Public Digitalisation in a legal perspective

Status, challenges and opportunities for Nordic-Baltic cooperation

Nordic Council of Ministers

Contents

This publication is also available online in a web-accessible version at:
https://pub.norden.org/temanord2024-503

AUTHORS

Professor Hanne Marie Motzfeldt
is a professor in Administrative Law and Digitalisation at the Faculty of Law, University of Copenhagen. Her research is strongly funded in administrative law and EU-law as she for the last decade s have focused on public authorities' use of new technologies in relation to administrative law, data protection, information security and protection of vulnerable groups of citizens' digital rights (such as language requirements and accessibility for citizens with disabilities)

Adam Hyldkrog Lindberg
is a graduate student at the Faculty of Law, University of Copenhagen. He has been employed as a research assistant on the DigiLaw project. In connection with his studies, he has specialised in EU data protection regulation and legislation regarding information security

Paloma Krõõt Tupay
teaches constitutional law at the University of Tartu in Estonia. In addition to fundamental rights and governance issues, her research and publications focus on data protection, e-governance and digital constitutionalism. She has previously worked as a legal advisor to the President of the Republic and the Minister of the Interior, among others.

Monika Mikiver
teaches administrative law at the University of Tartu. From 2022 to 2023, she participated as an expert in the work of the Council of Europe's Committee for European Judicial Cooperation (CDCJ) Working Group on Administrative Law and Artificial Intelligence (CDCJ-ADMIN-AI). Monika Mikiver has also worked as an advisor in the Public Law Department of the Ministry of Justice, as an advisor in the Chancellor of Justice's Office, and as a lecturer and Head of the Public Law Department at the Academy of Internal Affairs.

Sofia Heikkonen
is a doctoral researcher in the University of Helsinki's Legal Tech Lab, and she acquired her legal education from the United Kingdom and from Finland. Her main research interests lie in structural changes in the functioning of the state as a result of digitalisation. She has published work on the digitalisation of public administration and liability questions arising from AI.

Contact information: sofia.k.heikkonen@helsinki.fi

Prof. Dr Ida Koivisto
is associate professor of public law in the Faculty of Law at the University of Helsinki. Prior to her current position, she worked as a professor of public law at the University of Tampere, Max Weber Fellow at the European University Institute (Florence) and Global Hauser Fellow at New York University. She is a frequently consulted expert at the Constitutional Law Committee of the Parliament of Finland. Her research interests include digitalisation of public administration, the ideal of transparency, good governance, and the roles of humans in technology regulation.

Contact information: ida.koivisto@helsinki.fi

Prof. Dr Riikka Koulu
is the Associate Professor (Social and Legal Implications of AI) in the Faculties of Social Sciences and Law at the University of Helsinki, Finland. Since 2016, she has also been leading the University of Helsinki Legal Tech Lab, an interdisciplinary research hub that examines the intersections of law, technology, and society. She holds several positions inside and outside of academia, e.g., as the chairperson of the Finnish Data Protection Ombudsman's Expert Board and is an associate researcher at the Alexander von Humboldt Institute for Internet and Society HIIG (Berlin). Her current research interests include automation of legal practices, AI ethics, policy and regulation, and procedural perspectives to technological design.

Contact information: riikka.koulu@helsinki.fi

Anastasija Kaplane, LL.M
is a Lecturer in International Law and Human Rights at the Riga Graduate School of Law. She is also an Associate Researcher at the Baltic Human Rights Society. Her main research interests are state responsibility in cyberspace and the impact of digitalisation on human rights. She is currently pursuing a PhD at the University of Helsinki.

Contact information: anastasija.kaplane@rgsl.edu.lv

Aleksandrs Potaičuks, PhD
is an Assistant Professor (Docent) at the Riga Graduate School of Law and the Business Management College, specialising in Administrative Law and EU Law. He holds a PhD in law from the University of Latvia. Previously, he worked as Assistant to Judge and Judicial Counsellor at the Supreme Court of Latvia as well as a Judicial Counsellor at the Constitutional Court of Latvia where he specialised both in EU Law and Administrative Law. Experience has been supplemented abroad by internships at the University of Eastern Finland, Lund University, the Supreme Court of the Czech Republic and the Supreme Court of Lithuania.

Contact information: aleksandrs.potaicuks@rgsl.edu.lv

Prof. Dr Eglė Bilevičiūtė
is the professor of Mykolas Romeris University Law School since 2010 year. Since 2018 also member of Lithuania Administrative Disputes Commission, - quasi court institution, that examine administrative disputes. Her current research interests include digitization of administrative procedure and e-justice development's perspectives.

Contact information: eglek@mruni.eu

Samson Y. Esayas
is an Associate Professor at BI Norwegian Business School and a Faculty Associate at Harvard University's Berkman Klein Center for Internet and Society. His research explores the power dynamics stemming from control over data and mediated communications, with a focus on how these evolving power paradigms are addressed by competition and data privacy law. His book on the Interface between data privacy law and competition law is scheduled for publication by Oxford University Press in 2024. Dr. Esayas was a visiting researcher at Berkman Klein Center in 2023.

Contact information: samson.y.esayas@bi.no

Mathias K. Hauglid
is a PhD candidate and commercial lawyer who specialises in artificial intelligence and information technology. He is experienced with public sector digitalisation projects, including projects involving AI development. His research on legal and ethical aspects of artificial intelligence has been published in renowned international journals, and he is often engaged as a public speaker in this area. He wrote his doctoral dissertation at UiT the Arctic University of Norway, Faculty of Law, on the issue of bias in medical artificial intelligence. At the time of layouting this publication, Mathias is preparing to publicly defend his dissertation for the degree of PhD.

Contact information: mathias.hauglid@gmail.com

Lena Enqvist
is a senior lecturer of Law at Umeå University, Sweden. She specialises in administrative law, with one focal interest being rule of law challenges arising from the digitalisation and automation of public administration.

Contact information: lena.enqvist@umu.se

FOREWORD

Ensuring a just, inclusive, and sustainable digital development in the Nordic countries is an essential part in reaching the Nordic vision for 2030. The Nordic and Baltic nations have made significant advancements when it comes to digitalising their societies and the public administration systems over the last decade. Making sure that the core Nordic values of transparency, human rights and that our constitutional frameworks are upheld and secured throughout the process of digitalisation of the public sector is of utmost importance to maintain a high level of trust between individuals and between citizens and authorities in the Nordic-Baltic region.

In 2020, a pilot project, undertaken by Prof. Hanne Marie Motzfeldt at the University of Copenhagen, indicated that further investigation into how the rapid digitalisation of the public administrations and courts may impact and challenge basic constitutional, human rights and administrative law frameworks in the Nordic countries was required.

The following report culminates two years of research into this very topic undertaken by leading legal academics across the Nordic and Baltic countries. The project is funded by the Nordic Council of Ministers, and the research was carried out in the period March 2022 to December 2023, led by Prof. Hanne Marie Motzfeldt, University of Copenhagen, with a consortium of legal researchers from across the region.

The report strives to present an overview of the current status of the digitalisation of the national public administrations and courts in each of the Nordic and Baltic countries, from a legal perspective. While there are some notable constitutional differences between the Nordic-Baltic countries, the report also shows that certain experiences and challenges related to the digitalisation of the public sector are shared.

It is hoped that through its thorough status overviews of the digitalisation each of the Nordic-Baltic countries from a legal perspective, the report will help to identify possible areas for future cooperation and dialogue. Several of the authors indicate areas where they - based on their expertise and country-specific perspective - believe further cooperation would be valuable, and these recommendations in particular may well be taken forward for consideration.

RECOMMENDATIONS

Strengthening the Nordic-Baltic collaboration

Hanne Marie Motzfeldt

In the following, leading researchers within law and digitalisation from Norway, Sweden, Finland, Latvia, Estonia, Lithuania, and Denmark present the fundamental characteristics of digitalising their national public administrations from a legal perspective. Except from highlighting themes essential to touch upon in the investigations; the researchers have – in the Nordic-Baltic tradition – been free to examine relevant themes and form their conclusions and recommendations. It has not been considered suitable to bind their research by instructions, let alone by a strict questionnaire, which would hinder their free study and thus the opportunity to explore different – and potentially unexpected - topics and themes from their national arenas.

From different angles, all researchers have recommended strengthening the Nordic-Baltic cooperation regarding sharing experiences and handling challenges related to public digitalisation. The overall conclusion is that the DigiLaw project has uncovered that the Nordic-Baltic countries possess different specialised expertise, and further cooperation and knowledge sharing should be encouraged. For example, Finland is far in handling liability issues in relation to automated decision processes, while the Latvian state administration has extensive experience in the use of virtual assistants (consulting chatbots). Thus, Finland should be able to share experiences on regulating automated decision processes and Latvia in implementing generative AI such as ChatGPT in everyday administration.

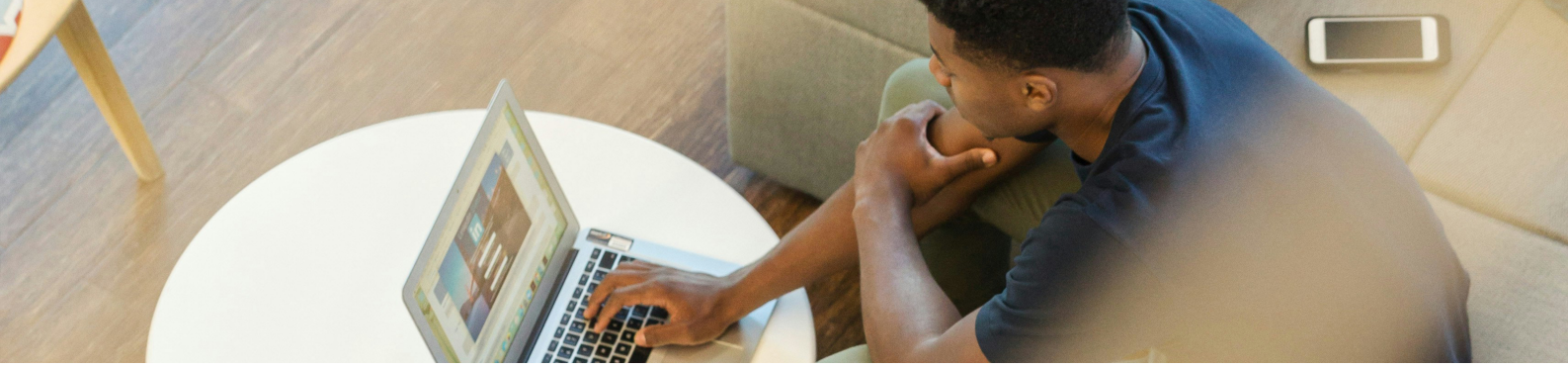
Further, the researchers have, in particular, pointed out that :

1. Collaboration centers around the regulatory sandboxes are recommended as the countries will be able to share experiences on how these can be organised most innovatively and efficiently. Initiatives on establishing such a collaboration center should be launched in the near future, as setting national sandboxes will be stipulated by the AI Act. The Norwegian Data Protection Authority might be an interesting and relevant partner as the institution holds considerable experience in sandboxes tailored for responsible AI.

2. The Nordic and Baltic countries differ from the majority of the EU member states as the Nordic-Baltic countries´ public sectors rank among the most digitalised in the world, and almost all public service and exercise of public authority depend on – assumedly in the light of worsened treats – too vulnerable systems. Therefore, EU information and cybersecurity regulations are inadequate to ensure robust public services and administrations. As information and cybersecurity should not be regarded as issues only relevant to the intelligence services, promoting robustness via coordinated regulatory initiatives in the Nordic-Baltic counties is recommended.

3. Data sharing, hereunder establishing more extensive sector-specific databases for developing machine learning-based models and other AI systems, can become instrumental in ensuring human rights, e.g. reducing biases against protected groups. Such cross-border collaborations require, however, a stronger focus on harmonisation, particularly in the regulatory terminology, semantics, and data definitions. Further, the researchers have debated whether a Nordic-Baltic Council of Data Ethics is recommendable. Here, pros and cons have led to the DigiLaw project recommending a debate hereon.

Further, a broader theme has repeated itself in several contexts, as researchers have noticed that the courts are primarily absent concerning the control of digital administration. The Nordic ombudsman institutions seem to take a leading role in ensuring an efficient, citizen-friendly, and compliant digital administration. In connection with the latter, the starting point seems to revolve around the requirements for good governance or the norms of good administration. As the institutions and the legal starting points share common denominators, strengthening the collaboration between the Nordic-Baltic ombudspersons is recommendable, if possible.



DENMARK

Status, new challenges and perspectives for Nordic-Baltic cooperation

Hanne Marie Motzfeldt and Adam Hyldkrog Lindberg

1. Introduction

The Danish digital administration is developed within an existing organisation and governance model. Yet, digitalisation in itself has affected these fundamental structures – changes and connected challenges which, to some extent, has been counteracted by regulative developments. Therefore, the following will begin with a brief, superficial introduction to the (traditional) organisation and governance structure of the Danish Public administration in section 2. Hereafter, the main characteristics of Danish digital administrations and some of the challenges that have occurred are presented in section 3. In section 4, the legal framework is introduced and debated; first, legal principles derived from the constitution; second, EU- and international fundamental rights regulation; and third, Danish administrative law. Fourth and final, the overall structure and regulatory model of the forthcoming EU regulation on artificial intelligence (hereinafter AI). This so-called AI Act is examined, and the regulation's future impact on the Danish legal system is discussed. In section 5, attention is drawn to a gap in existing regulation, which potentially poses a major threat to Danish society and citizens - natural and legal persons alike – and, thereby, the trust in public administration.

2. Organisational and Governance Structures of the Danish Public Administration

Since the June constitution of 1849 was adopted, the Danish public administration has been organised into two distinctive branches which today consist of: The (mainly) hierarchical-led, centralised administration and the collectively led, decentralised municipality and regional administration.[1]

1. *Forvaltningsret* / Mørup, S. H., Garde, J., Jensen, J. A., Jensen, O. F., Madsen, H. B., Revsbech, K., and Terkelsen, O. 7 ed. Copenhagen: Djøf Publishing, 2022. p 42 and 57.

The Central Administration consists of multiple entities divided into ministerial areas (jurisdictions) where the assigned administrative tasks (competencies) geographically cover the entire country. The competencies (jurisdictions) are delimited according to substantive criteria connected to legislation, e.g., tax law, environmental regulation, or religious matters. In alignment with the Danish constitution, this centralised administration is mainly hierarchical. At the top of each ministerial structure are the departments, in principle, managed directly by the ministers whom the prime minister appoints. In practice, however, management within the departments is steered by the Head of Departments, who acts as the right hand of the ministers.[2] Since the 1960s, the departments have developed into organisations that support the ministers' strategic and political initiatives. Consequently, supervisory tasks, handling administrative cases and even issuing execute orders have been pushed down to the lower organisations in the centralised organisation or to independent Board of Appeals. The tendency is that the directorates and agencies are entrusted with the supervision of the administration and the task of ensuring compliance via instructions and guidelines within the jurisdiction of the relevant Ministry. See below for more information on directorates and agencies. Handling citizens' and companies' complaints about decisions and actions taken by lower administrative units or municipalities and regions has mainly been placed with bodies established in legislation (appeal boards). Such appeal boards are, at the same time, usually given an independent status in the relevant legislation, ensuring they cannot be subject to orders from the politically appointed minister about the outcome of specific cases.

Under the departments, a range of agencies and directorates are to enforce regulation, ensure proper supervision of the administration within the ministerial jurisdiction, and, to some extent, act as appeal bodies and supervisory authorities. In other words, these lower directorates and agencies focus on governance and more citizen-oriented administration, including forming decisions in administrative cases related to their area of responsibility.[3] Examples of such Agencies are the Danish Agency for Labour Market and Recruitment and the Danish Agency for Higher Education.[4]

Further, as mentioned above, an extensive range of independent boards and councils, many of them appeal bodies and supervisory authorities, have been established in statutory law since the 1960s, deviating from the principle of hierarchical order between the administrative bodies within the central administration.[5]

The other major branch of the Danish administration consists of the Municipalities and the regions, which are entrusted with providing most of the welfare services and thus are highly citizen-oriented in their tasks. Municipalities and regions are collegially led administrations with democratically elected councils as the highest authority.[6] The regions' primary area of administration (competencies) is health care, combined with delimited tasks related to environmental matters, public transportation and institutions providing specialised care, whereas the municipalities are entrusted with tasks within almost all administrative areas.

The competencies of the Danish municipalities are traditionally divided into three categories: Service, regulation, and collection.[7] Services include very different areas, such as care of the elderly and disabled, renovation, libraries, day-care, schools, maintenance of infrastructure (roads) and public transportation. The regulatory functions include, for example, decision-making related to some social benefits, issuing building permits and other permits related to construction, as well as business permits and supervision of potential terms and conditions

2. Unlike many other countries, the Danish Head of Departments are not politically appointed and will act as head of the departments no matter the result of an election.
3. Almindelig Forvaltningsret / Bønsing, 5 ed. Copenhagen: Djøf Publishing, 2023, 71 p.
4. https://www.star.dk/en/ and https://ufm.dk/en
5. Almindelig Forvaltningsret / Bønsing, 5 ed. Copenhagen: Djøf Publishing, 2023, 7p 72p.
6. Almindelig Forvaltningsret / Bønsing, 5 ed. Copenhagen: Djøf Publishing, 2023, 73 p.
7. Almindelig Forvaltningsret / Bønsing, 5 ed. Copenhagen: Djøf Publishing, 2023, 58-59 p.

outlined in such permits within the geographic boundaries of the municipality. Regarding the tasks of collection, this has been narrowed down during the last decades as collective functions related to debt recovery and tax have been transferred to the highly digitalised central tax administration; today, the majority of collection tasks are associated with the services offered by the municipalities.[8]

Generally, governance in the Danish public administrations may be divided into governance within the hierarchy-led administrations and collegial-led administrations. In hierarchically organised administrations, the minister or leader of an entrusted organisation is, in principle, given the authority to execute (all) the administrative powers entrusted to the organisation. As an underlying condition for (the necessary) transfer of tasks and powers to subordinate civil servants or other public authorities, it follows both an access to give instructions and a duty to supervise the subordinates' execution of the transferred tasks and powers. This approach – and fundamental principle – originates from the Danish Minister Accountability Act and follows any further delegation of powers within the hierarchical systems, internally in the various organisations, as well as between the hierarchically organised units.[9] The appointed leaders – in the end, the minister – also have the power to overturn a decision or to initiate a general or specific 'call-in', the latter referring to taking over particular cases from a lover body or an employee. The access to give instructions – and to withdraw any transfer of power – does, however, not follow if the executive power in question is transferred to an independent organisation or a private person (natural or legal), e.g. a company providing a digital system for a public organisation. Therefore, such a transfer of executive power requires a basis in statutory regulation in Denmark.[10]

The leadership of the collegial-led administrations consists of multiple members with the same level of authority, and decisions will usually have to be made based on a majority vote. However, as such procedures are only realistic in matters of strategic or otherwise significant importance, everyday administration is delegated to administrative entities within different areas. These administrative entities are usually organised in a hierarchy under the collegial leadership.

The municipalities and regions are self-governing organisations and, therefore, not subject to the direct authority of the politically appointed Ministers. However, as stated in Article 82 of the Danish constitution, the municipalities are subject to supervision from centralised bodies as this supervision is defined in statutory law. The present supervision of the administration in the municipalities can be divided into two types.

First, the general supervision focuses on financial affairs and compliance with the regulation of municipalities and general administrative law, and second, supervision related to legislation, which only applies to specific areas of administration, e.g. environmental law. Whereas the general supervisory public agency, Ankestyrelsen, is located at the Ministry of the Interior and Health of Denmark, the special supervision rests with the appointed ministers within the different ministries' competencies (jurisdictions). The special supervision focuses on compliance with the legislation within the ministerial jurisdiction (although in practice, this special supervision has been pushed down to agencies and directorates or supervisory authorities, the responsibility of ensuring supervision and instructions still rests on the ministers due to the Danish Constitution and the Danish Minister Accountability Act). The general supervisory public agency, Ankestyrelsen, is in the relevant legislation given several remedies to enforce compliance, e.g. opposing fines on the democratic elected in the lead bodies of the municipalities. In contrast, the minister's supervision within the specialised areas does not have such powers vested in them (unless such is clearly stated in the relevant legislation).

8. Almindelig Forvaltningsret / Bønsing, 5 ed. Copenhagen: Djøf Publishing, 2023, 59 p.
9. Act no. 117 of 15. April 1964.
10. Developing Administrative Law into Handling the Challenges of Digital Government in Denmark. / Motzfeldt, Hanne Marie; Næsborg-Andersen, Ayo. I: Electronic Journal of e-Government, 2018.

The main aim of conducting public governance within this roughly described organisational framework is – and has long been – to ensure an efficient, citizen-friendly administration that acts within the powers legally granted to the said organisations and in compliance with the relevant regulatory framework. In Denmark, digitisation has long been regarded as a measure to support achieving these goals. Today, almost all services and administrative tasks are supported by or carried out through varying digital tools.

The development from a paper-based, analogue public administration to a highly digitalised, interconnected organisation has not only significantly impacted how the administration appears and acts externally towards citizens and businesses and governance within the public administration. See further regarding this issue in section 3.5. The digital transformation has simultaneously disrupted the above-described governance model. This shows itself in several contexts. First, workflows and activities were traditionally steered internally via general orders and guidelines developed by organisations or civil servants ranking higher in the hierarchy or by relevant supervisory bodies with a basis in legislative provisions. If harm or unlawfulness was caused by a lack of supervision from the higher-ranking public bodies, leaders and, in the end, the minister within the jurisdiction, said person could be held liable for neglecting the duty of supervision and relevant instructions.

Further, any civil servant performing a public task could be held liable if the person in question was not fulfilling his or her task in accordance with the law, orders, guidelines and professional standards. Today, process-support and process-steering digital systems significantly impact workflows, processes and even the outcome of decisions. Yet, private companies develop and maintain these systems, and the relationship between the public authorities and the private suppliers is only governed by contracts. In other words, the digital transformation has placed actors not bound by administrative law in a significant role in defining workflows and sometimes even how decisions directed at citizens and companies are formed.

Second, systems and databases have been increasingly cross-linked during the last decade, causing massive data flows and interconnected decision processes across entities and jurisdictions within the Danish public administration, thereby disrupting the traditional model of distribution of responsibilities and roles as well as blurring which body is supposed to supervise and ensure compliance in which scenarios.

An example illustrating this new organisational landscape and the disruption of the traditional model of governing in Danish public administration is the influential company KOMBIT, established and owned by Local Government Denmark –– the association and interest organisation of 98 Danish municipalities. KOMBIT specialises in the procurement of digital systems directed towards municipalities and has paved the way for shared use of the same systems across all Danish municipalities and new ways to share data between public entities. Further, KOMBIT has taken a lead role in defining standards and architecture models for at least the municipalities.[11] This impressive initiative does, however, have as a side effect that the knowledge and insight in the logic, architectures, designs – and flaws – of the digital systems used by the municipalities are gathered in KOMBIT and KOMBITs contract partners as opposite to the municipalities themselves.

Some of the different angles of this side effect showed themselves several times in 2020 and 2021 after KOMBIT launched the so-called KSD-system in 2019. The KSD-system was purchased by KOMBIT and developed by another private company, KMD. The KSD-system supports and automates the municipalities' case processing and payments in the area of social benefits in case of a natural person's illness. However, deficiencies and flaws in KSD caused extended case processing time and, to some extent, digitally generated incorrect consultation letters as well as

11. https://digitaliseringskataloget.dk/

wrongful decisions and payments. In the fall of 2020, when the Parliamentary Ombudsman sent a series of questions regarding the flaws in KSD to Herning, Holstebro and Viborg municipalities, the municipalities had to involve KOMBIT in order to answer the Ombudsman's questions.[12] Further, the Minister of Employment later briefed the Parliament Employment Committee on the progress of rectification of the flaws and deficiencies of the system. Here, he stated that: *"KOMBIT, which is owned by the municipalities via Local Government Denmark, sent a statement on the 9 of June to the Labour Market and Recruitment Agency (STAR) which describes that there has been a flaw in KSD, which resulted in wrong payments to smaller private companies and self-employed citizens. KOMBIT informs of a total wrong payment of up to DKK 110 million in the period November 2019 to March 2022."*[13]

In other words, the development from analogue to digitalised public administration has impacted how the public sector is organised and the embedded governance structure, especially as the systems are developed by private companies who are, per definition, not subject to administrative law.

3. The Digital administration in Denmark

3.1 Introduction

The high level of digitisation in the Danish public sector stems from early efforts later combined with more than 20 years of national public digitalisation strategies prioritising and pushing the development of digital infrastructure and different corporations across administrative areas and jurisdictions. This approach has resulted in the United Nations rating Denmark as the country in the world with the best digitalised public administration several times throughout the years.[14]

To present the Danish digital administration's main characteristics in a proper context, a brief historical overview will be given below in section 3.2. Hereafter, the key elements essential for the functionalities of the digitalised administration will be outlined in section 3.3. In order to provide an idea of the areas prioritised for further development and adjustment in the forthcoming years, the present Joint Government Digital Strategy is presented in section 3.4 before some recent challenges related to citizens' trust are outlined in section 3.5.

3.2 Historical development

As outlined above, the Danish Public sector is highly digitised. The journey towards this level of digitalisation began over 60 years ago as the first government agencies acquired so-called 'data processing machines.' These vast and rather clumsy machines were primarily used to transfer existing paper-based registers into the first databases, e.g. the population register (*Folkeregisteret*). Further, these first machines assisted some government agencies in performing complex or compressive calculations, e.g. within tax administration.[15] Accordingly, the software used at that time was customised to fit delimited tasks in a specific administrative area and created internally by developers hired as civil servants to address the public body's particular needs.

12. The Danish Parliamentary Ombudsman, letter to Herning Municipality of 2. marts 2021, dok.nr. 20/05623-22/STM, pkt. 2.
13. The Minister of Employment's briefing to the Parliamentary Employment Committee on erroneous payments to smaller private companies and the self-employed in the Municipal Sickness Benefit System (KSD) as a result of flaws in the system of the 1 of July 2022, Employment Committee 2021-22, appendix 312, https://www.ft.dk/samling/20211/almdel/beu/bilag/312/2603953.pdf.
14. In United Nations Department of Economic and Social Affairs, 2022, United Nations eGovernment Survey 2022 – The Future of Digital Government, the Danish Public administration is ranked number one.
15. Article 33 in the Ministry of the Interior's instructions for the population register no. 98 of 9 June 1956 mentions punch cards (§ 33 i Indenrigsministeriet instruks for førelse af folkeregister nr. 98 af 9. juni 1956)

With the later introduction of personal computers (PCs) and, subsequently, standard software for generic tasks, digital tools quickly became widespread in all areas of the Danish public administration. In continuation of this, the public authorities established small local networks, tying the PCs together to share resources, e.g., disk space and printers. These experiments took off a little later as the introduction of the Internet set in motion an action towards increased digital communication. Thus, from the late 80s, networks, printers, PCs, e-mails, and electronic calendar systems steadily replaced typewriters, calculators, mail carriers, and paper calendars. During the 90s, almost all internal communication became digitalised in the public sector in Denmark.

With the increased use of IT, early digitisation quickly followed as EDH and ESDH systems emerged (Electronic Document Handling and Electronic Case and Document Handling Systems). These systems introduced the potential of process support systems and are to be regarded as the beginning of the digitalisation era in the Danish public administration.

Legal literature generally refers to automatisation as a term covering all predefined processes, sometimes divided into fully and partly automatisation. Here, a distinction is made between digitalisation as process support and as process steering. Process support, as a term, covers digital elements that are 'simply' included in an otherwise analogue process, i.e., tools for caseworkers. Process steering, however, means that central functions in a process are predefined (automated) and embedded in a digital system, e.g. in a health and care system, where integrated workflows such as automatic calculation of medication and sharing of prescriptions with pharmacies are combined as workflows with decision-support elements that affect each other according to the defined rules. The difference between these two types of digitalisation can be illustrated via different designs of self-service systems. A process steering system automatically fills in information from public databases, and the process is designed to adapt according to different information, such as addresses, marital statuses, etc. A process support system may be a simple PDF to be submitted by the citizen via a portal. The latter form is often referred to in Denmark as "digital paper", as it is simply an electronic replication of one or more manual proceedings and not digitalisation as such.

During the late '90s and the '00s, larger, customised software became increasingly common in Public administration. An early example is the PAS (Patient Administration System), which was designed specifically for the Danish healthcare sector. The technological developments also prompted the Danish municipalities in 1970 to form a collaboration and establish a company, Kommunedata, which was assigned to develop and purchase digital systems for the Danish municipalities. This company was sold decades later, and KOMBIT was established; see about KOMBIT above in section 2. From this point, if one fast forward to 2023, the Danish public administration at all levels uses more than 4000 digital tools and process-support and process-steering digital systems, handling and steering everything from taxation to healthcare.

The development described above also caused almost symbolic changes in terminology. In the early times of digitalisation, the purchase of EDB (Electronic Data Processing) was the common phrase, later replaced by the term ITC or just IT (Information Technology). Today, the term IT is steadily replaced by digitalisation and digital systems, meaning that technology is used to rethink and merge with organisations, processes and governance.[16] However, the digitalisation stage has only been possible due to the development of a network of databases and a shared digital infrastructure. Here, Denmark has been a timely frontrunner.

3.3 Databases and digital infrastructures

As described above, the Danish public administration digital systems support or even handle almost all aspects of public administration. However, for these systems to function as intended, relevant and updated data needs to be accessible at all times. In other words, a doctor can only

16. Digital Forvaltning: Udvikling af sagsbehandlende løsninger. / Motzfeldt, Hanne Marie; Taheri Abkenar, Azad. Copenhagen: Djøf Publishing, 2019, and Fra forvaltningsjurist til udviklings- og driftsjurist: Retlige og dataetiske rammer for den digitale forvaltning. / Motzfeldt, Hanne Marie (ed). Djøf Publishing, 2024.

provide proper care for a patient with information from other healthcare personnel on the patient's former treatments, medicine and condition. The tax authorities will only be able to calculate and gather the correct amounts of taxes automatically if they have straightforward and easy digital access to relevant and accurate as well as updated information (data) on citizens income. Therefore, an almost unmanageable number of small and large databases feed the different systems with data gathered from citizens, companies and organisations, as well as by other public bodies.

Even before the digital era, the Danish public administration had a strong tradition of keeping large registers, record systems and archives structured and usable for civil servants when performing their tasks. For example, see the population register above in section 2 and just below in the present section. Since data regarding citizens and companies were already stored and maintained, the transition into databases started in the last century, and today, most of the extensive digital databases are readable and connected to multiple digital systems.

The Danish public administration's two largest and most essential databases are the Population register, which is named Central Person Register (CPR-Register) and the Central Company Register (CVR-Register). The Central Person Register consists of basic information on every citizen in Denmark connected to the national identification number given to every citizen seconds after being born or receiving a residence permit. This national identification number functions as a unique identifier across all the other databases in the Danish public administration. It enables accurate search for and identification of natural persons in all contexts, enabling crosswise data sharing. The other system – the Central Company Register – offers similarly basic information on legal persons, e.g. who owns a company or is responsible for an organisation. The real importance is, however, as the population register, that the Central Company Register provides a unique identifier given to all legal persons established in Denmark. As the national identification number for natural persons, this number functions as a 'can opener function', enabling information to be shared more efficiently between different public bodies.

Further, as digitalisation increased the demand for data and, thereby, data sharing, the national strategies of public digitalisation launched efforts to ensure common technical standards and definitions of data across the public administration as well as projects aiming at improving data quality, enabling easy connection between different systems and databases as well as trustworthy data. Further, several specific public agencies have been established to gather, format, and make data available for other public entities and the private sector. Typically, these agencies are tasked with collecting, structuring, processing, and sharing data from specific parts of the public sector or private actors, such as health data, geodata or data regarding education.

An example of such a Danish agency is the Danish Health Data Authority (*Sundhedsdatastyrelsen*), which gathers and formats data from the public and private Danish healthcare sector, such as doctors, hospitals, and private practitioners. The Danish Health Data Authority also maintains several national health databases, such as the Medicine Card (*Fælles Medicinkort*). Another example is the Agency of Data and Infrastructure (Styrelsen for Data og Infrastruktur), which is tasked with gathering geodata, including data on buildings, exact borders and sizes of regions and municipalities, as well as handling data regarding all building addresses in the country. This data is being shared with other public agencies, such as the tax authorities, who use the data to calculate property values for taxation purposes. A third example is the Agency for IT and Learning (*Styrelsen for IT og Læring*) gathering data from all schools and other educational institutions in Denmark, such as graduation data related to which courses students choose.

Besides the databases, centralised and decentralised, used by the Danish public administration, a range of shared systems and platforms have been developed at a central level during the last decades, enabling a high degree of digitalisation. First and maybe foremost, the Agency for Digital Government has had an authentication system, MitID, developed. MitID can be combined

with signature systems in compliance with the eIDAS regulation and is used across and at all levels of the Danish public administration.[17] Further, the platforms Borger.dk (Citizen.dk) and Virk.dk (Company.dk) are essential as they are a window for citizens – natural and legal persons – to gain information on public services, regulations and to access a wide range of self-service systems from different public bodies, which are gathered at the portals. Also available on the platforms is the public Digital Mail (*Digital Post*), an official mailbox dedicated to all communication between the public administration and citizens (natural and legal persons alike). Digital Post is regulated in statutory legislation, ensuring that possession and use hereof is mandatory for citizens (unless a dispensation is applied for due to, e.g. mental handicap) and that Danish authorities can write to both natural and legal persons with binding effect via this mail system.[18]

As MitID, Borger.dk and Virk.dk might be the most visible of the systems forming the infrastructure of the Danish digital administration they are supplemented by the databases and a large number of systems that support digitalisation internally and across different jurisdictions, e.g. the invoice system developed to ensure compliance with the standards set by the EU-Commission and the Agency for Public Digitalisations synthetic dataset developed for testing systems before they are taken into use.[19]

3.4 The Joint Government Digital Strategy

The development towards becoming one of the world's most digitalised public sectors has required significant investments and planning, coordination and prioritisation of initiatives and projects. Therefore, since 2001, the Danish Agency for Public Digitalisation, originally a part of the Ministry of Finance, now of the Ministry for Digitalisation and Gender Equality, has cooperated with other central, regional, and local government institutions in order to draft Joint Government Digital strategies every fourth year.[20] The latest of these strategies was published in 2022 and will thus steer initiatives and projects until 2025.[21]

The Joint Government Digital Strategy for 2022–2025 focuses on how digitalisation can solve some of Denmark's significant societal challenges in the coming years, mainly an increasing labour shortage, a need for a green transformation and a lack of resources within welfare and healthcare. The strategy is structured into four visions with specific initiatives to be funded to fulfil said visions. Across the visions are five so-called objectives – waypoints - to steer all the initiatives.[22]

The first vision is to develop a more coherent and user-friendly digital public sector for everyone. This includes 17 initiatives, including more cross-jurisdiction corporations, user-friendly digitalisation, improvements of the public power of attorney solution, further development of the so-called My Insight system (Mit Overblik) enabling citizens to access an overview of their cases and data and a national guide to health apps.[23] The second vision is to remedy the labour shortage in Denmark via digitalisation, which focuses on further automation and notably increased use of AI. The third vision is to utilise digitalisation to support the green transition, and the connected initiatives are, among others, the establishment of a database for the recycling and reuse of construction materials and to develop a CO2 calculator to be used at all levels of the

17. Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
18. Act no. 686 of 15. April 2021 on Digital mail from public authorities.
19. Commission Implementing Decision (EU) 2017/1870 of the 16 of October 2017 on the publication of the reference of the European standard on electronic invoicing and the list of its syntaxes pursuant to Directive 2014/55/EU of the European Parliament and of the Council.
20. See further https://en.digst.dk/policy/the-danish-digital-journey/
21. https://digst.dk/media/19302/national_strategi_for_kunstig_intelligens_final.pdf.
22. In subtitles, these waypoints are: Digitisation is a mean, not a goal in itself; everyone is to be included; focus on coherency, transparency and trust, responsible digital development and shared digital foundations. See further on inclusion in section 3.5.
23. https://en.digst.dk/strategy/the-joint-government-digital-strategy/

public administration. Finally, the fourth vision of the Joint Government Digital Strategy for 2022–2025 is to ensure a stronger foundation for future digital development, which, among others, will lead to initiatives strengthening the development of Danish language models and initiatives within cyber- and information security.

At first glance, all of these visions and initiatives seem to aim to further the digitalisation of the Danish public sector and bring even more advanced technology into use. In reality, some of the initiatives are; however, continuations, even adjustments of former initiatives as these are still not fully realised, or further initiatives turned out to have been realised via too far-reaching measures thereby negatively affecting citizens trust and inclusion.

3.5 Challenges

As mentioned above in section 2, the digitalisation of the Danish public sector has affected the traditional organisation and governance model. The long-term effects hereof have still not surfaced but will probably have to be handled in the future in order to ensure the values of democracy, the rule of law and a citizen-friendly public sector. In the summer of 2022, however, another challenge was uncovered as a heated public debate arose. The background hereof was that a rather large group of citizens claimed to feel helpless, alienated, and frustrated when interacting with the digitalised administration.

The background for this debate might illustrate how difficult it is to predict the challenges that will arise due to public digitalisation. In 2021, the Danish Agency for Public Digitization published a report that concluded a high degree of trust among the population in the digitalised administration.[24] However, in July 2022, a legal Think Tank, Justitia, published another report. The report from the independent legal Think Tank concluded that there were significant challenges to inclusion and as a result, also to citizens' legal certainty. It estimated that up to one-fourth of the population had significant or at least some difficulties navigating the digital administration.[25] The report from Justitia was the starting point for the abovementioned extensive debate, which introduced a new term in Denmark: The digital underclass. In line with a series of articles from a leading newspaper in Denmark, Politiken, the debate became broader. Even famous artists joined. The painter Per Arnoldi contributed by designing a sign for digitally vulnerable citizens, on which was written I(t)nvalid corresponding to the well-known sign for invalid. [26] The famous Danish actor Ghita Nørby was interviewed in several articles and at events as she claimed that digitisation had 'broken the welfare state'.[27]

This debate is mirrored in the first of the visions in the present Joint Government Digital Strategy for 2022–2025, as this vision implies a series of initiatives to increase accessibility and ensure non-digital citizens can contact public bodies (inclusion). As former strategies initiated legislation to turn the use of digital self-service systems, the public digital mail, and possession of the authentication system, MitID, mandatory, the present strategy acknowledges that those hush means lead to a public administration perceived distant and unapproachable by some citizens.[28] In other words, the present Danish vision of a digital administration for all citizens illustrates how the former strategies might have driven digitalisation far but also caused unforeseen consequences that are now to be mitigated in the present strategy.

24. https://digst.dk/nyheder/nyhedsarkiv/2021/november/ny-analyse-afdaekker-borgernes-tillid-til-den-digitale-offentlige-sektor/
25. https://justitia-int.org/digitalt-udsatte/
26. https://en.wikipedia.org/wiki/Per_Arnoldi
27. https://politiken.dk/danmark/art8920891/Velf%C3%A6rdsstaten-%C2%BBer-%C3%B8delagt-desv%C3%A6rre%C2%AB
28. The National Digitalisation strategy for 2011-2015 aimed at increasing citizens' use of self-service systems. Therefore, a basis for issuing executive orders turning the use hereof mandatory was given in Act no 742 of 1. June 2015, Act no. 552 of 2. June 2014, Act no. 622 of 12. June 2013 and Act no. 558 of 18. June 2012, see the Strategy https://digst.dk/media/12704/digitale_vej_til_fremtidens_velfaerd.pdf .

4. The legal framework

4.1 Introduction

The legal framework of the Danish digital administration can be divided into two overall categories. One consists of regulation applicable only to specific public bodies such as the police or for specific areas such as welfare regulation. The other category is the general regulation that applies to all public authorities' activities unless otherwise laid down in legislation. Within the latter category are, among others, constitutional law and legal principles derived from the constitution, EU- and international fundamental rights regulation and general administrative law. These legal disciplines interact with the overall legal framework of the Danish digital administration and are presented in the following sections 4.2–4.4. Section 4.5 presents the forthcoming AI Act, and the AI Act's impact on the Danish regulatory system is discussed in section 4.6.

4.2 Constitutional principles and legal basis for digitalisation

The Danish constitution has been linguistically almost unchanged since the June constitution of 1849 was adopted. In spite of this, national constitutional law, by virtue of tradition and interpretation of the historical text, does contain some basic principles of relevance for the digitalised administration.

First and foremost, it is recognised as an underlying value that the legislative power draws its legitimacy from democratic elections and that the executive power, which does not have such legitimacy, thus must be exercised in compliance with the regulation adopted or otherwise regarded as accepted by the legislator. Further, those who exercise the entrusted executive powers must be able to be held accountable by (at least) the courts.[29] Second, from Article 3 of the Danish constitution, constituting the legislative, executive and judicial powers, the requirement that the executive power must have a basis in law for its activities is derived.

The above generally implies for the Danish administration that public authorities must be authorised in law to carry out their activities, have to perform their tasks in accordance with applicable regulation and that legislation takes precedence over executive orders, administrative orders, guidelines and decisions (the principle of legality). However, the significance of this is not straightforward in relation to the development and use of digital systems in public administration.

There is, however, consensus that a basis in statutory law is required if burdens are placed on citizens (natural as well as legal persons) or their legal or financial status is affected by public authorities' activities. The heavier the burden or deeper the intervention, the more precise and unambiguous the legal basis must be.[30] On the other hand, an indirect presupposed and/or budgetary basis is usually sufficient to decide organisational matters, design workflows and similar internal matters. In some instances, such indirect presupposed problems and/or budgetary basis can even be extended to regulate the behaviour of citizens, e.g. issue t relevant and proportionate codes of conduct in a public institution.

Regarding the digitalisation of public administration, it is evident that a statutory legal basis is not required to buy and use simple digital tools such as office packages. A budgetary basis is

29. Further, but not quite as relevant for the digitalised administration, citizens are guaranteed a certain minimum of rights. The Danish constitution's catalogue of fundamental rights could be more impressive compared to other countries, but individual political and personal rights are nevertheless granted. The politically oriented rights are the freedom of expression, the freedom of association, the freedom of assembly, the individual personal freedom and the inviolability of housing and property rights.
30. *Forvaltningsret* / Mørup, S. H., Garde, J., Jensen, J. A., Jensen, O. F., Madsen, H. B., Revsbech, K., and Terkelsen, O. 7 ed. København: Djøf Forlag, 2022, p 148-155.

sufficient in such cases. On the other side, some digitisation projects may be so disruptive for the affected area of administration that the abovementioned ideals pull towards ensuring acceptance of the democratically legitimised legislature.[31] In addition, other circumstances may add additional weight for a legislative process, e.g. a high-risk economic profile of a digitalisation process or significant risk of imposing financial loss on citizens – natural and legal persons alike – due to e.g. prolonged response periods when a system is taken into use. Further, tendencies in legislative practice indicate that Danish public bodies, to some extent, either perceive themselves as obliged to or find it appropriate to seek legislative approval of more transformative digitalisation processes. Common denominators in seeking a legislative framework seem to be whether a planned digitalisation project possesses a risk of non-compliance with fundamental legal principles, a potential negative impact on the governance mechanisms within the public administration or the interaction with citizens. Finally, the project's financial risk profile, the risk of legal repercussions and data ethics considerations seem to be of relevance.

An example is an amendment to the Danish Tax Reporting Act and the Tax Control Act, adopted in 2021.[32] The amendment provided a legal basis *'to process, including share, possessed data to develop digital systems necessary for the customs' and tax administration's exercise of authority'* and that the tax authorities: *'may collect and process all necessary data about natural or legal person's financial and business affairs from other public authorities and from publicly available sources, and merge such data with data already in the custom's s and tax administrations possession, with the purpose of developing systems necessary for the customs and tax administration's exercise of authority'*. In harmony with the above described, it is indicated in the preparatory documents that the establishment of an unambiguous legal basis for the planned development of machine learning and analytical models had been found appropriate due to: *'fundamental societal values and basic legal principles'*.[33]

Further, the initially mentioned requirement of compliance with applicable regulation may presuppose legislative changes as efficient use of digital systems burdens citizens or a governance structure violates applicable rules. This was clearly shown during the National Digitalisation Strategy 2011–15 as this strategy initiated mandatory use of the majority of self-service systems to achieve a goal of 80 per cent of the population of legal age communicating with public authorities through these systems.[34] Requiring citizens to use a specific form of communication is, however, regarded as a burden and, at the same time, deviates from a fundamental principle of Danish administration stating that citizens (within reasonable limits) have the right to contact an administrative body in any form.

In the Danish Parliamentary Ombudsman's opinion, published in FOB 2015-36, he stated that the Municipality of Frederiksberg did not have a legal basis for – as indicated on the municipality's website – that citizens had to file complaints regarding parking charges via the municipality's digital self-service system. A similar statement can be found in the opinion published in FOB 2019-11 and the Parliamentary Ombudsman's newsletter, published on the 25th of May 2023.

In other words, a statutory legal basis is required if developing and/or using a digital system implies deviation from existing regulations. Article 32 b of the Danish Public Administration Act's derogation from the former signature requirement when automated decision-making is initiated, is an early example.[35] Another example is related to the doctrine of delegation (outsourcing of executive power), which led to the Act on NemID and, later on MitID, allowing private companies

31. *Forvaltningsret* / Mørup, S. H., Garde, J., Jensen, J. A., Jensen, O. F., Madsen, H. B., Revsbech, K., and Terkelsen, O. 7 ed. København: Djøf Forlag, 2022, p 178-182.
32. Act no. 2612 of 28. December 2021.
33. Bill no 73 of 10. November 2021
34. Act no. 742 of 1. June 2015, no 552 of 2. June 2014, no 622 of 12. June 2013 og nr. 558 of 18. June 2012.
35. Consolidated Act 2014-04-22 No. 433 Public Administration Act and Lovforslag nr. 13 af 2. oktober 2013 om ændring af forvaltningsloven, lov om Politiets Efterretningstjeneste (PET) og lov om Forsvarets Efterretningstjeneste (FE).

to operate, maintain and govern the systems on authentication.[36]

The Danish Parliamentary Ombudsman's case, published in FOB 2017-19, was initiated by a local ombudsman in the municipality of Faxe, who had tried to advise some elderly citizens who had been rejected a NemID by the municipality but needed a NemID in order to report their leasing of farmland (fields) via the mandatory self-service system for such (mandatory) reporting. As justification for the refusal, the municipality referred to the binding guidelines on NemID, which had been drafted by the private company Nets DanID. The background hereof was that the Agency for Public Digitalisation, who owned NemID, had outsourced the development and maintenance of NemID to Nets DanID. Net's DanID had later agreed with the municipalities that the municipalities handled the citizen-related tasks regarding issuing NemID as so-called registration units. As part of the agreement, the municipalities were obliged to comply with the guidelines and instructions drawn up by Nets DanID when issuing a NemID. In other words, outsourcing from the Danish Agency for Digitalisation to Nets DanID had been followed with Nets DanID's subsequent instructions to the in relation to the Danish Agency for Digitalisation independent municipalities. An agreement was therefore reached between the Ombudsman and the Agency for Digitalisation that an unambiguous legal basis for the outsourcing of NemID had to be established.

Finally, the legislator will probably be involved increasingly in connection with the initiation of – at least more extensive – projects when it is necessary to deviate from EU regulation (if such deviations are possible under EU law) *or* EU law requires a more precise and more unambiguous legal basis for processing personal data than required according to Danish constitutional and administrative law. An early example of such deviation is the Act on the Danish Business Authority's processing of data. Based on Article 23 of the data protection regulation (GDPR), this Act provided a mandate for executive orders deviating from the purpose limitation principle in Article 5, subsection 1, letter b, of the GDPR.[37] The preparatory documents state that the purpose hereof was to provide the Danish Business Authority with the opportunity to develop machine learning-based predictive modules and modern data analysis methods.[38]

The requirement of an unambiguous legal basis follows from the GDPR and Article 8 of the Charter of Fundamental Rights of the European Union, which states that a legal basis for processing personal data must be established. As a citizen's consent can rarely constitute the legal basis for processing personal data in the digital administration, public bodies must rely on Article 6, subsection 1, letter e, of the GDPR. According to this provision, the processing of personal data can be initiated if the processing is necessary for the exercise of public authority. The embedded requirement of necessity varies from an implicit to a strict assessment, requiring clear, precise and unambiguous national regulation allowing the processing in question. Clear, precise and unambiguous clarification in national law is especially needed if the processing of personal data can be regarded as high risk, e.g., profiling vulnerable citizens using sensitive personal data processing.[39]

The Act on an Active Employment Effort is another example of a regulation providing an unambiguous legal basis for processing personal data.[40] An amendment in 2019 provided the Agency for Labour Market and Recruitment with a legal basis to process personal data in order to develop and offer a nationwide digital profiling tool.[41] The tool entailed, among other things, that an assessment of the risk of long-term unemployment of newly unemployed citizens could be carried out based on data from the citizens and from the Ministry of Employment as well as from other public databases. Several years later, the Danish Data Protection Authority was asked if a municipality could lease and use a similar profiling system called Asta, which a private

36. Act no. 439 of 8. May 2018.
37. Regulation (EU) 2016/679 of the European Parliament and of the Council of the 27 of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
38. Act no. 438 of 8. May 2018 and Executive Order no 989 of 29. June 2018 and Bill no. 149 of 21. February 2018, section 3.1.2 and commentary on article 1.
39. The Danish Data Protection Agency Guide on Public Authorities Use of Artificial Intelligence, 2023, p. 19.
40. Consolidated Act no 701 of 22. May 2022.
41. Bill no 210 of the 27 of March 2019 and the Danish Data Protection Agency case no. 2019-11-0236

company had developed. Using Asta similarly entailed a machine learning-based analysis of newly unemployed citizens' risk of becoming long-term unemployed. However, the processing of personal data via Asta in contrast to the tool developed by the Agency for Labour Market and Recruitment did not have a clear national legal basis. The Danish Data Protection Authority stated, in general, that for completely harmless processing of personal data, the requirements [for clarity in national law] will not be particularly strict. If, however, the processing in question may be regarded as intrusive, as is the case of Asta, the demand for clarity of the necessity increases.

In summary, there is a tendency towards seeking a legal basis in legislation for at least a more significant high-risk digitalisation project. Such a basis will be required if the development or use of a system will imply a deviation from existing regulations or a clear and unambiguous basis for processing personal data. In other words, the core democratic functions must be regarded as integrated in relation to the digital administration, as the democratically legitimised legislature's acceptance of more far-reaching digitisation initiatives seems to be sought.

4.3 Fundamental Rights

4.3.1 Introduction

The result of an ageing Danish constitution, combined with a dualistic approach to international law, is that fundamental rights are primarily carried into the digital administration via EU law. Of lesser – but still some – influence are the international human rights instruments. Denmark has ratified and implemented the European Convention on Human Rights (hereafter ECHR) in Danish law, just as Denmark has ratified the UN Convention on the Rights of Persons with Disabilities. Together, the Charter and these international instruments form part of the overall legal framework to ensure citizens' fundamental rights in the digitalised Danish administration as in the former analogue and paper-based administration.

The relevance of international human rights regulation can be illustrated by cooperation between the Danish Institute for Human Rights and the German Agency for International Cooperation (GIZ). The institutions have introduced a tool to identify and assess human rights risks while developing digital systems.[42]

In the following, those provisions of the Charter of Fundamental Rights of the European Union, which assumedly will be essential elements of the legal framework for the digitalised administration in the forthcoming years, are presented in section 4.3.2, followed by a similar presentation of international human rights instruments in section 4.3.3. In section 4.3.4, an analysis of the capability of Danish Administrative law to ensure compliance with fundamental rights in digital administration is carried out before looking into the forthcoming AI Act and the EU regulation's potential impact on the Danish legal framework in sections 4.5 and 4.6.

4.3.2 The Charter of Fundamental Rights of the European Union

Within the scope of EU law, the Danish legislature and the executive power are obliged to respect the fundamental rights of citizens as these are recognised in EU law. This implies that public authorities just like the bodies of the EU are to observe the duties arising from the ECHR and the Charter of Fundamental Rights of the European Union (hereafter the Charter), cf. Article 51 of the Charter. Within the digital administration, the authorities must, therefore, not only respect secondary EU legislation applying to the development, implementation and use of digital systems but also if an activity is within the scope of EU law ensure compliance with fundamental rights and the core principles of EU law, e.g. equal treatment, protection of legitimate expectations and

42. https://digitalrights-check.bmz-digital.global/

proportionality.

According to Article 51 of the Charter, national public authorities and courts must ensure compliance with the Charter when they make decisions based on EU regulation or a national regulation implementing an EU directive. The same applies if there is a strong functional connection with EU law or national regulation that interferes with the four freedoms regarding goods, persons, services and capital.

The Charter consists of a broad pamphlet of rights not recognised in the Danish constitution and of legal principles, which in Denmark are regarded as case law-based principles of administrative law (even though EU and national legal principles are not entirely identical). In particular, articles 41, 8, 20 and 21 of the Charter are essential elements of the legal framework applying to the Danish digital administration.

For the digital administration, the underlying principles of Article 41 of the Charter laying down the requirement of good administration may be relevant for the Danish legislature's ability to deviate from the requirements for, among other things, a consultation (fair hearing) before a decision is taken. Article 41 does, in principle – in a relatively general form – only regulate administrative procedures within EU administration. However, the EU Court of Justice has stated that, among other things, the right to a hearing, established in Article 41, is a codification of an underlying principle. This legal principle binds the Member States if EU law applies – and will thus carry the contained procedural requirements into the digital administration.

Furthermore, the Charter's article 8, subsection 1, states that: "[e]veryone has the right to the protection of personal data concerning him or her" and in subsection 2, that: "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." Article 8 is, in particular, specified in the GDPR and the directive on data protection in law enforcement. See above in section 4.2.[43] The GDPR are – in a Danish context – regarded as a part of general administrative law.

Finally, articles 20 and 21 of the Charter will probably gain increasing importance as the development and use of machine learning and other forms of artificial intelligence expand – a goal pursued as a part of the visions in the Danish Joint Government Digital Strategy for 2022–2025, see above in section 3.2. Article 20 of the Charter proclaims that "Everyone is equal before the law ", and the Charter's Article 21, subsection 1 states that "Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited". Since an inherent risk of AI is that bias in training data is passed on to the developed models, these provisions will form a legal framework requiring that the use of AI does not lead to discrimination contrary to these provisions. This will, in particular, apply to profiling models used to assess citizens based on differences in variable values, which – depending on the model's design – may entail a risk of direct or indirect discrimination.

Direct discrimination against a protected group may occur if a profiling model uses a variable characterising a protected group of citizens. This could, for example, be gender, consequently awarding male citizens a higher probability of being classified positively while females are

43. Regulation (EU) 2016/679 of the European Parliament and of the Council of the 27 of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Directive (EU) 2016/680 of the European Parliament and of the Council of the 27 of April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

classified negatively (or vice versa). Indirect discrimination may occur if a model in practice places a protected group in an unfavourable position compared to others, even if the model does contain a variable characterising the protected group, i.e. even if the model is blinded to said group. An example could be a statistical connection between residence and ethnicity. If citizens of specific ethnicities are overrepresented in certain residential areas, a model with residence as a variable might affect some ethnicities more than others.

In continuation of the above, it is noteworthy that the Danish Institute for Human Rights has pointed out in a recent report that the use of opaque AI may increase citizens' difficulties in proving indirect discrimination unless the legal framework is adjusted into a shared burden of proof.[44]

4.3.3 The European Convention of Human Rights (ECHR)

The scope of the ECHR and the Danish dualistic approach entails that the ECHR affects the legal framework for the Danish digital administration differently than EU law. In contrast to the promotion of harmonisation and the enforcement of the EU interpretation style, the ECHR provides a relatively wide margin, and the EctHR have a distinctive focus on the circumstances of every individual case. The ECHR's impact on the Danish legal system has, therefore, primarily played out within the specialised administrative law, se about the distinction between general regulation and regulation applying to delimited areas above in section 4.1. This is, for example, forced fixation of psychiatric patients, expropriation and regard to the Danish legislation and case law on immigrants and refugees.

However, the ECtHR's expanding interpretation of the ECHR has historically shown to establish duties of care for public authorities that might become important as a part of the legal framework for the Danish digital administration, as this might lead to proactive measures must be taken in order for ensure that systems and the use hereof are design in such a way that compliance with the ECHR is promoted. Here, attention is drawn to six aspects expected to become relevant for those who develop and use digital digital systems for and in public administration.

Firstly, the ban on self-incrimination in Article 6 of the ECHR must be taken into account when citizens are required to provide data (information) to the public authorities via self-service systems and these data are intended to be used in different contexts, and Article 6 are relevant in some of these contexts. Secondly, the ECtHR has stated that article 8 of the ECHR – as article 41 of the Charter – contains procedural rights as the right to a fair hearing before a decision directed at a citizen is reached. Thirdly, case law from the ECtHR requires reasonable processing time. This might not seem relevant regarding digitalisation, but experience shows that implementing newly developed systems might cause prolonged processing time. Fourthly, in principle, Article 8 of the ECHR lays down requirements for processing personal data, just as this provision, in interaction with Article 10 of the convention, may impact certain groups' right to access documents. Finally – as the fifth theme – the ECHR requires that public bodies ensure translation services in a number of situations in order to ensure citizens can understand guidance from and decisions made by public authorities.

The latter requirement illustrates how legal requirements under the ECHR in Denmark will interact with other international obligations and national administrative law, thereby placing the ECHR in the background. In relation to translation services, Denmark has ratified the Nordic Language Convention, the European Charter for Regional or Minority Languages (the Language Pact) and the Council of Europe's Framework Convention of the 1 of February 1995 on the

44. https://menneskeret.dk/udgivelser/naar-algoritmer-sagsbehandler-rettigheder-retssikkerhed-offentlige-myndigheders-brug

Protection of National Minorities (the Minority Convention).[45] When interpreted into Article 7 of the Danish Public Administration Act, laying down an obligation to provide guidance for citizens, this spaghetti ball-like framework of conventions entails a duty to ensure that at least the digital self-service systems, which are mandatory for citizens to use, are offered in relevant foreign languages, or an alternative communication channel is available.

4.4 Danish Administrative law

4.4.1 Introduction

Danish administrative law only partially consists of legislation such as the Public Administration Act, the Freedom of Information Act, the GDPR, and the supplementary Danish Data Protection Act.[46] Case law-based principles apply next to this statutory regulation, thereby providing Danish administrative law with a somewhat dynamic nature, enabling the regulation based on underlying legal values to adapt to societal changes such as the digitalisation of the public administration. In accordance herewith, supervisory bodies, with the Parliamentary Ombudsman at the forefront, have developed Danish administrative law and set up requirements for the design and functionality of digital systems, their development, implementation and use.[47] This case law is under continuous development in line with the technological and societal changes and is characterised by searching: "the legal toolbox for regulation able to be meaningful in the new technological context."[48]

The development of administrative law in Denmark has revolved mainly around two starting points. First, administrative law and the norms of good administration are technology-neutral. Therefore, the regulatory requirements apply regardless of the technology a public body uses to perform its assigned tasks. Second, public administration must be organised and carried out in a compliant, efficient and trustworthy manner, no matter the technologies used. The following section, 4.4.2, will outline how these starting points led to a requirement of designing technologies and their use in such a way that compliance with administrative law is supported. Section 4.4.3 focuses on another requirements – namely, the demand for a prior compliance investigation, testing and supervision, respectively.

4.4.2 Administrative law by design

The Danish principles of good administration require that public authorities establish an organisation and implement workflows that are able to support a compliant and efficient administration. This fundamental requirement is mirrored in legislative practice. It is, for example, stated in the preparatory documents to Act on the Regions that the regional Council is *'responsible for ensuring that formalities are complied with, i.e. that sufficiently qualified personnel are employed, that these employees observe the principles of good administration and, that internal measures are taken to implement appropriate workflows, routines and supervisory procedures'.*[49]

45. Executive Order No. 16 of the 10 of March 1987 of the Nordic Convention of the 17 of June 1981 on the right of Nordic citizens to use their own language in another Nordic country, Executive Order No. 28 of the 23 of August 2001 of the European Pact on Regional or Minority Languages of the 5 of November 1992 and Executive Order No. 13 of the 23 of April 1998 of the Council of Europe's Framework Convention of the 1 of February 1995, see the conventions at https://www.norden.org/en/treaties-and-agreements/nordic-language-convention https://llengua.gencat.cat/en/serveis/legislacio_i_drets_linguistics/el-catala-i-europa/carta_europea_de_llengues_regionals/ and https://rm.coe.int/168007cdac
46. Consolidated Act no nr 145 of 24. February 2020, and act no. 502 of 23. May 2018.
47. The Danish Principle of Administrative Law by Design. / Motzfeldt, Hanne Marie. I: European Public Law, Bind 23, Nr. 4, 2017, s. 739-754.
48. Niels Fenger, Ombudsmanden – et værn for borgernes retssikkerhed, U 2020 B 37. See the same author (and the appointed Danish Parliamentary ombudsman), How do we digitise without harming our legal certainty? , FOB 2019.
49. Bill no. 65 of the 24th of February 2005, comments to article 16.

How the above-described approach has been carried into the digital era can be illustrated via a response from a former Minister of Health to the Danish Parliament's Health and Elderly Committee in 2017 regarding a system named Cura. The minister stated, among other things, *'Responsibility for patient safety in the healthcare system lies with the operators, i.e. regions, municipalities and private actors. It is the operators' responsibility to react if tasks are carried out in a way that endangers patient safety, just as the operators are obliged to ensure that the employees have the proper skills for the tasks they are carrying out. Similarly, it is the operators' responsibility to ensure that the digital systems used are reliable, that the employees are trained to use the systems and that the systems do not endanger patient safety'*.[50] Similarly, the Danish Parliamentary Ombudsman has stated in numerous opinions that digital systems for the public sector are to be designed to support a compliant and efficient administration.

This implies that Danish authorities are obliged to commit to a value-based design and ensure that administrative law is included in the design and use of their digital systems. The underlying idea is that since the design, architecture, functionalities and use of digital systems affect the administration, the responsible authorities are obliged to – similarly to designing analogue processes – proactively ensure the system's capacity to support a compliant and efficient administration.

An older yet illustrating case is published by the Parliamentary Ombudsman in FOB 2006.390. The case related to a record system used by the University of Copenhagen in connection with handling cases on student grants. The system lacked functionality for searching previous cases based on provisions of the applied legislation or similar substantive criteria. In his opinion, the Ombudsman raised doubt that it was possible to ensure a uniform practice in accordance with the principle of equality if the university was not able to conduct searches in the institutions' previous administrative decisions. In this specific case, the Ombudsman recommend measures to mitigate the effects of the deficiencies of the record system, for example, procedures for keeping lists or summaries based on substantial criteria. In other words, the opinion illustrates that digital systems should be designed to support compliance with the principle of equality.

The Danish principle of administrative law by design is, among others, codified in the Freedom of Information Act. Article 1, section 2 of the Act states that public authorities are to ensure that openness is considered to the widest possible extent when digital systems are chosen, developed and implemented. The Danish Freedom of Information Act entered into force in 2013. The value-based approach was, however, strengthened as a fundamental legal figure in Danish administrative law when the GDPR came into effect in 2018.

4.4.3 Proactive compliance assessments and supervision during use

The Danish administrative law requirements for developing and using technologies are somewhat similar to the EU regulatory models applied in the GDPR and regarding high-risk systems in the AI Act. First, a prior investigation of a digitalisation project's legal, practical and technical aspects must be carried out (a good administration impact assessment). Second, public authorities are to ensure proper testing of digital systems before they are taken into use and to initiate training of employees in using the system. Finally, the system and the impact on the administration are to be supervised, and action taken if system deficiencies or flaws lead to violations of regulation or the norms of good administration.

The good administration impact assessment is to be started up already in the early stages of a process of developing a digital system. The requirement for this procedure originates from a combination of the norms of good administration, the inquisitorial principle, the principles of civil

50. The Parliament Health Committee 2017–18, answer to question no. 402, https://www.ft.dk/samling/20171/almdel/SUU/spm/402/svar/1464763/1855071.pdf

servants' liability, and the principles of responsible use of public funds. Further, influence or inspiration from legislative trends is likely, as similar requirements can be found in the GDPR.

A preliminary status on the requirement for a good administration impact assessment has recently been given by the Parliamentary Ombudsman in FOB 2022-11 and FOB 2022-12. Here, the Ombudsman stated, *'It is a fundamental requirement that public digital systems support a correct application of the relevant legislation – including administrative law and fundamental principles. This can best be ensured by early identification and system incorporation of the relevant regulation. A proper organisation of the development of new digital systems for the public sector, therefore, presupposes, among other things, that an overview of the types of cases and processes affected by the planned system is created, that is mapped which formal rules (e.g. on hearing and reasons for decisions) and substantive rules (e.g. on the exercise of discretion in the individual case) that applies to the processes of the affected cases, including whether there may be a need for the regulatory changes in order to enable automatisation, that great care is shown in deciding how the new system have to be designed in order to be able to comply with the mapped regulation in the various processes, that relevant legal expertise is available in all significant phases of the development process, e.g. when preparing specifications and design and when carrying out tests etc. I hereby refer to my article, 'How do we digitise without harming our legal certainty?' in the Ombudsman's report for 2019 and to the Ministry of Justice's memorandum of the 18 of November 2015 on administrative law requirements for the public sector's digital systems. See also the Agency for Public Digitalisation guide on digitisation-ready legislation (2018), p. 28, according to which: 'The introduction of digitally supported public administration requires that both development of systems, data flows, administrative s needs, proceedings and regulation are considered. If the application of legislation is to be supported digitally, the public authority must, therefore, map the legal requirements, i.e. the material and formal rules that a digital system must support. In this way, the public authority will be able to identify the elements of the regulatory framework at an early stage that may pose challenges for digitalised administration [...] I finally refer to Hanne Marie Motzfeldt and Azad Taheri Abkenar, Digital Forvaltning (2019), p. 81: It seems to be firmly supported by case law, administrative regulations and legislative indications that public authorities are responsible for and obliged to proactively ensure that technologies are designed and used in such a way that they enable and contribute to the affected administrations' compliance with administrative law and promote the principles of good administration.'*

As mentioned above, testing is considered a prerequisite for bringing a digital system into use in the Danish public administration. This has been stated in several opinions from the Parliamentary Ombudsman, most recently in FOB 2023-7. The background to FOB 2023-7 was an EU directive with an implementation deadline in December 2019. In 2018, the Danish Police realised that a new process-support and process-steering system for weapons registration was needed to implement the directive. Therefore, public procurement procedures were conducted in 2019, and a developer was chosen in the summer of 2020. In April 2022, the developer wrote to the police that the system: *'was taken in use the 17 of January 2022 due to the EU deadline. At this point, the structured test was not completed, and therefore, there were more flaws in the system than normally; several integrations were incomplete, some minor development tasks were not completed [...], and letters and forms necessary for case processing had not yet been set up in the solution [...] The system is, therefore, in a state where it only supports the case processing in PAC to a limited extent.'* The Parliamentary Ombudsman criticised that the system had been taken into use before the responsible public authorities had ensured that the system was able to provide sufficient support to the affected administration. He stated that it is very regrettable that the untimely implementation of the system had affected citizens negatively – natural and legal persons alike – by causing an unreasonably prolonged case processing time.

According to Danish administrative law, the testing procedures must be supplemented with measures ensuring an efficient implementation followed by steady supervision of the system and its use. Such measures will usually be instructions for and training of the case workers or other employees in using the system. Furthermore, routines and workflows should be established to ensure that flaws or deficiencies are continuously detected, identified and rectified.

4.5 The forthcoming AI act

4.5.1 Introduction

Agreement on a regulation on AI has recently been reached within the EU, although the final text has not yet been published.[51] According to the proposal set forth by the Commission in 2021, the overall purpose of the regulation is to establish a well-functioning market for AI within the EU via harmonised regulation. Furthermore, the regulation is to ensure that AI on the EU Market is safe and respects existing legislation, fundamental rights and the EU's values. In addition, the regulation is to ensure regulatory clarity in order to promote investment and innovation and enable effective enforcement.

Public bodies developing and using AI must comply with the regulation when the act enters into force. If the final text corresponds roughly to the EU Commission's proposal and the later published agreements from the trilogue proceedings there will be three steps in order to ensure compliance. As a first step, it must be examined whether the development, adaptation (change) or use of a given digital solution falls within the scope of the regulation. In this connection and for the sake of the further process, it will often be necessary – similarly to the GDPR – to identify the various actors. Next, the second step is to be a categorisation of the system's future, changed, or current use. As the third step, the respective provisions for unacceptable risk, high risk and limited risk must be complied with. For the Danish administration, however, it should ideally be considered as a fourth step whether any measures for systems with limited or low risk should be implemented.

Rather than giving a detailed presentation of the regulation based on the preliminary texts, the following section, 4.5.2, focuses on describing the basic structure of the proposal, after which the impact on Danish regulation is discussed in section 4.5.3.

4.5.2 The structure of the AI Act

The proposal for AI regulation rests on a risk-based approach, meaning that the requirements follow the risks assumed to be associated with the various uses of AI. The risk classification is based on the intended purpose of the systems rather than their functions. The specific purpose of and the particular modalities in the use of the system have thus been – and in the future will be – decisive for determining the risk categories.[52]

The scale of risks is closely linked to the purpose of the proposal, which aims to ensure that the beneficial potential of AI is realised while harmful effects on society and humans are prevented. Focus is not only the risk of a negative impact on individuals' fundamental rights regarding decisions directed at citizens. For example, the need for precision, safety and robustness is mentioned in connection with the risk of major shutdowns or incorrect treatment in the health and care sector.

51. https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai
52. The Commission's proposal to the European Parliament and the Council Regulation on harmonised rules for artificial intelligence (Artificial Intelligence Act) and on amending certain of the Union's legislative acts, COM(2021) 206 final, section 5.2.3.

Based on an overall assessment of the severity and probability of the possible damages, the AI Act will divide the use of AI systems into the following risk categories: Unacceptable risk, high risk, limited risk and low or minimal risk.

It is not likely that Danish administrative authorities will consider the use of AI, which will be viewed as an unacceptable risk to society and the rights of individuals. These are listed in section II of the draft regulation on prohibited practices with regard to AI, which, among other things, includes some instances of evaluation or classification of persons' credibility by public authorities. The prohibited use is evaluation or classification based on citizens' social behaviour, personal characteristics or personality traits. However, the ban only applies if one of the following additional conditions is met. Firstly, the use has to lead to harmful or unfavourable treatment of individuals or smaller or larger groups in a social context unrelated to the contexts in which the data were originally generated or collected. Secondly, the harmful or unfavourable treatment has to be unjustified or disproportionate in relation to their social behaviour or the seriousness thereof. In both cases, the prohibition applies regardless of whether the evaluation or classification is carried out by a public authority or by private companies on behalf of a public authority.

Contrary to the unacceptable risk systems, some so-called high-risk systems *are* likely to be used in the Danish public administration. In the proposed chapter 1 of the AI Act, two main categories were identified as posing a high risk to society and the fundamental rights of individuals.

Chapter 2 sets out the proposed requirements for establishing a risk management system as well as requirements for data and data management, technical documentation, registration, transparency, information, accuracy, robustness, and cyber security. The proposed Chapter 3 laid down obligations on the various actors, while Chapter 4 proposed an administrative framework, and Chapter 5 contained detailed provisions, e.g. standards, certificates and registration.

The first category of high-risk systems will probably only be relevant for public service when using different tools such as welfare tech, as this category is AI intended to be used as a security component in a product or is itself one product. The second category – are independent systems assessed to pose a high risk to human health and safety or fundamental rights.

Besides the areas of law enforcement and immigration, including border control, the most relevant high-risk systems for the Danish administration must be assumed to be, firstly, the management and operation of critical infrastructure. Secondly, the area of education and vocational training is relevant. Here, the proposal lists systems intended to grant access to or allocate places at educational institutions, evaluate students, or assess participants in tests that are typically required to gain access to educational institutions. Such systems are considered risky due to their potential impact on citizens' educational and working life courses and thus affect their ability to secure a livelihood. Thirdly, AI within employment, management of workers and access to self-employment are regarded as high risk if they are intended for recruiting or selecting candidates, making decisions about promotion and dismissal, assigning tasks, and monitoring and evaluating the performance and behaviour of persons in work-related contractual relationships. It is, however, also included that AI systems used to monitor employees can affect their right to data protection and right to privacy. Fourthly, and probably the most significant area, is access to and use essential public services and benefits. AI intended to assess people's eligibility for public social benefits and services and assign, reduce, cancel or revoke such benefits and services is considered high-risk. On the other hand, the use of AI in other areas to conduct control – of natural and legal persons alike – does not seem to be considered high risk unless the use can be considered law enforcement.

During the legislative process, supplementary provisions for AI systems that can be used for different purposes were added. Such AI is termed AI for general purposes. The background for introducing the specific provisions hereon was mainly the progress within language models such as ChatGPT. These will be subject to transparency requirements, including technical documentation, compliance with EU copyright law, and disseminating detailed summaries about the content used for training. For so-called high-impact models with systemic risk, further requirements will be applied.

For high-risk systems, comprehensive compliance procedures will be required to ensure risk mitigation, data governance, detailed documentation, human oversight, transparency, robustness, accuracy, and cybersecurity, as well as conformity assessments prior to being put in use and ongoing supervision after the system has been put into use.

Systems with limited risk include all systems – high risk and not high risk –e intended to interact with people, recognise emotions, carry out biometric categorisation, or generate or manipulate images, audio or video content. However, the obligation to ensure transparency will mainly be relevant to the Danish Public sector in connection with chatbots. Here, public authorities will be obliged to inform citizens that they are interacting with an AI system if it is not otherwise clear from the context.

The low-risk systems are not subject to regulation according to the AI Act. The proposed text from 2021 did, however, encourage codes of conduct.

4.5.3 The AI Act's potential impact on the Danish regulatory system

Today, all AI systems developed for and used in the Danish public sector are subject to the requirements laid down in administrative law and are thereby designed to support compliance with relevant regulations, including fundamental rights. Further, a good administration impact assessment has to be performed as AI systems are developed, and the systems are, as outlined above in section 4.4.3, to undergo testing before being taken into use and monitored during use. The national case law has also touched upon the criteria for selecting datasets for training as the Parliamentary Ombudsman in FOB 2021-22 pointed out that a 'data-driven tool' to support the valuation of used cars had to be developed in order to provide qualified assistance to caseworkers, which among other things, involved mapping the appeals body's case law for which data to use and how to weight the developed variables.

When the AI Act enters into force, comprehensive compliance procedures will be required for (only) high-risk systems in a regulatory model with significant similarities with Danish administrative law's proactive approach, according to which digital systems may only be used when it is ensured in advance that the systems support a compliant administration or data processing. Also similar to Danish administrative law is the requirement for ongoing supervision after the system is implemented.

At present, the purposes of the AI Act and the use of regulation as opposed to a directive suggest that no At present, the purposes of the AI Act and the use of regulation as opposed to a directive suggest that the ECJ will not accept additional compliance requirements imposed on AI systems under national law when the regulation takes effect. In other words, the AI Act might disrupt the carefully developed and balanced national regulation. However, it might be possible to regard the national norms of good administration as a code of conduct applying (only) to the public sector.

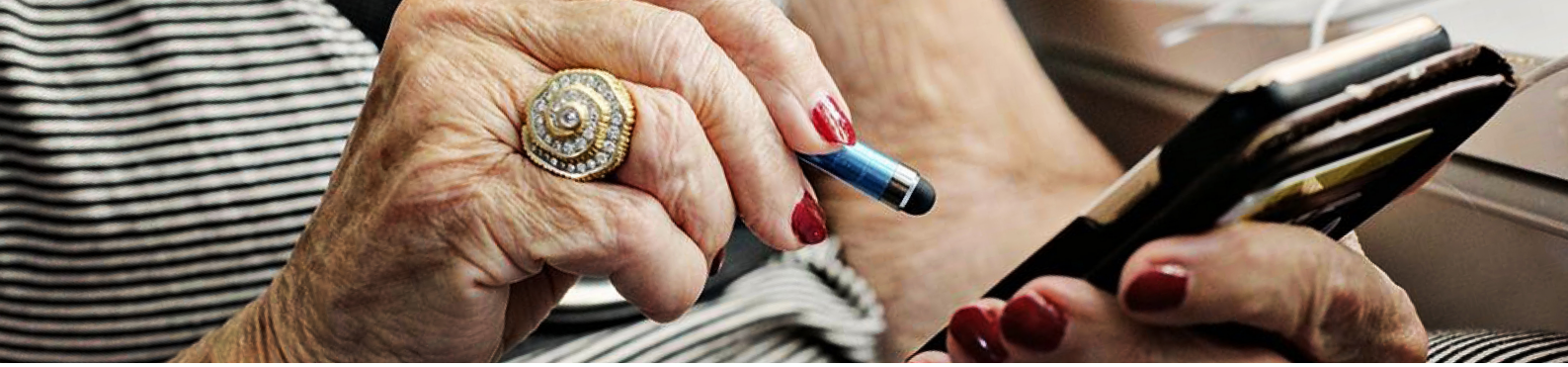
5. New and pressing challenges

As elaborated on in section 2, the traditional organisational and governance structures within the public administration in Denmark have been somewhat disrupted by digitalisation. First, process-support and process-steering digital systems are developed and maintained by private companies that are not subject to instructions unless set out in the contracts and are not under the regime of criminal and civil liability, which applies to public servants. In other words, the digital transformation has placed actors not bound by administrative law in a significant role in relation to the digital systems, which are indispensable for everyday administration, services, regulation and collection. Second, systems and databases have been increasingly connected across jurisdictions, further blurring the distribution of responsibilities and roles and establishing a new interdependence as one public body might be unable to perform its assigned tasks if one or more connected systems become inoperable.

The digital administration in Denmark has, as described above in section 3.2, been developed over decades. Most of the infrastructure, as well as the thousands of systems managing everything from learning activities in schools and other educational institutions to automated calculation and collection of income tax, was developed in what one might, in a dramatic tone, call a very different situation related to threats of cyberterror and crime. At the same time, the initiatives to strengthen information and cybersecurity in Denmark need to be more cohesive, which can be illustrated by the fact that the national cybersecurity strategy does not include the municipalities.[53] Further and in light of the high level of digitalisation in Denmark, the forthcoming EU regulation is hardly sufficient to raise the level of awareness and security – a concern that increases as the enforcement of the regulation seems to be somewhat superficial, probably because supervisory tasks have been fragmented into the various ministries.

In other words, as an overall conclusion, Denmark can benefit from stronger and closer Nordic-Baltic cooperation on regulatory issues related to public digitalisation. The most urgent theme – among the many – is probably regulation supplementing the EU's cyber- and information directives and regulations with private suppliers as subjects as well as the public bodies. While EU regulation may be relevant and adequate for the less digitalised countries within the EU, the high degree of digitalisation in the Nordic and Baltic countries necessitates further initiatives. Nordic-Baltic regulatory cooperation in information and cybersecurity might simultaneously increase the potential of systems developed in one of the Nordic-Baltic countries to be considered safe enough to be used in other countries.

53. https://en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/



ESTONIA

The Estonian e-state and challenges of regulating public sector digitalisation

Paloma Krõõt Tupay and Monika Mikiver

In collaboration with Sten-Marten Pukka and Marie Frosch

1. Introduction

According to § 3 of the Estonian Constitution, state power may be exercised only under the Constitution and laws in conformity with it. Therefore, the legal regulation and arrangement of the Estonian administration – including its digitalisation - must necessarily also be in accordance with the constitutional principles and the system of fundamental rights protection in Estonian law. With this in mind, chapter 2 of the analysis will first provide an insight into the legal framework of Estonian administration and its core principles. Following this, the reader is introduced to the cornerstones of Estonian digital administration and their regulation (section 3). Section 4 then deals with the following practical examples

Using various practical examples, chapter 4 then deals with the implementation of the principles of democracy and the rule of law, trust in public administration and respect for citizens' rights within the Estonian digital administration. Section 5 looks closer at the possible impact of the envisioned EU's AI Act on the Estonian administration.

Finally, based on the previous sections of the chapter, section 6 summarises the advantages and disadvantages of national legal regulations for digital administration. The concluding section also refers to the effect of EU law on the national regulation of digital administration.

2. Foundations of Estonian Public Administration

2.1 Constitutional principles and the system of protection of fundamental rights in Estonian law

2.1.1 The Estonian Constitution of 1992

The strenuous efforts of the Estonian independence movement to achieve the long-awaited restoration of the Republic of Estonia were finally rewarded on September 6, 1991, when, after more than 50 years of illegal occupation, the communist Soviet government was forced to recognise the independence of the Republic of Estonia. The new Constitution of the Republic of Estonia (EC) was adopted in the referendum on 28.06.1992 and came into force on 03 July 1992.[54]

The 1992 Constitution is built upon the idea of parliamentary democracy.[55] The Constitution states that Estonia is an autonomous and independent democratic republic, with supreme power vested in the people, and the parliament holds the legislative power.[56]

About the roots of the 1992 Constitution, one of the members of the Constitutional Assembly, Jüri Adams, stated: *'The current draft is based on the current German Constitution, as well as the Austrian Constitution. As far as possible, other Central European and Scandinavian countries have also been considered. This has been done deliberately, and the reason is that these countries are culturally close to us first and foremost, these societies and the way they think are psychologically close to us.'*[57] Inspiration was also taken from the previous Constitution of Estonia, adopted in 1938. Despite this, the authors of the Constitution decided to create an entirely new Constitution, not to carry over and modernise the previous one from 1938. The Constitution of 1992 can be described as "a perfect example" of a constitution being established after the fall of an authoritarian regime – it is fully binding and enforceable in courts.[58]

The Constitution of Estonia contains approximately 6700 words, making it a relatively compact constitution.[59] Therefore, concretising its content through legal practice and studies is particularly important, as the concise text regulates general principles but rarely the application of the Constitution to individual cases.

Due to its relatively complex formal amendment procedure, the Estonian Constitution is generally considered difficult to amend.[60] Due to this, there have been only five amendments so far.[61] As there is also political caution towards formal constitutional amendments, the interpretation and substantive change of the Estonian Constitution has therefore played an increasingly important role in its validity.[62]

---

54. National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law / Albi, Anneli; Bardutzky, Samo. The Constitution of Estonia: The Unexpected Challenges of Unlimited Primacy of EU Law / Ernits, Madis. Section 1.1. The Hague: T.M.C. Asser Press, 2019. p. 889.
55. The Constitution of the Republic of Estonia. Annotated Edition 2020, Introduction, par. 24. Available at: https://pohiseadus.ee.
56. The Constitution of the Republic of Estonia, paragraph 1 and 59.
57. The protocols of the Constitutional Assembly, 4. session, 04.10.1991. words of Adams, Jüri. Available at: https://www.riigikogu.ee/wpcms/wp-content/uploads/2015/03/4.-istung.pdf.
58. National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law / Albi, Anneli; Bardutzky, Samo. The Constitution of Estonia: The Unexpected Challenges of Unlimited Primacy of EU Law / Ernits, Madis. Section 1.1. The Hague: T.M.C. Asser Press, 2019. p. 889
59. Põhiseaduse muutmine ja muutused põhiseaduses. (Changing the Constitution and changes in the Constitution.) / Lõhmus, Uno. In: Juridica, The journal of Tartu University faculty of Law, No. 2011/1, p. 17.
60. Põhiseaduse muutmine ja muutused põhiseaduses. (Changing the Constitution and changes in the Constitution.) / Lõhmus, Uno. In: Juridica, The journal of Tartu University faculty of Law, No. 2011/1, p. 12, p. 19.
61. The Constitution of the Republic of Estonia, Preamble, par. 20.
62. Verfassung und Verfassungsänderung in Estland: eine Analyse zu Theorie und Praxis mit vergleichenden Anmerkungen zum deutschen Recht. (Constitution and constitutional change in Estonia: an analysis of theory and practice with comparative notes on German law). Tupay, Paloma Krõõt, Vol. 22. BWV Verlag, 2015. p. 265 f.

The most impactful amendment to the 1992 Constitution was adopted to enable Estonia to join the European Union (EU). The respective working group of the parliament decided in 2002 not to change the text of the 1992 Constitution but to create a new additional legal act ensuring conformity of Estonian law with EU law called the Constitution of the Republic of Estonia Amendment Act (CEAA). The CEAA is a constitutional act with the same legal force as the Constitution.[63] It was passed by referendum and contains the stipulations of joining the European Union, withholding four paragraphs.[64] According to the first paragraph of the law, Estonia can be a member of the EU as long as the fundamental principles of the EC are respected. The act's second paragraph states that as long as Estonia is a member of the EU, the EC will be applied considering the rights and obligations arising from the Accession Treaty.[65] This broad formulation has given the court a significant role in assessing – i.e., interpreting – the conformity of Estonian law with EU law.

As a result, many significant changes to the EC are not based on formal changes in the constitution's text but on the interpretation of the Constitution based on the CEAA.[66]

2.1.2 Core principles and values of the Estonian Constitution

According to the court's interpretation of the Estonian Constitution and legal practice, the core principles and values of the Constitution are human dignity, democracy, the rule of law, the social state, and national identity.[67] All but the principle of a national identity, which can be deducted, i.a., from the EC's preamble, are found in § 10 of the Constitution of Estonia.

Similarly to the list of core principles, the list of human rights enumerated in chapter two of the Estonian Constitution is not delimited by a *numerus clausus* rule.[68] EC § 10 states explicitly that the Constitution's fundamental rights may be expanded and supplemented by new ones that follow the Constitution's spirit and correspond to the principles of human dignity, the welfare state, and the democratic rule of law.

2.1.2.1 Human dignity

The Supreme Court of Estonia (ESC) has stated that human dignity *'is the basis of all fundamental rights of the person and the purpose of the protection of fundamental rights and freedoms.'*[69] Human dignity is determined in the Estonian Constitution as a fundamental right (EC § 18), but additionally, it is referred to as one of the core principles of the Estonian Constitution.[70]

According to the ESC: *'in a human-centred society, in situations of conflict of fundamental rights, the least limitation may be placed on human dignity - a complex fundamental right, the elements of which are, in particular, the right to a good name, the right not to fear for the existence of oneself and of one's loved ones, the right to legal equality with all other human beings, the right to a human identity, the right to informational self-determination, the right to physical integrity.'*[71]

---

63. This conclusion can be drawn from the CEAA § 3 which states that CEAA can only be changed by a referendum, putting it on the same level with EC in the hierarchy.
64. The Constitution of the Republic of Estonia. Annotated Edition 2020, paragraphs 1-4. Available at: https://pohiseadus.ee.
65. Pursuant to § 3 of the CEAA, amendments to the CEAA are subject to a referendum. Section 4 of the CEAA is a legally required provision, which states that amendments to the CEAA be made within a period of at least three months before they come into force. Available at: https://www.riigiteataja.ee/akt/631119.
66. See for more information A. Laurand. PSTS. Sissejuhatus. – U. Lõhmus (peatoim.). Eesti Vabariigi põhiseaduse kommentaarid (Annotations to the Estonian Constitution). Eesti Teaduste Akadeemia Riigiõiguse Sihtkapital. 2023. Available at: https://pohiseadus.riigioigus.ee/v1/eesti-vabariigi-pohiseaduse-taiendamise-seadus/pohiseaduse-taiendamise-seaduse-kommentaar.
67. The Constitution of the Republic of Estonia. Annotated Edition 2017, paragraph 10. Available at: https://arhiiv-2017.pohiseadus.ee/. pt. 5.
68. The Constitution of the Republic of Estonia. Annotated Edition 2017, paragraph 10. Available at: https://arhiiv-2017.pohiseadus.ee/. pt. 1.
69. RKHKo 22.03.2006, 3-3-1-2-06, pt. 10. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-3-1-2-06.
70. The Constitution of the Republic of Estonia. Annotated Edition 2017, paragraph 10. Available at: https://arhiiv-2017.pohiseadus.ee/. pt. 18.
71. RKKKo 26.08.1997, 3-1-1-80-97, pt. I. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-1-1-80-97.

2.1.2.2 Democracy

The General Assembly of the ESC considers that *'the democratic nature of the Estonian system of state governance is a very important constitutional principle'*[72], and even more so, *'democracy is one of the most important principles of the Estonian system of state-building'*.[73]

The core of the principle of democracy can be found in EC § 1, which states: *'Estonia is an independent and sovereign democratic republic wherein the supreme power of the state is vested in the people. The independence and sovereignty of Estonia are timeless and inalienable.'*[74] That implies the weight of the principle of democracy in the EC, stating that the whole constitution and the governance of the state rely upon it.

EC's third chapter regulates the two ways the people of Estonia can exercise their supreme power – the right to vote by electing the parliament and the right to vote through referenda.[75] However, possibilities for direct democratic participation are sparse and generally do not play a significant role in the Estonian state organisation.

2.1.2.3 Rule of law

The EC explicitly mentions the rule of law only in its § 10, which states that none of the fundamental rights can contradict the principle of the rule of law. However, the rule of law principle can be derived from the preamble to the Constitution and many other paragraphs of the Constitution. I.a. EC § 13 section 2 states that the law shall protect everyone from the arbitrary exercise of state power, and according to EC § 14, it is the duty of the legislature, the executive, the judiciary, and the municipalities to guarantee the protection of personal rights and freedoms. According to the ESC, the principle of the rule of law can be defined as follows: *'the content, scope, and manner in which state authority functions.'*[76]

According to § 10 of the EC, the fundamental rights mentioned in the second chapter of the EC can't contradict the principles of human dignity, social justice, and the democratic rule of law.[77] This means that Estonia is governed by general law principles recognised in the European judicial area.[78] Under the Constitution, one of the basic features of a state based on the rule of law is the guarantee of fair and effective protection of the rights of persons. Therefore, the fairness and efficiency of judicial proceedings presuppose their conformity with the procedural principles laid down in the Constitution. In Estonia, the universal right of access to justice is considered a fundamental right and a centrepiece of the rule of law.[79]

2.1.2.4 Welfare state

The welfare state principle consists of several different aspects. First, this principle requires that the public authorities take care of the needy members of society and leave no one in need.[80]

Secondly, the social state principle requires a commitment to social cohesiveness and sharing social responsibilities.[81] The welfare state requires public authorities to advance citizens' economic and social well-being, even if a minimum standard of living is already guaranteed.[82]

---

72. RKÜKo 01.07.2010, 3-4-1-33-09, pt. 52. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-33-09.
73. RKÜKo 01.07.2010, 3-4-1-33-09, pt. 67. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-33-09.
74. The Constitution of the Republic of Estonia, paragraph 1.
75. The Constitution of the Republic of Estonia, paragraph 56.
76. RKÜKo 12.07.2012, 3-4-1-6-12, pt. 132. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-6-12.
77. The Constitution of the Republic of Estonia, paragraph 10.
78. RKPJKo 17.02.2003, 3-4-1-1-03, pt. 14. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-1-03. Further information on the basis of the reference comes from the case of III-4/A-5/94 in 1994, where the ESC found: "In addition to the Constitution, the general principles of Estonian law must also take into account the general principles of law developed by the Council of Europe and the European Union. These principles are derived from the general principles of law of the Member States with a developed legal culture.". Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-1-03.
79. The Constitution of the Republic of Estonia. Annotated Edition 2020, paragraph 10, com. nr. 58. Available at: https://pohiseadus.ee.
80. The Constitution of the Republic of Estonia. Annotated Edition 2020, paragraph 10, pt. 21. Available at: https://pohiseadus.ee.
81. The Constitution of the Republic of Estonia. Annotated Edition 2020, paragraph 10, pt. 22. Available at: https://pohiseadus.ee.
82. The Constitution of the Republic of Estonia. Annotated Edition 2020, paragraph 10, pt. 22. Available at: https://pohiseadus.ee.

The social state principle includes setting up a social security system, providing pensions and allowances, ensuring education and universal schools, providing medical care, and many more.[83]

Although the Constitution does not define the social state principle, it is reflected in different fundamental rights. For example, the EC's § 12 prohibits discrimination based on social circumstances. The Supreme Court of Estonia has placed particular emphasis also on EC § 28,[84] which gives everyone the right to the protection of health and assistance in the case of need: *'The social state and the protection of social rights include the idea of assistance and care for those who are unable to provide for themselves adequately. The human dignity of these persons would be diminished if they were deprived of the assistance they need to meet their basic needs.'* [85] That wording only amplifies the fact that the core values of the Constitution of Estonia are deeply interconnected, shaping the basis of the Estonian Constitution.

2.1.2.5 National identity

The preamble to the EC requires, among other things, that the Estonian state guarantees the protection of internal peace and the preservation of the Estonian nation.[86] From this and the Supreme Court's legal practice,[87] Estonian legal scholars have derived the preservation of national identity as one of the EC's core values.[88]

2.1.3 The Estonian Legal Architecture of Human Rights Protection

2.1.3.1 International treaties and institutions

Estonia has made constant efforts to provide an increasingly comprehensive human rights protection. Estonia acceded to the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social, and Cultural Rights in 1991.[89] Estonia signed the Rome Statute in 1999 and deposited its instrument of ratification in 2002.[90] In 1996, Estonia ratified the European Convention on Human Rights.[91] Estonia is a member of the Organisation for Economic Cooperation and Development, the Council of Europe, and the European Union.[92] Estonia has become party to many international conventions and protocols, such as the Convention on the Rights of Persons with Disabilities (CRPD, 2012) and its Optional Protocol (OP-CRPD, 2012), the Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict (OP-CRC-AC, 2014) and Council of Europe Convention on Action against Trafficking in Human Beings in 2015. Estonia also ratified the Kampala Amendments to the Rome Statute of the International Criminal Court in 2013; the Council of Europe Convention on Action against Trafficking in Human Beings in 2015; the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (also known as the Istanbul

---

83. The Constitution of the Republic of Estonia. Annotated Edition 2020, paragraph 10, pt. 22-24. Available at: https://pohiseadus.ee.
84. RKPJKo 09.12.2019, 5-18-7/8, pt. 119. Available at: https://www.riigikohus.ee/et/lahendid/marksonastik?asjaNr=5-18-7/8.
85. RKUKo 21.01.2004, 3-4-1-7-03, pt 31. Available at: https://www.riigikohus.ee/et/lahendid/marksonastik?asjaNr=3-4-1-67-13.
86. The Constitution of the Republic of Estonia. Annotated Edition 2020, preambul (preamble), chapter about 1992. Available at: https://pohiseadus.ee.
87. Decisions of the ESC discussing questions of national identity: RKPJK 05.02.1998, 3-4-1-1-98, pt. II. Available at: https://www.riigikohus.ee/et/lahendid/?asjaNr=3-4-1-1-98; RKPJK 04.11.1998, 3-4-1-7-98, pt. III, IV. Available at: https://www.riigikohus.ee/et/lahendid/?asjaNr=3-4-1-7-98; RKPJK 03.05.2001, 3-4-1-6-01, pt. 9. Available at: https://www.riigikohus.ee/et/lahendid/?asjaNr=3-4-1-6-01.
88. Eesti õiguskorra „DNA" ja põhikorra tuum (The "DNA" of the Estonian legal system and the core of the constitution). Ernits, Madis. In: Juridica 4–5/2023, p. 284; Põhiõigused, demokraatia, õigusriik (Fundamental rights, democracy, rule of law). Ernits, Madis. Ch. 1. Tartu: Tartu Ülikooli Kirjastus, 2011. p. 67.
89. UN Treaty Body Database. Available at: https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Countries.aspx?Lang=en.
90. International Criminal Court. The States Parties to the Rome Statute. Eastern European States. Available at: https://asp.icc-cpi.int/states-parties/eastern-european-states/estonia#:~:text=Estonia%20signed%20the%20Rome%20Statute,Statute%20on%2030%20January%202002.
91. European Court of Human Rights. Press Country Profile. Estonia. Available at: https://www.echr.coe.int/documents/d/echr/cp_estonia_eng.
92. UN Human Rights Council, Working Group on the Universal Periodic Review Tenth session : Estonia, November 2010, A/HRC/WG.6/10/EST/1. Available at: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/WG.6/10/EST/1&Lang=E, p. 2, 5.

Convention);[93] the Council of Europe Convention on preventing and combating violence against women and domestic violence (also known as the Istanbul Convention); the Protocol of 2014 to the ILO Forced Labour Convention adopted in 1930 and the amendments to Article 8 of the Rome Statute regarding the jurisdiction of the ICC over the crime of aggression.[94] Estonia was also a member of the Human Rights Council from 2012–2015.[95]

Although discussed, as of 2023, Estonia has not ratified the UNESCO Convention against Discrimination in Education and the International Convention for the Protection of All Persons from Enforced Disappearance.[96][97] Estonia has also not ratified the Convention on the Reduction of Statelessness[98] because Estonia has established alien passports for foreigners who have a valid Estonian residence permit or right of residence and who do not have and cannot obtain a travel document from a foreign country.[99][100]

2.1.3.2 Estonian national legislation and institutions

Chapter II of the Estonian Constitution protects and lists fundamental rights, freedoms, and duties. The ECHR greatly influenced Chapter II of the Constitution and held a significant role in the drafting of Chapter II. The significance of the ECHR regarding the Estonian Constitution has also been stipulated by the Supreme Court, which has stated that national laws must also take into account the principles of the ECHR and that the Constitution must be interpreted in a way that ensures that its application is consistent with the ECHR and its application practice or else adequate national protection of individual rights would not be provided.[101] In the same chapter, the Constitution has a significant paragraph that allows the fundamental rights protected by the Constitution to progress and evolve. § 10 of the Constitution of the Republic of Estonia stipulates that *'the rights, freedoms, and duties set out in this Chapter shall not preclude other rights, freedoms, and duties which arise from the spirit of the Constitution or are in accordance in addition to that and are in conformity with the principles of human dignity and a social and democratic state governed by the rule of law.'*[102] § 10 EC is called the development clause. The purpose of § 10 is to expand the fundamental legal protection of individuals. The term 'development clause' is intended to show that fundamental rights are constantly capable of development and open to expansion and that fundamental rights must not be treated as something immutable. Additionally, the basic principles of the Constitution are stipulated in § 10. The development clause shows that the interpretation of the Constitution can change over time, and new provisions can also be added. The development clause is necessary when values evolve over time, which makes it possible to include new values in the protection area of an existing fundamental right or create a new one. The purpose of the development clause is to enable the existence of rights and obligations that are not clearly stated in the Constitution.[103]

Estonia adopted a separate Equal Treatment Act in 2009. Another significant effort made by Estonia was adopting and implementing the Strategy for Guaranteeing the Rights of Children 2004–2008. To combat the trafficking of human beings, Estonia established a functioning

93. UN Human Rights Council, Working Group on the Universal Periodic Review Twenty-fourth session : Estonia, 28 December 2015, A/HRC/WG.6/24/EST/1, available at: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/ HRC/WG.6/24/EST/1&Lang=E., p. 2.)
94. UN Human Rights Council, Working Group on the Universal Periodic Review Thirty-eighth session: Estonia, February 2021, A/HRC/WG.6/38/EST/1, p. 2. Available at: https://undocs.org/en/A/HRC/WG.6/38/EST/1.
95. UN Human Rights Council, Working Group on the Universal Periodic Review Twenty-fourth session : Estonia, 28 December 2015, A/HRC/WG.6/24/EST/1, p.2. Available at: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/WG.6/24/EST/1&Lang=E.
96. Status of Ratification Interactive Dashboard. Available at: https://indicators.ohchr.org/.
97. Conventions ratified. Available at: https://www.unesco.org/en/countries/ee/conventions.
98. Convention on the Reduction of Statelessness. Available at: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=V-4&chapter=5&clang=_en.
99. Alien's passport for an adult. Available at: https://www.politsei.ee/en/instructions/alien-s-passport-for-an-adult.
100. A full list of all human rights conventions that Estonia is a member of can be found on the Ministry of Foreign Affair's webpage: https://www.vm.ee/tegevus/inimoigused/inimoigused-valispoliitikas .
101. RKPJKo 25.03.2004, 3-4-1-1-04, pt. 18. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-1-04.
102. The Constitution of the Republic of Estonia, paragraph 10.
103. The Constitution of the Republic of Estonia. Annotated Edition 2020, paragraph 10. Available at: https://pohiseadus.ee/.

domestic cooperation network on human trafficking. It was created within the first Development Plan for Combating Trafficking in Human Beings 2006–2009.[104] Estonia has also implemented the Registered Partnership Act and amended the Citizenship Act, ensuring that children born in Estonia to parents with undetermined citizenship have the right to acquire Estonian citizenship through naturalisation.[105] On 19 June 2023, the *Riigikogu* passed an Act enabling gender-neutral marriage in Estonia starting from 1 January 2024.[106]

One of the most significant institutions ensuring the protection of constitutional rights in Estonia is the Chancellor of Justice, *'an independent official who shall review the acts of general application of the legislature and the executive and of municipalities for conformity with the Constitution and laws.'*[107] The Chancellor of Justice, established in 1993, was in 1999 also entrusted by the legislator with an additional 'ombudsman' task, intrusting in the office to supervise that state authorities guarantee fundamental rights as well as the principle of good administration and oversee local government agencies and bodies, legal persons in public law and private persons performing public functions.[108] The Chancellor of Justice has also been assigned over time with the duties of the national preventive mechanism stipulated in the Optional Protocol to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. This means that the Chancellor of Justice is also responsible for checking institutions where people's freedoms are being restricted to ensure that no torture or cruel or degrading treatment takes place. The Chancellor of Justice also acts as the institution of children's ombudsman and is responsible for supervising compliance with fundamental rights when executive power agencies gather, process, use, and supervise personal data. The Chancellor of Justice is responsible for promoting the implementation, upholding, and monitoring of the Convention on the Rights of Persons with Disabilities, guaranteeing the fundamental rights protection of disabled persons and holds the role of the national human rights institution (NHRI) in Estonia.[109] An Advisory Committee on Human Rights has been set up by the Chancellor, which advises the Chancellor in promoting, protecting, and monitoring human rights. Besides the Chancellor of Justice, the Minister of Foreign Affairs appointed a diplomatic representative with a unique human rights and migration mandate in 2020.[110]

2.1.3.3 The principle of good administration

After regaining independence, the Estonian administrative procedure lacked harmonised regulation and was characterised by eclectic and fragmented laws.[111] Although already in 1992, scholars of the University of Tartu developed a list of public legal acts "a proper state must have", drafting the Administrative Procedure Act began only in 1996.[112] The scholars recommended elaborating Estonian public law along the lines of the German and Austrian legal systems, warning however against copying other countries' laws.[113] The administrative law reform aimed

104. UN Human Rights Council, Working Group on the Universal Periodic Review Tenth session : Estonia, 8 November 2010, A/HRC/WG.6/10/EST/1, p.20. Available at: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/WG.6/10/EST/1&Lang=E.
105. UN Human Rights Council, Working Group on the Universal Periodic Review Twenty-fourth session : Estonia, 28 December 2015, A/HRC/WG.6/24/EST/1, p. 6,16-17. Available at: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/WG.6/24/EST/1&Lang=E.
106. Draft act for the The Act on Amendments to the Family Law Act Other Acts 207 SE. Available at: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5fcbb8fd-b3d9-47a4-b5c1-ed9959bf0c9c/perekonnaseaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus.
107. The Constitution of the Republic of Estonia, paragraph 139.
108. Õiguskantsler (Chancellor of Justice). / Ernits, Madis. In: Juridica 1/2003, p.21; UN Human Rights Council, Working Group on the Universal Periodic Review. Tenth session: Estonia, 8 November 2010, A/HRC/WG.6/10/EST/1, p.4. Available at: http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/WG.6/10/EST/1&Lang=E,.
109. History of the institution. Available at: https://www.oiguskantsler.ee/en/history-institution.
110. UN Human Rights Council, Working Group on the Universal Periodic Review Thirty-eighth session: Estonia, 16 February 2021, A/HRC/WG.6/38/EST/1, p.3. Available at: https://undocs.org/en/A/HRC/WG.6/38/EST/1.
111. Õigusriigi taastamine. Eesti seaduste ja institutsioonide reformid 1992-2002 (Restoring the rule of law. Reforms of Estonian laws and institutions 1992-2002) / Sein, Karin; Ristikivi, Merike. Tartu: Tartu Ülikooli Kirjastus, 2022. p. 87.
112. Õigusriigi taastamine. Eesti seaduste ja institutsioonide reformid 1992-2002 (Restoring the rule of law. Reforms of Estonian laws and institutions 1992-2002) / Sein, Karin; Ristikivi, Merike. Tartu: Tartu Ülikooli Kirjastus, 2022. p. 90.
113. Haldusõiguse üldosa reform Eesti Vabariigis 1990. aastate teisel poolel (Reform of the general part of administrative law in the Republic of Estonia in the second half of the 1990s) / Usk, Marge-Reet. In: Juridica 1/2023, p. 70.

'to create drafts that meet the best European standards on the one hand, and take into account the local conditions in Estonia on the other'.[114] These reforms were designed i.a. with the help of several German scholars.[115] As a result, five critical pieces of legislation were drafted. They later adopted: 2002 the Administrative Procedure Act, the State Liability Act, the Substitutive Enforcement and Penalty Payment Act, the 2003 Administrative Co-operation Act and in 2014, the Law Enforcement Act entered into force. All of these legal acts, apart from the Administrative Co-operation Act, are based on pan-European general principles of good administration and general concepts derived from the Committee of Ministers (CM) recommendations.[116]

The Estonian Supreme Court has derived a person's right to good administration from § 14 EC, which states that the protection of individual rights and freedoms is the duty of the legislature, executive, judiciary, and municipalities and considers it to be a fundamental right as well as a constitutional principle.[117] The main ideas of the principle of good administration can also be found in § 5(2) of the Administrative Procedure Act, according to which *'administrative procedure shall be purposeful, efficient and straightforward and conducted without undue delay, avoiding superfluous costs and inconveniences to persons.'*[118] The explanatory memorandum of the draft of the Civil Service Act emphasises that the Civil Service Act aims to ensure efficient, flexible, open, transparent and sustainable public services and competent, reliable, result-oriented and motivated officials.[119] Also, the Civil Service Act's § 12 foresees the establishment of a Council of Ethics of Officials, whose task is to reinforce officials' core values and ethics.

In addition to legislation, a code of ethics for public service[120] has been drawn up, which consists of 20 general principles that deal with the role and aims of Estonian public service and public servants' professional qualities, personal characteristics and duties.[121] The Estonian Code is based on the fundamental values of the public service of OECD countries, such as impartiality, legality, transparency, honesty, efficiency and expertise.[122]

In cases of maladministration, the Chancellor of Justice has been given the power to provide (non-binding) recommendations and suggestions to the administration to ensure that good administrative practice is put into practice. Therefore, the law foresees that *'everyone has the right of recourse to the Chancellor of Justice to have their rights protected by way of filing a petition to request verification whether or not a state agency, a self-governing agency or body, a legal person in public law or a natural or legal persons in private law performing public duties observes the principles of ensuring the fundamental rights and freedoms and good administrative practice.'*[123] The Chancellor of Justice may also assess compliance with good administrative practice on his or her own initiative.[124] One essential aim of the development of good administration in Estonian law has been to ensure that the supervision of the Chancellor of Justice extends to the entire public sector, which includes supervision of the legality of the exercise of public power and the quality of public services. Today, the Chancellor of Justice's

114. Academica 2013 konverents. IV teemablokk – Eesti haldusõiguse üldosa reformist 1995–2001. Eesti haldusõiguse üldosa määratlusest ja reformist. (Academica 2013 Conference. IV thematic block - the reform of the general part of Estonian administrative law 1995–2001. On the definition and reform of the general part of Estonian administrative law) / Loot, Heiki. Tartu, 24.10.2013. Available at: https://www.uttv.ee/naita?id=18304.
115. Professors of law Holger Schwemer, Ulrich Ramsauer, Friedrich Schoch; see: M.-R. Usk. Op. cit, p.62.
116. Good Administration and the Council of Europe. Law, Principles, and Effectiveness. / Stelkens, Ulrich; Andrijauskaité, Agné. 1 ed. Oxford University Press, 2020. p. 546-547.
117. RKPJKo 17.02.2003, 3-4-1-1-03, pt. 12, 14. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-1-03.
118. Administrative Procedure Act, paragraph 5(2). Available at: https://www.riigiteataja.ee/akt/103022023014.
119. Explanatory memorandum to the draft Civil Service Act (193 SE), p. 3. Available at: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/c99b9c50-6462-4182-a6ce-d182400e1bae/avaliku-teenistuse-seadus.
120. Civil Service Act, paragraph 12. Available at: https://www.riigiteataja.ee/akt/130062023018.
121. AMETNIKU EETIKAKOODEKS (CODE OF ETHICS FOR OFFICIALS). Available at: https://www.fin.ee/riigihaldus-ja-avalik-teenistus/avalik-teenistus/eetika.
122. Tuntud või tundmatu hea halduse põhimõte. (A known or unknown principle of good administration.) / Allikmets, Sille. In: Juridica 2014/3, p. 228.
123. Chancellor of Justice Act, paragraph 19. Available at: https://www.riigiteataja.ee/akt/126052020011.
124. Chancellor of Justice Act, paragraph 34(1).

Office issues recommendations to administrative bodies to ensure the quality of law-making, administrative practice, and citizens' awareness of fundamental rights.[125]

2.2 Legal Organisation of Estonian Public Administration

In the context of the restoration of statehood and the development of market economy relations, it was necessary to initiate massive changes at all three levels of public administration, i.e. at the state, county and municipality levels. In preparation for this, the Law on the Fundamentals of Local Self-Government was adopted already in 1989,[126] and the first elections to local government councils after WW II were held on 10 December 1989,[127] i.e. already before Estonia's formal regaining of independence in 1991.

The Constitution of the Republic of Estonia of 1992 and the first elections to the Estonian Parliament (*Riigikogu)* on 20 September 1992 made it possible to start creating a system of effective democratic public administration. The reformed Act on the Government of the Republic of 1996 created the legal basic framework for today's state administrative organisation, i.e. strong ministries to shape policymaking in their respective areas of responsibility and government institutions to implement this policy in their area of governance.[128] In 1996, the Civil Service Act entered into force, which provided for the establishment of a system of civil service.[129]

The period from 2000 is considered the next significant period in the legal development of Estonian public administration when discussions on a possible administrative reform coincided with the elaboration of the general part of administrative law and Estonia's accession to the European Union. Due to this, the reform process was accompanied by the need to demonstrate Estonian administrative capacity and the ability to effectively apply the acquis communautaire, which led to several organisational changes. The administrative reform, as well as the general part of administrative law, aimed at a citizen-oriented public administration and *'delineation and specification of the roles of government institutions and strategy management to optimise the division of labour and cooperation between institutions'*.[130] Many offices, inspectorates and subordinate agencies were reorganised, and privatization of public sector entities increased.[131]

3. Digitalization of Estonian Administration

3.1 Political and Legal Development of the Estonian e-State

3.1.1 Key stages in the development of the Estonian e-state

Already during Soviet times, in 1950 and 1960, the Estonian Academy of Sciences founded the Institute of Cybernetics (IoC) in Tallinn, which researched fields ranging from speech synthesis, mathematical methods, economic cybernetics, automated control systems, and artificial intelligence to linguistic cybernetics, physics, chemistry and architectural modelling.[132]

125. Allar Jõksi ettekanne avaliku sektori teenindusfoorumil 16.06.2004 Tallinnas (Allar Jõks' presentation at the public sector service forum on 16.06.2004 in Tallinn). Available at: https://www.oiguskantsler.ee/et/oiguskantsler/suhted-avalikkusega/koned/avaliku-sektori-teenindusfoorum-2004.
126. Law on the Foundations of Local Self-Government of the Estonian SSR (10.11.1989).
127. Explanatory memorandum on the basis for the development of public administration (1998), p. 3. Available at: https://haldusreform.fin.ee/static/sites/3/2012/09/1999_avaliku-halduse-arendamise-aluste-seletuskiri.pdf.
128. Valikud Eesti haldusorganisatsiooni loomisel (Options for the creation of an Estonian administrative organisation) / Taro, Külli, Parrest, Nele in: Juridica, 2014/10, p 717.
129. Civil Service Act 1996. Available at: https://www.riigiteataja.ee/akt/13276914.
130. See for more information K.Taro, N.Parrest, p 718.
131. See for more information K.Taro, N.Parrest, p 719.
132. The Estonian Information Society Developments Since the 1990s. Kalmet, Tarmo. 2007. no 29 PRAXIS publication 10, p. 21. Available at: https://www.praxis.ee/wp-content/uploads/2014/03/2007-Estonian-information-society-developments.pdf.

When the country regained independence, the traces of Soviet occupation left were immense. The economy was on its knees, and the state system was in ruins.[133] The whole state administration system needed to be rebuilt from the ground up, which is a plus, as the new solution can be innovated from a fresh and clean slate without hindrance from the former bureaucracy. Estonia was an impoverished country in the beginning of the nineties, with an average monthly income of 30 dollars in 1992.[134] As resources were limited, and the challenge was huge, solutions to get the country back on its feet again needed to be innovative and proficient. This brought about the idea of an information society.

In 1994, the first step was taken by the Estonian parliament. The parliament framed the first draft of the 'Principles of Estonian Information Policy', containing the ways to conquer the critical topics arising from a new and fast-evolving information society.[135]

One major next step towards modernisation and digitalisation was launching the so-called Tiger Leap Initiative in 1996. It aimed to equip Estonian schools with information and communication technology and provide the knowledge of how to use it.[136] The primary goal of the Tiger Leap Initiative was to introduce computers and internet connectivity into schools across Estonia. The initiative aimed to provide equal opportunities for all students to access technology and digital resources, regardless of their location or socioeconomic background.

In 1998, the Estonian parliament formally adopted the 'Principles of Estonian Information Policy', designating the following three main aims.[137] The first was the modernisation of legislation given an effective and functioning information society.[138] The second topic was supporting the development of the private sector. The aim was the creation of incentives for private sector actors to gain their interest in building the information society. Examples of measures used were tax incentives and subsidies.[139] The third aim was to enhance interaction between the state and citizens by raising awareness and informing people of the developments and possibilities of IT solutions.[140]

Today's achievements are characterised by the successful cooperation of information and communication technologies and the effective implementation of the ideas and interests of the private sector right from the start, in the 90s particularly in the form of Scandinavian telecoms and credit institutions.[141] Electronic and Internet banking emerged in Estonia at an unusually early stage - the first electronic banking solution was introduced in Estonia as early as 1993, while Internet banking services were first offered worldwide in 1995.[142] Banks have also played an important role as providers of authentication mechanisms, which public sector organisations started to use to access their e-services.[143]

---

133. Estonia, the Digital Nation - Reflections of a Digital Citizen's Rights in the European Union. Tupay, Paloma Krõõt, p.2. Available at: https://www.lexxion.eu/wp-content/uploads/2020/07/EDPL_Estonia_extended.pdf.
134. Estonia, the Digital Nation - Reflections of a Digital Citizen's Rights in the European Union. Tupay, Paloma Krõõt, p.2. Available at: https://www.lexxion.eu/wp-content/uploads/2020/07/EDPL_Estonia_extended.pdf.
135. The Estonian Information Society Developments Since the 1990s. Kalmet, Tarmo. 2007. no 29 PRAXIS publication 10, p.10. Available at: https://www.praxis.ee/wp-content/uploads/2014/03/2007-Estonian-information-society-developments.pdf.
136. The Estonian Information Society Developments Since the 1990s. Kalmet, Tarmo. 2007. no 29 PRAXIS publication 10, p.20. Available at: https://www.praxis.ee/wp-content/uploads/2014/03/2007-Estonian-information-society-developments.pdf.
137. The document (in Estonian) can be found at the homepage of the State gazette (n 10). Available at: https://www.riigiteataja.ee/akt/75308.
138. The document (in Estonian) can be found at the homepage of the State gazette (n 10), pt. 17. Available at: https://www.riigiteataja.ee/akt/75308.
139. The document (in Estonian) can be found at the homepage of the State gazette (n 10), pt. 13 and 15. Available at: https://www.riigiteataja.ee/akt/75308.
140. The document (in Estonian) can be found at the homepage of the State gazette (n 10), pt. 11 and 28. Available at: https://www.riigiteataja.ee/akt/75308.
141. The Estonian Information Society Developments Since the 1990s. Kalmet, Tarmo. 2007. no 29 PRAXIS publication 10. Available at: https://www.praxis.ee/wp-content/uploads/2014/03/2007-Estonian-information-society-developments.pdf, p. 16.
142. The Estonian Information Society Developments Since the 1990s. Kalmet, Tarmo. 2007. no 29 PRAXIS publication 10. Available at: https://www.praxis.ee/wp-content/uploads/2014/03/2007-Estonian-information-society-developments.pdf, p. 17.
143. The Estonian Information Society Developments Since the 1990s. Kalmet, Tarmo. 2007. no 29 PRAXIS publication 10. Available at: https://www.praxis.ee/wp-content/uploads/2014/03/2007-Estonian-information-society-developments.pdf, p. 18.

Another significant step in establishing Estonia as an e-state was to develop an e-governance system to streamline public administration work. Since 2000, the e-Cabinet provides the means for a paper-free and time-effective governmental decision-making process.[144] Necessary information for the decisions of the Government of the Republic (the Cabinet) can be queried directly from the e-Cabinet information system, 24 hours a day. As a result, the e-Cabinet system has become a multi-user information source and scheduler that keeps relevant information organised and updated in real-time while offering ministers a clear overview of each item under discussion. In 2000, the electronic tax board solution was introduced, allowing individuals to declare their taxes online.[145] Estonia's e-Tax Board offers the taxpayer a pre-completed tax declaration form, making it easy and fast to receive tax returns.[146] That positively impacted the citizens as it streamlined the lengthy and burdensome process of declaring one's taxes. That way, it provided a positive attitude toward digital administration.

Estonia was the first country in the world to introduce e-voting, using it for the first time in 2005 for local council elections. In 2007, e-voting was also made available for parliamentary elections, a world first. E-voting, which is used as an alternative to traditional voting on paper, has risen steadily ever since. For the first time, e-voting outnumbered paper ballots at parliamentary elections in March 2023. A total of 615 009 Estonian citizens eligible to vote cast their ballot, 301 495 of them voted by paper ballot and 313 514 using e-voting.[147]

In the development of the Estonian e-state, two cornerstones need particular emphasis: the single identity code, which determines the identity of every single person by eleven numbers and the x-road, which is a data exchange layer for the public and private sectors.[148] Following, both are briefly introduced.

3.1.2 Digital ID and a single identity code

All Estonians, no matter where they live, have a state-issued digital identity, automatically generated with birth. Aliens permanently resident in Estonia can also apply for an electronic identity. This electronic identity system, called eID, has existed for 20 years and is the cornerstone of the country's e-state.[149] The personal identification code is a unique 11-digit number assigned to everyone in Estonia. The first number indicates the person's gender (even numbers for women, uneven for men), and the following six correspond to the person's birth date, the next three are serial numbers for people born on the same day, and the last one serves as a control number.[150] Legal entities have their unique registration code in the business register, which allows data from different registers to be combined and cross-dataused. These codes are reliable identifiers across other systems and databases in Estonia.[151] Hence the personal identification and business registration codes are critical components of Estonia's e-governance infrastructure, allowing one to identify oneself online and use different public and private sector services online.

144. E-Estonia webpage, text under bulletpoint "2000". Available at: https://e-estonia.com/story/.
145. [14] E-Estonia webpage, text under bulletpoint "2000". Available at: https://e-estonia.com/story/, text under bulletpoint "2000".
146. Electronic Tax filling. SCOOP4C. Available at: https://scoop4c.eu/showcase/electronic-tax-filing-e-tax.
147. E-hääletamisel anti enim hääli valimiste viimastel tundidel (Most votes cast in e-voting in the last hours of the elections). ERR news webpage. 22.03.2023. Available at: https://www.err.ee/1608922715/e-haaletamisel-anti-enim-haali-valimiste-viimastel-tundidel.
148. Estonia, the Digital Nation - Reflections of a Digital Citizen's Rights in the European Union. Tupay, Paloma Krõõt. Available at: https://www.lexxion.eu/wp-content/uploads/2020/07/EDPL_Estonia_extended.pdf, p. 3-4.
149. E-identity. e-Estonia webpage. Available at: https://e-estonia.com/solutions/e-identity/id-card/.
150. See further, Electronic Identity (eID) Application Guide, A Short Introduction to eID https://e-estonia.com/solutions/e-identity/mobile-id/. As to the legal regulation: Population register Act para 39 s 1: 'A personal identification code is a number formed on the basis of the sex and date of birth of a person which complies with the standard of the Republic of Estonia and allows the specific identification of a person.'
151. Commercial Register Act, paragraph 2. Available at: https://www.riigiteataja.ee/akt/123122022034.

The personal ID card is the only mandatory identification document in Estonia; in physical form, it is also used as a travelling document. The chip on the ID card has two functions: it is used for the digital authentication of a person, and it enables the cardholder to sign documents electronically.[152]

In addition to the physical ID card, Estonia also offers a mobile ID, which allows individuals to use their mobile phones as a digital identification tool instead of a combination of a physical ID card and a card reader. Mobile ID uses a SIM card-based solution that enables individuals to authenticate and sign documents using their mobile devices.

Another additional authentication option is the smart ID solution. Smart ID uses a smartphone application that allows individuals to identify themselves.[153]

Both mobile ID and smart ID require the users to use a PIN1 code to log in to the different e-services and a PIN2 code to sign activities, such as bank transfers and others.[154]

These opportunities combined mean that formerly time-consuming actions like signing documents, voting or bank transactions become more casual and streamlined.

The digital ID system in Estonia has played a vital role in the country's e-governance development. It has provided secure access to online services for citizens and residents.

3.1.3 The X-road

To make digital governance as efficient as possible, interoperability between different organisations and information systems is necessary.[155] The X-road is a secured and decentralised data exchange platform developed in Estonia and widely used by the Estonian government and various other organisations. It is an open-source software solution that provides unified and secure data exchange between private and public sector organisations. In addition to Estonia, the X-road is also in active use in Finland, Iceland, and other countries. Finland's use of X-Road and its proximity to Estonia has facilitated cross-border data exchange and opened opportunities for making data usage and requests between the two countries more efficient.[156]

The principle of the X-road idea first came about in 2000. The challenge and goal was developing a technical solution that allows one state authority to use the data of another state authority when and to the extent necessary for performing its public tasks without creating a super-database for all the data gathered.[157]

In legal terms, the X-Road was created in 2003 by governmental decree, which stipulated that the Information Systems Data Exchange Layer (X-Road) is a technical and technological environment enabling secure Internet-based data exchange.[158] The management and development of the X-path are the responsibility of the Ministry of Economic Affairs and Communications, which ensures the secure exchange of data, access only to authenticated users, and the possibility of monitoring and identifying the activities performed by its users.[159]

---

152. ID card. e-Estonia webpage. Available at: https://e-estonia.com/solutions/e-identity/id-card/.
153. Smart ID. e-Estonia webpage. Available at: https://e-estonia.com/solutions/e-identity/smart-id/.

    More about QSCD recognition: https://ec.europa.eu/digital-building-blocks/wikis/display/ESIGKB/What+is+a+qualified+signature+seal+creation+device+QSCD.
154. Smart ID. Available at: https://www.id.ee/en/article/smart-id/.
155. Interoperability services. e-Estonia webpage. Available at: https://e-estonia.com/solutions/interoperability-services/x-road/.
156. Iceland latest nation to adopt Estonia's X-Road platform. BNS. 28.02.2019. Available at: https://news.err.ee/915067/iceland-latest-nation-to-adopt-estonia-s-x-road-platform.
157. Data exchange layer X-tee. Republic of Estonia Information System Authority. Available at: https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee.
158. Implementation of the Information Systems Data Exchange Layer Decree. paragraph 2 (1). Available at: https://www.riigiteataja.ee/akt/127092016004?leiaKehtiv.
159. Implementation of the Information Systems Data Exchange Layer Decree. paragraph 3 (1). Available at: https://www.riigiteataja.ee/akt/127092016004?leiaKehtiv.

Institutions were initially allowed to join the X-way voluntarily. However, by 2005, all government agencies were obliged to join the X-road.[160]

As mentioned in the section Key Stages in the development of the Estonian e-state, it was the implementation of the X-road system that made it possible to present one's tax declaration within only a few minutes: the tax and customs board forwards the taxpayer a pre-filled declaration in which information obtained by other institutions – in this case, the population register and the commercial register – has already been inserted. The taxpayer simply amends and approves it.[161]

The decentralised and standardised approach of the X-road principle has contributed to Estonia's reputation as a leader in digital governance and data interoperability.

3.1.4 The once only principle

The X-road project is deeply intertwined with the once-only principle. The once-only principle aims to eliminate the requirement to provide the same information more than once to public administrations. Instead, public administrations should have the means to re-use information already supplied by citizens transparently and securely.[162] According to the Public Information Act's (PIA) § 43[163] section 3, the *'[c]ollection of data in the database shall be based on the one-request-only principle.'* Although the once-only principle was not explicitly laid down in the PIA until 2019, the prohibition to collect the same data in different national databases has been implemented in practice already since 1997.[164] The Administrative Procedures Act of 2001 laid down as a general principle the duty of the administrative authority to conduct the procedure purposefully and efficiently, as well as simply and expeditiously as possible, avoiding unnecessary expense and inconvenience to the parties. According to the explanations in the 'Handbook of Administrative Procedure': *'The number of documents that can be required from citizens shall be limited. Wherever possible, the deciding authority must communicate with other authorities to gather information rather than require the individual to provide evidence of information already held by another authority. Until now, it was common for citizens to be forced to act as an intermediary between national authorities when applying for permits and other benefits. Today's information technology makes it possible to transfer, for example information on tax payments or data of the commercial register between authorities without any particular additional costs, making this additional burdening of citizens or businesspeople unnecessary.'*[165]

This idea of the 'Once-Only Principle' has also been embraced at the EU level to explore the possibility of its EU-wide application in its Digital Single Market Strategy.[166] Since the launch of the idea at the EU level in 2017, this project has succeeded in creating a reference architecture supporting the organisational and technical interoperability of national e-government systems across state borders. The solution has been tested and implemented within different pilot domains.[167]

---

160. Implementation of the Information Systems Data Exchange Layer Decree. paragraph 9. Available at: https://www.riigiteataja.ee/akt/127092016004?leiaKehtiv.
161. Electronic Tax filling. SCOOP4C. Available at: https://scoop4c.eu/showcase/electronic-tax-filing-e-tax.
162. Once only principle. SCOOP4C. Available at: https://scoop4c.eu/home.
163. National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law / Albi, Anneli; Bardutzky, Samo. The Constitution of Estonia: The Unexpected Challenges of Unlimited Primacy of EU Law / Ernits, Madis. Section 1.1. The Hague: T.M.C. Asser Press, 2019. p. 889.
164. Databases Act 1997, valid until 1.1.2008, paragraph 20 (4), since 2008 Public Information Act paragraph 43^3 (2). Available at: https://www.riigiteataja.ee/akt/107032023011.
165. Haldusmenetluse käsiraamat (Handbook of Administrative Procedures) / Aedmaa, Anno; Lopman, Evelin; Parrest, Nele; Pilving, Ivo; Vene, Einar. Tartu: Tartu Ülikooli Kirjastus, 2004. p. 39. Available at: https://dspace.ut.ee/bitstream/handle/10062/14765/9985568605.pdf.
166. TOOP makes the cross border once-only principle a reality in Europe. Providing data once only. Available at: https://www.toop.eu/node/424.
167. TOOP makes the cross border once-only principle a reality in Europe. Providing data once only. Available at: https://www.toop.eu/node/424.

However, the principle of purpose limitation, laid down in Article 5 of the General Data Protection Regulation (GDPR), according to which data has to be collected with a correctly and sufficiently determined objective, also poses challenges to the once-only principle. According to the European Digital Rights advocacy group, the once-only idea could reduce citizens' control over their data. Therefore, its implementation has to prioritise privacy by design and default.[168] The information must be collected for specified, explicit and legitimate purposes, and it shall not be further processed in a manner incompatible with them.[169]

The processing of personal data is based on the administrative body's general power to obtain personal data from other public bodies to perform its tasks.[170] Where there is a persistent need to get data from another administrative body, direct access to the respective database is established via the X-Road Data Exchange Layer.[171] For example, the traffic police can obtain data from various other databases for one single procedure: the photograph of a person from the identity documents database, information on current convictions from the criminal record, information on the person's driving license and the vehicle's technical inspection from the traffic register, etc.[172] It has been criticised that granting direct access to another administrative body solely based on a general power is not in line with the Estonian Constitution because, in this way, the executive authority decides on the scope of the infringement of a fundamental right.[173] It has also been argued that if the legislator does not determine which other administrative bodies may use personal data stored in a database and for what tasks, the transparency of data processing suffers. People do no longer know what is being done with their data.[174]

Upon the GDPR's entry into force, the Ministry of Justice did not consider it necessary to change the current regulation of digital administration, considering that the GDPR allows a Member State to maintain its current public administration system.[175] Article 6(4) of the GDPR, which more precisely regulates the processing of personal data for purposes other than the original, was not addressed in the respective evaluation of the ministry. However, in 2022, the Ministry of Justice analysed the compliance of the data collection regulation with the GDPR in more detail and found that the cross-use of data regulation must be regulated more transparently and accurately. The Government Cabinet also approved the conclusions contained in the analysis. However, these conclusions have not yet been implemented.[176]

---

168. European Digital Rights, 'Analysis: A truly Digital Single Market?' (2015), p.2. Available at: https://edri.org/files/DSM_Analysis_EDRi_20150617.pdf.
169. See further ''Once only' versus 'only once': Das Once-only-Prinzip zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit' Martini, Mario and Wenzel, Michael. (2017) DVBl p. 749.
170. The legal basis for the processing of personal data derives from the Act on Administrative Procedure (paragraph 7(5)), which provides that an administrative authority may, for administrative proceedings, process personal data relating to the facts of a case to issue an administrative act, performing an act or concluding an administrative contract, in conjunction with a specific act which lays down more detailed conditions for performing or refusing to perform an administrative act; available at: https://www.riigiteataja.ee/akt/103022023014.
171. Regulation of the Government of the Republic Information Systems Data Exchange Layer, paragraph 5. Available at: https://www.riigiteataja.ee/akt/127092016004.
172. Politsei peab sind kinni ja vaatab seejärel oma arvutisse. Mida ta seal näeb? (The police detain you and then look at their computer. What do they see?). Siseministeeriumi infotehnoloogia- ja arenduskeskuse ajakiri (Journal of the Information Technology and Development Centre of the Ministry of the Interior), nr. 5, January 2018, p. 9. Available at: https://dea.digar.ee/?a=d&d=AKsmit201801.2.6.1&e=-------et-25--1--txt-txIN%7ctxTI%7ctxAU%7ctxTA----------.
173. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2011. (Data Protection Inspectorate's Annual Review 2011: "Compliance with the Public Information Act and the Personal Data Protection Act in 2011".) Tallinn: Andmekaitse Inspektsioon 2012, p. 61. Available at: https://aastaraamat.aki.ee/sites/default/files/aastaraamatud/aastaraamat_2011.pdf.
174. Isikuandmete kaitse olemus ja arengusuunad. (The essence of the protection of personal data and future developments.) / Ilus, Tiina. In: Juridica 2002/7, p. 523.
175. Justiitsministeerium, 'Isikuandmete kaitse uue õigusliku raamistiku kontseptsioon' (10.05.2017 toimiku nr: 17-0584) (Concept of the new legal framework on the protection of personal data, Estonian Ministry of Justice 10 May 2017) 10, 33. Available at: http://eelnoud.valitsus.ee/main/mount/docList/db80bf57-35ca-41e3-be15-827a2f056fdd#aek0ABB.
176. Has the GDPR killed e-government? The "once-only" principle vs the principle of purpose limitation, Mikiver, Monika; Paloma Krõõt, Tupay. International Data Privacy Law, 2023; ipad010, ch. The GDPR's Article 6 (2) and (3) and The GDPR's Article 6 (4). Available at: https://doi.org/10.1093/idpl/ipad010.

3.2 Current status of the Estonian regulations on digital public administration

As of 2023, no specific legislation on digital public administration has been adopted. Regardless, other legal acts regulate particular aspects of digital public administration, the most important of which are the Public Information Act (PIA) and the Administrative Procedure Act.

3.2.1 The Public Information Act (PIA)

The purpose of the PIA, which entered into force in 2001, is *'to ensure that the public and every individual has the opportunity to access information intended for public use, based on the principles of a democratic and social state, the rule of law and an open society, aiming at creating opportunities for public scrutiny of the performance of public functions.'*[177] As a significant step forward in digital development, the law introduced the obligation for all public authorities to keep an electronic register of documents to be made public on the Internet, in which all incoming and outgoing documents were to be visible.[178] Documents without access restrictions should be open to everyone by clicking on them.[179] When the PIA came into force, in addition to the register of documents, the legislator introduced a list of dozens of categories of information institutions must publish on their websites.[180] Since 2008, the PIA has regulated all public authority databases and laid down the respective general principles.

3.2.1.1 Public authorities' databases

As the development of the Estonian information society was primarily based on the interoperability of the various public databases, which made the creation of different data services and the use of data by different administrative bodies possible, it was considered essential to have a separate regulation of public databases. Thus, the PIA contains today an individual chapter on databases held by the state, local authorities, other public bodies or private persons with a public-service mission.[181] As a general principle, a database shall be established by a legal act or a regulation based on a law.[182] The legislator has regulated databases of particular state interest in separate legal acts on the corresponding database, for example the Population Register[183] regulated by the Population Register Act[184]; the land register regulated by the Land Register Act[185]; the commercial register regulated by the Commercial Register Act [186] and the criminal records database regulated by the Criminal Records Database Act.[187] In most cases, however, the legislator decides on establishing a specific database but delegates the regulation of more specific details on the content and functioning of the database by decree to either the government or the relevant minister.[188] It has been debated over the years which aspects of establishing a database need to be regulated at the level of parliamentary law beyond the establishment of the database.[189] Usually, the law limits itself to foreseeing the establishment of the database and all further details, including the amount of personal data to

177. Public Information Act, paragraph 1. Available at: https://www.riigiteataja.ee/akt/107032023011.
178. Public Information Act, paragraph 11(1), 28(1)(31), 29(1).
179. Since 01.01.2009, Public Information Act, paragraph 12(4^1).
180. Public Information Act, paragraph 28.
181. Public Information Act Chapter 5^1.
182. Public Information Act, paragraph 43^3(1).
183. Population Register. Available at: https://www.siseministeerium.ee/en/activities/population-procedures/population-register.
184. Population Register Act. Available at: https://www.riigiteataja.ee/en/eli/ee/502012019008/consolide/current.
185. Land Register Act. Available at: https://www.riigiteataja.ee/en/eli/ee/525032019009/consolide/current.
186. Commercial Register Act[1]. Available at: https://www.riigiteataja.ee/en/eli/ee/503012023001/consolide/current.
187. Criminal Records Database Act. Available at: https://www.riigiteataja.ee/en/eli/ee/501042019021/consolide/current.
188. Analüüs. Andmekogud ja isikuandmed: EV Põhiseadusest ja IKÜM-st tulenevad nõuded regulatsioonile. (Analysis. Databases and personal data: requirements for regulation arising from the EV Constitution and the IKÜM.) / Mikiver, Monika, 2021, p.4. Available at: https://www.just.ee/media/3193/download.
189. Analüüs. Andmekogud ja isikuandmed: EV Põhiseadusest ja IKÜM-st tulenevad nõuded regulatsioonile. (Analysis. Databases and personal data: requirements for regulation arising from the EV Constitution and the IKÜM.) / Mikiver, Monika, 2021, p. 29-34. Available at: https://www.just.ee/media/3193/download.

be collected, the retention periods and the extent to which other agencies have direct access to the respective data are decided by executive decrees. This may, however, infringe the principle of relevance which requires the legislator to determine by itself the primary conditions and extent of restrictions on fundamental rights by the public authorities. The Cabinet of Ministers has approved the views that, in addition to the establishment of the database, the general characteristics of personal data collected therein, storage intervals and the purposes of the further processing of the data collected should be defined at the level of law, especially if direct access to the database is given to other institutions.[190]

Furthermore, the establishment of new databases, as well as modifications on the requirements of data collected in existing databases, must be coordinated, among other things, with the Data Protection Inspectorate, which will assess whether the collection of such personal data in the database is at all legitimate as well as if there is no duplication of data collection.[191] To date, more than 1 300 databases and information systems have been registered, whereby the notion of an information system may overlap with the notion of a database, but a single database may also contain several different information systems (as a technical solution for using the data in the database).[192]

3.2.1.2 Obligation to disclose information to individuals

The PIA also ensures transparency by obligating public administration to disclose certain information such as statutes of state or local government agencies and their structural units, budgets and draft budgets of state agencies, local governments and local government agencies, and reports on the implementation thereof; information concerning the receipt of state budget revenue and the document register of the agency.[193] State institutions such as The Chancellery of the *Riigikogu*, the Office of the President of the Republic, the Office of the Chancellor of Justice, the National Audit Office, courts, government agencies and legal persons in public law are obligated to maintain websites for the disclosure of information. A city or rural municipality government shall organise the maintenance of a website to provide details of the activities of the bodies and agencies of the city or rural municipality and to disclose information. The State Chancellery and ministries must implement measures to maintain websites by state agencies administered by them.[194]

3.2.1.3 National information gateway

To ensure that people have a primary channel and secure internet environment for obtaining information about and communicating with the state and that e-solutions are easily accessible for citizens, entrepreneurs and officials, Estonia has developed an information gateway called Eesti.ee.[195][196] According to the law, the Estonian information gateway is *'a website allowing access to public information related to the fields of activities of holders of information and the public services provided by them, and allowing access to public electronic services and reusable information.'*[197]

---

190. See Valitsuse kabinetinõupidamise päevakord, 31. märts 2022 (The agenda of the Government Cabinet Meeting of 31 March 2022). Available at: https://valitsus.ee/uudised/valitsuse-kabinetinoupidamise-paevakord-31-marts-2022. The decision of the Government of 31.03.2022 on the approval of the Memorandum on the analysis of databases is available at the Government Office.
191. Public Information Act, paragraph § 43^3(3). Available at: https://www.riigiteataja.ee/akt/107032023011.
192. All databases of the state, local government, or other legal entity under public law or private persons performing public duties must be registered in one separate register, which is called the administrative system of the state information system. Among other things, such a register also serves the purpose of getting an overview of the existing data and avoiding double collection of data. The website of the State Information System management system states that more than 1,300 databases and information systems are registered in the system: https://www.riha.ee/Avaleht.
193. Public Information Act, paragraph 28(1)(3), 28(1)(11), 28(1)(12), 28(1)(31). Available at: https://www.riigiteataja.ee/akt/107032023011.
194. Public Information Act, paragraph 31.
195. Eesti.ee. Available at: https://www.eesti.ee/en.
196. Estonian open data portal. Available at: https://avaandmed.eesti.ee/.
197. Public Information Act, paragraph 32^1(1).

3.2.2 The Administrative Procedure Act

The Administrative Procedure Act aims to *'ensure the protection of the rights of persons by the creation of a uniform administrative procedure which allows participation of persons and judicial control.'*[198] The Administrative Procedure Act plays a vital role in regulating the digitalisation of administrative activities. In Estonia, when conducting any administrative procedure,[199] digital signatures[200] and electronic seals[201] are to be used in administrative process under the relevant legal acts. Requests (applications),[202] administrative appeals[203] and administrative regulations[204] may be submitted and issued electronically. Administrative acts, summonses, notices and other documents can also be served electronically.[205] Administrative acts may also be issued in electronic form,[206] and digital signatures do not need to be added if the executive authority or a person authorised is identifiable according to the legal requirements.[207] Generally, if documents are delivered electronically, they are accessible in the relevant information system, the Estonian information gateway, or via the participant's e-mail address. Depending on the circumstances, a digital signature and/or an electronic seal are added.[208]

Although a significant part of the administrative procedure is digitised, the current Administrative Procedure Act does not regulate the issuing of automated administrative acts. The Amendment Act to the Administrative Procedure Act aims to create a legal basis for automatic administrative procedures, including automatic administrative acts or other administrative actions, which means public authorities' activities without the intervention of an official or employee acting on behalf of an administrative body. A corresponding bill was withdrawn from the parliamentary legislative process at the end of the last legislative period.[209] However, different automatic administrative procedures are already foreseen in certain legal acts regulating specific areas of digital public administration. For example, the tax authority has the right to issue administrative acts and documents in an automated manner without the direct intervention of a tax official.[210] The same is also stipulated in the Environmental Charges Act, where the Environmental Board can issue administrative decisions and documents in an automated manner, without interference by an official of the tax authority.[211] In other cases, the administration can act proactively, meaning no special requests from the person's side need to be made. Instead, certain data activates the administrative procedure. For example, to receive family benefits, no separate application is necessary. The registration of the birth of a child in the Population Register 'activates' the administrative procedure, and a benefits payment offer will be sent to the new parent.[212]

198. Administrative Procedure Act, paragraph 1. Available at: https://www.riigiteataja.ee/akt/103022023014.
199. Administrative Procedure Act, paragraph 5(6).
200. In Estonia, a digital signature is a signature that is legally valid and legally equivalent to a handwritten signature, where the user's identity, the background of the issuer of the certificate, and the time of the signature have been verified and accurately established. (https://www.id.ee/en/article/digital-signing-and-electronic-signatures/).
201. An electronic seal ("e-seal") is used to "certify electronically sent documents and prove that they originate from the institution that sent them." (https://e-estoniax.com/solution/e-seal/).
202. Administrative Procedure Act, paragraph 14.
203. Administrative Procedure Act, paragraph 76(3).
204. Administrative Procedure Act, paragraph 92(1).
205. Administrative Procedure Act, paragraph 25(1).
206. Administrative Procedure Act, paragraph 55(3).
207. Administrative Procedure Act, paragraph 55(4).
208. Administrative Procedure Act, paragraph 27(1).
209. The Act on Amendments to the Administrative Procedure Act and Amendments to Other Acts 634 SE. Available at: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/21f6df90-a333-413a-a533-ebbf7e9deebe/Haldusmenetluse+seaduse+muutmise+ja+sellega+seonduvalt+teiste+seaduste+muutmise+seadus.
210. Taxation Act, paragraph 46^2(1). Available at: https://www.riigiteataja.ee/akt/130062023044.
211. Environmental Charges Act, paragraph 33^6. Available at: https://www.riigiteataja.ee/akt/130062023025.
212. Family and children's allowances. Available at: https://www.eesti.ee/en/pensions-social-services-and-allowances/benefits-and-allowances/family-and-childrens-allowances

3.2.3 Estonian legal framework on data protection

In 1996, the *Riigikogu* adopted Estonia's first personal data protection law, ensuring its compliance with the data protection regulations of the EU, specifically with Directive 95/46/EC of the European Parliament and of the Council.[213][214] In 1999, the Data Protection was established.[215]

Today, when processing personal data, the GDPR and its requirements apply, as the regulation is directly binding and applicable in Estonia.[216] Initially, in Estonia, the GDPR was met with criticism out of fear that the new unified framework would make Estonia, an e-state based on the extensive cross-use of data, impossible or too complex to uphold.[217] However, the Ministry of Justice's analysis of the necessary national changes caused by the EU data protection reform stated more optimistically that Estonia aimed at maintaining the Estonian public sector's distinctive accessibility and cross-use of databases through the X-road, including the once-only principle, i.e. the cross-use of data.[218]

Data security issues are regulated by the Cybersecurity Act, which lays down requirements *'for the maintenance of network and information systems essential for the functioning of society, including network and information systems of the public sector, liability and supervision as well as bases for the prevention and resolution of cyber incidents.'*[219]

3.2.4 Legal regulation of open data

Since 1999, the EU has seen significant potential in the free availability of public sector data to stimulate markets and create innovative products and services. Public sector bodies hold a large amount of data in different domains, such as geographic data, tourism information, statistical and business data, weather information, etc. This data is essential for developing public policies and delivering services, but it is also very valuable for Europe's economic development.[220] Insofar the European lawmaker has only stated in general terms that EU regulations on open data leave intact and in no way affect the level of personal data protection ensured by law.[221] However, when the EU law on open data was transposed into Estonian law the question arose

213. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
214. Explanatory memorandum to the amended edition of the Personal Data Protection Act (1196 SE)), p. 20. Available at: https://www.riigikogu.ee/download/e681453c-ce0a-3934-ae8f-35142016cf29.
215. Andmekaitse Inspektsioon. Inspektsioonist. Eesmärk ja Visioon (Data Protection Inspectorate).
216. According to the Administrative Procedure Act paragraph 7(4), in administrative procedure, personal data shall be processed under the procedures for processing personal data deriving from Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 04.05.2016, p. 1–88) and the Personal Data Protection Act, taking account of the specifications provided for in the Act.
217. Eesti andmekaitse on Brüsseli reformi suhtes kriitiline. (Estonian data protection is critical to the Brussels reform.) / Sillaots, Marge. In: Õhtuleht, 30.01.2012. Available at: https://www.ohtuleht.ee/462330/eesti-andmekaitse-on-brusseli-reformi-suhtes-kriitiline; Indrek Teder: kas soovime suletud ühiskonda? (Indrek Teder: do we want a closed society?) / Teder, Indrek. In: Postimees, 07.06.2012. Available at: https://arvamus.postimees.ee/868200/indrek-teder-kas-soovime-suletud-uhiskonda; Euroopa Komisjon tõrjub Eesti hirme andmetsensuurist. (The European Commission rejects Estonia's fears of data censorship.) / Kund, Oliver. In: Postimees, 08.06.2012. Available at: https://www.postimees.ee/868834/euroopa-komisjon-torjub-eesti-hirme-andmetsensuurist.
218. Justiitsministeerium. ISIKUANDMETE KAITSE UUE ÕIGUSLIKU RAAMISTIKU KONTSEPTSIOON (Ministry of Justice. THE CONCEPT OF THE NEW LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA), 18.04.2017, p. 33. Available at: https://adr.rik.ee/jm/dokument/5087413.
219. Cybersecurity Act, paragraph 1(1); available at: https://www.riigiteataja.ee/akt/106082022018.
220. Commission of the European Communities. Public sector information: a key resource for Europe – Green Paper on public sector information in the information society. Brussels, 20.01.1999, COM(1998) 585 final. Available at: https://op.europa.eu/en/publication-detail/-/publication/599834ce-7a43-44fe-8cd8-334b3c19feba; see also: European Commission. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A Digital Agenda for Europe. Brussels, 19.5.2010 COM(2010)245 final, p.9. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF; The influence of the PSI directive on open government data: An overview of recent developments. / Janssen, Katleen. Government Information Quarterly 28, no. 4 (2011), p. 446.
221. DIRECTIVE 2003/98/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 November 2003 on the re-use of public sector information Art.1(4); now DIRECTIVE (EU) 2019/1024 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 June 2019 on open data and the re-use of public sector information Art. 1(2)(h), 1(4).

whether the re-use of public sector information also covered personal data.[222] The Estonian legislator took the view that the regulation on re-use is also applicable to personal data that have either already been disclosed by law, for example, if a register is by law publicly available on the internet or in case there are no particular restrictions concerning the access to the respective information held by public authorities.[223] However, according to the legal amendment's explanatory memorandum, if the administrative authority considers personal data to be open data, it must assess whether it is necessary to limit how it is made available for re-use (e.g. exclude full downloadability, etc.).[224]

Although personal data made available in the form of open data (downloadable and in machine-readable format) is still subject to the GDPR, it is questionable to what extent such extensive data processing can comply with the principles of personal data processing and the rights of the data subject enshrined in EU law. The different EU initiatives that ease access to and sharing of personal data serve without doubt the development and increase of data-driven solutions. However, there is also a need for further discussion and attention on how far the classification of personal data as open data can and should go. Since the (further) use of open data should not be subject to any restrictions according to its very wording, an EU-wide clarification of the question of what type of data open data can include would be helpful and necessary.

The following examples illustrate the consequences of the Estonian regulation, where the right to decide on the technical limitations of open data is left to the authorities.

For example, the land register contains the names of the immovable properties' owners, but is also linked to the map server of the Land Board, thanks to which various maps of the property of interest as well as aerial photos of fairly good resolution can be directly accessed from the land register.[225] The land register published on the Internet is not available for everyone to download, it is only possible to access the respective information by logging in to the online register and identifying oneself for each individual query.[226] At the same time, the list of members of Estonian political parties can be downloaded in CSV format by anyone (this question is handled in more detail below, 3.3).[227] Information on the person's political beliefs and affiliation can therefore be regarded in Estonia as less protected than information on the respective person's property.

3.2.5 Other regulations on Estonian digital public administration

In addition to legal acts, there are also non-binding regulations such as industry development plans, guidelines, and others that impact Estonian digital administration.

3.2.5.1 The e-state charter

The National Audit Office initiated the e-state charter. The charter mainly aims to list the rights of individuals when communicating with public authorities. It therefore contains assessment criteria to determine if peoples' rights are being ensured within the provision of public digital services. With the help of the charter, public authorities, local governments and service providers in the public sector can review their activity and establish goals for improving administrative procedures. The charter explains every listed right, including a reference to the laws in which

222. In fact, the issue arose during the transposition of both directives mentioned in the previous reference (the PSI Directive and the Open Data Directive). The issue was addressed in the explanatory memoranda of the draft laws relating to both directives. See the Explanatory Memorandum to the Act Amending the Public Information Act (Draft Act 263 SE), p. 4, in relation to the transposition of the PSI Directive. On the open data directive, see the Explanatory Memorandum to the Draft Act amending the Public Information Act 409 SE, p 4.
223. Act amending the Public Information Act. Available at: https://www.riigiteataja.ee/akt/130112021003. See the amendment to the Public Information Act explanatory memorandum, p. 4.
224. Explanatory memorandum to the Act Amending the Public Information Act 409 SE, p. 8-9. Available at: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/9482dd7e-69bd-4ebe-9276-484e06728d52/avaliku-teabe-seaduse-muutmise-seadus.
225. Land Register Act, paragraphs 11, 14. Available at: https://www.riigiteataja.ee/akt/117032023061.
226. See for more information: https://www.rik.ee/en/e-land-register/queries.
227. See for more information: https://ariregister.rik.ee/eng/political_party/members/80053370.

these rights are regulated. It contains control questions for agencies and individuals to check whether the listed right is being ensured. The rights recorded and analysed in the charter are following: the right to receive comprehensive information about public services, the right to use one's national e-ID, the right to obtain public services easily and conveniently, the right to receive information about the progress of service provision, the right to know what personal data public institutions have collected and how it is protected, the right to give feedback about the organisation of service provision is stipulated in the Constitution, the right to receive information from agencies electronically and the right to participate in decision-making processes.[228]

3.2.5.2 Estonia's Digital Agenda 2030

Estonia's Digital Agenda 2030 is centred around creating a policy to use digital technology to develop the Estonian economy, state and society Estonia's goal is to establish a leading user-experience for public services.[229] This agenda sets out the development plan, policy principles, development directions, operational goals and directions for the next ten years regarding the digital state. The agenda focuses on increasing the efficiency of state governance in Estonia by using information and communication technology and digital solutions.[230]

Several public sector institutions digitalisation, among them the Ministry of Economic Affairs and Communications (MKM) and the Data Protection Inspectorate, have issued guidelines, principles, and manuals regarding the digitalisation of administrative services. The MKM has published guidelines for implementing different regulations, aiming to ensure the regulation's uniform interpretation by authorities and provide advice.[231] The Council of Public Services (*Avalike teenuste nõukogu*) that supports the MKM in coordinating the development of public services,[232] developed ten principles for the development of digital services. Additionally, an "E-Services Design Manual" (*E-teenuste disainimise käsiraamat*) has been established to help state employees renew services and ensure their user friendliness.[233] Some more notable examples include the 2013 'Green Book on the Organization of Public Services' (*Avalike teenuste korraldamise roheline raamat*)[234] and an action plan 'Simpler state 2020' (*Lihtsam riik 2020*) [235]. The Data Protection Inspectorate has published several guides.[236]

---

228. Everyone's rights in e-state. The e-state Charter, p. 1-3. Available at: https://www.riigikontroll.ee/LinkClick.aspx?fileticket=E3_IEQ6A5A8%3D&tabid=305&mid=908&language=et-EE&forcedownload=true
229. Estonia's Digital Agenda 2030. Available at: https://www.mkm.ee/media/6970/download#:~:text=Estonia's%20Digital%20Agenda%202030%20includes,technology%20in%20the%20next%20decade.&text=knowledge%2Dbased%2C%20using%20new%20technologies,as%20flexible%20forms%20of%20work., p. 4, checked: 07.11.2023.
230. Protokolli märgitava otsuse "Eesti digiühiskond 2030 arengukava" kinnitamine" eelnõu seletuskiri (Explanatory memorandum to the "Approval of the "Estonia's Digital Agenda 2030"" to be noted in the minutes). Available at: https://www.mkm.ee/media/6790/download, p. 3, checked: 07.11.2023.
231. See e.g.: Juhised määruse "Teenuste korraldamise ja teabehalduse alused" rakendajatele (Instructions for the implementers of the "Bases of service organization and information management" regulation), avaliable at: https://www.mkm.ee/media/7309/download.
232. Majandus- ja kommunikatsiooniministeeriumi käskkiri ,,Avalike teenuste nõukogu ülesanded, koosseis ja töökord" (Directive of the Ministry of Economic Affairs and Communications "Tasks, composition and working procedure of the Public Services Council"). Available at: https://www.mkm.ee/media/7323/download pt. 5.11.
233. E-teenuste disainimise käsiraamat (Handbook of E-Service Design). Available at: https://www.mkm.ee/media/7327/download.
234. Majandus- ja Kommunikatsiooniministeerium. Avalike teenuste korraldamise roheline raamat. Otsesed teenused kohustuste täitmiseks ja õiguste kasutamiseks, ning teenuse osutamist toetavate keskkondade loomine info- ja kommunikatsioonitehnoloogia võimalusi ja vahendeid kasutades (Ministry of Economic Affairs and Communications. Green Paper on the Organization of Public Services. Direct services for the fulfillment of obligations and the exercise of rights, and the creation of environments that support the provision of services using the possibilities and tools of information and communication technology). Available at: https://www.mkm.ee/media/7326/download.
235. Lihtsam riik 2020. Tegevuskava infoühiskonna arengukava 2020 meetme "Dokumendihalduselt infohaldusele" täitmiseks (Simpler State 2020. Action plan for the implementation of the information society development plan 2020 measure "From document management to information management"). Available at: https://www.mkm.ee/media/7389/download.
236. e.g. Andmekogude juhend (Databases Guide). Available at: https://www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf; Avaliku teabe seaduse üldjuhend (General guide to the Public Information Act). Available at: https://www.aki.ee/sites/default/files/dokumendid/avaliku_teabe_seaduse_uldjuhend.pdf; Suurandmed ja privaatsus. Juhendmaterjal organisatsioonidel (Big Data and Privacy. Guidance for Organizations). Available at: https://www.aki.ee/sites/default/files/dokumendid/suurandmed_ja_privaatsus.pdf.

3.3 Main Stakeholders of the Digitalization of Estonian Administration

The main stakeholders of the digitalisation of Estonian administration are national bodies and agencies, advisory councils, municipalities, research institutions, judiciary and civil society.

3.3.1 Main stakeholders at the national level

In Estonia, legal acts – including those regulating the use of digital solutions by the state and where necessary, also by private persons - are passed by the Estonian parliament (*Riigikogu*). At least one member of the *Riigikogu*, *Riigikogu* parliamentary groups, *Riigikogu* committees, the government and the President of the Republic - for amendment of the Constitution - have the right to initiate laws.[237] The Estonian Electronic State Gazette (the *Riigi Teataja*) is the central database and official online publication for Estonian legislation.[238] The *Riigi Teataja* has been published also online since 1997 but the official electronic *Riigi Teataja* was presented in 2002.[239] Since 2010, all national legal acts have been public in electronic form only.[240]

In the Estonian public institutions, specific state officials work on Estonian digital administration. At the Ministry of Economic Affairs and Communications, the Undersecretary for Digital Transformation, the Government Chief Data Officer and the Government Chief Technology Officer all play essential roles in the development of digital solutions in Estonian administration. The Ministry of Justice is responsible for data protection and ensuring the protection of fundamental rights in connection with the general coordination of the ministries' law-making activities.[241] The area of responsibility of the Minister of Economic Affairs and Information Technology, who heads the Ministry of Economic Affairs and Communications, includes information technology and telecommunications.[242] The Ministry of Economic Affairs and Communications organises i.a. hackathons to incorporate the private and public sectors in innovation and cooperation concerning the e-state[243] and national digital services contests to determine the best digital service.[244] The Information State Authority (RIA) handles the development and administration of state information systems, oversees their interoperability, and handles any other proceedings regarding information security, including security incidents in Estonian computer networks.[245] The Estonian legislator has assigned a dual role to the Data Protection Inspectorate.[246] On the one hand, the Data Protection Inspectorate has been designated as a supervisory authority within the meaning of the GDPR. On the other hand, the Data Protection Inspectorate also supervises compliance with the requirements of the public information act (PIA; compare above, 3.2.1).[247] The inspection therefore has an inherently divergent dual role: it must protect people's privacy and ensure the transparency of public information at the same time. The IT and Development Centre of the Ministry of the Interior is Estonia's largest IT institution, which creates and manages the information systems necessary to save lives and ensure internal security (information systems of the police, rescue services and

237. Legislative Work. Available at: https://www.riigikogu.ee/en/introduction-and-history/riigikogu-tasks-organisation-work/what-does-riigikogu/legislative-work/.
238. Riigi Teataja Act, paragraph 1. Available at: https://www.riigiteataja.ee/akt/111032023085.
239. Riigi Teataja võrguväljaandest (About Online edition of *Riigi Teataja*). Available at: https://www.riigiteataja.ee/abiLeht.html?id=1.
240. Centre of Registers and Information Systems. State Gazette. Available at: https://www.rik.ee/en/international/state-gazette.
241. Government of the Republic Act, paragraph 59(1). Available at: https://www.riigiteataja.ee/akt/130062023011.
242. The competence of ministers in the management of the ministry and the areas of responsibility of the ministers pt. 6. Available at: https://www.riigiteataja.ee/akt/320042023001?leiaKehtiv.
243. Täna algav Digiriigi häkaton toob taas kokku riigiasutused ja IT-ettevõtted (The Digiriigi hackathon, which starts today, will once again bring together state institutions and IT companies). Available at: https://www.mkm.ee/uudised/tana-algav-digiriigi-hakaton-toob-taas-kokku-riigiasutused-ja-it-ettevotted.
244. Selgusid riigi digiteenuste konkursi "Su/g 2022" finalistid (The finalists of the national digital services competition "Su/g 2022" have been announced). Available at: https://www.mkm.ee/uudised/selgusid-riigi-digiteenuste-konkursi-sug-2022-finalistid.
245. Republic of Estonia Information State Authority. Authority, news and contact. Available at: https://www.ria.ee/en.
246. Personal Data Protection Act, paragraph 56(1). Available at: https://www.riigiteataja.ee/akt/111032023011.
247. Public Information Act, paragraph 44(1). Available at: https://www.riigiteataja.ee/akt/107032023011.

others).[248] In the case of violations of personal data by the state and security/surveillance or authorities, individuals can also inquire assistance from the Chancellor of Justice (compare above, B.I.3.c.).[249]

3.3.2 Advisory bodies

Two important advisory bodies of Estonian public administration digitalization are the E-Estonia Council and the e-Governance Academy (eGA). The E-Estonia Council, composed of experts, ICT sector representatives and related ministers and chaired by the Estonian prime minister, is in charge of overseeing the progress of Estonian digital society, e-governance and implementation of national digital agendas and its work is organised by the Strategy Unit of the Government Office.[250] The e-Governance Academy (eGA) is a joint initiative of the Estonian government, the Open Society Institute (OSI) and the United Nations Development Programme, which helps develop digital technologies for the public sector and civil society organisations by consulting, training, networking, research and assisting.[251]

3.3.3 Municipalities

Estonia has a one-tier local government system. The 79 local governments decide on local issues, however digitalization issues are mostly dealt with on a national level. Yet the government supports the activities of the Association of Estonian Cities and Municipalities (AECM) to further develop local governments' IT systems and capabilities. The two biggest cities of Estonia, Tallinn and Tartu, are the main developers of AI implementation at local level. For example, Tallinn has a driverless bus route, an AI based pedestrian crossing and autonomous snow shovelling robots intended for public use whilst Tartu is taking part in the European project SmartEnCity and is part of a joint project between Tartu, ICT companies and infrastructure companies called Estonian Smart City Cluster.[252]

3.3.4 Research institutions

Research institutions are also major stakeholders in the digitalisation of Estonian Administration. The University of Tartu (UT) offers an Information Technology Law program.[253] Tallinn University of Technology (TalTech) operates a Digital Governance Lab that aims to advance public governance models and frameworks.[254] TalTech also has a cooperation between TalTech Law School and NJORD Law Firm called TalTech Legal Lab, which joins together law and tech experts who have in-depth knowledge in technology law and are experts in AI, data protection, IT law and legal tech.[255] Other important research institutions include the Estonian Research Council, Praxis and the *Arenguseire Keskus* (Foresight centre). The Estonian Research Council is a governmental foundation aiming at guaranteeing the funding of research and development.[256] Praxis is a socio-economic research centre that creates evidence-based analyses and monitors the implementation of different policies.[257] Courts of first and second instance are administered in cooperation between the Council for Administration of Courts and the Ministry of Justice.[258]

The Arenguseire Keskus is a think tank situated at the Estonian Parliament that analyses

248. Siseministeeriumi infotehnoloogia- ja arenduskeskus (Information technology and development center of the Ministry of the Interior). Available at: https://www.smit.ee/.
249. Estonian Human Rights Centre. Digital Rights. Available at: https://humanrights.ee/en/topics-main/privacy/.
250. E-Estonia Council. Available at: https://www.riigikantselei.ee/en/supporting-government-and-prime-minister/councils-and-comittees/e-estonia-council.
251. e-Governance Academy. Available at: https://ega.ee/about-us/.
252. Artificial Intelligence, Big Data and Fundamental Rights. Country Research Estonia, 2020, p. 8-10. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-ai-project-estonia-country-research_en.pdf.
253. Information Technology Law. Master's. Available at: https://ut.ee/en/curriculum/information-technology-law.
254. Digital Governance Lab. Available at: https://digigovlab.ee/.
255. TalTech Legal Lab. Available at: https://taltechlegallab.com/.
256. Estonian Research Council. Available at: https://www.etag.ee/en/estonian-research-council/.
257. Praxis. Available at: https://www.praxis.ee/en/what-we-do/.
258. Arenguseire Keskus (Foresight Centre). Available at: https://arenguseire.ee/en/about/.

long-term development in society, identifies new trends and developments and drafts development scenarios.

3.3.5. Other Stakeholders

Courts of first and second instance are administered in cooperation between the Council for Administration of Courts and the Ministry of Justice.[259] The Supreme Court on the other hand, being a constitutional institution, administers itself.[260] Although the courts are also open to various IT solutions, as well as applications based on artificial intelligence as helpful tools,[261] such as automatic recording of court hearings using speech recognition technology, the rumour that Estonia is planning to introduce a robot judge is not true.[262]

One important Estonian civil society stakeholder concerning fundamental and digital rights is the Estonian Human Rights Centre. The Estonian Human Rights Centre is an independent non-governmental human rights organization that aims to ensure the respect for each individual's human rights.[263] However, in Estonia there are not many third-sector institutions focusing on the protection of fundamental rights in the digital sphere.

4. The Values of Democracy and Rule of Law, Trust in Public Administration and Respect of Citizens' Rights within the Framework of the Digitalization of the Estonian Administration

4.1 Democracy and the Rule of Law

Democracy and rule of law are both core principles of the Constitution of Estonia and are mentioned in its § 10. That means that both of those principles need to be retained and respected throughout the rapid development of digitalization of the Estonian Administration in order not to contradict the Constitution.

4.1.1 Democracy

The value of democracy is a key consideration within the framework of the digitalization of the Estonian administration. With the rapid developments in digitizing public administration, abiding by and implementing the principle of democracy has raised different questions concerning the people's right to be the source of the state's 'supreme power', as vested in § 1 of the Constitution.

Questions about the connection between democracy and digitalization have arisen in Estonia particularly in the context of e-elections, and these are closely linked to questions of trust in the system and its technical functioning.

In its decision on the constitutionality of e-voting the court in 2005 acknowledged the aims of e-voting – i.e. the increase of voter turnout, better integration of decision-making in people's common lives as well as the modernisation of electoral practice – to be legitimate but acknowledged that e-voting could jeopardise the principle of freedom of elections and the principle of secrecy of voting.[264] However, the court held that by providing the possibility of changing one's vote electronically, the legislator had struck an appropriate balance between the electoral principles deriving from the Constitution.[265]

In later cases concerning e-voting, the Supreme Court has acknowledged shortcomings in its legal

259. Courts Act, paragraph 39(1). Available at: https://www.riigiteataja.ee/akt/111032023019.
260. Brochure of the Supreme Court of Estonia. Available at: https://www.riigikohus.ee/sites/default/files/Tr%C3%BCkis/2019-Riigikohus-brozuur-2019-ENG.pdf, p. 18.
261. Villu Kõve: kohtute tööjõupuudust aitaks leevendada tehisintellekt (Villu Kõve: artificial intelligence would help alleviate the shortage of court manpower). / Kirsberg, Kristi. 08.06.2023. Available at: https://www.kohus.ee/en/node/41925.
262. „Can AI Be a Fair Judge in Court?" Denkt Estland so?. Herberger, Maximilian. NJW-aktuell /
263. Estonian Human Rights Centre. Available at: https://humanrights.ee/en/.
264. RKPJKo 01.09.2005, 3-4-1-13-05, pt. 25 -27 available at: https://www.riigikohus.ee/lahendid?asjaNr=3-4-1-13-05.
265. RKPJKo 01.09.2005, 3-4-1-13-05, pt. 32 available at: https://www.riigikohus.ee/lahendid?asjaNr=3-4-1-13-05.

regulation, but not found explicit unconstitutionality.[266] Recent cases contesting e-voting were brought before the court in March 2023, following parliamentary elections.[267] This also corresponds to a more recent, albeit not predominant, trend in society and politics that questions the legitimacy of e-voting. One of the complaints in this regard was submitted by the Conservative People's Party of Estonia, which can be classified as right-wing conservative.[268] The ESC dismissed all corresponding election appeals, but pointed out that the organisation of electronic voting needs to be more thoroughly written into law.

The Constitutional Review Chamber of the ESC noted i.a. that although the basic regulation of the organisation of electronic voting follow currently from the Riigikogu Election Act and the acts of the National Electoral Commission and the Electoral Service, the regulation of e-voting relies to a great extent on subordinate legislation. Therefore, regulations and processes are often difficult to understand.[269] Though the rapid development of technology can make it difficult for the legislator to keep pace with the relevant changes, the lawmaker has nonetheless a constitutional obligation to lay down the respective rules in electoral law in sufficient detail to ensure scrutiny and public confidence in elections.[270]

Estonia has also introduced digital solutions to better involve people in political decision-making. Two of them, called OSALE.ee and TOM.ee. and launched in the early 2000s, aimed at making it easier for people to contribute their suggestions and views on legislative proposals. However, both of these proved not really successful, mainly because of the sheer volume of information people were confronted with.[271] Today, direct participation is enhanced in particular through the possibility of submitting petitions to parliament as well as local governments. Petitions are handed in and signed digitally. The https://rahvaalgatus.ee/ environment has proven popular.[272]

The e-governance Academy (see also above, 3.3.2) uses a variety of (especially international) cooperation, training and projects to show how digital solutions can be used in the service of democratic decision-making.[273]

4.1.2 The Rule of Law

In the context of digitalization, issues focused exclusively on the rule of law have rarely been at the forefront of Estonian political and legal discourse. In this respect, the topics are mostly focused on the digitalization of the justice system and in particular the resulting simplification and acceleration of court proceedings.[274] However, two recent examples highlight possible challenges to the rule of law due to digitalization and refer to the question of the extent to which automatic decision-making processes require a legal basis in accordance with the rule of law.

The first example concerns the Estonian Environment Agency's decision to use automated felling

266. RKPJKo 24.10.2017, 5-17-32. Available at: https://www.riigikohus.ee/lahendid?asjaNr=5-17-32/2 ; RKPJKo 21.10.2021, 5-21-15. Available at: https://www.riigikohus.ee/lahendid?asjaNr=5-21-15/3 ; RKPJK 28.10.2021, 5-21-16. Available at: https://www.riigikohus.ee/lahendid?asjaNr=5-21-16/3 .
267. An overview of the individual election complaints can be found on the homepage of the ESC at: https://www.riigikohus.ee/et/lahendid?aasta=2023&asjaLiigidIds=37100582&defaultPageSize=25&kuvadaVaartus=Pealkiri&pageSize=25&sortAsc=false&sortVaartus=LahendiKuulutamiseAeg&tekst=valimiskomisjon.
268. The respective decision of the ESC can be found at: RKPJKo 30.03.2023, 5-23-20. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=5-23-20/5.
269. See also the corresponding information from the State Court: https://www.riigikohus.ee/et/uudiste-arhiiv/riigikohus-e-haaletus-tuleks-seaduses-tapsemalt-lahti-kirjutada. Further information about the ESC decision to dismiss election complaints: Supreme Court dismisses all election complaints, 30.03.2023. Available at: https://news.err.ee/1608932273/supreme-court-dismisses-all-election-complaints.
270. See also the corresponding information from the State Court: https://www.riigikohus.ee/et/uudiste-arhiiv/riigikohus-e-haaletus-tuleks-seaduses-tapsemalt-lahti-kirjutada. Further information about the ESC decision to dismiss election complaints: Supreme Court dismisses all election complaints, 30.03.2023. Available at: https://news.err.ee/1608932273/supreme-court-dismisses-all-election-complaints.
271. See for more information Why E-participation systems fail: The case of Estonia's Osale.ee./ Toots Maarja in: Government Information Quarterly 36, no. 3 (2019): 546-559.
272. For more detailed information, see: https://rahvaalgatus.ee.
273. Homepage of the e-Governance Academy: Digital Democracy Policy and Framework Development. Available at: https://ega.ee/services/digital-democracy/.
274. For more details see e.g.: E-Estonia Homepage: Factsheet E-Justice. Available at: https://e-estonia.com/wp-content/uploads/2020mar-facts-a4-v04-e-justice.pdf.

permits in certain situations. In one case, such a felling permit was challenged in court by a non-profit organization because, in the complainant's view, the information system was not able to assess both the existing green belt and the bird species nesting there. On this occasion, the court commented for the first time in more detail on the duties incumbent on public authorities in the context of the regulation and use of automated administrative procedures.

In this respect, the court took the view that the procedure in question was not to be classified as unlawful only due to the fact that the automated decision-making was not based on a corresponding legal basis. In particular, the court argued that the automatic decision was not based on the processing of personal data in the present case and therefore Article 22 GDPR did not apply. Nevertheless, the court noted that it cannot be ruled out that also outside the scope of Article 22 GDPR, an appropriate legal basis may in some cases be necessary for making important administrative decisions by means of more complex technologies, such as self-learning algorithms.[275]

However, according to the court's decision, the administrative principles of investigation and caution as well as the obligation to inform the public apply to the administrative procedure and issuance of felling permits regardless of whether the decision to register the forest declaration is taken by an individual public official or by an automated information system. The use of an automated system does – in other words – not in itself relieve the administrative authority of the obligation to comply with any of the relevant legal provisions.[276]

In the case at hand, the court declared unlawful the automated granting of felling permits by the Environment Agency without informing the public beforehand. The ESC found that the lawfulness of automated decisions is the responsibility of the authority implementing the information system, which must ensure that the underlying data used by the information system is accurate, complete and up-to-date, and that the information system complies with all legal standards. If the available technology does not allow these requirements to be met, the decision-making process must involve human intervention, the ESC added.[277]

The second example deals with the so-called consent service, a digital solution introduced by the Estonian public administration in 2021. The consent service gives people the opportunity to decide to share data concerning themselves and available in national databases with the private sector. For example, when applying for instalment payments, there is no need to take the necessary data from the Tax and Customs Board to prove one´s solvency – with the applicant's consent, the bank can quickly and conveniently get the respective information directly from the Tax and Customs Board.[278] With the consent service, a person can also give private entities the right to access one's health data stored in public databases, for example for personalized medicine applications.[279] According to the National Information System Authority, the health sector may be the one profitting most of such a consent service. Although it was already recognised at the beginning of 2021 that the implementation of the consent service would require a change in the law, the system has now been implemented, but the drafting of the bill has not yet been completed.[280]

Particularly in the context of health data and financial services, the practical implementation of

275. RKHKo 28.09.2023, 3-21-979, p 39. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-21-979/44.
276. RKHKo 28.09.2023, 3-21-979, p 39. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-21-979/44.
277. RKHKo 28.09.2023, 3-21-979, p 41. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-21-979/44.
278. Riigi Infosüsteemi Amet. Mis on nõusolekuteenus ja kuidas see kõigile kasu toob? (What is a consent service and how does it benefit everyone?). 08.09.2023. Available at: https://digipro.geenius.ee/blogi/turvalise-e-riigi-blogi/mis-on-nousolekuteenus-ja-kuidas-see-koigile-kasu-toob/.
279. Tervise Arengu Instituut. Tulevikus saab personaalmeditsiini teenuste jaoks anda nõusolekuid Terviseportaalis (In the future, you will be able to give consent for personalised medicine services through the Healthcare Portal). 26.04.2023. Available at: https://www.tai.ee/et/personaalmeditsiini-uudiskirjad/tulevikus-saab-personaalmeditsiini-teenuste-jaoks-anda-nousolekuid.
280. Uus nõusolekuteenus võimaldaks riigi kogutud andmeid jagada ettevõtetega. (New consent service to allow data collected by the state to be shared with businesses). 25.11.2021. Available at: https://www.err.ee/1608414620/uus-nousolekuteenus-voimaldaks-riigi-kogutud-andmeid-jagada-ettevotetega.

such an innovative solution without a corresponding legal basis raises a number of questions. Among other things, the question arises as to what extent a person's consent is actually free if, for example, the granting of a loan depends on it. Similarly, whether people are sufficiently informed about the scope of private companies' right to access their personal data and to what extent there is adequate regulation for legal responsibility and liability in the event that the public institution, for example, provides private third parties with information about the person that results in discriminatory decisions or other legal violations.

4.2 Trust in Public Administration

A functioning public administration is one of the constituent elements of any form of state. Not only this structural permanence, but also the positive relationship of the citizens to their institutions is a core value.[281] According to recent studies, the two most important determinants of citizens' trust in public institutions is the quality of public services and the level of social tensions as perceived by the citizens.[282] Estonia is known for the fact that, on average, its inhabitants have great confidence in data processing by the public sector.

According to a research project conducted by the Estonian Ministry of Justice in 2020, Estonian residents consider the collection of data by the state to be secure. Every third Estonian considers that concerns about personal data protection are overrated.[283] The fact that the state can access an individual's personal data without their consent is generally not considered to be a significant problem. Consequently, the general attitude towards the state combining data from different databases is rather positive. People do rather favour the possibility of combining information from different databases if this serves to improve the provision of services by the public sector.[284] Also in its "Estonia's Digital Agenda 2030" strategy paper, the Ministry of Economic Affairs and Communications draws special emphasis to the importance of ensuring transparency and reliability when implementing new technologies that may have an adverse impact on fundamental rights (e.g. AI, data analytics, etc.).[285]

Transparency is being enhanced by providing people with the possibility to get an overview of the public institutions that use the individual's personal data and on the respective purposes the data is used. With this in mind, the Estonian administration has introduced the so-called data tacker. The data tracker monitors the traffic of an individual's personal data in and out of different databases, extracts the necessary log records and stores them in the tracker. This information is displayed to the citizen on the state portal eesti.ee.[286] For example, the person concerned can see that his or her identity has been checked by the Estonian Police and Border Guard Board at the airport of Tallinn at a certain time. However, it is not mandatory for the administration to connect its databases to the data tracker. Therefore, although the data tracker is a step on the way to more transparency, to date the indicated information does not include all public

281. Vertrauen in die öffentliche Verwaltung–Zwischen Systemstabilität und Modernisierungsdruck. / Rölle, Daniel. In: dms–der moderne staat–Zeitschrift für Public Policy, Recht und Management, 2009, 2(1), p. 27-28.
282. Maintaining trust in a technologized public sector. Policy and Society / Bodó, Balázs; Janssen, Heleen. In: Policy and Society, 41(3), p. 414-429. p. 417.
283. Inimeste privaatsusõigused ja isikuandmete kaitsmine 2020 (People's privacy rights and personal data protection 2020). Webpage of the ministry of Justice of Estonia. 05.11.2020, p.47. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiT7dDakbOCAxVoAxAIHX1yBN4QFnoECA0QAQ&url=https%3A%2F%2Fwww.just.ee%2Fmedia%2F494%2Fdownload&usg=AOvVaw3CFN4NVZUksaT7gBjeQtvq&opi=89978449.
284. Inimeste privaatsusõigused ja isikuandmete kaitsmine 2020 (People's privacy rights and personal data protection 2020). Webpage of the ministry of Justice of Estonia. 05.11.2020, p. 8, 46. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiT7dDakbOCAxVoAxAIHX1yBN4QFnoECA0QAQ&url=https%3A%2F%2Fwww.just.ee%2Fmedia%2F494%2Fdownload&usg=AOvVaw3CFN4NVZUksaT7gBjeQtvq&opi=89978449
285. Estonia's Digital Agenda 2030. Ministry of Economic affairs and Communications development agenda of the field. p. 17. 2021. Available at: https://www.mkm.ee/media/6970/download.
286. Data Tracker. RIA webpage. Available at: https://www.ria.ee/en/state-information-system/people-centred-data-exchange/data-tracker.

databases but only some of them.[287] Considering that the Estonian e-government is largely based on the cross-use of different databases of the public administration, the regulation of mandatory use of the data tracker would be an important means to promote transparency.

The Chancellor of Justice explained in her 2022 annual report, that the e-government opens and speeds up the possibilities of communicating with the state. However, this should not lead to a new type of exclusion, which means that those who are excluded from the digital state can no longer actively participate in society. The opportunity to interact with the state must remain open to all people in Estonia, regardless of whether they are able or want to communicate via e-channels or not. Those who cannot or do not have the opportunity or knowledge to use e-channels must be helped by the state to improve their skills and be made aware of how to use the services the e-government provides.[288]

The Chancellor of Justice also emphasized the need to distinguish automated administrative decisions from decisions taken with the help of artificial intelligence, stating that it is important that the person knows that the decision was made by a machine and that they can challenge it effectively if needed.[289]

Trust in the context of the digitization of public administration is shaken if sensitive personal data falls into the wrong hands or becomes public. In February 2019, a mother sent a rehabilitation plan for her adult daughter with a mental disability to the Social Insurance Board (SKA). However, an employee of the agency forgot to add an access restriction to the information provided, as a result of which the health records described in the plan were publicly available in the online document register for two months. This health data was found in the register by a journalist who wrote a news story about his finding, drawing attention to the question of adequate data protection in general. The SKA restricted access to the data concerned as soon as it found out about the problem. The woman, having learned of the incident from the journalist, sought compensation from the SKA on behalf of her daughter for the non-material damage caused by the disclosure of her health data.[290] In its reply, the agency acknowledged the error and apologized, but refused to pay financial compensation.[291] The administrative and district courts hearing the appeal found that the Agency had acted unlawfully in disclosing the health data, but that financial compensation was not justified in this case.[292] The Supreme Court agreed with the judgment of the lower courts and stressed that it had been established that the data had been checked during its unlawful publicity only seven times in total and that it was not known that it had been accessed by anyone other than the SKA officials and the respective journalist. The SKA had also reacted immediately after learning of the incident and apologized to the complainant. Therefore, according to the Supreme Court, the damage caused did not exceed the threshold for the award of a financial compensation.[293] There have been similar cases, where personal information has been unlawfully openly accessible in public databases, but these cases have not caused general uncertainty in the public administration or digital administration, as research has shown.[294]

287. Usage of personal data. RIA webpage. Available at: https://www.eesti.ee/en/security-and-defense/safety-and-security/usage-of-personal-data.
288. Annual review of the Chancellor of Justice of 2022. p. 23; available at: https://www.oiguskantsler.ee/ylevaade2022/.
289. How to implement artificial intelligence in such a way that human rights are protected? Chancellor of Justice webpage. Available at: https://www.oiguskantsler.ee/en/how-implement-artificial-intelligence-such-way-human-rights-are-protected.
290. RKHK 06.01.2021, 3-19-1207, pt 1-5. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-19-1207/21.
291. RKHK 06.01.2021, 3-19-1207, pt 5. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-19-1207/21.
292. RKHK 06.01.2021, 3-19-1207, pt 7,9. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-19-1207/21.
293. RKHK 06.01.2021, 3-19-1207, pt 26.2. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-19-1207/21.
294. Kaheksa eestlast kümnest usaldab e-teenuseid (Eight out of ten estonians trust in e-services). Sillasoo, Signe. Äripäev. 04.06.2020. Available at: https://www.foundme.io/uudised/2020/06/04/kaheksa-eestlast-kumnest-usaldab-e-teenuseid. See more about cases brought against e-voting: https://www.riigikohus.ee/et/lahendid?tekst=elektroonilised%0D%0A&sortVaartus=LahendiKuulutamiseAeg&sortAsc=false&kuvadaVaartus=Pealkiri&pageSize=25&defaultPageSize=25

4.3 Respect of Citizens' Rights

4.3.1 Fundamental rights protected by the Constitution regarding digitalisation

Also, with a view to digitalisation by the administration, the respect for citizen's rights can be derived from the Constitution (EC). The following constitutional rights have to do with the gathering, receiving, storing and providing of information.

EC § 26 stipulates that *'everyone has the right to the inviolability of private and family life. State agencies, municipalities and their officials shall not interfere with the family or private life of any person except in the cases and pursuant to a procedure provided by law to protect the health, morals, public order, or the rights and freedoms of others, to prevent a criminal offence or to apprehend a criminal offender.'*[295] Informational self-determination also includes a person's right to decide whether and how much of their personal data is collected and stored. Therefore, an important part of the right to private life is also the protection of personal data. EC § 26 protects a person's right to decide to what extent personal data is published[296].

1. In addition to EC § 26, there are other provisions in the Constitution that regulate various aspects of privacy. For example, EC § 43 protects the right to the confidentiality of messages,[297] EC § 33 protects the inviolability of the home[298] and EC § 42 protects Estonian citizens from the collection and storage of data about their various beliefs (religious or philosophical and moral beliefs, political views, etc.).[299]

EC § 44 stipulates that *'everyone has the right to freely receive information disseminated for public use.'* A particular citizens' right to information is specified in section 3 of the paragraph: *'Estonian citizens have the right to access information about themselves held in state agencies and municipalities and in state and municipal archives, pursuant to a procedure provided by law. This right may be restricted on the basis of a law to protect the rights and freedoms of others or the confidentiality of a child's filiation, and in the interests of preventing a criminal offence, apprehending a criminal offender or ascertaining the truth in criminal proceedings.'*[300]

4.3.2 Privacy vs transparency in case-law and opinions

The digitalization of administration poses multiple new questions concerning the protection of personal rights. These problems are most often related to disclosure and processing of personal data.

An example of this is the Estonian regulation on political parties' membership. As already mentioned above (see 3.2.4), the Public Information Act obliges the disclosure of political parties' membership lists.[301] The constitutional conformity of this act was doubted by the Chancellor of Justice in 2003, who stated that political party membership lists should not be disclosed publicly. [302] Later, however, the Chancellor of Justice took the view that since the purpose of political parties is the exercise of state power, the transparency of state power also implies the need to ensure the openness of party members.[303] 2019, briefly before the Estonian parliamentary elections, journalists published online and in the newspaper all party members' names serving

295. The Constitution of the Republic of Estonia, paragraph 26.
296. The Constitution of the Republic of Estonia. Annotated Edition 2020, paragraph 26. Available at: https://pohiseadus.ee/, checked: 07.11.2023.
297. The Constitution of the Republic of Estonia, paragraph 43.
298. The Constitution of the Republic of Estonia, paragraph 33.
299. The Constitution of the Republic of Estonia, paragraph 42.
300. The Constitution of the Republic of Estonia, paragraph 44.
301. Public Information Act, paragraph 28(28).
302. Jõks salastaks erakondade nimekirjad (Jõks would make party lists secret). In: Delfi, 26.07.2003. Available at: https://www.delfi.ee/artikkel/6048372/joks-salastaks-erakondade-nimekirjad.
303. The Chancellor of Justice's opinion nr 6-1/080996/00808156 of 28 November 2008. Available at: https://www.oiguskantsler.ee/et/seisukohad/seisukoht/vastuolu-puudmine-erakonnaliikmete-nimekirjade-avalikustamine-0.

sentences and those with valid and time-barred offences and misdemeanours, including the acts committed by them.[304] Although it was mentioned on the fringes of the discussion that the especially the disclosure of those people whose conviction was already time-barred might be very unpleasant for them, the public as well as the parties did generally not call into question the behaviour of the journalists. There were also no debates concerning the legality of such a disclosure, as the journalists' investigations were clearly in line with current law. According to the Criminal Records Database Act, the person's name in the respective court decision shall be replaced by initials after the punishment has been time-barred. Anyhow, this regulation does not apply for certain offences, including murder, manslaughter, and offences against minors, but also trafficking of narcotics, affiliation in criminal organisations and money laundering.[305] Everyone has the right to access the databases' information freely, as far as concerns themself or a legal person. If information concerning another natural person is requested, the legal basis or objective of requesting the data has to be confirmed in the query.[306]

The publication of infringements has also been applied by administrative bodies. For example, in the beginning of the 2000s, the city of Tartu disclosed the information of debtors to the city and the Estonian police published information of people who committed drunk driving. As such measures were based on administrative practice only, they were abandoned with the legal anchoring of digital administration.[307]

Court rulings are generally public.[308] Court decisions that have entered into force are required to be made public online, whilst taking into account disclosure restrictions that arise from other provisions.[309] The information shall be disclosed on a website or through a link to a webpage through which the data can be accessed.[310] The Ministry of Justice has attempted to implicate stricter conditions for the publication of criminal court rulings on several occasions. However, this proposals have been met with criticism by the public and the media as restricting the freedom of the press and information and have not been approved by the parliament.[311] However, the personal identification number and name or date of birth of an underage accused are replaced by initials or a character sign, except if the disposition to be made public is at least the third one convicting the minor of a criminal offence.[312] In civil procedures, the data subject's name is replaced with initials or an alphabetic character and their personal identification number, date of birth, registration number or address are not published if the data subject requests so.[313] In administrative procedures, per request of the data subject, the name of the data subject is replaced by initials or a sequence of letters, and their personal identification code, date of birth, registration number, address or other particulars which would permit specific identification of the data subject are not published.

Since 2017, to combat the issue of youth neither in employment nor in education or training (*NEET youth*), local authorities can let automatically screen their local inhabitants up to twice per calendar year for young people between the age of 16 and 26 who match the NEET criteria and then proactively contact the individual possibly in need. The individual has the right to decline the

304. Paper: Over 300 Centre members carrying criminal punishments / ed. Vahtla, Aili. In: ERR, 08.02.2019. Available at: https://news.err.ee/908958/paper-over-300-centre-members-carrying-criminal-punishments; More than 400 Reform members have criminal record, 233 serving sentence / Cavegn, Dario. In: ERR, 06.02.2019. Available at: https://news.err.ee/907867/more-than-400-reform-members-have-criminal-record-233-serving-sentence.
305. Criminal Records Database Act, paragraph 28. Available at: https://www.riigiteataja.ee/akt/114032023027.
306. Criminal Records Database Act, paragraph 15(1).
307. Estonia, the Digital Nation - Reflections of a Digital Citizen's Rights in the European Union / Tupay, Paloma Krõõt, p. 12–13.
308. The Constitution of the Republic of Estonia, paragraph 24.
309. Public Information Act, paragraph 28(1)(29).
310. Public Information Act, paragraph 29(1).
311. See in more detail: Estonia, the Digital Nation - Reflections of a Digital Citizen's Rights in the European Union / Tupay, Paloma Krõõt, p. 9-10.
312. Code of Criminal Procedure, paragraph 408^1(2). Available at: https://www.riigiteataja.ee/akt/111032023026.
313. Code of Civil Procedure, paragraph 462(2).

processing of their personal data but in this case, the respective information on the decline remains in the database until the person's 27th birthday.[314] The Chancellor of Justice has questioned the proportionality of this regulation with a view to one's right to privacy.[315] However, the law not been contested in court.[316]

The Chancellor of Justice has had to deal with a number of appeals concerning a person's place of residence which in some of the online public state registers is openly displayed. For example in the public online business register, the name and personal identification number of the natural person associated with a company as well as its registered office and address are displayed.[317] In some instances, the personal data of natural persons is also published in the online register of economic activities, where the contact details of the entrepreneur (telephone number, e-mail address and postal address) are entered.[318] Individuals who contacted the Chancellor of Justice were disturbed by the disclosure of their personal data, primarily as this registers disseminate their public data to numerous online directories and economic information portals, which are also covered by the google search engine.[319] The Chancellor of Justice stressed that in some instances self-employed persons have no choice but to register a business at their home address. However, a person's home address constitutes personal data and is therefore protected by the fundamental right to privacy. The Chancellor of Justice questioned whether the data collected must be publicly available to anyone for enquiries and also completely downloadable from the register of economic activities, asking both the Minister of Justice and the Ministry of Economic Affairs and Communications to justify the publication of residence data on the Internet.[320] In its reply, the Ministry of Justice admitted that the same problem also occurs in other cases, e.g. in the case of limited liability companies with only one shareholder, as well as in the case of non-profit organisations with a single board member that do not have a separate office. The Ministry of Justice announced its intention to analyse the issue raised and its possible solutions in the framework of the revision of company law.[321] However, the matter has not yet been resolved.

4.3.3 Case-law regarding the infringement of fundamental rights due to digitalization

Digitalization and the processing of data as an infringement of fundamental rights has been a subject of examination for the Supreme Court of Estonia on several occasions. The court has stated that the *'collection, storage, use and disclosure of personal data is considered to be an infringement of the right to respect of privacy, among other things.'*[322]

In one case the Supreme Court had to decide upon, the Tartu municipality government refused against the instruction of the Data Protection Inspectorate to share upon request information on the wages for municipal employees in a personalized form. According to the law, the municipality only has the obligation to make salary data of the municipalities' officials public. However, the

314. Social Welfare Act, paragraph 15[1]. Available at: https://www.riigiteataja.ee/akt/130062023073.
315. Arvamus maksukorralduse seaduse ja sotsiaalhoolekande seaduse muutmise seaduse eelnõu kohta (Opinion on the draft law amending the Taxation Act and the Social Welfare Act). Available at: https://www.oiguskantsler.ee/et/seisukohad/seisukoht/arvamus-maksukorralduse-seaduse-ja-sotsiaalhoolekande-seaduse-muutmise-seaduse.
316. Estonia, the Digital Nation - Reflections of a Digital Citizen's Rights in the European Union / Tupay, Paloma Krõõt, p. 14.
317. Commercial Code paragraph 28 (1), 75(2). Available at: https://www.riigiteataja.ee/akt/123122022034.
318. General Part of the Economic Activities Code Act, paragraphs 51, 14, 15(1), 15(2). Available at: https://www.riigiteataja.ee/akt/106042021005.
319. Õiguskantsler. Füüsilisest isikust ettevõtjate andmete avaldamine (The Chancellor of Justice. Publication of self-employed data) nr 14-3/200725/2004572, 24.08.2020. Available at: https://www.oiguskantsler.ee/sites/default/files/field_document2/F%C3%BC%C3%BCsilisest%20isikust%20ettev%C3%B5tjate%20andmete%20avaldamine.pdf.
320. Õiguskantsler. Füüsilisest isikust ettevõtjate andmete avaldamine (The Chancellor of Justice. Publication of self-employed data) nr 14-3/200725/2004572, 24.08.2020. Available at: https://www.oiguskantsler.ee/sites/default/files/field_document2/F%C3%BC%C3%BCsilisest%20isikust%20ettev%C3%B5tjate%20andmete%20avaldamine.pdf.
321. Justiitsministeerium. Vastus märgukirjale (Ministry of Justice. Response to the letter) nr 10-4/5090-2. Available at: https://adr.rik.ee/jm/dokument/7513099.
322. RKHKo 12.07.2012, 3-3-1-3-12 pt. 19. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-3-1-3-12.

law does not regulate the possible communication of information concerning the wages of the employees of local governments. The Supreme Court stated that in the case at hand, two conflicting fundamental rights collided: the right to receive information from the local government about its activities (EC § 44 (2)) and the right of the local government's employees to privacy (EC § 26). However, the court decided that to ensure transparency of the use of local government property and to prevent corruption, the wages of the respective employees are information the local government is obliged to share upon request.[323] The public interest to information prevails insofar over the personal interest in privacy.

In another case, the Supreme Court analysed the constitutionality of a legal regulation obliging non-profit associations to submit their annual report electronically or through a notary for an additional fee of approximately 25 euros. Annual report submitted to the registrar on paper were not accepted and returned. The court found that the contested regulation violated the freedom of association, as it did not give non-profit associations the possibility to remedy their deficiency and therefore contradicted i.a. the principle of fair procedure, especially in the case at hand where the infringement could lead to a fine or even the deletion of the non-profit association from the register.[324] However, the Supreme Court *en banc* did not generally find the obligation to submit annual reports exclusively in an electronic form an unproportional infringement of the freedom of association. The court ruled the regulation demanding the presentation of annual reports exclusively in electronic form constitutional, as the law makes administration more uncomplicated and more effective and reporting more transparent and comparable.[325] The majority of judges did not agree with the claimant's view that the regulation could prove too burdensome for a small non-profit association which did not act for the public benefit nor carry out any economic activity.[326] Therefore in this case at, in the court's view, the interest of the public prevailed over possible individual legal limitations.

The Supreme Court has also in a recent court ruling for the first time dealt with issues concerning automated decision-making by the public authorities. In this case relating to felling permits (the case is discussed in more detail above, see 4.1.2), the court drew attention to the necessity of paying adequate attention to the principles of citizen-centric public administration also in the context of technological innovation.

5. The possible impact of the EU's envisioned AI Act on Estonian Administrative Law

5.1 Estonia's opinion on the EU's envisioned AI Act

The 'White Paper on Artificial Intelligence: a European approach to excellence and trust' was published by the European Commission in February 2020.[327] In April 2021, the European Commission published the "Artificial Intelligence Act, AIA proposal", a draft act for an AI regulation. According to the proposal, the AI Act will apply to public and private actors inside and outside of the EU, under the condition that users of AI systems are located within the Union.[328]

323. RKHKo 17.10.2018, 3-15-3228 pt. 15. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=3-15-3228/37.
324. RKÜKo 2.10.2018, 2-17-10423, pt. 43, 59.3. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=2-17-10423/20.
325. RKUKo 2.10.2018, 2-17-10423, pt. 46, 59.1. Available at: https://www.riigikohus.ee/et/lahendid?asjaNr=2-17-10423/20.
326. For more details see also: Estonia, the Digital Nation - Reflections of a Digital Citizen's Rights in the European Union / Tupay, Paloma Krõõt, p. 14.
327. European Commission, White Paper on Artificial Intelligence A European approach to excellence and trust, COM(2020) 65 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0065 .
328. 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 art 2(1b). Brussels, 21.4.2021, COM(2021) 206 final, 2021/0106(COD). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206.

The Estonian Government submitted its opinion on the planned AI Act in October 2020, declaring its general support for the proposal's aim to create a harmonised legal framework for AI and a risk-based approach as well as the prohibition for public authorities to use AI systems for social scoring based on the individual's behaviour. Estonia also agreed on advancing the EU's digital single market and mitigating risks that may derive from specific technologies. However, Estonia drew attention to the fact that the proposed legislation should be technology-neutral, efficient and worded in a future-proof way. Above that, Estonia proposed to narrow the scope of regulation, as in Estonia's view, the proposed definition for AI systems could otherwise lead to a too comprehensive understanding of AI and thus hinder legal clarity and uniform implementation of the regulation.[329] This proposal explicitly aimed to include approaches not traditionally categorised as AI systems, for example, statistical approaches, search and optimisation methods and certain logic and knowledge-based techniques. Estonia further noted that AI used for military objectives and autonomous weapon systems and AI used solely for national security should be outside the scope of regulation for the proposed AI Act and supported the drafting of separate legislation for using AI by law enforcement agencies.[330] Additionally, Estonia stated that the Act should include serious crimes of national importance, such as crimes against the state, in the list of crimes that permit real-time detection.[331] In Estonia's view, the restrictions imposed by the regulation in the field of law enforcement must not unduly hamper criminal proceedings or the ability of a Member State to fight crime.[332]

According to the explanatory memorandum on the Estonian opinion, the proposed AI Act would significantly impact the organisation of state institutions and local governments and the costs and revenues of the Estonian public sector.[333] The most affected institutions would be the ones using AI systems classified as high-risk. Approximately 40% of the AI solutions used by the public sector in Estonia can be qualified as such.[334] In Estonia's opinion, implementing the AI Act will

329. Eesti seisukohad Euroopa Parlamendi ja nõukogu määruse, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte (COM(2021) 85 final), eelnõu kohta (Estonia's views on the draft regulation of the European Parliament and of the Council providing for harmonized legal norms on artificial intelligence (artificial intelligence legislation) and amending certain Union legislation (COM(2021) 85 final), pt. 3.2., 5.2., 5.3., 5.9. available at: https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/458a144b-2a6e-4d67-a8aa-10994c5b94de/eesti-seisukohad-maaruse-millega-nahakse-ette-tehisintellekti-kasitlevad-uhtlustatud-oigusnormid-eelnou-kohta--com2021-206.
330. Eesti seisukohad Euroopa Parlamendi ja nõukogu määruse, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte (COM(2021) 85 final), eelnõu kohta (Estonia's views on the draft regulation of the European Parliament and of the Council providing for harmonized legal norms on artificial intelligence (artificial intelligence legislation) and amending certain Union legislation (COM(2021) 85 final), pt. 5.5., 5.11. available at: https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/458a144b-2a6e-4d67-a8aa-10994c5b94de/eesti-seisukohad-maaruse-millega-nahakse-ette-tehisintellekti-kasitlevad-uhtlustatud-oigusnormid-eelnou-kohta--com2021-206.
331. Eesti seisukohad Euroopa Parlamendi ja nõukogu määruse, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte (COM(2021) 85 final), eelnõu kohta (Estonia's views on the draft regulation of the European Parliament and of the Council providing for harmonized legal norms on artificial intelligence (artificial intelligence legislation) and amending certain Union legislation (COM(2021) 85 final), pt. 5.10. available at: https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/458a144b-2a6e-4d67-a8aa-10994c5b94de/eesti-seisukohad-maaruse-millega-nahakse-ette-tehisintellekti-kasitlevad-uhtlustatud-oigusnormid-eelnou-kohta--com2021-206.
332. Eesti seisukohad Euroopa Parlamendi ja nõukogu määruse, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte (COM(2021) 85 final), eelnõu kohta (Estonia's views on the draft regulation of the European Parliament and of the Council providing for harmonized legal norms on artificial intelligence (artificial intelligence legislation) and amending certain Union legislation (COM(2021) 85 final), pt. 11. available at: https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/458a144b-2a6e-4d67-a8aa-10994c5b94de/eesti-seisukohad-maaruse-millega-nahakse-ette-tehisintellekti-kasitlevad-uhtlustatud-oigusnormid-eelnou-kohta--com2021-206.
333. Eesti seisukohad Euroopa Parlamendi ja nõukogu määruse, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte (COM(2021) 85 final), eelnõu kohta (Estonia's views on the draft regulation of the European Parliament and of the Council providing for harmonized legal norms on artificial intelligence (artificial intelligence legislation) and amending certain Union legislation (COM(2021) 85 final), pt. 4.4. available at: https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/458a144b-2a6e-4d67-a8aa-10994c5b94de/eesti-seisukohad-maaruse-millega-nahakse-ette-tehisintellekti-kasitlevad-uhtlustatud-oigusnormid-eelnou-kohta--com2021-206.
334. What can Estonian experience offer for the European AI regulation? / Vihma, Peeter, 2022. Available at: https://investinestonia.com/what-can-estonian-experience-offer-for-the-european-ai-regulation/.

require notably higher one-time and ongoing costs for the authorities of member states than the Commission has accounted for.[335]

5.2 The EU's envisioned AI Act's impact on Estonian national legislation

Estonia does currently not have any specific national legislation on the development and use of AI.[336]

In May 2019, the Estonian AI Taskforce released a report, according to which there was no need for a harmonised national legal act on AI. It was argued that as AI executes tasks decided by humans and there are no "super agents" that operate independently from them, AI's actions could be attributed to the respective AI's user, be it public or private. With a view to the broader implementation of AI solutions, amendments concerning the wider possible use of AI, in addition to that connected questions on liability and rules and limitations for AI development were proposed.[337]

Estonia's National AI Strategy, published in July 2019, concluded that fundamental changes to the basics of the judicial system are not necessary. Still, a few amendments to different laws should be made, and the Ministry of Justice was to prepare the legislation bill for further adoption of AI.[338]

In 2020, however, the Ministry of Justice comprehensively analysed possible legal regulations on algorithmic systems. The report concluded that algorithmic systems need separate legal rules depending on the level of risk their use provides for fundamental rights. The primary purpose of an Estonian AI Act was seen to give transparency and better citizen rights protection.[339] However, especially with a view to the upcoming proposal on an AI Act by the European Commission, it was decided to put the development of a national regulation of algorithmic systems on hold.[340]

Estonia has opted for the sake of harmonisation and, to avoid contradictory regulations, decided to wait for the respective regulation at the EU level. However, within national law, the lawmaker has solved specific regulatory issues. In this regard, one of the current aims is to amend the Administrative Procedure Act, establishing a general rule concerning the possibility (basis of) and legal framework to issue automatic administrative acts (see also in more detail above, C.II.2.).

The Ministry of Economic Affairs and Communications, as a leader in the development of the e-state, has prepared several instructions regarding i.a. data management, artificial intelligence, data protection and project implementation.[341]

---

335. Eesti seisukohad Euroopa Parlamendi ja nõukogu määruse, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) ja muudetakse teatavaid liidu õigusakte (COM(2021) 85 final), eelnõu kohta (Estonia's views on the draft regulation of the European Parliament and of the Council providing for harmonized legal norms on artificial intelligence (artificial intelligence legislation) and amending certain Union legislation (COM(2021) 85 final), pt. 4.2.. Available at: https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/458a144b-2a6e-4d67-a8aa-10994c5b94de/eesti-seisukohad-maaruse-millega-nahakse-ette-tehisintellekti-kasitlevad-uhtlustatud-oigusnormid-eelnou-kohta--com2021-206.
336. Artifical Intelligence and Machine Learning Powered Public Service Delivery in Estonia. Oppurtunities and Legal Challenges. / Ebers, Martin; Tupay, Paloma Krõõt. ed. / Giovanni Comandè, Martin Ebers, Mimi Zou. Vol. 2 Springer, 2023. p. 44.
337. Report of Estonia's AI Taskforce. May 2019, p. 38. Available at: https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_486454c9f32340b28206e140350159cf.pdf.
338. Estonia's national artificial intelligence strategy 2019-2021, p. 10. Available at: https://f98cc689-5814-47ec-86b3-db505a7c3978.filesusr.com/ugd/7df26f_27a618cb80a648c38be427194affa2f3.pdf.
339. Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus („krati VTK") (Intention to develop regulation of effects of algorithmic systems ("krati VTK")), p. 22-23. Available at: https://projektid.edu.ee/download/attachments/48268843/Krati%20VTK.pdf?version=1&modificationDate=1598951601618&api=v2.
340. For further details see: Artifical Intelligence and Machine Learning Powered Public Service Delivery in Estonia. Oppurtunities and Legal Challenges. / Ebers, Martin; Tupay, Paloma Krõõt. ed. / Giovanni Comandè, Martin Ebers, Mimi Zou. Vol. 2 Springer, 2023. p. 45.
341. Majandus- ja Kommunikatsiooniministeerium. Juhendmaterjal krattide hankimiseks. (Ministry of Economic Affairs and Communications. Guidance material for procurement of artificial intelligence systems) November 2019. Available at: https://www.kratid.ee/juhised.

Estonia has also drafted voluntary procurement guidelines, which indicate frequent problems and solutions in data science projects.[342] Additionally, the Estonian Government is working on a self-assessment questionnaire for developers of AI and on a national metadata standard and data quality framework.[343]

It can therefore be concluded that although Estonia supports an EU-wide harmonised regulation to ensure a common market and to increase acceptance of AI by minimising risks, but a concern is that definition of AI may be too wide. A risk-based approach is supported.[344]

6. Pro's and Con's of National Legislative Reforms to Digitize Administrative Law, including questions of harmonisation

Digital development at the national level has enabled Estonia to establish its unique selling point as a digital pioneer. As explained above, the digitalisation of administrative tasks makes it possible to apply for benefits in an online environment, access one's data and check its accuracy whenever wanted, and access a wide range of public information. In the age of artificial intelligence and algorithmic decision support, this also means the possibility of mass processing of various types of data to identify actual or potential offenders, to profile and identify people in need of advice, and the provision of so-called proactive services on the basis of automatic risk-assessment. These new possibilities have both positive and negative effects on people's fundamental rights, including data protection issues.

As shown in the report at hand, it has been and will likely also in future be in the interest of Estonia to apply a variety of algorithmic decision support tools and artificial intelligence applications to reduce bureaucracy and make administration more efficient, but also to create more opportunities for people to access services of public administration, for example by the use of chatbots. This probably also applies to many other EU Member States. As digital solutions relieve the burden on the state budget and public resources, their increasingly widespread use is to be expected. However, Estonian experience also shows that the need to maintain, update and secure digital solutions also entails new and additional costs and complementary human resources in the IT sector.[345]

All EU Member States are again bound by their membership to the EU and the therewith connected obligation to follow EU law and accept its primacy. Creating a common legal framework for data protection, laid down in the GDPR, has proven successful.

Based on that, the EU has proceeded to set global standards with its legal proposals for a Digital Markets Act, the Digital Services Act,[346] and the Data Governance Act.[347] All these intend to facilitate and boost the reuse and sharing of data and in addition to that also the implementation and use of AI. Although the legislative initiatives mentioned are aimed at the private sector, their impact is wider than this. For example, the Data Governance Act also contains regulations on the use of data in the public domain, while other regulations require

342. Majandus- ja Kommunikatsiooniministeerium. Juhendmaterjal krattide hankimiseks. (Ministry of Economic Affairs and Communications. Guidance material for procurement of artificial intelligence systems) November 2019. Available at: https://www.kratid.ee/juhised.
343. Estonia AI Strategy Report. Available at: https://ai-watch.ec.europa.eu/countries/estonia/estonia-ai-strategy-report_en.
344. See also: What can Estonian experience offer for the European AI regulation? / Vihma, Peeter, 2022. Available at: https://investinestonia.com/what-can-estonian-experience-offer-for-the-european-ai-regulation/.
345. See e.g.: The National Audit Office analysed why the state's software development projects fail at times. / Webpage of the National Audit Office. 9.11.2019. Available at: https://www.riigikontroll.ee/Suhtedavalikkusega/Pressiteated/tabid/168/557GetPage/1/557Year/-1/ItemId/1077/amid/557/language/en-US/Default.aspx.
346. European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.
347. European Commission, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final.

control by the public sector. In part, this results in a double expectation on the public administration of the member states: On the one hand, they should vouch for data protection, but on the other hand, they should, in turn, make data available on a larger scale. It is therefore not always easy for the Member States to implement the EU's political objectives in matters of data use without contradictions.

As previously in the economic area of the EU internal market, the EU now also hopes to succeed in the (global) field of data markets and AI without giving up on the fundamental values of the Union, especially the protection of individuals' rights and freedoms.[348] With this in mind, the EU Commission has drafted its proposal for regulating AI.

For Estonia, a small country far north in the EU, participation in the common market and its regulation is of essential economic, legal and even existential importance. Nevertheless, as this study shows, the understanding of data processing and its use in Estonian politics and society differs considerably in certain aspects from that of other EU states and the EU itself. The openness and tolerance towards far-reaching data processing, which forms the basis of Estonia's success as a digital pioneer, is only sometimes reflected in other countries' legal cultures or EU law. For example, the German legal system and society attach far greater importance to data protection.[349]

Despite these differences, the regulation of digitisation within the EU sets a framework for legally uniform standards, thus facilitating data traffic within the Union and enabling more effective global action. At the same time, EU law leaves room for national specificities and integrates various aspects of data processing. While Estonia, for example, has set a standard for data processing throughout Europe with its successful once-only approach, the EU's framework in data protection has also increased the corresponding security of Estonian data subjects.

Supplementary legal standards regulating data traffic in the Nordic-Baltic area would likely make data exchange between these countries, the majority of which are also EU members, due to additional regulations, rather more difficult than more accessible. However, the Nordic-Baltic states also have several common features that could make closer cooperation in digital administration beneficial for them. Most Nordic countries are characterised in particular by their broad understanding of transparent administration and openness to implementing digital solutions in the public sector. Several examples of successful joint projects in digital administration can be cited, for instance, between Estonia and Finland. Among others, implementing the Estonian X-road solution also in Finland created a prerequisite for providing interoperable cross-border services for people in Estonia and Finland regardless of their place of residence, for example, concerning the provision of medical services.[350]

In this sense, Nordic-Baltic states' digital development in public administration can certainly benefit from an active exchange of knowledge and experience and exploring opportunities for cooperation between them. Active cooperation can also help to assert common interests and priorities at EU level. This particularly in view of the abovementioned fact that data processing at EU level does often leave room for specific approaches and solutions.[351]

---

348. Artifical Intelligence and Machine Learning Powered Public Service Delivery in Estonia. Oppurtunities and Legal Challenges. / Ebers, Martin; Tupay, Paloma Krõõt. ed. / Giovanni Comandè, Martin Ebers, Mimi Zou. Vol. 2 Springer, 2023. p. 217 f.
349. Compare e.g.: Tupay PK, Monika M (2015). Der estnische E-Staat - Zukunftsweisendes Vorbild oder befremdlicher Einzelgänger. Osteuropa Recht 1, pp 2-33.
350. Joint data platforms as X factor for efficiency gains in the public sector? Tonurist, Piret, Veiko Lember, and Rainer Kattel. No. 70. TUT Ragnar Nurkse Department of Innovation and Governance, 2016, p.18; See also about Estonian-Finnish cooperation "Challenges in knowledge sharing for innovation in cross-border context." Lepik, Katri Liis, and Merle Krigul. International Journal of Knowledge-Based Development 5, no. 4 (2014): 332-343; "The Case of Helsinki-Tallinn (Finland-Estonia) – Regions and Innovation: Collaborating Across Borders", Nauwelaers, C., K. Maguire and G. Ajmone Marsan. OECD Regional Development Working Papers, 2013/19, OECD Publishing. Available at: http://dx.doi.org/10.1787/5k3xv0lrt1r6-en.
351. Finnish cooperation "Challenges in knowledge sharing for innovation in cross-border context." Lepik, Katri Liis, and Merle Krigul. International Journal of Knowledge-Based Development 5, no. 4 (2014): 332-343; "The Case of Helsinki-Tallinn (Finland-Estonia) – Regions and Innovation: Collaborating Across Borders", Nauwelaers, C., K. Maguire and G. Ajmone Marsan. OECD Regional Development Working Papers, 2013/19, OECD Publishing. Available at: http://dx.doi.org/10.1787/5k3xv0lrt1r6-en.

FINLAND

Regulation and Doctrinal Challenges of Automated Decision-Making in Public Administration

Sofia Heikkonen, Ida Koivisto and Riikka Koulu

Abstract

In this chapter, we discuss the digital public administration in Finland from the perspective of automated decision-making. The digitalisation of public administration has been kicked into high gear within the last couple of decades and digital technologies have been adopted to assist and replace previous analogic public administrative work. New national legislation enabling the use of automated decision-making has been passed and multiple EU law instruments apply in the field and continue to do so. In this chapter we present, analyse and elaborate the legal landscape of digital public administration in Finland. The overview of the legal landscape shows the importance of understanding the adopted technology not only in relation to the applicable rules, but also in the deeper logics of administrative law as well as the situation-specific requirements within the administrative processes. Our focus is on a new national legislation which allows the use of automated decision-making in Finnish public administration. However, this is not the only framework which is applicable to digital administration. Instead, at the same time, the technologies used in public administration are contextually dependent on the logics of the administrative legal system and the specific material task that the technology is equipped to perform. That being the case, closer Nordic collaboration could be investigated further because of the cultural, linguistic, and legal similarities.

1. Introduction

The administration of Finland is going digital. In recent years, Finland has been taking important steps in digitalisation, although it has not always been easy or unproblematic. The digitalisation of public administration in general and legislation enabling automated decision-making (ADM) specifically have been pressing issues in legal and political discourses. In the wake of the parliamentary election held in spring 2023, new paragraphs in the Administrative Procedure Act and Information Management Act were adopted only days before the end of the previous Prime

Minister Sanna Marin's government. This means that the legislation enabling automated decision-making in public administration finally came into force and effect, although paradoxically, this does not mean the inception of such decision-making, as we will explain later.

This digitalisation enthusiasm is no wonder. Technological development has been astounding in recent decades, enabling both private enterprises and public administration to improve their performance and to make cost savings. Additionally, societally Finland can be considered to be fruitful soil for digital public administration. Its low societal hierarchy, light administration, small population, high societal trust, and self-service culture have paved the way for digitalisation. In the Marin governmental programme, one of the ambitions was to turn Finland's public administration into the best in the world. To that end, digitalisation was one of the key components. In the programme, the government promised that Finland would develop a legal environment in a way that would enable digitalisation, sustainable development and an extensive culture of experimentation.[352]

Despite this political mandate and high hopes, digitalisation has also faced some hurdles. First, as a member of the EU Finland is subject to EU legislation. This means that the General Data Protection Regulation (GDPR)[353] in all its complexities is directly applicable, when it comes to regulating automated decision-making, as we will explain later. Secondly, the compatibility with the national legal system has proven a tough nut to crack. The legislative process has shown how human agents have a legally privileged role in administrative law in terms of both power and responsibility. It is important to emphasise that legal systems do not consist only of legislation and case law but also of concepts and principles with deeper and longer roots in the self-understanding of the system. This is to say that digitalisation forces legislators to ponder some fundamental assumptions of administrative law, which in the analogue world would remain dormant. Recent legislation process has caused some of them to surface, such as the nature of administrative discretion, the concept of an administrative decision, and the personal nature of criminal liability in office. These assumptions have further translated into problems requiring legal solutions.

Besides the obligations laid down in the GDPR, Finland also has national ambitions on how to design a functioning automated administration. The Finnish legal system includes a doctrinal speciality that plays a significant role: the right to good administration. Good administration is a fundamental right in Finland,[354] and hence, digital administration must be good digital administration. Nevertheless, good administration is a manifold concept. In addition to a fundamental right, it can also be understood as a vocabulary of ethics, of economic efficiency, and even of societal development.[355] Importantly, good administration may both legitimise and hinder further digitalisation. Therefore, how good administration is understood as an administrative ideology further affects how the digitalisation of administration is legitimised and imagined in Finland.[356]

In this chapter, we present, analyse, and problematise the legal landscape of the Finnish digital public administration. By automated decision-making (ADM), we mean making fully automated administrative decisions without immediate human oversight or other involvement. We show that legal requirements on how to regulate the matter come from a variety of directions: from the EU, from international human rights duties, from national constitutional provisions and

352. Prime Minister Sanna Marin's government programme, 10 December 2019. p. 107.
353. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
354. Section 21.2 in the Constitution of Finland (hereafter, the Constitution).
355. Varieties of Good Governance: A Suggestion of Discursive Plurality. / Koivisto, Ida. In: International Journal for the Semiotics of Law, No. 27, 2014; From Moral Rules to Individual Rights – and Beyond? The Institutionalisation of Good Administration in Finland and in Europe. / Koivisto, Ida. In: Förvaltningsrättslig tidskrift, No. 1, 2018.
356. Imaginaries of Better Administration: Renegotiating the Relationship between Citizens and Digital Public Power. / Esko, Terhi; Koulu, Riikka. In: Big Data & Society, No. 1, 2023; Miten Hyvä Hallinto Digitalisoidaan? Haaste Oikeustieteelliselle Tutkimukselle. / Koivisto, Ida; Koulu, Riikka. In: Lakimies, No. 118, 2020.

administrative legal doctrine. Not to mention that what is doable in technology does not automatically translate into acceptable legislation and legal practices. We also show that recently, the main battles over whether, or how, to digitalise administration, have mostly already been fought. However, describing those battles illustrates how the Finnish legal system deals with legal irritants such as ADM. That said, although the ADM legislation is brand new in Finland and therefore lacks case law, it shows that ADM in public administration is possible without sacrificing the integrity and identity of administrative law.

The article is organised as follows. In section 1, we outline the administrative framework in Finland. We begin by describing the public bodies that constitute the various levels of state and local administration. This is to show that many public bodies are responsible for applying or overseeing the application of administrative legislation, including rules on ADM. In their various roles, these public bodies participate in shaping the adoption of digital and datafied technologies within public administration. Second, we briefly describe the legal sources, including international treaties, primary and secondary legislation of the EU, as well as the national constitutional and administrative legislation. The very fact that so much legislation exists demonstrates that ADM is not deployed within a legal void but instead, it needs to adhere to an extensive pre-existing legal framework.

In section 2, we describe the newly adopted legislation, which enables the use of ADM in public administration. We discuss how the legislative reform focused on issues of discretion, transparency, and personal accountability of civil servants, the last of which is a constitutional prerequisite of all administrative decision-making in Finland. A focal decision made in the reform was to define ADM as a rule-based system. This means excluding data-driven or AI techniques and decision types which require human discretion. Another point of interest in the drafting of the Finnish ADM legislation concerns the scope and framing of digital public administration: the need to establish national rules for ADM led also to regulating more broadly the use of digital systems in terms of information management. As a result, the new general administrative legislation also created new legal concepts, such as 'a decision to deploy an ADM system' or 'processing rules'.

In section 3, we deliberate on the effects of the upcoming Artificial Intelligence Act (AIA) on the Finnish legislation. From the Finnish perspective, one of the main issues concerns the scope of the AIA. The Finnish position was discussed and established in the Parliament in autumn 2023 and is to exclude the inclusion of rule-based systems from the definition of AI in the Act. If rule-based systems were included in the AIA, this would mean regulatory overlap and a potential need to revise the national legislation. So far, this is yet to be seen.

In section 4, we shift the level of abstraction. We discuss and position the challenge ADM poses on Finnish administrative law from two theoretical perspectives: those of legal evolution and socio-technical change. By applying legal philosopher Kaarlo Tuori's theory of critical legal positivism, we locate these ADM-related challenges not only at the law's surface level – legislation and cases – but also at the deeper levels of legal culture and the deep structure of the legal system. As it teases out and challenges embedded assumptions about the human subject, accountability, and justification, this analysis provides a theoretical understanding of why ADM invokes so many fundamental questions. Furthermore, we describe how the legal language of automation adopts new, technologically-oriented concepts, which become decisive tools for implementing the principles of good administration into administrative practice. We exemplify these changes by the growing importance of user interfaces and usability metrics for the digitalisation of public administration.

In section 5, we present some preliminary insights on collaboration between the Nordic and Baltic countries in relation to digital administration. In section 6, we provide a short conclusion.[357]

357. All online sources were last accessed 15 November 2023.

2. The Administrative Framework in Finland

Finland is a sovereign republic, based on democracy, the rule of law, the inviolability of human dignity and the rights and freedoms of individuals.[358] It is important to note that the Europeanised constitutional culture in Finland is quite young. Following joining the European Convention on Human Rights (ECHR), Finland renewed its catalogue of fundamental rights. The fundamental rights reform in 1995 confirmed a list of rights, which were included without change in the new Constitution of 2000.[359] In section 2, the Constitution lists 18 basic rights of individuals. These include equality (Section 6), the right to privacy (Section 10), freedom of expression (Section 12), the right of access to information (Section 12), protection of property (Section 15), the right to one's language and culture (Section 17), the right to work (Section 18), the right to social security (Section 19), and protection under the law (Section 21), among others. All the rights and freedoms listed in the Constitution must be followed in all state actions, including in the administrative field. Furthermore, ratified international human rights agreements have been integrated into the Finnish legal system, providing an avenue for strengthening them in the legal order. The most notable one in this respect is the ECHR and its multiple Protocols.

Unsurprisingly, these domestic rights and liberties are similar to the ones enshrined in the ECHR and the Charter of Fundamental Rights of the European Union (Charter).[360] While that is the case, the catalogues of rights are not identical. For example, the right to good administration (Section 21 in the Constitution of Finland), is not found in the ECHR. Good administration is an umbrella concept for a set of procedural rules and principles for administrative discretion. The right to good administration in Finland took shape without immediate international influence during the fundamental rights reform. It also had long roots in Finnish 'ombudsprudence'; the concept and its interpretation served as a predecessor of an Administrative Procedure Act. In recent decades, good administration has become one of the more influential principles governing administration, enabled by its current constitutional status as well as its flexible character. Indeed, in addition to its constitutional components, it can also be understood as a general symbol for sound and ethical administration.[361]

However defined, basic rights and liberties have no bearing without the rule of law. While the rule of law in academic debates has many faces, in the Finnish context the Constitution defines it as the exercise of public powers based in law and in all public activity, the law must be strictly observed (Section 2). The exercise of public powers is a central concept here. Whenever the exercise of public power is in play, it falls within the remits of the stricter legal requirements on its use and general administrative laws become applicable. In accordance with Section 124 of the Constitution, the exercise of public powers can be delegated to private actors as long as the task does not involve a 'significant exercise of public powers'. Such power can only be vested in public administrations. As mentioned, when public power is used the law must be strictly observed in that activity. This is known as the legality principle. Further, the right of good administration is

358. Sections 1 and 2 in the Constitution.
359. Chapter 2 in the Constitution. See more on the 1995 reform and general Europeanisation of Finnish law, Finland: European Integration and International Human Rights Treaties as Sources of Domestic Constitutional Change and Dynamism. / Ojanen, Tuomas; Salminen, Janne. Ed. / Anneli Albi; Samo Bardutzky. Springer, 2019. p. 359-404.
360. One of the objectives for the Constitutional reform was to align the Constitution with the international human rights obligations, see e.g., Perusoikeuskomitean mietintö. Komiteanmietintö 3/1992. Perusoikeusuudistus. Oikeusministeriön lainvalmisteluosaston julkaisu 6/1995 (The Report of the Constitution Committee, Committee Report 3/1992; Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta HE 309/1993 vp (Government Bill for the Reform of Constitutional Rights).
361. For more on good administration in the Finnish context see e.g., Varieties of Good Governance: A Suggestion of Discursive Plurality. / Koivisto, Ida. In: International Journal for the Semiotics of Law, No. 27, 2014; Good administration can also be discussed from international and EU perspectives as well. See e.g., Good Governance at the Supranational Scale: Globalizing Administrative Law. / Esty, Daniel. In: The Yale Law Journal, No. 115, 2006 (international); The Relationship between the Charter's Fundamental Rights and the Unwritten General Principles of EU Law: Good Administration as the Test Case. / Hofmann, Herwig; Mihaescu, Bucura. In: European Constitutional Law Review, No. 9, 2013 (EU).

laid down in Section 21(2) and further defined in the Administrative Procedures Act (APA, *hallintolaki*).[362]

In the spirit of legal positivism, the fundaments of administrative law should make a coherent entity. From the national perspective, in the Finnish hierarchy of laws, the Constitution takes the highest place.[363] What follows is that all other rules must be in line with the Constitution. The Constitution creates frames for the procedure and limits the content of lower-level rules. Considered hierarchically, the lower-level rules consist of firstly, parliamentary acts (*eduskuntalaki)* and secondly, other decrees and orders imposed by the Finnish government or ministries (*asetus*).[364] The parliamentary acts can be further separated into general and sectoral laws. In public administration, the general laws are the ones which apply across the board to all actors who use public power. This means that the general administrative laws are applicable also when a private actor performs a public task. These laws include rules relating to transparency[365] and language rights,[366] for example. Then again, sectoral laws are targeted legislation regulating the actions of specific public organisations or bodies. These include, for example, laws in relation to taxation.

However, Finland is a Member State of the European Union, which shuffles the traditional hierarchy. This means that the EU laws are applicable and the general principles such as the primacy of EU law[367] are binding. It also means that the Charter is applicable when implementing Union law.[368] Regarding fundamental rights, on top of being a member state of the European Union as well as the Council of European Union, Finland has signed and ratified six regional and seven international human rights treaties, which have become part of the Finnish legal order.[369] Due to the dualistic system, the international treaties are incorporated into the national legal order either by a parliamentary act or by a statute given by the government or a ministry. The choice between the two is governed by whether the legal obligation arising from international law is considered to fall within 'the scope of law'.[370] If the international law obligations fall within the scope, it must be legislated as a parliamentary act. The same stands for EU directives.

2.1 Public bodies and the organisation of administration

Though the Constitution defines fundamental principles and rights, it says less about the organisation of public administration. In addition to the state administration, the nationwide public services and the services provided by the municipalities form the core of the Finnish public administration system. On top of these two core administrative levels, the level of regional administration also exists, namely the newly adopted for healthcare and social welfare administration. The transnational level, in turn, consists primarily of EU administration. To a degree, this reflects the democratic structures: Democracy in Finland is upheld by parliamentary, presidential, regional, and municipal elections in which all Finnish and European[371] citizens over 18 years old can vote.[372]

362. Hallintolaki (APA) 434/2003.
363. With the caveat that EU law takes primacy over national law as found in Case 6 /64, Costa v ENEL, ECLI:EU:C:1964:66.
364. Finland: European Integration and International Human Rights Treaties as Sources of Domestic Constitutional Change and Dynamism. / Ojanen, Tuomas; Salminen, Janne. Ed. / Anneli Albi; Samo Bardutzky. Springer, 2019. p. 359-404, 400.
365. Laki viranomaisen toiminnan julkisuudesta 621/1999 (Freedom of Information Act).
366. Kielilaki 423/2003 (Language Act).
367. Case 6 /64, Costa v ENEL, ECLI:EU:C:1964:66.
368. Charter of Fundamental Rights of the European Union, OJ C 326/391, article 51(1); Case C-617/10, Åkerberg Fransson, ECLI:EU:C:2013:105.
369. International Justice Resource Center, https://ijrcenter.org/country-factsheets/country-factsheets-europe/finland-human-rights-factsheet/; Section 65 in the Constitution; Finland has also ratified several Council of Europe protocols.
370. Section 94(1) in the Constitution.
371. European citizens who are Finnish residents.
372. This is the case for Presidential and Parliamentary elections. In regional and municipal elections, the right to vote is limited to those residing in the given areas.

Again, the rule of law – or the principle of legality – plays an important role. The general principles governing all the national levels must be laid down by an act since the activities involve the exercise of public power.[373] Only provisions on the entities of state administration can be laid down by a decree.[374] In this section, we will outline the way in which public administration is construed from an organisational perspective. Thus, we will present the main actors involved in public administration in Finland. Since the organisational structure of the public administration is vast, it demonstrates the complexity of public organisations that potentially could deploy ADM processes. The heterogeneity of the various actors also highlights that digital public administration should not be perceived as one-size-fits-for-all endeavour.

In addition to national public authorities applying national law, national authorities are also responsible for applying European regulations in Finland, which makes them part of the EU's administrative field. In addition to national authorities, there are some EU-level authorities with information, overview, and regulatory functions in constrained policy fields and situations. The European Commission also has some administrative powers over the Member States, such as the power to initiate infringement procedures in cases of breach of EU law.[375]

2.1.1 State administration

State administration is divided into central, regional, and local levels, which involves a division of labour between the levels. The central government is responsible for general policy development and legislation that applies nationwide. In the central government, the Prime Minister and Cabinet of Ministers are responsible for leading the government and developing policies. The ministries are responsible for preparation and implementing these policies in their respective areas of responsibility. The central administration upholds the institutions which act nationwide as independent organs, such as the Bank of Finland, the Social Insurance Institution of Finland (KELA), the tax authority (Vero), the immigration authority (Migri), and the customs authority (Tulli), to name a few. Digitalisation applied in these central administrative agencies affects masses of people and forms the core of where the citizens meet the state.

The regional level of state administration consists of 19 regions that are responsible for implementing policies and regulations that fall under their competence. The Regional State Administrative Agencies (AVI) oversee the implementation of policies and regulation within their regions. The AVIs are responsible for supervising the activities of municipalities, promoting regional development, and providing services that are not provided by the municipalities. In practice, the function of the AVIs in the whole national administrative system remains marginal. During the COVID-19 pandemic, however, the AVIs role became more visible as they were in charge of implementing restrictions of public assembly, events, and the opening times of restaurants, for example.[376]

At the local level municipalities are responsible for implementing policies and regulations and providing basic services to citizens, such as education, public transportation, and certain healthcare and social services at the community level. The municipalities are self-governing entities[377] meaning that the central government has a limited ability to affect the decisions made at the local level. A piece of parliamentary legislation, the Municipalities Act (*kuntalaki*), provides more detailed rules for the general principles governing municipal administration as well as the duties of the municipalities. There are over 300 municipalities in Finland, and they are run

373. Section 119 in the Constitution.
374. Section 119 in the Constitution.
375. Treaty on the Functioning of the European Union, OJ C 326/47, article 258.
376. Tartuntatautilaki 1227/2016, Section 8; Aluehallintovirasto. Mitä tapahtumia aluehallintovirasto voi kieltää? 2 December 2020. https://avi.fi/blogi/kirjoitus/-/blogs/mita-tapahtumia-aluehallintovirasto-voi-kieltaa-konsertit-ja-urheilukisat-kielletty-kauppojen-ale-ruuhkat-jatkuvat.
377. Section 121 in the Constitution.

by democratically elected municipal councils. These councils and executive boards govern the municipalities and are responsible for decision-making on local policies and services.

Digitalisation in administration in the municipalities is closer to the citizens' everyday life from schooling to social services. Recently, the legal duties of the municipalities have been reduced. From 2023 on, the main healthcare, rescue, and social services have been transferred to the newly established welfare service counties which we will return to below. Nevertheless, the municipalities retained the responsibility for promoting the wellbeing of its residents.[378]

2.1.2 Healthcare and social welfare administration

After the recently completed reform, a new level of administration was created. Healthcare, social welfare, and rescue services were transferred from the municipalities to the newly established welfare service counties.[379] Digitalisation at this administrative level refers mostly to the healthcare and social welfare services, which do not engage as much with decision-making but rather with other forms of digitalisation.

Since the beginning of 2023, there are 21 self-governing wellbeing service counties comprising a collection of municipalities with Helsinki being an exception. Helsinki makes up its own wellbeing area with no separate county elections and council. Elsewhere, the highest decision-making power is vested in each wellbeing service county councils, members of which are elected in county elections held every four years. The tasks and functions of the welfare service counties have been written into law. However, as the new organisational structure has been in place only for some months at the time of writing, the effects of the reform are yet to be seen. The counties do not have a taxation rights, which means that they receive all the necessary funding from the state.

2.1.3 Legality control and the courts

All domestic legislation must be in harmony with the Constitution, which is ensured by constitutionality control. The courts, divided into two branches of administrative and general branches, are responsible for ex post constitutionality control, whereas the Constitutional Law Committee of the Parliament and the Chancellor of Justice exercise ex ante control.

Law drafting may inlclude input of the Consitutional Law Committee (CLC), which considers the constitutionality of the proposed legislation. If the CLC considers the proposal to be unconstitutional, or issues of a constitutional nature arises, the law proposal must be refined so that the constitutionality of the legislation can be assured. The overall legal system must be able to function coherently, which essentially means that new legislation must respect already standing legal principles and doctrines. The CLC functions as one of the main steps to consider the overall compatibility of the new legislation with the foundational legal order. The CLC consists of members of the parliament and frequently hears distinguished legal academics to ensure the quality and accuracy of their work. In the wake of the fundamental rights reform, the mechanisms of constitutionality control were widened to cover also complementary judicial control. However, the parliamentary pre-control remained unchanged.[380]

The Supreme Court and the Supreme Administrative Court have complementary powers of constitutionality control. The new Constitution brought with it a secondary judicial review mechanism. The courts were given the power to review the constitutionality of Parliamentary

378. Kuntalaki 410/2015, (Municipalities Act), article 1.
379. Laki sosiaali- ja terveyshuollon järjestämisestä 612/2021 (Healthcare and social welfare Act); Laki pelastustoimen järjestämisestä 613/2021 (Act on the organisation of rescue services; Laki sosiaali- ja terveydenhuollon sekä pelastustoimen järjestämisestä Uudellamaalla 615/2021(Act on Healthcare, social welfare and organisation of rescue services in Uusimaa).
380. Section 74 in the Constitution.

acts more widely, i.e., in light of fundamental rights. Previously, the courts' review power was limited to sub-statutory statutes. According to the Section 106 of the Constitution, if a provision in an act is in 'evident conflict' with the constitution, that provision must not be applied in that case. This widening of the courts' power to conduct judicial reviews has been characterised as being increasingly subordinated to rights-based judicial review.[381] Since the 1990s, cases concerning fundamental rights have been slowly increasing in the Supreme Court[382] and Supreme Administrative Court.[383] In public administration, the Supreme Administrative Court is the main judicial authority. Most of the cases that reach the Supreme Administrative Court concern migration and social welfare issues. Other topics include land use, the environment, taxation and public procurement. Cases relating to digital administration have included the use of e-mail as an avenue for dealing with public administration and public procurement of a digital services, among others.[384] Most of the cases decided in the Supreme Administrative Court are appeals from regional administrative courts.[385]

On top of their powers of pre-control and the option of taking actions to the Courts, the Chancellor of Justice and the Parliamentary Ombudsman can review cases relating to public administration. While both judicial oversight bodies have vast powers in relation to reviewing and inspecting the administrative action, the powers do not extend to the ability to change administrative decisions. The Chancellor of Justice (and Deputy Chancellor of Justice) is a historical judicial oversight entity in Finland, dating back to the 1700s.[386] It is attached to the government and oversees the legality of the activities of the Government, the President, the courts, and other public officials.[387] The Chancellor can begin an investigation based on a citizen or public official's complaint or its own initiative.[388] The Chancellor must investigate whether there is a cause for doubt that the public administration under review has acted unlawfully.[389] If the Chancellor finds the administration to have acted unlawfully or failed to follow its duties, they can give an official notice or in more extreme cases press charges. According to a recent act on separation of the duties of the Chancellor and the Parliamentary Ombudsman (*laki valtionneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen tehtävien jaosta*), overseeing the development and maintenance of public administrations automated systems falls within the responsibilities of the Chancellor.[390] Importantly, the Chancellor's attention to ADM practices in the social insurance institution (KELA)[391] was a springboard that fuelled the public conversation on the need to create a legal basis for ADM through national legislation.

381. Rights-Based Constitutionalism in Finland and the Development of Pluralist Constitutional Review. / Lavapuro, Juha; Ojanen, Tuomas; Scheinin, Marten. In: I CON, No. 9, 2011. p. 505-531; Pan-European General Principles of Good Administration in Finland: from Margin to Centre? / Koivisto, Ida. Eds. / Ulrich Stelkens; Agné Andrijauskaite. Oxford University Press, 2020. p. 431-448.
382. Korkein oikeus (KKO), Section 98 in the Constitution. The KKO deals with cases relating to civil, commercial and criminal matters.
383. Korkein hallinto-oikeus (KHO), Section 98 in the Constitution. The KHO deals with cases relating to administrative matters.
384. E-mail case, e.g., KHO 2018:152 (on informing citizens in digital administration); Public procurement case, e.g., KHO 28.1.2020/305 (on objective scoring in public procurement).
385. Korkeimman hallinto-oikeuden historia / Korkein hallinto-oikeus https://www.kho.fi/fi/index/korkeinhallinto-oikeus/historia.html#.
386. Ombudsman as a Global Institution: Transnational Governance and Accountability. / Erkkilä, Tero. Palgrave Macmillan, 2020. p. 69.
387. Section 108 in the Constitution.
388. Laki valtioneuvoston oikeuskanslerista 2000/193 (Act on the Chancellor of Justice), article 3.
389. Laki valtioneuvoston oikeuskanslerista 2000/193 (Act on the Chancellor of Justice), article 4.
390. Laki valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen tehtävien jaosta (Act on the separation of duties of the Chancellor of Justice and the Parliamentary Ombudsman) 330/2022, article 2(1); more on the history and the separate functions of the Chancellor of Justice and Parliamentary Ombudsman see, Ombudsman as a Global Institution: Transnational Governance and Accountability. / Erkkilä, Tero. Palgrave Macmillan, 2020. Chapter 3.
391. OKV/21/50/2019.

2.1.4 Ombudsmen and guidance for digital public administration

Finnish public administration also includes various ombudsmen who provide oversight of their own initiative as well as based on citizen complaints. For ADM, the focal actors are the Parliamentary Ombudsman and Data Protection Ombudsman. In addition, the newly established Information Management Board has certain oversight duties in addition to providing guidance areas of digital public administration.

The ombudsman institution has established legal tradition in Finland, dating back to the **Parliamentary Ombudsman**. Finland was the first country to copy the historical Swedish legal overseer, the Parliamentary Ombudsman.[392] Along with the first Finnish Constitution, the Parliamentary Ombudsman was implemented into the Finnish system in 1919 along the lines of what legal comparatists could call a legal transplant.[393] On top of the Parliamentary Ombudsman, there are several sectoral ombudsmen acting in specified fields. These ombudsmen focus on equality, the rights of children, the rights of elderly, and data protection, for example. All of the ombudsmen's' competencies are based on legislation outlining their respective mandates, powers, and tasks.

The Parliamentary Ombudsman is appointed by the Parliament[394] and is tasked to ensure that public officials obey the law and fulfil their obligations when they are performing a public task.[395] This oversight function thus overlaps with that of the Chancellor of Justice. The Ombudsman also submits an annual report of their work for the Parliament including all the observations as well as shortcomings in legislation.[396] Similarly, as the Chancellor of Justice, the Ombudsman may begin an investigation either by a citizen's request or on their own initiative. In case of finding shortcomings or illegality, depending on the gravity of the situation, the Ombudsman can either give an official notice to the public official, or order a police investigation of the matter. On top of the attention by the Chancellor to ADM practices, the Ombudsman also opened their own initiative inquiry on the ADM practices in the tax authority.[397] Thus, both of the main legal overseers were influential in the national discussion on the need to legislate ADM practices in public administration.

The **Data Protection Ombudsman** is the main authority responsible for ensuring compliance with the rules and obligations of GDPR and the Finnish data protection Act. The current national Data Protection Act that specifies and complements the regulation strengthened the functions of the old Data Protection Ombudsman (DPO), establishment of which dates back to the 1990s.[398] The requirements for national supervisory authorities stemming from the GDPR were incorporated into the mandate of the DPO.[399] The Finnish DPO monitors and enforces the application of data protection laws, primarily certain aspects of the GDPR, but also multiple national legislation. The DPO's tasks further include the imposition of administrative fine when a private entity has been found to breach the GDPR.[400] As the GDPR left room for national consideration whether such fines could be imposed on public actors,[401] Finland opted not to include such punitive measures in relation to the GDPR. Thus, administrative fines cannot be imposed on a public actor, but the DPO can issue warnings, reprimands, and other non-monetary corrective measures to a public actor who has found to breach the GDPR.[402] The decisions of the DPO can be appealed to the administrative courts.

---

392. OKV/21/50/2019, p. 71.
393. OKV/21/50/2019, p. 70.
394. Section 38 in the Constitution.
395. Section 109 in the Constitution.
396. Section 109 in the Constitution.
397. EOAK/3379/2018.
398. Finland: A Brief Overview of the GDPR Implementation. / Korpisaari, Päivi. In: European Data Protection Law Review, No. 5, 2019. p. 234.
399. Tietosuojalaki 1050/2018 (Data Protection Act) Chapter 3.
400. Other tasks are listed in GDPR, article 57.
401. GDPR, article 83(7).
402. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi HE 9/2018 (Government Bill for legislation supplementing the EU's general data protection regulation) p. 103; Tietosuojalaki 1050/2018 (Data Protection Act) Chapter 4.

Finally, the **Information Management Board** plays a role in overseeing digital public administration, its supervisory rights and duties increasing with the new general legislation on ADM in public administration (discussed below in section 2). The Board is a non-judicial oversight entity with powers to give out recommendations and best practice guidelines. The task of the board is to promote the data security and information management procedures outlined in the Act on Public Administration Information Management. The recommendations and other guidelines are not legally enforceable but provide standards which, when followed, ensure that the public actors fulfil the obligations stemming from the legislation in relation to information management.

2.2 Legal sources of public administration

Having described the organisation of public administration, we proceed to the applicable legal framework and various legal sources as well as doctrines that form the core of administrative law and which contextualise the Finnish ADM reform.

The legal sources of public administration are manifold. They consist of general laws targeting all administration and special laws enacted for specific administrative fields or topics. In addition, administrative law includes overarching principles and concepts, which must be considered in all administrative activity. These fundamental legal doctrines, if you will, emanate from the Constitution, international human rights agreements, and traditional concepts and principles of administrative law. The Constitution and international human rights treaties form a part of the legal sources of the public administration in verbatim. At the same time, however, they perform a dual role through practical adaptation of the doctrines into practice.

The legal framework guiding public administration can be systematised into six levels. These are 1) international human rights treaties, 2) EU law, 3) the Constitution, 4) general parliamentary legislation, and 5) sectoral, field-specific parliamentary legislation, and 6) lower-level laws and norms. The term levels should not be confused with the idea of hierarchy; it is used merely for systematisation purposes.

2.2.1 Constitutional foundations

As mentioned, the Constitution of Finland sits at the top of the national hierarchy of laws. Therefore, all lower-level rules must be in alignment with the Constitution.[403] The Constitution bases the multiple general principles, which must be followed in the use of public power. These include the obligations that the exercise of public power must be based in law (Section 2.3), equality before the law (Section 6), the right to access public documents (transparency) (Section 12.2), legal protection and good administration (Section 21). In addition, Section 22 of the Constitution provides that public power must ensure that human and fundamental rights are carried through. Furthermore, a delegation of administrative tasks to others not in the public administration is codified in Section 124 of the Constitution, according to which tasks, including the exercise of significant public power, cannot be delegated. These constitutional provisions cover legislation, administration and adjudication, and must be followed in automated decision-making in public administration.

International law in the form of signed and ratified human rights treaties binds the legislator, judicial oversight bodies as well as the public administration in performing its tasks. Further, Finland is a Member State of the EU. That means that EU legislation is applicable and must be followed in the context of public administration. In accordance with the principle of supremacy, EU law takes precedence when a conflict arises between EU and national law. The EU is increasingly legislating on aspects relating to digitalisation, which affects the digital public

403. Section 106 in the Constitution.

administration as well. As for now, the most important instrument in this is the GDPR, as we will specify in the following. The Constitution and the principles stemming from it first and foremost the principles of legality and good administration must be respected in all tasks relevant to public administration. At the same time, all lower-level laws and norms must be in line with the Constitution.

Other general legislation includes acts which provide more specific guidance on non-discrimination, linguistic rights, or access to information, for example. There is also general legislation which targets a specific part of the administrative procedure, especially in relation to digital public administration. The scope of these laws is technology specific, such as the Act on the Provision of Digital Services, which focuses on the accessibility of public sector applications and websites. Finally, sectoral legislation focuses on specific fields within the public administration, such as the taxation, or immigration services. As is apparent on one hand, the legal landscape of Finnish public administration is manifold and scattered. This is also visible regarding digital public administration. On the other hand, however, the constitutional principles and the doctrines of general administrative law provide a uniting component. Next, we will dive deeper into these different sources of law.

2.2.2 Human Rights Treaties

As mentioned, Finland has ratified six regional and seven international human rights treaties.[404] On top of these, Finland has ratified multiple European Convention on Human Rights (ECHR) protocols. Without a doubt, the ECHR has been the most influential treaty; its impact on the Finnish legal order has been transformative, as discussed above.

The ECHR came into force through a parliamentary act 438/1990 and was further complemented by Decree 439/1990 (provisions regarding the act becoming effective). The more important Council of Europe (CoE) conventions for public administration that Finland has ratified are the European Social Charter and the European Charter of Local Self-Government. Both Charters have also been incorporated into the legal system as an act. The status of the incorporating acts in the legal order is the same as any domestic parliamentary act meaning that it is not hierarchically superior. However, Koivisto has pointed out that the hierarchy of norms in this respect is not that straightforward due to the special nature of human rights.[405] Since article 22 of the Constitution states that '[t]he public authorities shall guarantee the observance of basic rights and liberties and human rights', there is distinct weight given to human rights, irrespective of their formal place in the hierarchy of norms.[406]

The Supreme Court and the Supreme Administrative Court both frequently refer to the ECHR and CoE Conventions and protocols. The case law of the European Court of Human Rights (EcoHR) is frequently followed and upheld in the national system. In digital administrative matters, however, the direct effect of the ECHR is rather marginal.[407] In cases in which there is overlap and more specific EU rules exist, Finland as an EU member state is required to follow the latter. That is the case especially with data protection, where Finland has ratified the CoE Convention on the Protection of Individuals with regard to Automatic Processing of Personal data and the EU has enacted the GDPR. It has been argued that CoE Conventions are given more weight in the law-drafting phase rather than in applying the law.[408] The long-standing practice

404. International Justice Resource Center, https://ijrcenter.org/country-factsheets/country-factsheets-europe/finland-human-rights-factsheet/.
405. Pan-European General Principles of Good Administration in Finland: from Margin to Centre? / Koivisto, Ida. Eds. / Ulrich Stelkens; Agné Andrijauskaite. Oxford University Press, 2020. p. 431-448.
406. There have also been instances in which such distinct weight has not been given, see e.g., Pan-European General Principles of Good Administration in Finland: from Margin to Centre? / Koivisto, Ida. Eds. / Ulrich Stelkens; Agné Andrijauskaite. Oxford University Press, 2020, para. 16.15.
407. Pan-European General Principles of Good Administration in Finland: from Margin to Centre? / Koivisto, Ida. Eds. / Ulrich Stelkens; Agné Andrijauskaite. Oxford University Press, 2020, para, 16.21.
408. Mäkinen argues this in relation to the Charter of local self-government in particular. Controlling Nordic Municipalities. / Mäkinen, Eija. In: European Public Law, no 23, 2017. p. 140-141.

of transparency and open government in Finland[409] as well as the influence of GDPR has created a situation in which the ECHR and related laws remain largely relevant but their direct effect in the digital public administration's legal context is not particularly emphasised.

2.2.3 EU law with a focus on the GDPR

The EU influences Finnish public administration most through its primary and secondary legislation. From a legal sources perspective, the founding treaties, the charter of fundamental rights and judge-made constitutional principles such as the primacy of EU law, direct effect, principles of equivalence and effectiveness as well as the presumption of validity, directly influences the functioning of national administrative systems.[410] The applicability of EU law has a major influence on the digitalisation of national public administration. It has brought in new legal concepts and placed restrictions. That is the case especially with the GDPR and will be the case with the upcoming Artificial Intelligence Act,[411] as we will present below.

In the context of digital public administration, the GDPR are of great importance, especially article 22. Besides its content, it also requires automated decision-making to be based in law in Member States, giving rise to doubts about whether the GDPR itself suffices as a legal basis for the use of ADM in public administration. This resulted in the law drafting on ADM to focus on establishing the legal basis for already existing automation practices in general administrative legislation. Despite the prior use of digital technologies in public administration in Finland, no clear rules governed their use before the GDPR. This was to change as the GDPR specifically conceptualised automated decision-making as a separate regulatory object. In Finland, the use of technology in public administration was not new but it seems that prior to the GDPR, the dominant framing of ADM systems was to consider them as unproblematic tools for organising administrative work and processes. However, now Finland had to legislate nationally on the use of ADM to continue the use of digital technology in administrative decision-making. Additionally, there was domestic pressure to do so, as we will explain later.

Nationally, there have also been tensions between the GDPR and the Finnish Freedom of Information Act. Similar to other Nordic countries, Finnish public administration emphasises a strong interpretation of publicity and freedom of information. The national Freedom of Information Act is currently being amended to reconcile some of the tensions and issues with parallel interpretation. The committee report on the assessment of regulatory needs is expected in fall 2023.

It is difficult to imagine an ADM process in public administration without the extensive processing of personal data, which makes the GDPR applicable. Indeed, in their daily work, public officials work with personal information constantly, and that does not change when the administration goes digital. If anything, the work intensifies. According to articles 5(1)(a) and 6(1)(c) of the GDPR, all processing of personal data must be based in law. Currently, after the national ADM amendments were enacted, automated-decision making is based in law in Finland. This already shows the importance of the new legislation in relation to GDPR compliance.

The conceptualisation of ADM by the GDPR is of great significance for the national legislation on ADM. ADM is not defined in the GDPR per se. Article 22 regarding automated individual decision-making, including profiling states that:

409. Transparency in Finland has its roots in 1766. Julkisuusperiaate / Mäenpää, Olli. 4 ed. Alma Talent, 2020. p. 1.
410. Hallinto-oikeus. / Mäenpää, Olli. 7 ed. Alma Talent, 2023. p. 50.
411. The proposal of 21 April 2021 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, 2021/0106.

'1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'

Article 4(2) provides a definition of 'processing' which means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means [...].' Recital 71 clarifies the situation slightly by stating that:

'[...] evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.'

What follows is that lack of human intervention seems to be a decisive factor while article 4 does not specify what is meant by 'automated'. There are many technical ways in which automation can be executed so that there is no human intervention.[412] Thus, the term 'automated' is not tied to specific computing techniques, but rather seems to be an all-encompassing term for any decision-making done without human intervention.

According to article 22 a person has the right not to be subject to a decision based on automated processing with certain limitations. The article leaves room to manoeuvre for Member States to incorporate ADM, if *'the decision [...] is authorised by [...] Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.'* In other words, the GDPR leaves room for Member States to include ADM on the conditions that the practice is based in law, it is generally in line with the GDPR, and the rights and freedoms of individuals are protected. Therefore, the use of ADM as well as the protective measures (recital 71) both must be written in law (legislation). Article 22 also requires that the public administration must provide an opportunity for the person to question the decision made in automated processes. The right to redress so that a human public official considers the decision needs to be maintained. Thus, this places limits on the automation of redress. Overall, these are the legal frames that the national legislation must be based on and as we will present in section 2, that was done with varying success.

The Finnish system of breaches of administrative law by the public administrations traditionally function on the basis of personal accountability of public officials. This includes tort and criminal liability.[413] Finland decided to make use of the room for manoeuvre left for the Member States in the GDRP and release the public administrations from the GDPR administrative fines mentioned in article 83(1).[414] Instead, the national system of personal tort and criminal liability of public officials was retained as equivalent and effective means to deal with breaches of the GDPR.[415] This approach has been criticised as leaning too much on individual public officials while it could in some circumstances be more beneficial for it to be possible to place a fine on the public administration as a whole. Thus, situations may arise when the accountability of individual public officials can seem excessive.[416] At the same time, this approach may be subject to change in the future. That is firstly due to the national implementation of the Digital Services Act (DSA)[417]

412. Thus, ADM conducted through rule-based or machine learning systems both seem to fall under article 22 of the GDPR. This distinction between rule-based and machine learning systems has been central in the national legislative process as well as in the debates of the upcoming artificial intelligence regulation. See more below in sections 3 and 4.
413. Sections 2(3) and 118 in the Constitution. Rikoslaki (criminal code) Chapter 40.
414. Tietosuojalaki 1050/2018 (Data Protection Act) article 24.4.
415. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi HE 9/2018 (Government Bill for legislation supplementing the EU's general data protection regulation) p. 55-56.
416. E.g., Virkavastuu julkishallinnon muuttuvassa toimintaympäristössä / Mäntylä, Niina; Karjalainen, Ville; Korhonen, Nora; Siikavirta, Kristian; Wenander, Henrik; Annola, Vesa. In: Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja, No. 14, 2022, pp. 94-95.
417. Regulation 2022/2065 of 19 May 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (DSA).

which in the future might include an option to impose a fine on public administrations.[418] Secondly, connected to the discussion on DSA, it remains an open question whether the fines provided in the GDPR should also be charged to public organisations in the future.

Regardless of the significance of the GDPR, the EU's regulation of technology is still expected to increase. This includes the plans to regulate the use of artificial intelligence. Along with the White Paper on AI,[419] the Commission published its agenda to shape the EU's digital future in early 2020.[420] The political agenda is currently known as 'A Europe fit for the digital age', a political strategy that has sprouted and continues to provide legislation relating to multiple aspects digital.[421] For example, the data package includes already adopted legislation on data governance[422] and the 2022 proposal for a European data act.[423] The EU's target to legislate AI has now moved from being a Commission proposal closer to the trilogue negotiations after the European Parliament adopted its negotiation position on the AIA in June 2023.

On top of enacted and proposed regulations, the EU has also enacted directives which have varying influence on digital public administration. The most notable one is the Web Accessibility Directive which places obligations on digital administrations to follow certain standards in their websites and applications.[424] The directive effectively places guidelines on how to ensure accessibility in public administration online platforms. In practice, all applications and websites must follow the Web Content Accessibility Guidelines (WCAG)[425] which have been created to ensure that accessibility is guaranteed especially for users with special needs, but which also benefit all users.[426] The directive was implemented nationally by the Act on the Provision of Digital Services (306/2019) described below.

2.2.4 General administrative legislation and principles of good administration

Above we described the frictions between the GDPR and national legislation that are reflected in relation to governing and regulating ADM use in public administration. In this section, we discuss the general administrative legislation and the principles of good administration it enshrines. The main instruments of general legislation are both the regulatory architecture, into which the legal basis for ADM rules was ultimately embedded, as well as the pre-existing constraints for the regulatory strategy and the ADM use it enables.

By general legislation we refer to national legislation which is applicable across the whole public administrative field. Most of all, it governs procedural rules in all public administration, whereas the substance of administrative decision-making (what kinds of decisions are being made, what field of policy it is in question) in turn, is regulated by field-specific laws (more below). Some fields of administration, such as taxation, have also their own procedural codes. The APA is of particular importance from the viewpoint of our study. Its provisions regulate administrative procedure and decision-making through a life-span structure. The APA also provides more substance to some Constitutional principles, such as the right to good administration, the right to have a reasoned

418. Hallituksen esitys eduskunnalle laiksi verkon välityspalvelujen valvonnasta ja eräiksi muiksi laeiksi HE 70/2023 vp (Government bill on legislation on monitoring of digital services) p. 109.
419. European Commission (2020) On artificial intelligence – A European approach to excellence and trust. White Paper. COM(2020) 65 final. Brussels 19.2.2020.
420. European Commission (2020) Shaping Europe's Digital Future https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf.
421. European Commission, A Europe fit for the digital age https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en.
422. Regulation 2022/868 of 30 May 2022 on European data governance and amending Regulation 2018/1724 (Data Governance Act).
423. Proposal of 23 February 2023 for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 2022/0047(COD).
424. Directive 2016/2102 of 26 October 2016 on the accessibility of the websites and mobile application of public sector bodies.
425. Directive 2016/2102 of 26 October 2016 on the accessibility of the websites and mobile application of public sector bodies. Recitals 37, 41-43, article 6; Accessibility requirements for ICT products and services EN 301 549 v3.2.1. (2021-03) www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf.
426. Web Content Accessibility Guidelines 2.1. (WCAG), Background www.w3.org/TR/WCAG21/.

decision, and the right to be heard. It also specifies the rights of individuals and the obligations of the public officials.

Administrative laws of a general nature are drafted in a way in which they apply across administrative organisations. They reflect and specify constitutional principles which were discussed above. For example, these cover equality before the law (Non-discrimination Act), transparency (Freedom of Information Act), legal protection and good administration (Administrative Procedure Act), linguistic rights (Language Act), electronic processing of administrative matters (Act on Electronic Services and Communication in the Public Sector), and information management (Act on Information Management in Public Administration), to name a few. These general acts are applied unless more specific legislation with the same legal status requires otherwise (lex specialis derogat legi generali).[427] As general legislation, these must be respected in digital administration as well.

Along with the horizontal general legislation, there are sector-specific acts targeting individual public administrations. These lex specialis include multiple laws relating to taxation, migration, social benefits, and many others; typically, administrative branches making masses of administrative decisions on an annual basis. It is important to note that special legislation can be either procedural (special process rules) and/or substantive (governing a specific field of administration). While the special legislation is influential for the individual administrative branch they are targeting (and often influence their digitalisation), in this section, we will focus on the general pieces of legislation applicable horizontally.

The APA is the most important piece of general legislation that applies across public administration. The APA was enacted in 2003, and it replaced its predecessor from 1983. The new APA's constitutional foundations are in Section 21 of the Constitution. Indeed, the act specifies some important aspects of the protection under the law, fair trial and good administration. The APA states that its purpose is to implement and promote good administration as well as to promote equality and performance of administrative services (article 1). More specifically, Chapter 2 of APA lays down the foundations of good administration which all public administrations and officials must respect. This follows the logic of the Constitution according to which principles relating to fair trial and good administration will be protected by law. In relation to ADM, APA is not a mere frame of reference, but the new ADM legislation included an insertion of a new chapter in the act (Chapter 8b) which we will get back to in section 2.

Chapter 2 of the APA lays down the legal principles of good administration. It is important to note that these principles govern first and foremost administrative discretion. This means a situation whereby a public official reaches a decision among many equally justifiable alternatives. The purpose of the principles is thus to guide the interpretation of vague norms and create institutional support for ethical considerations. This means also that their meaning in interactions other than discretionary decision-making is of less importance. Chapter 2 Section 6 of the APA reads as follows:

'An authority shall treat equally those to whom it is providing services in administrative matters and shall exercise its competence only for purposes that are acceptable under the law. The acts of an authority shall be impartial and proportionate to the objectives sought. These acts shall protect expectations that are legitimate under the legal order.'

The principles that arise from Section 6 and define good administration can be understood as binding law as they are, but also as norms which are wider in the scope of application than specific legal rules. In short, the core principles are:

427. Hallinto-oikeus. / Mäenpää, Olli. 7 ed. Alma Talent, 2023. p. 128.

1. *Principle of equality* – The public official has an obligation to treat all people dealing with the administration equally and consistently.
2. *Principle of adequacy* – The public official uses public power only for the purposes defined by law. This principle also aims to ensure that discretion is not misused.
3. *Principle of impartiality* – The public official's actions must be objectively justifiable and impartial.
4. *Principle of proportionality* – The public official's actions must be in line with the purpose of the law.
5. *Principle of trust* – The public official must protect the expectations that are justifiable based on the legal order.
6. *The service principle* (Section 7 APA) – The public official must seek to arrange the use of its services so that those who receive the administrative services receive it appropriately and the official can perform its duties effectively.

The Finnish Courts as well as other judicial oversight bodies further define the content, and scope of application of these principles. Furthermore, the APA includes other elements, which can be considered to be elements of good administration: the requirements of service culture, the ability to gain procedural advice, public officials' obligation to use clear and understandable language, co-operation within administration, transparency of the proceedings, fulfilment of linguistic rights, the right to be heard during the proceedings, the right to get a reasoned decision and the right to redress.[428]

2.2.5 ADM and principles of good administration

In digital public administration in general as well as in ADM specifically, the principles enshrined in the APA continue to be of high relevance. While replacing previously human administrative tasks by an automated system, the public administration must ensure that the principles stemming from the Constitution as well as general laws are respected. The principles in Section 6 may become relevant in varying situations and are arguably hard to code into a digital system, especially if the situation at hand includes discretion. On top of the legal principles, in digital administration, the right to gain advice as well as language rights are of relevance. Due to the gradual change towards digitalising the materials through which public administration is performed or which assist different aspects of it, the judicial oversight bodies have encountered cases where no specific or clear legislation has existed. In many of these instances, the judicial oversight bodies have resorted to the general principles of good administration ultimately enshrined in Chapter 2 of the APA.

Case OKV/3210/10/2021 Deputy Chancellor of Justice: Migration services had used too formal and hard to understand legal-technical language in documents relating to a person's right to work. The Deputy Chancellor of Justice found this to be an issue with the principle of proportionality, and the service principle.

Another case by a Deputy Chancellor of Justice illustrates well resorting to the principle of good administration and the service principle in seemingly unequitable situations arising from the digitalisation of public administration falling outside the scope of any specific legislation.[429] In this case, a revamp of an unemployment offices portal had resulted in poor usability when accessed through a mobile phone. Basing the argumentation on the right to good administration

428. Hallintolaki ja hyvän hallinnon takeet / Mäenpää, Olli. 5 ed. Edita, 2016, chapter 3; Varieties of Good Governance: A Suggestion of Discursive Plurality / Koivisto, Ida. In: International Journal for the Semiotics of Law, No. 27, 2014.
429. OKV/1611/2018.

and the service principle due to the lack of any specific legislation on the exact matter, the Deputy Chancellor of Justice found the unemployment office to be condemnatory on the issue. The Deputy Chancellor of Justice specified the service principle as meaning that dealing with the public administration must be conducted speedily, flexibly, and easily both for the citizen and the public official. As the right to good administration is not defined exhaustively, the situations that are seen to fall under it are continuously expanded in order to fit in situations, which are not caught by any specific legislation. Increasingly, these situations are related to the digitalisation of public administration. In addition to the principles of good administration, the general administrative legislation defines the scope and space for the discretion of civil servants. During the drafting of the law on the legal basis for ADM, much attention was paid to the relationship between ADM and discretion, which reflects the peculiarity of discretionary norms in administrative legislation. One way to approach discretion is as a conscious choice to delegate decision-making power to the administrative level. While discretion has not been mentioned in the Constitution nor in the APA, its existence can be typically inferred from the style of wording of different provisions, e.g., 'an authority may grant a subsidy' means that the public official has the power to decide whether to grant such a subsidy in each case.

On the one hand, discretion and its legitimate use are a key tenet of general administrative law. On the other, it is a practical question in the day-to-day work of public officials. Whenever an administrative decision includes discretion, the principles stemming from Section 6 are materialised in the decision-making. For example, the requirement that the public official's actions must be in line with the purpose of the law pushes a public official to ponder the meaning of the law in question and to use their discretionary powers accordingly.

The APA also governs the lifespan of an administrative decision from beginning to end. This is to say that the APA sets down more specific administrative procedural rules, including how to initiate a matter, and examine the matter, hearing of the parties, requesting, and submitting evidence, informing parties, and stating reasons for decisions, and procedures to request administrative and judicial review. While the APA also provides specific rules on what the administrative decision must contain, the overarching principles highlighted above create the space in which more specific rules function. Thus, when the administration goes digital, the digital processes must also respect these rules. In other words, digital public administration must be good digital public administration.

2.2.6 Transparency, non-discrimination, and language

The principle of transparency – or publicity, as it is formally called in Finland – is a constitutional principle, which guides the transparency of the public administration's activities. Finland, along with the tradition visible in other Nordic Countries, prides itself on vast and long-based transparency in governance activities.[430] Provisions on transparency of governing bodies activities can be found in the Constitution as well as in the APA. According to Section 12(2) of the Constitution, everyone has the right to gain information on the administration's public activities. The principle has been codified more specifically in the Freedom of Information Act (FOIA) which effectively bases the constitutional right on more tangible rules. In principle, the public administration's documents are public and exceptions to the general principle of transparency must be expressly provided by an Act, and they must be necessary.[431]

As mentioned above, the principle of equality is a constitutional principle as well; rooted in Section 6 of the APA and further specified in the Non-Discrimination Act (NDA, *yhdenvertaisuus-laki*).[432] The NDA places an obligation on the public administration to ensure non-discrimination as well as to promote equality in their functions (Section 5); see further below.

430. Julkisuusperiaate. / Mäenpää, Olli. 4 ed. Alma Talent, 2020. p. 1.
431. Section 12(2) in the Constitution; Laki viranomaisen toiminnan julkisuudesta 621/1999 (Julkisuuslaki, Freedom of Information Act) Section 1.
432. 1325/2014.

2.2.6.1 Freedom of Information Act (FOIA)

In practice, the principle of transparency in Finnish administration targets four domains. It includes the transparency of 1) documents and other presentations, 2) administrative process/ decision-making, 3) information provision, and 4) information management.[433]

The right of access to documents is rather broad, also including the right of access to information that is contained in an official document (Section 12 FOIA). While operation of the current FOIA is based on the terminology of access to 'documents', the definition of a document is a technical term which encompasses written and visual documents as well as other presentations which are decipherable only by means of a technical device. Understandability is part of the principle of transparency, precisely due to the terminology used in the Constitution. It is not enough that there is a right of access to documents, but those documents must also be understandable.

How the principle of transparency can be upheld in the digital realm has gained academic interest for some time.[434] In ADM, the ability to gain information on the decision-making process is inextricably connected to many other fundamental principles, such as legal protection, good administration, and official accountability. Since the operation of the FOIA is based on access to documents, in the digital environment a central question is whether the source code falls under the category of 'document'. Even though a decision is reached through automated means, the decision and its reasoning are to be provided.[435]

As the national access to documents regime encompasses not only documents per se but also the information contained within, another question is whether the mere provision of the source code is enough to meet that requirement. Rather, transparency of the source code allows the supervision of the system, but understandability requires more than the visibility of the code.[436] The obligation to state reasons for a decision ensures the ability to scrutinise the public authority on its decision. Since transparency in automated decision-making includes the obligation to state reasons, mere source code would not be enough, but it must also be understandable.[437]

An amendment to the FOIA is currently underway. As of 2021, the Ministry of Justice has started preparations, and the first stakeholder hearing round has been conducted.[438] The objective of the reform is generally to bring the legislation up to date and specifically consider whether the apparent interplay between access to documents/transparency under the national law and data protection under the GDPR could be clarified. While the conflicts have so far been solved without the need to forfeit the core of either of the rights, a practical adaptation of the transparency legislation and the GDPR has proved to be imaginative and unpredictable.[439] The reform aims to clarify the status quo for public officials and ease the application of the law on one hand, and on the other hand, ensure that the rights to gain information as well as rights ensured in the GDPR are respected.

433. Julkisuusperiaate. / Mäenpää, Olli. 4 ed. Alma Talent, 2020. p. 6.
434. E.g., Thinking Inside the Box: The Promise and Boundaries of Transparency in Automated Decision-making. / Koivisto, Ida. In: Academy of European Law working papers. No 1, 2020; Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. / Ananny, Mike; Crawford, Kate. In: New Media & Society, No. 20, 2016.
435. Including the algorithm that reaches to the decision. Julkisuusperiaate. / Mäenpää, Olli. 4 ed. Alma Talent, 2020. p. 121.
436. Läpinäkyvät Algoritmit? Lähdekoodin Julkisuus ja Laillisuuskontrolli Hallinnon Digitalisaatiossa. / Hakkarainen, Jenni; Koulu, Riikka; Markkanen, Kalle. In: Edilex, No. 18, 2020. p. 45.
437. Läpinäkyvät Algoritmit? Lähdekoodin Julkisuus ja Laillisuuskontrolli Hallinnon Digitalisaatiossa. / Hakkarainen, Jenni; Koulu, Riikka; Markkanen, Kalle. In: Edilex, No. 18, 2020. p. 37-44.
438. Oikeusministeriö (Ministry of Justice) Julkisuuslain ajantasaistaminen https://oikeusministerio.fi/hanke?tunnus=OM083:00/2020.
439. Yksityisyyttä vai Avoimuutta? Tietosuojan vaikutus julkisuusperiaatteeseen. / Lindroos-Hovinheimo, Susanna. In: Lakimies, No 5, 2022. p. 752.

2.2.6.2 Non-discrimination Act

The Constitutional principle of equality which is also rooted in Section 6 of the APA is further specified in the Non-Discrimination Act (NDA, *yhdenvertaisuuslaki*).[440] The NDA places an obligation on the public administration to ensure non-discrimination as well as to promote equality in their functions (Section 5). Differentiated treatment is allowed if it is based on an Act or if it has a righteous objective from a human rights perspective. In relation to the latter, that is nonetheless prohibited in relation to the use of public power. In general, the NDA grounds the principle of equality more clearly. Non-discrimination must be upheld in ADM processes as well.

2.2.6.3 Language Act

The Language Act (*kielilaki*),[441] then again, confirms the rights of individuals to use public services in either of the two official languages, Finnish or Swedish.[442] As Finland has two official languages as established in the Constitution, mentioned in the APA and further specified in the Language Act, this aspect must also be respected in digital public administration. In practice, the language requirements may boil down to the technical implementation of the ability to use the digital services in either of the two official languages. Furthermore, the official position of Sámi languages is gaining ground, but the law as it stands today is built around the Constitutional right to maintain and develop their culture. Separate legislation exists which provides the right for Sámi people to use public services in their own language.[443]

2.2.7 Information Management

The Information Management Act (IMA, *laki julkisen hallinnon tiedonhallinnasta*)[444] is a piece of general legislation which targets digital administration more specifically. The objective of the Act is to ensure the principles of transparency and good administration in public administration information and data management. On top of the general information management provisions, the IMA regulates uniformity and information sharing across public services, certain aspects of accessibility, as well as fulfilment of data protection within information management systems. The ADM reform included a new provision in the IMA, to which we will return below.

2.2.8 Acts on Digital Administration

Since dealing with public administration is increasingly executed through a digital interface, some legislation applicable to citizens' interaction with digital public administration has been enacted. The Act on Electronic Services and Communication in the Public Sector (ESCPS, *laki sähköisestä asioinnista viranomaistoiminnassa*)[445] which specifies actions required from the public and communication from public officials is noteworthy. Since dealing with the public administration in the end is about communication, the ESCPS specifies how that communication should be executed when it comes to providing information and sending as well as receiving electronic messages. As the legislation came into force in 2003, it was drafted with a different technological framework in mind than what we have today. This can be seen from the focus on emails rather than online portals. Nevertheless, the ESCPS still provides a legal framework for when an application is received, for example.

---

440. 1325/2014.
441. 423/2003.
442. The preparatory document for the Language Act mentions that it also meets the requirements from the Nordic Language Convention (Convention 11/1987), Hallituksen esitys Eduskunnalle uudeksi kielilaiksi ja siihen liittyväksi lainsäädännöksi HE 92/2002 vp (Government Bill on legislation for new language act).
443. Saamen kielilaki 1086/2003 (Sámi language act) Section 4. However, the position of Sámi languages is considerably weaker than Finnish and Swedish.
444. Laki julkisen hallinnon tiedonhallinnasta 906/2019 (IMA); There is a separate legislation for information and document archives and for national archives both of which target the perseverance and discoverability of more historical documents and information; Act on Common Support Services of the Public Administration (517/2016) aims essentially to ensure availability and usability of the internet across the country.
445. 13/2003.

The Accessibility Directive is nationally implemented in the form of an Act (PDS)[446], which provides more detailed guidance on the requirements of digital public administration services. It is built around four key principles which require the administration's digital solutions to be 1) perceivable, 2) operational, 3) understandable, and 4) robust. According to PDS article 2, accessibility means the principles and techniques that must be followed in the planning, development, maintenance, and updating the digital services for them to be more accessible. When considering the definition of usability as well as the European Telecommunications Standards Institutes (ETSI) and ultimately WCAG standards that the Directive requires to be followed,[447] it shows that the PDS emphasises the accessibility of digital services from the point of view of persons with special needs. The national preparatory documents voice similar concerns as the legislator had stated that the objective of the legislation is to promote and support the abilities of persons with special needs to function in the digital administration.

3. ADM Regulation in Finland

3.1 What do we mean by automated decision-making?

One of the difficulties of regulating ADM processes within public administration is that the concept itself orients the regulatory approach to administrative decisions, forcing us to elaborate and assess what constitutes a decision. In the Finnish administrative law doctrine, an administrative decision usually involves the use of public power.

Public administration can thus be seen as a function established to exercise public power, which can be understood as an obligation for public institutions. In the constitution, the concept of 'public power' has a double meaning: it is the subject that does things (e.g., public power must ensure that fundamental rights are upheld), and activity itself (e.g., an authority may use public power). Along with the principle that all use of public power must be based in law, it is specifically targeted to actions by the public administrations when they are using public power. In a strict sense, public administration uses public power in three main ways:

1. issuing administrative decisions,
2. providing general norms, and
3. using direct force.

The core of the use of public power is that the public official makes the final decision by applying the law. This is called an administrative decision.[448] As mentioned, a significant use of public power can only be exercised by a public administration. Some use of public power can be delegated to private actors,[449] such as health services through a service voucher, or private pension funds. In addition to public power per se, public administration includes other activities, such as providing services such as health care or education, and it may also engage in financial activities. In other words, the use of public power is at the heart of the public administration but cannot be reduced to it.

Administrative decisions form the core of administration as a function. It is the most common way in which public power is exercised. About ADM, the concept of administrative decision-making is of great importance precisely because it is this function that is being automated under

446. Laki digitaalisten palvelujen tarjoamisesta 306/2019 (Act on the Provision of Digital Services).
447. Accessibility requirements for ICT products and services EN 301 549 V3.2.1 (2021-03) (ETSI standards) www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf are built largely on the basis of the WCAG 2.1. standards. The national authorities mention WCAG criteria in their information page for usability www.saavutettavuusvaatimukset.fi/digipalvelulain-vaatimukset/.
448. Administrative decisions include issuing a norm, for example, a decree by a ministry, or an environmental protection order by a municipality. Also, the use of force by a police force, for example, is considered to be a use of public power thus making a decision to use it.
449. Section 124 in the Constitution.

the new national ADM legislation (discussion in section 2.4.). The features of administrative decisions vary depending on the context and applicable laws. It can be general or specific, delivered electronically, on paper, or verbally. The content can include either providing eligibility for a right or benefit, or a prohibition or restriction. The fixity and legal effects of an administrative decision also vary depending on the context, and different types of administrative decisions have different forms of appeal procedures provided by the applicable laws. An administrative decision is not a static concept but context-dependent and regulated by general and sector-specific laws. Thus, the fluid nature of the concept had to be reconciled in the ADM legislation and it was done through basing the ADM system's function in law.

The administrative decision is created through and by the process. The lifespan of the administrative procedure – resulting in an administrative decision and possible appeals – is laid down in the APA.[450] The most common way for an administrative decision to function is that a citizen sends an administrative matter application, which then is decided by the public official either allowing or denying the request.[451] In most cases, requests for administrative decisions to be rectified can be requested from the originating public administration.[452] The decision must include a guide on how the decision can be appealed.[453] If the citizen is unhappy with the result of the rectification request the originating public administration, they can then generally appeal to a regional administrative court. If applicable, the case can move all the way up to the Supreme Administrative Court in accordance with the applicable procedural law rules.

However, everyday public administration includes various other actions that result in a legally relevant decision. These other functions and actions form the internal administration of the public administration, its human resources, and economic aspects, to name but a few. From our viewpoint, these de facto administrative actions include areas such as education and medical activities. When we discuss the form of digital administration that is subject to specific legislation, it is important to stress that we are talking only about administrative decisions. As for now, other uses of digital tools in public administration are not regulated. This emphasis on administrative decisions may sound self-evident; automated decision-making in public administration means automated administrative decision-making. However, it is not always easy to demarcate administrative decisions from other administrative activities such as prior investigation or, for example, an act of registration.

3.2 Background for ADM: Decades of digitalisation efforts in public administration

It is important to note that the transition to digitalising administration was not sudden. In fact, the long history of digitalisation in Finnish public administration speaks volumes. The digitalisation of administration through a historical lens reveals how before the technological focus was mostly on mass-archiving information and to some extent computational decision-making.[454] Scholarly work in this field in Finland has historically predominantly focused on legal informatics.[455] In the 1980s in his doctoral dissertation, Kuopus noted that administrative law as

450. 434/2003.
451. Hallintolaki 434/2003 (APA) Part II.
452. Most decisions can be appealed in the public administration field that made a decision on the matter, but that is not the case for all. For the purposes of this chapter, we concentrate on the administrative decisions which can be appealed in the original administrative authority.
453. Hallintolaki 434/2003 (APA) Section 46.
454. Hallinnon lainalaisuus ja automatisoitu verohallinto: oikeustieteellinen tutkimus kansalaisen oikeusturvasta teknistyvässä valtionhallinnossa / Kuopus, Jorma. Lakimiesliiton kustannus, 1988; Kolme metodologista ongelmaa: oikeustieteen kehitys, marxilainen lainoppi ja oikeusinformatiikka / Klami, Hannu Tapani. In: Turun yliopiston yksityisoikeuden laitoksen julkaisuja. 1981.
455. This started to take root already in the late 1970's in Germany and the Nordic countries. Rechtsinformatik. / Reisinger, Leo. Walter De Gruyter, 1977; Miten hyvä hallinto digitalisoidaan? Haaste oikeustieteelliselle tutkimukselle. / Koivisto, Ida; Koulu, Riikka. In: Lakimies, No. 5, 2020. p. 803; Hallinnon lainalaisuus ja automatisoitu verohallinto: oikeustieteellinen tutkimus kansalaisen oikeusturvasta teknistyvässä valtionhallinnossa. / Kuopus, Jorma. Lakimiesliiton kustannus, 1988; Tehokkuus, informaatio ja eurooppalainen oikeusalue. / Pöysti, Tuomas. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja, 1999; ICT-oikeus sähköisessä hallinnossa. / Voutilainen Tomi. Edita, 2009.

it stood at the time was not able to conceptualise the idea of mass administration.[456] Relatedly, Pöysti, the current Chancellor of Justice, has explained that the missing definition of mass administration continues to complicate contextualisation and the applicable regulatory field of automation.[457]

Technological change and new innovations have brought new tools for the public administration to incorporate technological solutions into the administrative practises (such as ADM) while the mere fundamental questions on the nature and interconnectedness of law and technology have remained relatively unchanged. Digitalisation has been ongoing for more than 50 years without much fundamental attention from the legislator. Technology-specific legislation in the public administration field prior to the ADM reform largely focussed on data management and protection, and rules on sending and receiving applications electronically (mainly email).

ADM in the context of public administration means the functional replacement of a human decision-maker with a computational agent which has been created to apply certain rules in assessing the request and providing a decision. ADM has been used in a range of administrative processes in Finland for years. For example, KELA (the social security authority) and Vero (tax authority) have been using automated decision-making systems for some time.[458] It seems that ADM's inclusion in the public administration has been done gradually to ease the workload (and costs) through auxiliary and in some cases independent decision-making by an automated system.[459] The incorporation of ADM into the public administration seems to be fuelled with the idea that the technology for ADM has been available and no legislation outright prohibited its use.

ADM has been used in the context of de facto administrative functions without any basis in law, and consequently, other fundamental legal questions had not been considered. It seems that ADM quietly and stealthily, became part of day-to-day administrative functions. Enactment of the GDPR provided the legal vocabulary for ADM and therefore conceptualised the technological tool to a function with legal meaning and consequences. ADM brings with it entrenching differences in decision-making procedure as well as the decision-making entity neither of which had been realised properly by the legislator before. The realisation that ADM has become a part of administrative functions has slowly led to the recognition of problematic co-existence of constitutional requirements, such as the use of public power must be based in law, and the utilisation of ADM in administrative functions.

Framing the public administration as performing different activities allows us to understand ADM from both organisational and functional perspectives. As mentioned above, digital solutions have been used in public administration for decades and ADM practices had been incorporated into public administration before any discussion on the need to legislate arose. While ADM in practice forms a part of administrative decision-making, it is essential to point out that public administration is much more than mere decision-making procedures. Still, ADM is not merely utilised for administrative decision-making, but it can be used (and is used) in other forms of administrative actions as well.[460] Nevertheless, the current national ADM reform focussed on administrative decision-making, which forms only one, but an essential part of the public administration.

---

456. Hallinnon lainalaisuus ja automatisoitu verohallinto: oikeustieteellinen tutkimus kansalaisen oikeusturvasta teknistyvässä valtionhallinnossa. / Kuopus, Jorma. Lakimiesliiton kustannus, 1988.
457. Luottamuksesta hallinnon automaattiseen päätöksentekoon. / Pöysti, Tuomas. Juhlajulkaisu Pekka Vihervuori 1950. Ed. / Kari Kuusiniemi; Outi Suviranta; Veli-Pekka Viljanen. Suomalaisen Lakimiesyhdistyksen julkaisuja, 2020. p. 345-360.
458. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 25-26.
459. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 25.
460. For example, in schooling and social services. ADM is also adopted within the administrative practices that do not directly deal with citizens, such as automated auction procurement (water, energy, traffic, and postal services). Laki vesi- ja energianhuollon, liikenteen ja postipalvelujen alalla toimivien yksiköiden hankinnoista ja käyttöoikeussopimuksista 1398/2016.

3.3 Starting points for the new ADM legislation

As mentioned, the need to create a legal basis for ADM arose to the regulatory agenda triggered by Article 22 of the GDPR and the legality controllers' investigations. Questions relating to the legality of the use of ADM started to get attention from the CLC, the Chancellor of Justice, and the Parliamentary Ombudsman.

In 2018, the CLC stated that the need for general legislation on ADM had to be clarified.[461] This statement was the key finding in an opinion it gave regarding proposed legislation on the processing of personal information in migration issues. In 2019, the CLC repeated the need for such a review. It stated that in addition to the rules laid down in the GDPR, the use of ADM touches on other fundamental rights and the use of public power. In fact, this happened to the extent that there was an urgent need to review whether general legislation on ADM was necessary.[462]

In 2019, the Chancellor of Justice opened an own-initiative inquiry on the use of ADM in KELA where further legal questions related to the use of ADM were elaborated.[463] In the decision, he also emphasised the lack of legal basis for ADM but also brought up questions on transparency [464] and problematics surrounding the personal criminal liability of public officials in performing a public task.

The parliamentary Ombudsman also started an own-initiative inquiry in 2018 on the use of ADM in Vero.[465] She found that the ADM processes used in taxation did not fulfil constitutional requirements on good administration, and legal protection, and there was no legal basis for it. The Ombudsman's inquiry reached news outlets in which conspicuous headlines stated that 'the tax authority's robot has taken too much money from people and the parliamentary ombudsman considers that automated decision-making breaches the constitution'.[466] Similarly, to the Chancellor of Justice, the Ombudsman discussed the official accountability as well as transparency of the public administration. In this case, the Ombudsman held the use of ADM in Vero illegal due to the lack of legal basis.[467] The political pressure to legislate ADM became untenable.

From a purely legal perspective, the discussion on the urgency for legislating ADM in public administration was framed around three core legal issues. Firstly, there was a lack of legal basis for ADM at the time. As mentioned above, the requirement that the use of public power must be based on law stems from the Constitution, and the processing of personal information must be based in law in accordance with the GDPR. The realisation of the interconnectedness of article 22 of the GDPR to the national ADM practices seemed to be the kick-off point. The GDPR had brought the concept of ADM within the legal field and could no longer be ignored.

Secondly, the personal nature of official accountability had to be reconciled with the non-personal nature of ADM. The principle of official accountability of public officials performing a public task stems from Sections 2(3) and 118 of the Constitution which comprises criminal and tort-based liabilities.[468] When the public tasks are not directly performed by the public official, but ADM is incorporated into the process, the ability to identify the public official responsible becomes obfuscated. At the same time, the principle of legality in criminal cases (Section 8 Constitution)

461. Valiokunnan lausunto PeVL 62/2018 vp – HE 224/2018 vp (Statement of the Constitutional Committee).
462. Valiokunnan lausunto PeVL 7/2019 vp – HE 18/2019 vp (Statement of the Constitutional Committee).
463. OKV/21/50/2019.
464. OKV/21/50/2019. Especially the need to inform the citizen on the use of ADM in decision-making.
465. EOAK/3379/2018.
466. Verottajan robotti on karhunnut ihmisiltä liikaa rahaa, ja apulaisoikeusasiamiehen mukaan automaattinen päätöksenteko rikkoo myös perustuslakia. / Anu-Elina Ervasti. In: Helsingin Sanomat. 26 November 2019. https://www.hs.fi/kotimaa/art-2000006321422.html.
467. EOAK/3379/2018, p. 37.
468. Rikoslaki (criminal code) Chapter 40.

requires a heightened certainty of the person responsible,[469] a connection which may become difficult to prove when ADM is in use.

Thirdly, the principle of good administration includes a requirement to uphold a climate of trust between the public administration and the citizens. This includes the requirement for transparent decision-making, a requirement that stems also from the GDPR in relation to the automated processing of personal data. Furthermore, transparency regarding whether a decision-making has been conducted through ADM was largely criticised by the findings of both the Chancellor of Justice and the Parliamentary Ombudsman mentioned above. Thus, how to ensure transparency must be considered. On top of these, the overall legal protection of persons subject to ADM, the use of discretion by the public official, as well as the ability to give tasks to an entity other than a human administrative official needed to be addressed. The two latter issues relate to a broader question of whether the administrative legal landscape is built around the assumption that the one who makes decisions is a human and consequently, what abilities and features are assumed from that human actor.[470]

As a result of increasing attention from the CLC, the Chancellor, and the Parliamentary Ombudsman, the government gave a proposal to Parliament in the autumn of 2022.[471] It included several paragraphs, the purpose of which was to allow fully automated individual administrative decisions widely, regardless of the administrative branch. Importantly, the paragraphs were to be added into two already existing acts: the APA and the IMA. Some minor amendments were also proposed to some other acts. The proposal was drafted in two ministries: in the Ministry of Justice (APA) and in the Ministry of Finance (IMA). In the APA, the basic requirements of the ADM were laid down. The IMA, in turn, concentrated on the specificities of how to adopt such automated processes in different public administrations, which would further allow automated decision-making in practice, and laid down some control and accountability mechanisms. As of 1 January 2023, a new law on ADM was enacted. Specifically, the Parliament enacted two separate laws, lex generalis on the use of ADM in public administration (applicable since 1.5.2023),[472] and lex specialis on the use of ADM in tax and customs purposes (applicable from 1.1.2024).[473]

3.4 The New ADM rules in the Administrative Procedural Act and Information Management Act

Since May 2023, the use of ADM in public administration has legal basis and is subject to certain limitations. In other words, the status quo has now been legitimised.[474] This means that the previous practice of ADM in public administration may continue, however, so that certain criteria are met. We will specify those criteria in the following.

The amendment to the APA sets the ground rules for public authorities to automate their decision-making. Automation is possible only if all the criteria are met. The new Chapter 8b of the APA provides five main rules on regulating the use of ADM.

469. Section 8 in the Constitution. This principle of legality includes the principles of accuracy and predictability. Yleinen rikosoikeus. / Frände, Dan. Edita, 2005. p. 40.
470. We return to this point in section 2.6.
471. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration).
472. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration).
473. Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs).
474. As mentioned, the practice of using ADM in public administration is not new, but the legislation is. See more, Imaginaries of Better Administration: Renegotiating the Relationship between Citizens and Digital Public Power / Esko, Terhi; Koulu, Riikka. In: Big Data & Society, No 1, 2023.

Firstly, the decision must be based on pre-made processing rules (Section 53e). In practice, this means that only rule-based ADM is possible, and neither machine learning nor AI systems are included in the legislation.[475]

Secondly, the processing rules used in the ADM system must be created according to the applicable law (Section 53e). This means that only parts of the legislation which can be transformed into mathematical formulas can be automated.[476] For example, an age limit to apply for benefits can be transferred into an automated system which calculates the applicant's age based on the date of birth included in the application.

Thirdly, automated decision-making cannot include case-by-case or discretionary consideration (Section 53e). Whether an issue includes case-by-case consideration is first to be considered by a public official. Thus, the public administration must execute a 'pre-consideration' of whether the decision-making includes case-by-case consideration and if it does, it cannot be automated. This means that there is a form of 'meta-consideration' whether there is case-by-case consideration involved. This meta-consideration inevitably includes a level of discretion in which the particularities of the decision-making and its circumstances must be considered. Thus, even though discretion cannot be automated, it is included in the use of ADM in this type of meta-consideration form. In practice, decisions which include case-by-case consideration or another form of discretion must be conducted by a human public official, in accordance with the lex generalis.[477]

Fourthly, the subject of the decision must be informed that the decision has been made automatically to respect the principle of transparency (Section 53g). Finally, the party concerned must be able to appeal the decision for free to ensure the legal protection of individuals (Section 53f). Furthermore, rectification claims are always to be handled by a human public official (Section 53e).[478]

APA rules are complemented with more specific procedural rules in the IMA (Chapter 6a) for the launching and updating of the automated system. The rationale of the provisions in Chapter 6a is to ensure the fundamental principles such as accountability, transparency, and the legality of the proceedings.[479] In practice, this means five central obligations for the public administration.

Firstly, the pre-made processing rules mentioned in Chapter 8b of the APA must be documented and the legality of the rules must be ensured (Section 28a).[480] Secondly, the public administration must establish a specific decision to deploy an ADM system. It must include the legal qualification as well as the basis of its use (Section 28d). Thirdly, the public administration must ensure the ADM systems are high quality and continue to manage risks before it is put into use as well as while it is used (Section 28b). Fourthly, the administration must ensure that any defects that may occur are corrected (Section 28c). Finally, the public official must inform of the use of ADM in their respective public service (Section 28e).

475. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 99-100, 147.
476. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 99-100
477. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 98.
478. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 100.
479. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 31.
480. This directly links with the requirement from the APA that the processing rules of the ADM must be created in accordance with the applicable law.

As the legislation is relatively recent, the information management board is currently drafting a recommendation on how to ensure that the administrative organs follow the new Chapter 6a.[481] The recommendation will provide more specific guidance for the administrations to make sure that the somewhat technical requirements laid down in the Chapter 6a requirements are fulfilled. The recommendation is going to be presented and published in December 2023.

3.5 Lex specialis for ADM in taxation and customs

As mentioned, in addition to the enactment of general legislation, lex specialis was enacted for the use of ADM in tax and customs. The lex generalis still applies for tax and customs, but the lex specialis allows the use of ADM in some situations, in which it would not be allowed according to the lex generalis. According to the principle that all exercise of public power must be based on law, any divergence to the APA must be based in legislation. Thus, the lex specialis for tax and customs was drafted to allow the automation of decision-making in rectification claims which is not allowed under the new Chapter 8b of the APA.[482] The rectification claims which can be automated would have to be based on the same logic as the original applications, i.e., they could not include case-by-case consideration, and the rectification claim application needs to be clear and possible to translate into computational form.[483] In addition, ADM can be used only in certain rectification claims.[484] Furthermore, according to article 22(3) of the GDPR, there must remain a right to obtain human intervention and contest the decision. In other words, while the GDPR does not ban the automation of rectification claims, there always needs to be an opportunity for a human public official to review a decision reached automatically. While the lex specialis introduced exceptions to the ability to demand a manual processing of certain automatically reached rectification claims,[485] a new application can be sent in those instances in which being processed manually can be demanded.[486]

Just like the lex generalis on ADM as discussed above, the lex specialis for tax and customs added new paragraphs to already existing legislation. They were added to allow the automation of rectification claims in certain instances. Notably, a new Section 26f was included in the Act on Tax Procedure (*laki verotusmenettelystä*)[487] on the automation of rectification claims. The exception can be applied in accordance with pre-consideration of risk by an administrative official that the case does not include discretion or case-by-case consideration.[488] New sections referring to Section 26f of the Act on Tax Procedure were added to other acts which target specific taxes such as income, shipping, vehicles and others.[489] In relation to customs, the Customs Act (*tullilaki*)

481. Automaattisen ratkaisumenettelyn vaatimukset – muutokset tiedonhallintalakiin https://vm.fi/tapahtumat/2023-03-21/automaattisen-ratkaisumenettelyn-vaatimukset-muutokset-tiedonhallintalakiin-webinaari.
482. The preparatory documents mention that one of the objectives is to allow the already existing practice in the tax authority to use ADM in rectification claim; Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 4.
483. The preparatory documents mention that one of the objectives is to allow the already existing practice in the tax authority to use ADM in rectification claim; Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 34; Laki verotusmenettelystä 1558/1995 (Act on tax procedure) Section 26f.
484. Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 24. This means that ADM can only be used when an appeal is allowed. The ADM system cannot make the decision whether an issue can be reconsidered or not.
485. E.g., Laki verotusmenettelystä 1558/1995 (Act on tax procedure) Section 26f para 2.
486. Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 54.
487. 1558/1995.
488. Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 39.
489. Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 34.

[490] was revised with a new section similarly allowing more wide-reaching use of ADM than what lex generalis allows.

Alike the amendment to the APA, i.e., the lex generalis, the lex specialis also includes an aspect of meta-consideration. As mentioned, the special legislation's main objective is to allow the use of ADM in situations which would be prohibited under the general law, mainly rectification claims. According to the lex specialis, the use of ADM in rectification claims can only be used if a public administration first considers that the issue does not include aspects which would require case-by-case consideration or if a human public official has first settled those aspects of the issue.[491]

The law drafting was a joint effort with the Ministry of Justice and the Ministry of Finance with the idea to enact general legislation which would apply horizontally in the public sector.[492] However, the Ministry of Finance also started to draft special legislation for the use of ADM in tax and customs to allow more extensive automation in these areas.

Interestingly, the lex specialis on taxation received considerably less attention in the drafting phase than the lex generalis, although the automation was more pervasive. While the law drafting process for the lex generalis was relatively lengthy with over 60 expert opinion hearings, the lex specialis was pushed through comparatively swiftly with only 27 expert opinion hearings. [493] As the special legislation enables ADM in situations which are prohibited in the general legislation, it remains to be seen whether the speedy drafting and limited political debate present issues in the future. It remains unclear why the lex specialis was granted so little attention, especially since the lex generalis was heavily debated during law drafting.

The ministries responsible for law drafting had to tackle many issues. While the choice to legislate only rule-based automated systems and to focus only on administrative decisions seemed to be quickly accepted, constitutional questions arose concerning the sufficiency of legal safeguards (*oikeusturva/oikeusturvatakeet*) and the obligation to hear the parties during the administrative process. Furthermore, how to deal with discretion and cases which have a level of case-by-case consideration were brought up in many hearings. Furthermore, the compatibility with the novel logic of fully automated administrative action to the Finnish system of official responsibility based on criminal as well as tort liability had to be considered.

As the lex generalis sections added to the APA were a joint effort between the two ministries, finding a coherent whole was not an easy task. Even though their respective amendments targeted different pieces of legislation, the terminology used in the legislations had to fit together. In the first draft, that did not fully seem to be the case.[494] Indeed, the vocabulary adopted in the IMA paragraphs was different than it was in the APA paragraphs. For example, when APA referred to 'automated decisions', IMA referred to 'automated operating processes', although they were to refer to the same things. The difference is significant, as decisions and procedures are subject to different legal requirements.

---

490. 1466/1994.
491. Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 25.
492. The report prior to the proposal for new legislation did not mention two separate laws but only talked about the general legislation. The special legislation appeared during the process of drafting the lex generalis. The proposal for the lex generalis was given in 19th of September in 2022 and the lex specialis was given in 20th of October 2020. Arvomuistio hallinnon automaattisen päätöksentekoon liittyvistä yleislainsäädännön sääntelytarpeista. / Oikeusministeriö (Ministry of Justice). In: Oikeusministeriön julkaisuja. 2020.
493. For lex generalis, Asian käsittelytiedot HE 145/2022 vp https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_145+2022_asiantuntijalausunnot.aspx; For lex specialis, Asian käsittelytiedot HE 224/2022 vp https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_224+2022_asiantuntijalausunnot.aspx.
494. For lex generalis, Asian käsittelytiedot HE 145/2022 vp https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_145+2022_asiantuntijalausunnot.aspx; For lex specialis, Asian käsittelytiedot HE 224/2022 vp https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_224+2022_asiantuntijalausunnot.aspx

This was reflected in the constitutionality control: the CLC found that the amendments to the APA - including the terminology used – to be generally acceptable but the amendments to the IMA were quite heavily criticised. The draft amendments to the IMA were found to be stated to be unnecessarily obscure and detailed.[495] The consistency of this legislative totality is one thing to consider. Regardless, the committee disapproved of the use of technocratic language in general, not only because it was inconsistent with the APA paragraphs. As a result, the Committee concluded that the proposal could be processed in the ordinary legislative order only (and not in constitutional legislative order as an exception act), if many of the paragraphs in the IMA were rewritten, simplified and some were even omitted.

Much of the law drafting debates revolved around legal protection and safeguards for the citizens as well as the individual public officials (official accountability). From the citizens' point of view, recital 71 of the GDPR was at the centre of many conversations.[496] Recital 71 of the GDPR states that the data subject should have a right not to be subject to a decision based solely on automated processing. This raises the question of whether the data subject – in this context, a citizen acting with the public administration – has the right to demand that the decision is made by a human and therefore opt out from the use of ADM affecting her.[497] This question is not purely one that national law can solve, since the right to not be subject to a decision based solely on automated processing stems from recitals in the GDPR. The fact that it is written in the recitals also brings in another debate on how much legal force the right has and the only judicial body able to provide an answer is the CJEU. The idea behind the use of ADM seems to be that consent for the use of ADM will not be required in accordance with the general law and that for an initial decision made through ADM, a citizen cannot demand that the decision is not made by ADM system.

The lex generalis was designed so that the main way to ensure legal protection, equality, hearing of parties and sufficient reasoning, in general, is wide and continuous documentation of the use and functioning of the ADM systems (IMA Chapter 6a). The information management board was granted the responsibility for overseeing the fulfilment of the new Chapter 6a (more on the board in section 1.1.4 above). Practically this means that the board gained new obligations to oversee the fulfilment of the requirements stemming from Chapter 6a, but they also retained discretion on whether and when a given ADM system should be further reviewed. For example, the information management board may further review the way in which issues including discretion are dealt with, but only when the board sees it as being necessary.[498] Furthermore, the information management board is not a judicial oversight body, which means that it has very limited powers to pose legally binding compliance actions. Thus, there is a risk that questionable meta-consideration on whether an issue includes case-by-case consideration becomes incorporated into the institutional practices and consequently is left largely unsupervised.

Some of the IMA provisions that were deleted during law drafting were related to the planned new oversight powers for the information management board. In the early law drafting phases, it was planned for the information management board to be granted new functions such as overseeing the decision to begin the use of ADM and assessment of the ADM in use, some of which were later omitted. Some oversight powers, such as overviewing the documentation,

---

495. Valiokunnan lausunto PeVL 81/2018 vp – HE 145/2022 vp (Statement of the Constitutional Committee).
496. Statements by e.g., Data protection ombudsman https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-59745.pdf; Ida Koivisto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-65679.pdf; Susanna Lindroos-Hovinheimo https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-56783.pdf;
497. Koivisto brought this point up in the law drafting phase, Ida Koivisto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-65679.pdf.
498. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 42-43; Point mentioned by Ida Koivisto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-65679.pdf.

remained with the board. In its opinion, the information management board criticised the timeframe of enacting the new legislation and wished to extend it.[499] That was because the new oversight functions necessarily meant more resources would be required to allow for the increased workload.

Evidently, the organisational changes needed to fulfil the newly planned oversight functions take time to build. The Board's concerns regarding the timeframes were largely ignored, even though the oversight powers in the final law were lessened from those originally planned. This shows that the older administrative structures must be able to stand with the new processes and often it means changes within the old structures. The increase of information management board workload is a good example of how the new legislation has effects on the organisational structure of different public administrative sectors and their oversight bodies.

An aspect that was widely discussed in the law drafting phase was the confinement of the scope of ADM to only fully automated administrative decisions. Currently, there is no legislation that would regulate the use of decision support systems or automation of other phases of administrative decision-making, such as the initial request (*vireillepano*) or informing the party concerned (*tiedoksianto*). Also, data-based automated systems are not within the scope of the law. This means that data-based systems, including machine learning or AI systems, are currently without legal basis on the national level. Thus, public organisations are currently banned from using such techniques for fully automated decisions, although it is possible that to a certain extent, data-driven techniques could be used for decision support. At the same time, legislating rule-based ADM does not rule out the option of legislating on data-based ADM in the future.

Furthermore, the amendments do not target assisting ADM, which in many instances is largely used in the daily public administrative work. For instance, such assisting automation could relate to the filing of claims or redacting necessary information from documents. In addition, other administrative actions, such as in the schooling system, the healthcare system and social services, may also include automated processing of personal data which would fall under the requirements for national legal basis in accordance with article 22 of the GDPR but is not fully automated decision-making per se. Since the ADM legislation only targets administrative decisions, other types of automation used in the public administration remain without the necessary legal basis for its use.[500] This shows that automation in public administrative tasks varies greatly and the focus on automated *decision-making* does not provide an all-encompassing legal framing when it comes to the use of automation in public administration.

The lex specialis for tax and customs was drafted to allow the use of ADM in rectification claims which is not allowed under the lex generalis, as mentioned. The CLC mostly found the proposal to be acceptable.[501] However, it was also criticised based on the legal safeguards stemming from recital 71 of the GDPR and due to inconsistencies with specific sections of the GDPR.[502] For instance, while the GDPR article 13(2)(f) requires the controller to inform the data subject on the existence of automated decision-making at the time when the personal data are obtained, the national legislation currently requires informing the data subject on the use of ADM only in the exact decision that has been reached through ADM.[503] In other words, according to the national

499. Information management board https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-59522.pdf.
500. Pointed out by Susanna Lindroos-Hovinheimo https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-56783.pdf.
501. Valiokunnan lausunto PeVL 88/2022 vp – HE 224/2022 vp (Statement by the Committee).
502. E.g., Data protection ombudsman https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-63660.pdf; Olli Mäenpää https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-70917.pdf; Ida Koivisto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-70841.pdf;
503. Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 49.

law, the data subject is not personally informed about the possible use of their data in ADM prior to the decision having been made though an ADM system.[504]

Moreover, the legislation includes sections which are in tension with the GDPR's provisions on the data subject's right to express their views. In relation to the taxation procedure for taxes paid on one's own initiative, the data subject's right to express views is generally guaranteed because it is possible to express their views before a late payment fee is imposed.[505] However, if the late payment fee is less than €200, that right to express views is only allowed if it is 'necessary due to special circumstances'.[506] However, according to recital 71, the proper legal safeguards, such as the right to express view should always be possible when the use of data processing results in legal effects. In this respect, whether the special legislation is in line with the GDPR could be questioned.

3.6 ADM and the human assumption

The ADM reform can also be considered to be a reform of administrative legal thinking more widely. On top of the multiple legal-technical issues that the legislator had to consider the non-personal nature of ADM and legal concepts relying on human assumption had to be reconciled.[507] The most important such concepts are the use of discretion and official accountability. The question of discretion was simply resolved – automation of discretion was prohibited outright.[508] However, as mentioned, the laws introduced new forms of discretion (meta-discretion), which need to become uniform with the fundamental principles of the administrative law.

The national system of personal accountability of public officials, in turn, meant that the legislation had to take into account the personal aspect of accountability in the context of ADM.[509] The official accountability stems from the Constitution which provides that anyone who has suffered a violation of their rights or sustained a loss through an unlawful act or omission by a public official can request a criminal trial and the public official can be held liable for damages (Section 118). In other words, the Constitution provides criminal and tort-based liability for public officials in cases of unlawful action or omission. This approach was considered to supplement the legality principle according to which all public action must be based in law.[510]

Interestingly, limiting the use of ADM in rule-based systems is connected to the way in which official accountability is dealt within the legislation.[511] The idea seems to be that the public officials know how the system is built (APA – based on legislation), and how it is functioning (IMA – documentation). This knowledge would allow identification of the person to be held accountable. Much depends on the successfulness of the documentation: it is precisely due to the mandatory documentation on how the ADM system reaches the decision that makes it possible to later identify the responsible party.

504. Point raised by Data protection ombudsman https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-63660.pdf.
505. Late payment fee in this context refers to a fee that is a result of the taxpayer not providing the information for taxation in time in accordance with the Act on the Taxation Procedure for Taxes Paid on Own Initiative (Laki oma-aloitteisten verojen verotusmenettelystä 768/2016) art 30.
506. Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 33.
507. Human assumption central in Finnish public administration discussed in e.g., Modelling Justice by Emergence? Rights and Values in AI Development. / Honkela, Timo; Riikka, Koulu. How Will AI Shape the Future of Law? Eds. Koulu, Riikka/ Kontiainen Laura. University of Helsinki Legal Tech Lab, 2019. p. 155–193, 160, 172.
508. This is because the ADM must be created based on legislation that can be transferred into mathematical formulas. Discretion cannot be translated to such formulas.
509. See more from theoretical perspective, Virkavastuu ja päätösautomaatio – vastuun henkilökohtaisuus kriisissä? / Hirvonen, Hanne. In: Lakimies. No 3-4, 2022.
510. Hallituksen esitys eduskunnalle uudeksi Suomen hallitusmuodoksi 1/1998 (Government Bill for a new form of government) p. 172.
511. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 142.

In practice, identifying the responsible party may not be that straightforward. The decision to deploy an ADM system (*käyttöönottopäätös*)[512] required by Section 28 d of the IMA must include a description of the division of labour between the people responsible for different aspects of the ADM system.[513] Thus, the responsibility is divided according to the individual aspects of the operation of the system. However, a problem in the system may not be always be attributable to a single person. Yet, the national official accountability doctrine does not currently recognise joint official accountability nor accountability of the public administration as a whole.[514] Thus, even with meticulous documentation, identifying one person as being responsible might be hard.

In the end, the question was not only to make new rules to govern the use of ADM in the public administration. Instead, those rules needed to fit into the administrative system as a whole. As described, the ADM legislation has to fit in with the logic of criminal responsibility of individual officials. Such criminal responsibility consequently takes in the logic of Finnish criminal law and departs from the idea of personal choice and action. In a similar vein, the 'meta-consideration' that we have discussed above did not exist in the Finnish administrative legal system before.[515] The way in which it will fit into the administrative legal order remains to be seen.

4. EU Regulation for Artificial Intelligence

4.1 Potential overlap between national ADM rules and the Artificial Intelligence Act (AIA)

The EU does not have regulations on artificial intelligence at the time of writing. As for now, the upcoming EU legislation on AI is currently moving towards trilogue negotiations between the European Parliament (EP), the Council of the European Union (Council), and the Commission. Although it remains to be seen what the final regulation will look like, it is unlikely that the painstaking law drafting that has taken years and featured highly on the current Commission's political agenda would fail to produce any legislation at all. Much is still unknown at this stage, as even the scope – and the related question of defining the AI techniques the EU aspires to regulate – are still under debate. Once the final version is accepted, it will take years before case law on its interpretation starts to form.

In addition, uncertainties are connected to the subsequent interpretation of the regulation by national authorities in the member states and later the CJEU. It is also possible that the AIA will allow some national discretion, as was the case with the GDPR. Due to the ongoing legislative process of the AIA, next, we present four key discussion points that the interconnected nature of the national ADM legislation and the future AIA provide.

The saga about legislating AI on the EU level officially began in 2020 with the Commission's White Paper on artificial intelligence suggesting a range of options for regulating AI.[516] In the following year, the Commission gave out a proposal for AI regulation (AIA proposal).[517] The Council presidency at the time (Slovenia) and the subsequent two presidencies (French and

512. An example of such decision, Automaattisen ratkaisumenettelyn käyttöönottopäätös 20.6.2023 https://www.tyollisyysrahasto.fi/globalassets/automaattisen-ratkaisumenettelyn-kayttoonottopaatos-20.6.2023-.pdf
513. Other aspects that the decision must include are processing rules, testing reports, risk management plan, as well as description on quality control and how to identify and correct errors in the system.
514. Virkavastuu ja päätösautomaatio – vastuun henkilökohtaisuus kriisissä? / Hirvonen, Hanne. In: Lakimies. No 3-4, 2022.
515. Ida Koivisto https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-65679.pdf.
516. European Commission (2020) On artificial intelligence – A European approach to excellence and trust. White Paper. COM(2020) 65 final. Brussels 19.2.2020; More on the policy drafting before the proposal for regulation see Artificial Intelligence in the European Union: Policy, ethics and regulation. / Ulnicane, Inga. The Routledge Handbook of European Integrations. Eds. T. Hoerber; G. Weber; I. Cabras I. Routledge, 2022. p. 254-269.
517. Proposal of 21 April 2021 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, 2021/0106.

Czechia) have altogether given out 21 partial compromise proposals.[518] For the purposes of this section, we will consider the latest full Council proposal as the Council's stance on the AIA (Coreper AIA).[519] The EP adopted their negotiation position (EP AIA)[520] in June 2023 which included substantial amendments to the Commission's original proposal.[521]

Nonetheless, we can assume that the AIA would be significant in relation to the ADM in public administration. In fact, like the GDPR has conceptualised ADM in legal terms, the upcoming Artificial Intelligence Regulation would to the same to the use of AI, be it within or without the scope of ADM in public administration.

That said, it will not be easy to make the points of departure in AIA and public administration fit together seamlessly. This is because the market-oriented logic of the AIA may be difficult to reconcile with the public law nature of the national ADM legislation. The AIA draft is based on harmonising internal market rules[522] making it product safety legislation with market-oriented logic with parallel objectives to ensure fundamental rights.[523]

The AIA proposal is a horizontal, risk-based legislation which operates with four levels of risk. Firstly, most use of AI will be considered as minimal or no-risk which will be allowed, and secondly, some low-risk AI will have transparency requirements.[524] Thirdly, high-risk AI systems will be imposed on most rigorous requirements and the final level is AI systems which are considered so risky that they will not be allowed at all.[525] The market-oriented logic is visible from the approach to regulate the development, marketing and use of AI and it is mainly directed at manufacturers of AI systems.[526]

The AIA will inevitably create requirements for digital public administration as well. The risk-based approach functionally means that some AI systems used in administration would be considered to be high-risk or prohibited, but not all. This type of separation to risk levels is not common for public administration where the lex generalis creates overarching requirements for all public administration irrespective of the techniques used. Additionally, the public administration and the applied technologies are always context-specific, meaning that they must be in line with the broader administrative law principles and doctrines, but also the specific legislation regulating that administrative branch and function.

---

518. Some of which were classified as progress reports, some targeted individual articles and yet others were full compromise proposals. The AI Act, Documents https://artificialintelligenceact.eu/documents/.
519. Council of the European Union (2022) 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 – General Approach 2021/0106(COD) Brussels, 25 November 2022.
520. European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) P9_TA(2023)0236 https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf.
521. See list of key proposed amendments in European Parliament, Legislative train schedule https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence.
522. Legal basis for the proposal is Article 114 of the Treaty on the Functioning of the European Union, OJ C 326/47 (functioning of the internal market) Proposal of 21 April 2021 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, 2021/0106.
523. This approach has been present since the political declarations that AI should be regulated at the EU level. Artificial Intelligence in the European Union: Policy, ethics and regulation. / Ulnicane, Inga. The Routledge Handbook of European Integrations. Eds. T. Hoerber; G. Weber; I. Cabras I. Routledge, 2022. p. 254-269.
524. Proposal of 21 April 2021 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, 2021/0106.
525. Proposal of 21 April 2021 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, 2021/0106.; More on the risk-based approach and how AI systems risks will be assessed see Certification systems for machine learning: Lessons from sustainability. / Matus, Kira; Veale, Michael. In: Regulation & Governance. 2021; Demystifying the Draft EU Artificial Act: Analysing the good, the bad, and the unclear elements of the proposed approach. / Veale, Michael; Zuiderveen Borgesius, Frederik. In: Computer Law Review International. No 4, 2021.
526. Proposal of 21 April 2021 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, 2021/0106; Artificial Intelligence and the Law: can we and should we regulate AI systems? / Koulu, Riikka; Sankari, Suvi; Hirvonen, Hanne; Heikkinen, Tatjaana. Research Handbook on Law and Technology. Eds. B. Brozek; O. Kanevskaia; P. Palka. Edward Elgar, Upcoming 2024.

Furthermore, considered from a broader perspective, the inherent power asymmetries within administrative systems may become overlooked, if/when the legislation incorporates merely software-oriented safeguards (we will return to the safeguards below). Since none of the AIA proposals recognise public administration as its own context, it remains to be seen how the practical adaptation of AI rules fits in the public law logic of the national administrative system.

4.2 Objectives and the scope of the AIA

While the AIA proposal's purpose is also to protect fundamental rights, tangible human rights protection seems rather vague in the proposals.[527] The human rights protection aspect relates to the national public administrative field as well as the national ADM legislation precisely due to its inherent links to the right to good administration, for example. It seems that the AIA proposal's main means for human rights protection slips into the picture through the ban of non-allowed AI systems as well as mandatory industry self-assessment against harmonised standards and mandatory third-party CE certification.[528]

Self-assessment and CE certifications are not familiar rights protection techniques in administrative settings, which tend to rely on the principle of legality and appropriate accountability mechanisms. Additionally, it has been noted that the AIA proposal's lack of an individual appeal mechanism (which is a more traditional way for human rights protection within the public field) further hinders individuals' opportunity to stand up for their rights. The proposed AIA's approach to human rights protection sits well in line with the view that at the core of the proposed AIA is product safety and market surveillance legislation, and human rights protection comes into the picture as a side product.[529]

For purely speculative purposes, if rule-based systems were to be included in the final AIA, most (but not all) ADM systems used in the public administrative sector would be bound to follow it. Practically, for high-risk AI systems, the proposal would require heightened transparency obligations including enhanced monitoring and observability, and CE certification to ensure conformity with the regulation.[530]

It remains questionable how far requirements such as the main means of human rights protection will have an impact in public administration settings, which functions under different forms of public law logics that are much more historically rooted, as mentioned. Securing fundamental rights under public administration inevitably requires considerations that are not always present when the question is of private, non-fundamental services. For example, the ability to exercise the Constitutional right to social security should be fundamentally secured (Constitution Section 19). In comparison, the level of safeguards necessary to protect a person from being given incorrect information from ChatGPT cannot be considered to be as fundamental from a public law perspective.

527. Artificial Intelligence and the Law: can we and should we regulate AI systems? / Koulu, Riikka; Sankari, Suvi; Hirvonen, Hanne; Heikkinen, Tatjaana. Research Handbook on Law and Technology. Eds. B. Brozek; O. Kanevskaia; P. Palka. Edward Elgar, Upcoming 2024; Beyond Individual: governing AI's societal harm. / Smuha, Nathalie. In: Internet Policy Review. 2021.
528. This approach has been criticised, see e.g., Beyond Individual: governing AI's societal harm. / Smuha, Nathalie. In: Internet Policy Review. 2021; How the EU can achieve legally trustworthy AI: A response to the European Commission's proposal for Artificial Intelligence Act. / Smuha, Nathalie et al. In: SSRN. 2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991; Demystifying the Draft EU Artificial Act: Analysing the good, the bad, and the unclear elements of the proposed approach. / Veale, Michael; Zuiderveen Borgesius, Frederik. In: Computer Law Review International. No 4, 2021.
529. I.e., human rights as a side product see more Artificial Intelligence and the Law: can we and should we regulate AI systems? / Koulu, Riikka; Sankari, Suvi; Hirvonen, Hanne; Heikkinen, Tatjaana. Research Handbook on Law and Technology. Eds. B. Brozek; O. Kanevskaia; P. Palka. Edward Elgar, Upcoming 2024.
530. Proposal of 21 April 2021 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, 2021/0106.

Finally, the use of documentation for oversight purposes is a commonality between the AIA proposal and national ADM legislation. The main oversight function for judicial protection seems to be ensured in the AIA proposal through mandatory documentation.[531] As mentioned above, the national ADM legislation also relies heavily on documentation when it comes to judicial protection. Thus, in both the AIA and the national ADM legislation, documentation of the system is a fundamental way to ensure oversight of the system. Attaining this approach for oversight allows for the retention of discretion in the functionality of the systems with human actors. Considering the legality of the systems used, keeping humans in the loop remains a necessary component to ensure equity of the independently functioning technology.[532]

4.3 Potential parallel application of AIA and national ADM legislation

Whether the AIA will apply in parallel to the Finnish national ADM legislation on rule-based systems has not been settled. The ADM legislation's preparatory documents hardly scratch the surface of the upcoming AIA to affect the ADM legislation.[533] The AIA is mentioned very briefly, accompanying a statement that since the final version and scope of application of the AIA is not known yet, the impact of the future regulation must be assessed once the final regulation is agreed upon.[534] The central question is what the final definition of AI in the AIA will be; that definition will determine which systems will fall under the future AIA. This question is also one of the main debates in the ongoing trilogue negotiations.

In the AIA proposal, AI is defined as follows:

'software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.' [535]

This definition is not technology-specific in a way that would explicitly leave out rule-based systems. In other words, the definition does not state which systems it includes, which would practically mean that rule-based systems would most likely fall within the definition of AI.

However, the Council's negotiation position would limit the definition of AI as meaning machine learning and/or logic- and knowledge-based approaches, ultimately excluding rule-based systems from the definition.[536] In the latest Council's compromise proposal AI is defined as follows:

'a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge-based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts.' [537]

---

531. Proposal of 21 April 2021 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, 2021/0106.
532. Albeit there is an ongoing academic discussion about the nature of AI and other computational functions as an 'actor' under the law. As of now, the common approach is that technology is merely a tool for humans. See more, Human-algorithm hybrids as (quasi-)organisations? On the accountability of digital collective actors. / Beckers, Anna; Teubner, Gunther. In: Journal of Law and Society. No. 50. 2023.
533. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 7, 133.
534. Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi HE 145/2022 vp (Government Bill on legislation for automated decision-making in the public administration) p. 7.
535. Proposal of 21 April 2021 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, 2021/0106.
536. Council of the European Union (2022) 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 – General approach 2021/0106(COD) Brussels, 25 November 2022.
537. Council of the European Union (2022) 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 – General approach 2021/0106(COD) Brussels, 25 November 2022. p. 71.

The EP's adopted negotiation position would leave the definition of AI as general in line with the Commission's proposal, and not tie it to a specific technology.[538] More specifically, AI is defined by the EP as follows:

'a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.' [539]

Whether the definition of AI includes rule-based systems is fundamental for the applicability of the future AIA in parallel with the Finnish ADM legislation. Thus, the Council's position to leave out rule-based systems from the scope of the AIA is supported by the Finnish negotiators.[540] At the same time, according to the Finnish Constitutional Law Committee, considerations on fundamental rights and legality control have not been sufficiently considered during the drafting of the Finnish position.[541] The evident opposition to the all-encompassing definition for AI is highlighted, but the position seems to lack thorough constitutional assessment especially from the fundamental rights perspective. In the drafting of the ADM legislation, the Finnish legislator seems to have left the discussion on the future EU-level rules on AI fully outside the scope of concerns. Thus, in the end, if rule-based systems are included in the AIA, the national legislator and administrative actors will have a lot of work to do to consider how to apply the AIA together with the national ADM legislation. Also, some of the computational systems are so complex that identifying whether the system uses machine learning or other equivalent technology is not that simple to identify.

Furthermore, considering the AIA doctrinally, the proposal currently leaves open whether AI systems that are already functioning would fall under the scope of the regulation. Article 83(2) of the AIA proposal states that the regulation applies to high-risk AI systems that have already been put into service before the application of the Regulation 'only if, from that date, those systems are subject to significant changes in their design or intended purpose'. If the article remains unchanged in the final AIA, it seems that an already functioning ADM system that does not go through a 'significant change' would not be governed under the AIA. At this stage, however, what the final version of the AIA will look like and how individual rules included in the regulation will function practically remains speculative.

5. The challenge of law and technology

As discussed above, ADM and soon also AI are becoming conceptualised and regulated as administrative law issues. The EU legislation has brought in new concepts and some of them have already been incorporated into the national legal field through the ADM legislation. Above, we have mapped out the Finnish doctrinal landscape of the public administrative system with special attention to ADM. However, clearly, the administrative system does not merely consist of laws. It also consists of deeper layers of the legal system which guide and shape the functioning of the novel legal rules. At the same time, public administration is a practice which is increasingly

538. European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) P9_TA(2023)0236 https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf.
539. European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) P9_TA(2023)0236 https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf. p. 112.
540. Valiokunnan lausunto PeVL 4/2023 vp – U 28/2021 vp (Statement of the Constitutional Committee) p. 2.
541. Valtioneuvonston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi tekoälyn harmonisoiduksi sääntelyksi U 28/2021 vp; Valtioneuvoston U-jatkokirjelmä UJ 29/2022 vp; Valiokunnan lausunto PeVL 37/2021 vp (Statement of the Constitutional Committee); Valiokunnan lausunto PeVL 4/2023 vp (Statement of the Constitutional Committee).

conducted through digital technologies and interfaces. Thus, the technologies used in administration are contextually dependent on the broader administrative legal system on one hand, and the actual practical technological decision that affects the state-citizen interactions on the other.

In the next section, we use Kaarlo Tuori's theory of critical legal positivism to see how the general principles and theories of law enable and limit ADM. The aim is to show that legislation does not take place in a vacuum, but it is always part of a bigger doctrinal and cultural entity.[542] After that, we will outline recent Finnish socio-legal research in which the digitalisation of public administration is analysed through the lens of user interfaces. This research will provide an example of how the technological design, which to some extent is based on law, can be legally relevant. It illustrates the contextual significance of technology in engaging with the citizens through a digital interface.

5.1 Within the legal system – Tuori's Critical Legal Positivism

Some scholars have considered digitalisation to be legal irritant due to its way of challenging general principles of law.[543] On the one hand, in a digitalised society data and knowledge are gaining increasing significance as forms of governance; this is something that public administrative law has had trouble recognising.[544] On the other hand, incorporating ADM into our legal system pushes us to consider the place of constitutional principles, specific legislation, and even fields of law, such as public procurement, that are not evident at the outset. What is their meaning in the fabric of digitalising administrative law?

Finnish legal philosopher Tuori's critical legal positivism has been a prominent way to approach the understanding of 'legal order' in Finland and beyond. Here, it will allow us to consider the dynamic of change at the same time as the stability in law. We argue that it has special explanatory power for analysing the effects of the digitalisation of law.

Tuori's basic idea is that law is a three-layered phenomenon.[545] The three layers of the legal order are in constant interaction. The visible part of the legal order, namely its representation through enacted laws, lower-level norms, highest court rulings and influential legal research, is its mutable surface, the top layer.[546] The surface of the legal order is mutable exactly because changes can be rapid due to the possibility for the regulations to change relatively quickly and sometimes unpredictably by the will of the legislator. However, the surface level of the law is not only shaped by politics but also by the deeper layers' normative assertions.

Drawing inspiration from Foucault, the theory does not stop at the turbulent surface but accepts that the metastructure of the scientific knowledge, in this case, law, is not fully embodied in the visible representation.[547] Thus, the two layers that lie under the mutable surface, legal culture and the metastructure of law, play an important part in the legal order as the visible representation. Legal culture is a contested concept[548] but in the context of Tuori's contribution to Finnish legal philosophy, it can be understood as including legal principles, general doctrines, and concepts of law in different legal fields as well as legal professionals' culturally affiliated

542. Here by context, we mean the overall administrative legal system, individual branches of administration as well as technologies that are available.
543. Legal Irritants: Good Faith in British Law or How Unifying Law Ends Up in New Divergencies. / Teubner, Gunther. In: Modern Law Review. No. 61, 1998; Miten Hyvä Hallinto Digitalisoidaan? Haaste Oikeustieteelliselle Tutkimukselle. / Koivisto, Ida; Koulu, Riikka. In: Lakimies. No. 118, 2020. p. 799.
544. Kohti digitaalisen ajan hallinto-oikeutta. / Pöysti, Tuomas. In: Lakimies, No. 6-7, 2018. p. 873.
545. Critical Legal Positivism. / Tuori, Kaarlo. Ashgate, 2002. p.147.
546. Critical Legal Positivism. / Tuori, Kaarlo. Ashgate, 2002. p. 154-161.
547. The Order of Things: An Archaeology of the Human Sciences. / Foucault, Michel. Pantheon Books, 1970; Kriittinen oikeuspositivismi. / Tuori, Kaarlo. Werner Söderström Lakitieto OY, 2000. p. 79-88; Oikeus on, miten se systematisoidaan? Kysymys oikeudenalajaotuksesta ja hallinto-oikeudesta. / Koivisto, Ida. In: Lakimies, No. 7-8, 2015.
548. Especially in the field of Comparative law, the concept of legal culture has been a prominent academic debate for centuries.

methods.[549] Legal culture is shaped by long-standing legal practises that have been sedimented deeper in the legal structure as more or less unquestioned norms. While the second layer goes deeper into the understanding of the law, this is not enough to exhaustively understand the legal order.

The deep structure of law, the third and most fundamental layer, encapsulates the core of Western legal traditions.[550] Tuori approaches the explanation of the third layer by asking: despite the different surface and legal cultures in the USA, Germany, and Finland (examples), is there still something common? Consequently, he points out that the deepest layer includes, for example, human rights and the concept of legal subjects. This is the most abstract level at which changes are expected to be slow.

This layered approach supposes a normative hierarchy. The surface-level norms must be in line with the deeper-level norms. While that is the case, the layers interact and influence each other constantly. These interactions may happen top-to-bottom or bottom-to-top.[551] For example, legal culture may become obvious on the surface through culturally contextual legislation, or it can justify things happening on the surface. For example, once ADM has been used and issues have arisen while no legislation applies, the judicial oversight bodies have had to dig deeper into the structures of the legal order in order to find redress to seemingly inequitable situations, such as the principle of good administration. Another way for the layers to interact is how central legal practices become settled to the deeper levels. This shows the continuous flowing and organic nature of legal order, which is constantly (slowly) changing as a whole.

This approach helps in understanding the phenomenon of how societal changes challenge the basic doctrines of all fields of law.[552] Changes in administrative law majorly affect its construction and determining its dimensions.[553] When the public administration experiences changes in processes (quality, extent) or in law, these changes inevitably require reconsideration of its classical and more embedded doctrines.[554] When practical public administration is infused with novel solutions, it simultaneously requires placing attention on the concepts, principles, and doctrines to make sure that these more foundational levels correspond with and are corresponded to by the new/modern public administration.[555] While administrative law must redefine itself in relation to the changes in the fluctuating structural circumstances of public administration, the deeper layers may function as limitations for the intensity and direction of these changes.[556]

For example, public administration has become increasingly proceduralised.[557] Ida Koivisto has noted that the identity of public administration in Finland has been transformed to resemble a 'methodological quality overseer'.[558] This is to say, the focus has been increasingly on the quality procedures and their acceptability. While at the same time, public administration has also been influenced by a fundamental right to good administration, a principle that has become a constitutional right. As Olli Mäenpää states, modern Finnish administrative law is characterised by quality assurance and financial/economic efficacy,[559] logics borrowed from the private sector. Often, efficacy is pursued through outsourcing and privatisation projects.

---

549. Critical Legal Positivism. / Tuori, Kaarlo. Ashgate, 2002. p. 161-183.
550. Critical Legal Positivism. / Tuori, Kaarlo. Ashgate, 2002. p. 183-191.
551. Critical Legal Positivism. / Tuori, Kaarlo. Ashgate, 2002. Chapter 7.
552. Oikeus on, miten se systematisoidaan? Kysymys oikeudenalajaotuksesta ja hallinto-oikeudesta. / Koivisto, Ida. In: Lakimies. No. 7-8, 2015. p. 967.
553. Oikeus on, miten se systematisoidaan? Kysymys oikeudenalajaotuksesta ja hallinto-oikeudesta. / Koivisto, Ida. In: Lakimies. No. 7-8, 2015. p. 968.
554. Hallinto-oikeus. / Mäenpää, Olli. 7 ed. Alma Talent, 2023. p. 56-57.
555. Oikeus on, miten se systematisoidaan? Kysymys oikeudenalajaotuksesta ja hallinto-oikeudesta. / Koivisto, Ida. In: Lakimies. No. 7-8, 2015. p. 969.
556. Oikeus on, miten se systematisoidaan? Kysymys oikeudenalajaotuksesta ja hallinto-oikeudesta. / Koivisto, Ida. In: Lakimies. No. 7-8, 2015. p. 969; Kriittinen oikeuspositivismi. / Tuori, Kaarlo. Werner Söderström Lakitieto OY, 2000. p. 236.
557. Oikeus on, miten se systematisoidaan? Kysymys oikeudenalajaotuksesta ja hallinto-oikeudesta. / Koivisto, Ida. In: Lakimies. No. 7-8, 2015. p. 970-971.
558. Oikeus on, miten se systematisoidaan? Kysymys oikeudenalajaotuksesta ja hallinto-oikeudesta. / Koivisto, Ida. In: Lakimies. No. 7-8, 2015. p. 970.
559. Hallinto-oikeus. / Mäenpää, Olli. 7 ed. Alma Talent, 2023. p. 71-74.

This is also visible from the preparatory documents for the ADM legislation for tax and customs which emphasise allowing ADM to be used in rectification claims easing the workload and therefore enhancing productivity.[560] Here, we can observe gradual changes to the field of administrative law. It seems like the way in which the public administration meets the citizens is changing, as is the rationality. However, at the same time, the citizen and their rights, such as the right to good administration seem to become more buried in the layers of public administrative law.

It seems promising to understand how automated decision-making disrupts and is disrupted by the broader legal context with support of Tuori's theory. The discussion on whether and how ADM is governed in Finland is not only a question of the legislation, but also how it fits in the deeper understanding of the legal order, its functions and logics. Thus, while the surface is turbulent, the ADM legislation also touches the deeper levels of the legal system. There are underlying assumptions that become visible through the changes in the processes of public administration.

For example, the legislative debates surrounding how to deal with discretion and the personal nature of official accountability (discussed in section 3.4. and 3.6.) were not easy problems to solve because the solution had to be in line with not only the surface-level law, but the deeper assumptions on human-centred legal principles and the fact that the administrative field seems to function on human-public official assumptions. This is visible from terminology as well as the way in which national liability for public officials' errors is personal and placed for the *human* public official.

The automated procedure and consequent decision reached required rethinking assumptions present in deeper levels of the administrative legal system. The technology-specific legislation is contextually dependent on multiple other fields of law as well as deeper, more fundamental doctrines and principles of the legal system. Incorporating ADM in administrative functions raises questions of constitutional nature such as equality, access to justice and allocation of liability. Furthermore, the cross-sectional interdependence of certain administrative laws to other legal fields, such as criminal law had to be reconciled.

In addition, the new ADM legislation brought with it novel administrative law concepts and it is not yet known how they would fit the whole administrative law system. Institutional practices will most likely show their importance in the settlement of the new concepts into the administrative legal order. When the processes and practices change, they not only require a change in the text of law but also they influence and are influenced by the deeper layers of legality. Thus, we should not only look at the surface, i.e., how ADM is legislated and what issues arise, but also more fundamentally, i.e., how it affects and how it is affected by legal culture as well as the 'meta legality' of Finnish legal order.

Furthermore, it is not only the national legal order that affects and is affected by these changes. As discussed extensively throughout this section, EU law and currently the GDPR play an important role in relation to ADM. EU law is involved due to article 22, and therefore the whole GDPR is involved. We have discussed the issues brought by the legal safeguards presented in recital 71 and whether they are applicable in national administrative ADM. As mentioned, this is a question for the CJEU to decide. However, the application of the GDPR shows that it is not only the national legislative system that the use of ADM and individual provisions in the legislation must fit in, but also the EU legal order. The case will be the same with the upcoming AIA.

560. Hallituksen esitys eduskunnalle automaattista päätöksentekoa verotus- ja tulliasioissa koskevaksi lainsäädännöksi HE 224/2022 vp (Government Bill on legislation for automated decision-making in tax and customs) p. 7.

5.2 Within the administrative practice – the perspective of usability

In addition to the effect on the legal system comprehensively, the transformative nature of technology in public administration can be also approached from a more practical point of view. Recently, two of the authors of this report have also analysed digitalisation of public administration from the perspective of usability of digital interfaces.[561] In the previous research the technology-specific legal landscape was systematised through the way in which the digital public administration is construed.[562] It allowed the questions that stem from the more abstract requirements that the fundamental principles create to be defined better. The approach adopted was to systematise the legislation in accordance with whether it affects 1) administrative workers' user interface, 2) back-end solutions, or 3) citizens' user interface. These three entry points to the technology were used as heuristic tools on how to consider public administrative law from a socio-legal research perspective. This type of systematisation proved to be beneficial especially due to the fragmented nature of legislation which applies to digital public administration.

Since the relevant legislation was considered through IT concepts, i.e., 'user interface', 'front end' and 'back end', it seems necessary to briefly explain what these concepts mean. In computer science terms, user interface means the part of the technology or a digital artefact that is visible to the user and with which the user interacts with. The front end of a digital system can be considered to be a somewhat analogous term to user interface but it encompasses more functions that allow the user-interface to work as it does. The back end consists of the functionalities and abilities of the digital system that are not visible to the user. These include, for example, data management and interoperability of different systems.

Even though front end, back end and user interface are not legal terms, different aspects related to them are already mentioned under Finnish as well as EU law. For example, the preparatory documents for above mentioned IMA (more in section 1.2.7. above) and ESCPS (more in section 1.2.8. above) recognise the importance of the back-end systems to the usability of the digital service.[563] Thus, in the planning and building of the digital administrative system, the operability of the system is to be understood comprehensively. Although the legislation relating to the back-end systems of digital public administration implicitly recognises the connection of that specific part of the technological solution to the overall functioning of the system, there is little explicit reference to the comprehensiveness of the digital systems.

In other words, the connection between a proper functioning of the back end and the functioning of the whole digital service is not clearly written in the law, nor included in it as an obligation. Consequently, situations in which an issue at the back end of a digital system has caused negative consequences for a citizen cannot be properly addressed by the laws regulating the back end of the systems. In such cases, the courts and legality controllers can tackle the issue through core administrative law principles, such as the principle of good administration.

In relation to the citizens' user interface, the nationally implemented Accessibility Directive Act on the Provision of Digital Services (discussed in section 1.2.8. above) proved to be the most influential legislation regulating the usability of the digital public services. As mentioned above, the Act on the Provision of Digital Services as well as the standards that the legislation requires

561. Digitalisoituva julkishallinto: käytettävyys kuuluu kaikille. / Koulu, Riikka; Sankari, Suvi; Sormunen, Sofia. In: Edilex. No. 36, 2022.
562. Digitalisoituva julkishallinto: käytettävyys kuuluu kaikille. / Koulu, Riikka; Sankari, Suvi; Sormunen, Sofia. In: Edilex. No. 36, 2022. p. 11.
563. Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi 284/2018 vp (Government Bill for an act on the information management in public administration) p. 60, 123 (IMA); Hallituksen esitys eduskunnalle laeiksi hallinnon yhteisistä sähköisen asioinnin tukipalveluista sekä valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain muuttamisesta 59/2016 vp (Government Bill for an act on electronic services and communication in the public sector) p. 56.

to follow are both built to especially cater to people with special needs. However, accessibility and usability are not merely questions for people with special needs. There have been cases brought to the Chancellor of Justice that illustrate that anyone can encounter unclear situations in digital administration and therefore the question of accessibility and usability should be understood as all-encompassing and essential for everyone.[564]

Another point that the Act on the Provision of Digital Services brought was that the accessibility and usability of digital public services are to be ensured through principles and techniques followed in the planning and constructing of the system. However, these 'principles and techniques' are not properly defined. The preparatory documents illuminate that the techniques include user testing, which is guided by general standards.[565] "Standards" are mentioned but it has not been specified which standards are meant. Thus, even though the PDS seems to guide the provision of digital services so that they are in line with the four core principles, the more specific guidance on accessibility is vague in the law.

Still, usability becomes materialised precisely during the planning and construction of the digital system. Building a digital system is necessarily context-dependent and aims to cater to the needs of that specific public administrative function. Since the guidance for user testing – which forms the core for ensuring the usability of the system – remains relatively vague in law, it has not considered how legal protection or the principle of good governance could be used as guiding principles in constructing a digital system. Still, legal overseers have tackled cases relating to poor usability of public administration's digital system through the principle of good administration and the service principle. One case has signalled that the public administration needs to know the users and take their diversity into account when planning and creating these media.[566]

While the legislation is sparse when it comes to many specific situations, many laws touch upon the digital state's functions as mentioned above. When digital administration is considered from a usability point of view, it allows consideration of the issues beyond the applicable legislation. While legislation is essential, it is not all-encompassing when it comes to the legal protection of citizens acting with the public administration. All digital systems incorporated into the administrative function are context-dependent and built with the aim of catering to the needs of that specific function. The planning and constructing phase of a digital system is precisely the point in time when decisions that affect the legal protection of citizens are made. Usability as the entry point is a way to define this. Ensuring judicial protection, good administration and other fundamental principles is usually only possible through context-dependent technology.

6. Potential for Northern European collaboration

When technology is implemented to perform a public administrative function – by replacing or assisting a public official – that technology is created to cater to the specific needs of that branch of administration. In other words, the digital solution is made for the specific organisation catering to its practices and for its users. That context translates poorly from an administrative branch to another, not to mention from one country to another. However, the similarities between the Nordic administrative traditions and legal cultures make it worthwhile to consider the possibilities for deepening collaboration. Furthermore, Northern European countries may share similar needs and issues related to the preservation of their official languages, as globally AI development is dominated by English and Chinese languages and smaller language areas may lack the resources needed for developing contextual AI tools.

564. E.g., OKV/1179/2020; OKV/663/1/2019.
565. Hallituksen esitys eduskunnalle laeiksi digitaalisen palvelujen tarjoamisesta sekä sähköisestä asioinnista viranomaistoiminnassa annetun lain muuttamisesta 60/2018 (Government Bill for an act on the provision of digital services) p. 64.
566. OKV/1179/2020.

In the following, we raise two contextual factors that might limit the translatability of technology. Firstly, the applicable laws and secondly, the technology itself. Following Tuori's thesis, the surface-level legislation is intrinsically linked with the logics of the national legal order. The surface-level laws must reflect the norms, principles, and assumptions of the deeper levels. This means that the technology-specific national laws do not merely regulate the technology as they stand but aim to tie in the digital tools with the deeper legal context of the given legal system. While that is the case, transnational legislation, notably EU law, also fundamentally influences the digital administration. Still, as it is apparent from the national application of the GDPR, that while the regulation is directly applicable law, it includes many aspects which leave room for national interpretation and application (more in section 1.2.3. above). The same can be expected from the upcoming AIA. Only time will show us how fragmented the application of AIA will be within the 27 EU Member States, not to mention how the CJEU will interpret the individual articles. From a purely legal point of view, countries that share a similar legal history and culture would pose more fertile soil for sharing technology for public administration. Still, a similar legal culture and smaller language group do not remove the context dependency of the utilised technology.

The second contextual factor that limits the translatability of technology in public administration is the technology itself. The ability to make use of the same digital system in another context is not merely a legal question but also a practical one (in which legislation plays a role). When the digital tool for public administration is designed, it is designed for a specific context and for a specific user group. Ensuring the usability of the technological system is one of the fundamental ways for the given digital solution to be in line with many applicable fundamental legal principles. If the usability of the technology is poor, it can affect the legal protection of individuals and even make the technology redundant. However, as it is with other systems, usability is highly context-dependent in the digital public administrative systems as well.

We wish to explain this further with the help of an analogous example – Apotti, the Finnish patient information system for medical personnel. While Apotti is purely a digital system for the medical field, patient safety (that is at stake in the medical field) can be analogically considered with legal protection (that is at stake in the public administration field).[567]

Apotti became the patient information system in Finland because of a public procurement process. The system is based on a patient information system called Epic, which was developed by a company based in the United States (US).[568] Epic's translation into the Finnish context began in 2016 and resulted to Apotti 1.0. Apotti has undergone upgrades and smaller fixes during its time due to heavy criticism, especially by its users, medical professionals that is. Development of Apotti's second version began in 2021. Essentially Apotti has been criticised for its poor usability and fragmentation of information within the system, which has resulted in inability for a medical professional to see all necessary information on their user interface.[569]

One of the reasons for Apotti's issues has been its roots in the US system while further developing the system resulting in a complicated ensemble of technological parts also played a role.[570] The translation of Epic into Apotti did not merely include the language translation from English to Finnish, but also the translation of the technology designed for the US healthcare system's processes to correspond to the design of the Finnish healthcare system. Evidently, the healthcare systems are driven by different logics, as Nisula vividly explains: 'law and invoicing

567. Digitalisoituva julkishallinto: käytettävyys kuuluu kaikille. / Koulu, Riikka; Sankari, Suvi; Sormunen, Sofia. In: Edilex. No. 36, 2022. p. 18.
568. Sano aaa niin kuin Apotti – paraneeko tietojärjestelmä vaihtamalla? / Nisula, Sara. In: Finnanest, No. 52, 2019. p. 15.
569. Sano aaa niin kuin Apotti – paraneeko tietojärjestelmä vaihtamalla? / Nisula, Sara. In: Finnanest, No. 52, 2019. p. 15.
570. Digitalisoituva julkishallinto: käytettävyys kuuluu kaikille. / Koulu, Riikka; Sankari, Suvi; Sormunen, Sofia. In: Edilex. No. 36, 2022. p. 18.

driven hierarchical American healthcare system translated into Haaga healthcare centre, independently functioning midwives, and urgent care that costs €48,90 for the citizen.'[571] Customisation and finetuning of the digital system based on foreign processes and logic has not been cheap.

The situation with Apotti finally became untenable so that the national supervisory authority for welfare and health (Valvira) started to investigate the matter and have given two decisions on its issues. The first one was a result of more than 600 medical professionals' complaints and the second was based on own initiative inquiry.[572] Valvira stated that as it stands, Apotti is in line with the applicable laws, but they will continue to follow the development of the system and especially place attention for the improvement of its usability.[573] The own-initiative inquiry targeting Helsinki and the Uusimaa welfare regions' social and healthcare group was dimmer. Valvira gave multiple requests for improvement in relation to the visibility of certain information and following the demand of an individual not to share their data with other healthcare systems.[574]

All in all, the translation of the US-based system to the Finnish healthcare contexts shows how using the same system in similar (both healthcare systems) but different contexts has proved to be more difficult than originally thought. The same can be expected from a technology designed for other public administrative functions. While the context for the technology would largely be the same (public administration), the logic and the processes of different countries' administrative systems inevitably are not identical. Nevertheless, the Northern European countries have more similarities than the US and Finnish healthcare systems, and thus the risks for long-lasting further development would be smaller. In the end, the question is how beneficial sharing the technology would be.

7. Conclusion

In this chapter, we introduced the legal framework considering automated decision-making in public administration in Finland. We also presented the background and implications of the relevant legislation and analysed some of its theoretical and practical dimensions.

The most important thing is to highlight that as an EU member state, Finland's legal approach to ADM stems from the GDPR conception of ADM. Decades before the GDPR, computers were used in public administration, but ADM was not fully considered as an independent object of regulation. In the late 2010s and early 2020s, this discrepancy between the GDPR and constitutional principles, and approaching those technologies as tools only gained increasing critical attention. In spring 2023, Finland adopted a new ADM allowing legislation, which enables fully automated administrative decisions in all public administration, when certain criteria are met. As we have shown, the legal niche to accommodate this legislation has been rather small – due to the GDPR and national constitutional restrictions – while political pressure to adopt it was considerable.

571. Sano aaa niin kuin Apotti – paraneeko tietojärjestelmä vaihtamalla? / Nisula, Sara. In: Finnanest, No. 52, 2019. p. 16. Translation by the authors. Original: [...] juridinen ja laskutus edellä menevä hierarkkinen, amerikkalainen terveydenhuolto käännetään Haagan terveysasemaksi, itsenäisesti toimiviksi kätilöiksi ja kansalaiselle 48,90 euroa päivässä maksavaksi tehohoidoksi.'
572. Apottijärjestelmä vastaa lainsäädännön vaatimuksia, mutta valvonta jatkuu. / Valvira. https://www.valvira.fi/-/apotti-jarjestelma-vastaa-lainsaadannon-vaatimuksia-mutta-valvonta-jatkuu. Valvira kehottaa HUS-yhtymää korjaamaan Apotti-järjestelmään liittyviä ohjeitaan ja käytäntöjään. / Valvira. https://www.valvira.fi/-/valvira-kehottaa-hus-yhtymaa-korjaamaan-apotti-jarjestelmaan-liittyvia-ohjeitaan-ja-kaytantojaan. The latter decision concerned only Helsinki and the Uusimaa welfare regions' social and healthcare group.
573. Decision V/32836/2022
574. Decision V/32832/2022

To conclude, we wish to raise six points:

1. First, the new ADM legislation is decision-oriented. On the one hand, this is logical as the administrative decision is perhaps the most important way of using public power in Finland. On the other, however, this orientation may obfuscate the fact that digital technologies are also used in other administrative activities, and sometimes it is hard to demarcate an administrative decision from other activities. Thus far, those other activities remain unregulated.

2. Second, the concept of good administration is of key importance in both legitimating and curbing the extent of automated decision-making nationally. The constitutional nature of the principle gives it specific weight. Digital administration must be good digital administration. This also means that automated decisions need to meet the quality criteria of administrative decisions in general, and good administration can further serve as a tool for developing the digitalisation of administration.

3. Third, as for now, it remains uncertain how the upcoming AIA will affect the legal landscape of ADM in Finland. The decisive factor will be the definition of AI in the AIA: if AI covers rule-based systems, the Finnish ADM will fall under its scope, and pressure to amend the newly adopted legislation will emerge. If not, the national legislation and the AIA might not overlap, leaving current legal solutions intact. Neither does the AIA define public administration as a separate high-risk field, but only some parts of it, which further adds to the ambiguity.

4. Fourth, in the spirit of Kaarlo Tuori's critical legal positivism, the introduction of ADM as a regulatory object is not only a surface-level phenomenon in the Finnish legal order. Instead, it also challenges some of the fundamental doctrines of administrative law. As we have argued, this goes especially for personal criminal liability of public officials, and the use of discretionary powers in decision-making. Digitalisation may affect those doctrines beyond the use of digital technologies.

5. Fifth, we have shown how ADM is not only a matter of legislation, but its effectiveness and legitimacy also depend on usability and accessibility. Thus, with digital public administration, the legal and technological aspects become inseparable from one another.

6

Sixth and finally, we emphasise that Northern European countries have many similarities both in legal traditions and cultures as well as in the needs and concerns related to both technology development and deployment, and technology regulation. It remains unclear – and potentially worth investigating more closely – to what extent the cultural similarities can mitigate the context dependency and poor transferability of most digital technologies. However, the increasing European technology regulation has the potential to produce harmonised rules for the internal market, which could also enable new technological innovations of digital public administration.

LATVIA

The Digitalisation of the Public Administration

Anastasija Kaplane and Aleksandrs Potaičuks

The authors would like to express their gratitude to Mr. Gatis Ozols, Deputy State Secretary on Digital Transformation Affairs, for consultations during the research and writing process.

Abstract

In the present chapter, the authors provide an overview and analysis of the digitalisation of the Latvian administrative sector.

Section 1 sets the background, describing the structure of the Latvian administrative sector, domestic legislation regulating the Latvian administration and the digital tools that have been implemented in its operation: the national portal of state administration services www.latvija.lv, digital post for communication between individuals and authorities, virtual assistants (chatbots) and various national databases. Further, the section outlines the plans for future digitalisation.

Section 2 examines the challenges posed to the enjoyment of fundamental rights by these developments. To do that, the authors analyse the national practice: three judgments of the Constitutional Court of Latvia, six opinions of the Ombudsman and one judgment of the European Court of Human Rights in the case against Latvia. Preliminary conclusions are that, while digitalisation as such pursues legitimate aims, the proportionality test must be performed more carefully.

Section 3 answers the question of whether the current legal framework supports digitalisation by looking into the Cabinet of Ministers Regulations Regarding the Public Administration E-services and the national Digital Transformation Guidelines 2021–2027 as documents fostering digitalisation and then at the Latvian Administrative Procedure Act as an example of technology-neutral law.

In section 4, the authors take a look at the proposed European Union Regulation on Artificial Intelligence and identify three perspectives on how it could supplement national administrative law: by ensuring a new level of protection for businesses and individuals, accelerating existing public services and establishing a novel administrative legislative framework for the use of AI.

In section 5, the authors conclude with three suggestions: harmonisation of the digitalisation in the Nordic-Baltic region to minimise fragmentation, introducing a more elaborate impact assessment in the context of fundamental rights protection and – finally – changing the paradigm by looking at digitalisation as an inherent part of *any* reform in public administration.

1. Latvian administrative sector

The following section provides a brief overview of Latvian administrative law as well as digitalisation implemented in the administrative sector. First, in subsection 1.1. the Act on State Administration Structure, the Act on Local Municipalities and the Administrative Procedure Law is introduced. Next, subsection 1.2. presents the implemented digitalisation measures prioritised by Latvia. This subsection presents both legislative measures as well as the practical performance thereof. And finally, in section 1.3. authors briefly reflect on the future digitalisation plans of Latvia as stipulated by the "Digital Transformation Guidelines for the term of 2021–2027" adopted by the Cabinet of Ministers, that is the government of the state and the highest executive body of the country in all policy areas.

1.1 Overview

The legal framework or so-called *backbone* of the Latvian administrative sector is generally formed by the Act on State Administration Structure[575] adopted in 2002 and the Act on Local Municipalities[576] recently readopted in 2022. The Act on State Administration Structure sets out general principles for public administration; the institutional system of direct and indirect administration; the hierarchical order of state administration; the delegation of specific administrative powers; the participation of civil society in state administration; cooperation within state administration; the review of administrative decisions and liability thereof; the administrative contracts; the activities of administrative bodies in the sphere of private law as well as the liability of officials, property of administrative bodies, audit and public reports. Further, the backbone is completed by the Act on Local Municipalities that provides a legal framework for the local administration in Latvia, among others setting autonomous and delegated competencies of local municipalities; the institutional system thereof; the governance by local councils; supervision of municipalities; administration of property and the relationship between local municipalities and the Cabinet of Ministers.

In relation to this interaction between central and municipal governance, it is worth mentioning actualities in court case law. Namely, in Latvia, like in many other European countries, there are certain administrative tensions between local municipalities and central government. However, Latvia is unique in the Nord-Baltic (NB8) region in the sense that it provides a legal framework for councils of local municipalities to resolve such disputes with legislators in a public forum – the Constitutional Court.[577] As a result, it is common that vivid constitutional disputes on democracy questions take place in the court hearings and it imminently attracts not only the attention of legal scientists but helps to evolve administrative law science in Latvia.

In one of the recent cases, local municipalities contested the law on territorial reform adopted by the parliament in remote settings during the COVID-19 crisis. Municipalities claimed that the remote work of the parliament and thus the adoption of the contested provisions were contrary to Article 15 of the Constitution of the Republic of Latvia[578] that envisages parliament to hold

575. Act on State Administration Structure. Available at: https://likumi.lv/ta/en/en/id/63545-state-administration-structure-law, last accessed 27.08.2023
576. Act on Local Municipalities. Available at: https://likumi.lv/ta/id/336956-pasvaldibu-likums (in Latvian), last accessed 27.08.2023
577. Constitutional Court Law, Article 17 (1). Available at: https://likumi.lv/ta/en/en/id/63354-constitutional-court-law, last accessed 27.08.2023
578. Constitution of the Republic of Latvia, Article 15. Available at: https://likumi.lv/ta/en/en/id/57980-the-constitution-of-the-republic-of-latvia, last accessed 27.08.2023

its sessions in Riga City, but the remote work of members of the parliament who were spread across the country, according to the litigating municipalities, did not satisfy the respective provision of the Constitution. This high-profile case provided an opportunity for the judges of the Constitutional Court to express themselves on the electronic work of the parliament and the quality of legislative procedure.[579]

Besides the Act on State Administration Structure and the Act on Local Municipalities, there are a vast number of sectoral regulations of different hierarchical ranks creating a genuine *muscular system* of the Latvian administrative sector. The mentioned regulations cover different public sectors and include, for example, tax laws, construction laws, antitrust laws, access to public information laws, social security laws, laws regarding recruiting and promotion of public officials, disciplinary proceedings against public officials, prosecutors, attorneys, judges, as well as educational rights, migration and citizenship laws, food and drug safety laws, environmental laws, etc. Typically, this area of law these days in Latvia is strongly influenced by the European Union legislation or already qualifies as the European Union law de facto if the regulatory area is based on directly applicable EU regulations.

Finally, the state administrative structure is completed by Administrative Procedure Law[580] which operates and implements the above-mentioned regulatory framework and thus forms a sort of *circulatory system* of the regulation of the Latvian administrative sector. Administrative Procedure Law is the most fundamental procedural law when dealing with administrative cases by public servants and employees and is taught in depth to all law students in Latvia. The Administrative Procedure Law was adopted in 2001 (entered into force in 2024) and consists of two major unified procedural law sections, where the first one (Part A and B) sets administrative procedures when a citizen interacts with the state at an institutional level (either at first level institution or higher institution that reviews the decision of the first one) and the second one (Part C) sets administrative court procedure when individual adjudicates his case at administrative court (either first level administrative court, court of appeal or the Department of Administrative Cases within the Supreme Court of Latvia). Part A and B of the Latvian Administrative Procedure Law, and particularly the notion of 'administrative act', was built around the German administrative procedure apparent at that time, however, Part C on the rules for court procedures were built around Latvian Civil Procedure Law.[581] Thus, even these days civil and administrative judges can reference each other's case-law in judicially-procedural matters insofar as the respective procedures are related and are not contradictory.[582]

Even though the national administrative law was formed in a way that it could comprehensively regulate different decisions of governmental institutions, covering different domains and aspects of governance, these days the pressing needs of society and rapidly developing digital technologies are affecting the very core of administrative law and procedure.

1.2 Implemented digitalisation

Further on, the authors will reflect on the implemented digitalisation as well as plans for future digitalisation in the Latvian administrative sector. This includes a presentation of the general legal framework for digitalisation in state administration (subsection 1.2.1.), a few examples of digitalisation measures, such as a national portal of state administration services, electronic communication with national authorities (digital post), virtual assistants in state administration

579. Case No 2020-37-0106 of the Constitutional Court of Latvia. Available at: https://www.satv.tiesa.gov.lv/web/viewer.html?file=https://www.satv.tiesa.gov.lv/wp-content/uploads/2020/07/2020-37-0106_Spriedums_EN.pdf#search=2020-37-0106, last accessed 27.08.2023
580. Latvian Administrative Procedure Law. Available at: https://likumi.lv/ta/en/en/id/55567-administrative-procedure-law, last accessed 27.08.2023.
581. Ievads administratīvā procesa tiesībās (Introduction to Administrative Procedure Law) / Briede, Jautrīte; Danovski, Edvīns; Kovaļevska, Anita. Administratīvā procesa tiesības. Mācību grāmata. Rīga: TNA, 2023. p. 27.
582. Ievads administratīvā procesa tiesībās (Introduction to Administrative Procedure Law) / Briede, Jautrīte; Danovski, Edvīns; Kovaļevska, Anita. Administratīvā procesa tiesības. Mācību grāmata. Rīga: TNA, 2023. p. 28.

(chatbots) and composite and interlinked information management databases (subsection 1.2.2. to 1.2.5.). And finally, subsection 1.3. will conclude this section with a visionary presentation of future digitalisation plans, as stipulated by the "Digital Transformation Guidelines for the term of 2021–2027".

1.2.1 General framework of digitalisation in state administration

Even though digitalisation processes occur naturally, reflection thereof into the law often takes place at a much later stage.

Up to date, digitalisation is not explicitly mentioned in the Latvian Constitution, however, the most fundamental reflection of digitalisation in the law is seen in the most important law of the Latvian administrative sector – State Administration Structure Law, particularly Article 99 (previously referred as the backbone of Latvian administrative sector). Article 99 'Electronisation of State Administration Services' states that 'State administration shall arrange the provision of services electronically, where possible and feasible.' Additionally, part 2 of the mentioned article states that 'the procedures for the performance of electronisation of State administration services and ensuring of e-service accessibility shall be determined by the Cabinet of Ministers.' Thus, this article establishes a principle of general administrative law that authorizes and encourages state administrative institutions to act electronically where possible and feasible.

This provision was adopted in early 2016 and reflected the first attempt to mention digitalisation in the State Administration Structure Law. The *travaux préparatoires* of this article, however, stressed that the electronisation of state administration services does not prejudice the rights of the public to contact the administration in any other way unless otherwise stipulated by the law. Thus, the legislator was precautious with the attempt to fully digitalise the state administration services in order not to encounter strongly expressed objections from different groups of society and to ensure proportionality.

As for Administrative Procedure Law that establishes general framework rules for deciding any individual administrative case, there are no precise rules for deciding administrative cases electronically at an institutional level, however, there are explicit rules for deciding administrative cases electronically at a court level. That is, Article 112.2 'Basic rules for electronic case' envisages that administrative courts shall process administrative cases electronically (e-case) within the Court Information System whereby the court prepares, uploads and stores files of the case (Part 1). Decisions of a court or a judge shall be signed with a secure electronic signature (Part 3). If the document initially was prepared in written form, it shall be converted into electronic form (Part 4).

Even though there are no equal framework rules for deciding administrative cases electronically at an institutional level (unlike the court level), administrative institutions nevertheless are not restricted procedurally to process their cases electronically if possible and feasible. For comparative purposes, it is possible to reflect on the Estonian Administrative Procedure Act,[583] whereby Article 55 (3) explicitly states that an administrative act in writing may be issued in electronic form and the requirements set for written administrative acts apply to electronic administrative acts, taking into account the specifications arising from the electronic form of documents. However, the homologous Article 67 (1) of the Latvian Administrative Procedure Law simply states that an administrative act shall be issued in writing, thus, not excluding the electronic form (this is considered to be technology-neutral language). In practice, it is very common that electronic administrative acts are adopted and sent to the individuals if the last one has agreed to communicate electronically with the respective state institution. Latvian Law

583. Estonian Administrative Procedure Act. Available at: https://www.riigiteataja.ee/en/eli/527032019002/consolide, last accessed 27.08.2023.

on Notification sets clear procedures regarding the delivery of such electronic documents and administrative acts.[584]

At the current stage of digitalisation and development of Latvian administrative law, it is not possible neither to trace all the domains and aspects of governance being digitalised nor to describe it fully. This relates to the fact that digitalisation as well as legal development is fragmented and constantly under construction and change. Therefore, for the purpose of this article, authors will reflect only on the following aspects of digitalisation of administrative law: national portal of state administration e-services; communication electronically with the national authorities; virtual assistants (chatbots) in state administration; composite and interlinked state information systems (databases). The extent and way in which the current legal framework supports digitalisation in Latvia will be analysed further in the next section of this article.

1.2.2 National portal of state administration services

Article 100 of the State Administration Structure Law establishes a centralised portal of state administration services and a catalogue of services. The portal is a website that ensures accessibility to state administration services and information related thereto in one place for citizens and state administration, access to e-services and electronic communication between private individuals and state administration. The website address of the portal of State Administration Services is www.latvija.lv.[585]

This website provides popular online administrative services such as grant of sickness allowance (allowance paid to the worker or self-employed for the period during which the person cannot work), declaration of residence (mandatory obligation for Latvian residents that permits them to receive information from national and local authorities as well as to administer taxes), paying immovable property tax, requesting national authorities to issue different certificates or statements, registration in the register of enterprises registers, sign-up on voter initiatives, requesting information about the estimated amount of an old-age pension, application for maintenance allowance, unemployment allowance, childbirth allowance, maternity allowance, paternity allowance, etc. Statistically in Latvia, 83% of total Internet users use national administration e-services (that is well above the European Union average of 67%).[586]

Public administration e-services are comprehensively regulated by the Regulation of the Cabinet of Ministers No. 402[587] which prescribes the procedures by which public administration services are digitized and made available for the public.[588] It shall be stressed *that* the mentioned regulation includes explicit provision for service owners to promote the usage of their e-services in public. Namely, Article 18 of the regulation obliges service owners to develop such terms of service use. This, first, promotes the use of the e-service and, secondly, fulfils at least one of the following objectives:

1. a shorter time period for the electronic service than in person at the premises of the national authority;
2. a lower cost for the electronic service than in person at the premises of the national authority;

584. Law on Notification, Article 9. Available at: https://likumi.lv/ta/en/en/id/212499-law-on-notification, last accessed 27.08.2023.
585. Law on State Administration Structure, Article 100 (1) and (2).
586. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
587. Regulations Regarding the Public Administration E-services, Regulation of the Cabinet of Ministers No 402, 4 July 2017. Available at: https://likumi.lv/ta/en/en/id/292261-regulations-regarding-the-public-administration-e-services, last accessed 27.08.2023.
588. Regulations Regarding the Public Administration E-services, Regulation of the Cabinet of Ministers No 402, 4 July 2017. Article 1. Available at: https://likumi.lv/ta/en/en/id/292261-regulations-regarding-the-public-administration-e-services, last accessed 27.08.2023.

3. availability of the service only in electronic form, keeping in-person consultations at the premises of the authority only for the purpose of consulting the use of the e-service;
4. an identification mechanism (for the use of e-service) that is as accessible and convenient as possible.[589]

Thus, the Regulation of the Cabinet of Ministers No 402 has introduced the administrative principle of promoted use of administration e-services that obliges each service provider to implement digital services in the best interest of society.

The degree of complexity of and automatisation within different e-services varies. Some of the e-services have progressed up to the level that they can even perform registration and determination functions of the state administration. For example, the declaration of residence (registration) at the premises of your local municipality has been replaced with filling out an electronic form and automatic registration in the state information system. However, at the current stage of national administrative court case law, it has not yet been established whether acts of different computer systems and automated decision-making can constitute an administrative act or actual action (or failure to act) of an institution within the meaning of Article 1 (3) and 89 of the Administrative Procedure Law subjected to review by Latvian administrative courts. At the moment, there are new rules proposed in Latvia that would permit the State Tax Administration to adopt fully automated decisions within its Electronic Declaration System, thus punishing taxpayers for not submitting tax declarations or submitting them too late in an automated way.[590] However, these types of cases in the Latvian legal system are classified as administrative offence cases (similar to car speeding cases) and as such are not considered administrative acts or actual actions.

Increasing the number of such administration e-services provides the opportunity for individual applications to be handled by computer systems and thus relieves state administration officials and employees from purely technical work: there is no more need for technical delivery, acceptance and manual processing of individual paper submissions. Many of such e-services improve not only the customer experience of state administrative services but also allow the state human resources to be targeted to more intellectual work and supervision of the mentioned computer systems.

1.2.3 Electronic communication with national authorities (digital post)

From 2023, companies and foundations registered in Latvia are obliged to use the official electronic address (mandatory email registered for communication, particularly with state institutions). This is imposed by the Official Electronic Address Law that has the purpose of ensuring safe, efficient and high-quality electronic communication and circulation of electronic documents between state institutions, on the one hand, and private individuals, on the other hand.[591] At the moment, official electronic addresses are mandatory for state institutions, entities registered in state registers (mostly companies and foundations), reserve soldiers as well as active soldiers and related militants.[592] However, for natural persons, the usage of official electronic addresses at the moment is optional (opt-in system).[593] This digital post system is intended to be extended to larger groups of people in future.

589. Regulations Regarding the Public Administration E-services, Regulation of the Cabinet of Ministers No 402, 4 July 2017. Article 18. Available at: https://likumi.lv/ta/en/en/id/292261-regulations-regarding-the-public-administration-e-services, last accessed 27.08.2023.
590. Amendments in the Law on Administrative Liability. Amendment proposal No. 21-TA-183. Available at: https://tapportals.mk.gov.lv/legal_acts/994eaae5-5c22-459f-9d08-85c95b71e925 (in Latvian), last accessed 22.08.2023.
591. Law on the Official Electronic Address, Article 2. Available at: https://likumi.lv/ta/en/en/id/283229-law-on-the-official-electronic-address, last accessed 23.08.2023.
592. Law on the Official Electronic Address, Article 5(1). Available at: https://likumi.lv/ta/en/en/id/283229-law-on-the-official-electronic-address, last accessed 23.08.2023.
593. Law on the Official Electronic Address, Article 2. Available at: https://likumi.lv/ta/en/en/id/283229-law-on-the-official-electronic-address, last accessed 23.08.2023, Article 5(2).

Once the official electronic address (the digital post) is registered, national authorities are obliged to contact and deliver documents to the addressee via the official electronic address only.[594] However, historically electronic delivery of documents was not mandatory and thus had the potential to negatively affect businesses dealing with national authorities.

One such negative example is found in national administrative court case law. The applicant – the company producing electric energy – lost the licence to sell energy as a result of, as claimed by the applicant, the failure of the national authority to deliver correspondence to the applicant properly. The applicant claimed that previously the national authority sent all the documents electronically, however, at one point, the authority suddenly changed its practice and sent paper documents via the post (not electronically). As a result, the applicant seemingly failed to receive important documents but was legally presumed to have received the delivery. The applicant contested the national decision to administrative courts, claiming the failure to deliver the correspondence and the breach of the legitimate expectation that all documents would be sent electronically. However, the result in this particular case was negative for the applicant since the Supreme Court found that

'the national authorities are given discretion by the law to choose the most appropriate form for correspondence unless otherwise stipulated by the law. Thus, authorities are entitled to contact any legal entity both via the post or electronic email (Article 3 (1) 2) and 3) and (2) and Article 4 (2) of the Law on Notification). The legislation indeed permitted authorities to choose the best form of communication in each case individually. Thus, the district court in this particular case concluded correctly that even though the individual preferred one particular form for correspondence with the authority (electronic one), it did not restrict the national authority to choose any other form for delivery of documents if it found it to be more appropriate.' [595]

Such court cases are unlikely to repeat in future since after the introduction of the official electronic address (digital post), the Official Electronic Address Law restricts the discretion of state authorities to choose any other form of delivery instead of electronic form,[596] and thus the principle of priority of electronic delivery excludes the breach of legitimate expectation for private individuals.

1.2.4 Virtual assistants in state administration (chatbots)

One of the most interesting introductions in Latvian state administration is virtual assistants (consulting chatbots). At the moment, the most famous and commonly used virtual assistants are Tom (working on the website of the State Tax Administration), Eric (working on the national portal of state administration services www.latvija.lv), the hard-working Zintis (combining employment positions in more than 50 state administration websites), Mona (working in the website of the Central Bank of Latvia), Una (working on the website of the Latvian Register of Enterprises), Nora (working on the website of the State Environmental Service) and Justs (working on several websites managed by the National Court Administration).

At the moment, virtual assistants are mentioned in the Regulation of the Cabinet of Ministers No 445.[597] However, they are not extensively regulated by the law. The regulation states only that virtual assistants are maintained by the Cultural Information Systems Center (Article 51) and that virtual assistants receive the information necessary for their operations via the open data portal (Article 54).

---

594. Law on the Official Electronic Address, Article 2. Available at: https://likumi.lv/ta/en/en/id/283229-law-on-the-official-electronic-address, last accessed 23.08.2023, Article 12.
595. Decision of the Supreme Court of the Republic of Latvia in the case No. SKA-439/2022 (A420176720).
596. Law on the Official Electronic Address, Article 12. Available at: https://likumi.lv/ta/en/en/id/283229-law-on-the-official-electronic-address, last accessed 23.08.2023.
597. Procedures for Publishing Information on the Internet by Institutions, Regulations of the Cabinet of Ministers No. 445, 18 July 2020. Available at: https://likumi.lv/ta/en/en/id/316109-procedures-for-publishing-information-on-the-internet-by-institutions, last accessed 27.08.23.

The primary role of these virtual assistants is to consult citizens in the most frequently addressed questions to state administration employees.[598] Unlike search engines, virtual assistants are trained to recognise colloquial language and not only specific phrases that are typical for general search engines.[599]

The government benefits from such virtual assistants as they improve good governance in several ways: they reduce human consultancy work; they are capable of working 24 hours a day; they are trained to work in English as well as Latvian and thus have the potential to improve access to Latvian state administration to foreigners who visit Latvia for work and tourism purposes; and in the future, they will be trained for voice interactions to assist people who are blind, visually impaired or not are capable of writing.[600]

Usually, one virtual assistant is managed by 3 trainers, but the most advanced Latvian virtual assistant, Zintis, is managed by more than 120 trainers.[601] Zintis, unlike other virtual assistants, is capable of appearing on multiple websites and thus being able to consult in matters within the competence of different state authorities.[602] At the moment, Latvia is claimed to be the leading member state of the European Union in using virtual assistants in state administration[603] and is constantly seeking new and innovative solutions for improving accessibility of state administration.[604] It is worth mentioning that state authorities perceive their virtual assistants as ordinary employees and use them for marketing and guidance purposes.[605] For example, virtual assistant Tom is found everywhere on the State Tax Administration's premises (on billboards and self-service computer systems), but Una working in the Latvian Register of Enterprises always joins her human colleagues for different marketing events outside the premises of Latvian Register of Enterprises, appearing in presentations and billboards.[606]

1.2.5 Composite and interlinked information management databases

The impact of digitalisation on administrative law is also closely related to composite and interlinked information management systems between various authorities, especially information management databases. Such information systems exist not only at the European Union level, including the Internal Market Information System, the Schengen Information System, the Visa

598. 'Virtuālie asistenti valsts pārvaldē – Eiropas pirmrindnieki ar raksturu' ('Virtual assistants in public administration - European pioneers with character'). 13 October 2022. Available: https://mana.latvija.lv/virtualie-asistenti-valsts-parvalde-eiropas-pirmrindnieki-ar-raksturu/, last accessed 16.08.23.
599. 'Virtuālie asistenti valsts pārvaldē – Eiropas pirmrindnieki ar raksturu' ('Virtual assistants in public administration - European pioneers with character'). 13 October 2022. Available: https://mana.latvija.lv/virtualie-asistenti-valsts-parvalde-eiropas-pirmrindnieki-ar-raksturu/, last accessed 16.08.23.
600. 'Virtuālie asistenti valsts pārvaldē – Eiropas pirmrindnieki ar raksturu' ('Virtual assistants in public administration - European pioneers with character'). 13 October 2022. Available: https://mana.latvija.lv/virtualie-asistenti-valsts-parvalde-eiropas-pirmrindnieki-ar-raksturu/, last accessed 16.08.23.
601. 'Virtuālie asistenti valsts pārvaldē – Eiropas pirmrindnieki ar raksturu' ('Virtual assistants in public administration - European pioneers with character'). 13 October 2022. Available: https://mana.latvija.lv/virtualie-asistenti-valsts-parvalde-eiropas-pirmrindnieki-ar-raksturu/, last accessed 16.08.23.
602. 'Virtuālie asistenti valsts pārvaldē – Eiropas pirmrindnieki ar raksturu' ('Virtual assistants in public administration - European pioneers with character'). 13 October 2022. Available: https://mana.latvija.lv/virtualie-asistenti-valsts-parvalde-eiropas-pirmrindnieki-ar-raksturu/, last accessed 16.08.23.
603. 'Virtuālie asistenti valsts pārvaldē – Eiropas pirmrindnieki ar raksturu' ('Virtual assistants in public administration - European pioneers with character'). 13 October 2022. Available: https://mana.latvija.lv/virtualie-asistenti-valsts-parvalde-eiropas-pirmrindnieki-ar-raksturu/, last accessed 16.08.23.
604. 'Virtuālie asistenti valsts pārvaldē – Eiropas pirmrindnieki ar raksturu' ('Virtual assistants in public administration - European pioneers with character'). 13 October 2022. Available: https://mana.latvija.lv/virtualie-asistenti-valsts-parvalde-eiropas-pirmrindnieki-ar-raksturu/, last accessed 16.08.23.
605. 'Valsts pārvaldē virtuālo asistentu loma pieaug: tos ik dienas izmanto ap 2000 iedzīvotāju' ('The role of virtual assistants in the state administration is growing: they are used by around 2,000 citizens every day'). 21 December 2020. Available: https://lvportals.lv/dienaskartiba/323165-valsts-parvalde-virtualo-asistentu-loma-pieaug-tos-ik-dienas-izmanto-ap-2000-iedzivotaju-2020, last accessed 16.08.23.
606. 'Valsts pārvaldē virtuālo asistentu loma pieaug: tos ik dienas izmanto ap 2000 iedzīvotāju' ('The role of virtual assistants in the state administration is growing: they are used by around 2,000 citizens every day'). 21 December 2020. Available: https://lvportals.lv/dienaskartiba/323165-valsts-parvalde-virtualo-asistentu-loma-pieaug-tos-ik-dienas-izmanto-ap-2000-iedzivotaju-2020, last accessed 16.08.23.

Information System and the European Asylum Dactyloscopy Database, but also at the national level.

However, electronic systems raise several legal questions in relation to administrative decision-making processes, such as who is liable for damage caused by malfunctioning of those state-administered databases and false information entered into databases; is there an obligation to scrutinise the information obtained from these databases and what are the safeguards, including personal data protection, etc. These questions are partially addressed in the ReNEUAL Model Rules on European Union Administrative Procedure contained in Book VI draft rules on inter-administrative information management.[607]

In Latvia, a special Act on State Information Systems[608] has been adopted. This act:

1. determines unified procedures by which information systems are established, registered, maintained, used, reorganised or liquidated;
2. determines the functions of the controller of the information system and the rights and duties of the information system data subject;
3. governs the security management of information systems;
4. lays down the requirements to be conformed to for the protection of the information systems' integrator and the information systems being part of an integrated information system;
5. regulates the procedures by which the circulation of information is ensured with the assistance of an information systems integrator.[609]

The total number of national information systems varies, however, according to the national register there are more than 100 different state information systems in Latvia. The most commonly known is the Register of Natural Persons which includes information regarding different civil statuses; residence permits issued to foreigners, asylum seeker's status etc.[610] The law obliges several entities such as the Migration Office, local municipalities, courts, sworn notaries, the Enterprise Register and the State Revenue Service to provide the information to the register. Providers of information are responsible for the timely and correct provision of information to the Migration Office.[611]

Court information system includes information on different types of court cases and files, statistics, case law etc. that are available not only to judges and court staff, but state institutions and municipalities as well if it is necessary to perform their duties.[612]

The Criminal Convictions and Offenses Register (nationally called the "Punishment Register") was created to establish uniform record-keeping regarding persons who have committed criminal offences and administrative violations in order to facilitate the prevention and disclosure of such offences and violations, as well as regarding control of execution of the punishment imposed on a person.[613] There is also the Tax Information System, the Credit Register, the State Unified Computerised Land Register and many other electronic information databases in Latvia.

---

607. ReNEUAL model rules on EU administrative procedure / Hofmann, Herwig CH; Schneider, Jens-Peter; Ziller, Jacques; et al., eds. Research Network on EU Administrative Law (ReNEUAL), 2014.
608. Law on State Information Systems. Available at: https://likumi.lv/ta/en/en/id/62324-law-on-state-information-systems, last accessed 27.08.23.
609. Law on the Register of Natural Persons, Article 4. Available at: https://likumi.lv/ta/en/en/id/296185-law-on-the-register-of-natural-persons, last accessed 16.08.23.
610. Law on the Register of Natural Persons, Article 2 (2). Available at: https://likumi.lv/ta/en/en/id/296185-law-on-the-register-of-natural-persons, last accessed 16.08.23.
611. Law on the Register of Natural Persons, Article 15. Available at: https://likumi.lv/ta/en/en/id/296185-law-on-the-register-of-natural-persons, last accessed 16.08.23.
612. Rules of the court information system, Regulation of the Cabinet of Ministers No. 618 of 20 September 2016, Article 18. Available at: https://likumi.lv/ta/id/284905-tiesu-informativas-sistemas-noteikumi (in Latvian), last accessed 16.08.23.
613. Punishment Register Law, Article 1. Available at: https://likumi.lv/ta/en/en/id/261384-punishment-register-law, last accessed 16.08.23.

National administrative courts have pronounced several judgments on such information exchange between different state authorities. For example, in one case the administrative court has, inter alia, mentioned that the increasing access to information technologies and the quality, efficiency and speed of data exchange has allowed ever faster and better exchange of information between state authorities (in the particular case, between the Enterprise Register and the State Tax Authority), thus enabling them to assess better the information available and to take decisions which are in the best interest of the state.[614] Such exchange of information between state authorities is to be considered neither an administrative act nor an action within the meaning of Article 1 (3) and 89 of the Administrative Procedure Law. It is a simple operation between state institutions that *per se* cannot be contested by administrative courts.[615]

When information is shared on an information system and subsequently used by other administrative authorities the question of the correct information and the liability for mistakes gains particular significance, especially in the case if the information is used for concrete decisions which potentially interfere with the rights of individuals. The ReNEUAL Model Rules on European Union Administrative Procedure contained in Book VI draft rules on inter-administrative information management seemingly proposes specific rules for liability and the right to compensation in relation to composite information management activities. However, at the moment, this is not the case in the EU member states' national administrative law rules since there seem to be hardly any specific liability provisions in the member states' legal systems for advanced information exchange mechanisms.[616]

In Latvia, the Law on State Information Systems generally envisages that the controller of the state information system is 'responsible' for data collection, registration, input, processing, storage, utilisation, transmission, publication of data, compliance with data submitted, updating, correcting, as well as the quality of data in the State information system.[617] The controller of the state information system has to keep a reference to the data source, if data is not obtained directly from the data subject.[618] However, if the data is obtained directly from the data subject, according to Article 9(2) of the Law on State Information Systems the data subject must provide complete and true information in accordance with the procedures laid down in laws.[619] However, it must be stressed that these are general norms and it is not possible to exclude that specific laws can provide for a more detailed regulatory framework for liability issues linked to different electronic information systems.

Information systems and digital databases that store personal data have already posed several questions regarding the protection of privacy at the Constitutional Court of Latvia, which is a special court examining cases submitted by individuals or organs of the state regarding the conformity of laws and other legal acts with the Constitution, especially fundamental rights – a more detailed examination will follow in the next section.

614. Judgment of the Administrative District Court of 17 July 2019, Case No. A420227218, para. 10.2 (Judgment upheld by the Court of Appeal).
615. Judgment of the Supreme Court of 30 November 2016, case No. SKA-1572/2016, Judgment of the Supreme Court 17 August 2016, case No. A420180016, Judgment of the Supreme Court of 29 July 2016, case No. 680024916.
616. ReNEUAL II – Administrative Law in the European Union Administrative Information Management in the Digital Age / Vasco Barrón, Alban; Günther, Carsten. General report of the ACA-Europe Colloquium. Leipzig: Federal Administrative Court, 2020, p. 13. Available at: https://www.aca-europe.eu/images/media_kit/colloquia/2020/2020_Leipzig_GeneralReport.pdf
617. Law on State Information Systems, Article 8.
618. Law on State Information Systems, Article 8.
619. Law on State Information Systems, Article 9(2).

1.3 Plans for the future digitalisation

In 2021, in order to improve future digitalisation, the Cabinet of Ministers adopted Digital Transformation Guidelines for the term of 2021–2027 (further referred to as the "Digital Transformation Plan" or the "Guidelines").[620] The overarching objective of the Guidelines is to create a society, economy and state administration that purposefully uses existing digital technologies in order to improve the quality of life for everyone and the society at large as well as to boost the competitiveness of the state and economy.[621]

The Guidelines comprehensively focus on developing digital society at large and state administration, containing such general development areas as 'Digital transformation of the economy (including state administration)', 'Digital skills and education', 'Digital security and reliability', 'Accessibility of telecommunication services', 'Promoting information and communication technology innovations and commercialisation, industry and science'.[622] The document also relies on international papers, such as OECD Public Governance Policy Papers No.02 'The OECD Digital Government Policy Framework: Six dimensions of a Digital Government'. Structurally, the order provides vision, necessary action and measures as well as expected results for different digitisation projects.

For the purpose of this article, the authors will review only the section that concerns the subject of this article – the digitalisation of the state administration.

1.3.1 Further automatisation of the existing processes

The abovementioned current Digital Transformation Plan envisages further automatisation of the existing processes. The plan explicitly provides examples: usage of virtual assistants (consultancy chatbots) instead of human consultants; real-time automatic detection of speed drivers as well as automated decision-making etc.[623]

Also, automatisation should lead to a possibility of performing better causation analysis of different correlations in internal and external business management processes, such as public procurements: automatic price and cost comparisons, frequency of public procurements, results of comparable procurements, participation of different companies in public procurements, analysis of tender conditions that can lead to possible corruption risks in public procurement and consequently should be subject of attention for competent national supervisory authorities.[624]

The Digital Transformation Plan suggests that in order to purposefully optimise all the digitalisation processes, one must distinguish services that include the internal preparation phase within the institution (that is generally unique and specific for different services and institutions) from the phase when the service is requested on behalf of the individual and finally delivered. The latest phase is better suitable for unification and digitalisation and thus should be focused on more.[625]

620. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
621. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 1. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
622. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
623. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
624. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
625. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.9.2. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.

1.3.2 Further development of state e-service platforms

The current Digital Transformation Plan requires a further quantitative increase of e-services as well as substantively personalised and proactive services that even though possible currently, are not available or practised at a larger scale yet (because of the high consumption of human analytical resources and skills). This includes, for example, personalised and proactive medicine that in an automatised manner analyses patients' medical records, genetics, on-spot inspections by doctors, illnesses of their relatives as well as personal data from smart devices etc. in order to suggest the best possible diagnostics and health treatment.[626]

Similarly, this includes personalised and proactive social services for individuals from different socio-economic groups and of different real-life situations, for example, parents with newly born children should automatically and proactively receive all governmental services related to the child in a transparent and logical sequence (registration of a child, receiving allowances, declaration of residence, a permanent appointment for a primary care practitioner, etc).[627]

The Digital Transformation Plan envisages the principle that e-services must be subject to continuous progression and improvement. Such continuous transformation must be essential routine practice for both national and municipal authorities.[628] Also, the plan suggests that in order to constantly improve e-services of the state administration a new state institution shall be established: the Center for Public Service Management and Digitization Methodology.[629]

1.3.3 Single personal e-account and electronic correspondence (digital posts)

The Latvian Digital Transformation Plan envisages creating a single personal e-account that unifies all communication channels and services provided to this individual from different organisations. Such an account should provide all the official announcements, notifications, e-invoices etc. The plan references as an example the partly comparable GOV.UK Notify.[630]

The existing e-address (digital posts) that is mandatory for companies at the moment, is to be extended to private correspondence, that is, not only between the government and companies but also the correspondence between different companies (business-to-business) and consumer relations (business-to-consumer). This could be useful for the exchange of structured data such as financial documents (invoices, receipts, delivery notes).[631]

1.3.4 The platform for public participation and transparent governance and Open data platform

The Digital Transformation Plan envisages that digital technologies create a new digital space for the government and it must be organised in the way that suits the society best. However, society should have a sense of being responsible for the governance of the state and must actively engage in that process.[632]

---

626. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.9.2. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
627. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. 4.4.9.2. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
628. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.9.1. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
629. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.9.7. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
630. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.1. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
631. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.1., point 5.2. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
632. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.9. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.

One example is that the Digital Transformation Plan explicitly mentions that the state administration must employ all the new digital tools and applications that permit hearing society in a very fast and simple manner, thus implementing the principle of sound administration effectively.[633] The argument therefore is that public participation and transparent governance platforms are seen as an opportunity to provide open and public information on current legislative and planning processes to the public as well as a chance to increase and target public participation and obtain analysis for legislative processes.[634] In addition, an Open data platform is mentioned as a public and private data sharing site to assure business processes, for example, information about schedules of public transport, statistics etc.[635]

1.3.5 General challenges and concerns

Besides the above-mentioned digitalisation perspectives, the Digital Transformation Plan also mentions digital transformation of geospatial, environmental governance and planning,[636] circulation of financial documents,[637] digitalisation of the justice system, especially in relation to investigation of crimes and adjudication of various cases,[638] the use of digital advantages for civil protection in cases of emergence,[639] digitization of cultural heritage,[640] remote work by default for state employees to improve their productivity[641] and design approach on tactical level,[642] full digitalisation of all level education, including university education, as well as administration of schools,[643] implementing smart city technologies into urban infrastructure, [644] etc. However, considering concerns over further digitalisation, the plan also refers to cyber security risks and data protection aspects.

The plan envisages that the already existing Act on State Information Systems shall be transformed into the special National Digital Technology Management Act and shall contain a new legal requirement that before creating new information and communication technology services, the responsible authority shall be obliged to identify in advance possible cyber security risks.[645]

633. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.9.6. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
634. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. section 4.4.1., point 5.9; section 4.4.9.6. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
635. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.1., point 5.12. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
636. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.4. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
637. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.3. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
638. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.5. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
639. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.5. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
640. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.8. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
641. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.9.4. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
642. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.9.5. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
643. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.13. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
644. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.5.2. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
645. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 5 and 4.2.1., point 2. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.

Further digitalisation also challenges already existing technical and organisational measures of personal data protection. Even though the General Data Protection Regulation is technology neutral, the digitisation plan envisages the need for capacity-building of the National Data Protection Inspectorate (in relation to its technical capacities) as well as educating the public regarding the protection of their own personal data.[646]

2. Digitalisation and Human Rights: Potential Challenges

In the following section, the authors provide an overview of the relevant judgments of the Constitutional Court of Latvia, the Opinions of the Ombudsman of Latvia and the judgment of the European Court of Human Rights judgment in the case *Nagla v. Latvia.* Moving from the national to the international legal instruments, the authors examine the effect that the digitalisation of the public sector may have on the enjoyment of human rights.

2.1 The landscape of relevant human rights obligations

After the fall of the Soviet Union, the Latvian legal system has undergone fundamental changes. One of the characteristics is the inclusion of the human rights standards into the domestic legal order in the 1990's.

Satversme[647] – the Constitution of Latvia – was adopted in 1922 and supplemented with Section VIII titled Fundamental Human Rights in 1998. Section VIII enshrines a catalogue of 28 articles protecting both civil and political rights (such as the right to life, equality before the law, and the right to private life) as well as economic and social rights (such as the right to freely choose their employment, the right to a basic level of medical assistance and the right to education).

Out of all provisions of the Latvian Constitution, one is, perhaps, the most relevant when it comes to the digitalisation of public administration: Article 96 reads: 'Everyone has the right to inviolability of his or her private life, home and correspondence'.[648] This right corresponds to Article 8 of the European Convention on Human Rights,[649] which Latvia ratified in 1996. Article 8 reads:

1. *'Everyone has the right to respect for his private and family life, his home and his correspondence.'*
2. *'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'*

646. Digital Transformation Guidelines 2021-2027, Order of the Cabinet of Ministers No. 490, 7 July 2021. para. 4.4.2.2. and 4.4.2.4. Available at: https://likumi.lv/ta/id/324715-par-digitalas-transformacijas-pamatnostadnem-20212027-gadam, last accessed 27.08.2023.
647. Constitution of the Republic of Latvia. Available at: https://likumi.lv/ta/en/en/id/57980-the-constitution-of-the-republic-of-latvia, last accessed 27.08.2023
648. Constitution of the Republic of Latvia. Article 96. Available at: https://likumi.lv/ta/en/en/id/57980-the-constitution-of-the-republic-of-latvia, last accessed 27.08.2023.
649. European Convention on Human Rights, Article 8. Available at: https://www.echr.coe.int/documents/d/echr/convention_eng, last accessed 27.08.2023

2.2 Judgments of the Constitutional Court of Latvia

2.2.1 Judgment of the Constitutional Court in the case 2012-15-01

The case concerned Article 43.6 of the Road Traffic Act.[650] Based on it, if at the time of the road traffic offence fixed by the technical devices the driver has not been identified, the administrative penalty for the violation was applied to the owner of the vehicle. If the owner failed to pay the administrative fine, the law prescribed a ban on conducting a state technical inspection (roadworthiness test) and registering the vehicle and its driver in the state register.

Even if the owner of the vehicle was not the one *driving* it at the time of the offence, they did not have an opportunity to claim compensation from the actual perpetrator. In the Ombudsman's view, such a procedure violated the presumption of innocence as well as Article 92 of *Satversme*:

'Everyone has the right to defend his or her rights and lawful interests in a fair court. Everyone shall be presumed innocent until his or her guilt has been established in accordance with law. (...)' [651]

The Court stated that the presumption of innocence is not absolute and in certain cases allows the legislature to foresee other legal presumptions.[652] The Court began by identifying whether a presumption found in Article 43.[653] of the Road Traffic Act (that the unidentifiable driver is the owner of the vehicle) was prescribed by law. The opinions of the parties differed: The Ministry of Justice considered the legal basis to be found in the Latvian Administrative Violations Code, and the Ministry of Interior in the Civil Law.

The Court established that the Latvian legislation did *not* foresee the liability of the owner of the vehicle for offences committed by another driver.[654] Here, the Court calibrated its focus: it is not the presumption of innocence *per se* that posed an issue, but the (alleged lack of) procedural guarantees available to the owner of the vehicle – the right to be heard and the right to access the court.[655]

Article 43.[656] of the Road Traffic Act did not grant the owner of the vehicle an opportunity to inform the State that it was another person, driving the vehicle at the time of the offence. Article 43.[657] allowed *the driver* to appeal the decision, not the owner. This amounted to interference with the right to be heard and the right to access the court.

This interference was prescribed by law[658] and pursed the legitimate aim of protection of the rights of others.[659] For proportionality check, the Court divided the matter into separate sub-issues: (1) limitation of the right to be heard *before* the imposition of the fine and (2) limitation of

650. Road Traffic Law (as of 2012), Article 43.6. Available at: https://likumi.lv/ta/en/en/id/45467-road-traffic-law, last accessed 01.08.2023
651. The Constitution of the Republic of Latvia, 1922, Article 92.
652. Judgment of the Constitutional Court of Latvia in the case 2012-15-01, 28 March 2013, para.15.1. Available at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2012-15-01_Spriedums.pdf (in Latvian), last accessed 27.08.2023.
653. Latvian Administrative Procedure Law. Available at: https://likumi.lv/ta/en/en/id/55567-administrative-procedure-law, last accessed 27.08.2023.
654. Judgment of the Constitutional Court of Latvia in the case 2012-15-01, 28 March 2013, para. 15.3. Available at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2012-15-01_Spriedums.pdf (in Latvian), last accessed 27.08.2023.
655. Judgment of the Constitutional Court of Latvia in the case 2012-15-01, 28 March 2013, para. 15.4. Available at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2012-15-01_Spriedums.pdf (in Latvian), last accessed 27.08.2023.
656. Latvian Administrative Procedure Law. Available at: https://likumi.lv/ta/en/en/id/55567-administrative-procedure-law, last accessed 27.08.2023.
657. Latvian Administrative Procedure Law. Available at: https://likumi.lv/ta/en/en/id/55567-administrative-procedure-law, last accessed 27.08.2023.
658. Judgment of the Constitutional Court of Latvia in the case 2012-15-01, 28 March 2013, para. 18.1. Available at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2012-15-01_Spriedums.pdf (in Latvian), last accessed 27.08.2023.
659. Judgment of the Constitutional Court of Latvia in the case 2012-15-01, 28 March 2013, para. 18.2. Available at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2012-15-01_Spriedums.pdf (in Latvian), last accessed 27.08.2023.

the right to be heard in cases where the offence was not committed by the owner but another driver.

As to the first one, the Court found such a measure proportionate: the procedure of fixing the offence with technical devices and consequent imposition of the fine is rather common, and the percentage of appeals is relatively low.[660] As to the second, the Court found that imposing an obligation to pay the fine for an offence committed by another person in fact deprives the owner of the vehicle of the right to fair trial and violates Article 92 of the Constitution.[661]

2.2.2 Judgment of the Constitutional Court in the case 2018-18-01

The case originated from the individual claim contesting the compliance of Article 14.1 (2) of the Road Traffic Act, which reads:

'Information about a vehicle owned by a legal person, except for the information specified in Paragraph one of this Section, about a person's right to drive vehicles, on the fines imposed on a person for offences in road traffic which have not paid within the time period specified in the law, and also any other information contained in the State Register of Vehicles and Drivers Thereof and the State Information System of Tractor-type Machinery and Drivers Thereof shall be treated as generally accessible information.'[662]

The Latvian Road Traffic Act prescribed that a driver committing an administrative offence received the so-called 'penalty points', which were recorded in the State Register of Vehicles and Drivers Thereof.[663] Upon reaching a specified number of points, a driver would have to pass mandatory training sessions (seminars) on matters of road traffic safety or even pass the driving examination again. Based on Article 14.[1], the number of points received by a driver was publicly accessible, which, as claimed by the Applicant, contradicted Article 96 of the Constitution.[664]

The Latvian Parliament as the author of the contested norm, while agreeing that the publication of the penalty points constituted an interference with the person's private life, contented that it pursued a legitimate aim – namely, the protection of the rights of others and the protection of public safety.[665] In its view, the information about the penalty points may be crucial for the passenger carriers and taxi service providers – to evaluate whether a specific driver is trustworthy.

Interestingly, during the proceedings, the Constitutional Court had requested a preliminary ruling from the EU Court, *inter alia*, asking

'can the provisions of [the General Data Protection Regulation], in particular the principle of 'integrity and confidentiality' referred to in Article 5(1)(f) thereof, be interpreted as meaning that they prohibit Member States from stipulating that information relating to penalty points recorded against drivers for motoring offences falls within the public domain and from allowing such data to be processed by being communicated?'[666] [emphasis added]

---

660. Judgment of the Constitutional Court of Latvia in the case 2012-15-01, 28 March 2013, para. 18.2. Available at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2012-15-01_Spriedums.pdf (in Latvian), last accessed 27.08.2023.
661. Judgment of the Constitutional Court of Latvia in the case 2012-15-01, 28 March 2013, para. 18.3.3.2. Available at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2016/02/2012-15-01_Spriedums.pdf (in Latvian), last accessed 27.08.2023.
662. Road Traffic Law, Article 14.[1]. Available at: https://likumi.lv/ta/en/en/id/45467-road-traffic-law, last accessed 27.08.2023.
663. Road Traffic Law, Article 43.[1]. Available at: https://likumi.lv/ta/en/en/id/45467-road-traffic-law, last accessed 27.08.2023.
664. Judgment of the Constitutional Court of Latvia in the case 2018-18-01, 13 November 2021, para.2. Available at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2018/08/2018-18-01_Spriedums.pdf (in Latvian), last accessed 27.08.2023.
665. Judgment of the Constitutional Court of Latvia in the case 2018-18-01, 13 November 2021, para.3. Available at: https://www.satv.tiesa.gov.lv/wp-content/uploads/2018/08/2018-18-01_Spriedums.pdf (in Latvian), last accessed 27.08.2023.
666. *Judgment of the Court (Grand Chamber) in the case C-439/19, 22 June 2021, para.53(2). Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=243244&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=348678, last accessed 27.08.2023.*

The Grand Chamber concluded that the GDPR must be interpreted in a way that precludes the Member States from making the data on penalty points available to the public unless the person requesting that information has established *'a specific interest in obtaining that data'*.[667]

The Constitutional Court then employed a classical balancing test: whether the interference in question is prescribed by law, pursues a legitimate aim and is proportionate. The first criterion was satisfied.[668] The Court further accepted that the measures were intended to keep both the person who committed road traffic violations as well as others from such actions.[669] This corresponded to the protection of the rights of others and the protection of public safety.

When performing the proportionality test, the Court initially accepted that the contested article was appropriate to the attainment of intended aims.[670] However, the balancing act requires measuring whether less restrictive measures exist that could be used for the same purpose(s). Here, the Court made a necessary reference to the EU Court's reply in the preliminary ruling: publishing of information about a particular person's penalty points is contrary to the GDPR.

The Court had also requested the opinion of the Ombudsman of Latvia whose position was the same: although the pursued aim was legitimate, there was no urgent public need to access information about other drivers' penalty points.[671]

While some persons may have had a legitimate interest in obtaining that information, in fact, everyone had access to it. Other, less restrictive means could have been imposed to achieve the same aim, such as granting information about the person's penalty points to those persons who have road safety-related or other justified interests.[672] Thus, the interference stemming from the contested norm did not satisfy the proportionality requirement and violated Article 96 of the Latvian Constitution.

2.2.2.1 Judgment of the Constitutional Court in the case 2022-09-01

The case concerned the Punishment Register Law adopted in 2013. Article 23(1) reads:

The following information shall be stored in the archives database of the Register:

'1) regarding a person whose criminal record has been set aside or extinguished, against whom the initiated criminal proceedings have been terminated, regarding an acquitted person [...] – for one year after the information has been received from the Register of Natural Persons regarding the death of the person, however, not longer than 100 years after the birth of the person;'[673] [emphasis added]

The applicant, the Administrative District Court, submitted that the said provision did not comply with Article 96 of the Constitution. In its view, since an acquitted person was considered innocent, then, storing information about them in the Punishment Register for the whole lifetime of that person is, first, disproportionate and, second, incompatible with the purpose for which the Register was created.[674]

667. Judgment of the Court (Grand Chamber) in the case C-439/19, 22 June 2021, para.122. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=243244&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=348678, last accessed 27.08.2023.
668. Judgment of the Constitutional Court of Latvia in the case 2018-18-01, para.17.
669. Judgment of the Constitutional Court of Latvia in the case 2018-18-01, para.18.
670. Judgment of the Constitutional Court of Latvia in the case 2018-18-01, para.20.
671. Opinion of the Ombudsman, reference No. 1-6/18, 19 December 2018, p.8. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/viedoklis_st_lieta_nr_2018_18_01_1545992368.pdf (in Latvian), last accessed 27.08.2023.
672. Opinion of the Ombudsman, reference No. 1-6/18, 19 December 2018, para.21.2. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/viedoklis_st_lieta_nr_2018_18_01_1545992368.pdf (in Latvian), last accessed 27.08.2023.
673. Punishment Register Law, Article 23(1).
674. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, 22 December 2022, para.2. Available at: https://www.satv.tiesa.gov.lv/web/viewer.html?file=https://www.satv.tiesa.gov.lv/wp-content/uploads/2022/03/2022-09-01_Spriedums.pdf#search= (in Latvian)

The Latvian Parliament submitted that the contested norm pursued a legitimate aim – archival needs, and there is no other means to attain the same purpose while not interfering with the person's fundamental rights.[675]

In this case, the Court used the same three-step test: whether the interference in question is prescribed by law, pursues a legitimate aim and passes the proportionality check. As to the first criterion, the Court admitted that Article 23(1) was prescribed by domestic law: it has been properly adopted and made available to the public, and the norm was formulated sufficiently clearly.

The question of whether the contested norm pursued a legitimate aim deserves a more detailed examination. The Court made a distinction between two databases and, consequently, two different aims pursued. Thus, the personal data stored in the *current* (active) database of the Register pursued the aims mentioned in Article 1 of the Punishment Register Law – *'to facilitate the prevention and disclosing of such offences and violations, as well as regarding control of execution of the punishment and restriction of the rights imposed on a person for the committed offences and violations.'*[676] These aims, the Courts continued, differ from the aims pursued with the storage of personal data in the *archive* database of the Register, yet the law does not expressly name them.[677]

The Court agreed that the creation and maintenance of archives *per se* is related to the sustainability of a democratic state and the protection of the rights of others.[678] Specifically, information about acquitted persons may also be needed to ensure further criminal procedural activities, to protect public safety[679] and to ensure the data subject's own rights, such as the possibility of receiving official confirmation of their acquittal in a criminal process.[680] To sum up, the Court identified three legitimate aims pursued by Article 23(1): the protection of democratic state apparatus, public safety and the rights of others.

The Court began with the protection of public safety. The data of both innocent persons and the persons found guilty are processed in the same register and for the same period of time, meaning that the data of two distinctly different categories of persons receive the same treatment.[681] It also stems from the opinions of the Ministry of Interior and the State Police that the data in the archives database of the Register is used 'to conduct an in-depth examination of a person' or 'to check a person's reputation'. Although both these aims are related to safety, they do not *directly* lead to protection from an objectively identified threat. Thus, the Court found that the measures adopted do not correspond to the protection of public safety.

Further, the Court considered the protection of democratic state apparatus and the protection of the rights of others. The Archives Law prescribed that, before archiving, the archival value of a record must be determined,[682] yet the transfer of the data from the current database to the archives database of the Register took place automatically, i.e., without evaluation of the archived data. Moreover, the data was retained only one year after the death of the person. This goes contrary to the *rationale* of the archiving – the storage of the data should not depend on whether the person is alive. Thus, the disputed norm does not correspond to the protection of the democratic state apparatus and the protection of the rights of others.[683]

675. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, 22 December 2022, para.3. Available at: https://www.satv.tiesa.gov.lv/web/viewer.html?file=https://www.satv.tiesa.gov.lv/wp-content/uploads/2022/03/2022-09-01_Spriedums.pdf#search= (in Latvian)
676. Punishment Register Law, Article 1.
677. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, para.14.1.
678. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, para.14.2.
679. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, para.14.3.
680. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, para.14.4.
681. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, para.15.2.
682. Archives Law, Article 8(1). Available at: https://likumi.lv/ta/en/en/id/205971-archives-law, last accessed 20.08.2023.
683. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, para.17.1.

The Court accepted that the storage of personal data for a certain period of time could be helpful in case of renewed criminal proceedings.[684] The third criterion of the balancing test is the proportionality check. In all cases, the data of an acquitted person is stored for the same period of time, regardless of whether the statute of limitations for the respective criminal offence has already passed, and whether the stored data can still be used.[685] Data is also stored in the information system of the Ministry of Interior, which leads to the doubling of the data in several registers. Considering all these factors, the Court concluded that the disputed Article 23(1) of the Punishment Register Law contradicts Article 96 of the Latvian Constitution.

2.3 Opinions of the Ombudsman of Latvia

In the context of digitalisation and human rights, it is also worth mentioning the opinions of the Ombudsman of Latvia, whose task is to ensure human rights protection via, *inter alia*, review of individual applications, providing opinions in court proceedings, providing recommendations to state institutions, and so on.[686]

2.3.1 Opinion of 29 March 2011 on the publishing of personal data on the municipal news page

The application was submitted by a person whose personal data have been published in the minutes of the meeting of the municipal council (*pašvaldības dome*). The text provided: 'It was decided to rent the municipal apartment to the mentioned person, specifying the address'.[687] The Ombudsman observed the tension between the two rights: on the one hand, the societal interest in being informed about the decisions made by the municipality, especially those concerning the use of municipal resources and, on the other hand, the individual's right to respect for their private life.[688] Publishing the person's full address, personal safety and property interests are exposed to a higher risk. Thus, the municipality council, while respecting the public right to information, should have not posted the person's full name or full address to minimise that risk.

2.3.2 Opinion of 12 April 2017 on the processing of personal data

The opinion originates from the individual claim concerning the website, an official electronic database of auctions officially announced by bailiffs and insolvency administrators. The website published information about two properties owned by the applicant, including information on how she obtained these properties, the amount of her credit obligations and the applicant's personal code.[689] The Ombudsman observed that the term 'personal data' does not only enshrine data such as name, surname, identification number, location data, etc. Referring to the EU Court, the Ombudsman noted that

684. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, para.18.
685. Judgment of the Constitutional Court of Latvia in the case 2022-09-01, para.18.
686. Ombudsman Law, Articles 11-12. Available at: https://likumi.lv/ta/en/en/id/133535-ombudsman-law, last accessed 20.08.2023.
687. Opinion of the Ombudsman, reference No. 6-2/204, 29 March 2011. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/atzinums_par_pasvaldibas_zinu_lapa_publiskotajiem_personas_datiem_29_03_2011_1507136290.pdf (in Latvian), last accessed 20.08.2023.
688. Opinion of the Ombudsman, reference No. 6-2/204, 29 March 2011. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/atzinums_par_pasvaldibas_zinu_lapa_publiskotajiem_personas_datiem_29_03_2011_1507136290.pdf (in Latvian), last accessed 20.08.2023.
689. Opinion of the Ombudsman, reference No. 6-6/10, 12 April 2017, p.1. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/atzinums_lieta_nr_2016_10_5f_1492494782.pdf (in Latvian), last accessed 20.08.2023.

'the information about the person's transaction history and the number of credit obligations, namely the economic condition/behaviour, together with their name and surname are recognised as personal data.'[690]

The Ombudsman then reviewed the Regulations of the Cabinet of Ministers No. 318 'Terms of the site of electronic auctions'[691] and concluded that the regulations do not prescribe to specify the owner's economic status and personal code in the advertisement for forced auction of real estate.[692] The inclusion of the debtor's personal code in real estate thus was not necessary and was contrary to Article 96 of the Constitution and Article 8 of the ECHR. The Ombudsman called upon the Data State Inspectorate and the Ministry of Justice to take all necessary measures to stop the practice of publishing the debtors' personal codes in real estate auction advertisements.[693]

2.3.3 Opinion of 15 November 2017 on certain aspects of the e-health system

In May 2016, the Association of Family Doctors of Latvia submitted an application to the Ombudsman concerning the Regulations of the Cabinet of Ministers No. 134 'Regulations Regarding the Unified Electronic Information System of the Health Sector'.[694] The Association asked the Ombudsman to evaluate the procedure of transfer of persons' health (medical) data to the State Labor Inspectorate, the National Health Service, the Health Inspectorate and the State Social Insurance Agency as well as the indication of the diagnoses in the sick-leave certificates.[695]

In the framework of this evaluation, the Ombudsman has turned to the Ministry of Health, asking to improve the legal regulation of the e-health system with regard to the processing of health data. As a result, the proposals of the working group of the Ministry of Health were incorporated into the regulatory acts.

Notably, the amendments prescribed to not indicate the *precise* diagnosis in the sick leave certificate. Where the law prescribed to indicate the reason, it was worded in more generalised terms, such as 'occupational disease', 'accident at work', 'road accident', etc.[696] Diagnoses such as 'quarantine', 'prosthetics or orthotics', and 'rehabilitation' have been excluded as they reveal sensitive details about the person's health, and diagnoses 'pregnancy' and 'labour' have been substituted with 'prenatal period' and 'postnatal period' for greater precision.[697]

Amendments were also made to the procedure of issuing medical prescriptions.[698] The diagnosis would only be indicated on the special electronic prescription forms used for medicinal products subject to stricter control (narcotic and psychotropic medicine, narcotic analgesic substances, etc.) The ordinary electronic prescription form used for the majority of medicines would not contain the patient's diagnosis, which the Ombudsman considered a major improvement in the patient's data protection.[699]

690. Opinion of the Ombudsman, reference No. 6-6/10, 12 April 2017, p.2. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/atzinums_lieta_nr_2016_10_5f_1492494782.pdf (in Latvian), last accessed 20.08.2023.
691. Terms of the site of electronic auctions, Regulations of the Cabinet of Ministers No. 318, 16 June 2015. Available at: https://likumi.lv/ta/id/274951-elektronisko-izsolu-vietnes-noteikumi (in Latvian), last accessed 20.08.2023.
692. Opinion of the Ombudsman, 12 April 2017, p.3.
693. Opinion of the Ombudsman, 12 April 2017, p.5.
694. Regulations Regarding the Unified Electronic Information System of the Health Sector, Regulations of the Cabinet of Ministers No.134, 11 March 2014. Available at: https://likumi.lv/ta/en/en/id/264943-regulations-regarding-the-unified-electronic-information-system-of-the-health-sector, last accessed 20.08.2023.
695. Opinion of the Ombudsman, reference No. 6-6/39, 15 November 2017. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/atzinums_lieta_nr_2016_24_5d_1511348919.pdf (in Latvian), last accessed 20.08.2023.
696. Amendments to the Regulations Regarding the Unified Electronic Information System of the Health Sector, Regulations of the Cabinet of Ministers No. 318, 22 August 2017. Available at: https://likumi.lv/ta/id/293135-grozijumi-ministru-kabineta-2014-gada-11-marta-noteikumos-nr-134-noteikumi-par-vienoto-veselibas-nozares-elektronisko-informaci. (in Latvian), last accessed 20.08.2023.
697. Opinion of the Ombudsman, 15 November 2017, p.5.
698. Regulations Regarding Manufacture and Storage of Prescription Forms, as well as Writing out and Storage of Prescriptions, Regulations of the Cabinet of Ministers No. 175, 8 March 2005. Available at: https://likumi.lv/ta/en/en/id/104228-regulations-regarding-manufacture-and-storage-of-prescription-forms-as-well-as-writing-out-and-storage-of-prescriptions, last accessed 20.08.2023.
699. Opinion of the Ombudsman, 15 November 2017, pp.5-6.

Lastly, the Ombudsman highlighted the need to supplement the e-health system's legal regulation with more precise provisions on the rights of the State Health Inspectorate to process patients' sensitive data.[700] With amendments of May 2018, the recommended provision has been added to the regulations.[701]

2.3.4 Opinion of 12 November 2020 on personal data processing by technical means in road traffic

The Ombudsman received a private complaint concerning the processing of personal data taking place during traffic speed control by photo radars. The applicant considered that the data about the driver and the vehicle could be retained in the databases also in cases where the person has not consented nor has committed a violation of road traffic rules.[702] This, according to the applicant, violated the right to respect for private life (enshrined in Article 96 of the Constitution) as well as the presumption of innocence (Article 92).

The Ombudsman evaluated four issues separately: (1) failure to observe driving speed,[703] (2) driving a vehicle lacking a State technical inspection, (3) driving a vehicle lacking mandatory insurance[704] and (4) failure to pay road usage fees.[705]

Regarding the first point, the Ombudsman cited the Constitutional Court, which established that the prevention of speed limit violations pursued the protection of the rights of others: the right to life, health and property rights. Speed control was the primary reason for setting up the radars. Thus, the data processing taking place for such purposes is lawful.[706]

Regarding the second point, the Ombudsman noted that driving a vehicle to which the state technical inspection has not been carried out puts public safety at risk. Statistically, approximately 4% of the vehicles were lacking inspection; thus, blanket data processing was proportionate. However, the fact that the public was not informed about such data processing was evaluated negatively.[707]

Regarding the third point, statistics showed that at least 97% of vehicles had mandatory insurance. The Ombudsman concluded that the indirect processing of the personal data of several drivers undertaken to ensure the right of others to compensation was clearly disproportionate.[708]

Finally, the road feeds applied on 17 defined roads and only to vehicles with a full weight exceeding 3001 kg. Moreover, the drivers were informed that technical means were checking whether the payment had been made. Based on the two elements combined, such a measure was found proportionate.[709]

---

700. Opinion of the Ombudsman, 15 November 2017, p.10
701. Regulations Regarding the Unified Electronic Information System of the Health Sector, Article 33.^{5}.
702. Opinion of the Ombudsman, reference No. 6-6/30, 12 November 2020. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/par_personas_datu_apstradi_1608625042.pdf (in Latvian), last accessed 21.08.2023.
703. Latvian Administrative Violations Code (no longer in force), Article 149.8. Available at: https://likumi.lv/ta/en/en/id/89648-latvian-administrative-violations-code, last accessed 21.08.2023.
704. Latvian Administrative Violations Code (no longer in force), Article 149.24. Available at: https://likumi.lv/ta/en/en/id/89648-latvian-administrative-violations-code, last accessed 21.08.2023.
705. Latvian Administrative Violations Code (no longer in force), Article 149.40. Available at: https://likumi.lv/ta/en/en/id/89648-latvian-administrative-violations-code, last accessed 21.08.2023.
706. Opinion of the Ombudsman, 12 November 2020, para. 4.3.
707. Opinion of the Ombudsman, 12 November 2020, para. 13.
708. Opinion of the Ombudsman, 12 November 2020, para. 13.1.
709. Opinion of the Ombudsman, 12 November 2020, para. 13.2.2.

2.3.5 Opinion of 4 February 2021 on the publicity of the entries of the Enterprise Register online

The issue originated from a private person, who has by mistake registered as a sole proprietor. This commercial entity has been liquidated, yet several websites (including the website of the Register of Enterprises of Latvia) still contained personal data such as the private address of that person, allegedly violating their right to private life.[710]

Referring to Article 4(1) of the General Data Protection Regulation,[711] which defines personal data, the Ombudsman concluded that the place of residence falls under the private life guarantees.[712] However, the situation when the legal address of the merchant is at the same time the place of residence of the private person is not regulated. The publicity of legal addresses is dictated by the principle of transparency and the right to access information: the public should be able to find current and historical information about the legal entity. Such information is available to an *unlimited* number of persons for an *unlimited* time; therefore, for those persons whose place of residence is the entity's legal address, it constitutes an interference with the right to private life.[713]

Such interference is found in several laws – the Commercial Law[714] and the Law on the Enterprise Register of the Republic of Latvia[715] – making the interference lawful. The Ombudsman further noted that it protects the interests of third persons (creditors, investors, etc.) and helps prevent money laundering and financing of terrorism. Thus, such measures pursue a broad legitimate aim – the protection of the rights of others.[716]

The Ombudsman further noted that the approach in question was appropriate to the pursued aim. The question to be resolved was whether the same aim could be achieved with other, less interfering means. Two alternatives are: not to publish the legal address of the entity or not to allow the Register of Enterprises to pass it to the re-users. The first option was not considered viable. Firstly, it would be contrary to the right to information. Secondly, in the absence of public records online, interested persons could only find out the legal address by physically coming to the Register of Enterprises, which would disrupt its work.[717]

The second option was also rejected. The Ombudsman found no legal basis to prohibit the Register of Enterprises from passing the information to the re-users.[718]

Finally, the Ombudsman found that the public good achieved outweighs the risks posed to an individual whose personal address has been published. Based on that, no violation of the right to private life was found.[719]

Interestingly, the Ombudsman went further, recalling the right to be forgotten under the GDPR. The natural person whose address has been published (as the legal address of the associated entity) does not in fact have a possibility to limit access to their personal data. As a result, such data is retained for an unlimited time. As such cases are exceptional, a more flexible approach may have been adopted.[720]

---

710. Opinion of the Ombudsman, Inspection case No. 2019-06-5F, 4 February 2021. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/par_personas_datu_aizsardzibu_attieciba_uz_uznemumu_registra_ierakstu_publicitati_timeklvietnes_9_1613459577.pdf (in Latvian), last accessed 22.08.2023.
711. General Data Protection Regulation, 2016, Article 4(1). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, last accessed 22.08.2023.
712. Opinion of the Ombudsman, 4 February 2021, p.3.
713. Opinion of the Ombudsman, 4 February 2021, p.7.
714. Commercial Law, 2002, Article 8. Available at: https://likumi.lv/ta/en/en/id/5490, last accessed 22.08.2023.
715. Law On the Enterprise Register of the Republic of Latvia, 1990, Articles 4.[8], 6. Available at: https://likumi.lv/ta/en/en/id/72847-on-the-enterprise-register-of-the-republic-of-latvia, last accessed 22.08.2023.
716. Opinion of the Ombudsman, 4 February 2021, p.9.
717. Opinion of the Ombudsman, 4 February 2021, p.11.
718. Opinion of the Ombudsman, 4 February 2021, p.12.
719. Opinion of the Ombudsman, 4 February 2021, p.13.
720. Opinion of the Ombudsman, 4 February 2021, p.15.

2.3.6 Opinion of 27 May 2021 on the availability of the non-anonymised ruling of the Supreme Court online

The claim was initiated by a person who claimed that a non-anonymised court ruling against him pronounced in 1997 was still available online. The applicant claimed that the ruling contained their name, surname, date of birth, former workplace, a brief description of the criminal case and the sentence imposed on them.[721] The Ombudsman further indicated that other non-anonymised court rulings were also found on the websites www.likumi.lv (the official website publishing Latvian legal acts) and www.vestnesis.lv (web version of the official government gazette *Latvijas Vēstnesis*).

The Ombudsman confirmed that the ruling containing above mentioned personal details falls under the notion of data processing. Recalling the right to be forgotten, the Ombudsman noted that publishing the non-anonymised court ruling did not pursue a legitimate aim; moreover, Article 11 of the Law on Official Publications and Legal Information[722] requires the publisher to ensure appropriate protection of personal data.

Latvijas Vēstnesis as the data processor admitted that publishing of the non-anonymised decision is an excessive interference with the privacy of the applicant. As a remedy, it requested Google to no longer index (show in the search results) the applicant's data and stopped the practice of publishing non-anonymised court rulings online.

2.4 European Court of Human Rights judgment in Nagla v. Latvia

The applicant was working for the national television broadcaster *Latvijas televīzija* ('Latvian television'). She was approached by an anonymous source, a hacker calling himself Neo, claiming that the database of the State Revenue Service contains loopholes, making it possible to access the Electronic Declaration System without formally breaching security measures. The applicant informed the State Revenue Service about a data breach. Several days later, acting in her journalistic capacity, she revealed during the broadcast about the data leak.[723]

Almost three months later, the police searched the applicant's home without a search warrant. The warrant was approved by a judge retrospectively on the following day.[724] The applicant claimed that her right to receive and impart information was violated, as during the search the police received information that could disclose her source. The government submitted that the interference was prescribed by law and pursued a legitimate aim of protection of rights of others:

'[t]he balancing exercise in the present case involved the applicant's right to freedom of expression against the right of hundreds of thousands of individuals in Latvia to the protection of their personal data.'[725] [emphasis added]

The Court generally accepted that the interference was intended to prevent disorder or crime and to protect the rights of others.[726] However, the Court reasoned that by informing society about salaries in the public sector and about security flaws in the databases of the State Revenue Service, the applicant fostered public debate.[727] In the criminal proceedings, her status as a witness remained unchanged, yet the search warrant did not contain any specific reasons for

721. Opinion the Ombudsman, Inspection case No. 2021-31-5F, 27 May 2021. Available at: https://www.tiesibsargs.lv/wp-content/uploads/2022/07/atzinums_2021_31_5f_1642687192.pdf (in Latvian), last accessed 22.08.2023.
722. Law on Official Publications and Legal Information, Article 11. Available at: https://likumi.lv/ta/en/en/id/249322-law-on-official-publications-and-legal-information, last accessed 22.08.2023.
723. *Nagla v. Latvia,* Judgment of 16 July 2013, paras.6-9.
724. *Nagla v. Latvia,* Judgment of 16 July 2013, paras.21–24.
725. *Nagla v. Latvia,* Judgment of 16 July 2013, para.71.
726. *Nagla v. Latvia,* Judgment of 16 July 2013, para.92.
727. *Nagla v. Latvia,* Judgment of 16 July 2013, para.97.

conducting it with such urgency. Consequently, such actions amounted to a violation of Article 10 ECHR, noting that

'the investigating judge failed to establish that the interests of the investigation in securing evidence were sufficient to override the public interest in the protection of the journalist's freedom of expression'.[728]

2.5 Analysis

Comparing the three judgments of the Constitutional Court of Latvia analysed above, one may conclude that the Court does not automatically accept all digitalisation measures taking place in public administration. The judgments show that it is careful in balancing individual rights *vis-à-vis* the collective interests (such as public safety).

Interestingly, in all three judgments, the Court acknowledged that the measures in question pursued legitimate aims; where they 'failed' is the proportionality test. This indicates that digitalisation efforts in general should be more nuanced and carefully calibrated to counter the challenges they pose to human rights.

In the following subsections, the authors outline potential challenges posed to the right to a fair trial, the right to private life and the prohibition of discrimination.

2.5.1 Fair trial guarantees

In cases involving automatic registration of offences (such as with the use of photo and video radars in road traffic), the right to fair trial and the presumption of innocence are relevant. As seen in the Constitutional Court's judgment in the case 2012-15-01 concerning the use of radars in road traffic. To remind the reader, that where the actual driver was unidentifiable, the administrative penalty for the violation would have been applied to the owner of the vehicle. Although the applicant did rely on the presumption of innocence, the Court emphasised that it is not absolute and may be substituted with another legal presumption of fact.[729]

Such an argument can potentially be extended to the use of other devices in the future. For example, a personal computer or a mobile phone may be used to commit an offence. Following the same logic, if the actual holder/user of the device is impossible to identify at the time of the offence, the penalty could be sent automatically to the known owner of the device. That in turn, poses a bigger threat to the presumption of innocence.

Digitalisation also impacts the right to the fair as a whole. As noted in the first section, Administrative Procedure Law provides an overall framework for e-cases. The Latvian Digital Transformation Guidelines 2021–2027 set the aim of '*complete digitalisation of the processes related to the core activities of law enforcement, judicial and penal institutions.*'[730]

However, careful balancing is necessary in this context. The right to fair trial also enshrined the right of access to court, and in case of *complete* digitalisation of case management, some groups – seniors, people with lower income, and people with less advanced digital skills – may be limited in this right. Indeed, this is a long-term transition rather than an immediate threat, yet more vulnerable groups need to be taken into account when implementing the digital transition plan.

728. *Nagla v. Latvia,* Judgment of 16 July 2013, para.101
729. Judgment of the Constitutional Court of Latvia in the case 2012-15-01, 28 March 2013, para.15.1.
730. Digital Transformation Guidelines 2021-2027.

2.5.2 Private life guarantees

As digitalisation presupposes the processing of large masses of personal data, which is an element of personal life, the most pressing challenge links to Article 8 of the ECHR. The analysis of the Latvian practice also shows that the majority of cases concern Article 96 of the Constitution, which is a domestic 'twin' of Article 8 of the Convention.

Both the Constitutional Court and the Ombudsman found that the measures adopted by the state – such as the use of radars, ensuring online availability of laws and judgments or sustaining public registers – all pursued one or several legitimate aims embodied in Article 8(2) ECHR:

'*in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*'[731]

Thus, Latvia's incentive to ensure the '*active involvement of all state administrative institutions in the creation and implementation of the digital security policy*'[732] aims to strengthen national security, and '*complete digitalisation of the investigative process*'[733] would ensure the prevention of disorder or crime, '*preservation, restoration and improvement of an individual's health and quality of life [...] facilitated by a service ecosystem based on data and their digitalisation*'[734] corresponds to the protection of public health – and so on. In other words, one may find a 'matching' legitimate aim for virtually any step undertaken in the domain of digital transformation.

As also seen from national practice, the challenge *per se* lies in the proportionality test: as digitalisation often involves the processing of sensitive data (e.g., health data), the balancing of individual interests versus collective interests should be very careful.

The judgment in *Nagla v. Latvia* highlights the importance of installing proper security measures. If the management of personal data for public services becomes more centralised, for example, if the government creates something like a shared 'drive' for all competent institutions to access, the cost of error (such as data leak) increases dramatically.

Another potential issue here is the unwillingness to use digitalised public services. Some people do not wish to use new technologies and would prefer printing the document and physically bringing it to a state institution instead of doing it electronically. For that reason, a 'non-digital' version of public services is always available – thus, the Latvian public is not forced to use electronic services. Latvia, for all its digitalisation activities, has chosen an 'opt-in approach': a person has to him/herself *choose and agree* to use a digital version of the service instead of an offline one.

2.5.3 Prohibition of discrimination

Digitalisation efforts should also take into account more vulnerable groups such as visually impaired people, people with other disabilities, people having weaker digital skills, etc. In fact, the Latvian Digital Transformation Guidelines 2021–2027 explicitly recognise this risk, setting an aim

'to ensure that in the digital space of Latvia, every person (including, for example, persons with disabilities) can access safe digital services and reliable digital media without any discrimination, as well as can participate, express themselves, search for information and exercise all their rights in the digital space environment.'[735]

731. European Convention on Human Rights, Article 8(2).
732. Digital Transformation Guidelines 2021-2027, para.4.2.1.
733. Digital Transformation Guidelines 2021-2027, para.4.4.5.1.
734. Digital Transformation Guidelines 2021-2027, para.4.4.6.
735. Digital Transformation Guidelines 2021-2027, para.4.4.6.

As for now, for example, the Latvian State administration services portal www.latvija.lv only partially complies with the Procedures for Publishing Information on the Internet by Institutions.[736] Based on its 2022 self-evaluation[737] of the portal, some images are missing alternative texts for the people using a screen reader to be able to access the information; some video content lacks subtitles; in several portal sections, navigation using only the keyboard is not possible; the colour contrast is insufficient.

This problem has been addressed: since 2015, a network of State and Municipality Unified Customer Service Centres has been formed. In these centres, any person has access to a workplace with a computer and an Internet connection to use digital public services. If necessary, educated assistants are on-site to provide help.

3. Does the Legal Framework Support Digitalisation?

Within this section, the authors analyse how the Latvian legal framework supports public digitalisation, specifically reflecting on the legal instruments that are used in order to support and encourage public digitalisation in the administrative sector. Particular attention will be devoted to several methods that are expected to support digitalisation: the legislative obligation of self-digitalisation, the usage of policy papers to promote digitalisation and, finally, the usage of technology-neutral language in legislation. While the first two are intended to promote digitalisation, the third one is seen as a tool not to prevent technological innovations and potentials.

3.1 Legislative obligation of self-digitalisation

Firstly, it is possible to distinguish a legislative approach whereby the legislator obliges the state administration to provide services electronically. For example, Article 99 (1) of the State Administration Structure Law (that forms the backbone of the Latvian administrative sector, as previous mentioned) stipulates that the State administration shall arrange the provision of services electronically, where possible and feasible. Article 99 (2) stipulates additionally that the procedures for the performance of electronisation of State administration services and ensuring of e-service accessibility shall be determined by the Cabinet of Ministers (that is the highest executive body of the country). Thus, the obligation of self-digitalisation is established in the most important law of the public administration.

Further, the Cabinet of Ministers has adopted Regulation No. 402[738] which prescribes the procedures by which public administration services are digitised and made available for the public.[739] Firstly, Regulation No. 402 sets out conditions under which the service owner shall provide services in the form of e-services. Namely, Article 3 stipulates that a service owner, if it is possible and useful, shall provide services also in the form of e-services, if at least one of the following criteria is met:

1. within a year the number of requested service cases exceeds 5000 or 10% of the number of cases of all services provided by the service owner;
2. availability of the service would improve;
3. receiving the service electronically would be more convenient;
4. the administrative burden would be reduced;
5. the service provision process would optimise;

736. Procedures for Publishing Information on the Internet by Institutions.
737. Available at https://latvija.gov.lv/Content/Pieklustamiba (in Latvian), last accessed 27.08.2023.
738. Regulations Regarding the Public Administration E-services.
739. Regulations Regarding the Public Administration E-services. Article 1

6. the costs and time for the provision of services would decrease;
7. provision of the relevant service also in the form of an e-service would be preferred due to the equality considerations of specific client groups.

Secondly, setting up electronic services without continuous maintenance and development would lead to inefficiency. For this reason, Article 13 of the Regulation includes explicit rules to make service owners responsible for planning, ensuring, maintaining, and developing e-services. Namely, according to Article 13, the service owner among other responsibilities shall:

1. continuously co-ordinate the process of provision of e-services;
2. make sure that the provision of e-services conforms with the minimum technical and safety requirements laid down in the laws and regulations;
3. ensure that necessary changes for e-services are introduced and the previous testing process is implemented;
4. make sure that the rules for the use of the e-services are introduced;
5. ensure that the provision of the e-service is suspended, if, as a result of changes in the normative regulation or technical deficiencies, the e-service does not conform to laws and regulations;
6. inform the e-service provider and e-service users in advance of interruptions in the operation of the e-service and the planned resumption of the operation three working days before the planned interruption, but in case of an unplanned interruption - at the time of occurrence;
7. provide the consultative support of the e-service provider;
8. determine the means of e-identification of the individuals necessary for the e-service.

Thirdly, Regulation No. 402 includes explicit provision for service owners to promote the usage of their e-services in public. Thus, Article 18 of the regulation obliges service owners to develop such terms of service-use which, first, promote the use of the e-service and, secondly, fulfil at least one of the following aspects: 1) provide a shorter time period for the electronic service than in person at premises of the national authority; 2) provide a lower cost for the electronic service than in person at the premises of the national authority; 3) provide availability of the service only in electronic form, keeping in-person consultations at the premises of the authority only for the purpose of consulting the use of the e-service; 4) provide identification mechanism (for the use of e-service) that is as accessible and convenient as possible.[740] Thus, the Regulation has introduced the administrative principle of promoted use of administration e-services.

To conclude, the provision of electronic services to the public or the so-called digitalisation of the administration is promoted with the legislative obligation of self-digitalisation, on one hand, and the transparent setup of criteria for implementing the digitalisation by the Cabinet of Ministers, on the other hand.

3.2 Policy paper promoted digitalisation

Secondly, it is possible to distinguish an approach whereby the Cabinet of Ministers (that is the highest executive body of the country) encourages digitalisation by adopting special policy papers. As mentioned before, the Latvian government has adopted Digital Transformation Guidelines 2021–2027. This document takes the form of an executive order.

740. Regulations Regarding the Public Administration E-services. Article 18

Legally, the digital transformation plan as an executive order is rather a policy planning document. The digital transformation plan, firstly, designates the Ministry of Environmental Protection and Regional Development as the responsible institution for the implementation of the plan and, secondly, obliges the ministry with defined implementation measures, namely, to present to the Cabinet of Ministers an interim report on the implementation of the order by 31 May 2024.[741]

Substantially, the digital transformation plan contains visionary concepts as well as concrete directions of action and tasks to fulfil in order to implement the digital transformation plan. Thus, the transparency of planned activities of the government permits not only the administrative sector but also the private sector (that includes businessmen) to adopt their business perspectives to the common national digital transformation plan.

However, the disadvantage of such an executive order is that the visionary goals and results defined thereof are highly dependent on the amount of available funding. This is also clearly stated in the digital transformation plan itself.[742] Therefore, it is possible to conclude that these policy papers transparently establish the trajectory of the development, but do not guarantee or promise the result itself.

3.3 Technology-neutral language in legislation

In the authors' view, it is possible to distinguish an approach whereby technology-neutral language in legislation is used to ensure that existing or planned legislation in the administrative law domain, on the one hand, does not burden or restrict in any way technological advancements in practice, and on the other hand, does not prioritise technological advancements on the expense of administrative rights of individuals.

The term 'technologically neutral regulation' was used in the context of European electronic communications and was explained by Directive 2002/21/EC[743] whereby it was stated that *'Member States must ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, so that it neither imposes nor discriminates in favour of the use of a particular type of technology, does not preclude the taking of proportionate steps to promote certain specific services where this is justified.'*[744] In legal literature, the technology-neutral language is seen as an opposite to technology-specific legislation that refers to specific types or classes of technology[745] whereas technology-neutral language focuses on more general terms and general characteristics such as purpose and functions.[746] Technology-neutral legislation is seen as a solution to legislators' never-ending fight to keep up with the development and changes in technology.[747]

In this context, the Latvian Administrative Procedure Law is designed and maintained as a technology-neutral law.

First, the general terms such as an 'administrative act' and 'factual action' are designed in a way that would cover both acts by human beings and technologies. Thus, even if administrative acts are adopted by technological means (such as automated passport control machines at customs

741. Regulations Regarding the Public Administration E-services. paras. 2 and 4.
742. Regulations Regarding the Public Administration E-services, introductory part.
743. Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). Today, the regulation is repealed by the Directive 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code.
744. Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services, recital 18. Available at: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0021, last accessed 27.08.2023.
745. The Benefits and Challenges of Technology Neutral Regulation - A Scoping Review./ Puhakainen, Essi; Väyrynen, Karin Elisabeth. Twenty-fifth Pacific Asia Conference on Information Systems, 2021. p. 1.
746. The Benefits and Challenges of Technology Neutral Regulation - A Scoping Review./ Puhakainen, Essi; Väyrynen, Karin Elisabeth. Twenty-fifth Pacific Asia Conference on Information Systems, 2021. p. 2.
747. The Benefits and Challenges of Technology Neutral Regulation - A Scoping Review./ Puhakainen, Essi; Väyrynen, Karin Elisabeth. Twenty-fifth Pacific Asia Conference on Information Systems, 2021. p. 1.

and border protection points that streamline the entry process), such acts will be subjected to the Latvian Administrative Procedure Law and might be equally reviewed by the national administrative courts. At the moment, the Administrative Procedure Law does not distinguish acts adopted by human beings or technologies and thus does not exempt technologies from respecting basic principles of administrative law when adopting administrative acts or carrying out factual actions.

Secondly, The Latvian legislator decided to include in the Administrative Procedure Law catalogue of principles of administrative law that are explained in a very simple and comprehensive manner, such as the principle of equality and non-discrimination (Article 6), the principle of rule of law (Article 7), the principle of protection of legitimate expectations (Article 10), the principle of proportionality (Article 13), principle of procedural equity (Article 14-1), etc. Such a legislative tactic, in the authors' view, facilitates, on one hand, the work of technology developers who are not lawyers, and, on the other hand, individuals encountering technologies developed by national agencies: principles are easier to consider (unlike very specific provisions of laws) while the technologies are developed ('development' stage) as well as easier to consider when the technology is employed towards the individual ('employment' stage).

For example, if the national agency has developed a mobile application for the public that by accident or mistake works only for iPhone, but not for Android (or reverse), it is easier for an individual to claim that this act of the state constitutes a breach of the principle of non-discrimination (and thus possibly as a factual action defined by the Article 89 of the Administrative Procedure Law is a subject for administrative review in the higher institution).

Thirdly, what relates to electronic communication between state authorities, courts and individuals, the Administrative Procedure Law usually states the form of communication, but never the tool itself. For example, Article 210 permits the use of a videoconference regime for adjudicating cases, but not the specific videoconference tool. Similarly, several articles permit the use of electronic mail and signatures, but not the specific trustful service providers. Thus, procedures leave space for competition for different service providers and future technological developments.

The term 'technologically-neutral legislation' is also referred to in national case law and thus is familiar to national courts. It is possible to observe that the term has been referred both to procedural laws as well as to material laws. For example, as for procedural laws, the term refers to the form of evidence, such as the form of fixing the sound to materialise it in copyright disputes.[748] As for the material laws, the term was referred to in cases concerning personal data protection (as to the form and means on how third parties can reach personal data or the personal data is disclosed,[749] automatisation level of processing of personal data[750]) and electronic communications (as to the form how the sound is broadcast[751] or the form of the broadcast itself that can be technology specific and require licencing,[752] and granting the right to use Megahertz (MHz) frequencies[753]). Thus, the term 'technologically neutral regulation' is not only a theoretical perspective but is implemented into reality by all level courts.

748. Judgment of the Supreme Court of 28 December 2017, case No. C31553112, para. 6.1.
749. Judgment of the Administrative District Court of 18 June 2021, case No. A420230820, para 11; Judgment of the Administrative Regional Court of 24 February 2022, case No. A420230820, para 8.
750. Judgment of the Administrative District Court of 9 July 2021, case No. A420275120, para 7;
751. Judgment of the Supreme Court of 28 December 2017, case No. C31553112, para 6.1.
752. Judgment of the Supreme Court of 17 January 2017, case No. C27184811, point 8.
753. Judgment of the Administrative Regional Court of 24 February 2012, case No. A43004111, point 13.

4. Assessment of the Proposed EU Regulation on Artificial Intelligence

At present time, the European Commission's proposed regulation laying down harmonized rules on artificial intelligence (the so-called Artificial Intelligence Act) is undergoing negotiations.[754] This initiative aims to ensure that the rapidly developing artificial intelligence (AI) is developed and subsequently used within an appropriate legal framework that stimulates trustworthy Artificial Intelligence in the single market.[755]

Before the regulation is adopted and clear rules are laid down, it is not possible to *comprehensively* assess how it will supplement national administrative law and whether the AI regulation will fill (sufficiently) in any detected gaps. However, it is possible to anticipate at least a few aspects in this regard.

According to the Governmental informative report 'On the development of Artificial Intelligence Solutions' adopted in 2019, it is planned that AI will be specifically employed for various administrative tasks. For example, AI is already used and will be used more extensively for virtual assistants that consult clients of state administrative institutions and have ultimate access to various state-held databases and registers.[756] For this purpose, the government continues to improve the state administration language technology platform Hugo.lv which provides machine translation, speech recognition and synthesis that will enable virtual assistants to communicate with individuals verbally.[757]

Advantages provided by AI will be employed to analyse, control and improve road safety[758] as well as to empower the State Tax Administration to fight shadow economy and money laundering.[759] It is also planned that artificial intelligence will have access to such sensitive information as health data to diagnose and prevent, for example, cancer risks.[760] Thus, it is inevitable that currently and in the foreseeable future AI will significantly affect several fundamental rights, such as the right to human dignity, the right to privacy, the protection of personal data, the principle of equality and non-discrimination, the right to a fair trial, the general principle of good administration, as well as will pose several safety and transparency concerns in such domains as planning, health care and transport.

As for the assessment of how the proposed regulation will supplement national administrative law, it is possible to distinguish at least three different perspectives.

Firstly, Latvia, like all the EU Member States, will have to establish or designate a new national competent authority for the purpose of ensuring the application and implementation of the regulation (as proposed by Article 59 of the proposed regulation), thus introducing a brand-new level of protection for its citizens and transparency for businesses.

---

754. 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.
755. 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, subchapter 1.1.
756. Governmental informative report 'On the development of Artificial Intelligence solutions', p.11. Available at: https://www.varam.gov.lv/lv/jauns-informativais-zinojums-par-maksliga-intelekta-risinajumu-attistibu (in Latvian), last accessed 27.08.2023.
757. Governmental informative report 'On the development of Artificial Intelligence solutions', p.11. Available at: https://www.varam.gov.lv/lv/jauns-informativais-zinojums-par-maksliga-intelekta-risinajumu-attistibu (in Latvian), last accessed 27.08.2023.
758. Governmental informative report 'On the development of Artificial Intelligence solutions', p.12. Available at: https://www.varam.gov.lv/lv/jauns-informativais-zinojums-par-maksliga-intelekta-risinajumu-attistibu (in Latvian), last accessed 27.08.2023.
759. Governmental informative report 'On the development of Artificial Intelligence solutions', p.12. Available at: https://www.varam.gov.lv/lv/jauns-informativais-zinojums-par-maksliga-intelekta-risinajumu-attistibu (in Latvian), last accessed 27.08.2023.
760. Governmental informative report 'On the development of Artificial Intelligence solutions', p.12. Available at: https://www.varam.gov.lv/lv/jauns-informativais-zinojums-par-maksliga-intelekta-risinajumu-attistibu (in Latvian), last accessed 27.08.2023.

Secondly, it is possible to claim that practically the AI itself and its enhanced use that is promoted by the EU regulation will help the public administration to perform already established governmental tasks more efficiently. For example, it is clear that the public administration has an uncontested obligation to implement road safety measures and control the drivers. However, artificial intelligence has the potential to help the public administration perform this already existing function more efficiently in a way of collecting and analysing data as well as performing automated decision-making in order to punish lawbreakers. Also, it is clear that public administration has a public function to guide individuals and address their petitions. However, Artificial Intelligence has the potential to undertake some of specific functions via, for example, virtual consultants to ease the work of public servants and let them address more complicated and time-consuming public functions, thus, optimizing the work of public administration.

Thirdly, it is obvious that the proposed regulation will supplement national administrative law by establishing a novel administrative law framework for the use of AI. The current national legal framework in Latvia seems to be more focused on digitalisation generally (such as databases and e-services), whereas AI is seen as only one of the several services. However, the coming regulation seems to be more focused on one specific and complicated service, thus offering a new concept. In other words, AI cannot be 'put in one basket' together with other digitisation services as equal.

The proposed regulation clarifies the notion of 'artificial intelligence systems', prohibited practices as well as high-risk AI systems. Further, the proposed regulation sets standards for trustworthy Artificial Intelligence: risk management systems,[761] technical documentation before the system is placed on the market or put into service,[762] record-keeping requirements,[763] transparency requirements toward users of human oversight,[764] obligations of providers, users and other parties,[765] and what is more important, imposes the protection of fundamental rights when Artificial Intelligence technology is developed and used.[766]

Even though there are similar administrative requirements in place at the national level for secure and trustworthy e-services, the proposed regulation sets a new standard for Artificial Intelligence at the international level and thus this standard will have far-reaching consequences in a way of being a source of inspiration for different services at the national level, such as technology and digitalisation advancements as well as e-services, even though they are not directly related to Artificial Intelligence.

761. 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, Article 9. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, last accessed 27.08.2023.
762. 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, Article 11. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, last accessed 27.08.2023.
763. 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, Article 12. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, last accessed 27.08.2023.
764. 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, Article 13 and 14. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, last accessed 27.08.2023.
765. 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, Chapter 3. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, last accessed 27.08.2023.
766. 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, for example, Article 7, 14, 62. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, last accessed 27.08.2023.

5. Closing Remarks

To conclude, the authors would like to make three suggestions for future public digitalisation.

First, at the current stage, it appears that adjusting administrative law as well as digitalisation itself is highly fragmentary in the Nordic-Baltic region. Each individual country in the region sets its priorities, digitalisation measures, levels of digitalisation and the measures to protect human rights. Different levels of legal protection can consequently affect the regional pace of digitalisation as well as hinder the harmonisation of the EU internal market.

To tackle this problematic aspect, authors see the chance to continue researching the digitalisation of administrative law in the region, developing special model rules on the digitalisation of administrative law in the Nord-Baltic region (similarly as it was done by ReNEUAL model rules on EU administrative procedure).

Such digitalisation model rules developed by legal researchers shall contain authoritative provisions regarding not only the possible rules for different administrative law aspects, such as previous assessment of human rights impact before digitalisation solution is introduced; cross border cooperation between two authorities; information management in governmental databases; minimum technical and safety requirements; previous testing processes, etc.; but also principles for legislators developing administrative law, such as how to efficiently develop technologically neutral legislation etc. The development of common digitalisation principles is particularly important in domains that affect mobility, such as transport, tourism, movement of employees etc.

Development of such special model rules on the digitalisation of administrative law in the Nordic-Baltic region can lead to more foreseeability and clarity for businesses and programmers as well as serve as a good regional practice to other EU Member States.

Second, the existing case law of Latvian courts shows that different regulatory initiatives related to digitalisation were insufficiently considered by legislators and thus can jeopardize fundamental rights. The Achilles heel is the proportionality test and the (lack of) sufficient procedural guarantees for individuals.

Taking into account ever faster development of technologies and the accompanying regulations, policymakers should develop a more 'human-centric' approach not only to AI as proposed in the Artificial Intelligence Act but also to all advancements of technologies to ensure that the sectorial administrative laws mitigate the risks to fundamental rights. This can be achieved, firstly, by stricter impact assessment requirements for policymakers and legislators as well as, secondly, more clear and foreseeable rules for the possibility of contesting digital measures that infringe fundamental rights.

Finally, digitalisation processes in the administrative sector tend to be very frequent and fragmentary. At the same time, digitalisation seems to be intervening in all the processes of everyday businesses and life. This makes us reconsider whether digitalisation reforms should be seen as separate and independent at all. Instead, digitalisation reforms could be seen as a supplementing element of *any* reform taking place, be it reform of the health sector or judiciary. Thus, the administrative sector should have a strong vision that whenever any reform takes place, digitalisation aspects are an inherent part of it.

LITHUANIA

E-government in Context of Principles of Good Governance

Prof. Dr Eglė Bilevičiūtė

1. Introduction

Good governance is a requirement for all public administration entities and is implemented through the relationship between citizens and government representatives. Good governance must enable the rational management of public affairs, the efficient use of resources and the achievement of the public good, while guaranteeing human rights. Good governance creates a framework in which political, social, and economic priorities are based on a clear consensus among the various groups in society; it ensures respect for human rights and the rule of law; it strengthens democracy and promotes transparency and efficiency in public administration. The principles of good governance can be defined as the rules on which a public authority bases its activities.[767] The quality of a country's public administration is key to its economic performance and the well-being of its citizens. An effective and efficient public administration serves the needs of its citizens. It is essential that public authorities and their managers can adjust to changing circumstances, especially in times of crisis.

The European Institute of Public Administration (EIPA) has as its core mission to provide in-depth insights and practical knowledge on EU policy to all professionals involved in EU public affairs, with the main objective of further developing their skills and capacity to effectively manage national policymaking in the EU context. EIPA expertise and training:

- Effective public administration in the EU: quality management, the Common Assessment Model (CAM), data protection, human resources and new ways of working.
- Better governance in the EU: design and adoption of decisions, impact assessment, forms of inclusion and participation.
- Public finance management in the EU: fraud prevention, audit, procurement, project management.
- EU general policy: climate and environment, digitisation, state aid, social inclusion, economic governance / EU Semester
- EU in the world: external policy, enlargement and neighbourhood, security.

767. Rūta Petrauskienė and Eurika Predkelytė, „Gero valdymo principų įgyvendinimą viešosiose institucijose lemiantys veiksniai: teorinis pagrindimas", *Public security and public order*, 12 (2014): 147–160.

So, Lithuania joined EIPA on 29 May 2006 by signing an agreement between the Government of the Republic of Lithuania and EIPA on cooperation and financial support, expressing its willingness to contribute to EIPA's activities in the areas of training, research, consultancy, and publications.[768]

Later years, Lithuanian researchers have worked on e-government issues in the development of the e-government system in Lithuania, and their results provides an overview of the challenges and possibilities. Rimantas Garuckas and Adolfas Kaziliūnas[769] has emphasised the legal frameworks relevance for the implementation of the Lithuanian e-government concept, and analysed the legal acts regulating e-government and the state of electronic services in Lithuania. Elena Raginytė and Narimantas Kazimieras Paliulis have argued that the development of e-government in Lithuania is as relevant as it is throughout Europe. However, according to the two researchers, Lithuania still faces technical, legal, and methodological problems that hinders the full effectiveness of e-government. These hindrances are problematic as various national and international studies have shown, a low level of efficiency in public administration is a strong factor that reduces the competitiveness of businesses and the attractiveness of a country to invest and live in.

In regard to research directed at the present hindrances, most researchers have highlighted that development of e-government in Lithuania is a continuous process, implemented in stages and that the development and successful implementation of digital communication is an important stage. Vladislavas Domarkas and Vitalija Lukoševičienė believe that as e-government services provided to the public via the Internet are to be the main means of communication, the effectiveness of e-government depends on the content of the websites of the government institutions. Eglė Gaulė and Gintaras Žilinskas[770] have attempted to identify the external factors influencing the development of Lithuanian municipal websites. Vladislavas Domarkas, Akvilė Laukaitytė and Vidmantas Mačiukas[771] have discussed various methodologies of e-government evaluation and, using the methodology of evaluation of municipal websites developed by Rutgers University in the USA and Sungkyunkwan University in South Korea, evaluates the level of development of websites of municipalities in the Republic of Lithuania.

Some researchers have adopted broader perspectives. For example have Zinaida Manžuch, Arūnas Gudinavičius and Andrius Šuminas[772] examined the adaptation of IT to country development. The aim of the paper is to assess the strategic priorities and concrete measures to reduce the digital divide in Lithuania. Alvydas Baležentis and Gintarė Paražinskaitė[773] argues that society's wealth, power and knowledge are determined by the ability to organise society and make the most of new technological solutions, especially digital communication. The article presents the assessments of thirteen HR experts from ministries of the Republic of Lithuania. The results of the study show that in order to increase the use of IT innovations in the personnel administration services of the ministries of the Republic of Lithuania, it is necessary to maintain a balance between inhibiting and stimulating factors and to increase innovation. Žemyna Pauliukaitė-Gečienė and Ramunė Juozapaitienė[774] wants to offer a vision for the future of public governance in Lithuania, by looking at the maturity stages of the digital transformation of public

768. "The European Institute of Public Administration", accessed August 10, 2023, https://www.eipa.eu/.
769. Rimantas Garuckas and Adolfas Kaziliūnas, „E. valdžios ir viešojo sektoriaus sąveikos Lietuvoje analizė", *Viešoji politika ir administravimas*, 23 (2008): 59–67.
770. Eglė Gaulė and Gintaras Žilinskas, "E-governance in Lithuanian Municipalities: External Factors. Analysis of the Websites Development", *Viešoji politika ir administravimas*, 12, 1 (2013): 80–93.
771. Vladislavas Domarkas, Akvilė Laukaitytė and Vidmantas Mačiukas, „Lietuvos Respublikos savivaldybių interneto svetainių išvystymo lygio vertinimas", *Viešoji politika ir administravimas*, 11, 1, (2012): 23–36.
772. Zinaida Manžuch, Arūnas Gudinavičius and Andrius Šuminas, „Skaitmeninės atskirties mažinimo priemonės Lietuvoje: tikslai, auditorijos ir taikymo rezultatai", *Viešoji politika ir administravimas*, 17, 1 (2018).
773. Alvydas Baležentis and Gintarė Paražinskaitė, „Informacinių technologijų taikymas LR ministerijų personalo administravimo tarnybose", *Management Theory and Studies for Rural Business and Infrastructure Development*, 36, 4 (2014): 746–754.
774. Žemyna Pauliukaitė-Gečienė and Ramunė Juozapaitienė, *Lietuvos viešojo valdymo skaitmeninė transformacija: politiniai ir technologiniai aspektai*)Vyriausybės strateginės analizės centras, 2021), https://strata.gov.lt › tyrimai › 2021-metai.

governance, considering the opportunities created by digitalisation and the implications for the change in the relationship between the state and the citizen. The vision for the future of public governance in Lithuania is formulated and recommendations are made. It emphasises that the digital transformation requires maturity of both the public sector and society itself. Public organisations must be willing to initiate digitisation and be able to develop and use the results of digitisation, and users must be willing, able, and able to use them.

2. Review of the Lithuanian public administration sector system and the level and future development of e-government in Lithuania

2.1 Structure of the Lithuanian public administration sector

The Lithuanian public administration sector comprises the activities of public administration bodies in implementing initiatives set out in laws or regulations, ensuring the quality of life of citizens, the provision of public services, public security and justice, and the sustainable management of the state, social and economic regulation, and other matters of state and municipal governance. In other words, public administration entities may be a state institution or body, a municipal institution or body, an official, a civil servant, a state or municipal enterprise, a public institution owned or shared by the state or municipality, an association who has been authorised to carry out public administration in accordance with Law on public administration of the Republic of Lithuania[775] and the corresponding procedures laid down in the law on public administration.

The law on public administration establishes the basic principles of public administration, the fields of public administration, the system of public administration entities and the basis for the organisation of administrative procedure; the basic provisions for the supervision of the activities of economic operators; guarantees the right of individuals to appeal against actions, omissions or administrative decisions of public administration entities, as well as the right to a lawful and objective examination of requests and complaints from individuals; and establishes the rights and obligations of other individuals and public administration entities in the field of public administration. See further in section 3.

Public administration entities operate in a public sector environment and their objectives are characterised by the pursuit of quality of life for the citizens of the country, which is often measured in qualitative indicators, with a strong focus on the quality of administrative processes. Private sector entities have profit-oriented objectives, which are more often measured in quantitative terms. In Lithuania, there are over 4,000 organisations in the public sector (which includes the public administration sector, the education sector, the social services sector and other sectors) (in 2017, there were 4,244 public sector organisations, including 862 public sector organisations of the state and 3,382 public sector organisations of municipalities).[776] Number of enterprises in the institutional sector of general government on 1 January 2023 - 3177.[777] The Ministry of the Interior formulates state policy in the field of public administration and organises, coordinates, and controls the implementation of this policy.[778]

775. "Republic of Lithuania law on public administration 17 June 1999 No VIII-1234, new edition from 1 November 2020 No XIII-2987", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.83679/asr.
776. Viešojo administravimo sektoriaus paslaugų profesinis standartas ir kitų paslaugų sektoriaus profesinis standartas. Kvalifikacijų tyrimo ataskaita. (Vilnius: MRU, 2019).
777. "Official Statistics Portal. Institutional sectors and subsectors", accessed August 10, 2023, https://osp.stat.gov.lt/instituciniai-sektoriai-ir-subsektoriai.
778. "Ministry of the Interior of the Republic of Lithuania", accessed August 10, 2023, https://vrm.lrv.lt/lt/veiklos-sritys/viesasis-administravimas.

The network of public sector bodies in Lithuania consists of[779] (see table):

Central Bank	In the Republic of Lithuania, the central bank is the Bank of Lithuania, which is owned by the Lithuanian State. The Bank of Lithuania is an integral part of the European System of Central Banks and pursues the objectives and tasks of the European System of Central Banks in accordance with the guidelines and instructions of the European Central Bank.
2 794 budgetary institutions founded by the State or municipalities (2022-01-20)	Budgetary institution - a public legal entity with limited civil liability that implements state or municipal functions and is maintained from the appropriations of the state or municipal budgets, as well as from the budgets of the State Social Insurance Fund, the Compulsory Health Insurance Fund, and other state monetary funds.
18 state-owned enterprises (2022-01-20)	A state-owned enterprise is an enterprise established from state assets or transferred to the state in accordance with the procedure laid down by law, which belongs to the state by virtue of its ownership and owns, uses and disposes of the assets transferred to it and acquired by it under the right of entrustment.
69 joint-stock and private joint-stock companies in which the State participates as a shareholder (13-05-2022)	Joint-stock company - a company with limited liability and legal personality, whose authorised capital is divided into shares of equal nominal value. A private limited liability company is a private legal person with limited civil liability whose authorised capital is divided into shares. The main document regulating the activities of a private limited liability company is the Law on Joint Stock Companies of the Republic of Lithuania, and its shareholders may be both natural persons and legal persons who acquire shares in the company.
21 Municipal companies (2022-01-20)	A municipal enterprise is an enterprise established from municipal property or transferred to the municipality in accordance with the procedure laid down by law, which is owned by the municipality and owns, uses and disposes of the property transferred to it and the property acquired by it under the right of entrustment.
350 public bodies in which municipalities participate as owners or shareholders (2022-05-20)	Public body, a non-profit public legal person with limited civil liability serving the public interest. It carries out educational, training and scientific, cultural, health care, environmental protection, sports development, social or legal aid and other activities of public benefit.
253 private limited companies in which municipalities participate as shareholders (2022-05-20)	A municipality is a collection of a community of permanent residents, vested by law with the right of self-government, and its public authorities.

779. "Ministry of the Interior of the Republic of Lithuania", accessed August 10, 2023, https://vrm.lrv.lt/lt/veiklos-sritys/viesasis-administravimas/viesojo-sektoriaus-istaigu-tinklas.

2.2 Formulating and coordinating public policy on public administration

The Lithuanian Ministry of the Interior formulates state policy in the field of public administration and organises coordinates, and controls the implementation of this policy.

The public sector of the State in Lithuania consists of a set of public sector organisations at the central level of government, which are characterised by a variety of functions (both policy formulation and implementation, including the provision of public services to the population and other activities of public benefit) and legal forms (state budget institutions, public bodies, state-owned enterprises, (private) joint stock companies). Public sector organisations can be divided into key government institutions (ministries, departments), public sector agencies, public bodies, and state-owned enterprises.[780]

To ensure compliance with the principle of good governance, the Law on public administration of the Republic of Lithuania was adopted,[781] which established a framework for the activities of all entities with powers of public administration. Law on public administration of the Republic of Lithuania (LPA)[782] establishes the principles of public administration, the fields of public administration, the system of public administration entities and the bases for the organisation of administrative procedure; the basic provisions for the supervision of the activities of economic operators; guarantees the right of persons to appeal against actions, omissions or administrative decisions of public administration entities, as well as the right to a law-based and objective examination of requests and complaints from persons. The provisions of Chapters 2 and 3 of this Law shall apply to public administration entities performing functions in accordance with the procedure established by other laws, legal acts of the European Union or international treaties of the Republic of Lithuania, insofar as their activities in taking administrative decisions, providing administrative services, receiving and examining requests or complaints are not established by other laws, legal acts of the European Union or international treaties of the Republic of Lithuania regulating such activities.

According to the LPA,[783] the powers of public administration are:

- collegial or single-person state or municipal institutions, budgetary bodies having the organisational form of ministries, government bodies, other budgetary bodies accountable to the Government, bodies attached to ministries, budgetary bodies accountable to the Seimas, the Bank of Lithuania, the Lithuanian Armed Forces, and municipal administrations - in all the spheres of public administration referred to in Article 6 of the Public Administration Law.
- public bodies owned or part-owned by the State or a municipality - for administrative decision-making, the provision of administrative services, and the supervision of the implementation of, and compliance with, legislation and administrative decisions.
- for state and municipal enterprises – administrative decision-making, administrative services.
- Regional Development Councils – for administrative regulation, administrative decision-making, and the administration of public services.

780. OECD, "Organising the Central State Administration: Policies & Instruments", *SIGMA Papers*, 43 (2007), Lietuvos Respublikos vidaus reikalų ministerija su Vyriausybės strateginės analizės centru, *Viešojo sektoriaus ataskaita 2016–2019 m.* (Vilnius, 2020).
781. "Republic of Lithuania law on public administration 17 June 1999 No VIII-1234, new edition from 1 November 2020 No XIII-2987", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.83679/asr.
782. "Republic of Lithuania law on public administration 17 June 1999 No VIII-1234, new edition from 1 November 2020 No XIII-2987", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.83679/asr.
783. "Republic of Lithuania law on public administration 17 June 1999 No VIII-1234, new edition from 1 November 2020 No XIII-2987", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.83679/asr.

- associations operating under separate laws governing their activities - in all areas of public administration referred to in Article 6 of the Law on Public Administration.
- associations (other than associations operating under separate laws governing their activities) – for administrative decision-making, the provision of administrative services, and monitoring the implementation of and compliance with legislation and administrative decisions.
- for natural persons with special statutory status, in the areas of administrative decision-making, the provision of administrative services, and the supervision of the implementation of, and compliance with, legislation and administrative decisions.

Article 3 of the LPA states that the following principles shall guide the activities of public administration entities:

1. responsibility for decisions taken. This principle implies that a public administration entity, when carrying out administrative regulation or taking administrative decisions, must assume responsibility for the consequences of the administrative regulation or administrative decisions taken.
2. the prohibition of change for the worse (*non reformatio in peius*). This principle means that a public administration body may not, when adopting a decision in an administrative procedure, worsen the position of the person on whose application the administrative procedure was initiated.
3. efficiency. This principle means that, when taking and implementing decisions, a public administration body shall use the resources allocated to it at the lowest possible cost and with the best possible result.
4. the rule of law. This principle implies that the powers to carry out public administration must be conferred on public administration entities in accordance with the requirements laid down in this Law and that the activities of public administration entities must be in accordance with the legal bases set out in this Law. Administrative decisions relating to the exercise of the rights and obligations of individuals must in all cases be based on the law.
5. completeness. This principle means that the public administration body must respond to the request or complaint in a clear and reasoned manner, indicating all the circumstances that have influenced the examination of the request or complaint and the specific provisions of the legislation on which it has relied in assessing the content of the request or complaint.
6. equality of arms. This principle means that a public administration body, when taking administrative decisions, must take into account the fact that all persons are equal before the law and may not restrict or favour their rights on the basis of their sex, race, nationality, language, origin, social or property status, sexual orientation, education, religious or political opinions, type and nature of their activities, place of residence and other circumstances;
7. innovation and openness to change. This principle implies that a public administration entity should seek new and effective ways to better address the challenges of public administration and to continuously improve its performance through the application of cutting-edge methods, models, technologies, tools, or best practices.
8. non-abuse of power. This principle implies that public administration entities are prohibited to perform public administration functions without public administration powers granted in accordance with this Law or to take administrative decisions for purposes other than those established by law or other legal acts.

9. objectivity. This principle implies that the adoption of an administrative decision and other official actions of a public administration body must be impartial and objective.
10. proportionality. This principle implies that the scope of the administrative decision and the means of its implementation must be consistent with the necessary and reasonable objectives of the administration.
11. transparency. This principle implies that the activities of a public administration body must be public, except in cases provided for by law.
12. subsidiarity. This principle implies that decisions of public administration entities must be taken and implemented at the lowest level of the public administration system capable of ensuring efficiency.
13. single window. This principle means that a person is provided with information, a request or a complaint is received and answered at a single place of work. The public administration entity which examines the request or complaint and takes the administrative decision shall itself examine the request or complaint and obtain information from its administrative units, subordinate entities and, where appropriate, from other public administration entities, without being obliged to do so by the person who submitted the request or complaint.

The areas of public administration are regarded as:

- administrative regulation – the activities of public administration bodies in drafting laws and other regulatory legal acts and adopting regulatory administrative acts.

- administrative decision-making: the activities of public administration entities in drafting laws and other regulatory legal acts and adopting regulatory administrative acts.
- 'provision of administrative services' means the activities of a public administration entity, as defined in the Law on Public Administration, related to the issuance of documents or the provision of information.
- supervision of the implementation of and compliance with legal acts and administrative decisions.
- 'administration of public service provision' means the activities of public administration entities, as provided for by law, in establishing rules and procedures for the provision of public services, issuing authorisations for the provision of public services, establishing legal entities in the appropriate form, or selecting other persons to provide public services, and supervising the provision of public services.

Administrative services include:

- Services relating to the issue of documents required by law, the possession of which confirms the acquisition of a right conferred by a public administration body.
- Services relating to the action of a public administration entity in issuing documents required by law containing information held in public registers, public information systems, archives or by the public administration entity itself.
- Services relating to the receipt of documents or information required by law and provided by persons to public administration bodies.
- Services relating to the registration of information required by law in public registers or public information systems at the request of a person.

Public services activities carried out under the supervision of public administration entities, in accordance with the requirements laid down by law and/or by public administration entities, which create benefits guaranteed by the State or municipalities and equally accessible to members of the public.

Administration of the provision of public services - the activities of public administration entities, carried out in accordance with the procedures laid down by law, in establishing the rules and procedures for the provision of public services, in issuing authorisations for the provision of public services, in setting up legal entities in the appropriate form or in selecting other persons to provide public services, and in supervising the provision of public services.

Pursuant to Article 17(2) of the Law of the Republic of Lithuania on Strategic Management[784] and in the framework of the implementation of the National Progress Plan for the period 2021–2030, approved by the Resolution of the Government of the Republic of Lithuania No. 998 of 9 September 2020 On the Approval of the National Progress Plan for the period 2021–2030, the Government of the Republic of Lithuania approved the Public Governance Development Programme for the Ministry of Interior, the manager of the Development Programme, for 2022–2030.[785] Progress measures to address problems in public administration is:

- Reform the structure of public administration to optimise the scope of public functions and the rational distribution of public functions between national and local authorities.
- Improve the quality, accessibility, and delivery of administrative and public services.
- The integrated implementation of all these objectives will ensure a targeted, coherent, and coordinated improvement of public governance, covering all the key components of public governance - the structure of the public governance system, the functions of the institutions operating within it, the key processes of public governance, and the human resources - at all three levels of governance (state, regional and municipal).

2.3 Digital transformation of Lithuanian public governance

Today, we can observe changes in the forms of public service delivery, in the processes of policy formulation and decision-making, and in aspects of regulation and implementation. There is a focus on user-friendliness in public service delivery. In the area of policy formulation and decision-making, there has been a shift from decision-making in consultation with stakeholders to co-creation-based decisions. The potential of artificial intelligence is increasingly being exploited. At the level of regulation and implementation, there is a shift from long and rigid regulatory processes to dynamic and adaptive solutions. At the level of performance management, public organisations are integrating various functions and digitising their processes.[786]

784. "Republic of Lithuania law on Strategic Management 25 June 2020 No XIII-3096, new edition from 1 January 2022 No XIV-836", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/90386d20bab711ea9a12d0dada3ca61b/asr.
785. "Resolution No 206 of the Government of the Republic of Lithuania of 9 March 2022 "On approval of the public management development program of the Ministry of the Interior of the Republic of Lithuania, manager of the 2022–2030 development program", TAR, accessed August 10, 2023, https://www.e-tar.lt/portal/lt/legalAct/9ba13c90a4f911ec8d9390588bf2de65.
786. Žemyna Pauliukaitė-Gečienė and Ramunė Juozapaitienė, *Lietuvos viešojo valdymo skaitmeninė transformacija: politiniai ir technologiniai aspektai*)Vyriausybės strateginės analizės centras, 2021), https://strata.gov.lt › tyrimai › 2021-metai.

Promoting the digital transformation of governments remains a key priority for the European Union.[787] As part of the EU's Digital Decade ambition, Europe aims to deliver all essential public services online by 2030. Europe has developed a framework for more people-centred digital initiatives that respect European values, the Digital Rights and Principles Declaration.[788] The e-Government Benchmark compares how governments deliver digital public services across Europe. It has become an internationally recognised study that looks at how platforms for citizens, businesses, tourists and expat communities continue to improve.[789]

E-government is a cross-cutting public policy area that encompasses or is closely linked to other areas such as the development of the information society, public e-services, management of public information resources, e-signatures, ICT, and information technology security. The Strategy was adopted in 2010 – *A Digital Agenda for Europe*.[790] The European Commission stresses that eGovernment is first and foremost an element of public administration, and its development must therefore be focused on the application of IT to improve the public administration system, increase the accessibility and quality of public services, reduce costs, etc. The introduction of eGovernment improves the smoothness of administrative processes, the quality of services and the internal efficiency of the public sector. Digital public services reduce the administrative burden on businesses and citizens by making interactions with public administrations faster and more efficient, more convenient, more transparent and cheaper. In addition, the use of digital technologies, when integrated into strategies to modernise government, can have other economic and social benefits for society. Lithuania's strategic objectives in the digital transformation of public administration are influenced by the EU's digitisation policy. In 2021, the European Commission proposed a Digital Agenda for the European Union until 2030.[791] Ensuring that all essential public services are provided, and all medical records are available online, creating a secure and sustainable digital infrastructure.[792] By 2030, the EU framework should lead to the widespread adoption of trusted, user-controlled identities, allowing every citizen to control their own interactions and online presence. Consumers can easily and fully use online services across the EU while preserving their privacy. To be fully empowered, people should first have access to affordable, secure and high-quality connectivity, the opportunity to learn basic digital skills that should become a right for all, and other tools that together enable them to participate fully in the economic and social activities of today and tomorrow. They must also have easy access to digital public services based on a universal digital identity, as well as access to digital health services. In addition, the digital technologies and services used by people must comply with the applicable legal framework and respect the rights and values inherent in the "European way". In addition, a human-centred, safe and open digital environment should comply with the law, but also allow people to exercise their rights, such as privacy and data protection, freedom of expression, children's rights and consumer rights.[793]

---

787. eGovernment Benchmark 2022. Synchronising Digital Governments, Insight report, Written by Capgemini, Sogeti, IDC and Politecnico di Milano for the European Commission Directorate-General for Communications Networks, Content and Technology, July – 2022, European Commission B-1049 Brussels, (Luxembourg: Publications Office of the European Union, 2022).
788. "European Parliament, Council, European Commission.European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01)", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001.
789. eGovernment Benchmark 2022. Synchronising Digital Governments, Insight report, Written by Capgemini, Sogeti, IDC and Politecnico di Milano for the European Commission Directorate-General for Communications Networks, Content and Technology, July – 2022, European Commission B-1049 Brussels, (Luxembourg: Publications Office of the European Union, 2022).
790. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe, COM/2010/0245 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52010DC0245.
791. "European Commission. Proposal for a Decision of the European Parliament and of the Council establishing the 2030 Policy Programme "Path to the Digital Decade", COM(2021) 574 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0574.
792. Žemyna Pauliukaitė-Gečienė and Ramunė Juozapaitienė, *Lietuvos viešojo valdymo skaitmeninė transformacija: politiniai ir technologiniai aspektai*)Vyriausybės strateginės analizės centras, 2021), https://strata.gov.lt › tyrimai › 2021-metai.
793. "2030 digital compass. The European way for the digital decade", accessed August 10, 2023.

2.4 Electronic government gateways. Portal of Lithuanian administrative and public services[794]

In 2002, the Government of the Republic of Lithuania approved the e-Government Concept,[795] which set out the main objective of e-government – e-government aims to improve (using digital technologies) the provision of public services to state and municipal institutions and bodies, residents of the Republic of Lithuania, and business entities. At present, the conditions for the organisation of e-government are regulated by several legal acts.

Law on information society services of the Republic of Lithuania[796] regulates the provision of information society services and other activities of information society service providers. It defines an information system as a set of technical and software tools used to create, send, receive, store or otherwise process information electronically. Information society services' means services which are generally provided for remuneration by electronic means and at a distance at the request of an individual user of an information society service. The regulation of the provision of information society services and other activities of service providers shall be based on the principles of non-discrimination, technological neutrality, functional equivalence, freedom of contract, promotion of self-regulation, legal protection of personal data, consumer protection, proportionality, protection of intellectual property rights, objectivity, freedom of expression, legal certainty, and legitimate expectations.

Law on State Information Resources Management of the Republic of Lithuania[797] The objective is to ensure the proper development, management, operation, use, maintenance, interoperability, planning, financing, and security of the State's information resources. It has been defined that a state information system is a set of legal, organisational, technical and software tools for processing information necessary for a state institution (institutions) or a state body (bodies) to perform its statutory functions other than internal administration. State information resources' means the totality of the information managed by the institutions in the performance of their statutory functions, processed by means of information technology, and the information technology tools that process it. Resolution of the Government of the Republic of Lithuania *"On the use of the interoperability system of information systems of public administration institutions in the provision of public and administrative services in the electronic space"*[798] stipulates that ministries, government agencies of the Republic of Lithuania and other state institutions and bodies accountable to the Government of the Republic of Lithuania, bodies attached to ministries, and other state institutions and bodies subordinate to ministries, which administer public and administrative services in cyberspace, must, as of 1 March 2010, ensure the availability of these services through the portal of the system of interoperability of the information systems of public administration institutions. Provisions of the interoperability platform for public information resources[799] regulates the legal basis for the establishment of the State

794. "E-Government Gateway. Administrative and public e-services portal", accessed August 10, 2023, https://www.epaslaugos.lt/portal/.
795. "Resolution No 464 of the Government of the Republic of Lithuania of 13 May 2009 "On the Government of the Republic of Lithuania in 2004 April 28 resolution no. 488 "On approval of the strategy for the development of public administration until 2010" and 2002 December 31 resolution no. 2115 "On approval of the concept of electronic government" recognition as invalid", accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.344569?jfwid=10mfejburv.
796. "Republic of Lithuania law on information society services 25 May 2006 No X-614", TAR, accessed August 10, 2023, https://www.e-tar.lt/portal/lt/legalAct/TAR.8A719A97956F/asr.
797. "Republic of Lithuania law on State Information Resources Management 15 December 2011 No XI-1807", TAR, accessed August 10, 2023, https://www.e-tar.lt/portal/lt/legalAct/TAR.85C510BA700A/asr.
798. "Resolution No 1659 of the Government of the Republic of Lithuania of 16 December 2009 "On the use of the interoperability system of information systems of public administration institutions in the provision of public and administrative services in the electronic space", TAR, accessed August 10, 2023, https://www.e-tar.lt/portal/lt/legalAct/TAR.466BCE51694D/asr.
799. "Order No 4-886 of the Minister of Economy and Innovation of the Republic of Lithuania of 9 August 2021 "On regarding the modernization of the state information resources interoperability platform, the approval of the provisions of the state information resources interoperability platform and the data security provisions of the state information resources interoperability platform", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/99d5f6b2f94811ebb4af84e751d2e0c9?jfwid=12rj839ihb.

Information Resources Interoperability Platform (SIRIP), its purpose, objectives, tasks, functions, organisational, informational, and functional structure, procedures for the provision and use of data, data security requirements, financing, modernisation and liquidation. The objective of the VIISP is to provide a one-stop shop for natural and legal persons to access electronically the public and administrative services provided by the institutions referred to in the Law on the Management of State Information Resources, and to provide the institutions with the services referred to in that Law. Order of the Director of the Committee for Development of the Information Society under the Government of the Republic of Lithuania "On the approval of the rules for the functioning of the interoperability platform for state information resources"[800] regulates the procedure for the provision and administration of the services of the State Information Resources Interoperability Platform (VIISP), the rights and obligations of the VIISP manager, the users of the VIISP, the recipients of the VIISP services, the recipients of the data, the intermediary of the payment service, and the users of the VIISP self-service area. *General requirements for websites and mobile applications of state and municipal authorities and bodies* [801] Objective - to enable the public to access online all public information referred to in the Law of the Republic of Lithuania on the Right to Access to Information and the Re-use of Data about state and municipal institutions and bodies and other entities, their functions, draft laws and other regulatory legal acts and related legal information, to unify the institutions' websites, to ensure their efficiency, the relevance of the information they contain, their reliability, their searchability, the regular updating of the information, and the requirements of accessibility in terms of adaptation of the institution's website or mobile application.

Interoperability Platform for State Information Resources – consists of two main parts: the interoperability platform and the e-services portal "Electronic Government Gateway" (www.epaslaugos.lt), which is designed to provide a one-stop access to e-services in Lithuania for citizens, businesses and the public sector. Using information technology, public authorities are continuously updating the functionality and accessibility of e-services. The e-Government Gateway portal provides information and links to the most important public and administrative e-services available in Lithuania for citizens and businesses. The portal is designed to make it easier and more convenient for users to access the services, which are grouped by life cases and by service categories. The portal allows citizens to view the e-signed documents they have received (ADOC – electronically signed electronic document format. This format complies with the requirements of ADOC-V1.0, the Specification for Electronically Signed Electronic Documents, approved by the Lithuanian Department of Archives under the Government of the Republic of Lithuania), as well as to draw up and sign them with an e-signature (e.g., contracts, powers of attorney, etc.). To use e-services, users must authenticate their identity by logging in through one of the following channels: e-banking, electronic identification, or foreign identification (eIDAS). The Regulation is the basis for cross-border electronic identification, authentication, and trust services (eIDAS)[802] and website certification in the EU. The eIDAS Regulation is the basis for cross-border electronic identification, authentication, and trust services (eIDAS) and website certification in the EU.

800. "Order No T-228 of the Director of the Information Society Development Committee under the Government of the Republic of Lithuania of 1 December 2008 "On regarding the approval of the functioning rules of the state information resource interoperability platform", TAR, accessed August 10, 2023, https://www.e-tar.lt/portal/lt/legalAct/TAR.524ED597514C/asr.
801. "Resolution No 480 of the Government of the Republic of Lithuania of 18 April 2003 "On regarding the general requirements for the website and mobile applications of state and municipal institutions and bodies, the description of approval", new edition from 15 December 2018 No 1261, TAR, accessed August 10, 2023, https://www.e-tar.lt/portal/lt/legalAct/TAR.3FB3953EFFDC/asr.
802. "eIDAS Regulation", accessed August 10, 2023, https://digital-strategy.ec.europa.eu/en/policies/electronic-identification.

The Information Society Development Programme 2014–2020[803] "The Digital Agenda of the Republic of Lithuania" has been prepared because the development of the information society is a dynamic, fast-moving process in many spheres of the society and the state activities, affecting various spheres of the society's life and the sectors of the state economy. The purpose of the agenda is to set objectives and targets for the development of the information society to maximise and secure the use of information and communication technologies, in particular the Internet. The Programme has been prepared in the context of the European Commission's programming documents on the Digital Agenda for Europe.[804]

2.5 Information Society Development Outlook 2022[805]

2.5.1 Use of information technology by the population

According to the Lithuanian Statistics Department, in 2022, 80% of households will have personal computers at home and 88% will have internet access. In urban areas, 84% of households had personal computers at home and 90% had internet access, while in rural areas 73% and 84% had internet access. 88% of the population aged 16–74 used the internet in 2022. 100% of 16–24-year-olds used the internet, 57% of 65–74-year-olds. 82% of 16–74-year-olds used the internet daily. The main uses of the internet were information search, communication, leisure, and banking. For health-related purposes, 72% of the population aged 16–74 used the internet or mobile apps in 2022. 32% of the population aged 16–74 used the internet for learning, training, or self-education.

Developing public electronic services.[806] According to the data of the Lithuanian Statistics Department, 74% of the population aged 16–74, or 83% of internet users aged 16–74, used the electronic services of state institutions or other public service agencies at least once a year. According to a survey commissioned by the Committee for the Development of the Information Society in Q2 2022, 59% of the Lithuanian population visited the websites of public institutions and bodies in the last 12 months. The most frequent use of these websites is to search for information about a state institution or body, to use electronic public services provided by state institutions and bodies, to search for information about public services provided by state institutions and bodies and how to obtain them, to download applications and forms, and to search for information about employees and their contacts. The most popular e-services among the population are: income tax declarations (46%), health-related services (45%), car registration (20%), personal documents (20%) and job search.

According to the survey, 42% of the Lithuanian population visited the Electronic Government Gateway portal www.epaslaugos.lt . The most frequent reason for visiting the portal was to order or use an electronic service (66%). The majority of citizens who have visited the websites of public authorities in the last year (88%) reported that they have not experienced any security problems.

803. "Resolution No 244 of the Government of the Republic of Lithuania of 12 March 2014 "On regarding the approval of the 2014–2020 program "Digital Agenda of the Republic of Lithuania" for the development of the information society", new edition from 23 December 2017 No 1085", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/a66c0760b04011e3bf53dc70cf7669d9/asr?positionInSearchResults=7&searchModelUUID=43f2e906-984f-4050-a135-35248d34b76a.
804. For example, COM (2010) 245, COM (2012) 784, COM (2015) 192, COM(2016) 381, etc.
805. "Informacinės visuomenės plėtros 2022 m. apžvalga", accessed August 10, 2023, http://statistika.ivpk.lt/ataskaitos.
806. "Informacinės visuomenės plėtros 2022 m. apžvalga", accessed August 10, 2023, http://statistika.ivpk.lt/ataskaitos.

2.5.2 Use of information technology in enterprises[807]

According to the Lithuanian Statistics Department, 3.8% of companies used industrial or service robots at the beginning of 2022. In 2022, 38.3% of companies held remote meetings, 16.7% of companies had IT security rules for holding remote meetings online and 12.4% of companies had rules giving priority to remote meetings online. In 2022, 17.2% of companies had IT specialists.

2.5.3 Use of information technology in state and municipal institutions and bodies [808]

According to a survey conducted by the Lithuanian Statistics Department in early 2022, 47.2% of state and municipal institutions and bodies provide level 4 electronic services online, i.e., they are able to fully participate in the processes via the website, applications, case management, decision-making and other standard procedures are carried out via the website, and the applicant does not need to undergo any other formal "paper" procedures. And as many as 21.5% of the institutions provide Level 5 electronic services online, i.e., automatic provision of available information. At the beginning of 2022, 77.1% of offices made various forms available for download and 50.7% returned completed forms. 47.2% of the institutions indicated that they provide part of their services electronically. At the beginning of 2022, 61.5% of the institutions provided services via the electronic government gateway, 100% via email, 53.8% provided information services via social networks, 11.8% via internet phone connection and 8.7% via mobile applications. Information technology (IT) professionals accounted for 2.4% of all state and municipal institutions.

According to the United Nations Electronic Government Development Index (EGDI), Lithuania was ranked 24th out of 193 countries in the world in 2022.

The effectiveness of Lithuania's digitisation policy and the potential for digitisation development is indicated by the Digital Economy and Society Index (DESI). Over the last five years, Lithuania's position is in line with the EU average and, according to the DESI for 2020, Lithuania ranks 14th among EU countries with a score of 53.9. This compares with an EU average of 52.6 points. Lithuania's high level of digital security provides the preconditions for a successful digital transformation. Rapid technological development creates not only opportunities but also threats, which is why the focus is on the areas of legal regulation and national security. The State's vision for mitigating the potential negative impact of the opportunities offered by technology is defined in the Cybersecurity Strategy. The European Commission has published new results from the Digital Economy and Society Index (DESI), which show progress in digital competitiveness in the areas of human capital, broadband, the integration of digital technologies in enterprises and digital public services. In the report published by the Portulans Institute, which publishes the Networked Readiness Index (NRI), which assesses the ability of countries to exploit the potential of ICT, Lithuania is ranked 33rd out of 131 countries in the world in 2022, with a score of 62.78 points. According to the DESI, Lithuania ranks 14th out of 27 countries with a score of 52.7 in 2022.

Lithuania is ranked 3rd in the world in the cybersecurity component of the Digital Quality of Life Index, and therefore has excellent opportunities to implement a successful digitalisation policy by improving the efficiency of public governance and the data protection legal framework. The performance of the public sector in digitisation can be compared internationally through the results of the Digital Government Index (DGI). In 2019, Lithuania was ranked 27th among 33

807. "Informacinės visuomenės plėtros 2022 m. apžvalga", accessed August 10, 2023, http://statistika.ivpk.lt/ataskaitos.
808. "Informacinės visuomenės plėtros 2022 m. apžvalga", accessed August 10, 2023, http://statistika.ivpk.lt/ataskaitos.

countries in this index. In summary, Lithuania's progress in the digital transformation process is evident, but a successful digital transformation of public governance as a complex and long-term process requires strengthening the components of data openness, skills, and citizen engagement, as well as the further development of the cybersecurity domain, which creates the prerequisites for sustained progress in.[809]

In the European e-Government Scoreboard, a survey of 36 countries, Lithuania was among the top-ranked countries. Lithuania, along with Malta, Estonia, Finland, and Denmark, was ranked in the top five as the most technologically advanced country in terms of public e-services. Lithuania was among the leaders in the ranking of electronic services accessible via an eID. Lithuania also scored high in e-government transparency. Public e-services are assessed based on 4 main aspects: user-orientation, transparency, technical adaptability of e-services and cross-border provision of e-services.

Lithuania can be said to have made significant progress both in terms of technological level and digital maturity. The assessment of Lithuania's position in international digitisation indices shows that, compared to other countries, Lithuania is in a strong position in terms of progress in the digitisation of public services, the quality of digital life, is a leader in the field of GovTech, and has a high level of cybersecurity. However, a successful digital transformation of public governance, as a complex and long-term process, requires the strengthening of the components of data openness, skills, and citizen involvement, as well as further development of the cyber security area, which creates the preconditions for sustainable progress. The analysis of strategic documents has shown that in public governance, Lithuania aims to.[810]

3. Lithuania's legal framework for public administration with a focus on the relevant parts of national constitution and the human rights.

European principles of good administration are relevant not only for the Member States of the European Union, but also for all the Council of Europe countries, in defining the activities of public administration in their domestic law.

The development of the public administration sector is directly linked to public policy priorities and demographic changes, the best practices of international organisations (European Union, Organisation for Economic Development and Cooperation) and their member states, advances in information technology and other factors. The governance of the State and the real functioning of government decisions are inseparable from the activities of public administration institutions in the field of administrative regulation, which includes the adoption of normative administrative acts to implement laws and other legal acts. Regulatory administrative acts lay down generally binding rules of conduct of a general nature (a specific pattern of behaviour of the participants in the regulated legal relations) relevant to a particular area of State or municipal governance, which are necessary for the implementation of the rights conferred by laws or other legal acts or the fulfilment of the obligations imposed; such an act essentially lays down the procedure and conditions for the implementation of a particular law or other legal act.[811]

809. Žemyna Pauliukaitė-Gečienė and Ramunė Juozapaitienė, *Lietuvos viešojo valdymo skaitmeninė transformacija: politiniai ir technologiniai aspektai*)Vyriausybės strateginės analizės centras, 2021), https://strata.gov.lt › tyrimai › 2021-metai.
810. Žemyna Pauliukaitė-Gečienė and Ramunė Juozapaitienė, *Lietuvos viešojo valdymo skaitmeninė transformacija: politiniai ir technologiniai aspektai*)Vyriausybės strateginės analizės centras, 2021), https://strata.gov.lt › tyrimai › 2021-metai.
811. „Lietuvos vyriausiojo administracinio teismo praktikos, taikant teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatymo normas, apibendrinimas", accessed August 10, 2023, https://www.lvat.lt/veikla/teismu-praktika/teismu-praktikos-apibendrinimai/206.

In the Republic of Lithuania, the development of law, including administrative law, is inseparable from the processes of Europeanisation of law.[812] The application and interpretation of the Charter of Fundamental Rights of the European Union,[813] including at the national level, has been repeatedly studied by Lithuanian legal scholars.[814] The implementation of the principles enshrined in the Charter in the system of administrative law, as well as the impact of the right to good administration on the Lithuanian legal system, have also been the subject of research.[815] The provisions of Article 41 of the Charter (Right to good administration) are inextricably linked to the provisions of Article 47 of the Charter (Right to an effective remedy and a fair trial), which are designed to regulate the right to an effective remedy and to a fair trial. While the right to good administration under Article 41 of the Charter relates specifically to the relationship between individuals and the institutions of the European Union, the obligations of the national authorities of the Member States are often defined accordingly. The relationship between the principle of responsible governance and the principle of good administration is established in the Lithuanian legal system. The Constitutional Court of Lithuania has stated that the Constitution of Lithuania[816] the principle of responsible governance requires all state institutions and officials to exercise their functions in accordance with the Constitution, and the law, in the interests of the people and the State of Lithuania, and to exercise properly the powers conferred on them by the Constitution and the law.[817] It is possible to analyse the legal framework in Lithuanian national law in relation to the right to good administration enshrined in Article 41 of the Charter.

Lithuanian public administration legislation:

- Law on public administration of the Republic of Lithuania.[818]
- Law on the Government of the Republic of Lithuania.[819]
- Rules for examining requests and complaints of individuals in public administration entities.[820]
- Regarding the approval of the model administrative structure of the ministry and the model institution under the administrative structure of the ministry.[821]

812. Ingrida Danėlienė and Ieva Saudargaitė, „Europos Sąjungos Pagrindinių teisių chartijoje įtvirtinta teisė į gerą administravimą", *Teisė*, 99 (2016): 92–109.
813. "Charter of Fundamental Rights of the European Union, (2012/C 326/02), 26.10.2012", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
814. For example, Allan Rosas, "When is the EU Charter of Fundamental Rights Applicable at National Level?", *Jurisprudence*, 19, 4 (2012): 1269–1288; Skirgailė Žaltauskgitė-Žalimienė, "Interpretation and Application of the European Union Charter of Fundamental Rights". From *Žmogus, teisinė valstybė ir administracinė justicija: Mokslo studija, skirta Lietuvos vyriausiojo administracinio teismo dešimtmečiui* (Vilnius, 2012), 543–573; Inga Jablonskaitė-Martinaitienė and Salvija Kavalnė, „Europos Sąjungos pagrindinių teisių chartija Teisingumo Teismo praktikoje po Lisabonos sutarties įsigaliojimo: bendros tendencijos ir ateities perspektyvos". From *Žmogus, teisinė valstybė ir administracinė justicija: Mokslo studija, skirta Lietuvos vyriausiojo administracinio teismo dešimtmečiui* (Vilnius, 2012), 212–236.
815. Jurgita Paužaitė-Kulvinskienė, „Atsakingo valdymo principas bei jo procesinės garantijos", from *Administraciniai teismai Lietuvoje. Nūdienos iššūkiai*: kolektyvinė monografija (Vilnius: Lietuvos vyriausiasis administracinis teismas, 2010), 228–243; Ingrida Danėlienė, "The Right to Good Administration: the Impact of European Union Law on the Development of the Principles of Lithuanian Administrative Law", from *Žmogus, teisinė valstybė ir administracinė justicija*: Mokslo studija, skirta Lietuvos vyriausiojo administracinio teismo dešimtmečiui (Vilnius, 2012), 431–452.
816. "Constitution of the Republic of Lithuania", accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=rivwzvpvg&documentId=TAIS.211295&category=TAD.
817. Lietuvos Konstitucinio Teismo 2012 m. spalio 26 d., 2012 m. lapkričio 10 d. išvados, 2014 m. gegužės 27 d., 2014 m. liepos 11 d., 2015 m. lapkričio 19 d. nutarimai.
818. "Republic of Lithuania law on public administration 17 June 1999 No VIII-1234, new edition from 1 November 2020 No XIII-2987", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.83679/asr.
819. "Republic of Lithuania law on the Government 19 May 1994 No I-464, new edition from 28 April 1998 No VIII-717", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.5807/asr.
820. "Resolution No 875 of the Government of the Republic of Lithuania of 22 August 2007 "On the approval of the rules for handling requests and complaints of individuals in public administration entities", new edition from 7 December 2021 No 1014", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.303479/asr.
821. "Resolution No 1043 of the Government of the Republic of Lithuania of 17 October 2018 "On approval of the model administrative structure of the ministry and the model institution attached to the administrative structure of the ministry", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3169bfa4d60311e8a3fadd00a256c61a?jfwid=ppvfz0i5o.

- Guidelines for improving the system of public sector institutions.[822]
- Methodology for reviewing the functions of institutions accountable to the government.[823]
- Recommendations for the preparation of regulations of ministries, government institutions, institutions attached to ministries.[824]
- Description of the procedure for drawing up descriptions of public and administrative services.[825]
- Regulations of the information system for monitoring and analysing public and administrative services.[826]
- Methodology for identifying and assessing administrative burdens on citizens and other persons.[827]
- Methodology for calculating the public service user satisfaction index.[828]

Article 5 of the ***Law on public administration of the Republic of Lithuania*** (LPA)[829] states that public administration powers may be conferred by law, a directly applicable legal act of the European Union, a ratified international treaty of the Republic of Lithuania, a legal act adopted by a state authority or a council of a municipality, a resolution of the Government adopted to implement the provisions of the law, a directly applicable legal act of the European Union or a ratified international treaty of the Republic of Lithuania, etc.

Article 3 of the Republic of Lithuania Law on the Government[830] stipulates that the Government shall be guided in its activities by the Constitution of the Republic of Lithuania, the international treaties of the Republic of Lithuania, laws, the Government Programme, other legal acts, and shall coordinate its activities with the State Progress Strategy

Rules for examining requests and complaints of individuals in public administration entities[831] regulate the examination of requests and complaints and the treatment of individuals in public administration entities, as well as in entities that provide public services and deal with requests and complaints concerning these public services. The provisions of the Rules shall apply to the

822. "Resolution No 8615 of the Government of the Republic of Lithuania of 29 May 2018 "On the approval of the guidelines for the improvement of the system of public sector institutions and the action plan for the implementation of the guidelines for the improvement of the system of public sector institutions", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/e2db3340632b11e8b7d2b2d2ca774092/asr.
823. "Resolution No 968 of the Government of the Republic of Lithuania of 27 August 2011 "On approval of the methodology for reviewing the functions of institutions accountable to the Government of the Republic of Lithuania", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.405024/asr.
824. "Order No IV-15 of the Minister of Internal Affairs of the Republic of Lithuania of 18 January 2007 "On the approval of recommendations for the preparation of regulations of ministries, government institutions, institutions attached to ministries", new edition from 20 May 2020 No 1V-478", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.291559/asr.
825. "Order No IV-644 of the Minister of Internal Affairs of the Republic of Lithuania of 1 December 2009 "On approval of the description of the procedure for the preparation of descriptions of the provision of public and administrative services", new edition from 13 July 2017 No 1V-497", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.360388/asr.
826. "Order No IV-272 of the Minister of Internal Affairs of the Republic of Lithuania of 8 April 2016 "On the establishment of the information system for monitoring and analysis of public and administrative services and the approval of the provisions of the information system for monitoring and analysis of public and administrative services and data security provisions", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/fb4b5bc0fdc611e5bf4ee4a6d3cdb874/asr.
827. "Resolution No 213 of the Government of the Republic of Lithuania of 23 February 2011 "On the approval of the methodology for determining and evaluating the administrative burden on citizens and other persons", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.393064?jfwid=92zt7sdvu.
828. "Order No IV-339 of the Minister of Internal Affairs of the Republic of Lithuania of 30 June 2009 "On the approval of the methodology for calculating the satisfaction index of public services users", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.393064?jfwid=92zt7sdvu.
829. "Republic of Lithuania law on public administration 17 June 1999 No VIII-1234, new edition from 1 November 2020 No XIII-2987", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.83679/asr.
830. "Republic of Lithuania law on the Government 19 May 1994 No I-464, new edition from 28 April 1998 No VIII-717", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.5807/asr.
831. "Resolution No 875 of the Government of the Republic of Lithuania of 22 August 2007 "On the approval of the rules for handling requests and complaints of individuals in public administration entities", new edition from 7 December 2021 No 1014", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.303479/asr.

examination of requests and complaints from individuals and to the servicing of individuals in the institutions insofar as those legal relations are not regulated by laws, directly applicable legal acts of the European Union, international treaties of the Republic of Lithuania, or legal acts adopted based on such treaties. Provisions which are not laid down in laws, directly applicable legal acts of the European Union, but which are necessary for the smooth processing of requests and complaints from persons may be regulated by an internal administrative act adopted by the head of the institution. The wording 'electronic means of communication' used in the Rules includes the information technologies chosen and used by the institution for its public communications or for the service of persons. Rules for examining requests and complaints of individuals in public administration entities regulate the examination of requests and complaints and the treatment of individuals in public administration entities, as well as in entities that provide public services and deal with requests and complaints concerning these public services. The provisions of the Rules shall apply to the examination of requests and complaints from individuals and to the servicing of individuals in the institutions insofar as those legal relations are not regulated by laws, directly applicable legal acts of the European Union, international treaties of the Republic of Lithuania, or legal acts adopted on the basis of such treaties. Provisions which are not laid down in laws, directly applicable legal acts of the European Union, but which are necessary for the smooth processing of requests and complaints from persons may be regulated by an internal administrative act adopted by the head of the institution. The wording 'electronic means of communication' used in the Rules includes the information technologies chosen and used by the institution for its public communications or for the service of persons. Other terms used in the Rules are defined in Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market,[832] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,[833] the Postal Law of the Republic of Lithuania, the Law on the right to obtain information and data re-use of the Republic of Lithuania, the Law on the Civil Service of the Republic of Lithuania, and the Law on public administration of the Republic of Lithuania. In the cases provided for in the Rules, the protection of personal data shall be ensured in accordance with the provisions of Regulation (EU) 2016/679.

Guidelines for the drafting of regulations for ministries, government bodies and bodies attached to ministries[834] are functions specific to ministries, related to the purpose of the ministry as set out in the Law on the Government and contributing equally to the achievement of all the ministry's objectives, but not set out in any other legal acts (to prepare planning documents for the spheres of governance entrusted to the minister, to organise, coordinate and control their implementation; to prepare drafts of legal acts adopted by the Seimas of the Republic of Lithuania, Government decrees, decisions and resolutions, and other legal acts on issues within the ministry's remit, and to coordinate/organise their implementation; to transpose into national law and implement the European Union acquis, etc.)) are set out after the objectives of the Ministry.

832. "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32014R0910.
833. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.
834. "Order No IV-15 of the Minister of Internal Affairs of the Republic of Lithuania of 18 January 2007 "On the approval of recommendations for the preparation of regulations of ministries, government institutions, institutions attached to ministries", new edition from 20 May 2020 No 1V-478", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.291559/asr.

Description of the procedure for drawing up descriptions of public and administrative services[835] lays down the general requirements for the identification, grouping, structuring, and drafting of the description of the provision of a public and administrative service, its completion in the Public and Administrative Services Monitoring and Analysis Information System (PASIS) and its approval and publication. PASIS is an IS for monitoring and analysis of public and administrative services, which collects data on public and administrative services (descriptions of the provision of services and their monitoring indicators) and publishes them in the online portal "Catalogue of Lithuanian Services". The descriptions of administrative services in PASIS are filled in by public administration entities that provide administrative services to individuals. PASIS shall contain descriptions of all administrative services provided by the institution and of the public services they administer and provide.

Regulations of the information system for monitoring and analysing public and administrative services[836] establishes the legal basis, purpose, objectives and functions of the Public and Administrative Services Monitoring and Analysis Information System (PASIS), the organisational, informational and functional structure of PASIS, the procedures for the provision and use of PASIS data, the data security requirements of PASIS, the financing, upgrading and decommissioning of PASIS, and other information related to PASIS. Legal basis for the establishment of PASIS – Republic of Lithuania law on public administration[837] Article 17^1 of the Provisions of the Ministry of the Interior of the Republic of Lithuania, approved by Resolution No 291 of the Government of the Republic of Lithuania of 14 March 2001 "On the Approval of the Provisions of the Ministry of the Interior of the Republic of Lithuania". PASIS shall be established and maintained in accordance with the following legal acts:

- Law on State Information Resources Management of the Republic of Lithuania;[838]
- Law on public administration of the Republic of Lithuania;[839]
- Law on Local Self-Government of the Republic of Lithuania;[840]
- Law on Legal Protection of Personal Data of the Republic of Lithuania.
- Description of the Procedure for the Establishment, Creation, Modernisation and Liquidation of State Information Systems, approved by the Resolution of the Government of the Republic of Lithuania No 180 of 27 February 2013 "On the Approval of the Description of the Procedure for the Establishment, Creation, Modernisation and Liquidation of State Information Systems";
- Technical requirements for electronic information security of state registers (cadastres), departmental registers, state information systems and other information systems, approved by the Order of the Minister of the Interior of the Republic of Lithuania of 4 October 2013 No. 1V-832 "On the Approval of the Technical Requirements for the Electronic Information Security of State Registers (Cadastres), Departmental Registers, State Information Systems and other Information Systems".

---

835. "Order No IV-644 of the Minister of Internal Affairs of the Republic of Lithuania of 1 December 2009 "On approval of the description of the procedure for the preparation of descriptions of the provision of public and administrative services", new edition from 13 July 2017 No 1V-497", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.360388/asr.
836. "Order No IV-272 of the Minister of Internal Affairs of the Republic of Lithuania of 8 April 2016 "On the establishment of the information system for monitoring and analysis of public and administrative services and the approval of the provisions of the information system for monitoring and analysis of public and administrative services and data security provisions", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/fb4b5bc0fdc611e5bf4ee4a6d3cdb874/asr.
837. "Republic of Lithuania law on public administration 17 June 1999 No VIII-1234, new edition from 1 November 2020 No XIII-2987", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.83679/asr.
838. "Republic of Lithuania law on State Information Resources Management 15 December 2011 No XI-1807", TAR, accessed August 10, 2023, https://www.e-tar.lt/portal/lt/legalAct/TAR.85C510BA700A/asr.
839. "Republic of Lithuania law on public administration 17 June 1999 No VIII-1234, new edition from 1 November 2020 No XIII-2987", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.83679/asr.
840. "Republic of Lithuania law on the Local Self-Government 7 July 1994 No I-533, new edition from 1 April 2023 No XIV-1268", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.5884/asr.

- the description of the procedure for drawing up descriptions of the provision of public and administrative services approved by the Minister of the Interior of the Republic of Lithuania.[841]

The aim of PASIS is to collect and compile descriptions of public and administrative services provided and/or administered by public administration entities, information on indicators for monitoring the provision of services, and to enable searches of services and descriptions of service provision in the public catalogue by means of information technologies in an efficient and centralised manner. PASIS tasks: to collect and compile Service Profiles in an automated way, PASIS functions: to manage Service Profiles and data on Services and Indicators; to analyse data on Services and Indicators; to produce reports on Services, Service Profiles and Indicators, as well as other reports; to publish and make searchable the data on Services, Service Profiles, Indicators and other data on Service monitoring. The Ministry of the Interior is the controller of PASIS, and therefore the controller of personal data.

It is important to stress that the right to good administration is not enshrined as a separate subjective right in national administrative law, nor is the principle of good administration. The Republic of Lithuania law on public administration establishes the principles of public administration, the areas of public administration, the system of public administration entities and the basis for the organisation of administrative procedures, and guarantees the right of persons to appeal against actions, omissions or administrative decisions of public administration entities, as well as the right to a lawful and objective examination of requests, complaints and reports from persons. The law establishes the rights and obligations of a person participating in an administrative procedure, which are essentially equivalent in content to the procedural rights that form the content of the standard of good administration enshrined in Article 41 of the Charter.[842] The Charter is a source of law in the Lithuanian legal system. The jurisprudence of the Constitutional Court of Lithuania also refers to the provisions of the Charter.[843] Lithuanian legal scholarship recognises that administrative courts apply the Charter directly in certain cases, rather than simply relying on it as a source of interpretation. The provisions of the Charter, including those enshrining the right to good administration, are recognised as an important source for the interpretation of law. The case-law of the administrative courts confirms that the provisions of the Charter, including Article 41 thereof, undoubtedly constitute a source of interpretation of the law for the protection of the subjective rights of individuals who have been infringed, not only in the case of rights the exercise of which is intrinsically linked in one way or another to the legal rules laid down by European Union legislation, but also in the case of subjective rights which are derived exclusively from provisions of national law.[844]

Public administration directly influences the attitudes of citizens and other stakeholders towards the state, determines their trust in it, and shapes an active and aware society. Good administration and the search for an open, coherent, accountable, transparent, efficient, and citizen-oriented European public administration culture are currently receiving a great deal of attention.[845]

---

841. "Order No IV-644 of the Minister of Internal Affairs of the Republic of Lithuania of 1 December 2009 "On approval of the description of the procedure for the preparation of descriptions of the provision of public and administrative services", new edition from 13 July 2017 No 1V-497", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.360388/asr.
842. Ingrida Danėlienė and Ieva Saudargaitė, „Europos Sąjungos Pagrindinių teisių chartijoje įtvirtinta teisė į gerą administravimą", *Teisė*, 99 (2016): 92–109.
843. Lietuvos Konstitucinio Teismo 2015 m. gegužės 26 d. nutarimas.
844. Skirgailė Žaltauskaitė-Žalimienė, „Interpretation and Application of the European Union Charter of Fundamental Rights". From *Žmogus, teisinė valstybė ir administracinė justicija*: Mokslo studija, skirta Lietuvos vyriausiojo administracinio teismo dešimtmečiui (Vilnius, 2012), 543–573.
845. „Lietuvos vyriausiojo administracinio teismo praktika, taikant Lietuvos Respublikos viešojo administravimo įstatymo normas. Pritarta Lietuvos vyriausiojo administracinio teismo teisėjų 2016 m. birželio 1 d. pasitarime", accessed August 10, 2023, https://www.lvat.lt.

The European Convention on Human Rights[846] and the jurisprudence of the European Court of Human Rights play an important role as a source of good administration principles. To ensure the right of individuals to obtain information from state and municipal institutions and bodies, the Law of the Republic of Lithuania on the Right of Access to Information and Re-use of Data was adopted on 11 January 2000.[847]

At the constitutional level, the human right to receive information is established by Article 25 of the Constitution of the Republic of Lithuania. According to this Article, a person shall not be prevented from seeking, receiving and disseminating information (para. 2); the freedom to receive and disseminate information shall not be restricted except by law, if necessary to protect a person's health, honour and dignity, private life, morals or to defend the constitutional order (para. 3); a citizen shall have the right to receive, in accordance with the procedure laid down by law, the information about him or her that is in the possession of the State bodies (para. 5). These provisions are inseparable from the general principle enshrined in the Constitution that public authorities serve the people (Article 5(3) of the Constitution). The Constitutional Court of the Republic of Lithuania, interpreting the above-mentioned constitutional provisions, has consistently stated that the constitutional freedom to seek, receive and disseminate information unhindered is one of the foundations of an open, just, harmonious civil society and a democratic state, and that the Constitution guarantees and protects the public's interest to be informed (see the Constitutional Court's Opinion of 23 October 2002 on the Constitution, No, The Constitutional Court's decision of 23 October 2002, the Constitutional Court's decision of 4 March 2003, the Constitutional Court's decision of 26 January 2004, the Constitutional Court's decision of 8 July 2005, the Constitutional Court's decision of 19 September 2005, the Constitutional Court's decision of 29 September 2005, the Constitutional Court's decision of 21 December 2006, and the Constitutional Court's decision of 17 November 2011) The constitutional right to access information is an important prerequisite for the exercise of various personal rights and freedoms enshrined in the Constitution (Resolution of the Constitutional Court of 21 December 2006). The Constitutional Court has noted that the exercise of human rights and freedoms and the safeguarding of other constitutional values depend to a large extent on the access to and use of information from various sources (Resolution of 29 September 2005). The Constitutional Court has repeatedly stated in its acts that the freedom of information is not absolute, and that the Constitution does not allow for the establishment of a legal regulation which, by establishing guarantees for the implementation of the freedom of information by law, would create preconditions for the violation of other constitutional values and their balance (e.g., Resolution of the Constitutional Court dated 15 May 2007). The Constitution provides for the possibility to restrict the freedom of information if it is necessary to protect human health, honour and dignity, private life, morality or to defend the constitutional order, i.e. if the restrictions on the freedom of information are aimed at protecting, defending the values referred to in Article 25(3) of the Constitution, the list of which (contained in the Article 25(3) of the Constitution) as in its 2005 The list of constitutional values listed in Article 25(3) of the Constitution, as stated by the Constitutional Court in its rulings of 19 September 2005 and 29 September 2005, cannot be regarded as exhaustive, and therefore does not allow for the restriction of the freedom to receive and disseminate information where it is necessary to protect other constitutional values not expressly mentioned in Article 25(3) of the Constitution. The Law of the Republic of Lithuania on the Right to Obtain Information from State and Municipal Institutions and Bodies regulates in detail the legal relations concerning the right of a person to

846. "European Convention on Human Rights as amended by Protocols Nos. 11, 14 and 15 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16", accessed August 10, 2023, https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c.
847. "Republic of Lithuania law on the right to receive information and data reuse 11 January 2000 No VIII-1524, new edition from 17 July 2021 No XIV-491", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.94745/asr.

obtain information from state and municipal institutions and bodies. Article 1(1) of this Law stipulates that this Law guarantees the right of persons to obtain information from state and municipal institutions and bodies, establishes the procedure for the exercise of this right, and regulates the actions of state and municipal institutions and bodies in the provision of information to persons. The Law on the Right to Information implements both the right to obtain information on a person held by public bodies in relation to the performance of public administration functions, as laid down in Article 25(5) of the Constitution, and aims to create favourable conditions for persons to obtain information held by state and municipal institutions and bodies and to use it for commercial or non-commercial purposes. Article 3(1) of the Law on Access to Information stipulates that institutions are obliged to provide information to applicants. Refusal to provide information may be made in accordance with the procedure laid down in this Law. In addition, this Law implements Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. [848]

The Preamble to the Constitution of the Republic of Lithuania proclaims the aspiration for an open, just, and harmonious civil society and the rule of law (inter alia, the Constitutional Court of the Republic of Lithuania, 9 December 1998, 18 October 2000). The Constitutional Court has repeatedly stated that the constitutional principle of the rule of law is a universal principle which underpins the entire Lithuanian legal system and the Constitution itself. The constitutional principle of the rule of law implies, among other things, that human rights and freedoms must be guaranteed, that all State authorities and other State institutions exercising State power must act in accordance with the law and in obedience to the law, that the Constitution has the supreme legal force, and that laws, government resolutions and other legal acts must comply with the Constitution (inter alia, the Constitutional Court's Resolution of 23 February 2000). Inherent in the constitutional principle of the rule of law are also the imperatives, enshrined in Article 5 of the Constitution, that the powers of the authorities are limited by the Constitution and that the authorities are at the service of the people, as well as the constitutional principle of responsible government, which implies that state institutions and officials must exercise their functions in accordance with the Constitution and the law, in the interests of the Nation and the State of Lithuania, and in the proper exercise of the powers granted to them by the Constitution and the law (inter alia, the finding of the Constitutional Court on 26 October 2012). These fundamental constitutional imperatives and the various requirements they imply for legislative acts are also applicable to public administrations when they carry out administrative regulation. When adopting normative administrative acts, public administrative authorities must act within the limits of the competence defined in the legal acts governing their activities, respect the hierarchy of legal acts, the procedures for adopting and promulgating a legal act, and ensure that normative administrative acts comply with the Constitution and the principles and other requirements laid down in the Constitution and in the laws (inter alia, the Law on Public Administration). The legality of legal acts is one of the conditions for a person's confidence in the State and the law. Laws may not contradict the Constitution, and by-laws may not contradict the Constitution and laws. The principle of the legality of regulatory administrative acts is implemented through the institution of administrative justice. The Law on Administrative Proceedings of the Republic of Lithuania establishes the competence of administrative courts to hear normative administrative cases, i.e. to investigate the conformity of a specific normative administrative act (or part of a normative administrative act) with a higher-ranking legal act (or part of a legal act). After the legality review, the administrative court may declare that the examined normative administrative act (or a part thereof) is lawful or declare that it is contrary

848. "Lietuvos vyriausiojo administracinio teismo praktikos, taikant teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatymo normas, apibendrinimas", accessed August 10, 2023, https://www.lvat.lt/veikla/teismu-praktika/teismu-praktikos-apibendrinimai/206.

to the law or a normative legal act of the Government of the Republic of Lithuania (Article 117(1) of the Law on Administrative Proceedings). An important consequence of the declaration of unlawfulness of a normative administrative act is that the normative administrative act (or part thereof) may not, generally, be applied as from the date on which the final decision of the administrative court declaring the normative administrative act (or part thereof) to be unlawful has been published officially (Article 118(1) of the Law on Administrative Proceedings).[849]

4. The current Lithuanian administrative law system in terms of the content of the values of democracy and the rule of law, trust in public administration and respect for citizens' rights

Across Europe, the demand for justice is growing, increasing the workload of the judiciary and necessitating a constant re-engineering of working methods in an often-difficult budgetary environment. The development of e-Justice is one of the most important aspects of the modernisation of judicial systems. The introduction of information and communication technologies in the administration of the judiciary provides an opportunity to find ways to improve the functioning of the justice system, rationalise legal procedures and reduce costs. The development of information dissemination processes using modern electronic means is undoubtedly important for law enforcement and the judicial system. The European e-Justice Strategy is designed to create a European judicial area using information and communication technologies. The main objective of e-Justice is to make justice across Europe more efficient and more useful for citizens. From a technical point of view, e-Justice is aligned with the broader e-Government system.[850] The European e-Justice system is implemented in the European e-Justice portal (https://e-justice.europa.eu/).

The fair and efficient resolution of disputes arising in the field of public administration is usually ensured by specialised courts, namely administrative district courts and the Supreme Administrative Court of Lithuania. The procedure for handling disputes before these courts is regulated by the Law on Administrative Proceedings of the Republic of Lithuania (the APL). It should be noted that the Administrative Court decides on disputes concerning law in the field of public administration. The court does not assess the contested administrative act and action (or inaction) from the point of view of political or economic expediency, but only determines whether in a particular case a law or other legal act has been violated, whether the administrative entity has not exceeded its competence, and whether the act (action) is in accordance with the objectives and tasks for which the institution was established and for which it was given the relevant powers (Art. 3 of the APL).[851]

Each entity of the public administration system, in carrying out the functions assigned to it, is guided not only by the general Law on Public Administration but also by the special laws regulating the sphere of public administration in which it has been given the competence to carry out public administration, as well as by the sub-statutory acts related to the implementation of these laws (such as, for example, the Law of the Republic of Lithuania on Local Self-government, the Law on the State Civil Service;[852] Law on tax administration of the Republic of

849. "Lietuvos vyriausiojo administracinio teismo praktikos, aiškinant ir taikant norminių administracinių aktų teisėtumo tyrimą reglamentuojančias teisenos taisykles, apibendrinimas. Pritarta Lietuvos vyriausiojo administracinio teismo teisėjų 2019 m. birželio 12 d. pasitarime", accessed August 10, 2023, https://www.lvat.lt/veikla/teismu-praktika/teismu-praktikos-apibendrinimai/206.
850. "Draft Council conclusions on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe. Council document 17537/11 of 2011-12-01", accessed August 10, 2023, http://db.eurocrim.org/db/en/vorgang/286/.
851. "Lietuvos vyriausiojo administracinio teismo praktika, taikant Lietuvos Respublikos viešojo administravimo įstatymo normas. Pritarta Lietuvos vyriausiojo administracinio teismo teisėjų 2016 m. birželio 1 d. pasitarime", accessed August 10, 2023, https://www.lvat.lt.
852. "Republic of Lithuania law on Civil Service 8 July 1999 No VIII-1316, new edition from 1 January 2019 No XIII-1370", TAR, , https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.84605/asr?positionInSearchResults=0&searchModelUUID=6de0ecaa-c8ab-4af5-b5af-9cfb5ac40980; Law amending the Law on Civil Service of the Republic of Lithuania No VIII-1316. Project No XIVP-2066(3) 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/45f12782ed6711edb649a2a873fdbdfd.

Lithuania;[853] the Law on State Environmental Control of the Republic of Lithuania;[854] the Competition Law of the Republic of Lithuania etc.).

The case law of the Supreme Administrative Court of Lithuania shows that the Charter of Fundamental Rights of the European Union is of particular relevance when dealing with issues relating to European Union law in the field of public administration,[855] freedoms and principles, inter alia, the right to good administration enshrined in Article 41 of the Charter (see, e.g. Judgment of 29 March 2012 in Administrative Case No A822-2220/2012; Judgment of 7 July 2015 in Administrative Case No eA-2266-858/2015; Judgment of 8 December 2010 of the Extended Chamber of Judges in Administrative Case No A756-686/2010, Bulletin of the Supreme Administrative Court of Lithuania, Bulletin of the Supreme Administrative Court of Lithuania No 20, 2010[856]). The Court of Justice of the European Union has recognised the right to good administration as a general principle of law in its case law.[857]

According to the definition set out in the LPA, public administration is the activities of public administration entities regulated by law and intended to implement legislation: administrative regulation, adoption of administrative decisions, supervision of the implementation of legislation and administrative decisions, provision of administrative services, and administration of public service provision. Public administration comprises five main areas in which public administration entity's function, namely:

1. administrative decision-making.
2. monitoring the implementation of laws and administrative decisions.
3. the provision of administrative services.
4. the administration of the provision of public services.
5. internal administration of the public administration entity.[858]

The jurisprudence of the Supreme Administrative Court of Lithuania emphasises the obligation of public administration entities to comply with the principles of law (see, e.g., the ruling of 1 March 2012 in administrative case No A502-1605/2012, the decision of 28 June 2012 in administrative case No A492-2045/2012, and the decision of 3 April 2014 in administrative case No A492-801/2014).

Good public administration is based on the principles laid down in Article 3 of the Law on Public Administration (see in this respect the judgment of 30 April 2012 in administrative case No A492-1978/2012). Proper, responsible management, as repeatedly emphasised in the practice of the Supreme Administrative Court of Lithuania, is inseparable from the requirements of good administration (see the decision of the Extended Chamber of Judges of the Supreme Administrative Court of Lithuania of 21 December 2015 in administrative case No I-7-552/2015).

In the case law of the European Union, the principle of good administration is treated as part of the general principles of law (in this respect, see the judgment of 23 September 2014 in administrative case No A858-47/2014 and the case-law of the CJEU cited therein).[859]

---

853. "Republic of Lithuania law on Tax Administration 13 April 2004 No IX-2112", TAR, accessed August 10, 2023, https://www.e-tar.lt/portal/lt/legalAct/TAR.3EB34933E485/asr.
854. "Republic of Lithuania law on State Control of Environmental Protection 1 July 2002 No IX-1005", TAR, accessed August 10, 2023, https://www.e-tar.lt/portal/lt/legalAct/TAR.CB941ADCC055/asr.
855. "Charter of Fundamental Rights of the European Union, (2012/C 326/02), 26.10.2012 accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.
856. "Lietuvos vyriausiojo administracinio teismo biuletenis Nr. 20, 2010", 2012 accessed August 10, 2023, https://www.lvat.lt/veikla/teismu-praktika/teismo-biuleteniai/207.
857. "Lietuvos vyriausiojo administracinio teismo praktika, taikant Lietuvos Respublikos viešojo administravimo įstatymo normas. Pritarta Lietuvos vyriausiojo administracinio teismo teisėjų 2016 m. birželio 1 d. pasitarime", accessed August 10, 2023, https://www.lvat.lt.
858. "Lietuvos vyriausiojo administracinio teismo praktika, taikant Lietuvos Respublikos viešojo administravimo įstatymo normas. Pritarta Lietuvos vyriausiojo administracinio teismo teisėjų 2016 m. birželio 1 d. pasitarime", accessed August 10, 2023, https://www.lvat.lt.
859. "Regionų apygardos administracinio teismo Kauno rūmų Byla eI3-16-402/2020, 2020-07-01", accessed August 10, 2023.

The origins and scope of National Human Rights Institutions (NHRIs) are closely linked to the international human rights protection mechanism. The concept of NHRIs is formulated in UN General Assembly Resolution 48/134 of 1993, which encourages Member States to establish NHRIs and emphasises the need for such institutions to adhere to the principles defining their status, guidelines for their operation, and basic requirements, known as the Paris Principles. UN Coordinating Committee of National Human Rights Institutions, 23 March 2017. The Parliamentary Ombudsman's Office was accredited as an NHRI (level A) in line with the Paris Principles. In 2017, the Seimas of the Republic of Lithuania adopted the Law on Amendments and Supplements to the Law on the Seimas Ombudsmen of the Republic of Lithuania,[860] which defined new areas of competence of the Seimas Ombudsmen in the performance of the functions of a national human rights institution.

The mission of the Seimas Ombudsmen is to pay attention to and assist each individual by protecting and respecting human rights and freedoms, promoting dialogue between individuals and the government, and ensuring that government institutions serve the people well. The implementation of social and economic rights remains a very topical issue: the Constitution of Lithuania enshrines the State's obligation to ensure the protection and defence of human dignity. This means that state institutions and officials must respect human dignity as a special value.[861]

The crucial role of the NHRI in systematically analysing and synthesising information for reports, conducting investigations on substantive human rights issues, conducting assessments of national legislation in terms of its compliance with universally accepted human rights principles and standards, suggesting conditions for redressing possible human rights violations etc.

In terms of issues, 31% of all complaints received by the Seimas Ombudsmen in 2022 were related to the handling of complaints by individuals in state and municipal institutions, 30% were related to the restriction of liberty, 8% were related to the environment, and 6% were related to property issues. In 2022, the group of complaints concerning the rights of foreigners stood out compared to the previous year (3% of all complaints examined). This relates to ensuring the rights of war refugees from Ukraine and persons who have crossed the Lithuanian-Belarusian border into the Republic of Lithuania. The percentage of complaints on other issues remained similar. The provisions of the Law on the Seimas Ombudsmen give the Seimas Ombudsmen the right to make suggestions (recommendations) which must be examined by an institution and body or official and to inform the Seimas Ombudsmen of the results of the examination. In 2022, the Seimas Ombudsmen made a total of 1741 recommendations. The largest number of recommendations made by the Seimas Ombudsmen is in relation to the Ministries of Justice (501), Interior (206), Environment (156), Agriculture (140) and Social Security and Labour (66) and the bodies under their management.

The State Audit Office[862] is the supreme audit institution, which monitors the legal management and use of state funds and assets and the implementation of the state budget. It is the only institution in the European Union that simultaneously performs the functions of three bodies: the Supreme Audit Institution (SAI), the European Union Investment Audit Institution (EUIAI), and the Budget Monitoring Authority (BMA). The State Audit Office carries out public audits as part of its tasks. A state audit is an independent and objective assessment carried out by the Supreme Audit Institution on audited entities.

860. "Republic of Lithuania law on Controllers of the Seimas 3 December 1998 No Nr. VIII-950, new edition from 25 November 2004 No IX-2544", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.69069/asr.
861. Lietuvos Respublikos Konstitucinio Teismo 1998 m. gruodžio 9 d. nutarimas, 2004 m. gruodžio 9 d. nutarimas, 2009 m. rugsėjo 2 d. nutarimas.
862. "National Audit Office of Lithuania", accessed August 10, 2023, https://www.valstybeskontrole.lt/EN.

4.1 National audit reports

4.1.1 Information Resource Management in the Ministry of the Interior, 13 October 2016[863]

The report states that the objectives of the Ministry of the Interior are to formulate state policy, organise, coordinate, and control its implementation in the fields of public security, public administration, and the application of information technologies in the field of public administration, security of state information resources, migration, and physical education and sports. The Ministry manages 16 information resources, which ensure the availability of data to the population, the operational activity of services and the functioning of the Schengen cooperation tools. The Ministry of the Interior's IT strategic planning was found to be deficient, which increases the risk that financial, technological, and human resources will not be adequately deployed. It was found that the Ministry manages eight critical state information resources but does not comply with the Law on State Information Resources Management. The existing documentation of the information resources managed by the Ministry does not reflect the actual volume of computerised functions and information processed; failure to determine the importance and sensitivity of the information managed by the Ministry and its subordinate bodies may not ensure information security requirements for the publication, transmission and disclosure of such information. The organisational structure of the Ministry's IT governance needs to be improved. IT change management procedures are not in place for all information resources managed by the Ministry. The Ministry's controls to ensure the confidentiality, integrity and availability of e-information/data are insufficient. Recommendations were made, including the following: to improve IS and registers in a coherent and targeted manner, to develop and adopt a strategic IT plan for the management area of the Ministry of the Interior; to draw up and keep up-to-date an inventory of all the IS, registers and other software used in the Ministry; to draw up and approve a directory of the IT services provided by the Department of Informatics and Communications and to determine the level of provision of these services.

4.1.2 Building an e-Health system, 26 April 2017[864]

The health sector is increasingly dependent on information and communication technologies. eHealth became passive after the completion of the development work at the end of 2015, and conflicting views between users and developers on the achievement of the development objectives, quality and security of the system have emerged in the public domain. It has been found that the development projects planned for the development of the eHealth system have been implemented, but not all results are achieved, measurable and in line with users' expectations. It is recommended that the Ministry of Health of the Republic of Lithuania, in or developed, sustainable development of the eHealth system and sound financial management principles, should take measures to ensure that the new phase of the eHealth system development does not repeat the mistakes made in the previous phases of the development: the following: provisions related to the eHealth system in the strategic planning documents have not been aligned; the development of measurable qualitative and quantitative eHealth system programme indicators and their measuring methodology has not been developed; the development of a sustainable governance model for eHealth system.

863. "National audit office of Lithuania. Valstybės kontrolė", Vidaus reikalų ministerijos informacinių išteklių valdymas, 2016 m. spalio 13 d. Nr. VA-P-90-2-19, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.
864. "National audit office of Lithuania. Valstybės kontrolė", Elektroninės sveikatos sistemos kūrimas, 2017 m. balandžio 26 d. Nr. VA-2017-P-900-3-12, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.

4.1.3 Developing the state's electronic communications infrastructure, 14 July 2017 [865]

'Electronic communications infrastructure' means the totality of apparatus, equipment, lines, pipelines, cables, ducts, conduits, manifolds, towers, masts, and other means for the conduct of electronic communications activities.[866] The audit found that the existing infrastructure of the State's electronic communications networks is inefficiently managed, with duplication of infrastructure development decisions and the provision of electronic communications services. There is no centralised coordination mechanism for infrastructure development in the country. It is recommended that the Ministry of Transport and Communications of the Republic of Lithuania, to ensure the efficient use of the infrastructure of the State's electronic communications networks, should eliminate the duplication of physical infrastructure and services; and should envisage measures to promote the highest possible data transmission services in all areas where broadband connectivity is available. It is recommended that the Ministry of National Defence of the Republic of Lithuania, in order to ensure a high level of security of state-owned electronic communications networks, taking into account the current cyber threats, the prospects for network integration and the ongoing changes in the division of responsibilities and competences, should establish unified security requirements for state-owned electronic communications networks.

4.1.4 Readiness to make decisions on the transformation of administrative and public service delivery, 29 September 2017[867]

The Ministry of the Interior's actions to ensure the provision of administrative and public services that meet the needs of the public and the rational use of public resources for this purpose were found to be insufficiently coherent and effective. Centrally managed information on the provision of administrative and public services is not complete and reliable. The administrative and public services that should be provided by the State are not identified and no system is in place to select the most appropriate public service provider. The control mechanism set up by the Ministry of the Interior does not ensure that complete and reliable data are provided to the Information System for Monitoring and Analysis of Public and Administrative Services. The information system is not easy to use. The online portal of the Information System for Monitoring and Analysis of Public and Administrative Services, the 'Catalogue of Lithuanian Services', is not functioning properly and not at full capacity. It is recommended that the Ministry of the Interior, when formulating the state policy in the field of administrative service provision and administration of public service provision, should identify the administrative and public services that should be provided by the state; and establish a mechanism for the administration of public service provision.

4.1.5 Legislative process, 16 March 2018[868]

The implementation of the Legislative Process has been found not to provide the right conditions for the development of a coherent, consistent, cohesive, and effective legal system, as the adequacy of the existing legal framework is not ascertained, and responsible lawmaking is not always ensured in the drafting and adoption of legislation. Fragmented and low-quality

865. "National audit office of Lithuania. Valstybės kontrolė", Valstybės elektroninių ryšių infrastruktūros plėtra. 2017 m. liepos 14 d. Nr. VA-2017-P-900-1-15, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.
866. "Electronic Communications Law of the Republic of Lithuania 15 April 2004 No IX-2135, new edition from 1 December 2021 No XIV-635", TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232036/asr.
867. "National audit office of Lithuania. Valstybės kontrolė", Ar pasirengta priimti sprendimus dėl administracinių ir viešųjų paslaugų teikimo pertvarkos. 2017 m. rugsėjo 29 d. Nr. VA-2017-P-40-2-17, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.
868. "National audit office of Lithuania. Valstybės kontrolė", Teisėkūros procesas, 2018 m. kovo 16 d. Nr. VA-2018-P-40-6-2, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.

regulatory monitoring does not provide information on the necessity, appropriateness, adequacy, sufficiency, and effectiveness of the existing legal framework, and therefore does not allow for a targeted and consistent improvement of the existing legal framework and an adequate response to the changes taking place in different areas of society. There is no effective system for assessing the impact of the envisaged legal regulation. The large number of bills submitted to the Parliament and the very frequent use of urgent or special urgency procedures for the consideration of bills shorten the time available for the consideration of bills, which does not allow for the establishment of an appropriate legal framework and the transparency and openness of the law-making process. Delays in the drafting of legislation transposing EU Directives into national law, resulting in inadequate implementation of Lithuania's EU obligations. When drafting such legislation, the options for the most appropriate solution in Lithuania's interests are not always considered. It is recommended that the Board of the Seimas of the Republic of Lithuania should ensure that sufficient time is allocated for the drafting and adoption of laws and that the urgency and special urgency procedures should be applied only in exceptional cases when unforeseen extraordinary social, economic or political circumstances in the life of the country require it. It is recommended that the Government of the Republic of Lithuania restructure the system of monitoring legal regulation in such a way that the competencies of the different institutions for the assessment of legal regulation are concentrated and that there is a shift from piecemeal assessments of legal regulation to systematic assessments of relevant and problematic areas of regulation. Establish measures to ensure the timely preparation of legislation aligning the national legal framework with EU law, considering all transposition alternatives.

4.1.6 Management of Critical State Information Resources, 28 June 2018[869]

State information resources are the totality of the information managed by the institutions in the performance of their statutory functions, processed by means of information technology, and the information technology tools that process it. State information resources of special interest - electronic information of special interest - are managed in the first category State information systems, registers and cadastres (IS). Well-designed and efficiently implemented information technology processes enable effective protection of information resources against emerging cyber threats. The trends in the maturity of the management of critical State information resources have been identified as positive, but the progress observed is too slow in the light of the increasing level of cyber threats and the security of these resources needs to be better ensured. The system for identifying critical national information resources is not effective enough to implement security solutions that meet real needs. It is recommended that the Government of the Republic of Lithuania develops a national information architecture and its governance mechanism to objectively determine the importance of the State information resources and to adequately control the process, and to harmonise the mechanisms for determining the critical State information resources and the Critical Information Infrastructure. It is recommended that the Ministry of Defence improves the management of cyber security risks by updating requirements, and methodologies, and implementing a national IT risk management system to effectively manage nationally relevant risks.

869. "National audit office of Lithuania. Valstybės kontrolė", Ypatingos svarbos valstybės informacinių išteklių valdymas, 2018 m. birželio 28 d. Nr. VA-2018-P-900-3-6, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.

4.1.7 Smart tax administration system, 17 September 2019[870]

It has been found that the Smart Tax Administration System solutions have been developed as a prerequisite for reducing the administrative burden on business, but that this effect has not yet been achieved and that the potential of data analytics is not yet sufficiently exploited to reduce the shadow economy at the national level. It is recommended that the Ministry of Finance, the Chancellery of the Government of the Republic of Lithuania should have the greatest possible impact on all its manifestations, including by improving the tax administration process and reducing the administrative burden of taxes, by making use of the available institutional and inter-institutional capacities for data analysis. It is recommended that the State Tax Inspectorate carry out a more detailed analysis of the needs and expectations of taxpayers, assessing the problems encountered in tax administration, and, based on the results, plan measures to raise the level of e-services progress and reduce the administrative burden.

4.1.8 Judiciary, 22 June 2020[871]

Under the Constitution of the Republic of Lithuania, the Lithuanian courts are the only institution that administers justice in the country. The right to justice is one of the most fundamental human rights and one of the indispensable pillars of civil society. The main task of the courts is to resolve legal disputes and to ensure that the perpetrator of a criminal offence is justly punished and that no innocent person is convicted. There are 22 courts of general competence and specialised courts. Each year, the courts of first instance receive more than 200,000 new cases. Around 75% of the cases we receive are civil cases, which is why we have paid more attention to the process of handling this category of cases. We found that the judiciary does not provide all the necessary conditions to ensure that cases are dealt with efficiently, i.e., in the shortest possible time, without compromising the quality of the decisions taken. Decisions are needed to improve the efficiency of the judicial system. The stability of the judicial system is important and relevant for society, as instability and uncertainty in this system can have negative consequences for the quality of justice. Reforms to improve the efficiency of the judiciary should only be undertaken if they are unavoidable, well thought out and based on economic and qualitative criteria. The Seimas of the Republic of Lithuania, the Government of the Republic of Lithuania and the Council of Judges are involved in the decision-making process on changes in the judicial system and express their will. Having a common vision would facilitate planning and informed decision-making for the improvement of the judicial system. In Lithuania, there is no vision for the improvement of the judiciary, no priority directions, goals, objectives and expected results for improving efficiency. It is recommended that the Judicial Council and the Ministry of Justice, by removing functions that are not inherent to the courts and allowing for the specialisation of judges, should set out long-term priorities, goals, objectives and expected outcomes for the improvement of the judicial system. It is recommended that the Judicial Council should develop adequate human resources to enable the effective handling of cases and to create the necessary conditions for ensuring the safety of the most vulnerable participants in the proceedings and the organisation of hearings. It is recommended that the National Judicial Administration provide all courts with the necessary facilities to organise hearings remotely.

870. "National audit office of Lithuania. Valstybės kontrolė", Išmanioji mokesčių administravimo sistema. 2019 m. rugsėjo 17 d. Nr. VA-6, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.
871. "National audit office of Lithuania. Valstybės kontrolė", Teismų sistema, 2020 m. birželio 22 d. Nr. VAE-5, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.

4.1.9 How effective is the fight against cybercrime? 16 July 2020[872]

Although the development of information technology has brought about many positive changes, it has also influenced the emergence of cybercrime. According to the Convention on Cybercrime, [873] these crimes include crimes against the confidentiality, integrity and availability of computer data and systems, and other cybercrimes such as cyber fraud, crimes related to the sexual exploitation of children, infringements of copyright and related rights, and crimes of a racist and xenophobic nature. The 2015 EU Council Conclusions on the renewed EU Internal Security Strategy 2015–2020[874] announced that the fight against cybercrime is one of the three main security priorities.

According to the European Cyber Security Strategy,[875] Criminal activities in this space are seen as a growing and serious threat to public security. As cybercrime grows, society needs to be prepared to recognise the threats of cybercrime and to be able to protect itself against them. It has been found that preventive activities do not create the conditions for the public to feel safe in cyberspace. Preventive activities against cybercrime are carried out by the police and other institutions: the National Cyber Security Centre under the Ministry of National Defence, the Communications Regulatory Authority, the State Inspectorate for Data Protection, the State Consumer Rights Protection Authority, the Office of the Inspector of Journalists' Ethics, the Ministry of Culture, the Committee for Development of the Information Society, the Government Chancellery. However, the participating institutions act within their area of competence and in accordance with the priorities set by them, do not coordinate their preventive measures, do not carry out impact assessments of cybercrime prevention activities, and there is no inter-institutional system for planning, coordinating, and measuring the impact of preventive activities at the national level. Blocking rights, which should restrict access to unwanted and harmful content on the internet, have been granted to 7 authorities. However, those who distribute unwanted and harmful content on the internet can circumvent the blocking mechanism, so these measures are temporary and the illegal and harmful content remains unremoved. Weaknesses in cyber incident management do not allow for the identification of all incidents that are potentially criminal acts. The police and the National Cyber Security Centre do not share data on cyber incidents and events. Specialised units for cybercrime in the Criminal Police were launched in 2015 in the District Chief Police Offices. The performance of these units is not satisfactory. The model for the management of the specialised units for cybercrime is not sufficiently effective. Insufficient identification of systemic cybercrime at the national level. The General Prosecutor's Office identifies pre-trial investigations carried out in different commissariats which are not identified as part of a systemic crime and are not merged. The Lithuanian Criminal Police Bureau does not have all the information on identified systemic crimes. There is a lack of specialised capacity to investigate cybercrime. The specialisation of police units and prosecutors in cybercrime is not sufficiently clear. Long queues for investigations of information technology objects, e.g. at the Forensic Investigations Unit of the Vilnius County Chief Police Commissariat, the waiting time for investigating objects is about 19 months, at the Forensic Investigations Centre it is about 10 months. The network of specialised prosecutors in cybercrime is not yet fully operational, nor has the network of officers been created to exchange good practice and

872. "National audit office of Lithuania. Valstybės kontrolė", Ar veiksmingai kovojama su elektroniniais nusikaltimais. 2020 m. liepos 16 d. Nr. VAE-7, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.
873. "Council of Europe. Convention on cybercrime. Budapest, 23.XI.2001, ETS 185", accessed August 10, 2023, https://www.europarl.europa.eu. Konvencija dėl elektroninių nusikaltimų, priimta Budapešte 2001-11-23, ratifikuota Lietuvos Respublikos 2004-01-22 įstatymu Nr. IX-1974, o 2006-06-08 įstatymu Nr. X-674 – Konvencijos dėl elektroninių nusikaltimų Papildomas protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo.
874. "Internal Security Strategy (ISS)", accessed August 10, 2023, https://eur-lex.europa.eu/EN/legal-content/glossary/internal-security-strategy-iss.html.
875. "The EU Cybersecurity Strategy", accessed August 10, 2023, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

experience between the participants in the system. The Public Security Development Programme 2015–2025[876] and the National Cyber Security Strategy[877] The measures envisaged to combat cybercrime are insufficient as they do not address the problems of prevention; removal of illegal and harmful content on the internet; management of cyber incidents that may constitute cybercrime; identification of systemic cybercrime; development of specialised competences; long queues of investigations of information technology objects; and insufficient profiling of cybercrime. Inadequate attention to preventing and improving the investigation of cybercrime could further reduce investigative performance and public safety in the future around cybercrime. It is recommended that the Ministry of the Interior should have a greater impact on the ability of the country's population to identify these threats and ensure inter-institutional planning, coordination, and measurement of the impact of preventive activities in the field of cybercrime. It is recommended that the Ministry of Defence, the General Prosecutor's Office and the Police Department improve the identification of cyber incidents by cybersecurity actors that may constitute cybercrime and strengthen cooperation between the police and the National Cyber Security Centre in this area. It is recommended that the Police Department review and improve the operational model of the Cybercrime Specialised Units to identify all systemic cybercrimes at the national level, to mobilise sufficient specialised investigative and expert capacity and to increase the scope of criminal intelligence activities. It is recommended that the General Prosecutor's Office improve the specialisation of prosecutors so that all pre-trial investigations of cybercrime by specialised officers are led by specialised prosecutors in this field. It is recommended that the Department of Prisons design and implement measures to prevent cybercrime from places of deprivation of liberty. It is recommended that the Ministries of the Interior and National Defence include in their national strategic planning documents measures to address the current problems in cybercrime.

4.1.10 State information resources managed by the Centre of Registers, 6 December 2021[878]

Public information resources are the totality of the information managed by the institutions in the exercise of their statutory functions, processed by means of information technology, and the information technology tools that process it. The Centre of Registers shall ensure that the information resources of the State are managed in such a way that the data contained therein are reliable, secure, quickly and conveniently accessible to State and municipal institutions and bodies, to businesses and to the public. The audit found that the conditions for the development of the State's information resources are not appropriate, no common information technology architecture has been developed and no common information technology architecture document exists. The conditions for proper management of the maintenance, servicing and support processes of the State information resources managed by the Centre of Registers are not in place. It is recommended that the Ministry of Economy and Innovation, as the institution exercising the rights and duties of the owner of the State Enterprise Centre of Registers, should provide measures to ensure that state and municipal institutions and bodies use the most cost-effective way of obtaining data possible. It is recommended that the State Enterprise Centre of Registers should improve the conditions for the development of state information resources managed by the Centre of Registers and ensure the continuity of good practice in information technology management.

876. "Resolution No XII-1682 of the Seimas of the Republic of Lithuania of 7 May 2015 "On approval of the 2015–2025 public security development program, TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.425517.
877. "Resolution No XII-1682 of the Seimas of the Republic of Lithuania of 7 May 2015 "On approval of the 2015–2025 public security development program, TAR, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.425517.
878. "National audit office of Lithuania. Valstybės kontrolė", Registrų centro tvarkomi valstybės informaciniai ištekliai, 2021 m. gruodžio 6 d. Nr. VAE-7, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.

4.1.11 Cybersecurity. 27 October 2022[879]

The cybersecurity framework needs to be improved, as the national level does not ensure adequate management of cybersecurity risks and incidents, does not provide adequate conditions for monitoring compliance with security requirements, does not yet consolidate the legal framework for cybersecurity and electronic information security, and does not ensure consistent implementation of cybersecurity planning. The security management system is not sufficiently effective. The absence of identified national cybersecurity risks, the lack of a national cybersecurity risk management plan, the absence of a national cybersecurity risk management plan, the absence of an acceptable national cybersecurity risk and tolerance thresholds, and the lack of coordination of the risk management process at the national level. Between 2019 and 2021, almost half (45%) of the managers/maintainers of state information resources have not carried out an IT security compliance assessment. The Ministry of Defence's takeover of cyber security in 2015 and the development of the State Information Resources (electronic information security) policy in 2018 have not resulted in a consolidated legal framework in these areas. Some of the requirements for cybersecurity and electronic information security are identical in different legislation, which makes it difficult for cybersecurity entities that manage and/or maintain state information resources to implement security requirements. Improvements are needed in the management of cyber incidents. Consistent implementation of cybersecurity planning is not ensured. It is recommended that the Ministry of National Defence should ensure the use of cyber protection, prevention and response measures and that an IT security risk management process (including cyber risks) should be implemented and coordinated at the national level, which would allow the information obtained on the state of cyber security risks to be used for strategic decision-making on strengthening cyber security. Adopt measures to improve the communication of cyber incidents through the Cybersecurity Information Network. Develop and approve a detailed standard cyber incident management plan and mandate cybersecurity entities to develop or update their internal cyber incident management plans/procedures based on the model of this standard plan.

Between 2011 and 2020, Lithuania received recommendations from the EU and the OECD to improve the design of public sector institutions. Despite Lithuania's efforts to change the governance of state-owned enterprises in line with the OECD guidelines and recommendations, some of the suggestions remain relevant. For example, in its 2020 report "Governance of State and Municipal Owned Enterprises and Public Bodies", the State Audit Office recommended further optimisation of the portfolio of state-owned enterprises, the transformation of state enterprises with a non-advanced legal form into legal entities with other legal forms and other necessary measures.[880] A new round of restructuring of state-owned enterprises (SOEs) was announced at the end of 2021, which is expected to lead not only to a reduction in the number of SOEs but also to a change in their legal form.[881]

OECD reports on public governance in Lithuania mostly include recommendations on the following aspects: recommendations to implement the reform of state-owned enterprises (2015, 2016, 2018); recommendations to consolidate business oversight functions (2015); or to concentrate competencies in evidence-based management agencies (2020). Recommendations on the consolidation of public management agencies also remain relevant. The 2020 State Audit Report "Consolidation of bodies supervising the activities of economic operators" stated that

879. "National audit office of Lithuania. Valstybės kontrolė", Kibernetinio saugumo užtikrinimas. 2022 m. spalio 27 d., Nr. VAE-10, accessed August 10, 2023, https://www.valstybeskontrole.lt/LT/Product/All/1?m=2023;2022;2021;2020;2019;2018;2017;2016.
880. Valstybės kontrolė, *Valstybės ir savivaldybių valdomų įmonių bei viešųjų įstaigų valdysena, 2021 m. balandžio 6 d., Nr. VAE-3.*
881. Vitalis Nakrošis, *Studija „Viešojo valdymo institucinės sąrangos tobulinimas: politiką įgyvendinančių institucijų pertvarkymo įi Viešojo sektoriaus agentūras galimybės". Galutinė ataskaita. Vilnius, 2021 m. lapkričio 22 d.*, accessed August 10, 2023, https://vrm.lrv.lt/lt/veiklos-sritys/viesasis-administravimas.

only one consolidation decision out of ten planned consolidations had been implemented by the beginning of 2020 (i.e. the reorganisation of the State Inspectorate of Energy and the State Commission for Price and Energy Control into the State Energy Regulatory Council). Other consolidation decisions were cancelled, not implemented or delayed.[882] The roadmap for the implementation of the Government Programme for 2020–2024 foresees the development of a methodology for assessing the decisions (reasonableness) of consolidation decisions of supervisors on the activities of economic operators, the assessment of supervisors based on this methodology, and the development of a consolidation plan for the supervisors, but the development of the consolidation plan is planned to be relatively late, only in Q4 of 2022. Due to the lengthy preparation and legislative process, this reduces the likelihood that significant consolidation of business supervisors will take place before the end of the 18th government term.[883]

The Charter of Fundamental Rights of the European Union establishes everyone's right to good administration, which means that the authorities should deal with matters impartially, fairly and within the shortest possible time (Article 41(1) of the Charter of Fundamental Rights). According to Article 41(2) of the Charter of Fundamental Rights, the right to good administration includes: the right of every person to be heard before any individual measure against him or her is taken (point (a)); the right of every person to have access to his or her file in the exercise of his or her right to legal confidentiality and to professional and business secrecy (point (b)); and the duty of the administration to state the reasons on which it bases its decisions (point (c)). These provisions of the Charter of Fundamental Rights express legal values of a general nature, which may be taken into account as an additional source of legal interpretation when deciding on the content of the principle of good administration in Lithuania (see the decision of the Supreme Administrative Court of the Supreme Administrative Court of Lithuania of 29 March 2012 in Administrative Case No. A822-2220/2012 of 29 March 2012, the ruling of 7 July 2015 in administrative case No. eA-2266-858/2015, the decision of 8 December 2010 of the Extended Chamber of Judges in administrative case No. A756-686/2010, Bulletin of the Supreme Administrative Court of Lithuania, No. 20 of 2010).

Furthermore, Article 51(1) of the Charter of Fundamental Rights states that the provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union, having due regard to the principle of subsidiarity, and to the Member States when implementing Union law. They must therefore respect the rights, observe the principles and apply them by their respective powers, without prejudice to the powers conferred on the Union by the Treaties. The Court of Justice of the European Union has stated in its case law that decisions taken by the authorities of the Member States based on regulations fall within the scope of European Union law, including the Charter. In the case law of the Courts of the European Union, the principle of good administration is treated as part of the general principles of law (see, in this respect, the order of 23 September 2014 in Administrative Case No A858-47/2014 and the case-law of the CJEU cited therein). The European Union's position is that any initiative, in this case in the field of robotics and artificial intelligence, should take a gradual, pragmatic and cautious approach.[884]

882. Valstybės kontrolė, *Ūkio subjektų veiklos priežiūrą atliekančių institucijų konsolidavimas*, *2020 m. gegužės 12 d., Nr. VAE-4*.
883. Vitalis Nakrošis, *Studija „Viešojo valdymo institucinės sąrangos tobulinimas: politiką įgyvendinančių institucijų pertvarkymo¸i Viešojo sektoriaus agentūras galimybės". Galutinė ataskaita. Vilnius, 2021 m. lapkričio 22 d.*, accessed August 10, 2023, https://vrm.lrv.lt/lt/veiklos-sritys/viesasis-administravimas.
884. "European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52017IP0051.

5. Proposed EU AI Regulation to complement Lithuanian administrative law

Artificial Intelligence (AI) is a man-made technological system that equals and mimics human intelligence, capable of learning from mistakes, analysing its environment and making independent decisions to achieve its goals. These technologies improve work efficiency, process large amounts of information, and flag and filter out inaccuracies. The European Commission's White Paper on AI notes that AI is based on the processing, collection, analysis and iterative aggregation of large amounts of data, including personal data, from a wide range of sources. Artificial Intelligence refers to systems that behave intelligently by analysing their environment and making relatively autonomous decisions to achieve a goal. AI systems can be software-only and operate in the virtual world (e.g. voice synthesizers, image analysis software, search engines, speech and facial recognition systems), or they can be embedded in hardware (e.g. intelligent robots, self-driving vehicles, unmanned aerial vehicles or Internet of Things objects).[885]

The design and development of AI must fully respect fundamental rights and existing legal rules. [886] The same level of protection for the use of AI should be ensured in both the digital and the physical world. Such a standard of protection, in accordance with Article 52(1) of the Charter of Fundamental Rights of the European Union, includes any restriction on the exercise of the rights and freedoms recognised by that Charter, which, in accordance with the principle of proportionality, may only be imposed where it is necessary and genuinely in the common interest as recognised by the European Union, or for the protection of others' rights and freedoms, and which is provided for by law, and which does not alter the substance of those fundamental rights and freedoms.[887] The use of AI must respect the intended fundamental rights and freedoms of individuals, as well as ensure compliance with data protection and privacy legislation and provide effective remedies.[888]

In some cases, artificial intelligence, like any other disruptive technology, may raise new ethical and legal issues, such as liability or potentially biased decision-making. The EU must therefore ensure that AI is developed and deployed within an appropriate legal framework that promotes innovation in line with the Union's values and fundamental rights, as well as ethical principles such as accountability and transparency. The EU is well-placed to lead this debate at global level.

Goda Strikaitė-Latušinskaja[889] explores why when we talk about artificial intelligence, we should talk about law. The author argues that, at the current level of technological development, there is a risk that the technical abilities, horizons, preferences, interests, and biases of those who develop applications will be reflected in the applications that are developed. Another important aspect from a legal point of view is liability when a person makes a mistake, it is easy to say that he or she should be held responsible for that mistake. When it comes to AI applications, the situation is not yet the same it would often not be so easy to answer the question of who should be liable in one case or another. The situation is not made easier by the fact that it is not always possible to predict how a programme will work, nor is it always possible to explain the circumstances that led

885. *Jurgita Baltrūnienė, Dirbtinis intelektas ir duomenų apsauga kriminalistikos plėtros kontekste (Vilnius: MRU, 2022),* accessed August 10, 2023, https://repository.mruni.eu › bitstream › handle.
886. "Council of the European Union. *Presidency conclusions—The charter of fundamental rights in the context of artificial intelligence and digital change* (Note 11481/20 FREMP 87 JAI 776, 2020)", accessed August 10, 2023, https://www.consilium.europa.eu/media/46496/st11481-en20.pdf.
887. "Council of the European Union. *Presidency conclusions—The charter of fundamental rights in the context of artificial intelligence and digital change* (Note 11481/20 FREMP 87 JAI 776, 2020)", accessed August 10, 2023, https://www.consilium.europa.eu/media/46496/st11481-en20.pdf.
888. "Council of the European Union. *Presidency conclusions—The charter of fundamental rights in the context of artificial intelligence and digital change* (Note 11481/20 FREMP 87 JAI 776, 2020)", accessed August 10, 2023, https://www.consilium.europa.eu/media/46496/st11481-en20.pdf.
889. Goda Strikaitė-Latušinskaja, „Europietiškas" dirbtinis intelektas – koks jis?", „Teise.Pro", 2022-09-30, accessed August 10, 2023' https://www.teise.pro/index.php/2022/09/30/g-strikaite-latusinskaja-europietiskas-dirbtinis-intelektas-koks-jis/.

to a particular conclusion the so-called black box problem. What matters is for whom and for what purpose a particular AI program is and/or will be used. After all, AI in itself is neither good nor bad it depends on when, for whom and how it is used. The development of the use of AI is well ahead of the legal regulation of the use, impact, and liability of AI. To sum up, European artificial intelligence should be seen as a dual objective, with two goals: one is to catch up with and surpass the leaders, China and the United States, in terms of inventions, and the other is to ensure that the human rights guaranteed by European Union law, which have been developed over so many years. AI algorithms and systems-based technologies are welcomed in the Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, in a letter stating that 'the promotion of IT-driven innovation is closely linked to the realisation of the European Data Strategy, including the recently tabled Data Governance Act',[890] as IT can only be successfully developed if seamless access to data is ensured.[891]

Authors on the issue of law enforcement functions acknowledge that issues of the functions and interaction of law enforcement agencies are among the most important in ensuring the effectiveness of law enforcement activities.[892] All law enforcement authorities carry out law enforcement activities in accordance with their aims and objectives, as reflected in the functions they perform.[893] Therefore, law enforcement functions should be defined as activities to enforce the rule of law, to protect and defend human rights and the administration of justice, and to provide advice, representation and, where necessary, defence. Law enforcement authorities should be able to operate in a rapidly changing criminal environment to enhance the protection and security of all individuals.[894] AI-based applications can provide cybersecurity by helping to gather intelligence on potential threats, by analysing experience and by identifying certain trends in potential risks and threats.

EU Member States are increasingly using AI systems in home affairs, which have proven useful in improving investigations into various types of crime and public order, helping officers to make better decisions, and fighting terrorism.[895] Stronger cooperation between EU countries is needed in the development and deployment of AI technologies in law enforcement and home affairs. Law enforcement authorities and organisations see the AI as a tool to prevent cybercrime in particular.[896] The implementation of AI systems applications brings with it requirements for seamless, fast, user-friendly digital systems. EU Member States have therefore identified an important milestone as a political priority: the need to support the functioning of the area of freedom, security, and justice, so that law enforcement authorities can use AI in their daily work, with clear safeguards in place.[897]

---

890. "European Commission. Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) 25.11.2020, COM(2020) 767 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767.
891. "European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Fostering a European approach to Artificial Intelligence, 21.4.2021, COM(2021) 205 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A205%3AFIN.
892. Pranas Kuconis and Vytautas Nekrošius, *Teisėsaugos institucijos* (Vilnius: Justitia, 2001).
893. Malcolm Davies, Hazel Croall and Jame Tyrer, *An Introduction to the Criminal Justice System in England and Wales* (Harlow by Pearson education, 2005).
894. "European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Fostering a European approach to Artificial Intelligence, 21.4.2021, COM(2021) 205 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A205%3AFIN.
895. "European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Fostering a European approach to Artificial Intelligence, 21.4.2021, COM(2021) 205 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A205%3AFIN.
896. Vincenzo Ciancaglini, Craig Gibson and David Sacho, *Malicious Uses and Abuses of Artificial Intelligence* (UNICRI Trend Micro, 2020), accessed August 10, 2023, https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence.
897. "Council of the European Union. Council Conclusions on Internal Security and European Police Partnership. 24 November 2020. 13083/1/20 REV 1", accessed August 10, 2023, https://data.consilium.europa.eu.

Artificial Intelligence (AI) is a rapidly developing group of technologies. These technologies have the potential to deliver a wide range of economic and societal benefits in a wide range of industries and social activities. AI contributes to the optimisation of operations, the allocation of resources and the tailoring of services to individual needs. In the face of rapid technological change and potential challenges, the EU is committed to furthering the EU's technological leadership and to ensuring that Europeans have access to new technologies that are developed and operate in accordance with the Union's values, fundamental rights and principles.[898] On 19 February 2020, the European Commission published a White Paper on "Artificial Intelligence. A European approach to competence and trust ".[899] The White Paper identifies policy options to achieve the dual objective of encouraging wider deployment of AI and reducing the risks associated with certain uses of the technology. This proposal pursues the second objective of creating an ecosystem of trust by proposing a legal framework for a reliable AI.

In 2020, the European Parliament adopted several resolutions related to PSI, including resolutions on ethics,[900] liability[901] and copyright.[902] In 2021, these resolutions were followed by resolutions on PSI in criminal matters[903] and PSI in the educational, cultural, and audiovisual sectors.[904] EP resolution on the ethical framework for artificial intelligence, robotics and related technologies sets out the text of the proposal for a regulation under the legislative procedure on the ethical principles to be followed in the development, deployment and use of AI, robotics, and related technologies.

- In this policy context, the Commission puts forward a proposed regulatory framework for AI that pursues these specific objectives:
    - To ensure that IT systems placed and used on the Union market are safe and compatible with existing legislation on fundamental rights and Union values.
    - to ensure legal certainty to facilitate investment and innovation in the field of IT.
    - Improve governance and effective enforcement of existing legislation governing fundamental rights and safety requirements for AI systems.
    - facilitate the development of a single market for legitimate, secure, and reliable AI applications and prevent market fragmentation.

Full consistency with existing Union legislation, the EU Charter of Fundamental Rights and existing secondary Union legislation on data protection, consumer protection, non-discrimination and gender equality must be ensured. The proposal does not affect the General Data Protection

---

898. "European Commission. 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, 21.4.2021, COM(2021) 206 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.
899. "European Commission, White Paper. On Artificial Intelligence - A European approach to excellence and trust, 19.2.2020 COM(2020) 65 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX%3A52020DC0065.
900. "Framework of ethical aspects of artificial intelligence, robotics and related technologies. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL))", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52020IP0275.
901. "Civil liability regime for artificial intelligence. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52020IP0276.
902. "Intellectual property rights for the development of artificial intelligence technologies. European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI))", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52020IP0277.
903. "European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI))", accessed August 10, 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html.
904. "Artificial intelligence in education, culture and the audiovisual sector, 2020/2017(INI)", accessed August 10, 2023, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2017(INI); "European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Digital Education Action Plan 2021-2027 Resetting education and training for the digital age, 30.9.2020, COM(2020) 624 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0624.

Regulation (Regulation (EU) 2016/679[905]) and the Law Enforcement Directive (Directive (EU) 2016/680[906]) and complements them with a set of harmonised rules for the design, development, and use of certain high-risk AI systems, and with limitations on the use of certain remote biometric identification systems.

The proposal is also in line with the Commission's overall digital strategy.[907] It sets out a coherent, effective, and proportionate framework to ensure that AI is developed in a way that respects human rights and earns people's trust, helping Europe to adapt to the digital age and make the next ten years the digital decade.

The promotion of AI-driven innovation is closely linked to the Data Governance Act,[908] the Open Data Directive[909] and other initiatives of the EU Data Strategy,[910] which will contribute to the development of reliable mechanisms and services for the reuse, sharing and aggregation of data essential for the development, use and quality of data-driven AI models.

National Artificial Intelligence Strategy from the Ministry of Economy and Innovation[911] The aim is to create a legal and ethical framework for the application of DI in Lithuania, to facilitate its development and maximise its economic potential. It also provides additional tools for businesses and research institutions wishing to carry out AI research. The strategy provides an opportunity to maximise the potential of AI and to join the global AI community.

AI and IT growth in Lithuania should focus on key sectors such as industry, law enforcement, etc. These sectors have been identified based on two factors - their importance for the Lithuanian economy and business and for public security. However, in the current period, there is no major strategic approach and significant investment by the state in IT development systems, but several measures have been put in place that would rapidly improve the development of IT technologies in Lithuania. There is a need to increase the use of digital systems in the private sector. As an incentive for setting up new systems, companies could be awarded an IT badge to demonstrate their leadership in digital. This could be achieved through public support and various systemic tax incentives. In the public sector, an appropriate innovation culture is envisaged to encourage the development, deployment and testing of IT solutions. Public bodies need to be encouraged to implement IT systems that are not only designed to deliver public services to the public but are also capable of measuring and optimising workflow. Another strategic avenue to accelerate the development of IT is the identification of key economic sectors that can potentially benefit most from the application of IT systems at the Lithuanian and European level, and the targeted development of systems in line with the needs of these sectors. To achieve greater benefits, it is recommended to develop tailored approaches to adapting IT innovations for the manufacturing, agriculture, healthcare, transport and energy, and law enforcement sectors.[912]

---

905. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679.
906. "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016L0680.
907. "European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Shaping Europe's digital future, 19.2.2020, COM(2020) 67 final", accessed August 10, 2023, EUR-Lex - 52020DC0067 - EN - EUR-Lex (europa.eu).
908. "European Commission. Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) 25.11.2020, COM(2020) 767 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767 .
909. "Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32019L1024 .
910. "European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data, 19.2.2020, COM(2020) 66 final", accessed August 10, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 .
911. Elijus Čivilis et al., *Lietuvos dirbtinio intelekto strategija. Ateities vizija* (Ekonomikos ir inovacijų ministerija, 2019), accessed August 10, 2023, https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf .
912. Elijus Čivilis et al., *Lietuvos dirbtinio intelekto strategija. Ateities vizija* (Ekonomikos ir inovacijų ministerija, 2019), accessed August 10, 2023, https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf .

One specific area of IT application to be mentioned is law enforcement. Experts argue that the proper use of AI could also lead to more effective law enforcement outcomes.[913] The main areas of particular interest in terms of the use of IT systems in law enforcement are data analysis systems, as well as the interpretation of new previously unknown patterns and their interfaces.[914] As AI-based systems are increasingly enabled in law enforcement, data protection rules and other legal and ethical safeguards must be ensured, and appropriate safeguards put in place. One of the strategic projects being implemented in Lithuania is the "Challenges of implementing personal rights in modern society: dilemmas of new and evolving rights (2021–2025)" programme,[915] prepared by the Ministry of Education, Science and Sport of the Republic of Lithuania. The programme aims to explore the legal challenges facing modern society as the content of established personal rights changes and a new generation of personal rights emerges, and to make proposals for the further development of the legal system. A long-term investment plan has been developed to implement these strategies in Lithuania.[916]

AI-based systems and applications are a relatively new area of law enforcement activity. In Lithuania, many law enforcement agencies are already actively exploring the use of AI and the possibility of incorporating robots in certain functions to enhance crime prevention and control. A wide range of IT applications are being developed in line with national crime prevention priorities. IT systems and technologies used in all the following Lithuanian law enforcement agencies:

- Police Department under the Ministry of the Interior.
- State Border Guard Service under the Ministry of the Interior.
- Prison Department under the Ministry of Justice of the Republic of Lithuania.
- Public Security Service under the Ministry of the Interior.
- Management Security Service.
- Customs Department under the Ministry of Finance.
- Ministry of Justice.
- Ministry of National Defence.

The competencies of these law enforcement authorities are implemented using applications and algorithms developed by the AI model. Law enforcement authorities have different types of systems, of which the AI algorithms are one component.[917]

In law enforcement, AI systems are applied in process automation (document analysis, automated reports, etc.), vehicles (automatic number plate scanning, violation detection), facial recognition systems (airports, border crossing), robots (automated demining robots, street patrols), and in the web technology environment. AI and technology allow much more accurate prediction of potential crimes in public places and can also help in the detection of other crimes. AI differs from conventional computer algorithms in that it can train itself, and as a result, it may behave differently when performing the same action, depending on what it has done before.

913. "Council of the European Union. *Presidency conclusions—The charter of fundamental rights in the context of artificial intelligence and digital change* (Note 11481/20 FREMP 87 JAI 776, 2020)", accessed August 10, 2023, https://www.consilium.europa.eu/media/46496/st11481-en20.pdf.
914. Donatas Murauskas „Dirbtinio intelekto metodai teisės taikymo srityje – galimybes varžo etiniai klausimai", *Vilniaus universiteto „Spektrum"* (2019 accessed August 10, 2023, https://naujienos.vu.lt/dirbtinio-intelekto-metodai-teises-taikymo-srityje-galimybes-varzo-etiniai-klausimai/.
915. „Lietuvos socialinių mokslų centras. Asmens teisių įgyvendinimo iššūkiai modernioje visuomenėje: naujų ir besikeičiančių teisių dilemos (2021–2025 m.)", accessed August 10, 2023, https://lcss.lt/asmens-teisiu-igyvendinimas/.
916. "Lietuva po COVID-19: investicijos, kurios keis ekonomikos DNR" *Mano vyriausybė,* 2020 m. gegužės 15 d., accessed August 10, 2023.
917. European Commission, *Directorate-General for Migration and Home Affairs. Feasibility study on a forecasting and early warning tool for migration based on artificial intelligence technology - Executive summary* (Publications Office, 2021), accessed August 10, 2023, Feasibility study on a forecasting and early warning tool for migration based on artificial intelligence technology - Publications Office of the EU (europa.eu)

The use of AI-based systems in law enforcement can lead to problems with the application of these systems, such as the violation and restriction of human rights. In applying the legislation governing the operation of the AI, law enforcement authorities must consider the fair and lawful use of these systems.

E-justice is an area of development activity that can make a meaningful contribution to the strategic priorities of the United Nations Development Programme (UNDP) and make a real difference in people's lives while tackling systemic exclusion and discrimination. The study on e-justice trends reveals how quickly technology is changing the delivery of justice. Legal systems that do not change cannot benefit from global trends towards modernised, accountable, and accessible justice. The sudden onset of the global COVID-19 pandemic in 2020 revealed the vulnerability of justice systems that have not adapted to new technologies and new ways of delivering services.[918]

Many researchers are working on e-justice issues. Vytautas Nekrosius and other scholars in his article analyse the potential of IT to speed up civil proceedings, identify the main directions of successful use of these technologies, discuss the problems of IT application in court proceedings, and the possibilities of their solution and overcoming. Elena Alina Ontanu argues that to create an EU e-justice system that facilitates and supports cross-border litigation, law and technology need to be properly integrated into a single system linking national and European systems. The author examines the digitisation of cross-border procedures and the evolution of the components on which such an e-Justice system depends. Dory Reiling and Francesco Contini[919] The article discusses the development of the e-Justice platform and its impact on judicial management. Procedural decisions and court work processes can now be encoded in a digital court work environment. This may have implications for core values such as fair trial and the impartiality and independence of the judiciary. The paper concludes by discussing the governance needed to ensure fair process and the proper functioning of IT in courts. Joana Covelo de Abreu[920] discusses the new e-Justice strategy 2019–2023 (Council of the European Union, 15 January 2019, 5139/1/19 REV 1). Chitranjali Negi[921] states that the Commission considers that the first objective of e-Justice is to increase the efficiency of justice across Europe for its citizens, and therefore gives priority to the development of electronic signatures (E-Signatures) and electronic identities (E-Identities), which are of particular interest from a judicial perspective.

5.1 IT services in Lithuanian courts[922]

Technological innovations introduced in Lithuanian courts allow participants in the process to save time and money, and to receive the information they need quickly and clearly.

1. ***Electronic case***. On the portal e.teismas.lt, citizens can use court services from the comfort of their own home: form and submit procedural documents to the court, pay the stamp duty, get access to the case file, receive court documents, listen to audio recordings of court hearings. The e.teismas.lt portal can be accessed via electronic banking, using a personal identity card, with an electronic signature or by obtaining direct login details from the court. The e.teismas.lt portal is used by 40,600 users (32,000 natural persons, about 6,000 lawyers and their assistants, 2,500 legal persons).

---

918. UNDP. *Strategic Transformation through e-Justice* (One United Nations Plaza, New York, 2022), accessed August 10, 2023, https://www.undp.org/publications/e-justice-digital-transformation-close-justice-gap
919. Dory Reiling and Francesco Contini, "E-justice platforms: challenges for judicial governance", *International Journal for Court Administration* 13, 1 (2022): 1–19.
920. Joana Covelo de Abreu "e-Justice paradigm under the new Council's 2019–2023 Action Plan and Strategy – some notes on effective judicial protection and judicial integration" (2019), accessed August 10, 2023, https://officialblogofunio.com/2019/02/27/e-justice-paradigm-under-the-new-councils-2019-2023-action-plan-and-strategy-some-notes-on-effective-judicial-protection-and-judicial-integration/.
921. Chitranjali Negi, "What is E - Justice?" (2023), accessed August 10, 2023, http://www.legalsl.com/it/what-is-e-justice.htm.
922. "Lithuanian Courts", LVAT. IT paslaugos teismuose, accessed August 10, 2023, https://www.lvat.lt/teismo-lankytojams/it-paslaugos-teismuose/679.

2. ***Remote hearings.*** For people living abroad, who are unable to attend court due to illness or other important reasons, it is now possible to attend court remotely. This requires an application to the court and, once the court has considered the application and approved it, it is possible to attend the hearing directly from your home, a medical institution, or another institution.
3. ***Full information about the case.*** Anyone in the country who wants to find out where and when their case will be heard, which judge will rule on their case, access the materials of final judgments, or find out what is waiting for them in the courtroom can easily do so by visiting the following portals: Public Search of Court Schedules; Public Search of Judgments; Open Court. lt, which provides all relevant statistics related to the work of the courts, provides a more detailed overview of the work of all Lithuanian courts and specific judges, and allows you to compare them with each other on the basis of how long it takes to hear a case, the experience of the judges, the cost of maintaining the courts, and other criteria; one of the first initiatives of its kind in the world, initiated in cooperation with Transparency international; sale. teismai.lt allows you to watch a virtual court session, get acquainted with its course, rights and obligations of the participants in the court proceedings, and find answers to topical questions related to the court's activities.
4. ***Audio recordings of the hearing.*** People can listen to high-quality audio recordings of court hearings from the comfort of their own home - all of them, together with the case file, can be found on e.teismas.lt and listened to.
5. ***Automatic case allocation.*** All cases in the courts are automatically assigned to a particular judge using a special system which, after assessing certain criteria (e.g. a judge's specialisation, the number of cases received), draws up a list of judges available to hear a case and assigns it to the judge at the top of the list.

5.2 LITEKO (Lithuanian Court Information System)

The Regulations of the Lithuanian Judicial Information System[923] shall regulate the objectives and purpose of the Lithuanian Judicial Information System (LITEKO), the legal basis for its establishment, its organisational, informational, and functional structure, the data to be processed, the sources of the data to be collected, the processing of data, the requirements for data security, the establishment, modernisation, and liquidation of LITEKO.

LITEKO users - judges, civil servants of courts or employees working under employment contracts, who have been granted the right to use LITEKO resources for the performance of their functions in accordance with the procedure established by law. Service recipients - participants in civil, administrative, administrative offence or criminal court proceedings: citizens of the Republic of Lithuania or natural persons holding a permanent residence permit in the Republic of Lithuania or legal entities registered in the Republic of Lithuania, acquiring rights and obligations in civil, administrative, administrative offence or criminal court proceedings and receiving a public electronic service provided by means of LITEKO.

The purpose of LITEKO is to electronically manage the data on the cases pending and disposed of in Lithuanian courts, to record the progress of the proceedings and to provide the conciliation mediation and public electronic services provided for by the legislation. LITEKO holds approximately 5 million cases, comprising 20 million documents.

923. "Order No 6P-112-(1.1) of the Director of the National Judicial Administration of 28 November 2011 "On the approval of the provisions of the information system of the Lithuanian courts and the provisions of data security of the information system of the Lithuanian courts", LRS, accessed August 10, 2023, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415655?jfwid=.

The European Commission-funded project "Effective e-access to court decisions" under the Justice Programme November 2022 – November 2024. The project is implemented by the National Judicial Administration. The project will integrate the European Case Law Identifier (ECLI) into the newly developed Lithuanian Judicial Information System LITEKO (LITEKO II) and will create interfaces with the e-Justice portal.

5.3 Ensuring the speed and security of the Judicial Information System and the modernisation and development of electronic court services [924]

Project purpose: To complete the modernisation of the Lithuanian Courts Information System (LITEKO II), to ensure the smooth and efficient work of the courts in the system, to ensure the high quality of the public electronic services provided, and to ensure the reliability of the technological infrastructure used in the system.

5.4 Hearings of Lithuanian courts[925]

The e.teismas.lt (eCJ) portal for public electronic services of the courts, which was launched on 1 July 2013, will be in its tenth year of operation at the end of 2022. During these years, the trend of increasing use of the services for creating, submitting to, and receiving procedural documents in civil and administrative cases, managing stamp duty information, managing fines imposed by the courts and costs awarded to the State, and accessing the case file has continued.

In 2022, the number of civil and administrative cases handled exclusively in electronic form was 86%. In 2022, electronic administrative cases accounted for 79.93% of the total number of administrative cases handled by courts. The number of electronic administrative cases at first instance (in district administrative courts) is 83.63% in 2022. The share of electronic administrative cases heard on appeal at the Supreme Administrative Court of Lithuania has increased considerably, reaching 63.51% in 2022. The increase in the number of e-teismas.lt (ECJ) users over the past years has continued to grow, with 126 039 ECJ users at the end of 2022. At the end of 2022, 2 192 lawyers; 1 118 legal assistants; 5 38 mediators; 23 981 persons are listed as representatives of legal persons in the accounts of legal persons (a total of 14 880 accesses by legal persons); 98 210 other natural persons are listed as representatives of legal persons in the portal e.teismas.lt. The number of remote hearings using videoconferencing equipment decreased in 2022. In 2020, following the acquisition of licences for the ZOOM platform for the working needs of the courts, hearings and working meetings started to be organised using this platform. This has led to a decrease in the number of remote hearings conducted using the fixed video conferencing equipment installed in the courts. In 2022, the number of remote hearings and working meetings held using video conferencing equipment is 1360, while the number of hearings and working meetings held using the ZOOM platform is 42954.

In 2022, the National Judicial Administration (NJA) represented the interests of the Judicial Council and the judiciary on various issues.[926] A draft resolution of the Council of Judges on the amendment to the description of the procedure for processing non-public data in the Lithuanian Courts Information System has been prepared to ensure the protection of non-public data processed in courts as well as to ensure a unified practice of the courts in LITEKO in processing data related to non-public case materials. As of 1 January 2022, the courts started to keep records of stamp duty. In the light of the changes in the legal regulation, the functionality of the LITEKO Public Electronic Services subsystem was adapted to provide information on the payment of stamp duty and costs related to the proceedings, as well as the relevant payment

924. "Lithuanian Courts", accessed August 10, 2023, https://www.teismai.lt/lt/projektai/igyvendinami-projektai/it-projektai/4953.
925. "Lithuanian Courts", Veiklos rezultatai 2022 m., accessed August 10, 2023, https://www.teismai.lt › 2023/03 › teismai2023-1.
926. "Lithuanian Courts", Nacionalinės teismų administracijos 2022 metų veiklos ataskaita. 2023 m. vasario 22 d. NR. 3R-454-(1.2), accessed August 10, 2023, https://www.teismai.lt.

codes. The automation of the generation of reports on stamp duty credited and refunded in LITEKO has also been carried out, as well as the introduction of LITEKO functionality enabling the presentation of stamp duty data in these reports according to the public sector entities. In order to improve the work of the courts, in 2022 the NTA upgraded the data backup equipment to ensure the security of the Category I information system and other data, purchased and made available to the courts the next generation of antivirus software, 33 sets of juvenile interrogation room equipment, 595 sets of laptops, 67 TVs and brackets, 2 uninterruptible power supplies (UPS), 90 managed video conferencing cameras, 54 Office licences, 38 multifunctional machines and 8 printers. It also renewed, as it does every year, 285 Zoom licences for remote hearings. In 2022, 20 878 new users registered on e.teismas.lt.

We can conclude that all main administrative procedure principles (access to justice, independence of judges and the judiciary, publicity in court proceedings, principles of inquiry and impartiality, expedition and economy of proceedings, clarification of the rights and obligations of the parties to proceedings and others) are implemented in administrative courts of Lithuania.

6. Conclusions and proposals for legislative reforms in Lithuania to bring administrative law into the digital space

Good public administration is based on the principles laid down in Article 3 of the Law on Public Administration. Proper, responsible management, as repeatedly emphasised in the practice of the Supreme Administrative Court of Lithuania, is inseparable from the requirements of good administration.

The principle of good administration is a fundamental principle of the legal system of the European Union and the Republic of Lithuania. The principle of good administration is enshrined in the case law of the Supreme Administrative Court of Lithuania, in the application of the norms of the Law on Public Administration in the most important national (Article 5(3) of the Constitution of the Republic of Lithuania) and international documents (Article 41 of the Charter of Fundamental Rights of the European Union, etc.).

Both national and international strategic documents emphasise the improvement of the quality of services and their delivery and the quality of service to the population, the provision of services that meet the needs of consumers, the digitalisation of services, and the transparent provision of services. In EU Member States, digitisation and public service improvement initiatives have dominated the public governance reform agenda in recent years. However, many EU administrations have pursued reform initiatives for better government organisation and management.

The digital transformation of public governance is an ongoing process that changes the organisational structure and processes of public governance, creating the conditions for strengthening democracy. Digital transformation also involves fundamental changes in culture, staff structure and skills, communication with citizens and the long-term delivery of public services. Digital transformation is thus accompanied by significant changes in public services and their interactions, and digital transformation also focuses on the social nature of these changes, not just on technical issues.[927]

Digital technologies, including artificial intelligence, can strengthen the protection of fundamental rights and democracy. Effective public governance is a strategic objective for Lithuania the deployment of technological solutions is one of the key conditions for positive

927. *Caroline Fischer, Moritz Heuberger and Moreen Heine,* "The impact of digitalization in the public sector: a systematic literature review", *dms – der moderne staat – Zeitschrift für Public Policy, Recht und Management*, 14, 1 (2021): 3–23.

change. Lithuania's strategy for progress "Lithuania 2030"[928] is the basis for strategic decisions on the country's development priorities and their implementation up to 2030. The Strategy identifies three strands of governance: strategically capable government, open and empowering governance, and governance that responds to the needs of society. The importance of digitisation of public administration is directly addressed in Lithuania 2030 around efficient service delivery: *"ensuring the use of the latest technologies, and the delivery of public services in cyberspace"*. The digital transformation of public governance is included in the National Progress Plan (NPP) 2021–2030.

For example, an administrative order is an offer to a person to voluntarily pay within a certain period of time a fine equal to half of the minimum fine established for the administrative offence committed by the person (Article 610(1) of the Administrative Offences Code of the Republic of Lithuania (ANC)). The automated option for the adoption of this document only came into force in 2019, following the adoption of amendments to the Code, and became effective on 1 January 2020. With the automation of the institution of the administrative order, the ANC has established an exhaustive list of administrative offences recorded outside the presence of the person suspected of having committed the administrative offence, for which the administrative offence report with the administrative order is drawn up automatically. Automation in this process should be understood as the preparation of administrative offence reports using software, eliminating human intervention. The current legal framework for automated administrative instruction in Lithuania needs to be improved. The choice of applying automation to the formulation of certain administrative instructions does not correspond to the European vision of integrating technology into the public sector. In view of the risks of the problems outlined above, it is proposed to move towards a hybrid model for the adoption of administrative instructions, where automation is understood and used as a tool to speed up the adoption of administrative instructions, but where the burden of making the final decision is placed on the official. Such a model would be in line with the European Union's emerging approach to incorporating technology into public sector decision-making.

Advances in information technology and its increasing applicability in the public sector (e.g. eGovernment, electronic document management, etc.) not only allow for transparency, but also for the optimisation of processes and the reduction of the human resources needed to carry out standard and routine tasks. The new era of technology and innovation places extremely high demands on lawyers in terms of qualification and integral competence, which require not only the precise application of legal knowledge but also the skilful application of the modern elements of modern management - organisation, planning, workload management, workload management. As society becomes more modern, the link between legal knowledge and electronic services is becoming an integral part of a lawyer's professional activity.

At national level, it is recognised that the State is not exploiting the full potential of digitisation, i.e., not enough new technology-based solutions are being developed to be deployed in the delivery of smart public services. The problem is identified as being due to inefficient management, untapped data potential, lack of technological solutions, competences, and cooperation. The pre-assessment of the digitisation of society, commissioned by the Ministry of Economy and Innovation It found insufficient progress in the digital transformation of the public sector, a lack of long-term vision and alignment of actions, and low ambition. Investments addressing technical issues are predominant, but there is a lack of fundamental change in the transformation of institutions' business processes. Digitisation projects are large and lack flexibility. The public sector lacks a culture of experimentation to foster innovation by harnessing business potential.

928. "Resolution No XI-2015 of the Seimas of the Republic of Lithuania of 15 May 2012 "On the approval of the State Progress Strategy "Lithuania Progress Strategy "Lithuania 2030", LRS, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.425517.

The vision for the digital transformation of public governance in Lithuania requires an integrated and broad approach, encompassing the technological and value levels, whose interaction, harmony, and solutions would ensure a successful digital transformation of public governance. The technological level encompasses the four main objects of digital transformation (decision-making and e-democracy, internal processes of public organisations, public services, and data) and defines the quality of public services and the ways in which the state should deliver them, the level of digital maturity of the internal processes that should be put in place, the way in which decisions are taken and the data policy. The value/context level covers the institutional and cultural framework that enables the development of digitisation capacities. Key factors include strategy, leadership and culture, skills and capabilities, legal environment, governance model and organisational structure, technology, and other resources.

Principles of administrative law and procedure, also principles of good governance will be ensured in case if applicants have the choice to use the IT or not. The main disadvantage of e-tools for public administration activities and administrative cases procedure is the lack of real communication with person. Law on public administration of the Republic of Lithuania and Law on Administrative Procedure of the Republic of Lithuania states the alternatives to use IT technologies or e-tools for applications and complaints or not. So, Lithuania ensured the proper access to information and examination of applications for public administrative entities and courts.

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.

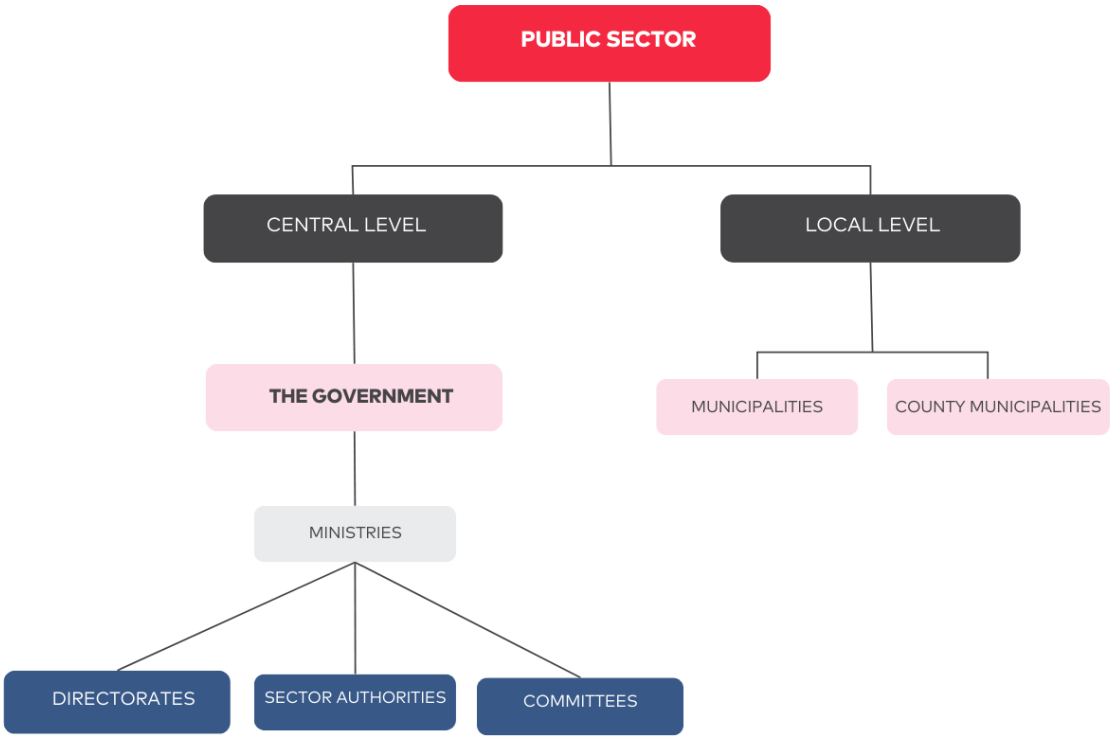


Figure 1. Organization of the Norwegian public sector.

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.

SWEDEN

Rule of Law in the Digital Age: Legal Landscape for Public Digitalisation

Lena Enqvist

Abstract

This chapter examines the Swedish administrative model in the context of digitalisation and automation of tasks and decision-making, from a rule of law perspective. Against the background of ambitious national political ambitions to leverage technologies for enhancing the functions of public authorities, the chapter explores some distinctive aspects of the Swedish regulatory strategy toward digitalisation – emphasising its predominantly technology-neutral stance. This implies a somewhat restrained purpose-specific and direct regulatory impact on digitalisation initiatives and specific procedural safeguards for administrative matters influenced by digitisation or automation. However, the chapter also contends that there is a discernible shift towards an increased level of national regulatory initiatives and control, often aimed at reducing legal obstacles to digitalisation and automation. The chapter also highlights, as a second typical feature of the Swedish approach to public digitalisation, that the relatively strong independence of the government as well as municipal authorities in relation to central government has probable explanatory value for why national public digitisation initiatives are often initiated and prioritised at authority level rather than through political or regulatory governance. This independence is a probable factor contributing to cross-agency collaborations, which not only aim to facilitate implementation but also seek to clarify the boundaries of the governing regulatory frameworks. It concludes that the multifaceted challenges posed by technology to maintaining the rule of law in public administration require diligent oversight, collaborative initiatives, and the exchange of knowledge to effectively tackle common issues.[1071]

1071. This work was supported by the Swedish Research Council under Grant number 2020-02278. I would like to extend my gratitude to Henrik Wenander, Professor of Public Law at Lund University, Sweden, for valuable and insightful comments and suggestions during the preparation of this chapter.

1. Digitalising the Public Sector in Sweden

From a rule of law perspective, it is clear that digital transformations of public services and decision-making are means to an end, rather than a goal in itself. However, when navigating a broad legal landscape which harbours multiple intermediary goals, comprising also service and efficiency objectives, the specific mandates of the rule of law values may not always be clear. It therefore becomes evident that the realisation of the 'rule of law' within the digital realm depends on legal and practical materialisation at various levels in the legal frameworks and administrative structures governing the integration of technologies into public activities. Careful consideration of the interplay between the technologies, legal requirements, and the administrative structures in which the technologies are to be implemented is therefore necessary.

Sweden generally exhibits a high level of digital maturity. However, it consistently attains higher rankings in terms of economic and societal digitalisation than it does regarding digital public governance.[1072] While ranking outcomes are largely dependent on the specific focus with which they are performed, as well as on the methods used, the Swedish public administration does exhibit quite large variations in the manifestations of digitalisation or automation implementations between different authorities. These variations encompass both the breadth and focus of the digital or automated services provided to citizens, and the extent of digital or automated support systems employed to facilitate operations and decision-making processes. Here, the underlying course and trajectory of this development has been influenced by the interplay of administrative culture and organisation combined with the legislative culture and organisation. The subsequent sections will therefore delve into the foundational legal aspects of the Swedish administrative model, to provide a background for further analysis of how the rule of law underpins and interacts with Sweden's regulatory approach as well as response to digitalisation within public administration.

1.1. Introduction to the Swedish Administrative Model

When trying to summarise the features of a nation's administrative legal order, one generally must start at the constitutional level, since the constitutional acquis sets the framework for the administrative order both institutionally and in terms of powers. The Swedish constitutional order is commonly described as being of Scandinavian or Nordic type. Common characteristics are a rooting in the Roman civil law tradition, a primary reliance on codified laws (distinguishing judges from formal law makers). Furthermore, the incorporation of a social dimension in legal reasoning, a significant emphasis on the role of the people's will in law-making, and a tradition of legal cooperation among Nordic countries are distinctive features.[1073] From an international, and in part also from a Nordic perspective, the Swedish administrative order, however, displays some unique characteristics which bears effects on the national strategies, advantages as well as challenges to further the digitalisation process within the public sector.

In Sweden, the constitution and governance are founded on a separation of functions rather than a separation of powers.[1074] Importantly, the Swedish administrative order does not build on a 'separation of powers' doctrine and is therefore not arranged around ideas on balancing of

1072. See, for example The Digital Economy and Society Index (DESI)./ European Commission https://digital-strategy.ec.europa.eu/en/policies/desi Accessed 12 December 2023; eGovernment Benchmark 2023 Executive Summary./ European Commission 2023.
1073. General Features of Swedish Law./ Strömholm, Stig. Swedish Legal System. Ed./ Michael Bogdan. Norstedts Juridik 2010; What Is Scandinavian Law?/ Bernitz, Ulf. In: Concept, Characteristics, Future, Scandinavian Studies in Law 15 2007; The Vision and Legal Reality of Regional Integration in the Nordic States./ Wenander, Henrik. Free Movement of Persons in the Nordic States. EU Law, EEA Law, and Regional Cooperation. ed./ Katarina Hyltén-Cavallius and Jaan Paju. Hart 2023, p. 9–30.
1074. Swedish Constitutional Response to the Coronavirus Crisis The Odd One Out?/ Dahlqvist, Julia and Reichel, Jane. Pandemocracy in Europe: Power, Parliaments and People in Times of COVID-19. Ed./ Matthias C Kettemann and Konrad Lachmayer. Hart Publishing 2022. p 140.

powers between a legislative, executive and judicial branch. The foundational principle is, instead, the notion of popular sovereignty (*folksuveränitetsprincipen*), which builds on the idea that all public power emanates from the people, for which the democratically elected Parliament (*riksdag*) is the main representative.[1075] This means that the will of the people will be channelled through legislative acts (as they are adopted by political bodies which have been attributed legislative powers by the people). The constitutional order of Sweden thus emphasises the democratic rule of law principle, where legislators via attribution are meant to enjoy a fairly generous space for manoeuvre precisely because they are channelling the will of the people.[1076]

That the will of the people can change, and that the legislature therefore may adapt to changing circumstances or policy concepts through rapid regulatory changes, is thus an important part of the idea of popular sovereignty. Consequently, constitutional limitations on legislative power or the role of the courts in limiting it have traditionally not been so strong. Today, Sweden is bound by several international agreements, where not least the ratification and incorporation of the European Convention of Human Rights,[1077] ECHR, into Swedish law, as well as the membership to the European Union, have imposed limits on the Swedish legislature's powers. In turn, this means that the Swedish 'will of the people' often cannot have the same direct impact and turnaround in the design of national legislation as the principle of popular sovereignty implies.[1078]

The Swedish *administrative* tradition is generally considered to be of east Nordic type, essentially meaning that there is a particularly strong kinship to the Finnish administrative order. Important features are the existence of designated administrative courts and a high degree of institutional independence for administrative authorities.[1079] This autonomy has an organisational component in that those authorities which organisationally sort under the Government are seen as free standing and independent from each other. This autonomy and independence (between the authorities) is also reinforced by the fact that the Parliament, by law, and the Government, by ordinance or other directives, allocates different responsibilities and assignments to these authorities (which are also often regulated in different regulations). The fairly strong independence of Swedish government authorities also has a normative component in that the constitutional Instrument of Government states that no administrative authority, including the Government, or decision-making body of any municipal authority, may determine how an administrative authority shall decide in a particular case relating to the exercise of public authority vis-à-vis an individual or a municipality, or relating to the application of law.[1080] As a main rule, this means that the administrative authorities' application of law must be made independently and without political influence.

Despite this relatively strong independence from Government or other authorities, there are means of control for Parliament as well as Government over national administrative authorities. They may (under the limitations set by the Instrument of Government) decide which tasks are to be assigned to which authority and add or delete such tasks by regulation or decision.[1081] Another important instrument is of course the budgetary power, where it is the Parliament that decides on the respective budgets of the authorities based on proposals made by the

1075. Chapter 1 Sections 1 and 4 Instrument of Government.
1076. Administrative Independence Under EU Law: Stuck Between a Rock and Costanzo?/ Enqvist, Lena and Naarttijärvi, Markus. In: European Public Law, Vol. 27 2021, p. 712 et sec; Full Judicial Review or Administrative Discretion? A Swedish Perspective on Deference to the Administration./ Wenander, Henrik. Deference to the Administration in Judicial Review. ed./ Zhu, Guobin. Ius Comparatum - Global Studies in Comparative Law, Vol. 39, Springer 2020, p. 405–415.
1077. Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as Amended) [1950].
1078. Administrative Independence Under EU Law: Stuck Between a Rock and Costanzo?/ Enqvist, Lena and Naarttijärvi, Markus. In: European Public Law, Vol. 27 2021, p. 721 f.
1079. Europeanisation of the Proportionality Principle in Denmark, Finland and Sweden./ Wenander, Henrik. In: Review of European Administrative Law, Vol. 13 No. 2 2020. p. 133–152, at p. 135.
1080. Chapter 12 Section 2 Instrument of Government.
1081. Chapter 8 Instrument of Government.

Government.[1082] The Government thus possesses considerable influence over the functioning of government authorities, but lacks authority to interfere with the authorities' decisions regarding the application of the law or their exercise of power in specific cases. While in many other nations, individual ministers have the power to directly intervene in an authority's daily operations, this is not the case in Sweden. Instead, collective decision-making by the Government and the prohibition against instructing authorities in individual matters are measures to prevent 'ministerial rule'. The Government is responsible for monitoring and preventing any such rule. In the event that the Government finds that an authority has not correctly implemented a law, the available recourse is thus to seek amendment of the relevant legislation.[1083]

In other words, the idea is that Parliament should exercise its control over the national administration through legislation. The same applies to a large extent to the Government's control of its state authorities, although these possibilities are not as limited. Authorities have a duty of obedience to the Government, but this is limited in three important respects. Firstly, the Government's ability to control the administration is limited by legislation passed by Parliament, and thus the Government cannot issue binding directives to an authority that contravene a law passed by Parliament. Secondly, the Government can only take decisions that are binding on the authorities as a collective, which means that individual ministers cannot direct the authorities' activities. The third important restriction is the aforementioned requirement of independence, which means that the authorities must observe independence when applying the law and taking decisions in individual cases involving the exercise of public authority. One could say that this arrangement expresses the idea of a division between the political and administrative levels – in that the authorities are supposed to function independently within the organisation of the Government.[1084]

However, the strong position of the principle popular sovereignty does not mean that the legislative mandate is reserved exclusively for Parliament. Legislative power may in many cases be delegated, not only to the (politically constituted) Government, but also to a large extent to parliamentary, government or municipal authorities.[1085] Swedish authorities together account for the majority of Swedish regulations. In summary this means that the Swedish public sector is highly decentralised, with municipalities, regions and government authorities typically each making their own decisions when it comes to digitalisation and IT.

1.2. A Model Built on a Separation of Functions Rather than of Powers

The Swedish administrative organisation is divided into three levels – national, regional and local – at each of which elections are held to democratically composed decision-making assemblies.

At the national level, the elected assemblies consist of the Parliament (*riksdag*) and the (indirectly elected) Government (*regering*), both of which have legislative powers. The detailed division of legislative powers will not be discussed here, but Parliament is the main legislator, and the division of legislative powers is regulated in Chapter 8 of the Instrument of Government. The Government is assisted in its work by the Cabinet Office, which is mainly made up of a number of ministries with different responsibilities. By international standards, Sweden has a relatively small Government Office. This is explained by the fact that administrative tasks are largely carried out by authorities that sort under the Government (there are currently some 340 such authorities).[1086]

1082. Chapter 9 Instrument of Government.
1083. Rättsliga ramar för styrning av förvaltningen i Danmark och Sverige./ Wenander, Henrik. In: Nordisk administrativt tidsskrift, Vol. 93 No. 1 2016. p. 57-74, at p. 64 et sec.
1084. Administrative Independence Under EU Law: Stuck Between a Rock and Costanzo?/ Enqvist, Lena and Naarttijärvi, Markus. In: European Public Law, Vol. 27 2021, p. 713 (including references).
1085. The conditions for such delegation are found in Chapter 8 Instrument of Government.
1086. Europeanisation of the Proportionality Principle in Denmark, Finland and Sweden./ Wenander, Henrik. In: Review of European Administrative Law, Vol. 13 No. 2 2020. p. 133–152, at p. 135 et sec, referencing Nordic Reflections on Constitutional Law./ Husa, Jaakki. In: A Comparative Nordic Perspective 158 (Peter Lang 2002). See also Tjugofem år av europarätt i Sverige./ Reichel, Jane and Åhman, Karin. In: Svenska institutet för europapolitiska studier 5 2020, p. 53 et sec.

At the regional level, Sweden is divided into 21 counties where each county is administered by a government regional authority, a County Administrative Board *(Länsstyrelse)*. Their tasks include, for example, coordinating regional emergency preparedness and the management of certain environmental issues, and issues related to regional business, social development, animal welfare, gender equality, integration, transport, infrastructure, and housing. Also at the regional level, Sweden is divided into 20 different so-called 'regions'. These are primarily responsible for health care, but also hold other responsibilities in areas such as regional development strategies and planning for regional transport infrastructure.[1087]

Finally, at the local level, Sweden is divided into 290 municipalities. Each municipality is run by a municipal council, which is an elected assembly that makes decisions on municipal matters. Municipalities are responsible for services such as schools, elderly care, culture and leisure, and water and sewage.

Although regions and municipalities have different geographical responsibilities and different overall responsibilities, there are also many overlaps and similarities between their basic legal powers and functions. Both regions and municipalities are constitutionally empowered to levy taxes on their residents to finance their activities.[1088] Both regions and municipalities also enjoy a fairly high degree of independence from Parliament and Government through the constitutionally enshrined so-called principle of local self-government. This means that municipalities and regions are, by default, granted the authority for self-determination that is independent and unrestricted. While the central government is responsible for ensuring that local governance functions in a manner that supports a stable economy, it also establishes some limitations for self-governance through legislation. However, municipalities have the right to exercise autonomy beyond what is prescribed by the Parliament and the Government within the established framework. Only the Parliament can limit this autonomy by imposing tasks on regions or municipalities by ordinary legislative acts.[1089]

The constitutional mandate for local self-government states that any restrictions on municipal self-government should not go beyond what is necessary with regard to the purposes that have prompted it.[1090] Taken together, this essentially means that the Parliament is obliged to respect a principle of proportionality before placing any statutory burdens on regions or municipalities, thus creating a presumption of local self-government. Despite the constitutional status of the principle, however, it must be said that the activities of both the regions and the municipalities are today largely governed by law. Despite this principle of local self-governance, there is thus nevertheless extensive statutory regulation that imposes a number of mandatory tasks on municipalities. In addition, there has been a tendency to impose more and more statutory tasks on municipalities, with a consequent reduction in the scope for local self-government. Swedish state control over municipalities and regions has increased especially since the early 1990s, both through regulatory control and through targeted government grants or agreements and strategies with more or less detailed objectives.[1091] This has, for example, spurred a debate in political and legal literature on the de facto strength of the principle. In other words, despite local self-government, there is still a relatively substantial basis for the Parliament to control parts of local government work. Notably, this control has not been extensively exercised in the realm of digitalisation matters. However, one important example exception, to which I will return in section 2.3, is the introduction in the Local Government Act (*Kommunallag (2017:725)*) of a power to make decisions automatically for a large part of municipal decision-making.

1087. Sections 5–7 law (2010:630) on regional development responsibility (*lag (2010:630) om regionalt utvecklingsansvar*).
1088. Chapter 14 Section 4 Instrument of Government.
1089. Chapter 8 Section 2 Instrument of Government.
1090. Chapter 14 Section 3 Instrument of Government.
1091. Statlig förvaltningspolitik och kommunal självstyrelse – utvecklingstendenser och framtidsfrågor./ Edström Fors, Eva. Statlig förvaltningspolitik för 2020-talet - en forskningsantologi. ed./ Statskontoret 2020. p. 69 et sec.

In summary, the Swedish administrative structure, characterised by its national, regional, and local levels, reflects a tiered and decentralised governance approach. The relatively strong independence that these levels have in relation to each other also creates a dynamic interplay of autonomy and collaboration. This has shaped a diverse landscape where regions and municipalities, while constitutionally empowered for self-determination, navigate a regulatory environment that has evolved over time, impacting the extent of their local self-government. As will be developed in the next section, this is also one critical aspect discussed in relation to Swedish governance strategies for the digitalisation of public administration, highlighting the balancing between local autonomy and centralised oversight in the face of technological advancements.

1.3. Digitalisation in the Face of the Decentralised Swedish Administrative Order

It is a recurring notion that has been surfacing both in research and in legal policy contexts that the Swedish administrative model may not be well suited to the realisation of broad and comprehensive digitisation strategies.[1092] The manifestations or the legal anchoring of this notion is, however, rarely explored more in depth. What is usually meant is that the Swedish decentralised administrative structure, in which the relatively large degree of independence that the authorities enjoy, can make it difficult to implement digitalisation initiatives which require cross-sectoral solutions and initiatives. The separate and independent authorities are usually responsible discretely and individually for interpreting their regulated mandates, where, as has been shown, neither the government nor other authorities are allowed to exert pressure (although the government does have the authority to influence such initiatives mainly through regulation). As will be shown, neither the Parliament nor the Government makes much use of their options for detailed regulatory control of digitalisation initiatives in public administration. Although increasingly common, it is still fairly unusual that statutory obligations to implement specific digitalisation initiatives are placed directly on public authorities. More common is that the Government opts to, via decisions or appropriation directions, assign authorities to cooperate with a defined set of other authorities for a defined digitalisation objective.[1093] Such governance options are, however, only available to the government in relation to government authorities. For the municipal level (both local and regional), the government's available governance tools include the enabling or encouraging of digitalisation initiatives by, for example, allocating budget funds.[1094]

In 2018 the OECD concluded, in an evaluation of Sweden's digital transformation, that Sweden is far ahead in utilising the opportunities of digitalisation, but that the government needs to develop its capacity for analysis and monitoring in order to improve its governance of the sector.[1095] Partially against this background, the Swedish Agency for Public Management (*Statskontoret*) (which is the Swedish Government's organisation for analysis and evaluation of state and state-funded activities), evaluated the Swedish government's digitalisation governance. The authority found that there are few Swedish authorities with direct statutory responsibilities in relation to national public digitalisation policy (it identified the Swedish Post

1092. The Swedish Administrative Procedure Act and Digitalisation./ Magnusson Sjöberg, Cecilia. 50 Years of Law and IT. The Swedish Law and Informatics Research Institute 1968-2018. ed./ Peter Wahlgren. The Swedish Law and Informatics Research Institute 2018. p. 309-320, at p. 320.
1093. Styrning av digitala investeringar delrapport./ The Swedish Agency for Public Management (*Statskontoret*) dnr 2020/40-5. p. 12 et sec.
1094. The Swedish local government regime, managed through municipalities, is fundamentally based on the principle of local self-government, Chapter 1 Section 1 Instrument of Government, where the municipalities themselves choose and prioritise their tasks. Swedish municipalities do have many regulated responsibilities, but as any statutory obligation restricts the principle of local self-government these must be given in the form of a law and not restrict local self-government beyond what is necessary, pursuant to chapter 8, Section 2, paragraph 3 and Chapter 14, Section 3, of the Instrument of Government. This means that the Government lacks direct powers to impose tasks on the municipalities.
1095. Going Digital in Sweden – OECD Reviews of Digital Transformation. OECD, 2018. p. 13 et sec.

and Telecom Authority *(Post- och telestyrelsen*) and The Agency for Digital Government (*Myndigheten för digital förvaltning*), DIGG, as having the most explicit and pronounced responsibilities). The authority, however, also found that responsibilities for various initiatives which contribute to those same digitalisation objectives were distributed amongst around 60 other Swedish authorities. One general finding was that the Government mainly controls these initiatives through temporary government assignments (rather than through regulation), and that many authorities contribute to digitisation objectives more indirectly by implementing various digitisation initiatives of their own within the framework of their instructions. The summary conclusion was that this arrangement overall appeared reasonable in light of that digitalisation should be seen as a means of achieving objectives in other areas. The overall assessment was therefore that the Swedish Government as a whole has an administrative structure for implementing initiatives in most areas of the national digitalisation strategy.[1096] On a similar note, DIGG, in a 2022 follow-up of the digitalisation of government authorities, concluded that while the Swedish administrative structure may be associated with some challenges to coordinated digitalisation initiatives, it can also be seen as particularly well suited to managing the changes brought about by digitalisation – precisely because the model is both decentralised and dynamic. Instead, the authority identified that the biggest challenges stem from a lack of understanding of what digitalisation of public administration means, as well as from a lack of a fundamental vision of how it can contribute to the development of society. DIGG emphasised collaboration between the various actors in the administration and open communication between the Government Offices and the authorities as a path to success.[1097]

The view that the Swedish administrative model creates challenges for the digitalisation of public administration is, thus, not unanimous. However, even though opinions on the drawbacks or benefits of the administrative model's configuration in relation to the feasibility of substantial digitisation initiatives may differ, it remains grounded in a multi-level governance system. This system intricately delegates the exercise of public power to an (in itself) intricate structure of public authorities, each possessing a substantial degree of independence from the central government. In the context of public sector digitalisation, this has meant that much of the digitisation work undertaken by Swedish authorities to date has taken place within the separate authorities. As will be seen further on in this section, the Swedish government has in many cases, at a general level, pressed for the imperative to increase digitisation, automation, or the use of artificial intelligence in public administration, and has also allowed these ambitions to be reflected in the budgets of the authorities.[1098] However, in general there has been little direct steering of the authorities' digitisation work by the Parliament and the Government. As a result, there is relatively little national legislation that directly regulates digitisation efforts or the conditions for, for example, automating administrative activities. At the same time, however, the EU, through regulations such as the General Data Protection Regulation,[1099] the Singe Digital Gateway Regulation,[1100] has introduced direct imperatives or requirements for Swedish national authorities to collaborate as well as design and implement the technical solutions required for compliance.[1101]

1096. Fortsatta former för digitaliseringspolitiken - Utvärdering av Digitaliseringsrådet och kartläggning av regeringens styrning./ Statskontoret 2020:3. p. 12.
1097. Uppföljning av statliga myndigheters digitalisering 2021 - en enkätundersökning./ Agency for Digital Government (*Myndigheten för digital förvaltning*) 2021 dnr: 2021-2731. p. 47 et sec.
1098. See section 3.
1099. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
1100. Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012.
1101. See, for example, Långsiktig utveckling och förvaltning av datadelning med särskilt fokus Sveriges nya dataportal som en förvaltningsgemensam digital resurs för att främja tillgång och användning av data till nytta för hela samhället. Delrapport avseende uppdrag främja delning och nyttiggörande av data./ Agency for Digital Government (*Myndigheten för digital förvaltning*) 2021 dnr: 2021-1502.

The Swedish constitutional framework, in conjunction with its administrative structure, is thus designed to ensure that government authorities apply the law and make decisions in individual cases autonomously, free from interference by the government or other entities. As a result, digitisation efforts within the Swedish public administration have frequently operated with limited direct national political oversight. However, as the Swedish mode of governance revolves much around governance by law, it is time to turn to the general tendencies in the Swedish legislative approach to digitalisation efforts within public administration.

2. Swedish Rule of Law and Good Administration Principles in Light of Public Sector Digitalisation

The digitalisation and automation of public administration has the potential to introduce tensions concerning the administration's capacity to uphold the rule of law and principles of good administration in varied ways. This may involve diverse aspects of the authorities' activities, including a reduction in transparency as technology introduces an element of opacity to the exercise of their power. The digital transformation could also introduce or amplify risks to personal integrity, life, health, and national security, adding layers of complexity and potential vulnerabilities in these areas. These examples underscore the intricate interplay between technological advancements and legal frameworks, highlighting their implications for the rule of law and good administration in the context of public sector digitalisation. The subsequent sections will therefore, from the perspective of Swedish public sector digitalisation, delve into main aspects and regulatory conditions for public sector digitalisation across human rights, constitutional, and administrative law levels.

2.1 Swedish Public Sector Digitalisation and Human Rights Law

A comprehensive account for Sweden's international commitments is not expedient here. Sweden is, however, an EU member state and has also ratified several international human rights instruments, including the United Nation, UN, Convention on the Rights of the Child,[1102] CRC, the UN Convention on the Elimination of All Forms of Discrimination Against Women,[1103] CEDAW, the UN Convention on the Rights of Persons with Disabilities,[1104] CRPD, and the UN International Convention on the Elimination of All Forms of Racial Discrimination,[1105] ICERD. Sweden has also ratified several regional human rights instruments, including the Council of Europe´s European Convention on Human Rights, ECHR, and the European Social Charter,[1106] ESC, (with the revised charter).

Of the above-mentioned instruments, the ECHR and the CRC enjoy special legal status in Sweden as they are both legal instruments which have been incorporated in the national legal order. The ECHR is often said to enjoy a semi-constitutional status, as Chapter 2 Section 19 of the constitutional Instrument of Government prohibits any regulatory body to adopt any law or other provision which contravenes Sweden's undertakings under the ECHR. As the EU Charter of fundamental rights,[1107] CFR, in turn, holds the rights guaranteed in the ECHR as the minimum standard for the rights of the charter, this means that the ECHR and thus the ECtHR case law must be taken into consideration by national legislators utilising the space for manoeuvre provided for by EU and other national legislation to regulate and implement different digitalisation strategies.[1108] No comprehensive legal study on the ECHR's influence on the design

1102. Convention on the Rights of the Child, 20 November 1989, United Nations.
1103. Convention on the Elimination of All Forms of Discrimination Against Women, 18 December 1979, United Nations.
1104. Convention on the Rights of Persons with Disabilities, 24 January 2007, United Nations.
1105. International Convention on the Elimination of All Forms of Racial Discrimination, 21 December 1965, United Nations.
1106. European Social Charter, 18 October 1961, ETS 35, Council of Europe.
1107. Charter of Fundamental Rights of the European Union [2000] OJ C 364.
1108. Article 53 CFR.

of Swedish national legislation affecting the legal conditions for digital public administration has yet been done. However, at least in those legislative inquiries which have been broadly tasked with examining the boundaries of current law as well as the need for legislative initiatives in the field of digitalisation, especially discussions about the Article 8 ECHR right to respect for private and family life seems to have been influential. This is the case mainly against the background of the technologies' associated risks of increased privacy intrusion through their reliance on, or capacity to, process large amounts of personal data.[1109] There is, however, as of yet, no national case law where the rights and freedoms of the ECHR has been tried against the imposition of limitations on what national legislation may permit in a national and digital administration setting.

The CRC's legal status in Sweden has a different orientation than the ECHR's. The convention has no constitutional anchoring but is since 2018 incorporated into Swedish law via the Law (2018:1197) on the United Nations Convention on the Rights of the Child *(Lag (2018:1197) om Förenta nationernas konvention om barnets rättigheter)*, which states that the Articles 1-42 of the CRC shall apply as Swedish law. The stated aim was to clarify for those tasked with applying Swedish provisions affecting children's rights, such as administrative authorities and legal practitioners, that they must interpret such provisions so that they conform with Sweden's obligations under the CRC. Consequently, the CRC should therefore be applied by authorities and courts as a binding legal instrument (although the CRC does not take precedence over national legislation). As of yet, the incorporation of the CRC does not seem to have led to any direct national regulatory imprint in relation to the legal conditions for digital public administration. There are, for example, no direct national provisions related to technologically assisted public administration operations concerning children (such as automated decision-making or profiling, for example).[1110]

However, there are examples where the CRC's fundamental principle of the best interests of the child, through its substantive manifestations in national law, has been viewed to limit the possibilities of automating decision-making concerning children. Although the principle of the best interests of the child antedates the CRC in parts of Swedish national law, the Convention reinforced the principle's legal status and impact outside the area of custody and access issues.[1111] In preparatory works relating to the legal conditions for municipalities to engage in automated decision-making, the type of procedural requirements introduced to ensure that account is taken to the best interests of the child were discussed as possibly affecting which decisions on children that can be automated. The preparatory works exemplified and expressed the opinion that the legal requirements for carrying out adoption investigations (Chapter 14, sections 4-5 of the Children and Parents Code *(Föräldrabalk (1949:381))*) must be taken to mean that only a natural person can perform them. Another mentioned example was the requirement in Chapter 11, Section 10 of the Social Services Act, SSA, *(Socialtjänstlag (2001:453)),* requiring that children must be given the opportunity to express their opinions in matters relating to them. As it was considered difficult to ensure that the child's views in such cases were accounted for by other means than a natural person, the view was that the regulation prohibits fully automated procedures where applicable. A further example is the regulation in Chapter 3, Section 3 as of the SSA, which imposes special competence requirements on caseworkers who perform certain tasks

1109. Swedish Governmental Inquiry 2018:25. Law as support the digitalisation of the administration (*Juridik som stöd för förvaltningens digitalisering*). p. 61 et sec.
1110. It should, however, be noted that children merit specific protection with regard to their personal data under the GDPR, as made clear in, for example, Recital 38, and that Recital 71 GDPR holds that decisions based solely on automated processing and which produces legal effects or similarly significantly affects an individual should not concern a children. The Article 29 Data Protection Working Party Guidelines on Automated Individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 28, also states that, where possible, controllers should not rely upon the exceptions in Article 22(2) GDPR to justify solely automated decision making about children, with legal or similarly significant effect.
1111. Barnkonventionens bärande idé: I barnets intresse./ Hammarberg, Thomas. In: SOU 1997:116, Bilaga till huvudbetänkande: Del 1 Barnets bästa – en Antologi 1997. p. 14.

in cases involving children and young people.[1112] This reasoning from the preparatory works have later been included in the non-binding but influential guidelines on automated decision-making in local and regional municipalities issued by The Swedish Association of Local Authorities and Regions.[1113] The CRC and its applications in Swedish national law thus have effects on the legal conditions for automating administrative tasks involving benefits or responsibilities relating to children.

As indicated above, a complete overview of the impact of Sweden's international or regional commitments on the national legal landscape for different aspects of public administration digitalisation cannot be given. In addition to the already mentioned instruments, the Convention on the Rights of Persons with Disabilities,[1114] CPRD is, however, also one instrument which have influenced Swedish law in various ways – and of interest here particularly in the area of digital services by public administrations. Sweden, like all member states of the EU including the EU itself, has ratified the CPRD.[1115] The convention intersects public digitalisation strategies or regulations as it includes obligations on the accessibility of public services and lays down obligations to ensure that digital services and decision-making systems respect the privacy of persons with disabilities.[1116] The CPRD's most direct influence on the Swedish digital public administration arises by proxy of the EU's Web Accessibility Directive,[1117] which draws from and builds on the CPRD.[1118] The Swedish implementation of the directive is found in the Act (2018:1937) on accessibility to digital public services.[1119] The act establishes a general obligation for public authorities as well as for other specified actors performing public tasks to comply with the accessibility requirements under regulations issued pursuant to the Act. More specific digital accessibility requirements are therefore specified and fleshed out by DIGG (via delegated regulatory powers),[1120] as well as supervised by DIGG in terms of compliance.[1121]

Furthermore, the CPRD has also laid the basis for the national Ordinance on the responsibility of state authorities for implementing disability policy. This ordinance places obligations on government authorities to ensure that their premises, activities and information are accessible to people with disabilities, and Section 1 of the ordinance explicates that the CPRD shall provide guidance in this work.[1122] Administrative authorities implementing digital solutions must therefore ensure, among other things, that technical choices, interfaces or the design of various public digital services do not exclude potential user groups. They must also try to ensure that new technologies are compatible with various additional services such as assistive devices that people with disabilities may need. Here, the Swedish Agency for Participation *(Myndigheten för delaktighet)* has a monitoring role for which the CPRD also is to form the basis of the work. The authority's overarching assignment is to promote the implementation of disability policy. The authority is also specifically assigned to contribute to the development of knowledge in matters relating to 'welfare technology'. This assignment, amongst other, includes to monitor and where

1112. Swedish Government Inquiry 2021:16. A well-functioning system of elections and decision-making in municipalities and regions (*En väl fungerande ordning för val och beslutsfattande i kommuner och regioner*]) p. 94.
1113. Automatiserat beslutsfattande och ny lag om proportionella val i kommuner och regioner./ Swedish Association of Local Authorities and Regions (*Sveriges kommuner och Regioner*) Cirkulär nr 22:47, dnr SKR2022/00578. p. 3.
1114. Convention on the Rights of Persons with Disabilities. Treaty Series, 2515, 3. United Nations. (2006).
1115. United Nations Convention on the Rights of Persons with Disabilities. European Commission https://ec.europa.eu/social/main.jsp?langId=en&catId=1138. Accessed 12 December 2023.
1116. Articles 3 and 9 CPRD.
1117. Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies.
1118. Recitals 12, 13 and 38 of the Web Accessibility Directive.
1119. Lag (2018:1937) om tillgänglighet till digital offentlig service.
1120. Section 2 Act (2018:1937) on accessibility to digital public services; Sections 3-5 Ordinance (2018:1938) on accessibility to digital public services [*Förordningen (2018:1938) om tillgänglighet till digital offentlig service*]; Statutory instrument on accessibility to digital public services (MDFFS 2019:2) [*Föreskrifter om tillgänglighet till digital offentlig service (MDFFS 2019:2)*].
1121. Section 6 Ordinance (2018:1938) on accessibility to digital public services.
1122. Section 1 Ordinance (2001:526) on the responsibility of state authorities for implementing disability policy (*Förordning (2001:526) om de statliga myndigheternas ansvar för genomförande av funktionshinderspolitiken).*

necessary participate in strategically important national and international standardisation in welfare technology and accessibility, and work to ensure that accessibility and universal design are included in relevant standards.[1123]

This short account for Sweden's international and regional legal commitments shows that these make up an intricate web of obligations in the human rights law area, which intersects with digitalisation policies as well as digitalisation legislation in different ways. As introduced in section 1.3, the Swedish legislature generally has not made much use of the option to enact technology specific regulations. Consequently, the considerations related to international and regional legal commitments, particularly in the field of human rights law, are not concentrated within dedicated technology regulations. Instead, these considerations are often dispersed across various sectors and regulations that are often designed without a specific focus on technology.[1124]

2.2 Swedish Public Digitalisation and Constitutional Law

At the constitutional level, the Swedish legal framework is built up around four fundamental laws: the 1974 Instrument of Government, the 1810 Act of Succession, the 1949 Freedom of the Press Act, the 1991 Fundamental Law on Freedom of Expression.[1125] Of these, especially the Instrument of Government and the Freedom of the Press Act have impacted the legal conditions for public administration digitalisation, while having a predominantly technologically neutral design.

The Instrument of Government contains, inter alia, fundamental provisions of the form of government, fundamental rule of law principles as well as basic protection of personal integrity. An in-depth analysis of the potential impact of these regulations on the digitalisation of public administration is beyond the scope of this section. However, some examples of where the administration's digitalisation efforts have led to discussions about compatibility with the regulation may be noted.

The Parliamentary ombudsman have, for example, found practises where digital communication is treated more favourably timewise than analogue (paper) communication without objective reasons, to be in breach of fundamental requirements to observe equality before the law as well as objectivity and impartiality.[1126] In the case, the Migration Agency had prioritised online applications over paper-based ones, for the reason of encouraging people to apply online.[1127] Another example relates to the social services' use of so-called welfare technology in performing care tasks. The core question has been whether the use of such technologies could conflict with the constitutional protection against significant intrusion into personal integrity (where such intrusions take place without consent and involves monitoring or mapping of the individual's personal circumstances), as protected in Chapter 2, Section 6 in the Instrument of Government. The Swedish committee on welfare technology in elderly care in 2020 identified the perceived legal uncertainties in the area to be a decisive obstacle to the government's policy objective of increasing the use of such technologies.[1128] Against this background, the Swedish government has therefore adopted specific statutory regulation explicitly clarifying that such uses must be based on consent of the individual and their cohabiting family.[1129]

1123. Sections 3 and 4 Ordinance (2014:134) with instructions for the Swedish Agency for Participation (*Förordning (2014:134) med instruktion för Myndigheten för delaktighet*). The agency is thus tasked with monitoring the digitalisation of the Swedish administration based on the requirements of the CPRD, but does not function as a supervisory body, Från digital teknik till digitalisering Redovisning av ett regeringsuppdrag om delaktighet, självbestämmande och trygghet./ Swedish Agency for Participation (*Myndigheten för Delaktighet*) Nummer 2019:7 2019. p. 6 et sec.
1124. See further in section 3.4.
1125. Kungörelse (1974:152) om beslutad ny regeringsform; Successionsordning (1810:0926)]; Tryckfrihetsförordning (1949:105)]; Yttrandefrihetsgrundlag (1991:1469).
1126. Chapter 1. Section 9 Instrument of Government.
1127. Swedish Parliamentary Ombudsman, decision 2015/16:JO1, ref. 5497-2013.
1128. Swedish Governmental Inquiry 2020:14. Future technologies in the service of care *Framtidens teknik i omsorgens tjänst*. p. 425.
1129. Swedish Legislative Bill 2022/23:131. Welfare technology in elderly care *Välfärdsteknik inom äldreomsorgen*, as will start to apply in March 2024.

Lack of clarity about the constitutional limitations on the digitalisation of public administration has been identified by various official inquiries. One such example, which was highlighted by the The Digitisation Law Committee *(Digitaliseringsrättsutredningen)*, is the legal uncertainty regarding if and under what circumstances the utilisation of private companies for developing systems used to make automated decisions may conflict with the express prohibition in Chapter 12 Section 4 of the Instrument of Government against delegating administrative functions which involves the exercise of public authority to other legal entities or to individuals without statutory recognition.[1130] Another example is that the Integrity Committee *(Integritetskommittén)* identified diverging interpretations and applications of Chapter 2 Section 6 in the Instrument of Government between different official inquiries, authorities as well as within the Government Offices. The provision protects individuals in their relations with the public institutions against invasions of personal privacy, and thus aims to strike a balance between, inter alia, individual interests of privacy protection and the benefits of integrity intrusive data processing often associated with public administration digitalisation. The committee stressed that a more uniform understanding and application of the provision would benefit both the protection of privacy and the digitalisation of the administration.[1131]

For digitalisation, the Freedom of the Press Act also importantly features a general principle of public access to official documents.[1132] In relation to the digitalisation of public administration, this principle has primarily raised questions about when information should be considered official in digital contexts. Unlike when both internal as well as incoming and outgoing communication was primarily handled through paper documents, the transition to new digital communication and data management methods has in some cases been associated with certain difficulties in assessing what the right of access to official documents covers in digital contexts. By extension, questions about transparency in the digital administration have therefore been raised, where the right to transparency in automated decision-making has received particular attention. Unlike the Instrument of Government, the Freedom of Press Act does contain some specific provisions that have been added to clarify its application against the background of some technological developments.[1133] Following a legislative proposal in 2001, the act now includes a specific provision on so-called material recorded for automatic data processing.[1134] Clarifications on the scope and meaning of the principle of public access to official documents have also been made in case law. The Supreme Administrative Court, for example, has clarified that that computerised messages, so-called cookie files and global/history files, are official documents,[1135] and that the same applies to e-mail logs of the authorities.[1136] A related challenge is that digitalisation has shifted the focus from the documents themselves to the information content or data as the carriers of information. Questions have then arisen about the extent to which the authorities, within the framework of the principle of public access to official documents, must assist in compiling information that is not readily available. Here, for example, the Supreme Administrative Court, with reference to a statement in the preparatory works of the act, has stated that the provision in Chapter 2, Section 3, second paragraph of the Freedom of the Press Act is an expression of the principle of equality, which means that the public should have access to computerised information to the same extent as it is available to the authority.[1137] However, the court did not consider that a compilation of data from a recording for automated data

1130. Swedish Governmental Inquiry 2018:25. Law as support the digitalisation of the administration (*Juridik som stöd för förvaltningens digitalisering*). p. 189.
1131. Swedish Government Inquiry 2017:52. How we strengthen personal integrity (*Så stärker vi den personliga integriteten*). p. 20.
1132. Chapter 2 Freedom of the Press Act.
1133. The Swedish Administrative Procedure Act and Digitalisation./ Magnusson Sjöberg, Cecilia. 50 Years of Law and IT. The Swedish Law and Informatics Research Institute 1968-2018. ed./ Peter Wahlgren. The Swedish Law and Informatics Research Institute 2018. p. 309-320, at p. 311.
1134. Swedish Legislative Bill 2001/02:70. The principle of public access to official documents and information technology (*Offentlighetsprincipen och informationstekniken*).
1135. Swedish Supreme Administrative Court RÅ 1999 ref 18.
1136. Swedish Supreme Administrative Court RÅ 1998 ref 44.
1137. Swedish Supreme Administrative Court HFD 2015 ref 25 with reference to Legislative Bill 2001/02:70, p. 16.

processing that requires a labour input of 4–6 hours as being accessible with such routine measures as referred to in the provision.[1138]

As shown by the examples above, there has been some discussions as well as legal developments regarding how Swedish constitutional provisions impacts the legal conditions for digitalising the public administration. Generally, however, complex legal questions on the boundaries and application of constitutional provisions in specific digital contexts are often left to the authorities themselves to resolve through statutory interpretation.[1139] Further legal analysis or developments in case law would therefore be welcome.

2.3 Swedish Public Digitalisation and Administrative Law

At the administrative level, the Administrative Procedures Act (*Förvaltningslagen 2017:900*), APA, serves as the legal framework in Swedish law that delineates the fundamental standards governing effective and legally sound administrative practices. Its primary objective is to ensure legal certainty in interactions with public authorities. The APA is generally applicable on all the processing of matters at administrative authorities as well as the processing of administrative matters at the courts.[1140] The applicability of specific APA-provisions may be overridden through exceptions in ordinary acts or government ordinances, but overall, the regulation has a broad applicational scope on public sector operations. It is thus an important component of the legal, technical, and organisational infrastructures within which the authorities at the national as well as regional and local levels operate. The APA is therefore also a central legislation to ensure that the digitalisation and automation of public administration does not challenge the soundness of their operations from a rule of law perspective.[1141] The Swedish emphasis and preference for a technology neutral approach to legislation is also evident in the APA. The technology-neutral design of the APA means that the actual materialisation of the various legal certainty requirements in the regulation's provisions need to be interpreted and applied to digital environments, both internally within authorities and in relation to individuals.[1142]

Over the past 40 years, the APA has undergone two major reforms, in 1986 and 2017. Already at the time of the 1986 reform, public authorities were using technology to varying degrees to process their cases. The 1986 APA did not, however, contain any provisions that specifically regulated either the digitalisation or automation of case administration. The preparatory works did nevertheless hint an emerging recognition that different types of technological support was becoming an increasingly integral aspect of the administrative practice, as these made clear that the act applied also to automated procedures and automated decision-making.[1143]

The first time the APA was subject to any amendments explicitly aimed at adapting the wording of the legislation to some features of technological developments was as late as in 2003. An express (and since then repealed) provision which established an obligation for authorities to respond private individuals via telefax or email was then introduced.[1144]

1138. Swedish Supreme Administrative Court HFD 2015 ref 25. See also, section 4.1.
1139. Swedish Governmental Inquiry 2018:25. Law as support the digitalisation of the administration (*Juridik som stöd för förvaltningens digitalisering*). p. 146.
1140. Section 4 APA.
1141. The Swedish Administrative Procedure Act and Digitalisation./ Magnusson Sjöberg, Cecilia. 50 Years of Law and IT. The Swedish Law and Informatics Research Institute 1968-2018. ed./ Peter Wahlgren. The Swedish Law and Informatics Research Institute 2018. p. 309-320, at p. 320.
1142. The Swedish Administrative Procedure Act and Digitalisation./ Magnusson Sjöberg, Cecilia. 50 Years of Law and IT. The Swedish Law and Informatics Research Institute 1968-2018. ed./ Peter Wahlgren. The Swedish Law and Informatics Research Institute 2018. p. 309-320, at p. 311.
1143. Swedish Legislative Bill 1985/86:80. About a new administrative procedures act (*Om ny förvaltningslag*). p. 57.
1144. Swedish Legislative bill 2002/03:62. Some administrative law issues (*Några förvaltningsrättsliga frågor*). p. 12–13; IT-anpassningen av 5 § förvaltningslagen – inte bara en kodifiering av praxis./ Magnusson Sjöberg, Cecilia. In: Förvaltningsrättslig Tidskrift, No. 3 2004, p. 285-305. At p. 286. This provision has in the current APA been replaced by a more technology-neutral provision, according to which the authorities must be available for contacts with individuals and inform the public about how and when such contacts can be made, Section 7 APA. See also, Regulating Automation of Swedish Public Administration./ Reichel, Jane. In: CERIDAP No. 1 2023, p. 75–94.

By the time of the 2017 reform of the APA, the technology use had obviously increased significantly in most areas of public administration. There were discussions on whether and how to reflect this new standard mode in the APA, and the initial proposal of the 2017 APA did include some substantive provisions relating to digitalisation - in particular to the handling of electronic documents and how to determine their time of arrival.[1145] These proposals did, however, not follow through to the final act. Proposals for some more technology-specific or digitalisation-friendly provisions in the APA have continued to be made to some extent. Some of the discarded proposals of explicit regulation on the handling of electronic documents were, for example, repeated by The Digitisation Law Committee (*Digitaliseringsrättsutredningen*) shortly after the 2017 APA entered into force. That inquiry, which was tasked with proposing legislative amendments to improve the legal conditions for a digitally cooperating administration, also made further propositions for additions and amendments to the 2017 APA – such as to add an express obligation for authorities to appropriately designate one or more digital reception functions and rules on digital communication (including a right for individuals to notify that they do not wish to communicate digitally).[1146] However, none of these proposals have yet been realised. Even though there have been some investigations and proposals to provide the APA with more specific regulation in relation to the increasingly digital forms of administration, the regulation is thus still essentially characterised by a technology-neutral approach.

As will be elaborated, an exception to the APA's essentially technology-neutral approach is that the regulation since its 2017 reform clarifies that decisions may be made automatically. The relevant Section 28 of the APA is, however, primarily of a declaratory nature. The provision does not specify the substantive conditions for lawful automated decision-making but was rather implemented against the background of many years of legal uncertainty as to whether automated decision-making in Swedish administrative law should be considered to require explicit legal authorisation. Before the 2017 APA, public automation efforts had been the subject of some, but not particularly intense, discussions in legal research and the legislative process. As fully automated decision-making became more prevalent in Swedish public administration, debates did emerge particularly around the legality of such practises and whether specific statutory recognition was a prerequisite.[1147] This legal uncertainty was reflected though the fact that specific legislation expressly allowing for specific automated decision-making was introduced in some legislative sectors, such as the social security, tax and transportation sectors, while automated decisions were also made in other government sectors without any such specific statutory authorisation.[1148]

A public inquiry carried out by the so-called E-delegation (*E-delegationen*) investigated and made the overall assessment that Swedish law did now require any explicit statutory recognition for the authorities to make decisions automatically, and recommended as a consequence that all the sector specific regulations allowing for automated decision-making that had already been introduced should be repealed.[1149] Perhaps boosted by the E-delegation's conclusions, it over time became widely accepted that government authorities could switch from manual to

1145. Swedish Governmental Inquiry 2010:29. A new Administrative Procedures Act (*En ny förvaltningslag*). p. 53 and 393. See also the report Elektroniska förfaranden – delredovisning av Förvaltningslagsutredningen (Ju 2008:08) which was annexed to the inquiry. p. 729-787.
1146. Swedish Governmental Inquiry 2018:25. Law as support the digitalisation of the administration (*Juridik som stöd för förvaltningens digitalisering*). p. 35. It may also be mentioned that the same public inquiry also proposed that a provision be introduced in the Public Access to Information and Secrecy Act [*offentlighets- och sekretesslagen (2009:400)*] stating that an authority must ensure that information can be provided on how the authority, when handling cases or matters, uses algorithms or computer programmes that, in whole or in part, affect the outcome or decision in automated selections or decisions. However, no such provision was introduced.
1147. Swedish Government Inquiry 2014:75. Automated decisions – fewer rules mean clearer regulation (*Automatiserade beslut – färre regler ger tydligare reglering*). p. 49.
1148. Chapter 112, Sections 6-7 in the Social Insurance Code (2010:110) (*Socialförsäkringsbalken (2010:110*); Swedish Government Inquiry 2014:75. Automated decisions – fewer rules mean clearer regulation (*Automatiserade beslut – färre regler ger tydligare reglering*). p. 24 et sec.
1149. Swedish Government Inquiry 2014:75. Automated decisions – fewer rules mean clearer regulation (*Automatiserade beslut – färre regler ger tydligare reglering*). p. 64 et sec.

automated decision-making without the need for express legislative authorisation.[1150] Against the recommendations of the E-delegation, however, some sector specific regulation authorising automated decision-making remained in force.[1151] Requests for a clear and comprehensive regulation were therefore reiterated, and eventually led up to the introduction of the provision that made it expressly clear that no specific legal authority is required for public automated decision-making in Section 28 of the 2017 APA. The government acknowledged that automation has become increasingly prevalent in those parts of the administration that handle a large volume of cases, and by enshrining the use of automated decision-making in law, it sought to eliminate the need for specific rules in sector-specific acts. The specified overarching goal was to improve the conditions for the continued growth of digital administration.[1152]

Without further specification, Section 28 now simply states that decisions can be made automatically and according to the preparatory works this merely codifies the law that had already been established.[1153] The first paragraph in Section 28 now reads as follows:

'A decision can be made by an officer on their own or by several jointly or be made automatically. In the final processing of a matter, the reporting clerk and other officers can participate without taking part in the determination.'

The novelty here is the addition of the phrasing 'or be made automatically' to the provision regulating how decisions may be made. Notably, however, the provision does not impose any explicit limitations or include any additional criteria or instructions regarding which types of decisions that are suitable for being made automatically.

Section 28 of the APA thus makes clear that there are no formal constraints on automating any type of administrative decision-making, while at the same time also making it clear that it is not a qualifying rule (but rather one of declaratory nature). Whether a particular decision may be made automatically must thus be assessed against the broader legal context in which it is to be made.[1154] For one, the automated decision-making system must operate in a lawful way, meaning that it must comply with substantive rules such as data protection rules, data security rules, etc. It also means that the automatic decision-making process must meet the fundamental requirements of legality and equal treatment, as well as the principles of good administration set out in the APA (such as those provisions aimed at materialising the right to be heard or the duty to state reasons, for example).

Since the fact that a system has a lawful design does not guarantee that it will also produce lawful decisions, a system's capacity to support or make both procedurally and substantively correct decisions also needs to be qualitatively evaluated before it could be put into lawful use. While such a qualitative evaluation is predominantly risk-based, the question of whether a system can be trusted to produce lawful decisions is of course imperative from a legality- as well as a broader rule of law perspective. It is noteworthy here that Swedish administrative law does not, neither in the APA or any other comprehensive administrative regulation, expressly regulate the responsibility for conducting such proactive or preventive evaluations of an automated system's functionality. However, such obligations in some cases apply under European law. Express obligations to make data protection impact assessments where a type of processing, in

1150. This question, as will be elaborated further on, had a slightly different legal orientation in the local government sector.
1151. See, for example, Chapter 112 Sections 6–7 *(Socialförsäkringsbalk (2010:110))*.
1152. Swedish Legislative Bill 2016/17:180. A modern and legally secure administration – a new Administrative Procedures Act (*En modern och rättssäker förvaltning – ny förvaltningslag*). p. 179.
1153. Section 28 APA.
1154. As noted by Hanne Marie Motzfeldt and Frederik Waage in Rule of Law and Public Digitalisation – Pilot Project . Nordic Council of Ministers 2021:502 2021. p 24., there was nothing in the preparatory works concerning possible constitutional or human rights law frameworks for application of Section 28 APA.

particular when using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons follow from Article 35(1) GDPR.[1155] In 2019, for example, the Swedish Authority for Privacy Protection (*Integritetsskyddsmyndigheten*) found the municipality of Skellefteå to have acted in breach of Article 35 GDPR for having deployed facial recognition tools for purposes of identification in local schools without having performed a data impact assessment.[1156] Furthermore, as far as the technologies used will qualify as AI technologies under the EU Artificial Intelligence Act,[1157] AIA, this regulation will at least for high-risk AI systems (such as those deployed in the areas of access to and enjoyment public services and benefits) likely require fundamental rights impact assessments and conformity assessments before they are put into used, as well as and risk management systems to be implemented and maintained during their use.[1158]

Thus, even though there are some regulations in place at the EU level requiring impact assessments to be made prior to the use of IT systems for public administration or decision-making in cases where the risks for adverse consequences are high, and even though the principle of legality contains an abstractly formulated requirement to assess, consider and minimise risks to unlawful practises, there are no explicit, general or comprehensive rules at the Swedish national level. For Swedish authorities assessing whether an automated system can operate lawfully as well as with low risk of adverse consequences to legality or proportionality, for example, the APA is therefore a key legal instrument to serve as a yardstick for the rule of law requirements to be realised. At the same time, and as a result of the technology neutral approach of the APA combined with the relatively sparse commentary or explanation in legal preparatory works as well as in case law, there are many legal issues still in need of clarifications in order for the act's framework in the digital context to relief more clearly. Some of these issues, including the national discussions around them, will be addressed below.

One example where the APA's technologically neutral language has led to legal uncertainty relates to how the legality of digital administrative practices should be affected when they take a form that in a strictly formal sense does not match the wording of the regulation. As an example, Section 31 of the APA states that there for every written decision should be a document showing which person or persons took the decision (or were the reporting officers or participated in the final processing without taking part in the determination of the decision). As this requirement is not realisable in contexts where decisions are made fully automated (as no human decision-maker has taken part in the decision and therefore cannot be named), a formalistic interpretation of the Section 31 requirements would mean that the APA, despite Section 28 expressly allowing for automated decision-making, hinders such decisions. The preparatory works of the APA does directly address this issue from a pragmatic standpoint and argue that since automated decisions may not fulfil all the formal requirements regarding what information to be

1155. As most processing of personal data are based on Article 6(1)(e) of the GDPR (processing necessary for performing tasks in the public interest or exercise of official authority vested in the controller), and as Article 35(10) states that no impact assessment needs to be made in cases where the processing has a legal basis in Union or Member State law and such an assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, an obligation to carry out an impact assessment does not arise in all cases where there is a high risk to the rights and freedoms of natural persons. In its commentary to Article 35(10) GDPR, The Swedish Authority for Privacy Protection *[Integritetsskyddsmyndigheten]*, noteworthily, states that it as of yet does not know of any cases where this exemption applies, https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/konsekvensbedomningar-och-forhandssamrad/dataskyddsforordningen-om-konsekvensbedomningar-och-forhandssamrad/, Accessed 12 December 2023. See, however, for example, Swedish Legislative Bill 2017/18:112. Adaptation of labour market register regulations to the EU Data Protection Regulation (*Anpassningar av registerförfattningar på arbetsmarknadsområdet till EU:s dataskyddsförordning*). p. 31 et sec, where the Government stated that Article 35 GDPR did not require any new impact assessments to be made in relation to the design of the register regulations for certain labour market authorities as the processing of personal data covered by these regulations had already been subject to impact assessments at the time when they were adopted.

1156. Decision by Datainspektionen (now the Swedish Authority for Privacy Protection *(Integritetsskyddsmyndigheten)*) 2019-08-20, DI-2019-2221. The municipality was also found to have acted in breach of Articles 5 and 9 GDPR.

1157. EU Artificial Intelligence Act. References to the act in this chapter are based on the February 2024 text of the provisional agreement resulting from interinstitutional negotiations between the European Parliament and the EU Council of Ministers. This text outlines the content of the Regulation but may undergo minor, primarily editorial changes before final adoption.

1158. See Articles 9(1), 17(1), 19(1), 29 a and 43(1) AIA. See section 5.

included in written decisions, such requirements should not be taken as obligating the authorities to structure their decision-making process to include all information at all times, including in cases of automated decision-making. This argumentation was based on an application practise that had been established around Section 21 of the Government Agency Ordinance *(Myndighethetsförordningen 2007:515)*, which is a corresponding rule to Section 31 of the APA but which only applies to Government authorities.[1159] In other words, the preparatory works indicated that information which was not relevant to a specific decision-making process, such as names in automated decision-making, may be omitted from the formal decision. Today, however, there are still some public authorities which have express exemptions from the obligation to name decision-makers[1160] while other public authorities omits the decision-makers name from automated decisions without any explicit statutory exemption from the letter of Section 31 APA (just as argued in the preparatory works of the APA).[1161] This piecemeal regulation has been perceived as leading to unnecessary legal uncertainty, as clear from government official reports both before and after Section 28 of the 2017 APA was enacted.[1162] As of yet, no amendments has, however, been envisaged.

Another example of when the APA's aptness to protect values of good administration and the rule of law in digital contexts has been discussed relates to whether the regulation's included range of legal safeguards are sufficiently equipped to counterbalance those risks which may be specific to certain technologies or their uses. A specific example relates to the fact that neither the APA nor any other national regulation contains any explicit provisions requiring human oversight of automated decision-making processes. This is noteworthy given that the notion of 'human oversight' over technologies used in public administration, as will be seen, is likely to assume increasingly strong regulatory contours in the next years.

Human oversight measures are usually stressed as safeguarding measures which may (ideally) counterbalance some of the risks that the rigidity and datafication which the digitalisation or automation may premise on in technologically supported exercises of public power. What particular practises that the notion of human oversight may include is a matter of legal as well as scientific debate. In essence, however, the rationale behind human oversight typically involves utilising the more context sensitive judgements of humans to help identify errors or inconsistencies in the workings or outputs of automated systems, to avoid any inherent biases or injustices to affect the subjects which the systems assist in exercising powers on.[1163] The functions of humans overseers may thus include the perceiving and accounting for nuances and complexities which are relevant from a legal perspective, and the factoring in of discretion and human contextual assessments that may reveal a decision to be unfair or erroneous in a specific situation. Human oversight is thus a concept which may include many different more specific practises as well as focuses which the human overseer shall exercise in the course of his or her 'oversight'. The appropriate focus and sufficient extent of such oversight is also matter of debate, as is to what extent that elements of human oversight can be expected to counteract the risks of automation through complex systems.[1164]

1159. Swedish Legislative Bill 2016/17:180. A modern and legally secure administration – a new Administrative Procedures Act (*En modern och rättssäker förvaltning – ny förvaltningslag*). p. 185, 319. A corresponding rule to Section 31 of the APA is also found in Section 21 of the Government Agency Ordinance (2007:515) *(Myndighetsförordningen 2007:515)*.
1160. See, for example, Section 39 Ordinance (2017:154) with instructions to the Swedish Tax Agency *(Förordning (2017:154) med instruktion till Skatteverket)*; Section 14 Ordinance (2009:1174) with instructions for the Swedish Social Insurance Agency *(Förordning (2009:1174) med instruktion för Försäkringskassan)*.
1161. Regulating Automation of Swedish Public Administration./ Reichel, Jane. In: CERIDAP No. 1 2023, p. 75–94. At 82 et sec.
1162. Swedish Government Inquiry 2014:75. Automated decisions – fewer rules mean clearer regulation (*Automatiserade beslut – färre regler ger tydligare reglering*). p. 64; Swedish Governmental Inquiry 2018:25. Law as support the digitalisation of the administration (*Juridik som stöd för förvaltningens digitalisering*). p. 223.
1163. Approaching the Human in the Loop – Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts./ Enarsson, Therese, Enqvist, Lena and Naarttijärvi, Markus. In: Information & Communications Technology Law, Vol. 31. No. 1 2022, p. 123–153. At p. 128. 'Human Oversight' in the EU Artificial Intelligence Act: What, When and by Whom?'/ Enqvist, Lena. In: Law, Innovation and Technology, Vol. 15 No. 2 2023, 508-535. p. 1 et sec.
1164. 'Human Oversight' in the EU Artificial Intelligence Act: What, When and by Whom?'/ Enqvist, Lena. In: Law, Innovation and Technology, Vol. 15 No. 2 2023, 508-535. p. 4 et sec.

That human oversight is becoming an increasingly stressed safeguarding measure is visible through the Article 22 GDPR's enshrined right not to be subject to solely automated decisions, the EU AIA's Article 14 regulation of human oversight over high-risk AI systems, and the Council of Europe's draft of a new Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. As of yet, Article 22 GDPR and the right not to be subject not to a decision based solely on automated processing (of personal data), is the only one of the abovementioned provisions that have yet entered into force. The article establishes a main rule prohibiting fully automated decision-making. It does not, however, introduce a general right to human oversight where public administrations make fully automated decisions, as the article also includes the important exemptions to that prohibition.[1165] Importantly, Article 22.2(b) allows for decisions to be made fully (solely) automatically if authorised by Union or Member State law to which the controller is subject if this law also lays down suitable measures to safeguard the rights, freedoms and legitimate interests of the data subject. For public sector decision-making, Article 22 GDPR thus allows for rather generous exemptions, albeit conditional upon there being an appropriate level of safeguards assured through regulation. From the Swedish perspective and in the context of the digitalisation and automation of the national public administration, a relevant question has thus been whether a sufficient level of safeguards by the standards of the GDPR is guaranteed though the national legal system. Against this background, the APA, as it applies to the handling of matters at administrative authorities, has naturally been of interest in the national discussions.[1166] Although the GDPR was underway at the time of the 2017 APA revision, the preparatory works of the latter regulation did not touch upon whether Article 22 GDPR would prompt the need for introducing any specific safeguards in the national system. Later discussions in preparatory works as well as amongst legal scholars have, however, related to the interpretation of Recital 71 of the GDPR, as it states that any fully automated processing, even if mandated by law, should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention. Although non-binding, the recital's express mention of human intervention in combination with the phrasing 'should include' has spurred some national discussions on whether the recital implies that human intervention, in general or at least in some contexts, must be seen as a required safeguarding measure – and whether a right to human intervention therefore should be secured through an amendment of the APA.[1167]

That the Swedish government's position is that the APA in its present form contains a sufficient level of safeguards to allow for decisions to be made fully automated has, nevertheless, been made clear through later legislative bills.[1168] The Swedish Authority for Privacy Protection *(Then Datainspektionen,* now *Integritetsskyddsmyndigheten)*, which is the national competent data protection authority under GDPR, did not agree on this position and questioned that the generally applicable APA provisions show that the safeguarding requirements under Article 22(2)(b) are met.[1169] As indicated, however, the Government's stance on the matter is still that the APA's general provisions on administrative procedure, including the principles of legality, objectivity, and proportionality, as well as the right to be heard, the possibilities and obligations to correct, change and vary decisions, and make appeals, collectively provide adequate safeguards by the standards of Article 22 GDPR. The entering into force of the GDPR did thus not lead to any specific amendments of the APA, and no legislative proposals yet have concerned requirements of human intervention or oversight.

1165. Case C-634/21, OQ v Land Hessen, ECLI:EU:C:2023:957, paragraph 52.
1166. Section 1 APA.
1167. Den digitala statsförvaltningen – Rättsliga förutsättningar för automatiserade beslut, profilering och AI./ Karlsson, Rikard. In: Förvaltningsrättslig Tidskrift, No. 1 2020, p. 51-80. At p. 74 et sec.
1168. See for example Swedish Legislative Bills 2017/18:95 Adaptation of certain tax, customs and enforcement legislation to the EU Data Protection Regulation (*Anpassningar av vissa författningar inom skatt, tull och exekution till EU:s dataskyddsförordning*). p. 100; 2017/18:112 Swedish Legislative Bill 2017/18:112. Adaptation of labour market register regulations to the EU Data Protection Regulation (*Anpassningar av registerförfattningar på arbetsmarknadsområdet till EU:s dataskyddsförordning*). p. 64 et sec.
1169. Remissvar Juridik som stöd för förvaltningens digitalisering (SOU 2018:25)./ Datainspektionen (now the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten), DI-2018-7602.

Turning to the AIA, its Article 14 expressly includes human oversight as one safeguarding measure in relation to certain AI system usages. As the AIA takes effect in 2026, his provision will apply to all AI systems which qualifies as being high-risk systems, for example including AI systems deployed in many public sector settings such as where used in the areas of access to and enjoyment of essential private services and public services and benefits, or the administration of justice and democratic processes.[1170] The regulation will apply to both public as well as private parties, as well as to any deployment of high-risk AI systems (and not just in those cases where AI technologies are used to make decisions). It is, however, noteworthy that the focus of the AIA is on the technical capacity of AI systems to *enable* human oversight to be performed. This means that the draft indicates that requirements are imposed primarily on the oversight functionalities of AI systems, and that the regulation does not go so far as to impose *direct* requirements on system deployers (such as public authorities) to also utilise these oversight capabilities to any specified scope or modality. It should be added that system deployers, under the Articles 13 and 29 of the AIA, are obliged to use the system in accordance with its instructions – where instructions on human oversight performance may be included. Deployers must also ensure that ensure that the natural persons assigned to ensure human oversight of the high-risk AI systems have the necessary competence, training and authority as well as the necessary support. Overall, however, the AIA does not impose any direct requirements on public authorities to carry out human oversight at given intervals or on given impulses. The regulation nevertheless requires public administrations to provide the various AI systems they use with human oversight capabilities, which will at least indirectly raise questions about what should be overseen, when the oversight should be carried out and by whom.[1171] Swedish administrative law does not provide direct answers to these questions and there is reason to consider whether, for example, the APA or any national implementing legislation to the AIA should be amended to provide more direct guidance to the authorities on their responsibilities to carry out human oversight over AI systems. In the event of such a development there is, however, a need to consider, from a national perspective, whether a threshold effect in terms of available safeguards would be justified when only based on whether the authorities use AI systems as compared to when they use automated systems based on other technologies. Such threshold effects might appear unwarranted from the perspective of good administration, as other technologies may also build complex systems with associated risks of rigid and formalistic applications, where human oversight may be just as pertinent.

Further on, the Council of Europe's envisaged AI Convention states as its aim to set out standards for a human rights-based approach to AI.[1172] Article 15 of the draft includes the principles of transparency and oversight, which would oblige the contracting parties to ensure that adequate oversight mechanisms as well as transparency and auditability requirements tailored to the specific risks arising from the context in which the artificial intelligence systems are applied are in place. If the convention is finalised in a similar form as well as is ratified by Sweden, it is thus possible that it eventually will necessitate or encourage amendments to Swedish administrative law, in order to equip it with some more direct regulation ensuring a convention compliant level of human oversight.

All in all, and in the present, it is thus debatable whether any direct requirements for the Swedish legislator to introduce human review requirements in certain cases can be derived from the GDPR. Whether any such direct obligations are present at the European level will further depend

1170. Annex III 5 and 8 AIA. High-risk AI systems are defined in Article 6 AIA. Of relevance here is that 6(2) AIA refers to annex III as containing a list of AI systems to be categorised as high-risk in the regulation, based on the intended uses of the systems. The above exemplification is illustrative, and a complete list or analysis of which public sector uses of AI may be covered by the AIA will not be made.
1171. 'Human Oversight' in the EU Artificial Intelligence Act: What, When and by Whom?'/ Enqvist, Lena. In: Law, Innovation and Technology, Vol. 15 No. 2 2023, 508-535. p. 13 et sec.
1172. Revised Zero Draft [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law./ Council of Europe, Committee on Artificial Intelligence (CAI). CAI(2023)01 6th of January 2023.

on the application of the AIA and the final form of the future Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (which in turn also depends on ratification). The legal developments in the coming years will show whether the Swedish lack of specific human review or oversight regulation will be called into question. It seems likely that the issue of human oversight requirements needs to be monitored in Swedish law.

Another question that has brought to the fore the possible tensions between technology-neutral principles of good administration in the APA and the impact of these principles in digital or automated contexts, concerns the extent to which the duty to state reasons in Section 32 of the APA may impose any legal restrictions on the possibilities for automated decision-making. The ability of individuals to understand the grounds on which a decision has been made, and thus also the grounds on which public power has been exercised, is central to the functioning of the rule of law. This is important both for those that are subject to a decision to be able to challenge it, as well as for courts or other supervisory bodies to be able to scrutinise the legality of the exercised powers. As one of the known drawbacks of automated decision-making is the inability of, or challenges for, such systems to account for and respond to the specific circumstances of each individual case, it is typically a challenge for automated decision-making systems to produce individually tailored and sufficiently clear reasons in more complex cases.[1173] The ensuring that the introduction of automated decision-making does not come at the expense of the authorities' capacities to fulfil their duty to state reasons is thus also a matter of concern from a legal security and rule of law perspective.[1174]

Section 32 of the APA requires that reasons are stated for 'all decisions affecting a person in a not insignificant way' unless it is 'obviously unnecessary'. From the perspective of automation, it should therefore be noted, as a distinction, that the challenges to meeting these requirements are of a chiefly practical rather than of legal orientation. As long as the automated decision-making systems are technically able to produce sufficiently reasoned decisions by the standards of Section 32 APA (or any European standards that may apply to particular decisions), the provision does not lay down any limitations to automation. This difference is reflected in some preparatory works touching on issues related to automated decision-making in taxation and the municipal sector, where Section 32 of the APA is described as setting a 'practical' legal limit for which decisions that may be made automatically.[1175] While the distinction above is an important one, the legal content and scope of the obligation will nevertheless set one bar for lawful automated decision-making in Swedish administrative law.
An in-depth account for Section 32 APA is not expedient here. The preparatory works and decisions from the Parliamentary Ombudsmen lays down that the reasons given should include which circumstances that the decision-making authority have given importance and how they have been evaluated, and that this includes that the authority typically shall explain how it has assessed any objections made by the individual in the case.[1176] The preparatory works considered it to be 'obvious' that the reasons must be allowed to vary in scope and detail according to the importance and complexity of the case.[1177]

1173. Discretion, Automation, and Proportionality./ Enqvist, Lena and Naarttijärvi, Markus. The Rule of Law and Automated Decision-Making. ed./ Markku Suksi Springer, 2023 Cham, p. 147-178. At p. 158 et sec.
1174. This reasoning naturally also applies in relation to the obligation of the administration to give reasons for its decisions as stated in Article 42 (1)(c) of the CFR, when the Charter is applicable in the administration by national public authorities.
1175. Swedish Legislative Bill 2019/20:196 Revised rules for the taxation of agricultural units and for automated decision-making in property taxation [*Ändrade regler för taxering av lantbruksenheter och för automatiserat beslutsfattande vid fastighetstaxeringen*]. p. 34; Swedish Legislative Bill 2021/22:125 Elections and decisions in municipalities and regions [*Val och beslut i kommuner och regioner*]. p. 29.
1176. Swedish Legislative Bill 2016/17:180. A modern and legally secure administration – a new Administrative Procedures Act [*En modern och rättssäker förvaltning – ny förvaltningslag*]. p. 321; Swedish Parliamentary Ombudsman, decision 1994/95 p. 390.
1177. Swedish Legislative Bill 2016/17:180. A modern and legally secure administration – a new Administrative Procedures Act [*En modern och rättssäker förvaltning – ny förvaltningslag*]. p. 195.

What qualifies as sufficient statement of reasons for a decision can thus vary between types of cases, but also with the specific circumstances that arise in individual cases of comparable type. While framed in technologically neutral language, the duty to state reasons in Section 32 APA thus entails direct substantive requirements for automated decision-making.
Although Section 32 of the APA establishes a clear main rule that all decisions must be reasoned, the provision also contains some exemptions that allow decision-making without elaborated reasons. The perimeters of such exemptions are relevant for the permissibility of automated decision-making since the systems deployed in cases where such an exemption applies does not need to be technically capable of producing nuanced or elaborated decision-making reasons. The exemption which potentially has the greatest impact on the legal conditions for automated decision-making is that reasons may be omitted if it is 'obviously unnecessary' to provide them (which, due to the APA's technology-neutral approach means that exemption also applies to automated decision-making).[1178] This exemption requires that an assessment must be made of whether reasons for the decision need to be given in order to satisfy the interests of the concerned parties, and the preparatory works of the provision states that the assessment should be made on the basis of the circumstances of the individual case.[1179] Assessments on a case-by-case basis is principally challenging in the context of automated decision-making, as any system not capable of producing elaborated reasons may only be deployed where this exemption applies. The preparatory works, however, also specifies some typical cases where the exemption should apply. One example, which has been extensively utilised in the context of Swedish public automated decision-making, is that decisions which are based on an application and could be seen as indisputably favourable to the applicant as well as having been made on sole basis of the information provided by that applicant usually does not need to be reasoned, since the authority in such cases makes a decision completely in line with the individual's claim.[1180]

In practice, the 'obviously unnecessary' exemption to the duty to state reasons in Section 32 of the APA thus allows for a large number of decisions within, for example, social insurance and student funding etcetera, to be made without elaborated reasons. The exemption therefore functions as a fairly substantial 'enabler' of automated decision-making, even though its impact in this respect has barely been discussed in the preparatory works of the APA or in national doctrine.[1181] While the APA, as stated above, does not impose any formal restrictions on making adverse decisions by automated means, it appears that the form of the duty to state reasons has explanatory value for why the lion's share of automated decision-making in the Swedish public administration takes place for favorable decision-making. In addition, there is also specific legislation in certain sectors which stipulates that automated decision-making is only permitted in such cases in which the APA's exemption is applicable (it can be pointed out that such legislation has typically been enacted before the entry into force of Section 28 of the APA, and

1178. Section 32 APA also allows for a statement of reasons to be wholly or partly omitted if the decision concerns the employment of a person, a significant public or private interest that requires the decision be issued immediately, is necessary in view of national security, the protection of private persons' personal or financial circumstances or some other comparable circumstance, or the decision is about the issue of provisions referred to in Chapter 8 of the Instrument of Government.
1179. The 1986 APA allowed for omitting the reasons for a decision in all cases where the decision is not adverse to any party. This exemption did not carry through to the 2017 APA based on the reasoning that the assessment of whether the reasons for a decision may be omitted must be individually assessed.
1180. As an example, the preparatory works of the APA states that decisions, even though favourable to the individual, might still need to be reasoned based on the fact that it has effects on third parties (to whom the reasons for the decision must also be clear) It should be added that the APA stipulates that the individual always has the right to request a statement of reasons for his or her decision, even if the exception in Section 32 APA was applied. At request, authorities are thus obliged to provide a statement of reasons ex post if this is necessary for him or her to be able to exercise his or her rights. Swedish Legislative Bill 2016/17:180. A modern and legally secure administration – a new Administrative Procedures Act (*En modern och rättssäker förvaltning – ny förvaltningslag*). p. 192. Cases to be dismissed upon withdrawals was another specified example of when the exemption typically applies, although the need for individual assessments was stressed, p. 192 (where a reference was made to Swedish Parliamentary Ombudsman, decision 1975/76 p. 475).
1181. See, for example, Swedish Government Inquiry 2014:75. Automated decisions – fewer rules mean clearer regulation [*Automatiserade beslut – färre regler ger tydligare reglering*]. p. 58 et sec; Rättsstatliga principer och beslutsprocesser i en (alltmer) digitaliserad och automatiserad förvaltning./ Enqvist, Lena and Naarttijärvi, Markus. Rättsstaten i den svenska förvaltningen : en forskningsantologi. Statskontoret 2022, p. 217–249.

now serves as lex specialis limiting which decisions may be made automatically within its applicational scope). The design of the duty to state reasons therefore seems to have a major impact on Swedish administrative law practice regarding automated decision-making, even if the trend is towards more adverse decisions also being made automatically (where they must then meet the requirements for sufficient reason-giving).

It should be pointed out in this context that sufficient reasoning, although a key safeguarding measure for transparent and contestable public exercise of powers, has often been challenging for authorities also in manual administration. It is a recurring criticism from the Parliamentary Ombudsman that public authorities fail to state sufficient reasons for their decisions, also for manual decisions. Such criticism often relates to the stated reasons having been too concisely framed so that they don´t allow for the subject of the decision to understand the true causes for that decision. Another recurring theme of criticism is that the stated reasons tend to merely account for the applicable legislation rather than account for how the rules were applied in the specific case.[1182] Against the background that the duty to state reasons has been identified as one critical obligation for the lawful use of automated decision-making, it is unsatisfactory that clear guidance on the boundaries to the exemption provision is yet lacking. In addition, it would be beneficial to have further guidance on when the duty to state reasons is fulfilled, in particular regarding whether any specific requirements as to the substance of the reasons applies when decisions are made automatically.

At present, there is not much case law or other guiding decisions on the specific implications of the duty to state reasons in the context of automated decision-making. One noteworthy example is, however, that the Swedish Migration Agency was criticised by the Swedish Parliamentary Ombudsman as the automated decision-making system deployed by the authority to decide on so-called delayed action cases did not manage to produce reasons in a manner compliant with the with Section 32 of the APA. According to the Ombudsman, the automated decisions did not account for the circumstances that had been decisive for the decision. The provided reasons merely stated that the authority up until the point that the complaint on slow procedure had been made had not had time to decide the case, but did not give any reasons as to why. The true reasons for why the case had not yet been decided were therefore not apparent for the subjects of these decisions. In consequence, the Ombudsman stated that the handling of, and reason-giving in relation to, the decisions thus gave the impression that there was no actual examination of whether the matter could be decided as intended through the regulation on slow procedure.[1183] The decision is noteworthy as it is the first where the Ombudsman has specifically addressed the duty to state reasons in the context of fully automated decision-making. At the same time, the specific circumstances of the case made it quite apparent that the duty had not been fulfilled. The Ombudsman therefore had no reason to discuss in more detail the distinction between fictitious and real reasons, which could have provided relevant guidance on the content and boundaries of the duty in the context of automated decision-making. Further jurisprudence on Section 32 in the APA would therefore be welcome, and an important component in clarifying the standards which systems used for automated decision-making must meet.

The APA applies also to municipal activities at the local and regional level, with certain limited exceptions.[1184] However, the municipal decision-making powers are regulated in the Swedish Local Government Act *(Kommunallag (2017:725))*, SLA, and, in sum, requires that any automatically executed decision-making authority must have been lawfully delegated to the automated system. The question of automated decision-making, therefore, has a slightly

1182. See, for example, Swedish Parliamentary Ombudsman, decisions 2015/16 p. 311 and 2020/21 p. 428.
1183. Swedish Parliamentary Ombudsman, decision 2022/23 p. 481.
1184. The APA applies to 'administrative authorities', which, following the terminology used in the Instrument of Government, means that the APA is applicable to both state and municipal administrative authorities but not to the Government. Swedish Legislative Bill 1985/86:80. About a new administrative procedures act [*Om ny förvaltningslag*]. p. 57.

different legal configuration in the municipal sector as compared to in the government sector. According to the SLA, municipal as well as regional decisions (even when made by municipal or regional officials), are formally made by the municipal or regional council via delegation.[1185] Up until as late as 2022, the existing law did not expressly allow for delegating decision-making rights to automated systems. For this reason, the prevailing interpretation of the SLA (as opposed to in the case of the government authorities' mandates for automated decision-making) became that the letter of the law exempted fully automated decision-making within the local and regional municipal sectors.[1186] This view created some tension, as some Swedish municipalities were already using automated decision-making practices in, among other things, subsistence allowance/income support.[1187]

In mid-2022, however, an amendment was made to the SLA.[1188] Sections 37–38 in Chapter 6 of the act now allows for delegation of decision-making to automated systems for the majority part of the local and regional municipal operations. This authorisation is, however, more narrowly defined when compared to Section 28 of the APA, as it exempts certain decisions from being made automatically. The exemptions include such decision-making procedures that are not covered by the procedural safeguards in the APA, such as those municipal decisions who's legality may be reviewed after an appeal by any member of the municipality (and which thus typically concern collective interests), decisions which may not be appealed, procurement matters, or matters concerning the national so-called freedom of choice system (which relates to an individual right to choose the supplier of certain social or health services among publicly contracted suppliers).[1189]

Apart from the above-mentioned exemptions, the municipal-specific authorisation to make automated decisions within in the SLA (just as Section 28 of the APA) does not provide any guidance or set any explicit criteria for what types of matters that may be automated in a lawfully compliant manner. The provision is thus a general qualifying rule which allows for automated decision-making when no other legal barriers stand in the way of the practice. Just as in the case of government authorities, the legality of a specific automated decision-making procedure and the system it runs on, will thus have to be assessed on the basis of its compliance with those regulatory frameworks that generally applies to the specific decision-making. This assessment must include whether the system is capable of operating lawfully, when taking for example data protection or cyber security rules into consideration, and whether it can be relied upon to produce or support lawful decisions when taking the probabilities and risks associated with flawed functionality into consideration.

As demonstrated in the preceding discussion, the APA plays a pivotal role as a legal framework regulating administrative practices and the implementation of rule-of-law values in their operations. While maintaining a technology-neutral stance, the application of the APA has adapted to address certain challenges presented by digitisation. Nevertheless, the absence of specific, technology-oriented criteria in the regulation necessitates that the authorities shoulder the primary responsibility for ensuring that fundamental rule of law principles are still adhered to. Consequently, the APA underscores the continuous need for in-depth legal assessments and discussions within the rapidly advancing landscape of technology utilisation in administrative practises.

1185. The decision-making powers are primarily regulated in Chapter 5 of the SLA.
1186. Automatiserade beslut i förvaltningen. En lärobok / Otter Johansen, Tormod. AI, digitaliseringen och rätten. ed./ i Gregor Noll, Studentlitteratur, 2021. p. 110.
1187. Discretion, Automated Decision-Making and Public Values: Background and Test of an Approach for Unpacking Human and Technological Agency./ Ranerup, Agneta and Svensson, Lupita. Electronic Government. ed./ Marijn Janssen and others, Springer International Publishing 2022.
1188. Chapter 6, Sections 37-38 SLA; Swedish Legislative Bill 2021/22:125 Elections and decisions in municipalities and regions [*Val och beslut i kommuner och regioner*]. p. 23.
1189. Chapter 6, Sections 37-38 SLA.

3. Trajectories in Swedish Public Sector Digitalisation Efforts

As indicated, Swedish public administration has a longstanding tradition of deploying computer technology and automated decision-making within the administrative practise. Swedish public authorities have been using computational assistance in their operations since the 1950's.[1190] The first entirely automated decisions commenced in 1970's (computational assistance is here understood as utilising computing power for analysis and processing, while automated assistance is understood as performing tasks automatically, reducing manual intervention).[1191] The growing dependence on computers and Automatic Data Processing (ADP) technology, combined with an expansive welfare state and associated collection of vast amounts of citizen data, raised apprehensions about an 'all knowing' state. This prompted political debates on the need for data protection within this new computational state order. Consequently, the 1973 Data Protection Act (1973:289), one of the world's first comprehensive data protection regulations, came to mark a significant development by imposing a general prohibition on the compilation of data within government registries. The notion of solely relying on secrecy regulations was no longer deemed sufficient to safeguard individuals from unwarranted intrusions by the public sector or other entities. The data protection legislation, by curbing the authorities' capacity to generate, share, and consolidate records, aimed to create a safeguarded sphere for individuals.[1192]

Although Swedish public sector technology use has been associated with privacy concerns since its commencement, a notable transformation in the rationales behind its facilitation has occurred. Initially, the primary goal was generally to enhance the internal efficiency of authorities. However, as computational and automated assistance became more commonplace, 'technologies' also came to be perceived as a fundamental element in providing services to citizens. The evolution of government activities especially propelled into a new phase especially following the arrival of the Internet in the 1990's.[1193] At that time, governmental bodies already possessed a relatively high level of technological maturity, and the introduction of e-services became a means to not only facilitate external communication but also streamline information exchange. In the year 2000, the government strategy coined as the '24-hour authorities' strategy was launched through a government bill aimed at facilitating 'An Information Society for All'.[1194] The primary objective behind this initiative was to enhance the efficiency of services provided and improve accessibility. Citizens were now referred to as 'customers', leading to a focus on delivering user-centred and interactive e-services. As the array of e-services expanded, there was a growing call for authorities to interconnect their e-services and structure them in alignment with citizens' life situations, advocating for a citizen-centred or administration-driven approach to e-government.[1195]

The above historical account is very schematic, but nonetheless shows that Sweden has demonstrated a positive and solution-oriented outlook on the prospects of integrating advanced technologies into public administration. This sentiment is underpinned by the present national aim to assume a world-leading position in utilising digital and AI technologies in the public

1190. Swedish Government Inquiry 2009:86 Strategy for the authorities' work on e-government [*Strategi för myndigheternas arbete med e-förvaltning*]. p. 33.
1191. Automated decision-making in public administration – effective and efficient, but inadequate control and follow-up./ Swedish National Audit Office (Riksrevisionen) RiR 2020:22 2022. p. 1 et sec.
1192. Legislative Bill 1973:33 The royal majesty's proposition with proposals for amendments to the Freedom of the Press Act, etc. (Kungl. Maj:ts proposition med förslag till ändringar i tryckfrihetsförordningen, m.m.). p. 89; Swedish Government Inquiry 2009:86 Strategy for the authorities' work on e-government (*Strategi för myndigheternas arbete med e-förvaltning*). p. 33.
1193. Förvaltningslagen och digitaliseringen./ Magnusson Sjöberg, Cecilia. In: Förvaltningsrättslig tidskrift, No. 3 2018, p. 519–530. At p. 519 et sec.
1194. Swedish Government Inquiry 2009:86 Strategy for the authorities' work on e-government (*Strategi för myndigheternas arbete med e-förvaltning*). p. 33; Prop. 1999/2000:86, Ett informationssamhälle för alla.
1195. Swedish Government Inquiry 2009:86 Strategy for the authorities' work on e-government (*Strategi för myndigheternas arbete med e-förvaltning*). p. 33.

sector.[1196] To delve a bit deeper into this aim and trajectory, the following subsections will explore some of the general trends in government and administrative strategies to realise this objective.

3.1 'Digital first' for Enhanced Service and Efficiency

The 'digitalisation' of the Swedish public administration broadly denotes a transformation process made up of many individual and different implementations of technologies by public authorities to support their tasks. 'Digitalisation' thus entails a plethora of disparate as well as sometimes interconnected operations. By introducing some examples of Swedish public digitalisation initiatives and operations, this section will provide an outline for some general features of the ongoing national developments.

One fundamental manifestation of the public administration's digitalisation is that contacts with the authorities, and thus also the interaction with them, has increasingly become electronically mediated and often take place through various types of e-service functions (often called self-service functions). These include, for example, chatbots that answer questions about the services and obligations of public authorities, or electronic application procedures as well as contacts. The Swedish government has stated as a general objective for the public administration that digital solutions should be the first-hand choice for their activities or contacts with private individuals and businesses. This principle of 'digital first' has mainly been advocated against the background of prospects for time and cost savings, but also against the background of new service opportunities towards the public.[1197]

As of today, there are no generally applicable regulations on the national public administration's use or design of digital contact channels or digital communications. There is also no formal requirement of a specific legal basis for introducing e-services (provided, of course, that the services fulfil any data protection or security requirements etcetera, that may be applicable). Public e-services may, however, in some cases be subject to direct regulation. Examples are that the digital e-services or self-services offered by the Swedish Social Insurance Agency and the Swedish Pensions Agency are subject to certain specific provisions established through ordinary (parliamentary) acts.[1198] Other examples are that the Swedish Public Employment Service and the Swedish Tax Agency have (via delegated regulatory powers) issued statutory instruments.[1199] These types of provisions often regulate what categories of information that may be submitted electronically by individuals or businesses, but rarely establishes any obligations for the authorities in terms of the services that must be offered. One general regulation which relates to the public use of e-services is the Act (2018:1937) on accessibility to digital public services *(Lag (2018:1937) om tillgänglighet till digital offentlig service)* which implements the EU Web Accessibility Directive.[1200] This regulation does not establish any obligations on authorities to provide for digital services, but rather establishes availability standards for those services that the authorities have opted for providing in digital form. Additionally, the EU Single Digital Gateway Regulation imposes certain requirements for some types of administrative matters to be handled digitally and interoperably across

1196. Swedish Legislative Bill 2011/12:1 Budget proposition for 2012 (*Budgetpropositionen för 2012)* utg. omr. 22; Parliamentary decision rskr. 2011/12:87.
1197. Swedish Legislative Bill 2019/20:1 Budget proposition for 2020 (*Budgetpropositionen för 2020*); Parliamentary decision rskr. 2019/20:129.
1198. See Chapter 111 in the Swedish Social Insurance Code (2010:110)) (*Socialförsäkringsbalken (2010:110*); ' Self-services via the Internet' *(Självbetjäningstjänster via Internet)* and Act (2004:115) on self-service via the Internet in social insurance administration (*Lag (2004:115) om självbetjäningstjänster via Internet inom socialförsäkringens administration*).
1199. Find a list at Skatteverkets föreskrifter om e-tjänster./ The Swedish Tax Agency [*Skatteverket*] https://www.skatteverket.se/privat/etjansterochblanketter/allaetjanster/foreskrifterometjanster.4.18e1b10334ebe8bc80003285.html Accessed 12 December 2023.
1200. See also, section 2.1.

Europe.[1201] None of these regulations, however, establishes any comprehensive regulatory framework on the types of services that Swedish public authorities must offer (as well as for what purposes). The same is true for how the technological design of such services is to be coordinated nationally.

Partly due to the lack of general regulation, but also probably as a consequence of the Swedish decentralised administrative structure including the largely independent positions which the authorities hold in relation to each other, the national e-service digitisation efforts of the authorities have largely taken place within each authority separately. At the same time, developments are underway that aim to facilitate a more coherent and cross-sectoral infrastructure which can cater to common basic administrative needs (instead of each public actor developing their own solutions). One such major coordination effort is the establishment of a common infrastructure for digital government, which is lead and managed by DIGG.[1202] The legal and organisational background and setup of the common infrastructure for digital government will be detailed more in the next section. One citizen-centred aspect and building block of this common infrastructure should, however, be highlighted here as it is one important component in many public e-services – namely the enabling of official digital communication between authorities and individuals as well as businesses.

Public authorities may use different digital means to communicate with individuals and businesses. Many authorities offer advisory and other services via chat functions, for example. E-mail is also a common form of electronic communication. Since there is a risk that such functionalities are used by people other than who they claim to be, or that the communication ends up in the wrong hands, it is often not advisable for all the authority's case communication to take place via e-mail or other less secure channels. The need for, as well as the conditions for, official digital mail are thus strongly influenced by the interest in ensuring that communication only takes place with duly qualified persons. To be able to receive official mail from a national authority digitally, the individual must therefore have signed up for a digital mailbox and use e-identification (to secure that any communications only reach or are transmitted by the correct recipient or sender).

There are currently three digital mailboxes to choose from. Two of these are privately governed and offers the functionality to receive digital mail from both public organisations and private companies, and one is state governed by DIGG and exclusively allows for receiving digital mail from authorities or regional and local municipalities. Sending authorities and municipalities accede by entering into an agreement with DIGG and in accordance with the Ordinance (2018:357) on government-wide infrastructure for secure electronic mail.[1203] The voluntary nature of accession for both government agencies and private entities means that not all authorities have adopted the digital communication infrastructure. Consequently, they might resort to alternative digital communication methods or may not always have the option to communicate digitally. The accession rate amongst individual users is increasing but have yet not been considered satisfactory by DIGG or the Government. The Government has therefore launched an inquiry into the legal conditions and suitability for introducing, in a similar way to Denmark and Norway, an obligation for authorities as well as private individuals or legal entities to acquire a digital mailbox in order to be able to send or receive secure electronic mail from

1201. Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012. See also, for national implementing measures, the Law (2022:126) with supplementary provisions to the EU regulation on a single digital gateway *[Lag (2022:126) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång]*, and the Ordinance (2022:127) with supplementary provisions to the EU regulation on a single digital gateway *(Förordning (2022:127) med kompletterande bestämmelser till EU:s förordning om en gemensam digital ingång)*.
1202. The project of developing of a common digital infrastructure precedes the formation of DIGG. The prior coordinating agency was the Swedish Tax Agency.
1203. Ordinance (2018:357) on inter-agency infrastructure for secure electronic mail items (*Förordning (2018:357) om myndighetsgemensam infrastruktur för säkra elektroniska försändelser*).

authorities. In light of the risks that such requirements could reinforce digital exclusion for those groups with no or limited capacity to utilise digital mailboxes, the committee is also requested to propose how exemptions from such an obligation could be designed.[1204] In the Swedish context, a regulated (at least presumed) obligation to communicate digitally would mean a step towards clearer regulatory contours for digital public administration. Although it remains to be seen whether such an obligation will be introduced, the investigation can be seen as an example of how regulation increasingly seems to be considered for enabling as well as speeding up the digitalisation of public administration. It is therefore conceivable that the governance of digitalisation initiatives that require major infrastructure investments and inter-authority solutions will increasingly take the form of regulation in the future. In the long term, such a development may also lead to a shift in the Swedish regulatory design tradition towards regulations having a less technology-neutral design.

3.2 The Agency for Digital Government as One Node for the Strategic Development of Digital Administration

As already indicated, a particularly important authority for the digitalisation of the Swedish public sector is the Swedish Agency for Digital Government *(Myndigheten för digital förvaltning)*, DIGG. The authority was established in 2018 and has a broad and general responsibility to coordinate and support the government-wide digitalisation.[1205] Its tasks also include gathering and providing the Government with information on public and societal digitalisation developments.[1206] Apart from these overarching aims and functions, DIGG's responsibilities also include many specific tasks which serve as building blocks for the public administration's digitalisation in various ways. DIGG is the responsible authority for establishing a national common digital infrastructure, for promoting the use of the infrastructure for secure electronic mail, and for coordinating issues concerning common standards, formats, specifications and similar requirements for the public administration's electronic information exchange.[1207] DIGG thus has a strong coordinating role for the digitalisation of the Swedish public sector, and serves as a key actor in realising the level of interoperability required to facilitate secure and efficient data exchange and communication between different public authorities and services.

One strategic digitalisation programme that DIGG has been assigned to manage and coordinate is the so-called Ena project, which seeks to establish a common public digital infrastructure in Sweden (*Sveriges digitala infrastruktur*).[1208] The aim is to ensure information exchange through access to public data (basic data), to increase the number of authorities reusing existing digital services, and to increase the interoperability level within the public sector.[1209] The development and design of the Ena-infrastructure is ongoing, and while DIGG is the coordinating authority, its realisation relies much on voluntary cross-authority cooperation. The government has been active in instructing a number of authorities to take part in the development (the Public Employment Service, the Companies Registration Office, the National Courts Administration, the eHealth Agency, the Social Insurance Agency, the Land Survey, the Civil Contingencies Agency, the

1204. Tilläggsdirektiv till Postfinansieringsutredningen./ Ministry of Finance (*Finansdepartementet*) Dir. 2023:7, (I 2020:03).
1205. Section 1 Ordinance (2018:1486) with instructions for the Swedish Agency for Digital Government *(Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning)*. However, the mandate does not cover the digitisation of the Government Offices of Sweden, the Swedish Security Service, The Swedish Fortifications Agency, the Swedish Defence University and authorities sorting under the Ministry of Defence (*Regeringskansliet, Säkerhetspolisen, Fortifikationsverket, Försvarshögskolan samt myndigheter som hör till Försvarsdepartementet*).
1206. Section 2 Ordinance (2018:1486) with instructions for the Swedish Agency for Digital Government *(Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning)*
1207. Section 4 Ordinance (2018:1486) with instructions for the Swedish Agency for Digital Government *(Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning)* and Section 18 and Annex I to the Ordinance (2022:524) on the contingency planning of state authorities *(Förordningen (2022:524) om statliga myndigheters beredskap)*.
1208. Section 1 Ordinance (2018:1486) with instructions for the Swedish Agency for Digital Government *(Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning)*.
1209. Statusrapport för etablering av förvaltningsgemensam digital infrastruktur./ DIGG 2022. p. 2

National Archives, the Tax Agency, Statistics Sweden and the Transport Administration).[1210] The more specific project activities are, however, distributed between these authorities based on voluntary agreements. Ena is, so far, the largest Swedish digital infrastructure project in terms of intended scope. As of yet, however, the project has not been realised to the extent that it fully operates as a comprehensive state infrastructure. In a 2023 revision, the Swedish National Audit Office, NAO, found that the project yet have delivered few concrete results and is perceived as a rather abstract project even by some of the participating authorities. NAO also found that it seemed unclear to the authorities what joining the project actually meant in terms of commitment as well as in terms of possible future services.[1211]

Objectives for a common administrative digital infrastructure have been a central part of the Government's digitalisation policy for a long time, although the focus of that policy has shifted somewhat during the years. The policies were initially concerned primarily with digital services and solutions such as e-commerce in the state, e-identification and digital mail. In recent years, the policies have turned more to pushes for facilitating common infrastructures for enabling a better overall view and efficiency of public services, via, for example, the consolidation and standardisation of the infrastructure's various components and solutions. A perceived challenge to a common administrative digital infrastructure for information exchange is the Swedish administrative model due to its administrative dualism. DIGG has highlighted that this complicates horizontal coordination between different authorities each enjoying their relative independence from the political decision-making functions.[1212]

While an emphasised objective, the pace of realising the common digital infrastructure is thus rather slow. This has been perceived as a shortcoming by the government, in response to which it in 2022 set up an official inquiry to investigate the practical and legal conditions for realising the Ena-project. The inquiry has been instructed by the government to consider whether, and if so, how, the regulation of cross-sectoral interoperability should and could be developed, whether there is a need for further regulatory mandates in this area, and if so, propose the scope of such mandates.[1213] As the findings of the inquiry thus might lead up to proposals of extending DIGG's regulatory mandates into the area of a common public digital infrastructure, it might possibly render DIGG a new future role as not just a coordinator, but also a more active standard setting authority for public digitalisation efforts. Such a development would represent a break from the Swedish tradition of realising the policy goal of a common Swedish public digital infrastructure almost solely through voluntary cooperation between the authorities.

As seen by the numerous digitalisation-related tasks and objectives placed on DIGG to realise, the authority's responsibilities are broad. A part from the above discussed coordinating role in establishing a common digital infrastructure for the public sector, the authority, for example, also serves as the competent authority for the Swedish connection points (nodes) for cross-border electronic identification in accordance with the EU eIDAS Regulation.[1214] As another example, DIGG also serves as the national coordinating authority under the EU Single Digital Gateway Regulation,

1210. *Arbetsförmedlingen, Bolagsverket, Domstolsverket, E-hälsomyndigheten, Försäkringskassan, Lantmäteriet, Myndigheten för samhällsskydd och beredskap, Riksarkivet, Skatteverket, Statistikmyndigheten SCB, Trafikverket*
1211. Digitala tjänster till privatpersoner – stora utvecklingsmöjligheter för statliga myndigheter./ Swedish National Audit Office (*Riksrevisionen*) RiR 2023:6. p. 63 et sec.
1212. Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte Swedish Agency for Digital Government *(Myndigheten för Digital förvaltning*)AD 2019:582.
1213. Utvecklad reglering och styrning av interoperabilitet vid datadelning inom den offentliga förvaltningen och från den offentliga förvaltningen till externa aktörer./ Ministry of finance (*Finansdepartementet*) Dir. 2022:118.
1214. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

SDG.[1215] This role includes coordinating those national authorities which, under the SDG, must provide online access to information, administrative procedures, and assistance services across EU borders.

In addition to explicitly regulated responsibilities, DIGG's central role in informing the public administration's digitalisation strategies is also manifested through the many different government assignments which the authority has received.[1216] As one example, DIGG was in 2022 tasked with conducting a review over Swedish welfare legislation to identify obstacles for automation, as well as to model proposals of legislative changes to enable further automation. Although national inquiries have been done before into the need for reducing legal barriers for digitalisation or automation,[1217] this assignment is the widest and most specified yet in Swedish digital-ready legislation efforts within the welfare sector. The authority is expected to report its findings in 2024.

Furthermore, aside from the more specific tasks assigned to DIGG and exemplified above, the authority also provides general support for the authorities' digitalisation efforts without direct involvement in each individual implementation. One such example is that the authority has developed a set of principles for digital collaboration intended to support public authorities in their continuous efforts to develop the capacity for coherent digitalisation, so that they can work effectively together. The strategy is based on ten principles and includes, amongst others, a principle of seeing collaboration as the first hand choice of operation (where collaboration opportunities with other actors are sought at an early stage in the development work), a principle of working actively with the law (partly to ensure that the legal perspective is included early in the digitisation work) and principles of open data and reusing solutions between each other in the public sector.[1218] The principles have been developed taking into account the conditions of the Swedish administrative system and the principle of legality, but are not binding in themselves. However, they express DIGG's role as a knowledge distributor and node in facilitating a lawfully compliant and efficient digital transformation.

From the perspective of public sector digitalisation, DIGG's responsibilities span from overarching and rather abstract goals of promoting efficiency and effectiveness through supporting cross-government digitalisation, to a number of more specific tasks of supporting, coordinating or executive nature. While a fairly new authority within the Swedish public administrative structure, DIGG has thus overall become a key actor in facilitating digitalisation within the decentralised national administrative order. Recent developments in terms of legislative inquiries into expanding DIGG's regulatory mandates will, if implemented, only further amplify the authority's coordinating role for the overall strategies and implementation of digital administration initiatives.

1215. Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012. Section 1 Ordinance (2018:1486) with instructions for the Swedish Agency for Digital Government *(Förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning)*.
1216. Uppdrag att stödja regeringens arbete med fortsatt digitalisering av välfärden genom att identifiera rättsliga hinder./ Swedish Government, Ministry of Infrastructure 2022. I2022/00620.
1217. Swedish Governmental Inquiry 2018:25. Law as support the digitalisation of the administration (*Juridik som stöd för förvaltningens digitalisering*); Swedish Government Inquiry 2014:75. Automated decisions – fewer rules means clearer regulation (*Automatiserade beslut – färre regler ger tydligare reglering*).
1218. Grundläggande principer för digital samverkan./ DIGG https://www.digg.se/kunskap-och-stod/svenskt-ramverk-for-digital-samverkan/grundlaggande-principer-for-digital-samverkan#h2-2Arbetaaktivtmedjuridiken Accessed 12 December 2023.

3.3 Cross-authority Collaborations as One Strategy to Facilitate Digitalisation

As indicated, cross-authority collaborations are one clear national strategy for facilitating the digital transformation of Swedish public administration. While DIGG is the Swedish authority with the most pronounced responsibilities for serving a coordinating role in the facilitation of this transformation, coordinating roles have also been distributed between other authorities in relation to more defined tasks.[1219] Coordinating roles may range from specific responsibilities to act as nodal points for cross-sectoral and strategic discussions on specific digitalisation issues, to specific responsibilities which include the provision of material resources.

The public IT sector offers examples where cooperative structures for securing the efficiency and well-functioning of IT systems utilised in the public sector are meant to be facilitated through coordination by specific authorities. One example is that the Swedish Social Insurance Agency *(Försäkringskassan)*, on the basis of a government assignment which has been renewed periodically since 2017, is responsible for offering an infrastructure for coordination of government IT operations. At present, the authority manages and offers various IT services which can be used by other authorities on a voluntary basis. Those (typically smaller) authorities with small IT resources of their own may make a full or partial commitment to use the SSA's services.[1220] There are also other coordination initiatives in areas where specific needs have been identified for IT. As an example, the Swedish National Courts Administration *(Domstolsverket)*, also based on a government assignment, offers IT operations to all the country's courts and certain other court administration authorities.[1221] In the field of IT, coordination efforts are also being made outside of the more centralised initiatives, initiated by the authorities themselves. In 2021, almost every third Swedish authority (50 authorities) stated that they coordinate their IT operations with another authority. This may involve limited and specific services, such as HR and payroll-related services, but in some cases also overall commitments to pooling IT resources.[1222]

In addition to those collaborative structures that have been initiated by Government assignments or by the authorities themselves on a smaller scale, Swedish public authorities (including local and regional municipalities) have also been active in initiating some more broad-scale collaborative structures on their own motion. Two examples, which will be elaborated further below, is the informal formation of the so-called eSam group which focuses on facilitating cooperation on public sector digitalisation, and the founding of the digital welfare infrastructure-oriented limited company Inera by Swedish Association of Local Authorities and Regions *(Sveriges kommuner och regioner)*, together with most Swedish local and regional municipalities.

eSam is a member-led collaboration structure which works to enable its members to seize the opportunities of digitalisation. eSam currently comprises 36 member organisations, of which 35 are government authorities. The 36:th member is The Swedish Association of Local Authorities

---

1219. Another Swedish agency, which alongside DIGG, have some of the most pronounced responsibilities for the national digital transformation is the Swedish Post and Telecom Agency *(Post och telestyrelsen)*. The agency has an overarching responsibility in the field of postal services and electronic communications, which are important components of the possible digitalisation of public administration, although not exclusively linked to this objective. However, the agency also has some more specific administration-oriented coordinating responsibilities, such as working to increase network and information security in the area of electronic communications, through collaboration with authorities and other relevant actors Sections 1 and 4, Ordinance (2007:951) with instructions for the Swedish Post and Telecom Agency *(Förordning (2007:951) med instruktion för Post- och telestyrelsen)*. The agency is also a designated contingency planning agency with sectoral responsibility for electronic communications under the Ordinance (2022:524) on the contingency planning of state authorities *(Förordningen (2022:524) om statliga myndigheters beredskap)*.
1220. Swedish Governmental Inquiry 2021:97 Secure and cost-effective IT operations - proposal for permanent arrangements for coordinated government IT operations (*Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift*). p. 125.
1221. Swedish Governmental Inquiry 2021:97 Secure and cost-effective IT operations - proposal for permanent arrangements for coordinated government IT operations (*Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift*). p. 177.
1222. Swedish Governmental Inquiry 2021:97 Secure and cost-effective IT operations - proposal for permanent arrangements for coordinated government IT operations (*Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift*). p. 177.

and Regions *(Sveriges kommuner och regioner)*, which is a private organisation that brings together all Swedish municipalities and regions (i.e. public actors) and functions as an interest group which monitors issues of importance to municipal or regional operations. The eSam programme was established in 2015 but did have roots in an earlier collaborative constellation which had been based on a government mandate between the years 2009-2015. Between those years an expert group called the 'e-delegation' was tasked with leading and coordinating the work on making it easier for citizens and businesses to exercise rights and fulfil obligations through digital means.[1223] When the E-Delegation's mandate was cancelled in 2015, the Directors-General of the partaking authorities chose to continue the established cooperation on public sector digital development in the same spirit, but on a voluntary basis. The member organisations of eSam thus decide their priorities themselves, which means that the composition of cooperating authorities within the various initiatives and projects might vary. eSam's activities involves representatives of the member organisations participating in projects or practical or legal nature.

So far, prioritised work within eSam has been the development of guidelines, recommendations or checklists aimed at supporting and guiding eSam members on how to develop or implement different digital solutions. These guidelines and recommendations are not binding (as eSam has no standard-setting or regulatory mandate), but they are the results of collaborations between (often technical or legal) experts from several different authorities. They have therefore come to have quite a strong influence on the interpretation of existing law by national public authorities on various issues related to the digitisation of public administration, such as the use of cloud services by the public sector, etc. Sometimes eSam also collaborates with other public authorities on specific issues. For example, eSam's 'Legal Guidance for eLegitimation and eSignatures' has been developed by eSam's legal expert group in cooperation with the former E-legitimation Board (*E-legitimationsnämnden*) and the Swedish Civil Contingencies Agency (*Myndigheten för samhällsskydd och beredskap*) with some representatives of banking organisations also participating in the work.[1224] The aim of eSam is thus to provide a forum for bringing together, on a voluntary basis, competences in complex and common areas in order to promote administrative efficiency and service through digitisation.

eSam's co-operation on legal issues is partly facilitated through a 'Legal General-Directors' Forum' which is comprised of the leading lawyers of every eSam member and meets a few times a year. The main objectives include prioritising and choosing legal issues that eSam should address to find solutions that can benefit all members.[1225] Additionally, eSam also hosts a lower-level legal expert group, which collaborates to reduce digitalisation disincentivising uncertainties relating to existing law, to identify legal barriers to digitisation and demonstrate legally sustainable solutions that support the protection needs of individuals. The work of the eSam Legal Expert Groups is mainly concretised through guidelines and legal statements.[1226] Examples are guidelines on the legal conditions relating to cloud computing, software licensing, etc. eSam has, for example, produced a general recommendation called 'Digitalisation made right' with the stated aim of assisting public authorities in transitioning to completely digital systems for managing information, including in their operational systems as well as in general support functions such as message communication, e-identification, e-signatures, e-archives, and

1223. Delegation för e-förvaltning. Ministry of Finance (*Finansdepartementet*) Dir. 2009:19. p. 6.
1224. Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1./ eSam 2018 https://www.esamverka.se/download/18.1d126bc174ad1e6c39c8ca/1598467569167/eSam%20-%20V%C3%A4gledning%20E-legitimation%20och%20E-underskrift%201.1.pdf Accessed 12 December 2023; Vägledningar, ramavtal, e-legitimation./ Swedish Association of Local Authorities and Regions (*Sveriges kommuner och Regioner*) https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/informationsforsorjningdigitalinfrastruktur/elegitimation/vagledningarramavtalelegitimation.29241.html Accessed 12 December 2023.
1225. Rättschefsforum./ eSam https://www.esamverka.se/om-esam/organisation-och-forum/rattschefsforum.html Accessed 12 December 2023.
1226. Expertgrupp i juridik./ eSam https://www.esamverka.se/om-esam/organisation-och-forum/expertgrupp-juridik.html Accessed 12 December 2023.

personal storage space.[1227] It aims to promote that these functions are used in a coordinated and legally compliant manner within the digital administration 'ecosystem'. Another project of practical significance for digitalisation in the Swedish public administration, and which eSam is working on, concerns the development of standardised IT agreements and conditions adapted to public administration. The background is that the so-called The Digitisation Law Committee (*Digitaliseringsrättsutredningen*) in 2018 had noted that the authorities' need for support on contractual IT agreements had increased with growing outsourcing and more complex IT agreements.[1228] In addition to eSam's standardised working groups, there are also other networks run by one or more of eSam's members. One such example is the so-called GDPR network, which has been set up to monitor national legal developments in the field of data protection and to discuss interpretations of the provisions of the GDPR based on the needs of the participating businesses. The network is run by the Pensions Authority and is aimed at lawyers within the respective authorities.[1229]

eSam is an example of an informal structure which can be seen against the background of the Swedish decentralised administrative order, but also as one example of that orders 'intended functioning' (that public authorities are supposed to collaborate with each other in their areas of activities to promote an efficient and well-functioning administration, Section 8 APA). For the digitisation or automation of specific public authority tasks it may, of course, be the case that the legal conditions surrounding such initiatives are so authority- or task-specific that collaboration with other authorities appears superfluous or unfeasible. However, as shown by eSam's activities, there are a number of digitalisation issues that have common denominators for a wide range of authorities. This is especially true for cooperation on the interpretation of existing law in relation to more specific digitisation-related circumstances or needs. Legal uncertainties have often by, for example, the government or the authorities themselves, been identified as one major inhibitor of digitalisation initiatives. The emphasis that eSam has put on producing legal guidelines has had standard setting effects on the Swedish public administration's digitalisation and the perception of the authorities of legal challenges as well as possible practical solutions to overcome such challenges.[1230]

As indicated, another example of a self-initiated structure for developing public digital infrastructures is found in the undertakings of the limited company Inera. Inera is a national company which was formed to coordinate, simplify and streamline the digitalisation work of local and regional municipalities for the objective of providing good and equal welfare. Inera is a private legal entity (thus organised primarily under private law) but is wholly owned by Swedish Association of Local Authorities and Regions *(Sveriges kommuner och regioner)*, together with most Swedish local and regional municipalities (in their separate capacities).[1231] The often-emphasised reason for this set-up is that the chosen organisational format allows the company to develop various digital services which municipalities may utilise without having to procure them. The company has been responsible for the development of different digital infrastructures used by municipalities, such as the national infrastructure for digital first line health care services *(1177 Vårdguiden)* and a national infrastructure for the electronic exchange of medical records between both private and public healthcare providers *(Sammanhållen journalföring)*. Inera has also been responsible for providing the technical solutions for so-called secure digital communication *(Säker digital kommunikation)*, SDK, which is a digital infrastructure enabling

1227. Digitalisera rätt. En praktisk juridisk vägledning./ eSam 2019 https://www.esamverka.se/download/18.1d126bc174ad1e6c39b352/1561720847142/Digitalisera%20r%C3%A4tt%20-%20en%20praktisk%20juridisk%20v%C3%A4gledning.pdf Accessed 12 December 2023.
1228. Swedish Governmental Inquiry 2018:25. Law as support the digitalisation of the administration [Juridik som stöd för förvaltningens digitalisering]. p. 387 et sec.
1229. Nätverk./ eSam https://www.esamverka.se/om-esam/organisation-och-forum/natverk.html Accessed 12 December 2023.
1230. See, for example, Molntjänster och staten: En diskussion om röjandebegreppet i offentlighets- och sekretesslagen./ Karlsson, Rikard and Morseth Edvinsson, Atle. In: Förvaltningsrättslig tidskrift, No. 5 2021, p. 855–888. At p. 856.
1231. Ineras uppdrag./ Inera https://www.inera.se/om-inera/ineras-uppdrag/ Accessed 12 December 2023.

public organisations to exchange sensitive digital information with other public or publicly funded actors in a consistent and secure way.[1232]

Affiliation is voluntary but open to public authorities and local and regional municipalities (and is therefore not only intended for utilisation at the municipal level). The affiliates are organised in a so-called federation, in which they agree on common rules for technology and information security. Inera is the current owner of the federation and is in that capacity responsible for approving the software of those authorities or municipalities that wants to join the secure digital connection infrastructure. Inera's role in developing digital infrastructures for public (and primarily municipal) use is thus interesting against the background that the foundation of the company as such can be seen as a type of collaborative structure. The company has a public and multi-actor ownership but was formed to operate primarily under private law with the aim of serving as a national unifying actor for digitalisation in municipalities and regions. The example of Inera's role in developing specifically the SDK infrastructure for secure digital communication is also particularly interesting against the background that it shows how digitalisation developments based on initiatives at the local and regional level can be subsumed as a national and state level interest and concern. Because even though the SDK infrastructure so far has been built by Inera, it has transitioned to wholly public ownership and management by DIGG in 2023 (and thus to state ownership). This arrangement has been made possible through the public ownership of Inera. Since the government has no competence to directly regulate or decide on a transition to state ownership, it is based on an agreement between the government and the Swedish Association of Local Authorities and Regions.[1233] DIGG has, in turn, then been assigned this task by a separate government decision.[1234] The state ownership takeover of SDK may raise some questions in the light of the above mentioned Ena project which DIGG already manages and which also includes secure digital communication.[1235] According to DIGG, however, the long-term direction of the SDK developments after the takeover will be that its infrastructure should build on and complement the work being done to establish Ena. DIGG states that further work remains to be done within the authority to see how SDK specifically will be integrated with Ena, but the ambition shows that DIGG may also have a coordinating role in bringing together discrete development initiatives into a collaborative whole.[1236]

This section has showcased that ambitions of digitising the public sector often requires infrastructure investments which, for reasons of overall time and cost efficiency as well as functionality, often requires the crossing administrative boundaries. This fact also makes visible that the Swedish administrative system, through its constitutional as well as organisational traditions is primed to promote cross-authority cooperation and collaboration as the key instrument or measure for realising substantial infrastructure developments as well as maintenance. As exemplified, there are regulatory tools available for governing such initiatives, but they are typically used as a last hand option. As seen, the Government is also increasingly active in shaping common digital infrastructures or promoting cooperation for such objectives

1232. Rapporter och resultat./ Inera https://www.inera.se/utveckling/rapporter-och-resultat/ Accessed 12 December 2023. It should be emphasised that the secure digital communication infrastructure developed by Inera neither covers nor is intended to cover all communication between public actors. As stated, channels for digital communication are being developed within the so-called Ena project (see section 3.2). E-mail exchanges between certain government authorities also take place via the communication service Swedish Government Secure Intranet, SGSI, provided by the Swedish Civil Contingencies Agency *[Myndigheten för samhällskydd och beredskap]*, MSB, where all data traffic between the connected authorities is encrypted. SGSI - Swedish Government Secure Intranet./ Swedish Civil Contingencies Agency www.msb.se/sv/verktyg--tjanster/sgsi/ Accessed 12 December 2023.
1233. En överenskommelse mellan staten och Sveriges Kommuner och Regioner om etablering och införande av infrastruktur för säker digital kommunikation i offentlig sektor./ Government Offices of Sweden and Swedish Association of Local Authorities and Regions (*Regeringskansliet och Sveriges kommuner och regioner*) https://skr.se/download/18.117b327517db288a7c83f7d9/1640015115390/WEBB-33-21-01604-Bil-Overenskommelse-med-SKR-om-saker-digital-kommunikation.pdf Accessed 12 December 2023.
1234. Uppdrag att tillhandahålla infrastruktur för säker digital kommunikation i offentlig sektor./ Swedish Government, Ministry of Infrastructure 2021. I2021/03317.
1235. See section 3.2.
1236. SDK - Frågor och svar./ DIGG https://www.digg.se/digitala-tjanster/saker-digital-kommunikation-sdk/sdk-fragor-och-svar Accessed 12 December 2023.

though distributing tasks via specific assignments and budget allocations. Furthermore, the administrative independence that the authorities enjoy may also have a 'permissive' function or effect for the authorities in that they, even outside the confines of a direct legal or political mandate, frequently choose to proactively identify needs and engage in various formal or informal collaborative structures. This tendency is exemplified not the least in the establishment of eSam and Inera. Thus, the fact that the authorities themselves in many cases may also consider cross-authority collaboration desirable for implementing digital practices or sharing experiences and opinions on technical and legal matters is also highlighted.

3.4 The Swedish Regulatory Approach to Digitalisation

As seen, the Swedish legislator has to a large extent chosen a so-called technology-neutral approach to drafting legislation, by focusing on the functions and purposes of the law instead of relating it to the specific affordances of a particular technology. This approach allows for some flexibility in relation to technological or societal developments to avoid the legislation becoming obsolete, and echoes a functional approach to the legal design. As indicated, however, this approach might also render the legislation ambiguous in cases where the use of technologies affects the conditions for public administration and decision-making in specific ways. This increases the risk that the administration or individuals are not given sufficient guidance on how to apply the rules in a predictable and consistent way.[1237] As have been discussed, such uncertainties have in some cases arisen on how to interpret and apply technology neutral constitutional or administrative frameworks (such as the APA).[1238] As also have been seen, however, the technology neutral approach has not been applied to the full extent, and there are indications that, at least regarding more narrowly defined administrative tasks of specific authorities, it is more frequently the case that technology-specific regulations are being introduced into Swedish legal frameworks.

Additionally, it has also become increasingly common for the conditions for digitalisation and automation to be considered already in the legislative drafting phase, so that the rules are designed to support the rules' legal application of or in relation to technologies. Here, both DIGG and eSam have produced guides for digital-ready legislation.[1239] The guides include details on the pros and cons of regulatory frameworks tailored for computational execution. They offer recommendations on crafting comprehensive regulations, maintaining consistent use of concepts, employing high-quality data, ensuring transparent decision-making, and formulating criteria, including logical or arithmetic judgments. However, there are no regulated obligations to consider or implement the recommendations of these guidelines in legislative drafting.

As also seen in this section, another characteristic to the Swedish regulatory approach to digitalisation is that (although also increasingly common) it is still fairly unusual that statutory obligations to implement specific digitalisation initiatives are placed directly on Swedish authorities. More common is that the Government opts to, via decisions or appropriation directions, assign authorities to cooperate with a defined set of other authorities for a defined digitalisation objective.[1240] Such governance options must, however, not conflict with the constitutional independence of the authorities, and are also only available to the government in relation to government authorities. For the municipal level (both local and regional), the government's available governance tools include the enabling or encouraging of digitalisation

1237. Cecilia Magnusson Sjöberg, The Swedish Administrative Procedure Act and Digitalisation, 50 Years of Law and IT. The Swedish Law and Informatics Research Institute 1968-2018. Ed. Peter Wahlgren, pp. 309-320, p. 310.
1238. See section 2.
1239. Skapa automationsvänliga regelverk,/ DIGG https://www.digg.se/kunskap-och-stod/skapa-automationsvanliga-regelverk Accessed 12 December 2023; Digitaliserbar lagstiftning./ eSam ES2023-09 https://www.esamverka.se/download/18.43a3add4188b9f2345a2fe2b/1687332593062/ES2023-09%20Promemoria%20Digitaliserbar%20lagstiftning.pdf Accessed 12 December 2023.
1240. Styrning Av Digitala Investeringar Delrapport./ The Swedish Agency for Public Management [*Statskontoret*] dnr 2020/40-5. p. 12 et sec.

initiatives by, for example, allocating budget funds.[1241] While it should be stressed that the government does not lack governance options, the technology-neutral approach combined with modest elements of direct rule governance and a decentralised administrative structure can be said have an interlinked effect that manifests another distinctive feature of the Swedish digitalisation strategy – namely, that digital developments often are expected to be accomplished through cross-sectoral and cross-authority collaborations. As have also been exemplified in this section, the forms and substance of such collaborations can be subject to both weak or strong governance through government mandates and regulations – or rely entirely on the authorities' own interpretation of their needs and mandates.

Thus, while there is a discernible shift toward a more direct regulatory approach to technologies (also partly mandated by EU regulations such as the GDPR, the AIA and the Single Digital Gateway Regulation), the fundamental imperative remains. Even as we look ahead, Swedish national authorities will need to adeptly interpret and apply a predominantly technology-neutral regulatory framework. They must also translate it into practical, technology-enabled activities, ensuring that such endeavours uphold essential rule of law values such as legality, equality, and proportionality. In the face of both current and potential future legal uncertainties and complexities, the nurturing of collaborative cross-sectoral and cross-authority initiatives appear important to prevent the scattering and fragmentation of the understanding and implementation of rule-of-law values, ensuring they are not confined to narrow interpretations within specific sectors.

4. Swedish Public Sector Accountability in the Digital Era

Accountability may be regarded as a bedrock of democracy. The concept of accountability is, however, multifaceted. Its materialisation within the Swedish legal order is also multi-layered. The following subsections will focus on public sector accountability in the digital era from the primary perspective of democratic accountability, while recognising that there are other subjects as well as objects of accountability that are imperative for the realisation of the rule of law in the digital context.

4.1 Democratic Accountability

Democratic accountability is a broad concept that includes questions about how the institutional structure of the state can safeguard the democratic arrangement. Within the context of rule of law as a fundamental component of this democratic framework, this section emphasises the aspect of democratic accountability, with a particular focus on transparency as a fundamental element supporting a system of public governance that can withstand close examination.

Transparency can be perceived as an essential prerequisite for democratic accountability. Just as the concept of accountability, however, transparency is also a multifaceted concept as well as a relational one in the sense that its realisation (that is, to attain transparency) depends on what is supposed to be transparent and for whom.[1242] Main attention will here be paid to transparency of the state's technologically mediated exercise of power in relation to citizens. This means that the 'what' is supposed to be transparent is the operation and decision-making of state authorities and institutions, and that the 'whom' transparency is supposed to benefit is the general public, ensuring that citizens are well-informed and have access to critical information about their government's actions and policies.

1241. As seen in section 1.3 the Swedish local government regime is fundamentally based on the principle of local self-government where the municipalities themselves choose and prioritise their tasks. Swedish municipalities do, however, also have many regulated responsibilities. But, as any statutory obligation which restricts the principle of local self-government must be given in the form of a law and not restrict local self-government beyond what is necessary, the Government lacks direct powers to impose tasks on the municipalities.
1242. Robots and Transparency: The Multiple Dimensions of Transparency in the Context of Robot Technologies./ Felzmann, Heike, Fosch-Villaronga, Eduard, Lutz, Christoph and Tamo-Larrieux, Aurelia. In: IEEE Robotics & Automation Magazine, Vol. 26 No. 2 2019, p. 71–78.

It might be noted from this section's earlier accounts of the APA that Swedish administrative law lacks any provisions requiring computer programmes or algorithms to be documented or added to the basis for decisions in individual cases.[1243] It also lacks any specific provisions on explainability of automated systems used for decision-making or administrative tasks.[1244] Furthermore, the APA's duty to state reasons does not cover the system logic or the functioning of the algorithm(s) that have executed the decision-making, but rather the legal basis for the decision-making. The same can be said of the APA right to access to information for parties (which applies only to private persons who is a party in an administrative matter). Notably, the party informational rights do include access to 'all material included in the matter', thus including access also to documents which do not have official document status (unless there are confidentiality restrictions as established in the Chapter 10, Section 3 of the Public Access to Information and Secrecy Act (*Offentlighets- och sekretesslagen (2009:400)*), OSL). However, system documentation relating to the general functioning of an automated system which has assisted the administration of the matter will typically not be regarded as having been 'included' in that specific matter.[1245]

Notwithstanding the above, the extensive and constitutional right of access to official documents means that Swedish law does provide transparency rights which carries over to public sector uses of automated systems etcetera to assist their public tasks. Especially the question of whether the right to access official documents covers algorithms or computer systems is pertinent. In this context, one question is whether algorithms are to be regarded as complete electronic documents within the meaning of the Freedom of the Press Regulation or whether they are to be regarded as independent parts of a programme which must therefore be compiled in order to be made available. If a question of compilation, the authorities must only provide a specific compilation to the extent that this can be done by 'routine measures'. Mention may also be made here of the case mentioned earlier, in which the Supreme Administrative Court ruled that a labour input of 4-6 hours to compile certain data from a recording for automated processing is too much to be regarded as routine measures.[1246]

A detailed account for the requirements that must be met for an algorithm used by an authority qualify as an official document is not expedient here. However, it is worth noting that in several instances, national courts have recognised source code as official documents. For instance, the Supreme Administrative Court ruled in two cases that source code indeed falls under this category.[1247] In 2020, an administrative court of appeal made a similar judgment regarding an algorithm employed by the Trelleborg municipality for automated decisions concerning income support.[1248]

Nonetheless, the classification of source code as an official document does not automatically imply unrestricted disclosure, as there are various secrecy regulations that can restrict transparency rights. In the aforementioned Trelleborg Municipality case, Chapter 31, Section 16 of the OSL, which safeguards individuals' business and operational interests, was considered. The court concluded that the software supplier would not suffer harm if the source code were revealed, given that the municipality owned the software directly and not solely through a supplier license.[1249] Hence, the right to access the source code could not be curtailed in this instance to safeguard the supplier's business relationships. However, the rule was applied with a different outcome by the Supreme Administrative Court in the above-mentioned case from 2016.

1243. Swedish Governmental Inquiry 2018:25. Law as support the digitalisation of the administration [*Juridik som stöd för förvaltningens digitalisering*]. p. 173.
1244. Of note is that the GDPR informational requirements in Articles 13–14 do apply.
1245. Swedish Governmental Inquiry 2018:25. Law as support the digitalisation of the administration (*Juridik som stöd för förvaltningens digitalisering*). p. 155 f.
1246. Supreme Administrative Court HFD 2015 ref. 25. See also section 2.2.
1247. Supreme Administrative Court RÅ 2004 ref. 74; Supreme Administrative Court dom 2016-09-26 mål 3969-16.
1248. Supreme Administrative Court dom 2016-09-26 mål 3969-16.
1249. Supreme Administrative Court dom 2016-09-26 mål 3969-16.

The case concerned a request for access to two printed pages of an executable file concerning the Windows operating system used by the Administrative Court of Appeal in Gothenburg. As stated above, the Supreme Administrative Court found that, although the official document criteria were met, the requested pages constituted a part of the operating system and were covered by Microsoft's business and operating conditions which triggered the application of Chapter 31, Section 16 OSL.[1250]

Furthermore, Chapter 19, Section 1 of the OSL is also noteworthy in this context, as it mandates confidentiality for an authority's business or operational interests if disclosing the information could benefit others with similar activities at the expense of the authority. The Supreme Administrative Court evaluated this provision in a 2004 case involving a request for access to the source code and system structure information of an administrative system at Stockholm University. The court found that secrecy provision did not apply since the system was not used in any commercial activity and the university could not be considered to be engaged in a commercial activity. The documents were therefore to be disclosed.[1251]

Lastly, Chapter 18, Section 8, Paragraph 3 of the OSL pertains to confidentiality regarding security or surveillance measures for systems engaged in automated information processing. For example, an administrative court of appeal rejected a request for access to the software or algorithms underpinning the Swedish Social Insurance Agency's decisions on dental care subsidy, citing the potential risk of undermining the purpose of the automated measure, which was to ensure that dental care allowances were allocated only to those entitled to them. The court argued that disclosing the data could indirectly reveal ways to circumvent the system.[1252]

A further example is also found where the Swedish municipality of Trelleborg, in June 2021, was criticised by the Parliamentary Ombudsman for taking too long to provide requested information about a system used to make automated decisions on income support (*Försörjningsstöd*).[1253] The background was that a Swedish trade union, Akademikerförbundet SSR, had requested that the municipality, on the basis of the principle of public access to official documents, would provide information on how the algorithm which controlled the automated decision-making system worked. The municipality initially responded by requesting a specification of what information the request covered, and this request was later followed by e-mail correspondence combined with one physical meeting between the parties. The municipality did successively email different types of information relating to the system, but which the trade union did not consider corresponded to its request or answered the questions posed. During their meeting, the parties agreed that the union would receive a set of screenshots, including a graphical representation of a 'decision tree'. The union specifically requested this to better comprehend the system's functioning. However, these screenshots were not disclosed until after the trade union had chosen to file a complaint with the Ombudsman against the municipality.

The Ombudsman's assessment in the case was characterised by the fact that the municipality (although late) had already disclosed the agreed information at the time of the review, and was therefore focused on the fact that the request had not been handled promptly. The Ombudsman did initially frame the legal question of the case to be whether the requested information referred to an official document according to the constitutional Freedom of the Press Act (*Tryckfrihetsförordning (1949:105)*) regulations, but, however, did not make any own assessment of whether this was the case. Instead, the Ombudsman referred to the custom practise that an Ombudsman, as a starting point, should be reluctant to comment on an authority's assessments in substance in individual cases. As a consequence, the Ombudsman, in absence of information to

1250. Supreme Administrative Court dom 2016-09-26 mål 3969-16.
1251. Supreme Administrative Court RÅ 2004 ref. 74.
1252. Administrative Court of Appeals, Stockholm, dom 2019-08-27 mål nr 4995-19.
1253. Swedish Parliamentary Ombudsman, decision JO 6783-2019, 9th of June 2021.

the contrary, did not question the municipality's assessment that the screenshots did not constitute official documents. The Ombudsman did, however, criticise the municipality for its slow administration of the information request, and stated that this handling had been too slow regardless of whether the request could be seen as having been based on a right to access official documents by virtue of Chapter 2, Section 15 of the Freedom of Press Act, or whether the municipality instead should be seen as having offered a copy of the screenshots by virtue of its service obligation regulated in Section 6 of the APA. Despite this being the express wish of the complaining party (the trade union), the Ombudsman did thus not express an opinion on whether the requested information qualified as official documents or not, which would have been desirable from the point of view of legal guidance regarding access to information on algorithmically supported public decision-making.[1254]

The overview provided in this section shows that the transparency rights regarding technologically mediated exercises of powers in relation to citizens that Swedish law may provide in addition to GDPR informational rights and obligations, primarily hinges on access to official documentation rights. As these rights are access to document-rights, however, they do not obligate public administrations to organise this documentation in a way that is (in a pedagogical sense) aimed at enabling the public to understand how the systems can influence the exercise of power either in general or in an individual case. Furthermore, there are legal ambiguities concerning the specific application of secrecy regulations, as well as questions regarding whether access to source code genuinely provides substantive transparency to citizens, or rather acts as a barrier to understanding how public powers are wielded (as it typically demands specialised knowledge held by a select few). With the upcoming AIA, public authorities utilising AI systems in settings which will qualify as high-risk under the regulation will be subject to rather substantial requirements of documentation and records-keeping regarding system functionalities.[1255] Though the AIA's primary intent for this documentation is to facilitate supervision and establish internal governance structures for system providers (and, to some degree, for system deployers), the increased documentation volume resulting from these requirements is likely to produce a greater number of documents containing system information that also meet the criteria for official documents in the Swedish setting. This underscores the need for legal developments to delineate the parameters governing the application of national confidentiality rules.

4.2 The Role of Courts and Supervisory Bodies in Enforcing Accountability

The development of administrative law principles for the digital age has not been a focus in Swedish case law. As seen above, the Supreme Administrative court have been fairly active in matters pertaining to public access to official documents and the associated extent of applicable secrecy regulations. But while the national administrative courts, for example, have reviewed automated decisions for many years, they have seldom addressed principled questions regarding the role of administrative procedure in a digital context. This is likely to have, at least partially, to do with national administrative procedure in which the court review focuses on the substantive correctness of individual decisions. As a result, findings that an authority's automated processing has led to an incorrect decision or failure to comply with formal requirements would typically result in the rectification of that individual decision (or in the matter being remanded to the decision-making authority for reconsideration and a new individual decision) – and not in the automated system as such being subject to review.[1256]

1254. As a side note, it can also be noted that Trelleborg thus applied procedures with a fully automated decision-making procedure at a time before the above-mentioned amendments of the SLA entered into force in 2022, and thus before there was a legal basis for such decision-making. The circumstances behind the decision therefore also reflect the legal uncertainty regarding automated decision-making in the municipal sector before the 2022 amendments
1255. See more about the AIA in section 5.
1256. On the general legal perimeters for review and decision-making powers of the Swedish administrative courts, see Domstolsprövning av förvaltningsbeslut. Svensk, dansk och österrikisk rätt i komparativ belysning./ Larsson, Torvald. LL.D Thesis Lunds University, Media-Tryck, 2020. p. 301 et sec.

Instead of in national courts, the preparation of matters in an efficient and secure manner is typically addressed by supervisory bodies. The Swedish supervision and control of the administrative authorities is usually distinguished into 'ordinary' supervision performed by competent national authorities with designated and specified supervisory objectives as well as mandates, and 'extraordinary' supervision performed by the constitutionally established supervisory bodies the Parliamentary Ombudsman (set up under the Parliament) and the Chancellor of Justice (set up under the Government). Since these bodies have different mandates and competences to carry out their oversight, the extent to which the public administration's digital practices as such become subject to review may vary.

As of yet, the Parliamentary Ombudsman *(Justitieombudsmannen)* has been the most active in providing legal guidance on issues related to the digital public administration. The Ombudsman has handled multiple cases involving public digital services or automation, for example, where it has issued non-binding statements of critique. One example is the above-mentioned Ombudsman decision where the Ombudsman found the Swedish Migration Agency's use of fully automated decision-making on complaints on slow procedure to have several shortcomings.[1257] In addition to the discussed circumstance that the system could not produce section 32 APA-compliant reasons for its decisions, one other alarming circumstance was that the Ombudsman found that the system was not able to take into account the individual circumstances of a case. While the transition to automated decision-making had enabled the authority to deliver decisions in time, the Ombudsman stressed that the procedure in practice meant that the outcome had been predetermined. The Ombudsman also found that the result in *all* cases had been that the system had rejected the complaint. The conclusion was that the automated processing had led to individuals not getting the effective examination of whether the handling of their case had been unnecessarily delayed that the regulations on bringing an action for delay was meant to realise. The Ombudsman stated that the Migration Agency's automated procedure thus in practise meant a circumvention of the regulation on remedies for delayed action in Section 12 of the APA. As a result, the Migration Agency partly changed its procedures for administering these types of cases.

The Ombudsman has also in other cases investigated and issued critical statements based on complaints where the deployment of automated procedures had led to erroneous decisions being taken, but where the authorities have been slow to correct them. The Swedish Road Administration was, for example, criticised for slow rectification of an erroneous tax decision that was made after a vehicle had, incorrectly, been identified by an automated system as having passed a payment zone.[1258] In another decision, the Swedish Social Insurance Agency was criticised for not having adjusted, in time, errors that had arisen in the automated processing relating to sickness benefit qualifying income, as this error had resulted in the individual having decided to withdraw an appeal and therefore had suffered a loss of rights as a result.[1259]

The Swedish Public Employment Service has also, for example, been repeatedly criticised for the fact that, as a result of automated processing practices, having recurrently informed jobseekers that they risked sanctions or even suspended their right to compensation without there being any reason to do so.[1260] In the decisions, the Ombudsman did not touch specifically on any legal issues related to the respective authorities' mandates for applying automated procedures, but rather emphasised the responsibility to have safeguarding measures in place to correct errors arisen through automated processes. On a similar note, the Parliamentary Ombudsman has also repeatedly criticised the Swedish Transport Agency since the automated procedures applied by the authority in some cases had led to claims being handed over to the Swedish Enforcement

1257. Swedish Parliamentary Ombudsman, decision JO 2022/23 p. 481. See section 2.3.
1258. Swedish Parliamentary Ombudsman, decision JO 2008/09 p. 277.
1259. Swedish Parliamentary Ombudsman, decision JO 2008/09 p. 374.
1260. Swedish Parliamentary Ombudsman, decision JO 2017/18 p. 42 and JO 2021/22 p. 27.

Authority *(Kronofogdemyndigheten)* for collection without a payment reminder being sent to the individual. In all these cases, errors in the automatic transfer or storage of address data had led to incorrect registering of addresses in the road traffic register – even though the correct address was readily available in the population register. The system, however, only sent payment reminders to the transferred addresses in the road traffic register, and additionally applied the practice of cancelling the mailing after two mailings were returned at least two months apart. This meant that the individuals affected by the system error that did not receive a payment reminder, while their debts were still automatically sent to the Enforcement Authority for collection.[1261]

Just as the Ombudsman, the Chancellor of Justice has also reviewed the Swedish Transport Agency's automated processing for the collection of taxes and fees, and extensively criticised these practises in a (non-binding) formal statement.[1262] The criticism included the same deficiencies in the automated management of fee and tax collection that were previously highlighted by the Ombudsman (that cases might be handed over to the Swedish Enforcement Authority for collection without any payment notice having been sent to the debtor). The Chancellor stressed, from a legal certainty point of view, that it is unsatisfactory that a payment obligation and delay could arise through an automatic transaction in an authority's internal system without this being manifested externally in any way. He also pointed out that it must not occur that collection is sought before any payment obligation has arisen. In addition, the Chancellor also criticised that the system in some cases imposed reminder and additional fees on the individual despite the fact that no mailings regarding neither the original fee, nor the reminders, had been sent, and that there was no statutory recognition for this practise. The Swedish Transport Agency stated that it, since the time of review, had upgraded the system functionality in key respects, and the Chancellor marked the probable need for returning to some of the highlighted issues in future supervision.

It should be noted that automated processing practices has not only been the subject of review, but has also been emphasised by the Chancellor of Justice as a recommended measure for how to address other (predominantly manual) problems that have been identified during review. In a review of the fulfilment by three criminal investigation authorities of their obligation to notify the Swedish Transport Agency of decisions affecting the withdrawal of driving licences, the Chancellor found that this obligation was unsatisfactory met.[1263] The Chancellor found these problems to largely relate to inadequate procedures for documentation and information transfer, and argued that a suitable remedy would be increased automation of the processes. The Chancellor stated, in particular against the background of the Swedish Prosecution Agency's *(Åklagarkammaren)* view that it is becoming increasingly difficult to enforce manual procedures when more and more of the activities are automated and digitised, that this view confirms the importance of automation to ensure correct application of the law.

In addition to the Ombudsman and the Chancellor of Justice reviews, it has also become more common for supervisory authorities to address digitisation and automation-related legal issues in their regular supervision. No comprehensive account is expedient here. However, some of the more comprehensive and wide-ranging reviews carried out in recent years will be outlined below as they provide an overview of the perceived merits and problem areas of digital administrative practices.[1264]

1261. Swedish Parliamentary Ombudsman, decisions of 10 January 2018 in case 7713-2016, of 25 June 2014 in cases 3822-2013 and 2732-2013 and of 20 June 2013 in case 5445-2012.
1262. Chancellor of Justice, decision JK dnr 2060-19-2.4.1 21 October 2020.
1263. Chancellor of Justice, decision JK dnr 2021/3068 26 October 2022.
1264. See also, Rättsstatliga principer och beslutsprocesser i en (alltmer) digitaliserad och automatiserad förvaltning./ Enqvist, Lena and Naarttijärvi, Markus. Rättsstaten i den svenska förvaltningen : en forskningsantologi. Statskontoret 2022.

Under 2020, for example, the Swedish National Audit Office, NAO, reviewed the effectiveness and efficiency as well as legality of automated decision-making practices by government authorities. The review in particular examined parental benefits administration at the Swedish Social Insurance Agency, the administration of annual income taxation of private individuals at the Swedish Tax Agency, as well as of the driving licence learner's permits at the Swedish Transport Agency. NAO found that automated decision-making did increase the efficiency and effectiveness of these practices, and that they also had led to some improvements in fundamental legal certainty due to increased uniformity. However, NAO also found procedural shortcomings in cases with a high risk of fraud and error and identified as a problem the limited follow-up on the correctness of automated decisions. In this context, NAO pointed to problems regarding the unclear division of responsibilities for automated decision-making processes, and to a lack of clear and readable documentation of the automated processes. The review showed that the documentation of follow-up activities had shortcomings, and that the authorities' manual controls of cases with a high risk of fraud and errors were inadequate. Another finding was that the fully automated decisions were only monitored to a limited extent, resulting in insufficient frameworks for detecting and rectifying incorrect decisions. The ability to translate legislation into machine code was identified as a critical factor in ensuring correct and legally certain automated decisions, at the same time as the authorities also experienced challenges in securing adequate competencies to ensure correct conversions. Based on its findings, NAO highlighted the need for knowledge bases and support functions for authorities to be developed. The Swedish Agency for Digital Government (DIGG) was found to be the national authority best suited for developing and administering such a knowledge basis.[1265]

Another example of monitoring activities by national supervisory bodies is found in a survey made by the Swedish Equality ombudsman in 2022 on how government authorities use AI and automated decision-making, and to what extent they consider the risks of discrimination and barriers to equal rights in the application of these technologies. The authority found that 14 out of the 34 surveyed authorities were deploying automated decision-making that concerned a large number of individuals. It also, overall, found that these authorities showed some insight into the risks of discrimination related to automated procedures, but that they primarily focused on ethics and integrity challenges rather than discrimination challenges. It was found that those authorities that deploy automated procedures do conduct different types of risk analyses and quality assurance follow-ups, but that these rarely consider the grounds of discrimination. The surveyed authorities did stress that they would like to see knowledge-exchange with the Equality Ombudsman on these issues, and pointed, as one potential risk of discrimination to the risk of case officers giving too much weight to the automated decisions and losing the ability to critically appraise them. However, the Equality Ombudsman concluded that the perspective of discrimination was largely absent from the automated decision-making processes at the reviewed government authorities, and that few of them saw any need to do more to reduce the risk of individuals being disadvantaged. Based on this, the Equality Ombudsman remarked that Swedish government authorities need to increase their awareness of the prohibition of discrimination in the context of AI and automated decision-making (the Ombudsman also noted that there is reason to think that this need is present amongst public authorities beyond those surveyed as well).[1266]

In an audit from 2023 of some ten major authorities' use of digital services in their contacts with private individuals, NAO found that most of the audited authorities offered a wide range of digital services, and that work is underway in many areas to digitise further services. However,

1265. Automated decision-making in public administration – effective and efficient, but inadequate control and follow-up./ Swedish National Audit Office (Riksrevisionen) RiR 2020:22 2022. p. 1 et sec.
1266. Transparens, träning och data - Myndigheters användning av AI och automatiserat beslutsfattande samt kunskap om risker för diskriminering./ Equality Ombudsman (*Diskrimineringsombudsmannen*) 2022:1.

the audit also pointed to some significant obstacles to the development of government services that are fully digitised as well as coordinated between authorities, which were found to be of primarily legal nature. These legal obstacles were found to be of general as well as sector specific character, and mainly related to the conditions for information exchange between authorities. The summary conclusion was that the Government has been too passive in removing such regulatory obstacles.[1267]

While the above examples do not amount to a comprehensive account, they underline that it primarily is the Swedish supervisory bodies that (at least as of yet) have provided the most guidance on the legal boundaries for public administration digital practices (such as automated case management or decision-making or digital services). More research is needed on the how the national administrative procedure is equipped to provide legal guidance on issues relating to public digital practises. The same is true for how the national supervisory system is equipped to identify, review and rectify any actual or potential digital- or automation related malpractices by public authorities.[1268] The national supervisory comprises many different supervisory bodies with different types of supervisory objectives as well as mandates. These differences also affect how the authorities may or are likely to exercise their supervisory powers against authorities utilising technologies in their services, decision-making and other concrete activities.

Against the discussion above, one fundamental aspect of note is also whether the supervision takes place as a result of an impulse via an individual complaint, or whether the supervision is initiated on the supervisory body´s own motion. Another fundamental aspect is whether the review is focused on lawful compliance in the handling of individual cases, or whether it is focused rather on organisational or systemic issues which might render non-compliance (or a risk thereof). Neither the Ombudsman nor the Chancellor of Justice have an obligation to investigate all individual complaints, even where it can be established that rules have been breached.[1269] They both, however, may initiate investigations based on individual complaints as well as on their own motion. They therefore have some discretion in deciding which complaints should be reviewed. From the perspective of the individual's possibilities to bring about a review of an authority's digital or automated practices, neither the Ombudsman nor the Chancellor of Justice's supervision offers any right to review individual cases. Neither one of them constitute appeal bodies and may not alter administrative decisions.[1270] Their decisions are also not binding on the subjects of the supervision (here, the authorities) as well as cannot be appealed. However, the statements of the Ombudsman or the Chancellor of Justice traditionally hold significant influence over the behaviour of public authorities. The Ombudsman and the Chancellor thus wield a soft power to promote the rule of law in public administration, as well as hold one sharp but rarely used tool in their box to initiate criminal proceedings for official misconduct *[tjänstefel]* as a last resort.[1271] However, for the complaints that the Ombudsman or the Chancellor chooses to review, the examination framework is relatively free and allows for the review of issues typically outside the purview of courts.[1272] Therefore, within the framework of their mandate to review that the exercise of public power remains in accordance with laws and regulations, both the Ombudsman and the Chancellor have good formal conditions for reviewing and providing legal guidance on the public administration's digital practices, automated decision-making, or other technological practices from the perspective of legality and good administration. Their

1267. Digitala tjänster till privatpersoner– stora utvecklingsmöjligheter för statliga myndigheter./ Swedish National Audit Office (Riksrevisionen) RiR 2023:6. p. 1 et sec.
1268. The reference to the national supervisory system here includes when the authorities act as competent national authorities performing supervision under EU law provisions.
1269. No such obligation is regulated either in the Act (1986:765) with instructions for Parliamentary Ombudsmen *(Lag (1986:765) med instruktion för Riksdagens ombudsman]*, in the Act (1975:1339) on the supervision of the Chancellor of Justice *[Lag (1975:1339) om justitiekanslerns tillsyn)*, or in the Ordinance (1975:1345) with instructions for the Chancellor of Justice *(Förordning (1975:1345) med instruktion för Justitiekanslern)*.
1270. Swedish legal system./ Wong, Christoffer, and Bogdan, Michael. 2 ed. Stockholm: Norstedts juridik, 2022. p. 72.
1271. The Chancellor of Justice is, additionally, also competent to reach out of court settlements on behalf of the State in actions for damages.
1272. Swedish legal system./ Wong, Christoffer, and Bogdan, Michael. 2 ed. Stockholm: Norstedts juridik, 2022. p. 72.

frameworks also allow them to approach not only isolated malpractices, but also systemic issues where digital and automated procedures are associated with either identified malpractices or risks of such conducts (such as seen in the examples of critique statements above).

No comprehensive account can be given for how well aligned the mandates and powers of those authorities who discretely but together form and perform the so-called 'ordinary' supervision of public practises are to capture errors and risks arising from public digital practices. Some of these authorities may decide to review incoming complaints at their discretion, and others may be obliged to review such complaints. Furthermore, some of them might only have a mandate to perform systemic reviews with one or more specified focuses (such as legality review, economic review, equality review etcetera). The conditions for, or likelihood of, these different supervisory bodies to focus specifically on the legality of digital practices in the context of this supervision may therefore vary. As seen in this section, however, a tentative trend can be discerned at least in the more systemically oriented supervision – that focus is increasingly directed towards digital and automated practices in public administration. Recent large-scale examinations and evaluations, such as those concerning authorities' procedures to mitigate discrimination risks related to AI systems or their procedures regarding automated decision-making (as demonstrated in this section), serve as clear indicators of this trend.

Thus, as an overall reflection, it is clear that the Swedish administrative system is inclined towards trusting supervisory bodies to take the lead role in addressing the challenges that public sector digitalisation or automation may introduce into the administrative practise from a rule of law and good administration perspective. While the digital transformation has been ongoing for decades, a cautious trend can be discerned towards digital practises increasingly coming under the purview of supervision. This shift in focus seems to be driven by several factors, including technology advancements, changes in the public's access to digital services, and the evolving landscape of administrative practices. While it should be emphasised that an overall view of the review-system reveals rather limited options for individuals to initiate a review of the administration's digital practices, there are established review mandates in place to enable the monitoring of the lawful and responsible use of technology in the activities of public authorities. If the trend towards heightened scrutiny gains traction it will hopefully lead to the development of more comprehensive legal guidance. This would be welcome particularly in areas pertaining to the application of technology-neutral provisions within technology-affected contexts.

5. The Proposed EU Regulation on Artificial Intelligence from a Swedish Perspective

Sweden aims to be world-leading in utilising AI technologies in the public sector (a goal which Sweden seems to share with many other countries such as several other Nordic-Baltic states).[1273] As discussed, the efforts to realise this vision have taken many forms but have generally been subject to relatively little direct regulatory governance.[1274] As has also been touched upon, and as will be the topic of further elaboration in this section, however, the AIA introduces a battery of technology-specific provisions placing obligations on public administrations utilising AI technologies. This warrants the question of whether and, if so, how the Swedish national administrative law regime, which is primarily designed to be technology-neutral, can be challenged or complemented by the new AIA.

1273. Swedish Legislative Bill 2011/12:1 Budget proposition for 2012 [Budgetpropositionen för 2012] utg. omr. 22; Parliamentary decision rskr. 2011/12:87. Förstärkt AI-förmåga i Sverige/ Ministry of Finance (*Finansdepartementet*) Dir. 2023:164.
1274. See section 3.

The AIA's overarching objectives encompass the dual goals of ensuring the safety and compliance of AI systems with existing laws pertaining to fundamental rights and Union values, while also improving the governance and efficient enforcement of these laws.[1275] The regulations, particularly outlined in Chapter 2 of the AIA, which cover data governance, documentation, transparency, human oversight, robustness, accuracy, and security, introduce several requirements that will impact the organisational structures of authorities. Roughly, the requirements for pre-testing, risk management, and human oversight can be seen as aiming to protect other fundamental rights by reducing the likelihood of erroneous or biased AI-assisted decisions in critical domains. In the event that violations of fundamental rights do occur, a combination of transparent and traceable AI systems, along with robust post-implementation checks as mandated by the AIA, are meant to enable effective remedies for affected individuals.[1276] These requirements emphasise principles of transparency, fairness, and accountability. While they do have a specific connotation and application in the context of AI technology design and use, they do also align with the general rule of law and good administration principles within EU law, as well as in the Instrument of Government and the APA.[1277]

However, before any conclusions can be drawn about the impact that the AIA will have on the public sector's AI use more generally, one primary question is to what extent the authorities' AI use will trigger the obligations in (especially) Chapter 2. The risk-based orientation of the regulation, namely, in essence means that only those AI systems that qualify as high-risk will be subject to the stricter and more substantive compliance regime (all the above-mentioned chapter 2 obligations will only apply to AI systems which qualify as such).[1278] In the Annex III AIA list of the areas for AI deployment that qualify as high-risk, there are many areas where public sector use seems to occur (or be most common). For instance, AI systems used in domains related to essential services, like assessing eligibility for public assistance, are included. The annex also outlines potential high-risk AI applications in education, vocational training, law enforcement, migration, asylum, border control, and the administration of justice. Each of these sector-specific uses are further elaborated and exemplified in the annex. The list clarifies that many AI applications within the public sector will indeed fall into the high-risk category – at the same time making clear that not all of them will. Consequently, authorities will need to address delineation issues, as not all AI applications within public administrations will meet the criteria for high risk. In general, however, it can be noted that most uses of AI systems that are closely linked to the authorities' exercise of power over individuals will likely qualify as high risk.

The detailed obligations of the AIA cannot be expanded on here. Of note is, however, that while the Chapter 2 obligations (which applies to 'providers' of high-risk AI systems) orients the obligations towards training and system design issues, they also have, by extension, effects on the organisational facets within the authorities responsible for ensuring compliance. The Article 9 AIA requirement of putting a risk management system in place is one example, as it mandates the establishment of the organisational structure needed to effectuate the management and maintenance of that management system. The Article 10 obligation to ensure that the training, validation and testing of data sets are subject to appropriate data governance and management practices is another example. The AIA also emphasises transparency and proper documentation as well as traceability and scrutability of high-risk AI-systems, especially through the Article 11 obligations on technical documentation, the Article 12 obligations on record-keeping, Article 13 obligations on transparency and provision of information to users and the Article 14 provision on

1275. Explanatory memoranda of the European Commissions 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. section 1.1.
1276. Explanatory memoranda of the European Commissions 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. section 3.5.
1277. See section 2.
1278. Article 8 AIA.

ensuring human oversight capabilities. Article 15 establishes obligations on securing that high-risk AI-systems achieve an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle.

Authorities must also, when acting as deployers of a high-risk AI system under Annex III, prior to putting the system in use, in most cases moreover perform a fundamental rights impact assessment in relation to the specific context of use. This assessment requires a comprehensive examination of key elements, including defining the system's purpose and scope, identifying affected individuals and groups, ensuring compliance with relevant laws on fundamental rights, evaluating foreseeable impacts on fundamental rights, assessing risks to marginalised or vulnerable groups, considering environmental consequences, and formulating a detailed plan for mitigating identified harms. Additionally, it mandates the establishment of a governance system, encompassing human oversight, complaint-handling, and redress mechanisms.[1279]

Taken together, these obligations are to serve a preventive function as well as aid efficient supervision of high-risk AI systems both internally (by producers and deployers of AI-systems) and externally (by the designated supervisory bodies). Another principal aspect of the AIA is that it comes with its custom compliance and accountability structure (including penalties and fines), as well as with a custom and comprehensive supervisory structure similar to that of the GDPR.[1280]

When focussing more specifically on the interplay between the AIA and Swedish administrative law, it is thus clear that the AIA within its scope of application will introduce a number of obligations on public authorities which utilise AI technologies. The rather extensive requirements for different types of risk assessments and documentation etcetera will mean that they will have to structure their considerations and decisions around the deployment of such systems in a more formalised way. This structured approach serves dual purposes: promoting both preventive measures and risk awareness while also enabling more effective supervision.

One aspect of the AIA which potentially reduces its regulatory grasp over the public sector AI utilisation is, however, that, although the regulation distributes obligations between both providers and deployers of AI systems, it places most of these obligations on the providers (meaning those natural or legal persons that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark).[1281] While this arrangement implies that public authorities might duck most of the AIA obligations by purchasing AI systems from external parties (making them the mere 'deployers' of such systems), the AIA does refer provider obligations on deployers in certain situations. If the deployer place on the market or put into service a high-risk AI system under their name or trademark, if they make a substantial modification to it or if they modify the indended purpose of a system so that it becomes a high-risk system.[1282] This means that where AI systems are purchased and later modified to a substantive extent to suit the specific needs of the deployer, deployers (such as public authorities) may come to take on and over the initial provider's obligations in relation to that specific AI system. In other words, it means that public authorities utilising AI systems which have been substantively adopted to suit specific deployment purposes often will qualify as providers under the AIA even where they have commissioned the AI system form a private party.

While the above discussed feature of the AIA is likely to have a significant impact on the applicability of AIA in public sector AI use, it should be stressed that the AIA is not a regulatory framework which intervenes on the administrative practises and decision-making procedures of

1279. Article 29 a AIA.
1280. Supervision of Artificial Intelligence in the EU and the Protection of Privacy./ Chamberlain, Johanna and Reichel, Jane. In: REALaw blog 2023 https://wp.me/pcQ0x2-Jc Accessed 12 December 2023.
1281. Article 3(2) AIA.
1282. This also applies to distributors, importers and other third-parties who make substantial modifications to the system, Article 28(1) AIA.

the administrative authorities as such. The focus of the AIA, as modelled primarily on a combination of fundamental rights, product safety and consumer protection law regulations, is the ensuring of safe and proper system functionality.[1283] While these objectives might broadly align with principles of good administration, the AIA does not regulate administrative procedure as such (except in matters relating to the administrative procedures for supervision of regulatory compliance). The AIA also lacks important individual procedural safeguards, such as the right to appeal decisions made by or with regard to AI systems.[1284] For any public sector AI uses, the availability and application of any individual procedural safeguards in contexts where AI technologies are utilised to make or assist public decision-making and exercises of power, will therefore largely depend on the national administrative procedures regulation (although taking note of the fact that the GDPR may provide individual rights to information, rectification, erasure and to object etcetera, by proxy of the fact that AI technologies generally utilises personal data to operate).[1285]

As a final remark it is also worth noting that much of Sweden's automated decision-making practices, at least as of yet, do not rely on AI technologies but rather on systems governed by rule-based logics that are more static and require human intervention (which are likely to escape the application of the AIA). While this scenario may change due to the accelerating uptake of AI technology in various deployment contexts, there is reason to believe that public administrations for the foreseeable future will still utilise rule-based systems which will not qualify as AI systems under the AIA. Consequently, these systems will not trigger the application of the regulation irrespective of whether they will be deployed in settings that the AIA would classify as high risk. Viewing the rule of law in the broader context of the public administration's use of technology for diverse tasks, the focus cannot therefore exclusively be fixed on the material scope and substance of the AIA. Despite the harmonising effect of the AIA, existing regulations to administrative procedure and rule of law in the evolving landscape of technology use in public administration are still highly relevant.

6. Conclusions

As demonstrated in this chapter, the influence of the Swedish administrative tradition is evident in shaping the trajectory of national public digitalisation initiatives as well as the regulatory framework within which they are executed. This influence underscores an emphasis on the authorities to leverage existing legal conditions to actualise visions of a digital administration characterised by both high-level service and legal certainty. Despite Sweden's high ambitions in leveraging the potential of technologies within the public sector, this chapter has, however, also highlighted several uncertainties or potential gaps in the regulatory landscape. These uncertainties or gaps pose challenges for the authorities in navigating the regulatory framework throughout the national, European and international levels.

6.1 Dimensions of legality-challenges

Focusing on the fundamental tenet of the rule of law, the principle of legality, three primary dimensions of challenges to legality may be discerned.

The first challenge-dimension relates to the tendency of already at the stage of legislative drafting adapt the regulations for computational execution (making them 'digital-ready'). While considerations about the conditions for automation at the legislative level are positive from both

1283. Demystifying the Draft EU Artificial Intelligence Act./ Veale, Michael Frederik Zuiderveen Borgesius, Frederik. In: Computer Law Review International No. 4 2021, p. 112.
1284. Article 68(b) AIA, however, contains a right lodge a complaint with a national supervisory authority if they consider that the AI system relating to him or her infringes the Regulation.
1285. While not the focus here, it should also be noted that the specific application of the GDPR individual rights may vary, as the many of those provisions which contain individual rights also contain express exemptions or opening clauses which allow for Union of Member state laws to make certain restrictions to these rights. Especially Article 23 authorises Member states to limit the rights of data subjects as outlined in articles 12–22 GDPR to safeguard public interests.

the perspectives of democratic grounding and systematic legal examination, there are also risks associated with this approach. The potential pitfalls include the simplification of laws to such an extent that the legislative framework's ability to achieve its intended goals is compromised, and associated risks for an overly formalistic application and the inadvertent creation of discriminatory effects.[1286] This risk therefore necessitates vigilant monitoring to prevent such unintended consequences.

The second challenge-dimension relates to legal uncertainties surrounding the conditions for developing or using technologies for public tasks, such as service provision and decision-making. As advancements in technology have tended to outpace the originally intended scopes of many legal frameworks, the absence of well-defined legal parameters can lead to arbitrary applications of technology in public services. Such uncertainty may also result in authorities refraining from considering new technological tools, even when these could have been beneficial from a legal certainty, service or efficiency perspective, for example. The Swedish lack of comprehensive principled discussions on technology-induced risks to the rule of law in the preparatory works of constitutional or administrative procedure regulations comes with the risk of diverse interpretations and sectoral applications among authorities. While variations may well be justifiable in their specific contexts, disparity also complicates the monitoring and assessment of whether rule of law values are susceptible to drifting in digital contexts, as well as of whether such deviations are warranted. This chapter has demonstrated that there are collaborative structures in place for many Swedish authorities to join forces with one another to leverage their perspectives and interpretations regarding such uncertainties at both the national and European levels.[1287] While this collaborative approach may aid in preventing unnecessary disparities, it also underscores that perceived challenges relating to legal uncertainties persist.

The third challenge-dimension is interrelated to the second one, but extends further into legal uncertainties regarding the safeguards that must be in place to mitigate the risks associated with the use of such technologies. The potential for unintended consequences, misuse, or infringement of individual rights necessitates a clear and comprehensive regulatory framework. Without explicit guidelines on the necessary safeguards, there is a heightened risk of unchecked technological interventions that may compromise the rule of law. Here, the chapter has discussed that the Swedish starting point is that the APA's general (and technologically neutral) safeguards provide sufficient protection in relation to the requirements set out in Article 22 GDPR for fully automated decision-making. At the same time, it has been discussed at the national level, among other things in light of the fact that Recital 71 mentions a right to human intervention, whether Swedish legislation should explicitly ensure such a right at least to some extent.[1288] The fact that the AIA will require high-risk systems to be equipped with technical human oversight capacities, and that deployers in their fundamental rights impact assessments must include what governance system the deployer will put in place, including human oversight, complaint-handling and redress, are additional factors that indicate that the issue of human oversight needs to be highlighted more in the Swedish national context. This is especially pertinent against the dual background of advancements in technology and EU regulatory changes. In light of these considerations, it would be commendable for the Swedish government to initiate a comprehensive inquiry aimed at analysing *whether* and, if so, *how* national legislation, such as the APA, should be adapted to explicitly incorporate rules pertaining to human oversight in decision-making substantively facilitated by technologies. Questions that such an inquiry could address

1286. Rättsstatliga principer och beslutsprocesser i en (alltmer) digitaliserad och automatiserad förvaltning./ Enqvist, Lena and Naarttijärvi, Markus. Rättsstaten i den svenska förvaltningen : en forskningsantologi. Statskontoret 2022, p. 217–249. At p. 229 et sec; Chapter Eight Digitally Ready Legislation in Danish Law: The Strengths and Weaknesses of Digital Simplicity in New Legislation./ Gøtze, Michael. Digitalisation of Administrative Law and the Pandemic-Reaction. ed./ Russel L Weaver and Herwig CH Hofmann Cambridge Scholars 2022, p. 132–160.
1287. See sections 2 and 3.
1288. See section 2.3.

include determining the criteria or principles that should guide when oversight should be carried out, specifying the focus of oversight (such as the technology's functioning or its output, for example), identifying the appropriate individuals to conduct oversight (e.g., administrators or technicians), and pinpointing the stages within a decision-making process where oversight is deemed essential (including whether supervision should take place at given intervals or on specific impulses).[1289]

The chapter has also discussed the fact that Swedish national law lacks any specific regulation regarding the individual's right to information about the use of, and case specific application by, automated systems. This issue has been partly inquired in a Swedish context but has not led to legislation.[1290] As part of the broader examination of Swedish procedural safeguards concerning technology-assisted decision-making, as advocated here, the Swedish legislator should also revisit this issue. A renewed inquiry is (too) particularly crucial, given the evolving landscape in both technology and EU regulations. In such an inquiry, comparative insights from the Nordic-Baltic experiences and interpretations of rule of law challenges as well as the need for, and design of, safeguards would be of great interest.

6.2 Rule-of-Law Proactiveness: Mitigating Risks Through Impact Assessments

The ideal concept of a rule-of-law state is that the legal system and administration should have such an open and well-configured organisation that the activities and decision-making of authorities are legally grounded by default. An important question, therefore, is how authorities avoid introducing technologies into their operations that may impact issues of legality, predictability, equal treatment, and proportionality, etcetera. In this context, risk and impact assessments have emerged as important rule of law safeguards. That such proactive and risk-oriented measures have gained regulatory traction is evident at the European level. In the chapter, the Article 35 GDPR requirement to perform data protection impact assessments, in particular where a type of processing using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, has been discussed.[1291] Furthermore, some risk-mitigation oriented obligations placed on providers and deployers of high-risk AI systems under the AIA, such as the provider obligations to put a risk management system in place, Article 9 AIA, and deployer obligations to perform a fundamental rights impact assessment, Article 29(a) AIA, have also been mentioned.[1292]

In the context of Swedish law, there is no specific statutory requirement imposing a general duty on national public authorities to conduct a 'rule of law' impact assessment before introducing new technologies into their operations and exercises of powers. However, a more abstractly formulated requirement to consider and minimise risks can be directly derived from the principle of legality.[1293] The legality principle assumes that authorities should not act in ways that might jeopardise its realisation, thereby necessitating risk or impact assessments before introducing technologies and systems that can affect the fundamental principles of the rule of law. Due to its high-level legal grounding, the perimeters of this assessment is, however, in comparison to the risk management and impact assessment obligations as mandated by the GDPR and the AIA, more abstract in terms of what particular risks is to be assessed, the methods to be used for the assessment, and how identified risks are to be mitigated. Clearer guidance on the principles of sound digital administration, if not in regulatory form, at least through more precise interpretations particularly from supervisory authorities, would therefore be welcome.

1289. 'Human Oversight' in the EU Artificial Intelligence Act: What, When and by Whom?'/ Enqvist, Lena. In: Law, Innovation and Technology, Vol. 15 No. 2 2023, 508-535. p. 13 et sec.
1290. See section 2.3.
1291. See section 2.3.
1292. See section 5.
1293. See section 2.3.

All in all, these proactive and risk-oriented measures are crucial safeguarding measures in preserving the integrity of the rule of law. However, ensuring that they actually go to such a detailed depth that they can identify real risks to rule of law values and the right to privacy, and are not just performed pro forma, requires diligent implementation. This can be particularly challenging as a combination of technical and legal expertise is often required. The fact that risk and impact assessments must encompass both legal and technical as well as organisational aspects is therefore essential. Here, too, there are opportunities for valuable comparative Nordic-Baltic insights concerning the comprehension and practical application of risk monitoring and impact assessments.

6.3 Rule-of-Law Responsiveness: Addressing Consequences Through Diligent Oversight

Although the ideal concept of a rule of law-state entails that decisions should, by default, be lawful, the legal system also presupposes that errors are committed or do occur. Therefore, it is also a central component in the practical realisation of rule of law values that safeguards are in place to detect and rectify any legal violations.[1294] The question then becomes when and how this should be done, and whether existing safeguards at the national constitutional level or in procedural rules such as the APA, combined with other regulations such as the ECHR or EU legislation, are sufficient to counteract technology-induced risks.

The question is broad and encompasses the above-mentioned proactive safeguards, such as human oversight. Such safeguards do serve a proactive function in that they are meant to preemptively address and mitigate potential risks to the legality, equality, or proportionality of decision-making. They may, however, also serve a reactive function as part of a responsive mechanism to react to, as well as ensure the rectification of errors. The relevance of reviewing whether specific human oversight requirements should be introduced in Swedish administrative law is therefore pertinent from this perspective.

This chapter has also noted the fairly limited involvement of Swedish courts in identifying and addressing rule of law issues associated with the administration's use of technology. This observation should not be misconstrued as an indication that courts lack legal mandates to oversee rule of law values tied to the use of technologies by public authorities. Instead, it should be underscored that the courts have crucial roles to play in monitoring and rectifying deficiencies on a case-by-case basis. For instance, the courts have a pivotal role in overseeing automated processes linked to case handling and decision-making, ensuring that such processes do not lead to authorities neglecting their duty of care. Additionally, the courts are essential in scrutinising the adequacy of the authorities' stated reasons for their decisions. This scrutiny is crucial to ensure that neither the courts nor the individuals affected by the decision face difficulties in comprehending the rationale behind it. In this regard, one critical aspect is the courts' monitoring of whether an individual assessment of the legally relevant circumstances has been conducted. This emphasises the importance of the judiciary in safeguarding the rule of law by ensuring that each case is considered on its merits and that the decision-making process remains transparent and comprehensible to the parties involved.

The chapter has also pointed out that Swedish supervisory authorities have been somewhat more active in addressing legal issues related to the administration's use of technology.[1295] It is true that the supervisory authorities have different primary objects of supervision. For instance, the Ombudsman's primary role is to oversee that those conducting public activities adhere to laws and statutes, fulfill their obligations, and notably ensure compliance with constitutional

1294. Administrative due process when using automated decision-making in public administration: some notes from a Finnish perspective./ Suksi, Markku. In: Artificial Intelligence and Law, Vol. 29 2021, p. 87–110. At p. 95 et sec.
1295. See section 4.2.

mandates regarding objectivity, impartiality, and non-interference with individuals' fundamental rights and freedoms.[1296] As an example, IMY will, on the other hand, will monitor compliance with privacy protection and the legality of the processing of personal data under the GDPR.[1297] The different orientations mean that the focus and scope of the oversight are limited, which can potentially lead to certain aspects of the use of technology being overlooked, and thus risk affecting rule of law values. Despite these limitations, overall, oversight contributes to opportunities to address different dimensions of technology use by public authorities. For instance, supervisory authorities typically possess the authority to scrutinise both organisational and technical factors that collectively shape the decision-making process in individual cases. Moreover, they usually have the autonomy to initiate reviews independently. This adaptability enables a more comprehensive supervisory approach, encompassing both technical and organisational factors that impact decision-making (aspects that are not typically covered by the courts' review process).

To identify risks or errors, both courts and regulators must enhance their awareness of technologies. This entails a heightened understanding of issues such as the risks of bias and effective methods to identify them, both at the group level and in individual cases. Another aspect is the necessity to increase awareness of the risks associated with an overly formalistic application of rules. Such awareness is imperative for courts or supervisory authorities to be able to identify and address any shortcomings in legality or safeguards in relation to the technological normativity that technologies introduce. It can be expected that the digital competence and capability of legislators, administrative authorities, courts and regulators will increase over time, resulting in judgments and decision-making practices that can clarify certain legal ambiguities without the need for specific regulatory initiatives at the national level. Also in this respect, there are clear benefits in learning from other Nordic-Baltic experiences in the oversight practices of supervisory authorities or courts.

6.4 Need for a Wide Lens on Technology-Induced Risks to the Rule of Law

While rule of law values such as legality, foreseeability, equality, and proportionality generally are strongly recognised in the Swedish legal system, as well as materialised throughout regulations from the human rights, constitutional and administrative law levels, their true realisation requires constant monitoring which is also adapted to societal changes – such as the use of new technologies in the public sector. A nuanced and comprehensive monitoring approach which recognises the gradient of effects that technology utilisation can introduce into the exercise of public powers is therefore crucial. This gradient perspective emphasises the need to assess each impact on rule of law values and to acknowledge the intricate interplay between technological advancements and these values.

The ongoing discourse on digitisation and automation often fixates on advanced technologies like artificial intelligence or far-reaching technology uses like fully automated decision-making. However, adopting a rule of law perspective requires the recognition of the broader socio-technical context in which authorities operate, urging consideration of factors that influence legally secure procedures at multiple levels of governance. This involves not only the design and drafting of legislation, but also the strategic procurement, design, and implementation of technologies by authorities.[1298]

1296. Sections 11–12 Act (2023:499) with instructions for the Parliamentary Ombudsmen (*Lag (2023:499) med instruktion för Riksdagens ombudsmän (JO)*).
1297. Section 2 a Ordinance (2007:975) with instructions for the Swedish Authority for Privacy Protection. (*Förordning (2007:975) med instruktion för Integritetsskyddsmyndigheten*).
1298. Rättsstatliga principer och beslutsprocesser i en (alltmer) digitaliserad och automatiserad förvaltning./ Enqvist, Lena and Naarttijärvi, Markus. Rättsstaten i den svenska förvaltningen: en forskningsantologi. Statskontoret 2022, p. 217–249. At p. 241 et sec.

In essence, effective monitoring should transcend the fixation on specific technology types. Given the imperative for diligent monitoring, the further need for knowledge and perspectives on technology utilisation through a rule of law lens becomes apparent. Therefore, a closer examination of other Nordic-Baltic experiences, as well as communication between relevant entities on legal challenges, regulatory design choices, as well as on choices and experiences of technical and organisational safeguards to address specified rule of law challenges, offers clear advantages. The different administrative traditions of the Nordic-Baltic countries are both based on, and have explanatory value for, the fact that there are large variations in how the public exercise of power is substantively as well as procedurally regulated. Extensive Nordic-Baltic legislative harmonisation would therefore be cumbersome to realise on a broad basis, not the least since such an endeavour would need to extend into detailed sectoral regulations. The strong common ground between the countries that do exist in terms of the shared commitment to rule of law values, nevertheless, creates opportunities for leveraging informal collaboration to improve resilience against the challenges posed by advancing technologies.[1299] Such knowledge and experience exchanges can and should take place at various levels. By broad as well as specific comparative analyses, national legislative drafters ought to consistently draw on upon the legislative as well as practical experience of the other Nordic-Baltic countries to inform their own drafting. Supervisory authorities should establish, maintain, or enhance collaboration with – or at least closely monitor – the practices of other Nordic-Baltic supervisory authorities. This could improve their capacity to identify technology implementations that may pose specific risks to rule of law values, to prioritise their supervision as well as to perform it diligently. Furthermore, sectoral authorities should establish, maintain, or enhance collaboration across borders to help develop cohesive strategies for addressing common challenges posed by public technology utilisation. As one last example, there is also a need for continuous input from legal scholarship to provide principled and holistic as well in-depth analysis and guidance, which can give or serve as a foundation for comparative insights. That the Nordic Council of Ministers can play an important role in facilitating such communication is exemplified by this book.

1299. See further on the more limited prospects for extensive legislative harmonisation in the field of administrative law in the Nordic region, The Vision and Legal Reality of Regional Integration in the Nordic States./ Wenander, Henrik. Free Movement of Persons in the Nordic States. EU Law, EEA Law, and Regional Cooperation. ed./ Katarina Hyltén-Cavallius and Jaan Paju. Hart 2023, p. 9–30.

About this publication

Public Digitalisation in a legal perspective

Status, challenges and opportunities for Nordic-Baltic cooperation

Hanne Marie Motzfeldt (Denmark)
Adam Hyldkrog Lindberg (Denmark)
Paloma Krõõt Tupay (Estonia)
Monika Mikiver (Estonia)
Sofia Heikkonen (Finland)
Ida Koivisto (Finland)
Riikka Koulu (Finland)
Anastasija Kaplane (Latvia)
Aleksandrs Potaičuks (Latvia)
Prof. Dr Eglė Bilevičiūtė (Lithuania)
Samson Y. Esayas (Norway)
Mathias K. Hauglid (Norway)
Lena Enqvist (Sweden)

TemaNord 2024:503

ISBN 978-92-893-7785-0 (PDF)
ISBN 978-92-893-7786-7 (ONLINE)
http://dx.doi.org/10.6027/temanord2024-503

Cover photo: Sigmund/Unsplash
Other photos: Getty Images/Unsplash, Yadid Levy/norden.org, Yadid Levy/norden.org, LinkedIn Sales Solutions/Unsplash, Maud Lervik / Norden.org, Ricky John Molloy / norden.org, standret/Unsplash, Mario Gogh/Unsplash, Israel Andrade/Unsplash

Published: 14/5 2024

Disclaimer

This publication was funded by the Nordic Council of Ministers. However, the content does not necessarily reflect the Nordic Council of Ministers' views, opinions, attitudes or recommendations.

Rights and permissions

Any queries regarding rights and licences should be addressed to:
Nordic Council of Ministers/Publication Unit
Ved Stranden 18
DK-1061 Copenhagen
Denmark
pub@norden.org

Nordic co-operation

Nordic co-operation is one of the world's most extensive forms of regional collaboration, involving Denmark, Finland, Iceland, Norway, Sweden, and the Faroe Islands, Greenland and Åland.

Nordic co-operation has firm traditions in politics, economics and culture and plays an important role in European and international forums. The Nordic community strives for a strong Nordic Region in a strong Europe.

Nordic co-operation promotes regional interests and values in a global world. The values shared by the Nordic countries help make the region one of the most innovative and competitive in the world.

The Nordic Council of Ministers
Nordens Hus
Ved Stranden 18
DK-1061 Copenhagen
pub@norden.org

Read more Nordic publications on www.norden.org/publications