A blue text on a black background

Description automatically generated

**Privacy International’s response to the call for input to a report on the centrality of care and support from a human rights perspective by the Office of the High Commissioner for Human Rights pursuant to Human Rights Council resolution 54/6**

**April 2024**

1. **Introduction**

## Privacy International (PI)[[1]](#footnote-1) welcomes the opportunity to provide input to inform the expert workshop and the report of the Office of the High Commissioner for Human Rights (OHCHR) to the Human Rights Council, pursuant to resolution 54/6. We believe that this forthcoming report on the centrality of care and support from a human rights perspective could assess the extent to which states, companies, and other actors have implemented the recommendations contained in previous OHCHR reports on the rights of persons with disabilities in particular, as well as recommendations and findings of other relevant UN human rights experts and bodies.

In this submission, we aim to outline developments from around the world as they relate to key areas of concern that are being explored by the mandate for its report. The following sections provide PI's information and analysis of some of the topics listed in the call for submission, [[2]](#footnote-2) and in particular this submission builds on PI’s and our global partners’ research and reporting around the use of data and technology in the design, delivery and management of social protection programmes.

1. **Recommendations**

We recommend that the upcoming Report of OHCHR on care and support systems:

1. Examines the impact that growing digitisation and the use of new and emerging technologies across sectors has upon the rights of persons with disabilities;
2. Urges states to ensure that the deployment of digital technologies is in accordance with the rights of persons with disabilities, including their right to privacy and to regulate for the safe deployment of digital technologies in accordance with principles of legality, necessity and proportionality, ensuring among others specific safeguards to uphold data protection principles and preserve the rights of persons with disabilities;
3. Recognises the risks that the use of automated decision-making poses to persons with disabilities and urges states to refrain from relying on automated decision-making in the social protection context due to the dangers that the use of such technology poses including in, but not exclusive to, social protection contexts;
4. Recommends that states ensure that the use of digital technologies in social protection programmes, including digital welfare systems, does not result in exclusionary or discriminatory impacts on persons with disabilities;
5. Urges states to systematically conduct human rights due diligence, including regular comprehensive human rights and data protection impact assessments, that takes the rights of persons of disabilities into account, including before the establishment of social protection programmes or public private partnerships related to assistive technologies;
6. Recommends that global funders of social protection programmes must conduct human rights due diligence as a pre-condition to the approval of funding;
7. Urges states to adopt and enforce national data protection laws and regulatory frameworks in order to regulate and limit data processing activities, including by enhanced safeguards for sensitive data, such as health data;
8. Recalls the responsibility of all business enterprises to respect human rights, and states’ duty to protect human rights even collaborating with private companies in order to facilitate the provision of assistive technologies, products or services to persons with disabilities; and
9. Require that all public private partnership collaborations are carried out in accordance with international human rights standards, including the United Nations Guiding Principles on Business and Human Rights.
10. **The impact of digitisation and use of new technologies on persons living with disabilities**

The growth of worldwide digitisation of our societies, alongside rapid proliferation of new technologies such as information and communication technologies (ICT), has a unique and often exacerbated impact upon the rights persons with disabilities. These impacts present an array of threats to persons with disabilities’ enjoyment of their fundamental rights, with particular regard to the right to privacy, as enshrined in Article 12 of the Universal Declaration on Human rights and Article 17 of the International Covenant on Civil and Political Rights, both of which apply to all without discrimination. Equally, the UN Convention on the Rights of Persons with Disabilities (CRPD) provides explicitly for the right to privacy of persons with disabilities under Article 22, and under Article 9 of the Optional Protocol.[[3]](#footnote-3)

The significance of the context of increasing digitisation was recognised by the UN Department of Social and Economic Affairs, which stated that “*Information and communication technologies and infrastructures are rapidly growing in importance in the provision of information and services to the population*” in its proposed supplement to the Standard Rules on the Equalization of Opportunities for Persons with Disabilities, and this significance was further acknowledged during the 16th Conference of State Parties to the Convention on the Rights of Persons with Disabilities.[[4]](#footnote-4) The Department also underscored the need to ensure these technologies are made accessible to persons with disabilities.[[5]](#footnote-5)

As this submission will unpack, the use of such technologies, or indeed, participation in increasingly digital societies, must never come at the expense of persons with disabilities’ fundamental human rights.

1. **Key concerns**

Whilst it is clear that the use of new technologies as part of a wider digital transformation is having an impact on the rights of persons with disabilities, the submission will address the following three main areas of focus: (i) automated decision-making, (ii) the digitisation of social protection programmes, (iii) processing personal data of people with disabilities and (iv) assistive technologies.

1. **Automated Decision-Making**

Of all global technological developments and proliferations, a growing area of concern is the use of Artificial Intelligence (AI), with particular regard to automated decision-making (ADM) across public and private sectors.[[6]](#footnote-6) This was reflected by the decision of the mandate of the UN Special Rapporteur on the rights of persons with disabilities to dedicate their 2021 thematic report to the question of AI.[[7]](#footnote-7) While the use of AI is wide-ranging in its applications and impacts, this section will focus on social protection (e.g., welfare systems).

Indeed, the digitalisation of welfare and other public systems invariably involves a growing reliance upon ADM technologies, which are often used to determine eligibility of welfare recipients and thus have a highly significant impact upon the lives of persons with disabilities. ADM includes both semi-ADM, an algorithmic decision-making system where a human is involved in the decision-making process, and full ADM, where the decision is taken solely by the algorithmic decision-making system.[[8]](#footnote-8) Whilst this section will focus on the use of semi-ADM, references to ADM encompass both definitions unless otherwise specified.

Whilst the European Union’s General Data Protection Regulation (GDPR) (Article 22, Recital 71) provides,[[9]](#footnote-9) in relation to full ADM, for the right of individuals “*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*”,[[10]](#footnote-10) no restrictions exist for semi-ADM, making it crucial that the human review element that acts as the distinguishing characteristic between full and semi-ADM be meaningful, in order to avoid the augmented risks posed by full ADM.

For example, Amnesty International found that Dutch tax authorities “*automatically approved*” risk scores given to childcare benefit applications by an algorithmic system, rather than actually assessing the decisions taken by the ADM system.[[11]](#footnote-11) Equally, in 2016 the Wisconsin Supreme Court recognised the importance of meaningful human review when it comes to the use of semi-ADM systems when it sanctioned the COMPAS risk assessment system, which made racially discriminatory decisions. COMPAS gave automated risk scores in the criminal justice system in order to predict the likelihood of an individual committing a future crime, which was used to inform sentencing decisions by judges. The Court highlighted the insufficiency and limitations of the COMPAS tool as the sole basis for a sentencing decision, and the need for judges to take into account a series of other factors.[[12]](#footnote-12)

1. **The dangers of automated decision-making**

The risks of unreliability and bias attaching to ADM technologies powered by AI have been well documented. This is further complicated by the opacity of ADM systems which often operate as a “black box” and pose serious transparency problems, since they are extremely difficult to challenge. This in turn leads to a lack of redress and accountability mechanisms to understand how data has been used, or why a given decision has been made.

There is a recognised right not to be subjected to full ADM. According to the European GDPR (“EU GDPR”), the use of such technology requires data processors to have additional safeguards in place and that individuals should be able to opt out of ADM processes.[[13]](#footnote-13) Further, when it comes to ADM, individuals have a right to be informed of the existence of ADM and at the very least meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data subject.[[14]](#footnote-14)

In 2023, the EU Parliament expressed their concerns over the dangers of ADM when they voted on the Artificial Intelligence Act to prohibit AI systems that pose an “*unacceptable level of risk to people’s safety*”, such as “*biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation)*”.[[15]](#footnote-15) When it comes to persons with disabilities, the use of biometric information about their disability and health in ADM systems would fall under the sensitive characteristics that the EU GDPR provides for. UN mandates have also repeatedly warned of the dangers of ADM, including the UN Special Rapporteur on the right to health who acknowledged the discriminatory impacts that such technologies can have, as they “*can perpetuate […] ableism*” since “*data sets that reflect human biases, predictions based on biased data sets and automated decision-making may inadvertently result in discriminatory outcomes*” and went on to state that this may lead to the “*data invisibility*” of groups including persons with disabilities.[[16]](#footnote-16)

Moreover, the 2021 thematic report on AI by the UN Special Rapporteur on the rights of persons with disabilities discusses the “*well-known discriminatory impacts*” of AI-powered ADM, stating that: “*the risks associated with machine learning can be much more acute because of the so-called “black box” or transparency problem […] it is nearly impossible to determine, retrospectively, whether discrimination has occurred. That lack of transparency is a real barrier to the right to equal treatment of persons with disabilities*” and therefore termed it “*exceptionally difficult*” to challenge ADM practises.[[17]](#footnote-17) The Special Rapporteur also explicitly recognised the pervasive and negative impact that ADM systems can have upon the lives of persons with disabilities, including in the context of welfare systems, stating that: “*Biased data sets and discriminatory algorithms can restrict persons with disabilities from employment or benefits making them even more vulnerable to poverty and marginalization, and in ways that are more systematic and harder to detect*”.[[18]](#footnote-18)

1. **The digitisation of social protection and impacts on the privacy of persons living with disabilities**

The pernicious threat that the digitisation of global welfare systems poses to human rights has been well-documented.[[19]](#footnote-19) The wake of the Covid-19 crisis saw a further proliferation of digital welfare systems which were rapidly developed and rolled out as emergency responses across the globe, with governments increasingly relying on automated and opaque eligibility processes and forsaking privacy considerations and inclusion.[[20]](#footnote-20) Such systems, which are either already in place or in emergence in many countries around the world, present unique threats to the rights of persons with disabilities.

Indeed, in his 2019 report, the UN Special Rapporteur on extreme poverty and human rights recognised the impact that digital welfare has on persons with disabilities specifically, remarking that, “*the digital welfare state often seems to involve various forms of rigidity and the robotic application of the rules*”, and going on to note that extenuating circumstances that may result from a disability “*are often not taken into account in a predominantly digital context*” by these systems.[[21]](#footnote-21) The importance of adopting a rights-based approach was explicitly addressed by the UN Special Rapporteur on the rights of persons with disabilities in 2017, where she stated: *“[a]ll support services and arrangements must be […] designed to respect the privacy of those concerned*”.[[22]](#footnote-22) Equally, in 2023 the mandate once again warned that although advances in technology present opportunities for realising the rights of persons with disabilities, there are serious risks that accompany them.[[23]](#footnote-23)

1. **The impact of automated decision-making on human rights in digital welfare systems**

The serious risks posed to fundamental rights which accompany ADM in the context of social protection are widely recognised.[[24]](#footnote-24) Current and emerging AI-supported ADM processes to access social welfare are designed and managed in a way that comes at the cost of everyone’s privacy, dignity and autonomy.

From the stage of eligibility and registration to access benefits, recipients need to turn over vast amounts of personal (and often sensitive) data – including about their employment, health conditions, and relationship status – which is processed by AI applications to make (or support the making of) decisions related to access to social welfare benefits.[[25]](#footnote-25)

Concerns about the negative impact of the use of AI applications in the welfare context have already been expressed by UN human rights experts[[26]](#footnote-26) and national courts are beginning to rule against these systems on the grounds that they fail to comply with human rights law.[[27]](#footnote-27) Some of these concerns include but are not limited to:

* **Discrimination:** There have been various examples of discriminationbased on nationality and racial profiling, including in the ADM fraud-detection system adopted by Dutch tax authorities[[28]](#footnote-28) and the workings of the City of Rotterdam’s welfare fraud algorithm.[[29]](#footnote-29) These examples provide evidence that the use of protected characteristics and sensitive personal data about a person by an algorithm can lead to conclusions that are biased and discriminatory.
* **Lack of transparency:** As noted above, the opacity of ADM systems is of concern and in a welfare context it means that it is impossible to ascertain how individuals’ eligibility or lack of eligibility is being decided. This is what we saw play out with the roll-out of Colombia’s Solidarity Income (“Ingreso Solidario”) during the Covid-19 pandemic, where selected beneficiaries were notified of their entitlement by way of SMS messages based on prior information held by the Colombian government and in the absence of publicly available eligibility criteria or guidelines.[[30]](#footnote-30) Similarly Nigeria’s COVID-19 Cash Transfer Project[[31]](#footnote-31) and Angola’s KWENDA Covid-19 digital social protection programmes[[32]](#footnote-32) were not made public.

These concerns were addressed in detail in the OHCHR report on AI, which outlined recommendations for governments and companies to adopt urgently underscoring “*that only a comprehensive human rights-based approach can ensure sustainable solutions to the benefit of all*”.[[33]](#footnote-33) The report also highlighted that particular attention should be paid to the disproportionate impacts of the use of AI on persons with disabilities.[[34]](#footnote-34)

1. **Welfare systems’ ADM impact upon persons with disabilities**

The use of ADM in digital welfare systems poses a unique threat to the rights of persons with disabilities, including their right to privacy. There is a risk that the use of ADM in such a context fails to comply with core data protection principles including purpose limitation, transparency, accuracy and accountability. Below we outline some examples.

*The Allegheny Family Screening Tool*

One case in point which illustrates the dangers that ADM use in welfare systems can pose to the rights of persons with disabilities specifically, took place in Allegheny County, Pittsburgh, USA. In March 2023, it was reported than opaque ADM-driven child welfare services tool, "the Allegheny Family Screening Tool", used by the Allegheny County Department of Human Services to predict risks of harm to children, discriminated against persons with disabilities, leading in one case to child services taking two disabled parents' baby daughter into foster care as they were flagged as a risk to their child.[[35]](#footnote-35)

The algorithmic ADM tool "*tracked whether parents were ever on public benefits*", which it used as proxy data to ascertain whether "*parents or other children in the household have disabilities, by noting whether any family members received Supplemental Security Income, a federal benefit for people with disabilities*.".[[36]](#footnote-36) The data fields underpinning the ADM algorithm calculating risk included disability status and there was no way for disabled parents to appeal or challenge the "risk score" given to them. The U.S. Justice Department has launched an investigation into the county's child welfare system to determine whether it discriminates against people with disabilities.[[37]](#footnote-37)

*The UK Department of Work and Pensions*

PI’s research[[38]](#footnote-38) revealed that the UK’s Department of Work and Pensions (DWP) makes it an explicit objective to assess whether someone who is claiming disability benefits is, in fact, disabled, stating: “*The most important aspect of an investigation into disability benefits is understanding exactly what the customer has declared they can and cannot do, and gathering evidence which either proves or disproves their statement*”.[[39]](#footnote-39) The guidelines encourage the use of surveillance to this end, commenting that: “*Surveillance should be used to obtain evidence of a person’s physical capability and in some cases their mental capability too*”, and specifically provides for “*Surveillance teams” and “Surveillance Officer[s]”* who may carry out such work.[[40]](#footnote-40)

Compounding the threat that such policies pose to the rights of persons with disabilities are the propensity of computer algorithms to discriminate against them. Indeed, the DWP is facing legal action by a disability rights group regarding the algorithm used to flag particular individuals as ‘fraud risks’, on the basis that it is unfair and discriminatory.[[41]](#footnote-41) By profiling individuals who interact with caseworkers and the DWP on the basis of unknown data points, the DWP is creating derived, inferred, and predicted profiles which may be inaccurate or systematically biased. This type of profiling can lead to individuals being misidentified, misclassified, or misjudged.[[42]](#footnote-42) Without a concrete understanding of how specific data points are being used by the DWP to assess whether welfare claims are legitimate or not, the systems being developed will continue to pose a serious risk to the social welfare system as a whole and persons with disabilities’ human rights.

*Serbia’s Social Card Law*

Similarly, the Serbian government employ an ADM system for their Social Card system, underpinned by a Social Card Law introduced in March 2022. The law’s introduction led to a joint legal complaint being filed by NGOs who called for the law’s roll-out to be halted and a full assessment of whether the legislation complies with the country’s obligations under human rights law, due to it being an “*intrusive surveillance system that could harm the most marginalized members of society*”,[[43]](#footnote-43) including persons with disabilities who represent a notable portion of individuals in receipt of social support, as the ADM system assesses their eligibility for receiving state benefits under the Social Card system.[[44]](#footnote-44)

### The responsibility of global institutions as funders and implementers

Global institutions play a key role in the funding, design, and implementation of social protection programmes. In some cases, it is not clear whether global institutions systematically account for the risks associated with data-intensive and tech-reliant social safety-net programmes as we recently documented with regards to eight Covid-19 Response projects funded by the World Bank in Nigeria, Haiti, Mozambique, Sierra Leone, Angola, Morocco, Jordan and Lebanon.[[45]](#footnote-45)

Given the risks identified in relation to ADM systems and people with disabilities, it is essential that funders and implementers exercise due diligence to ensure that they are not building or entrenching systems with discriminatory features.

In instances where global institutions are the funder, they should be requiring as part of conditions of funding that the relevant legal frameworks be in place before a digital welfare programme is rolled out, and to make the existence and effective enforcement of these safeguards a pre-condition for approving funding.

**(iii) Effectively regulating the processing of data of persons with disabilities**

The need for limiting data collection and ensuring transparency in data processing, is of particular importance to ensure that persons with disabilities do not face discrimination and rights violations when accessing public services, using products and benefiting from social protection.

The importance of observing data protection principles in order to uphold the right to privacy is supported by Article 31 of the CRPD on statistics and data collection, which obliges member-states to “*Comply with legally established safeguards, including legislation on data protection, to ensure confidentiality and respect for the privacy of persons with disabilities*” and further to “*Comply with internationally accepted norms to protect human rights and fundamental freedoms and ethical principles in the collection and use of statistics*”. Equally, the UN Committee on Rights of Persons with Disabilities has recognised the importance of said data protection principles in its recommendations to states, including to Estonia in April 2021 where it called upon the state to “*Develop a system and procedures for collecting data on persons with disabilities […] [which] should ensure confidentiality and respect the privacy of persons with disabilities*”.[[46]](#footnote-46)

These internationally accepted norms and principles when it comes to data protection of persons with disabilities should be robustly incorporated by states in their national legislations, including national data protection legislation. Should states fail to do so, they risk exposing some of their most vulnerable citizens to rights violations, particularly the right to privacy.

For example, in 2022 PI relayed findings on emergency social protection in Mozambique, which found that as well as lack of transparency in the cash-transfer programme itself, throughout its roll-out there were reports of benefit claimants being subjected to intimidation, threats and harassment over the phone by individuals demanding they hand over the phone(s) to which the benefit was linked. It remains unclear how beneficiaries’ phone numbers got into the hands of these individuals.[[47]](#footnote-47)

Below we outline key issues that have emerged in the context of data processing of data of personal with disabilities that require further attention to ensure that their rights and data are protected.

1. **Processing of sensitive personal data and need for enhanced safeguards**

International data protection frameworks categorise data revealing health conditions as sensitive personal data.[[48]](#footnote-48) Insofar as information related to a person’s disability may be considered health data, this information is subjected to higher privacy safeguards.

This is a core principle of data protection, recognised in Article 6 of Convention 108, which stipulates that such data “may not be processed automatically unless domestic law provides appropriate safeguards”[[49]](#footnote-49). National data protection laws adopted the world over similarly impose additional safeguards as a pre-condition to the processing of health data.

Generally, the processing of data from persons with disabilities should occur only where necessary to achieve the purpose for which they have been collected. Where this data concerns their disability it must be subject to enhanced safeguards to regulate the collection and processing of such data due to its sensitive nature.

1. **Data minimisation**

The data minimisation principle requires that any entity, public or private, must only process the minimum amount of data necessary is to achieve the specific and legitimate purpose of collection.[[50]](#footnote-50)

There have been well-documented concerns that our devices, systems, and infrastructure process vast and excessive amounts of personal data,[[51]](#footnote-51) often without a clear purpose and without robust application of safeguards including for example the protection of security and integrity of devices and data.[[52]](#footnote-52) These concerns have led to disability groups calling for better privacy protections for persons living with disabilities given not only the increasing amount and diversity of data being processed, but also how data, that may not be disability data specifically can reveal and identify persons living with disabilities.[[53]](#footnote-53)

Minimising the data collected from persons with disabilities is key to ensuring that their right to privacy is upheld and minimising the risks to people and their rights by reducing the attack surface to which they may be subject.[[54]](#footnote-54)

1. **Purpose limitation**

Any data processing should occur for a determined, specific, and legitimate purpose. Any further processing must not be incompatible with the purposes specified at the outset (i.e. the point of collection). Indiscriminate data collection must not occur, but data collected must be for a specific and clearly defined purpose.[[55]](#footnote-55)

We are concerned by the practices we have observed of states’ indiscriminate or widespread collection of data to assess eligibility of social support claimants and subject them to surveillance or fraud detection, as outlined in examples contained within section 4.ii.b. of this submission, and which poses a particular threat to the right to privacy of persons with disabilities, as well as other rights such as their right to non-discrimination.

1. **Legal basis**

Any processing of data of persons with disabilities should rely on an appropriate legal basis provided by law. There are multiple legal bases that can apply, independently or simultaneously, to the processing of health data of people with disabilities.

The CRPD requires states to collect appropriate information, including disaggregated statistical and research data, to enable them to give effect to the Convention.[[56]](#footnote-56) This in itself constitutes a legal basis for processing as it entails a state’s own compliance with its legal obligations.

Additionally, Convention 108 accepts as valid legal bases the free, specific and informed consent of data subjects, or any other legitimate basis laid down by law.[[57]](#footnote-57) In its explanatory report, the Convention contemplates several other purposes as a lawful basis for processing, ranging from the fulfilment of contractual or legal obligations to the protection of a person’s vital interests.[[58]](#footnote-58) As stated above, the processing of sensitive data, such as health data, requires additional safeguards. Some of the additional requirements set by legal frameworks in this context as a pre-requisite to processing include,[[59]](#footnote-59) among others, explicit consent, or necessity in the field of employment or social security, where a substantial public interest is concerned, or in a health or social care environment.[[60]](#footnote-60)

Legal frameworks require for that legal basis to be communicated to data subjects prior to or at the time of processing, alongside the categories of data processed, the recipients of such data, and the means for them to exercise their rights.[[61]](#footnote-61)

Clearly stating the legal bases for the processing of any personal data is crucial for a data subject to be able to exercise their rights. Where the basis purports to be free and informed consent, it is key that the dignity, autonomy and needs of persons with disabilities are respected.[[62]](#footnote-62)

1. **Upholding the right to privacy when accessing assistive technologies**

The right to privacy of persons with disabilities is of particular importance when it comes to accessing Assistive Technologies (ATs), including assistive products and services, and medical assistive devices. This is not an exhaustive list but below we outline a few areas of concern that PI and others have observed.

* 1. **The involvement of the private sector and private-public partnerships**

When contracting private entities to facilitate access to ATs to persons with disabilities, states must comply with their obligation to protect against abuses by non-state actors and responsibilities of the private sector, including the technology industry,[[63]](#footnote-63) under UN Guiding Principles on Business and Human Rights.[[64]](#footnote-64) The privatisation of public responsibilities can be deeply problematic if deployed without the safeguards required to ensure human rights are protected.

For this reason, PI has developed a set of recommended safeguards which should be adopted when engaging in public-private partnerships related to surveillance technologies and data processing, which encourage centring transparency, proper procurement, legality, accountability, oversight and redress in these partnerships. We urge the Office to integrate these safeguards to the recommendations towards states and companies in its upcoming report.[[65]](#footnote-65)

It is true that new technologies, including AI, can assist in the personalisation of services and may have enormously beneficial potential for many persons with disabilities, as recognised by the World Health Organisation in 2023 who stated: “*Without assistive technology, people are often excluded, isolated, and locked into poverty, thereby increasing the impact of disease and disability on a person, their family, and society*”.[[66]](#footnote-66) That being said, it is critical ensure that such technologies do not come at the expense of the human touch and their use does not infringe upon fundamental rights, including the right to privacy. The risk that data collected by the private sector from persons with disabilities via their use of ATs may be exploited, or abused, has been brought to PI’s attention informally by Organisations of Persons with Disabilities (OPDs). The OPDs in question expressed concern at the intrusive level of seemingly irrelevant personal information that persons with disabilities are required to input into a given AT as a pre-condition in order to access and use said AT product or service.[[67]](#footnote-67)

* 1. **Safety of assistive products and devices**

The importance of protecting the right to privacy in the context of AT use is reflected in the EU Accessibility Act (Directive 2019/882) which stipulates that products must “protect the user’s privacy when he or she uses the accessibility features” and that products or services incorporating accessibility features “shall provide at least one mode of operation that maintains privacy when using those features that are provided for accessibility”.[[68]](#footnote-68)

Furthermore, the EU Parliamentary Research Service have argued for a privacy-by-design approach when it comes to ATs for persons with disabilities due to the risk they pose to the right to privacy, stating in their 2018 publication “Assistive technologies for people with disabilities*”* that, “*the European Data Protection Supervisor might have to adopt a series of initiatives in order to address the relevant privacy risks*”.[[69]](#footnote-69) The publication further identifies that ATs pose a unique threat to the right to privacy of persons with disabilities due to these technologies’ “access to traditionally protected spaces and sensitive personal information” and their “capacity to extract, collect and share sensitive information independently”. It further states that the use of ATs could result in “unwanted supervision” that might take place without the person being aware.[[70]](#footnote-70)

In light of these risks, the EU Parliamentary Research Service stresses that user privacy must be taken into account to ensure patient safety, and that users must be informed and given agency over how their information is processed and stored by ATs, stating that they should be provided with, “*options to prevent data archiving, delete historical data, and amend incorrect or misinterpreted data over the lifespan of the robot […]*”. In addition, their report stresses “*the process by which robots and artificial intelligence collect, use and process personal data must be transparent and comprehensible. Users should be able to understand fully the extent of monitoring, including how data are gathered and processed, by whom, for what purpose, for how long and where they are stored, and with whom they are or can be shared*”.[[71]](#footnote-71)

1. Privacy International (PI) is a London-based non-profit, non-governmental organization (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples’ personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development and the UN Refugee Agency. [↑](#footnote-ref-1)
2. United Nations Office of the High Commissioner for Human Rights (OHCHR), “Subject: Human Rights Council resolution 49/12” (2023) <https://www.ohchr.org/sites/default/files/documents/issues/disability/cfi-hrc-49-12-disability/Note-Verbale-Res-49-12-States-EN.pdf> [↑](#footnote-ref-2)
3. UN Convention on the Rights of Persons with Disabilities (CRPD), Article 22; Optional Protocol to the UN CRPD, Article 9. [↑](#footnote-ref-3)
4. United Nations Department of Economic and Social Affairs, “Reaching the most vulnerable: proposed supplement to the Standard Rules on the Equalization of Opportunities for Persons with Disabilities [Annex E/CN.5/2004/4]” (2004) <https://www.un.org/development/desa/disabilities/resources/reaching-the-most-vulnerable-proposed-supplement-to-the-standard-rules-on-the-equalization-of-opportunities-for-persons-with-disabilities-annex-ecn-520044.html#f>

   See also: United Nations, Conference of State Parties to the Convention of the Rights of Persons with Disabilities (COSP 16) (2023) <https://indico.un.org/event/1004737/> [↑](#footnote-ref-4)
5. United Nations Department of Economic and Social Affairs “Reaching the most vulnerable: proposed supplement to the Standard Rules on the Equalization of Opportunities for Persons with Disabilities [Annex E/CN.5/2004/4]” (2004) <https://www.un.org/development/desa/disabilities/resources/reaching-the-most-vulnerable-proposed-supplement-to-the-standard-rules-on-the-equalization-of-opportunities-for-persons-with-disabilities-annex-ecn-520044.html#f> [↑](#footnote-ref-5)
6. A/HRC/48/31 [↑](#footnote-ref-6)
7. ## UN Special Rapporteur on the rights of persons with disabilities “A/HRC/49/52: Artificial intelligence and the rights of persons with disabilities - Report of the Special Rapporteur on the rights of persons with disabilities” (December 2021) <https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F49%2F52&Language=E&DeviceType=Desktop&LangRequested=False>

   [↑](#footnote-ref-7)
8. Amnesty International, “Glossary” in “Xenophobic machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal” (2021) <https://www.amnesty.org/en/documents/eur35/4686/2021/en/> [↑](#footnote-ref-8)
9. General Data Protection Regulation (‘GDPR’), Article 22 and Recital 71. [↑](#footnote-ref-9)
10. GDPR, Recital 71 “Profiling”, <https://eur-lex.europa.eu/eli/reg/2016/679/oj/> [↑](#footnote-ref-10)
11. Amnesty International, “Xenophobic machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal”, p. 15 (2021) <https://www.amnesty.org/en/documents/eur35/4686/2021/en/> [↑](#footnote-ref-11)
12. *Loomis v. Wisconsin*, 881 N.W.2d 749 (2016). [↑](#footnote-ref-12)
13. For example, EU GDPR Article 22 provides rights in relation to solely automated decisions which have legal or other significant effects, stating: “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling […]”.

    See also: Convention 108+, <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> [↑](#footnote-ref-13)
14. Privacy International “The Keys to Data Protection” (August 2018) <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf> [↑](#footnote-ref-14)
15. European Parliament, “MEPs ready to negotiate first-ever rules for safe and transparent AI” (June 2023) <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai> [↑](#footnote-ref-15)
16. UN Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health “Digital innovation, technologies and the right to health”, para.s. 11, 82, (2023) <https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F53%2F65&Language=E&DeviceType=Desktop&LangRequested=False> [↑](#footnote-ref-16)
17. UN Special Rapporteur on the rights of persons with disabilities, “Rights of persons with disabilities” (2021) <https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F49%2F52&Language=E&DeviceType=Desktop&LangRequested=False> [↑](#footnote-ref-17)
18. UN Special Rapporteur on the rights of persons with disabilities, “Artificial intelligence and the rights of persons with disabilities” (2021) <https://srdisability.org/thematic-reports/artificial-intelligence-and-the-rights-of-persons-with-disabilities/> [↑](#footnote-ref-18)
19. Privacy International, “When Big Brother Pays Your Benefits” https://privacyinternational.org/taxonomy/term/675

    See also: Centre for Human Rights and Global Justice, “Digital Welfare State and Human Rights Project” <https://chrgj.org/focus-areas/technology/digital-welfare-state-and-human-rights-project/>

    See also: Human Rights Watch, “The disastrous roll-out of the UK's digital welfare system is harming those most in need” (2019) <https://www.hrw.org/news/2019/06/10/disastrous-roll-out-uks-digital-welfare-system-harming-those-most-need> [↑](#footnote-ref-19)
20. Privacy International, “Emergency Social Protection responses to Covid-19 around the world” <https://privacyinternational.org/long-read/4882/emergency-social-protection-responses-covid-19-around-world> [↑](#footnote-ref-20)
21. UN Special Rapporteur on extreme poverty and human rights, “Extreme poverty and human rights” (2019) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/312/13/PDF/N1931213.pdf?OpenElement> [↑](#footnote-ref-21)
22. UN Special Rapporteur on the rights of persons with disabilities, “Report of the Special Rapporteur on the rights of persons with disabilities”, p. 13, (2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/436/64/PDF/G1643664.pdf?OpenElement> [↑](#footnote-ref-22)
23. UN Special Rapporteur on the rights of persons with disabilities, “Transformation of services for persons with disabilities”, p. 15. (2022) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/613/79/PDF/G2261379.pdf?OpenElement> [↑](#footnote-ref-23)
24. In 2019, the UN Special Rapporteur on extreme poverty and human rights dedicated the mandate’s thematic report to outlining the risks of the digital welfare state. See:

    UN Special Rapporteur on extreme poverty and human rights, “Extreme poverty and human rights” (2019) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/312/13/PDF/N1931213.pdf?OpenElement> [↑](#footnote-ref-24)
25. Privacy International, “When Big Brother Pays Your Benefits” <https://privacyinternational.org/taxonomy/term/675> [↑](#footnote-ref-25)
26. UN Special Rapporteur on extreme poverty and human rights, “Report of the Special rapporteur on extreme poverty and human rights” (2019) <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiSmbDi0beAAxVIP-wKHZ8DB1gQFnoECB8QAQ&url=https%3A%2F%2Fwww.ohchr.org%2FDocuments%2FIssues%2FPoverty%2FA_74_48037_AdvanceUneditedVersion.docx&usg=AOvVaw1jRH0rb0geojazfZCC8f3V&opi=89978449> [↑](#footnote-ref-26)
27. In a landmark ruling, a Dutch has now concluded that the use of SyRI is unlawful as it violates the right to

    privacy. The court found that the Dutch government had failed to strike a balance between the right to

    privacy and the public interest in detecting welfare fraud, and that the use of SyRI was disproportionate to

    the aim it sought to achieve.

    See: Privacy International, “The SyRI case: a landmark ruling for benefits claimants around the

    world” (2020) <https://privacyinternational.org/news-analysis/3363/syri-case-landmark-ruling-benefits-claimants-around-world> [↑](#footnote-ref-27)
28. Amnesty International, “Xenophobic machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal” (2021) <https://www.amnesty.org/en/documents/eur35/4686/2021/en/> [↑](#footnote-ref-28)
29. Eva Constantaras, Gabriel Geiger, Justin-Casimir Braun, et. al., “Inside the Suspicion Machine” (2023) <https://www.wired.com/story/welfare-state-algorithms/> [↑](#footnote-ref-29)
30. Privacy International, “The Case of the Solidarity Income in Colombia: the experimentation with data on social policy during the pandemic” (March 2021) <https://privacyinternational.org/long-read/4473/case-solidarity-income-colombia-experimentation-data-social-policy-during-pandemic> [↑](#footnote-ref-30)
31. Privacy International “Emergency Social Protection responses to Covid-19 around the world” <https://privacyinternational.org/long-read/4882/emergency-social-protection-responses-covid-19-around-world> [↑](#footnote-ref-31)
32. [Ibid.](https://privacyinternational.org/long-read/4882/emergency-social-protection-responses-covid-19-around-world) [↑](#footnote-ref-32)
33. United Nations High Commissioner for Human Rights, “The right to privacy in the digital age” (2021) <https://daccess-ods.un.org/tmp/4240980.44633865.html> [↑](#footnote-ref-33)
34. Ibid, para 49. [↑](#footnote-ref-34)
35. Sally Ho and Garance Burke “Here’s how an AI tool may flag parents with disabilities” in AP News, (2023) <https://apnews.com/article/child-protective-services-algorithms-artificial-intelligence-disability-02469a9ad3ed3e9a31ddae68838bc76e> [↑](#footnote-ref-35)
36. Ibid. [↑](#footnote-ref-36)
37. Sally Ho and Garance Burke, “Child welfare algorithm faces Justice Department scrutiny” (2023) <https://apnews.com/article/justice-scrutinizes-pittsburgh-child-welfare-ai-tool-4f61f45bfc3245fd2556e886c2da988b> [↑](#footnote-ref-37)
38. Privacy International, “Shedding light on the DWP Part 1” <https://privacyinternational.org/long-read/4395/shedding-light-dwp-part-1-we-read-uk-welfare-agencys-995-page-guide-conducting> [↑](#footnote-ref-38)
39. UK Department for Work and Pensions, “Fraud investigations: staff guide ”, pp. 275-6 (2012) <https://www.gov.uk/government/publications/fraud-investigations-staff-guide> [↑](#footnote-ref-39)
40. Ibid. [↑](#footnote-ref-40)
41. # GMCPD, “GMCDP & Foxglove Legal Challenge to the Department for Work and Pensions DWP Fraud Algorithm” <https://gmcdp.com/gmcdp-foxglove-legal-challenge-department-work-and-pensions-dwp-fraud-algorithm>

    See also: Greater Manchester Law Centre, “Algorithmic injustice: an interview with Rick Burgess from GMCDP” (2022) <https://www.gmlaw.org.uk/2022/03/31/algorithmic-injustice-an-interview-with-rick-burgess-from-gmcdp/> [↑](#footnote-ref-41)
42. Privacy International, “Data is Power: Profiling and Automated Decision-Making in GDPR” (2017) <https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf> [↑](#footnote-ref-42)
43. Amnesty International, “Serbia: Social Card law could harm marginalized members of society – legal opinion” (2022) <https://www.amnesty.org/en/latest/news/2022/11/serbia-social-card-law-could-harm-marginalized-members-of-society-legal-opinion/> [↑](#footnote-ref-43)
44. Privacy International, “The Keys to Data Protection” (August 2018) <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai> [↑](#footnote-ref-44)
45. # Privacy International, “The World Bank & social protection during crises: a privacy trade-off?” (2022) <https://privacyinternational.org/long-read/4944/world-bank-social-protection-during-crises-privacy-trade>

    [↑](#footnote-ref-45)
46. Committee on the Rights of Persons with Disabilities, “Concluding observations on the initial report of Estonia” (2021) <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhslxq2MulDp%2FqMKQ6SGOn0%2FMA1LSpvgYM3DCkpjGjvUUy2myJFM%2BOsTgWsCuGm4B2qohcBwHoCCrB5BpbRCKf6tkvX63EJgdwjV2NmUEVRnVD> [↑](#footnote-ref-46)
47. Privacy International, “The World Bank & social protection during crises: a privacy trade-off?” (August 2022) https://privacyinternational.org/long-read/4944/world-bank-social-protection-during-crises-privacy-trade [↑](#footnote-ref-47)
48. Convention 108+, Article 6. [↑](#footnote-ref-48)
49. Convention 108+. [↑](#footnote-ref-49)
50. Council of Europe Convention 108, Article 5(4)(c); EU GDPR, Article 5(1)(c). [↑](#footnote-ref-50)
51. European Commission, Article 29 Working Party, ‘Opinion 02/2013 on Apps on Smart Devices’ (n 101) (2013) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202\_en.pdf;

    See also: Privacy International, “Internet of Things” https://privacyinternational.org/learn/internet-things [↑](#footnote-ref-51)
52. Privacy International, “Best Before Date for our devices” <https://privacyinternational.org/campaigns/best-before-date-our-devices-campaign> [↑](#footnote-ref-52)
53. Centre for Democracy and Technology et. al, Letter to Nansi Pelosi (2022) <https://cdt.org/wp-content/uploads/2022/08/2022-08-25-ADPPA-Disability-Rights-Groups-Letter-to-Pelosi.pdf> [↑](#footnote-ref-53)
54. Stanislaw Piasecki , Jiahong Chen “Complying with the GDPR when vulnerable people use smart devices”, International Data Privacy Law, Volume 12, Issue 2, Pages 113–131, (May 2022) <https://doi.org/10.1093/idpl/ipac001> [↑](#footnote-ref-54)
55. Convention 108, Article 5(4)(b); EU GDPR, Article 5(1)(b). [↑](#footnote-ref-55)
56. CRPD, Article 31. [↑](#footnote-ref-56)
57. Convention 108+, Article 5(2). [↑](#footnote-ref-57)
58. Convention 108+, Explanatory Report, para. 46. See also EU GDPR, Article 6. [↑](#footnote-ref-58)
59. GDPR, Article 9. [↑](#footnote-ref-59)
60. Ibid. [↑](#footnote-ref-60)
61. Convention 108+, Article 8. [↑](#footnote-ref-61)
62. CRPD, Article 25(d). [↑](#footnote-ref-62)
63. Application of the UN Guiding Principles to the technology industry was reaffirmed by the UN High Commissioner for Human Rights in the OHCHR’s B-Tech Foundational Paper on The UN Guiding Principles in the Age of Technology, <https://www.ohchr.org/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf> [↑](#footnote-ref-63)
64. UN Human Rights Council Resolution, “Human Rights and transnational corporations and other business enterprises” (2011) <https://undocs.org/en/A/HRC/RES/17/4> [↑](#footnote-ref-64)
65. Privacy International, “Safeguards for Public-Private Surveillance Partnerships” (2021) https://privacyinternational.org/sites/default/files/2021-12/PI PPP Safeguards [FINAL DRAFT 07.12.21].pdf [↑](#footnote-ref-65)
66. World Health Organization, “Assistive technology” (2023) <https://www.who.int/news-room/fact-sheets/detail/assistive-technology> [↑](#footnote-ref-66)
67. PI’s informal conversations with representatives of Organisations of Persons with Disabilities, European Accessibility Summit 2023.

    See also: European Disability Forum, “European Accessibility Summit 2023” (2023) <https://www.edf-feph.org/events-slug/european-accessibility-summit-2023/> [↑](#footnote-ref-67)
68. European Parliament, “Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance)”, Annex 1, 2(k), (2019) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0882> [↑](#footnote-ref-68)
69. European Parliamentary Research Service, “Assistive Technologies for people with disabilities | Part IV: Legal and socio-ethical perspective”, p. 17 (2018) <https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/603218/EPRS_IDA(2018)603218(ANN4)_EN.pdf> [↑](#footnote-ref-69)
70. Ibid. [↑](#footnote-ref-70)
71. Ibid. [↑](#footnote-ref-71)