NORWAY

Current Trends and Challenges in the Legal Framework

Samson Y. Esayas and Mathias K. Hauglid

Abstract

This chapter explores Norway's public digitalisation efforts, assessing the effectiveness of legislative and policy measures in advancing the public sector's digitalisation and examining the adequacy of safeguards for fundamental rights. Norway stands out for its highly digitalised public sector, a result of strategic legislative and policy initiatives promoting a digital-friendly environment. We pinpoint three key areas of focus in these endeavours.

First, there have been numerous legislative initiatives enabling profiling and automated decision-making in public agencies. While driven by efficiency objectives, these initiatives tend to be seen as tools to promote equal treatment. Second, changes have been made to counter challenges in data reuse hindering digital transformation and Artificial Intelligence (AI) implementation. Third, the advocacy for regulatory sandboxes emerges as a powerful force for experimentation and learning, with platforms like the Sandbox for Responsible AI setting examples.

Despite the progress, challenges persist. Firstly, most initiatives focus on enabling decisions via hard-coded software, often neglecting advanced AI systems designed for decision support. Secondly, discretionary criteria in public administration law and semantic discrepancies across sector-specific regulations continue to be a stumbling block for automation and streamlined service delivery. Importantly, few laws directly tackle the challenges digitalisation presents to fundamental democratic values and rights, due to a fragmented, sector-focused approach.

Furthermore, we assess the AI Act's potential to facilitate AI implementation while redressing national law gaps concerning human rights and boosting AI use in public agencies. The Act places public administration under sharp scrutiny, as the bulk of the prohibitions and high-risk AI applications target the public sector's use of AI. This focus promises to enhance the protection of individuals in this domain, especially concerning transparency, privacy, data protection, and anti-discrimination. Yet, we identify a potential conflict between the AI Act and a tendency in the Norwegian legal framework to restrict the use of AI for certain purposes.

Finally, we put forth recommendations to boost digitalisation while safeguarding human rights. Legislative actions should pave the way for the integration of advanced AI systems intended for decision support. There is a need for coordination of sector-specific initiatives and assessment of their impact on fundamental rights. To amplify these national endeavours, we point out areas where cross-border collaborations in the Nordic-Baltic regions could be vital, emphasizing data sharing, and learning from successful projects. Regulatory sandboxes offer another promising avenue for collaboration. With its considerable experience in sandboxes tailored for responsible AI, Norway stands as a beacon for other nations in the Nordic and Baltic regions.

1. Overview of Public Sector and Digitalisation Projects

Norway stands as one of the countries with a highly digitalised public sector, ranked no. 5 in the European Commission's 2022 Digital Economy and Society Index. While this section broadly covers Norway's efforts in public sector digitalisation, it places particular emphasis on the implementation of AI technologies. This aspect of digitalisation is arguably the most significant transformation currently occurring in how public sector services and decisions are conducted, with profound implications for safeguarding fundamental rights and upholding the values of the Norwegian democracy.

1.1 Organization of the Public Sector

Norway is a constitutional democracy.[929] According to the Norwegian Constitution, the highest executive power is vested in 'the King'.[930] In practice, however, the King's powers are mostly ceremonial and symbolic in nature. In the context of executive powers in the Constitution, the powers vested in the King are exercised by the Government.

The central administration consists of the government, ministries, and directorates, which govern units at the regional and local levels. The division of the central administration into various administrative bodies is primarily based on policy areas or tasks, not on geographical criteria. Various supervisory authorities and other sector-specific authorities are typically organized under the respective ministries. In addition, there are some collegial bodies (committees) with specific and limited functions, such as acting as an appellate body or advisory body on certain matters. A higher-level body can normally instruct subordinate bodies in the organizational hierarchy, both generally and in individual cases. As a main rule, however, the central administration bodies cannot instruct the local administration (municipalities and county municipalities).

[929] Konstitusjonelt demokrati. / Smith, Eivind. 5th ed. 2021, p. 30.
[930] The Norwegian Constitution, Article 3.

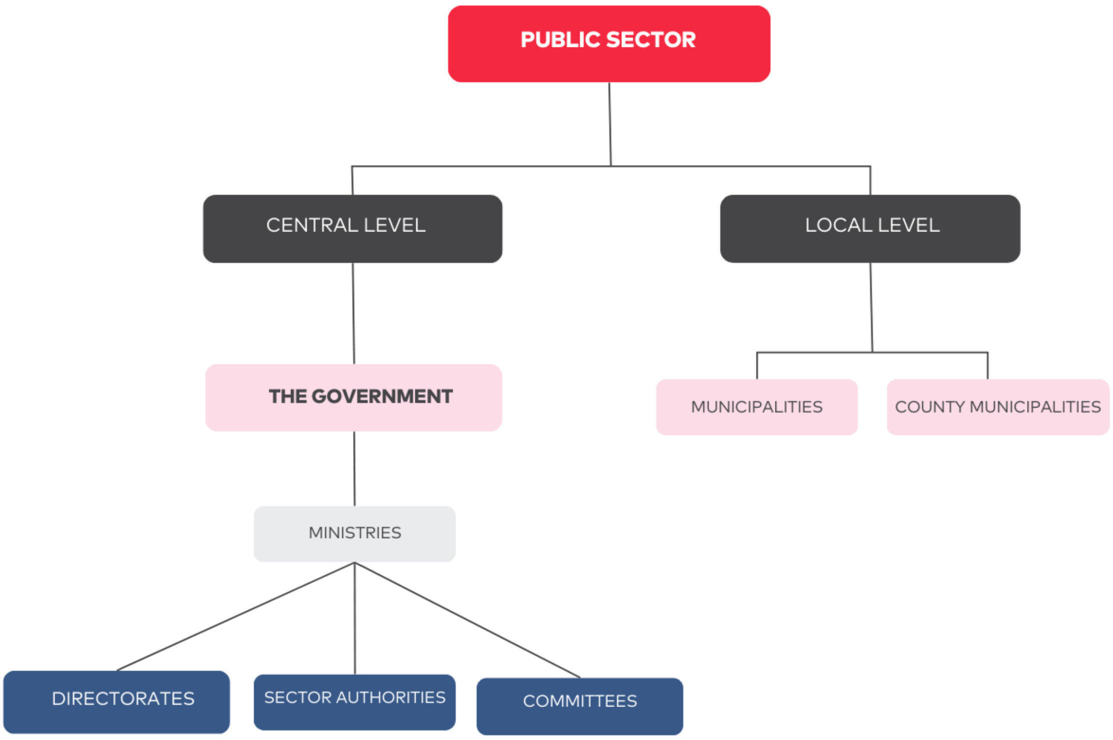

Figure 1. Organization of the Norwegian public sector.

1.2 Implemented and Planned Projects

1.2.1 Overview

Norway is at the forefront of digitalizing its public services, with a dedicated Directorate for Digitalisation (Digdir) driving the initiatives in the public sector. While there is a vast array of digitization projects within the public sector, certain projects have garnered widespread attention. Since 2019, Digdir has recognized and awarded projects that showcase the potential of digitalisation. To receive the award, projects must be 'innovative and contribute to a better and more efficient public sector - and to an easier everyday life for citizens'.[931]

Moreover, the Norwegian Artificial Intelligence Research Consortium (NORA) and Digdir established a comprehensive database that provides an overview of both ongoing and completed AI projects in the public sector.[932] The database contains more than 150 different AI projects across various fields and is a valuable resource for anyone interested in exploring the applications of AI in the public sector. The health sector leads with 54 projects (40%), public administration with 33 projects (24%) and transport sector with 22 projects (16%).[933] The database covers early-stage research and development projects as well as projects that are closer to implementation. This is particularly the case with projects in the health sector, where few AI systems have currently been implemented into clinical practice.

[931] Her er årets tre beste offentlige innovasjoner. / Directorate for Digitalisation (Digdir) 30 May 2022 https://www.digdir.no/digitaliseringskonferansen/her-er-arets-tre-beste-offentlige-innovasjoner/3615. All links are last accessed 05 October 2023.

[932] Kunstig intelligens – oversikt over prosjekter i offentlig sektor. / Felles datakatalog, Directorate for Digitalisation (https://data.norge.no/kunstig-intelligens).

[933] Kunstig intelligens – oversikt over prosjekter i offentlig sektor. / Felles datakatalog, Directorate for Digitalisation (https://data.norge.no/kunstig-intelligens).

The creation of this database is a first good step towards promoting transparency and accountability in the public sector's use of AI. It contributes to a transparent public sector, giving citizens and other stakeholders insight into how AI is used. Additionally, the database plays a crucial role in reducing redundant efforts and facilitating the exchange of best practices on how to use AI. This not only ensures the efficient use of resources but also contributes to the responsible use of AI in the public sector. In the following, we highlight some projects that have gained attention and are also relevant from a regulatory respective. Before proceeding further, it is apt to highlight the specific areas where AI is being employed by public agencies.

In a 2022 survey conducted by Vestlandsforsking and commissioned by the Directorate for Children, Youth, and Family, various applications of AI within public agencies were examined.[934] The research identified the following eight key use areas, each involving specific types of AI techniques—ranging from rule-based and explainable AI to black-box models and machine learning—as well as differing types of data, such as personal and synthetic test data:

- *Data Quality Enhancement*: The first area focuses on using rule-based AI to augment the integrity of datasets. Rather than processing the data, AI algorithms are employed to identify and rectify errors within datasets, which may contain personal information.
- *Error Detection and User Experience:* AI is also deployed to uncover gaps or inaccuracies in systems, aiming to enhance user interaction with various services. By providing predictive recommendations, AI helps users avoid making mistakes. These projects typically use highly explainable models, and the datasets may contain individually identifiable information recast as event descriptions.
- *Organizational Needs Prediction:* AI assists in forecasting internal needs within an organization, such as predicting employee absence rates. The ultimate goal is system optimisation. Explainable models are the technology of choice here, working with data that may include individual records.
- *Fraud and Misuse Detection:* Some projects employ 'black-box' AI models to reveal suspicious patterns within systems. The primary objective is to flag misuse, and the data involved may encompass personal and contact details.
- *User Behavior Prediction in Welfare Services:* AI is utilised to anticipate the behaviour of welfare service users, aiming to enhance accessibility and minimise fraudulent use. AI systems with explainable models analyze data that has been converted into event descriptions.
- *Medical Treatment Applications:* In healthcare settings, AI plays a role in patient treatment, such as image-based diagnostics. Machine learning algorithms analyze individual data for this purpose.
- *Synthetic Test Data Analysis:* One specialized project focuses on the use of machine learning for generating and analyzing synthetic test data.
- *Case Handling Support:* Lastly, AI systems with explainable models aid case handlers in streamlining the case management process, making decision-making more efficient and reliable.

In the following, we describe a selection of digitalisation projects, with a particular focus on AI technologies that have been implemented or are planned within the Norwegian public sector.

[934] Bruk av Kunstig Intelligens i Offentlig Sektor og Risiko for Diskriminering. / VF-Rapport nr. 7-2022. Vestlandsforsking, 2022, p. 30–31 (hereinafter VF-Rapport nr. 7-2022).

1.2.2 Implemented Projects

1.2.2.1 Automating decisions on citizenship applications

The Norwegian Directorate for Immigration (UDI) won the 2022 prize for best public digitalisation project for its work in automating decisions in the handling of citizenship applications.[935] Driven by the surge in citizenship applications and work disruptions caused by the pandemic, UDI implemented a project to automate the assessment of citizenship applications. The aim was to reduce processing time and allow case managers to focus on complex cases. To achieve this, UDI collaborated with an external IT consulting company, Computas, to develop an innovative automation solution and case management system. The initial phase of the automation system involves assessing whether an application satisfies all requirements and can thus be fully automated. To do this, the system analyses the information from the application together with information from the Immigration Database, the National Register of Citizens (*Folkeregisteret*), Kompetanse Norge, the police and foreign missions. The result shows which conditions have already been met and which ones require examination. If something requires verification by a case manager or if the application needs to be rejected, it goes through manual processing at UDI. If an application meets the requirements to be handled automatically, it is further checked against data from different databases including the *Folkeregisteret*, the Tax Agency, the Immigration Database and local police districts. As of 1 May 2022, UDI had fully automated just under half of the decisions made in citizenship cases and nine out of ten of these applications are granted, and the applicants receive an answer immediately.[936] This has led to a sharp reduction in the processing time per application—in some cases from months to seconds. With less routine work to manage, case managers have more time to focus on complex cases. The success of UDI's automated citizenship project has opened up opportunities for further investments in automation. With this project, UDI has gained valuable knowledge about their potential for automation, and it is already working on new projects, including those related to Ukrainian refugees seeking asylum in Norway.[937]

1.2.2.2 Using AI for Residential Verification by the Norwegian State Educational Loan Fund

The Norwegian State Educational Loan Fund (*Lånekassen*) successfully utilised machine learning to select candidates for 'residential verification—a process to confirm the addresses of students claiming to live away from their parents' home. In 2018, out of 25,000 students verified, 15,000 were chosen through AI, while 10,000 were randomly selected. The AI method proved more effective, with 11.6% failing the verification, compared to 5.5% from the control group.[938] This efficiency reduces the need for verification for genuine cases, decreasing the administrative burden for the agency and documentation required from students. Selected students had to prove they lived separately from their parents.

1.2.2.3 Vestre Viken Health Region's Use of AI Medical Image Analysis

Medical image analysis is one of the tasks at which AI systems are currently performing well. Internationally, radiology stands out as an area within medicine where AI systems are most frequently implemented. One of the first implementations of an AI system for diagnosis based on image analysis in Norway took place in 2023 when a hospital in the Vestre Viken health region started using an AI system for the analysis of images from patients suspected of suffering from minor bone fractures. The main benefit of implementing the AI system is time and resource efficiency: the time from taking an image to receiving the result is said to decrease from hours to

[935] Automatisering kutter ventetiden for å bli norsk. / Directorate for Digitalisation (Digdir) 16 August 2022 https://www.digdir.no/digitaliseringskonferansen/automatisering-kutter-ventetiden-bli-norsk/3780

[936] Automatisering kutter ventetiden for å bli norsk. / Directorate for Digitalisation (Digdir) 16 August 2022 https://www.digdir.no/digitaliseringskonferansen/automatisering-kutter-ventetiden-bli-norsk/3780

[937] Automatisering kutter ventetiden for å bli norsk. / Directorate for Digitalisation (Digdir) 16 August 2022 https://www.digdir.no/digitaliseringskonferansen/automatisering-kutter-ventetiden-bli-norsk/3780

[938] One Digital Public Sector: Digital Strategy for the Public Sector 2019–2025. Ministry of Local Government and Modernisation. 2019 (hereinafter Digital Strategy for the Public Sector 2019–2025) p. 23.

1–2 minutes.[939] The implemented AI system was acquired as a call-off under a framework agreement that can potentially be used to acquire and implement other AI systems in the near future.

1.2.3 Planned Projects

1.2.3.1 The NAV AI Sandbox Project to Predict Duration of Sickness Absence

In Spring 2021, NAV (the Norwegian Labour and Welfare Administration) collaborated with the Data Protection Authority's AI sandbox initiative.[940] Within this framework, NAV sought to harness AI, notably machine learning, to predict which individuals on sick leave might transition into extended absences. The motivation behind the project is NAV's belief that there are excessive, possibly unnecessary meetings, consuming the time of employers, professionals (like doctors), the individuals on sick leave, and NAV's advisers.[941] By employing a machine learning model that profiles the individuals on sick leave, NAV advisers could render more precise judgments regarding the necessity of a dialogue meeting and the subsequent support needed for the person on sick leave. To this end, NAV set out to use various data points including the individual's age, occupation, place of residence, and diagnosis. Moreover, NAV needed to process a vast amount of historical data encompassing personal details of those previously on sick leave to develop the software.

The objective of this sandbox project was to assess the legality of using AI in such a context and find ways on how profiling persons on sick leave can be performed in a fair and transparent manner.[942] However, the project was put on hold due to uncertainty related to the legal basis for developing the algorithm, as this would require the processing of large amounts of personal data on a significant number of people who are no longer on sick leave.[943]

1.2.3.2 Digitalising the right to access

The project aims to create a platform that gives citizens an overview, insight and increased control over their own personal data. This initiative is a crucial component of the government's Digital Agenda, specifically focusing on the 'Once-Only Principle', which aims to facilitate the delivery of seamless, proactive services while also promoting data-driven innovation and a user-centric experience.[944] As part of this initiative, the government has identified three key focus areas aimed at facilitating citizens' access to and sharing of their data.

The first pivotal element is the creation of the National Data Directory, which serves as a foundational step toward achieving the 'Once-Only Principle.'[945] This Directory is designed to enhance transparency in the processing of personal data. It provides citizens with a comprehensive overview of what types of personal information are being processed and identifies the specific sectors within the public domain responsible for this processing. This enables citizens to know precisely who to contact and about what topics, empowering them to exercise their rights under data protection regulations effectively.

[939] Er vi forberedt på å la maskinene behandle oss? / Topdahl, Rolv Christian, Mullis, Magnus Ekeli, and Nøkling, Anders. NRK, 25 September 2023 https://www.nrk.no/rogaland/xl/snart-vil-kunstig-intelligens-analysere-kroppen-din_-_-vi-er-for-darlig-forberedt-1.16553955

[940] Exit Report from Sandbox Project with NAV Themes: Legal Basis, Fairness and Explainability. / Datatilsynet. 03 January 2022 https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/reports/nav---exit-report/

[941] Exit Report from Sandbox Project with NAV Themes: Legal Basis, Fairness and Explainability. / Datatilsynet. 03 January 2022 https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/reports/nav---exit-report/ p. 4.

[942] Exit Report from Sandbox Project with NAV Themes: Legal Basis, Fairness and Explainability. / Datatilsynet. 03 January 2022 https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/reports/nav---exit-report/ p. 3.

[943] Ditt personvern – vårt felles ansvar Tid for en personvernpolitikk. / Norges offentlige utredninger (NOU) 2022: 11, Rapport fra Personvernkommisjonen, 26 September 2022 (hereinafter NOU 2022:11), p. 67.

[944] Digital Strategy for the Public Sector 2019–2025, p. 28.

[945] Digital Strategy for the Public Sector 2019–2025, p. 21.

The second focus area involves centralizing both guidance for public agencies and the option for citizens to request information access, all in a single platform. This approach puts the citizen at the forefront of public data management. Additionally, there is a proposal to standardize how public entities should respond to access requests, thereby creating a uniform experience for citizens. The third focus area specifically deals with citizens' ability to access and share their own personal information. The aim here is to amplify data sharing by granting citizens the ability to use their own data for various purposes. One proposed strategy is to delineate a set of core data elements—such as driver's licenses, academic diplomas, or income records—over which citizens can have varying degrees of control.

1.2.3.3 Several ongoing AI initiatives in the healthcare sector

While the Norwegian healthcare sector is often criticized for lagging in terms of digitalisation, several innovative projects pertaining to AI technologies are currently in motion. One such initiative is underway at Akershus University Hospital (Ahus), Norway's most expansive emergency hospital. Ahus is planning to develop an algorithm that predicts heart failure risks, utilizing factors such as ECG measurements as its foundation. This tool, designed for clinical settings, aims to enhance patient care by facilitating timely assessments and treatments, particularly for those exhibiting higher heart failure probabilities.

Moreover, at the University Hospital of North Norway (UNN), a project is underway to develop an AI system intended to support decisions on whether a patient should have spine surgery.[946] The main objective of the project is to enhance the results of spine surgery, as a considerable number of patients do not have satisfactory outcomes from certain types of spine surgery. By predicting individual patient outcomes, an AI system could enable more precise recommendations on which patients should undergo surgery.

In another noteworthy endeavour by the Bergen Municipality, there is a focus on forecasting stroke risks using data from emergency calls and preceding hospital contacts. This project is structured in three distinct phases. Initially, a comprehensive survey will analyze the healthcare interactions stroke patients in Helse Bergen have had prior to their admission and subsequent entry into the Stroke Register. Following this, the second phase emphasizes the development of an AI model. This model will be informed by an intricate analysis of emergency ('113') call data and structured datasets from the Norwegian patient register. Once developed, the final phase involves integrating the AI model at the Emergency Department at Haukeland University Hospital Bergen to determine if the AI's inclusion boosts the accuracy of stroke diagnoses. The goal transcends stroke predictions, with aspirations to implement AI assistance in diagnosing other acute medical conditions, including heart attacks and sepsis.

1.2.3.4 Government commits one billion NOK to bolster AI research

On September 7th, 2023, the government pledged one billion Norwegian kroner (approximately 94 million USD) to strengthen research in AI and digital technology over the coming five years.[947] This investment aims to deepen understanding of the societal ramifications of AI and other emerging technologies, thereby paving the way for innovative opportunities in both the private and public sectors. The government has identified three core areas for research:

- Delving into the societal repercussions of AI and various digital technologies, with a spotlight on their influence on democracy, trust, ethics, economy, rule of law, regulations, data protection, education, arts, and culture.

[946] In the interest of disclosure, it is noted that one of the authors of this chapter (Hauglid) has been involved in one of the 'work packages' pertaining to initial stages of the spine surgery project.

[947] Regjeringen med milliardsatsing på kunstig intelligens. Regjeringen, Pressemelding 07 September 2023 https://www.regjeringen.no/no/aktuelt/regjeringen-med-milliardsatsing-pa-kunstig-intelligens/id2993214/

- Undertaking research centred on digital technologies, which encompasses fields like artificial intelligence, digital security, next-generation ICT, novel sensor technologies, and quantum computing.
- Exploring the potential of digital technologies to foster innovation in both public and private spheres. This also includes studying the ways AI can be intertwined with research spanning diverse academic disciplines.

2. Overview of the Legal Framework in Supporting Digitization, Values and Rights

2.1 Relevant Legal Framework for the Protection of Human Rights

2.1.1 Human Rights and the Norwegian Constitution

Since the very adoption of the Norwegian Constitution in 1814, certain foundational principles resembling a modern understanding of human rights have found their place therein as citizen rights. These include the right to freedom of expression, the right to property, a prohibition of torture and a prohibition against arbitrary house searches.

Norway ratified the European Convention of Human Rights (ECHR) in 1952 and incorporated the convention directly into Norwegian law in 1999, through the Norwegian Human Rights Act – a significant milestone in strengthening the status of human rights in Norwegian law. The Human Rights Act also incorporates the following UN conventions into Norwegian law: The Covenant on Economic, Social and Cultural Rights (CESCR), the Covenant on Civil and Political Rights (CCPR), the Convention on the Rights of the Child (CRC), and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). Not only do these human rights instruments form an integral part of Norwegian law, they also take precedence over other provisions of Norwegian legislation in case of conflict. Moreover, Norway has ratified several UN human rights conventions such as the Convention on the Elimination of All Forms of Racial Discrimination (CERD) and the Convention on the Rights of Persons with Disabilities (CRPD).

The status of human rights in Norwegian law was further strengthened by a reform of the Constitution in 2014. The reform elevated several human rights to explicit recognition at the constitutional level. A new chapter in the Constitution now amounts to what can be likened to a 'bill of rights' for Norway.[948] In addition to the rights already enshrined in the Constitution before 2014, the new chapter includes human rights such as the right to life, the right to freedom of movement, the presumption of innocence, the right to equality before the law and non-discrimination, the right to a fair trial, the right to respect of privacy, family life and correspondence, the right to form and participate in organizations, children's right to integrity and human dignity, and the right to education.

While the human rights that are now enshrined in the Constitution have been recognized in Norwegian law long before the constitutional reform, the elevation to constitutional status signifies that these human rights are among the foundational values of the Norwegian constitutional democracy. To further underscore the status of human rights in Norway, the 2014 constitutional reform also introduced in the Constitution a general obligation for all authorities of the state to respect and ensure human rights.[949]

[948] Norges Høyesterett, Grunnloven og menneskerettighetene. / Bårdsen, Arnfinn. Menneskerettighetene og Norge. ed. / Andreas Føllesdal, Morten Ruud and Geir Ulfstein. Universitetsforlaget, 2017, p. 65. Vol. 1 1. ed. Universitetsforlaget, 2017, p. 65.

[949] Article 92 of the Norwegian Constitution.

Due to the status of human rights in Norwegian law, the jurisprudence of the European Court of Human Rights (ECtHR) is a significant source of interpretation when applying Norwegian law, including the constitutional human rights provisions.[950] As regards the rights that find their counterpart in UN Conventions, the decisions and guidance of the relevant UN committees are also applied as sources of interpretation.[951] Thus, the Norwegian Constitution is a living document influenced by the development within European and international human rights law.

2.1.2 Norwegian Public Administration Law

The Norwegian public administration is governed by the 1967 Public Administration Act (PAA). The PAA lays down procedural rules that generally apply to administrative agencies and officials across all sectors. It operationalizes the foundational principles of Norwegian public administration law, such as freedom of information, the right to participation and contestation, the rule of law and legal safeguards for the individual citizen, neutrality, and proportionality.[952]

For example, the PAA sets forth the requirements as to a public official's impartiality, the duty of confidentiality, information rights for parties involved in administrative cases, and the requirements pertaining to the preparation and provision of the grounds for an administrative decision that affects individual citizens. The PAA is supplemented by the 2006 Freedom of Information Act (FIA), which provides that the case documents, journals and registries of an administrative agency shall, as a main rule, be available to the public free of charge.[953] Citizens are also entitled to access a collation of information pertaining to specific cases or case types, from digital databases held by an administrative agency.[954]

In addition to the PAA and the FIA, Norwegian public administration is regulated in more detail by sector-specific statutes. Over the years, the PAA and the sector-specific statutes have been amended several times, including piecemeal adaptations to accommodate the increased importance of digital technologies in the Norwegian public sector. An extensive effort was made in 2000, to amend regulations that prevented electronic communication between citizens and administrative agencies (the eRegulation project).[955] Thereafter, a principle was established that regulations shall be interpreted as technology-neutral, and that any requirements for paper-based communication shall be specifically stipulated in the relevant provisions.[956] Technological neutrality is currently a guiding principle for legislative efforts in Norwegian public administration law. Hence, the Norwegian legislature's strategy is to create rules prescribing certain functions, rather than prescribing the means through which such functions are performed.[957]

Moreover, a proposal for a comprehensive reform of the PAA is currently being processed at a political level. Not surprisingly, the proposal addresses the need to facilitate digitalisation. The proposal is further discussed in section 3.3, where we identify certain trends in the legislative reforms related to the digitalisation of the Norwegian public sector and examine how this continuously evolving landscape promotes core principles and values of the Norwegian democracy while facilitating digitalisation.

[950] Judgment of the Norwegian Supreme Court, 18.12.2014 (Rt. 2014 p. 1292), paragraph 14.
[951] Judgment of the Norwegian Supreme Court, 19.12.2008 (Rt. 2008 p. 1764).
[952] Alminnelig forvaltningsrett. / Graver, Hans Petter. 4 ed.: Universitetsforlaget, 2015, chapters 4–8.
[953] Article 3 FIA, cf. Article 8 FIA.
[954] Article 9 FIA, cf. Article 28 FIA.
[955] Article 15 a PAA.
[956] Digital Strategy for the Public Sector 2019–2025, p. 11.
[957] Norges offentlige utredninger (NOU) 2019: 5 Ny forvaltningslov (hereinafter NOU 2019: 5**)**, p. 259.

2.2 Core Principles and Values Guiding Public Sector Digitalisation in Norway

Core principles and values for digitalisation in the Norwegian public sector are outlined in the 2019–2025 National Strategy for Digitalisation of the Public Sector. This strategy document is titled "One Digital Public Sector", and alludes to the overarching objective of ensuring integrated, seamless and user-centric public services based on real-life events and an 'only once' principle. The goal is for users – citizens, and public and private enterprises – to perceive their interaction with the public sector as seamless and efficient, as 'one digital public sector'.[958] As part of this objective, the digitalisation strategy highlights the importance of data sharing within and from the public sector as well as data re-use, enhanced cooperation and coordination across administrative levels and sectors (specifically through the implementation of common digital solutions and common digital infrastructures), enhanced digital literacy in the public sector, and digital security. Furthermore, it specifically underscores the need to develop a digitalisation-friendly legal framework. In 2023, the Government announced that it had initiated work on the development of a new digitalisation strategy. We expect that the new strategy will address AI technologies in more depth and that it will provide the Norwegian Government's perspective on the EU's forthcoming AI Act.

Norway's current strategy for AI, announced in 2020, also emphasises the potential for enhancement of public services through digitalisation. It particularly depicts the implementation of AI technologies as a crucial element of future digitalisation efforts in the public sector. As regards the guiding principles and values for AI development and deployment, the strategy underscores, above all, that AI developed and used in Norway should adhere to ethical principles and respect human rights and democracy. The strategy relies heavily on the Guidelines for Trustworthy AI developed by the EU High-Level Expert Group on AI. These guidelines set out key ethical principles that there is considerable consensus about in the contemporary discourse around AI technologies.[959] These principles have influenced Digdir's guidance on responsible development and use of AI in the public sector.[960]

On the basis of the aforementioned documents, digitalisation and implementation of AI technologies in the Norwegian public sector is guided by the following core principles and values (the list is non-exhaustive):

- **Privacy and data protection:** Privacy and data protection are the most prominent concerns in policy documents relating to the digitalisation of the Norwegian public sector, including the National AI Strategy. There is a high level of awareness of the privacy and data protection risks associated with data sharing between public agencies and the use of data for AI training purposes.
- **Human agency and oversight:** The National AI Strategy emphasises that AI development should enhance rather than diminish human agency and self-determination.[961] It particularly highlights the right not to be subject to fully automated processing of personal data and suggests that humans should be involved in all stages of a decision-making process.

[958] Digital Strategy for the Public Sector 2019–2025, p. 13; Stortingsmelding nr. 27 (2015–2016) Digital agenda for Norge.

[959] The Global Landscape of AI Ethics Guidelines. / Anna Jobin, Marcello Ienca and Effy Vayena. In: Nature Machine Intelligence, No. 1, September 2019, p. 389–399; A Framework for Language Technologies in Behavioral Research and Clinical Applications: Ethical challenges, Implications and Solutions. / Catherine Diaz-Asper et al. In: American Psychologist, 2023 (the article is forthcoming and will be available, upon publication, via DOI: 10.1037/amp0001195.

[960] Råd for ansvarlig utvikling og bruk av kunstig intelligens i offentlig sektor. / Directorate for Digitalisation, https://www.digdir.no/kunstig-intelligens/rad-ansvarlig-utvikling-og-bruk-av-kunstig-intelligens-i-offentlig-sektor/4272.

[961] National AI Strategy, p. 59.

- **Technical robustness and safety:** The concepts of robustness and safety in relation to AI and digitalisation encompass various aspects, including information security, human safety, and the safe use of AI. AI systems should not harm humans. To prevent harm, AI solutions must be technically secure and robust, safeguarded against manipulation or misuse, and designed and implemented in a manner that particularly considers vulnerable groups. AI should be built on technically robust systems that mitigate risks and ensure that the systems function as intended.
- **Transparency and explainability:** Transparency is a central element of the rule-of-law and in building trust in the administration, especially when new systems like AI are being deployed. An open decision-making process allows one to assess whether the decision was fair and also allows for the possibility of lodging complaints. The National Strategy for Digitalisation of the Public Sector emphasizes that the public sector *'shall be digitalised in a transparent, inclusive and trustworthy way.'*[962]
- **Non-Discrimination, equality, and digital inclusion:** Concerns about discrimination have become more salient in the Norwegian digitalisation discourse in recent years, as it has been recognized that AI systems might discriminate against vulnerable groups. In relation to digitalisation not involving AI systems, the objective of non-discrimination has been heralded as an argument in favour of digitalisation because automated, rule-based systems are perceived as more 'neutral' than human assessments. However, AI technologies may display biases that could lead to discrimination. Recognising this problem, the Norwegian Equality and Anti-Discrimination Ombud released a guidance document on '*innebygd diskrimineringsvern*,' in November 2023.[963] '*Innebygd diskrimineringsvern*' literally translates to 'embedded protection against discrimination,' and is inspired by the emerging notion of 'non-discrimination by design.'[964] Closely related to non-discrimination and equality, diversity and digital inclusion are also core values of digitalisation in the Norwegian public sector. Digital inclusion involves engaging a diverse range of users in the development and implementation of digital technologies, to better understand and meet various needs. For example, legislation in Norway concerning workers' rights guarantees that workers and their representative bodies have a say in the integration of new technologies into the work environment.[965]
- **Accountability:** While accountability has arguably not been at the forefront of the Norwegian discourse on digitalisation and AI implementation, this principle is emphasised in the EU's principles for trustworthy AI and has been enshrined in the National AI Strategy. In the Strategy, accountability is explained as an overarching requirement pertaining to the need to implement AI solutions that enable external review.[966]
- **Environmental and societal well-being:** Environmental and societal well-being is an important political and legislative principle guiding digitalisation efforts in Norway. Article 112 of the Norwegian Constitution protects the right to a healthy, productive and diverse environment. This article emphasizes the duty of the state to ensure both current and future generations' right to a healthy environment and provides citizens with a right to information concerning the state of the natural environment and the effects of planned

[962] Digital Strategy for the Public Sector 2019–2025, p. 8.

[963] Innebygd diskrimineringsvern. / Likestillings- og diskrimineringsombudet, 2022, https://ldo.no/globalassets/_ldo_2019/_bilder-til-nye-nettsider/ki/ldo.-innebygd-diskrimineringsvern.pdf .

[964] Innebygd diskrimineringsvern. / Likestillings- og diskrimineringsombudet, 2022, https://ldo.no/globalassets/_ldo_2019/_bilder-til-nye-nettsider/ki/ldo.-innebygd-diskrimineringsvern.pdf . p. 19; Non-Discrimination by Design. / van der Sloot et al., 2023, https://www.tilburguniversity.edu/about/schools/law/departments/tilt/research/handbook .

[965] Norwegian Position Paper on the European Commission's Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021) 206), p. 5.

[966] National AI Strategy, p. 60.

> or implemented measures. This provision has been the subject of a lively societal debate in Norway in recent years a debate that has been driven particularly by a lawsuit from two environmental organizations unsuccessfully seeking to invalidate a governmental decision to allocate petroleum extraction licenses on the Norwegian continental shelf.[967] In addition to Article 112 of the Constitution, it is worth highlighting that Norwegian law lays down a general statutory obligation to consider the environmental impact whenever public authority is exercised.[968]

In section 3, we refer to these principles as we assess the adequacy of the current and emerging legal framework in terms of its ability to support digitalisation while ensuring the governing principles and rights. Before proceeding, it is worth noting that while there is a certain level of agreement on the core principles, it is inescapable that these principles cannot be equally satisfied in all circumstances. For example, it is often recognised that the maximisation of an AI system's accuracy might not be compatible with the maximisation of explainability.[969] Another trade-off arises between data privacy and accuracy or explainability, especially in cases where a technological solution is likely to improve if larger amounts of personal data are used to develop it. It is in relation to these types of trade-offs between commonly recognised digitalisation principles that diverse opinions tend to emerge in the Norwegian discourse.

3. Adequacy of the Legal Framework in Supporting Digitalisation, Values and Rights

3.1 Adequacy of Current (or Emerging) Framework in Supporting Digitalisation

This section explores ongoing legislative efforts in Norway to facilitate public sector digitalisation. We identify two primary categories of legislative changes driving these initiatives: those related to data sharing and reuse, and those governing the use of automated data processing and decision-making technologies. Furthermore, we examine the extent to which the Norwegian framework accommodates pilot schemes and regulatory sandboxes, which are pivotal to the adaptation of new technologies.

3.1.1 Ongoing Legislative Efforts

As mentioned earlier, Norway stands as one of the countries with a highly digitalised public sector. This is partly due to concerted efforts to adapt existing legal frameworks to be more conducive to digitalisation. Electronic communication between public administration and citizens is particularly facilitated by the current legal framework. However, we expect that future legislative efforts will contain more specific regulations aimed at fostering further digital transition. Furthermore, continuous efforts are being undertaken to overcome any obstacles to public sector digitalisation.

In this section, we describe significant legislative efforts that have been made or proposed to facilitate public sector digitalisation. According to the Law Commission on the PAA, regulations

[967] Judgment of the Norwegian Supreme Court, 22.12.2022 (HR-2020-2472-P). A crucial question concerned the extent to which Article 112 of the Constitution provides a right that individuals can invoke to invalidate decisions by state authorities. The Supreme Court ruled that the constitutional provision can only be relied on as such a right in a very limited set of circumstances. According to the ruling, this right cannot be relied on to invalidate decisions in matters that have been assessed by the Parliament, except in cases where the Parliament has grossly neglected its duties.

[968] Nature Diversity Act of June 19, 2009, No. 100, § 7.

[969] Ethics and Governance of Artificial Intelligence for Health: WHO Guidance. / World Health Organization, Geneva, 2021.

should be *'clear and understandable, without undue complexity or unnecessary discretionary provisions.'*[970] Furthermore, regulations should facilitate increased data sharing and seamless services, and use harmonised concepts.

The ongoing reform of the PAA stands out as an obvious venue for the facilitation of public sector digitalisation in Norway. The proposal for a new PAA takes a balanced approach to digitalisation, highlighting opportunities and risks. As regards risks, the proposal is particularly concerned with the privacy of citizens. Hence, it underscores the need to ensure that the processing of personal data is based on purpose limitation and proportionality. While the comprehensive PAA reform could take years to implement, certain piecemeal adaptations of sector-specific legislation have been enacted in recent years. In the following, we consider the main digitalisation efforts in Norwegian law, including the PAA proposal as well as some of the sector-specific changes that have been proposed, to give an overview of the extent to which the current/emerging legal framework supports digitalisation. As mentioned, our principal emphasis is on the facilitation of AI technologies.

3.1.2 Data Sharing and Data Reuse

Regulations pertaining to the use or reuse of data are often highlighted as barriers to digitalisation and, particularly, AI development, in Norway. For example, the Law Commission on the PAA notes the difficulty of implementing cohesive services without sharing data across agencies.[971] The lack of authority to share information can pose challenges in effectively organizing public administration. It might prevent full automation of administrative proceedings in areas that lend themselves to this. The Commission therefore proposes that authority be given to share confidential information with other administrative bodies on a need-to-know basis, widening the legal basis for such data sharing.[972] Following the proposal, a provision has been enacted in the PAA (§ 13 g) which gives the Government the authority to issue regulations concerning information sharing between public agencies irrespective of the general duty of confidentiality. This authority has been utilised to issue a regulation facilitating the sharing of confidential information to effectively fight and prevent crime within the labour market and working life.[973] The regulation specifies the agencies that may share confidential information, the lawful purposes of data sharing, and the categories of personal data these agencies may share. It also contains provisions on controllership responsibility according to the GDPR and erasure requirements.

Moreover, as regards data sharing, the National AI strategy particularly notes how current regulations '*provide no clear legal basis for using health data pertaining to one patient to provide healthcare to the next patient unless the patient gives consent.'*[974] There are examples of cases where AI projects have been discontinued because of privacy concerns, particularly a lack of legal basis for training AI.[975]

In sector-specific legislation, certain rules have been introduced in response to concerns about limitations on the access to data as barriers to digitalisation and AI development. Notably, a specific provision concerning the possibility of applying for permission to use health data for the purposes of developing and using clinical decision support systems was added to the Health Personnel Act in 2021. In the preparatory works, the Ministry of Health acknowledges that the

[970] NOU 2019: 5, p. 102.
[971] Digital Strategy for the Public Sector 2019–2025, p. 18.
[972] National AI Strategy, p. 27; Consultation Memorandum of the Justis- og beredskapsdepartementet (Ministry of Justice and Public Security), September 2020, Ref. No. 20/4064.
[973] Regulation 17 June 2022 No. 1045 (Forskrift om deling av taushetsbelagte opplysninger og behandling av personopplysninger m.m. i det tverretatlige samarbeidet mot arbeidslivskriminalitet (a-kriminformasjonsforskriften).
[974] National AI Strategy, p. 23.
[975] VF-Rapport nr. 7-2022, p. 47.

permissibility of using health data for these purposes was ambiguous before this. The new provision is an example of how the use of special categories of personal data (as per Article 9 GDPR) can be regulated at the national level. It was relied on in the Ahus sandbox project mentioned in section 1.2.[976]

3.1.3 Facilitation of Automated Processing and Decision-Making

The potential for automation of administrative case handling is highlighted in the 2019 PAA proposal. As mentioned in section 1, several examples of automated processing already exist in the Norwegian public sector.[977] The 2019 PAA proposal emphasizes the potential for increased efficiency and equal treatment of similar cases, due to the assumed consistency of software-based case handling. Hence, the automation foreseen by the 2019 PAA proposal primarily anticipates the use of hard-coded software programs handling cases according to pre-defined rules. It is noted in the proposal that the main potential pertains to decisions that are favourable to those concerned by the decisions, where the decisional outcome is governed by precise criteria not involving individual case assessments.[978] Thus, the proposal reflects a rather careful approach to automated decision-making, and it does not discuss the potential for advanced AI-based decision-making in much depth. Since the proposal was set forth, the potential for automated and semi-automated decision-making based on AI technologies has become more imminent. We therefore expect that the risks and benefits of using AI systems, which may be capable of conducting individual assessments based on more discrete criteria, will be raised as an important topic in the ongoing legislative process.

As regards the need for a legal basis in national law for fully automated decision-making, pursuant to Article 22 GDPR, the 2019 PAA proposal suggests a general provision according to which the Government is given the authority to issue regulations governing the use of fully automated decision-making in specific types of cases. However, decisions that do not have important restrictive impacts on the rights and interests of an individual can rely on fully automated means, according to the proposal.[979] This is in line with the general starting point under current Norwegian law, which is that fully automated decision-making is allowed unless anything else is specified. Due to the 'qualified prohibition' of making important individual decisions based on fully automated processing of personal data in Article 22 GDPR,[980] specific provisions facilitating such decision-making are typically required at the national level. There are a few examples of such provisions in Norwegian legislation, to which we shall now turn.

One example of a provision facilitating fully automated decision-making is found in § 11 of the 2014 Norwegian Patient Journal Act. According to this provision, certain decisions can be based solely on automated processing of personal data, when the decision is of minor impact to the individual. In the preparatory works, which are important sources of legal interpretation in Norway, decisions concerning small monetary amounts are mentioned as an example of minor impact decisions.[981] Furthermore, the preparatory works state that a fully automated decision must depend only on criteria that are clear and objectively verifiable, for example, decisions on reimbursement of travel expenses, etc. The provision does not permit full automation of decisions

[976] A Good Heart for Ethical AI: Exit Report for Ahus Sandbox Project (EKG AI). Theme: Algorithmic Bias and Fair Algorithms. / Norwegian Data Protection Authority (Datatilsynet), February 2023 (https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/reports/ahus-exit-report-a-good-heart-for-ethical-ai/objective-of-the-sandbox-project/).

[977] See also NOU 2019: 5, p. 259.

[978] NOU 2019: 5, p. 174

[979] NOU 2019: 5, p. 263.

[980] Regulating Automated Decision-Making: An Analysis of Control over Processing and Additional Safeguards in Article 22 of the GDPR. / Mariam Hawath. In: European Data Protection Law Review, Vol. 7, No. 2, 2021, p. 161–173.

[981] Prop. 91 L (2021–2022) Endringer i pasientjournalloven mv. (hereinafter 'Prop. 91 L (2021–2022)), p 43.

determining a patient's access to healthcare services.[982] Such decisions are not deemed as minor impact decisions. The legislature assumes that these and other non-minor impact decisions would require specific regulations containing safeguards tailored to the risks associated with fully automated decision-making. While such specific regulations are not set out in the current legal framework pertaining to the health sector, the Patient Journal Act provides the Government with the authority to issue such specific regulations.

A similar example is found in provisions added simultaneously to the 1949 Norwegian Act on the State Pension Fund (*Statens pensjonskasseloven*) (§ 45 b), the 2006 Act on the Norwegian Labour and Welfare Administration (*NAV-loven*), and the 2016 Norwegian Tax Administration Act, in 2020 and 2021. These provisions permit the State Pension Fund, NAV, and the Tax Administration, to make decisions based on fully automated processing of personal data, given that such decision-making is compatible with the right to data protection and is not based on criteria that require the exercise of decisional discretion. An exception from the latter restriction is applicable for decisions where the outcome is not questionable.[983] This is to be interpreted as referring to cases where the outcome of a decision would be clear and obvious to a human case handler, even if there appears to be an element of discretion inherent in the relevant criterion.[984] The purpose of these provisions is primarily to facilitate automated decisions concerning the amount of pension payments or welfare/social security benefits a person is entitled to.[985] While these provisions do not formally restrict the use of AI in decision-making, the use of AI is in practice restricted by the limitation against automated processing when the criteria governing a decision imply an element of discretion. The practical implication of this rule is that the legislation only facilitates automation based on hard-coded software systems.

In addition to providing a limited basis for automated decision-making, the Norwegian Tax Administration Act explicitly facilitates profiling by the tax administration based on personal data when profiling is deemed necessary for the purpose of imposing targeted measures promoting compliance with the tax legislation. We return to this example in section 3.2 in connection with the discussion of to what extent the rights and values governing the digitalisation of the Norwegian public sector are protected within the emerging legal framework.

3.1.4 Pilot Schemes and Sandboxes

In addition to specific initiatives, there are overarching systems in place designed to accelerate the digitalisation of the public sector.

Central to AI adoption are the pilot programs for public administration and the government's emphasis on sandboxes. Norway has a unique law, the Act on Pilot Schemes by Public Administration of 1993 (*Lov om forsøk i offentlig forvaltning (forsøksloven)*), which is designed to foster experimentation within the public sector. This law aims to cultivate efficient organizational and operational capabilities in public administration via trials or experiments and seeks to optimize task distribution among various administrative bodies and levels. A significant focus lies in enhancing public service delivery, ensuring optimal resource use, and fostering robust democratic governance (Article 1).

Under this legislation, particularly Article 3, public agencies can request the Ministry of Local Government and Modernisation for permission to deviate from prevailing laws and regulations.

[982] Prop. 91 L (2021–2022) Endringer i pasientjournalloven mv. (hereinafter 'Prop. 91 L (2021–2022)), p 43.

[983] Act 28 July 1949 No. 26 on the State Pension Fund, § 45 b, second indent; Act 16 June 2006 No. 20 on the Labour and Welfare Administration, § 4 a, second indent.

[984] Prop. 135 L (2019–2020) Endringer i arbeids- og velferdsforvaltningsloven, sosialtjenesteloven, lov om Statens pensjonskasse og enkelte andre lover (hereinafter 'Prop. 135 L), p. 20.

[985] Prop.135 L (2019–2020), p. 58 and 60.

This provision provides them with the flexibility to experiment with novel organizational methods or task executions for up to four years. Such trial periods can receive extensions of up to two years, and if there are impending reforms aligned with the trial's objectives, the duration can be extended until the reforms become operational. In 2021, Oxford Research conducted the first review of the Pilot Scheme Act since its enactment in 1993 and concluded that the Act is little known and rarely used.[986] Out of a total of 143 identified experiments, 45 of them are based on the Pilot Scheme Act, while 55 are without legal basis. Since 2008, only two experiments have been based on the law.[987]

The National AI Strategy highlights that the government plans to release a white paper assessing if the Pilot Scheme Act offers ample leeway to trial innovative AI-based solutions.[988] Notwithstanding this, the Norwegian Data Protection Authority is sceptical that the current form of the Pilot Scheme Act offers sufficient flexibility for public agencies to experiment with AI.[989] First, the Agency is sceptical that experiments with AI fit within the objectives of the Act and emphasizes that if the Act is to serve as a legal basis for conducting experiments related to the use of AI, it should be explicitly stipulated. Second, confidentiality presents a significant challenge for AI-related experiments. This is partly due to the exceptions provided in the Act, specifically Article 4 (3–4), which prevent experiments that deviate from rules designed to protect individual rights and the rule of law. Consequently, experimentation would not justify deviations from confidentiality rules or the weakening of individual rights.

Therefore, as the Pilot Scheme Act stands today, experiments with AI would not be feasible, in part because of the exception related to confidentiality and citizens' rights and obligations.[990] This suggests that if the Pilot Scheme Act were to permit AI experiments, the Data Protection Authority believes that the law should, at the very least, reference the GDPR.[991] However, in its present state, the Act lacks provisions that establish a legal basis for processing personal data, and it is assumed that general rules and any specific laws for processing of personal data would be applicable. Accordingly, the evaluation study recommends amending the Pilot Scheme Act to allow public agencies to experiment with new technologies, especially in the realm of AI.[992] This is because the current law's purpose clause emphasizes resource utilization and efficiency.

Moreover, the Norwegian government has been a strong proponent of using regulatory 'sandboxes' to foster innovation across diverse sectors. In 2019, the Norwegian Financial Supervisory Authority (*Finanstilsynet*) created a sandbox specifically for financial technology (fintech). This initiative aimed to deepen the Financial Authority's grasp of emerging technological solutions in the financial sector and simultaneously enhance businesses' understanding of regulatory requirements for new products, services, and business models.[993] This approach has since been expanded to other domains, such as transportation and data protection. Starting in 2016, the government has established different test beds in the transportation sector to facilitate trials for autonomous vehicles and maritime vessels. These sandbox initiatives have occasionally set the stage for the development of new legislation. In 2018 and 2019, laws were passed permitting the testing of autonomous vehicles and authorizing autonomous coastal shipping within specified channels.[994]

In 2022, the sandbox strategy was broadened to cover privacy and AI with the creation of the

[986] Evaluering og utredning av forsøksloven. / Oxford Research. 2021.
[987] Evaluering og utredning av forsøksloven. / Oxford Research. 2021, p. 1.
[988] National AI Strategy, p. 24.
[989] Evaluering og utredning av forsøksloven. / Oxford Research. 2021, p. 40.
[990] Evaluering og utredning av forsøksloven. / Oxford Research. 2021, p. 52.
[991] Evaluering og utredning av forsøksloven. / Oxford Research. 2021, p. 40.
[992] Evaluering og utredning av forsøksloven. / Oxford Research. 2021, p. 53.
[993] National AI Strategy, p. 24.
[994] National AI Strategy, p. 24.

'Sandbox for Responsible AI'. Overseen by the Norwegian Data Protection Authority, this endeavour aims to boost AI innovation within Norway.[995] As demonstrated in section 4, public sector projects have prominently featured in this sandbox, bringing significant benefits to the public administration sector.

3.2 Adequacy of Current (or Emerging) Framework in Strengthening Values and Rights

As described in the previous section, the legal framework governing the Norwegian public sector does not entail a holistic approach to digitalisation or AI technologies. Consequently, there are few laws that specifically address the potential negative impacts of digitalisation on the fundamental rights and values upon which the Norwegian constitutional democracy is founded. This has led to criticism from stakeholders suggesting that government initiatives are not backed by adequate safeguards to protect fundamental rights, democracy, and the rule of law. In the following, we discuss the current and emerging legal framework's ability to enhance the values and rights that were highlighted in section 2.2, which ought to govern the digitalisation of the Norwegian public sector.

3.2.1 Privacy and Data Protection

Although the government's strategies for digitalisation of the public sector and AI emphasize the importance of user privacy, the Commission for Data Protection (*Personvernkommisjonen*) has highlighted shortcomings in effectively addressing data protection issues.[996] Specifically, the Commission identifies several key challenges.

First, there is an absence of a unified approach to privacy across public administration. As it stands, no single public agency bears overarching responsibility for assessing the aggregate use of personal data in public services. Current evaluations tend to be conducted within the confines of individual sectors or as part of specific legislative or regulatory efforts. This fragmented approach results in a glaring absence of a holistic overview concerning the collection, use, and further processing of personal data within public administration.[997] Moreover, there is a lack of clarity and comprehensive guidance on how administrative agencies should evaluate data protection issues and weigh them against other considerations.[998]

Second, and closely related to the first point, there exists a noticeable gap in establishing a comprehensive framework for assessing the impact of legislative changes on user privacy.[999] While general requirements exist for conducting privacy impact assessments for new legislation or proposed amendments, these mandates have not been consistently implemented in practice. Several factors contribute to this lack of attention to privacy during the regulatory development process including insufficient guidance, a scarcity of expertise and resources, and a failure to adequately consult with the Data Protection Authority as outlined in Article 36 (4) of the GDPR.[1000] In this context, the Commission refers to the amendments to PAA that would significantly broaden the scope for sharing confidential information, including personal data, between administrative agencies.[1001] This amendment also paved the way for the issuance of Ministerial orders that provide further specifications on inter-agency information sharing. Despite the preliminary work on these proposed changes emphasizing the imperative to consider data

[995] Regulatory Privacy Sandbox. Datatilsynet https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/
[996] NOU 2022: 11, p. 61.
[997] NOU 2022: 11, p. 71–72.
[998] NOU 2022: 11, p. 73.
[999] NOU 2022: 11, p. 73–74.
[1000] NOU 2022: 11, p. 75.
[1001] NOU 2022: 11, p. 75.

protection and privacy interests, the Ministry of Justice failed to conduct a formal impact assessment to gauge the implications of these changes on individual privacy.[1002] Similarly, the Commission identifies a growing trend to implement measures with significant effects on citizens' privacy through Ministerial orders (*forskrifter*), rather than through laws passed by Parliament. Beyond causing fragmentation in terms of data protection, this approach effectively deprives Parliament of the opportunity to exercise oversight over the use of personal data within the administrative framework.[1003]

Third, the Commission draws attention to the widespread use of broad legal bases for the processing of personal data by public agencies.[1004] In this regard, the Commission commissioned a study to examine the legal basis for citizen profiling, specifically for the purpose of detecting and monitoring fraud in the use of public benefits. The findings indicate that the legal grounds supporting the Tax Authority (*Skatteetaten*) and the Norwegian Labour and Welfare Administration (NAV) in their collection and use of personal data for fraud detection are based on inadequate evaluations. These evaluations fall short in light of Article 102 of the Norwegian Constitution and Article 8 of the ECHR, which calls for respect for private life, family life, home, and communication. The study highlights that only superficial, summary evaluations have been conducted to establish these legal frameworks, suggesting a need for more rigorous analysis.[1005]

Another area of concern relates to the legal provisions allowing public agencies to implement automated decisions, as specified in GDPR Article 22(2)(b). This article provides exceptions for the use of automated decisions if permitted by member states' laws. The report notes that as of Spring 2022, there have been more than 16 laws and ministerial orders in Norway that permit such automated decisions by public agencies.[1006] In this context, Article 22(2)(b) also mandates that any law permitting automated processing must include *'suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.'* However, beyond generalized provisions for considering privacy issues, these Norwegian laws have not provided further rules to ensure the protection of people's rights and freedoms.[1007]

Fourth, there is a notable deficiency in essential routines and expertise for assessing the impact of digitalisation on data security.[1008] Despite a generally high level of public trust in the public sector, the report indicates that citizens have low confidence in authorities' capabilities to maintain information security. This erosion of trust is partially attributed to an increased public awareness of privacy issues, exacerbated by incidents such as cyberattacks on the Parliament and Østre Toten municipality. Finally, the Commission identifies multiple challenges related to the sharing of personal data between public agencies. One such obstacle is the absence of a well-defined legal framework to govern this sharing. Another significant concern is the unclear demarcation of roles among these agencies when it comes to adhering to privacy regulations, including the implementation of users' rights.[1009]

While these challenges specifically pertain to data protection issues, they also underscore the broader absence of an adequate framework to strengthen the democratic process and rule of law. Notably, the lack of Parliamentary oversight for many of these changes, as well as the absence of impact assessments for fundamental rights, are of particular concern and have implications that extend to other areas. Other scholars share these concerns identified by the

[1002] NOU 2022: 11, p. 75.
[1003] NOU 2022: 11, p. 72.
[1004] NOU 2022: 11, p. 73–74.
[1005] NOU 2022: 11, p. 81.
[1006] NOU 2022: 11, p. 189.
[1007] NOU 2022: 11, p. 189–90.
[1008] NOU 2022: 11, p. 61
[1009] NOU 2022: 11, p. 77.

Commission. For example, Broomfield and Lintvedt criticise some of the changes introduced in 2021 to the Tax Administration Act, which granted the Tax Administration Office a legal basis to process personal data for activities like compilation, profiling, and automated decision-making.[1010] The amendment is aimed at giving the Tax Authority the possibility of using profiling and automated decision-making in evaluating tax determinations and risks of fraud. Their criticism pertains to the expansion of the Act's scope without thorough debate and the inadequacy in addressing concerns voiced by the Data Protection Authority. These concerns revolve around the unclear definitions of which information can be used for what purposes and the lack of proposed measures to safeguard individual rights and freedoms.[1011] Additionally, there is unease over the absence of measures evaluating how these changes might impact individuals' rights under the ECHR, the Norwegian Constitution, and the Data Protection Regulation, in particular as it relates to the right to protection against discrimination.[1012]

In contrast, as described in the previous section, the provisions facilitating fully automated decision-making in the Labour and Welfare Administration do not address the use of AI for profiling or other processes if this requires discretionary assessment, such as when determining benefits. This qualification to exclude the use of automated processing to make decisions based on discretionary criteria is partially motivated by the protection against non-discrimination, as recognized under § 98 of the Constitution and Article 14 of the ECHR, as well as individuals' data privacy rights, particularly their right against solely automated decisions that have significant impact. However, it is becoming increasingly evident that the use of outputs from automated processing of personal data, such as categorizing people into risk groups based on profiling, can have a significant impact on individuals, even though the decision is ultimately made by a human being. In her study, Lintvedt points out that process-leading decisions, such as selections for inspection, can be of such an intrusive nature that it could have a similar impact on the individual as a decision.[1013] Indeed, if the output from automated data processing is likely to unduly influence human decisions, it merits careful consideration. This is particularly relevant in light of research on 'automation bias', where people tend to favour results generated by automated systems, even when they might be flawed or incorrect.

Certain courts have begun evaluating the implications of risk assessment systems. A notable example occurred in February 2020, when the District Court of The Hague handed down a landmark decision concerning the controversial System Risk Indication (SyRI) algorithm deployed by the Dutch government.[1014] Primarily targeting neighbourhoods predominantly inhabited by poor or minority groups in the Netherlands, SyRI was an algorithmic tool used to detect fraud. It constructed risk profiles of individuals to uncover various types of fraud, such as those related to social benefits, allowances, and taxes.

The Court concluded that even though the use of SyRI does not inherently aim for legal effect, a risk report significantly impacts the private life of the individual it pertains to. This determination, coupled with other findings like the system's lack of transparency, led the Court to rule that the scheme violated Article 8 of the ECHR, which safeguards the right to respect for private and family life. However, the Court refrained from definitively answering whether the precise definition of automated individual decision-making in the GDPR was met, or whether one or more of the GDPR's exceptions to its prohibition applied in this context.

[1010] Snubler Norge inn i en algoritmisk velferdsdystopi? / Broomfield, Heather and Lintvedt, Mona Naomi in Tidsskrift for velferdsforskning, 25/3 2022.

[1011] Snubler Norge inn i en algoritmisk velferdsdystopi? / Broomfield, Heather and Lintvedt, Mona Naomi in Tidsskrift for velferdsforskning, 25/3 2022, p. 8.

[1012] Snubler Norge inn i en algoritmisk velferdsdystopi? / Broomfield, Heather and Lintvedt, Mona Naomi in Tidsskrift for velferdsforskning, 25/3 2022.

[1013] Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering. / Lintvedt, Mona Naomi. Utredning for Personvernkommisjonen. 2022.

[1014] Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities. / Vale, Sebastião Barros and Fortuna, Gabriela Zanfir. Future of Privacy Forum. 2022.

A German Court has referred this issue to the CJEU for resolution. The case pertains to the business model of SCHUFA, a German credit reference agency. SCHUFA provides its clients, including banks, with information about consumers' creditworthiness using 'score values.'[1015] Instead of focusing solely on the downstream decisions based on these scores (e.g., automatic loan application rejections), the Court preliminarily appears to scrutinize the upstream credit scoring as an automated decision in itself. This is because the process has a significant impact on subsequent decisions affecting data subjects. The key question posed by the referring Court to the CJEU is whether credit scoring qualifies as an automated decision that might be prohibited under Article 22 of the GDPR. [1016] Similar queries have been forwarded to the CJEU by other national courts. These cases offer an opportunity for the CJEU to provide clarity on the relevance of Article 22(1) to such automated personal data processing that is used to inform decisions potentially having a significant impact on individuals. Regardless of the outcomes, the key takeaway from the above discussion is that simply excluding automated decisions with significant determinations based on discretionary criteria is not in itself sufficient to ensure safety or protect individual rights.

3.2.2 Environmental Well-Being

In a digitalisation context, the implication of Article 112 of the Norwegian Constitution is that decisions concerning digitalisation measures must take the environmental impact of the measure into account. This might involve assessing the energy consumption of digital technologies. In theory, environmental impact assessments could be decisive when choosing between different solutions to implement. Such considerations could also influence the direction of future research and development initiatives supported by the Norwegian state. For instance, due to the substantial energy consumption involved in training machine learning algorithms using large datasets, the Norwegian public sector might be inclined to support initiatives that either rely on or develop innovative approaches to machine learning using smaller datasets. Currently, the ability of machine learning from smaller datasets to achieve the necessary predictive accuracy for most tasks in the public sector is limited. However, if the potential for machine learning from small data improves in the future, perhaps approximating but not quite achieving the same level of accuracy as AI systems based on big data, a trade-off might emerge. This trade-off could involve choosing between technology that offers the highest level of accuracy or opting for technology that performs slightly less accurately but has a lower environmental impact.

3.2.3 Transparency and Explainablity

The Norwegian legal framework has various provisions mandating transparency and explainability of public-sector decision-making. The PAA § 25 demands that individual decisions must be justified. The justification should refer to the relevant rules and factual circumstances. As regards criteria that involve the exercise of discretion, the justification must describe the main considerations determining the outcome of the discretionary assessment. Additionally, if the use of AI involves personal data, there are additional requirements for transparency and for providing information to those about whom the data is being used (GDPR Articles 5(1(a), 12–14).

It is widely recognized that the use of 'black-box' AI systems to support or automate administrative decision-making might have a negative impact on the values and rights pertaining to transparency and explainability in the public sector. While the legal framework in Norway does

[1015] Case C-634/21 Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 15 October 2021 – OQ v Land Hesse

[1016] The CJEU has confirmed that generating credit scoring will be covered by Article 22(1) if a third party (e.g a bank) 'draws strongly' on that score to make decisions about whether to grant a loan or not. See Case C-634/21 REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany) ECLI:EU:C:2023:95, para 73.

not specifically address these impacts of AI systems, the general requirement that individual decisions need to be properly explained with reference to the content of discretionary considerations entails a boundary for the use of black-box AI systems in this context. Even if such AI systems are used only as decision support, this might contradict an individual's right to an explanation of the decisive considerations. Consequently, further research is needed to develop explainable AI particularly as regards discretionary criteria that may be involved in public-sector decision-making.

3.2.4 Non-Discrimination, Equality, and Digital Inclusion

The central non-discrimination law in Norway is the 2017 Equality and Non-Discrimination Act. Applicable to all sectors, the Act establishes in § 6 a prohibition against discrimination based on 'gender, pregnancy, leave for birth or adoption, caregiving responsibilities, ethnicity, religion, worldview, disability, sexual orientation, gender identity, gender expression, age, or combinations of these grounds.'

Concern about the impact of digitalisation on equality and non-discrimination is particularly salient in relation to AI technologies. In the international discourse on the use of AI systems in the public sector, the risk of discrimination due to biases in AI systems is a prominent concern, often referred to as 'algorithmic discrimination'.[1017] Concern about algorithmic discrimination is also found in the preparatory works accompanying the provisions concerning fully automated decision-making in the Norwegian public sector. This concern is part of the reason why the current framework only permits fully automated decision-making in cases where there is limited discretion involved or the outcome of the decision is obvious. However, the issue of bias and discrimination in AI systems is not limited to fully automated decision-making. AI systems may display biases that can lead to discrimination also when they are used as decision support. Algorithmic discrimination can be very difficult to detect for decision-makers relying on AI systems and individuals that are potentially victims of discrimination.

There are no specific provisions addressing algorithmic discrimination in current Norwegian law, but Norwegian non-discrimination law is technology-neutral and applicable to decision-making where AI is involved. As regards important concerns related to algorithmic discrimination, there are certain strengths and weaknesses of Norwegian non-discrimination law which are worth highlighting.

One strength is the Equality and Non-discrimination Act's clear prohibition of intersectional discrimination. Intersectional discrimination occurs if a person is discriminated against because of a combination of protected characteristics, for example, if a provision or practice is specifically detrimental to persons of a particular ethnic background who also have a particular sexual orientation.[1018] The importance of addressing intersectional disparities –potentially constituting intersectional discrimination – is highlighted in a study by Buolamwini and Gebru.[1019] The study found that commercially available facial analysis algorithms intended to classify a person's gender performed worse for darker-skinned females than for other combinations of skin-type and gender that were assessed.

[1017] E.g., Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law. / Hacker Philipp. In: *Common Market Law Review*, Vol. 55, No. 4, 2018; Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience. / Xenidis, Raphaële. In: Maastricht Journal of European and Comparative Law, Vol. 27, No. 6, 2020, p. 736–758.

[1018] Prop. 81 L (2016–2017) Lov om likestilling og forbud mot diskriminering (hereinafter 'Prop. 81 L (20116–2017), p. 113.

[1019] Gender shades: Intersectional accuracy disparities in commercial gender classification / Buolamwini, Gen Joy and Gebru, Timnit. In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81, 2018, p. 77–91.

Another clear strength of the Equality and Non-Discrimination Act when it comes to potential algorithmic discrimination in the public sector is the emphasis on proactive measures to prevent discrimination. According to Article 24 of the Act, public authorities are obligated to make "active, targeted and systematic efforts to promote equality and prevent discrimination". This implies that public authorities in Norway are legally obligated to address the issue of algorithmic discrimination before implementing AI technologies. Furthermore, the provision in § 24 specifies that the measures shall be aimed at counteracting stereotyping, which is a widespread concern associated with AI technologies.

In addition to the general provisions pertaining to non-discrimination, the Equality and Non-Discrimination Act stipulates requirements for universal design of ICT systems. Universal design is an important way of providing reasonable accommodation in the access to public services by persons with disabilities. It entails, for example, enlarging text, reading text aloud, captioning audio files and videos, providing good screen contrasts, and creating a clear and logical structure.[1020] These requirements promote digital inclusion, which is underscored both in the Guidance for Responsible AI and the National Strategy for Digitalisation of the Public Sector and the AI Strategy.[1021]

However, there are also issues related to AI bias that Norwegian non-discrimination law is less prepared to tackle. For instance, academic literature on AI bias discusses the possibility that algorithms might discriminate against other groups than those protected by non-discrimination laws, despite being worthy of protection.[1022] Protection of such groups would require an open-ended prohibition of discrimination that does not comprehensively list the protected characteristics.[1023] For example, in Article 14 ECHR the words "such as" are placed before the list of protected characteristics, indicating that the list is not exhaustive. In contrast, the Norwegian Equality and Non-Discrimination Act only prohibits discrimination based on the characteristics that are explicitly listed in Article 6 of the Act. This was a deliberate choice as the legislature assumed that the consequences of prohibiting discrimination based on an open-ended list of protected characteristics would be difficult to foresee.[1024]

Another potential weakness is arguably the wide possibility of justification of potentially discriminatory behaviour under Norwegian non-discrimination law. Justification is generally possible regardless of whether a decision-making process constitutes potential direct or indirect discrimination. In comparison, the EU Equality Directives permit justification of potential direct discrimination only in exceptional circumstances that are specifically described in the relevant directives.

3.2.5 Safety and Security

Various laws, including Articles 5(1(f)) and 32 of the GDPR, impose security requirements when software and/or AI systems process personal data. In addition, a core principle in the National AI strategy is that 'cyber security should be built into the development, operation and administration of systems that use AI'. The National Strategy for Digitalisation of the Public Sector also 'requires that cyber security be integrated into the service development, operation and management of common IT solutions, in accordance with the objectives of the National Cyber Security Strategy for Norway'.[1025]

Despite this, in recent years, several incidents have highlighted vulnerabilities in the cyber and data security of public agencies in Norway. A prominent example is the cyber-attacks on the

[1020] Prop. 81 L (2016–2017), p. 325.
[1021] Digital Strategy for the Public Sector 2019–2025, p. 18.
[1022] E.g., The theory of artificial immutability: Protecting algorithmic groups under anti-discrimination law. / Wachter, Sandra. In: Tulane Law Review, Vol. 97, No. 2, 2022, p. 149–204, p. 149.
[1023] Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence Articles and Essays. / Gerards, Janneke and Zuiderveen Borgesius, Frederik. In: Colorado Technology Law Journal, Vol. 20, No. 1, 2022, p. 1–56.
[1024] Prop. 81 L (2016–2017), p. 97.
[1025] Digital Strategy for the Public Sector 2019–2025, p. 8

Norwegian Parliament (*Stortinget*). In September 2020, the Parliament faced a significant cyberattack, leading to several MPs and staff members' email accounts being compromised and various amounts of data being extracted.[1026] Another breach occurred in March 2021 when attackers exploited flaws in Microsoft software to target the Parliament.[1027]

Local administrative bodies also experienced security breaches. Notably, the Norwegian Data Protection Authority imposed a fine on the Municipality of Østre Toten due to insufficient information security.[1028] In January 2021, the municipality suffered a significant cyberattack. As a result, employees lost access to most IT systems, data was encrypted, and backups were deleted. Subsequent investigations in March 2021 revealed that portions of the compromised data, including highly sensitive details about residents and employees, were leaked on the dark web. Roughly 30,000 documents were affected by this breach. The Data Protection Authority determined that the Municipality of Østre Toten had significant security shortcomings. These included inadequate log analytics, unprotected backups, and an absence of two-factor authentication or similar security measures. Their firewall was minimally configured, leading to insufficient logging of internal traffic. Moreover, backups were left vulnerable to deletion, tampering, or unauthorized access.

The report from the Commission for Data Protection underscores that these failures are affecting the trust in public administration.[1029] Despite a generally high level of public trust in the public sector, the report indicates that citizens have low confidence in authorities' capabilities to secure information and critical infrastructure.

3.3 Emerging Trends and Challenges

Based on the abovementioned examples of legislative efforts to facilitate digitalisation in the Norwegian public sector, certain trends can be identified. One salient trend is the focus on creation of specific provisions providing a legal basis for certain data processing operations. This tendency can be traced back to the fact that there is high awareness of the potential impact of digitalisation on privacy and data protection in the National Digitalisation Strategy and in the legislative work that has been done so far. Particularly, the legislature has been mindful of the need for a legal basis for data sharing/re-use and automated decision-making.

However, Norway does not currently have a holistic approach to the regulation of digitalisation generally or AI technologies, specifically. The examples we have mentioned of laws facilitating digitalisation are piecemeal examples. If one compares the legislative amendments that have been implemented to the principles and values mentioned in section 2.2, which ought to guide digitalisation efforts in Norway, it appears that the parts of the legal framework that have been adjusted to accommodate digitalisation focus more narrowly on data protection-related issues.

The legislative trends we have observed have important limitations when it comes to the question of to what extent they facilitate digitalisation. The legislation pertaining to the Labour and Welfare Administration and Tax Administration has been amended with provisions concerning fully automated decision-making, but these amendments currently only foresee hard-coded software systems. These systems tend to be highly predictable and explainable and, thus, they do not invoke the same concerns in relation to the rights and values mentioned in section 2.2 as more advanced AI systems do. Arguably, the use of AI as decision support raises more profound concerns than full automation based on hard-coded software programs. Yet, regulatory provisions pertaining to AI systems intended for decision support are largely absent in the current and emerging legal framework in Norway.

[1026] Cyberattack on the Storting. / Storting. 03 Sep 2020. https://www.stortinget.no/nn/In-English/About-the-Storting/News-archive/Front-page-news/2019-2020/cyberattack-on-the-storting/
[1027] New cyberattack on the Storting. / Storting. 11 March 2021 https://www.stortinget.no/nn/In-English/About-the-Storting/News-archive/Front-page-news/2020-2021/new-cyberattack-on-the-storting/
[1028] Municipality of Østre Toten fined. / Datatilsynet. 7 June 2022 https://www.datatilsynet.no/en/news/aktuelle-nyheter-2022/municipality-of-ostre-toten-fined/
[1029] NOU 2022: 11, p. 61.

From the perspective of the Norwegian legislature, the existence of legal provisions in public administration law that contain discretionary criteria have been highlighted as a challenge to the automation of public administration. It has been argued that regulations suitable for automated administrative proceedings ought to be machine-readable so that they can be applied by AI-systems.[1030] Moreover, the National AI Strategy highlights semantic differences as a challenge to digitalisation and automation: different sector-specific regulations may use the same concepts in different ways. Income, for example, does not mean the same in the Norwegian Tax Administration as it does in the Norwegian Labour and Welfare Administration (NAV), and the concept of co-habitant is defined in a variety of ways in different regulations. Recognizing such semantic challenges, the Norwegian Government has made semantic interoperability an objective of legislative efforts to facilitate digitalisation. This way, it is expected that legislative provisions can be read more easily by machines and applied by AI systems.[1031]

Another trend discernible across numerous policy documents from Norwegian authorities appears to be the inclination towards viewing digitalisation and technology as instrumental in ensuring citizens' rights. The government's AI strategy emphasizes the role of automation as an important element in its endeavour to uphold and promote citizens' constitutional and fundamental rights.

"Automation can also promote equal treatment, given that everyone who is in the same situation, according to the system criteria, is automatically treated equally. Automation enables consistent implementation of regulations and can prevent unequal practice. Automated administrative proceedings can also enhance implementation of rights and obligations; for example, by automatically making decisions that grant benefits when the conditions are met. This can particularly benefit the most disadvantaged in society. More consistent implementation of obligations can lead to higher levels of compliance and to a perception among citizens that most people contribute their share, which in turn can help build trust."[1032]

Some of the planned projects are also in line with this perspective. For example, one of the planned digitalisation projects, namely the Digitalising the right to access, aims to create platform that gives citizens an overview, insight and increased control over their own personal data. There is a similar tendency to view AI deployment as a way to address stereotypes and errors in human judgement, thereby aiming to ensure equal treatment.[1033]

Some scholars point out that the government's policy overwhelmingly favours AI, with few reservations.[1034] Indeed, there is no doubt that technology can be part of the solution. However, it is important to note that automation and AI do not operate in a vacuum. Many processes and deployments of such automated and AI systems are influenced by human judgment, including in the selection of training data, areas of deployment, and desired outcomes. The Dutch welfare scandal is a stark example of how such systems could lead to an outcome completely opposite to the aspiration of the Norwegian policy, disproportionately impacting the vulnerable groups in the population.

In this case, the so-called 'System Risk Indication' (SyRI) was developed as a government tool to alert the Dutch public administration about the fraud risk of citizens.[1035] The algorithm processes large amounts of users' personal data gathered from government databases that were

[1030] National AI Strategy, p. 21.

[1031] National AI Strategy, p. 21–22.

[1032] National AI Strategy, p. 26.

[1033] Snubler Norge inn i en algoritmisk velferdsdystopi? / Broomfield, Heather and Lintvedt, Mona Naomi in Tidsskrift for velferdsforskning, 25/3 2022, p. 5–6.

[1034] Snubler Norge inn i en algoritmisk velferdsdystopi? / Broomfield, Heather and Lintvedt, Mona Naomi in Tidsskrift for velferdsforskning, 25/3 2022, p. 6.

[1035] High-Risk Citizens. / Braun, Ilja. *Algorithm Watch*, 4 July 2018 https://algorithmwatch.org/en/high-risk-citizens/ . Why the resignation of the Dutch government is a good reminder of how important it is to monitor and regulate algorithms. / Elyounes, Doaa Abu.. Berkman Klein Center Medium Collection, 10 February 2021. https://medium.com/berkman-klein-center/why-the-resignation-of-the-dutch-government-is-a-good-reminder-of-how-important-it-is-to-monitor-2c599c1e0100 previously held in silos, such as employment, personal debt and benefit records, and education and housing histories. The data is analysed to identify which individuals might be at higher risk of committing benefit fraud. Based on certain risk indicators, the software allegedly detects an 'increased risk of irregularities', i.e. whether someone is acting against the law. Reports show that the algorithm was deployed only in the poorest neighbourhoods of the Netherlands where underprivileged and immigrant populations tend to make up a large share of the demographic. This has raised several concerns regarding the rights of individuals. Subsequent investigations show that the SyRI has incorrectly classified more than 26,000 families as committing fraud and thus blocked them from receiving social benefits to which they were entitled. Many of these families were immigrants and had low socio-economic backgrounds. A crucial factor in such disproportionate impact lies in the government's decision to selectively deploy these systems in the poorest neighbourhoods.

Related to the aforementioned trend is the emphasis on rule-based AI systems as a means to alleviate threats to human rights, especially regarding transparency and discrimination concerns. For instance, the national strategy for AI notes that a characteristic shared by *'all current automated case management systems is that they are rule-based.'*[1036] This is deemed crucial in ensuring transparency in decision-making and safeguarding citizens' rights to contest and challenge decisions.[1037] It is true that a rule-based AI system can have several advantages over machine learning approaches, particularly in addressing concerns over transparency and explainability in data use. Firstly, rule-based AI systems function based on explicit rules and algorithms, which are predetermined by developers. This means the reasoning process of the AI is clear and straightforward, enhancing transparency. Secondly, as the logic and decision-making process are pre-defined, these systems are highly explainable. The outcomes can be traced back to a specific set of rules, making it easy to understand why the AI made a particular decision. Thirdly, unlike machine learning, which demands a significant amount of data for training, rule-based systems can be designed with minimal data, adhering to the principle of data minimization. Fourthly, rule-based systems can help reduce bias that might have been present in the training dataset, providing the ability to trace and address sources of bias once identified. Moreover, the Norwegian Data Protection Authority views rule-based systems as a mechanism to mitigate automation bias, where humans uncritically use machine predictions.

However, it is worth noting that rule-based systems might exhibit discrimination arising from biases embedded within the rules themselves. For example, if driving between 3 to 5 PM is associated with a higher risk of drunk driving and consequently linked to higher insurance premiums, such rules could unintentionally discriminate against individuals working lower-wage jobs, like janitors, who may be driving early in the morning due to their work schedules. Likewise, an overly specific rule-based system might perform poorly when introduced to new data, resulting in potential discrimination. Hence, while rule-based AI systems offer benefits in terms of transparency and explainability, they also necessitate careful consideration of potential discrimination risks. Again, the Dutch welfare scandal is an example of how human bias can infiltrate AI systems. The fraud detection system was deliberately deployed only in poorer neighbourhoods. This in turn reinforced the algorithm to associate people with immigrant backgrounds as high risk. A Dutch Court determined that merely deploying the system to target poor neighbourhoods constitutes discrimination based on socioeconomic or immigrant status.[1038]

[1036] National AI Strategy, p. 26.
[1037] National AI Strategy, p. 26.
[1038] Welfare surveillance system violates human rights, Dutch court rules. / Henley, Jon and Booth, Robert. IN: *The Guardian*, 5 February 2020. https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules

4. Impact of Proposed EU AI Act

This section assesses how the proposed EU regulation on artificial intelligence (the AI Act) will supplement national administrative law and to what extent it (sufficiently) will alleviate the challenges we have identified. Specifically, it explores the impact of the AI Act from two perspectives: Firstly, how the Act addresses the challenges concerning human rights protection, and secondly, how it aids in overcoming the barriers to AI adoption by public agencies.

4.1 The Impact of the Proposed AI Act in Strengthening Human Rights Protection

Section 3.1 evaluates the current national legal framework concerning AI adoption by public agencies and the protection of citizens from AI-related harms. Challenges remain in effectively safeguarding citizens' rights in the specific context of digitalisation. This has been highlighted by the Commission for Data Protection, especially in terms of data protection and privacy. However, this overarching weakness in the national framework extends to other areas as well. In this regard, the discussion in section 3.2 has shown the limitations of existing laws in addressing new discrimination harms associated with AI systems.

The AI Act could be pivotal in addressing many of these concerns. The proposed AI Act is geared towards promoting human-centric AI, ensuring its development respects human dignity, upholds fundamental rights, and ensures the security and trustworthiness of AI systems.[1039] Central to the AI Act is the principle that AI should be designed and developed with full regard for human dignity and fundamental rights, such as privacy, data protection, and non-discrimination. Furthermore, the AI Act emphasizes the creation of AI that is safe, secure, and robust. AI designs should mitigate risks of errors or biases and remain transparent and interpretable for users. Additionally, the Act mandates rigorous testing and evaluation of AI systems to confirm their reliability and safety.

The proposed AI Act adopts a risk-based approach, categorizing AI systems into four risk levels: (1) 'unacceptable risks' (that lead to prohibited practices), (2) 'high risks' (which trigger a set of stringent obligations, including conducting a conformity assessment), (3) 'limited risks' (with associated transparency obligations), and (4) 'minimal risks' (where stakeholders are encouraged to follow codes of conduct).[1040] This classification depends on the potential risk posed to health, safety, and fundamental rights.

Most of the prohibited practices concerning AI usage are directed at public agencies. This encompasses the use of real-time biometric identification and social scoring. Similarly, most of the stand-alone high-risk AI applications focus on public agencies' use of AI in the following areas: access to and enjoyment of essential services and benefits, law enforcement, migration, asylum, and border management, administration of justice and democratic processes. Clearly, the public administration sector is under scrutiny, and many of these provisions aim to enhance the protection of individuals from harms within this domain.

Examining the prohibited practices, the AI Act addresses two primary categories of AI systems used by public agencies. First is the use of real-time biometric identification by public agencies for law enforcement purposes. While biometric identification includes fingerprints, DNA, and facial features, the prohibition notably emphasizes facial recognition technology. A system that would

[1039] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM(2021) 206 Final (hereinafter Proposed AI Act)

[1040] Explanatory Memorandum to the Commission's AI Act Proposal, p. 12.

fall under this prohibition might be an expansive CCTV network on public streets integrated with facial recognition software. The deployment of such systems has significant ramifications for individual rights, including data protection, privacy, freedom of expression, and protection against discrimination. Facial recognition technology possesses the capability to process and analyse multiple data streams in real time, enabling large-scale surveillance of individuals, subsequently compromising their rights to privacy and data protection. The pervasive nature of this surveillance can also influence other foundational rights, such as freedom of expression and non-discrimination. The omnipresence of surveillance tools may inhibit individuals from voicing their opinions freely. People tend to self-censor and alter their behaviour when they feel overly surveilled. Similarly, in most cases, the negative impact of AI-driven surveillance is felt acutely by the marginalized groups in the population. Thus, strengthening existing safeguards against potential harms from facial recognition technology is vital.

Another prohibited practice pertinent to public administration is social scoring. The AI Act prohibits public authorities from employing AI systems to generate 'trustworthiness' scores, which could potentially lead to unjust or disproportionate treatment of individuals or groups. This prohibition seems inspired by the Chinese Social Credit System, where the government assigns scores to citizens and businesses based on various factors, including financial creditworthiness, compliance with laws and regulations, and social behaviours.[1041] These scores can then be employed to either reward or sanction individuals or entities. China's Social Credit System has sparked widespread concerns about human rights violations. To derive these social credit scores, the system gathers comprehensive data on its citizens. This broad data collection infringes on an individual's right to privacy. Moreover, the system might penalize individuals for online expressions or content shared, thereby potentially stifling freedom of speech. There is also concern that this system exacerbates social inequality. Those with lower scores might struggle with tasks like securing jobs or renting properties, and they could even be subject to public humiliation. Thus, these safeguards against the use of real-time biometric identification and social scoring undoubtedly complement national laws protecting user privacy and non-discrimination, including those in Norway.

Indeed, Norwegian law already outlines certain restrictions on AI use by public agencies, even before the introduction of the AI Act. There are existing laws that prevent public agencies from making specific decisions using AI. A prime example is the limited scope of the NAV Act, Article 4 a. While this provision is meant to facilitate automated decision-making, it does not facilitate the use of AI technologies. It prevents NAV from using fully automated decision-making except for cases where the applicable criteria are absent of discretion and the outcome of the decision is obvious. This is grounded in the belief that methods capable of automating decisions relying on more discretionary criteria (i.e, in practice, advanced AI systems) present 'a greater risk of unjust and unintended discrimination.'[1042]

In contrast, while the AI Act categorizes AI systems intended for these purposes as high-risk systems, it permits the placement of such systems on the market. Hence, a certain tension arises between the legal framework in Norway and the AI Act's ambition for harmonization. While Norwegian law does not permit certain uses of AI in the public sector due to concerns about the risks of discrimination (among other concerns), the AI Act assumes that these risks are sufficiently addressed if the requirements pertaining to high-risk AI systems are complied with. There may be good reasons for limiting the use of AI systems through national legislation, but it is worth questioning whether such limitations remain justified when they rely on risks that are

[1041] China's 'social credit' system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy. / Canales, Katie and Mok, Aaron. IN: *Business Insider*, 28 Nov 2022.

[1042] Prop. 135 L (2019–2020), Chapter 5.3.1.

addressed by the AI Act. Going forward, we would advise Norwegian legislators to consider this aspect of the relationship between the AI Act and national legislation.

Many AI systems pertinent to the public administration sector fall under the AI Act's high-risk category. For example, this includes public agencies' use of AI in distributing benefits, making decisions in immigration and border control, law enforcement, and infrastructure management. In this context, the requirements for conducting risk assessments, ensuring human oversight, maintaining data quality, and adhering to cybersecurity standards will bolster protection against potential harms. These obligations are especially significant for countries like Norway, which boasts a vast public administration sector and a comprehensive social safety net. Given this context, AI could play a pivotal role in the government's initiatives to modernize and optimize the welfare system. The discussions in section 1, detailing implemented and planned projects, underscore the use of AI in automating decisions related to citizenship applications, NAV's ongoing project to leverage AI in predicting the duration of sick leaves, and Lånekassen's use of AI in student loan applications. Similarly, many of the ongoing AI projects in the health sector would also qualify as high-risk AI systems. In this context, the above-mentioned requirements for high-risk AI systems are crucial in strengthening the protection of human rights. For instance, requirements assessing the relevance and representativeness of data can mitigate potential biases embedded in datasets. Requirements on human oversight and involvement can help public agencies detect and rectify potential biases. While reflecting overarching rights and values that are protected by general provisions in Norwegian law, these legal requirements address AI technologies and associated risks at a level of specificity that is currently not found in the Norwegian framework.

The Dutch welfare scandal serves as a stark example of public agencies deploying AI systems without essential safeguards. This system was notoriously opaque. When the non-profit organization *'Bij Voorbaat Verdacht'* requested insights into the software's evaluation criteria for welfare abuse, the government countered that disclosing such information might aid potential wrongdoers. The absence of human oversight was glaringly evident, as even minor omissions in filling a form led to high-risk classifications. The provisions of the AI Act on risk assessment, transparency, and human oversight could likely have averted or lessened the repercussions of this scandal.

In Norway, a report by the Data Protection Authority highlighted that the Norwegian Tax Authority has developed a predictive tool to aid in the selection of tax returns for potential discrepancies or tax evasion.[1043] This tool is crafted through a comprehensive analysis of data, encompassing details like current and previous year deductions, age, financial specifics such as income and assets, and individual tax return elements. Intriguingly, the Tax Authority admitted that they 'don't necessarily know what it is that gives a taxpayer a high ranking for risk. The ranking is the result of complex data aggregation in the model.'[1044] The AI Act, particularly the requirements concerning transparency and human oversight, are expected to influence the deployment of such systems.

The obligations for high-risk AI systems introduced by the AI Act also complement and address some of the gaps present in the GDPR. One significant area where the AI Act provides additional clarity is concerning decisions that, while not entirely automated, could have substantial impacts, such as credit scoring. As highlighted earlier, the study commissioned by the Commission for Data Protection underscores that process-driven decisions, like selections for inspections, can be so intrusive that they might equate to a 'decision' in their impact on an individual.[1045] However, the

[1043] Artificial intelligence and privacy. / Datatilsynet. 2018, p. 12
[1044] Artificial intelligence and privacy. / Datatilsynet. 2018, p. 12
[1045] Kravet til klar lovhjemmel for forvaltningens innhenting av kontrollopplysninger og bruk av profilering. / Lintvedt, Mona Naomi. Utredning for Personvernkommisjonen. 2022.

protections stipulated by the GDPR, especially Article 22(3), do not necessarily cover such uses of AI or profiling for inspection and fraud monitoring. The current Norwegian legislative framework is also oriented towards automated decision-making while paying less attention to AI-supported decision-making. In contrast, the AI Act appears to offer a broader scope of protection and safeguards for AI systems employed in the distribution of public benefits. This arguably encompasses the use of AI in areas like fraud detection and monitoring.[1046]

Despite this, many civil society organizations, including Amnesty and Human Rights Watch (HRW), have criticized the inadequate human rights safeguards, especially considering governments' increasing use of AI to deny or limit access to lifesaving benefits and other social services. This exacerbates existing concerns over inequality and the digital divide. For instance, HRW conducted a detailed study on the AI Act's impact on the distribution of social security and highlighted the following:

'While the EU regulation broadly acknowledges these risks, it does not meaningfully protect people's rights to social security and an adequate standard of living. In particular, its narrow safeguards neglect how existing inequities and failures to adequately protect rights – such as the digital divide, social security cuts, and discrimination in the labour market – shape the design of automated systems and become embedded by them.'[1047]

This is partly related to the narrow focus of the prohibitions and high-risk AI systems. Consider, for instance, the mounting evidence over recent years about the potential dangers of biometric identification. The prohibition in this domain appears so narrowly defined that its relevance is debatable. Firstly, it targets only 'real-time' systems that can capture, compare, and identify individuals 'instantaneously, near-instantaneously, or without a significant delay.' This leaves out 'post' systems which may analyse biometric data after an event, such as retrospectively identifying individuals present at protests. Notably, the prohibition is restricted to biometric identification used by public authorities for law enforcement. This means it does not cover the use of remote biometric identification for non-law enforcement purposes, like authentication for social welfare. This limitation is particularly concerning given the rising use of facial recognition technology by public agencies to provide public benefits.

HRW has documented how various governments use of facial recognition to verify the identities of those applying for welfare benefits. A case in point is the national welfare office in Ireland, the Department of Employment Affairs and Social Protection (DEASP).[1048] The Irish Council for Civil Liberties questioned the DEASP's extensive personal data collection for identity verification, challenging the necessity of analyzing facial images when simpler methods, such as passport and address verification, could suffice.[1049] Furthermore, substantial research underscores the racial and gender biases inherent in facial recognition technology. For example, a 2018 study from MIT revealed that commercial facial recognition systems from leading tech giants like IBM and Microsoft demonstrated significantly higher accuracy when identifying white males compared to women or individuals with darker skin tones.[1050] Such inaccuracies in the technology, when used by law enforcement, have led to a number of wrongful arrests, predominantly of people of colour.[1051] Similarly, the use of such systems in verifying for social security purposes heightens the risk

[1046] Proposed AI Act, Annex III (5(a)).

[1047] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p. 3.

[1048] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p. 7.

[1049] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021.

[1050] Gender shades: Intersectional accuracy disparities in commercial gender classification / Buolamwini, Gen Joy and Gebru, Timnit. IN *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81:77-91, 2018

[1051] Kashmir Hill, 'Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match' (*The New York Times*, 6 Jan 2021) of discrimination. However, because of the narrow scope of the prohibition in the AI Act, the use of facial recognition technology in social welfare settings is not addressed or restricted.[1052]

Similarly, the prohibition on 'trustworthiness' scoring seems to target 'general purpose' scoring systems where public authorities generate a single score that can be applied across various contexts, such as deciding whether individuals can board a plane, obtain a loan, or secure certain jobs. However, this focus on 'general purpose' scoring systems overlooks the potential harms arising from the growing reliance on scoring systems in welfare fraud detection, such as the Dutch SyRI. As noted above, the Norwegian Tax Authority uses AI to detect tax evasions. Even though such systems are specifically designed for detecting fraud and might not fall under the prohibition, they can still lead to severe human rights implications. For instance, these systems may erroneously flag individuals as fraud risks or deprive them of the necessary support.[1053] Consequently, there are calls for broader protection in this domain.[1054]

Indeed, the use of facial recognition technology, as well as the application of AI for distributing public benefits, falls under the high-risk category. This implies that both fraud detection systems, like the Dutch SyRI, and facial recognition technology used for verifying identity in welfare would need to adhere to certain obligations. Yet, concerns persist regarding the adequacy of these safeguards in protecting individuals against the harms from high-risk systems in the context of social welfare.

A primary concern is that the bulk of the AI Act's obligations for high-risk systems are placed on the 'providers' of welfare technology rather than the agencies that use them.[1055] Thus, while obligations like risk assessment, transparency, and human oversight apply when public agencies develop AI systems in-house, the responsibility shifts to the provider when agencies procure such tools off the shelf. This skewed distribution of regulatory responsibility means that harm caused by off-the-shelf technologies might not be as rigorously regulated, even when their impacts can be as profound as those caused by in-house software.[1056] This indicates that regulation of AI users could be an important area where national legislation and, potentially, regional legislative cooperation could supplement the AI Act. Particularly, public procurement regulation emerges as a crucial venue for ensuring the protection of rights and values when AI is purchased by the public sector.

Relatedly, the obligations for high-risk applications overlook systemic issues. While the requirement for establishing a data governance framework, which mandates the data used to train AI systems to be relevant and representative, might help mitigate discrimination arising from biased data, it does not tackle the systemic concerns ingrained in both the systems and their human overseers. The Dutch welfare scandal is a poignant illustration: the deployment of the system predominantly targeting impoverished neighbourhoods is discriminatory by design. Similarly, the extensive exemptions from transparency requirements for law enforcement and migration control authorities could obstruct accountability for AI systems, posing significant threats to individual rights.[1057] For instance, providers are expected to disclose 'electronic instructions for use' that elucidate the underlying logic of how a system functions, and limitations in the performance of the system, including known or foreseeable risks to discrimination and

[1052] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p. 7.

[1053] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p. 17.

[1054] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p. 21.

[1055] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p. 18.

[1056] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p.18

[1057] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p. 20.

fundamental rights.[1058] However, the Act stipulates that this information 'shall not be provided in the areas of law enforcement and migration, asylum, and border control management.'[1059] Consequently, there is a risk that vital information about a wide array of law enforcement technologies, which might affect human rights – including criminal risk assessment tools and 'crime analytics' software analyzing vast datasets to identify suspicious behaviour patterns – will remain concealed.[1060]

To address these concerns, there are recommendations to mandate human rights impact assessments throughout the entire lifecycle of high-risk systems when public agencies deploy AI in distributing public benefits.[1061] This encompasses scenarios where public agencies purchase high-risk AI systems from third parties or make significant modifications to the operations of such acquired systems that heighten or introduce human rights risks.[1062] Furthermore, many civil society organizations have underscored the importance of empowering individuals and public interest groups to lodge complaints and pursue remedies for damages caused by these systems. The identified gaps highlight opportunities for national, Nordic, and Baltic region initiatives to supplement the AI Act's measures in enhancing fundamental rights.

4.2 The Impact of the Proposed AI Act in Enabling Public Agencies' Use of AI

In addition to the measures that strengthen human rights, the AI Act contains provisions that facilitate the use of AI by public agencies. Notable examples include provisions that permit the processing of sensitive personal data to scrutinize AI systems for potential discrimination and the introduction of regulatory sandboxes. While the provision on using sensitive data for testing seems a measure to strengthen human rights protection, it can also be seen as an enabler of digitalisation efforts. This is because it establishes a legal basis for the use and reuse of data for testing, which is currently a significant hurdle for public agencies implementing AI.

As highlighted in section 3, the National AI Strategy recognizes the significant constraints posed by regulatory restrictions on repurposing existing data for AI development, including testing. This is evidenced by the NAV sandbox example. In this instance, the Data Protection Authority determined that NAV required a specific legal basis to utilize data for AI training. Similar reservations have been voiced regarding AI systems assisting in email archiving. Although the agency conceded that public agencies might invoke Article 6(1)(c) in conjunction with specific provisions under the Archive Act, the Regulations Relating to Public Archives, and the Freedom of Information Act, such provisions do not explicitly provide a legal basis for an algorithm's continuous learning. In both cases, the agency advocated for the anonymization of personal data prior to its use in training or refining algorithms.

Additionally, the NAV AI sandbox illustrates some of the tensions between data protection and fairness where detecting and counteracting discrimination requires more processing of personal, often sensitive, information about individuals. Indeed, the AI Act does resolve some of the problems. Article 10(5)) creates an exception to the prohibition of processing such type of data to the ones listed in GDPR Article 9(2). However, the exception only applies to high-risk AI systems and allows the processing of special categories of personal data to the extent that this is strictly necessary for the purposes of ensuring bias monitoring, detection and correction. Importantly,

[1058] Proposed AI Act, Article 13, and Recital 47.

[1059] Proposed AI Act, Annex VIII(11), Articles 51 and 60.

[1060] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p. 20.

[1061] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p.19.

[1062] Q&A: How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net. / Human Rights Watch. 2021, p. 26.

this provision does not allow the use of data for training purposes, which is the first hurdle in public agencies' adoption of AI. Thus, whether a more widely applicable legal basis for training, bias monitoring and the avoidance of discrimination is needed, is a question that legislators should assess at the national level.

The AI Act introduces regulatory sandboxes as a key enabling measure. Regulatory sandboxes permit public agencies to design AI projects and test their deployment with real users in a live setting, all while under regulatory oversight. This arrangement ensures that potential risks are effectively managed and promotes compliance with relevant regulatory requirements. Furthermore, regulatory sandboxes foster a feedback loop between the regulator and the regulated entity. This dynamic allows regulators to stay informed about the latest technological innovations and applications, while technology developers and users receive early guidance on potential regulatory issues.

Despite this, the introduction of regulatory sandboxes does not represent significant changes within the Norwegian landscape. As highlighted in section 2, the Government has established the 'Sandbox for Responsible AI' under the auspices of the Norwegian Data Protection Authority. While this was set to run for two years, in the 2023 state budget, the Government proposed making the DPA's regulatory sandbox a permanent fixture.[1063] Additionally, the Government has recommended broadening the sandbox's scope beyond just AI technologies. While it will continue to target new technology, it will now encompass the more expansive theme of 'privacy-friendly innovation and digitalisation.'[1064] However, this initiative is currently at a policy level. Therefore, the introduction of regulatory sandboxes by the AI Act would solidify these initiatives into law.

To date, the Sandbox has collaborated with over ten projects, several of which involve the use of AI by public agencies. Notable examples include collaborations with NAV and the Bergen Hospital. These projects have been crucial not just in aiding public agencies in meeting their regulatory obligations, but also in equipping the data protection authorities with insights into various challenges. Furthermore, upon the completion of the sandbox projects, reports detailing encountered challenges and proposed solutions are published, offering insights to non-participating businesses and public agencies. The Data Protection Authority has already amassed a significant amount of experience working with regulatory sandboxes focused on AI. It would be a significant oversight if the authority under the AI Act to administer sandboxes is not conferred upon it.

5. Assessment of National Legislative Reforms

The discussions above, especially section 3.1., delve into the multifaceted ongoing initiatives to adjust Norwegian administrative law, making it more digitalisation friendly. These discussions spotlight the primary motivations behind such initiatives. They aim to enhance the public sector efficiency by reducing duplicated efforts and promoting better coordination and data sharing. The goal is to position the user at the forefront by developing innovative and more streamlined services centred around significant life events. The 'only-once' principle embodies these advantages, aiming to facilitate the delivery of streamlined, proactive services while also advancing data-driven innovation and a user-centric experience. Furthermore, many digitalisation efforts are recognized for championing individuals' fundamental rights. As depicted in sections 3.1. and 3.3., many automation efforts are perceived as ways to enhance equal treatment in

[1063] Regulatory Privacy Sandbox. / Datatilsynet https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/

[1064] Regulatory Privacy Sandbox. / Datatilsynet https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/

decision-making processes. Additionally, certain digitalisation initiatives explicitly aid users in exercising their rights under Norwegian law. A prime example is the project focused on the digitalisation of individuals' rights of access to their data held by public administration. This project aspires to build a platform providing citizens with a comprehensive view, deeper insight, and enhanced control over their personal data.

Despite these advantages, there are concerns associated with the ongoing reforms. Firstly, as highlighted in sections 2 and 3, many of these initiatives adopt a sector-specific and piecemeal approach. This leads to concerns about potential fragmentation, both in terms of effective service delivery and governance mechanisms. For instance, section 3.1 discussed challenges stemming from a lack of harmonization in semantic issues. While the Government acknowledges these challenges, the piecemeal strategy and sector-specific adjustments might exacerbate such problems. Importantly, this scattered and sector-specific approach poses challenges in adequately safeguarding citizens' rights. As mentioned in section 3.2, the Commission for Data Protection (*Personvernkommisjonen*) observed that no single public agency holds overarching responsibility for assessing the cumulative use of personal data in public services. Furthermore, there is not a comprehensive framework for evaluating the impact of legislative changes on user privacy. The multiple amendments to sector-specific laws allowing the processing of personal data, along with the utilization of automated decisions, will only intensify these concerns. Similarly, while the ambition to provide seamless services across public agencies is commendable, it poses challenges regarding user rights unless such initiatives are complemented by a clear delineation of the roles and responsibilities of various agencies with respect to users' rights.

In this regard, we defer to the Commission for Data Protection's suggestion to establish a dedicated entity within public administration, similar to Denmark's Data Ethics Council.[1065] This entity would work across various sectors, comprehensively addressing privacy and other related issues. In Denmark, the Data Ethics Council offers advice and insights to the government, the Folketing (Parliament), and other public authorities concerning data ethical matters linked to the utilization of data and new technology. A corresponding agency in Norway could concentrate its efforts on coordinating and ensuring a greater level of alignment in the development of regulations across the public sector. This includes ensuring that the impacts of legislative changes on individuals' fundamental rights are assessed and establishing a clear and user-friendly guide for evaluating privacy consequences in legislative and regulatory work. Additionally, there is a need for the agency to actively ensure the harmonization of term definitions across different regulations. Moreover, this agency can spearhead coordination in more complex collaborative projects, making sure responsibilities are more distinctly defined by law or regulations.[1066]

Furthermore, as highlighted in section 3, a significant portion of the regulatory modifications aims to enable automated decisions via hard-coded software. This approach often overlooks the nuances of AI systems based on machine learning designed for decision support. Similarly, a majority of the amendments, as well as proposed changes that ease data sharing and reuse, predominantly focus on inter-agency data sharing within the public sector, rather than emphasizing the reuse of data to train AI models. Insights from the Regulatory Sandbox on responsible AI highlight that public agencies require a specific legal basis to utilize data for training AI systems. There have been instances where the absence of such a legal foundation for AI training has resulted in the termination of projects within the public sector. Notably, NAV had to pause its project that aimed to predict the duration of sickness absences due to the lack of a legal foundation for training the AI. Therefore, legislative initiatives should broaden the scope to

[1065] NOU 2021: 11, p. 73.
[1066] NOU 2021: 11, p. 78.

accommodate AI systems meant for decision support and establish a clear legal basis for data utilization during AI training, as the Norwegian legislature has provided for when it comes to data from electronic health records, as noted in section 2.1.

In this context, the 1993 Pilot Scheme Act (*forsøksloven*), which permits public agencies to experiment with novel organizational structures and, diverge from existing laws and regulations, serves as an excellent starting point. This perspective is reinforced by a recent evaluation of the Act, which called for its revision considering emerging technologies.[1067] Furthermore, the National AI Strategy identifies the need to assess whether the Pilot Scheme Act sufficiently facilitates the testing of cutting-edge AI solutions. Any governmental guidance or revision of the Act should actively encourage public agencies to explore innovations, particularly within AI. As highlighted by the Norwegian Data Protection Authority, if the Act is intended to provide a legal basis for AI-related experiments, it must be expressly defined as such. Moreover, given the constraints on experimentation when it impacts confidentiality obligations and individuals' rights, the Authority suggests that any amendments should clearly define a legal basis for the processing of personal data, with explicit references to the GDPR.[1068] We concur with the Agency's recommendations.

National efforts can be further strengthened through cross-border collaborations across the Nordic-Baltic region. Harmonization efforts, especially in semantics, are crucial to facilitate the cross-border use of services across both the Nordic and Baltic areas. Moreover, one might consider the development of a shared database or platform for showcasing successfully implemented digitalisation projects. In this context, the annual award given by DigDir in Norway, which recognizes outstanding digitalisation initiatives, presents an exemplary model of how countries can learn from one another. A similar scheme could be considered to recognize and award projects of significance to the Nordic-Baltic region. In the field of AI, a database that compiles AI use cases from public agencies, akin to the one recently launched by NORA and DigDir, could serve as an excellent foundation for ensuring transparency. These measures should also be complemented with an effort at safeguarding the rights of affected citizens, particularly by enabling developers and users of AI systems to implement preventive measures.

The AI Act encourages AI providers to consider the risks associated with potential biases in AI systems. We recognise that this is a challenging task during the early years of AI adoption. Risk assessment requires an understanding of potential pitfalls – the 'known unknowns'. However, there will always be 'unknown unknowns', sources of risk that remain unaddressed in risk assessments. We suggest that a regional cooperation between the Nordic and Baltic countries could establish a database for registration of instances where AI developers and users experience unexpected errors or biases. For example, as regards the risk of algorithmic discrimination, there is an imminent need to collect information about existing patterns of inequality or biases which may become ingrained in AI systems. A regional database could contain information about such patterns discovered during research or AI development, so that AI developers and users can assess the importance of these findings in relation to the specific AI applications they are working on.[1069]

Another area for collaboration might be in relation to the regulatory sandboxes under the AI Act. Article 53(5) states that '*Member States' competent authorities that have established AI regulatory sandboxes shall coordinate their activities and cooperate within the framework of the European Artificial Intelligence Board. They shall submit annual reports to the Board and the*

[1067] Oxford Research, 'Evaluering og utredning av forsøksloven' (2021).

[1068] Oxford Research, 'Evaluering og utredning av forsøksloven' (2021), p. 40.

[1069] Bias and Discrimination in Clinical Decision Support Systems Based on Artificial Intelligence. / Mathias K. Hauglid, PhD thesis submitted at UiT the Arctic University of Norway, Faculty of Law, 18 November 2023, 382.

Commission on the results from the implementation of those scheme, including good practices, lessons learnt and recommendations on their setup and, where relevant, on the application of this Regulation and other Union legislation supervised within the sandbox.’ The Norwegian Data Protection Authority has already accumulated a fair amount of experience working on sandboxes for responsible AI. This scenario not only enables Norway to offer insights but also fosters a symbiotic environment where countries in the Nordic and the Baltic region can mutually benefit from shared experiences and expertise.

The recommendation to establish shared databases and share best practices is consistent with recent studies on the Nordics. In 2022, the Nordic Innovation sponsored a study that maps the current AI ecosystem in the Nordics, emphasizing public sector and national initiatives and programs in the area.[1070] One key recommendation from the study encourages the Nordic countries to *‘increase the sharing and utilization of national datasets,’* including those related to healthcare, taxes, and employment. The goal is to enhance cross-border public service usage and to foster innovation in the private sector. Another suggestion promotes the sharing of best practices, use-cases, and knowledge regarding policy initiatives and strengths they possess. The proposals to establish shared databases on AI projects in the public sector, highlight successfully implemented digitalisation projects, and provide databases on common vulnerabilities, as well as platforms for sharing experiences on AI sandboxes, should form part of cross-border collaboration within the Nordics and the Baltic region as well. Finally, public procurement policy could be an important topic of regional collaboration in the Nordics and Baltics, particularly considering that countries in these regions are often at similar levels of public sector digitalisation.

6. Conclusion

This section delves into Norway's public digitalisation endeavours, evaluating various legislative and policy measures for their effectiveness in advancing the digitalisation of the public sector. Additionally, we consider whether these initiatives are underpinned by robust safeguards for fundamental rights. Norway is distinguished as one of the nations with a profoundly digitalised public sector, with a dedicated Directorate for Digitalisation. The country’s prominence in digitalisation can be attributed to strategic legislative and policy shifts tailored to foster a digital-friendly environment. We pinpoint three primary focal areas within these legislative and policy endeavours.

1

First, Norway has introduced numerous amendments to sector-specific laws enabling different public agencies to utilize profiling and automated decision-making. These initiatives, while motivated by efficiency goals, are also perceived as mechanisms to enhance equal treatment in decision-making processes.

[1070] Nordic Innovation, ‘The Nordic AI and Data Ecosystem’ 2022

2. Second, existing regulations around data utilization and reuse are often cited as hindrances to digital transformation and, in particular, AI development. In response, amendments to the PAA have been rolled out to facilitate data sharing between public entities. There is a wide emphasis on policies championing the 'only once' principle, asserting that citizens should provide their data to the public sector just a single time. Importantly, sector-specific legislative measures have been introduced to enhance data sharing and reuse capabilities. A standout in this context is the 2021 modification to the Health Personnel Act, allowing for the potential use of health data in the development and deployment of clinical decision support systems.

3. Third, the Norwegian government has been a strong advocate for regulatory sandboxes to foster innovation and enhance both corporate and regulatory agencies' understanding of regulatory requirements and their application to innovative technologies. Prime examples include the Sandbox for Responsible AI and Fintech, supervised by the Data Protection Authority and Financial Authority, respectively

Despite the progress, Norway still faces significant hurdles in its digitalisation journey. Firstly, a significant portion of the regulatory amendments aims to enable automated decisions via hard-coded software, neglecting the importance AI systems based on machine learning designed for decision support. Secondly, certain legal provisions within public administration law that encompass discretionary criteria pose challenges to automating public administrative tasks. This discretion, often integral to human decision-making, is hard to encapsulate within automated systems. Thirdly, semantic discrepancies across different sector-specific regulations continue to be a stumbling block for digitalisation, automation and streamlined service delivery.

Moreover, the legal structure overseeing the Norwegian public sector lacks a comprehensive approach towards digitalisation and AI technologies. Few laws directly tackle the challenges digitalisation presents to core democratic values, fundamental rights, and rule of law. This primarily stems from a sector-specific and fragmented approach to facilitating digitalisation. This not only hampers the efficiency of public services and amplifies concerns about semantic discrepancies across various sectors but also clouds the understanding of the real impact these legislative measures have on individual rights.

The AI Act redresses some of the existing gaps in national laws related to human rights protection and further facilitates AI adoption within public agencies. Promising to enhance the protection of individuals against potential AI-driven harms, it provides legal requirements not currently found in the Norwegian framework, which specifically address AI technologies and associated risks. Nevertheless, in certain cases, Norwegian law imposes more stringent restrictions than the AI Act, especially in contexts where it limits the use of advanced AI systems for decision-making that involves discretionary authority, such as in the determination of welfare benefits. This raises the question of whether the AI Act can potentially legitimize automated decision-making processes that would not have been lawful based on the current legal framework in Norway.

Beyond its human rights fortification, the AI Act also includes provisions that streamline AI's incorporation within public institutions. A few key examples are rules allowing the use of sensitive personal data to evaluate AI systems for potential bias and the establishment of regulatory sandboxes. While the provision to assess AI systems using sensitive data to detect possible discrimination is a commendable inclusion, the introduction of regulatory sandboxes does not usher in a notable shift in the existing Norwegian framework.

Finally, we put forth recommendations to boost digitalisation efforts while concurrently safeguarding human rights. Legislative actions should pave the way for the integration of AI systems, especially those intended for decision support and establishment legal basis for reusing data to training AI. In terms of strengthening human rights safeguards, we support proposals for the creation of a dedicated entity within the public administration. Drawing inspiration from Denmark's Data Ethics Council, this entity would lead efforts to achieve semantic and regulatory consistency across various sector-specific initiatives. Crucially, the agency should ensure that any legislative changes' ramifications on individuals' fundamental rights are thoroughly evaluated.

National efforts can be further strengthened through cross-border collaborations across the Nordic-Baltic regions. A focus on harmonization, particularly in terminology and semantics, is pivotal to enabling seamless cross-border service utilization across both the Nordic and Baltic landscapes. Promoting data-sharing, exchanging best practices, highlighting success stories in digitalisation projects, and creating sector-specific databases to register recurring patterns in datasets (which might induce biases against protected groups) can be instrumental. Another promising avenue for collaboration centres around the regulatory sandboxes stipulated by the AI Act. The Norwegian Data Protection Authority, with its considerable experience in sandboxes tailored for responsible AI, stands as a beacon for other nations in the Nordic and Baltic regions.