2020

Developing a Digital Welfare State: Data Protection and the Use of Automated Decision-Making in the Public Sector across Six EU Countries

Choroszewicz, Marta

University of California Press

Tieteelliset aikakauslehtiartikkelit
© 2020 by the Regents of the University of California
All rights reserved
http://dx.doi.org/10.1525/gp.2020.12910

https://erepo.uef.fi/handle/123456789/8237
Downloaded from University of Eastern Finland's eRepository
Communication and Media

Developing a Digital Welfare State: Data Protection and the Use of Automated Decision-Making in the Public Sector across Six EU Countries

Marta Choroszewicz1, Beata Mäihäniemi1

1 Department of Social Sciences, University of Eastern Finland, 2 Faculty of Law, University of Helsinki

Keywords: the european general data protection regulation, automated decision-making, digital welfare state, data protection, legal framework

https://doi.org/10.1525/gp.2020.12910

Global Perspectives
Vol. 1, Issue 1, 2020

This article uses the sociolegal perspective to address current problems surrounding data protection and the experimental use of automated decision-making systems. This article outlines and discusses the hard laws regarding national adaptations of the European General Data Protection Regulation and other regulations as well as the use of automated decision-making in the public sector in six European countries (Denmark, Sweden, Germany, Finland, France, and the Netherlands). Despite its limitations, the General Data Protection Regulation has impacted the geopolitics of the global data market by empowering citizens and data protection authorities to voice their complaints and conduct investigations regarding data breaches. We draw on the Esping-Andersen welfare state typology to advance our understanding of the different approaches of states to citizens’ data protection and data use for automated decision-making between countries in the Nordic regime and the Conservative-Corporatist regime. Our study clearly indicates a need for additional legislation regarding the use of citizens’ data for automated decision-making and regulation of automated decision-making. Our results also indicate that legislation in Finland, Sweden, and Denmark draws upon the mutual trust between public administrations and citizens and thus offers only general guarantees regarding the use of citizens’ data. In contrast, Germany, France, and the Netherlands have enacted a combination of general and sectoral regulations to protect and restrict citizens’ rights. We also identify some problematic national policy responses to the General Data Protection Regulation that empower governments and related institutions to make citizens accountable to states’ stricter obligations and tougher sanctions. The article contributes to the discussion on the current phase of the developing digital welfare state in Europe and the role of new technologies (i.e., automated decision-making) in this phase. We argue that states and public institutions should play a central role in strengthening the social norms associated with data privacy and protection as well as citizens’ right to social security.

INTRODUCTION

The legal protection of citizens and legal framework for data protection are central to the development and use of automated decision-making (ADM) systems. Such protections include safeguarding citizens’ basic rights and access to welfare benefits. Issues of justice and equality go far beyond technological solutions to potential bias and discrimination and concern international and national legislation related to data protection and ADM use. Despite its limitations, the General Data Protection Regulation (GDPR) can be considered the global standard for regulation of data protection and ADM because it has empowered data protection authorities and citizens in the European Union to voice their complaints and conduct investigations regarding breaches of data protection law. It has also provided opportunities to promote awareness and public discussion about data privacy, identity, and discriminatory treatment and processing of personal data.

"ADM" is a term that describes a broad range of systems controlled by algorithms, which are currently being developed and implemented to either assist or replace human decision makers in public administration and the private sector (AlgorithmWatch 2019, 9). Artificial intelligence (AI) is increasingly being used to make decisions that severely affect people’s lives in terms of, for example, education, recruitment, welfare entitlements, lending, and criminal risk assessment (AlgorithmWatch 2019). In general, these systems assist people in making decisions, and they appear disarmingly simple, efficient, and harmless. However, this is not the case for all people impacted by these systems (Eu-banks 2017; O’Neil 2016).

Public-sector institutions and private-sector organizations are investing increasing resources to achieve the anticipated benefits of data collection and data analytics for delivery of public services. Benefits include seemingly lower costs, better efficiency in service production, prediction and anticipation of service demand, development of targeted
interventions, and personalized diagnoses and identification of high-risk groups (McKinsey Global Institute 2017; Murdoch and Detsky 2015). Public institutions in Europe are also experimenting with the use of ADM across welfare domains for reasons of efficiency and cost-effectiveness, albeit often without appropriate safeguards for verification of automated decisions (AlgorithmWatch 2019; Koulou et al. 2019).

Scholars have noticed that, in the United States, citizens may be subject to computational classifications, privacy invasions, or other types of surveillance that are applied unequally to the general population and could be in violation of existing regulatory protections (Barocas and Selbst 2016; Fourcade and Healy 2015). In her book Weapons of Math Destruction, O’Neil (2016) notes that the currently popular algorithms are used in areas dominated by disadvantaged members of society, such as in low-paying jobs. These algorithms appear to be cheap and efficient, but they were not necessarily tested for fairness and justice. In a study of the automation of US public services, which used predictive risk models of child protective services and welfare eligibility systems, Eubanks (2017) noticed that when ADM is used to assist humans in decision-making, people tend to agree with the system rather than challenge its decisions. If people do not feel comfortable in challenging ADM, these systems can produce identical biases at a larger scale than those produced by human decisions.

In this article, we examine the legal regulations related to data protection and ADM in six European countries that have adopted two contrasting welfare state regimes (Esping-Andersen 1990): the social democratic/Nordic regime (Denmark, Sweden, and Finland) and the Conservative-Corporatist regime (Germany, the Netherlands, and France). Through this study, we enhance the understanding of the current phase of the digital welfare state in Europe and how ADM influences citizens’ participation in society. We also discuss the lack of effective regulatory frameworks for ADM development and use and the impact of this situation on the realization of citizens’ rights.

**SURVEILLANCE CAPITALISM AND DATAFICATION PERFORMED BY DIFFERENT WELFARE STATES**

Zuboff (2015, 75) perceives big data as a foundational component of “surveillance capitalism,” which is characterized by invasive and often illegal data collection, extraction, and prediction practices done in service of economic logic. These practices separate people from their own behavior by turning private human experiences into products. She argues that this is an attack on human agency, as many private companies design their data collection and use practices so that they remain hidden and people remain unaware. Surveillance capitalism, which facilitates numerous predictive and data-driven systems, challenges democratic norms by, for example, usurping people’s decision-making for others’ gain (Zuboff 2019). These systems also unevenly burden the poor (Eubanks 2017; O’Neil 2016; Taylor 2017).

Historically, not only private companies but also public administration institutions have collected large amounts of citizen data. For instance, European countries have diverse traditions regarding national registries that collect structured data on their citizens. This issue is especially pronounced in the Nordic context, where a register-based mechanism of producing statistics has existed since the 1970s (Alastalo 2009). These national registries and the use of a personal identity number that is assigned to all citizens at birth or at the time of immigration enable different public and private authorities to collect a range of citizen data (Thygesen and Erbsbøll 2011). Drawing on the GDPR and national regulations on data protection, public and private authorities are currently exploring the possibilities for combining citizen data from different sources.

The datafication conducted by welfare states has predominantly led to the collection of provided, derived, and inferred data (Wachter and Mittelstadt 2019, 316). Provided data is directly provided by citizens to a data controller. Derived and inferred data are created by data controllers or any other third party using data provided by citizens and other background data (Wachter and Mittelstadt 2019). An example of derived data is deriving a citizen’s country of residency from their postcode, whereas an example of inferred data is an outcome of a health assessment (Wachter and Mittelstadt 2019).

While data collection has been always central to the role of public administration, currently, there is a push from within public administrations to facilitate the sharing and combining of datasets between different authorities as well as to make greater use of data. When public administrations experience economic pressures, ADM may serve as a solution to increasing public costs—specifically, savings attributable to the assumed potential benefits of ADM for identifying and ranking welfare beneficiaries and possible fraudsters more quickly and cheaply (Gantchev 2019). Yet the development and use of ADM is dependent on the availability of large amounts of good-quality data. Thus, public institutions are pressured to reuse primary data for purposes other than those for which they were initially created or to create new data based on primary data (Kitchin 2014). Specifically, secondary data use is focused on and treated as the “new oil” because it enables various forms of value creation (Tempini 2017). Additionally, the benefits of derived and inferred data are increasingly recognized (Wachter and Mittelstadt 2019). Yet, as Gitelman (2013, 7) aptly reminds us, “raw data” is an oxymoron: “Data are not facts, they are ‘that which is given prior to argument’ given in order to provide a rhetorical basis. Data can be good or bad, better or worse, incomplete and insufficient.” Pasquale (2018) points out that people lose control not only over how and where they are being represented but also over the use of their data. He argues that there is always a threat that even accurate data can be discriminatorily employed (Pasquale 2018).

Public administrations have a responsibility to ensure citizens’ fundamental rights along with a strong imperative to protect citizens’ data. However, research shows that states differ in the levels of protection they offer (Gantchev 2019). Our analyses indicate that countries adapt the GDPR with varying degrees of leeway. In addition, governments may “nudge” citizens to assist public administration institutions with data collection, combination, and reuse. Nudging is a relatively new intervention tool used by governments to affect citizens and corporate behavior (Mosely and Stoker 2013). It is based on rearrangement of a choice architecture that guides people to make better choices according to their own interests or the interests of public administration. Sunstein (2014, 584) argues that resorting to nudging could be regarded as a form of “soft paternalism” that is used in the absence of more specific regulations, and its purpose is to intentionally affect citizens’ behavior. He also notes that the use of nudges has increased in both the public and the private sectors because they are a fairly cheap and efficient way to promote economic and public goals (Sunstein 2014, 583). As Wachter and Mittelstadt (2019, 306) argue, nudging can be done through inferences that identify “small but meaningful links between individu-
uals and constructing group profiles from personal, third-party, and anonymized data.” If the use of inferences in nudging is counterintuitive, unpredictable, and done without individuals’ awareness, it could threaten individuals’ privacy, identity, data protection, reputation, and informational self-determination (Wachter and Mittelstadt 2019).

In our analysis, we focus on six countries that represent different welfare state regimes and legal traditions in the European context. We use Esping-Andersen’s (1990) welfare state typology, focusing on countries belonging to the Nordic regime (Denmark, Sweden, and Finland) or the conservative-corporatist regime (Germany, the Netherlands, and France). The Nordic regime is characterized by a universalist welfare paradigm that promotes individual autonomy and equal access to justice for all citizens. The state has adopted a central role in the provision and regulation of citizens’ social security and the regulation of markets (Esping-Andersen 1990). The state has also collectivized the responsibility for its citizens’ social security; citizens bond through a shared sense of responsibility to participate in actions that increase their own and others’ well-being (Rose and Miller 1992). Indeed, the legal systems of the Nordic countries have developed to provide considerable protections to citizens and an inclusive view of social justice (Husa, Nuotio, and Pihlajamäki 2007, 1–39).

The conservative-corporatist regime is often characterized by differential provisions and protections based on the stratification of society that maintain and reinforce class differences (Esping-Andersen 1990). The legal systems of conservative-corporatist countries have developed highly stratified societies and thus rely on extensive codification, theorization, and scientification. This is especially true in Germany, which is a Germanistic civil law country (De Geest 2012; Husa, Nuotio, and Pihlajamäki 2007). France and the Netherlands are Napoleonistic civil law countries. The French legal system is a very formalistic and top-down system, while the Dutch system is based on a mixture of the French and German systems (De Geest 2012). The legal systems of these countries rest on state authority to provide legal protection to the state’s citizens through enforcement of order and conformity to regulations.

In our analyses, we aim to examine whether the welfare state typology could enhance our understanding of states’ different approaches to data protection and the use of new technologies. We can expect that countries belonging to these two different welfare state regimes would exhibit important differences in terms of how they set and enforce rules concerning data collection and protection as well as secondary data use, such as for ADM.

EUROPEAN GENERAL DATA PROTECTION REGULATION

The GDPR regulates the process of data collection and ADM in the European Union (EU) by requiring data processors (i.e., public or private organizations or persons) to become more transparent about, among other things, the sources of data and the purposes for which they are being collected. The GDPR also provides data subjects with rights to protect their privacy during data collection and processing, such as the right of access (Article 15: “the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information”) or right to erasure (Article 17: “the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay”) under specific grounds.

Under Article 22 (1) of the GDPR, data subjects have the right to not be subjected to a decision based solely on automated processing, such as profiling, that has legal effects or other significant effects. However, the regulation focuses only on full ADM and not situations in which AI assists a human in decision-making. However, paragraph 2 provides exceptions whereby automatic decision-making is possible, such as with the express consent of the data subject (lit. c) or through a decision adopted by the law of an EU member state that lays down appropriate measures to protect the data subject’s rights and freedoms. According to Article 22 (2) lit. c, ADM decisions can be made with the explicit consent of those registered. However, in the case of vulnerable groups, data subjects may be unable to assess the content and effects of their consent, and therefore the consent exception may not be appropriate in all situations (Koulu et al. 2019, 89).

It seems that the GDPR provides a quite valid control mechanism for data subjects that is subject to certain exceptions; however, Wachter and Mittelstadt (2019, 499) point out that data subjects have only limited control over how the exceptions are evaluated. This lack of significant control occurs despite the existence of the purpose limitation principle and data minimization principle, which can be found in Article 5 (1) lit. b and c, respectively. The purpose limitation principle demands legitimate, explicit, and specified purposes for data processing, and the data minimization principle limits the conditions under which data may be collected, stating that data need to be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” (Wachter and Mittelstadt 2019, 499).

While ADM cannot be made without a sufficient amount of data, secondary use of data is not adequately regulated, and although data subjects can control how data that was gathered for the original purpose is collected to a certain extent, they may not be aware that it will later be used for secondary purposes. Secondary use of data is possible because of exceptions made, for example, for scientific and archival purposes in the public interest.

The GDPR is a general regulation that contains a number of open clauses and exemptions, providing leeway for national legislation based on Article 6 (2). Thus, member states can introduce more specific provisions to adapt their application of the GDPR’s rules. The GDPR does not specify requirements for national provisions (Wagner and Benecke 2016), but it does specify that the open clauses and exemptions are to be used to adapt applications of the GDPR with regard to processing for compliance with the legal obligations to which the data controller is subject (Article 6 [1] lit. c) or when the processing of personal data is necessary to perform a task carried out in the public interest or to exercise the data controller’s official authority (Article 6 [1] lit. e). These opening clauses provide member states and their public administrations with more opportunities to process personal data and limit data subjects’ rights (McCullagh, Tambou, and Bourton 2019, 62).

METHODOLOGY

While there is a lack of systematic information about the legal framework and ADM use, we drew upon prominent recent reports (Koulu et al. 2019; AlgorithmWatch 2019) and our own searches for relevant legal documents, regulations, and use of ADM of databases including Edilex, HeinOnline,
Table 1: Regulatory measures and ADM examples in the studied countries.

<table>
<thead>
<tr>
<th>Country</th>
<th>Regulatory Measures</th>
<th>ADM Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finland</td>
<td>• Secondary Law&lt;br&gt;• Information Management Law&lt;br&gt;• Data Protection Law&lt;br&gt;• Government proposal to the Parliament on personal data processing law in the Immigration Administration and certain related laws</td>
<td>• Automated tax decisions&lt;br&gt;• Credit score decisions&lt;br&gt;• Espoo child welfare experiment&lt;br&gt;• Kela’s (planned) automation</td>
</tr>
<tr>
<td>Denmark</td>
<td>• The concept of “samkøring og samstilling”&lt;br&gt;• Data Protection Act</td>
<td>• The Gladsaxe Model&lt;br&gt;• Decisions on student stipends&lt;br&gt;• Taxing&lt;br&gt;• Child welfare&lt;br&gt;• Udbetaelling Danmark—automated payments and control of social funds</td>
</tr>
<tr>
<td>Sweden</td>
<td>• 28 § of the Administrative Act&lt;br&gt;• Data Protection Act</td>
<td>• Traffic tax&lt;br&gt;• Trelleborg model—decision-making on social benefits</td>
</tr>
<tr>
<td>Germany</td>
<td>• 35a § of the Administrative Procedure Act&lt;br&gt;• Federal Data Protection Act&lt;br&gt;• Other sectoral laws: Abgabenordnung—automation of tax decisions in the tax code, national social security legislation acts—Sozialgesetzbuch X (SGB X)</td>
<td>• Inferring insights from large datasets in the health sector&lt;br&gt;• Tax administration&lt;br&gt;• Pension assessment&lt;br&gt;• Developing traffic safety</td>
</tr>
<tr>
<td>France</td>
<td>• The Computers and Freedom Law (1978, mod. 2017)&lt;br&gt;• Digital Republic Law and the Administrative Law&lt;br&gt;• Personal Data Protection Act&lt;br&gt;• Code of Education</td>
<td>• Personalized health files (Dossier Médical)&lt;br&gt;• Selection of university students (Parcoursup)</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>• Digital Government Act&lt;br&gt;• Court verdicts&lt;br&gt;• GDPR Implementation Act (2018)&lt;br&gt;• Articles 64 and 65 of the Dutch Work and Income Act</td>
<td>• System for Risk Indication (System Risico Indicatie/SyRI)&lt;br&gt;• Preventing and detecting school absence and early leaving&lt;br&gt;• Detecting child abuse and/or domestic violence</td>
</tr>
</tbody>
</table>

Westlaw, Helka, and Google Scholar.

In our analyses, we focused on hard laws that cover the legal instruments that bind states, their institutions, and private persons. In contrast to soft laws, hard laws stipulate binding responsibilities and rights that can be enforced in court. Analysis of hard laws offers valuable insights into the current regulatory landscape, including its shortcomings and benefits. In our study, we focused on cases of national adaptations of GDPR and use of ADM by public administrations. We limited the scope of the analysis to cases that focus on provided, derived, and inferred data (see Wachter and Mittelstadt 2019, 516).

Our analytic process focused on (1) mapping existing regulatory measures linked to restrictions or additional guarantees related to citizens as data subjects and (2) publicly available and internationally discussed examples of ADM in each chosen country (see table 1). This process involved six country-specific analyses followed by a comparative approach in which we iterated our analyses based on the Esping-Andersen welfare state typology, legal research, and empirical material available on each country. Our analyses were guided by the following research question: how can we better understand states’ different approaches to citizen data protection and ADM use in Europe?

First, we present country-specific case studies of legal frameworks and initiatives related to data protection across the studied countries. Second, we describe some prominent examples of ADM from these countries. Third, we discuss problematic issues related to some policy responses and our observations regarding the trend toward digital welfare states.

COUNTRY-SPECIFIC NATIONAL LEGISLATION CASE STUDIES

FINLAND

There is no law in Finland that directly regulates ADM. Thus, the legal status of administrative ADM is unstructured, and there are numerous legal problems connected to the use of robotic automation and AI-based systems (Koulu et al. 2019, 66).

As in other member states, a national GDPR adaptation
has existed in Finland since the beginning of 2019. The Data Protection Act (Tietosuojalaki) addresses exceptions or exemptions to personal data processing conditions (Oikeusministeriö 2018). These exceptions mean, inter alia, that data subjects are not, for example, entitled to access information concerning themselves. The purpose of these derogations is to preserve existing regulations. Deviations from data subjects’ rights include the requirement for data controllers to process a data protection impact assessment or commit to a specific code of conduct. Data on health, sexual behavior and orientation, religion, and political views continues to be available for research and statistical purposes (Oikeusministeriö 2018). There are also restrictions that limit the processing of personal identification numbers to specific conditions, such as the need to perform a lawful task (§ 29). Furthermore, there are exceptions and safeguards for personal data processing for scientific and historical research and statistical purposes (§ 31) as well as exceptions and safeguards for personal data processing for archiving purposes that are in the public interest (§ 32).

One of the most pressing concerns is the limitation on the controller’s obligation to provide information to data subjects (§ 33). In particular, data subjects’ rights to access the data collected from them may be restricted when disclosure of this information could affect national security, defense, or a public order or when the data were collected to prevent or detect crime; when provision of this information could seriously endanger the health or care of the data subject or the rights of the data subject or another person; or when personal data are used for supervisory and control purposes and nondisclosure is necessary to safeguard important economic or financial interests of Finland or the EU (§ 34).

Additional legal changes have been imposed to address ADM in sensitive areas. First, the so-called Secondary Law (Laki sosiaali- ja terveystietojen toissijaisesta käytöstä) was introduced to enable efficient and secure processing of personal data stored for social and health care activities. Secondary use of social and health information means that customer and registry information generated by social and health care activities can be used for purposes other than those for which it was originally stored, including scientific research, statistics, development and innovation, authority control and supervision, planning and reporting by public authorities, teaching, knowledge management, and collection of national monitoring data (Sosiaali- ja terveysministeriö 2019).

In addition, the Information Management Law (Laki julkisen hallinnon tiedonhallinnasta), which is more general, was introduced to ensure consistent management of authorities’ data files and secure data processing. This law is supposed to improve the information management of the authorities so that they can provide services in accordance with good governance and carry out their tasks effectively. It also seeks to promote the interoperability of information systems and data resources (Eduskunta 2019). According to § 1, the purpose of the law is to (1) ensure consistent and high-quality management of public records and secure data processing in order to comply with the publicity principle (i.e., the citizens’ right to information about the activities of public authorities); (2) enable the safe and efficient utilization of governmental information materials so that public authorities can carry out tasks and provide services to clients of the administration in an efficient and high-quality manner; and (3) promote the interoperability of information systems and data resources.

Finally, the newest government proposal to Parliament, which concerns the personal data processing law of the Immigration Administration and certain related laws (HE 18/2019 vp), aims to regulate personal data processing by the Immigration Administration by centralizing the personal data processing regulations of other immigration legislations. Importantly, the proposal includes technical changes to personal data processing laws enacted by the Criminal Sanctions Authority, the Identity Card Act, the Law on the Use of Air Passenger Name Record Data to Combat Terrorist Offenses and Serious Crime, and the Law on Amending the Law (HE 18/2019 vp).

DENMARK

In Denmark, some legal mechanisms to protect citizens from the development of ADM have been introduced, but they seem to be largely unsuccessful. The administrative law by design includes a provision for the development of technology. It is based on the prerequisite that the design and develop ADM systems in accordance with governmental values (see Motzfeld 2017).

With respect to legal ADM regulations, the Danish national GDPR adaptation, the Data Protection Act (Databeskyttelsesloven), contains a significant number of provisions that either modify or provide exemptions from the GDPR (McCullagh, Tambou, and Bourton 2019, 62). One of these modifications extends public authorities’ right to process personal data. This is a derogation of Article 5 (1) lit. b of the GDPR, which states that personal data shall be collected only for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. However, changing the purpose of data processing after data collection is lawful under certain conditions set out in Article 6 (4) of the GDPR. For example, the purpose can change based on laws of member states that stipulate necessary and proportionate measures to safeguard the objectives laid out in Article 25 of the GDPR in a democratic society (McCullagh, Tambou, and Bourton 2019, 62). Moreover, the right to process personal data is extended based on the Danish Data Protection Act, § 5 (3), which enables practically any minister to issue executive orders that could specify when secondary personal data use occurs. This should be done in cooperation with the minister of justice (McCullagh, Tambou, and Bourton 2019, 62).

Data subjects’ rights can also be restricted based on Article 23 of the GDPR, which states that member states are allowed to restrict the scope of data subjects’ rights and corresponding obligations when such restrictions respect the essence of citizens’ fundamental rights and freedoms and are a necessary and proportionate measure in a democratic society to safeguard certain objectives enumerated in the provision. Based on this provision, member states can introduce legislation that limits data subjects’ rights to a rather large extent, particularly to safeguard the “other important objectives of general public interest” objective (McCullagh, Tambou, and Bourton 2019, 62).

In the Danish Data Protection Act, this provision was used to restrict Danish citizens’ rights to information on the processing and sharing of their data for purposes other than the original purpose for which the data were collected (McCullagh, Tambou, and Bourton 2019, 63).

In Denmark, the concept of samkøring og samstilling was developed to refer to the process of combining and sharing data in individual cases (Raugland 2018). In such situations, large amounts of data are shared within public administrations from one registry to another (Raugland 2018). A good example of a samkøring og samstilling situation is that of students’ financial aid application (i.e., study grants), which
is based on a specific law (SU-loven) related to this issue (see Koulu et al. 2019, 43). An applicant completes the application through an online system, and an ADM decision is made regarding the applicants’ right to study. If the right to study is granted, tax information must be obtained from the tax office. Information required for a successful application is obtained partly automatically from a number of public registers and partly from study-unit documents (Raugeland 2018). This concept is especially powerful because in the Danish public sector, especially municipalities, large amounts of information about citizens are stored, and only a small amount of data is erased. This enables the creation of detailed citizen profiles without citizens being aware of it (Næsborg-Andersen and Motzfeldt 2019).

SWEDEN

In Sweden, ADM for public administration purposes was introduced to the Administrative Law in July 2018 (2017:900). According to § 28 of the law, a decision can be made automatically, by a single public officer or by a group of officers (Koulu et al. 2019, 44). Thus, this law distinguishes between ADM and automated decision support, even though the line between these concepts is considered to be quite fine (AlgorithmWatch 2019, 129). No requirements regarding how ADM should be performed in public administrations have been set. In addition, these new legislative changes to the Administrative Act do not cover the municipalities for which a legal framework that enables and regulates the use of ADM is currently missing (AlgorithmWatch 2019, 129).

The Swedish Data Protection Act (Lag med kompletterande bestämmelser till EU:s dataskyddsförordningen) offers a number of additional ADM restrictions. Chapter 3 addresses the processing of certain personal data categories and encompasses provisions for when sensitive personal data may be processed according to the GDPR (Article 9 [1]): in the fields of employment, social security, and social protection when there is an important public interest; in the fields of health services, medical care, and social care; and in the fields of archives and statistics. According to § 4 of the act, the government may issue further regulations regarding the processing of sensitive personal data when deemed necessary to serve an important public interest. The chapter also contains provisions for personal data relating to criminal offenses and identification numbers (McCullagh, Tambou, and Bourton 2019, 43). Chapter 4 stipulates limitations of data use for archives and statistics (McCullagh, Tambou, and Bourton 2019). However, of particular relevance to this study is chapter 5, which sets limitations for certain rights and obligations, including the freedom of opinion and right to information (McCullagh, Tambou, and Bourton 2019, 43–44). For example, § 1 of the act limits data subjects’ right to access their personal data based on Articles 13–15 of the GDPR, according to which such disclosure is not allowed by law, statutes, or decisions based on the constitution.

GERMANY

In Germany, § 35a of the Administrative Procedure Act (Verwaltungsverfahrensgesetz) enables ADM decisions by defining the preconditions for automating particular kinds of decisions. According to this act, ADM use requires a new law in each individual case, and decisions should not involve any potential considerations or the need to evaluate the use (Koulu et al. 2019, 48).

The national GDPR adaptation, the Federal Data Protection Act (Bundesdatenschutzgesetz, or BDSG) restricts the rights of data subjects, including the right to information (§ 52 and 53), the right to access (§ 54), the right to erasure (§ 35), the right to object (§ 56), and automated individual decision-making (§ 37). Furthermore, it limits the rights of data subjects in situations with secrecy obligations (BDGS, § 29). For example, the right to erasure is not applicable to cases of nonautomated data processing, in which erasure would be impossible or would involve a disproportionate effort due to the mode of storage, or to cases in which the data subjects’ interest in erasure can be regarded as minimal (BDSG, § 55; McCullagh, Tambou, and Bourton 2019, 32).

Additionally, special personal data categories can be processed by both public and private bodies when they relate to social security, medicine, and public health (BDGS, § 22 [1][1]). However, § 22 (2) of the BDSG states that "appropriate and specific measures shall be taken to safeguard the interests of the data subject" and lists a number of such measures (McCullagh, Tambou, and Bourton 2019, 32–33). Koulu et al. (2019, 48) point out that a number of sectoral regulations enable ADM use in Germany. Primarily, the automation of tax decisions in the tax code (Abgabenordnung, § 155) enables automation of, for example, tax proposals, tax credits, tax deductions, and prepayments.

German legislation includes a separate data protection regime for welfare agreements, and it is based on national social security legislative acts (Sozialgesetzbuch X SGB, § 67–85) (Gantchev 2019, 14). Importantly, these acts take precedence over the general data protection regime of the above-mentioned Federal Data Protection Act (Gantchev 2019, 13). In particular, two rules, SGB II § 52 and SGB XII § 118, concern specific details about the welfare agreements as well as the purpose limitation principle from the GDPR (Article 5 [1] lit. b). This limits the possibility of processing personal data to what is indispensable for ensuring compliance under a particular social security system. Such a legal rule limits the control of the public administration and increases the rights to transparency of welfare beneficiaries (Gantchev 2019, 14).

Federal government data protection agencies and eight German federal states have called for increased ADM transparency as an important tool for the protection of human rights (Informationsfreiheitsbeauftragten nachfolgendes Positionspapier 2018). According to these institutions, processes should be intelligible, audited, and controlled, with decisions explaining, on demand, the underlying logic and that very sensitive ADM systems should undergo a risk assessment prior to their implementation and authorization (AlgorithmWatch 2019, 80). Further, they argue that citizens should be guaranteed ways to redress or reverse decisions and that very sensitive ADM systems should undergo a risk assessment prior to their implementation and authorization (AlgorithmWatch 2019, 80).

FRANCE

In France, the 2016 Digital Republic Law (Loi pour une République numérique) changed the Administrative Law (Code des relations entre le public et l’administration). A paragraph was added to the Administrative Law (L.311-5-1) that imposes algorithmic transparency. It obliges the public administration to inform citizens when decision-making involves the use of an algorithm; the logic and behavior of the algorithm are required to be available upon request (AlgorithmWatch 2019, 68–69). The application of this paragraph is regulated in a separate decree (Décret relatif aux droits des personnes faisant l’objet de décisions individuelles pris sur le fondement d’un traitement algorithmique), which
provides individuals with the right to, on demand, be informed about the logic underlying a decision-making algorithm and the main reasons for an automated decision. Furthermore, the decree also sets a procedure for how an individual can exercise the right to access information (Koulu et al. 2019, 49). This denotes an individual's right to obtain information on the background and reasons for a decision more broadly than provided by the GDPR (see Edwards and Veale 2017, 53). The individual can be informed about, for example, the extent and form of algorithmic decision-making that was used to make a decision; what information was used in the decision-making process and where it was derived from; the parameters of algorithmic processing and, if possible, their role in decision-making; and how the information was processed. This law is applied to both full ADM and decisions for which AI or robotics were used as supporting tools (Koulu et al. 2019, 50).

The French Supreme Court for Administrative Matters expressed its opinion about fully automated decisions (Berne 2018) in June 2018, pointing out that such decisions can be made only when the algorithm and its logic can be explained to the affected person. Although the law makes it mandatory for all branches of government to make their algorithms transparent, not all branches have complied (AlgorithmWatch 2019, 66).

The importance of human responsibility for ADM has been stressed in France. In particular, there have been calls to set ethical boundaries for the proactive algorithms used in law enforcement (AI for Humanity 2018). Therefore, while processing the data used to perform predictive analysis, the legal rights of citizens, such as the right to efficient legal protection or to explanation, should be ensured. This right is connected to the prohibition of profiling in Article 22 of the GDPR (Koulu et al. 2019, 50–51).

The French Personal Data Protection Act (Loi relative à la protection des données personnelles) was modified in 2018 to comply with the GDPR. After the modifications, it has been criticized for its complexity and opportunities for competing interpretations. The French Personal Data Protection Act “tries to compensate for the limitations of data subjects by introducing safeguards” (McCullagh, Tambou, and Bourton 2019, 60). For instance, it offers two guarantees for data subjects regarding individual decisions based solely on automated processing: (1) generalization of the right to obtain human intervention and (2) the introduction of a real right to explanation (McCullagh, Tambou, and Bourton 2019, 65–66). The use of open source aims to benefit the public administration and improve their efficiency (McCullagh, Tambou, and Bourton 2019, 60).

Finally, the Computers and Freedom Law of 1978 (Loi relative à l’informatique, aux fichiers et aux libertés) was modified in 2017 to make compatible with the GDPR. It now provides strict limitations on the use of ADM by both public and private authorities when their decisions on human behavior imply any kind of profile or personality of the person (AlgorithmWatch 2019, 69).

THE NETHERLANDS

In the Netherlands, while ADM is not regulated by the Dutch General Administrative Law Act 1994 (Algemene wet bestuursrecht), two important decisions paved the way for ADM use in the public sector (Koulu et al. 2019, 55). The first is a 2017 verdict of the State Council, one of the administrative courts in the Netherlands, that concerns ADM in terms of environmental permitting (Raad van State 2017). The verdict points out that partial ADM may not be transparent and verifiable because of a lack of access to the inner workings of the algorithm and the data. Therefore, interested parties are put in an unequal position because they cannot check, for example, the grounds on which a particular decision is made and thus cannot employ legal remedies for such decisions (Raad van State 2017). To minimize this inequality, the verdict requires public agencies to justify the reasons for decisions so that the employed data becomes more verifiable and transparent and the assumptions used for ADM are explained. This guarantees citizens legal protection against such decisions because a judge could determine the legality of a decision based on the provided information (Raad van State 2017). In addition, on August 17, 2018, there was another court verdict issued by the Dutch Supreme Court that followed the verdict of the State Council in the assessment of automated calculation models of property value that were used to evaluate property tax (Hoge Raad 2018).

In addition to these verdicts, the Netherlands introduced the GDPR Implementation Act, which is policy-neutral as the changes introduced to the law were rather minor (McCullagh, Tambou, and Bourton 2019). Nevertheless, it includes some exceptions available by the GDPR to provide legal basis for “the continuation of practices that already existed under the Dutch Data Protection Act” (McCullagh, Tambou, and Bourton 2019, 69–70). For example, it allows data processing for health issues in social security-related matters. Moreover, special categories of personal data can still be processed when doing so would serve a public interest. For example, under specific circumstances, these special categories of personal data can be used for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes.

Certain legal proposals are currently being developed, such as the Digital Government Act (Digital overheid) (Overheid 2019; Tweede Kamer 2018), which was submitted to the Parliament in June 2018. The act sets out the regulatory framework under the Digital Government Agenda, providing rules regarding, among other things, the power to impose certain (technical) standards on the government’s electronic communication, data, and information security; responsibility for the management of facilities and services within a generic digital government infrastructure; and the digital access of citizens and businesses to public services (AlgorithmWatch 2019, 99). The act was passed by the House of Representatives in February 2020 (Digital overheid 2020).

REVIEW OF ADM USE IN PUBLIC ADMINISTRATION

In all six countries, public institutions have been experimenting with ADM use to provide citizens with faster decisions about welfare benefits and more efficient public services (from the institutions’ perspective). Below, we provide an overview of some particularly controversial and internationally discussed examples of ADM in the contexts of social benefits, health care, child welfare, and taxation.

Some types of ADM usage did not attract much attention among citizens, such as the wide use of chatbots for customer service and customer data analytics in Finland. The Finnish Immigration Service has a special chatbot, Kamu, that serves as a virtual assistant and answers recurring questions about, for example, application processing time (EOAK/3579/2018). In Denmark, decisions about student stipends for higher education are decided upon after processing requests that are made only after all the necessary information is obtained from the tax office and other registers (AlgorithmWatch 2019, 49). However, some other uses, which touch upon the distribution of welfare benefits, iden-
tification of citizens in vulnerable circumstances, or detection of fraud, have attracted more critiques from citizens. While all ADM usages can significantly impact citizens’ legal security, these impacts are rarely considered in the design and deployment phases of ADM (Koulu et al. 2019, 90).

For example, in Finland, the Espoo experiment, which was conducted in the context of child welfare services, aimed to use data analytics to identify risk factors for becoming a user of child welfare services (Espoo city 2018). The information released by the parties involved in the experiment informed the public that datasets were merged from different public registers and included social, health, and early education information from over half a million people and 37 million customer contacts (Espoo city 2018). While the system was acquired from a private company, the child welfare service was in charge of the data used in the experiment. As the experiment was conducted when the Secondary Law did not exist, many ethical questions related to data privacy and secondary data use were raised. The outcome of the experiment was communicated to the public as a success because 280 risk factors were identified, but no additional information on the process and implications of the experiment for future use were revealed, leaving citizens without much information or opportunities for reaction.

In Denmark, three local authorities collaborated on the development of the Gladsaxe model, which was intended to trace children in vulnerable social circumstances before they exhibit symptoms of special needs (AlgorithmWatch 2019, 50–51). While the Danish government planned to apply the model to the whole country, it was not introduced because of public resistance (AlgorithmWatch 2019, 51). Similar to the Espoo experiment in Finland, the Gladsaxe model used data from a combination of different sources to identify risk indicators. The points-based model was developed with parameters such as mental illness, unemployment, missing a doctor’s or dentist’s appointment, and divorce. Three municipalities were involved in the experiment, and, for the purpose of the experiment, they requested exemption from the regulations around data protection (AlgorithmWatch 2019). However, the experiment was criticized because individual assessments were arranged and stored without parents’ knowledge and did not comply with existing laws (Kjær 2018). The experiment, much like in the Finnish case, focused on merging data and was not originally designed for automated flagging; thus, it only created records that could be used later in automated risk assessment (AlgorithmWatch 2019, 51). The reasons for profiling citizens in a sensitive area such as parenting capacity and ability are unclear, especially considering that individuals were not informed about this potential profiling. These types of ADM applications could lead citizens to be unwilling to share any information with the government in the future (Næsberg-Andersen and Motzfeldt 2019).

In Sweden’s Trelleborg model, aspects of decision-making regarding social benefits were automated. While the model is used in several municipalities around the country, its legal status is questionable and publicly debated because of the lack of a legislative framework addressing the use of ADM at the municipal level (AlgorithmWatch 2019, 129). In this model, new applications for social benefits were automatically checked and cross-checked with related databases, such as the tax agency or the housing support unit (AlgorithmWatch 2019, 130). The automation led to reductions in the number of staff and the number of recipients of social benefits. Additionally, the use of the model is questionable since the applicants were not explicitly informed about the automated nature of the decision (AlgorithmWatch 2019, 130).

In the Netherlands, the Dutch government has used ADM to detect welfare fraud (System Risk Indication, or SyRI). SyRI is based on Articles 64 and 65 of the Dutch Work and Income Act (Public Interest Litigation Project 2015). The dataset included information about individuals’ date of birth, family composition, history of benefits received, and additional information obtained from the Tax and Customs Administration, the Land Registry, or the Netherlands Vehicle Authority (AlgorithmWatch 2019, 101). The system identified certain risk indicators that indicate probability of whether a citizen is committing benefit fraud. If such a situation is identified, an alarm is set off, and the case is handled by an employee from the Ministry of Social Affairs and Employment, who may create a risk report to be forwarded to the relevant authorities. If the suspicion is confirmed, state aid can be reclaimed (Braun 2018). This tool can also be used upon request by state institutions, such as the Dutch tax office or the immigration authority, as well as by some municipalities to detect welfare fraud, which occurs when social benefits are wrongly collected or social security institutions or other income-related state benefits are abused (AlgorithmWatch 2019, 101). The tool is highly problematic because it violates the purpose limitation principle by failing to inform individuals of the purpose of data collection. Moreover, citizens are not informed that they are classified as “high-risk,” even though these decisions personally affect them (Braun 2018). As pointed out by Gantchev (2019, 17), the purpose limitation principle can be found in Article 64 (1) of the Work and Income Implementation Structure Act (Overheid 2019). However, it is extensive and cannot be limited to one social security scheme (Gantchev 2019, 17). The narrow scope of the tool is also problematic because, as a result of using it publicly, authorities can take serious measures against citizens, such as imposing fines, canceling benefits, or, in the worst case scenario, opening criminal proceedings. Additionally, citizens are unable to assess the reasons for the report and correct them if needed, which makes it difficult for them to fulfill the burden of proof (Nederlands Juristen Comité voor de Mensenrechten 2018). In March 2018, the Dutch state was sued for using SyRI by a broad coalition of legal professionals and human rights organizations (Gantchev 2019, 18). In February 2020, it was deemed illegal as it violated Article 8 (2) of the European Convention of Human Rights (Court of the Hague 2020).

In some countries, such as Finland, Denmark, Germany, and Sweden, ADM has been broadly applied for tax administration. In Germany, about 25 percent of individuals’ tax statements are rated automatically by an algorithm, and the percentage is expected to increase to 40 percent in 2020. The German law allows other actions regarding tax assessments, such as decrees, corrections, retractions, recalls, repeals, and alterations (Etscheid 2018).

In Sweden, processes regarding the traffic tax have been automated, becoming a typical “yes” or “no” robotics-based system (see Lag om trängselskat). The traffic tax is generated after a vehicle is spotted by a camera in an area in which this tax is deducted. Thereafter, the owner of the vehicle is required to pay the traffic tax. It is a concrete example of a situation in which the requirement of legality can be met by specific legislation. However, this is a clear-cut case in which an automated public administration task is both familiar and narrow in scope and does not involve any secrecy on the part of the public institution (Koulu et al. 2019, 46).
In Finland, currently, taxpayers’ legal rights to receive accurate services and justification for taxation decisions are unclear. The deputy parliamentary ombudsman, Maija Sakslin, has expressed concerns about whether the principles of good administration and legal protection for taxpayers are fulfilled when information letters and taxation decisions generated by automated taxation systems are being sent out by the tax administration (AlgorithmWatch 2019, 58). As she points out, these letters include only the telephone numbers of the tax administration office. These tax officials were not involved in the automated processing of the case and do not have detailed information about the basis for the decision.

In France, two cases draw special attention to discrimination related to the use of ADM by public administrations. The personalized health files project (Dossier Médical), which began in 2004, aimed to centralize all personal health data; however, so far, only a few test projects related to breast cancer and complex ultrasound diagnosis are in progress (AlgorithmWatch 2019, 72). The second ADM use case was enacted by the French government to provide universities with the right to turn down applications from prospective students (AlgorithmWatch 2019). An online tool, Parcoursup, was created to match students’ preferences with available offerings. This tool is an update of the previous version of the platform, because it offers two potential opportunities for human intervention. To make administrative decisions about admissions, the platform collects data and course preferences from future students. Parcoursup was authorized by a ministerial ruling; however, the reform was labeled as discriminatory (McCullagh, Tambou, and Bourton 2019, 58). Later on, the government published the source code of the platform’s matching section, but it did not mention or explain the sorting of students (AlgorithmWatch 2019, 72). It remains unclear whether the law on the use of Parcoursup complies with the GDPR (McCullagh, Tambou, and Bourton 2019, 58).

**DISCUSSION**

Our analysis of the national laws and regulations and experimental use of ADM in six European countries shows that the current phase of the digital welfare state in Europe largely follows established models of civil law, such as the Nordic and conservative-corporatist regimes. In particular, our results indicate that all six countries, in their national adaptations of the GDPR, draw on the leeway offered by the GDPR to ensure the continuation of already existing practices or the expansion of the use of citizens’ data.

In the Nordic context, data collection for public registers and citizens’ data use for public administration take place on a larger scale compared to countries under the conservative-corporatist regime. The regulations of data protection are rather general. For these reasons, the state and its institutions can legitimately experiment with using ADM systems, which are not necessarily regulated, to provide citizens with more efficient services (from the state’s perspective). While the Nordic countries offer additional guarantees for citizens regarding the collection and use of data for ADM, they draw on citizens’ trust in the public administration, and thus the legislation includes a range of exceptions and safeguards for personal data processing, especially for the public administration. Another issue is the extent to which citizens are aware of their rights or the abuse thereof in such situations and have the ability to interpret the existing legislation. Yet the example of Denmark shows that it is quite hazardous to delegate privacy-protection-related matters to government ministers when adapting the GDPR to a national context because it provides the government with unlimited control over citizens.

In the Nordic regime, citizens may be "softly" directed toward sharing their data for the public good (i.e., privacy protection decisions that are beneficial to the public administration) by introducing default opt-in and opt-out options (i.e., nudges) into the governmental systems. Yet if this is done by inferences, which are so far unregulated by law, it could threaten citizens’ privacy, identity, data protection, reputation, and autonomy, as argued by Wachter and Mittelstadt (2019, 506). The use of inferences for nudging purposes strongly contrasts with the basis of the Nordic regime, which is to promote individual autonomy and secure equal access to justice for all its citizens.

While the legislation related to data protection and use of ADM in the Nordic regime appears to be inspired by the idea of simplicity, which is a characteristic of this type of civil law system (for more, see Husa, Nuotio, and Pihlajamäki 2007), legislation in countries under the conservative-corporatist regime continue to rely on extensive codifications, including a mixture of general and sectoral regulations. These countries have introduced explicit regulations regarding ADM, and so perhaps experimental use of ADM appears to be less common than in countries under the Nordic regime. However, due to extensive codification of the law, citizens might not be able to understand the regulations, which are often difficult even for legal professionals to interpret (for more, see De Geest 2012). Some regulations tend to limit the scope of the public administration’s power over citizens, which might be regarded as an expression of lack of trust between the public administration and citizens. This type of regulation may protect citizens to some extent against the use of ADM in sensitive areas of social security, such as welfare fraud, if citizens draw actively on their rights. However, the German, Dutch, and French national adaptations of GDPR also include the restrictions of citizens’ rights as data subjects in case of data breaches when the data processing is done in the public interest. There also seems to be more public debate around the use of citizens’ data by both public and private organizations as well as the use of ADM in countries under the conservative-corporatist regime in contrast to countries under the Nordic regime.

The examples of Germany and the Netherlands show that sectoral regulations may be better suited for regulating ADM in particular areas and for providing additional legal obligations for citizens regarding ADM. However, if such regulations are very broad, they may not fulfill their tasks. Additionally, the reasons underlying restrictive interventions, the indispensability of ADM for governmental operations, the indispensability of secondary data use, and whether inferences can be drawn from personal data obtained from citizens may be unclear. In Germany, a sector-specific regulation that concerns personal data processing for welfare fraud detection has had at least two positive outcomes: it has limited data processing by the government to the bare minimum, and it has improved the transparency of ADM for citizens (Gantchev 2019, 14). In contrast, the Netherlands has enabled the government to exercise its powers in a practically unlimited way due to broad legislation regarding welfare administration (Gantchev 2019). Unwarranted expansion of the control of the government may lead to more repression of citizens in the form of conditions and sanctions with respect to their welfare benefits (Gantchev 2019).
CONCLUSION

Our results show that there are important concerns about control and transparency in relation to the regulatory framework and current use of ADM across the studied countries. Legal protections for citizens are especially important in contexts in which ADM is used for sensitive decision-making, such as social and health service interventions or efforts to detect welfare fraud. When making decisions about citizens’ fundamental rights, the unpredictable consequences of ADM use can be significant. Thus, above all, a leading question for public administrations across the studied countries is whether some decisions should be outsourced to data- and code-driven computing systems at all.

Currently, the GDPR, its national adaptations, and some sectoral laws in certain countries are insufficient to protect citizens as data subjects. Our study shows that one prominent problem related to ADM in the public sector is that wide derogations can be found in national adaptations of the GDPR. In particular, derogations from the purpose limitation principle allow governments to broaden their secondary data use. When evaluating use of secondary data for ADM, there is a need to balance measures to ensure that both personal data protection and privacy are ensured as fundamental rights of citizens. Although the GDPR is an EU regulation that was expected to significantly limit ADM, it appears to not be sufficiently powerful due to its numerous shortcomings (see, e.g., Wachter and Mittelstadt 2019). In addition, data protection law does not reach as far as necessary to ensure the accuracy of decision-making processes or good administrative practices (YS, M and S v. Minister voor Immigratie, Integratie en Asiel 2014 Section IV C). Assessment of the decision-making process is confined to sectoral and member state law as well as to specific governing bodies (Wachter and Mittelstadt 2019). Yet the GDPR has initiated the process of strengthening data protections and unifying national legislation across EU countries. As the GDPR applies to both state and nonstate actors, it has had global implications in today’s interconnected world.

We agree with Spielkamp (2019), who argues that whether or not automation and predictive data analytics will benefit citizens is primarily a political issue. Such decisions need to be preceded by a public debate about values, citizens’ rights, and the definition of social justice to be realized by ADM systems. Too often, these systems are built by private firms and kept secret from the public (Spielkamp 2019; Pasquale 2015). They are applied in a range of areas, often without providing much knowledge to citizens regarding their functioning and design. Applied as such, they empower governments and public institutions by strengthening welfare conditionality, which makes citizens accountable to stricter state obligations and tougher sanctions than before (Gantchev 2019). Thus, we argue that the studied countries are in the critical phase of building digital welfare states, in which new digital technologies such as ADM are utilized to strengthen the power of the state and its institutions over citizens. While we have observed some prominent differences between countries under the Nordic regime and the conservative-corporatist regime, there is a need for further welfare analyses to understand existing differences in approaches to data protection and the use of ADM in Europe and beyond.

Our study clearly indicates the need for additional legislation regarding use of citizens’ data for ADM and regulation of ADM. The activities of both private companies and public administrations as well as the collaboration between the organizations of both sectors related to data protection and privacy should be also better regulated. In addition, the differences in the degree to which public and private organizations are bound by legislation should be decreased to enable sustainable, safe, and democratic data infrastructures and practices to be developed in the public sector of digital welfare states. Furthermore, datafication and the use of ADM should be considered in relation to broader social justice policies (Dencik et al. 2018) instead of explicit economic goals. We argue that states and their public institutions should play a central role in strengthening the legal and social norms associated with privacy and protection of citizens’ data as well as citizens’ right to social security.

AUTHOR BIOGRAPHIES

Marta Choroszewicz is Postdoctoral Researcher in sociology at the Department of Social Sciences, University of Eastern Finland. Her research has broadly investigated social inequalities in the professions. She is currently working in a project, Data-Driven Society in the Making, which focuses on the use of digital data and learning algorithms in healthcare and social services in Finland. In this project, Choroszewicz focuses on the data-driven welfare state, algorithmic decision-making and the mechanism of inequalities related to technology development and deployment. Her work has been published in: Sosiologia, International Journal of the Legal Profession, Kultura i Społeczeństwo, Equality, Diversity and Inclusion: An International Journal, Professions and Professionalism, and Human Relations. She published, in collaboration with Tracey L Adams, an edited book titled, Gender, Age and Inequality in the Professions (Routledge, 2019).

Beata Mäihäniemi is Postdoctoral Researcher in law and digitalization at the Legal Tech Lab, the start up at the Faculty of Law, University of Helsinki. She is currently involved in the project on ‘Potential and Boundaries of Algorithmic Transparency’ funded by the Academy of Finland. Her research interest circulates around access to information and automated decision-making, both in public and private sectors. She has been a part of research project on ‘Algorithm as a decision-maker? The possibilities and challenges of artificial intelligence in the national regulatory environment’. What is more, her recently published book, Competition Law and Big Data. Imposing Access to Information in Digital Markets, focuses on actions of online platforms that can be possibly anticompetitive and harmful to consumers. She has also researched on digitalization of legal professional and education.

LEGAL DOCUMENTS

• 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.

DANISH LEGISLATION


DUTCH LEGISLATION

• Bundesdatenschutzgesetz - Federal Data Protection Act (BDSG) of 30 June 2017 (Federal Law Gazette I p. 2097).

FINNISH LEGISLATION


FRENCH LEGISLATION

ciety in the Making,” funded by the Academy of Finland (no. 317303) and University of Eastern Finland, as well as the project on "Potential and Boundaries of Algorithmic Trans-
parency" funded by the Academy of Finland (no. 324116) and the University of Helsinki.

Global Perspectives
REFERENCES


Kitchin, Rob. 2014. The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences. Los Angeles: SAGE Publications Ltd. [link]


Global Perspectives

13

