THE DANISH INSTITUTE FOR HUMAN RIGHTS

PUBLIC PROCUREMENT AS A TOOL TO ADDRESS HUMAN RIGHTS RISKS IN THE USE OF DIGITAL TECHNOLOGY TO DELIVER ESSENTIAL PUBLIC SERVICES

A DISCUSSION PAPER
FEBRUARY 2024

PUBLIC PROCUREMENT AS A TOOL TO ADDRESS HUMAN RIGHTS RISKS IN THE USE OF DIGITAL TECHNOLOGY TO DELIVER ESSENTIAL PUBLIC SERVICES
A DISCUSSION PAPER
FEBRUARY 2024

This publication was possible thanks to the support from the Danish International Development Agency (DANIDA) and the Swedish International Development Cooperation Agency (Sida) and. Responsibility for the content rests entirely with the Danish Institute for Human Rights.

Authors: Daniel Morris and Cathrine Bloch Veiberg
Researchers and reviewers: Fernando Porto de Sá, Line Gamrath Rasmussen, Anja Møller Pedersen, Elin Wrzoncki, and Rikke Frank Jørgensen

e-ISBN: 978-87-7570-237-4

Cover illustration: David Zamorano
Layout: Michael Länger

Denmark's National Human Rights Institution
Wilders Plads 8K, DK-1403 Copenhagen K
Phone +45 3269 8888
www.humanrights.dk

At the Danish Institute for Human Rights we aim to make our publications as accessible as possible. We use large font size, short (hyphen-free) lines, left-aligned text and strong contrast for maximum legibility. For further information about accessibility please click www.humanrights.dk/accessibility

CONTENTS

1 INTRODUCTION

This paper aims to stimulate dialogue on public procurement as a tool to address human rights risks in the use of digital technology to deliver essential public services. Further, it aims to provide public procurement policy makers, buyers, and contract managers with an introduction to some human rights risks and considerations when procuring digital technology to deliver essential public services.

The public sector procures technology in many forms, from hardware such as computers, to software such as accounting systems and office software suites. Within the last two decades, digital technology has been increasingly procured and used by States to deliver essential public services in areas such as education, health and social care, and public transportation. The delivery of essential public services is a way for the State to meet its human rights obligations.[1] The use of digital technology to deliver essential public services can improve efficiency and help a State more effectively realise associated human rights obligations in these areas.[2]

However, there are a range of examples of when citizens have suffered harm due to the use of digital technologies in the delivery of public services,[3] through violations of the right to privacy, the right to freedom of expression, equality, and the right not to be discriminated against, among others. The challenges emphasise the need for a human rights-based approach to the delivery of essential public services through digital technologies ensure the availability, accessibility, acceptability, and quality (AAAQ) of services to all citizens.[4] This means that human rights challenges should be considered at all stages of digitalisation, from planning, to procurement, through to the application of the technology.

This paper highlights that public procurement is a key junction to identify risks of negative human rights impacts and put mitigating measures in place to address such risks before harm occurs.

Digital technologies are often designed and developed by the private sector and commissioned and purchased by the State. In many cases the public authority and private provider would work together to tailor specific technologies or develop additional features to align with needs. While businesses have a responsibility to ensure that their digital technologies respect human rights, States have an obligation to ensure that the digital technologies procured to deliver essential public services do not cause harm to users as well as other rightsholders.[5]

The UN Guiding Principles on Business and Human Rights (UNGPs) highlight that "States conduct a variety of commercial transactions with business enterprises, not least through their procurement activities. This provides States – individually and collectively – with unique opportunities to promote awareness of and respect for human rights by those enterprises, including through the terms of contracts".[6]

The UNGPs also articulate human rights due diligence as a means to identify and address human rights risks. States should conduct human rights due diligence to identify and address human rights risks in the development, production, and use of digital technologies to deliver essential public services. The State is often the largest buyer at the national level and, as a part of their duty to protect human rights, should use their leverage to ensure that their suppliers also conduct human rights due diligence.[7]

The type and severity of the risks,[8] the type of digital technology being procured, and the leverage the public buyer has, shape what measures can be implemented to address the risks at different stages of the public procurement lifecycle.[9] (NB: This discussion paper is focused on highlighting the range of human rights risks in the use of different types of digital technology).

A number of States have taken steps to integrate human rights due diligence into public procurement.[10] However, focus has largely been on identifying and addressing risks arising in the value chain of goods (e.g. extraction, manufacture, transportation) and risks related to services of a more tangible nature such as cleaning, care, and food services. Human right risks related to the procurement of digital technologies, including algorithms and artificial intelligence, remain largely unexplored and focus is often narrowly placed on the benefits that these digital technologies can offer to citizens and the public at large. Focusing solely on benefits can results in overlooking risks of adverse human rights impacts which can have negative impacts on users and other rightsholders that may undermine positive contributions.[11]

Human rights due diligence and technology regulatory environment(s) are evolving quickly. In Europe, for example, a range of mandatory human rights due diligence laws have been developed at the national level.[12] There is also an ongoing process to develop a EU Directive on Corporate Sustainability Due Diligence Directive (CSDDD) which will require large companies operating in the European market to exercise environmental and human rights due diligence.[13] However, the CSDDD is unlikely to oblige public entities to exercise environmental and human rights due diligence when conducting corporate activities, such as public procurement.[14] Furthermore, the EU has put in place, and proposed, a series of regulations addressing risks to fundamental rights in the scope of the digital ecosystem. The regulations have been focused on specific activities (e.g., data processing), specific technologies (e.g., AI systems), and specific actors (e.g., intermediary services providers). The main developments in this area are the General Data Protection Regulation (GDPR),[15] the Digital Services Act (DSA),[16] and the Artificial Intelligence (AI) Act.[17] All three regulations include a range of obligations placed on tech companies and activities in the digital sphere that aim to address significant, systematic, or severe risks to fundamental rights and freedoms.

In other regions we have also seen significant developments to measures to address human rights related impacts of digital technology. Currently, 61% of African countries have legislation in place that regulates electronic transactions, whilst just over half (52%) have laws on digital consumer protection. Legislation relating to privacy and data protection exists in jurisdictions covering 61% of the different jurisdictions across Africa, whilst 72% have enacted legislation on cybercrime.[18] However, there is often little reference to the role of public procurement as a tool to address human rights risks in the use of digital technology to deliver essential public services in these developments, nor

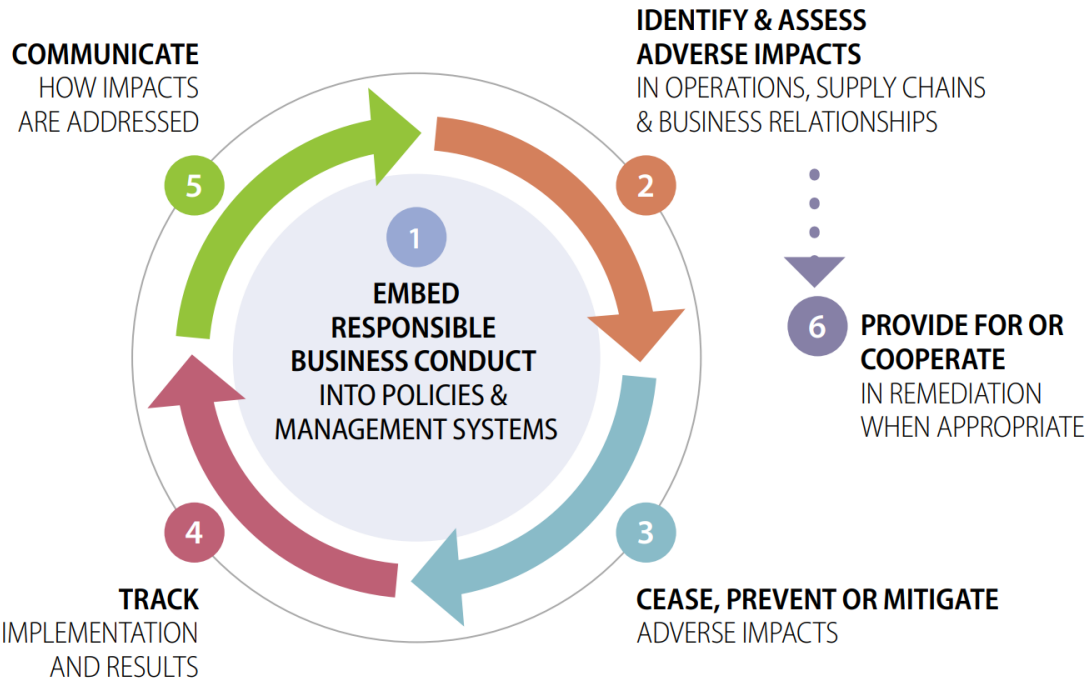
guidance or support for public buyers in the process of procurement of such services. There are a range of human rights due diligence developments in Latin America.[19] However, these are nascent developments and the applicability of human rights due diligence to public procurement and/or digital technology is yet to be addressed.

In the following sections we first provide a brief outline of the topic of public procurement and human rights after which we highlight six selected areas in which we are seeing digitalisation in public service delivery and provide illustrative examples of human rights risk. We conclude this discussion paper with conclusion and considerations for further discussion.

2 PUBLIC PROCUREMENT AND HUMAN RIGHTS

States have international human rights law obligations to respect and protect human rights and ensure remedy for human rights abuses which occur. In addition, a state should support suppliers in meeting the business responsibility to respect human rights. A state can contract out the supply of goods and services, but it cannot contract out its human rights obligations. One of the earliest opportunities a State has to identify and address the risks from the use of digital technologies to deliver essential public services is when it is procuring digital technology.

Identifying human rights risks is done through a process of due diligence, which is articulated in the UNGPs and the OECD Guidelines for Multinational Enterprises.[20] The due diligence process of the OECD Guidelines for Multinational Enterprises covers due diligence on impacts to people and the environment,[21] and is laid out in the graphic below.



Source: https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf

From a public procurement perspective, human rights due diligence should be undertaken by public buyers.[22] A public buyer can mitigate some human rights risks identified requiring and encouraging suppliers to implement human rights due diligence across their operations and value chains.

Risk identification, assessment, and management are often three distinct steps in a human rights due diligence process. In terms of digital technologies, the first step includes identifying **human rights risks linked to the development of digital**

technology, risks linked to its design as well as **risks lined to its use, misuse, and abuse**. There are risks to several specific human rights linked to various technologies.[23] A significant inherent to digital technology relates to **data protection and security**, including ensuring informed consent to data gathering, processing, and sharing. A further risk in the development and use of digital technologies, especially algorithmic decision-making, includes **bias and discrimination**. For example, the use of algorithmic decision-making technology includes the risk that the decision-making will reflect past decision-making which may be biased and discriminatory, in its procurement and application in e.g. social service delivery. It is therefore necessary to assess the data being fed to the algorithm for past biases as well as implement a process for human checks of results prior to implementation in social security (e.g. benefits) schemes. These risks maintaining or reinforce existing structures of inequality which often negatively impacts the most vulnerable groups in society. Algorithms and artificial intelligence are increasingly present in digital technology and while they present opportunities to realise human rights, they also present additional human rights risks, especially when they can learn and adapt. As experience unfortunately show, the **lack of human oversight** and **lack of accountability and transparency** on how decisions are taken enable severe human rights impacts. When States choose to procure digital technologies to deliver essential public services, then it is important to consider risks from the potential and reasonably foreseeable **use, misuse, and abuse of digital technology** (e.g. hacking) and potential unavailability of the digital technology (e.g. denial of services). Furthermore, there are risks associated in becoming **locked in** to certain digital technologies or providers.[24] In addition to risks of the use of digital technology for the provision of individual services, there are risks related to the **cumulative impact** of the use of digital technology, which often occur through digitalisation (i.e. replacing existing non-digital means of delivery through broad digitalisation plans), which raises issues of **accessibility** and can create a digital divide and digital exclusion.

HUMAN RIGHTS IMPACT ASSESSMENT

A human rights impact assessment (HRIA) is a process for systematically identifying, predicting and responding to the potential human rights impacts of a project or activity on rights-holders. It is one-off in-depth risk assessment which can be implemented when, for example, heightened human rights risks have been identified, such as risks arising from algorithms and artificial intelligence in digital technology.[25] A HRIA can be conducted by a range of different actors, including businesses developing such digital technology and state actors intending to procure such digital technologies.

New requirements outlined in the EU Digital Services Act (DSA) (and in the proposed EU Artificial Intelligence Act) will also require actors to assess fundamental rights risks of the product, service and/or application. In particular, the DSA requires very large online platforms to identify, assess and put in place mitigation measures for significant systemic risks related to their services, the scope of which includes any actual and foreseeable negative effects for the exercise of fundamental rights.[26] The proposed EU Artificial Intelligence would also place requirements on providers (and potentially deployers) of a high-risk AI system to inform authorities where the application presents a risk to fundamental rights.

To date, in depth analysis of risks in the use of algorithms only comes to light ex post facto.[27] However, there are methodologies to conduct HRIA to identify and address risks before human rights harms occur. In 2020 the Danish Institute for Human Rights published a guidance on how to conduct a HRIA for digital business activities. While originally designed for business, it can also be used by public procurers to support their human rights impact assessment for digital service procurements. The guidance includes an outline of the key criteria for HRIA of digital project, product and services, a step by step guidance to conducting HRIA of digital business activities, and some resources to address core challenges for HRIA in the digital space, i.e. lack of geographical boundaries and the difficulty in identifying and engaging with impacted stakeholders.

Read more here: Human rights impact assessment of digital activities | The Danish Institute for Human Rights.

Once risks have been identified, they should be assessed to understand their likelihood, severity, and consequences. The assessment informs what measures should be included across the public procurement lifecycle, including at the following stages:

- Sourcing and market research (e.g. research to understand market maturity to inform sourcing methodology and requirement definitions);
- Supplier registration (e.g. requiring suppliers to commit to code of conduct to bid);
- Needs definition and technical specifications (e.g. high-level descriptive specifications requiring suppliers to address human rights risks, tailored performance and functional specifications, labels and certificates, international standards);
- Supplier qualification (e.g. mandatory minimum requirements, exclusion grounds);
- Evaluation and award criteria (e.g. weighted scoring criteria, verification measures);
- Contractual provisions or performance clauses (e.g. requiring contractors to conduct human rights due diligence, adhere to specific standards, monitoring, auditing and investigation, corrective action, and termination);
- Contract management (e.g. regular meetings and contractors reporting against key performance indicators, site inspections and audits);
- Sanctions.

A significant challenge in addressing human rights risks related to digital technologies is a lack of transparency, especially when algorithmic tools are used to support decision-making by public authorities.[28] It important to consider how public procurement can help encourage **transparency** by suppliers and to **communicate** relevant information publicly on what digital technology has been procured, how it is being used, and what algorithmic tools it contains.[29]

Further information on how to design actions to implement human rights due diligence in public procurement can be found in these publications:

- Danish Institute for Human Rights, Driving change through public procurement, A toolkit on human rights for policy makers and public buyers (March 2020);
- Dataethics.eu White Paper on Data Ethics in Public Procurement of AI-based Services and Solutions (April 2020); and
- OECD, Advancing accountability in AI (February 2023).

3 HUMAN RIGHTS RISKS IN THE USE OF DIGITAL TECHNOLOGY TO DELIVER ESSENTIAL PUBLIC SERVICES

This chapter highlights examples of human rights opportunities, risks, and impacts associated with the use of digital technologies to deliver essential public services in the following areas:[30]

3.1. E-government
3.2. Education
3.3. Transportation
3.4. Justice systems and law enforcement
3.5. Social Protection
3.6. Healthcare

These areas of focus were selected based on desktop research of the areas that are often under public administration and where there in recent years has been increased digitalisation. The case examples are meant to illustrate potential negative human rights impacts of the digital services applied in these areas.[31]

3.1 E-GOVERNMENT

E-government (short for electronic government) means the use of digital technology to provide public services to citizens and other persons in a country or region. E-government is becoming increasing common; in the EU, the European Commission eGovernment barometer showed that 68% of key services were available online in 2022, and that there is a political aim to provide all key public services online by 2030.[32] The World Bank notes that e-government technologies can ensure the "better delivery of government services to citizens" and "citizen empowerment through access to information".[33] Further, it has been noted by some scholars that e-government can improve good governance, which is a key component of realising the sustainable development goals.[34]

Digital technologies have been developed and applied to transactional services, such as passport application management system, national civil registration systems (births/deaths), tax and revenue collection systems, and voting systems.[35] E-government often requires the use of electronic identities and digital IDs to access services such as education and healthcare. However, digital IDs require citizen's personal data to operate and facilitate communication and transfer of large amounts of personal data. Further, there may be challenges around access to digital ID for citizens with limited digital literacy or with a lack of access to the hardware and internet required. This is compounded when digitalisation programmes mandate that e-government is the only way of accessing essential public services, and when States rely entirely on e-government as a means of operating.

E-government services: In Denmark, e-government services are accessed through NemID and MitID portals, developed and run by the private company Nets A/S in partnership with the Danish Agency for Digital Government. NemID and MitID use personal data to identify citizens and long-term residents in connection with their tax (CPR) numbers, addresses and dates of birth. In 2013, NemID was targeted in a distributed denial-of-service (DDoS) attack,[36] shutting down its servers and access to all e-banking and e-government services for 7 hours.[37] Likewise, the service has been criticised for its underperforming cryptology and vulnerability to phishing.[38] These leading to concerns about user privacy. Further, studies show that some citizens are unable to access these services due to challenges around the ease of service and digital literacy. The Danish digitalisation authority and local government Denmark has emphasised that approx. 10-15 % of citizens, while having access to services are still unable to use services in the needed manner.[39]

Digital ID: In Kenya, the Huduma Namba had the aim of merging legal ID with digital ID by requiring the user to integrate all government-issued ID with mobile phone numbers and, at times, bank accounts. The project was immediately decried by human rights watchdog organisations who filed a petition before the High Court challenging the legality of the National Integrated Identity Management System and the way data would be collected to implement the Huduma Namba. The High Court's in 2020 ruled that, while the benefits of the National Integrated Identity Management System could be acknowledged in theory, these would need a solid human rights-based data protection legal framework[40] and the judgment shows that the government began collecting personal data without taking adequate steps to ensure that the data would be appropriately protected, contrary to the Kenyan Data Protection Act No 24 of 2019. The Huduma namba project was later abandoned, but its replacement – the Maisha namba – has been criticised by civil society group for repeating the mistakes that stalled Huduma Namba.[41]

3.2 EDUCATION

Educational technology (EdTech) is a growing field, valued at USD $254.80 billion in 2021 and expected to reach USD $605.40 billion by 2027.[42] The covid-19 pandemic illustrated the role of digital technology in ensuring access to education in many parts of the world and the stark divide in children's education in areas where digital technology was not available. The right to education is articulated in many international human rights instruments,[43] and access to computer facilities and information technology have been recognised as an essential feature of the right.[44] However, digital technology procured to support the provision of education can have negative impacts, including on privacy, freedom of thought, information and non-discrimination.[45] For example, through improper use of EdTech, children can be exposed to targeted advertising[46] and inappropriate content.[47]

Adaptive Learning: The development of EdTech software has allowed companies to develop tools that use AI algorithms to deliver personalised learning experiences and feedback. Those tools are usually developed by private tech firms and start-ups in a market that reached USD $1.86 billion in 2020.[48] However, adaptive learning often

requires personalised data in order to operate as intended, which raises concerns over data policies. For example, in July 2020, the government of the state of São Paulo (Brazil) started a free partnership with the German EdTech firm Mangahigh through the end of 2021.[49] The company provided a tool for individualised and gamified maths learning and its website markets "adaptive quizzes" and "real-time analytics with AI support for differentiation".[50] The government championed the partnership as an opportunity for students who could not attend physical classes at the height of the Covid-19 pandemic. Yet, a 2022 Human Rights Watch report listed the company among those which shared personal data with third-party advertisers, including session recording and key-logging data that children and parents could not opt-out of.[51]

Classroom Management: Software can help teachers and educators manage in-classroom activities. This type of service is particularly useful to distance learning as it allows educators to keep track of their students through online-teaching activities.[52] However, classroom management software may – sometimes even inadvertently to the developers – track personalised data and share it with advertisement firms. This was the case with the Diksha learning platform developed and owned by the Indian Ministry of Education, launched in 2017.[53] During its development, two Google-owned software development kits (SDKs), Firebase Analytics and Crashlytics, were used. Embedded in those kits there were features that tracked students' precise location and shared it with Google.

Student Collaboration: Well-known platforms such as Microsoft Office and Google Workspace can provide students with tools for greater collaboration in classroom assignments (e.g., through simultaneous writing and communication features). In the EU, public authorities are expected to assess the risks associated with the use of those platforms for the processing of personal data whenever there is a "high risk to the rights and freedoms of natural persons", which includes the processing of children's personal data.[54] In 2022, Datatilsynet, the Danish Data Protection Authority (DPA), suspended the use of Chromebooks and Google Workspace software in the Helsingør municipality, which they had procured for all primary schools (**folkeskoler**) in the region.[55] The DPA held that there was an unmitigated risk for transfer of personal data made available to Google due to its position as a controller using data for its own purposes. As a result of this, the Danish Data Protection Authority "Datatilsynet" has developed guidance for public authorities on use of artificial intelligence with key considerations before technologies or developed or deployed.[56]

3.3 TRANSPORTATION

Digital technology can help implement mobility solutions for public authorities in a market that is expected to grow from USD $47.9 to USD $243.47 billion dollars globally by 2030.[57] Access to affordable and accessible transportation is an essential requirement for people to enjoy rights related to education, healthcare, and workplaces, and families, and the sustainable development goals provide that States should "provide access to safe, affordable, accessible and sustainable transport systems for all".[58]

AI-powered traffic light systems can impact greenhouse gas emissions by reducing the number of times cars have to brake and restart the engine.[59] Likewise, driverless metro systems can ensure longer operational time and increase user experience satisfaction.[60] However, automated traffic monitoring systems have been shown to reproduce racial biases, and algorithms used in city planning can serve to further isolate vulnerable communities from public services.

Automated traffic enforcement (ATE): While many cities are still heavily car-dependent, traffic rules violations are bound to happen in large numbers. Issuing and appealing tickets burdens the often-understaffed traffic departments and small claim courts. As a solution, cities such as Washington, D.C.[61] have adopted ATE solutions like Automated License Plate Readers (ALPRs). Those systems automatically record drivers' license plates in cases of speeding and other traffic incidents and tickets are then mailed to the car's registered address. However, not only were ALPRs disproportionally installed in minority neighbourhoods, a 2018 D.C. Policy Center report found that minority residents are on average more likely to receive more and higher fines through those systems, despite the overall number of crashes per capita being about the same across different areas of the city.[62]

Public transport modelling: As many cities prepare to transition to carbon-neutrality, public transportation plays key role in measures to decrease emissions. Yet, modelling transport grids for hundreds-of-thousands of users with the need for real-time decision-making requires tech and AI systems to process large amounts of data.[63] However, biased data input can lead to solutions that exclude groups from the benefits of the mobility grid. For example, while women have different mobility needs than men,[64] using gender aggregated data can lead to biased outputs such as modelling transportation after work commute patterns, not considering how women rely more often on several daily short trips.[65]

Transit system payment solutions: Some modern mobility systems allow integrated payment options that automatically calculate the fare based on the zone or station a user "checked in" and "check out" at. The Transport for London Corporation, for example, offers users the possibility to simply tap contactless payment cards or devices while entering and exiting their route,[66] a technology they have been licensing to other cities.[67] Users have the option to provide personal data if they want to have access to additional features such as discounts and a travel history log, however if they don't provide the data, individualised credit card information is used when paying. Protecting payment information data in such cases is especially relevant since it can track individual position and mobility patterns in real-time.[68] Public buyers should be diligent on the treatment of this data, especially in cases where vulnerable persons are at risk of being targeted through geolocation data.[69]

3.4 JUSTICE SYSTEMS AND LAW ENFORCEMENT

Over the last decade, services and products have been developed aimed at addressing access to justice needs,[70] which range from record management platforms to predictive policing algorithms. The law enforcement tech market was valued at USD $13.6

billion in 2021 and research estimate its annual growth rate at 8.6%.[71] An effective justice system is fundamental to the right to an effective remedy and the sustainable development goals requires that States "provide access to justice for all".

Digital technology can help create a more effective justice system, for example, the use of past offender DNA sample databases demonstrably reduces criminal recidivism and deters future criminal behaviour.[72] However, studies have identified potential impacts that the use of such software may create, especially on the right to a fair trial and the prohibition of arbitrary and discriminatory arrests.[73]

Record and case management software: All layers of the justice system need access to identifying or identifiable data to process cases. Sensitive data and confidential case files may also be made available for public officials through privately-owned software. In some instances, the lack of proper contractual safeguards led to the sale of data to malicious third-parties.[74] Cybersecurity breaches such as those in Brazilian high courts[75] must also be taken as a risk factor when contracting with private software companies to ensure they provide necessary safeguards against system breaches. Furthermore, accessibility solutions for users with disabilities must be considered when developing public record-keeping software.[76]

Corrections and detention agencies management software: Besides the issues common to the employment of record management software, data leaks from correction and detention agencies may lead to impacts on the right to employment[77] and property,[78] by delivering criminal record data unduly to potential employers or landlord, for example. In extreme cases, such leaks may even expose inmates and security officers to life-threatening risks. For instance, during the retreat of Western forces from Afghanistan, several reports indicated that the Taliban obtained access to biometric databases,[79] including the Afghan Automated Biometric Identification System (AABIS) which identified criminals and members of the Afghani police and army who were later targeted by the organisation. This demonstrates that when dealing with conflict situations, public buyers are required to exercise a higher degree of due diligence ahead of acquiring security software anticipating risks in application.[80]

Surveillance and predictive policing: Among the most controversial services contracted by public officials are those concerning surveillance and predictive policing. Predictive policing is a method of using data and algorithms to forecast and prevent potential crimes. However, if not properly designed, they may impact the right to privacy and perpetuate discriminatory policing practice. In one case, a piece of software called Intrepid Response was used to profile journalists covering protests in Minnesota.[81] Advocates were concerned that the manner in which the application was used to share information across agencies without official communications would turn the least restrictive privacy policy into the standard. Likewise, PredPol, one of the most used predictive policing software, has been criticised for using past data to identify crime "hot spots".[82] As the data reflects historically overpoliced and marginalised areas, the algorithm may reproduce existing discriminatory policing practices even if it does not incorporate data on race. Those investigating the use of AI in the UK have that "[i]n many cases, departments and police forces used an array of exemptions to freedom of information rules to avoid publishing details of their AI tools."[83]

Correctional offender management profiling: Profiling software are used by criminal courts and law enforcement agencies to give a score on the likelihood of a convict to reoffend. Advocates for the use of these software claim that they are more capable and less biased than humans in assessing the risk of recriminalisation and are an important tool in criminal justice reform.[84] Nevertheless, critics suggest that profiling software disproportionally give higher risk of reoffending scores to people from racial minorities, especially since some algorithms "black boxes" make it impossible to guarantee cross-examination. A ProPublica investigation on Northpointe's COMPAS profiling tool, for example, highlighted that in the dataset analysed containing 7,000 people arrested in Broward country, Florida, black people were 77% more likely to be deemed high risk for violent crime.[85]

3.5 SOCIAL PROTECTION

Social protection (often referred to as social security or welfare) is the protection from a lack of sufficient income (often work-related income in cases of sickness, disability, maternity, employment injury, unemployment, old age, or death of a family member), unaffordable health care, and insufficient family support (particularly for children and adult dependents).[86] While the type of social security varies considerably by States, digital technology is increasingly being used in its delivery. This includes systems for social protection registration, contribution collection, beneficiary identification, benefit payments, statistics and reporting and early warning of abuse. The use of digital technology in the provision of social services can help reduce waiting times and deliver a more personalised outcome for beneficiaries. However, such systems can rely on profiling solutions that may entail human rights risks, in particular related to discrimination and privacy.

Public service profiling: The use of AI for case-handling and decision-making in public service delivery can have a significant impact on citizens' rights and legal certainty. This is the main conclusion of a report by the Danish Institute for Human Rights on the benefits and risks of using profiling algorithms in Danish public services, identifying some key challenges and dilemmas in their usage.[87]

Social security fraud signalling: Social security fraud is an important budgetary issue. For example, in the USA alone, social security overpayments accounted for a deficit of USD $6.8 billion in 2021.[88] Addressing social security fraud is, therefore, an important task to ensure good use of public funds, which can be aided by tech services.[89] However, in some cases algorithms can misinterpret data and signal legitimate benefit applications as fraudulent ones. For instance, in a scandal that led to the resignation of the Dutch prime minister, the Dutch System Risk Indication (SyRI) collected restricted and often inaccurate data to profile citizens, resulting in payment denials for often small application mistakes and affecting especially families from immigrant or economically vulnerable backgrounds.[90] In February 2020, the Dutch Court at First Instance ruled that the legislation setting up the fraud detection system was unlawful based on the right to privacy.[91] In Australia, roughly 400,000 recipients of welfare payments were wrongly accused of misreporting their income by an automate debt recovery system and received fines, which was later described by a government

minister as a "massive failure of policy and law".[92] A Royal Commission investigated and highlighted the human impacts of failure included "families struggling to make ends meet receiving a debt notice at Christmas, young people being driven to despair by demands for payment, and, horribly, an account of a young man's suicide."[93]

Unemployment profiling: Tech solutions can provide benefits to those in unemployment. For example, they can offer a choice for job-seekers to fill a questionnaire that then uses publicly available data to sort out a profile through simple and transparent indicators, enabling a case-worker to offer them personalised options for work, training and education.[94] However, such profiling solutions may entail human rights risks; the Austrian Arbeitsmarktservice (AMS) demonstrates how such algorithms may lead to a replication of bias.[95] In the specific case, a study by the Austrian Academy of Sciences highlighted that the system did not have any safeguards against bias, in specific when it comes to gendered bias in predicting the likelihood of future employment.[96]

Child abuse early warning:[97] In 2018, news coverage of the so-called Gladsaxe prediction model caused public debate. The year before, Gladsaxe municipality (in the suburbs of Copenhagen) had started to develop a data-driven model to identify vulnerable children from a very early stage. The purpose of the model was to trace children who were vulnerable due to social circumstances before they showed actual signs of special needs. Based on statistics, the authorities proposed to combine various information sources to locate children at risk.[98] The model used a points-based system, with indicators such as mental illness (3000points), unemployment (500 points), missing a doctor's appointment (1000 points), or dentist's appointment (300 points). Information about divorce was also included in the model's risk estimation, which was to be rolled out to all families with children in the municipality.[99] As part of the development process, the municipality asked for exemption from the data protection law to be able to combine personal (and sensitive) data from different data sources.[100] Gladsaxe's request was rejected, allegedly because the government intended to make a general exemption for all municipalities as part of a so-called Ghetto package.[101] Towards the end of 2018, the project was stalled due to the relatively high error rate of the model. The error rate was partly due to the limited amount of historical data, i.e., only 117 cases with vulnerable children age 0–6 years that could serve as training data for the model. Although the specific project was never implemented, it is illustrative of how the municipality envisioned that, data-driven models could support vulnerable groups such as children. The model was designed to sort the families according to strong statistical correlations between the selected data points. It was developed by combining statistical analysis of historical cases with qualitative analysis of the cases by domain experts. Based on the analysis, 44 data points were selected as relevant, such as parents' work status and history, citizenship, paternity relationship, parents' place of residence, the child's dental records, notifications from public authorities, caretaking, and language. In total, the model pulled data from nine different sources, including the employment system used by job centres (KMD Momentum), the central personal register (CPR), dentists' journals, the day-care system (pladsanvisningen), and notifications of concern received by public authorities (SBSYS). The idea was to use the model regularly and then notify case workers when data from a specific family was flagged. Based on the data, the case worker would decide if a specific intervention was to be taken. If it was decided to investigate the case, the family would have to consent to their case being examined.

3.6 HEALTHCARE

The healthcare sector is a large part of the global economy with overall healthcare spend "expected to reach $12 trillion in 2022, up from $8.5 trillion in 2018."[102] The World Health Organization's Global has highlighted that "the Internet of things, virtual care, remote monitoring, artificial intelligence, big data analytics, blockchain, smart wearables, platforms, tools enabling data exchange and storage and tools enabling remote data capture and the exchange of data and sharing of relevant information across the health ecosystem creating a continuum of care have proven potential to enhance health outcomes by improving medical diagnosis, data-based treatment decisions, digital therapeutics, clinical trials, self-management of care and person-centred care as well as creating more evidence-based knowledge, skills and competence for professionals to support health care."[103]

Digital technologies can help realise the right to health and the Sustainable Development Goals aim to "ensure healthy lives and promote well-being for all, at all ages." However, risks exist in receiving informed consent for data to inform the development of new treatments and diagnostics, and risks of discrimination in their use. Furthermore, when digital technologies are relied upon there are risks in terms of access for those who do not have the internet and elderly citizens, for example.

E-Health: In the UK in 2016, DeepMind, owned by Alphabet Inc., partnered with the Royal Free London NHS Foundation Trust to use machine learning to assist in the management of acute kidney injury. Critics noted that patients were not afforded agency over the use of their information, nor were privacy impacts adequately discussed.[104]

Electronic patient record (EPR) systems: The UK's Health Services Safety Investigations Body (HSSIB) notes that 90% of hospital trusts in the UK use EPR systems but that "a variety of safety issues associated with EPR systems that can impact on patient safety if they are launched or used without a proactive view on their safety." Since 2018, the HSSIB has "published nine investigations in which there were specific findings and safety recommendations relating to EPR systems. We also see some level of EPR issues in nearly every investigation we undertake."[105] Failures includes:

- a "hospital trust failed to send out 24,000 letters from senior doctors to patients and their GPs after they became lost in a new computer system."[106]
- "Guy's and St Thomas' in London, suffered a catastrophic failure when their IT system went down last summer, during a heatwave. A report showed operations were cancelled when doctors could not access medical records, putting some patients at serious risk."[107]
- "a patient diagnosed with lung cancer, but not followed up because of IT problems, who died two months later
- another, given the wrong medications because of a mix-up with their electronic notes, who died 18 days later" [108]

Ransomware attacks: In the UK in 2022, a cyber-attack on a major IT provider of the National Health Service (NHS) caused disruption in the provision of health services and left the health data of patients exposed.[109] This was not the first attack, as a global ransomware attack in 2017 impacted on the ability of the NHS to provide healthcare services to citizens.[110]

4 CONCLUSION AND CONSIDERATIONS FOR FURTHER DISCUSSION

The use of digital technology to deliver essential public services carries many benefits. However, the range of human rights challenges and harms which have occurred are concerning. This should give rise to pause and reflection on how best to address these risks at the earliest stage possible. The purpose of this discussion paper is to stimulate dialogue on public procurement as a tool to address human rights risks in the use of digital technology to deliver essential public services. It also aims to provide public procurement policy makers, buyers, and contract managers with an introduction to some human rights risks and considerations when procuring digital technology to deliver essential public services. As previous sections suggest, there can be no doubt about the human rights risks and opportunities in the application of technology in public sector service delivery. The question is, however, how public procurement can be used as a means to consider and address these risks.

Policy makers and public procurement professionals have key roles in ensuring that the use of digital technology to deliver essential public services improves efficiency and helps the State realise its human rights obligations.

Policy makers

1. **Policy makers can articulate the role of public procurement in addressing human rights risks when developing digitalisation plans and policies.**
   This includes:
- Ensuring that digitalisation strategies and efforts at country and regional level be accompanied by a reflection on identifying, assessing, and addressing any potential human rights risks and harm. This should happen at the conceptualisation and development phase of the strategy or effort, and should include specific reflections on the role of public procurement as a key junction to identify and address risks of negative human rights impacts;
- Ensuring that public sector service delivery strategies (e.g. in health, education, logistics, justice etc.) consider potential human rights risks of digitalisation and the role of public procurement. This can help set the stage for these considerations to be reflected in the planning of public procurement of the digital solutions in these areas.[111]

2. **Policy makers can ensure that human rights due diligence is integrated into public procurement.** This includes:

- Ensuring the human rights due diligence approaches within public procurement are coherent with, and mutually reinforcing to, broader measures to ensure responsible business conduct in a state. Public procurement bodies and public buyers are one of the frontlines in implementing human rights due diligence and ensuring responsible business conduct, and there is a need to coordinate with other public bodies to ensure effective implementation (including with digital technology and human rights experts to identify and address risks,[112] and with supervisory and investigative authorities to ensure that suppliers are implementing measures to respect human rights);
- Considering the procurement processes available/ commonly used in the procurement of the relevant digital technology (e.g. open, collaborative, joint) and the implications these have on the implementation of human rights due diligence;
- Ensuring that human rights due diligence is embedded in public procurement policies. Policies should clearly articulate measures which can be taken across the public procurement cycle to identify and address human rights risks, and how, including; sourcing, supplier registration, requirements definition, supplier qualification, evaluation and award criteria (e.g. weighted scoring criteria, verification measures), contractual provisions,[113] contract management, sanctions (see Section 2 for more information). Policies should recognise the responsibilities of different public bodies required to ensure effective implementation of human rights due diligence in public procurement, and the scope of the human rights due diligence expectations on public buyers;[114]
- Ensuring that human rights due diligence is embedded across public procurement systems and processes in a coherent manner.[115] This includes ensuring that victims of human rights harms, including harms which result from the use of digital technologies, have access to effective remedy mechanisms. This requires recognising that human rights due diligence should be implemented internally when i) undertaking procurement planning [116] and ii) undertaking specific procurement exercises, and iii) externally to ensure that suppliers implement human rights due diligence within the activities and value chains;
- Ensuring that adequate resources are allocated to addressing human rights risks as part of public procurement planning. For example, for when procuring profiling solutions for social services, public buyers have access to the necessary technical expertise to ensure transparency and quality of data;
- Encouraging transparency by suppliers and communicate relevant information publicly on what digital technology has been procured, how it is being used, and what algorithmic tools it contains;
- Ensuring monitoring and evaluation systems can capture human rights due diligence measures implemented (e.g. through indicators), and publicly communicate on these;
- Considering how the private sector can be harnessed to support the implementation of human rights due diligence in public procurement and identify and maximise synergies between public and private procurement practices around human rights due diligence;
- Ensuring that innovative procurement practices which collect information from key stakeholders and end-users to inform the design of the digital technology, gather information on human rights risks and needs of rightsholders.

3. **Policy makers can support public procurement professionals in identifying risks related to digital technologies.** This includes:

- Providing guidance, training, and tools to support public procurement professionals to understand what human rights due diligence looks through the lens of procurement processes, and support public procurement professionals identify and assess human rights risks related to digital technologies;
- Considering human rights impact assessments when heightened human rights risks have been identified, such as risks arising from the use of algorithmic decision making technologies;
- Ensuring that human rights considerations are incorporated into life-cycle costing. This includes considering the costs for monitoring risks and adjusting the technology to address human rights impacts such as data privacy and bias/discrimination, as well as ensuring continued access to essential public services, through, for example, license updates, user onboarding and support, and user interface requirements;
- Mapping and coordinate with relevant public bodies to ensure effective implementation of human rights due diligence in public procurement;
- Promoting collaboration and the sharing of information among public buyer networks.

Public procurement professionals

4. **Public procurement professionals can learn about risks and opportunities related to the digital technologies they are procuring;**
5. **Public procurement professionals can undertake human rights due diligence undertaking procurement planning and undertaking specific procurement exercises, and based on the human rights risks identified, require, and encourage suppliers to implement human rights due diligence across their operations and value chains;**[117]
6. **Public procurement professionals can monitor and follow-up on measures to ensure that contractors undertake human rights due diligence and consider coordinating with relevant supervisory and investigative authorities;**
7. **Public procurement professionals can ensure dialogue and channels of communication between procurement units and public sector project managers and rights-holder representative organisations (e.g. consumer networks, patient associations, parents associations etc.) to engage with them actively in both the development and roll-out of technologies;**
8. **Public procurement professionals can ensure dialogue between procurement units and public sector project managers and private sector providers and developers of digital services to make them aware of the risks and how they should be considered in the development and provision of the service.**[118]

5 RESOURCES

Relevant resources include:

- Danish Institute for Human Rights, Driving change through public procurement, A toolkit on human rights for policy makers and public buyers (March 2020);
- Dataethics.eu White Paper on Data Ethics in Public Procurement of AI-based Services and Solutions (April 2020);
- OHCHR B-Tech, Bridging Governance Gaps in the Age of Technology – Key Characteristics of the State Duty to Protect, A B-Tech Foundational Paper (May 2021)
- Business for Social Responsibility and Global Network Initiative, Human Rights Due Diligence Across the Technology Ecosystem (September 2022);
- OECD, Advancing accountability in AI (February 2023);
- European Center for Non-for-Profit Law, Framework for Meaningful Engagement (March 2023);
- The Supreme Audit Institutions of Finland, Germany, the Netherlands, Norway and the UK, Auditing machine learning algorithms (April 2023);
- The United Nations Interregional Crime and Justice Research Institute (UNICRI), The Toolkit for Responsible Artificial Intelligence Innovation in Law Enforcement (June 2023).

ENDNOTES

1 UN Committee on Economic, Social and Cultural Rights, General comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, 2017, UN Doc. E/C.12/GC/24 at para 23. Also see Marlies Hesselman, Antenor Hallo de Wolf, and Brigit Toebes, Socio-Economic Human Rights in Essential Public Services Provision, in Human Rights and International Law Series (Routledge, Abingdon 2017); Claire Methven O'Brien, Essential Services, Public Procurement and Human Rights in Europe, University of Groningen Faculty of Law Research Paper No. 22/2015

2 See, for example, OECD, Using AI to support people with disability in the labour market, Opportunities and challenges, 24 November 2023

3 A range of harms are detailed in the United Nations, Report of the Special Rapporteur on extreme poverty and human rights, Philip Alston, 2019, UN Doc. A/74/493, and in section 3 of this discussion paper.

4 See, E/C.12/2000/4: General Comment No. 14 on the highest attainable standard of health (2000), The Committee on Economic, Social and Cultural Rights | OHCHR; and the AAAQ toolbox | The Danish Institute for Human Rights

5 See the UN OHCHR, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, HR/PUB/11/04, 2011; the OECD Guidelines for multinational enterprises, 2011 (updated 2023); Olga Martin-Ortega and Claire Methven O'Brien, Public procurement and human rights: interrogating the role of the state as buyer, Public Procurement and Human Rights, 2019

6 UN OHCHR, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, HR/PUB/11/04, 2011, Principle 5, Commentary

7 See Danish Institute for Human Rights, Driving change through public procurement, A toolkit on human rights for policy makers and public buyers (March 2020), page 9

8 I.e. its scope (number of people affected), scale (seriousness of the impact) and whether it is 'remediable' or not (can an individual impacted by the risk be restored to at least the same, or equivalent, situation as before the adverse impact occurred?).

9 For example, the ability to address risks in the development of a digital technology is limited when considering off-the-shelf products, whereas when a public body commissions the creation of a tailored digital technology to deliver a specific service the ability to address risks in development is significantly higher.

10 See Danish Institute for Human Rights, Driving change through public procurement, A toolkit on human rights for policy makers and public buyers (March 2020); also see International Learning Lab on Public Procurement and Human Rights, Public Procurement and Human Rights: A Survey of Twenty Jurisdictions, 2016

11 See, for example, Danish Institute for Human Rights, Responsible business conduct as a cornerstone of the 2030 agenda – a look at the implications, a

discussion paper, June 2019; Danish Institute for Human Rights, Human rights at development finance institutions, Connecting the dots between environmental and social risk management and development impact, 2021, page 5

12 See, for example, France, LOI n° 2017-399 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre (March 27, 2017). Germany, Lieferkettensorgfaltspflichtengesetz ("LkSG") (BGBl. I S. 2959) (July 16, 2021). Norway, Lov om virksomheters åpenhet og arbeid med grunnleggende menneskerettigheter og anstendige arbeidsforhold (åpenhetsloven) LOV-2021-06-18-99 (June 18, 2021).

13 European Commissio, Corporate sustainability due diligence (europa.eu)

14 The 2014 Public Procurement Directive does not require due diligence per se, so it is unclear how the requirements for socially responsible public procurement will align with due diligence as articulated in the CSDDD. See Danish Institute for Human Rights, How Do The Pieces Fit In The Puzzle? Making sense of EU regulatory initiatives related to business and human rights, updated August 2023, Section G

15 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

16 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

17 Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts

18 UNCTAD, 'UNCTAD Global Cyberlaw Tracker: Summary of Adoption of E-Commerce Legislation Worldwide' (2021),

19 Danish Institute for Human Rights, Nota informativa: Regulación de la debida diligencia obligatoria en materia de empresas y derechos humanos en América Latina y el Caribe (forthcoming)

20 See the UN Guiding Principles on Business and Human Rights and OECD Guidelines for Multinational Enterprises

21 There is a growing recognition of a right to a healthy environment and recent regulatory develops address both environmental and human rights due diligence. However, environmental risks are beyond the scope of this discussion paper.

22 The UNGPs provide that states should require, where appropriate, state-owned or controlled enterprises to exercise human rights due diligence (UNGP 3). They clarify that this duty extends to situations where states enter into commercial relationships, including through public procurement (UNGP 6 and 8). Where states engage in privatisation or "contracting out" services that may impact on human rights, they must "exercise adequate oversight", including by ensuring that contracts or enabling legislation communicate the state's expectation that service providers will respect the human rights of service-users, i.e. their citizens. In practice, this oversight can be achieved by the state implementing HRDD. The UNGPs also highlight that states must ensure 'policy coherence', in other words, alignment with human rights obligations of standards and policies across all state departments, agencies, and other state-based institutions that shape business practices (UNGP 10), which includes public procurement bodies. The

OECD Recommendation of the Council on the Role of Government in Promoting Responsible Business Conduct, 12 December 2023, recommends that Adherents "Us[e] public procurement as a strategic tool for RBC and including RBC in procurement policies (regulatory and strategic frameworks), as well as promoting due diligence for RBC in public procurement".

23 One resource that outlines these risks of generative AI is the OHCHR Business and Technology Project's Taxonomy of Human Rights Risks Connected to Generative AI

24 Although not strictly a human rights risk, it has human rights implications

25 Danish Institute for Human Rights, Når Algoritmer Sagsbehandler: Rettigheder og retssikkerhed i offentlige myndigheders brug af profileringsmodeller (When Algorithms Manage Cases: Rights and legal certainty in the use of profiling models by public authorities), 2021. Also see Copenhagen University, Algorithmic fairness: Learnings from a case that used AI for decision support, November 2023

26 See Access Now and ECNL, Towards Meaningful Fundamental Rights Impact Assessments Under The DSA, September 2023

27 See, for example, Ziad Obermeyer, Brian Power, Christine Vogeli and Sendhil Mullainathan, Dissecting racial bias in an algorithm used to manage the health of populations, 2019; Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, Aaron Rieke, Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes, 2019

28 See the approaches in the UK on an Algorithmic Transparency Recording Standard Hub

29 Danish Institute for Human Rights, Når Algoritmer Sagsbehandler: Rettigheder og retssikkerhed i offentlige myndigheders brug af profileringsmodeller (When Algorithms Manage Cases: Rights and legal certainty in the use of profiling models by public authorities), 2021.

30 This chapter includes illustrative examples not directly linked, but still relevant to, the delivery of essential public services by the State. This chapter does not provide a complete overview of all digital technology used to deliver essential public services, nor does it provide a comprehensive list of all human rights risks associated with the digital technologies highlighted.

31 Further examples of risk are detailed in the United Nations, Report of the Special Rapporteur on extreme poverty and human rights, Philip Alston, 2019, UN Doc. A/74/493

32 European Commission, eGovernment Benchmark 2022

33 e-Government (worldbank.org)

34 Iyad Dhaoui, E-Government for Sustainable Development: Evidence from MENA Countries, J Knowl Econ. 2022; 13(3): 2070–2099; Glass, L. M., & Newig, J. (2019). Governance for Achieving the Sustainable Development Goals: How Important Are Participation, Policy Coherence, Reflexivity, Adaptation and Democratic Institutions? Earth System Governance, 2, Article ID: 100031.

35 National Democratic Institute, Internet voting in Estonia, 2013.

36 A DDoS attack is "a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic." Cloudfare, What is a DDoS attack?; Versio2, Nets om kollapset NemID-forsvar: DDoS-angreb var 'massivt', 12 April 2013

37 Version2, Nets om kollapset NemID-forsvar: DDoS-angreb var 'massivit' (Nets on the collapsed NemID defense: DDoS attack was 'massive'), 2013.

38 Version2, NemID er ikke kryptologisk sikker – og myndighederne er ligeglade (NemID is not cryptologically safe – and authorities are indifferent), 2016.
39 The digitalisation authority: https://digst.dk/media/24389/digital-inklusion-i-det-digitaliserede-samfund.pdf
40 Nubian Rights Forum and 2 Others v Attorney-General and 6 Others; Child Welfare Society and 8 Others (Interested Parties) [2020] Consolidated Petitions No. 56, 58 and 59 of 2019 (High Court of Kenya, Nairobi) eKLR, 1047 (I)
41 Kenya Human Rights Commission - Human Rights Organizations Urge Government to Expand Consultations and Safeguards before Unique Personal Identifier/Maisha Namba Rollout (khrc.or.ke)
42 Research and Markets, EdTech Market – Global Outlook & Forecast 2022-2027, 2022
43 International legal instruments for the right to education | UNESCO
44 The Abidjan Principles
45 UN Special Rapporteur on the Right to Education, Impact of the Digitalization of Education on the Right to Education, 2022.
46 HRW, How Dare They Peep My Private Life?, 2022.
47 The Wall Street Journal, Google's YouTube Kids App Criticized for 'Inappropriate Content', 2015.
48 Emergen Research, Adaptive Learning Market Forecast to 2028, 2021.
49 Governo do Estado de São Paulo, Plataforma matemática concede acesso gratuito para profesores e alunos da rede estadual (Maths platform grants free access to teachers and students in state schools), 2020.
50 See Mangahigh's website, accessed 2022
51 HRW, How Dare They Peep My Private Life?, 2022.
52 Agente, Digital Classroom Management Software Development A-Z
53 HRW, How Dare They Peep My Private Life?, 2022.
54 Article 35 of the GDPR
55 Datatilsynet, Datatilsynet Fastholder Forbud i Chromebook-sag (Datatilsynet Maintains Prohibition in the Chromebook Case), 18-08-2022.
56 Offentlige myndigheders brug af kunstig intelligens: Inden I går i gang (datatilsynet.dk)
57 Beyond Market Insights, Smart Mobility Market Report, January 2023.
58 United Nations, Sustainable transport, sustainable development: Interagency report for second Global Sustainable Transport Conference, 2021.
59 AI4Cities, IX3-system
60 Intelligent Transport, The Copenhagen Metro: a 24/7 system, 22 December 2009
61 Electronic Privacy Information Center (EPIC), Screened & Scored in the District of Columbia, 2022.
62 D.C. Policy Center, Predominately black neighborhoods in D.C. bear the brunt of automated traffic enforcement, 2018.
63 International Association of Public Transport, Artificial Intelligence in Mass Public Transport, 2018.
64 Ramboll, Gender and (Smart) Mobility, Green Paper March 2021.
65 ITF-OECD, Transport Innovation for Sustainable Development: A Gender Perspective, 2021.
66 Transport for London, Contactless and mobile pay as you go
67 PYMNTS, Transport for London Licenses Contactless Payment Technology, 2016.
68 TransitCenter, Do Not Track: A Guide to Data Privacy for New Transit Fare Media, 2021.

69 Reuters, How Myanmar's military moved in on the telecoms sector to spy on citizens, 2021.
70 World Justice Project, Measuring the Justice Gap: A people-centered assessment of unmet justice needs around the world, 2019.
71 Allied Market Research, Law Enforcement Software Market by Offering (Software, Service), by Deployment Model (On-premise, Cloud): Global Opportunity Analysis and Industry Forecast, 2021-2031, 2022.
72 Manhattan Institute, The Deterrent Effects of DNA databases, 2020.
73 Council of Europe (CoE), Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications, 2017.
74 Jason Tashea, Use Copyright Law to Battle Mugshot Extortion, 2018.
75 Sergiu Gatlan, Brazil's Court System under Massive RansomExx Ransomware Attack, 2020.
76 World Wide Web Consortium (W3C), Web Content Accessibility Guidelines (WCAG) 2.0, 2008.
77 United States Bureau of Justice Statistics, Employment of Persons Released from Federal Prison in 2010, 2021.
78 The Hill, Without Access to Credit, Ex-cons May Return to Lives of Crime, 2019.
79 Human Rights Watch (HRW), New Evidence that Biometric Data Systems Imperil Afghans, 2022.
80 Principle 7 of the UNGPs require that States and enterprises enact heightened due diligence in conflict situations. UNDP and UNWG-BHR, Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide, 2022.
81 MIT Technology Review, The Secret Police: Inside the app Minnesota police used to collect data on journalists at protests, 2022.
82 The Markup, How We Determined Crime Prediction Software Disproportionately Targeted Low-Income, Black, and Latino Neighborhoods, 2021.
83 Kiran Stacey, UK risks scandal over 'bias' in AI tools in use across public sector, The Guardian, 23 October 2023
84 Anthony W. Flores et al., False Positives, False Negatives, and False Analyses: A rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks.", 2017.
85 ProPublica, Machine Bias: There's software used across the country to predict future criminals. and it's biased against blacks, 2016.
86 About the right to social security and human rights | OHCHR
87 Danish Institute for Human Rights, Når Algoritmer Sagsbehandler: Rettigheder og retssikkerhed i offentlige myndigheders brug af profileringsmodeller (When Algorithms Manage Cases: Rights and legal certainty in the use of profiling models by public authorities), 2021
88 Social Security Administration, Agency Financial Report, 2021.
89 Danish Institute for Human Rights, Når Algoritmer Sagsbehandler: Rettigheder og retssikkerhed i offentlige myndigheders brug af profileringsmodeller (When Algorithms Manage Cases: Rights and legal certainty in the use of profiling models by public authorities), 2021, p. 141.
90 Digital Future Society, Governing algorithms: perils and powers of AI in the public sector, 2021, p. 15.
91 Marvin van Bekkum and Frederik Zuiderveen Borgesius, Digital welfare fraud detection and the Dutch SyRI judgment. European Journal of Social Security, 23(4), 323-340.

92 Reuters, FEATURE-Australian Robodebt scandal shows the risk of rule by algorithm, 15 December 2022
93 Royal Commission into the Robodebt Scheme, Report, 7 July 2023
94 Danish Institute for Human Rights, Når Algoritmer Sagsbehandler: Rettigheder og retssikkerhed i offentlige myndigheders brug af profileringsmodeller (When Algorithms Manage Cases: Rights and legal certainty in the use of profiling models by public authorities), 2021, p. 143.
95 Digital Future Society, Governing algorithms: perils and powers of AI in the public sector, 2021, p. 16.
96 Austrian Academy of Sciences, An algorithm for the unemployed? Socio-technical analysis of the so called "AMS-Algorithm" of the Austrian Public Employment Service (AMS), 2020
97 This example is drawn from, with the author's permission, Rikke Frank Jørgensen, Data and rights in the digital welfare state: the case of Denmark, Information, Communication & Society, 2021, page 8
98 Ministry of Social Affairs and the Interior, Dataunderstøttet tidlig opsporing af udsatte børn, December 21, 2017
99 B. Alfer in AlgoritmWatch, Automating society Denmark (29 January 2019)
100 Gladsaxe Municipality, Ansøgning om konkrete forsøg i Frikommuneforsøg II, 1 November 2017
101 The Danish Government, Tidlig opsporing af udsatte børn, 3 March 2018
102 World Economic Forum, Global Health and Healthcare Strategic Outlook: Shaping the Future of Health and Healthcare, INSIGHT REPORT, JANUARY 2023
103 WHO, Global strategy on digital health 2020-2025
104 Transforming health care: How artificial intelligence is reshaping the medical landscape | CBC News from Privacy and artificial intelligence: challenges for protecting health information in a new era | BMC Medical Ethics | Full Text (biomedcentral.com)
105 Health Services Safety Investigations Body, Electronic patient record systems: recurring themes arising from safety investigations, By Helen Jones, 19 December 2023
106 BBC, Newcastle Hospitals says computer error lost patient letters, 26 September 2023
107 BBC, IT failures causing patient deaths, says NHS safety body, 19 December 2023. Also see NHS Guy's and St Thomas' NHS Foundation Trust, Review of the Guy's and St Thomas' IT Critical Incident Final Report From the Deputy Chief Executive Officer, January 2023
108 BBC, IT failures causing patient deaths, says NHS safety body, 19 December 2023
109 NHS IT supplier held to ransom by hackers - BBC News
110 S. Ghafur et. al, A retrospective impact analysis of the WannaCry cyberattack on the NHS, NPJ Digital Medicine, 2019
111 Data protection authorities in some countries have also developed guidance on the use of technology by public authorities. An example is the Danish Data Protection Authority "Datatilsynet" who has developed guidance for public authorities on use of artificial intelligence with key considerations before technologies or developed or deployed: Offentlige myndigheders brug af kunstig intelligens: Inden I går i gang (datatilsynet.dk)
112 Especially when measures at the procurement stage alone are unlikely to be sufficient to address human rights risks identified, such as risks related to bias and discrimination.

113 See e.g. work within the EU to develop a EU model contractual AI clauses to pilot in procurements of AI | Public Buyers Community (europa.eu)
114 In other words, what should a public buyers be expected to do as a minimum, what requires support from other public bodies, and what is beyond the scope of public procurement
115 See Danish Institute for Human Rights, Driving change through public procurement, A toolkit on human rights for policy makers and public buyers (March 2020).
116 Or when procurement happens within projects, at the project planning stage.
117 See Danish Institute for Human Rights, Driving change through public procurement, A toolkit on human rights for policy makers and public buyers (March 2020).
118 For example, through ex-ante human rights impact assessments.

THE DANISH
INSTITUTE FOR
HUMAN RIGHTS