute to trustworthy AI.

Defining, reporting and monitoring AI incidents

With the rapid development and adoption of AI systems, the associated risks are already beginning to manifest. Understanding these events and their implications has become a priority for policymakers. In February 2025, the OECD published a Common Reporting Framework for AI Incidents, which provides a flexible structure for reporting and monitoring AI incidents. The framework was developed jointly with the Expert Group on AI Incidents. It contains 29 criteria for describing and reporting an AI incident, partly based on the OECD Framework for the Classification of AI Systems.
Reporting and monitoring AI incidents will enable policymakers, developers, users, and other stakeholders to identify risky systems in different contexts, gain insight into both current and developing risks, and evaluate their impact on affected individuals, groups, rights, or values.

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 impact of AI systems. It will facilitate the identification of AI risk patterns, including those related to privacy and data governance, at both the global and regional levels. It will also enhance understanding of the multifaceted nature of impacts and harms resulting from the development, use, and operation of AI systems.

Balance between innovation, privacy and data governance

AI relies on massive data sets to function effectively. Sometimes, these sets intentionally or unintentionally contain personal data. This leads to significant privacy risks, including potential misuse of personal data, bias, and a lack of transparency about how personal data is collected, processed, and shared. The OECD Privacy Guidelines provide strong foundational principles for protecting privacy and data rights in the AI era. These guidelines have been recognized as a global minimum standard since 1980 and were updated in 2013.

In 2024, the OECD established an Expert Group on AI, Data & Privacy to explore synergies and develop coordinated policy solutions within the AI and privacy communities. This initiative is based on the recognition that these communities traditionally operate in isolation, potentially leading to fragmented approaches and regulatory gaps. A key achievement of this group was the mapping how OECD Privacy Guidelines relate to the OECD AI Principles, which are intended to help policymakers and practitioners balance the opportunities of AI-driven innovation with the need to integrate privacy and data governance considerations throughout the AI lifecycle, from design to deployment.

From this perspective, the OECD is also examining the privacy and data protection implications of the mechanisms used to collect data for training datasets for AI models. 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 interacts with various intellectual property rights. In the future, the OECD will also examine the privacy and data protection implications of other relevant data collection mechanisms used to build AI training datasets.

Access to high-quality data is crucial for developing AI models, but access to this data must be balanced with robust protection. The OECD Recommendation on Improving Data Access and Sharing provides a framework for balancing open access to data with legitimate protection. Protection and safeguards, applying the principle of making data “as open as possible, as closed as necessary.” The OECD report on Improving Data Access and Sharing in the AI Era highlights how governments can improve access to and sharing of data and certain AI models while safeguarding privacy and other rights and interests.

To complement this work, the OECD actively promotes privacy-enhancing technologies (PETs) as a key component of responsible AI and data governance strategies. When used appropriately, such as *federated learning*, *homomorphic encryption*, or *differential privacy*, AI models can be trained and deployed with reduced use of—and reduced risk to—personal data. This supports privacy by design throughout the entire AI lifecycle.

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

For more information visit:
https://oecd.ai
https://oecd.ai/site/incidents
https://oecd.ai/site/data-privacy

3. AI and emotion recognition

QUICK TO THIS PART

Emotions are an essential part of human existence. They play a defining role in our daily lives: from social interaction to our perception, how we learn, and the decisions we make and how. A growing number of AI systems claim to be able to recognize emotions based on biometrics. The market for applications of such systems has seen steady growth in recent years.[84] [85] Yet, the fundamental assumptions underlying these systems are shaky. Their effectiveness is therefore questionable. Moreover, if these systems are deployed anyway, they pose risks of violating fundamental rights and public values. For example, their deployment could lead to discrimination, curtailment of human autonomy, and violations of privacy.

3.1 Emotion recognition based on biometrics

Biometric data is increasingly used to recognize people's emotions. Biometric data are physical and behavioral characteristics of people. These have long been used for verification and identification of individuals. Automated analysis of biometrics and the use of more data sources have enabled the development of new applications.[86] There are now also a growing number of systems that aim to recognize emotions. These systems analyze biometric data and attempt to recognize 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 to *how are you*.[87]

As early as the 1970s, researchers attempting 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 analyze facial expressions and voice tones. The breakthrough came with the rise of *machine learning*, which allowed AI to process large amounts of data. This made the systems more accessible and accurate. Since then, companies and other organizations have seen opportunities to use this technology for various applications.[89]

Various sectors are currently looking at or already using various emotion recognition systems. There are systems that attempt to determine a person's emotions through facial expressions. There are also systems that measure and assess skin conductance, heart rate, or voice tone. Various organizations use this technology for a variety of purposes, including marketing, customer service, job applications, education, public safety, and healthcare.
The market for monitoring stress and preventing burnout is also growing rapidly. Emotion recognition can also be used without you even realizing it. Consider the use of emotion recognition in advertising and marketing, for example, to assess and influence purchasing behavior.

The development and use of emotion recognition is growing because organizations and individuals believe it can deliver significant benefits. Organizations use recognized emotions to improve products, services, and health, or for safety. Moreover, wearables have facilitated personal use, for example, for tracking stress. Companies also recognize the importance of emotion recognition for improving customer interactions. Chapter 4 discusses various examples of emotion recognition. Several scientific articles mention the potential benefits of emotion recognition. For example, researchers describe how systems can improve healthcare by making patients' emotions more transparent. This could make anticipating patient needs easier and reduce the healthcare burden. Emotion recognition is also used to support people with autism in social interactions. Both research into emotion recognition and the market for the systems have thus increased.

At the same time, experts question the very foundation of emotion recognition systems and warn of risks of infringement of fundamental rights and public values. During deployment and development, risks arise that fundamental rights and public values, such as privacy, human dignity, and non-discrimination, are violated. But there are also doubts about two controversial assumptions underlying these 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 that aim to recognize emotions based on biometrics. This includes, for example, heart rate, voice, but also posture, scent, and DNA. Box 4.1 explains when "biometric data" is used. The types of systems in this chapter are referred to in various scientific terms.
This is because different disciplines examine emotions. In technical literature, these systems are considered "affective computing." This chapter does not address sentiment analysis: these are AI systems that infer emotions from text. Such systems are often referred to in scientific literature as emotion recognition systems.[90]

The term 'emotion recognition system' is also included in the AI Regulation[91], but this thematic study looks broader than the regulation. The chapter covers all systems that attempt to recognize emotions based on biometrics. This report also outlines various risks for infringement of fundamental rights and public values, thus providing a comprehensive picture.

The chapter also discusses stress. Stress is often described as an emotional state, rather than an emotion like happiness, sadness, or shame. However, stress is often used as an indicator of certain emotions and is therefore relevant to emotion recognition research.

Using the term 'emotion recognition' does not mean that the systems can actually recognize emotions. This chapter therefore contains serious doubts about the functioning of these systems.

3.2 Shaky basic principles of emotion recognition

A first principle is that emotion recognition systems use the same emotion classification for everyone. This assumption that the same classification applies to everyone is highly controversial. The basis of this assumption is that there are natural emotions that everyone experiences and expresses in the same way. This is also known as the "universality hypothesis." Emotion recognition systems are often trained based on Western ideas about emotion, which are not necessarily apply to everyone.[92]In reality, emotions are often complex and context-dependent.[93]Culture thus has a strong influence on how emotions are experienced, expressed, and named. The importance of context doesn't necessarily mean that people have no emotional common ground.[94]

Secondly, to build emotion recognition systems, it must be assumed that emotions can be recognized based on general and easily measurable signals. This assumption is also controversial. It is said
It's assumed that there are general (physical and physiological) signals that indicate the presence of certain emotions. Think of a smile as an expression of happiness, or a high heart rate as an indication of fear. Developers use the relationship between a measurable signal and the emotion. The signal is therefore a "proxy" for the emotion. The idea that a proxy is sufficient to attribute a single emotion is controversial.[95]It could be a signal of more than one emotion.[96]For example, a high heart rate isn't always an indication of fear, and a harsh voice isn't always an expression of anger. These can also be indicators of more positive emotions, for example. This makes emotion recognition insufficiently reliable, specific, and not universally applicable.[97]

3.3 The training and functioning of emotion recognition systems

The two controversial assumptions are reflected in the training and operation of the AI systems. The training and operation of many different emotion recognition systems are roughly similar. Figure 3.1 shows the steps of these systems schematically. This is a simplified representation of how many emotion recognition systems work.

There are different types of data, or “modalities,” that emotion recognition can use. There are systems that recognize emotions based on voice analysis. For example, speaking quickly and loudly can indicate anger or aggression. Other systems use facial analysis: emotions are recognized in the position of the corners of the mouth, eyes, and eyebrows. Other modalities include heart rate, perspiration, brain activity,

DNA and scent. Besides systems that use a single modality, there are also multimodal systems. These systems combine different types of biometric data. For example, gestures combined with heartbeat.[98]

The AI system first measures data to recognize emotions. This can be done in various ways. Cameras and microphones can capture voice, facial expression, and posture, among other things. These are well-known and frequently used applications of measurement systems. There are also wearables that measure heart rate and even brain activity, such as smartwatches, rings, and headphones.
These are becoming increasingly affordable and smaller, making them more accessible to everyone. Wearables are worn on the body. There are also remote measurement systems, such as cameras with facial recognition.

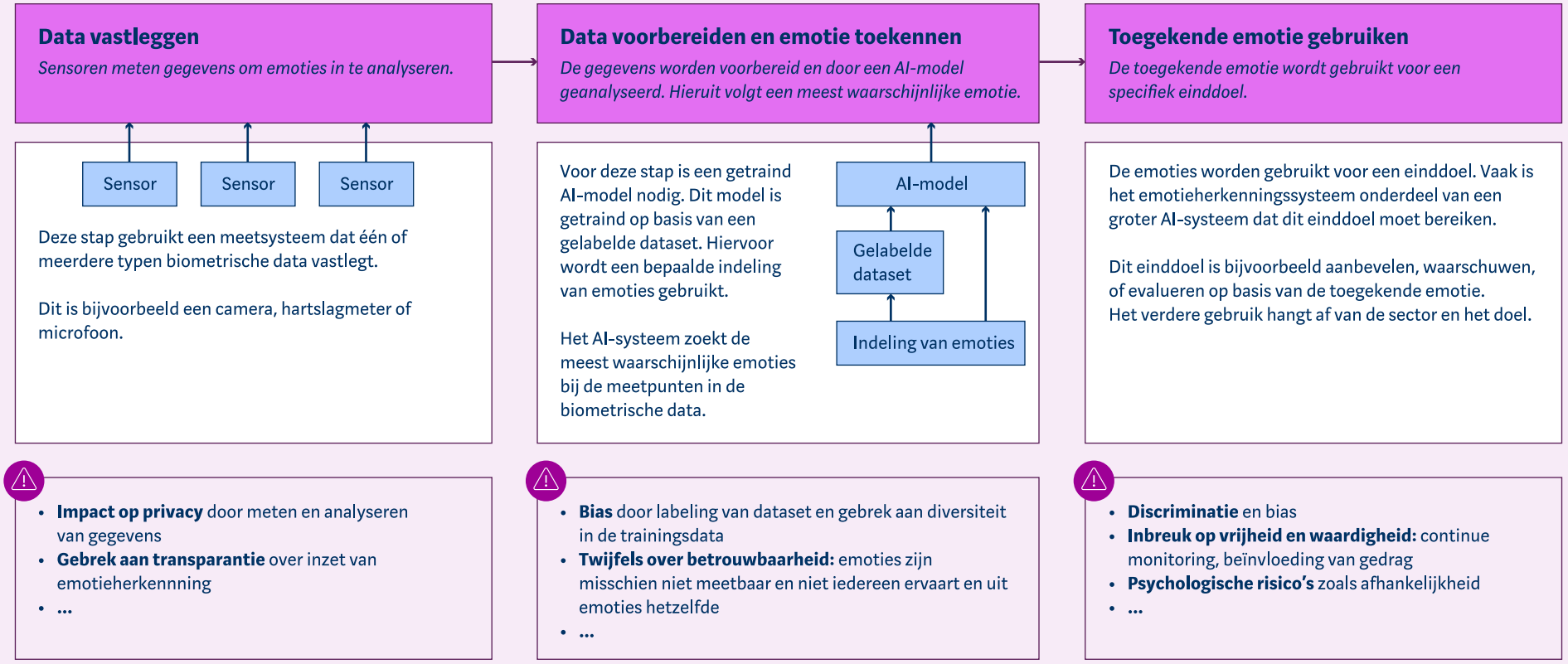
The measured data are first prepared for use in the emotion recognition system. During the preparation phase, a photo might be cropped, for example, or noise might be removed from a voice recording. Afterward, the system often selects only certain features, such as facial expressions in a photo. These features are converted in such a way that they are usable by the AI system. For example, by using a code for a raised eyebrow.[99] Only an abstraction of the data, the code, enters the further AI system.
The preparation and conversion of data is often also performed by an AI model. An emotion recognition system then essentially consists of multiple AI models.

The AI model analyzes the input and assigns the most likely emotion(s) based on a specific categorization of emotions. There are several classifications. 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 classification is widely used in AI systems because it's easy to translate into an algorithm.[101] You can also further classify emotions in a two-axis model.[102] The first dimension is whether something is experienced as positive or negative ('valence'). The second dimension is the degree of arousal.[103] For example, a positive emotion with neutral arousal is happiness. And a negative emotion with little arousal is boredom.

The AI model was trained for this purpose with data to which 'labels' with emotions were added. The way these labels are created varies by system. If the model uses facial expressions, for example, the training data consists of photos with an emotion label. Labels can be created in various ways. A test subject can indicate which emotion they are experiencing, or someone else can assign the emotion label to the data.[104] The data can be collected "in the wild" or in the lab. In the lab, emotions are sometimes elicited, for example, by showing certain images. Someone may also be asked to simulate an emotion. This doesn't necessarily have to be the emotion they actually experience. All of this determines what the system learns to predict.

Ultimately, the assigned emotions are further used for a specific end goal. An emotion recognition system is often part of a larger AI system. In such cases, emotions are used further, for example, to provide recommendations, evaluations, or warnings. This sometimes requires even more contextual data. Other times, assigning an emotion is the end goal. For example, in an app that tracks emotions or emotional states like stress. Chapter 4 discusses various practical applications of emotion recognition systems.

FIGURE 3.1 | SIMPLIFIED OPERATION OF EMOTIVE RECOGNITION SYSTEMS IN THREE STEPS



Box 3.2

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

The development and operation shown concerns emotion recognition systems that were explicitly created for this purpose. These systems are also called narrow AI. They are designed for specific tasks within defined domains. They also use pre-selected emotional classifications. Therefore, they can only recognize emotions for which they have been trained.[105]

In addition, general purpose AI systems are emerging that can also perform emotion analysis without explicit training.[106]These systems are therefore not specifically designed for emotion recognition. Analyzing emotions is an additional capability of the model. While a narrow-spectrum AI system, for example, can only recognize the emotions it has been trained to recognize, a general AI system doesn't stay within a single specific categorization. They can also be applied to tasks in various domains.

However, it is less clear how these AI systems arrive at results.[107]The analyses are not trained in a specific way, but are derived from pattern recognition on large and diverse datasets. Currently, this mainly concerns systems that analyze emotions. can analyze text (sentiment analysis). In the past five years, a growing number of systems have also appeared on the market that can analyze photos and sound. These systems can also perform emotion analysis based on these modalities.

Research into emotion recognition in text may show inconsistent results, for example because the large datasets contain many different types of data.[108]If these systems are deployed, they can lead to misleading results and bias in the outcomes. Moreover, this potential inconsistency is difficult to estimate, making the resulting bias difficult to structurally measure.
It's more difficult for general AI systems to detect or address such bias than for narrow AI. The dataset is larger and not specifically focused on emotions. Model training isn't specifically designed for this either; it's an additional skill. Therefore, safeguards will primarily focus on prompts and benchmarks on the outcomes, which are frequently circumvented. However, underlying bias in datasets remains unaddressed.

General purpose AI systems often describe outcomes convincingly, even if they are incorrect, incomplete, or otherwise misleading. For example, the answer might be an explanation of the recognized emotion, while this analysis might be incorrect. The explanation might give more weight to the outcome and lead to a more accurate prediction from the model.[109]

The trade-off between control on the one hand and average quality on the other will become increasingly important in emotion recognition. It is expected that the average quality of emotion recognition will be higher in the future for systems based on general AI systems than for narrow-AI systems.[110]
However, the above-mentioned disadvantages of inconsistency, lack of explainability, verifiability and over-confidence still remain.

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

3.4 Risks of emotion recognition

The use of emotion recognition systems and the use of their outcomes poses risks of infringement of public values and fundamental rights of citizens. These risks can arise during the various steps of AI systems' development. Development also contributes to the emergence of these risks.

This means that AI systems can discriminate due to bias in the labels of training data. Humans often label the training data for AI systems designed to recognize emotions. These labels, therefore, represent the emotions the system must ultimately recognize. Biases from the labelers may be passed on to the training data and thus become part of the AI system. This bias also affects the emotions the system assigns. So, it's not just important what the system learns, but also from whom.[111]

The systems can also lead to discrimination if the training data is not sufficiently representative. The model is less adept at selecting the correct data points and at attributing emotions to a group that is rarely present in the dataset. Datasets are often insufficiently diverse in terms of culture, skin color, age, and gender.[112]For example, studies have shown that biometric systems don't work equally well for all skin colors. Sometimes they even attribute more negative feelings to Black people.[113] Data on children and the elderly are also often lacking, while emotions and expressions differ across age groups. Finally, neurodivergent individuals, such as those with autism,[114], and persons with health problems deviate from the training data.[115]With the commitment

For example, emotion recognition can lead to someone being wrongly given a bad job assessment or being labelled as unsuitable during a job application.

Emotion recognition systems can make suggestions or specific recommendations based on their analysis. This can restrict people's freedom of choice and autonomy. Recommendations based on attributed emotions can consciously or unconsciously influence people's behavior. For example, if purchasing behavior is influenced by perceived emotions, this can undermine freedom of choice. Especially if this occurs in a manipulative or deceptive way, it violates fundamental rights.

The constant monitoring of emotions by these systems can also violate human dignity.[116]If the systems are used, constant emotional monitoring can be perceived as both annoying and intimate surveillance. This can occur, for example, at work, in education, and in (semi-)public spaces. This can increase stress or pressure people to suppress or hide their emotions.[117]Even if the use of such systems is unknown, they can undermine human dignity by reducing people and their emotions to simplistic measurements of a system.

Private use of emotion recognition systems is also becoming increasingly accessible. It's important that users are aware of risks. Wearables make it easier for people to track their own emotions and emotional states, such as stress. Apps also provide tips for reducing stress and improving well-being. Improve. These systems can also play a significant role in how people experience emotions. This can lead to dependency and excessive self-monitoring.[118]People may also start to doubt their own judgments. The AI system could come between the user and their own emotional experience. This could make it harder for people to understand or manage their own emotions independently. Provided the user is aware of any limitations, such technology can also offer opportunities and insights into emotional well-being and health.[119]

The use of biometrics by emotion recognition systems poses risks to data protection and privacy. Emotion recognition systems use personal data, such as photos, to analyze emotions. The recognized emotions are also highly intimate information and therefore privacy-sensitive.[120]It is therefore important that people know what data emotion recognition systems use and which emotions are being analyzed.

In some cases, unequal power relations can make it difficult for people to refuse to recognize emotions. For example, in emotion recognition at work or in education. The power dynamics here are unequal. This makes it difficult for employees and students to refuse the use of emotion recognition. Partly for this reason, the use of emotion recognition based on biometrics in education and the workplace has been prohibited under the AI Regulation since February 2, 2025.[121]This is related to the questionable scientific basis of such systems. Refusal of use can also occur in other areas of application.

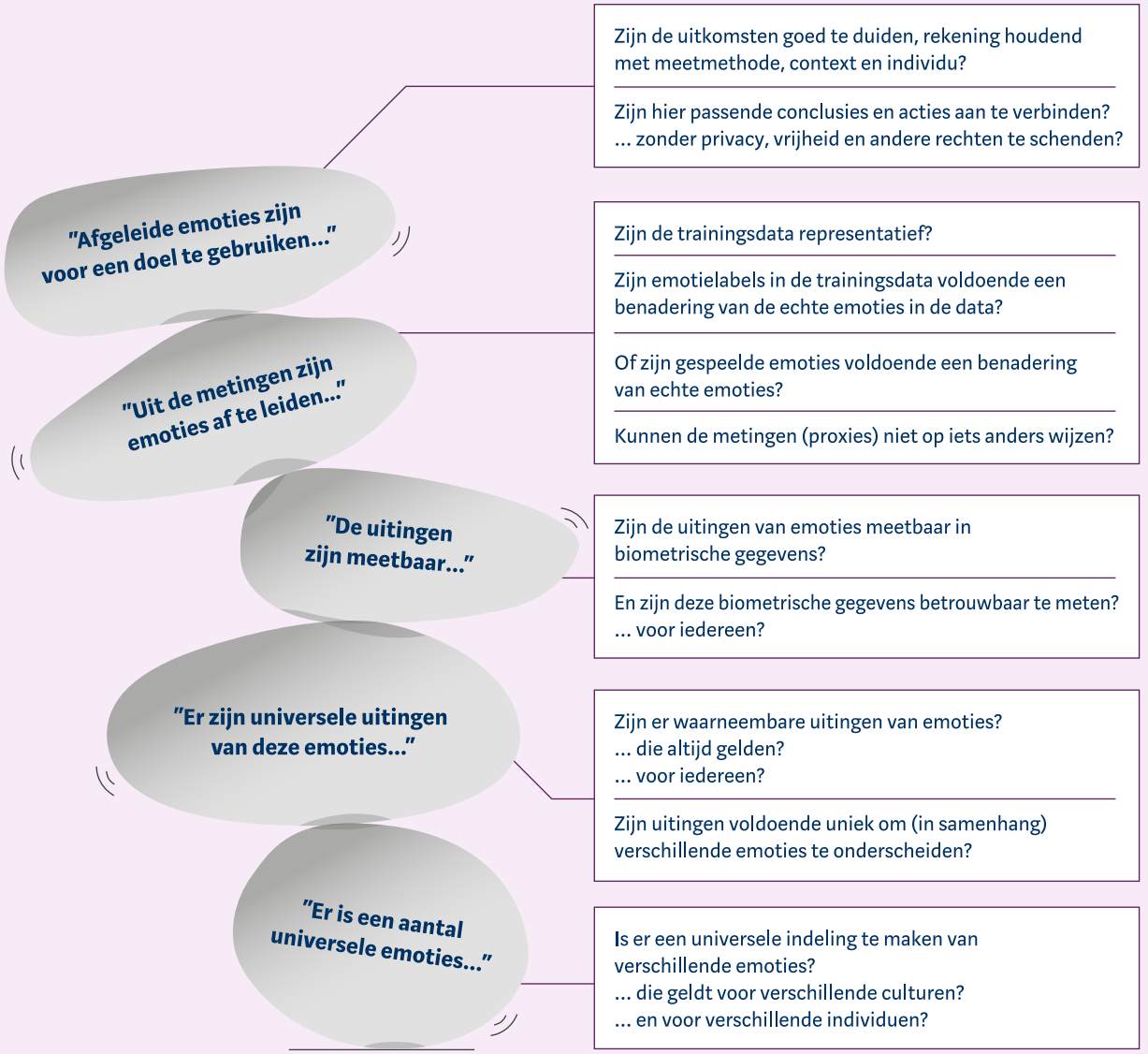
can be difficult, such as in healthcare, public spaces or certain marketing contexts.

It is therefore also important that transparency about the operation and use of such systems is in order, so that people can make informed decisions. People often don't choose to use the systems themselves. Besides the power dynamics mentioned above, there can also be skewed knowledge dynamics. Organizations that use emotion recognition systems know more than the people whose emotions are being recognized. For example, they don't know whether emotions are being tracked in the background. Recognizing emotions isn't always the end goal. A person receiving advice doesn't immediately know that their emotions are being used to arrive at that advice. Therefore, it's important to be transparent about the use of emotion recognition.

Emotion recognition systems are emerging due to 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, along with their technical operation, deployment, and use, form a precarious foundation. This is illustrated in Figure 3.2. These assumptions about emotions are controversial, but are nevertheless used in the systems. Bias can arise during development, and the deployment of these systems carries various risks. For these reasons, this technology should be used with extreme caution. The next chapter explores several application areas in more detail. It discusses other risks, concrete practical examples, and the potential opportunities of emotion recognition.

FIGURE 3.2 | BUILDING BLOCKS FOR EMOT I RECOGNITION SYSTEMS

De werking van AI voor emotieherkenning veronderstelt een wankele basis van aannames op vijf onderdelen.



4. Emotion recognition in practice

QUICK TO THIS PART

Praktijktest 1: Wearables →
Praktijktest 2: Taalmodellen →
Praktijkonderzoek 3: Klantenservice →

How do you come into contact with emotion recognition? The Dutch Data Protection Authority (AP) examined three areas of application:**wearables, language models and their use in customer service**This shows that it's not always clear how emotions and stress are recognized. Furthermore, emotion recognition isn't always effective. And although AI is regularly used, this isn't always clear to the person being analyzed. Technological progress is also evident. Devices are getting smaller, and algorithms and AI are being developed. Organizations and individuals see opportunities and increased use in the future. In practice, a risk-aware path forward is crucial, given the risks and the shaky theoretical foundation on which emotion recognition is based. Regulators and policymakers face the challenge of determining whether the use of emotion recognition is desirable in various domains. These include public spaces, marketing, healthcare, service provision, and customer contact.

Opportunities are believed to exist in various applications of emotion recognition, but there are also risks. Figure 4.1 provides an overview of several frequently discussed application areas. It includes opportunities, examples, and risks from the literature. This clarifies how the systems are viewed. The overview offers a glimpse into various applications, but is not exhaustive.

The AP looked at three areas of application to gain insight into emotion recognition in practice. The Dutch Data Protection Authority (AP) tested several systems in two application areas: personal health and generative language models. A survey also provided insights into the use of emotion recognition systems within customer service organizations in the Netherlands. These three areas are further explained in this chapter.

An overarching observation is that the use of emotion recognition in practice entails sector- and domain-specific considerations. The AI Regulation explicitly states that the use of emotion recognition systems in various domains is risky. For education and the workplace, it has even been explicitly stated that the risks are so great that the use of emotion recognition is prohibited there under the regulation. In all other cases, emotion recognition based on biometrics is a high-risk system under the regulation.

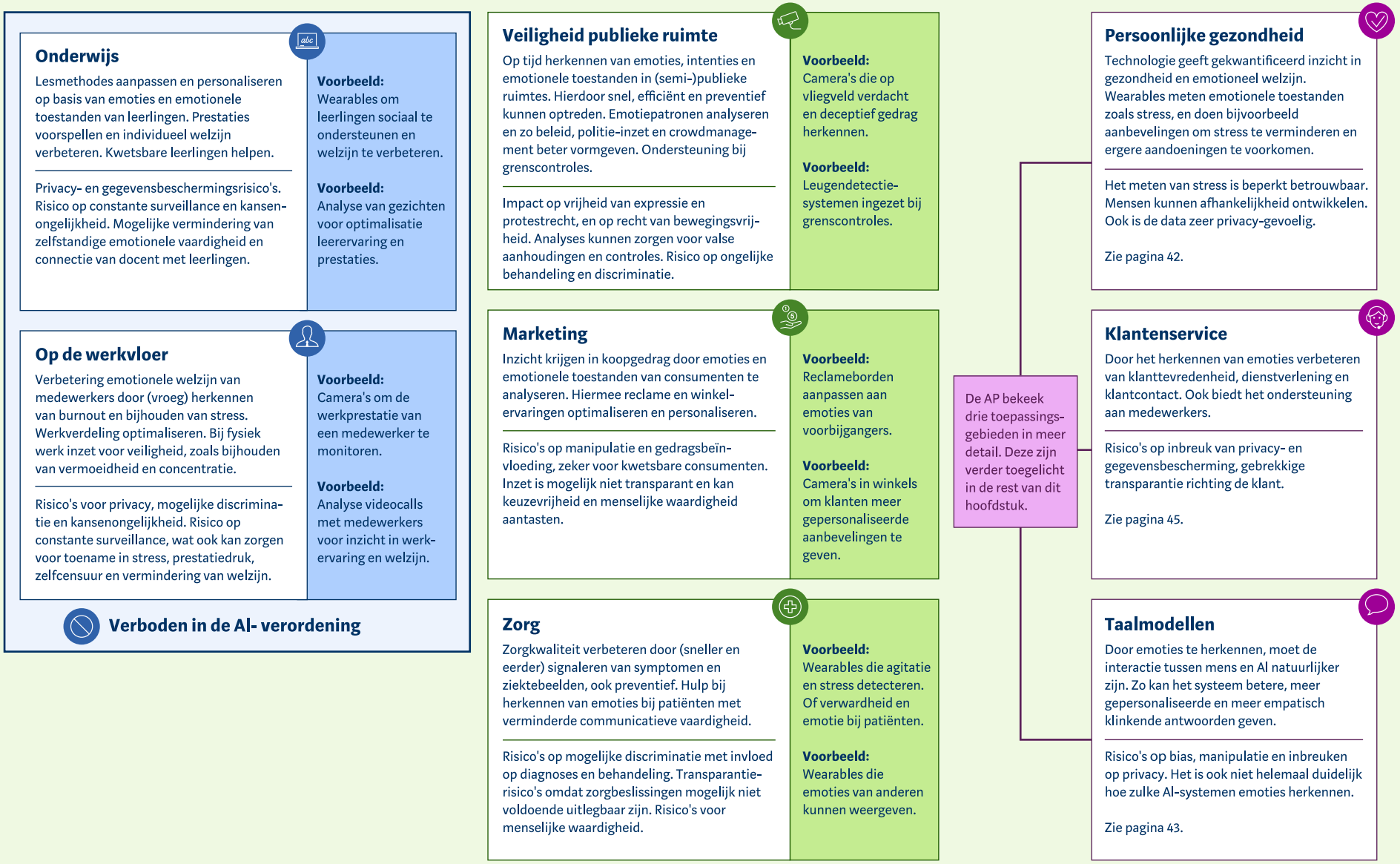
In addition to managing high-risk systems under the AI Regulation, it is important for regulators and policymakers to consider whether the use of emotion recognition is desirable, even where it is not prohibited. The primary objective of controlling high-risk systems under the AI Regulation is to ensure that these

Whether systems are safe and meet product requirements is another matter. The desirability of deploying these systems, however, is a different matter. Ultimately, it is a political decision to determine to what extent these systems are desirable and for what purposes they may be used. An analogy can clarify this: product regulation helps ensure that fireworks offered on the Dutch market are safe. But the question of where and under what circumstances fireworks may be set off involves different considerations. A similar distinction between regulation and oversight of the product on the one hand, and the use of that product on the other, also applies to emotion recognition.

Developers and users should be aware of the risks associated with each specific application. Responsible deployment of systems requires security and transparency. Transparency about this analysis and how it's conducted is essential for the individuals whose emotions are being analyzed. Furthermore, obtaining consent from the individuals being analyzed is a crucial first step for organizations to deploy the systems responsibly. This chapter discusses three practical examples of emotion recognition. But working towards responsible, conscious, and transparent deployment is also important for other applications.

FIGURE 4.1 | OVERVIEW OF APPLICATION AREAS FOR EMOT I RECOGNITION

Emotieherkenning in de praktijk: kansen en risico's in verschillende toepassingsgebieden.



Practical test 1: Wearables

Wearables have been very popular for a long time and offer more and more options. These are devices you can wear, for example, on your wrist. Using various sensors, they measure movement, heart rate, temperature, and sleep, among other things. Algorithms can reveal patterns and make recommendations.

The AP looked at three wearables that measure stress to gain insight into these functions. The test was conducted using a watch, a ring, and a fitness activity tracker. These are products available on the Dutch consumer market. All wearables display stress scores and offer suggestions for reducing stress. The accompanying apps offer exercises for this. The apps also provide insight into causes of stress, such as insufficient sleep and exercise.

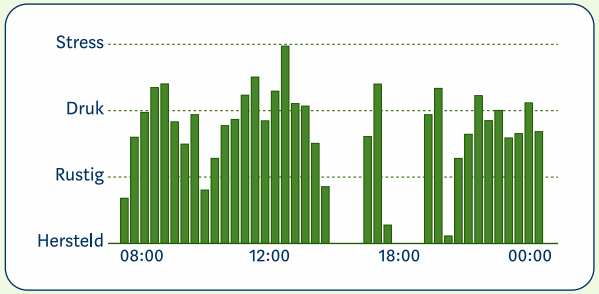
How exactly wearables calculate stress scores is not entirely clear and the underlying data is not always transparent. How the various indicators are used together to detect stress is unclear. While the variables are sometimes identified, the relationships between them are not. Furthermore, it's not always possible to consider these variables separately.

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. Therefore, the apps sometimes do not provide any data during exercise.

score again. Or perhaps a very high stress score. A high stress score can also indicate exercise.

The presentation makes stress scores look reliable and objective. Stress is displayed in an app in clear diagrams with categories and clear scores. This makes it appear reliable. It also appears objective, while the subjective side of stress is also very important.

FIGURE 4.2 | SIMPLIFIED VIEW OF HOW A WEARABLE MAKES EMOTIONS VISIBLE IN AN APP



Explanation: The app says: "You were stressed for 3 hours, so it was a stressful day."

Insights, notifications, advice and various features draw a lot of attention to the apps. This draws users to the apps multiple times a day. Stress scores can sometimes be displayed multiple times an hour. The apps provide notifications with recommendations, for example, to do exercises from the apps.

New features are also becoming available for the same device all the time, even though it is not measuring new types of data. These are new analyses based on the same input. Algorithms combine input in new ways. The hardware remains the same, the software changes. There are also features like chat and exercises that are independent of the measurements.

The different functions are part of the revenue model behind the wearables. All tested devices offer subscriptions. Without a subscription, not all features are available. Or the app provides scores but no detailed analysis. Users often have to pay for analysis and exercises to improve their health.

If the user consciously uses the wearables, they 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 them to better understand what's being measured, what the shortcomings are, and what the scores mean for them.

Practical test 2: Language models

Emotion recognition can make interactions with language models more personal. This allows answers to be more closely aligned with the user's emotions. A chatbot can thus better respond to emotions.

Several language models have gained speech and photo options in addition to text over the past year. This allows you to have a live conversation with the language model. You can also upload photos of yourself or your surroundings.

The AP conducted an exploratory test with four language models to look at emotion recognition in images and sounds. During conversations, the same texts were recited in different ways. Photos were also entered with different poses and simulated facial expressions. The systems were repeatedly asked which emotions they recognized. The main results are shown in Table 4.1.

The different models appear to convert sound into text and analyze it. One model indicated it could also analyze changes in pitch, loudness, and speed. However, this wasn't reflected in the model's responses. It seemed to rely primarily on message content. The other three language models indicated they only analyzed text, or immediately converted spoken words into text and analyzed it.

In photos of faces, three of the four models attributed the 'acted' emotions reasonably well. In their answers, they primarily mentioned eyes, mouth, eyebrows, and facial tension. Based on this, they suggested various possible emotions. Figure 4.3 shows an example.

The models were also able to analyse postures, but could only attribute limited emotions to them. They were able to identify the pose, and three models also linked it to a meaning. A pose with arms raised above the head is "enthusiastic" or "triumphant," but can also be "a request for help." The interpretation depends heavily on the facial expression recognized in the same photo.

The applications build a compelling story based on the input. The environment, clothing, and accessories also play a role in this. For example, a model noticed that photos were taken in an office. This led the model to conclude that the emotions might have been feigned. An example of such a story is shown in Figure 4.4.

How exactly emotions are assigned remains unclear. In their answers, the models refer to various features they use. However, how they use these features isn't entirely clear. For example, the models state that they "study," "interpret," or "analyze patterns in visual data" of the features.

TABLE 4.1 | MODAL TEAM TEN THAT USE AI LANGUAGE MODELS TO RECOGNIZE EMOTIONS*

Modality	Language model 1	Language model 2	Language model 3	Language model 4
Voice (audio)	not recognized/ unknown	not recognized	not recognized	not recognized
Face (photo)	well recognized	well recognized	well recognized	not recognized
Posture (photo)**	well recognized	well recognized	well recognized	not recognized

* During field test execution (April-May 2025)

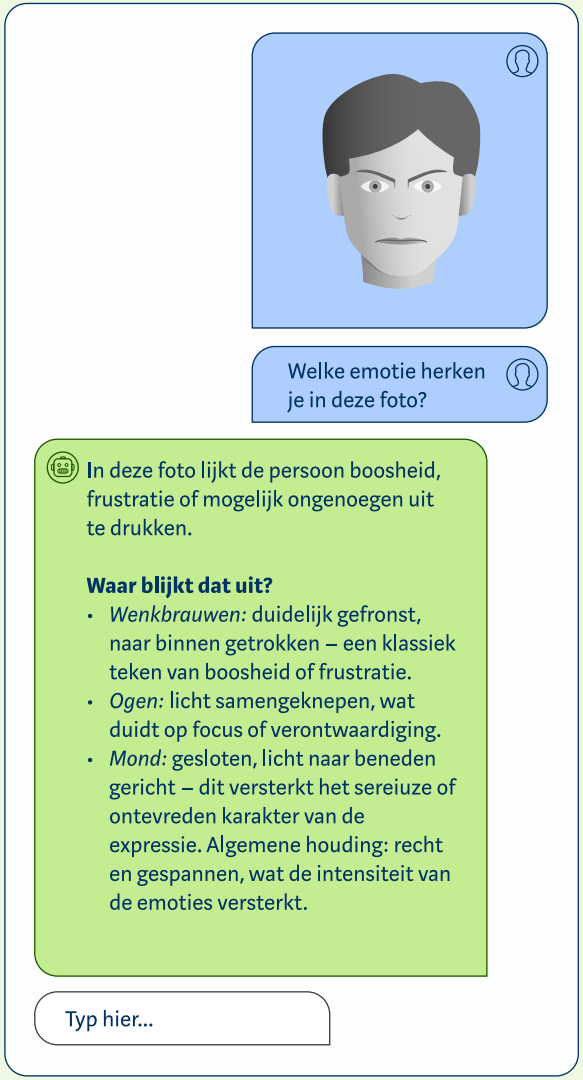
All models were able to analyze posture to some extent. Three were able to analyze it in relation to emotion, but facial expressions still seemed to dominate.

However, two models refer to controversial emotion theories, which are apparently present in training data. These theories were already mentioned in Chapter 3. They are much discussed and likely strongly present in the training data. Therefore, the models likely use these theories. See, for example, Figure 4.4. In that case, flaws and biases from the theories are passed on to the AI model.

Risks arise if such models are used further. Organizations can use the language models to build new systems. These systems can then recognize emotions, even though emotion recognition may not be the direct goal of the new systems.

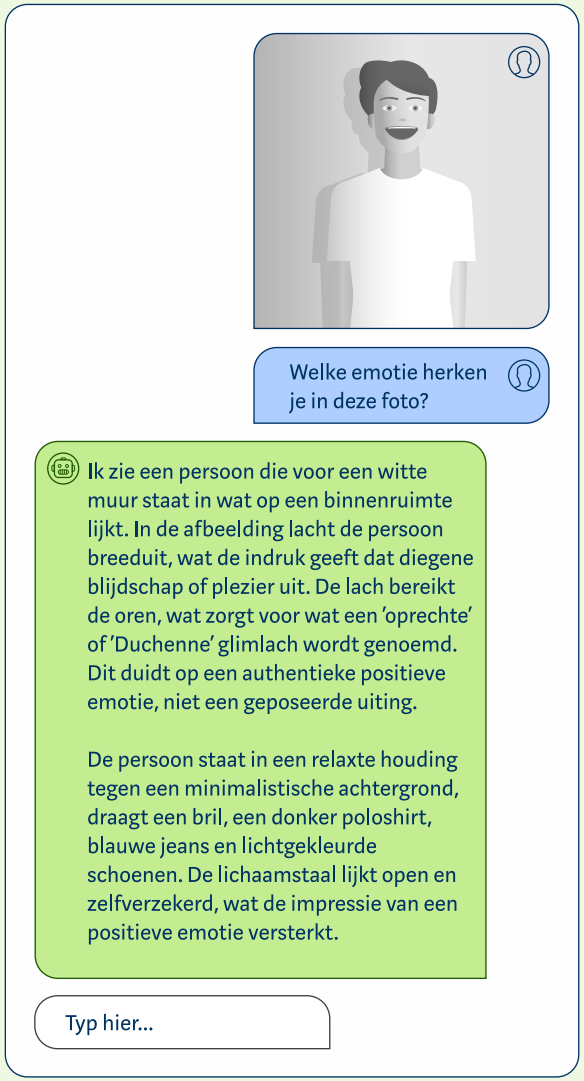
Personalization based on recognized emotions can lead to risks in private use. For example, a chatbot can have manipulative effects or be addictive. People can become dependent, for example, if they use language models for friendship and therapy. The risks of this are explained in the AI and Algorithm Risks Report for the Netherlands (RAN) from spring 2025. Using language models for these purposes makes the risks more acute for an even wider audience.

FIGURE 4.3 | EXAMPLE OF EMOTIONS RECOGNITION BY LANGUAGE MODEL



Explanation: Passage from a test with a language model, performed in spring 2025.

FIGURE 4.4 | LANGUAGE MODEL WEAVES EMOTIONS AND THEORIES IN RESPONSE TO REQUESTS FOR RECOGNIZED EMOTIONS



Explanation: Passage from a test with a language model, performed in spring 2025.

Practical research 3: Customer service

Customer service plays an important role in the relationship between customer and company.A good understanding of customer emotions can improve customer relationships. A customer service representative can better respond to a customer's emotions and thus provide an optimal customer experience. This makes customer service more personalized and often more effective. Therefore, the Dutch Data Protection Authority, in collaboration with the Customer Service Federation, conducted a survey among Dutch organizations with *in-house* and *facilities* customer service and suppliers. The goal was to gain insight into the (future) use of emotion recognition systems for optimizing customer contact.

The AP gained insight into the use of emotion recognition systems based on biometrics in customer services through a survey. About thirty organizations, both suppliers and organizations with *in-house* or *facilities* Customer service professionals provided insights into their perspectives on the use of emotion recognition in customer contact. Questions addressed the (potential) use, opportunities, and risks, as well as the expected future deployment of emotion recognition systems in customer contact in the Netherlands.

The survey among organizations with *in-house* or *facilities* Customer service shows that 45% of respondents see potential in emotion recognition for customer contact.One of the customer service organizations employs between 50 and 249 customer service representatives and already uses emotion recognition through voice recordings (see Figure 4.1). considers this somewhat effective. A smaller organization that already uses emotion recognition assesses its effectiveness neutrally. Organizations that indicate they are using these systems also indicate they are working on AI literacy. Employees receive the necessary training or education on how to use such systems.

The number of customer service organizations that indicate that they already use emotion recognition is therefore small. There's also a chance that organizations don't yet fully realize their systems incorporate emotion recognition, for example, because it's not labeled as such. Organizations may also not automatically interpret these applications as AI. This is relevant because these applications will soon fall under specific AI regulations and must still comply with GDPR requirements due to the personal data being processed.

According to respondents, emotion recognition offers various opportunities.A large proportion of respondents believe that emotion recognition can contribute to customer satisfaction and improve service quality. Organizations also see the benefit of supporting and protecting employees. A few also mention that emotion recognition can be used as a new source of customer data. The goal can be to personalize service. Moreover, emotion recognition in customer service serves as quality monitoring. conversations. One respondent questions the extent to which technology is a useful addition here. "Aren't employees perfectly capable of recognizing emotions themselves?"

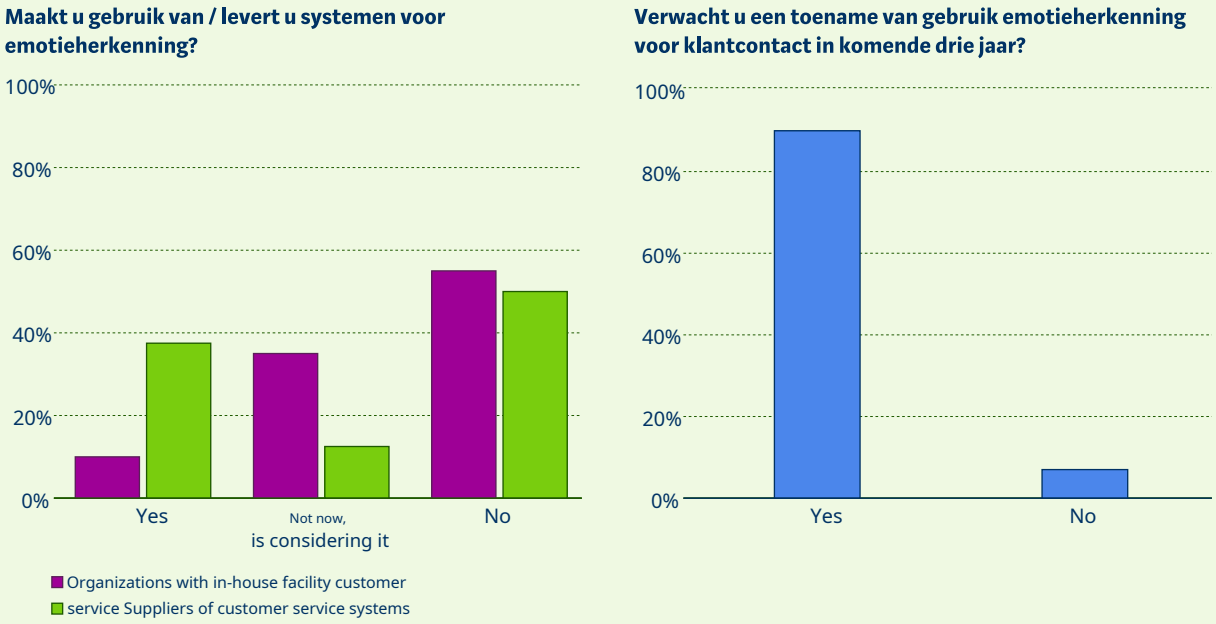
The majority of customer service organizations are also aware of the risks. Respondents indicate that the use of emotion recognition can be unreliable and can lead to bias and a sense of excessive control among employees. Several organizations are also aware of the risk of breaching customer privacy. One respondent (supplier) clarifies that there are no risks if the application of emotion recognition provides real-time support, and is therefore meaningful and untraceable. However, risks can still arise in such situations. When processing personal data or biometric data, compliance with the GDPR, the General Data Protection Regulation (AIV), and other relevant laws and regulations must be observed at all times.

Some respondents emphasize that risks are greater when applied at an individual level than when applied at an aggregated level. One respondent indicated that emotion recognition can be used to draw conclusions anonymously and at an aggregated level. They believe this can improve the quality of service. Emotion recognition can also be used at the individual level to personalize service. However, according to respondents, this entails too many risks.

At an aggregated level, it is advisable to consider the possible risks and legal requirements.

Half of customer service system vendors surveyed say they offer or are considering emotion recognition. See graph 4.1. The main driver for the suppliers surveyed is improving customer satisfaction and service delivery. It is argued that understanding customer emotions through emotion recognition systems can also contribute to faster complaint handling. Suppliers indicate that emotions are recognized both during and after customer contact.

GRAF I EC 4.1 | DEVELOPMENTS IN THE USE OF EMOTIVE RECOGNITION WITHIN CUSTOMER CONTACT



Source: Our own research among organizations with in-house or facility-based customer service and customer service system vendors. The survey was designed in collaboration with the Customer Service Federation (n=29) and conducted between April and May 2025.

Suppliers and customer contact organizations indicate that emotions are mainly measured through voice recordings. Emotions are derived from various data: voice tone, intonation, or volume, and also from factors such as pauses or silences. See also Figure 4.5.

The use of emotion recognition during customer contact is not directly indicated by respondents. Respondents provide a general message or only provide an explanation if a customer asks. Transparency about the use of algorithms and AI, and the use of biometric data, is important. This gives customers a choice about sharing their data and insight into its use. This best mitigates the risk of potentially unfair treatment due to the results of an emotion recognition system. Consent to the use of biometric data for emotion recognition and a clear explanation of its purpose will often be a first step. The explanation should be more concrete than, for example, simply a general term like "quality and training purposes."

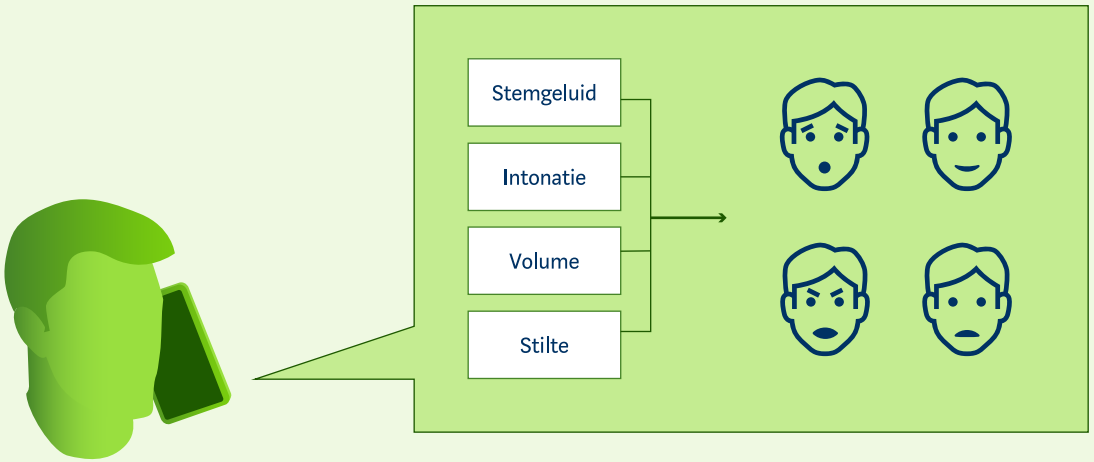
Some organizations indicate that they are wary of legal compliance risks in the event of incorrect use. Moreover, more than 80% of respondents consider establishing clear guidelines for emotion recognition systems important to very important. This indicates that the risks are understood, but also that it is important to share knowledge and provide training for the use of such systems.

At the same time, 90% of respondents expect an increase in the use of emotion recognition systems by Dutch customer contact organizations. Some also believe it's likely that various modalities will be used. A few expect restraint or a reduction in the use of the drug.

It is essential that organizations take a critical stance towards emotion recognition systems. In doing so, they must consider the shaky fundamental principles, technical operation, and associated risks of such systems. Those developing and deploying these systems would do well to clearly define the added value of the technology for achieving the intended goal.

When deploying emotion recognition systems, it is crucial to be transparent about the use and operation of these systems, and the collection of certain data. Furthermore, employees using the systems must have the necessary knowledge and skills. It is therefore crucial that organizations have AI literacy skills in place.[122]
For example, employees must understand the risks. Furthermore, organizations that use emotion recognition through AI systems must comply with the high-risk requirements of the AI Regulation.

FIGURE 4.5 | METHOD OF EMOTIVE RECOGNITION IN CUSTOMER CONTACT



Explanation: Emotions are analyzed based on various data.

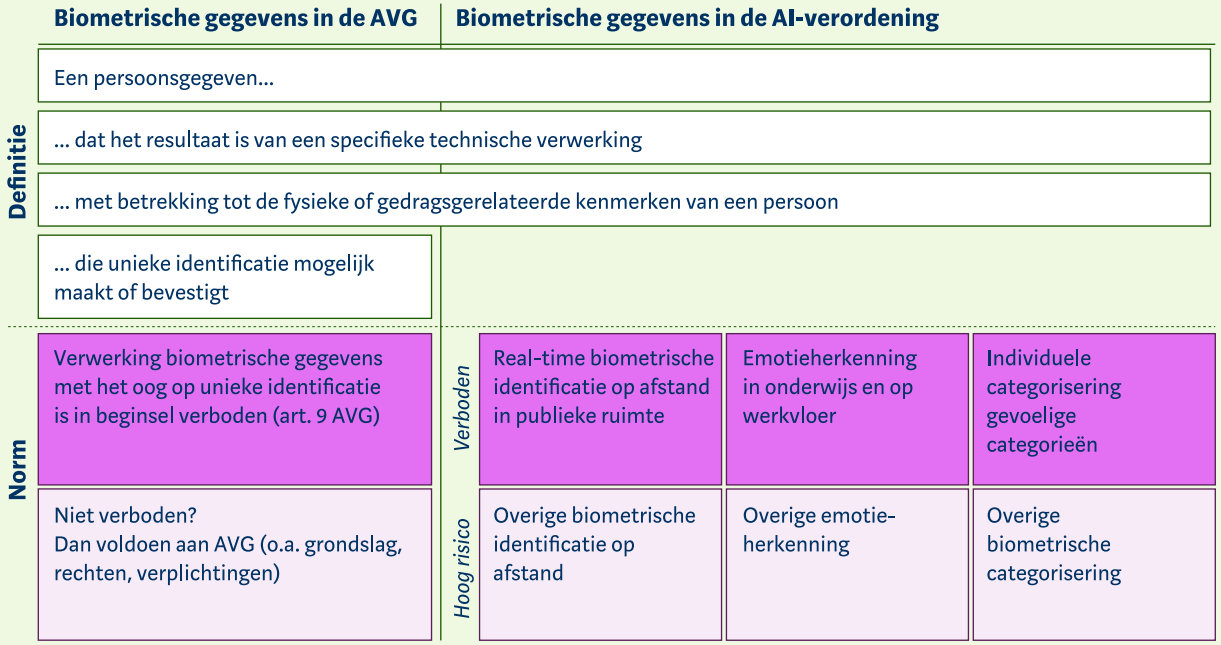
Box 4.1

Biometric Data Regulation: Zooming in on AI Systems for Emotion Recognition Based on Biometrics

The use of emotion recognition technology based on biometrics affects both the AI Regulation 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 Regulation must be interpreted in light of the GDPR. However, the responses to the AP's call for input on the ban on emotion recognition in the AI Regulation it appears that there is confusion about this among stakeholders.[125]This requires further clarification, also at European level.[126]

The AI Regulation states that biometric data should be understood in light of the concept of the same name in the GDPR.[127]Both regulations have similar objectives: the protection of fundamental rights and the promotion of the internal market. They also complement each other when it comes to the regulation of emotion recognition systems. In both definitions of biometric data, it is basically about (1) personal data, (2) which are the result of a*specific technical processing*(3) relating to the physical, physiological, or behavioral characteristics of humans.[128]

FIGURE 4.6 | BIOMETRIC DATA IN THE GDPR AND THE AI REGULATION



The GDPR also includes the requirement that the personal data must enable or confirm the unique identification of that natural person. This must therefore involve data resulting from specific technical processing relating to a person's physical, physiological or behavioural characteristics, which allow you to identify that person or confirm his or her identity.

Biometric data for the purpose of uniquely identifying a person are special personal data under the GDPR. Processing such data carries significant risks of violating fundamental rights and public values. Therefore, processing this data is afforded additional protection under the GDPR: you may only process it if specific conditions are met.[129] Biometric data are, for example, reference data in databases for facial recognition, or the analysis of measurement data about someone's 'walk', if this makes it possible to identify someone.

Identify. A simple photo of someone, or a video of someone walking, is not in itself biometric data. This is because it does not involve the technical processing of such data for the purpose of uniquely identifying someone or confirming their identity.

The AI Regulation provides protection, among other things, for AI systems that recognize emotions and categorize people based on biometric data. The rules in the AI Regulation are risk-based and depend on the intended application. For example, AI systems for emotion recognition based on biometric data prohibited in education and the workplace.[130]Also prohibited are, for example, AI systems that individually classify people into sensitive categories based on biometric data, such as political views or sexual orientation.[131]Such AI systems may not be marketed or used. At the same time, some other AI systems based on biometric data are considered high-risk. These must meet specific product requirements. Consider, for example, emotion recognition in all situations other than the workplace and education. Figure 4.6 illustrates this.

AI systems for emotion recognition fall within the scope of the AI Regulation if they use biometric data for the purpose of inferring emotions. Consider, for example, behavioral and movement biometrics or the analysis of electrocardiograms (ECGs). The use of an ECG by an AI system is not in itself the use of biometric data. However, if ECGs, possibly in combination with other data points, are analyzed in an AI system to determine a person's emotions, this constitutes emotion recognition within the meaning of the AI Regulation.[132]

Attachment

Getting started with algorithm registration

About this document

As the coordinating supervisory body for algorithms and AI, the Dutch Data Protection Authority (AP) helps organizations manage AI and algorithm risks. This appendix provides organizations with several tools to get started with algorithm registration. It should be noted that research, policymaking, and standards in the field of algorithms and AI are still in full development.

Organizations in both the public and private sectors are increasingly reliant on algorithms for all sorts of processes and applications. Registering algorithms is a good start to managing the risks associated with algorithm use.

The Dutch Data Protection Authority (AP) recognizes that many organizations consider this a challenge to get started. In this appendix, the AP provides eight concrete tools to get started with algorithm registration. The AP also offers 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 use of algorithms. It is a kind of logbook or database containing information about the purpose, the training data, and who is (internally) responsible for the algorithm. A register can be for a single organization or for multiple organizations simultaneously, for example, a joint register for the education sector. A register can also take various forms: it can be an Excel file or a publicly accessible website, such as the Algorithm Register of the

Dutch government (see box 1).

Broadly speaking, algorithm registration has two overarching goals. The first goal is to promote internal control, because the register provides insight into algorithm use.

The second goal is to promote external control by providing transparency. These goals are parallel (see Figure 1).

Objective 1: Promoting internal control of algorithms (*governance*).This includes, among other things, managing the development, implementation, responsibilities, risks and compliance with laws and regulations surrounding algorithm use. A

An algorithm register is a key component of this, as it provides an overview of algorithms and their associated development, deployment, and monitoring. Research also shows that establishing a register encourages employees within an organization to actively consider algorithm use, resulting in a "disciplinary effect."

Goal 2: Promote external oversight of algorithms (*transparency*). A lack of transparency characterizes many problems associated with the use of algorithms, as this makes it difficult to verify the outcomes and compliance with laws and regulations. Recording algorithms in an externally accessible register contributes to transparency because end-users, journalists, regulators, and other individuals affected by an algorithm can gain insight into and verify its operation. Moreover, a public register promotes knowledge sharing between organizations regarding the use and management of algorithm risks. See also Box 2 for the supervisory perspective.

FIGURE 1 | OBJECTIVES ALGORITHM REGISTRATION

Het bevorderen van interne controle op algoritmes (governance)

Het bevorderen van externe contole op algoritmes (transparantie)

A European database will be established in which new or modified high-risk AI systems must be registered from August 2026 onwards once they have been placed on the market and have been CE marked. This applies to providers of AI systems before they are released to the market and to users of AI systems in the public sector (Article 49 of the AI Regulation). This database may overlap with an algorithm register, but is not a substitute for establishing your own algorithm register. The database is for high-risk AI systems according to the regulation with a CE mark, while an algorithm register can cover the use of all types of algorithms. An algorithm register can therefore also cover algorithmic processes that do not meet the definition of an AI system according to the AI Regulation. These algorithms can still entail high risk. Furthermore, an algorithm register is, in principle, free of form. Registration in the European register is therefore not the same as registration in the Dutch government's algorithm register.

Algorithms can also be registered in a processing register for personal data. Organisations also maintain a processing register for certain high-risk processing operations, such as special personal data (Article 30 GDPR, Article 24 RGR).
A processing register is intended to account for the processing of personal data. Algorithms that do this can therefore be included.

Whether algorithm registration actually contributes to risk mitigation depends on the implementation. Registration is only valuable if measures are also taken to control algorithms, such as audit or governance measures. The quality is also

The registration itself is important. Registrations containing incomplete and unclear information can contribute little to preventing algorithm risks and incidents, and, in the worst case, contribute to a false sense of security.134

Box 1

The Dutch government's Algorithm Register

In 2022, the Ministry of the Interior and Kingdom Relations launched a central algorithm register to provide more insight into the use of impactful algorithms in the public domain. Examples of high-impact algorithms that belong in the register include "algorithms that have legal consequences for people, or that cause the government to classify people." Government organizations can register information in the register about the algorithm's function (general information, responsible use, and operation), its category (high-risk, high-impact, or other), whether and which impact assessments have been conducted, and its development status. The Algorithm Register website contains a dashboard that provides insight into registered algorithms. Currently, around 1,000 algorithms are registered in the register. The Algorithm Register is located at:www.algorithmregister.nl .

The Dutch government is working on a legal framework for the Algorithm Register. The legal framework must provide clarity regarding the mandatory registration of algorithms. However, even without this requirement, the Algorithm Register is already a valuable and practical tool for providing transparency and promoting oversight of government algorithms. However, not all organizations are utilizing the Algorithm Register yet. The Dutch Data Protection Authority (AP) encourages government organizations to utilize it as much as possible.

The Algorithm Register can be embedded in existing work processes, for example when contacting citizens. For example, citizens may receive a letter containing a decision made using, or supported by, algorithms or AI. If the recipient wants to know more, the letter can refer them to the Algorithm Register for information about the operation of the algorithm involved in the decision. This effectively integrates the Algorithm Register into workflows.

A reliable government provides useful, relevant information in an accessible way. This information can reach citizens in various ways. For example, by requiring citizens to be involved in the development of risky processing 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. The positive use of tools and information can help organizations handle algorithms and AI responsibly. But above all, it enables citizens to become aware of the use of algorithms and AI, and to question or challenge the results. This contributes to greater trust in the technology and its use in the public sector.

2. Eight handles for algorithm registration

Algorithm registration often raises questions: what do you register, for whom, and in how much detail? To help organizations and sectors set up and complete algorithm registers, the Dutch Data Protection Authority (AP) offers eight practical guidelines. These help in making choices about the purpose, content, and approach to registration.

Step 1: Determine the purpose for algorithm registration in advance. The purpose of algorithm registration determines the target audience and the necessary content and format. Is a register primarily intended for employees to improve the internal governance of organizational algorithms? Then an Excel file with organizational jargon might suffice. Is the goal of a financial service provider to make credit rating algorithms transparent and traceable for clients? Then an accessible and non-technical explanation in a register where clients can consult it is essential.

FIGURE 2 | EIGHT HANDLES FOR ALGORITHMEREGISTRAT IE

Explanation: Establishing algorithm registration requires a structured approach. This ensures that an algorithm register is accessible and complete, based on a clear purpose and scope, with appropriate transparency, and where a proper division of responsibilities ensures updating and quality assurance.
The eight handles enable sectors to tackle this.

Handle 2: Describe in detail which algorithms fall within the purpose of registration. Many organizations use numerous computer programs that employ algorithms. Which algorithms should be included in the registry is therefore an important question. For example, there are many operational and everyday algorithms that don't necessarily need to be included in a registry. Consider an application that automatically schedules appointments (*auto-scheduling*), a spell checker or algorithms that rank sales figures.
The chosen purpose for algorithm registration determines which algorithms should be included in the register. Is the goal to provide transparency to parents about algorithm use in education? Then, algorithms that are relevant to them should be registered first. For example, algorithms that influence their children's academic performance, such as student monitoring systems. Registering algorithms that are not relevant to this target group in such a situation does not contribute to overview and transparency, but rather to more noise. Other considerations for registration may include the complexity, impact, or context of the algorithm. If algorithms have certain inherent risks, it is always useful to include these in the register. For example, algorithms that assign certain risk scores to people.

Step 3: Start with the available information and then develop further. Completing a register can raise questions about how an algorithm works, what processes are involved, and how this information can be recorded meaningfully for the target group.
Formulating answers to these kinds of questions is essential for algorithm monitoring, but can also be challenging and lead to procrastination. Therefore, don't set your standards too high initially and start with the available information.

For example, if only a brief description of how the algorithm works is available, it's a good starting point to record this information now, rather than waiting until the information is complete. Even with less refined or incomplete information, recording can begin. This contributes to the dialogue about an algorithm, which can also contribute to better information. At the same time, organizations should strive to refine and supplement information over time, as incomplete information can also lead to ambiguity. A balance must be found between the speed of recording and the completeness or detail of the recording.

Example 1

Algorithmic Transparency Standard

Seven European municipalities that are leading the way in algorithm registration, including Amsterdam, Eindhoven and Rotterdam, have jointly *Algorithmic Transparency Standard* developed. This standard includes a template with categories to get started with algorithm registration.
The standard is aimed at municipalities, but also contains useful information for other organizations.
The standard is available together with a guidance document on www.algorithmregister.org .

Tip 4: Go beyond the basic features and also consider the context when registering. Basic features for registering an algorithm include a description of its operation (decision rules), what the algorithm does, who is responsible for it, and the data and technology used. But just as important as the basic elements are the underlying administrative, economic, or policy considerations for using the algorithm. This is useful, for example, to better understand the algorithm's existence in the future or, if it turns out, is no longer effective in achieving the initial objectives. For example, an algorithm may implement certain legislation or be based on outdated (scientific) standards. Using information from the algorithm register can better inform the decision to adapt or phase out an algorithm.

Example 2

Subsidy scheme with income limit

The fictional municipality of Koornwoude established a subsidy program in 2018 to make homes more heat-resistant for low-income earners. Koornwoude uses an algorithm to filter applications: incomes higher than €32,000 per year are automatically rejected, even if the difference is small. The municipality considered it advisable to apply a strict income threshold when the program was created due to limited budgets and support for low-income earners.

In the following years, Koornwoude changed its policy and the municipality made it a priority to offer more customized services. In 2025, there was considerable outrage in the city council when it emerged that many subsidy applications were automatically and unjustified rejected for people with non-heat-resistant homes who should have been prioritized. Research in the algorithm register showed that the strict income threshold criterion was the cause, and that this criterion was based on outdated policy views.

Step 5: Make the risks and the control measures taken transparent. The use of algorithms can entail risks in areas such as privacy, discrimination and bias, deception, technological sovereignty, or cybersecurity. Therefore, pay particular attention to identifying risks in a register. Consider a description of the risks with a risk classification system, for example, which can be used to classify algorithms as low, medium, or high risk. Factors that play a role here include complexity, autonomy, whether there is human intervention, and the impact of the algorithm. The use of an algorithm in a high-risk area of the AI Regulation (Annex 3) is also a good indicator of high risk, because algorithm use in these areas—for example, education or recruitment and selection—

– can also carry additional risks.135 It is also important to record risk management measures taken. Consider impact assessments such as a DPIA, audits conducted during the algorithm's lifecycle, procedures for reporting and complaining about the algorithm, and, if applicable, a risk assessment: the rationale for continuing to use the algorithm despite (remaining) risks.

Example 3

Include objective justification in the algorithm register

A significant risk associated with the use of algorithms is that they can lead to bias, exclusion, and even discrimination. Organizations must mitigate these risks as much as 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 be permissible. But only in certain situations where organizations can provide a so-called objective justification. Organizations in this situation are well-advised to include their justification for this legal review in the algorithm register. This is especially useful for the legitimacy of an algorithm, especially in sensitive considerations. It provides insight into the considerations made and facilitates control, oversight, and dialogue.136

Step 6: Facilitate external control by being as transparent as possible. There may be reasons not to disclose certain information publicly. Considerations often cited include cybersecurity, trade secrets, and the potential for misuse (*gaming the system*) or security considerations in certain sectors. The basic principle here is that registration and transparency should be pursued as much as possible, despite these reasons. For example, sensitive information can still be included in a non-public part of the register that is, for example, only accessible to supervisory authorities. This also parallels the regime in the AI Regulation for AI systems for law enforcement, migration, asylum, and border control. These will have to be registered in a non-public part of the European Commission's register (Article 49, paragraph 4, AI Regulation).

In addition, transparency is not black and white and can be given to a greater or lesser extent depending on circumstances. For example, it can be decided to omit only certain information (see the District Court's ruling). Transparency applies particularly to government organizations and semi-governmental bodies. Access to information is an important democratic principle for government accountability; therefore, non-registration must be justified.

Example 4

Algorithm register contributes to compliance with transparency obligation, court rules

A recent court ruling underscores the importance of algorithm registration and the importance of being as transparent as possible about algorithms. The dispute concerned information about algorithms that the Dutch Tax and Customs Administration had redacted in a journalist's Open Government Act (WOO) request. The omitted passages allegedly revealed information about the auditing technique, which, according to the Dutch Tax and Customs Administration, could be abused to circumvent audits.
The court ruled that the importance of effective inspection of the omitted information in this situation outweighed the journalist's interest in checking the algorithms for discrimination. The court considered that the Tax and Customs Administration had made information public as much as possible and had also placed information about algorithms in the Dutch government's Algorithm Register. 137

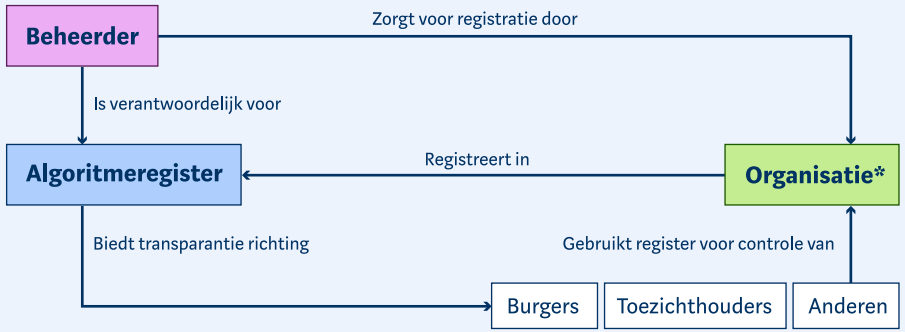
Tip 7: Invest in accessible design for the register. Design plays a key role in achieving the objectives of algorithm registration. If the focus is on external auditing by including a large amount of information in the register, it is especially useful to incorporate functionality into the register to easily search or filter information based on different categories (see, for example, the Dutch Algorithm Register in Box 1). If the register serves various target groups, it is also advisable to organize information at multiple levels, such as a first level with accessible information (preferably at B1 language level) for citizens or customers, after which more detailed or technical information can be clicked for experts. Also, ensure that the algorithm register is easy to find, for example, in a prominent location on the organization's website. And link to it for articles or services involving algorithms. For internal registers, this could be on the intranet, another internal knowledge platform, or a shared folder or file.

Step 8: Ensure consistent management of the algorithm register and a clear division of roles. Proper management of an algorithm registry is necessary to ensure structural activities such as functionality, openness, and security of the registry. In addition, an administrator of the algorithm registry can fulfill a quality assurance role to ensure that organizations actually comply with registration requirements. Managing the algorithm registry is a task, not necessarily a role assigned to a specific person. In many cases, the administrator's role will not be the same as the registering role: the organizational unit or person responsible for registering algorithms. This

For smaller registries, the responsibility for registering can overlap with the management responsibility. It is important that the administrator has sufficient authority to request additional information and to hold others accountable for the quality of registrations. The administrator also acts as a source of information and contact for internal and external algorithm registration matters. From the perspective of the registration responsibility, it is important that there is a mandate within the organization based on which registration tasks are integrated into various business processes, such as ensuring that contracts stipulate that software providers provide the correct information when purchasing new systems. Figure 3 illustrates a conceptual division of roles in algorithm registration.

In the case of a shared algorithm registry with algorithms from multiple organizations, the question of who is the administrator depends on the specific context of a sector or area of application in which algorithms are used. The purpose and scope of the algorithm registration (tools 1 and 2) are important. Consider algorithms in the education sector: The registration of these algorithms is relevant because these systems and processes can impact pupils and students. A conceivable situation here is that an algorithm register is managed by a sectoral organization, for example, for a specific educational domain (primary education, higher education) or Dutch education as a whole. An algorithm register could be managed by a public organization, a trade association, or a partnership within the sector. For other application areas, such as algorithms and AI systems for HR applications or biometric applications, potentially all organizations in the Netherlands use it. For such applications, an algorithm register will need to be managed differently. Customization is essential.

FIGURE 3 | CONCEPTUAL ROLE DIVISION ING ALGORI TMEREGISTRAT IE



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

Box 2

View on the importance of algorithm registration for supervisors

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

Supervision takes shape, among other things, through external control. Facilitating this is one of the two objectives of algorithm registration. Thanks to algorithm registers, regulators can see which algorithms and AI systems are being used and based on which considerations. This creates a significant efficiency gain: regulators don't have to "search" for algorithms, but can rely on proactive information provision. It contributes to the accountability of algorithms to the regulator and ensures that they are aware of (new) developments in a timely manner. This is essential for risk-based supervision.

It is important for supervisors that an administrator has been appointed for the algorithm registration process. The administrator plays an important role in algorithm oversight (see Figure 3). If further information is required, this person will act as a point of contact for the supervisor and other external parties.

It is desirable to give supervisors access to a deeper layer of the algorithm register...
Oversight may require more detailed information than is appropriate for the general public. This facilitates information management and allows oversight to focus on actual control of algorithms rather than searching for and requesting information about them. A register provides a concrete resource for the supervisory authority. A multi-layered algorithm register also aligns with situations where certain information about algorithms can or must remain confidential (tip 6).

Explanation of the report

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

AI systems, at their core, automate actions and decisions that humans previously made. Or that were previously not possible in this way. In simple terms, we then speak of algorithms and AI. This ranges from relatively simple applications, in which a single algorithm functions based on static decision rules, to highly complex applications of machine learning or neural networks. The risk analysis in this report does not distinguish based on the technical operation of algorithms and AI, which aligns with the emerging policy consensus on the meaning of the term "AI system."

The Algorithm Coordination Directorate (DCA) of the Dutch Data Protection Authority (AP) monitors the potential impact of the use of algorithms and AI on public values and fundamental rights, based on the AP's AI and algorithm coordination role. It reports on this periodically.
This contributes to a more responsible use of AI and algorithms.

The AI & Algorithms Netherlands (RAN) Report describes trends and developments. The RAN describes risks associated with the use of algorithms and AI that can affect individual Individuals, groups of individuals, or society as a whole can be affected, ultimately disrupting society. The Dutch Data Protection Authority (AP) establishes the RAN to raise awareness of these risks to stakeholders—private and public organizations, politicians, policymakers, and the public—in a timely manner, enabling them to take action. Two caveats apply to the description of trends and developments in these risks. First, the use of algorithms and AI not only entails risks but can also make positive contributions, including to public values and fundamental rights. The oversight focus is on (removing) risks. Second, this periodic reporting emphasizes trends and developments. This means that the analysis focuses on structural risks.

The RAN does not contain predictions. The Dutch Data Protection Authority (AP) aims to use current knowledge and available information to provide a concise and comprehensive overview of the current risks associated with the use of algorithms and AI, and the challenges involved in managing these risks. Where possible, the AP proposes policies to mitigate these risks. This should not yet be considered concrete guidance. The analyses and recommendations in the RAN offer organizations and policymakers insights to reduce the risk of undesirable effects when deploying algorithms. The RAN can also be used to better understand algorithms and AI and to strengthen the dialogue about the opportunities and risks of algorithms in society.

This is the fifth edition of the RAN, which is published bi-annually. The content is based on knowledge gained through the Dutch Data Protection Authority's supervisory network, including desk analysis and interviews with more than one hundred relevant national and international organizations. However, developments are moving rapidly, and visibility on many fronts is still incomplete. With this in mind, the Dutch Data Protection Authority is attempting to build the most comprehensive picture possible of current risks and developments in control measures, and to link this to constructive policy recommendations. Errors or omissions in this RAN are, however, possible.

Get in touch with us. Your comments and suggestions on the RAN are welcome. You can email them to dca@autoriteitpersoonsgegevens.nl

1 Government programme of the Schoof cabinet (13 September 2024). https://www.rijksoverheid.nl/documenten/uitgeverij/2024/09/13/regeerprogramma-kabinetschoof

2 BNR web editors and ANP (May 28, 2025). Heinen and Agema agree: 400 million euros for healthcare innovation.https://www.bnr.nl/nieuws/nieuwspolitiek/10575003/akkoord-in-kabinet-overfinanciering-aanvullend-zorgakkoord

3 VZVZ (February 20, 2025). AI in practice: pilot launched in five Dutch hospitals. https://www.vzvz.nl/nieuws/ai-de-praktijk-pilot-vijfnederlandse-ziekenhuizen-van-start-gaan

4 UMCG (November 13, 2023)UMCG answers patient questions with the help of AI

5 IGJ publication (10 February 2025).IGJ urges healthcare providers to handle generative AI applications with care | Publication | Health and Youth Care Inspectorate

6 Schut, MC, Luik, TT, Vagliano, I., Rios, M., Helsper, CW, van Asselt, KM, ... & van Weert, HC (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 Public Health and Society Council (April 15, 2025). Almost everyone sick - On the downsides of expanding diagnoses.https://www.raadrvs.nl/adviezen/iedereenbijna-ziek

8 Corperijmedia (March 13, 2025). The future of housing brokerage: how AI agents will serve house hunters more intelligently. https://www.corporatiegids.nl/nl/nieuws/de_toekomst_van_woonruimtebemiddeling_hoe_AI_agents_home_seekers_smarter_go_serve-9688

9 CorporatieNL Editorial Team (20 January 2025). https://www.corporatienl.nl/artikelen/welbions-startmet-visie-op-ai-beleid/

10 IEA (2025), Energy and AI, IEA, Paris https://www.iea.org/reports/energy-and-ai ACM (17 July 2024). ACM market study: algorithmic trading on the wholesale energy market https://www.acm.nl/nl/publicaties/acm-marktstudiealgoritmische-handel-op-de-groothandelsmarkt-voorenergie

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-deelektriciteitssector-bewaak-duurzaamheid-enmachtsbalans

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 Explore

14 European Parliament (8 July 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. (June 13, 2025). The Verge. Meta is paying $14 billion to catch up in the AI race https://www.theverge.com/meta/685711/meta-scaleai-ceo-alexandr-wang

16 Court of Audit (15 January 2025). Publication The Kingdom in the cloud.https://www.rekenkamer.nl/publicaties/rapporten/2025/01/15/het-rijk-in-de-cloud See 17 Chapter 2 Policy and regulations.

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

Letter to Parliament on the Groningen AI factory proposal. (June 27) 2025).https://www.rijksoverheid.nl/documenten/kamerstukken/2025/06/27/indiening-voorstel-aifabriek-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 The GPT-3 version was 1,024 characters, while the latest version (based on GPT-4.1) can handle 1 million characters.

25 For example, OpenAI's o3-mini model achieves similar results as the previous o1 model, at 15x lower costs.

26 R. Bommasani, SR Singer, et all (June 17, 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, YT, Situ, J., Liao, XH, Beresnitzky, AV, ... & 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 Art. 37 Charter of the EU. See also UN Human Rights judicial council, resolution:A universal right to a healthy environment

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

31World 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). TheWashington Mail. 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-electricitywater-data-centers/

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

36 NOS. (May 22, 2025). New research: AI consumes 11 to 20 percent of global data center power. New research: AI consumes 11 to 20 percent of global data center power

37 Bloomberg Technology. (May 8, 2025). AI is draining water from areas that need it mostbloomberg.com/graphics/2025-ai-impacts-data-centers-water-data/

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

39 Scientific Advisory Council Police (June 2025), Navigating No Man's Land: Seven Urgent Challenges Surrounding Digitalization and AI in Policing. https://www.wetenschappelijkeadviesraadpolitie.nl/uploads/publications/Navigeren-in-niemandsland.pdf 40 Scientific Advisory Council for the Police. (June 5, 2025). Publication Navigating in no man's land. 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 Advisory Committee on the Implementation of Allowances (March 2020), Final advice Looking back in wonder 2.

44 Dutch Data Protection Authority (2020), Research Tax authorities childcare allowance. Tax and Customs Administration investigation into childcare allowance | Dutch Data Protection Authority

45 See also the Authority's publication on this matter Personal data concerning meaningful human intervention (2025).Consultation on meaningful human intervention in algorithmic decision-making | Dutch Data Protection Authority 46 Hemmer, P., Schemmer, M., Vössing, M. and Kühl, N. (2021), Human AI Complementarity in Hybrid Intelligence Systems: A Structured Literature Review. *PACIS 2021 Proceedings*. 78.

47 See also the Authority's publication on this matter Personal data concerning meaningful human intervention (2025).

48 College for Human Rights. (18 February 2025).Meta Platforms Ireland Ltd. makes illegal discrimination based on gender when displaying job vacancy ads to Facebook users in the Netherlands. | Netherlands Institute for Human Rights

49 The Hague District Court, February 5, 2020, ECLI:NL:RBDHA:2020:865

50 See ECLI:EU:C:2025:117 (Judgment of the Court (First Chamber of 27 February 2025, Case C-203/22)

51 Expertise Centre for European Law (11 March 2025). The Court of Justice of the European Union clarifies what information a controller must provide in the context of automated decision-making. https://ecer.minbuza.nl/-/eu-hof-verduidelijkt-welkeinformatie-een-verwerkingsverantwoordelijke-in-decontext-van-automatisering-besluitvorming-moetververlening .

52 See also Dutch Data Protection Authority (10 October 2024). Advice on Article 22 GDPR and automated selection tools.https://zoek.officielebekendmakingen.nl/blg-1168066.pdf

53 See Article 15, paragraph 1, point (h) of the GDPR (2016/679).

54 See Article 86 of the AI Regulation (2024/1689).

55 Dommering, E. (December 2023). Artificial Intelligence: Where has reality gone? *Computer Law 2023/258*.https://www.ivir.nl/publications/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. (November 29, 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 (May 8, 2025). New OMB memos signal continuity in federal AI policy,https://www.brookings.edu/articles/new-omb-memos-signal-continuity-infederal-ai-policy/;

60 The White House (April 3, 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 Ministry of the Interior and Kingdom Relations relationships (2025).Letter to Parliament on the results of the AI facility in the Netherlands

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

68 Ministry of the Interior and Kingdom Relations relationships (2025).Government-wide guidance for the responsible use of generative AI

69 Dutch Data Protection Authority (2023). AI & Reporting Algorithm Risk, Chapter 1 ofAI & Algorithm Risk Report Netherlands (RAN) - Autumn 2023 | Dutch Data Protection Authority

70 Ministry of the Interior and Kingdom Relations relationships (2025).Collection letter digitalization May 71 2025 Ministry of the Interior and Kingdom Relations (2025).Letter to Parliament on progress of motion on scientific standard for models and algorithms

72 Parliamentary Papers II 2024/2025, 32 761, no. 322.Motion of Member Van Nispen on algorithms that may use risk profiling and automated selection tools to publish in the Algorithm Register

73 European Commission (15 May 2025).Commission preliminary 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 Chamber Papers 2024/2025, 36531, no. 12 (Amendment from Member Six Dijkstra CS to replace that used under No. 8).

76 European Commission (2025).The Commission publishes the guidelines on prohibited practices in the field of artificial intelligence (AI), as defined in the AI Regulation

77 European Commission (2025)The Commission publishes guidelines for the definition of AI systems to facilitate the application of the rules of the first AI Regulation

78 Dutch Data Protection Authority (2025). AI & Reporting Algorithm Risk, Chapter 3 ofAI & Reporting Algorithm Risks Netherlands (RAN) Winter 2024/2025 | Dutch Data Protection Authority

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 Dutch Data Protection Authority (2025).Call for input 61 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 Dutch Data Protection Authority (2025).Form proposal Dutch 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 behavioral 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/futurebiometric-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 behavioral 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, paragraphs 34 and 39, Article 5, & recital 44, of the AI Regulation.

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, April 10). There are 19 types of smile but only six are for happiness.*BBC*. https://www.bbc.com/future/article/20170407-whyall-smiles-are-not-the-same

97 See also recital 44 of the AI Regulation. 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, DL and O Keefe, SF (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 basics emotions: what should affective computing compute? *In CHI'13 extended abstracts on human factors in computing systems*(pp. 2287-2294).

102 There are also layouts that use more dimensions, for example also dominance, see for example: Khare, SK, Blanes-Vidal, V., Nadimi, ES, & Acharya, UR (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, BW (2024). Refashioning emotion recognition modeling: The advent of generalized large models. *IEEE Transactions on Computational Social Systems*. 106 Zhang, Z., Peng, L., Pang, T., Han, J., Zhao, H., & Schuller, BW (2024). Refashioning emotion recognition modeling: The advent of generalized 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 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.

110 Awais, M., Naseer, M., Khan, S., Anwer, R.M., Cholakkal, H., Shah, M., ... & Khan, F. S. (2025). Foundation Models Defining a New Era in Vision: a Survey and Outlook.*IEEE Transactions on Pattern Analysis and Machine Intelligence*.

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, January 3). Emotion reading tech fails the racial bias test.*The Conversation*. https://theconversation.com/emotion-reading-techfails-the-racial-bias-test-108404

114 Whittaker, M., Alper, M., Bennett, CL, 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, EL, & Lodder, AR (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). SpringerNature. https://doi.org/10.1007/978-3-031-80111-2_6

117 Janssen, A., Kool, L., & Timmer, J. (2015). Close to the skin: facial and emotion recognition in the Netherlands. *Rathenau Institute*.

118 Sarah R. Blackstone, SR, & Herrmann, LK (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 Regulation

122 AP Guidance: Getting started with AI literacy (2024) 123 See also the Data Protection Directive for law enforcement (2016/680).

124 See also thelegal framework for facial recognition from the AP (May 2024), and therelevant EDPB guidelines , among others EDPD, 63 Guidelines 3/2019 on the processing of personal data through video equipment and EDPB, 63 Guidelines 05/2022 on the use of facial recognition technology in law enforcement.

125 AI Systems for Emotion Recognition in the Workplace or in education: Summary of responses and next steps (AP, February 2025)

126 For example, in December 2024, the EDPB announcedto publish guidelines on the interaction between the GDPR and the AI Regulation . 127 Ovw. 14 AI Regulation.

128 Article 4 (14) GDPR, see also opw. 51 GDPR; Article 3 (34) AI Regulation, see also section 14 AIV.

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

130 Art. 5 (1) (f) AI Regulation

131 Art. 5 (1) (g) AI Regulation

132 Article 3(39) AI Regulation and Ovw. 18 AI Regulation; see alsoEC guidelines on prohibited AI practices under the AIV , para. 250-252, see 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 Dutch Data Protection Authority. Risk groups AI Regulation. https://www.autoriteitpersoonsgegevens.nl/themas/algorithms-ai/ai-regulation/risk-groups-ai-regulation

136 See also: Chapter 2,AI & Reporting Algorithm risks Netherlands February 2025

137 The Hague District Court, 20 May 2025, ECLI:NL:RBDHA: 2025:9525.

AP | bescherming in een digitale wereld