Lessons Learned? Accountability in Digital Governance

A Sociotechnical Perspective

Leiden University

Faculty of Governance and Global Affairs

M.Sc. Public Administration: International and European Governance

Supervisor: Dr. H. I. Huang

Ömer Bülent Yavuz

S2761246

January 14th, 2026

Word count: 9995

“A computer can never be held accountable, therefore a computer must never make a management decision” – IBM Training Manual 1979

Abstract

Accountability is often vaguely conceptualized and defined, also when it comes to accountability in AI in public organizations. This thesis conducts a single-case study applying a qualitative content analysis for which a coding frame derived from relevant academic literature was developed. On one side, the results contribute to accountability literature by confirming a differentiated conceptualization of accountability as a virtue and accountability as a mechanism. On the other, the results establish the objectives of the Dutch accountability regime in AI in public organizations. Accompanied with this accountability regime, the results demonstrate a proactive use of accountability in which accountability serves as a virtue, a desirable state of affairs. Derived from the results, this thesis recommends policy and decision-makers to seriously explore the reactive use of accountability and its mechanical structures with an particular emphasis on enforcement objectives.

Acknowledgements

I am eternally grateful to my loving parents for their unconditional support and care throughout my entire education and beyond. I am equally grateful to my sister, who has been a source of inspiration to me and motivated me to pursue a university degree while I was working in the factory. Without my family, it would all have remained a dream.

I would also like to express my deepest gratitude to my supervisor, Dr. Hsini Huang, for her guidance, support, and foremost, her patience throughout this thesis project. Additionally, I am also deeply grateful for Mr. Wiebe Posthuma with his invaluable support and advice throughout my academic education.

In particular, I want to thank Adam Vittek for his support during this thesis project and for his great company throughout my academic education – the best of friends are the ones you can learn from. Many thanks to Ozan, Efe, Koray, Toma, Helin, Mirkan, and Irfan for their companionship throughout my studies. And special thanks to Iris, Enes, Fatih, Yusuf, and Cihan, who have been supporting me since day one.

Table of Contents

1. Introduction

As a form of digital governance, artificial intelligence (AI) governance is shaped by the increasing embeddedness of AI in public services to support or automate decision-making (Young et al., 2019). The main argument for this development is to improve organizational efficiency of public services, on one side (Widlak et al., 2020). On the other, however, growing evidence stresses that AI in public services not only lacks accountability but also poses serious risks (Young et al., 2019). These risks revolve especially around automated decision-making due to its opaque character. The Childcare benefit scandal in The Netherlands, for instance, induced disproportionate and extended damage, both socially and financially, in an unprecedented way and was mainly driven by a fraud-detection algorithm that mislabelled more than 26 thousand recipients as outright fraudsters[1]. For a long time it remained unclear how and why recipients where labelled as fraudsters. Thorough evaluation exposed rigid bureaucracy within the chain of public administration, discriminatory risk-profiling, lack of transparency and accountability, and restricted access to justice of citizens (van Dam et al., 2020; Bouwmeester, 2023). In its aftermath, no single entity was held accountable for the scandal. It was rather described as the failure of an entire system. In the meantime, the fraud-detection application at the core of the Childcare benefit scandal was terminated in 2020. Regardless, the Dutch Applied Scientific Research Organization (TNO) found that AI applications in Dutch public organizations increased explosively by 254% in comparison to 2019, despite a more narrow definition (Hoekstra et al., 2024). This raises serious concerns regarding human-AI collaboration in public organizations and the accountability of AI in The Netherlands. This thesis aims to contribute to AI accountability literature and attempts to assess the governance of accountability in AI in The Netherlands.

1.1 Technical, organizational, and sociotechnical perspectives

Accountability in AI is a novel academic field still in its infancy with relatively little existing literature that is often normative. Traditional accountability literature refers to different concepts generating accountability from various social, technical and political angles. For some, it encompasses transparency, liability, controllability, responsibility, and responsiveness (Koppell, 2005). For others, it is an umbrella term that covers transparency, equity, democracy, efficiency, responsiveness, responsibility, and integrity (Behn, 2004). Accountability, therefore, remains a contested concept (Behn, 2004; Bovens, 2007; Novelli et al., 2023). The reason for this contestation is the multilayered origin of accountability resulting in a context-dependent

[1] For a detailed reconstruction, see Frederik (2021). *Zo hadden we het nooit bedoeld*. De Correspondent.

understanding (Sinclair, 1995; Lindberg, 2013). Nonetheless, this ambiguity is highly controversial as it poses risks to undermine the public debate and governance that conceals implicit trade-offs among various choices regarding the governance of accountability, also in AI (Novelli et al., 2023).

In general, accountability in AI suggests designers, developers, and deployers to comply with legislative requirements (Fjeld et al., 2020; Busuioc, 2021). Its opaqueness and unpredictability hinders detecting the causes and reasons of undesired outcomes (J. Kroll et al., 2017; Tsamados et al., 2022). This leads to the perpetration of wrongdoings by AI, such as discrimination as a result of biased data for training, bugs in the system, errors during programming, continuation and replication of social discrimination, and sometimes a combination of these issues (Novelli et al., 2023). The Childcare benefit scandal has demonstrated such wrongdoings. Yet, assessing accountability for these undesired outcomes becomes complicated due to its wicked nature. On the technical level, AI applications indeed require both accessibility and explainability to monitor and understand their outcomes (J. Kroll et al., 2017). However, the manner in which AI is applied by public organizations and the rules and regulations in these institutions and organizations matter as well (Porumbescu et al., 2022; Nieuwenhuizen, 2025).

On the organizational level, identifying responsibilities becomes complex in these applications involving multiple actors and resources (Novelli et al., 2023). As a result of distributed responsibilities suboptimal equilibria emerge (Floridi, 2013, 2016). This implies that no legal or natural person may feel the obligation to prevent undesired outcomes (Hardin, 1968). Besides, the ‘many-eyes’ issue arises when more than one forum employ various oversight standards (Bovens, 2007). In combination with failing administration, two contrasting challenges emerge. On one side, accountability gaps when nobody is held accountable, on the other, accountability surpluses when various accountability rules and procedures do not complement or align with each other (Bovens, 2007; Busuioc, 2021). Both accountability gaps and surpluses reflect the absence of norm-setting (Novelli et al., 2023).

Nonetheless, AI cannot be considered a mere technical instrument or a social system (Novelli et al., 2023). The technological and organizational context surrounding AI demand a sociotechnical approach to accountability, a perspective that is not enough illuminated (Novelli et al., 2023). This perspective suggests a comprehensive view including the technical side on one hand, and the organizational side on the other (Baxter & Sommerville, 2011; Long, 2013). Based on this perspective, accountability in AI is carefully conceptualized and defined establishing an analytical framework that identifies two factors shaping the governance of accountability in AI (Novelli et al., 2023). On one side, a proactive use, and on the other, a reactive use of accountability mechanisms

relevant to its decision-making and accountability objectives. Proactive accountability refers to accountability as a virtue, while reactive accountability refers to accountability as a mechanism. The former implies an ex-ante approach with a planning purpose as ‘‘it comes before events and aims to prevent failures’’, whereas the latter implies an ex-post approach as ‘‘it comes after events and aims to redress failures’’ (Novelli et al., 2023, p. 1882). Novelli and colleagues argue that accountability goals are often complementary while decision-makers prioritize some over others. Subsequently, this approach serves as a ‘‘useful guide to examine policy strategies for AI’’ (Novelli et al., 2023, p. 1881). Besides, while it addresses European regulations, it has also not been applied to national context thus far. Applying this framework to assess governance of accountability in AI in public organizations aligns with the purpose of this thesis. In parallel, it also contributes to AI accountability literature by deductively testing the framework and its comprehensive conceptualization of accountability. In particular, this approach allows to examine the governance choices, identify the accountability regime type and its objectives in AI in The Netherlands.

1.2 Research question

This thesis is focusing on accountability as the subject of interest in the context of AI applications in public organizations and is concerned with its decision-making, policies, structures and processes to ensure accountability in AI. This is relevant to the governance of human-AI collaboration since the explosive increase of AI applications in public organizations and the transition to digital governance in The Netherlands. Subsequently, the above mentioned research gap results in the following question central to this thesis:

Which objectives shape the Dutch accountability regime in AI in public organizations, and what is its accountability type?

All in all, the main inquiry aims to examine the choices that shape the accountability regime in AI in public organizations in The Netherlands. The first part of the question explores the governance choices of accountability in AI. It is particularly concerned with the question (1) what choices are made and why? The choices between different objectives illuminate the accountability type in AI while also revealing relevant trade-offs in governance. Subsequently, this leads to the question (2) what are the accountability objectives of the Dutch government? This question aims to provide a better understanding of the accountability regime, its objectives, and implications. Lastly, (3) is accountability in AI utilized proactively or reactively in public organizations? This demonstrates

whether the accountability regime is ex-ante in which accountability serves as a virtue or ex-post in which accountability functions as a mechanism.

The next chapter presents the literature review discussing relevant academic perspectives and presents the scope of this thesis in which accountability, its features, and other relevant themes are discussed, conceptualized, and defined leading to measurable hypotheses. In the research design section, the methodology is presented, followed by the operationalization of measurable indicators to test the hypotheses in the case-study. Then, the analysis section consists of the research testing the hypotheses and discusses their interpretation. Lastly, in the conclusion section, the implications are discussed and the limitations are highlighted. Given that no single entity was held accountable for the Childcare benefit scandal, implies the failure of accountability mechanisms. This hints at a reactive mechanisms of accountability in AI in Dutch public organizations aiming to redress previous failures.

2. Literature review

Understanding accountability depends on its context (Sinclair, 1995; Lindberg, 2013), and remains heavily contested as mentioned earlier. From an institutional perspective, accountability can be described as a deliberately narrow relationship between an actor, such as an institution or organization, and a forum, such as a court, parliament, or audit body (Bovens, 2007). This approach suggests a relationship in which an actor is obliged to explain and justify its conduct to a forum that can question, judge, and if necessary, sanction the actor. Herein, accountability is closely coupled with answerability. This theory was further refined distinguishing between accountability as a virtue from a normative perspective, and accountability as a mechanism from an institutional perspective (Bovens, 2010). Largely overlapping with the actor-forum theory, it can also be described as a principal-agent theory suggesting a relationship between the principal which demands information and justification from the agent and holds the right to sanction (Lindberg, 2013). Accountability can also be viewed as inherently relational to transparency in a linear relationship between the two (Fox, 2007). It is concerned with the questions of who is to be transparency to whom, and who is to be accountable to whom? This approach argues that disclosing information does not necessarily result in transparency, and transparency does not naturally generate accountability in public organizations (Heald, 2006; Fox, 2007). Various studies demonstrate that transparency does indeed not automatically produce accountability (Cucciniello & Nasi, 2014; J. Kroll et al., 2017; Nieuwenhuizen, 2025)

In contrast to these linear theories, the new public management theory suggests that accountability entails multiple and overlapping relationships among various public actors. Similar to private-sector principles, the public sector contains diffused accountability mechanisms which multiplies the actors whom are accountable to the entitled audiences (Almquist et al., 2013). Although insightful, this approach neglects public values and their accompanied dynamics as private organizations and public organizations maintain different priorities (Tomazevic, 2019). Acknowledging the multilayered factors of accountability while drawing upon the actor-forum theory, accountability can also be understood as a relational process between an actor and multiple forums (Schillemans & Busuioc, 2015). This approach furthermore highlights that not only actors could fail to account but also forums could fail to use their formal powers to enforce accountability, a process referred to as forum drifting. These general accountability theories mainly concern traditional governance. Meanwhile, the growing embeddedness of AI is expanding digital governance in the public sector reshaping societies. Thus, how is accountability in AI shaped?

Similar to the contestation of accountability in general, accountability in AI in public organizations is also imprecisely defined (Novelli et al., 2023). Several studies assessing accountability regimes in AI incorporate traditional accountability approaches. Drawn on the actor-forum theory, for instance, Madaline Busuioc (2021) investigated the challenges, its deficits, and explored safeguarding accountability in AI in public organizations. She argues that accountability in AI is about answerability as suggested by Bovens' (2007) actor-forum theory. Busuioc highlights transparency as a necessary but insufficient condition for accountability, similar to a traditional governance context. Simultaneously, it also resembles Fox's (2007) linear theory suggesting that disclosing information does not necessarily lead to transparency, and transparency does not naturally produce accountability. The study holds a particular focus on the technical level as it incorporates computer science perspectives as well. In conclusion, Busuioc argues that AI applications need to be designed in a way that explains automated decision-making. Such system architecture should be demanded from the industry by ‘‘public sector purchasers and regulators’’ (Busuioc, 2021, p. 833). With its technical transparency focus, the study reveals an accountability mechanism between the industry as an actor and public sector as the forum. Industrial architects of AI applications should be held accountable by public purchasers and regulators to design transparent AI applications that are understandable and explainable in their decision-making. Yet, it emphasizes the technical level and lacks to address the organizational circumstances appropriately. Hence, how is accountability in AI shaped on an organizational level?

A later study focusing on accountability in AI draws further on Bovens' actor-forum theory and identifies necessary conditions for the architecture of accountability regimes (Novelli et al., 2023). The study argues that a sociotechnical system merges tools, machinery, infrastructure, and technology on the technical side, and rules, procedures, metrics, roles, expectations, cultural background, and coordination mechanisms on the social side (Novelli et al., 2023). The synthesis of the two sides ''prevents their disentanglement as single observable parts for specific outcomes, just as it prevents the detection of a general function, as such hybrid systems are embedded in a network of individual actions'' (Novelli et al., 2023, p. 1882). In this context, accountability in AI requires distribution among the network of technological and social influences (Kaminski, 2020). Accordingly, Novelli and colleagues conceptualize accountability coupled closely with answerability, and subsequently, developed a framework that incorporates the actor-forum theory in symmetry with the principal-agent theory.

2.1 Structures of accountability

Novelli and colleagues define accountability specifically coupled with answerability drawing further on Bovens' definition. This thesis draws further on this definition. Answerability reflects the notion of interrogation regarding ''the adequacy of the information or the legitimacy of conduct'' (Bovens, 2007, p. 451). Their conclusion for this definition is that it aligns with the given conceptualization of accountability in European regulations, such as the High-Level Expert Group (HLEG), the General Data Protection Regulation (GDPR), and the EU AI Act (AIA), which all imply answerability (Novelli et al., 2023, p. 1872). Similar to Bovens' (2007) description meaning ''the obligation to explain and justify conduct (p. 450), Novelli et al. (2023) describe accountability as the ''obligation to inform about, and justify one's conduct to an authority'' (p. 1872). Drawn on Bovens' actor-forum theory, the authors elaborate that accountability formally implies a relationship between an Agent (**A**) and a Forum (**F**), in a manner that A needs to justify its conduct to F, whereas F supervises by interrogating and judging A grounded on the given justification. Both A and F can be individuals, groups or legal persons, such as organizations.

Subsequently, the authors do not consider the principal-agent theory as theoretical trade-off to the actor-forum theory. Instead, they suggest that accountability is a counterbalance to another relationship that logically occurs, namely delegation. In this sense, the principal-agent theory is merely on the other-side-of-the-coin from the actor-forum theory. Both depict similar structures but highlight distinct relationships. For instance, delegation to A of a given Task (**T**) by a Principal (**P**), on behalf of which A acts (Lindberg, 2013). In accumulation, P and F may differ as A may be delegated T by P but is accountable for T to F. Accountability can therefore be considered in a

binary or ternary relation (Novelli et al., 2023), involving both A and F or P, but can include T as well. Isolating these structures on both sides of the coin to purely sec accountability assumes F equals P (Novelli et al., 2023). In other words, forum and principal are used interchangeably depending on the given circumstances. Although this assumption does not impact the cogency of the framework, it outlines circumstantial differences whereas the principal, for instance, regulates rules and conditions of accountability mechanisms, the forum merely administers them (Novelli et al., 2023).

Combining these structures results in the identification of three conditionalities of accountability consisting of (1) authority recognition, (2) interrogation, and (3) limitation of power (Novelli et al., 2023). Although foundational to the framework, this component is omitted from the analysis for the purpose of this thesis as it is safe to assume that The Netherlands meets these conditions considering its long-standing democratic tradition, which the authors imply with these conditionalities (Novelli et al., 2023).

2.2 Traditional accountability

Seven traditional features of accountability are revealed when the previously mentioned structures are linked with answerability. It considers its (1) context (what for?), (2) range (about what?), (3) agent (who is accountable?), (4) forum (to whom an account is due?), (5) standards (according to what?), (6) process (how?), and (7) implications (what follows?) to understand this relationship (Novelli et al., 2023, p. 1873). An overview with typical examples is presented in table 1 in the appendix, derived from Bovens (2007) and Mashaw (2006). In extent, it highlights several values, practices, and measures referring to accountability. Filtering these items through a synthesized framework of several studies reveals the objectives that accountability should be serving (Schedler, 1999; Mulgan, 2003; Rubenstein, 2007; Bovens, 2007 in Novelli et al., 2023). Accountability regimes are shaped by the chosen objectives categorised as (1) compliance, (2) report, (3) oversight, and (4) enforcement (Novelli et al., 2023, p. 1974). These objectives can be pursued exclusively or simultaneously (Schedler, 1999). The choices in these objectives determine different tasks and obligations for the agent and forum or principal (Schedler, 1999 in Novelli et al., 2023). Although several reasons could lead to the separation of the objectives. Some objectives are emphasized or prioritized over others consequential to topics that require more legislative accountability (Srinivasan & San Miguel González, 2022). When the legislative accountability is less present, Novelli and colleagues suggest that some objectives should be prioritized over others depending on the circumstances. Particularly in the context of governing accountability in AI.

2.3 Accountability in AI

Accountability in AI encompasses similar structures, but naturally results in differing characteristics given its AI specific context. These features and their accompanied characteristics are displayed in Table 2 in the appendix. Although these features are not subject to the assessment in this thesis, they offer useful insights for the analysis. Similarly, the objectives are also overlapping but contain once more context specific characteristics as well. Traditionally, the (1) compliance objective is suggested to be normative as ‘‘a set of standards for the behaviour of actors’’ (Bovens, 2010, p. 949). In the context of AI, this objective aims to align AI applications to binding ethical, legal, or technical norms. It determines the design, development, and deployment standards that should be met with through the lifecycle of AI (Novelli et al., 2023). Compliance is usually understood as a preliminary measure for AI providers aligning with the EU AI Act that constitutes ex-ante compliance for high-risk AI after market introduction (Novelli et al., 2023).

The objective of (2) reporting traditionally implies to be a ‘‘mirror of (and surrogate for) the act of direct monitoring by the principal of the behaviour and act’’ (Dubnick, 2005, p. 383). In other words, monitoring the agent’s conduct ensures explainability and justification to the forum or principal about its conduct. In AI, monitoring reflects the deliberative aspect of accountability (Novelli et al., 2023). In practice, it ensures the explanation and justification of AI behaviour and its outcomes. For instance, the right to appeal against automated decision-making is ensured through reporting, which is also constituted by Articles 21 and 22 of the General Data Protection Regulation. Especially because of the opaqueness of AI applications, reporting is not merely a transparency instrument but provides a functional tool to interpret and explain AI outcomes (Novelli et al., 2023). On one side, AI explanations do not always include all available data, rather only data that is relevant for its context. For example, when comparing counterfactual cases relevant to the interaction between the agent and the forum (Miller, 2019). On the other, the interpretation of AI provides data only understandable for experts working with these applications, which then lacks completeness for broader audiences as it neglects user’s cognition, knowledge, and biases (Gilpin et al., 2018).

As an objective, (3) oversight enables the assessment of information, acquire evidence, and evaluate the conduct of the agent in the traditional sense (Novelli et al., 2023). It fosters robust scrutiny as well as ex-ante checks and balances of decision-making processes by the forum. However, it can in contrast also cross-examine the explanations and justifications as ex-post oversight accounting for the rules of deployment, for instance, through judicial review (Novelli et al., 2023). In the context of AI, the oversight objective aims to find facts or data relevant to establish

evidence for evaluating the performance of AI (Novelli et al., 2023). Oversight has become crucial in AI governance which is also emphasized by the EU AI Act in article 14 (Novelli et al., 2023). Oversight can be produced by different bodies, internally or externally, or also through human-machine interactions. Moreover, oversight could also imply human-in-the-loop mechanisms which has been suggested by many scholars regarding ethical accountability (Kaler, 2002; Almquist et al., 2013; Kroll et al., 2017; Tsamados et al., 2022). Such a mechanism requires to be systemically designed before a given AI system enters the market and becomes operational (Kroll, 2020). In this case, different oversight mechanisms may also overlap. For instance, an internal audit could be compatible with an external judicial review carried out by different organizations (Novelli et al., 2023).

Lastly, the objective of (4) enforcement traditionally determines the consequences the agent faces in line with the collected evidence during report and oversight, which could be sanctions, authorizations, or prohibitions (Bovens, 2007; Novelli et al., 2023). In the context of AI, enforcement binds monitoring and evaluation of the performance to formal or informal consequences (Novelli et al., 2023). The aim of this objective is deterring undesired behaviours or outcomes. Aligned with the EU AI Act, enforcement can consist of either the outcome or conformity assessment per article 43 of the Act (Novelli et al., 2023).

For analysing accountability in AI, the authors emphasize that a goal-based analysis is beneficial as ‘‘each goal relates to different sociotechnical aspects of AI applications, duties of the policy-makers, and trade-offs between values and interests of stakeholders’’ (Novelli et al., 2023, p. 1879). The analytical framework revolves around three aspects. Firstly, accountability objectives differ in their regulative focuses in a sociotechnical context. For instance, if the accountability regime is focusing primarily on compliance, the regulative focus should be on the duties of designers and developers to build AI applications that meet ethical, legal, and technical requirements (Novelli et al., 2023). On the other hand, if the report objective is prioritized, the focus rests on information exchange or transparency requirements such as data sources, metrics, and procedures. Then, the objective of enforcement relates to the duration and magnitude of infringement based on article 72 of the EU AI Act.

Secondly, the distinction between accountability objectives allows to identify different degrees of commitment for policy-makers and decision-makers that govern accountability in AI (Novelli et al., 2023). As compliance is value-based objective, it provides greater responsibilities to lawmakers to design accountability regimes that align with their preferences. In contrast, objectives dominated

by regulatory measures, such as oversight, is procedure-based and requires strong judicial interaction both nationally and on the EU level (Novelli et al., 2023).

Finally, a goal-based analysis illuminates the trade-offs between various interests and its bargaining space informing political agreements on accountability regimes (Novelli et al., 2023). The political processes resulting in a particular accountability regime differ with each objective. For instance, the process in which compliance prevails differs from the process in which enforcement prevails (Novelli et al., 2023). On the EU level, compliance enjoys political consensus revolving around general values, such as fairness, trustworthiness, and privacy, whereas oversight or enforcement rules remain undefined leaving responsibility for political settlement in each member state (Novelli et al., 2023).

2.4 Accountability regimes in AI

The above mentioned objectives shape the accountability regime in AI. As mentioned earlier, policy and decision-makers often prioritize one goal over others in their choices. Bovens (2010) distinguishes between accountability as a virtue and as a mechanism. Novelli and colleagues (2023) draw further on this distinction, suggesting that two factors determine the choices in governance of accountability. This results in in two accountability regime types. On one side, a proactive use, and on the other, a reactive use of accountability in AI in public organizations (Novelli et al., 2023). The former focuses on the question of how accountability in AI should be shaped, while the latter is concerned with the question how AI should be held accountable (Novelli et al., 2023). Proactive accountability is characterized by its positive nature setting norms for the use of AI and its planning purpose as it comes before a relevant event with the aim to prevent failures or undesired outcomes. It intends to identify and correct organizational aspects that could cause wrongdoings and mistakes beforehand. Moreover, it requires AI applications to be designed with clear targets, precise role divisions, responsibilities, and chain of commands. This perspective defines accountability as a virtue which AI applications must acquire in their functioning (Novelli et al., 2023). In order to correct systemic errors proactively, greater emphasis is given to norm-setting through the compliance objective and preliminary checks on adherence to those norms through the oversight objective. For instance, the 2022 Algorithmic Accountability Act in the US promotes proactive reporting by publishing a register containing impactful automated decision-making applications (Novelli et al., 2023). However, with its preventive aim this accountability type offers limited governance regarding wrongdoings and undesired outcomes of AI in public administration as its objectives are not anticipating for those situations (Novelli et al., 2023). Hence, proactive accountability is an ex-ante regime type

In contrast, reactive accountability is characterized by its negative nature in the sense that the accountability regime is a mechanism to redress failures or undesired outcomes subsequent to a relevant event (Novelli et al., 2023). As a mechanism, this accountability type triggers rewards or sanctions after an event. When the event leads to wrongdoings or undesired outcomes, reactive accountability aims to redress the accompanied failures, defining accountability more as mechanism than a virtue. Herein, greater emphasis is given to the report and enforcement objectives. The mechanism focuses on the provision of explanations and justifications provided by the agent to the forum after a relevant event, and the consequences subsequent to accountability assessments (Novelli et al., 2023). Nonetheless, oversight retrospectively plays an essential role in this mechanism as well, through a judicial review for instance (Novelli et al., 2023). Thus, reactive accountability is an ex-post regime type.

Both proactive and reactive accountability are often combined in a particular accountability regime but one type usually prevails over the other (Novelli et al., 2023). For example, the EU AI Act contains both types but emphasizes proactive accountability more as measures for compliance and oversight are prioritized through article 9 and 17 (Novelli et al., 2023). In parallel, similar patterns are observed in the 2019 HLEG ethical guidelines for trustworthy AI in public organizations, which was foundational for the EU AI Act (Novelli, et al., 2023). Table 3 in the appendix provides an overview of the accountability regime types.

As mentioned earlier, the fact that no single entity was held accountable for the Childcare benefit scandal presents a stark indication of an accountability gap at the time implying the absence of prior norm-setting on one side. On the other, the Dutch government introduced a governance strategy for AI in public organizations only after the scandal occurred, with the introduction of an online public algorithm register for public organizations as the first country in the world for instance (Ministry of Interior and Kingdom Affairs, 2025). These two events hint at an ex-post accountability regime type suggesting a reactive use of accountability as a mechanism to redress failures and undesired outcomes. In that case, the Dutch government would likely choose to prioritize both reporting and enforcement.

2.5 Hypotheses

If that were to be true, then the assessment in this thesis expects to find that H_1) *The Dutch government prioritizes reporting over compliance*. Since the authors suggest that the objectives are usually combined and not mutually exclusive as one objective rather prevails over the other. Besides, the EU AI Act contains both proactive and reactive use of accountability as Novelli and

colleagues established, whereas The Netherlands is evidently subject to European Law. Thus, this expectation can be mirrored as well, resulting in H_2) *The Dutch government prioritizes compliance over reporting*. Furthermore, aligning with the report objective, it is also expected that H_3) *The Dutch government prioritizes enforcement over oversight*, and again mirroring this expectation leads to H_4) *The Dutch government prioritizes oversight over enforcement*, aligning with the compliance objective. Establishing the uneven-numbered hypotheses when the Dutch government chooses to prioritize both the report and enforcement objectives in its turn would then imply the reactive use of accountability in an ex-post regime in which accountability functions as a mechanism. On the other hand, if the even-numbered hypotheses were to be supported when the Dutch government chooses to prioritize the compliance and oversight objectives then it would imply the proactive use of accountability in an ex-ante regime in which accountability serves as a virtue. The figure below provides an overview of the hypotheses distinguishing between the reactive and proactive use of accountability in AI.

Reactive use of accountability in AI	**Proactive use of accountability in AI**
H_1) *The Dutch government prioritizes reporting over compliance*	H_2) *The Dutch government prioritizes compliance over reporting*
H_3) *The Dutch government prioritizes enforcement over oversight*	H_4) *The Dutch government prioritizes oversight over enforcement*

Figure 1) Overview of the hypotheses, derived from Novelli et al. (2023)

3. Research design

Based on the previously discussed and established theoretical framework, this thesis aims to conduct an in-depth single-case study to examine the governance of accountability in AI in public organizations in The Netherlands. Novelli and colleagues argue that accountability objectives are often complementary while decision-makers prioritize some over others. Meanwhile, European regulations leave room for political settlements in each member state for the governance of accountability, at least regarding the objectives of oversight or enforcement (Novelli et al., 2023). Hence, much of accountability governance in AI remains open-ended within the political realm and is subject to public debate due to its novelty. Also in The Netherlands, accountability in AI and its

governance remains under development thus far as the responsible decision-maker is in actively deliberating with multiple public and private entities (Szabó, 2025a).

3.1 Methodology

When it comes to politics and political settlement, written and spoken word is the medium for conflict and cooperation (Grimmer & Stewart, 2013). In this case, written and spoken word becomes the primary source of information and data for assessing governance from a public administrative perspective (Hollibaugh, 2019). In particular, not only publicly disclosed documents of public organizations provide relevant data, but also the publicly disclosed transcripts of deliberations provide relevant data as well. Whereas documents of public organizations entail policies, strategies, and procedures, public deliberations with decision-makers reveal choices, priorities, and processes in decision-making (Yanovitzky & Weber, 2020). Therefore, to address the question central to this thesis, qualitative content analysis is an appropriate method for the extraction of information from textual data. Moreover, this methodology allows to systematically assess the content of various textual data as it enables to reduce phenomena or events into priorly defined categories providing an appropriate technique to empirically analyse and interpret relevant data (Harwood & Garry, 2003). In Public Administration research, it requires the validation of the measurement to correspond with the claimed concepts (Grimmer & Stewart, 2013; Hollibaugh, 2019). This is further elaborated in the operationalization section in this chapter.

3.2 Case selection

The transition to digital governance is primarily led by the ministry of Interior and Kingdom Affairs, and by the Department of Digitalization in particular. The State Secretary of Digitalization and Kingdom Affairs bears the coordinating role within the government and is politically responsible for the decision-making. Beside AI (and algorithms), digital governance encompasses other technologies and innovations such as Big Data, cloud computing, and mobile telecommunication technologies. These are omitted from the scope of this thesis as the focus is solely on accountability in AI. Furthermore, the concepts of AI and algorithmic applications are sometimes used interchangeably. To further safeguard the scope of digital governance in this thesis, the definition provided by the Dutch Court of Audit is followed, which is also followed by Dutch public organizations. It employs a definition that distinguishes between algorithms and AI in that the latter consists of algorithms but not all algorithms are AI. As such, algorithms are defined as ‘‘a set of rules and instructions that are automatically followed by a computer for making calculations to solve a problem or to answer a question,’’ while solving a problem or answering a question is also

interpreted as ‘‘performing a task or process or reaching a decision’’ in the given definition (Ministry of Interior and Kingdom Affairs, 2025, p. 7). In particular, AI possesses a learning component that an algorithm do not possess. Nonetheless, AI is considered a subset of algorithms in the given definition. Thus, accountability in AI then also implies accountability in algorithms and vice versa. Subsequently, the governance of accountability in AI applies to both of these digital governance technologies in this thesis.

The transition to digital governance is a topic part of the broader dossier Information and Communication Technology (ICT) with number 26.643 that tracks back to 2010. The Dutch system organizes a theme or field into a dossier that consists of all relevant documents to that theme or field. Hence, the dossier ICT 26.643 is the main case in this thesis. Within this dossier, the government introduced the Working agenda Value-driven Digitalization 2022 in light of the transition. It entails a particular focus on AI and algorithm applications in public organizations (van Huffelen, 2023). The Working agenda was refurbished a couple times before it was reintroduced as the National Digitalization Strategy (NDS) in 2025 by the incumbent cabinet. Meanwhile, the EU AI Act entered into force in 2024. Nonetheless, the aim of the thesis is not to investigate any differences in accountability in AI over time, but rather aims to examine the status quo. As such, the National Digitalization Strategy is the particularly selected case for this assessment as it contains the documents entailing the most recent long-term strategy on AI in public organizations, its policies, objectives, and procedures (Veldkamp, 2025). In addition, relevant supporting documents such as debate transcripts and governmental elaborate on the choices, priorities, and processes in decision-making, explicitly focusing on AI in public organizations. Thus, these relevant documents are subject to the assessment as well.

3.3 Data collection

Subsequently, the data is collected from the sources of the case NDS within dossier ICT (26.643). The table below entails a list of the primary sources in the relevant case from which the data is collected. These sources are derived from the websites of the Dutch Senate and Parliament. The website of the Senate provides an excellent overview of the dossiers, their accompanied documents, and the current state of affairs. Searching the dossier number on the website instantly directs to the webpage with all the relevant information. The website of the Parliament provides an equally excellent overview of the documents relevant to the standing committee for digitalization, in which dossier ICT (26.643) is mainly discussed, offering reports of committee debates including their accompanied agenda documents on its search webpage.

The starting point for the data collection is the NDS. In addition, the committee debates regarding digital governance and their accompanied agenda documents are also relevant sources from which the data is collected. References to documents regarding AI regulations and strategies in the private domain, such as the Strategy Digital Economy, are excluded from the data as the focus is solely on public organizations. To cover the most recent relevant data, only the sources of textual data in the year 2025 are subject to the assessment. In summary, all relevant documents refer to one of the following themes encompassing digital governance in relation to public organizations in 2025: Dutch Digitalization Strategy (NDS), digitalization, digital inclusion, algorithm (applications), AI (applications), and the EU AI Act. In total, the data of 17 documents consisting of 364 pages is collected. A list of the collected data, theme, date, and document number is provided in table 4 in the appendix.

3.4 Operationalization

As required for a qualitative content analysis, a coding frame is developed derived from the framework provided by Novelli and colleagues. The coding frame aims to increase the validity and reliability of the research. Nevertheless, while it ensures high internal validity and reliability grounded in established relevant academic literature, it does not provide external validity and reliability given that it is a single-case study.

The coding frame is developed based on the four aforementioned objectives and their descriptions in section 2.3. It aims to establish supporting or rejecting empirical evidence given that the hypotheses are rivalling. For each objective, its characteristic is described which then provides several indicators to measure the prioritized objectives in the accountability regime in AI in public organizations. With the coding frame, the collected data informs which objective prevails over its rivalling counterpart by implying, describing, or referring to an objective, its characteristic, and one of its indicators. In contrast, an objective, its characteristic, and indicator can also be explicitly or implicitly rejected by the decision-maker, demonstrating its subordination to its rivalling counterpart. A single decision, objective, policy, strategy, procedure, priority, or process can be mentioned multiple times in the collected data. Repetitive data aligning with a similar indicator is not double coded, unless it provides additional context necessary for the analysis. Then, the data is added to the same indicator code. This prevents an unbalanced reflection of the objectives and their indicators.

Coding frame, derived from Novelli et al. (2023)

Objectives	*Characteristic*	*Indicator*
1. Compliance	1.1. Adherence to set of standards by design, development, and/or deployment throughout the entire lifecycle of an AI application. Designers, engineers, producers bear more accountability, aiming to prevent undesired outcomes/failures.	1.1.1. Ethical norms 1.1.2. Legal norms 1.1.3. Technical norms
2. Report	2.1. Monitoring through reporting or notifying, and assessments, frequent or spontaneous. Public organizations as end-users bear more accountability, aiming to redress undesired outcomes/failures.	2.1.1. Elaboration of conduct 2.1.2. Justification of conduct
3. Oversight	3.1. Evaluation of provided information by data collection and/or fact checks, can be internal/external through different institutions, or through human-machine interactions. Aims to prevent undesired outcomes/failures through supervision.	3.1.1. Collection of evidence 3.1.2. Evaluation of conduct 3.1.3. Human-in-the-loop mechanism by design
4. Enforcement	4.1. Deterrence of undesired behaviour or outcomes by binding monitoring and evaluation to consequences. Aims to correct undesired outcomes/failures through punishment or reward.	4.1.1. Formal consequences such as sanctions (fines), legal prosecutions, suspensions, termination, or outcome/conformity assessment 4.1.2 Informal consequences such as praise or disapproval, reputational promotion or demotion

For each indicator, an exemplary data quote is provided that most accurately represents the intention of the code. In addition, it also demonstrates the adequate saturation of the coding frame. The overview of examples can be found in table 5 in the appendix. Subsequently, the coding frame is first manually applied to the collected data. For the translation from Dutch to English, Google Translate is used along manual translation. Subsequently, the coded data offers information which

is then analysed and interpreted to acquire empirical evidence for supporting or rejecting the hypotheses in the next chapter. The results per data source are provided in table 6 in the appendix.

4. Analysis

The analysis starts with an empirically substantiated evaluation of the current accountability regime in AI in public organizations in The Netherlands. In the evaluation, relevant theories, frameworks, and accompanied aspects are addressed in order to adequately present the results with which the hypotheses are tested.

The transition to digital governance in The Netherlands is governed by four strategies. Considering the aim of this thesis, only the National Digitalization Strategy is subject to the assessment as one of the fields at the core of this strategy is AI in public organizations (Veldkamp, 2025). At the same time, accountability in AI is not particularly defined and governed in this strategy. Moreover, the definition of accountability in The Netherlands from a public administrative perspective remains vague, in general and in comparison to other countries (Pérez-Durán, 2024). This poses risks undermining the public debate and decision-making concealing implicit trade-offs among various choices regarding the governance of accountability in AI (Novelli et al., 2023). Nonetheless, several aspects of accountability in AI, their trade-off, and its governance are identified from the collected data according to the framework provided by Novelli and colleagues.

In principle, accountability is traditionally organized by the constitution foremost, through which international and European regulations prevail over domestic regulations (Besselink, 2022). For instance, the United Nations Good Governance principles which contain accountability as a key principle (Sano, 2002), and the European Convention of Human Rights which also outlines accountability values (Pijnenburg, 2025). Also several EU regulations and domestic laws organize accountability to a certain extent. Within the strategy, two instruments are particularly relevant for accountability in AI. First, the Algorithm framework which offers ‘‘an overview of requirements for the application of AI and offers recommendations, instruments, and best practices to meet these requirements’’ based on the ‘‘theme, role, or phase in the lifecycle of the AI (Szabó, 2025, p. 3), implying a robust compliance objective. Second, the voluntary Algorithm register which provides ‘‘more insight into which algorithms the government uses in its processes’’ and which data is used primarily aimed to increase transparency towards citizens (van Dooren, 2025, p. 7; van Marum, 2025c), which resembles both the reporting and oversight objectives.

4.1 Compliance

The data demonstrates the dominance of legal standards by frequently referring to relevant laws and regulations. This significantly emphasizes compliance by adhering to a set of standards by design, development, and/or deployment throughout the entire lifecycle of an AI application. Almost all of these sets of standards differentiating between ethical, legal, and technical norms are obligated. While some choices may offer trade-offs, the legal standards in particular cannot be considered a negotiable option. They must be met by public organizations or others in any case. The decision-maker states that ‘‘this is always necessary, as the principle of legality requires it.’’ Under the rule of law, ‘‘the government must always base its actions on sound, clear legal provisions. The GDPR is also very clear on this point: the processing of personal data must have a legal basis’’ (Wingelaar et al., 2025, p. 34). Also, the EU AI Act prohibits AI practices ‘‘that pose an unacceptable risk to fundamental rights, health, and safety’’ and public organizations are responsible to comply with this regulation and responsible to ensure compliance within their own organization (Zsabó, 2025c, p. 1). As a result, for new AI applications ‘‘that fall under the high-risk provision and that public organizations are considering purchasing, commissioning, or developing themselves,’’ the government advises to ‘‘already carefully consider the requirements of the AI regulation and to take these into account in the procurement or development process’’ (van Dooren, 2025, p. 9). In extent, every single public organization remains responsible for the ‘‘secure use of data, results, and processes, even when the organization outsources their activities’’ (Wingelaar & Muller, 2025, p. 2). For this, the government provides both guidance and training for civil servants to improve their ‘‘AI literacy in relation to their tasks’’ such as developing, purchasing, or operating with AI or algorithm applications (Wingelaar & Muller, 2025, p. 9). In addition, the government recommends to establish specific purchasing conditions (Wingelaar & Muller), which implies that designers, engineers, and producers become legally liable and, thus, bear more accountability characterizing the compliance objective.

Also certain risk assessments are mandatory under the EU regulation, for instance, Article 9 and 26 also mandatory for end-users, which are public organizations in this case (van Dooren, 2025). The Algorithm framework, therefore, aids public organizations with measures and tools to ‘‘meet legal requirements, including measures aimed at scientific assessment, such as verification, validation, accuracy, and bias assessments’’ (Wingelaar et al., 2025, p. 20). For further institutionalizing accountability, the government investigates the ‘‘need and possibilities for improving existing regulations and working methods’’ upon request by the parliament (van Dooren, 2025, p. 7). Beside, the NDS aims to implement the digital standards introduced by the (European)

law in all public organizations (Rijksoverheid, 2025). With these tools, the government aims to ‘‘prevent accidents as much as possible’’ (Wingelaar et al., 2025, p. 20). This explicitly confirms the preventive character of the compliance objective as Novelli and colleagues described.

Furthermore, the decision-maker prefers ethical norms and outlines a framework ‘‘within which public organizations can operate and provide clarity on how generative AI can be deployed in a valuable, responsible, and ethical manner’’ (Szabó, 2025d, p. 2). Also a UNESCO evaluation positively confirms that The Netherlands ‘‘made significant progress in developing policy instruments for ethical development and deployment of AI systems’’ referring to the Algorithm register, the Impact Assessment of Human Rights and Algorithms (IAMA), and the existing framework of European legislation and regulations (van Marum, 2025, p. 15). In addition, the government actively organizes ethics sessions on various related topics in which existing values such as privacy, security, democracy, and well-being are addressed (Muller, 2025). Also several actions are outlined for the development of AI applications ‘‘to counter the negative consequences of online misinformation and disinformation’’ (Muller, 2025, pp. 16-17). The data shows that ethical norms are not just expressed as a preference by words, but also turned into action by concrete policy measures confirming the prioritization of the compliance objective. Nonetheless, an ethics committee ensuring the embeddedness of ethics in procedures and processes is ‘‘considered but not recommended’’ by the government (Wingelaar & Muller, 2025, pp. 9-10), and organizations can now choose between several impact assessments in addition to the Data Protection Impact Assessment (DPIA) or the IAMA in an aim to balance between the opportunities the technology offers and the risks involved (Wingelaar & Muller, 2025).

As for technical norms, the Dutch government outlined clear guidance for increasing the transparency of (generative) AI models with the introduction of suggestive model cards that elaborate on the technical details as well as the possible risks of the model (Wingelaar & Muller, 2025). In addition, the government also actively working on robust policies to ensure technical standards by design, development, and/or deployment throughout the entire lifecycle of an AI application. The decision-maker particularly intends to act in a normative manner ‘‘focusing on standardization of policy and standards’’ to achieve more effective management in digital governance (Muller, 2025, p. 11). For this, the government introduced the Federated Data System (FDS), providing new impetus to use primary data preventing unnecessary copies of data. In particular, ‘‘if public organizations have a legal obligation to process data, the agreements, standards, and safeguards, in the FDS ensure that data of the FDS participants is reused’’ (Muller, 2025, p. 15).

On the other hand, there are some indications for a reporting objective. The Algorithm framework provides, for instance, guidance for establishing explainability and accountability as part of good AI governance, which is also valued by the government (Wingelaar & Muller, 2025). Also the disclosures in the Algorithm register indicates not only the elaboration of conduct, but also the justification of conduct. Yet, disclosing AI applications in the Algorithm register is not mandatory for public organizations and the government is not committed to make it mandatory any time soon (Wingelaar & Boeve, 2025b, p. 34). Hence, on a voluntary basis the Algorithm register offers what it intends: clarity and transparency on algorithms in processes and decision-making in public organization. However, the voluntary character and non-commitment of the government in this context reflect a lack of evidence to support that the Dutch government prioritizes reporting over compliance. Ultimately, the General Administrative Law constitutes that a decision is made correctly and carefully requiring a thorough investigation of information and facts, a careful decision-making process, and sound decision-making, produced by robust legal norms rather than good AI governance through explainability and accountability. Hence, H_1 can therefore be rejected. Evidently, the objectives are not mutually exclusive as Novelli and colleagues predicted. As such, the data provides overwhelming empirical evidence to support H_2, that is, the Dutch government prioritizes compliance over reporting.

4.2 Oversight

Further down the road, the government looks how the Algorithm register can be ‘‘fully filled with disclosed information and what the relevance of this information is in the upcoming years’’ (Wingelaar et al., 2025, p. 19). Indeed, it takes time and resources to analyse existing AI systems and gather and coordinate the necessary information (Wingelaar et al., 2025), indicating a process for the collection of evidence. According to the Dutch Data Protection Authority (DDPA), the progress of disclosing AI and algorithms remains insufficient resulting in a lack of adequate insight regarding compliance to, for instance, EU regulations (van Marum, 2025). Currently, the government is actively developing a working method in which the Algorithm Framework also addresses compliance. For this, the government intends to impose joint (auditable) standards for AI applications in public organizations (van Marum, 2025c). Moreover, the government chooses to focus on further developing European standards in domestic regulations with the intention ‘‘to assess the use, development, and procurement of AI in a governmental context by establishing joint auditable standards for AI applications wherever possible (van Marum, 2025b). In this context, auditable standards indicate the collection of evidence for the objective of oversight. Especially since the DDPA noted that the ‘‘management of AI systems in public organizations requires a more

comprehensive, open, and responsible approach'' that goes beyond the focus on specific laws and regulations embracing a ''more holistic approach to cross-sectoral regulations or the overlap of regulations and other frameworks'' (van Marum, 2025b, pp. 3-4). This requires interplay between systems and organizations that build on each other (van Marum, 2025b), resembling the multilayered factors of accountability highlighted by Novelli et al. (2023). Upon this assessment, the government issued recommendations on the organization of supervision of the AI regulation in The Netherlands, while the government currently develops the details of this supervision structure (van Marum, 2025b).

In extent, the government encourages public organizations to disclose their algorithms in the Algorithms register. For this, the government proactively contacts public organizations and provides assistance with various instruments, such as the ''Algorithm register guidelines, vendor templates, implementation team support, so-called connection sessions, a regional tour, a newsletter, and articles with tips from organizations that have already published'' in the register (van Dooren, 2025, p. 8). This certainly implies the proactive collection of evidence. Besides, the government also checks the registration of an algorithm prior to disclosure in the register (van Dooren, 2025). Aligning with the compliance objective, the decision-maker explicitly confirms the oversight objective stating that ''without oversight, there is no compliance'' (Wingelaar et al., 2025, p. 29). As the main supervisory body for AI in public organizations is the DDPA which evaluates conduct, the government is putting words into action by increasing the budget for the DDPA for algorithm oversight (Wingelaar et al., 2025).

At the same time, as each public organization is responsible for its own IT management, these organizations are also responsible for maintaining internal supervision over their own systems (Szabó, 2025b). The government has implicitly expressed its valuation of transparency and accountability, and views a key role for existing control mechanisms, such as annual departmental reports, policy reviews, and accountability reports, which are all subject to internal and external audits by the central government and the Dutch Court of Audit (Szabó, 2025b). These internal and external accountability structures reflect the evaluation of conduct once more indicating the oversight objective.

Another overwhelming indicator for the oversight objective is the human-in-the-loop mechanism. The DDPA states that additional legislation for risky AI applications concerning automated selection and decision-making is not required if the human-in-the-loop mechanism is ensured (Wingelaar et al., 2025). The government is clear about human intervention in multiple ways. For generative AI, the government states that it is a tool that cannot be assumed any responsibility

(Wingelaar & Muller, 2025). Therefore, civil servants are always required to review the output of generative AI before it is used in communications, policy, or decisions. The decision-maker explicitly considers ‘‘the human dimension absolutely essential’’ (Wingelaar & Boeve, 2025d, p. 51). The government encourages ‘‘all levels of government to actively assess potential bias in (training) data or outcomes when deploying generative AI, and to establish transparent processes and human oversight’’ contributing to a fair, verifiable, and inclusive deployment of AI (Wingelaar & Muller, 2025, p. 9). Therefore, the Algorithm framework incorporates the recommendations of the DDPA to prevent bias, including an human rights impact assessment when using algorithms. In addition, ‘‘it is necessary to ensure human review of a decision by involving someone authorized and competent to make and change a decision’’ (Wingelaar & Muller, 2025, p. 23).

Also the objectives of oversight and enforcement are not mutually exclusive. Hence, the government also maintains governance instruments to suspend or terminate certain AI applications if violations occur (Wingelaar et al., 2025, p. 24). These instruments have already been used multiple times. Also the DDPA can impose sanctions when deemed necessary. Nonetheless, the government explicitly chooses to avoid punitive measures regarding accountability in AI. The decision-maker, for instance, prioritizes to not create ‘‘inability through penalties, fines, and the like’’ in a trade-off against ‘‘providing general advice on what is permissible,’’ which is preferred (Wingelaar et al., 2025, p. 37). The data therefore provides significant evidence supporting H_5 as the Dutch government prioritizes oversight over enforcement, while the evidence then also rejects H_4 in which enforcement is prioritized over oversight.

4.3 Implications & discussion

Contrary to the original expectations, the results of the analysis were surprising considering the extent of the social and financial impact of the Childcare benefit scandal. These findings imply an ex-ante accountability regime in AI in which accountability is used proactively and serves as a virtue, aligning with the theory of Bovens (2010) and predictions of Novelli and colleagues (2023) in the first place. This regime emphasizes that accountability is used as ‘‘normative concept, a set of standards for behaviour of actors, or as a desirable state of affairs’’ (Bovens, 2010). In addition, the fact that accountability in the EU AI Act is used more proactively (Novelli et al., 2023), suggests that in The Netherlands accountability would also be used more proactively. Especially since European laws prevail over domestic Dutch laws (Besselink, 2022). Nonetheless, it demonstrates that The Netherlands as a member state adheres to European regulations. The direct references to the GDPR and EU AI Act in the NDS confirm that as well. At the same time, the government

increased its efforts to align its national standards with future European standards. This is also reflected in the data as most data is coded with indicator 1.1.2 *legal norms*. Overall, it demonstrates the robustness of the rule of law both domestically and in Europe as the positive regime aims to prevent failures or undesired outcomes in AI in public organizations.

Furthermore, 2.1.2 *evaluation of conduct* is the second most coded indicator. Although the supervision structures for the oversight objective currently seem dispersed, the government actively works to improve this. Nonetheless, this does not imply that the current supervision is insufficient, rather it suggests that the supervision structures require modernization. Digitalization and the use of AI exceeds all domain and sector boundaries, meaning that ‘‘supervisory issues increasingly fall under the jurisdiction of different supervisory bodies’’ (Wingelaar & Muller, 2025, p. 7). For example, algorithms in healthcare processing personal data would fall under both the supervision of the DDPA and the Youth Care Inspectorate. In such a situation, these supervisory bodies can ‘‘mutually determine, for example, through a cooperation agreement, how supervision and/or enforcement will be conducted in a specific case’’ (Wingelaar & Muller, 2025, pp. 7-8). It also requires ‘‘coordination and exchange between (many different) supervisory bodies, specifically to ensure consistency in supervision and prevent the accumulation of regulations’’ (Wingelaar & Muller, 2025, p. 8). In this case, the government aims to prevent the ‘many-eyes’ issue that was described by Bovens (2007).

Notwithstanding, this positive approach implies also some negative consequences as it offers limited governance regarding failures and undesired outcomes because it does not anticipate such failures (Novelli et al., 2023). Especially because risks are potentially mitigated, but not eliminated. Even though both the government and the Dutch Data Protection Authority possess instruments to enforce compliance in the form of sanctions, it seems rather insufficient. After the Childcare benefit scandal in 2020, another large-scale failure occurred as a result of an algorithmic process in an public organization. In 2024, the DDPA observed and concluded that the fraud-detection system used by the Education Executive Agency (DUO) produced undesired discriminatory outcomes leading to the termination of this system (Autoriteit Persoonsgegevens, 2024). Most recently in October 2025, the DDPA concluded that more than 50 algorithms within the Dutch Tax Agency are illegal as they breach the basic principles of the GDPR (Strop & Davidson, 2025). This is especially striking because the Tax Agency announced it cannot terminate these systems with immediate effect as demanded by the DDPA and continues to use these illegal algorithms for at least another two years (NOS, 2025). In response, the DDPA only demands a four-monthly reporting by the Tax Agency in the upcoming two years (NOS, 2025). Hence, as effective as the

proactive use of accountability may seem initially, it does not produce the desired state of affairs in which adequate governance of accountability in AI in public organizations prevent such wrongdoings from occurring. Moreover, this does not only undermine accountability as a virtue, but also poses serious risks undermining the rule of law.

Therefore, this thesis would recommend policy and decision-makers to seriously explore the reactive use of accountability and its mechanical structures with an particular emphasis on enforcement objectives. Especially, since no entity is held accountable once more, yet this time, the illegal algorithms cannot even be terminated.

5. Conclusion

Addressing the research question, it is safe to conclude that the objectives of compliance and oversight shape the Dutch accountability regime in AI in public organizations, and the type is the proactive use of accountability. In conclusion, the accountability regime in AI is ex-ante in which accountability serves as a virtue, a desired state of affairs. This regime is positive in the sense that it aims to prevent failures rather than redressing them. It reflects a typically Dutch proverb: *voorkomen is beter dan genezen* which literally translates to ‘prevention is better than curing’ synonymous to ‘better safe than sorry’. On the other side, however, this positive approach does not always result in positive outcomes as discussed in the previous section.

Nonetheless, this thesis contributes to academic accountability literature by confirming the reliability of a differentiated conceptualization of accountability as a virtue and accountability as a mechanism (Bovens, 2010), and confirms a reliable understanding of accountability defined as the ‘‘obligation to inform about, and justify one’s conduct to an authority’’ (Novelli et al., 2023, p. 1872).

Regardless, the results of this thesis remain unreliable for generalization of accountability in AI in the European Union, for example, given the fact that is concerns an in-depth single-case study. In addition, the results of this thesis cannot be extrapolated to accountability in AI in the private domain. However, the approach developed in this thesis may be of inspiration for similar future academic single-case studies concerned with accountability in AI.

As for the title question, whether lessons were learned after the Childcare benefit scandal is hard to conclude based on the results of this thesis. On one hand, the government proactively governs accountability in AI in public organizations, ensuring that the risks are mitigated as much as possible. On the other, however, the recent examples suggest that much still needs to be learned

when it comes to accountability in AI in public organizations, and likely, in the private sector as well given the novelty and continuous development of this technology. Whatever the future may bring, a computer must never make a decision because a computer cannot be held accountable.

Bibliography

Almquist, R., Grossi, G., Van Helden, G. J., & Reichard, C. (2013). Public sector governance and accountability. *Critical Perspectives on Accounting*, *24*(7–8), 479–487. https://doi.org/10.1016/j.cpa.2012.11.005

Autoriteit Persoonsgegevens. (2024). *DUO: Gebruik van geautomatiseerde risicoclassificering op basis van een risicoprofiel bij Controleproces Uitwonende Beurs (CUB)* (p. 24). Autoriteit Persoonsgegevens. https://www.autoriteitpersoonsgegevens.nl/system/files?file=2024-10/Advies%20geautomatiseerde%20besluitvorming%20artikel%2022%20AVG.pdf

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Behn, R. D. (2004). *Rethinking Democratic Accountability*. Rowman & Littlefield.

Besselink, L. (2022). Artikelen 93 en 94: Doorwerking en voorrang internationaal recht. In A. Ellian & B. Rijpkema, *Een Nieuw Commentaar op de Grondwet* (pp. 406–420, 622–625). Boom. https://pure.uva.nl/ws/files/146201055/Besselink_-_Artikelen_93_en_94_GW_met_noten.pdf

Bouwmeester, M. (2023). System failure in the digital welfare state: Exploring parliamentary and judicial control in the Dutch childcare benefits scandal. *Recht Der Werkelijkheid*, *44*(2), 13–37. https://doi.org/10.5553/RdW/138064242023044002003

Bovens, M. (2007). Analysing and Assessing Accountability: A Conceptual Framework. *European Law Journal*, *13*(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Bovens, M. (2010). Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. *West European Politics*, *33*(5), 946–967. https://doi.org/10.1080/01402382.2010.486119

Busuioc, M. (2021). Accountable Artificial Intelligence: Holding Algorithms to Account. *Public Administration Review*, *81*(5), 825–836. https://doi.org/10.1111/puar.13293

Cucciniello, M., & Nasi, G. (2014). Transparency for Trust in Government: How Effective is Formal Transparency? *International Journal of Public Administration*, *37*(13), 911–921. https://doi.org/10.1080/01900692.2014.949754

Dubnick, M. (2005). Accountability and the Promise of Performance: In Search of the Mechanisms. *Public Performance & Management Review*. https://doi.org/10.1080/15309576.2005.11051839

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3518482

Floridi, L. (2013). Distributed Morality in an Information Society. *Science and Engineering Ethics*, *19*(3), 727–743. https://doi.org/10.1007/s11948-012-9413-4

Floridi, L. (2016). Faultless responsibility: On the nature and allocation of moral responsibility for distributed moral actions. *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences*, *374*(2083), 20160112. https://doi.org/10.1098/rsta.2016.0112

Fox, J. (2007). The uncertain relationship between transparency and accountability. *Development in Practice*, *17*(4–5), 663–671. https://doi.org/10.1080/09614520701469955

Frederik, J. (2021). *Zo hadden we het niet bedoeld*. De Correspondent.

Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining Explanations: An Overview of Interpretability of Machine Learning. *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)*, 80–89. https://doi.org/10.1109/DSAA.2018.00018

Grimmer, J., & Stewart, B. M. (2013). Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts. *Political Analysis*, *21*(3), 267–297. https://doi.org/10.1093/pan/mps028

Hardin, G. (1968). The Tragedy of the Commons: The population problem has no technical solution; it requires a fundamental extension in morality. *Science*, *162*(3859), 1243–1248. https://doi.org/10.1126/science.162.3859.1243

Harwood, T. G., & Garry, T. (2003). An Overview of Content Analysis. *The Marketing Review*, *3*(4), 479–498. https://doi.org/10.1362/146934703771910080

Heald, D. (2006). Transparency in historical perspective. In C. Hood & D. Heald (Eds), *Transparency: The Key to Better Governance? Proceedings of the British Academy (135)* (No. 135; pp. 3–23). Oxford University Press. http://www.oup.co.uk/

Hoekstra, M., Dom, L., & van Veenstra, A. F. (2024). *Quickscan AI in de Publieke Dienstverlening III* (No. TNO 2024 R11005; p. 43). TNO Vector.

Hollibaugh, G. E. (2019). The Use of Text as Data Methods in Public Administration: A Review and an Application to Agency Priorities. *Journal of Public Administration Research and Theory*, *29*(3), 474–490. https://doi.org/10.1093/jopart/muy045

Kaler, J. (2002). Responsibility, accountability and governance. *Business Ethics: A European Review*, *11*(4), 327–334. https://doi.org/10.1111/1467-8608.00292

Kaminski, M. E. (2020). Understanding Transparency in Algorithmic Accountability. In W. Barfield (Ed.), *The Cambridge Handbook of the Law of Algorithms* (pp. 121–138). Cambridge University Press. https://doi.org/10.1017/9781108680844.006

Koppell, J. G. (2005). Pathologies of Accountability: ICANN and the Challenge of “Multiple Accountabilities Disorder”. *Public Administration Review*, *65*(1), 94–108. https://doi.org/10.1111/j.1540-6210.2005.00434.x

Kroll, J. A. (2020). Accountability in Computer Systems. In M. D. Dubber, F. Pasquale, & S. Das (Eds), *The Oxford Handbook of Ethics of AI* (p. 0). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190067397.013.10

Kroll, J., Huey, J., Barocas, S., Felten, E., Reidenberg, J., Robinson, D., & Yu, H. (2017). Accountable Algorithms. *University of Pennsylvania Law Review*, *165*(3), 633.

Lindberg, S. I. (2013). Mapping accountability: Core concept and subtypes. *International Review of Administrative Sciences*, *79*(2), 202–226. https://doi.org/10.1177/0020852313477761

Long, S. (2013). *Socioanalytic Methods: Discovering the Hidden in Organisations and Social Systems* (1st edn). Routledge Taylor & Francis Group. https://www.routledge.com/Socioanalytic-Methods-Discovering-the-Hidden-in-Organisations-and-Social-Systems/Long/p/book/9781780491325

Mashaw, J. L. (2006). Accountability and Institutional Design: Some Thoughts on the Grammar of Governance. *Yale Law School*, *Public Law Working Paper*(116), 47.

Miller, T. (2019). Explanation in artificial intelligence: Insights from the social sciences. *Artificial Intelligence*, *267*, 1–38. https://doi.org/10.1016/j.artint.2018.07.007

Ministry of Interior and Kingdom Affairs. (2025). *Handreiking Algoritmeregister—Versie 1.3* (p. 24) [Guidance]. Interprovinciaal Overleg; Vereniging van Nederlandse Gemeenten; Unie van Waterschappen; Ministeries: EZK, LNV, JenV, FIN, IenW en BZK; Rijksdienst voor Ondernemend Nederland; Uitvoeringsinstituut Werknemersverzekeringen; Belastingdienst. https://aienalgoritmes.pleio.nl/attachment/entity/4aa4fc75-a622-44c6-a64a-ce18a7389d2a

Mulgan, R. (2003). Issues of Accountability. In R. Mulgan (Ed.), *Holding Power to Account: Accountability in Modern Democracies* (pp. 1–35). Palgrave Macmillan UK. https://doi.org/10.1057/9781403943835_1

Muller, S. (2025, March 11). *Report of the written correspondence regarding the collection letter of Digitalization (26643, Nr. 1310)*. Tweede Kamer der Staten-Generaal.

https://www.eerstekamer.nl/behandeling/20250311/verslag_van_een_schriftelijk/document3/f=/vmlln3gm1moy.pdf

Nieuwenhuizen, E. (2025). Trust and transparency in algorithmic governance: A multi-level framework. In *Handbook on Trust in Public Governance* (pp. 116–135). Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/book/9781802201406/chapter8.xml

NOS. (2025, December 3). *Belastingdienst blijft privacyschendende systemen nog zeker twee jaar gebruiken*. https://nos.nl/nieuwsuur/artikel/2593055-belastingdienst-blijft-privacyschendende-systemen-nog-zeker-twee-jaar-gebruiken

Novelli, C., Taddeo, M., & Floridi, L. (2023). Accountability in artificial intelligence: What it is and how it works. *AI & SOCIETY*, *39*(4), 1871–1882. https://doi.org/10.1007/s00146-023-01635-y

Pérez-Durán, I. (2024). Twenty-five years of accountability research in public administration: Authorship, themes, methods, and future trends. *International Review of Administrative Sciences*, *90*(3), 546–562. https://doi.org/10.1177/00208523231211751

Pijnenburg, A. (2025). Accountability for violations of economic, social and cultural rights. In K. Henrard & M. Duin, *Research Handbook on Accountability for Human Rights Violations* (pp. 182–196). Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/book/9781035306930/chapter11.xml

Porumbescu, G., Meijer, A., & Grimmelikhuijsen, S. (2022). *Government Transparency: State of the Art and New Perspectives*. Cambridge University Press. https://doi.org/10.1017/9781108678568

Rijksoverheid. (2025, June). *De Nederlandse Digitaliseringsstrategie*. Rijksoverheid. https://www.eerstekamer.nl/overig/20250704/de_nederlandse/document

Rubenstein, J. (2007). Accountability in an Unequal World. *Journal of Politics*, *69*(3), 616–632. https://doi.org/10.1111/j.1468-2508.2007.00563.x

Sano, H.-O. (2002). Good Governance, Accountability and Human Rights. In *Human Rights and Good Governance* (pp. 123–146). Brill Nijhoff. https://doi.org/10.1163/9789004479357_009

Schedler, A. (1999). Conceptualizing accountability. *The Self-Restraining State: Power and Accountability in New Democracies*, *14*. https://books.google.com/books?hl=en&lr=&id=MD8Vx1HLOZgC&oi=fnd&pg=PA13&dq=info:fUHqEpMeRhsJ:scholar.google.com&ots=-nP3sqtQQ3&sig=j_Vka1IIHBzWf5u5x8gMQoy1xAY

Schillemans, T., & Busuioc, M. (2015). Predicting Public Sector Accountability: From Agency Drift to Forum Drift. *Journal of Public Administration Research and Theory*, *25*(1), 191–215. https://doi.org/10.1093/jopart/muu024

Sinclair, A. (1995). The chameleon of accountability: Forms and discourses. *Accounting, Organizations and Society*, *20*(2–3), 219–237.

Srinivasan, R., & San Miguel González, B. (2022). The role of empathy for artificial intelligence accountability. *Journal of Responsible Technology*, *9*, 100021. https://doi.org/10.1016/j.jrt.2021.100021

Strop, J.-H., & Davidson, D. (2025, October 11). Meer dan 50 algoritmes van de Belasting-dienst zijn illegaal, zegt de Autoriteit Persoons-gegevens. *FTM*. https://www.ftm.nl/artikelen/meer-dan-50-algoritmes-van-de-belasting-dienst-zijn-onrechtmatig

Szabó, F. Z. (2025a, January 8). *Letter from the State Secretary of Internal and Kingdom Affairs (26643, Nr. H, 36382, CXLVII)*. Eerste Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250108/brief_van_de_staatssecretaris_van/document3/f=/vmk2jo617kzl.pdf

Szabó, F. Z. (2025b, March 12). *Letter from the government: Overview governmental ICT of the national government (26643, Nr. 1314)*. Tweede Kamer der Staten-Generaal.

https://www.eerstekamer.nl/behandeling/20250312/brief_regering_overzicht_overheids/document3/f=/vmlln3gm1np1.pdf

Szabó, F. Z. (2025c, March 17). *Letter the from government: Response on request from the committee regarding inquiries into prohibited AI systems (26643, Nr. 1326)*. Tweede Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250317/brief_regering_reactie_op_verzoek_4/document3/f=/vmlsn0r2n6wk.pdf

Szabó, F. Z. (2025d, April 22). *Letter from the government: Government opinion on generative AI (26643, 29362, Nr. 1331)*. Tweede Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250422/brief_regering_overheidsbreed_2/document3/f=/vmnc2dyknnzj.pdf

Tomazevic, N. (2019). Social Responsibility and Consensus Orientation in Public Governance: A Content Analysis. *Central European Public Administration Review (CEPAR)*, *17*(2), 189–204.

Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Roberts, H., Taddeo, M., & Floridi, L. (2022). The ethics of algorithms: Key problems and solutions. *AI & SOCIETY*, *37*(1), 215–230. https://doi.org/10.1007/s00146-021-01154-8

van Dam, C. J. L., Kuiken, A. H., van Aalst, R. R., Leijten, R. M., Belhaj, S., van der Lee, T. M. T., van Wijngaarden, J., & Kooten-Arissen, F. M. (2020). *Ongekend onrecht* (p. 132) [Parliamentary Inquiry Committee]. Tweede Kamer der Staten-Generaal. https://www.tweedekamer.nl/sites/default/files/atoms/files/20201217_eindverslag_parlementaire_ondervragingscommissie_kinderopvangtoeslag.pdf

van Dooren, W. A. J. M. (2025, May 7). *Written correspondence with State Secretary of Internal and Kingdom Affairs regarding the report 'Focus op AI bij de Rijksoverheid' by the Court of Audit (26643, Nr. J)*. Eerste Kamer der Staten-Generaal.

https://www.eerstekamer.nl/behandeling/20250507/verslag_van_een_schriftelijk_2/document3/f=/vmnciz7svxye.pdf

van Huffelen, A. C. (2023, May 24). *Letter from the State Secretary of Internal and Kingdom Affairs to the Speaker of the Parliament (26.643, Nr. 1029)* [Governmental letter]. Tweede Kamer der Staten-Generaal.

van Marum, E. (2025a, July 11). *Letter from the government: Collection letter regarding Digitalization Q2 (26643, Nr. 1371)*. Tweede Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250711/brief_regering_verzamelbrief/document3/f=/vmp5jyhynprn.pdf

van Marum, E. (2025b, August 21). *Letter from the government: Cabinet's response on the report AI & Algorithm Risks Netherlands by the Dutch Data Protection Authority (26643, Nr. 1382)*. Tweede Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250821/brief_regering_kabinetsreactie_op/document3/f=/vmq4iimc4pyv.pdf

van Marum, E. (2025c, September 9). *Letter from the government: Development Algorithm framework and register (26643, Nr. 1394)*. Tweede Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250909/brief_regering_doorontwikkeling/document3/f=/vmqnih89lzzk.pdf

Veldkamp, C. C. J. (2025, May 16). *Letter from Minister of Foreign Affairs: Communication on AI Continent Action Plan (22112, 26643, Nr. 4059)*. Tweede Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250516/brief_regering_fiche_mededeling_ai_2/document3/f=/vmno26zfs5zv.pdf

Widlak, A., van Eck, M., & Peeters, R. (2020). *Towards principles of good digital administration: Fairness, Accountability and Proportionality in Automated Decision Making* (SSRN Scholarly Paper No. 3771857). Social Science Research Network. https://papers.ssrn.com/abstract=3771857

Wingelaar, N. T. P., & Boeve, L. (2025a, March 11). *Report of the committee debate, held on 30 Januari 2025, regarding emerging and future technologies (26643, Nr. 1311)*. Tweede Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250311/verslag_van_een_commissiedebat/document3/f=/vmllhbrkfxvj.pdf

Wingelaar, N. T. P., & Boeve, L. (2025b, May 28). *Report of the committee debate, held on 23 April 2025, regarding Digitalizing government (26643, Nr. 1345)*. Tweede Kamer der Staten-Generaal. https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?id=2025Z10906&did=2025D19692

Wingelaar, N. T. P., & Boeve, L. (2025c, September 26). *Legislative correspondence: Q&A list regarding the Dutch Digitalization Strategy (26643, Nr. 1401)*. Tweede Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250926/lijst_van_vragen_en_antwoorden_2/document3/f=/vmr6myor4xyx.pdf

Wingelaar, N. T. P., & Boeve, L. (2025d, October 20). *Report of the deliberation, held on 29 September 2025, regarding the Dutch Digitalization Strategy (26643, Nr. 1427)*. Tweede Kamer der Staten-Generaal. https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?id=2025Z14285&did=2025D44605

Wingelaar, N. T. P., & Muller, S. (2025, August 29). *Legislative correspondence: Q&A list regarding government opinion on generative AI (26643, Nr. 1331)*. Tweede Kamer der Staten-Generaal. https://www.eerstekamer.nl/behandeling/20250829/lijst_van_vragen_en_antwoorden/document3/f=/vmqee00tgxpn.pdf

Wingelaar, N. T. P., Nijhof-Leeuw, J. M., & Boeve, L. (2025, February 18). *Report of the committee debate, held on 28 January 2025, regarding algorithm applications and data-ethics within the government (26643, Nr. 1283)*. Tweede Kamer der Staten-Generaal. https://www.tweedekamer.nl/kamerstukken/commissieverslagen/detail?id=2024Z11902&did=2025D04120

Yanovitzky, I., & Weber, M. (2020). Analysing use of evidence in public policymaking processes: A theory-grounded content analysis methodology. *Evidence & Policy*, *16*(1), 65–82. https://doi.org/10.1332/174426418X15378680726175

Young, M., Katell, M., & Krafft, P. M. (2019). Municipal surveillance regulation and algorithmic accountability. *Big Data & Society*, *6*(2), 205395171986849. https://doi.org/10.1177/2053951719868492

Appendix

Table 1)

Examples of traditional accountability types (Novelli et al., 2023, p. 1874)

Features	**Examples**		
Context (what for?)	Electoral	Juridical	Administrative
Range (about what?)	Choices of political direction, laws, and recruitment	Conducts, omissions, and decisions	Policy implementation
Agent (who?)	Representatives, leaders, parties, governments, and institutional bodies	Natural persons, legal persons, states, and assets	Public officials and institutions
Forum (to whom?)	Citizens, voters, taxpayers, political parties, and institutions	Individual and collective entities (including states and courts)	Citizens, auditors, inspectors, and ombudsman
Standard (according to what?)	Reliability, coherence, and ideology	Legal rules, principles, and precedents	Efficiency, effectiveness, and legal norms
Process (how?)	Public debate (media), internal or external vigilance (e.g., judicial review), and elections	Judicial and extra-judicial review	Auditing, internal supervision, and judicial review
Implications (what follows?)	Electoral outcomes, political reputation, careers, and funding	Reparations, remands, detentions, fines, and prohibitions	Certifications, validations, revocations, penalties, suspensions, and seizures

Table 2)

Accountability features in AI (Novelli et al., 2023, p. 1878)

Features	Sub-features		
Context (What for?)	*By field* Finance, healthcare, justice, military, commerce, engineering, automotive, and public administration	*By function* Natural language processing, machine vision, information retrieval, filtering, classification, and robot control	*By level of autonomy* Manual control, action support, shared control, decision support, blended decision-making, automated decision-making, and full automation
Range (About what?)	*Design* Planning, audience focus, architecture design, data strategy, development strategy, and interfaces design	*Development* Coding, implementation, model training (e.g., data processing), security mechanisms (IP protection), testing, and integration	*Deployment* Monitoring, maintenance, and use
Agent (Who?)	*Individuals* AI designer, data experts, AI developers, manufacturers, and domain practitioners	*Hierarchies* Patent-holders, managers, superiors, supervisors, and testers	*Corporate or collective* Policy-makers, development firms, data controllers, and shareholders
Forum (To whom?)	*Individuals* Decision-subjects, data-subjects, and domain practitioners (e.g., customers and users)	*Hierarchies* Managers, superiors, and supervisors	*Corporate or collective* Citizens, shareholders, external bodies, authorities, and institutions
Standard (According to what?)	*Legal* Torts, crimes, unfair commercial practices, privacy, and risk tolerance (e.g., EU AI Act)	*Ethical* Fairness, transparency, human autonomy, inclusion, vulnerability, trustworthiness, and sustainability	*Technical* Robustness, adaptability, accuracy, efficiency, maintainability, (cyber)security, and self-healing
Process (How?)	*Internal* Internal audits, simulations, self-assessments, and post-market monitoring	*Human-Machine Interaction* Feedback loops, supervisory controls, and interactive machine learning	*External* Systems validation, external audits, external conformity and impact assessment, ombudsman, and judicial reviews
Implications (What follows?)	*Decisions* Recommendations, approvals, refusals, and prohibitions	*Lawful facts* Reputation, market profit or loss	*Unlawful facts* Reparation, remands, fines, disciplinary measures, detentions, suspensions, revision, and revocation

Table 3)

Type of accountability regimes in AI in public organizations (Novelli et al., 2023, p. 1880)

Proactive use of accountability in AI	Reactive use of accountability in AI
Positive sense: accountability as a virtue Planning purpose: it comes before events and aims to prevent failures	Negative sense: accountability as a mechanism Responsive purpose: it comes after events and aims to redress failures
Objectives: - Compliance - Oversight	Objectives: - Report - Enforcement
Ex-ante accountability regime	Ex-post accountability regime

Table 4)

List of collected data

Collected data, from dossier ICT (26.643)

Document number and link	*Document type*	*Theme*	*Date*
26643, H, 36382, CXLVII	Letter from the State Secretary of the Interior and Kingdom Affairs	NDS	08-01-2025
26643, 32761, Nr. 1283	Report of the committee debate	Digitalization	18-02-2025
26643, Nr. 1310	Report of written correspondence	Digitalization	11-03-2025
26643, Nr. 1311	Report of the committee debate	EU AI Act	11-03-2025
26643, Nr. 1314	Letter from the government	NDS	12-03-2025
26643, Nr. 1326	Letter from the government	AI (applications)	17-03-2025
26643, Nr. 1331	Letter from the government	AI (applications)	22-04-2025
26643, J	Written correspondence	AI (applications)	07-05-2025
26643, Nr. 1345	Report of the committee debate	Digitalization	28-05-2025
26643	The Dutch Digitalization Strategy	NDS	June 2025
26643, Nr. 1371	Letter from the government	Digitalization	11-07-2025
26643, Nr. 1382	Letter from the government	AI (applications)	21-08-2025
26643, Nr. 1331	Legislative correspondence	AI (applications)	29-08-2025
26643, Nr. 1394	Letter from the government	Algorithm (applications)	09-09-2025
26643, Nr. 1401	Legislative correspondence	NDS	26-09-2025
26643, Nr. 1427	Report of the deliberation	NDS	20-10-2025
26643, Nr. 1435	Letter from the government	Digitalization	17-11-2025

Table 5)

Examples per indicator of the coding frame

Code	Data	Source
1.1.1.	This position paper provides a solid foundation for reaping the benefits of this promising technology organized by the central government. It outlines a framework within which public organizations can operate and provides clarity on how generative AI can be deployed in a valuable, responsible, and ethical manner (Szabó, 2025d, p. 2)	26643, Nr. 1331
1.1.2.	With the entry into force of the AI regulation, additional obligations have been created for AI systems, including AI systems for facial recognition. I would like to note that the General Data Protection Regulation, the GDPR, is the primary legal instrument for regulating facial recognition technology. This framework imposes strict requirements on the processing of biometric data for the identification of a person trough, for example, facial recognition. Due to its impact on data protection, facial recognition is a key focus for the Dutch Data Protection Authority, who oversees it (Wingelaar & Boeve, 2025, p. 18)	26643, Nr. 1311
1.1.3.	There are several ways to make (generative) AI models more transparent. Users can benefit from clear and concise model cards – instructions detailing the technical details and potential limitations of the AI model in question. Such an instruction leaflet can help (end) users determine whether a model is suitable for a specific application and whether there are any potential risks associated with its use. The Dutch Data Protection Authority also points this out in its AI & Algorithm Risk Report for The Netherlands in autumn 2023 (Wingelaar & Muller, 2025, p. 22)	26643, Nr. 1385
2.1.1.	With the Algorithm register, I want to give citizens and enterprises more insight into which algorithms the government uses in its processes. Discussions are currently underway, including fellow government bodies, about the best way to inform citizens about the algorithms and the Algorithm register. […] as decision-making can also provide insight into the algorithms used and may even allow for referral to the Algorithm register (van Dooren, 2025, p. 7)	26643, J

2.1.2.	The Algorithm register offers room to disclose the results of the human rights assessment (Szabó, 2025, pp. 3-4).	26643, 36382, CXLVII, H
3.1.1.	[The government] is also looking how the Algorithm register can be fully filled with disclosed information and what the relevance of this information is in the upcoming years. In particular, the relevance for journalists, scientists, but also citizens, enterprises, and the [the government] itself (Wingelaar et al., 2025, p. 19)	26643, 32761, 1283
3.1.2.	[…] I take the focus on further development of European standards to heart, as this will help meet the requirements for high-risk systems. In line with this, I want to more consistently assess the use, development, and procurement of AI in a government context by establishing joint (auditable) standards for AI use wherever possible. This will be further developed within the framework of the NDS (van Marum, 2025b, p. 2)	26643, Nr. 1382
3.1.3.	I believe that it's important that employees review the output of generative AI before using it in communications, policy, or decision. The government-wide guidelines on generative AI contain recommendations for end-users, including critically assessing the result of generative AI, for example, for potential biases or hallucinations. Regarding responsibility for the results: generative AI is a tool and cannot assume any responsibility (Wingelaar & Muller, 2025, pp. 8-9)	26643, Nr. 1385
4.1.1.	[…] I also look at which measures or instruments are needed. […] Besides, the Algorithm register will be filled providing an overview of high-risk algorithms. As it turns out that there are illegal algorithms among them, they will be terminated (Wingelaar et al., 2025, p. 24)	26643, 32761, 1283
4.1.2.	A lot of ‘‘naming-and-shaming’’ has been done, and public organizations and ministries have been addressed to organise their accessibility [in AI and algorithms] for a long time (Wingelaar et al., 2025, p. 18)	26643, 32761, 1283

Table 6)

List of coded data, per collected data source

Data source: 26643, H, 36382, CXLVII

Code	*Data*
1.1.1	The cabinet encourages public organizations to conduct human rights assessments when deploying algorithms and AI. The European AI Act requires a human rights assessment for high-risk AI systems used by governmental organizations (Szabó, 2025, p. 3)
1.1.2	The State Secretary stresses the importance of the protection of fundamental rights, such as privacy, non-discrimination, and (judicial) autonomy regarding AI applications in the judiciary as a result of increasing technological innovations due to a decline in staff and increase in legal cases (Szabó, 2025, p. 3)
1.1.3	The 'Algorithm framework' provides an overview of requirements for the application of AI and offers recommendations, instruments, and best practices to meet these requirements. These requirements are outlined based on the theme, role, or phase in the lifecycle of the AI (Szabó, 2025, p. 3)
2.1.1	The importance of an open-source community is that a broad audience can review the source code of publicly disclosed software. This builds trust because independent individuals, i.e., those with no vested interest in the software's operation, can see how it works from the outside. The open-source communities we're discussing here are inherently voluntary and not strictly organized. They are not accountable to anyone, either legally or financially (Szabó, 2025, p. 2) The ministries have promised the parliament to at least disclose their high-risk AI applications (according to the EU AI Act) by the end of 2025 in the Algorithms register (Szabó, 2025, p. 4)
2.1.2	The Algorithm register offers room to disclose the results of the human rights assessment (Szabó, 2025, pp. 3-4)
3.1.1	-
3.1.2	-
3.1.3	-
4.1.1	-
4.1.2	-

Data source: 26643, 32761, Nr. 1283

Code	*Data*
1.1.1	-
1.1.2	In the Algorithm framework, for example, provides measures and tools to help public organizations meet legal requirements, including measures aimed at scientific assessment, such as verification, validation, accuracy, and bias assessments (Wingelaar et al., 2025, p. 20) […] ensuring that these instruments are seriously utilized to prevent accidents as much as possible (Wingelaar et al., 2025, p. 20) The effective and responsible use of algorithms is, of course, linked to the quality of the data it uses. The Algorithm register provides space for including information about the data used. However, this option is not always used. Yet, the most impactful algorithms use personal data. The GDPR sets specific rules for sharing and disclosing this [personal] data (Wingelaar et al., 2025, pp. 25-26) I would like to add that each ministry is, of course, responsible for assessing whether algorithms are used, for what purpose, and how they are subsequently used. Whether for law enforcement, service provision, or emergency services, we must ensure appropriate regulations. This is always necessary, as the principle of legality requires it. The government must always base its actions on sound, clear legal provisions. The GDPR is also very clear on this point: the processing of personal data must have a legal basis (Wingelaar et al., 2025, p. 34)
1.1.3	The Algorithm framework offers therefore already a as complete as possible overview of the rules to which public organizations must adhere, and the measures that public organizations can implement for that (Wingelaar et al., 2025, p. 19) There can be mistakes in the data or models leading to bias or arbitrariness. I commit to transparency through the Algorithm register, which can provides us more insight about this. Also with the Algorithm framework I offer public organizations assistance to prevent bias or arbitrariness in algorithms (Wingelaar et al., 2025, p. 21)
2.1.1	The Dutch Data Protection Authority emphasizes in its advise that such automations must require several safeguarding. For example, it must be periodically monitored for

	discrimination and ensure sufficient transparency. In response, [the government] started analysing case studies in relation to selection-instruments in the current implementation practices (Wingelaar et al., 2025, p. 19) [The government is] currently analysing, through online consultation on Algorithmic Decision-Making, and the General Administrative Law (Awb), which additional measures are needed to improve transparency, among other things (Wingelaar et al., 2025, p. 31)
2.1.2	-
3.1.1	[The government] is also looking how the Algorithm register can be fully filled with disclosed information and what the relevance of this information is in the upcoming years. In particular, the relevance for journalists, scientists, but also citizens, enterprises, and the [the government] itself (Wingelaar et al., 2025, p. 19) It does indeed take time and resources to analyse existing [AI] systems and gather and coordinate the necessary information. As far as I know, an inventory has been completed at government departments. I assume the departments are now preparing for the next phase. To determine high-risk AI systems, for which I have written a guideline for inventorying, identifying, and classifying AI systems. I hope this helps public organizations to accurately assess their AI systems (Wingelaar et al., 2025, p. 30)
3.1.2	At the moment in which the potentials of AI and algorithms in public organizations enjoy most attention, the Dutch Data Protection Authority's advisory report confirmed once more that the responsible deployment of AI and algorithms within public organizations requires sharp attention, highlighting the potential opportunities, but also the negative aspects and potential risks (Wingelaar et al., 2025, p. 19) Without oversight, there is no compliance. Finally, I would also like to emphasize the importance of independent oversight of algorithms and AI within public organizations. In 2025, the government will increase the budget for algorithm oversight at the Dutch Data Protection Authority. […] In addition, the supervision of the AI regulations is currently being prepared, and the cabinet, under the direction of the Minister of Economic Affairs, will provide the parliament with a government opinion on the supervision of the AI regulation this year. Public organizations also fall under this

supervisory system. Together with the [public organizations], I am committed to further developing the framework known as horizontal oversight. Essentially, I want to encourage democratic oversight among [public organizations], including the use of algorithm and AI applications. Therefore, I want to incorporate this aspect into the Dutch Digitalization Strategy, which I am working on (Wingelaar et al., 2025, p. 20)

Does the State Secretary agree that the Algorithm register plays an essential role in providing citizens with insight into why a particular decision was made?
The Algorithm register does indeed play a significant role in transparency for citizens (Wingelaar et al., 2025, p. 29)

3.1.3 Automated selection instruments and automated decision-making are indispensable for the government to perform tasks efficiently. The Dutch Data Protection Authority suggests that it does not require particular lawmaking for such risky instruments. At least, only when the consequences for the concerned individual establishes after meaning human intervention (Wingelaar et al., 2025, p. 19)

I take the Dutch Data Protection Authority's recommendations to heart. They have already been incorporated as much as possible into the Algorithm framework. For example, you could consider tools in the field of bias assessments or providing information about how to organize human intervention [in AI applications]. My goal is […] to check which measures and instruments are further needed to help public organizations to meet the requirements suggested by the Dutch Data Protection Authority. These will be implemented in the Algorithm framework (Wingelaar et al., 2025, p. 20)

I want to emphasize that after risk selection, a human being must always consider what needs to be done and whether, for example, control is necessary. The human dimension remains important when using risk selection. In that context, I can say the following about the human aspect. I always emphasize, also at the ministry, that the civil servant, when performing their duties, must always put themselves in the shoes of a citizen or company – the recipient – in order to carry out their processes as effectively as possible. If there are any improvements, they must report them (Wingelaar, pp. 23-24)

	Human intervention must be meaningful. This means that the official handling the case must be able to assess whether selection is justified in a particular case (Wingelaar et al., 2025, p. 24) However, it is not just about the tool itself, but also about how it is used. I want to emphasize that the tool is not, and certainly should not be used for automated decision-making regarding the next steps for a young suspect. This tool, this algorithm, must be used as a guideline for a decision alongside other information about the same young suspect. In other words, the decision is made by the Public Prosecution Service in consultation with the relevant partners. This means there is – or should be – substantial human intervention, as prescribed by the Dutch Protection Authority (Wingelaar et al., 2025, p. 35)
4.1.1	[…] I also look at which measures or instruments are needed. […] Besides, the Algorithm register will be filled providing an overview of high-risk algorithms. As it turns out that there are illegal algorithms among them, they will be terminated (Wingelaar et al., 2025, p. 24) Public organizations are actively encouraged to map their current AI systems. Any prohibited AI system must be stopped. Prohibited AI practices are AI systems that pose such a risk of violating fundamental rights, health, and safety that they are not permitted (Wingelaar et al., 2025, p. 27) In the Netherlands, we could shift the focus to providing general advice on what is permissible, rather than creating inability to act through penalties, fines, and the like. The government play a role in this. This is a rather fundamental discussion, or rather, a vision, as you would like, for how the Dutch Data Protection Authority will fulfil its duties in the future (Wingelaar et al., 2025, p. 37)
4.1.2	A lot of ‘‘naming-and-shaming’’ has been done, and public organizations and ministries have been addressed to organise their accessibility [in AI and algorithms] for a long time (Wingelaar et al., 2025, p. 18)

Data source: 26643, Nr. 1310

Code	*Data*
1.1.1	The Dutch government organizes ethics sessions on various topics related to digitalization. Each year, the government selects various topics within the theme of digitalization based on specific technical applications and then engages in discussions with citizens, enterprises, end users, and professionals who work with the technology. During these sessions, existing values such as privacy, security, democracy, and well-being (including that of children) are addressed. The outcomes of these sessions serve as input for policy and/or regulations (Muller, 2025, p. 16) In Jun 2024, the progress letter on the government-wide disinformation strategy was shared with the parliament. Most of the actions outlined in this letter are currently underway or will be initiated this year. One example of an action is a comparative study of various forms of content moderation […]. The government is also encouraging the development of AI applications to counter the negative consequences of online misinformation and disinformation (Muller, 2025, pp. 16-17).
1.1.2	-
1.1.3	It is therefore my commitment to work together to achieve more effective management of our digital government, with the intention of acting in a normative manner, when necessary, focusing on standardization of policy and standards (Muller, 2025, p. 11) With the introduction of the Federated Data System (FDS), [the government is] giving new impetus to using data the source, instead of public organizations making unnecessary copies [of the data]. If public organizations have a legal obligation to process data, the agreements, standards, and safeguards, in the FDS ensure that the data of FDS participants is reused, so that the data does not have to be requested again from citizens and enterprises. Compliance regarding monitoring [of the FDS] still needs to be further developed. It should be noted, however, that the 'once-only principle' is not absolute. Several legal exceptions apply. For example, if data is needed in which case this data may still be requested again (Muller, 2025, p. 15)
2.1.1	-
2.1.2	-
3.1.1	Because [the government is] working according to an ''open approach,'' and this manual is an open-source product, all stakeholders can provide their input and

	feedback within [platform] of the Ministry of the Interior and Kingdom Relations (Muller, 2025, p. 14)
3.1.2	-
3.1.3	-
4.1.1	-
4.1.2	-

Data source: 26643, Nr. 1311

Code	*Data*
1.1.1	As a sole government, I want to set a good example by focusing on the responsible application of AI. This means paying attention to opportunities and scaling up, safeguarding public interests, and modernizing our services (Wingelaar & Boeve, 2025, p. 13) Then there is the question from Ms. Koekkoek of Volt whether the State Secretary and the cabinet share the ambitious safeguards for AI, such as freedom of information, etc. Yes I am committed to the responsible use of new technology. It is important that any negative consequences the use of technology may have on our public values, human rights, and fundamental rights are limited and prevented; that goes without saying. This applies to AI, but also to other technologies I'm discussing today. (Wingelaar & Boeve, 2025, p. 16). Yes, I agree that the Netherlands needs alternatives to these kinds of AI developments, based on public values (Wingelaar & Boeve, 2025, p. 16)
1.1.2	Mr. Six Dijkstra of NSC sees a trend emerging where we allow real-time facial recognition in public spaces. Can the State Secretary ensure that the AI Act is enforced by the government and the business community and that anonymity in public spaces is not suspended? With the entry into force of the AI regulation, additional obligations have been created for AI systems, including AI systems for facial recognition. I would like to note that the General Data Protection Regulation, the GDPR, is the primary legal instrument for regulating facial recognition technology. This framework imposes strict requirements on the processing of biometric data for the identification of a person through, for example, facial recognition. Due to its impact on data protection, facial

	recognition is a key focus for the Dutch Data Protection Authority, who oversees it (Wingelaar & Boeve, 2025, p. 18) Real-time facial recognition and other forms of biometric identification in public spaces are prohibited, except in very specific cases such as national security. One example is the temporary use of facial recognition in serious incidents, such as the search for missing persons or to prevent terrorist attacks (Wingelaar & Boeve, 2025, p. 30)
1.1.3	-
2.1.1	-
2.1.2	-
3.1.1	-
3.1.2	-
3.1.3	-
4.1.1	-
4.1.2	-

Data source: 26643, Nr. 1314

Code	*Data*
1.1.1	-
1.1.2	-
1.1.3	-
2.1.1	-
2.1.2	-
3.1.1	-
3.1.2	Each [public organization] is responsible for its own IT management. All parts of the central government are responsible for maintaining internal supervision over their own systems. […] The government values transparency and accountability and sees a key role for existing control mechanisms in this regard. Departmental annual reports, policy reviews, and accountability reports provide insight into policy expenditures and results. These are subject to internal and external audits by the Central Government Audit Service, and the Court of Audit, respectively (Szabó, 2025b, p. 1)
3.1.3	-
4.1.1	-
4.1.2	-

Data source: 26643, Nr. 1326

Code	*Data*
1.1.1	-
1.1.2	-
1.1.3	-
2.1.1	-
2.1.2	-
3.1.1	-
3.1.2	The European AI Regulation (hereinafter: AI regulation) prohibits, from February 2, 2025, AI practices that pose an unacceptable risk to fundamental rights, health, and safety, such as manipulative AI and social scoring. Under this system, [public organizations] are responsible for complying with the AI regulation and ensuring compliance within their own organization (Szabó, 2025c, p. 1) In early November 2024, [the government] issues a formal information request (hereinafter: request) to departmental Chief Information Officers (CIOs) requesting information about AI systems that fall under prohibited AI practices, as defined in Article 5 of the AI Regulation (hereinafter: prohibited AI systems). I personally have a coordinating role with the departments, setting the framework, providing support, and, where necessary, encouraging action. The scope of this request covered the entire department, including the relevant implementing bodies, agencies, inspectorates, and independent administrative bodies (ZBOs) that fall under the responsibility of the relevant ministry. To support the inventory, [the government] developed and issued a guideline providing guidance for identifying and classifying AI systems. Based on this guideline, the departmental assessment was made as to whether prohibited AI systems were being used. […] In the submitted data, ministries reported that within their own ministry, or within organizations under ministerial responsibility, no AI systems are used that fall under the prohibited AI practices listed in Article 5 of the AI regulation. Furthermore, no systems were reported that were in use and discontinued as a result of the inventory (Szabó, 2025c, pp. 1-2)
3.1.3	-
4.1.1	-
4.1.2	-

Data source: 26643, Nr. 1331

Code	*Data*
1.1.1	This position paper provides a solid foundation for reaping the benefits of this promising technology organized by the central government. It outlines a framework within which public organizations can operate and provides clarity on how generative AI can be deployed in a valuable, responsible, and ethical manner (Szabó, 2025d, p. 2)
1.1.2	-
1.1.3	-
2.1.1	-
2.1.2	-
3.1.1	-
3.1.2	-
3.1.3	-
4.1.1	-
4.1.2	-

Data source: 26643, J

Code	*Data*
1.1.1	-
1.1.2	The cabinet believes that citizens should be able to know how a decision, including one prepared or taken using algorithms, was reached. Transparency in this regard contributes to a reliable government. For this reason, I am investigating the need and possibilities for improving existing regulations and working methods. My predecessor promised this to the parliament in 2023. In 2024, during the consultation on the bill 'Strengthening the Guarantee Function of the General Administrative Law Act', the reflection document 'Algorithmic Decision-Making and the General Administrative Law Act' was also submitted for consultation. The responses to this document have been collected and are being analysed. The analysis will be sent to the parliament shortly. I will provide the senate with a copy (van Dooren, 2025, p. 7) Through the Algorithm framework, I provide government-wide insight into the assessment frameworks and risk analyses that must be met. One of these, is the

mandatory risk assessment required under Articles 9 and 27 of the EU AI Act during the development and use of a high-risk AI system, respectively. This obligation rests with the provider (the party placing the system on the market) and the user (in this case, the government). In my coordinating role, I support organizations in this process. The requirements for the responsible use of algorithms and AI are evolving rapidly. Many new possibilities, as well as new laws, regulations, standards, and instruments, are emerging in relatively short time. The Algorithm framework provides insight into how minimum standards are met, responsible use is ensured, and which instrument should be applied when. The Impact Assessment on Human Rights and Algorithms is a useful tool for risk analysis and can be found through the Algorithm framework (van Dooren, 2025, p. 8)

I agree that it is important for public organizations to properly prepare for the requirements from the AI regulation. The deadline for existing AI systems in public organizations with the opportunity in the coming years to gradually work towards the requirements for high-risk AI systems under the AI regulation. These AI systems must already comply with existing laws and regulations, such as the General Administrative Law Act (Awb) and the GDPR (van Dooren, 2025, p. 9)

For (new) AI systems that fall under the high-risk provisions and that public organizations are considering purchasing, commissioning, or developing themselves, it is highly advisable to already carefully consider the requirements of the AI regulation and to take these into account in the procurement or development process (van Dooren, 2025, p. 9)

In August 2024, the Council of the European Union adopted a decision authorizing the European Commission to sign, on behalf of the European Union, the Framework Convention on AI and the Protection of Human Rights, Democracy, and the Rule of Law. The EU signed the treaty on September 5th, 2024. This means the framework convention has also been signed on behalf of the Netherlands. […] The government supports a successful ratification. The European Commission is currently in the process of ratifying the treaty on behalf of the entire European Union, including the Netherlands (van Dooren, 2025, p. 10)

	The AI regulation sets requirements that all developers of high-risk AI must comply with to ensure the protection of fundamental rights and mitigate risks. For example, a quality management system is mandatory, which also ensures effectiveness. A risk management system must also be established to identify all potential risks and mitigate them where possible. European standards will be developed for these requirements providing AI developers with guidance how to comply. These standards will not be mandatory, but they are expected to be widely adopted, standardizing procedures as much as possible. Those who fail to do so will be responsible for demonstrating compliance with all requirements for those systems. These requirements are not imposed by the AI regulation for AI that does not fall into one of the high-risk categories. Member States may not require them in addition to the regulation, as this could disrupt the internal market and lead to higher administrative burdens. However, developers of such AI may, of course, use such systems voluntarily (van Dooren, 2025, p. 10)
1.1.3	-
2.1.1	With the Algorithm register, I want to give citizens and enterprises more insight into which algorithms the government uses in its processes. Discussion are currently underway, including fellow government bodies, about the best way to inform citizens about the algorithms and the Algorithm register. This ties in with the aforementioned analysis of responses to the reflection document 'Algorithmic Decision-Making and the General Administrative Law Act', as decision-making can also provide insight into the algorithms used and may even allow for referral to the Algorithm register (van Dooren, 2025, p. 7)
2.1.2	-
3.1.1	I encourage public organizations, both within the national government and other government bodies, to publish the algorithms they use. To this end, I proactively contact government bodies and assist them with various tools, such as the Algorithm Register Guidelines, vendor templates, implementation team support, so-called connection sessions, a regional tour, a newsletter, and articles with tips from organizations that have already published. Furthermore, all ministries have committed to register all high-risk AI systems they use in the Algorithm register by the end of 2025. From August 2nd, 2026, all government bodies are required by the AI regulation to register high-risk AI systems. This does not require any adjustments to the Algorithm register. In parallel, discussion are being held with other government bodies to improve the quality of the

	registration. My ministry also checks the registration of an algorithm before it is published (van Dooren, 2025, p. 8)
3.1.2	This ministry also checks the registration of an algorithm before it is published [in the Algorithm register] (van Dooren, 2025, p. 8)
3.1.3	-
4.1.1	-
4.1.2	To ensure that harmful AI practices do not occur, the AI regulation establishes a robust supervisory system. This gives the (market) supervisor, yet to be designated, the authority, to impose sanctions when organizations use (or continue to use) prohibited AI practices. From February 2nd, 2025, violations of the prohibitions may result in civil liability. (Market) supervisors will also de designated for other risk categories, such as high-risk AI (van Dooren, 2025, p. 9)

Data source: 26643, Nr. 1345

Code	*Data*
1.1.1	-
1.1.2	A responsible use of generative AI was published [on May 27th, 2025]. It essentially provides guidelines for how to use generative AI responsibly. These guidelines cover legal, ethical, technical, and governance aspects. These aspects apply not only to AI in many cases, but also to other digitalization initiatives [the government pursues] (Wingelaar & Boeve, 2025b, p 24) To provide the State Secretary with an explanation about training AI with general data, such as that processed by Statistics Netherlands (CBS; does this not involve personal data? The GDPR also applies fully to training AI models. Personal data, including personal data collected by CBS, cannot simply be used for this purpose. The principle is that public data, also knows as open data, is used for training AI. The use of personal data is note excluded. If it is permitted, there are strict conditions and requirements (Wingelaar & Boeve, 2025b, p. 33).
1.1.3	-
2.1.1	-
2.1.2	-

3.1.1	Can the State Secretary explain why the Algorithm register has not been made mandatory and how it can be enforced? The algorithm register has been populated since 2022. I have made administrative agreements within the national government regarding its completion, such as the requirement that high-risk AI is registered by the end of 2025. If it is not completed, I'll consider making the register legally mandatory. I believe I mentioned this in a previous debate, but I think it is useful to reiterate that here. [The government does not] build these kind of registers without obligation Wingelaar & Boeve, 2025b, p. 34)
3.1.2	If there are topics for discussion, for example, if the standardization is not progressing satisfactorily or if there is something wrong with the Algorithm register, you can contact me and submit those topics. Then I can see if I can find a solution through the Dutch Council of Ministers. That is how I see my own role as well (Wingelaar & Boeve, 2025b, p. 24)
3.1.3	-
4.1.1	-
4.1.2	Yes, that is what I mean. I do mean that we should also establish AI awards. I do not want to commit to that completely yet, because first I want to carefully consider the relevance. In another life, I also served on juries, and then I had to assess all sorts of companies and solutions. So if we do it, we have to get it right the first time, because then it will add value to the AI community. They will work even harder to win such an award! (Wingelaar & Boeve, 2025b, p. 44)

Data source: 26643, De Nederlandse Digitaliseringstrategie (NDS)

Code	*Data*
1.1.1	With this NDS, we contribute to putting citizens and enterprises first by implementing several acceleration initiatives. For example, citizens and enterprises should experience contact and interaction from a single government. The guiding principle is: 'always at the right door'. Citizens and enterprises are proactively provided and offered (information about) public services and products. The service experience of citizens and enterprises is central (Rijksoverheid, 2025, p. 3) As a unified government, we will capitalize on opportunities and ensure the responsible use of AI and algorithms, ensuring transparency, security, and democratic oversight, and maintaining high-quality services even in a tight labour market. […] We will

establish joint (auditable) standards for 'AI use by the government', including an algorithm framework and procurement guidelines. We will explore the establishment of a government-wide AI competency centre. We will work together to develop AI (Rijksoverheid, 2025, p. 7)

1.1.2 We are introducing a strengthened approach to agreeing on, implementing, and enforcing (digital) standards. This includes support during implementation. Digital standards introduced by the (European) law must be implemented by all public organizations (Rijksoverheid, 2025, p. 3)

1.1.3 We share and utilize data responsibly across government levels. We achieve this by working data-driven across the government through federal data-system, which includes binding agreements and standards. Domain-specific agreements aligned with this. We are developing a government-wide system to identify data bottlenecks that organizations encounter, resolve them collectively, and prevent future bottlenecks (Rijksoverheid, 2025, p. 3)

We strive for a high-quality AI infrastructure that the government also uses, consisting of, among other things, high-quality data, open language models from the Netherlands and/or the EU, the training and retention of available talent, and sufficient computing power (Rijksoverheid, 2025, p. 3)

Data sharing issues are being resolved, and data is becoming more discoverable, usable, and interoperable. Processes are being thoroughly overhauled, prioritizing citizens and enterprises, and data is being organized around them. This require data-literate public organizations with high-quality data, which is also crucial for the development of AI and proactive service delivery (Rijksoverheid, 2025, p. 6)

With the Federated Data System (FDS), we will share data responsibly across public organizations. Now we must ensure everyone is on board. We must remove barriers between public organizations: data remains at the source and is organized consistently, making it easier to find (re)use, and exchange. We will establish clear rules for how data can be used responsibly across organizational boundaries, with safeguards for responsible use. We will redesign processes. […] The entire government will operate data-driven through the FDS, with binding agreements and standards. Domain-specific agreement frameworks will be aligned with this (Rijksoverheid, 2025, p. 6)

2.1.1	-
2.1.2	-
3.1.1	-
3.1.2	We support public organizations in implementing these standards, demonstrate best practices, clarify when organizations do not comply with the shared standards, and engage in discussions with them about this. The use of standards is no longer optional, and we will ensure that uses them, although the pace of adoption may vary (Rijksoverheid, 2025, p. 4) We collaborate on implementing digital legislation and removing legal bottlenecks. Dozens of (sectoral) laws alone govern government data management. Organizations must implement all this (European) legislation quickly. This requires oversight, knowledge, and the pooling of legal expertise. In this way, we align ourselves with the EU Competitiveness Compass, which simplifies legislation and regulations (Rijksoverheid, 2025, p. 4) An NDS Council will be established, comprised of (external) digitalization experts. This council will advise the cabinet and Administrative Consultation on Digitalization and will drive the implementation of the NDS. The relationship between de NDS council and existing consultative bodies, such as the Government-wide Policy Consultation on Digital Government (OBDO), will be determined and formalized later (Rijksoverheid, 2025, p. 4) An NDS implementation program will be developed, prioritizing implementation and feasibility, and ensuring collaborative project execution. The program has several objectives: a directing/monitoring role for all components of the NDS, including promoting the speed of implementation, the quality of execution, and the effectiveness of results; a facilitating role for public organizations, where this offers added value; ensuring knowledge sharing; a pioneer role for structural functions arising from the NDS (Rijksoverheid, 2025, p. 4) Using the tasks from the NDS, we establish concrete goals and map out the preconditions through intergovernmental co-creation. We determine the standards that we will apply together and provide direction (Rijksoverheid, 2025, p. 4)

3.1.3	-
4.1.1	-
4.1.2	-

Data source: 26643, Nr. 1371

Code	*Data*
1.1.1	In the June 2024 summary letter, the Dutch government announced it would have Dutch AI policy assessed against the UNESCO Recommendation on the Ethics of AI using UNESCO's Readiness Assessment Methodology (RAM), which considers both qualitative and quantitative indicators. The Netherlands is the first EU Member State to complete such a study. The results of the study are positive: the Netherlands has made significant progress in developing policy instruments for ethical development and deployment of AI systems. Good examples include the Algorithm register and the Impact Assessment on Human Rights and Algorithms (IAMA), as well as the existing frame of European legislation and regulations. The RAM report contains ten recommendations for The Netherlands, which have been addressed along the lines of the government's existing and future AI policy. UNESCO has published the RAM report. This allows other countries to draw inspiration from Dutch policy instruments, and the report contributes to the creation of a global overview of AI policy in all UNESCO Member States. The RAM also serves as the Dutch contribution to the first four-yearly monitoring round of the implementation of the Recommendation, an important building block in the emerging global AI governance (van Marum, 2025, p. 15)
1.1.2	-
1.1.3	We apply the 'open, unless' principle when using and developing government software. This means that the source code is generally released as an open source, unless there are valid reasons not to do so, such as national security or confidentiality. Regarding the 'unless' principle, our policy is aligned with the exceptions under the Open government act (Woo). After all, the source code of government software is government information (van Marum, 2025, p. 5)
2.1.1	-
2.1.2	-
3.1.1	-
3.1.2	-
3.1.3	-

4.1.1	-
4.1.2	-

Data source: 26643, Nr. 1382

Code	*Data*
1.1.1	-
1.1.2	-
1.1.3	If the government decides to develop and/or use generative AI models such as AI chatbots, it is important to be clear about the purchasing conditions. These conditions can contain important agreements regarding effectiveness and reliability, the safe use of data (privacy, security), and maximum transparency of data used in models (van Marum, 2025b, p. 3)
2.1.1	Regarding the Dutch Data Protection Authority's plea for more research into the risks and implications of chatbots, for example, on effectiveness/reliability and on (addictive) behaviour, I can tell that currently no research is being conducted specifically for therapeutic guidance in mental health care (van Marum, 2025b, p. 3) A full-fledged and responsible deployment of AI, utilizing its potential while avoiding or mitigating risks, requires further professionalization of organizations in this regard. […] A maturity model, as the DDPA suggests, is a useful tool in this regard. I have therefore included several examples of a maturity model in the Algorithm framework for public organizations. These also relate to DDPA's initial initiative for a multi-year action plan to promote AI literacy within organizations, for which I am grateful to the DDPA. […] Various efforts are being made to enhance the AI skills of civil servants. For example, the digital craftmanship program focuses on strengthening the digital skills of civil servants, including AI and data skills. Generative AI is an explicit component of this. The program addresses both the technical and legal aspect of generative AI, to the extent necessary for proper execution. To improve digital literacy, the National Academy for Government Digitalization and Information Technology (RADIO) was established. It offers, for example, a basic course on the opportunities and risks of generative AI for government officials. Furthermore, within the framework of the NDS, AI literacy will be actively promoted, and this issue will be addressed government-wide (van Marum, 2025b, p. 4)
2.1.2	-

3.1.1 Supervisory authorities are intensifying preparations for the AI regulation and its implementation in The Netherlands, the DDPA has noted. They are doing this by explaining how organizations can comply with the requirements. This process is still ongoing. The DDPA has noted that private and public organizations are adapting to the new requirements (van Marum, 2025b, p. 4)

3.1.2 The Dutch Data Protection Authority concludes that the Dutch government has taken good steps in managing AI and algorithm risks with AI/algorithm frameworks and registrations. According to the DDPA, progress in AI and algorithm registration is still insufficient, resulting in a lack of adequate insight into the higher-risk applications. The grip on AI, in particular, needs to be strengthened, given the rapid developments in this technology and the new concerns it raises. The DDPA cites recent incidents at home and abroad that affect multiple application areas that will be regulated under the AI regulation. The DDPA recommends incorporating the European standards from the AI regulation in the further development of the Algorithm framework. These standards are currently being developed by the EU and will help meet the requirements

I take the focus on further development of European standards to heart, as this will help meet the requirements for high-risk systems. In line with this, I want to more consistently assess the use, development, and procurement of AI in a government context by establishing joint (auditable) standards for AI use wherever possible. This will be further developed within the framework of the NDS (van Marum, 2025b, p. 2)

Furthermore, the DDPA notes that practical experience shows that proper management of AI systems in public organizations requires a more comprehensive, open, and responsible approach. This approach goes beyond focusing on specific laws and regulations, and instead embraces a more holistic approach to cross-sectoral regulations or the overlap of regulations and other frameworks. Organizations with sufficient maturity are able to take control and embrace opportunities for positive impact and flourishing innovation. For example, it is important that civil servants and citizens understand exactly what AI does and can ask the right questions and/or recognize flaws in a timely manner to improve it if necessary. The deployment of algorithms and AI is increasingly characterized by an AI chain. This requires interplay between systems and organizations that build on each other, concludes the DDPA. These are complex roles where sharing information within the chain is necessary to achieve effective and an appropriate division of responsibilities (van Marum, 2025b, pp. 3-4)

	I agree that proper risk management requires a more comprehensive, open, and responsible approach, and I am working on this. […]The DDPA rightly states that AI literacy is important because it enables us, in our various roles, to view AI with critical insight (van Marum, 2025b, p. 4)
	At the end of 2024, the National Inspectorate for Digital Infrastructure (RDI) and the DDPA issued recommendations on the organization of supervision of the AI regulation in The Netherlands, commissioned by the Ministries of Economic Affairs, the Interior and Kingdom Relations, and Justice and Security. The government is currently preparing the structure of this supervision. [The parliament] will be further informed about this in autumn of 2025. Based on the implementing law – which is also in preparation – the relevant supervisory authorities will conduct feasibility assessments to determine the financial consequences of these (new) supervisory tasks (van Marum, 2025b, p. 5)
	The DDPA's periodic reports are a good indicator, and the results enable the cabinet to tighten policy where necessary (van Marum, 2025b, p. 5)
3.1.3	-
4.1.1	-
4.1.2	-

Data source: 26643, Nr. 1385

Code	*Data*
1.1.1	The added value of an ethics committee is that the use and implications of new technology, such as AI, are considered from the perspective of various values and interests. A diverse composition increases the likelihood that values and interests are not overlooked. An ethics committee is considered, but not recommended. This is primarily because there are several ways to ensure attention to ethics. This can be achieved, for example, through feasibility and/or evaluation studies (such as audits or human rights assessments, such as the Impact Assessment Human Rights and Algorithms (IAMA)), which can address the ethical outcomes of generative AI. Another way is by ensuring multidisciplinary teams or organizing meetings (seminars, hackathons, etc.) where ethics is discussed. Some of these recommended measures are also included in the Algorithm Framework (Wingelaar & Muller, 2025, pp. 9-10)

The use of generative AI applications under consumer conditions was also prohibited for the central government under the previous cabinet's position. It's difficult to determine the percentage of individual civil servants who did use this, and in which processes. However, I am working on increasing AI literacy among civil servants to raise awareness of so-called ‘shadow AI’ (Wingelaar & Muller, 2025, p. 17)

1.1.2 The government-wide position applies to all generative AI applications deployed by or on behalf of the government. Every public organization remains responsible for the secure use of data, results, and processes, even when the organization outsources these activities. This requires clear agreements with and transparency from external parties. These agreements can be laid down in, for example, purchasing conditions. Just as for privacy and information security, the requirements specific to generative AI must also be incorporated into the procurement process. A process for this is already underway (Wingelaar & Muller, 2025, p. 2)

It is up to public organizations that wish to deploy generative AI applications to implement the preconditions described in the position statement. Protection of sensitive or confidential information when using generative AI, as with other types of IT systems, can be assessed through a risk analysis such as the Government Information Security Baseline (BIO). If the (intended) deployment of generative AI involves processing personal data, the GDPR applies, and a (pre-scan) DPIA must be performed as a mandatory risk analysis. To support these public organizations in implementing this position statement in practice, they can use resources such as the government-wide guidelines for the responsible use of generative AI and the Algorithm framework (Wingelaar & Muller, 2025, p. 2)

When generative AI is deployed, AI-generated content must be recognizable as such, in accordance with the Generative AI Guidelines and the transparency obligations under the European AI Regulation (Article 50, paragraph 4). This means that when AI is used in government communications, human review and editorial control are mandatory before publication. This is intended to prevent any inaccurate information created with generative AI applications from ending up in government communications. Through the AI Regulation, Europe also requires that providers of general-purpose AI models share information about the model's operation with developers who build on that model. Furthermore, all AI-generated content must clearly indicate this. These

requirements contribute to better understanding which content created with AI is potentially uncertain, incorrect, or unverified. These obligations will take effect on August 2, 2025 (Wingelaar & Muller, 2025, p. 4)

The AI Regulation also introduces transparency obligations for certain AI systems, including generative AI systems, starting in August 2026. For example, generated content must be clearly marked as artificially generated or manipulated. This obligation also affects government organizations that use AI systems for communication. Even if the organization is not a provider but does use such a system, it must make it clear that the content has been generated or manipulated. This can be done, for example, by indicating in the captions of images that they were created by AI. Transparency obligations also apply to AI systems that communicate with citizens, such as chatbots. Users must know that they are talking to an AI system and not a human. This is particularly relevant for online services of government organizations (Wingelaar & Muller, 2025, p. 8)

The Algorithm Framework is a central tool available to all government organizations. It was developed with the cooperation of a broad representation of government organizations and academics. The Algorithm Framework is designed to be applicable to both the national government and, for example, municipalities, provinces, and water boards, ensuring the entire government has the same starting point. It provides organizations with an overview of applicable regulations and offers tools for applying these regulations. Centrally sharing tools and measures helps standardize the application of these regulations. By increasing awareness of the Algorithm Framework, the effectiveness of this approach increases. Once the European standards in this area have been formally adopted, the Algorithm Framework will be updated accordingly to achieve further standardization (Wingelaar & Muller, 2025, p. 11)

The Algorithm Framework is based on legal requirements, particularly those set by the European AI Regulation, but also by the General Administrative Law Act (Awb) and the GDPR. All these requirements are addressed within this framework. In this way, I provide the most comprehensive overview possible of all matters that government agencies must comply with, in addition to some matters that are not strictly legally mandated but can be crucial for responsible deployment. The Algorithm Framework

also refers to tools, guidelines, and best practices developed elsewhere. This gives organizations the freedom to assess which tools are most suitable or relevant for their domain and the algorithm to be deployed (Wingelaar & Muller, 2025, p. 12)

Through my government-wide position, I emphasize that government organizations must comply with legislation, such as the European AI Regulation, when deploying generative AI. The AI Regulation sets requirements for how AI models are trained. Providers of "general-purpose AI models," which include generative AI models, are obligated to share information about the model's operation with developers who build on it. It must also be clear how copyright is respected, and all AI-generated content must clearly indicate this. These requirements contribute to better understanding which content was created using AI and is potentially uncertain, incorrect, or unverified. Additional requirements apply if the general-purpose AI model poses systemic risks under the AI Regulation. The intention is for the AI Regulation to regulate the most powerful AI models on the European market (Wingelaar & Muller, 2025, p. 16)

Therefore, I recommend that organizations, when purchasing generative AI systems, include in the (draft) agreement that the provider agrees not to infringe copyrights with the training data, and that the provider actively monitors this throughout the development and lifecycle. When government organizations develop AI models themselves, they are, of course, responsible for correctly handling the copyrights of their own data (Wingelaar & Muller, 2025, p. 16)

Training generative AI is a form of text and data mining. In line with Article 4 of EU Directive 2019/790 "Copyright and Related Rights in the Digital Single Market," the Copyright Act stipulates that making a copy of a work for text and data mining purposes is permitted under two conditions. First, the works used to train generative AI must originate from a lawful source. Second, the rights holders must not have made a reservation that would prevent the training of generative AI. If a reservation has been made, permission to use the copyrighted material is required. Rights holders may attach conditions to this permission, such as the payment of a fee (Wingelaar & Muller, 2025, p. 17)

AI functionalities are regularly added to existing systems or devices through software updates. Think of phones, computers, or online applications used by the government. I believe it's important that government organizations make sound agreements with their suppliers about this, including data sharing and storage. If AI functionalities can only be offered under consumer terms, the feature should be disabled. Preference is not given to platforms without AI, but to platforms where AI can be deployed safely and responsibly. AI tools (apps) from countries with an offensive cyber program against the Netherlands are prohibited under the government-wide app policy. Therefore, DeepSeek is not accessible from government work devices. Organizations can also ask their IT service providers to disable certain websites, such as freely accessible generative AI through the browser. They are responsible for this themselves (Wingelaar & Muller, 2025, p. 19)

By establishing specific purchasing conditions, I want to establish government-wide agreements on the level of transparency. Therefore, the Ministry of the Interior and Kingdom Relations (BZK) has asked the Centre for Information Security and Privacy Protection (CIP) to initiate a process regarding AI procurement for the entire government. This includes clear supplementary purchasing conditions and further training for purchasers. With this, I want to support organizations in the procurement or development process, so they can start using responsible generative AI more quickly (Wingelaar & Muller, 2025, p. 20)

Furthermore, the European AI Regulation includes obligations for providers of general-purpose AI models, which are models capable of performing a wide variety of tasks and can be integrated into many different AI systems. These are referred to as "general-purpose AI models." Providers of these models are required to share information about the model's operation with developers who build on it. These obligations take effect on August 2, 2025 (Wingelaar & Muller, 2025, p. 22)

Clearly defining the purposes also touches on the due diligence requirement under the General Administrative Law Act, which requires that a decision be prepared with due care and made correctly. This requires, among other things, a thorough investigation of information and facts, a careful decision-making process, and sound decision-making (Wingelaar & Muller, 2025, p. 26)

1.1.3 The position paper encourages all levels of government to actively assess potential biases in (training) data or outcomes when deploying generative AI, and to establish transparent processes and human oversight. This will contribute to the fair, verifiable, and inclusive deployment of AI (Wingelaar & Muller, 2025, p. 9)

Since February, the AI Regulation has required organizations using AI to work on AI literacy. Organizations are responsible for ensuring employees have the appropriate level of knowledge, depending on the AI application they use. The required level of knowledge also depends on the specific role an employee plays within the organization. For example, compliance officers, lawyers, data scientists, or purchasers have roles requiring a certain level of knowledge when the organization uses generative AI applications, for example. The relevant (government) organization is also responsible for the training its employees receive (Wingelaar & Muller, 2025, p. 9)

The preliminary position paper from 2023 focused significantly on the risks of generative AI. This revised position paper seeks a balance between the opportunities the technology offers and the risks involved. Therefore, the position paper still requires organizations to conduct risk analyses. However, it no longer prescribes which tool organizations must use for this purpose. In practice, this means that organizations can now choose other impact assessments, in addition to the Data Protection Impact Assessment (DPIA) or the IAMA, if these better suit the generative AI application they intend to develop or deploy. Moreover, if the GDPR requires a (pre-scan) DPIA because personal data is being processed, that obligation still applies (Wingelaar & Muller, 2025, p. 13)

According to the government-wide position, conducting a risk analysis is a prerequisite for the use of generative AI. Unlike the preliminary position from 2023, the current position no longer prescribes which tool should be used for the analysis (Wingelaar & Muller, 2025, p. 14)

There are several ways to make (generative) AI models more transparent. Users can benefit from clear and concise model cards—instructions detailing the technical details and potential limitations of the AI model in question. Such an instruction leaflet can help (end) users determine whether a model is suitable for a specific application and

whether there are any potential risks associated with its use. The DDPA also points this out in its AI & Algorithm Risks Report for the Netherlands from autumn 2023 (Wingelaar & Muller, 2025, p. 22)

Although content generated by generative AI often appears credible at first glance, generative AI models do not always provide factually correct answers. This is because generative AI models are not optimized for accuracy. Generating false output is called "confabulation," or better known as "hallucination." For example, a generative AI model can present an incorrect piece of information as fact. The quality of a generative AI model's training data and the quality of the prompt (the "prompt") significantly influence the quality of the output. For example, the results of generative AI models may provide an incomplete picture or be outdated due to incomplete or outdated training data. Governments and employees must be aware of this. Even if the governance surrounding such AI applications is in place and the risks are mitigated as effectively as possible, there is still a chance that generative AI systems will hallucinate. This requires some degree of AI literacy among government employees, a requirement also set out in the AI Regulation (Wingelaar & Muller, 2025, p. 23)

The risk of errors can be mitigated in several ways. First, by ensuring that the data the system is trained on is current, reliable, and context-specific. This reduces the risk of hallucinations, as the system needs to consider less "irrelevant" information when formulating an answer. However, this never completely eliminates the risk of incorrect output. Second, organizations can use AI systems that generate source references. This is a good way for an end user to verify whether an answer is correct. I recommend that government organizations include this as a requirement during the design phase of an AI system or specify this need during the procurement process. Third, it is necessary to ensure human review of a decision by involving someone authorized and competent to make and change a decision. This must be embedded in the work processes used for AI systems. I raise awareness of these and other techniques, including by referring organizations to the Algorithm Framework, which includes the above techniques and further explanation (Wingelaar & Muller, 2025, p. 23)

2.1.1 I believe explainability of generative AI applications is important, whether they are open source or not. Regarding accountability for the output/result: generative AI is a tool and cannot assume responsibility. Both explainability and accountability are part of

	establishing good AI governance. The Algorithm Framework offers guidance in this regard (Wingelaar & Muller, 2025, p. 22)
2.1.2	-
3.1.1	To what extent is generative AI already being used by government employees? Within (local) government, work has been underway for some time on the use of generative AI. Examples include (internal) chatbots that make internal government information easier to find, AI applications used for metadata extraction, or AI applications used to support objection or [information request]-procedures. In this context, see also the collection letter of December 18th, 2024, which discusses ongoing generative AI initiatives (Wingelaar & Muller, 2025, p. 2) Is generative AI currently being used in drafting government communications or policy documents? If so, can you indicate how many government messages and policy documents are currently being written by AI? Many public organizations are currently experimenting with generative AI based on the guidelines. They are exploring how this new technology can be used responsibly for government communications and policy documents. These are typically pilots conducted in a securely protected test environment. These pilots are not intended to publish the products. It cannot be ruled out that communications have been created using generative AI. The Ministry of General Affairs is currently conducting an inventory of the use of generative AI in government communications (Wingelaar & Muller, 2025, p. 3) Who is responsible if generative AI introduces incorrect information into an official document? Government organizations are responsible for establishing governance around generative AI and algorithms in general. Clearly defining responsibilities is an explicit part of this. The Algorithm Framework provides tools for organizations to do this, such as establishing a RACI matrix (Responsible, Accountable, Consulted & Informed). Furthermore, the European AI Regulation contains obligations for providers of General Purpose AI models (GPAI). These are models capable of performing many different tasks and can be integrated into many different AI systems. These are referred to as "general-purpose AI models." Providers of these models are required to share information about the model's operation with developers who build on it. It must also

be clear how copyright is respected, and all AI-generated content must clearly indicate that this is the case. These requirements contribute to better understanding which content was created using AI and may be uncertain, incorrect, or unverified. These obligations will take effect from August 2, 2025 (Wingelaar & Muller, 2025, p. 6)

3.1.2 Under the European AI Regulation, affected individuals, such as citizens, must have the right to an explanation if a decision is primarily based on the output of certain high-risk AI systems. This explanation must be clear and meaningful and must serve as the basis upon which affected individuals can exercise their rights. Furthermore, Chapter 9 of the General Administrative Law Act (Awb) establishes a regime for filing an objection and handling complaints. Objections and complaints about decisions and conduct of a government organization involving AI can, in principle, be filed and handled under this regime (Wingelaar & Muller, 2025, pp. 6-7)

The government-wide position paper calls on all levels of government to engage in dialogue with their elected representatives and actively involve them in decision-making regarding generative AI deployment, so they can effectively fulfill their supervisory and policy-setting roles. In the Generative AI guidance, I also encourage organizations to involve as diverse a group of experts as possible in decision-making regarding generative AI deployment. Representatives can be part of this group (Wingelaar & Muller, 2025, p. 7)

As also explained in the letter to Parliament "Supervision in the Digital Domain," digitalization and AI transcend domain and sector boundaries. In practice, this means that supervisory issues increasingly fall under the jurisdiction of different supervisory bodies. For example, an algorithm in healthcare that processes personal data can fall under the jurisdiction of both the Dutch Data Protection Authority (AP) and the Health and Youth Care Inspectorate (IGJ). Supervisory bodies can mutually determine, for example, through a cooperation agreement, how supervision and/or enforcement will be conducted in a specific case. Furthermore, the cross-domain nature of AI requires coordination and exchange between (many different) supervisory bodies, specifically to ensure consistency in supervision and prevent the accumulation of regulations. In the Netherlands, several supervisory bodies assume coordinating tasks. For example, the Directorate for Algorithm Coordination (DCA) at the AP and the National Inspectorate for Digital Infrastructure (RDI) have various types of coordinating tasks in

the field of AI and algorithms. For example, the DCA is committed to cross-domain risk identification in the field of algorithms and the development of concrete guidance for supervised entities, so that it is clear in advance how and which frameworks they must comply with when deploying AI and algorithms. The AI Regulation provides enforceable requirements for transparent and secure general-purpose AI models, with or without systemic risks. Generative AI is also included. Developers of general-purpose AI models are required to prepare and keep technical documentation about the model available to supervisory authorities and to prepare information for developers who wish to integrate the AI model into their own AI system. If a general-purpose AI model could also pose systemic risks, the provider must also conduct a model evaluation, mitigate systemic risks, share incident information with the supervisory authority as quickly as possible, and ensure an appropriate level of cybersecurity. These requirements from the AI Regulation can be enforced by the European AI Office, which will oversee the requirements for general-purpose AI models. In some cases, they may also choose to withdraw a general-purpose AI model from the market. The government is currently preparing the structure for this oversight. Your House will be informed about this in the autumn of 2025 (Wingelaar & Muller, 2025, pp. 7-8)

The guidance document is supportive and was developed through intergovernmental collaboration. All levels of government have expressed their commitment to this. It is now up to the individual organizations at all levels of government to share the guidance document internally and disseminate its content. We are building a growing network of AI experts within the government. Sharing knowledge and products, including the guidance document, is also happening through this channel (Wingelaar & Muller, 2025, p. 9)

The market surveillance authorities will monitor compliance with the requirements of the AI Regulation, including those for the protection of fundamental rights. In addition, the Dutch Data Protection Authority (AP) and the Netherlands Institute for Human Rights (CRM) will ensure that the actions of public and private organizations do not violate the General Data Protection Regulation (GDPR) and non-discrimination legislation. The AP, the CRM, the Attorney General at the Supreme Court (PGHR), the President of the Administrative Jurisdiction Division of the Council of State (ABRvS), the judicial board of the Central Appeals Tribunal (CRvB), and the judicial board of the

Trade and Industry Appeals Tribunal (CBb) have been designated as authorities for the protection of fundamental rights under the AI Regulation (Wingelaar & Muller, 2025, p. 12)

With this position paper, I want to support governments in purchasing or building a safe alternative to generative AI under consumer conditions. By offering an alternative, government officials will be less likely to use free online versions. Organizations can also ask their IT service providers to disable certain websites. They are responsible for this themselves. For example, we see that the Chinese DeepSeek is often inaccessible on government equipment due to the ban on this AI application (Wingelaar & Muller, 2025, p. 15)

I believe that depends on the application and impact of the AI applications. Article 86 of the AI Regulation provides a right to explanation for decisions (that have legal consequences or a significant impact) taken based on input from a high-risk AI system. AI systems used by public authorities to provide essential government benefits and services are considered high-risk AI systems. Furthermore, the General Administrative Law Act requires sound and clear reasoning for decisions (Wingelaar & Muller, 2025, p. 21)

Transparency regarding the use of AI and explanations about its operation and role in the decision-making process should enable citizens to assess its accuracy. Citizens can appeal against decisions through legal means, such as filing an objection (Wingelaar & Muller, 2025, p. 24)

One of the conditions I stipulate in the government-wide position is that the purpose served by deploying the generative AI application must be sufficiently clear. Questions and internal discussions about the purpose, including in relation to the social outcome, are often part of a tendering process or risk analysis (Wingelaar & Muller, 2025, p. 26)

3.1.3 I believe it's important that employees review the output of generative AI before using it in communications, policy, or decisions. The government-wide guidelines on generative AI contain recommendations for end users, including critically assessing the results of generative AI, for example, for potential biases or hallucinations. Regarding

	responsibility for the results: generative AI is a tool and cannot assume any responsibility (Wingelaar & Muller, 2025, pp. 8-9)
4.1.1	
4.1.2	

Data source: 26643, Nr. 1394

Code	*Data*
1.1.1	-
1.1.2	-
1.1.3	-
2.1.1	-
2.1.2	-
3.1.1	I also see that the government, as well as your House, needs to embed a working method in which the Algorithm Framework also addresses compliance. To address this need, the Dutch Digitalization Strategy includes work on joint (auditable) standards for AI use by the government. This means further developing the existing Algorithm Framework into an auditable framework within which we have secured compliance (van Marum, 2025c, p. 2)
3.1.2	Although the algorithm register is primarily aimed at increasing transparency towards citizens, it increasingly plays a role towards governments, regulators and science (van Marum, 2025c, p. 1) An independent IT auditor can then provide an opinion on the extent to which an organization complies with an auditable framework, such as a standard or legislation. This framework forms the basis for the audit and specifies the requirements. The auditor uses this framework to determine whether the organization's IT systems, processes, and controls meet the requirements and reports on this in an audit opinion (van Marum, 2025c, p. 2) Ensuring complete and substantively accurate registration of impactful AI and algorithm applications by the government depends entirely on robust oversight. I believe it's important that we, as public authorities, jointly perform these oversight tasks. An auditable Algorithm Framework therefore forms the basis for a functioning accountability process, both horizontally and vertically. In this process, the board of a

	government organization accounts for an audit report to the elected representatives in the (municipal) council or other government bodies. This is called horizontal oversight. Horizontal accountability forms the basis for the vertical accountability process towards the (central) supervisory authority(ies). The Algorithm Coordination Directorate (DCA), part of the Dutch Data Protection Authority, has been the coordinating supervisory authority for algorithms and AI that pose risks to fundamental values and rights since 2023 (van Marum, 2025c, p. 2)
3.1.3	-
4.1.1	-
4.1.2	-

Data source: 26643, 1401

Code	*Data*
1.1.1	-
1.1.2	-
1.1.3	-
2.1.1	The House of Representatives is periodically informed about the progress of the digitization policy, including progress on the NDS. This is done through the usual digitalization collection letters. Naturally, I will also keep the House informed of any important developments, if necessary outside of the collection letters (Wingelaar & Boeve, 2025c, p. 3) The NDS shared with your House and the accompanying reports are the relevant political documents through which your House can monitor the objectives and progress made. The NDS implementation program refers to the organization that will drive implementation. The program organization, together with the organizations and other authorities involved in the NDS, has already begun implementing the NDS. You will be kept informed periodically through the digitization summary letters (Wingelaar & Boeve, 2025c, p. 9)
2.1.2	-
3.1.1	-
3.1.2	-
3.1.3	-
4.1.1	-

4.1.2	-

Data source: 26643, Nr. 1427

Code	*Data*
1.1.1	-
1.1.2	-
1.1.3	-
2.1.1	-
2.1.2	-
3.1.1	-
3.1.2	How does the NDS guarantee that something like the benefits scandal never happens again in relation to the use of AI? I want to do everything I can to prevent the government's use of AI from leading to new scandals. The NDS stipulates that the use of AI and algorithms must be done responsibly. That's why we, as a government, are also establishing joint standards for the use of AI. These standards must be concrete and verifiable. That's why I'm researching how the algorithm framework can be made auditable. None of this is optional. That's why the Dutch Data Protection Authority has been monitoring the use of algorithms in government since early 2023 (Wingelaar & Boeve, 2025d, p. 49) How do we ensure that oversight and enforcement of AI applications are sufficiently robust? The cabinet is currently working on establishing oversight for the AI Regulation (Wingelaar & Boeve, 2025d, p. 49) How does the State Secretary ensure that frameworks, such as the Algorithm Framework and CODIO, aren't shelved, but are also used in daily work at all levels of government? I encourage this, among other things, by organizing meetings across the country to explain the Algorithm Framework. The provinces, municipalities, and water boards met for this purpose. I also addressed this issue in various ways within the ministries. The Central Government Audit Service is evaluating the Algorithm Framework in a study to better align it with the processes of government organizations and to enhance its embedding. I also had the CODIO framework further developed into a practical tool to support government bodies in digitalization projects (Wingelaar & Boeve, 2025d, p. 50)

3.1.3	The answer to the question of how frameworks like CODIO and the Algorithm Framework actively assess the human dimension and prevent bias is as follows. I consider the human dimension absolutely essential. For this reason, the Ministry of the Interior and Kingdom Relations has incorporated the recommendations of the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) regarding last year's automated selection tools into the Algorithm Framework. Examples of measures to prevent bias include conducting the human rights impact assessment when using algorithms, the IAMA, and the use of a so-called blind assessment, which was added to the Algorithm Framework in response to the recent motion by MP Van Nispen. The CODIO tool helps governments to incorporate and assess relevant values in their decision-making processes for digitalization projects, including values such as the human dimension (Wingelaar & Boeve, 2025d, p. 51)
4.1.1	-
4.1.2	-