CODED INJUSTICE

SURVEILLANCE AND DISCRIMINATION IN DENMARK'S AUTOMATED WELFARE STATE

AMNESTY INTERNATIONAL

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

First published in 2024
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: EUR 18/8709/2024
Original language: English

amnesty.org

Cover illustration: *© Ard Su*

AMNESTY INTERNATIONAL

CONTENTS

1. GLOSSARY

WORD	DESCRIPTION
ARTIFICIAL INTELLIGENCE (AI)	Broadly speaking, AI is any technique or system that allows computers to mimic human reasoning.
MACHINE LEARNING (ML)	A subset of AI, ML is a technique to provide AI with the capacity to learn from data to perform a task (either specific or general) and, when deployed, ingest new data and change itself over time.
DEEP LEARNING	A subset of AI and ML, deep learning is a type of ML characterized by (1) the use of artificial neural networks (a type of algorithm that attempts to mimic human reasoning) and (2) having the ability to digest and learn from vast amounts of data. It is commonly used for tasks like image and voice recognition tools.
ALGORITHM	An algorithm is a list of mathematical rules which solve a problem. The rules must be in the right order – think of a recipe. Algorithms are the building blocks of AI and ML. They enable AI and ML technologies to train on data that already exists about a problem so that they can solve problems when working with new data.
ALGORITHMIC DECISION-MAKING SYSTEM	An algorithmic system that is used in (support of) various steps of decision-making processes.
AUTOMATED DECISION-MAKING SYSTEM	An algorithmic decision-making system where no human is involved in the decision-making process. The decision is taken solely by the system.
SEMI-AUTOMATED DECISION-MAKING SYSTEM	An algorithmic decision-making system where a human is involved in the decision-making process, or the algorithm is used to support the decision-making. Often, these systems are used to select cases for human review or to assist in the decision-making process by providing information and/or suggested outcomes.
BLACK-BOX ALGORITHM	An algorithmic system where the inputs and outputs can be viewed, but the internal workings are unknown to its designer. This terminology most readily applies to more complex ML algorithms.
ACCURACY	In the field of AI, accuracy measures are generally used to ascertain the number of "correct" outputs that a system produces, whether those outputs are predictions, identifications or simpler calculations (as a percentage of the number of total outputs made).

WORD	DESCRIPTION
EXPLAINABILITY	Designing an AI system such that a human can understand and explain the way the model works (counter to the idea of a black-box system) and retain oversight over its functioning.
PROFILING	In the European Union General Data Protection Regulation (GDPR), profiling is described as any form of automated processing of personal data to evaluate personal aspects of a person, in particular, to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, and produce legal effects concerning them or similarly significantly affecting them.
FAIRNESS	There are numerous suggested methods, approaches and definitions for embedding fairness into AI systems to avoid algorithmic bias. They are all predicated on the idea of eliminating any prejudice, discrimination or preference for certain individuals or groups based on a characteristic from the output of an AI system. Though fairness methods are an important element of ensuring AI systems are unbiased, Amnesty International generally considers them to be a limited tool in and of themselves, as discrimination and bias present within AI systems is not solely a technical issue.
FRAUD-CONTROL MODELS OR ALGORITHMS	ML algorithms used to identify recipients and claimants of social protection schemes who are at higher risk of committing fraud or an error in their application. The systems often use historical data on behaviours and characteristics that are considered to be commonly associated with fraud and error.
INTEROPERABILITY	Interoperability refers to the functionality that enables information systems to exchange data and to enable sharing of information. For example, multiple databases can be considered interoperable if information within each can be merged, aggregated, exchanged and interpreted in a unified manner.
ALGORITHMIC DISCRIMINATION	Algorithmic discrimination occurs when automated systems contribute to unjustified disparate treatment or impacts which are unfavourable to people based on their race, colour, ethnicity, sex (including pregnancy, childbirth, and related medical conditions, gender identity, intersex status, and sexual orientation), religion, age, national origin, disability, genetic information, or any other classification protected by law.
MITID (PREVIOUSLY KNOWN AS NEMID)	MitID (the Danish national electronic ID) is Denmark's digital ID that residents are required to use to access public services.
PREDICTIVE ALGORITHMS	The use of AI techniques to make future predictions about a person, event or any other outcome.
CLASSIFICATION	Classification is a supervised ML method where a vast number of data points are labelled with descriptors or put into categories. The model does this by looking at input data and predicting the correct label, among a known finite set of labels. For example, a model may look at pictures of different animals and label them as "cat" or "dog". In classification, in order to carry out labelling, the model is first fully trained using training data, and then evaluated on test data before being used to perform predictions on new data.
CLUSTERING	Clustering is the process of grouping similar objects into categories, or clusters. Clustering is an unsupervised ML technique for identifying and grouping related data points in large datasets without human input as to what that clustering should look like. It groups objects in such a way that objects in the same category, called a cluster, are in some sense more similar to each other than objects in other groups.

WORD	DESCRIPTION
RISK-SCORING	The semi- or fully-automated processing of data to assess or predict for the risk that an outcome will occur, either at the individual or community level, or in a specific event or scenario.
SOCIAL REGISTRIES	Social registries are information systems that support the process of outreach, registration and assessment of needs to determine the potential eligibility of individuals and households for one or more social protection programmes.
SOCIAL PROTECTION	Social protection refers to a broad range of contributory programmes (those financed through contributions made by an individual or on their behalf) and non-contributory programmes (those funded through national tax systems). Social protection programmes can include (1) social insurance, such as pension insurance; (2) employment and labour programmes, including skills training, unemployment benefits and job search assistance; and (3) social assistance and cash benefits for people living in poverty.
SUPERVISED LEARNING	In supervised learning, AI is trained from examples consisting of inputs and labelled outputs (see above example provided in the definition of "classification"). The system learns to find patterns and relationships between the inputs and labelled outputs, and the developer has a specific objective or target for the system to predict or categorize. In this way, the AI system starts to make its own predictions on any new inputs (without corresponding labelled output), based on the historical associations between inputs and labelled outputs identified in the training data.
UNSUPERVISED LEARNING	In unsupervised learning, AI systems discover patterns or relationships in unlabelled data. Humans do not actively indicate to the AI system the target or output of the exercise.

2. EXECUTIVE SUMMARY

Denmark is lauded for having a welfare state that offers an adequate social safety net for its residents, with the government spending 26% of GDP on welfare benefits. With an increase in digitization, Denmark has positioned itself as a model digital welfare state and is often seen as a digitization frontrunner in Europe. The country's transition to a digital welfare state is informed by the government's efforts to streamline administrative tasks and to increase the effectiveness and efficiency with which welfare and other essential public services are delivered.

However, the reality is that Denmark's transition to a digital welfare system now poses human rights risks and violations for social security benefits recipients.

This report discusses the findings of Amnesty International's research in Denmark on the country's social benefits system, including the Danish government's use of fraud control algorithms to inform the distribution of social benefits through a public authority, Udbetaling Danmark (UDK or Pay Out Denmark), and a company, Arbejdsmarkedets Tillægspension (ATP), which has a mandate from the Danish government to administer social benefits on behalf of UDK.

In 2012, the Danish government established UDK through the enactment of the Udbetaling Danmark Act to centralize the payment of welfare benefits overseen by municipalities, including child allowances, pension benefits, housing benefits, unemployment benefits, maternity and sick pay benefits under the welfare state system. UDK/ATP established a Joint Data Unit tasked with developing data-driven fraud control algorithms with the purported aim of identifying fraudulent social benefit applications for further investigations, in collaboration with private companies. The Joint Data Unit links or merges the personal data of millions of Danish residents from registers (public databases) that contain information about benefits recipients and their family members or other household members. This information includes, but is not limited to, their residency and residency moves, citizenship, place of birth, family relationships and circumstances, housing arrangements and building conditions, employment, income, tax, health and education. UDK uses profiling models (which analyse aspects of an individual's personality, behaviours, interests and habits to make predictions or decisions about them) to analyse this data in order to identify persons who supposedly have an increased risk of receiving benefits fraudulently, and flag them for further investigations. The models generate a "wonderlist" ("question list" in English) of persons who are purportedly at high risk (calculated statistically) of fraudulently or erroneously receiving benefits. As of 2019, UDK was reported to be using about 60 different artificial intelligence (AI) and machine learning (ML) models to identify individuals it believed were highly likely to be receiving benefits fraudulently.

Although technology use in the public sector is often presented as objective and unbiased, it is virtually impossible to create value-neutral technologies since they inherently reflect the underlying laws, rules, norms, patterns of attitudes and behaviour of the environments in which they are produced. In the public sector context, and even more so when used for fraud detection purposes, these often encourage discrimination against certain groups based on their race, ethnicity, religion, migration status, income, gender, disability and age.

This report defines and interrogates the ways in which UDK and ATP's use of algorithms to detect fraud in the distribution of social benefits negatively affects the human rights of social security benefits recipients, including their rights to privacy, equality and non-discrimination, dignity, social security and remedy.

The report also demonstrates how social benefits recipients are subjected to mass surveillance through the use of traditional and digital surveillance mechanisms. It highlights the discriminatory effects that result from UDK/ATP's use of algorithmic systems for fraud detection purposes. Amnesty International's research has found how these discriminatory effects are occurring in the context of discriminatory or unequal structures

present in Danish societal institutions – in hostile Danish laws, rules, norms, patterns of attitudes and behaviour that create and promote "othering" or the differentiation of groups. These are practices that not only encourage discrimination against marginalized groups, but that also allow for mass surveillance of populations in general.

Further, the report highlights ways in which the use of technology and digitization by UDK/ATP excludes marginalized groups from accessing the social benefits system and unfavourably includes or forcibly includes groups who do not wish to be included in the system.

DENMARK'S HUMAN RIGHTS OBLIGATIONS

Under various international human rights legal instruments and standards, EU law and standards, as well as national laws and policies, Denmark has an obligation to respect and protect the rights to privacy and data protection, freedom of expression, equality and non-discrimination and society security, among others. Denmark also has special responsibilities to respect and protect the human rights of children, women and LGBTI people, people with disabilities, and older persons. It also has an obligation to ensure transparency, accountability and a right to remedy. Finally, corporations have a responsibility to respect human rights in all their business activities, and states have an obligation to protect against human rights abuses within their territory and/or jurisdiction by third parties, including business enterprises.

'DUVET LIFTING': MONITORING AND SURVEILLANCE OF BENEFITS APPLICANTS, RECIPIENTS AND THEIR AFFILIATES

Amnesty International's research found that the Danish government has implemented privacy-intrusive legislation that allows for the collection of data from residents in receipt of benefits and their household members, without their consent, for the purposes of surveilling its population to control for fraud. These laws allow for and govern UDK/ATP's and municipalities' mass-scale extraction and processing of personal data of social benefits recipients for fraud detection purposes, including laws on merging of government databases and the use of fraud control algorithms on this data, and the unregulated use of social media and the reported use of geolocation data for fraud investigations.

Our research has found that the collection and merging of large amounts of personal data contained in government databases has effectively forced social benefits recipients to give up their right to privacy and data protection in order to exercise their right to social security and other social and economic rights.

The collection and processing of large amounts of data – including sensitive data which contains characteristics that could reveal race and ethnicity, health, disability, sexual orientation – the centralization or interoperability of databases for fraud investigations without residents' consent, and the use of social media are highly invasive and disproportionate methods to detect fraud. Moreover, they are of questionable utility. Authorities should seek less invasive means of detecting fraud that meet the tests of necessity and proportionality laid out under international human rights law.

Benefits applicants and recipients are also subjected to "traditional" or "analogue" forms of surveillance and monitoring for the purposes of fraud detection. These analogue forms continue to be used together with fraud control algorithms. Such methods include the persistent reassessment of eligibility by municipalities, fraud control cases or reports from other public authorities, including tax authorities and the police, and anonymous reports from members of the public. Pervasive surveillance and monitoring by fellow residents, municipalities and other public authorities interferes with or restricts benefits applicants' and recipients' rights to privacy, human dignity and social security, further compounding the human rights violations enabled by these digital and analogue forms of surveillance.

These analogue forms of monitoring and surveillance, when coupled with overbroad methods of digital scrutiny, have created a system of pernicious surveillance. Constant surveillance of benefits recipients also has a negative impact on people's mental health, causing significant stress and anxiety.

STRUCTURAL DISCRIMINATION, HEIGHTENED RISK OF ALGORITHMIC DISCRIMINATION

In the case of Denmark, its social benefits system exists in an already hostile environment for asylum seekers, people who have been granted refugee status in Denmark, migrants, and racialised communities, which could encourage discrimination against these groups based on their race, ethnicity and religion.

This discrimination is demonstrated by the differential allocation of non-contributory child benefits to people who have been granted refugee status in Denmark. The Danish government's imposition of lengthy, excessive and disproportionate residency requirements on people claiming child benefits has discriminatory impacts on people granted refugee status in Denmark, particularly from countries including Syria, Afghanistan, Lebanon and Iraq. This restricts their right to access full child benefits, which are non-contributory benefits, on an equal basis with other groups as stipulated under human rights law. The lack of access to full child benefits negatively affects the ability of parents to meet their children's basic needs. This is compounded by the fact that migrant and refugee parents often cannot access the job market when they arrive in Denmark because of language barriers and a lack of relevant contextual knowledge and networks in Denmark.

Amnesty International's research has also found that, at its core, discrimination through UDK/ATP's algorithms is happening in the context of unequal structures laws, rules, institutions, norms and values present in Danish society. These discriminatory structures are embedded in the design of UDK/ATP's algorithmic models and enable the creation and promotion of categorizations based on difference or "othering". Specifically, laws, rules, norms and patterns of attitudes designed or established by dominant groups in Denmark that appear to be neutral or "race agnostic" can, in practice, have a discriminatory effect.

Amnesty International has found that UDK/ATP's use of fraud control algorithms to identify social benefits applicants and recipients likely to commit fraud risks dangerously and disproportionately targeting already marginalized groups. These are people whom UDK/ATP has constructed as "others" in Danish society because they have differing or "unusual" living or family arrangements or "foreign affiliations".

Marginalized groups are constructed by Danish authorities as more likely to commit fraud or as underserving of benefits, and there is a risk that they will be flagged for fraud based on their family and living arrangements and foreign affiliations. These are characteristics or variables that can act as proxies for race, migration status and social and economic status, and can encourage discrimination based on persons having these characteristics.

Amnesty International has found that categorization based on "othering" or difference risks indirectly and directly discriminating against low-income groups, racialized groups, migrants, refugees, ethnic minorities, people with disabilities, and older people. This has punitive outcomes for these groups because their right to equal treatment and non-discrimination are violated, but simultaneously they also risk being denied their right to social security.

UNUSUAL HOUSEHOLD, FAMILY AND RESIDENCY PATTERNS

One of the main principles behind UDK/ATP's fraud control models is to identify "unusual" or "atypical" living patterns or arrangements; that is, atypical relationships and unusual residency patterns as an indicator of fraud, which warrant further investigation. Despite not clearly defining what constitutes "unusual" or "atypical arrangements" in law, leaving the door open to arbitrary decision-making, the algorithms use information such as household size, composition and evidence of co-habitation, and are designed to find "statistical outliers"; that is, beneficiaries whose circumstances sufficiently deviate from the "norm". The algorithms risk discriminating against groups based on their race and ethnicity, class and relationship status because the models are embedded with social norms that reflect the view of dominant groups in Denmark about what a household or a family is. They fail to consider contextual factors such as existing inequalities within Danish society, including class and disability-based inequalities, and differing and evolving cultural norms or differences among different groups that inform living arrangements and household composition. Failure to take into account relevant contextual factors, existing societal inequalities and differing and evolving cultural norms allows the use of these models to disproportionately target low-income groups, people with disabilities, racialised people, migrants, and older people. UDK/ATP should therefore re-examine its fraud detection policies on the use of data relating to "unusual" residency, family or household patterns.

FOREIGN AFFILIATION OR TIES

In addition to identifying unusual patterns in household composition, Amnesty International has found that inputs related to "foreign affiliation" are used by UDK/ATP as part of its algorithmic models, particularly within pensions and child benefit distribution. This is because UDK/ATP are concerned that social benefit recipients may be living abroad without informing the agency and taking their welfare entitlement with them unjustly. To try and control for this, UDK/ATP uses an algorithm called the "Model Abroad".

The "Model Abroad" generates a score for a beneficiary's "foreign affiliation" by creating a relative measure of an individual's "strength of ties" with each country. The documentation provided in response to an FOI request provides only partial information on the model's inputs and specific deployment cases. While it indicates that "foreign affiliation" will not be used directly to identify cases of potential fraud, it is nevertheless used to refine the search for cases that UDK will target for fraud investigations and therefore acts as a de facto indicator. More specifically, the output of the model is used to identify groups of beneficiaries who are deemed to have "medium and high-strength ties" with non-EEA countries and prioritizes these groups for fraud investigations. This is constructed as a relative metric, meaning "medium and high-strength ties" are defined in relation to other social security beneficiaries rather than being defined by objective criteria. This simultaneously reiterates how the algorithm is designed such that beneficiaries are assessed against the "norm" or dominant group in Denmark, and emphasizes the need for greater transparency, as the algorithm and output is a self-constructed metric (as opposed to being a metric taken from academic literature that has been statistically validated by a group of experts).

UDK uses data collected by the Joint Data Unit Abroad on residents' foreign residence, entry and exit abroad, marital status, number of children, real estate or vehicles abroad and social benefits received, to be used within the algorithm. The use of citizenship and other foreign affiliation-related criteria explicitly targets people from countries outside the EEA and, therefore, directly discriminates on the basis of nationality, ethnicity and migration status. This violates the right to equality and non-discrimination of racialized groups. It also risks interfering with people's right to social security.

Further, data inputs used to create, train and operate AI systems are often reflective of historical, systemic, institutional and societal discrimination. Thus, the introduction of fraud control algorithms risks entrenching historical injustice against marginalized communities, including those living in poverty. Several of the fraud control models directly include inputs related to an individual's salary and income. From the redacted documentation received by Amnesty International, it is not possible to determine the precise impact of including income or salary indicators within the algorithms; however, their inclusion intends for the systems to distinguish between social benefit beneficiaries on this basis, presenting an unacceptable risk of disadvantaging and explicitly targeting beneficiaries on lower incomes. Additionally, several of the models present significant concerns around their analytical integrity, whether due to the inputs included in the model, the use of self-constructed and subjective metrics, or concerns around the representativeness of the datasets on which they are trained.

Technical evaluations and audits have become an increasingly popular tool to assess the performance and impact of algorithms and diagnose problematic behaviour. While UDK provided redacted documentation on a select few of their fraud control models, any requests for data that would allow researchers to conduct bias and fairness testing were denied. The rejections demonstrate a lack of transparency within UDK to ensure the availability of information that allows their algorithms to be scrutinized and tested.

DIGITAL EXCLUSION AND FORCED INCLUSION

Amnesty International's research has found that automation and digitalization of the benefits system not only allows for the exercise of surveillance and control over benefits applicants and recipients but that the system also creates a barrier to accessing social benefits for some marginalized groups, including women in crisis centres and people with disabilities. Digitization also risks the exclusion of older people. As a result, the system risks restricting their rights to social security and non-discrimination.

Amnesty International collaborated with LOKK (Denmark's National Organization of Women's Shelters), which represents 46 women's shelters around Denmark, to design a survey to study the accessibility of UDK's system for women living in shelters due to intimate partner violence.

Amnesty International's research has found that digitization of Denmark's social benefits system has led to people with disabilities being forcibly or unfavourably included in UDK's system. Unfavourable inclusion is defined as "being forced to be included in deeply unfavourable terms". People with disabilities are forcibly or

unfavourably included because they have no choice but to share their data with third parties to access the benefits system. This inclusion raises data privacy and security concerns for them because of risks surrounding the misuse of their personal information by government-provided personal assistants who have access to their personal information. Access to systems must, therefore, not be solely and exclusively digital; authorities must provide viable alternatives that are inclusive and accessible for the most disadvantaged and marginalized groups without discrimination, such that all groups in society are able to participate in the social security system without risks to their privacy and data protection.

LACK OF STATE OVERSIGHT, LACK OF TRANSPARENCY, AND RISKS TO REMEDY

Amnesty International's research has found that the Danish government has delegated the distribution of benefits to ATP, a company established as a self-governing institution under the ATP Act 1964. Amnesty International has also found that there is a lack of adequate, independent oversight over UDK/ATP's data and algorithmic practices, creating risks of human rights violations. Oversight gaps evident in the existing UDK/ATP governance structure and the lack of proactive investigatory powers of the Danish Data Protection Authority are clear failings of the Danish government to respect and protect human rights by ensuring that there is effective oversight over the public authority UDK as well as the company ATP, which is accountable to the state. Further, Amnesty International has found that ATP does not appear to be conducting anti-bias or anti-discrimination training for its staff, publishing data protection impact assessments or conducting adequate audits of its fraud control algorithms, all of which could be measures undertaken to either identify or mitigate the risk of potential harm related to their algorithmic systems. Additionally, Amnesty International has found that ATP is not carrying out human rights due diligence in line with international human rights standards to identify, mitigate and prevent the harmful effects of the UDK/ATP benefits system, and thus is failing to respect human rights.

Regarding access to remedies by affected people, Amnesty International has identified risks to the right to remedy arising from two sources. First, there is a lack of transparency and clear notification regarding UDK/ATP's use of fraud control algorithms in flagging individuals up for further fraud investigations. Second, the Public Administration Act does not contain provisions that mandate public authorities to inform a person that the case against them has arisen from an algorithm. As a result, because a person flagged for fraud by UDK/ATP algorithms is unaware that they are the subject of an automated process, they cannot effectively challenge UDK/ATP's decision-making process.

FORTHCOMING OBLIGATIONS UNDER THE EU AI ACT

Amnesty International believes the evidence gathered for this investigation indicates UDK/ATP's algorithmic models should also fall under the social scoring prohibition of Article 5(1)(c) of the Act, which would mean the system should be banned. Amnesty International believes that this system is a social scoring algorithm because the system assigns an explicit set of metrics which constitute "social scores", as they are related to the trustworthiness of an impacted person - their likelihood of committing fraud. The system continues to evaluate and classify people based on data relating to their social behaviour or personal characteristics, which is unrelated to the original purpose for which the data was collected, and which leads to their unfavourable treatment, through being flagged up for fraud investigations.

Unless UDK and ATP can provide sufficient evidence otherwise, Amnesty International argues that the system in its current formation should be paused until UDK and ATP provide adequate evidence demonstrating that their practices do not constitute social scoring.

Amnesty International wrote to UDK and ATP detailing why we believe that their fraud control models constitute a social scoring system as outlined in the EU AI Act and invited their response. Amnesty International also asked UDK and ATP to provide adequate explanations and evidence if they believe that the models would not fall under the definition of a social scoring system. UDK stated in its response to allegations in our report that its algorithmic practices do not constitute social scoring under Article 5 of the EU AI Act, as the controls have a clearly defined purpose, are proportionate, and are aimed at ensuring the correct payment of social benefits and because its fraud controls comply with applicable EU and national legislation. UDK and ATP have not provided Amnesty International with any detailed evidence or independent assessments that their algorithmic practices are not a social scoring system under Article 5 of

the EU AI Act, nor have they provided us with any evidence that their practices are necessary and proportionate.

The specific interpretation of Article 5, including the social scoring ban, will be clarified in the European Commission's upcoming guidance on what constitutes prohibited practices under Article 5. The European Commission should clarify that risk-scoring algorithms which lead to discriminatory outcomes for impacted affected people, such as UDK's fraud detection algorithm, are prohibited under the Act.

Any algorithmic systems used by UDK/ATP to detect benefits fraud that are assessed not to constitute social scoring, are classified as high-risk systems under the EU Artificial Intelligence Act 2024 (AI Act), which came into force on 1 August 2024. According to Annex III, high-risk systems are "AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services". As a result, at the very minimum, Danish authorities are required to ensure that UDK and ATP's fraud-detection algorithmic systems meet risk management, transparency requirements and other provisions placed on deployers and providers as outlined in the AI Act. The provisions on high-risk systems outlined above will not apply until 2 August 2030. Nevertheless, Amnesty International recommends the Danish authorities ensure these are being implemented as soon as possible to ensure greater transparency in the use of high-risk systems.

RESPONSES FROM AUTHORITIES AND COMPANIES

Amnesty International shared the findings of our research with UDK/ATP on 17 October 2024 and the Ministry of Employment (the Danish Agency for Labour Market and Recruitment or STAR) on 18 October 2024 and sought their written responses to specific allegations detailed in this report ahead of its publication. UDK responded to the allegations in the report on 30 October 2024 and 1 November 2024, while the Ministry of Employment responded to the allegations in the report on 1 November 2024. Amnesty International also wrote to the company NNIT on 23 October 2024 about their mention in this report and sought their responses to further questions. NNIT responded on 1 November 2024. All responses are reflected, where relevant, in the text of the report.

In their responses, Danish authorities refuted specific findings of this report. Where relevant, their responses are reflected in the full text of the report.

KEY RECOMMENDATIONS

The research builds on Amnesty International's previous research publications, including *Xenophobic Machines: Discrimination through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal* (2021), *Trapped by Automation: Poverty and Discrimination in Serbia's Welfare State* (2023) and *Use of Entity Resolution in India: Shining a Light on How New Forms of Automation Can Deny People Access to Welfare* (2024).

TO THE DANISH AUTHORITIES:

- Ensure that Udbetaling Danmark/ATP stops using algorithms that evaluate or classify people based on data on their social behaviour or sensitive personal characteristics or proxies thereof, which lead to the violation of their human rights.
- Pause the system in its current formation until adequate evidence is provided to make a full and final assessment of the system and the applicability of the social scoring ban of the AI Act.
- Ensure a strong and rights-respecting implementation of the AI Act at the national level and a strong, effective and Charter-based interpretation of prohibited and risky technologies under the AI Act as soon as possible and no later than the legally set deadlines including the provisions of article 9, 10, 11, 13, 26, 27, 85, 86, and 87 of the EU AI Act to manage risks that high risks systems can pose to fundamental rights and to ensure greater transparency in the use of high-risk systems.

TO THE DANISH MINISTRY OF EMPLOYMENT AND UDBETALING DANMARK:

- Establish a clear, unambiguous and legally binding ban on the use of data regarding citizenship, "foreign affiliation", or nationality, or proxies thereof, in risk-scoring for the purposes of fraud control.

- Review and amend Udbetaling Danmark/ATP's norms, policies and laws that inform risk-profiling through Udbetaling Danmark/ATP's fraud control algorithms that could perpetuate discrimination based on income, race, ethnicity, religion, migration status, gender, disability or age, and ensure that they comply with relevant international human rights standards.
- Ensure that Udbetaling Danmark/ATP ends the practice of mass extraction, processing, and exploitation of residents' data for fraud-control purposes, and the use of social media.
- Ensure that Udbetaling Danmark/ATP is fully transparent and provides meaningful information to affected individuals about the underlying logic, importance and expected consequences of decisions, even if they are not fully automated, regardless of the level of human involvement in the decision-making process.
- Ensure that Udbetaling Danmark/ATP and municipalities inform benefits applicants and recipients that they have been identified for fraud investigations by an algorithm in a clear, comprehensible and detailed manner.
- Ensure that Udbetaling Danmark/ATP publishes clear information about the fraud control inputs it uses to make risk assessments for fraud and error (including publishing regular reports and key statistics); information about how the fraud control models work; information on performance and bias assessments conducted; and information on human rights impact assessments and data protection impact assessments performed prior to and during the use of fraud control systems, including during the processing of data through the systems.
- Ensure that Udbetaling Danmark/ATP and municipalities conduct independent human rights and data protection impact assessments of the UDK system. These impact assessments should include, at the very minimum, an evaluation of the discriminatory effects of the use of fraud control algorithms on marginalized groups, including low-income groups; racialized groups, including migrants and people who have been granted refugee status in Denmark; ethnic minorities; people with disabilities; and older people.
- Ensure that Udbetaling Danmark/ATP and municipalities provide caseworkers with additional training and capacity building where necessary to address and prevent issues related to discriminatory effects, such as automation bias.
- Ensure that Udbetaling Danmark takes steps to end the exclusion of women in crisis centres, older people and people with disabilities, occasioned by the digitization of Udbetaling Danmark's benefits system, by ensuring that the system is, in practice, fully accessible through non-digital means for groups who cannot use the necessary technology.
- Ensure that Udbetaling Danmark/ATP provides social assistance applicants with clear and accessible information about how decisions are made in their cases and how to appeal such decisions. Where needed, ensure that applicants receive support in lodging their appeal, including legal and/or financial support.
- Require companies developing AI products to conduct adequate human rights due diligence to identify and address actual or potential human rights harms that might appear at any stage of the supply chain or product lifecycle as outlined in the UN Guiding Principles on Business and Human Rights.

DANISH PARLIAMENT:

- Review and amend section 2(1)(7) of Executive Order of the Child and Youth Benefit Act LBK no. 724 of 25/05/2022 and section 5(a) of the Executive Order of the Act on Child Allowance and Advance Payment of Child Support (LBK no. 63 of 21/01/2019) to remove excessive and lengthy residency requirements that restrict access to child benefits for people granted refugee status in Denmark.
- Review and amend the Danish Public Administration Act to include provisions on automated decision-making that guarantee that benefit applicants and claimants can access their right to an effective remedy.
- Enact legislation to establish an independent public authority with oversight over the UDK/ATP and that monitors UDK/ATP's use of AI systems, to strengthen accountability mechanisms and increase human rights protection. This includes establishing an independent authority that has oversight over Udbetaling Danmark/ATP's activities in compliance with Article 70 of the EU AI Act.

TO THE DATA PROTECTION AUTHORITY:

- Exercise its supervisory authority under Article 29 of the Danish Data Protection Act and Article 58 of the GDPR to order that Udbetaling Danmark/ATP and municipalities provide it with information on its data practices and any data protection impact assessments that these entities have conducted.
- Ensure that Udbetaling Danmark/ATP and municipalities comply with all relevant provisions of the Danish Data Protection Act and the GDPR, including Articles 5 and 6 on the processing of data defined in these regulations.

TO MUNICIPALITIES:

- Provide caseworkers with additional training and capacity building to address and prevent issues such as automation bias, discrimination and the violation of welfare recipients' dignity and privacy when assessing their eligibility for benefits.
- Conduct independent human rights and data protection impact assessments of their fraud investigation practices. Impact assessments should include, at the very minimum, an evaluation of the discriminatory effects of fraud control algorithms on marginalized groups, including low-income groups, racialized groups and people with disabilities.
- Ensure that social assistance applicants receive clear and accessible information about how decisions are made in their cases, how to appeal such decisions and, where needed, ensure that applicants receive support in lodging their appeal, including legal and/or financial support.

TO THE EUROPEAN COMMISSION:

- Ensure that the upcoming guidance by the European Commission on the practical implementation of the prohibited practices referred to in the AI Act provides legal clarity and addresses relevant AI-based social scoring practices across the EU, including discriminatory fraud detection and risk profiling systems in the context of social protection.

TO ATP:

- Urgently take steps to ensure that ATP does not contribute to human rights violations or abuses through its involvement in the UDK benefits system, and to address any human rights violations when they do occur, including where necessary by cooperating in their remediation.
- Provide evidence that caseworkers in the fraud control units have the necessary competence and authority to intervene in the fraud investigation and decision-making processes when a person is identified for a fraud investigation by UDK/ATP's algorithms.
- Provide caseworkers with additional training and capacity building where necessary to address and prevent issues such as automation bias and discrimination.
- Undertake proactive, ongoing human rights due diligence throughout the lifecycle of algorithmic technologies, both before and after the roll-out and implementation of new systems, in order that risks can be identified during the development stage and human rights abuses and other harms immediately picked up once the technologies have been implemented.

Publicly disclose the steps it has taken to identify, prevent and mitigate human rights abuses and risks in its business operations, including through its involvement and business relationship with UDK.

3. BACKGROUND

As datafication[1] and the use of AI systems becomes ubiquitous in society, tensions are constantly emerging between the advantages of technology and serious concerns about the human rights violations that can arise from the unchecked introduction and use of such technologies.[2] These tensions are exacerbated by a lack of understanding among both policymakers and developers and providers of these systems of the types of human rights violations that flow from using technology, as well as a lack of proper oversight or regulation, including prohibitions and safeguards where the use of technology violates human rights.

As AI advances, the use of algorithms is increasingly promoted as, and is becoming the preferred solution for, service delivery by governments. Governments around the world are increasingly using data and AI systems in the delivery of public services such as social protection, health care and education, with the justification that they guarantee efficient and effective service delivery.[3] The increasing use of technology by governments for the delivery of public services such as social protection was highlighted in a 2019 report by the former UN Special Rapporteur on extreme poverty, who noted that "systems of social protection and assistance are increasingly driven by digital data and technologies".[4]

While this trend of increased digitization is often presented by states as a neutral or technocratic solution to achieve greater coverage, improve administrative systems, detect fraud and enhance security, there has been significant research to show that digitization of social protection poses many risks to human rights, including by exacerbating inequality and discrimination and entrenching existing flaws. For example, research by Amnesty International and many other organizations has shown that the increased use of data and AI systems, particularly the use of algorithmic risk-based systems by governments for public service delivery, can infringe upon human rights including the rights to privacy, social security and equality and non-discrimination, among others.[5] The use of these systems also raises concerns that automated decision-making substantially erodes the ability of populations subjected to these technologies to assert their rights

---

[1] Datafication refers to the process of transforming aspects of everyday life into quantifiable data.

[2] Ben Green, "The flaws of policies requiring human oversight of government algorithms", 2022, Computer Law & Security Review, Volume 45; Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, 2018; Lorna McGregor and others, "International human rights law as a framework for algorithmic accountability", 2019, International and Comparative Law Quarterly, Volume 68, Issue 2, https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/international-human-rights-law-as-a-framework-for-algorithmic-accountability/1D6D0A456B36BA7512A6AFF17F16E9B6; https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/international-human-rights-law-as-a-framework-for-algorithmic-accountability/1D6D0A456B36BA7512A6AFF17F16E9B6

[3] Amnesty International, *Xenophobic Machines: Discrimination Through Unregulated Use of Algorithms in the Dutch Childcare Benefits Scandal* (Index: EUR 35/4686/2021), 25 October 2021, https://www.amnesty.org/en/documents/eur35/4686/2021/en/
Amnesty International, "Trapped by automation: Poverty and discrimination in Serbia's welfare state", 4 December 2023, https://www.amnesty.org/en/latest/research/2023/12/trapped-by-automation-poverty-and-discrimination-in-serbias-welfare-state/
Ryan Calo and Danielle Keats Citron, "The automated administrative state: A crisis of legitimacy", 2021, Emory Law Journal, Volume 70, Issue 4; Rikke Frank Jørgensen, "Data and rights in the digital welfare state: the case of Denmark", 2 June 2021, Information, Community and Society, Volume 26, Issue 1, https://www.tandfonline.com/doi/abs/10.1080/1369118X.2021.1934069
Julie Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, 2019; Shoshana Zuboff, "Big other: Surveillance capitalism and the prospects of an information civilization", 1 March 2015, Journal of Information Technology, Volume 30, Issue 1, https://doi.org/10.1057/jit.2015.5

[4] Special Rapporteur on extreme poverty and human rights, Report, 11 October 2019, UN Doc. A/74/48037, para. 3.

[5] Virginia Eubanks, *Automating Inequality* (previously cited); Emnet Almedom and others, "Algorithms and child welfare: The disparate impact of family surveillance in risk assessment technologies", 2020, Berkeley Public Policy Journal, Fall 2020, https://bppj.berkeley.edu/2021/02/02/algorithms-and-child-welfare-the-disparate-impact-offamily-surveillance-in-risk-assessment-technologies/
Phillip Alston, "What the 'digital welfare state' really means for human rights", 8 January 2020, https://www.openglobalrights.org/digital-welfare-state-and-what-it-means-for-human-rights/
Amnesty International, *Xenophobic Machines* (previously cited); Amnesty International, "Trapped by automation: Poverty and discrimination in Serbia's welfare state" (previously cited).

and to hold governments to account for the harms created from their use because of a pervasive lack of transparency.[6]

Denmark is one country where the authorities have deployed technology in the realm of social protection.[7] Denmark has been lauded for having a welfare model that offers adequate social protection for its residents, with authorities spending 26% of the country's GDP on welfare benefits.[8] Denmark has, over the years, positioned itself as a model digital welfare state and is often seen as a leader in digitization in Europe.[9] It has a highly digitized public sector, whereby government decision-making utilizes data-driven technologies, service delivery and communication, with residents predominantly relying on information technologies to access essential public services. The population, meanwhile, has a high level of digital literacy.[10]

Denmark's transition to a digital welfare state and its implementation of algorithmic governance systems is primarily driven by the government's efforts to streamline administrative tasks and increase the effectiveness and efficiency with which welfare and other essential public services are delivered.[11]

In 2012, the Danish government claimed that the establishment of Udbetaling Danmark (UDK), an authority set up to centralize the payment of social benefits, would enable the government to save 35% in administrative costs.[12]

The national Danish digitization agenda is informed by the government's need to capture, analyse and share data to facilitate the use of automated decision-making systems which are framed as crucial components of governing domains of social life, such as, detecting fraud in tax returns and social benefits to ensure that "underserving" groups do not have access to benefits or the use of predictive scoring to estimate the likelihood of child abuse occurring.[13]

While efforts to reduce administrative costs in delivering welfare payments may be a legitimate goal, the introduction of digital technologies is taking place in the context of highly politicized narratives that benefit fraud is out of control.[14] This mirrors trends in other countries, where austerity efforts have also informed the welfare policies of other states in Europe and beyond, and therefore also inform the ways in which technologies are adopted and deployed in this context.[15] The former UN Special Rapporteur for extreme poverty noted in 2019 that:

"the digitization of welfare systems [globally] has been accompanied by deep reductions in the overall welfare budget, a narrowing of the beneficiary pool, the elimination of some services, the introduction of demanding and intrusive forms of conditionality, the pursuit of behavioural modification goals, the imposition of stronger

---

[6] Sandra Wachter and others, "Counterfactual explanations without opening the black box: Automated decisions and the GDPR", 2017, Harvard Journal of Law and Technology, Volume 31, Issue 2; Michael Veale and Irina Brass, "Administration by algorithm? Public management meets public sector machine learning", in Karen Yeung and Martin Lodge (editors), *Algorithmic Regulation*, 2019.

[7] Herbert Obinger and others, "Denmark: The survival of a social democratic welfare state", in T*ransformations of the Welfare State: Small States, Big Lessons*, 2010; Gabriel Geiger, *How Denmark's Welfare State Became a Surveillance Nightmare*, 2023, https://www.wired.com/story/algorithms-welfare-state-politics/

[8] OECD, "Social spending", https://www.oecd.org/en/data/indicators/social-spending.html?oecdcontrol-38c744bfa4-var1=OECD%7CAUS%7CAUT%7CBEL%7CCAN%7CCHL%7CCZE%7CDNK%7CEST%7CFIN%7CFRA%7CDEU%7CGRC%7CHUN%7CISL%7CIRL%7CISR%7CITA%7CJPN%7CKOR%7CLVA%7CLTU%7CLUX%7CMEX%7CNLD%7CNZL%7CNOR%7CPOL%7CPRT%7CSVK%7CSVN%7CESP%7CSWE%7CCHE (accessed on 02 October 2024).

[9] European Commission, *The Digital Economy and Society Index (DESI) 2021,* 12 November 2021, https://digital-strategy.ec.europa.eu/en/news/digital-economy-and-society-index-2021 p. 4;
Minister of Digitalization - Committee Hearing on Udbetaling Danmark 19 April 2023; Rikke Frank Jørgensen, "Data and rights in the digital welfare state: the case of Denmark" (previously cited).

[10] Rikke Frank Jørgensen, "Data and rights in the digital welfare state: the case of Denmark" (previously cited).

[11] Jannick Schou and Morten Hjelholt, *Digitalization and Public Sector Transformations*, 2018; Rikke Frank Jørgensen, "Data and rights in the digital welfare state: the case of Denmark" (previously cited).

[12] Henning Jensen (2012), "Municipalities warn: Loss of millions due to large-scale operations", 22 March 2012 https://nyheder.tv2.dk/2012-03-22-kommuner-advarer-milliontab-ved-stordrift (in Danish); Nicolas Kayser-Bril, "In a quest to optimize welfare management, Denmark built a surveillance behemoth", 2020, https://algorithmwatch.org/en/udbetaling-danmark/

[13] Rikke Frank Jørgensen (2021), 'Data and rights in the digital welfare state: the case of Denmark,' Information, Communication and Society and Brigitte Alfter (2018), "Denmark." In Automating Society: Taking Stock of Automated Decision-Making in the EU, edited by M. Spielkamp. https://algorithmwatch.o rg/wp-content/uploads/2019/01/Automating_Societ y_Report_2019.pdf.

[14] Gabriel Geiger, *How Denmark's Welfare State Became a Surveillance Nightmare* (previously cited); "Knowledge of social security fraud and wrong payments", February 2014, Annika Lindberg, *The production of precarity in Denmark's asylum regime*, 2020, Zeitschrift für Sozialreform, Volume 66, Issue 4, 2020

[15] Lina Dencik and Anne Kaun, "Datafication and the Welfare State," 2020, Global Perspectives, Volume 1, Issue 1; Amos Toh, "The disastrous roll-out of the UK's digital welfare system is harming those most in need", 10 June 2019, https://www.hrw.org/news/2019/06/10/disastrous-roll-out-uks-digital-welfare-system-harming-those-most-need
Rikke Frank Jørgensen, "Data and rights in the digital welfare state: the case of Denmark" (previously cited); Helle Zinner Henriksen, "One step forward and two steps back: E-government policies in practice", in J. Ramon Gil-Garcia and others (editors), *Policy Analytics, Modelling, and Informatics*, 2018, https://doi.org/10.1007/978-3-319-61762-6_4

sanctions regimes and a complete reversal of the traditional notion that the State should be accountable to the individual."[16]

Governments are increasingly deploying new technologies and administrative practices for fraud-control purposes in the delivery of welfare. Authorities often use contested claims regarding the scale of social security fraud to justify the implementation of fraud-control measures that drive a reduction in social benefits spending, as well as to justify over-broad and discriminatory surveillance of benefits claimants.[17]

This report presents the findings of Amnesty International's research on the Danish government's use of fraud-control algorithms to inform the distribution of social benefits through UDK, which is a public authority, and Arbejdsmarkedets Tillægspension (ATP), a private company that has a mandate from the Danish government to administer social benefits on behalf of UDK.[18] This report focuses on the use of fraud-control models in the distribution of social benefits and the human rights impacts resulting from the use of these systems.

3.1 USE OF FRAUD-CONTROL ALGORITHMS BY UDBETALING DANMARK (UDK)

The public authority UDK was established in 2012 through the Udbetaling Danmark Act to centralize the distribution of benefits under a single authority to improve "efficiency and more uniform case processing".[19] UDK has become a cornerstone of the Danish welfare state and is responsible for paying out many social security benefits[20] including child support, pensions, maternity and paternity benefits, housing benefits, unemployment benefits, study grants and sick pay benefits. During a meeting of the Digitization and IT Parliamentary Committee[21] held in Copenhagen in April 2023 to discuss the data and algorithmic practices of UDK, the Minister for Digitization reported that, in 2021 alone, UDK had paid out around DKK 241 billion (about EUR 32.3 billion)[22] to approximately 2.4 million benefit recipients.[23] As of 2019, UDK was reported to be using about 60 different AI and ML algorithms to identify people who were supposedly highly likely to be fraudulently receiving benefits.[24]

Previous case studies of the deployment of automated or semi-automated decision-making tools in Denmark have highlighted the potential for such systems to violate the rights to privacy and non-discrimination.[25] For example:

1. The Gladsaxe model, piloted in 2018, used an ML model that combined data related to unemployment, health care and social conditions to analyse more than 200 risk indicators and attempted to predict children's risk of vulnerability due to social circumstances. It faced significant public backlash due to its invasion of people's privacy,[26] and was discontinued in 2019.
2. The STAR algorithm, introduced prior to 2019, attempted to predict job seekers' risk of long-term unemployment. The algorithm included the variable "origin" and was found to be discriminatory by a

[16] UN Special Rapporteur on extreme poverty and human rights, *Digital Welfare States and Human Rights*, 11 October 2019, UN Doc. A/74/493, para. 5.
[17] Privacy International, "Stage 3 - The policing of social benefits: punishing poverty", 7 August 2019, https://privacyinternational.org/node/3114
Dean Herd and Andrew Mitchell, "Cutting caseloads by design: The impact of the new service delivery model of Ontario Works", 2003, Canadian Review of Social Policy, Volume 51.
[18] Interviews with Udbetaling Danmark officials on 11 January 2024 and 23 November 2023; Birgitte Arent Eiriksson, "Udebetaling Danmark's systematic monitoring", 2019, https://justitia-int.org/wp-content/uploads/2019/07/Analyse-Udbetaling-Danmark-systematiske-overva%CC%8Agning.pdf (in Danish); Marya Akhtar and others, "When algorithms handle cases – Rights and legal certainty in the use of profiling models by public authorities", in Marya Akhtar and others (editors), *Når Algoritmer Sagsbehandler*, 2021 (in Danish).
[19] FOI request responses from the Ministry of Employment, the government agency that supervises Udbetaling Danmark's Board of Directors, 4 December 2023; Interview with Udbetaling Danmark officials on 23 November 2023.
[20] ATP, "Udbetaling Danmark", https://www.atp.dk/en/our-tasks/processing-welfare-benefits/udbetaling-danmark (accessed on 3 October 2024).
[21] Danish Parliament, "The Digitalisation and IT Committee", https://www.thedanishparliament.dk/en/committees/committees/diu#:~:text=The%20Digitization%20and%20IT%20Committee%20addresses%20any%20topic%20associated%20with,Artificial%20Intelligence)%20and%20IT%20security (accessed on 3 October 2024).
[22] Exchange rates for this report taken as 1 Danish Kroner to 0.13 Euros (as of June 2021).
[23] Minister of Digitalization - Parliamentary Committee Hearing, 19 April 2023.
[24] Marya Akhtar and others, "When algorithms handle cases" (previously cited).
[25] Brigitte Alfter, 2020 "Denmark" in Fabio Chiusi and others (editors), *Automating Society: 2020 Report*, October 2020, https://automatingsociety.algorithmwatch.org/report2020/denmark/
[26] Rikke Frank Jørgensen, "Data and rights in the digital welfare state: the case of Denmark" (previously cited).

journalist in collaboration with academics from Copenhagen University. After a public discussion in 2019, it was discontinued.[27]

Despite such cases, UDK has continued to deploy data-driven solutions in the form of predictive analytics tools.[28] Predictive analytics tools use data, statistical modelling and ML to predict future outcomes and trends. Within the social security context, UDK draws on insights from historical or current data to predict which beneficiaries are at higher risk of committing fraud or error. Previous investigations and studies have highlighted the human rights violations and risks of fraud control algorithms and tools deployed in other countries, for example:

1. In 2021, when researching fraud detection in childcare benefits payments in the Netherlands, Amnesty International found that one of the "risk factors" that the algorithmic system adopted was whether the applicant had Dutch nationality. Consequently, people of non-Dutch nationalities received higher risk scores meaning they were more likely to have their benefits suspended and be subject to investigation for fraud. 39 This pushed many families into serious financial difficulties, including debt and bankruptcies. Many people were evicted from their homes when they could no longer afford their rent. Some people also reported suffering serious stress, which impacted their mental health. The algorithmic system behind the discriminatory fraud detection was later rolled back by the Dutch government, and a scheme was put in place to compensate people with a fixed amount regardless of their individual assessments. The use of an individual's nationality as a "risk factor" also shows the discriminatory assumptions held by the designer, developer and/ or user of the system that people of certain nationalities would be more likely to commit fraud or crime than people of other nationalities[29]
2. In 2023, Lighthouse Reports published an investigation on a fraud control algorithm deployed by Rotterdam. From 2017 to 2021, the city used a machine learning model to flag welfare recipients who may be engaged in "illegal" behaviour (cheating the welfare system). The investigation found the system discriminated based on ethnicity, age, gender, and parenthood. It also revealed evidence of fundamental flaws that made the system both inaccurate and unfair.[30]

Amnesty International's research in this report expands on previous research on UDK by organizations such as the Danish Institute for Human Rights, Justitia, and Lighthouse Reports on UDK's use of fraud-detection algorithms for the distribution of social benefits.[31] It also builds on previous Amnesty International research on automation and digitalization in the Netherlands, India and Serbia, and the resulting human rights risks and impacts.[32]

3.2 HOSTILE LAWS, PRACTICES AND ATTITUDES AGAINST MARGINALIZED GROUPS IN DENMARK

Although technology used in the public sector is often presented as objective and unbiased, it is virtually impossible to create a value-neutral technology. This is because technologies are designed within and introduced into societies that already contain social, political and structural discrimination. Technologies, therefore, inevitably reflect the underlying biases and worldviews of the people who built them. Introducing technology into social protection systems can have unpredictable and unintended consequences for individuals. Such impacts can also vary widely depending on whether those individuals are already subject to systemic and intersectional forms of discrimination and marginalization.

In the case of Denmark, its social security system exists in an already hostile environment for migrants, people who have been granted refugee status in Denmark and racialized groups more broadly, that both reflects and encourages discrimination against individuals based on their race, ethnicity, migration status,

[27] Catherine Seidelin, "Auditing risk prediction of long-term unemployment", 2022, Proceedings of the ACM on Human-Computer Interaction, Volume 6.
[28] Evidence from UDK presentation detailing the historical timelines for the introduction of technology to social security administration in Denmark, alongside information and context of four fraud control models deployed. Given to Amnesty International on 9 January 2024.
[29] Amnesty International, *Xenophobic Machines* (previously cited);
[30] Gabriel Geiger, *Inside the Suspicion Machine, 2023,* https://www.lighthousereports.com/investigation/suspicion-machines/
[31] Gabriel Geiger, *How Denmark's Welfare State Became a Surveillance Nightmare* (previously cited); Rikke Frank Jørgensen, "Data and rights in the digital welfare state: the case of Denmark" (previously cited); Birgitte Arent Eiriksson, "Udebetaling Danmark's systematic monitoring" (previously cited).
[32] Amnesty International, *Xenophobic Machines* (previously cited); Amnesty International, "Trapped by automation: Poverty and discrimination in Serbia's welfare state" (previously cited); Amnesty International, "India/global: New technologies in automated social protection systems can threaten human rights", 29 April 2024, https://www.amnesty.org/en/latest/news/2024/04/india-global-new-technologies-in-automated-social-protection-systems-can-threaten-human-rights/

and religion. This hostile environment is reflected in public attitudes about race and cultural superiority, and political discourses or communications by politicians on welfare in Denmark.[33] publicly stated: "Too many people have come to Denmark and gone around on social welfare for many years without working. We cannot accept this."[34] Such attitudes and narratives, as academic studies on social welfare and migrant control in Denmark show, often dangerously and falsely pit "hard-working" Danish families against migrants or migrant families. They do so by contending that the welfare system is too generous towards migrants, creating an incentive for them to come to Denmark, and that migrants are "lazy", "undeserving of benefits", and prone to commit welfare fraud.[35]

This hostile environment for migrants and people who have been granted refugee status in Denmark is also evidenced by the enactment of restrictive and discriminatory laws and policies. This includes laws that allow for the differential allocation of child and early retirement pension benefits in favour of ethnic Danes through the imposition of lengthy and disproportionate residency requirements. In addition, the controversial "jewellery law," which came into effect in February 2016, gives Danish authorities the power to search refugees and asylum seekers from the Middle East and North Africa region, who are often fleeing war and persecution, and confiscate their cash, jewellery and other valuables above DKK 10,000 (about EUR 1,340). [36] The Danish government claimed this was to ensure that "those seeking asylum are treated in the same way as citizens by expecting them to contribute to their own support rather than relying on state hand-outs".[37] Ukrainian refugees arriving from 2022, however, were reportedly exempted from this law.[38]

Another stark example of restrictive and discriminatory laws includes those passed by successive Danish governments since 1994, enacting six different "ghetto law packages" to "reduce the concentration of non-Western immigrants and descendants" in neighbourhoods identified as "ghettos".

"Ghetto" laws and policies are emblematic of how Danish authorities denote differences between groups and promote "othering" through the classification of minority groups as "others" because they are "non-Western" migrants and their descendants.[39] Statistics Denmark, the government authority responsible for creating statistics on Danish society, defines a "Western" person as someone born in any of the "28 EU countries and Andorra, Iceland, Liechtenstein, Monaco, Norway, San Marino, Switzerland, Vatican State, Canada, USA, Australia and New Zealand".[40] An "immigrant" is defined as "a person born abroad whose parents are both (or one of them if there is no available information on the other parent) foreign citizens or were both born abroad". A "descendant" is defined as "a person born in Denmark whose parents (or one of them if there is no available information on the other parent) are either immigrants or descendants with foreign citizenship".[41] These categorizations are not neutral ways to organize data as they are based on prevalent racialized attitudes and norms and can exacerbate discrimination on the basis of ethnic origin and nationality.

Former Prime Minister Løkke Rasmussen, in his 2010 opening speech to the Danish parliament (*Folketinget*), declared that "a series of holes has appeared in the map of Denmark. Places where Danish values are clearly no longer upheld". He went on to state that "the government [had] identified 29 such ghetto areas with particularly great challenges… areas where a large part of the residents are out of work. Where many criminals live. And where many Danes with an immigrant background live". He called for

---

[33] Teun A. van Dijk, "What is political discourse analysis?", 2013, https://e-l.unifi.it/pluginfile.php/909651/mod_resource/content/1/Van%20Dijk%20Waht%20is%20political%20discourse%20analysis.pdf, p. 2.
[34] Ritzau/The Local, "Denmark cuts basic benefit for 10,000 unemployed immigrants", 2023, https://www.thelocal.dk/20231013/denmark-cuts-basic-benefit-for-10000-unemployed-immigrants
[35] Annika Lindberg, "The production of precarity in Denmark's asylum regime", 2020, Zeitschrift für Sozialreform, Volume 66, Issue 4, 2020; Benjamin Leruth and others, "Categorizing discourses of welfare chauvinism: Temporal, selective, functional and cultural dimensions", 2024, Journal of European Social Policy, Volume 34, Issue 2; Edward Koning (ed.), *The Exclusion of Immigrants from Welfare Programs: Cross-National Analysis and Contemporary Developments*, 2022.
[36] Euro-Mediterranean Human Rights Monitor, "Denmark: Exempting Ukrainians from jewellery law while applying it to others is outright discrimination", 15 March 2022, https://euromedmonitor.org/en/article/4963/Denmark:-Exempting-Ukrainians-from-jewelry-law-while-applying-it-to-others-is-outright-discrimination
[37] Amnesty International, "Denmark: We'll take your valuables but not your family", 27 January 2016, https://www.amnesty.org.uk/blogs/yes-minister-it-human-rights-issue/denmark-take-your-valuables-not-your-family
Euro-Mediterranean Human Rights Monitor, "Denmark: Exempting Ukrainians from jewellery law while applying it to others is outright discrimination" (previously cited).
[38] Euro-Mediterranean Human Rights Monitor, "Denmark: Exempting Ukrainians from jewellery law while applying it to others is outright discrimination" (previously cited).
[39] Hettie O'Brien, "If you think Denmark is all Borgen and social equality, take a look at its awful 'ghetto' law", 27 June 2022, https://www.theguardian.com/commentisfree/2022/jun/27/denmark-ghetto-law-eviction-non-western-residents-housing-estates
[40] Statistics Denmark, "Documentation of statistics for immigrants and descendants 2017 Month 01", 2017, https://www.dst.dk/en/Statistik/dokumentation/documentationofstatistics/immigrants-and-descendants--discontinued-/statistical-presentation
[41] Statistics Denmark, "Documentation of statistics for immigrants and descendants 2017" (previously cited).

decisive action, "to put an end to a misguided tolerance of the intolerance that prevails in parts of the ghettos [where] Danish values are not fully established".[42]

The government has attempted to justify the creation of "ghetto" policies and the surveillance of groups identified as living in areas classified as "ghettos" on the alleged grounds that, among other things, so-called "parallel societies" are a financial burden and a security concern, and that migrants neither participate in the labour market nor integrate into Danish society.[43]

Subsequently, in 2018, the Danish Parliament implemented a law amending the Social Housing, Renting Social Housing, and the Rent Act – known as L38 or the "ghetto package". The purpose of enacting the law was to change the composition of residents in areas classified as "vulnerable areas", "ghettos" or "hard ghettos"[44] through demolition and/or privatization of social housing.[45] According to the explanatory remarks on the package, the implementation of L38 will entail the privatization or demolition of approximately 11,000 social welfare homes meant for families. Several social housing associations stated that it is highly unlikely that it will be possible to procure necessary alternative affordable housing for the people evicted from their original housing.[46] Amnesty International stated in its submission to the UN's Universal Periodic Review (UPR) of Denmark in 2021 that this would lead to the eviction of tenants, rendering them homeless and infringing upon their right to adequate housing.[47]

"Ghetto" laws and policies are emblematic of how Danish authorities denote differences between groups and promote "othering". In 2021, the UN Committee on the Elimination of Racial Discrimination (CERD Committee) criticized the use of the terms "Western" and "non-Western" in the package of laws previously known as the "ghetto package" as having a discriminatory impact on ethnic minorities.[48] The CERD Committee stated that there was a "discriminatory ethnic and racial element to these laws, which can result in stigmatisation in various areas of life, such as employment, housing, and access to services", contrary to Articles 3 and 5 of the Convention.[49] In 2019, the UN Committee on Economic, Social and Cultural Rights recommended that Denmark "adopt a rights-based approach" in its efforts to address residential segregation and to enhance social cohesion. In this regard, it recommended that Denmark remove the definitional element of a "ghetto" with reference to residents from "non-Western" countries, which it found to be discriminatory on the basis of ethnic origin and nationality, and repeal all provisions that have a direct or indirect discriminatory effect on migrants and people who have been granted refugee status in Denmark.[50]

It is in this existing context of a hostile environment for already marginalized groups that UDK/ATP designs fraud control algorithms that reflect the norms of the majority or dominant groups in Denmark. (See Chapter 8).

This report highlights ways in which human rights violations created by algorithmic systems, coupled with traditional surveillance mechanisms present in UDK's benefits system, occur in the context of discrimination that is structural in nature or embedded within existing structures or institutions – laws, rules, policies, attitudes, norms and values – that drive Danish authorities to distinguish between different groups in Denmark in their fraud detection efforts. This report illustrates how these hostile laws, rules, policies, attitudes, norms and values are embedded in the fraud-control algorithms used by UDK to identity people for fraud investigations.

---

[42] Lars Løkke Rasmussen, Speech at the opening of the Danish Parliament on Tuesday 5 October 2010, https://www.stm.dk/statsministeren/taler/statsminister-lars-loekke-rasmussens-tale-ved-folketingets-aabning-tirsdag-den-5-oktober-2010/

[43] The former Danish Prime Minister, Lars Løkke Rasmussen, stated in a New Year's speech in 2018:
"Parallel societies are a great burden on the cohesion of society and for the individual… it is a financial burden when citizens do not participate in the labour market. The latest report from the Ministry of Finance shows that immigrants and descendants with a non-Western background cost Denmark DKK 36 billion in 2015. Danish taxpayers could have saved almost DKK 17 billion if non-Western immigrants had been employed to the same extent as Danes. We must once and for all tackle the very large task of integration, where a group of immigrants and descendants have not embraced Danish values and isolate themselves in parallel societies."
Lars Løkke Rasmussen, *Prime Minister Lars Løkke Rasmussen's New Year Address 1 January 2018, 2018:* https://english.stm.dk/the-prime-minister/speeches/prime-minister-lars-lokke-rasmussen-s-new-year-address-1-january-2018/

[44] Denmark, Act on Social Housing (LBK nr 119 of 01/02/2019), https://www.retsinformation.dk/eli/lta/2019/119, section 61a.

[45] Denmark, Act on Social Housing (previously cited), sections 27c, 28(3) and 168a.

[46] Housing associations critical of the bill include: Lejerbo, AKB, Øst-jysk Bolig, AAB, Civica, FAB. Danmarks almene Boliger. Amnesty International, *Denmark: Human Rights Must be Ensured for All: Amnesty International's Submission for the Universal Periodic Review (UPR) of Denmark, 38th Session of the UPR Working Group* (Index: EUR 18/3229/2020), 15 October 2020,

[47] Amnesty International, *Denmark: Human Rights Must be Ensured for All: Amnesty International's Submission for the Universal Periodic Review (UPR) of Denmark, 38th Session of the UPR Working Group* (Index: EUR 18/3229/2020), 15 October 2020, https://www.amnesty.org/en/documents/eur18/3229/2020/en/, p. 6; Section 61a(1-4) of the Social Housing, Renting Social Housing, and the Rent Act (named L38 or the "ghetto package") defines a "vulnerable area" as an area which meets at least two of the following criteria: an area composed of a large number of residents with higher-than-average rates of unemployment, criminal convictions, low education (primary education), and low incomes. Section 61a(5) defines a "ghetto" as "a residential area where the proportion of immigrants and descendants from non-Western countries exceeds 50 per cent, and where at least two of the criteria [outlined above under section 61a(1-4)] are met". Section 61a4(4) defines a "hard ghetto area" as "a residential area that has fulfilled the conditions in subsection (2) for the past 4 years".

[48] Amnesty International, *Denmark: Human Rights Must be Ensured for All* (previously cited), p. 6; UN CERD Committee, Concluding Observations: Denmark, 1 February 2022, UN Doc. CERD/C/DNK/CO/22-24.

[49] CERD Committee, Concluding Observations: Denmark, 1 February 2022 (previously cited).

[50] UN Committee on Economic, Social and Cultural Rights (CESCR), Concluding Observations: Denmark, 12 November 2019, UN Doc. E/C.12/DNK/CO/6 (2019), para 52(a) and (d).

4. METHODOLOGY

Amnesty International Secretariat collaborated with Amnesty Denmark on the research since 2022. To determine whether the UDK case study was a suitable case for research, Amnesty International Secretariat held consultative meetings with Amnesty Denmark and other local partners in Denmark. The research has been led by the Amnesty International Secretariat's Technology and Human Rights team. Amnesty International worked jointly with Amnesty Denmark throughout the course of the project.

This research investigates the human rights impact of UDK's social benefits system. It focuses on the following main areas:

a. UDK's use of fraud-control algorithms, which we argue are surveillance tools, to inform the distribution of social benefits and the impact this has on low-income and racialized groups, people with disabilities, and people with refugee status and migrants.

b. UDK and municipalities' use of analogue or traditional forms of surveillance (such as regular assessments and home visits from officials such as social workers) to inform fraud control in the distribution of social benefits.

c. Ways in which UDK's digitization practices enable forms of digital exclusion and forced inclusion.

d. The laws and policies which govern UDK's practices and administration, with a particular focus on transparency and oversight

Amnesty International undertook research for this report between May 2022 and April 2024 in several stages using a combination of desk research, qualitative interviews, focus groups, a survey, and technical research methods.

Desk research included a review of laws on the establishment of UDK and ATP, laws on social benefits in Denmark; relevant international human law instruments and standards; relevant reports and studies by the UN, media, academics and civil society organizations; and a review of government responses to freedom of information requests (FOIs) submitted by Amnesty International.

As part of its qualitative research, Amnesty International conducted interviews and focus group discussions with government officials, academics, journalists, community leaders and affected individuals.

The technical research methods employed included a combination of interviews with officials and the filing of FOIs to gather data and documentation on the technical infrastructure and algorithms deployed by UDK (details provided in Table 1). This included scrutiny of any documentation provided, and discussion of statistical approaches taken by UDK data scientists. Through FOIs, Amnesty International also attempted to collect statistics and empirical data to test whether the algorithms in question are discriminatory (known as disparate impact testing).

During the first stage of the research from May 2022 to April 2023, Amnesty International conducted desk research to investigate whether UDK's practices raised human rights concerns. At this stage, Amnesty International reviewed relevant secondary literature including reports, articles and documents on the UDK benefits system and its use of fraud-control algorithms to detect social benefits fraud. These sources were published by various organizations including, among others, the Danish Institute for Human Rights, Lighthouse Reports and Algorithm Watch. Amnesty International also reviewed documentation on UDK's fraud-control algorithms shared by journalists from Lighthouse Reports. Amnesty International then held a total of nine consultative meetings with nine relevant stakeholders including academics, journalists and

leaders of civil society organizations working with marginalized groups in Denmark to understand the human rights impacts of UDK's system. These meetings took place between June and August 2022.

From September 2023 to January 2024, during the second stage of the research, Amnesty International conducted 34 semi-structured interviews, both online and in-person, with government officials, parliamentarians, academics, journalists and affected individuals and groups, as well as two focus group discussions with affected groups. The interviews and focus group discussions were conducted in person in the Danish capital, Copenhagen, in January 2024. They were conducted in Danish, Arabic and English, with translation and interpretation support where required.

Amnesty International further conducted nine interviews with a total of 12 government officials responsible for implementing and regulating UDK/ATP as follows:

- Two interviews with UDK/ATP officials (with a total of four officials attending the interviews, including officials from the control unit, officials responsible for external relations at UDK, and UDK in-house data scientists);
- One interview with a case manager in Copenhagen Municipality's fraud-control unit;
- One interview with a control officer in Aalborg Municipality's fraud-control unit;
- One interview with two officials from the Danish Appeals Board, which hears appeals on UDK decisions;
- One interview with the Danish Data Protection Authority;
- One interview with the Danish Business Authority, the entity responsible for the Central Business Register in Denmark which contains information about companies;
- One interview with a social worker in Copenhagen Municipality;
- One interview with a consultant at Copenhagen Municipality.

In addition to conducting interviews with government officials and regulators, Amnesty International also conducted an interview with a Member of Parliament for Socialistisk Folkeparti – SF (Green Left, which has previously raised concerns in parliament on the risks of UDK's practices) and the Chair of the Parliamentary Committee for Digitalization and IT, and an interview with a former social worker in Copenhagen municipality. We also interviewed an official from the Danish Institute for Human Rights, Denmark's national human rights institution.

To highlight voices of marginalized groups affected by UDK's practices, Amnesty International conducted two focus group discussions and six interviews with affected individuals who receive benefits via UDK. The focus groups were carried out in partnership with Dansk Handicap Foundation and SoS Racisime. Participants in the focus groups lived in Copenhagen, specifically Hovedstaden in Greater Copenhagen, and the region of Syddanmark (Southern Denmark). Interview participants were from Copenhagen, Odense and the Lyngby-Taarbæk and Kobenhavn municipalities.

Amnesty International conducted two separate focus groups with people with disabilities at the Dansk Handicap Foundation. The first focus group had three participants and the second had nine participants, all of whom live with physical and/or cognitive disabilities. Of the 12 focus group participants, six were women and six were men. One participant was under 50 years old; the other 11 were over the age of 50.

Amnesty International conducted interviews with six women benefits recipients with a refugee background, who now have either had residency or citizenship in Denmark. We recruited these participants in partnership with Mino Danmark, an organization that works with marginalized communities in Denmark. Two of the recipients were originally from Syria, three from Iraq, and one from Lebanon. Three of the women were over 50 years old and three were between 35 and 45 years of age.

Amnesty International interviewed seven community leaders from civil society groups. Two were from SoS Racisme Danmark, and there was one representative each from Dane Age Association, Mino Danmark, Refugees Welcome Denmark, National Organization of Women's Shelters (LOKK), and the Center for Muslimers Rettigheder i Danmark (CEDA). These interviews were conducted to understand how the lived experiences of older people, women, people of African descent and people from the Middle East and North Africa region are affected by UDK's system.

Amnesty International also partnered with the LOKK, an umbrella non-profit organization and trade association that represents 46 women's shelters around Denmark, to design a survey to study the impact of UDK's system. LOKK conducted the survey with caseworkers in 45 of their shelters in October 2023 on

behalf of Amnesty International and received responses from 25 caseworkers in 25 shelters. Among other schemes, fraud-control algorithms are used in social security schemes that affect women, such as maternity benefits. Therefore, the survey sought to understand whether women living in crisis shelters because of intimate partner violence:

a. Have access to the technology required to apply for benefits from UDK (including maternity, child and youth benefits or other benefits). This includes access to the internet, computers, MitID (a digital identity system that residents in Denmark use to identify themselves to access public and private sector services) and NemID (a key card used to access public and private sector digital services, which was discontinued in October 2023);[51]

b. Have been accused of fraud in relation to claiming maternity benefits;

c. Are refused benefits by UDK because of digitization of the social benefits system.

Amnesty International interviewed six academics from the IT University of Copenhagen, Copenhagen Business School (Department of Business, Humanities and Law), University of Copenhagen, Brunel University, Birmingham University, and the German Centre for Integration and Migration Research (DeZIM) to understand the current laws, policies, practices and narratives around welfare and "ghetto laws", as well as UDK's data and fraud-control practices.

Additionally, Amnesty International researchers met and conducted unstructured interviews with journalists from Lighthouse Reports and Politikken, both of whom had previously investigated UDK's data and fraud-control practices.

Amnesty International also filed FOI requests to the following authorities:

TABLE 1: FOI REQUESTS SENT BY AMNESTY INTERNATIONAL

NAME OF ENTITY TO WHICH AMNESTY INTERNATIONAL SENT FOIS	NATURE OF INFORMATION REQUESTED	DATE OF REQUEST	DATE OF RESPONSE
Danish Data Protection Authority	The authority's regulation of UDK's data practices	5 October 2023	7 November 2023
Danish Ministry of Employment	The ministry's supervisory role over UDK's Board of Directors	11 October 2023 and 25 March 2024	4 December 2023 and 8 April 2024
Copenhagen Municipality Fraud Control Unit	The role of Copenhagen Municipality's control units and data practices	25 March 2024	8 April 2024
Aalborg Municipality Fraud Control Unit units	The role of Aalborg Municipality's control units and data practices	25 March 2024	4 April 2024
Aarhus Municipality Fraud Control Unit units	The role of Aarhus Municipality's control units and data practices	27 March 2024	12 April 2024
Ishoj Municipality Fraud Control Unit units	The role of Ishoj Municipality's control units and data practices	27 March 2024	10 April 2024
UDK /ATP	UDK/ATP's data practices and collaboration with NNIT A/S (NNIT)	25 March 2024	19 April 2024
UDK/ATP	Documentation on the design of fraud-control algorithms and statistics on outputs of algorithmic models, including risk designations and demographic characteristics of welfare beneficiaries	25 March 2024	26 April 2024

[51] NemID, "NemID is closed from 31 October 2023", https://lifeindenmark.borger.dk/apps-and-digital-services/nemid (accessed on 31 July 2024).

On 7 September 2023, Amnesty International obtained from Copenhagen Municipality a template of the letters the municipality sends to people who have been identified for fraud investigations as a result of Denmark's use of fraud-control algorithms, and a copy of a presentation from UDK during an in-person interview with the UDK project team at their offices on 11 January 2024.

To understand the role that private sector entities play in UDK's system, we conducted company searches on private sector companies engaged by UDK to distribute benefits and to design its fraud-control algorithms. In particular, we contacted the Danish Business Authority and the Danish Financial Supervisory Authority to obtain information on ATP, the company that delivers UDK's social benefit distribution remit and oversees the development of its fraud-control algorithms. We also conducted company searches through the Danish Business Authority's website on NNIT, which has been sub-contracted to develop some of UDK/ATP's fraud-control algorithms. Chapter 10 analyses the governance structure of ATP and the role of NNIT.

In preparation for this report, Amnesty International reviewed and relied on findings from prior FOI requests submitted by journalists requesting documentation on UDK's SPARK System.

Technical evaluations are critical to conducting assessments of algorithmic systems. They ideally rely upon sufficient access to all of the documentation, code and data (although some analysis can be conducted with access to only one or two of these elements). Access to the code and data has been consistently denied by UDK, including in response to Amnesty International's requests, under the justification that the data is sensitive, and information on the models would allow fraudsters too much insight into how UDK controls benefit distribution, allowing them to defraud the system.[52] In the absence of full documentation, Amnesty International has built an understanding of UDK's practices from multiple alternative sources.

UDK provided Amnesty International with redacted documentation on the design of some of the algorithmic systems in question. In addition, Amnesty International requested UDK to provide demographic data and outcomes for the people who are subject to the algorithmic models, which could be used to examine if the algorithmic systems for which we had documentation were discriminatory, either directly or indirectly. This was denied by UDK/ATP, citing the fact that they did not hold the demographic data requested, and that information on the cases classified as high-risk was consistently overwritten, meaning that historical data is not saved.

In this report, the names of some of the individuals who have shared their stories and experiences have been anonymized to protect their privacy and confidentiality.

Finally, Amnesty International shared the findings our research with UDK/ATP on the 17 October 2024 and the Ministry of Employment (the Danish Agency for Labour Market and Recruitment or STAR) on the 18 October 2024 and sought their written responses to specific allegations detailed in this report ahead of its publication. UDK responded to the allegations in the report on 30 October 2024 and 1 November 2024 while the Ministry of Employment responded to the allegations in the report on 1 November 2024. Amnesty International also wrote to the company NNIT on 23 October 2024 about their mention in this report and sought their responses to further questions. NNIT responded on 1 November 2024. All responses are reflected, where relevant, in the text of the report.

This research has encountered challenges which have restricted Amnesty International's ability to make a full assessment of the human rights implications raised by Udbetaling Danmark's use of fraud control algorithms to investigate benefits fraud. These challenges are as a result of the UDK/ATP's failure to provide Amnesty International with adequate documentation of its maternity, child and pensions models making it challenging to fully understand the fraud control systems used by UDK/ATP. Additionally, UDK/ATP claimed they could not provide demographic data alongside the risk designations of the people being assessed by the algorithms, owing to the fact UDK did not hold this data, making any bias or fairness testing challenging. Whilst the data requested is highly sensitive, and from a data protection perspective UDK deleting or not collating this preserves people's right to privacy, UDK/ATP should retain aggregate demographic statistics to allow for bias and fairness testing, which was the data Amnesty International requested in the FOI.

Furthermore, Amnesty International encountered challenges in identifying affected people who were prepared to share their experiences of being investigated for fraud by UDK because of a pervasive fear of backlash from the authorities for participating in the research.

[52] In January 2024, Amnesty International requested a collaborative audit to UDK data scientists which was rejected on these grounds in an email dated 2 Feb 2024. Amnesty International subsequently sent an FOI on 25 Mar 2024 requesting data and documentation on the fraud-control models; access to the former was denied and redacted information was provided on the latter.

Despite these challenges and the fear of retribution that many affected people and communities are living with, this research was only possible because of the participation of a huge number of partners and collaborators willing to speak up about UDK's systems. Amnesty International extends its deepest gratitude to everyone who participated in this research, in particular to those willing to share their stories, and to the Danish Institute for Human Rights, Dansk Handicap Foundation, SoS Racisme, Mino Danmark, LOKK, Lighthouse Reports, Refugees Welcome Denmark and the Centre for Muslimers Rettigheder i Danmark, among others.

5. OVERVIEW OF UDBETALING DANMARK'S FRAUD-CONTROL PRACTICES

Denmark's social protection scheme is vast, with roughly half of Danish residents receiving some form of social assistance from the state.[53] The government offers a multitude of social protection schemes. A non-exhaustive list of those relevant for this report can be found in Table 2 below.

While the process of administering and distributing these benefits varies from scheme to scheme, the ongoing management of cases and processing of applications can be conducted either by UDK or the municipality. This is the stage at which both UDK and municipalities introduce checks (referred to as "control" by UDK/ATP) to clamp down on "unauthorized benefits". These controls are for the purported aim of reducing or eliminating welfare fraud. The controls are generally split into three phases:[54]

- *Control step 1* is connected with the allocation of benefits and assesses whether the applicant is entitled to said benefit.
- *Control step 2* relates to ongoing case-management of select cases, where benefit recipients are followed up for statutory checks by caseworkers from UDK or the relevant municipality.
- *Control step 3* is triggered when there has been a question, or "wonder" (Danish: *undring*) that requires "in-depth control" in a particular case.

Control steps 1 and 2 are carried out by caseworkers based in the municipalities, while control step 3 is carried out by the control team, either at UDK/ATP or within the municipality. Control step 3 is the stage at which fraud investigators review and take on cases which are flagged as being at risk of fraud or error. Control step 3 is the main focus of this research.

Cases are selected for control step 3 through a variety of avenues, including tip-offs from a neighbour, social services, police or other authorities. Cases can also be selected via the use of fraud-control algorithms. These algorithms make risk assessments about beneficiaries and provide a list of those classified as presenting the highest risk of committing fraud to the respective control teams in UDK and the municipality.

While some social security schemes in Denmark are means-tested, in that beneficiaries must meet specific eligibility criteria, control step 3 and therefore the fraud detection models are all deployed post-hoc (after the person has begun receiving the social security payment and is therefore already deemed eligible). The fraud

[53] Some 2.4 million citizens, as per Minister of Digitalization – Parliamentary Committee Hearing of 19 April 2023, equates to roughly 50% of the 4.8 million adult population, https://www.dst.dk/en/Statistik/emner/borgere/befolkning/befolkningstal
[54] Information provided by Aarhus Municipality in response to an Amnesty International FOI request dated 12 April 2024.

detection models do not provide a simple database check of beneficiaries against eligibility criteria. Rather, they aim to predict how likely current social security beneficiaries commit fraud or error in their application.

TABLE 2: SOCIAL PROTECTION SCHEMES ADMINISTERED BY UDK[55]

SOCIAL PROTECTION SCHEMES	ENTITY WHICH ADMINISTERS CONTROLS
Family benefits, including: • Child and youth benefits (the "child cheque") • Ordinary child allowance payable to single parents • Extra child allowance payable to single parents • Advance maintenance payments (child support and alimony)	UDK
Sick leave benefits	Municipality
Maternity and paternity benefits	UDK
Pensions, including: • State pension • Pension supplement • Early retirement pension	 UDK UDK Municipality
Student benefit	UDK
Unemployment benefits	Municipality

5.1 UDK'S ADMINISTRATION, USE OF DATA AND ALGORITHMS

The Danish government has delegated public authority in the distribution of benefits to ATP, a company established as a self-governing institution under the ATP Act 1964.[56] Prior to 2012, ATP was responsible for processing pension payments. However, in 2012 the Danish parliament passed the Udbetaling Danmark Act which established the public authority UDK and, from 2012 to 2015, brought a selection of other social security schemes previously distributed by municipalities under the centralized control of UDK and by extension ATP, which provides "technical and administrative" assistance to UDK for social protection schemes that fall under within UDK's responsibilities.[57] Subsequently, the Udbetaling Danmark Act also gave UDK, and by extension ATP, the powers to extract large quantities of personal data of residents in Denmark, without their consent, and to carry out "register mergers" of databases or registers containing this data for the purposes of fraud control.[58]

These databases are either held by public authorities or are obtained by requesting data from foreign public authorities (where a Danish citizen is living abroad).[59] UDK/ATP established a Joint Data Unit tasked with developing data-driven fraud-control algorithms. The Joint Data Unit links or merges personal data collected and held by public authorities with private data and builds fraud control algorithms that can utilize this data to create a "*undringslisten*" or "wonderlist" of "questionable" scenarios and individuals who should be further investigated for potentially committing social benefits fraud.[60]

Table 3 below summarizes the kinds of data collected and merged by UDK/ATP from public authorities, which is then used to identify individuals who are flagged for further fraud investigations. This data, directly or through proxies (see Chapter 7), reflects protected characteristics, as defined in Article 9 of the GDPR and Article 21 of EU Charter of Fundamental Rights, including a person's racial or ethnic origin, health, and intimate details of a person's relationships, including marital status, their sexual life or sexual orientation.

[55] ATP, "Udbetaling Danmark" (previously cited).
[56] ATP, "About us", https://www.atp.dk/en/about-us (accessed on 3 October 2024).
[57] ATP, "Udbetaling Danmark" (previously cited).
[58] LBK no. 240 of 12/02/2021 (Applicable), Promulgation of the Act on Udbetaling Danmark.
[59] See: https://www.atp.dk/vores-opgaver/administration-af-velfaerdsydelser/udbetaling-danmark-internationalt
[60] Interview with UDK officials on 23 November 2023.

TABLE 3: GOVERNMENT DATABASES THAT ARE USED BY THE JOINT DATA UNIT FOR REGISTER MERGERS

CENTRAL CIVIL REGISTRATION SYSTEM (CPR)	Database that contains information on residence and residence changes, citizenship, place of birth, family relationships and circumstances, including marital status and information about household members
CENTRAL REGISTER OF BUILDINGS AND DWELLINGS (BBR)	Database that contains information on building and housing conditions of individuals
CENTRAL BUSINESS REGISTER (CVR)	Database that contains information about company ownership and the business relationships of individuals
INCOME DATA	Database that contains income data
R75	Database that contains tax information
REGION'S DATA	Database that contains health data
VAT	Database that contains Value Added Tax data
STAR DATA	Database that contains cash benefits and sickness benefits
SU DATA	Database that contains data on state education grants offered to students in youth and higher education in Denmark to cover living expenses
MOTOR VEHICLE REGISTER	Information on car ownership and use

In addition to the data collected and linked through the merging of the above registers, UDK and municipalities have access to data held by the Joint Data Unit Abroad.[61] The Joint Data Unit Abroad collects data on behalf of UDK and municipalities from foreign authorities where a resident has applied for or is in receipt of social benefits. Information collected includes data about a resident's foreign residence, information related to entry and exit to go abroad, marital status, children, real estate or vehicles abroad, and social benefits received abroad.[62]

Municipalities and UDK/ATP are also mandated under law to continually exchange information about residents receiving benefits and members of their households, without their consent. This includes information such as who receives benefits, "his/her spouse, cohabiting partner or presumed cohabitant, and other household members or presumed household members".[63] To conduct fraud investigations, municipality control units also have access to and rely on federal and local government databases that hold data on residents and data held by foreign authorities. For example, in response to Amnesty International's FOI request dated 25 March 2024, the Copenhagen Control Unit stated that, in order to conduct fraud investigations, it has access to and relies on the income and tax databases, the Alien (foreigners) Information Portal, and SAP and KMD cases systems which contain data on children in schools and childcare centres.[64] Aarhus Municipality's Control Unit stated that it has access to the Joint Data Unit Abroad.[65] Additionally, municipality control units can obtain data on "purely private affairs and other confidential information", such

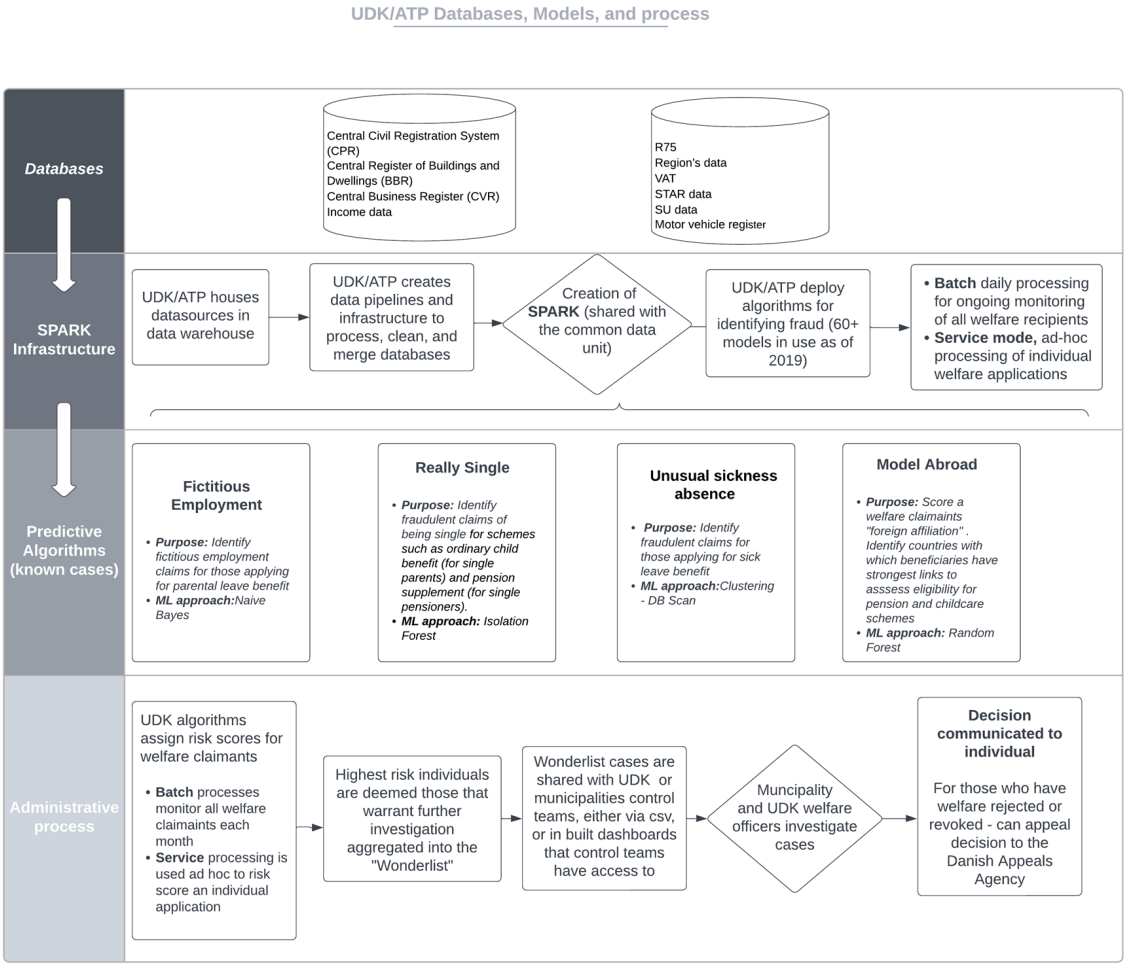
[61] FOI responses from Copenhagen Municipality Control Unit dated 8 April 2024, and Aarhus Municipality Control Unit dated 12 April 2024.
[62] UDK, "Common Data Unit Abroad", https://www.atp.dk/vores-opgaver/administration-af-velfaerdsydelser/udbetaling-danmark-internationalt, accessed on 18 May 2024.
[63] LBK no. 240 of 12/02/2021 (Applicable), Promulgation of the Act on Udbetaling Danmark, section 9.
[64] FOI response from Copenhagen Municipality dated 8 April 2024.
[65] FOI responses from Copenhagen Municipality Control Unit dated 8 April 2024, and Aarhus Municipality Control Unit dated 12 April 2024.

as medical transcripts from health care professionals, and financial information from private actors such as employers and financial institutions, as specified in Section 11a, of the Legal Security Act.[66]

After creating an "*undringslisten*" or "wonderlist" of fraud cases for investigation based on its fraud-control algorithms,[67] UDK/ATP's fraud control unit (the Joint Data Unit) shares the list with municipality fraud control units, where relevant, in order for municipalities to conduct further fraud investigations on the listed individuals.[68] Some municipalities can also access the list via the Joint Data Unit database.[69] To enable municipalities to conduct further fraud investigations, UDK/ATP shares the "wonderlist" or the predictions made by its algorithms (but not the internal workings of the models) with municipalities. Municipalities use this information to conduct further investigations of benefits applicants and recipients that UDK claims are at risk of committing benefit fraud.[70]

UDK uses a cloud-based infrastructure known as SPARK[71] to process the data and run the algorithms. Amnesty International's understanding of the UDK system is depicted in Figure 1 below, including the four predictive models.

FIGURE 1: A GRAPHICAL REPRESENTATION OF UDK CLOUD, DATABASE AND ALGORITHMIC INFRASTRUCTURE



[66] LBK nr 261 of 13/03/2024 – Act on Legal Security and Administration in the Social Area, cf. Consolidated Act No. 1109 of 24 August 2023.
[67] Interview with UDK officials on 23 November 2023.
[68] FOI responses from the Ministry of Employment dated 4 December 2023; interview with UDK officials on 23 November 2023; interviews with a Copenhagen Control Unit Official on 4 September 2023 and Aalborg Municipality Control Unit on 14 September 2023.
[68] LBK no. 240 of 12/02/2021 (Applicable), Promulgation of the Act on Udbetaling Danmark.
[69] Interview with Aalborg Municipality Control Unit, 14 September 2023.
[69] LBK no. 240 of 12/02/2021 (Applicable), Promulgation of the Act on Udbetaling Danmark.
[70] FOI responses from the Ministry of Employment dated 4 December 2023; interview with UDK officials on 23 November 2023; interviews with a Copenhagen Control Unit Official on 4 September 2023 and Aalborg Municipality Control Unit, 14 September 2023.
[71] Documentation on the SPARK cloud infrastructure provided to Amnesty International by journalists in October 2023.

5.2 FRAUD-CONTROL ALGORITHMS

As of 2019, UDK were using up to 60 different algorithms for fraud detection and other purposes. Amnesty International requested information on any algorithms used for fraud detection purposes in the domains of maternity and paternity benefits, pensions benefits, childcare benefits, student benefits and sick leave benefits. Through FOI requests, Amnesty International gained access to redacted documentation on four of the algorithms in use, which constitutes only a small number of the total models in use. To build an understanding of how they function and the context of their deployment, we have triangulated information from the redacted documentation with evidence gathered in two interviews with UDK and ATP legal counsel, data scientists and other staff, and two meetings with journalists.

The models are designed either to detect fraud for a particular welfare scheme (such as the "fictitious employment" algorithm, which is used in the maternity benefits domain) or they are used across welfare schemes to detect patterns that UDK believe are strong indicators of fraud. For instance, they use the "really single" algorithm, which attempts to predict a person's relationship status, in both the child benefits and pensions domains where single people are entitled to receive more money. Details on the algorithms, their intended purpose, the type of algorithmic system and the known inputs are included in Table 4 below.[72]

Information being redacted from the documents presents two key barriers to our understanding of the systems. First, many of the inputs (data points that are fed into the model) are redacted and others are difficult to interpret without further information on why they are included and how they are constructed. And second, information on the *weight* of each input is redacted. In ML, the weight of each input indicates their relative importance to the model. A high weight means an input plays a critical role in determining the risk classification assigned to a subject. By contrast, a weight of zero means the input has no effect on the risk score assigned.

TABLE 4: DETAILS ON KNOWN UDK FRAUD-CONTROL ALGORITHMS

ALGORITHM	PURPOSE	ALGORITHM AND DESCRIPTION	KNOWN INPUTS
"Fictitious employment"	**Retrospective control of maternity allowance[73]**	Supervised ML - Naïve Bayes algorithm[74] The model uses characteristics identified in roughly 30 known cases of fraudulent maternity benefit claims to predict the risk that new or current beneficiaries are claiming the benefit fraudulently.	• Evidence of a beneficiary failing to return to their job after the maternity leave. • Duration of the employment contract. • Timely registration of salary. • The company is eligible for refusion. • Salary increase prior to entering maternity-earning-period. • The salary rate paid to an employee. • Number of salary registrations by citizens. • The citizen has left Denmark. • The company is owned by family or family is a leader.

[72] FOI responses, including redacted documentation on the four models, from UDK officials dated 26 April 2024; UDK presentation and interview on 11 January 2024.
[73] "Retrospective" in this context, as outlined in section 5.1, highlights how the fraud control algorithms are introduced at control step 3, after an individual has received social benefits.
[74] Naive Bayes is a ML classifier, for more information please access https://towardsdatascience.com/naive-bayes-classifier-81d512f50a7c

"Unusual sickness absence"	**Retroactive control of sickness allowance**	Unsupervised ML – DBSCAN[75] The model uses a clustering approach to identify unusual or suspicious patterns of sick leave for beneficiaries claiming sick leave benefits.	• Inputs contain too much redaction to be included.
"Really single"	**Retrospec tive control of ordinary child allowance and pension supplement (for single pensioners).**	Unsupervised ML – Isolation forests[76] to detect anomalies The model employs an algorithm to identify outliers, or unusual applications, for benefits granted to beneficiaries that are single to determine whether this is their correct relationship status.	• Father new child: Time since father was single. • Income. • Is married or not. • Length of stay in area and country. • Lived with (partner). • Housing score: information on square meters of home and number of rooms. • Regional contact (unclear what this input measures).
"Model abroad"	**Control of undeclared departure**	Supervised ML – Naïve Bayes and Random Forest[77] The model creates a relative measure of beneficiaries' strength of "ties" or attachment to other countries, particularly for those outside of the EEA.	• Entry/exit. • Citizenship. • Unknown spouse. • Income. • Advance information. • Property. • Bank account. • Other unknown inputs.

In 2019 the UN Special Rapporteur on extreme poverty warned that digital welfare states were using digital technologies to address, among other things, social benefits fraud. The Special Rapporteur noted that: "systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish".[78] The Special Rapporteur acknowledged that welfare fraud is a major concern for governments around the world and can lead to loss of large sums of money (a concern that was also expressed by UDK/ATP officials during interviews[79]). However, the Special Rapporteur also noted that there was evidence that "the magnitude of these problems is frequently overstated and that there is sometimes a wholly disproportionate focus on this particular dimension of the complex welfare equation".[80]

This point was emphasized in 2019 by Privacy International, which noted that, although governments are increasingly investing in benefit fraud detection technology, "intentional, wrongful deception by social benefits claimants and recipients is generally extremely rare".[81] Privacy International has called for more

[75] DBSCAN is a ML clustering approach, for more information please access https://towardsdatascience.com/dbscan-clustering-explained-97556a2ad556
[76] Isolation forests are a ML approach used for anomaly detection – that is the task of identifying data points that are "very strange" compared to the majority of observations.
[77] Random Forests are a ML classification or regression approach, for more information please access https://towardsdatascience.com/understanding-random-forest-58381e0602d2
[78] UN Special Rapporteur on extreme poverty and human rights, Report, 15 February 2019, UN Doc. A/74/50, para. 3.
[79] In an interview with UDK officials on 11 January 2024, an official expressed the viewpoint that the UDK needs to control for benefits fraud because the Danish government pays large amounts of money in child benefits.
[80] UN Special Rapporteur on extreme poverty and human rights, *Digital Welfare States and Human Rights* (previously cited), para. 26.
[81] Privacy International, "Stage 3 - The policing of social benefits: punishing poverty" (previously cited).

scrutiny of situations that may be labelled as fraud because they may not involve an intentional act of fraud on the part of a beneficiary but may be a result of, for example, automated systems incorrectly processing case files or situations where a person is unable to produce a document.[82]

In response to Amnesty International's findings that are contained in this section, UDK stated that it is not making automated decisions to the detriment of the citizens based on its use of algorithmic models. UDK states this would be against the law and that "any action [by an algorithm] is contingent on a caseworker reviewing and processing the individual case in accordance with legislation, including the Public Administration Act."[83]

As noted, and described in detail in this chapter, Amnesty International has clearly outlined that the fraud identification and investigation process is subjected to the review of caseworkers. Nevertheless, Amnesty International finds that the automation of the fraud identification process in order to flag individuals for investigations raises serious concerns and violates benefits recipients' human rights, specifically the right to privacy, equality and non-discrimination, human dignity and social protection. These findings are detailed in the subsequent chapters.

[82] Privacy International, "Stage 3 - The policing of social benefits: punishing poverty" (previously cited).
[83] Right of Reply response from UDK 302024

6. DENMARK'S HUMAN RIGHTS OBLIGATIONS AND THE RESPONSIBILITY OF CORPORATE ACTORS

This chapter summarizes the relevant human rights law frameworks at the European and international levels that are applicable to the human rights violations and risks detailed in this report.

6.1 DATA PROTECTION AND THE RIGHT TO PRIVACY

Both digital and analogue forms of surveillance may threaten the right to privacy. The right to privacy is guaranteed under the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights, the Convention on the Rights of Persons with Disabilities (CRPD) and the Charter of Fundamental Rights of the European Union – all of which are binding on Denmark. To comply with human rights law and standards, restrictions on the right to privacy must meet the principle of legality, serve a legitimate aim, and be necessary and proportionate to that aim.[84]

In a 2018 report on the right to privacy in the digital age, the United Nations High Commissioner for Human Rights notes that the use of AI systems has a tremendous impact on fundamental rights because these systems incentivize extensive data collection, processing and storage which can interfere with people's right to privacy.[85] The respect for private life guaranteed by Article 17 of the ICCPR is closely linked to the protection of personal data. The right to privacy and protection of personal data defines how much states and private entities can interfere with a person's private life or circumstances.[86]

The right to data protection is guaranteed by Articles 8(1) and (2) of the Charter of Fundamental Rights of the European Union, as well as numerous international and regional treaties and regulations, including the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+)[87], and the General Data Protection Regulation (GDPR) of the European Union.[88]

[84] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report, 17 April 2013, UN Doc. A/HRC/23/40, para. 29.
[85] OHCHR, *The Right to Privacy in the Digital Age*, 3 August 2018, UN Doc. A/HRC/39/29, para. 12.
[86] OHCHR, *The Right to Privacy in the Digital Age* (previously cited), para. 5.
[87] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, https://rm.coe.int/1680078b37
[88] General Data Protection Regulation (EU) 2016/679.

Denmark's Data Protection Act largely mirrors the GDPR. The GDPR defines the principles that govern the collection, processing and storage of personal data and applies to the processing of data held by public and private entities. Under Article 5 of the regulation, it requires, among other things, that data be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);

(a) collected for specified, explicit and legitimate purposes ("purpose limitation");

(a) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");

(a) accurate and, where necessary, kept up to date ("accuracy");

(a) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed ("storage limitation");

(a) processed in a manner that ensures appropriate security of the personal data ("integrity and confidentiality").[89]

Regarding automated decision making, Article 22 of the GDPR outlines provisions for the regulation of automated decision making in instances where processes are fully automated and requires that "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".[90]

In *OQ v Land Hessen*, the Court of Justice of the European Union (CJEU) highlighted that, to constitute automated decision making, Article 22(1) of the GDPR required three conditions to be met. There must be a decision; the decision is established solely by automated means and the decision must have a real impact or affect the data subject.[91]

6.2 RIGHT TO FREEDOM OF EXPRESSION

In addition, human rights concerns related to the right to privacy and data protection in Udbetaling Danmark/ATP's use of surveillance for the purposes of fraud control has implications for the right to freedom of expression. Denmark has an obligation to uphold its residents' right to freedom of expression as defined in Article 19 of the ICCPR.[92] Freedom of expression can only be restricted if the restriction is provided for in law and if it is necessary for the right to be restricted.[93]

The UN Human Rights Committee has stated that the protection of freedom of expression is an essential condition for the full development of the person, for the promotion and protection of human rights.[94] The Committee explains that protection of freedom of expression includes protection of all forms of expression and their dissemination including through "electronic and internet-based modes of expression".[95]

6.3 RIGHT TO EQUALITY AND NON-DISCRIMINATION

States' obligations to respect, protect and promote the rights to equality and non-discrimination are defined in several international human rights law instruments.[96] Discrimination undermines the fulfilment of other human rights.[97] Furthermore, several articles in the EU Charter on Fundamental Rights recognize the right to equal treatment under the law and the dignity of a human person which constitutes the real basis of fundamental rights,[98] and the right to equality and non-discrimination on the grounds of "sex, race, ethnic or social origin, genetic features, language, religion or belief, political opinion, disability, age or sexual

[89] General Data Protection Regulation (EU) 2016/679, Articles 5(1)(a-f)
[90] General Data Protection Regulation (EU) 2016/679, Article 22(1).
[91] CJEU, Case C-634/21, *OQ v Land Hessen*, Joined party: SCHUFA Holding AG, paras 45-52.
[92] ICCPR, Article 19.
[93] ICCPR, Article 19.
[94] UN Human Rights Committee (HRC), General Comment 34, 12 September 2011, UN Doc. CCPR/C/GC/34, para. 2.
[95] HRC, General Comment 34 (previously cited), para. 12.
[96] Charter of the United Nations, Articles 1 and 55; Universal Declaration of Human Rights, Article 2; ICCPR, Article 26; Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), Article 2; Convention relating to the Status of Refugees (Refugee Convention) Article 3; Convention on the Rights of Persons with Disabilities (CRPD), Article 4 and 5.
[97] CESCR, General Comment 20, 2 July 2009, UN Doc. E/C.12/GC/20, para. 2.
[98] CJEU, Case C-377/98, *Netherlands v. European Parliament and Council* [2001] ECR I-7079, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61998CJ0377 paras 70-77.

orientation".[99] Denmark has obligations to respect, protect and promote the right to equality and non-discrimination. UDK/ATPs use of fraud-control algorithms affects realization of these rights. (See Chapter 8.)

The UN Special Rapporteur on racism has noted that AI systems that classify, differentiate, rank and categorize are "systems of discrimination" because they "reproduce bias embedded in large-scale data sets capable of mimicking and reproducing implicit biases of humans, even in the absence of explicit algorithmic rules that stereotype".[100] The Special Rapporteur stated that "digital technologies can be combined intentionally and unintentionally to produce racially discriminatory structures that holistically or systematically undermine enjoyment of human rights for certain groups, on account of their race, ethnicity or national origin, in combination with other characteristics [and] digital technologies [are] capable of creating and sustaining racial and ethnic exclusion in systemic or structural terms".[101] The Special Rapporteur called on states to end "not only explicit racism and intolerance in the use and design of emerging digital technologies, but also, and just as seriously, indirect and structural forms of racial discrimination that result from the design and use of such technologies".[102] The Special Rapporteur moreover called for an equality-based approach to human rights governance of emerging digital technologies by moving beyond "colour-blind" or "race neutral" strategies because "a colour-blind analysis of legal, social, economic and political conditions commits to an even-handedness that entails avoiding explicit racial or ethnic analysis in favour of treating all individuals and groups the same, even if these individuals and groups are differently situated, including because of historical structures".[103]

Article 2(1)(a) of the Convention on the Elimination of All Forms of Racial Discrimination (CERD) places obligations on Denmark to "condemn racial discrimination and undertake to pursue by all appropriate means and without delay a policy of eliminating racial discrimination in all its forms" and not to engage in any "act or practice of racial discrimination against persons, groups of persons or institutions and to ensure that all public authorities and public institutions, national and local, shall act in conformity with this obligation". Furthermore, Article 2(1)(c) requires that Denmark takes "effective measures to review governmental, national and local policies, and to amend, rescind or nullify any laws and regulations which have the effect of creating or perpetuating racial discrimination wherever it exists". The CERD Committee has clarified that discrimination under the Convention includes "purposive or intentional discrimination and discrimination in effect" and that discrimination is constituted not simply by an unjustifiable "distinction, exclusion or restriction" but also by an unjustifiable "preference".[104]

The CERD Committee also discusses discrimination against non-citizens and notes that "differential treatment will constitute discrimination if the criteria for such differentiation, judged in the light of the objectives and purposes of the Convention, are not applied pursuant to a legitimate aim, and are not proportional to the achievement of this aim".[105] Additionally, Article 3 of the 1951 Convention and Protocol Relating to the Status of Refugees (Refugee Convention) also prohibits discrimination based on race, religion or country of origin.

Direct and indirect discrimination is prohibited under international law. Distinctions, restrictions or preferences made between citizens and non-citizens cannot be used for the purposes of promoting xenophobic and racial discrimination. Xenophobia is defined both as "discrimination based on the perception of being a foreigner and non-citizen [and also discrimination that is based on] an intersection between racial and other grounds such as religion or language".[106]

Denmark has obligations to guarantee the right to equality and non-discrimination in the access of social benefits for non-nationals, people who have been granted refugee status in Denmark, stateless persons, asylum seekers and other disadvantaged groups. With respect to ensuring equal access to social benefits by non-nationals, the UN Committee on Economic Social and Cultural Rights notes that states parties (which include Denmark) should not discriminate against social benefit applicants and recipients on the grounds of nationality.[107] This is reflected in Article 2(2) of the International Covenant on Economic, Social and Cultural

[99] Charter of Fundamental Rights of the European Union, Articles 20, 21, 25 and 26.
[100] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis*, 18 June 2020, UN Doc. A/HRC/44/57, para. 7.
[101] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis* (previously cited), para. 38.
[102] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis* (previously cited), para. 45.
[103] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis* (previously cited), para. 2.
[104] CERD Committee, General Recommendation 32, 24 September 2009, UN Doc. CERD/C/GC/32, para. 7.
[105] CERD Committee, General Recommendation 32 (previously cited), para. 8.
[106] Amnesty International, *Submission to the UN CERD-CMW Joint General Comment/Recommendation on 'Obligations of State Parties on Addressing and Eradicating Xenophobia and its Impact on the Rights of Migrants, their Families and Other Non-Citizens Affected by Racial Discrimination* (Index IOR 40/7898/2024), 4 April 2024, https://www.amnesty.org/en/documents/ior40/7898/2024/en/, p. 3.
[107] CESCR, General Comment 19, 4 February 2008, UN Doc. E/C.12/GC/19, paras 36 & 77.

Rights (ICESCR). The Committee has also stated that: "Non-nationals should be able to access non-contributory schemes for income support, affordable access to health care and family support" and that any "restrictions, including a qualification period, must be proportionate and reasonable". [108]

Regarding discrimination against persons with disabilities, Article 5(2) of the CRPD requires that states parties, including Denmark, "prohibit all discrimination on the basis of disability". Article 2 of the CRPD defines such discrimination as:

"any distinction, exclusion or restriction on the basis of disability which has the purpose or effect of impairing or nullifying the recognition, enjoyment or exercise, on an equal basis with others, of all human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field. It includes all forms of discrimination, including denial of reasonable accommodation."

To guarantee the human rights of persons with disabilities, states should adopt legislative, administrative and other measures, including modifying or abolishing laws, regulations, practices and customs that facilitate discrimination against persons with disabilities.[109] This includes introducing measures that promote accessibility to enable persons with disabilities to "live independently and participate fully in all aspects of life"[110] and shall include "the identification and elimination of obstacles and barriers to accessibility [in respect to]… Information, communications and other services, including electronic services and emergency services".[111] The CRPD requires that states should also take appropriate measures to "promote access for persons with disabilities to new information and communications technologies and systems, including the Internet".[112]

The CRPD Committee has noted that:

"Accessibility is a precondition for persons with disabilities to live independently and participate fully and equally in society [and that] without access to the physical environment, to transportation, to information and communication, including information and communications technologies and systems… persons with disabilities would not have equal opportunities for participation in their respective societies."[113]

The Committee also clarified that "new technologies can be used to promote the full and equal participation of persons with disabilities in society, but only if they are designed and produced in a way that ensures their accessibility".[114]

6.4 RIGHTS TO SOCIAL SECURITY

Denmark has an obligation to respect and protect the right to social security of its residents. The right to social security is recognized and enshrined by EU and international human rights law. Article 34 of the Charter of Fundamental Rights of the European Union, Article 9 of the ICESCR and Article 22 of the Universal Declaration of Human Rights recognize that everyone has a right to social security. The Committee on Economic, Social and Cultural Rights has noted that the right to social security is "of central importance in guaranteeing human dignity" and is an important tool to combat discrimination, to reduce and alleviate poverty and social exclusion and to promote social inclusion.[115] The Committee further noted that states must ensure that social support within their countries is:

a) available – that a social security system needs to be in place under domestic law;

b) adequate – that social support is sufficient in quantity and duration so that everyone can realize their rights to family protection and assistance and a reasonable standard of living and access to health care;

c) affordable – that the costs and charges associated with contributions to social security must be economical for all so that they do not compromise the realization of other Covenant rights; and

[108] CESCR, General Comment 19 (previously cited), para. 37.
[109] CRPD, Article 4(1)(a-b).
[110] CRPD, Article 9(1).
[111] CRPD, Article 9(1)(b).
[112] CRPD, Articles 9(2)(g) and (h).
[113] CRPD Committee, General Comment 2, 22 May 2014, UN Doc. CRPD/C/GC/2, para 1.
[114] CRPD Committee, General Comment 2 (previously cited), para. 22.
[115] CESCR, General Comment 19 (previously cited), paras 1 and 3.

d) accessible – that the social security system should cover all persons especially those who are most disadvantaged and marginalized.[116]

Convention 102 of the International Labour Organization also provides for minimum standards for social security.

Denmark also has obligations under Article 30(a) of the European Social Charter of 1996, which mandates that, in order for states to ensure "effective exercise of the right to protection against poverty and social exclusion", they should "promote the effective access of persons who live or risk living in a situation of social exclusion or poverty, as well as their families, to, in particular, employment, housing, training, education, culture and social and medical assistance".

Article 28(1) of the CRPD imposes a duty on Denmark to:

"recognise the right of persons with disabilities to an adequate standard of living for themselves and their families, including adequate food, clothing and housing, and to the continuous improvement of living conditions, and [to] take appropriate steps to safeguard and promote the realisation of this right without discrimination on the basis of disability."

Article 28(2)(e) also mandates states, including Denmark, to take appropriate steps to safeguard and promote the realization of this right, including measures to "ensure equal access by persons with disabilities to retirement benefits and programmes". Article 28(2)(b) meanwhile provides that states must ensure access by persons with disabilities, in particular women, girls and older persons with disabilities, to social protection programmes and poverty reduction programmes. Article 19 of the CRPD notes that states have an obligation to ensure that "persons with disabilities have access to a range of in-home, residential and other community support services, including personal assistance".

Article 24(1)(b) of the Refugee Convention also contains provisions on social security and mandates states to "accord to refugees lawfully staying in their territory the same treatment as is accorded to nationals" in respect of social security, including access to maternity, sickness, unemployment, disability and old age benefits.

Article 5(e)(iv) of CERD mandates that states must undertake to prohibit and to eliminate racial discrimination in all its forms and to guarantee the right of everyone, without distinction as to race, colour, or national or ethnic origin, to equality before the law, notably in the enjoyment of economic, social and cultural rights, including the right to public health, medical care, social security and social services.

6.5 RIGHTS OF THE CHILD

Under Articles 3(1) and (2) of the Convention on the Rights of the Child (CRC), Denmark has obligations to ensure that "in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child… [remain] a primary consideration". Further, Article 3(2) of CRC requires that states parties, including Denmark, take all appropriate legislative and administrative measures to ensure a child "such protection and care as is necessary for his or her well-being, taking into account the rights and duties of his or her parents, legal guardians, or other individuals legally responsible for him or her".

Denmark also has obligations under Article 26(1) of CRC which requires that states parties recognize every child's "right to benefit from social security, including social insurance", and take all necessary measures to achieve the full realization of this right in accordance with domestic law.

Further, Article 16 of CRC expressly protects children's right to privacy. Recital 38 of the GDPR notes that children merit specific protection regarding their personal data.[117]

[116] CESCR, General Comment 19 (previously cited), paras 11, 22, 25 & 23.
[117] GDPR, Recital 38, https://gdpr-info.eu/recitals/no-38/

6.6 TRANSPARENCY, ACCOUNTABILITY AND THE RIGHT TO REMEDY

Algorithmic systems and the data used to make fraud predictions are often not made public by those implementing these systems, creating a "black box" effect.[118] This lack of transparency creates barriers to meaningful participation in debates surrounding the use and governance of these systems for people who are likely to be affected by them. Lack of transparency also creates barriers for those affected to hold the deployers and users of these systems accountable for any resulting human rights harms.[119] The Special Rapporteur on racism has noted:

"This 'black box' effect makes it difficult for affected groups to overcome steep evidentiary burdens of proof typically required to prove discrimination through legal proceedings, assuming that court processes are even available in the first place."[120]

The principles of transparency are defined in Article 5 of the GDPR, which requires that data subjects are made aware of the ways in which their personal information is being used by data controllers.

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CoE Framework Convention) contains legally binding provisions on transparency and accountability under Articles 8 and 9 respectively. The CoE Framework Convention has been signed by the EU, and hence will be binding on state parties, including Denmark, when it comes into force. Article 8 of the treaty imposes a duty on EU member states to:

"adopt or maintain measures to ensure that adequate transparency and oversight requirements tailored to the specific contexts and risks are in place in respect of activities within the lifecycle of artificial intelligence systems, including with regard to the identification of content generated by artificial intelligence systems."

Article 9 mandates that EU member states "adopt or maintain measures to ensure accountability and responsibility for adverse impacts on human rights, democracy and the rule of law resulting from activities within the lifecycle of artificial intelligence systems".

Denmark will also be required to comply with the transparency provisions on high-risk artificial systems as outlined in the final text of the EU AI Act 2024, which came into force on 1 August 2024. Annex III of the Act classifies the AI systems used to provide social protection as high-risk systems. According to Annex III, high risk systems are:

"AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services."

However, where adequate criteria are met, such systems could also be classified as social scoring systems, which are subject to a ban under the EU AI Act. (See Chapter 13 for a detailed discussion.)

At the very minimum, transparency requirements are binding and applicable to the Danish authorities for high-risk systems under article 26 of the AI Act, which establishes obligations for deployers of high-risk AI systems, including public database registration obligation of the relevant systems (art 26.8) and obligation to inform the natural persons that they are subject to the use of the high-risk AI system (art 26.11). In addition, article 27 of the EU AI Act stipulates that, prior to the deployment of these AI systems, public and private actors should conduct assessments of the impact of these systems on fundamental human rights. The assessment should include:

"(a) a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose; (b) a description of the period of time and frequency in which each high-risk AI system is intended to be used; (c) the categories of natural persons and groups likely to be affected by its use in the specific context; (d) the specific risks of harm likely to impact the categories of persons or group of persons identified pursuant point… (e) a description of the implementation of human oversight measures, according to

[118] Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, 2016.
[119] Niklas Kossow and others, "Algorithmic transparency and accountability", 2021, https://knowledgehub.transparency.org/helpdesk/algorithmic-transparency-and-accountability
[120] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis* (previously cited), para. 44.

the instructions of use; (f) the measures to be taken in case of the materialization of these risks, including their arrangements for internal governance and complaint mechanisms."

Once this assessment has been performed, the deployer of the system shall notify the market surveillance authority of its results.[121]

Further, the Danish government has obligations to ensure that anybody adversely affected by UDK/ATP's data and algorithmic practices has a right to effective remedy. The right to effective remedy is defined in the EU Charter on Fundamental Rights and various other human rights instruments. Article 47 of the Charter states that "everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal". Article 8 of the Universal Declaration of Human Rights states that "everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights".[122] This requirement is also specified in Article 2(3)(a-b) of the ICCPR which requires state parties to "ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy", determined by "competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State".[123]

Articles 85-87 of the EU AI Act also contain provisions on the right to remedy. Article 86 of the Act states that an affected person subjected to a decision of a high-risk AI system "shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken".[124]

Further, states parties are obliged to guarantee the right of every person within their jurisdiction to an effective remedy against the perpetrators of acts of racial discrimination, without discrimination of any kind, whether such acts are committed by private individuals or state officials, as well as the right to seek just and adequate reparation for the damage suffered.[125] The Special Rapporteur on racism has noted that:

"In the context of effective remedies for racial discrimination in the design and use of emerging digital technologies, States must ensure the full spectrum of effective remedies, including access to justice, protection against possible violations, and guarantees of cessation and non-recurrence of violations, while also combating impunity."[126]

Adherence by states and corporate actors to the transparency requirements discussed above is essential to the effective exercise the right to remedy by those subjected to automated decision-making processes.

6.7 STATE AND CORPORATE RESPONSIBILITY UNDER HUMAN RIGHTS STANDARDS

States and corporations have a responsibility to respect human rights in all of their business activities as set out in the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises.[127] States must implement the UN Guiding Principles on Business and Human Rights "in a non-discriminatory manner".[128] States are also required to provide guidance to corporate actors on respecting human rights, including guidance on "how to consider effectively issues of gender, vulnerability and/or marginalization, recognizing the specific challenges that may be faced by indigenous peoples, women, national or ethnic minorities, religious and linguistic".[129]

The Committee on Economic, Social and Cultural Rights has clarified that states have specific obligations to respect, protect and fulfil human rights and may be "directly responsible for the action or inaction of

[121] EU AI Act, Article 27.
[122] UDHR 1948, Article 8.
[123] ICCPR, Article 2 (3) (a-b).
[124] EU Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act. Accessed on 09 October 2024 at: [Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)Text with EEA relevance. (europa.eu)]
[125] CERD Committee, General Recommendation 31, 2005, UN Doc. A/60/18, para. 6
[126] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis* (previously cited), para. 65.
[127] CESCR, General Comment 24, 10 August 2017, UN Doc. E/C.12/GC/24; OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, p. 25.
[128] UN Guiding Principles on Business and Human Rights, p. 1.
[129] UN Guiding Principles on Business and Human Rights, Principle 3, pp. 5-6.

business entities".[130] States, including Denmark, must "adopt legislative, administrative, educational and other appropriate measures, to ensure effective protection against Covenant rights violations linked to business activities, and that they provide victims of such corporate abuses with access to effective remedies".[131] The obligation also includes requiring that business entities exercise human rights due diligence in order to identify, prevent and mitigate the risks of violations of Covenant rights as a result of the decisions and operations of business entities. Imposition of due diligence requirements to prevent abuses of Covenant rights should be extended to "a business entity's supply chain and by subcontractors, suppliers, franchisees, or other business partners".[132]

The UN Human Rights Committee and the CERD Committee also note the obligations of states in guarding against discrimination not only by public sector actors but also by private actors. The Human Rights Committee notes that states are required to ensure effective remedies for racial discrimination attributable to private actors, including corporations, by ensuring that they "take appropriate measures or exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities".[133] The CERD Committee has clarified that states must enact special measures to achieve and protect racial equality not only throughout the public but also private spheres.[134]

The UN Guiding Principles on Business and Human Rights also contain provisions outlining the responsibilities of business enterprises. Principle 13 states that the responsibility to respect human rights requires companies to avoid causing or contributing to human rights abuses through their own business activities, and address impacts in which they are involved, including by remediating any actual abuses. The responsibility to respect human rights requires that business enterprises "seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts".

Principle 15 of the UN Guiding Principles establish that, to meet their corporate responsibility to respect human rights, companies should have in place an ongoing and proactive human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights.

Additionally, Principle 21 of the UN Guiding Principles states that corporate actors should communicate the human rights impacts of their practices publicly, including how they are addressing these impacts. As Principle 22 makes clear, companies "need to know and show that they respect human rights". In this case, "showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders".

The OECD has provided practical guidance for conducting due diligence in its Due Diligence Guidance for Responsible Business Conduct (OECD Due Diligence Guidance). This guidance, which elaborates on the due diligence responsibilities of companies under the OECD Guidelines for Multinational Enterprises, is designed to help companies in all sectors, regardless of their size, geographic location, or value chain position, to understand and implement their due diligence responsibilities. The six-step framework provides detailed guidance to companies on how to:

1. Embed responsible business conduct into policies and management systems;
2. Identify and assess adverse impacts in operations, supply chains and business relationships;
3. Cease, prevent or mitigate adverse impacts;
4. Track implementation and results;
5. Communicate how impacts are addressed; and
6. Provide for or cooperate in remediation, when appropriate.

[130] CESCR, General Comment 24 (previously cited), paras 10-11.
[131] CESCR, General Comment 24 (previously cited), para. 14.
[132] CESCR, General Comment 24 (previously cited), para. 16.
[133] HRC, General Comment 31, 26 May 2004, UN Doc. CCPR/C/21/Rev.1/Add. 13, para. 8.
[134] CERD Committee, General Recommendation 32 (previously cited).

7. ‘DUVET LIFTING’ MONITORING AND SURVEILLANCE OF BENEFITS APPLICANTS, RECIPIENTS AND THEIR AFFILIATES

This chapter details both the digital surveillance methods and the “traditional” or “analogue” surveillance approaches deployed for the purposes of fraud control by Danish authorities. It details how digital methods amplify “traditional” methods to allow for surveillance on a scale not previously possible.

7.1 DIGITAL SURVEILLANCE

7.1.1 MASS SURVEILLANCE THROUGH REGISTER MERGERS

This section provides an overview and analysis of the digital surveillance of benefits applicants and recipients by Danish authorities. It discusses ways in which UDK surveils applicants and recipients through “register mergers”; that is, fraud control algorithms on data merged from several public databases for the purported aim of detecting fraud. This mass-scale extraction and processing of the personal data of social benefits applicants and recipients for fraud detection purposes is incompatible with human rights and data protection laws and standards (see Chapter 6).

Amnesty International has found that the Danish government has implemented privacy-intrusive legislation that allows for the collection of data from residents in receipt of benefits and members of their households without their consent for the purposes of surveilling the population to control for fraud.

The collection and merging of large amounts of personal data contained in various government databases – as described in Table 3 in Chapter 5.1 – has effectively forced social benefits recipients to give up their right to privacy and data protection to exercise their right to social security and other social rights. The interoperable databases are used to build a 360-degree profile of welfare beneficiaries, in practice building a

datafied picture of their entire lives including where they live, whom they live with, where they work, when and where they travel and their health records.

The collation and aggregation of sensitive data on every aspect of individuals' lives for the purposes of fraud control is in effect a system of mass surveillance that is privacy-violating by design. It is also inherently ineffective, given that the data does not have sufficient nuance to capture the complexity of people's everyday lives. As discussed in detail in Chapter 8, attempting to accurately record a person's living situation or relationship status in administrative data is challenging for several reasons. For example, a person's living arrangements may be transient, or their exact circumstances may be open to subjective interpretation as there are no strict legal definitions of what constitutes "cohabitation".

Proportionality likewise requires that such practices must also be justified considering their "impact on the overall situation and particularly other human rights potentially infringed during the implementation process".[135] These practices must also be accompanied by adequate safeguards against abuse, including transparency.

These principles are reflected in laws which are binding on Denmark, including Articles 5 and 6 of the GDPR (the provisions of which are contained in sections 5 and 6 of Denmark's Data Protection Act 2018)[136] as well as the Charter of Fundamental Rights of the European Union[137] and numerous international standards, as detailed in Chapter 6.

Processing of data by UDK in the manner detailed in this report is not transparent. Amnesty International submitted FOIs to attempt to understand the total number of cases classified as high risk (individuals that are considered more likely to commit fraud) and the percentage of those that are erroneous or fraudulent applications, alongside a breakdown of the demographic characteristics of such cases. UDK rejected this request on the basis that it does not have the figures to hand and cases are constantly overwritten, meaning that data on this is very challenging to obtain. The absence of demographic data prevents statistical bias and fairness testing (discussed further in Chapters 8 and 10), but the absence of basic evaluation statistics on the performance of the algorithms does not allow for scrutiny of how effective the algorithms are at their purported task – identifying fraud and error. When requesting evidence on evaluation metrics, such as a confusion matrix,[138] of the algorithms' performance in FOIs, Amnesty International received the following response:

"Evaluation metrics have been used in the development of the model, but they have not been documented. No new evaluation metrics are created, but the model's training cases are continuously monitored".[139]

In a letter to UDK prior to the publication of this report, Amnesty International again requested data on performance assessments over its data-driven controls (without any demographic characteristics) for the year 2023. UDK stated the following and provided the following data:

"Udbetaling Danmark assesses the quality of the data-driven controls based on the proportion of cases that HOK (the control team) assesses as suitable for further manual processing as actual control cases. We report the number of cases that Udbetaling Danmark choose to receive (number of requested cases). Of these, we report how many are assessed as suitable for further processing as actual control cases (number of established control cases), as shown in the table below. Finally, we report how many cases result in citizens having their benefits stopped or reduced (number of cases with revenue). It is important to note that cases initiated as control cases in one year are not necessarily concluded in the same year. Therefore, it cannot be inferred that the number of cases with revenue, e.g., in 2023, is a proportion of the cases established in 2023."

[135] UN Special Rapporteur on the right to privacy, *Working Draft Legal Instrument on Government-led Surveillance and Privacy, Including the Explanatory Memorandum*, version 7.0, 28 February 2018, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf

[136] Data Protection Act (No. 502 of 23 May 2018), ttps://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf

[137] Charter of Fundamental Rights of the European Union. 26.10.2012, OJ C 326/391

[138] A confusion matrix is a table that is used to define the performance of an algorithm . A confusion matrix visualizes and summarizes the performance of a classification algorithm.

[139] FOI response from UDK/ATP dated 26 April 2024

TABLE 5: STATISTICS FOR DATA-DRIVEN CONTROLS USED BY UDK IN 2023

	RELEVANT MODEL	REQUESTED CASES	ESTABLISHED CONTROL CASES	CASES WITH REVENUE
Single status (child benefit and pension supplement)	"Really Single"	412	292	135
Unreported departures (State and disability pension)	"Model Abroad"	511	351	36
Parental leave benefits (fictitious employment + income during paternal leave)	"Fictitious Employment"	491	207	72

To contextualise the figures in Table 5 for the Really Single Model:

- 412 requested cases - the number of cases provided by the algorithm to the relevant control team
- 292 Established control cases – the number of cases the control team assessed warranted an investigation (after receiving the 412 cases from the algorithm)
- 135 Cases with revenue – the number of cases that were found to be fraudulent or erroneous after an investigation was conducted (and therefore resulted in revenue recovery for the agency)

The data above provides an indication of how effective the fraud control models are at their stated purpose. It demonstrates how some of the algorithms, such as the Really Single Model, are used across different social benefit domains (as discussed in Chapter 5). For each model, the figures provide an indication of the number of false positives - that is the number of cases that are classified by the models as high risk of fraud or error (therefore warranting further investigation or "control") but are in fact legitimate.

Whilst UDK assesses the quality of the algorithmic models based on the proportion of cases that HOK (the control team) assesses as suitable for further manual processing as actual control cases (i.e. simply the number of potentially fraudulent cases the model picks up), Amnesty International would argue this assessment is overly broad. Critically, it does not account for the number of cases that actually result in revenue recovered (indicating the case was in fact fraudulent or erroneous) and therefore the cases that were incorrectly flagged for fraud investigations. When accounting for this within the assessment of the algorithms, table 5 above demonstrates only 33% of cases result in revenue recovered for the Really Single algorithm, 7% for the Model Abroad, and 15% for the Parental leave benefits controls (which includes the Fictitious Employment model).

Critically the data also provides estimates for the number of individuals that are investigated as a result of being flagged by the models but resulted in no further action. For each algorithm, 54% of cases opened resulted in no further action for the Really Single Model, almost 90% of cases opened resulted in no further action for the Model Abroad, and 65% of cases opened resulted in no further action for the Parental Leave benefit controls.

In terms of the scope of the systems, in an interview the UDK/ATP control team stated that roughly 30% of cases investigated come from the algorithmic systems, and the UDK/ATP control team would like this be higher:

"[In general], we will manage between 5,000 to 6,000 cases per year. And around 1,800 are from these cases that I'm getting. And that's because, you know, from a control point of view, I would actually like more of those cases [from the algorithmic models]. But, you know, in Danish law, you have to make sure that you take all the cases that others [for example, reports from neighbours and public authorities] are sending in."[140]

[140] Interview with UDK, officials 11 January 2024.

These figures raise serious concerns around the necessity and proportionality of data processing, given UDK is processing the personal data of millions of social benefits recipients, yet are both only able to inspect a few thousand cases each year for fraud, of which, as the data in Table 5 indicates, a substantial proportion are false negatives and are therefore incorrectly investigated.

It is questionable therefore whether the use of fraud control algorithms is effective at identifying fraud in this context. This would be concerning from a human rights point of view, as an ineffective tool cannot, by definition, be necessary. Contrary to the perspective of the UDK/ATP control team, who wanted more referrals from the algorithmic systems, an official from the Copenhagen Control Unit raised concerns about the accuracy of the fraud detection algorithms:

"[When UDK/ATP sends us cases] more often than not there is no fraud. That's why I said before that we have participated in the meetings with them [UDK] and given them the input that we have… the models, I don't think they're very useful… I think the models are made by people who haven't been working with cases."[141]

In an FOI request sent to Copenhagen Municipality on 25 March 2024 requesting information on the number of fraud cases it receives from /ATP, Copenhagen Municipality shared information about the low number of cases flagged for fraud investigations through register mergers, compared to those received from other, analogue sources such as anonymous or non-anonymous tip-offs.[142] These are shown in Table 6.

The data in Table 6 raises further questions about whether extensive surveillance of millions of residents for fraud detection purposes through the extraction of large amounts of their intimate and sensitive personal information from public databases is: (a) necessary – whether it is the least intrusive measure that can be used to detect fraud, and (b) proportionate – whether the harm or violations to human rights, including the right to privacy, caused by the surveillance outweighs the desired outcome of identifying cases for fraud investigations because of the low number of fraud cases identified through register mergers.

TABLE 6: STATISTICS FROM THE COPENHAGEN MINISTRY

RESIDENCE CASES (CASES OF A PERSON'S RESIDENCY)	2022	2023
REGISTER SEARCHES	22	80
CITIZEN ENQUIRIES	9	11
PUBLIC AUTHORITIES	327	329

In its response to Amnesty International's findings that UDK/ATP is collecting large amounts of sensitive data for the purposes of detecting benefits fraud, UDK has claimed that the collection and use of vast amounts of data for fraud detection is "legally grounded." In addition, in its response to Amnesty International's findings, the Danish Agency for Labour Market and Recruitment stated that, "UDK is only authorized to collect and cross-reference non-sensitive personal data from its own registers, including information obtained from other authorities, for the purpose of controlling a specific case or for general monitoring of applicants or recipients of cash benefits or financial aid."

International human rights law and standards require that any interference with an individual's right to privacy through surveillance may be allowed if it is "legal" or prescribed by law to meet a legitimate aim, such interference must be strictly necessary and proportionate to meet the said legitimate aim. This means that UDK/ATP must ensure that any surveillance measures it imposes on social benefits recipients and those affiliated with them must provide for the lowest degree of interference with the right it restricts (necessity) and that when balancing the nature and the extent of the interference against the reason for interfering with an individual's right, UDK/ATP should demonstrate that the harm caused does not outweigh the desired outcome (proportionality). As demonstrated in this section, UDK's processing of data for the purposes of fraud control does not meet these tests, and moreover the methods are of questionable utility.

In addition, the merging of numerous public databases for the purposes of fraud control contains sensitive personal data which could act as proxies and reveal personal information such as race and ethnicity, health, or disability (See Chapter 5).

These practices reveal highly invasive and disproportionate methods to detect fraud. UDK in its responses has not demonstrated that these measures are the least invasive means of detecting fraud.

[141]Interview with an official at Copenhagen Municipality's control unit, 4 September 2023.
[142] FOI Response from Copenhagen Municipality's Fraud Control Unit, 8 April 2024.

7.1.2 SOCIAL MEDIA MONITORING AND REPORTED USE OF GEOLOCATION DATA

In addition to relying on data held in public databases for fraud investigations, UDK/ATP and municipalities also rely on social media data to identify and investigate individuals believed to be committing fraud or likely to commit fraud. In its response to Amnesty International's letter prior to the publication of this report, the UDK confirmed its use of social media data for fraud investigations. It stated that, "In individual case processing – and only there – follow-up can include visiting publicly accessible social media profiles."

The unregulated use of data gathered from social media platforms including Facebook and Instagram to investigate benefits fraud is prevalent in Denmark. In 2019, a report by DK Denmark highlighted Vejen Municipality's use of Facebook data to determine whether a cash benefits recipient was committing benefit fraud. The report found that, as of 2019, only three of the country's 93 municipality control teams did *not* use social media data to conduct investigations of benefits fraud.[143]

In the same report, researchers found that Vejen Municipality investigated an individual named Annette Hansen for fraud using her Facebook activities. The municipality relied on posts Annette Hansen made on her Facebook page to conclude that she was living with her boyfriend Annette Hansen was accused of fraudulently claiming additional benefits that are intended for single people and was required to repay DKK 12,500 (EUR 1,650). The decision of the municipality was overturned by the National Appeals Board because the board did not find that Annette Hansen and her boyfriend were in a marriage-like relationship.[144] This example sheds light on how the use of social media data to make conclusions about people's circumstances can lead to erroneous decision making.

During a focus group convened with people with disabilities at Dansk Handicap Foundation, several people told Amnesty International that they had heard of instances where municipalities had used social media platforms to investigate people claiming child benefits or pensions benefits. In their experience, municipalities used social media platforms to check whether the claimants were single or appeared to be living with a partner. A single person is entitled to a higher amount of child or pension benefits than a person in relationship or who is cohabiting, according to section 49 of the Executive Order of the Social Pension Act. One of the focus group participants at Dansk Handicap Foundation claimed that:

"The municipality has somebody looking at their Facebook also saying, 'Oh, we've seen now she's not single any longer, she's posted a lot of pictures of her boyfriend'. Something like that, then they will investigate it. So, it's on all levels that you are actually being investigated, whether you know it or not."[145]

The use of social media for control purposes or to investigate fraud was confirmed by UDK and Aalborg Municipality Control Unit officials during interviews. Two officials from UDK stated the following during an in-person interview:

"[Y]ou can say that you can access the information that is publicly available, so if you have a control case on a person who has an open Facebook profile, you can go in and take a look."[146]

An official from Aalborg Municipality's Control Unit stated that they use Facebook and Instagram data to determine people's living arrangements; specifically, whether they are cohabiting. The official stated:

"[We use social media platforms to find out] if the mum and dad lives together. We look at what they write and whether we can see that they live together. And then we can make a screen grab that we can use in a possible interview."[147]

A focus group participant at Dansk Handicap Foundation and an official at SoS Racisme stated during a focus group and interview respectively that people felt constantly surveiled by municipalities and that they lived in fear and anxiety because of this surveillance.[148] Focus group participants stated that people were

---

[143] Diana Bengtsen and others, **"Accused of social security fraud:** Annette was confronted with 52 pages from Facebook", 17 February 2019, https://www.dr.dk/nyheder/indland/anklaget-socialt-bedrageri-annette-blev-konfronteret-med-52-sider-fra-facebook#!/ (in Danish).
[144]Diana Bengtsen and others, "Accused of social security fraud" (previously cited).
[145] Focus group participant Gitte Nielsen the Chairman of the Social- and Labor market policy committee at Dansk Handicap Foundation 10 January 2024. Concerns about the use of Facebook data for fraud investigations by municipalities was further expressed by Stig Langvad a Senior consultant at Dansk Handicap during a focus group discussion on 10. January 2024 and an official at SoS Racisime 15 January 2024.
[146] Interview with UDK Officials 23 November 2023.
[147] Interview with an official from Aalborg Municipality's Fraud Control Unit 14 September 2023.
[148] Focus group participant Gitte Nielsen the Chairman of the Social- and Labor market policy committee at Dansk Handicap Foundation 10 January 2024; interview with an official at SoS Racisime 15 January 2024.

hesitant and afraid of posting photographs of themselves and those affiliated with them or their activities on social media platforms because of how municipalities used these platforms to monitor their behaviour and activities.[149]

The unregulated use of social media data may pose risks to a person's rights to privacy, freedom of expression and social security under Articles 17 and 19 of the ICCPR and Article 9 of the ICESCR respectively. Social media information contains a wealth of personal information, including sensitive personal data on people's relationships, sexuality and health. The use of social media data for fraud control purposes thus constitutes overbroad surveillance whereby information that people have posted while exercising their freedom of information online is being used without adequate checks and oversight.

The use of social media data for surveillance purposes also creates a chilling effect as people are forced to censor themselves and refrain from sharing information through mediums of their choice for fear of being watched by their municipality's and/or UDK/ATP's control teams, undermining their right to freedom of expression.

Further, reliance on social media information to prove social benefits fraud may be ineffective as social media does not always reflect a person's real-life circumstances. Reliance on this information as evidence of fraud can therefore lead to wrongful assumptions of criminality based on the misinterpreting of normal or ordinary social media activity. It can erroneously restrict people's right to social security and have a negative impact on a person's mental health, due to the stress and anxiety that results from wrongful investigations and assumptions of criminality.

In addition to using social media data to identify and investigate people for fraud, a report by Politiken revealed, through information obtained under the Freedom of Information Act, that UDK uses geolocation data to check whether benefits applicants and recipients are committing fraud. The data is used to determine whether a person claiming benefits lives within or outside of Denmark, among other things.[150] In UDK's letter responding to Amnesty International's findings, they stated, however, that they do not use geolocation data. UDK should provide further clarity about the original findings contained in Politiken's report.

Use of geolocation data is restricted under Article 15 of the EU's 2022 Privacy and Electronic Communications Directive[151]:

"a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".[152]

Restrictions on the use of geolocation data are also outlined in the European Convention on Human Rights, as interpreted by the rulings of the European Court of Human Rights.[153]

This prohibition is also reflected in a 2021 ruling from the CJEU, which held that countries are prohibited from obtaining geolocation data unless they can justify the collection and demonstrate that it was needed for the purposes of "combating serious crime or preventing serious threats to public security". There is no reasonable justification for any authority to use geolocation data for the purposes of identifying welfare fraud nor any evidence that it is necessary because it is not the least intrusive method of identifying such cases.[154]

The reported use of geolocation data to track the movement of the Danish population raises concerns about the risks to people's right to privacy. It also raises concerns over the lack of transparency.

In sum, the collection and processing of large amounts of data, including sensitive data which contains characteristics that could act as proxies and reveal race and ethnicity, health, disability and sexual

[149] Focus group participant, Gitte Nielsen, the Chairman of the Social- and Labor market policy committee at Dansk Handicap Foundation on 10 January 2024; interview with a community leader at SoS Racisme 15 January 2024.
[150] Politiken, "The Danish tax authorities are keeping an eye on where thousands of citizens are - and when", 9 April 2024, https://politiken.dk/viden/art9846498/Skat-holder-%C3%B8je-med-hvor-tusinder-af-borgere-er-henne-%E2%80%93-og-hvorn%C3%A5r (in Danish).
[151] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications dir_2002_58_en.pdf (europa.eu), Article 15.
[152] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications dir_2002_58_en.pdf (europa.eu), Article 15.
[153] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Recital 11.
[154] CJEU, Judgment of the Court (Grand Chamber) of 2 March 2021 (request for a preliminary ruling from the Riigikohus – Estonia) – Criminal proceedings against H.K. (Case C-746/18), para 35.

orientation, the centralization or interoperability of databases for fraud investigations without residents' consent, and the use of social media are highly invasive and disproportionate methods to detect fraud, as well as being of questionable utility. The Danish authorities should seek less invasive means of detecting fraud.

7.2 TRADITIONAL OR ANALOGUE FORMS OF MONITORING AND SURVEILLANCE: INTERFERENCE WITH THE RIGHTS TO PRIVACY, HUMAN DIGNITY, SOCIAL SECURITY AND HEALTH

This section provides an overview of ways in which benefits applicants and recipients are subjected to traditional or analogue forms of surveillance and scrutiny for the purposes of fraud detection. These analogue forms of surveillance pre-date the introduction of UDK's fraud detection algorithms, and they continue to be used together with fraud control algorithms in the politicized quest to identify welfare fraud. These forms of surveillance restrict social security recipients' rights to privacy, human dignity, social security, further compounding the human rights violations enabled by digital forms of surveillance

7.2.1 SURVEILLANCE AND MONITORING BY MUNICIPALITIES TO ASSESS PEOPLE'S ENTITLEMENT TO BENEFITS

As discussed in Chapter 5, UDK is responsible for paying the majority of social benefits, however some are "controlled" by the municipalities and therefore decisions about whether an individual is eligible to receive these benefits are made by the municipalities themselves.[155] In addition to municipality fraud control units investigating cases shared with them by UDK/ATP, municipality control units also exercise two other forms of fraud control to assess individuals' entitlement to benefits.

Municipalities exercise fraud control at the benefits application stage to assess whether an applicant is entitled to a particular benefit. They also conduct ongoing reassessments and monitoring to determine whether benefits payments should continue.

At a focus group discussion at the Dansk Handicap Foundation, participants with disabilities told Amnesty International how challenging it is for them to access their early retirement pension.[156] This included representatives of the Foundation who also have disabilities, who receive early retirement pension and are entitled to apply for personal assistants to help them with personal care and work-related tasks because of their illness or disability. Participants also described how they are monitored and treated with suspicion by municipalities and constantly feel at risk of being accused of fraud.

A participant explained how people claiming these benefits are subjected to intrusive and unnecessary questioning about their medical histories and their ability to work when caseworkers are assessing their eligibility for benefits. This intrusive line of questioning occurs even though caseworkers have access to medical reports showing that the applicant cannot work. A staff member at Dansk Handicap Foundation shared the following experience of one of its members:

"And just two days ago, I was sitting nearby a member of the DHF [the Dansk Handicap Foundation] and they [a panel of caseworkers from the municipality] said, 'are you the one who should get earlier retirement? Or do we still see a small, tiny bit of employment effort?' And they are sitting seven people around the table asking this and it's like an interrogation for the person. It is really, really, really awful. [They kept asking the person:] 'Are you absolutely sure you have the disease you are saying you have, and couldn't it be dealt with something else? Isn't there any medicine you can get?'"[157]

[155] Interview with UDK Officials 11 January 2024.
[156] Focus group participant 'Albert' not his real name at a focus group held at the Dansk Handicap Foundation 10 January 2024; Interview with Gitte Nielson, the Chairman of the Social- and Labor market policy committee at Dansk Handicap Foundation 10 January 2024; Section 6 of the "Executive Order of the Act on Compensation for Disabled Persons in Business.
[157] Interview with Gitte Nielson, the Chairman of the Social- and Labor Market Policy Committee at Dansk Handicap Foundation 10 January 2024.

Social workers can use medical records alone to determine people's ability to work and thus do not need to employ these invasive measures. This intrusive line of questioning not only violates the claimant's right to privacy but also their right to human dignity.

Zahra (not her real name) arrived in Denmark from Iraq as a refugee and now has permanent residency in Denmark. Zahra is in receipt of early retirement pension benefit because of her inability to work due to injuries she sustained in an explosion during the Iraq War. She told Amnesty International how the municipality monitored her for four years to determine whether she was entitled to early retirement pension via a "patient rehabilitation programme". She explained how, before she was granted early retirement, she was forced to undertake challenging work despite medical reports showing that she had undergone 13 surgeries on her ears, chest and legs and was living with numerous health problems and the trauma of war. Zahra told Amnesty International:

"When I went to the job centre, they told me that I had to work... In the beginning, the nature of the work was light work, such as cleaning weeds around trees [but then I had to use a] lawn mower. I told them that the sound of the machine hurt my ears. So, [the Job Centre] transferred me to other jobs… such as a sewing workshop. There I was sewing some bags, but the sound of the sewing machine was very loud. I couldn't… The supervisors [at a school]… told me that my condition required immediate retirement, and that if it were up to them, they would have referred me to retirement immediately, but they told me that this is the law of the Job Centre[158] and that I must serve the four years."[159]

Another form of intrusive monitoring that interviewees mentioned was assessments to determine whether a person requires a personal assistant to provide them with routine domestic support. One focus group participant described how their interaction with social workers who conducts these assessments in fact seemed to be a form of monitoring of people with disabilities in order to determine whether a person is getting the correct level of personal assistance:

"They put a social worker in your home 24/7, seven days or a fortnight and follow you into the shower, into everything. It is so *humiliating*… To see if you are getting the right personal assistance. They say, 'We need to have this information to ensure that you get the right.' [They] see it as a right for them to reduce the amount of personal assistance. But what would you think if I came into your bathroom every morning and just watched [to see] if you are washing yourself correctly?"[160]

This form of excessive monitoring and surveillance is unnecessary and appears to have no additional utility in determining the level of personal assistance required, beyond intruding into the private lives of benefits recipients.

Benefit recipients are also subjected to ongoing monitoring and reassessments about their entitlement to early retirement pension and disability allowance even when a person has a permanent disability. A representative at Dansk Handicap Foundation described how, on one occasion, she had had to intervene during the assessment to stop the caseworker from asking insensitive questions. She stated:

"There was one time, and this was the only time, that I simply went beyond my companion role and hit the table hard. It was because a case manager was sitting in front of someone who was a double leg amputee. And then this young case manager says [with regard to the person's disability] 'but it's temporary'. And I simply had to say: 'Legs don't grow back once they've been amputated'."[161]

A municipality social worker explained how the process of regular reassessment was a form of control. She stated:

"[I]f you have children who have a disability, and you apply for benefits for them, we [Municipal Authorities] follow up… we follow up once a year, and it is stressful for some of these families, because once a year they

---

[158]Executive Order of the Social Pension Act (LBK no 527 of 25/04/2022), section 18.

[159] Interview with 'Zahra' (not her real name) 14 January 2024.

[160] Focus Group participant Stig Langvad of Dansk Handicap Foundation 10 January 2024. Another official stated how someone with disabilities under constant reassessment had to be able to keep digital records to document their need for personal assistants, a requirement that would as discuss in Part 7.1 above would digitally exclude a large group of people from adequately documenting their need for personal assistants. The official stated:

'You record every minute, minutes even for second for second. "What kind of help they are doing? Did they sneeze your nose? What are they doing? Oh, there was half an hour where they didn't help you. You were just sitting. That is not good. We can reduce one half an hour now. Stig, you are not having any help right now. So, you don't need 24 hours.' (Focus Group participant Gitte Nielson of Dansk Handicap Foundation 10 January 2024)

[161] Focus group participant Gitte Nielson of Dansk Handicap Foundation, 10 January 2024.

have to write again: How much was it?… We call them for an interview, and we conduct it, that is, by telephone… We call it a follow-up, but in reality, it is control: 'What are you still going to do… [how] often?… Are you still buying this number of shoes for your child? Does your child still have the challenges they had last summer?' There is absolutely no trust in the system between the system and the citizens, there is a long way to go."[162]

A focus group participant with disabilities told Amnesty International that monitoring by municipalities is also accompanied by monitoring by private pension insurance companies. The participant explained that private pension insurance companies hire private detectives to monitor a person's activities over a period of time, including taking photos of them. The aim of the surveillance is to investigate whether individuals receiving early retirement pension are committing fraud.[163] He stated the following about the role of private insurance companies hiring detectives to conduct investigations:

"I think that there is one side of this which we have not talked about, and that is about the private insurance. Everyone in the labour market [is] covered by some kind of [private] pension scheme insurance. And when you are having mobility impairment and are not able to be employed… then you should get something from your insurance. And they provide perhaps a decision for five years, and then they will follow up and see, is it still the situation? Has your leg certainly appeared again? [laughter] Or whatever… You are always risking this to be accused of being some kind of fraud… [Private insurance companies are] surveiling of all your activities over a fortnight or something… like the man in the grey coat, just watching, taking photos… [It] is not just for us with a disability. This is for everybody… everybody getting anything from Udbetaling Danmark."[164]

As detailed in Chapter 6, to comply with the human rights law requirements of proportionality, municipalities and insurance companies should rely on the least intrusive means available to them to ascertain a person's entitlement to benefits, rather than using such pervasive and invasive forms of monitoring. The least intrusive means available to determine entitlement to early retirement pension and personal assistants is through claimants' medical records. These provide the necessary information and are available to municipality social workers and private insurance companies. Therefore, the surveillance methods described by interviewees and focus group participants are pervasive and invasive and fail to meet the tests of necessity and proportionality.

Constant surveillance of benefits applicants has a negative impact on people's mental health. In a focus group discussion with people with disabilities at the Dansk Handicap Foundation, two participants described how being constantly treated with suspicion and being subject to constant reassessments had affected their mental health. A staff member of Dansk Handicap Foundation stated:

"It is eating you up. Actually, we see a lot of our members… they do have depression because of this interrogation."[165]

Another focus group participant described the anxiety that many people with disabilities felt because of this monitoring:

"[It felt like] going for a [medical] exam [or like] sitting at the end of the gun. We are always afraid [as if] if the gun is pointing at us."[166]

7.2.2 SURVEILLANCE BY OTHER PUBLIC AUTHORITIES AND BY RESIDENTS

In addition to surveillance and monitoring by municipalities and through UDK/ATP's "wonderlist", benefits applicants are also subjected to surveillance by other public authorities and fellow residents.

UDK/ATP and municipalities receive fraud control cases or reports from other public authorities including tax authorities and the police when these agencies have suspicions about a person, which municipalities then investigate.[167] They also receive anonymous and non-anonymous reports from residents reporting other residents whom they believe are committing benefits fraud. Residents can report one another via the website borger.dk or can write to or telephone either a municipality or UDK/ATP. In this way, residents can report

[162] Interview with a social worker at one of Denmark's municipalities 15 January 2024.
[163]As a participant with disabilities stated about the role of private insurance companies hiring detectives to conduct investigations: "So making a surveillance of all your activities over a fortnight or something… like the man in the grey coat, just watching, taking photos… is not just for us with a disability. This is for everybody… everybody getting anything from Udbetaling Danmark." (Focus group participant Stig Langvard of Dansk Handicap Foundation, 10 January 2024.)
[164] Focus Group participant Stig Langvard of Dansk Handicap Foundation 10 January 2024.
[165] Focus Group participant Gitte Nielsen of Dansk Handicap Foundation 10 January 2024.
[166] Focus Group participant Stig Langvad of Dansk Handicap Foundation 10 January 2024.
[167] Interview with Aalborg Municipality control unit, 14 September 2023; interview with UDK officials, 23 November 2023.

anyone on the grounds that they suspect them of committing benefit fraud because of their living arrangements, residency status and other circumstances.[168]

A participant in the Dansk Handicap Foundation focus group stated that it is common knowledge that municipalities conduct fraud investigations of people receiving child and pension benefits to determine whether they are cohabiting. The focus group participant stated that residents report each other to municipalities and that the subsequent investigations by municipalities were highly invasive:

"[We call it] 'sheet looking', because they [municipality] would say, 'Are you one or two in the bed tonight?...' [The municipality tells the claimant] 'Okay, we have been told that you have a boyfriend, and he has been sleeping with you for 14 days now, now you're not single any longer.' And that is what we call 'sheet looking'… It's common knowledge."[169]

Pervasive surveillance by fellow residents, municipalities and other public authorities interferes with benefits applicants' and recipients' right to privacy and the right to be treated with dignity. When coupled with overbroad methods of digital scrutiny, these analogue methods add up to a system of pernicious surveillance.

[168] Interview with UDK Officials 23 November 2023.
[169] Focus group participant Gitte Nielsen of Dansk Handicap Foundation, 10 January 2024.

8. STRUCTURAL DISCRIMINATION AND THE HEIGHTENED RISK OF ALGORITHMIC DISCRIMINATION

8.1 STRUCTURAL DISCRIMINATION

Structural discrimination refers to "rules, norms, routines, patterns of attitudes and behaviour in institutions and other societal structures that represent obstacles to groups or individuals in achieving the same rights and opportunities that are available to the majority of the population".[170]

Evidence in this chapter demonstrates that human rights violations that result from UDK/ATP's data and algorithmic practices are embedded within the context of discriminatory or unequal structures present in Danish society. These take the form of laws, rules, norms, patterns of attitudes and behaviour that create and promote "othering" – the idea of "them and us" (See Chapter 3.) Othering in Denmark takes the form of a hierarchy based on racism. Racism is explicitly outlawed by CERD, to which Denmark is a state party.[171]

As shown in this chapter, the discrimination within UDK/ATP's algorithms exists within the context of structural discrimination present in Danish society. Structural discrimination occurs when "society is built to exclude certain minority groups from participation in economic, political, and social institutions",[172] and "when the legal [frameworks] and institutional structures seem to afford equal enjoyment of rights to all citizens but, in effect, deny the enjoyment of their rights to one or more sectors of society".[173]

As detailed in Chapter 3, Denmark's social benefits system exists in an already hostile environment for migrants and people who have been granted refugee status in Denmark; an environment that encourages discrimination against these groups based on their race, ethnicity and religion. This hostile environment is reflected in public attitudes about race and cultural superiority, political discourses and communications by politicians on welfare in Denmark, and in existing welfare laws.

---

[170] Mirjana Najcevska, "Structural discrimination – definitions, approaches and trends (summary)", 2010.
[171] Jean-François Staszak "Other/otherness", 2008, *International Encyclopedia of Human Geography*, https://www.unige.ch/sciences-societe/geo/files/3214/4464/7634/OtherOtherness.pdf
[172] Luiza Lodder, "Understanding structural racism", February 2019, https://www.ted.com/talks/luiza_lodder_understanding_structural_racism
[173] OHCHR, "Structural discrimination: UN expert body to discuss 'the new face of racial discrimination'", 2010, https://www.ohchr.org/en/press-releases/2010/04/structural-discrimination-un-expert-body-discuss-new-face-racial

For example, section 2(1)(7) of the Executive Order of the Child and Youth Benefit Act[174] and section 5(a) of the Executive Order of the Act on Child Allowance and Advance Payment of Child Support[175] impose lengthy residency requirements for individuals seeking to claim child benefits and allowances. Both provisions state that, in order for a person to claim full child benefits, at least one of the caregivers of the child must have been resident or employed in Denmark for at least six out of the last 10 years.

This requirement disproportionately affects racialized people who have been granted refugee status in Denmark particularly from countries including Syria, Afghanistan, Lebanon and Iraq that make up the majority of refugees from non-Western countries in Denmark[176] and has a discriminatory impact on these groups. This is because people who have been granted refugee status in Denmark cannot access non-contributory benefits on an equal basis when compared to other groups due to disproportionate residency requirements. The UN Committee on Economic, Social and Cultural Rights notes that: "Non-nationals should be able to access non-contributory schemes for income support, affordable access to health care and family support. Any restrictions, including a qualification period, must be proportionate and reasonable."[177]

The European Committee on Social Rights, in a 2023 report detailing its conclusions on Denmark, stated that the residency requirements that Denmark has imposed on family benefits (child allowance and child benefits) are:

"not in conformity with Article 16 of the 1961 [EU Social] Charter on the grounds that the length of the residence requirement is excessive (i) for the entitlement to family allowance and (ii) for entitlement to child allowance for nationals of certain States Parties (non-EU/EEA) lawfully resident in the country."[178]

The negative effect of excessive residency requirements on people who have been granted refugee status in Denmark was made clear during an interview with Michala Bendixen, the Head of Refugees Welcome Denmark, an organization that works with people who have been granted refugee status in Denmark. Michala Bendixen explained that the lack of full access to child benefits adversely affects the ability of parents to provide for their children. This is compounded by the fact that refugees often cannot access the job market upon arrival because of language barriers and lack of relevant contextual knowledge and relevant networks in Denmark. Michala Bendixen stated:

"Basically, as a newly arrived refugee in Denmark, you get half of what an unemployed Danish person without private insurance or union membership would get in unemployment benefits from the state… and when it comes to foreigners, and people who have been granted refugee status in Denmark in particular, it will take those families six years until they have earned the right to full child benefits – so the first year you only get one-sixth of the full amount and then it gradually rises every year."[179]

By enacting and enforcing laws containing disproportionate and excessive residency requirements for claiming child benefits, Denmark has failed to take into consideration the best interests of children under Articles 3 and 26 of the CRC on the protection of children,[180] and is also acting in violation of the Race Equality Directive 2000/43/EC of 29 June 2000, CERD,[181] Article 21 of the EU Charter on Fundamental Rights on the right to non-discrimination,[182] and Article 9 of the ICESCR on the right to social security.[183]

Amnesty International wrote to the Ministry of Employment for a response to allegations that differential allocation of benefits based on lengthy and excessive residency requirements are disproportionate and as a result, have discriminatory impacts on people granted refugee status in Denmark. In their response, the Danish Agency for Labour Market and Recruitment, STAR stated that they did not have adequate time to obtain the input of the Ministry of Taxation which is responsible for child benefits. STAR did however, state that during the introduction of laws increasing the accrual period of child allowance and child and youth benefits, the government concluded the laws were not discriminatory because they were "compatible with Denmark's international obligations, including Article 14 of the European Convention on Human Rights

[174] LBK no. 724 of 25/05/2022.
[175] LBK no. 63 of 21/01/2019.
[176] Refugees Welcome Denmark, *Well-Founded Fear – Credibility and Risk Assessment in Danish Asylum.*
[177] CESCR, General Comment 19 (previously cited), para. 36.
[178] European Committee on Social Rights, Conclusions XXII-4 on Denmark, March 2023, https://rm.coe.int/conclusions-xxii-4-2023-denmark-en-2769-0339-2521-1/1680aedd43, p. 6.
[179] Interview with Michala Bendixen, Head of Refugees Welcome Denmark 12.01.2024
[180] Articles 20, 21, 25.26, Charter of Fundamental Rights of the European Union (2000/C 364/01).
[181] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012; The International Convention on the Elimination of All Forms of Racial Discrimination 1965.
[182] Articles 20, 21, 25.26, Charter of Fundamental Rights of the European Union (2000/C 364/01).
[183] International Convention on Economic, Social and Cultural Rights 1966. Accessed on 11.10.2024 at: [International Covenant on Economic, Social and Cultural Rights | OHCHR].

regarding the prohibition of discrimination." [184] They further stated that child and youth benefits and child allowances are supplementary benefits rather than basic welfare benefits. Individuals covered by the accrual rules are entitled to basic welfare benefits and other benefits, including needs-based single benefits under the Act on Active Social Policy, provided that the conditions for these are met.

Regardless of the entitlement of other basic welfare benefits, Amnesty International highlights the findings of the European Committee on Social Rights' 2023 report that finds excessive residency requirements to be disproportionate, particularly in the case of child benefits which are non-contributory. Authorities in Denmark should review these laws and clearly assess the discriminatory impacts arising from the lengthy residency requirements.

It is in this existing context of a hostile environment for already marginalized groups that the fraud control models' fraud detection efforts are being deployed by the UDK.

These structures are part of the algorithmic models' design and enable the creation and promotion of categorizations based on difference or "othering". This categorization is defined in laws, rules, norms and patterns of attitudes designed or established by dominant groups in Denmark that appear to be neutral or colour-blind but, in reality, can have a discriminatory effect.

UDK/ATP's use of fraud control algorithms to identify social benefits applicants and recipients likely to commit fraud risks dangerously and disproportionately targets already marginalized groups. Data inputs used to create, train and operate AI systems are often reflective of historical, systemic, institutional and societal discrimination[185] and, consequently, so are the outputs (in this case, identification of potentially fraudulent benefits recipients). Thus, the introduction of fraud control algorithms risks entrenching historical injustice against marginalized communities in the context of welfare. These are people whom UDK/ATP have constructed as "others" in Danish society because they have differing or "unusual" living or family arrangements or "foreign affiliations". Marginalized groups are politically constructed by Danish authorities as more likely to commit fraud or as underserving of benefits because of certain characteristics they embody (discussed in detail below). These same characteristics or variables can act as proxies for race, migration status and socio-economic status in fraud detection, all of which the Udbetaling Danmark Act allows for the collection of in large quantities, thus encouraging discrimination.

INDIRECT & DIRECT DISCRIMINATION THROUGH ALGORITHMIC PROXY

The HRC defines discrimination as "any distinction, exclusion, restriction or preference, which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms."[1]

Article 2(2)(a) of the EU Race Equality Directive defines direct discrimination as occurring "where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin". Article 2(2)(b) defines indirect discrimination as occurring "where an apparently neutral provision, criterion or practice would put persons of a racial or ethnic origin at a particular disadvantage compared with other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary."[1]

A proxy is an input or variable, such as an individual quality defining human beings, that is used by an AI system to make distinctions between individuals and/or social groups. A proxy may appear to be an innocuous piece of data to be included in an algorithm. Yet, where it directly or indirectly correlates with a protected characteristic such as gender, age, race or ethnicity, a proxy leads to biased decisions being generated by the AI system.

For example, when an input such as postcode is included within an algorithm, it is often correlated with, and becomes a proxy for, socioeconomic status and race. It may therefore indirectly discriminate against certain racial or ethnic groups due to historical residential segregation. In short, discrimination by proxy here is very similar to discrimination by association, which is a form of discrimination that relies on elements that are predictive of one or more protective criteria that could be grounds for discrimination.

[184] Right of Response from the Ministry of Employment 01.11.2024.
[185] Virginia Eubanks, Automating Inequality (previously cited).

Amnesty International's 2021 report *Xenophobic Machines* highlighted the risk of discrimination by proxy.[1] An algorithm introduced in the Netherlands for childcare benefits fraud detection included an input of whether the citizen had Dutch nationality, which acted as a proxy for race, ethnicity and social origin. The algorithm systematically assigned higher risk scores to those without Dutch nationality, meaning the system was discriminating on this basis.[1]

Amnesty International has found in its research on Denmark that categorization based on "othering" or difference risks indirectly and directly discriminating against low-income groups, racialized groups, migrants and people who have been granted refugee status in Denmark, ethnic minorities, people with disabilities, and older people. This has negative outcomes for these groups both because their rights to equal treatment and non-discrimination are violated and because there are also risks that they are denied their right to social security.

In the context of the Netherlands, a former UN Special Rapporteur on extreme poverty and human rights has expressed concerns that the use of emerging digital technologies in the provision of social welfare resulted in human rights violations against the poorest and most marginalized groups.[186] These concerns were echoed by a former UN Special Rapporteur on contemporary forms of racism, who noted in a 2019 report that a move towards digitized welfare systems can "produce racially discriminatory structures that holistically or systematically undermine enjoyment of human rights for certain groups, on account of their race, ethnicity or national origin, in combination with other characteristics".[187] In the report, the Special Rapporteur on contemporary forms of racism also urged states to "deploy a structural understanding of the prohibition on racial discrimination in line with international human rights law" and not only address "explicit racism and intolerance in the use and design of emerging digital technologies, but also, and just as seriously, indirect and structural forms of racial discrimination that result from the design and use of such technologies".[188] The Special Rapporteur on contemporary forms of racism further stated that governments should "reject a 'colour-blind' approach to governance and regulation of emerging digital technologies, one that ignores the specific marginalization of racial and ethnic minorities and conceptualizes problems and solutions relating to such technologies without accounting for their likely effects on these groups".[189]

In its response to Amnesty International, UDK rejected findings the report that discriminatory structures are embedded in the design of the algorithm models, but did not provide additional responses or explanation on this finding. As detailed in the subsequent sub-sections of this Chapter, what seem to be neutral policies and features in UDK/ATP's models to identify "unusual" patterns in behaviour as an indicator of benefits fraud, are in fact design features that risk discriminating against marginalised groups based on their migration status, race, class, disability, age, and marital or relationship status.

8.2 UNUSUAL HOUSEHOLD, FAMILY AND RESIDENCY PATTERNS

Denmark has several social security schemes in the pension and childcare domains that provide supplementary payments to people who are single. To check for fraud, the authorities deploy the "Really Single" algorithm to predict a person's family/relationship status. These fraud control algorithms include inputs and variables that appear neutral, but which are not. They are driven by norms, standards or ideas developed by dominant or powerful groups in Denmark of what a household or a family is or should be. The norms that underlie the predictions made by UDK/ATP's fraud control algorithms fail to consider differing and evolving cultural norms based on the diverse cultural differences present in Denmark that inform living arrangements and household composition. They also fail to consider contextual factors such as existing inequalities within Danish society based on race, ethnicity, class and disability that affect living

[186] UN Special Rapporteur on extreme poverty and human rights, "*Amicus curiae brief* in the case of NJCM c.s./De Staat der Nederlanden (*SyRI*) the District Court of The Hague (Rechtbank Den Haag). Case Number C/09/550982/ HA ZA 18/388", 2019, https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf
[187] UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis*, 18 June 2020, UN Doc. A/HRC/44/57, para. 38.
[188] UN Special Rapporteur on racism, *Racial Discrimination and Emerging Digital Technologies* (previously cited), para. 48.
[189] UN Special Rapporteur on racism, *Racial Discrimination and Emerging Digital Technologies* (previously cited), para. 48.

arrangements. As a result, these algorithms risk disproportionately targeting low-income groups and groups that have differing family and housing composition, such as people with disabilities, racialized communities, and older people, compared to "traditional" or "mainstream" Danish families.

One of the main principles behind UDK/ATP's fraud control models is to identify unusual or atypical living patterns or arrangements, relationship patterns and residency patterns as an indicator of fraud. The "Really Single" algorithm, which is used to control supplementary pension and child allowance payments made to single people, employs a supervised anomaly detection ML approach which is, by design, an algorithmic model to flag social benefits recipients who are statistical "outliers". The core idea is to repeatedly split the data based on a number of inputs (detailed in Chapter 5.2) and to subsequently identify claimants who look substantially different from most other beneficiaries (across the select data points included within the model) based on variables such as the size of and number of people living in a single home, and evidence of cohabitation.

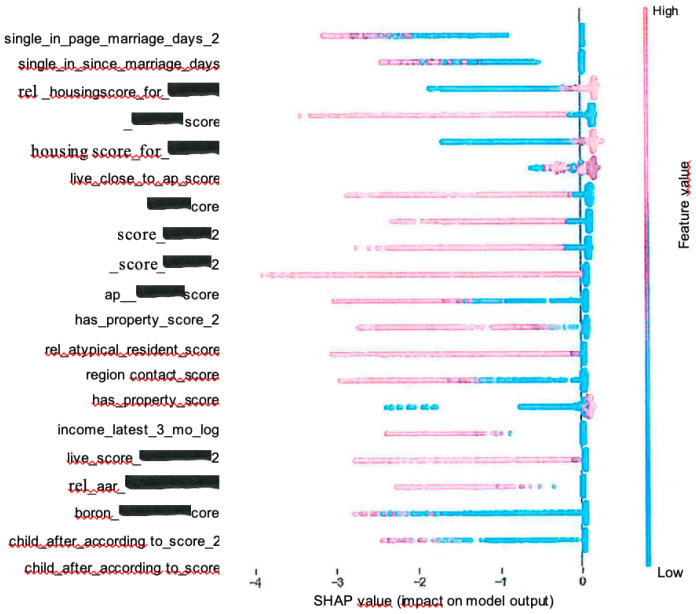
Figure 2 below provides SHAP (SHapley Additive exPlanations) values for the "Really Single" model. SHAP values were developed in AI research to improve the explainability of algorithmic outputs and they provide an indication of the importance, or "weighting", of each input to the model. Documentation shows that UDK generates multiple inputs related to housing and residency (for example "housing score" and "rel atypical resident score") which are included in the algorithm and appear to be heavily weighted, significantly impacting the prediction. Although information on how each input is precisely constructed is redacted, it is clear that, at a minimum, the model will incorporate information on the size and number of rooms of the beneficiary's home.[190] In practice, given that the model is built to detect statistical outliers, this is likely to target beneficiaries that live in a large home alone, or beneficiaries that live in a smaller space with an "unusually" high number of residents.[191]

No ML model is likely to be 100% accurate. They are fallible in two key ways: incorrectly labelling something as true (false positives), and incorrectly labelling something as false (false negatives). For example, in the context of UDK's algorithms, a false positive occurs when a system incorrectly labels a legitimate case as fraudulent or erroneous, and a false negative occurs when the system labels a fraudulent or erroneous case as legitimate. Developers must always strike a balance between these two errors, as one cannot be reduced without risking an increase to the other.

The consequences of incorrectly labelling an application as fraudulent or erroneous are serious as this means an individual or family may be incorrectly investigated. UDK provided information on the performance of its Really Single algorithm in response to Amnesty International's RoR. Statistics from 2023 showed 54% of cases opened by the control unit were in fact legitimate. To ensure it does not violate people's rights, UDK must ensure false positives do not occur.

[190] FOI response from UDK/ATP, 26 April 2024.
[191] Documentation provided by UDK officials in response to FOI request by Amnesty International.

FIGURE 2: SHAP VALUES DETAILING THE IMPORTANCE OF INPUTS TO THE "REALLY SINGLE" MODEL



According to statements made in interviews by UDK/ATP officials, as well as documentation submitted by UDK/ATP in response to Amnesty International's FOI requests, UDK/ATP uses data held in various public databases (discussed in Chapter 5) including the central persons register (CPR) and the buildings and dwellings register (BBR), despite concerns about the accuracy of data contained in these databases.[192] These databases are used to determine: (a) a person's residency and citizenship – whether a person is registered at the correct address and whether they live at the address; (b) whether a person is single or in a relationship and whether they are cohabiting with a partner; and (c) whether a person is living with other people as part of their household (of particular interest is the number of people in a household). Points (b) and (c) are used by UDK/ATP to assess household composition.[193]

In an interview, UDK/ATP officials summarized the data points from the CPR and BBR on which they rely to identify unusual residency and relationship patterns as follows:

"[In] the CPR [we look at a person's] name… address… status, are you married or not, Danish citizen? Are you in the country… And in the BBR [we look at whether the house or building is registered in the person's name person and size and structure of the house or building] square meters, number of rooms… how many kitchens, how many bathrooms… the energy source for your house… So, this is what we use."[194]

During an in-person interview with UDK/ATP officials in January 2024, officials stated that a residential address recorded in the CPR database with "far too many residents" in relation to its size would be regarded as an indicator of fraud.[195] They stated that, in such cases, UDK/ATP models would flag this as a suspicious case and open a fraud investigation. In particular, UDK/ATP seeks to confirm whether people claiming supplementary pensions or child benefits are in fact living at a residence they claim to live in and whether they live with a partner or the partner lives elsewhere .[196] Another indicator of fraud would be if officials came across a "very strange residence pattern" such as "20 grown-up people registered in a flat with only two rooms".[197] An official at the Copenhagen Municipality Control Unit stated during an interview with Amnesty International that the control unit also uses large household size as an indicator for fraud when investigating

[192] Regarding errors in the CPR and BBR databases, an official stated:
"there were a lot of mistakes because people need to inform if there are changes on the address. Otherwise, all the information in there will be from when the house was built, if you don't actually update it… if you own a house, you have an interest in making sure that information is correct… But more errors in the BBR than the CPR, I would say." Interview with UDK officials, 11 January 2024.
[193] Interview with UDK officials, 11 January 2024; interview with UDK officials, 23 November 2023.
[194] Interview with UDK officials, 11 January 2024.
[195] Interview with UDK officials, 23 November 2023.
[196] Interview with UDK officials, 11 January 2024.
[197] Interview with UDK officials, 11 January 2024.

cases on child, pensions and State Education Fund (or SU grants) benefits fraud from UDK/ATP's "wonderlist" and cases it receives from public authorities and residents.[198]

UDK does not clearly define within the law what constitutes "unusual" or "atypical arrangements" in regard to households, leaving the door open to arbitrary decision-making. However, following Amnesty International FOI's request, UDK shared guidelines about its case-processing practices. The guidelines reveal that UDK/ATP uses a broad and subjective definition of cohabitation. This definition creates a risk that UDK/ATP have the power to define a large number of people as cohabitors who need to be investigated for fraud. The Common Rules for Family Benefits and Pension guidelines used by UDK/ATP's Joint Control Unit caseworkers define cohabitation as follows:

"A person is considered [to be] cohabiting when they share the same household with another person with whom it is possible to marry [and that] cohabitation occurs when the persons have the same financial and practical advantages that married and cohabiting people have by having two people paying fixed and current expenses and two people doing the practical work in the home".

However, the guidelines also state:

"There are no fixed boundaries for when a person is single or cohabiting… You can be considered cohabiting without being in a relationship with the person or intending to get married."[199]

This broad definition of cohabitation creates a risk that people or groups living in the same household in what are regarded as "unusual" living or family arrangements are more likely to be flagged for fraud.

The use of fraud control models such as the "Really Single" model on data drawn from the CPR and BBR databases to identify unusual residency and relationship patterns risks disproportionately targeting and surveilling people with non-traditional living arrangements, such as people with disabilities, older people, low-income groups and migrants. This is because, for example, due to cultural preferences, households with people from migrant backgrounds tend to be composed of multigenerational families, unlike "traditional" Danish households.[200] A 2022 study of ethnic minority elders in Denmark found that ethnic minorities lived in extended families where they share a home with children and grandchildren and that "while only 3 percent of the majority Danish elderly live in this way… 14 percent of the Arab elderly, 22 percent of the elderly from Turkey and as many as 41 percent of the elderly from Pakistan"[201] lived in extended families. Additionally, low-income groups in Denmark often have no choice but to live in large households because they lack the means to access housing on their own.[202]

The human rights risks of UDK/ATP's use of "unusual" residency and family relationships as an indicator for fraud were evident during interviews with officials at civil society organizations and an affected individual. In a focus group at Dansk Handicap Foundation, a participant receiving pensions benefits claimed that he had received a letter from the municipality investigating his marital status and stating that it should be changed to "separated", because his wife lives in a nursing home due to her disability. He described the exchange to Amnesty International:

"[They said:] 'Are you still married, because now you live in two different addresses, and you should be separated.' I got so angry, and said to them: 'Why should we separate? We love each other, we have been married for a long time – 46 years this year – so we don't intend to separate or to live apart in other ways than we have to, because of her disability'… We had to prove that we were still married. I had to sign a letter, telling them that we are still married, and we don't intend to separate and to divorce… It didn't have any impact on our relationship, but our relationship with the municipality was at a very low point.'[203]

A former head of the Citizens Service in Denmark also described the complexities involved in defining family arrangements and relationships because these structures are increasingly fluid. He also stated how overbroad and vague definitions that fail to consider contextual and differing norms can be problematic. He drew on a case he and his team had investigated that examined the household composition of a couple

[198] Interview with Copenhagen Municipality fraud control unit, 4 September 2023.
[199] FOI response from UDK/ATP dated 19 April 2024.
[200] Interview with former social worker in Mjølnerparken, 13 January 2024; interview with an academic and board member of the Centre for Muslim Rights Denmark, 22 May 2024; Kirsten Just Jeppesen and Anne Nielsen (1995) Tosprogede småbørn i Danmark Rapport nr. 4 fra forløbsundersøgelsen af børn født i 1995, Socialforskningsinstitutte
[201] Anika Liversage and Mikkel Rytter, 'De nye gamle: Karakteristika ved den voksende gruppe etniske minoritetsældr.' 2022, https://danskgerontologi.dk/wp-content/uploads/2022/06/202215.pdf (in Danish).]
[202] Interview with an academic and board member of the Centre for Muslim Rights Denmark, 22 May 2024.
[203] Focus group participant 'Charles' (not his real name), at Dansk Handicap Foundation, 10 January 2024.

identified for fraud investigation prior to the setting up of UDK/ATP, which highlighted the complexities of defining a family or household. He stated:

"I had a lot of discussions with my staff about this issue. [For example], we had a couple and they were divorced, he lived on the 4th floor to the right and she lived on the ground floor to the left... They had three children [who spent] time where they wanted to, up and down. They ate together twice a week, and shared an old car – in order to take children to their various activities they needed the car. [This arrangement can be regarded as if these two parents] have a common household but they don't. They have their individual lives and just made a very good arrangement… we cannot [impose] our own morals or our own sense of what a family is... we have much more varied types of families and types of arrangements and people divorcing."[204]

The complexities surrounding definitions of household composition were also expressed in interviews with an official from Dane Age Association who claimed that the organization has, in the past, received reports of older pensioners being investigated for fraud on the grounds that they are cohabiting because they spend a lot of time with a particular person, although they do not live together. She described the challenges that people face when trying to prove that they live alone because an assessment of whether or not people are cohabiting can be very subjective, intrusive and stressful. It is difficult for a person to prove that they are single, yet they face losing the benefits they are claiming as a single person. She stated:

"We occasionally hear… about someone who has been asked to indicate how much they spend time together, and whether they have a financial relationship, and whether they eat together every day, and so on. Whether they do practical tasks for each other… It's typically a letter they get from Udbetaling Danmark. And Udbetaling Danmark knows about it… they get anxious. It's hard to prove that they are not as together as Udbetaling Danmark thinks… You can't prove it. You can prove it by showing how much electricity you use or water you use or something like that. But it's not that easy."[205]

This evidence demonstrates that the use of what seem to be neutral policies and features in UDK/ATP's models to identify "unusual" patterns in behaviour as an indicator of benefits fraud can lead to stress and anxiety, particularly for marginalized communities, when faced with needing to prove that they are not cohabiting.[206] This evidence also shows that the use of these policies and features in UDK/ATP's models can lead to indirect discrimination of groups based on their migration status, race, class, disability, age and marital or relationship status, which can subsequently lead to denials of the right to social security if they are forced repay the benefits they have received, or if benefits are unduly delayed. The European Court of Human Rights, in acknowledging the existence of indirect discrimination, has stated that "a difference in treatment may take the form of disproportionately prejudicial effects of a general policy or measure which, though couched in neutral terms, discriminates against a group".[207]

UDK/ATP should therefore re-examine its policies on the use of unusual residency and family or household patterns as indicators for fraud, to prevent the disproportionate targeting of marginalized groups. UDK/ATP should also stop the blanket use of vague and overbroad definitions that do not consider contextual factors such as the living arrangements of people with disabilities, older persons, migrants and other marginalized groups, to prevent indirect discrimination.

8.3 FOREIGN AFFILIATION OR TIES

In addition to identifying unusual patterns in household composition, our research has found that inputs related to "foreign affiliation" are used by UDK/ATP as part of its algorithmic models, particularly within pensions and child benefit distribution. UDK/ATP implement this to "control" benefit recipients who they believe may have moved abroad without informing the agency and therefore may be unjustly taking their social benefits with them. Within the European Economic Area (EEA), this is a relatively uncomplicated process as Denmark has specific agreements in place with these countries, however, it is more complex in non-EEA countries where Denmark may not necessarily have an agreement in place.[208] To do this, UDK/ATP

[204] Interview with a former head of the Citizens Service in Denmark, 25 October 2023.
[205] Interview with an official at Dane Age, 16 October 2023.
[206] Universal Declaration of Human Rights 1948 and the International Convention on Economic and Social Rights 1976.
[207] Amnesty International, *Europe: A Human Rights Guide for Researching Racial and Religious Discrimination in Counter-Terrorism* (Index: EUR 01/3606/2021), 2019, https://www.amnesty.org/en/documents/eur01/3606/2021/en/ p. 33.
[208] ATP, "Udbetaling Danmark – Internationally", https://www.atp.dk/en/our-tasks/processing-welfare-benefits/udbetaling-danmark-internationally (accessed 10/10/2024).

uses the "Model Abroad" algorithm, which acts as a filter to prioritize the investigation of cases where they believe social security beneficiaries have "strong ties" to countries outside of the EEA.

As part of its targeting of people with foreign affiliations for fraud investigations, our research has also found that UDK uses data collected by the Joint Data Unit Abroad on residents' foreign residence, entry and exit abroad, marital status, number of children, real estate or vehicles abroad and social benefits received, to be used within its algorithm (as detailed in Chapter 5) to flag people for further investigation for social benefits fraud.[209]

The "Model Abroad" algorithm generates a score for a beneficiary's "foreign affiliation" by creating a relative measure of an individual's "strength of ties" with each country. Amnesty International only has partial information on the model's inputs and specific deployment cases; however, the documentation indicates that although "foreign affiliation" is not included directly as a risk factor or indicator, the "Model Abroad" model attempts to identify groups of beneficiaries who are deemed to have "medium and high-strength ties" with non-EEA countries, and prioritizes these groups for fraud investigations. This is constructed as a relative metric, meaning "medium and high-strength ties" are defined in relation to other social security beneficiaries rather than being defined by objective criteria.

The documentation obtained on the "Model Abroad" model details retrospective testing of the model on previous cases that have been investigated to assess where the strength of foreign affiliation to non-EEA countries is statistically correlated with previous known fraud or control cases. In practice, the documentation obtained from the FOI requests indicates that, although foreign affiliation will not be used directly as an input to identify fraud, it is used to refine the search for cases that UDK will target for fraud investigations and is therefore a de facto indicator:

"As can be seen from previous sections, there is thus good sense in removing cases from the heaps with High or Medium non-EEA affiliation. It is therefore agreed with HOK (the UDK/ATP control unit) that we focus the search on these two groups and select those with the most "wonderful" [linked to "wonderlist" – highest risk] living conditions in the usual way".[210]

The model directly includes citizenship as an input, and therefore the model is likely to in effect, prioritise cases based on nationality as a marker, directly discriminating against people who are considered to have non-EEA affiliation. The use of features such as foreign ties or affiliations can act as a proxy for race, religion, and ethnicity, which can fuel direct discrimination against groups based on these identity markers, thus violating their right to equality and non-discrimination, which is protected in various human rights treaties.[211]

UDK refused to provide statistical data to allow Amnesty International to conduct statistical bias and fairness testing to assess if the model discriminates against or disparately affects minority groups. Nevertheless, in an in-person interview, UDK/ATP officials stated that when using algorithmic models, they investigate citizenship and foreign ties to determine whether a person is committing pension and child benefits fraud. Regarding the use of foreign affiliation in pension fraud investigations, an official stated:

"We [look at] citizenship… [because] when you retire in Denmark and you are of foreign citizenship, you have a larger incentive to move [back] home [because]… you have family you would like to go home to… You do have a larger draw towards [moving] abroad… And in that case, we actually [by looking at foreign affiliation in our models, give only] a slight unfairness towards Danes, because we have a little bit lower rate [of Danes moving abroad when they retire] than [we do] the foreigners. That's often because we can't really connect [foreigners] to a country, and if we can't connect them to a country, then it's very difficult to know where they actually stay."[212]

While the Danish authorities can use residence, and notably tax residence, to evaluate eligibility for social security schemes, evaluating a person's "ties" with foreign countries based on a self-constructed set of vague criteria is not justifiable or objective based on this research, and is unlawful and discriminatory. There is no reasonable justification to use foreign affiliation-related inputs in a fraud control model to check whether a person is residing in the country for pensions and childcare benefits, or whether a citizen is taking their social security entitlement outside of the EEA, given that these do not evidently correlate to fraud.

First, the use of citizenship and other foreign affiliation-related criteria explicitly targets people from countries outside the EEA and therefore directly discriminates on the basis of nationality, race, ethnicity and migration

[209] ATP, "Udbetaling Danmark – Internationally" (previously cited).
[210] FOI response from UDK/ATP dated 26 April 2024.
[211] For example, the International Covenant on Economic Social and Cultural Rights, the International Covenant on Civil and Political Rights and International Convention on the Elimination of All Forms of Racial Discrimination, Amnesty International (2021), 'Xenophobic machines *(previously cited)*.
[212] Interview with UDK Officials 23 November 2023.

status. This violates the right to equality and non-discrimination of racialized groups under Article 2(1)(a) of CERD and various other international human rights instruments (see Chapter 6). Second, the model and metric produced are created in-house at UDK/ATP and the indicators that are seen as markers of foreign ties do not accurately reflect the reality of individuals. In practice, people can have complex relationships with a variety of countries, and indicators such as entries to and exits from a country, or bank accounts opened in other jurisdictions, are not definitive evidence of someone living abroad. Finally, using foreign affiliation-related inputs are not the least intrusive means available to check whether someone is residing in Denmark; other simpler indicators such as tax residency are easily available.

The use of foreign affiliation within UDK/ATP's algorithmic models as a filter to triage fraud investigations, and therefore as a de facto indicator of fraud, also risks interfering with people's right to social security, specifically migrants and members of racialized communities within Denmark, who could be denied social security on the basis of these markers.

The use of foreign affiliation also creates opportunities for the promotion of racial ideologies claiming that foreigners are more prone to commit fraud and are more deceitful, which are then used to justify the need to control the distribution of benefits.

UDK/ATP state in their response to Amnesty International, "the control consists of two modules, that is attachment to Denmark and attachment abroad. If a person is attached to Denmark, it weighs more than any attachment to abroad. Furthermore, to fall out for follow up, it is assumed that a citizen has weak or no attachment to Denmark and at the same time has medium or high attachment to a country outside Denmark. Citizenship in a country outside Denmark weighs low, and citizenship alone will always only give a weak attachment to the country in question".[213]

Regardless of the weight of the inputs, the use of "foreign affiliation" related inputs are discriminatory for the reasons outlined in this Chapter.

UDK also claimed that information about citizenship is "a non-sensitive personal data that objectively links a citizen to a country." However, the use of citizenship as a feature could reveal a person's race, ethnicity, migration status, and directly discriminate on the basis of national origin and therefore falls under the definition of sensitive data under Article 4 of the General Data Protection Regulations (GDPR), which defines sensitive data as including data that reveals a person's racial and ethnic origin.

8.4 RISK OF DISCRIMINATING AGAINST LOW-INCOME GROUPS THROUGH POOR ANALYTICAL PRACTICE

Of particular concern across several of UDK's fraud control algorithms is the risk of direct or indirect discrimination against low-income groups. As detailed in Chapter 5.3, "income" is directly included as an input in both the "Really Single" and "Model Abroad" algorithms, and "salary" is directly included within the "Fictitious Employment" model. As discussed in Chapter 3, these algorithms are not simply cross-referencing income databases to ensure beneficiaries are meeting any income-related eligibility criteria. Rather, they include inputs such as income to distinguish between beneficiaries and classify them into risk categories. Depending on the type of ML model deployed, this occurs in different ways.

Where models rely on historical cases of fraud and use supervised ML approaches, this risks entrenching and perpetuating bias against low-income groups if they have historically been overrepresented in fraud investigations. Although Amnesty International does not have requisite access to information to make an assessment on this, there is a particular concern in the "Fictitious Employment" model's design. The algorithm is trained using 25 historical cases of maternity benefit fraud, all dating back to 2016, which analytically constitutes a very small sample size to draw general conclusions about the characteristics of beneficiaries that are likely to commit maternity benefit fraud in the future. In other words, UDK's model to assess all applicants is based purely on a small number (roughly 30) of instances of fraudulent or erroneous cases from just one year, which raises significant concerns about how representative these cases are.

Moreover, by directly including salary as an input, UDK runs the risk of discriminating against low-income groups if low-salaried individuals were historically more often targeted for fraud investigations, possibly making them overrepresented in the sample of 30 cases. In this way, the "Fictitious Employment" model risks introducing feedback loops which perpetuate the over-targeting of these groups. Further, the small sample size raises significant questions as to how efficacious any algorithm or model built from them can be. The documentation obtained did not include any detail on the model's performance.

[213] Right of Reply Response from UDK 30 October 2024.

Where models rely on unsupervised ML approaches, such as those within the "Really Single" model, we cannot determine the effect that the inclusion of income-related inputs will have without further information. The documentation does not provide exact details on the weighting of income-related inputs and their effect on the risk designations the models make. However, it does contain information that the income input is attempting to identify people reporting lower incomes:

"The income feature is used, among other things, to find citizens who have such a small monthly income that it is unlikely that they can manage with their own income."[214]

Alongside this, the SHAP values (Figure 2 above) demonstrate that they have a presence within the model and a not-insignificant effect on the outcome for a beneficiary. Including inputs related to an individual's salary and income is intended to ensure that the system distinguishes between beneficiaries on this basis. Although the evidence is not conclusive, it suggests the model risks explicitly disadvantaging and explicitly targeting beneficiaries on lower incomes. UDK must provide greater transparency on its analytical practice to ensure this is not the case.

In addition, as noted in Chapter 8.2, use of proxies like unusual household, family and residency patterns also risk disproportionately targeting low-income groups.

The evidence presented in this section from Amnesty International's research shows that, although the Danish welfare system is often regarded as being based on a high level of trust,[215] this claim does necessarily always hold true. The benefits fraud control system is, at its core, facilitated by unequal structures present in Danish societal institutions that promote and exacerbate discrimination against marginalized groups or individuals, in particular low-income groups and those with marginalized ethnic or racial backgrounds. This discrimination could prevent certain individuals from accessing and achieving the same rights and opportunities available to the majority of the population.

[214] Documentation obtained in FOI response from UDK/ATP dated 26 April 2024.
[215] "Trust a cornerstone of Danish culture", Accessed on 23 April 2024 at: https://denmark.dk/people-and-culture/trust

9. DIGITAL EXCLUSION AND FORCED INCLUSION OF GROUPS

While automation of UDK's benefits fraud control system facilitates surveillance of and discrimination against marginalized groups, Amnesty International has also found that the digitization of UDK's system leads to exclusion.

This chapter uses evidence gathered primarily from individual and focus group interviews with social benefit applicants and recipients with disabilities, disability advocates and a municipality official, as well as a survey of caseworkers in women's crisis centres. It highlights the ways in which digitization of UDK's benefits system unduly restricts the right to social security by excluding potential and existing beneficiaries from the benefits system rather than increasing inclusion and expanding the reach of social programmes for these groups.

Social security benefits applicants and recipients, specifically persons with disabilities, are also unfavourably included in the benefits system by being forced to share their data with third parties to access social security, which creates data privacy risks.

9.1 DIGITAL EXCLUSION, INDIRECT DISCRIMINATION

Technology can disproportionately exclude marginalized groups from accessing public services to which they are entitled.[216]

Amnesty International's research has found that automation and digitization of the benefits system in Denmark allows for the exercise of surveillance and control over benefits applicants and recipients. Moreover, it has found that the system creates a barrier to accessing social benefits for some marginalized groups including women in crisis centres and people with disabilities and, as a result, risks restricting their right to social security and discriminating against groups based on their gender and disability. Digitization also risks exclusion of older persons. The UN OHCHR states that one of the key components of the right to social security is accessibility. Specifically, that "all persons should be covered by the social security system, especially the most disadvantaged and marginalized groups, without discrimination… [and that] beneficiaries of social security schemes must be able to participate in the administration of the social security system."[217]

[216] UN Special Rapporteur on racism, *Racial Discrimination and Emerging Digital Technologies* (previously cited), paras 7 and 40.
[217] OHCHR, "OHCHR's overview on the right to social security/social protection", www.ohchr.org/sites/default/files/documents/issues/socialsecurity/2022-10-07/One-pager-social-protection-Socialsecurity.pdf (accessed on 3 October 2024).

Anyone applying for benefits from UDK is required to do so online on the government portal, www.borger.dk, and benefits applicants and recipients are required to communicate with UDK/ATP and municipalities through "the digital post" or digital e-boxes. When accessing UDK/ATP's system via the government portal, applicants or benefits recipients are also required to use their personal digital ID, known as MitID, to identify themselves, which requires the use of a smart phone.[218]

The digitization of the benefits system is a barrier to accessing social benefits for some marginalized groups, either by excluding them completely or making it challenging to access these benefits. As a staff member at Dansk Handicap Foundation stated in relation to the extensive digitization of the benefits system: "You can't even apply for a new wheelchair or a seating pillow… You are not able to apply for anything in Denmark without digitalization."[219]

Amnesty International collaborated with LOKK (Denmark's National Organization of Women's Shelters), an umbrella non-profit organization and trade association that represents 46 women's shelters around Denmark, to design a survey to study the accessibility of UDK's system for women residing in shelters due to intimate partner violence. Some 40% to 50% of women in these shelters are migrants – including from Southeast Asia, the Middle East and Northeastern Africa.[220] In survey responses provided by caseworkers from 25 women's crisis centres, 28% of crisis caseworkers stated that women in the shelters did not have access to the technology required to apply for social benefits from UDK because they do not have access to the internet, computers, MitID and NemID.[221] This could be because, as one researcher at LOKK told Amnesty International, women in shelters tend to be isolated from the Danish system and from family and friends as a result of being exposed to sexual and other forms of physical, verbal and economic violence for long periods of time before they have access to a shelter.[222] As a result, they often do not have the capacity and resources to exercise their rights, including their right to social security, because of their circumstances.

Women's right to access UDK's social security system comes under Article 13 of CEDAW and Article 9 of the ICESCR. Article 13 of CEDAW provides that states must "take all appropriate measures to eliminate discrimination against women with respect to social benefits." [223]

A social worker in one of Denmark's municipalities told Amnesty International that older people could also face challenges using technology to apply for benefits from UDK and could be forced to rely on their adult children to make applications for benefits for them and to access and read messages from UDK/ATP and municipalities in their digital e-boxes.[224] These claims are supported by studies that show varying degrees of digital exclusion among older people, with some studies stating that between 15% to 23.8% of people aged 60 and above in Denmark experience digital exclusion.[225]

To protect the rights of older people, Denmark has obligations under Article 23 of the European Social Charter 1996 to adopt measures that enable older persons to participate in social life, "to remain full members of society for as long as possible".[226] Additionally, a UN Human Rights Council resolution calls upon states to "promote and ensure the full realization of all human rights and fundamental freedoms for older persons, including by taking measures to combat age discrimination".[227] Denmark should carry out its obligations under Article 23 of the European Social Charter to ensure that older people have adequate access to the UDK benefits system.

Amnesty International has also found that, although section 5 of the Executive Order of the Act on Digital Post from Public Senders[228] states that certain groups, including people with disabilities, can be exempted from the use of technology to access the UDK/ATP system and can instead use traditional methods of communication such as postal mail and in person attendance, UDK and municipalities appear to have strict practices that all communications must be conducted digitally. This practice by municipalities was

---

[218] Focus group participants 'Albert', 'Anton' and 'Arne' (not their real names), at the Dansk Handicap Foundation focus group, 10 January 2024.
[219] Focus group participant Gitte Nielsen of Dansk Handicap Foundation, 10 January 2024.
[220] Informal interview with a representative of LOKK (Denmark's National Organization of Women's Shelters), 11 December 2023.
[221] Survey designed by Amnesty International's Algorithmic Accountability Lab in collaboration with LOKK and conducted by LOKK on behalf of Amnesty International in October 2023.
[222] Interview with a researcher at LOKK, 11 December 2023.
[223] Convention on the Elimination of all Forms of Discrimination Against Women 1979 accessed on 8 May 2024 at: [Text of the Convention on the Elimination of All Forms of Discrimination against Women (un.org)]
[224] Interview with a social worker at one of Denmark's municipalities, 15 January 2024.
[225] iAge, *Barriers and Needs in ICT Use of Older People: A Transnational iAge Study*, 2014, http://archive.northsearegion.eu/files/repository/20141216163625_PO14101602-iAgeBarriersandneedsinICT-compleet-LR.pdf
Zinran Lu and others, "Digital exclusion and functional dependence in older people: findings from five longitudinal cohort studies", December 2022, eClinicalMedicine, Volume 54, https://www.thelancet.com/journals/eclinm/article/PIIS2589-5370(22)00438-2/fulltext
[226] European Social Charter (revised) 1996, Council of Europe, European Treaty Series - No. 163.
[227] UN Human Rights Council, Resolution 24/20 on the human rights of older persons, 27 September 2013, UN Doc. A/HRC/RES/24/20.
[228] Act on Digital Post from public senders, (LBK nr 686 of 15/04/2021), https://www.retsinformation.dk/eli/lta/2021/686, section 5.

confirmed by a focus group participant with disabilities who is also the National Chairman of Dansk Handicap Foundation.[229]

A social worker in one of Denmark's municipalities also noted during an interview that people with disabilities face access barriers to their right to social security because of the government's general practice policy on the digitization of social benefits for all groups.[230]

Focus group participants at Danish Handicap Foundation described how, because of their disabilities – including cognitive impairments and cerebral palsy, multiple sclerosis and spinal cord injuries, conditions that lead to paralysis of a person's arms and legs – they cannot access the UDK benefits system unless they rely on family members or personal assistants.[231]

Some participants described not being able to hold or swipe their smart phone or scan the QR code on the computer with their smart phone to access their MitID because of paralysis of hands or muscle weakness. Those with cognitive disabilities said they cannot use digital options because they have trouble with memory, learning new things, concentrating or making decisions that affect their everyday life. A focus group participant with multiple sclerosis summarized the challenges he and other people with disabilities face:

"I have sclerosis or multiple sclerosis. I have paralysis in my legs, my arms and my hands, which means that I can't use a smartphone or a tablet, so I have to use a very ordinary PC, computer and with the help of a special programme I use, called OnScreen Keys… The only thing I can't use is MitID… I have to talk to my assistant or another person to help me get my MitID. I can get it on the screen, but I can't, even with the card number reader I had to get – I can't see the six-digit number there. So, I have to have my disability supporter tell me that."[232]

To guarantee the human rights of persons with disabilities, the Danish government is required, under Article 4 of the CRPD, to adopt legislative, administrative and other measures, including modifying practices and customs that facilitate discrimination against persons with disabilities. Article 9(1) of the CRPD specifically calls on governments to eliminate obstacles and barriers to accessibility in respect to information technologies in order to enable persons with disabilities to "live independently and participate fully in all aspects of life".[233]

The digitization of the UDK/ATP system has made *the benefits system difficult to access for people with disabilities and women* in crisis centres, thus restricting their rights to social security and to equality and non-discrimination, and leading to their social exclusion, "a state in which individuals are unable to participate fully in economic, social, political and cultural life, as well as the process leading to and sustaining such a state".[234] It entails lack of access to material resources and agency or control over decision making.[235] Digitization also risks the exclusion of older persons.

Amnesty International wrote to UDK and the Ministry of Employment for a response on the allegations that marginalised groups are excluded from accessing the UDK benefits system due to digitisation.

STAR responded by stating that citizens with disabilities or others who face challenges have the opportunity to receive assistance or to be exempted from digital requirements when accessing UDK's benefits system. Although STAR claims that people can be exempted from digital requirements when accessing social benefits from UDK, testimonial and survey evidence gathered by Amnesty in this report shows that in practice people with disabilities and women in crisis face challenges in accessing the benefits system.

The Danish government must, therefore, ensure access for women in crisis centres, older people and people with disabilities who face difficulties in accessing UDK/ATP's benefits system because of digitization. Access to systems must not be solely and exclusively digital in practice, and authorities must provide viable alternatives in policy and practice. Authorities must ensure systems are inclusive and accessible for the most disadvantaged and marginalized groups without discrimination, such that all groups in society can participate in the administration of the social security system.

---

[229] Focus group participant Susanne Olsen, National Chairman of Dansk Handicap Foundation, 10 January 2024.
[230] Interview with a social worker at Copenhagen Municipality 16.01.2024
[231] Focus group participants Stig Langvard, Gitte Nielsen, Susanne Olsen and 'Albert'(not his real name) at the Dansk Handicap Foundation focus group, 10 January 2024.
[232] Focus group participant 'Felix' (not his real name) at the Dansk Handicap Foundation focus group, 10 January 2024. This view was echoed by another focus group participant who has two children with muscular dystrophy ('Albert' [not his real name], at the Dansk Handicap Foundation focus group, 10 January 2024).
[233] CRPD, Article 4 and 9(1).
[234] UN Department of Economic and Social Affairs, *Leaving No One Behind: The Imperative of Inclusive Development*, 2016, www.un.org/esa/socdev/rwss/2016/full-report.pdf, p.18.
[235] UN Department of Economic and Social Affairs, *Leaving No One Behind: The Imperative of Inclusive Development* (previously cited), p.18.

9.2 FORCED INCLUSION OR UNFAVOURABLE INCLUSION, DATA PRIVACY RISKS

Amnesty International also found that, while persons with disabilities are excluded from using the UDK system as a result of digitization, they are also unfavourably included in the benefits system. Some interview and focus group participants stated that the digitization of UDK's social benefits system and their inability to access the system as a result of their disabilities meant that they were forced to share their personal information with third parties – state assigned personal assistants – to access the system, which creates data privacy risks for them.[236]

They expressed concerns that, although their personal assistants signed consent forms undertaking to keep their personal information confidential, relying on personal assistants to access the benefits system created data privacy risks and infringed on their right to privacy and exposed them to potential identity fraud.[237] Participants explained that, in order to access the UDK system, a person must share their secret personal mobile phone log in codes with five or six personal assistants each week or about 50 personal assistants in their lifetime.[238] A focus group participant summarized the view expressed by several participants:

"Every single time I have to enter a MitID, I have to have my disability helper, or wife, or whoever is nearby, to whom I dare to entrust the information, to stand and watch the screen where I enter my codes… Then I have to have a helper, or my wife, or others take my smartphone and read the code that is sent and tell me what to write on the screen. But every single time, it's my life at stake when I share personal information [with] a third person. And it is my identity that can be stolen from me on a daily basis, several times."[239]

This evidence highlights how people with disabilities have no option but to risk their right to privacy to be unfavourably or forcibly included in UDK/ATP's system. Unfavourable inclusion is defined as "being forced to be included in deeply unfavourable terms".[240] People with disabilities are forcibly or unfavourably included because they have no choice but to share their data with third parties. This inclusion leads to data security concerns for them because of risks surrounding the misuse of their personal information by personal assistants to commit fraud. Misuse of personal information through identity theft or fraud can lead to concrete injuries for people with disabilities, including financial losses and emotional distress.[241]

The Danish government must therefore ensure that any digitization laws and policies it implements do not violate the right to privacy of people with disabilities as guaranteed under Article 17 of the ICCPR. It must also assess the risks associated with access to data by third parties under existing laws to ensure that there are adequate protections under the law to protect marginalized groups against risks of data misuse.

Amnesty did not receive a response from STAR on the allegation that people with disabilities are unfavourably or forcibly included in the benefits system at the time of publication of this report.

---

[236] Focus group participants 'Ingrid' and 'Albert' (not their real names) at the Dansk Handicap Foundation focus group, 10 January 2024; Focus group participants, Gitte Nielsen, Susanne Osen and Stig Langvad at the Dansk Handicap Foundation focus group, 10 January 2024.
[237] Focus group participants 'Ingrid' and 'Albert' (not their real names) at the Dansk Handicap Foundation focus group, 10 January 2024.
[238] Focus group participants, Gitte Nielsen, Susanne Osen and Stig Langvad at the Dansk Handicap Foundation focus group, 10 January 2024.
[239] Focus group participant 'Noah' (not his real name) at the Dansk Handicap Foundation focus group, 10 January 2024.
[240] Amartya Sen, *Social Exclusion: Concept, Application And Scrutiny*, 2000, https://www.adb.org/sites/default/files/publication/29778/social-exclusion.pdf
[241] Daniel J. Solove, "The new vulnerability: data security and personal information", 2008, in Anupam Chander and others (eds), *Securing Privacy in the Internet Age* pp. 111-136; Helen Nissenbaum, "Securing trust online: wisdom or oxymoron?", 2001, Boston University Law Review, Volume 81, Issue 3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573181

10. LACK OF STATE OVERSIGHT AND TRANSPARENCY, AND RISKS TO REMEDY

The Danish government has delegated public authority in the distribution of benefits to the ATP Group (ATP), a private entity established as a self-governing institution under the ATP Act 1964.[242] ATP is Denmark's largest pension and processing company.[243] ATP's activities are regulated by Danish law which gives it the power to administer pensions and other statutory schemes. In addition to this, ATP also provides "technical and administrative" assistance to UDK for social protection schemes that fall within UDK's responsibilities.[244] ATP is accountable to the state[245] but also has its own human rights responsibilities as a corporate entity. (See Chapter 6 on the Methodology for a discussion of ATP's corporate responsibilities.)

As such, this chapter is split into two sections:

- Part 10.1 discusses the failure by Danish Authorities – namely UDK's board of directors, the Ministry of Employment and the Danish Data Protection Authority – to provide adequate oversight over UDK/ATP's activities.
- Part 10.2 discusses the failure by municipalities and ATP to put in place mitigation measures to ensure that their practices respect human rights.

10.1 LACK OF EFFECTIVE OVERSIGHT BY THE DANISH GOVERNMENT AND UDBETALING DANMARK

The UN Committee on Economic, Social and Cultural Rights notes that states have an obligation to respect economic, social and cultural rights and a duty not to prioritize the interests of business entities over Covenant rights. The Committee clarifies that the duty to respect economic, social and cultural rights entails the adoption of "legislative, administrative" measures, "to ensure effective protection against Covenant rights violations linked to business activities".[246]

[242] ATP, "About us" (previously cited).
[243] ATP (2024) "The Organisation", https://www.atp.dk/en/about-us/organisation (accessed on 10 October 2024).
[244] ATP, "Corporate governance in the ATP Group", https://www.atp.dk/en/dokument/corporate-governance-atp-group (accessed on 10 October 2024).
[245] ATP, "Corporate governance in the ATP Group" (previously cited).
[246] CESCR, General Comment 24 (previously cited).

Additionally, the Committee notes that states should require "business entities to exercise human rights due diligence in order to identify, prevent and mitigate the risks of violations of Covenant rights". The imposition of human rights due diligence requirements extends to private actors involved in a "business entity's supply chain and by subcontractors, suppliers, franchisees, or other business partners".[247]

Amnesty International's research has established that there is a lack of adequate, independent oversight over UDK/ATP's data and algorithmic practices, creating risks of human rights violations. As Principle 1 of the UN Guiding Principles makes clear, states' international human rights law obligations require them to respect and protect human rights in the context of corporate activities through regulation, oversight, investigation, adjudication and punishment. States' obligations are based on the human rights treaties they have ratified and other international standards. Furthermore, Principle 5 of the UN Guiding Principles states that governments should exercise "adequate oversight in order to meet their international human rights obligations when they enter into contracts with corporations to provide services which may have an impact on the enjoyment of human rights". [248]

10.1.1 THE MINISTRY OF EMPLOYMENT AND UDBETALING DANMARK

By delegating authority to ATP, the government has given ATP broad discretion to use data and algorithms for fraud control purposes without proper oversight over its activities. In 2012, UDK, the public authority responsible for the distribution of social benefits in Denmark, entered into an administrative agreement with ATP outside of usual public procurement rules. ATP was exempted from complying with public procurement rules because, according to interviews with UDK/ATP officials, it has the trust of the Danish government and the necessary apparatus to administer the distribution of benefits on behalf of the Danish government. It has also handled similar tasks as a technical supplier on behalf of other government authorities.[249]

While UDK is responsible for the payment of a number of public benefits including pension, child and maternity benefits, it is ATP that acts as the technical and administrative supplier of services for UDK. It conducts register mergers for fraud control, designs the fraud control algorithms in collaboration with private companies and uses these algorithms to flag individuals for benefits fraud. Amnesty International's research has found that UDK does not have any employees and that, under the administrative agreement between UDK and ATP, ATP is the supplier of technical services and provides all of the employees and IT for UDK's operations.[250]

Although UDK's board of directors – which is supervised by the Ministry of Employment – is responsible for ensuring that ATP fulfils the tasks specified in the Udbetaling Danmark Act,[251] the board does not have supervisory oversight over ATP's daily data and algorithmic practices. ATP not only designs the fraud control models in collaboration with other companies, like NNIT, but it is also responsible for creating and implementing GDPR and data guidelines in its fraud control practices. The board of directors does not have a say over the creation or implementation of these guidelines. UDK/ATP officials stated:

"[ATP] are also the ones who create GDPR, data security, ethical guidelines, and things like that. Which then goes across the organization. And the board [at UDK] can't really do much about that. The board can't say that we don't want higher or lower GDPR security and things like that."[252]

Additionally, although the Ministry of Employment receives annual reports from UDK's board of directors about UDK/ATP's compliance with data protection laws, it does not supervise the daily activities of UDK and ATP, including the tasks of the Joint Data Unit. In a response to Amnesty International's request for information on whether it has oversight over UDK/ATP data and algorithmic practices, the Ministry stated:

"Please note that Udbetaling Danmark is an independent administrative authority and that the Ministry of Employment does not have the power to instruct Udbetaling Danmark. This means that the Ministry of Employment does not issue instructions to Udbetaling Danmark/ATP regarding case processing or training of employees etc."[253]

---

[247] CESCR, General Comment 24 (previously cited), para. 16.
[248] UN Guiding Principles on Business and Human Rights page 8.
[249] Interview with UDK officials, 22 November 2023.
[250] Responses to FOI requests made to the Ministry of Employment dated 4 December 2023.
[251] Interview with UDK officials, 22 November 2023.
[252] Interview with UDK officials, 22 November 2023.
[253] Responses to FOI requests made to the Ministry of Employment dated 4 December 2023.

The Ministry's supervisory role is primarily aimed at ensuring UDK fulfils its objectives under section 19 of the Udbetaling Danmark Act[254] which are: guaranteeing the efficiency of the administration of the benefits system through digitization and ensuring better fraud control by "preventing cheating and erroneous social benefits payments".[255]

Amnesty International sought to obtain a response to the allegations made in this report about the lack of adequate and independent oversight by the Ministry of Employment and UDK Board of directors over UDK and ATP's algorithmic practices prior to publication of the report. In their written responses dated 1 November 2024, the Ministry of Employment through the Danish Agency for Labour Market and Recruitment (STAR), the agency that supports the Minister for Employment in the work of policy formulation and implementation, rejected the findings in Amnesty International's report.

In its written responses, STAR stated that, in its assessment, there is adequate oversight over UDK's use of data and algorithmic practices. STAR claimed that UDK's Board "provides an account of GDPR compliance in connection with [its] annual oversight," and that both the Board and the Danish Parliament "have the opportunity to continuously request information and follow up on ongoing oversight cases and UDK's administration more broadly."

Although STAR claims in its written responses to the allegations that the Board and Parliament have oversight over UDK, as discussed above, evidence STAR provided to Amnesty International in its FOI responses dated 4 December 2023 reveals that they are crucial oversight gaps in the supervision of UDK and ATP. In the said FOI response, STAR states that the oversight provided by the Board under the law is limited to ensuring the efficiency of the administration of the benefits system through digitization and ensuring better fraud control by "preventing cheating and erroneous social benefits payments".[256]

The Ministry of Employment's supervisory authority does not therefore focus on ensuring compliance with human rights with respect to UDK and ATP's data and algorithmic practices.

Further, the lack of oversight over UDK and ATP's data and algorithmic practices is also, as discussed above, detailed by STAR in its FOI responses to Amnesty dated 19 April 2024. In this FOI response, STAR stated that the Ministry of Employment "does not have powers to instruct UDK [or to] issue instructions to Udbetaling Danmark/ATP regarding case processing or training of employees etc."[257] Additionally, STAR in its FOI dated 4 December 2023 stated that while it supervises UDK directors, it "does not supervise the day-to-day operations of Udbetaling Danmark." [258]

10.1.2 THE DANISH DATA PROTECTION AUTHORITY

In addition to the lack of appropriate oversight over UDK/ATP through Udbetaling Danmark's board of directors and the Ministry of Employment, FOI responses from the Danish Data Protection Authority found that the Authority's supervisory power under the Danish Data Protection Act and the GDPR are limited. In response to Amnesty International's FOI request about whether it has oversight over UDK/ATP's data and algorithmic practices and whether it has investigated any complaints about UDK's use of data and fraud control algorithms, the Data Protection Authority stated that the responsibility to ensure that appropriate safeguards were in place during UDK/ATP's data processing lay with the data controller, in this case UDK/ATP as per Article 24 of the GDPR.[259] The Authority also stated that it can only monitor and intervene under Article 57 of the GDPR to ensure an entity's adherence with data protection when it receives inquiries or complaints about a company or organization and that the decision to conduct Data Protection Impact Assessments lays primarily with UDK/ATP, the data controller, as specified in Article 35 of the GDPR.[260] The self-regulatory requirements specified in Article 24 of the GDPR and the requirements that investigations be triggered by the logging of complaints with the Authority limits the Authority's powers to ensure that entities exercise due diligence and comply with their legal obligations under the Danish Data Protection Act and the GDPR in the use of data and algorithmic systems. As the AI systems used by UDK/ATP are opaque and people are rarely aware that they are selected for fraud investigations because of the decision of an algorithm, they are less likely to make complaints about how these systems affect them.

[254] Responses to FOI requests made to the Ministry of Employment dated 4 December 2023.
[255] Responses to FOI requests made to the Ministry of Employment dated 4 December 2023.
[256] Responses to FOI requests made to the Ministry of Employment dated 4 December 2023.
[257] Responses to FOI requests made to the Ministry of Employment dated 19 April 2024.
[258] Responses to FOI requests made to the Ministry of Employment dated 4 December 2023.
[259] Responses to FOI requests made to the Danish Data Protection Agency dated 7 November 2023.
[260] Interview with an official from the Data Protection Authority, 8 October 2023.

The limited powers of the Danish Data Protection Authority under the GDPR and the Danish Data Protection Act further show that there is a lack of adequate and independent oversight over UDK and ATP data and algorithmic practices. The Danish Data Protection Authority should investigate UDK and ATP's data and algorithmic practices in light of the information revealed in this report.

The oversight gaps evident in the existing UDK/ATP governance structure and the lack of proactive investigatory powers of the Danish Data Protection Authority are clear failings of the Danish government to respect and protect human rights by ensuring that there is effective oversight over the public authority UDK as well as the company ATP which is accountable to the state. The Danish government, specifically the Ministry of Employment as the supervisory authority with oversight over UDK, has failed to act in accordance with human right laws and standards.

Further, the Danish government should establish binding laws for the creation of an independent supervisory authority to supervise UDK and ATP's algorithmic practices.

10.2 LACK OF TRANSPARENCY AND FAILURE TO IMPLEMENT MITIGATION STRATEGIES

10.2.1 LACK OF TRANSPARENCY AND FAILURE TO CONDUCT ANTI-BIAS AND ANTI-DISCRIMINATION TRAINING

The lack of oversight over UDK and ATP is compounded by the fact that ATP and municipalities do not conduct anti-bias and anti-discrimination training for their caseworkers. Such training can be one measure to mitigate the risk of and prevent any actual harmful human rights effects of UDK/ATP's data and algorithmic practices.

MINISTRY OF EMPLOYMENT AND MUNICIPALITIES

Amnesty International wrote to the Ministry of Employment on 18 March 2024, Copenhagen and Alborg Municipality Control Units on 25 March 2024, and the control units of Ishoj and Aarhus municipalities on 27 March 2024 to request information on whether they conduct anti-bias and anti-discrimination training.

In its reply, the Ministry of Employment failed to respond to whether UDK conducts such training, although it did state that an audit of UDK has not revealed any evidence that "the data processor [has] contravened the requirements of the legislation concerning Udbetaling Danmark, the data protection rules in force at any time or other public law legislation".[261]

The FOI responses from Aarhus, Aalborg, Ishoj and Copenhagen municipalities stated that their caseworkers do not undergo bias and anti-discrimination training prior to or when analysing and processing data and using fraud control algorithms to investigate benefit fraud.[262] The municipalities did, however, claim that case processing in fraud investigations is conducted in full compliance with the GDPR, Data Protection Act, Danish Legal Security Act and Public Administration Act.[263]

ATP

Amnesty International wrote to ATP on 25 March 2024 to enquire whether ATP conducts anti-discrimination and bias training for its caseworkers and whether the third-party developer company of its fraud control algorithms – NNIT – is required to adhere to data protection and human rights requirements when developing its algorithms.

ATP, in its FOI response, stated that its caseworkers follow guidelines and standards on how to handle cases and complete GDPR training, but they did not specify whether caseworkers receive anti-discrimination or bias training. ATP also stated that it does not have any requirements in place for third-party suppliers of its IT systems, including NNIT, to comply with data protection and human rights requirements because this

[261] Responses to FOI requests made to the Ministry of Employment dated 25 March 2024.
[262] Responses to FOI requests made to UDK/ATP dated 19 April 2024, and to Aarhus, Aalborg and Copenhagen municipalities dated 12 April 2024.
[263] Responses to FOI requests made to Aarhus, Aalborg and Copenhagen municipalities dated 12 April 2024.

supplier "does not carry out data-driven control of Udbetaling Danmark's services" despite them developing UDK/ATP's fraud control models.

10.2.2 FAILURE TO PROVIDE INFORMATION ON DATA PROTECTION IMPACT ASSESSMENTS

Although the Ministry of Employment, municipalities and DK/ATP claim that their fraud control practices are in compliance with the GDPR and the Danish Data Protection Act, Amnesty International has not been able to verify these claims. This is because neither UDK/ATP, nor the Ministry of Employment, nor Copenhagen, Aalborg, Aarhus or Isjoh municipalities have provided Amnesty International with the requested information on the findings of any data protection impact assessments they have conducted on their practices prior to and during the development and use of UDK/ATP's fraud control algorithms.

10.3 LACK OF TRANSPARENCY: STATISTICS AND TECHNICAL AUDITS

Technical evaluations and audits have become an increasingly popular tool to assess the performance and impact of algorithms and diagnose problematic behaviour. They can play an important role in helping companies to identify, prevent and mitigate actual and potential harm linked to their algorithmic systems. As demonstrated by the audit showing that the Danish Ministry of Employment's STAR algorithm was discriminatory (discussed in Chapter 3), audits are a useful tool to assess for any algorithmic bias or discrimination in their design or outputs.[264]

Audits can include a range of approaches to examine algorithms such as checking governance documentation, testing an algorithm's outputs and impacts, or inspecting its inner workings.[265] The basic premise of an audit is to monitor the outcomes of an algorithm, then map these back to the inputs to build a picture of how the algorithm may be functioning.

Amnesty International submitted FOIs requesting access to the documentation for the algorithmic models, including, crucially, what inputs are used for each. Redacted documentation was provided; however, the information on the algorithms' inputs was excluded. This was on the grounds that UDK cannot disclose the inner workings of the models to Amnesty International, as doing so would allow general insight into how the controls work, allowing people who commit fraud to know how to evade these controls. As described in the methodology section, Amnesty International sought to circumvent these issues by requesting statistical data to conduct bias and fairness testing of the models' outputs. UDK/ATP denied all requests for the demographic data required to do this, on the basis that they do not have the relevant data and therefore cannot provide this information.

Denial of these requests demonstrates a lack of transparency from UDK to release crucial information that allows its algorithms to be scrutinized and tested. Additionally, it suggests that UDK is not equipped to conduct its own adequate bias and fairness testing, if this data is not easily available to UDK's analysts. In an interview with UDK in January 2024, Amnesty International sought to understand UDK's current approach to bias and fairness testing. UDK's current approach has focused on equalizing the "true positive rate" (TPR)[266] of its algorithms across different demographic groups:

"But we are very conscious about the fact that the actually positive cases that needs to be... Yeah, this needs to be roughly the same [across different demographic groups]."[267]

Although there is an ongoing debate within the academic community regarding how best to measure bias and fairness statistically, the deployment of only one metric is an insufficient and inadequate process for testing, and thus for identifying, the potential for harm. The use of TPR alone has several significant

[264] Cathrine Seidelin and others, "Auditing risk prediction of long-term unemployment", 2022, Proceedings of the ACM on Human-Computer Interaction, Volume 6, https://dl.acm.org/doi/10.1145/3492827
[265] Danaë Metaxa and others, "Auditing algorithms: understanding algorithmic systems from the outside in", 2021, Foundations and Trends in Human-Computer Interaction, Volume 14, Issue 4, https://ieeexplore.ieee.org/document/9627858
[266] In statistics and ML, the true positive rate (TPR) is a measure used to evaluate the performance of a classification model such as the fraud-control algorithms discussed in this report. It represents the proportion of actual positive cases that were correctly identified or classified as positive by the model. TPR is also known as sensitivity, recall or hit rate. In the case of UDK, it is a measure of the proportion of 'true' fraud and error cases that were correctly identified as such.
[267] Interview with UDK/ATP officials, 11 January 2024.

drawbacks. The primary concern is that it does not take into account the number of individuals that are wrongly accused of fraud (the false positive rate) as it does not measure this, and second, it neglects other commonly proposed measures of fairness such as demographic parity. In practice, this means UDK is not adequately keeping track of how often its algorithms incorrectly accuse beneficiaries of fraud or error. When Amnesty International requested access to documentation of the evaluations and tests conducted, UDK denied this request on the grounds that it did not keep this information, highlighting the poor internal analytical practice at UDK and a lack of transparency.

As discussed above, the UN Guiding Principles make clear that companies should communicate the human rights impacts of their practices publicly, including how they are addressing these impacts,[268] while "providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders".[269] Similarly, the OECD Due Diligence Guidance also provides guidance on how companies can communicate how their impacts are being addressed. However, UDK has refused to release important information which would allow its algorithms to be scrutinized, thus failing to carry out human rights due diligence in line with international standards. Furthermore, UDK's current approach to fairness testing of deploying one metric is an inadequate measure for assessing and identifying the impacts of its algorithmic systems.

The Danish government should mandate that UDK/ATP discloses copies of contractual arrangements it has entered into with NNIT, including data sharing arrangements it has with these companies, and details of the workings of its fraud control models and any reports of data protection impact assessments conducted by UDK, ATP, or NNIT. The Danish government should ensure that ATP proactively and adequately discloses all relevant information pertaining to statistics and technical audits.

10.4 CORPORATE RESPONSIBILITIES AND LACK OF HRDD OF THE ATP GROUP

As discussed in Chapter 10.1, the Danish government has delegated public authority in the distribution of benefits to ATP, Denmark's largest pension and processing company, which is accountable to the Danish government. ATP is responsible for designing the fraud control part of UDK's Joint Data Unit. To develop its profiling models, ATP has partnered with a multinational corporation, NNIT.

NNIT develops maternity benefits fraud control models based on ATP's specifications. ATP retains control over the data models and has the capacity to make alterations; however, this is often done in collaboration with NNIT as outlined above.[270] Amnesty International has not assessed whether NNIT is fulfilling their responsibility to respect human rights in relation to their business relationship with ATP.

As discussed above, under the UN Guiding Principles, companies should avoid causing or contributing to adverse human rights impacts through their own activities and should address such impacts when they occur. This corporate responsibility to respect human rights is independent of a state's own human rights obligations. To fulfil this responsibility to respect human rights, ATP, as a private actor, should "have in place policies and processes appropriate to their size and circumstances, including… a human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights".[271]

Amnesty International could not find any information on ATP's human rights due diligence policies or practices. Furthermore, as discussed above, ATP does not appear to be conducting anti-bias or anti-discrimination training for its staff which is a critical element of what would be an appropriate human rights due diligence process in the use of algorithmic systems. Additionally, ATP does not appear to publish data protection impact assessments nor is it conducting adequate audits of its fraud control algorithms. All of these are measures which ATP could undertake to either identify or mitigate the risk of potential harm related to its algorithmic systems.

Given the central role that ATP plays in UDK's use of fraud control models, ATP is contributing to the human rights violations perpetrated by the Danish government, namely the creation of a hostile system based on surveillance and intrusion into people's private lives, which results in violations of people's rights to privacy, non-discrimination and social security, among other rights. Furthermore, ATP is failing to conduct human

[268] UN Guiding Principles Commentary on Principle 21, p. 23.
[269] UN Guiding Principles Commentary on Principle 22, pp. 23-24.
[270] Interview with UDK/ATP officials, 11 January 2024.
[271] UN Guiding Principles on Business and Human Rights, Principle 15, pp. 15

rights due diligence in line with international human rights standards in order to identify, mitigate and prevent the harmful impacts of the UDK/ATP benefits system and is thus failing to respect human rights.

Amnesty International wrote to UDK and ATP on 18 October 2024 for a response to allegations that they do not appear to be conducting human rights due diligence processes. In our letter, we asked UDK and ATP the following questions:

a. what human rights due diligence policy and processes they have in place to identify, mitigate, prevent and account for its actual or potential impacts on human rights

b. whether ATP did any human rights due diligence on its relationship with UDK and operations to distribute state benefits before entering into an agreement with UDK?

c. if ATP conducts HRDD on its operations to distribute social benefits, what risks and abuses has it identified and what steps has it taken to mitigate the risks and prevent abuses?

UDK/ATP did not provide detailed responses to our questions at the time of the publication of the report.

Amnesty International also wrote to the multinational company NNIT noting that they have been named in this report, and also asking them for information about contractual arrangements between UDK/ATP and NNIT, as well as information about NNIT's human rights due diligence practices. NNIT did not provide further information about contractual arrangements citing confidentiality obligations, and did not provide specific information about any human rights due diligence it undertook before entering into its agreement with UDK/ATP.

10.5 LACK OF AN EFFECTIVE REMEDY, ALGORITHMIC OPACITY

International human rights law requires that, when human rights violations occur, individuals are guaranteed the right to an effective remedy and the right to adequate redress.[272] The UN Special Rapporteur on freedom of expression has highlighted how automated decision-making systems often interfere with the right to remedy because individuals are often unaware of the scope, extent or even existence of the algorithmic decision-making processes that may have an affect their rights, and because these systems cannot be scrutinized.[273]

Amnesty International has found that there is a risk that persons flagged for fraud by UDK/ATP may not have access to effective remedy for two main reasons.

First, Amnesty International has identified a risk to the right to remedy caused by the lack of transparency and clear notification regarding UDK/ATP's use of fraud control algorithms in the distribution of benefits. During an interview with an official from Copenhagen Municipality Control Unit in September 2023, the official stated that social benefit recipients flagged for fraud by UDK/ATP's algorithms receive letters from municipalities stating that a residence case has been opened against them as a result of a register merger or register coordination. The official stated that recipients of these letters often do not know what "register merger" or "register coordination" means and often resort to calling the municipality to find out what the letter means.[313]

On 7 September 2023, Amnesty International obtained a template of the letter that Copenhagen Municipality sends to people flagged for a fraud investigation. The relevant parts of the letter read as follows:

"Today, the Control, IT Security and Licensing Board (the Control Unit) has opened a residence case regarding your residence conditions. The control unit will check whether it is correct that you live and reside permanently at the address... You have been selected in a registry comparison... The register coordination has been carried out by the Joint Data Unit under Udbetaling Danmark. The information from the register coordination was then obtained in the Control Unit. The information concerns your place of residence and any public benefits. The control unit finds that, on the basis of the information, there is a need for a closer examination of your residence conditions… The Control Unit works in accordance with the Act on the Central Population Register (CPR Act) and must ensure that residence registrations in the Central Population Register (CPR) are correct. When there is a

[272] Universal Declaration of Human Rights, Articles 8 and 10; ICESCR, Article 2; CERD, Article 6.
[273] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 29 August 2018, UN Doc. A/73/348, para. 40.

question about incorrect registration of residence, the Control Unit is obliged to carry out an investigation of this, cf. section 10(1) of the CPR Act. It is on this basis that the residence case has been created…

Registry coordination means that your information in a number of public registers has been combined based on certain criteria. The purpose of register coordination is to ensure that public benefits are paid on a correct basis. The Joint Data Unit carries out register coordination for the municipalities and Udbetaling Danmark in connection with their control work…

In connection with the investigation of your residence case, the Control Unit will obtain further information about the case. If you have information about where you live, how you live and who you may live with that can help shed light on the case, you are welcome to send it to the Control Unit. You also have the option of sending documentation in the form of a copy of, for example, the lease agreement, rent payment, bank statement, etc. You can send secure mail to "ATT: The control unit" in the subject line. In the field "Specify what your enquiry is about", select "Report a move in Denmark"

Once the Control Unit has processed the information, you will either be contacted by telephone, by letter or be summoned to an interview where you have the opportunity to present further information and give your explanation."[274]

While the letter does not outline what inputs or indicators are used to flag people for fraud, it does indicate that the basis for the fraud investigation is to assess whether the recipient lives at the address where they claim to live. The letter provides an imperfect opportunity for the recipient to exercise their right to remedy if they present evidence of where they live. The investigation may be closed once they do so, and the affected person has a right to appeal the decision. Nevertheless, the process may be onerous and stressful to recipients.

In addition, the lack of full transparency about what a residency investigation means, including the fact that the decision is partially based on an algorithm, means that the recipient does not have all the information they need about the basis of the investigation to exercise their right to remedy. Additionally, sending the letter to people with lower digital literacy levels and those who find it challenging to access their digital e-boxes because they do not have access to technology, as discussed in Chapter 9, creates challenges for these individuals to exercise their right to remedy.

Second, Amnesty International has found that the Public Administration Act (*forvaltningsloven*)[275] does not offer adequate opportunities for social security benefits applicants subjected to automated decision-making to seek remedies. Section 19 of the Public Administration Act places obligations on a public authority, prior to making any decision, to notify the person affected by the decision that it is in possession of specific unfavourable information on the facts of the case and to give the person the opportunity to make a statement. Nevertheless, the Act does not contain provisions that mandate public authorities to inform a person that the case against them has resulted from an algorithm. As a result, because a person flagged for further fraud investigations by UDK/ATP algorithms is unaware that they have been the subject of a semi-automated process, they are not in a position to effectively challenge UDK/ATP's decision-making process.

[274] Template letter on the opening of a residence case from Copenhagen control unit, 7 September 2023.
[275] LBK nr 433 of 22/04/2014.

11. DENMARK'S FORTHCOMING OBLIGATIONS UNDER THE EU AI ACT

As discussed in Chapter 6.6, Denmark will be required to comply with the relevant transparency, accountability and remedial requirements of the EU Artificial Intelligence Regulation (AI Act),[276] which came into force on 1 August 2024. The enforcement of most of its provisions commences in August 2026; however, the enforcement of prohibitions mandated under the AI Act commences in February 2025.[277] The AI Act introduces a uniform framework across all EU countries, implementing a tiered risk-based approach whereby AI systems are categorized into one of the following:

1. Minimal risk: Most AI systems such as spam filters and AI-enabled video games face no obligation under the AI Act, but developers and deployers of AI systems can adopt codes of conduct for voluntary application of specific requirements under the AI Act, including the requirements for high-risk systems.
2. Limited risk with specific transparency obligations: Systems like chatbots must clearly inform users that they are interacting with a machine, while certain AI-generated content must be labelled as such.
3. High risk: High-risk AI systems such as AI-based medical software or recruitment systems must comply with strict requirements. Developers of such systems must include risk-mitigation systems, high-quality of data sets, clear deployer information, human oversight and other safeguards. Deployers must conduct fundamental rights impact assessments, alongside a suite of public and individual transparency obligations.
4. Unacceptable risk: For example, AI systems that allow "social scoring" by governments or companies are considered a clear threat to people's fundamental rights and are therefore banned.

The obligations on UDK/ATP will be dependent on the relevant category the algorithmic models are legally considered to fall under. Under Article 5(1)(c) on prohibited AI practices, the Act bans the "use of AI systems for the purpose of the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

[276] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (previously cited).
[277] EU AI Act, Article 113, Entry into force and application.

(i) detrimental or unfavourable treatment of certain natural persons or whole groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity".

The AI Act does not contain an explicit definition of social scores. However, from the four models on which we have gathered evidence, Amnesty International believes the system assigns an explicit set of metrics which constitute "social scores", as they are related to the trustworthiness of an impacted person - their likelihood of committing fraud. The system continues to evaluate and classify residents on this basis over time, with models regularly updated and re-run monthly.

The use of data routinely collected by different government departments (such as marital status, travel history, and citizenship) for fraud detection suggests that UDK/ATP are using data that is unrelated to the context in which the data was originally generated or collected, and which has detrimental and unfavourable effects for certain persons or groups. The unfavourable and detrimental treatment includes people being flagged for fraud control or investigation and subjecting them to further monitoring and surveillance, infringing on their right to privacy and risking their right to social security. Further, as detailed in Chapter 8, the structural discrimination that underpins UDK's fraud control practices, the inclusion of foreign affiliation-related measures as a de facto indicator of fraud, and the high risk of algorithmic discrimination presents an unacceptable risk of detrimental or unfavourable treatment of people living in poverty, migrants, racialized communities, and families not adhering to common perceptions of "normal" family structures, who can be flagged up for further fraud investigations based on these criteria.

Amnesty International believes the evidence gathered for this investigation indicates that UDK/ATP's algorithmic models do fall under the social scoring definition. Therefore, unless UDK/ATP can provide sufficient evidence otherwise, Amnesty International argues that the system in its current formation should be paused until adequate evidence is provided to make a full assessment of the system. It is also important to highlight that the AI Act clarifies that Article 5, including the social scoring ban, "shall not affect the prohibitions that apply where an AI practice infringes other Union law." This means that even if a system is not prohibited by the AI Act but is for example infringing EU equality or data protection legislation, a legal ban under those frameworks applies.

The specific interpretation of Article 5, including the social scoring ban, will be clarified in the European Commission's upcoming guidance on what constitutes prohibited practices under Article 5. In alignment with civil society calls[278] , the European Commission should clarify that risk scoring algorithms which lead to discriminatory outcomes for impacted affected people, such as UDK's fraud detection algorithm, are prohibited under the Act. This also highlights the urgency for UDK and ATP to provide full transparency in the form of unredacted documentation and code access and the publication of evaluations and risk assessments. This will allow for a fuller understanding of how the system operates, and how it should be interpreted under Article 5.

Amnesty International wrote to UDK and ATP detailing why we believe that their fraud control models constitute a social scoring system as outlined in the EU AI Act and invited their response. Amnesty International also asked UDK and ATP to provide adequate explanations and evidence if they believe that the models would not fall under the definition of a social scoring system. Amnesty International also asked UDK and ATP to provide details on what risk category their system should fall under the AI Act framework if they disagreed with the assessment that it's a social scoring system, and provide details on what obligations that would necessitate and how UDK and ATP planned to meet them.

UDK stated in its response to allegations in our report that its algorithmic practices do not constitute social scoring under Article 5 of the EU AI Act, as the controls have a clearly defined purpose, are proportionate, and are aimed at ensuring the correct payment of social benefits and because its fraud controls comply with applicable EU and national legislation. UDK and ATP have not provided Amnesty International with any detailed evidence or assessments that their algorithmic practices are not a social scoring system under Article 5 of the EU AI Act, nor have they provided us with any evidence that their practices are necessary and proportionate. UDK and ATP did not provide an alternative risk category that they assessed their system would fall under, nor did they provide any detail on the obligations the system would meet and how they planned to meet them. Amnesty calls on the European Commission to issue clear guidelines to clarify what systems ought to be defined as social scoring systems.

[278] Human Rights Watch, 'EU: Artificial Intelligence Regulation Should Ban Social Scoring: Strong Social Scoring Ban Needed to Protect Rights', October 19, 2023, available at: https://www.hrw.org/news/2023/10/09/eu-artificial-intelligence-regulation-should-ban-social-scoring

While social scoring systems will be subject to a ban, when using AI systems in the context of welfare provision, Denmark, at a minimum, will be required to comply with the obligations on high-risk AI systems of the EU AI Act. UDK/ATP's algorithms not deemed to fall into the "unacceptable risk" category would therefore still have to comply with high-risk requirements of the AI Act. According to Annex III, relevant high-risk systems are:

"AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services."

The text does not specify whether fraud detection systems in the social protection domain would fall under this broad category.

The AI Act includes obligations for both deployers and providers of High-risk systems, both are discussed below.

OBLIGATIONS FOR DEPLOYERS OF HIGH-RISK SYSTEMS

Article 26 of the EU AI Act sets out the obligations for deployers, which includes putting in place a suite of technical and organizational risk mitigation measures. It also includes ensuring there is human oversight from persons who have the necessary competence, training and authority. Crucially, deployers of high-risk systems who are public authorities or agencies are required to register their system in the EU database, in accordance with Article 49.

Article 27 of the EU AI Act stipulates that, prior to the deployment of these systems, public and private actors should conduct assessments of the implications of these systems for fundamental human rights. The assessment should include:

"(a) a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose; (b) a description of the period of time and frequency in which each high-risk AI system is intended to be used; (c) the categories of natural persons and groups likely to be affected by its use in the specific context; (d) the specific risks of harm likely to impact the categories of persons or group of persons identified pursuant point… (e) a description of the implementation of human oversight measures, according to the instructions of use; (f) the measures to be taken in case of the materialization of these risks, including their arrangements for internal governance and complaint mechanisms."

Article 27 and recital 96 of the EU AI Act do not, however, create an explicit obligation for deployers to either stop their deployment or ensure that assessments of risks are acceptable under human rights law.

OBLIGATIONS FOR PROVIDERS

In addition to requirements for deployers and noted obligations on transparency, accountability and redress in Chapter 6.6, Article 13 of the EU AI Act states that high-risk AI systems must be designed to be transparent, so that those deploying them can understand and use them correctly.

Providers of high-risk AI systems are required to draw up technical documentation "before that system is placed on the market or put into service and shall be kept up-to-date" to demonstrate compliance and to provide authorities with the information to assess that compliance.[279]

Additionally, under Article 9(1)-(2) of the EU AI Act, providers of high-risk systems are required to establish a risk-management system.[290] The risk-management system shall be "a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating throughout the high-risk AI system's lifecycle".[291] The risk-management system shall include:

"(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose; (b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse."[292]

Providers of high-risk AI systems are also required to conduct data governance, ensuring that training, validation and testing datasets are relevant, sufficiently representative and, to the best extent possible, free of errors and complete according to the intended purpose.[293] Following the implementation of these sections of

[279] EU AI Act, Article 11.

the EU AI Act, any high-risk system will have to undergo a suite of pre-deployment tests in the form of conformity assessments, either conducted internally or by a third party, which will ensure greater transparency and will likely include some form of algorithmic auditing.

The provisions on high-risk systems outlined above will not apply until 2 August 2030. Nevertheless, Amnesty International recommends the Danish authorities ensure these are being implemented as soon as possible. With the AI Act only recently coming into force, and given UDK/ATP's current lack of transparency, Denmark must ensure a strong and rights-respecting implementation of the AI Act at the national level and a strong, effective and Charter-based interpretation of prohibited and risky technologies under the AI Act including the provisions of Article 9, 10, 11, 13, 26, 27, 85, 86, 87 of the AI Act to ensure greater transparency in the use of high-risk systems.

12. CONCLUSIONS AND RECOMMENDATIONS

This report demonstrates how the practices of Udbetaling Danmark/ATP and municipalities have created a system of surveillance that infringes on people's right to privacy and human dignity. The report has also discussed ways in which the discriminatory impact that results from Udbetaling Danmark/ATP and municipalities' data and algorithmic practices are happening in the context of discriminatory or unequal structures present in Danish societal institutions through – laws, rules, norms, patterns of attitudes and behaviour that create and promote "othering."

The report has also discussed ways in which the Udbetaling Danmark benefits system creates a barrier to accessing social benefits for some marginalised groups, including women in crisis and people with disabilities and as a result, risks restricting their right to social security and discriminating against groups based on their gender, disability and age. Further, it has also discussed ways in which digitisation of the social benefits system has led to people with disabilities being forcibly included or unfavourably included in Udbetaling Danmark's system.

RECOMMENDATIONS

In light of the findings detailed in this report, Amnesty International has the following recommendations:

TO DANISH AUTHORITIES

- Ensure that Udbetaling Danmark/ATP stops using algorithms that evaluate or classify people based on data on their social behaviour or sensitive personal characteristics or proxies thereof which lead to the violation of their human rights.
- Pause the system in its current formation until adequate evidence is provided to make a full and final assessment of the system and the applicability of the social scoring ban of the AI Act.
- Ensure a strong and rights-respecting implementation of the AI Act at the national level and a strong, effective and Charter-based interpretation of prohibited and risky technologies under the AI Act as soon as possible and no later than the legally set deadlines including the provisions of article 9, 10, 11, 13, 26, 27, 85, 86, and 87 of the EU AI Act to manage risks that high risks systems can pose to fundamental rights and to ensure greater transparency in the use of high-risk systems.

TO THE MINISTRY OF EMPLOYMENT AND TO UDBETALING DANMARK:

- Establish a clear, unambiguous and legally binding ban on the use of data regarding citizenship, "foreign affiliation", or nationality or proxies thereof, in risk-scoring for the purposes of fraud control.
- Review and amend Udbetaling Danmark/ATP norms, policies, and laws that inform risk-profiling through Udbetaling Danmark/ATP's fraud control algorithms that could perpetuate discrimination based on income, race, ethnicity, religion, migration status, gender, disability, age, and ensure that they comply with relevant international human rights standards.

- Ensure that Udbetaling Danmark/ATP ends the practice of mass extraction, processing, and exploitation of residents' data for fraud-control purposes and the use of social media.
- Ensure that Udbetaling Danmark/ATP is fully transparent and provides meaningful information to affected individuals about the underlying logic, importance and expected consequences of decisions, even if they are not fully automated, regardless of the level of human involvement in the decision-making process.
- Ensure that Udbetaling Danmark/ATP and municipalities inform benefits applicants and recipients that that they have been identified for fraud investigations after they are flagged up by fraud control algorithms in a clear, comprehensible, and detailed manner.
- Ensure that Udbetaling Danmark/ATP publish clear information about the fraud control inputs it uses to make risk assessments for fraud and error (including publishing regular reports and key statistics), information about how the fraud control models work, information on performance and bias assessments conducted, information on human rights impact assessments and data protection impact assessments performed prior to and during the use of fraud control systems including, during the processing of data through the systems.
- Ensure that Udbetaling Danmark/ATP and municipalities conduct independent human rights and data protection impact assessments of the UDK system. This impact assessment needs to include, at the very minimum, an evaluation of the discriminatory effects on marginalised groups – low-income groups, racialised groups, including migrants and people who have been granted refugee status in Denmark, ethnic minorities, people with disabilities, and older people - through the use of fraud control algorithms.
- Ensure that Udbetaling Danmark/ATP and municipalities provide caseworkers with additional training and capacity building where necessary to address and prevent issues such as automation bias.
- Ensure that Udbetaling Danmark takes steps to end the exclusion of women in crisis centers, older people and people with disabilities that is facilitated by the digitisation of Udbetaling Danmark's benefits system by ensuring that the Udbetaling Danmark system is fully accessible in practice through non-digital means for groups who cannot use technology.
- Ensure that Udbetaling Danmark/ATP provides social assistance applicants with clear and accessible information about how decisions are made in their cases, how to appeal such decisions, and, where needed, ensure that applicants receive support in lodging their appeal, including legal or financial support.
- Require companies developing AI products used by the Ministry and UDK to conduct adequate human rights due diligence to identify and address actual or potential human rights harms that might appear at any stage of the supply chain or product lifecycle as outlined in the United Nations Guiding Principles on Business and Human Rights.

DANISH PARLIAMENT

- Review and amend section 2(1)(7) of Executive order of the Child and Youth Benefit Act LBK no. 724 of 25/05/2022 and section 5 (a) of the Executive Order of the Act on Child Allowance and Advance Payment of Child Support (LBK no. 63 of 21/01/2019) to remove excessive and lengthy residency requirements that have discriminatory impacts on people granted refugee status in Denmark.
- Review and amend the Danish Public Administration Act to include provisions on automated decision-making that guarantee that benefit applicants and claimants have a right to an effective remedy.
- Enact legislation to establish an independent public authority with oversight over the UDK/ATP and that monitors UDK/ATP's use of artificial intelligence systems, to strengthen accountability mechanisms and increase human rights protection. This includes, establishing an independent authority that has oversight over Udbetaling Danmark/ATP's activities in compliance with Article 70 of the EU AI Act.

TO THE DATA PROTECTION AUTHORITY:

- To exercise its supervisory authority under Article 29 of the Danish Data Protection Act and Article 58 of the GDPR to order that Udbetaling Danmark/ATP and municipalities provide it with information on its data practices and any data protection impact assessments these entities have conducted.
- To ensure that Udbetaling Danmark/ATP and municipalities comply with all relevant provisions of the Danish Data Protection Act and the GDPR, including articles 5 and 6 on the processing of data defined in these regulations.

TO MUNICIPALITIES:

- Provide caseworkers with additional training and capacity building to address and prevent issues such as automation bias, discrimination and the violation of welfare recipients' dignity and privacy when assessing their eligibility to benefits.
- Conduct independent human rights and data protection impact assessments of their fraud investigation practices. This impact assessment needs to include, at the very minimum, an evaluation of the discriminatory effects on marginalised groups, including – low-income groups, racialised groups, people with disabilities through the use of fraud control algorithms.
- Ensure that social assistance applicants receive clear and accessible information about how decisions are made in their cases, how to appeal such decisions, and, where needed, ensure that applicants receive support in lodging their appeal, including legal or financial support.

TO THE EUROPEAN COMMISSION:

- Ensure that the upcoming guidance by the European Commission on the practical implementation of the prohibited practices referred to in the AI Act provides legal clarity and addresses relevant AI-based social scoring practices across the EU, including discriminatory fraud detection and risk profiling systems in the context of social protection.

TO ATP:

- Urgently take steps to ensure that it does not contribute to human rights violations or abuses through its involvement in the UDK benefits system, and to address any human rights violations when they do occur, including where necessary by cooperating in their remediation.
- Provide evidence that caseworkers in the fraud control units have the necessary competence and authority to intervene in the fraud investigation and decision-making process when a person is identified for a fraud investigation by UDK/ATP's algorithms.
- Provide caseworkers with additional training and capacity building where necessary to address and prevent issues such as automation bias and discrimination
- Undertake proactive, ongoing human rights due diligence throughout the lifecycle of algorithmic technologies, both before and after the roll-out and implementation of new systems, in order that risks can be identified during the development stage and human rights abuses and other harms immediately picked up once the technologies have been implemented.
- Publicly disclose the steps it has taken to identify, prevent and mitigate human rights abuses and risks in its business operations, including through its involvement and business relationship with UDK.

TO ALL STATES

- Ensure that digital technologies are used in line with human rights law and standards, including on privacy, equality, and non-discrimination, as well as data protection standards, and that they are never used in ways that could lead to people being discriminated against or otherwise harmed. States must draw clear red lines on and prohibit the development, production, sale, and use of digital technologies that are incompatible with human rights.
- Critically assess whether automation and deployment of AI is the correct and most appropriate approach to reaching public policy or other stated aims, particularly making sure that AI deployment

does not exacerbate or pose a risk of human rights violations and drawing red lines on technologies incompatible with human rights, identify underlying systemic problems that require attention, acknowledge the limits of proposed technological solutions and explore alternative solutions and approaches.

- Develop and enact binding and enforceable human rights-based AI regulation, by accounting for intersectional harms of technologies. Address extra-territorial impact and reject differential approaches to protecting "citizens" versus "non-citizens".
- Ensure meaningful participation of impacted communities in the development and deployment of AI regulation, by centring policy discussions around the needs and priorities of those communities, enabling equal participation of representative advocates and organizations through resource allocation, and creating level-field between all stakeholders and rightsholders, and valuing experiential expertise.
- Ensure transparency around the use of digital technologies by public authorities. While transparency requirements will differ according to the context and use of the system, they should be implemented with a view to allowing affected people as well as researchers to understand the decisions made in the system and how to challenge incorrect decisions.
- Ensure that when a new system is introduced, information about how it functions, the criteria it considers and any appeals mechanisms in place to challenge decision-making are widely disseminated in accessible formats and languages.
- Require in law that technology companies carry out ongoing and proactive human rights due diligence to identify and address human rights risks and impacts related to their global operations, including by legally requiring human rights impact assessment of any public sector use of automated and algorithmic decision-making systems. This impact assessment must be carried out during the system design, development, use, and evaluation, and – where relevant – retirement phases of automated or algorithmic decision-making systems. The impact on all human rights, including social and economic rights, must be assessed and properly addressed in the human rights due diligence process. The process should involve meaningful engagement with relevant stakeholders, including independent human rights experts, individuals from potentially impacted, marginalized and/or disadvantaged communities, oversight bodies, and technical experts.
- Establish comprehensive and independent public oversight mechanisms over the use of automated or semi-automated decision-making systems, to strengthen accountability mechanisms and increase human rights protection, in addition to mechanisms for grievance redressal for individual decisions.
- Factor in and address the multiple and intersectional forms of discrimination that many groups, including women, people with disabilities, older people, people living in poverty, children and people belonging to racialized and minoritized communities such as refugees and migrants, face when trying to claim their human rights, and the specific barriers they may face when interacting with automated decision making in social protection systems and/or when trying to appeal against a decision made by these systems.

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US


info@amnesty.org


+44 (0)20 7413 5500

JOIN THE CONVERSATION


www.facebook.com/AmnestyGlobal


@Amnesty

CODED INJUSTICE

SURVEILLANCE AND DISCRIMINATION IN DENMARK'S AUTOMATED WELFARE STATE

This report investigates the use of Artificial Intelligence (AI) powered fraud control algorithms in Denmark's Welfare system. The welfare system known as Udbetaling Danmark (Pay Out Denmark), undermines human rights through its use of analogue and digital forms of surveillance to detect social benefits fraud. Analogue forms of surveillance include monitoring by fellow residents, municipalities and other public authorities while digital forms of surveillance include the use of fraud control algorithms to flag individuals up for further investigations. This pervasive surveillance restricts benefits recipients' rights to privacy as well as to human dignity and social security.

To identify individuals and groups likely to commit fraud, algorithms are deployed by UDK to classify or predict a person's circumstances, such as their relationship status, or whether they've left the country without informing the welfare agency. To do this, information such as citizenship, marital status, income, household size, composition, and evidence of co-habitation is used, often with the aim of finding individuals whose circumstances deviate from the "norm". These characteristics or variables can act as proxies for race, migration status, and socio-economic status and can encourage discrimination.

Discrimination is also present as a result of the digitalization of the benefits system. This is because for some marginalised groups, including women in crisis and people with disabilities, accessing a digital service independently is not possible, and digitization risks restricting their right to social security based on their gender and disability.

INDEX: EUR 18/8709/2024
NOVEMBER 2024
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL